Predict | Protect | Prevent

ARCON|PAM

Administrative Guide | Version 4.8.5.0_U16

arcon

Table of Contents

1 About this Manual

This user manual is a comprehensive documentation for those wanting to get the most out of ARCON PAM (Privileged Access Management). It combines step–by–step instructions to help you accomplish specific tasks with detailed description of each feature of the application.

1.1 Disclaimer

This Manual of ARCON PAM solution is being published to guide administrators with the step-by-step procedures involved in configuring, monitoring, and managing ARCON PAM.

The manual is in the nature of a guide for the users and if any of the statements in this document are at variance or inconsistent it shall be brought to the notice of ARCON PAM through the support team. Wherever appropriate, references have been made to facilitate better understanding of the PAM solution. The ARCON PAM team has made every effort to ensure that the information contained in it was correct at the time of publishing.

This Manual of ARCON PAM solution contains information, which is the intellectual property of ARCON PAM. This document is received in confidence and its contents cannot be disclosed or copied without the prior written consent of ARCON PAM.

Nothing in this document constitutes a guaranty, warranty, or license, expressed or implied. ARCON PAM disclaims all liability for all such guaranties, warranties, and licenses, including but not limited to: Fitness for a particular purpose; merchantability; non-infringement of intellectual property or other rights of any third party or of ARCON PAM; indemnity; and all others. The reader is advised that third parties can have intellectual property rights that can be relevant to this document and the technologies discussed herein, and is advised to seek the advice of competent legal counsel, without obligation of ARCON PAM.

1.2 Copyright Notice

ARCON PAM retains the right to make changes to this document at any time without notice. ARCON PAM makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein.

1.3 Trademarks

Other product and corporate names may be trademarks of other companies and are used only for explanation and to the owners' benefit, without intent to infringe.

1.4 Related Documents

Below are the related documents, which help to understand the **ARCON PAM** in detail

- **ARCON PAM Overview Guide** gives the overview of ARCON Privilege Access Management.
- **ARCON PAM Installation & Configuration Guide** describes how to prepare the environment, install, and configure the ARCON Privilege Access Management Solution.

- **ARCON PAM Privileged Access Management (PAM) User Guide** describes the features, benefits, functionalities.
- **ARCON PAM Set-up Pre-requisite** describes the hardware and software required for deployment of ARCON PAM in the user environment.
- **ARCON PAM Troubleshoot** provides the basic information for ARCON PAM issues.
- **ARCON PAM Client Manager Guide** describes a web console which supports multi-domain authentication, dual factor authentication, multi-tenancy and target connectors.

1.5 Target Audience

This guide is intended for auditors, consultants and security experts responsible for securing, auditing and monitoring server administration processes; especially remote server management. It is also useful for IT decision makers seeking for a tool to improve the security and auditing of their servers or to facilitate compliance to the unique standard.

The following skills and knowledge are necessary for a successful ARCON PAM administrator:

- Basic system administration knowledge.
- Basic understanding of networks, TCP/IP protocols, and general network terminology.
- Working knowledge of the Windows operating system is not mandatory, but highly useful.
- In-depth knowledge of various servers and server applications is required for forensics situations.

1.6 Symbols and Conventions

The Following are the symbols and conventions used in this manual:

Symbols	Description
Note :Note_icon:	Indicates helpful tips, shortcuts, and suggestions.
Information :Information_icon:	Indicates additional information.

This manual uses the following conventions to refer to sections, navigation, and other information.

Convention	Description
Bold	Keywords and menu names are displayed in bold.

1.7 Acronyms

The acronyms used in this manual are as follows:

Acronyms	Description
PAM	Privileged Access Management
SM	Server Manager
CM	Client Manager
LOB	Line of Business

Acronyms	Description
SSH	Secure Shell
RDP	Remote Desktop Protocol
OTP	One Time Password
DB	Database
EPAM	Enterprise Privilege Access Management
PVSL	Password Vault & Session Logging
SGS	Secure Gateway Server

1.8 POC (Point of Contacts) & Support Information

The product is developed and maintained by **ARCON PAM TechSolutions Private Limited**. We at ARCON are continuously thriving to develop and deliver the best quality products. Being our valued customer, we would like to know your feedback, suggestions and ideas for improvements with regards to our products and services. You can always reach out to us through the below ways of communication:

Web

https://arconnet.com/

Sales Contact

You can directly contact us with sales related topics at the email address *sales@arconnet.com*, or leave us your contact information and we will call you back.

Support Contact

To access ARCON PAM Support Centre (ASC), Sign in with your account.

- Remote support is available 24*7.
- ARCON PAM Support System is available only for registered users with a valid support package.
- ARCON PAM Support Centre (ASC): *https://support.arconnet.com/*
- Central Support E-mail Address: *arcos.support@arconnet.com*
- Support hotline:
    - Global: +91 8080005577 (For ARCON PAM Support Press 3)
    - UAE: 800035703628 (Press 1)

2 Overview

The Server Manager is the core of the application and is developed to provide an easy to configure a organization structure within the application. This in turn will help in structuring the operations within the data center for various teams as well as cross functional teams such as the application support teams. It provides the privilege control module i.e. access control features for various operating systems, databases and networking devices. These features are easy to use and configurable for groups or users for specific devices. It also includes both black-listing as well as white-listing of commands.

The key feature offered by SM is the session monitoring and command logging functions. There is a complete audit trail of the actions performed by any shared privilege user mapped to the end user as well as his machine or device from where the access is established. The session monitoring is available in various formats such as txt, jpg, avi. The commands captured are real time. The reports and analytical tools available further helps to capture the audit trails and showcase the outputs in an easy to understand format thereby improving decision making for an organization.

The Privilege Password Manager in SM offers a readily configurable password policy profiler and a password generator, where the passwords generated are unique. The passwords generated are updated on the end devices including dependencies, if any, such as services, tasks, scripts etc. These passwords are stored in an electronic vault, which are completely encrypted. The Electronic vault has release request workflow including secured printing. In addition, there is a 'password sync' module to conduct live reconciliation of privilege users and passwords on target devices which are out of sync. It can also identify privilege accounts on the target devices which are not integrated in ARCON PAM.

Server Manager helps to administer, manage, and monitor privilege identities and servers across the organization. In addition, all the actions performed by any application support engineer on the databases including queries are also logged in SM.

The following sections are covered in detail under SM:

- Login Management
- Entity Management and Mapping
- Privilege Management
- Password Management
- Command Profiler
- Scheduler
- Workflow Management
- Log Management
- Tool Management
- Settings

3 Login Management

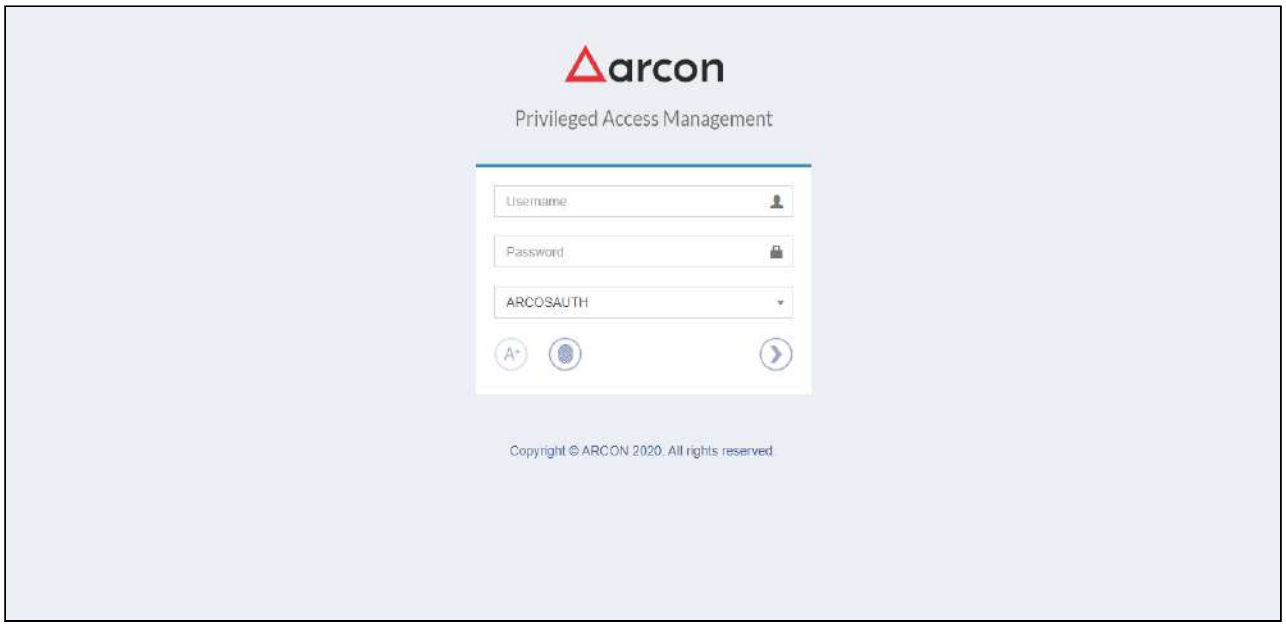
In computer security, logging in, (or logging on or signing in or signing on), is the process by which an individual gains access to a computer system or an application by identifying and authenticating themselves through user credentials. The user credentials are basically username and password, which are sometimes referred to as a login, (or a logon or a sign in or a sign on). In addition, due to digital thefts and breaches modern secured systems often use a second authorization for extra security of their application. Hence, ARCON PAM uses this second or dual factor authorization such as Mobile OTP, SMS OTP, Biometric Device, and Hardware Token configuration.

3.1 Server Manager Login

This section helps you to login into Server Manager application. When access is no longer needed, you can log out (log off, sign out or sign off) from the application.

Follow the below steps to login into Server Manager:

1. Enter the URL <http(s)://ip-address:port> in the address bar. The **ARCON PAM Login** screen is displayed.



2. Before you login, you need to install and configure **Java/ ActiveX**.

⚠
- For **Mozilla Firefox**, you need to install and configure **Java**.
- For **Internet Explorer,** you need to install and configure **ActiveX**.

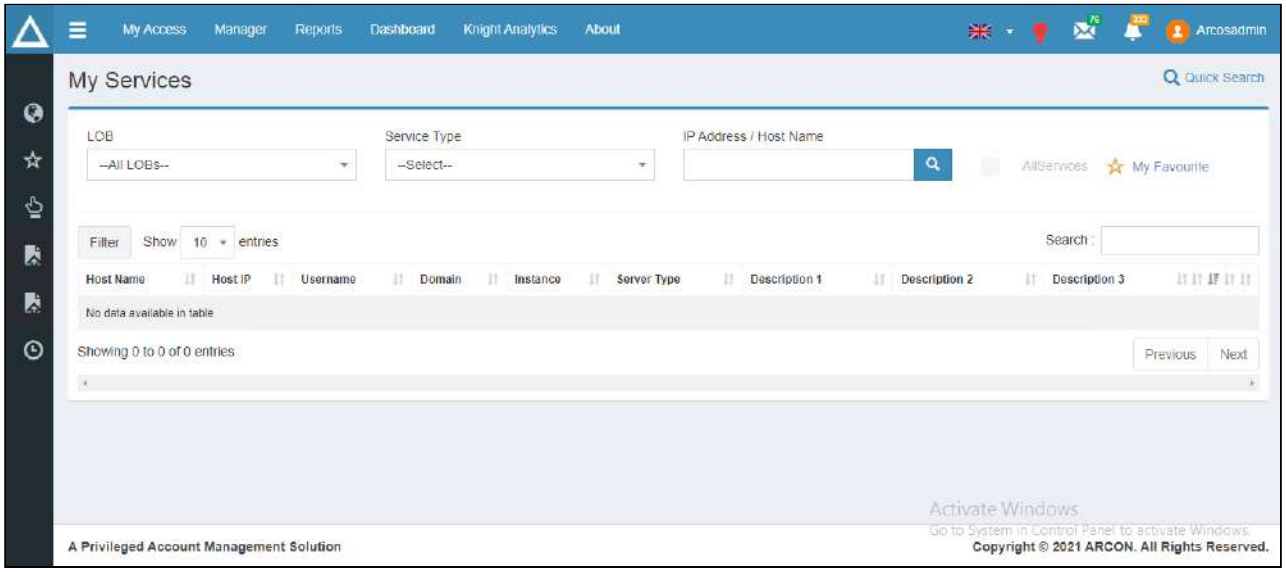
3. For **Java Applet Help or ActiveX Help**, you need to click  icon, viewed in the application.
4. On installing and configuring Java/ ActiveX, the Login is enabled.

⚠
If the Server and Client ActiveX Version does not match, the  icon will be disabled and  icon will be enabled. Also, it will prompt the Administrator to download the latest ActiveX version from the server.

The **ARCON PAM** login screen contains the following fields:

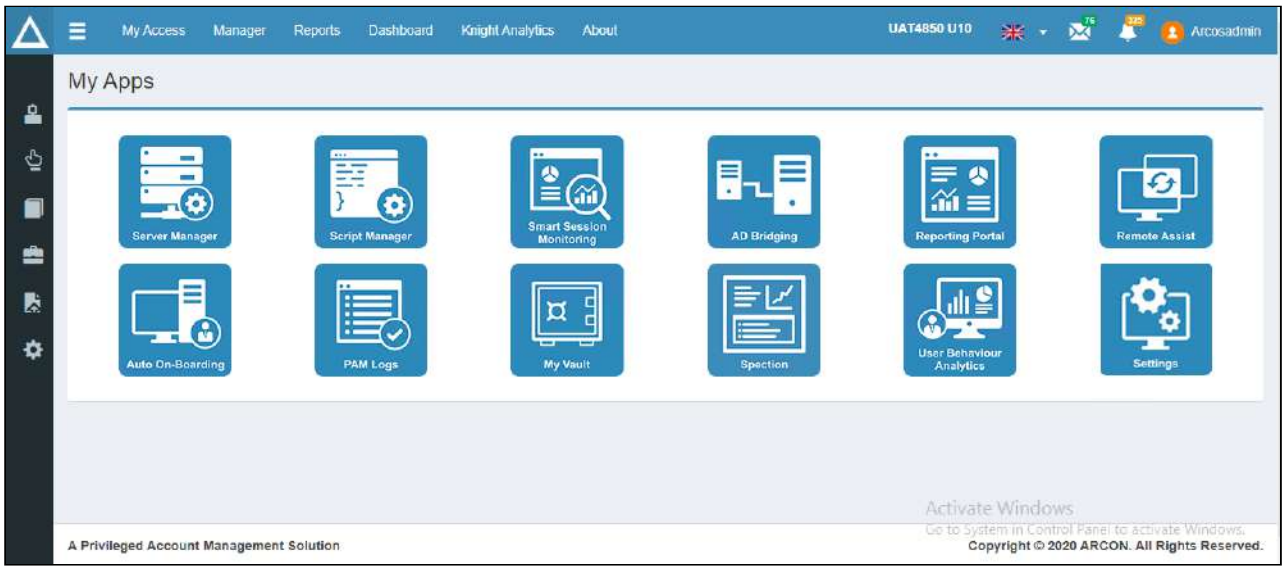
Field Name	Description
Username	Enter the username.
Password	Enter the password.
Domain	Select the domain from the drop down list.

5. Enter the credentials in the above fields and click the button, viewed in the application. The **ARCON PAM Home** screen is displayed.

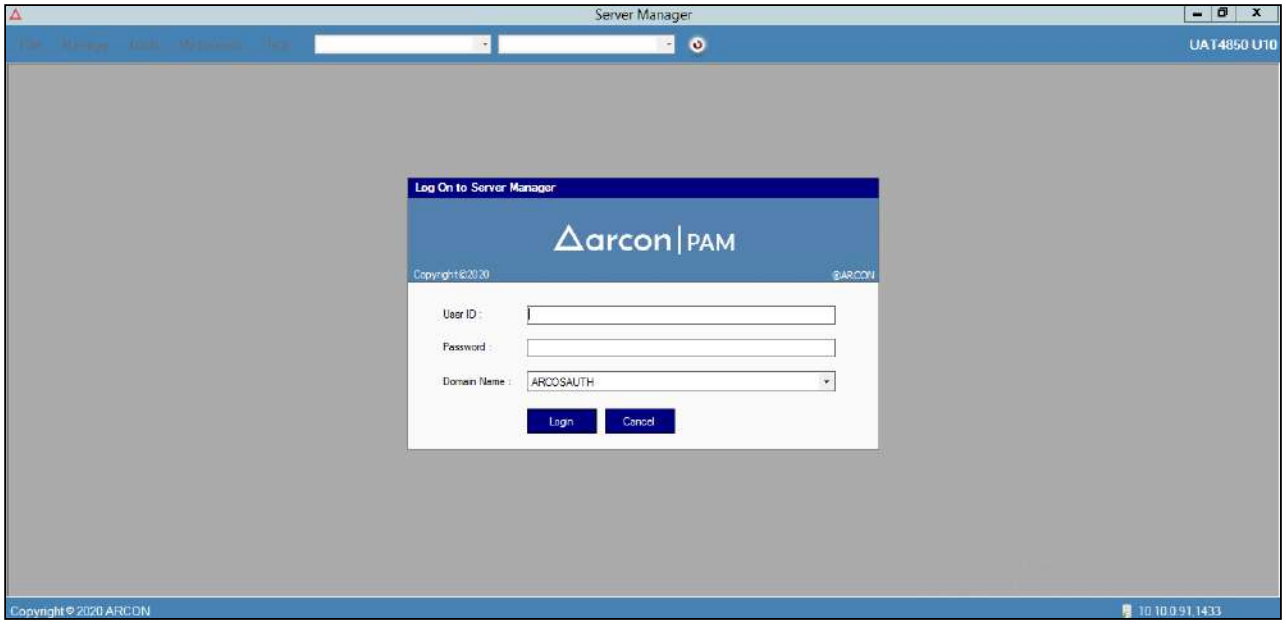


6. Click the **Manager** menu. The **My Apps** screen is displayed.

> ⚠ Client Users having **Manager Menu Display** privilege will only be able to view **Manager** menu in **Client Manager.**



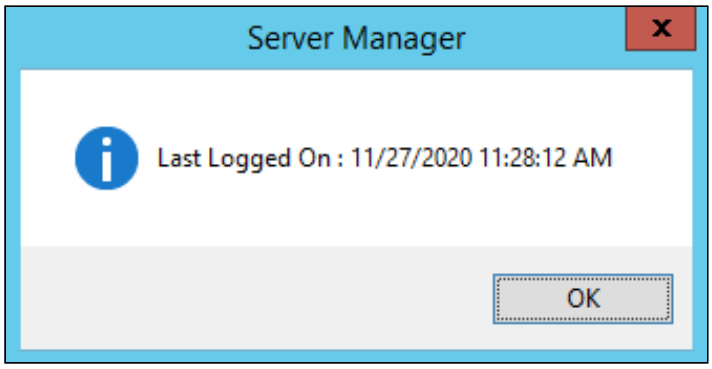
7. Click **Server Manager** icon. The **Server Manager Login** screen is displayed.



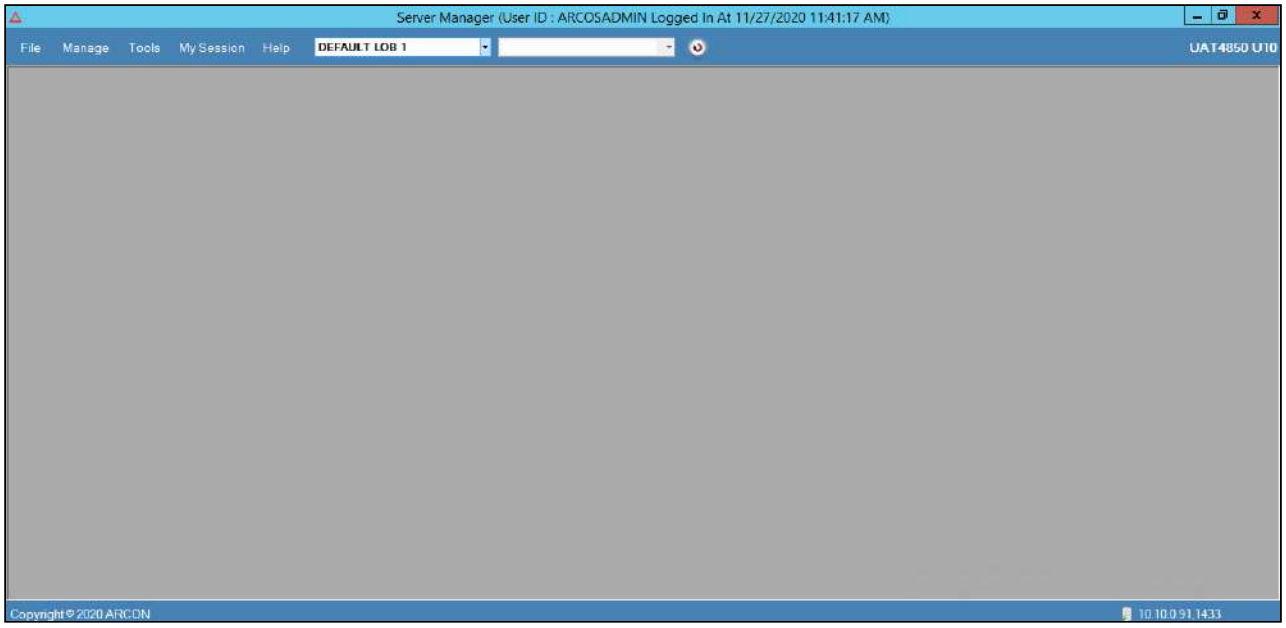
The **Server Manager Login** screen contains the following fields:

Field Name	Description
User ID	Enter the User ID.
Password	Enter the Password.
Domain Name	Select the Domain from the drop down list.

8. Click **Login**. The **ARCON PAM Server Manager** window pops up and gives the last logged on timestamp information of the User.



9. Click **OK**. The **ARCON PAM Server Manager Home** screen is displayed.



⚠ The error messages displayed for the login attempt failure by Users are as follows:

- The **User is Dormant** error message is displayed, if User attempts to login into the application exceeding the dormancy days configured in Application Configuration.
- The **User is Lockout** error message is displayed, if User attempts to enter invalid password more than configured lockout attempts configured in Application Configuration.
- The **User is Disabled** error message is displayed, if User has expired or has been dropped by the Administrators.

4 Entity Management and Mapping

In ARCON PAM, the users are mainly the Administrators. These users use various kind of services to access the privilege accounts. Hence, it offers a wide range of services and support privileges to make the privileged account secure and meet compliance regulations for these accounts. The various services created helps to implement, maintain, support and control the privilege identities with ease. Users can request for an access to these services, which are to be approved by the Admin/Approver. The Administrator is responsible for managing users. The users can be created, disabled, and modified through User Management module. It includes features such as Manage Users, Map Groups/Users, and Map Users/Services for managing and mapping users and services. In addition, you can configure user group to access various services, through group mapping.

This section includes the following topics:

- LOB
- User
- Service
- Groups
- Mapping
- Revoke and Share

4.1 LOB

Line of Business (LOB) is a general classification of operations used by the organization. A business basically describes the set of products or services that are grouped together under one department or team, based on factors planned by the organization. ARCON PAM helps to segregate different users and services. For example, a company may have a dedicated team working independently which can be segregated as a part of LOB. Therefore, different users and services are segregated under one particular department/LOB. The LOB concept is true to support multi-tenancy. LOB becomes a root for all the entities (Users, Services, User Group, and Server Group) when integrated in ARCON PAM. These entities are then mapped to their respective LOB's.

> ⚠ The Administrator who is assigned privileges listed in **Manage LOB/Profile** in **Server's Privileges** can perform respective action in **LOB/Profile Master & Manager**.

4.1.1 Create LOB

This section explains the steps to create or modify details of LOB (Line Of Business). The Administrators having **Add New LOB** privilege shall only be able to create or modify details of an LOB.

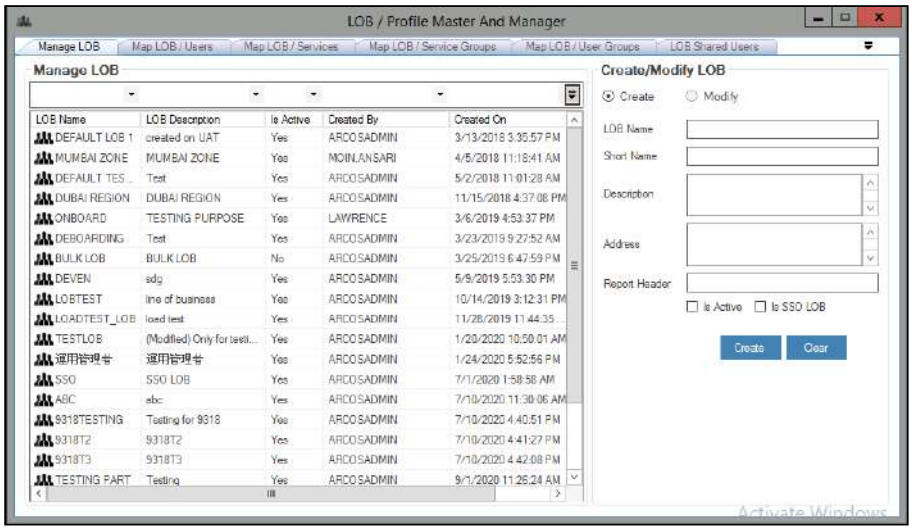
> ⚠ Administrators, who have been assigned **Add New LOB** privilege will be able to create new LOB and view all the LOB's in **Select LOB/ Profile** dropdown in **Server Manager Home Page** whereas Administrators, who have not been assigned **Add New LOB** privilege will be able to view only those LOB's which are mapped to them.

To create an LOB:

To create a line of business use the following path:

Manage → LOB/Profile Master and Manager → Manage LOB

1. Click the **Manage LOB** tab. The **Create/Modify LOB** screen is displayed.



The **Create/ Modify LOB** screen contains the following fields:

Field Name	Description
Create (radio button)	Select to create LOB.
Modify (radio button)	Select to modify details of an existing LOB. ▪ Administrators having **Modify LOB** privilege in Server's Privileges will only be able modify LOB name, description, address and Report Header of existing LOB. ▪ To modify details of LOB, select the required LOB from the grid on the left pane. The LOB details are displayed under **Create/Modify LOB** pane on the right side. Modify the required details and click **Modify**, to update the details.
LOB Name	Specify the name for LOB.
Short Name	Specify a short name for LOB.
Description	Specify the description for LOB.
Address	Specify the address of LOB.
Report Header	Specify the header name for LOB report.
Is Active	Enables the LOB once it is created.

2. Click **Create**. A window pops up with the following message: **"New LOB Created".**
3. Click **OK**. A new line of business is created.

4.2 User

A User is an entity who has the authority to use an application. Users shall be of two types such as Client User and Admin User. The Client type of User shall be responsible only for checking reports and accessing services. The Client User will not have admin privileges to perform any admin activity in Server Manager whereas the Admin User shall be able to perform all the activities in ARCON PAM.

While Logging into ARCON PAM, the Admin/Client type of User shall select the respective domains (AD Domain/ Local Domain) for authentication. The Users authenticated from Active Directory shall be called as Domain Users whereas, the Users authenticated from local Domain are known as Local User.

- **Domain User:** A domain User is a User whose username and password are stored on a domain controller rather than the computer through which the User is logging into. When you log in as a domain User, the computer asks the domain controller what privileges are assigned to you. When the computer receives an appropriate response from the domain controller, it logs you in with the permissions and restrictions.
- **Local User:** A local User is one whose username and encrypted password are stored on the computer itself. When you log in as a local User, the computer checks its own list of Users and its own password file to see if you are allowed to log into the standalone computer.

⚠ The Administrators having **Read Only Access** privilege (under **Manage User**) can view details displayed under Manage Users and Map Groups/Users tab.

This section includes the following topics:

- Create Domain User by Maker
- Create Local User by Maker
- Approve Domain/ Local User by Checker
- Modify Details of a User
- User Access Control
- User Access Review

4.2.1 User Creation Approval Process

4.2.1.1 Overview

A User is an entity that has the authority to use an application. Users shall be of two types such as Client User and Admin User. While Logging into ARCON PAM, the Admin/Client type of User shall select the respective domains (AD Domain/ Local Domain) for authentication. The Users authenticated from Active Directory are called Domain Users whereas, the Users authenticated from local Domain are known as Local User.

User Creation Process

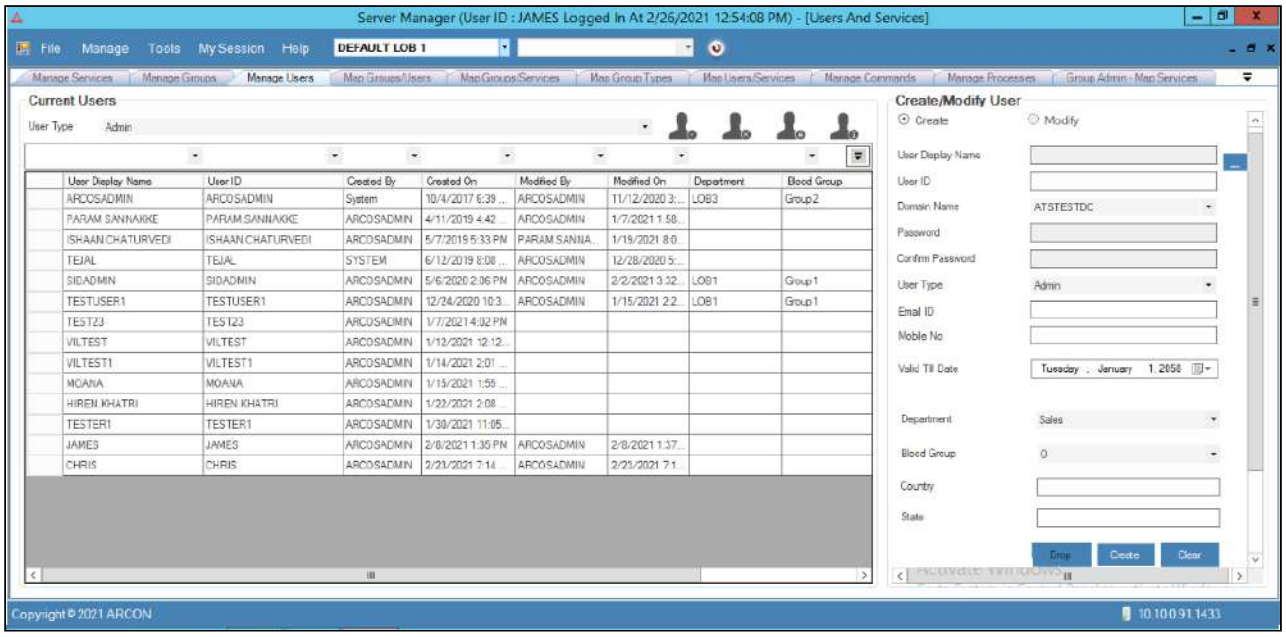
The process of User Creation and Approving this process is given below.

⚠
- The Administrator having **Add User** privilege will be able to create a User.
- The **Domain User** created must be present in the Active Directory. The User is then authenticated using Active Directory while logging into the application.
- If **User Maker Checker – Is Enabled** is **enabled** in **Settings**, then the User created will be sent for approval to Checker, whereas if Disabled, then the User will be directly created in ARCON PAM without the approval process.

Domain and Local Users are created from Manage Users.

The following steps are used to create Domain or Local User:

1. To create a User, use the following path:
   Server Manager → Manage → Users and Services → Manage Users



- For Domain Users, you need to enter the User ID in the **User ID** textfield, and select the Domain Name from the **Domain Name** dropdown list and then click the ... icon besides the **User Display Name** text field to fetch the details of the User from the Active Directory.
- To search a specific set of rows, enter keywords (space separated) on the column's header, and the relevant rows are pulled out.

2. The **Create/Modify User** screen contains the following fields:

Field Name	Description
Create (radio button)	Select to create a new User.
Modify (radio button)	Select to modify details of an existing active User. To modify details of User, select the required User from the grid on the left pane. The User details are displayed under **Create/Modify User** pane on the right side. Modify the required details and click **Modify** button, to update the User details.
User Display Name	Specify the name of the User. For Domain User, the data in this field is auto populated, once you enter the **User ID** and select the **Domain Name** from the dropdown list and then click the ... icon besides the **User Display Name** text field.
User ID	Specify the ID of the User.
Domain Name	Select the local domain or Active Directory (AD) domain from the drop down list.

Field Name	Description
Password	Specify the password. ⚠ For Domain Users, ▪ The data in this field is auto-populated, once you enter the **User ID** and select the **Domain Name** from the dropdown list and then click the ... icon besides the **User Display Name** text field. ▪ The ... icon verifies the domain name from the AD and if it successfully verifies the domain name, it fetches and displays the name in the **User Display Name** field. If the verification fails, then an error message "**Server was unable to process request….. No Users Found on Domain With Specified User Name**" is displayed.
Confirm Password	Re-enter the password to confirm that the entered password matches the previous password entered. ⚠ For Domain Users, The data in this field is auto populated, once you enter the **User ID** and select the **Domain Name** from the drop down list and then click the ... icon besides the **User Display Name** text field.
User Type	Select the type of the User. The valid values are: ▪ Client ▪ Admin
Email ID	Specify the Business Email ID
Mobile No	Specify the Business Mobile No
Valid Till Date	Select the end date. This is the date from which the User will be inactive to access the application. ⚠ This field is enabled, once you select the **Enable** checkbox.
Department **Customized field	Select the Department of the User from the dropdown. ⚠ ▪ This field name and the values in the dropdown are bespoke and can be set according to an organization's needs. ▪ This can be set in **Configure User Tag** in **Settings.**
Blood Group **Customized Field	Select the Blood Group of the User from the dropdown. ⚠ ▪ This field name and the values in the dropdown are bespoke and can be set according to an organization's needs. ▪ This can be set in **Configure User Tag** in **Settings.**

Field Name	Description
Country **Customized Field	Specify the name of the country user belongs to. ⚠ ▪ The field name is bespoke and can be set according to an organization's needs. ▪ This can be set in **Configure User Tag** in **Settings.**
State **Customized Field	Specify the name of the state in the country user belongs to. ⚠ ▪ The field name is bespoke and can be set according to an organization's needs. ▪ This can be set in **Configure User Tag** in **Settings.**
Drop Button	Click **Drop**, to disable the User in ARCON PAM. ⚠ ▪ Administrator having **Drop User** privilege will be able to disable a User. ▪ To drop a User, select the required User from the grid on the left pane. The User details are displayed under **Create/Modify User** pane on the right side. View the details and click **Drop**, to disable the User.

3. Enter or select the details and click **Create** to initiate the User creation process.

⚠
- If **User Maker Checker** configuration is enabled in **Settings,** then the User will be displayed in Administrator's **Maker's Checker.** Whereas, if this configuration is not enabled, then ARCON PAM will check whether **User Transaction** (Object Type) for **Creation** (Operation Type) is enabled in **ARCOS Workflow Approval Matrix**. If it is enabled, then Approval Email will be sent to configured User's email ID.
- If **User Maker Checker** configuration is enabled in **Settings** and **User Transaction** for **Creation** is enabled in **ARCOS Workflow Approval Matrix**, then User approval will be through **Maker Checker** process.

User Approving Process

Approving new User can be through **Maker Checker** or **ARCOS Workflow Approval Matrix**.

A. Approving User through Maker Checker

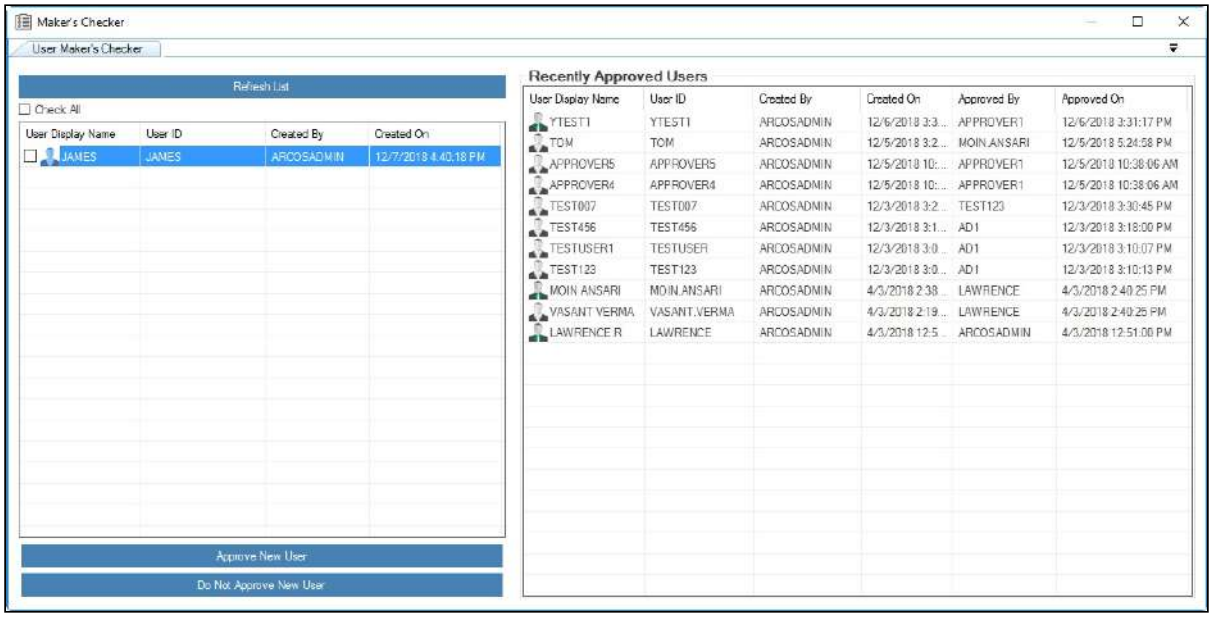
Maker - Checker is one of the central principle of authorization in ARCON PAM. The maker-checker concept means that for each request sent by the User/Administrator, there shall be at least two individuals or two level of authority to complete the User Creation process. A maker is an individual who shall create a user and the checker is an individual who shall be involved in confirming/authorizing the user created by the maker.

⚠
- The Administrator having **Approve User (Checker)** privilege will only be able to approve or reject newly created Users.
- The **Send Alert To All Checker When Maker Creates New User** configuration under **Settings** sets whether alert will be sent to all Checkers when Maker creates new User

- If toggle value is disabled then alert will not be sent to any Administrator; but request will be displayed in **Maker's Checker** screen of Admins having **Approve User (Checker)** privilege.
- If toggle value is enabled then alert will be sent to Administrators having **Receive Alert On User Creation By Maker** and **Approve User (Checker)** privilege.

The following steps are used to Approve User from Maker's Checker:

1. To approve a domain or local User use the following path:
   Server Manager → Manage → Maker's Checker
2. Click the **Maker's Checker** sub menu. The **User Maker's Checker** screen is displayed.
3. To approve the User created, select the checkbox in the **User Display Name** column.



4. Click the **Approve New User** link. A window pops up with the following message:
   Selected Users Has Been Checked Successfully.
5. Click **OK**. The User created is approved successfully.

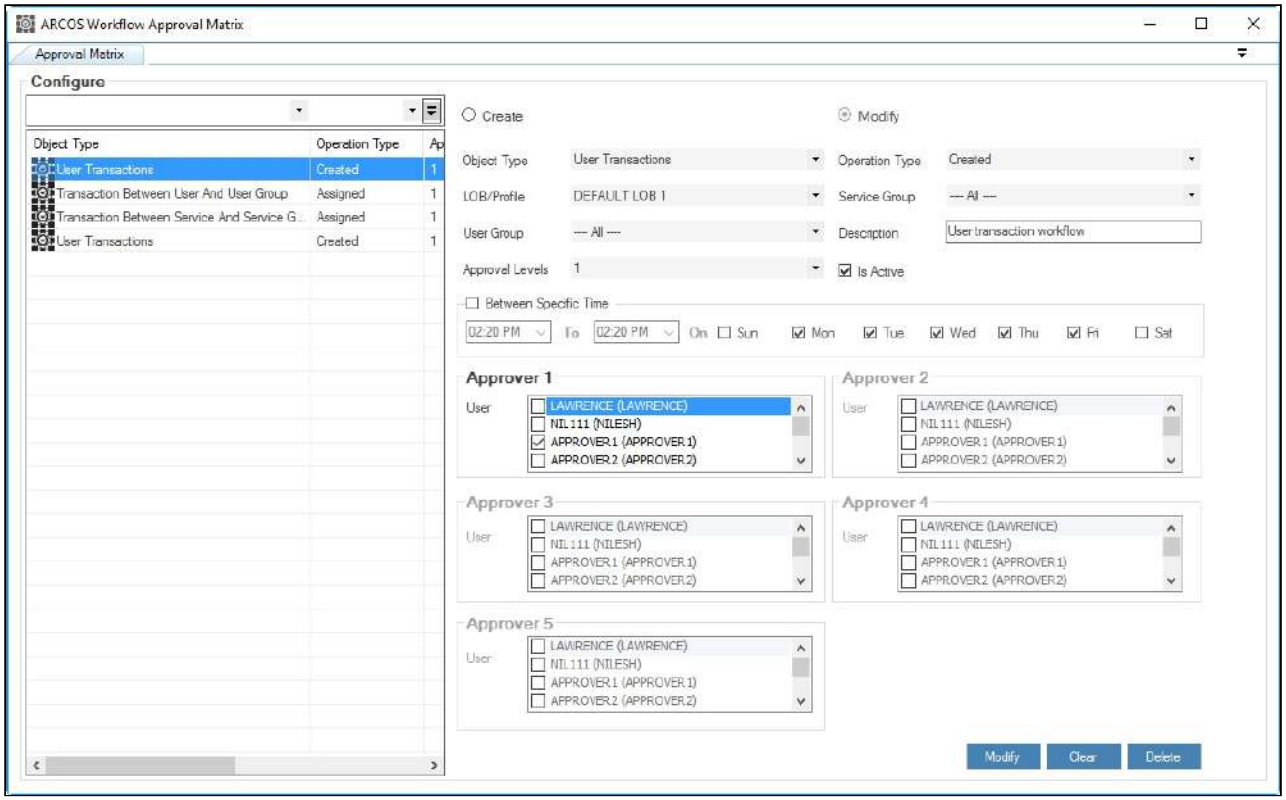
- To reject the request raised by Maker, click **Do not Approve New User** button.
- Once the request is approved or rejected by Checker/Approver, an alert notification is sent to the User. The notification is only sent to the User who is configured to receive notifications in **Alert and Notification Configuration**. For more information, refer **Alert and Notification Configuration** section from **Tool Management**.

B. Approving User through Approval Link

ARCOS Workflow Matrix helps you to configure approval levels for transactions performed in ARCON PAM. You should configure **User Transaction** of **Creation** Operation Type to send email notification to approvers for approving new created User .

The following steps are used to Configure Workflow and Approve request:

1. To navigate to ARCOS Workflow Approval Matrix, use the following path:
   Server Manager → Tools → Advanced Configuration → ARCOS Workflow Approval Matrix

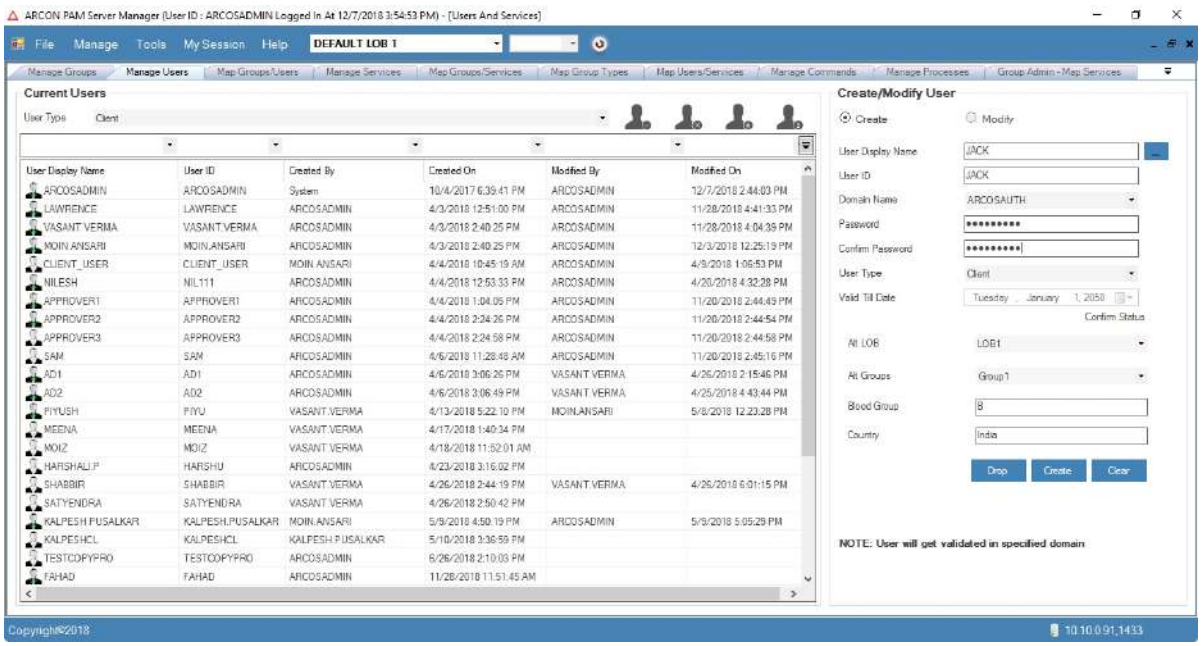


The **Approval Matrix** screen contains the following fields:

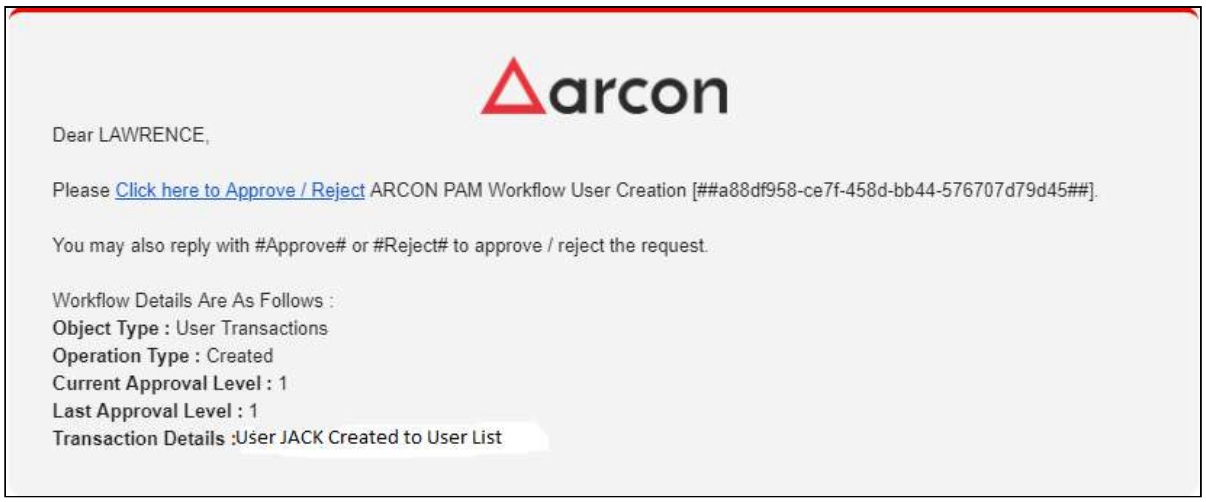
Field Name	Description
Object Type	Select the type of object. The valid values are: ▪ **User Transactions:** Used for creation, deletion, modification of User's. ▪ **Service Transactions:** Used for creation, deletion, modification of Services. ▪ **Transaction Between User and User Group:** To map User(s) with their respective User Groups. ▪ **Transaction Between Service and Service Group:**To add or remove services to/ from their respective Server Group. ▪ **Transaction between User And Service:** To assign or revoke Services to/from User's. ▪ **Transaction Between User Group And Service:**To map or remove User Group to/ from Service Group and vice versa.

Field Name	Description
Operation Type	Select the type of operation. The valid values are: ▪ Created ▪ Modified ▪ Deleted ▪ Assigned ▪ Revoked ▪ CheckerApproved ▪ CheckerNotApproved ▪ Accessed ▪ Viewed ▪ Shared ▪ Un-Shared
Approver Levels	Select the levels of approval for the selected object type. The valid values are: ▪ 1 ▪ 2 ▪ 3 ▪ 4 ▪ 5 ⚠ You can select up to 5 levels of approval.
Is Active	Enable the configuration for approval.
LOB/ Profile	Select the LOB/Profile.
Service Group	Select the service group.
User Group	Select the user group.
Description	Specify the description for the selected object type.
Between Specific Time	To set the specific time for approval.
Approvers	Select the name of the approver to approve the request. ⚠ For the User ID's to appear for selection in the drop box, the Users in ARCON PAM needs to have email ID's configured in user settings.

2. Select/Enter the fields and click **Create** to create Workflow.
3. When a User is created under **Manage Users** tab, approval email will be sent to Approver.
   Example: Below is example of User creation approval process through Workflow Matrix.
   - User 'Jack' is created under **Manage Users** tab.

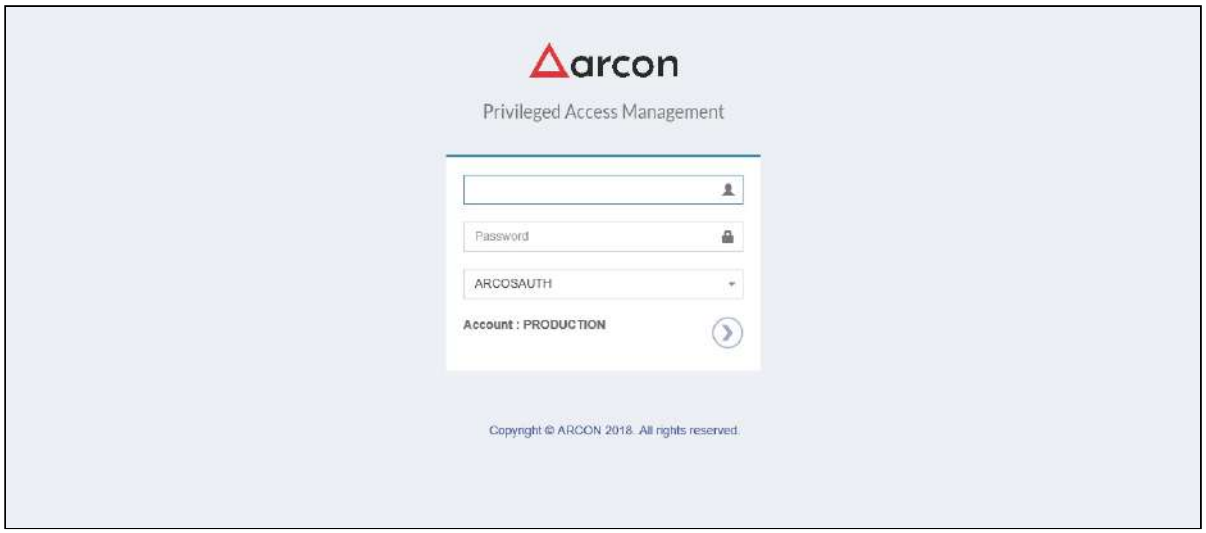


- Approval link is sent to Approver configured in **ARCOS Workflow Approval Matrix**.

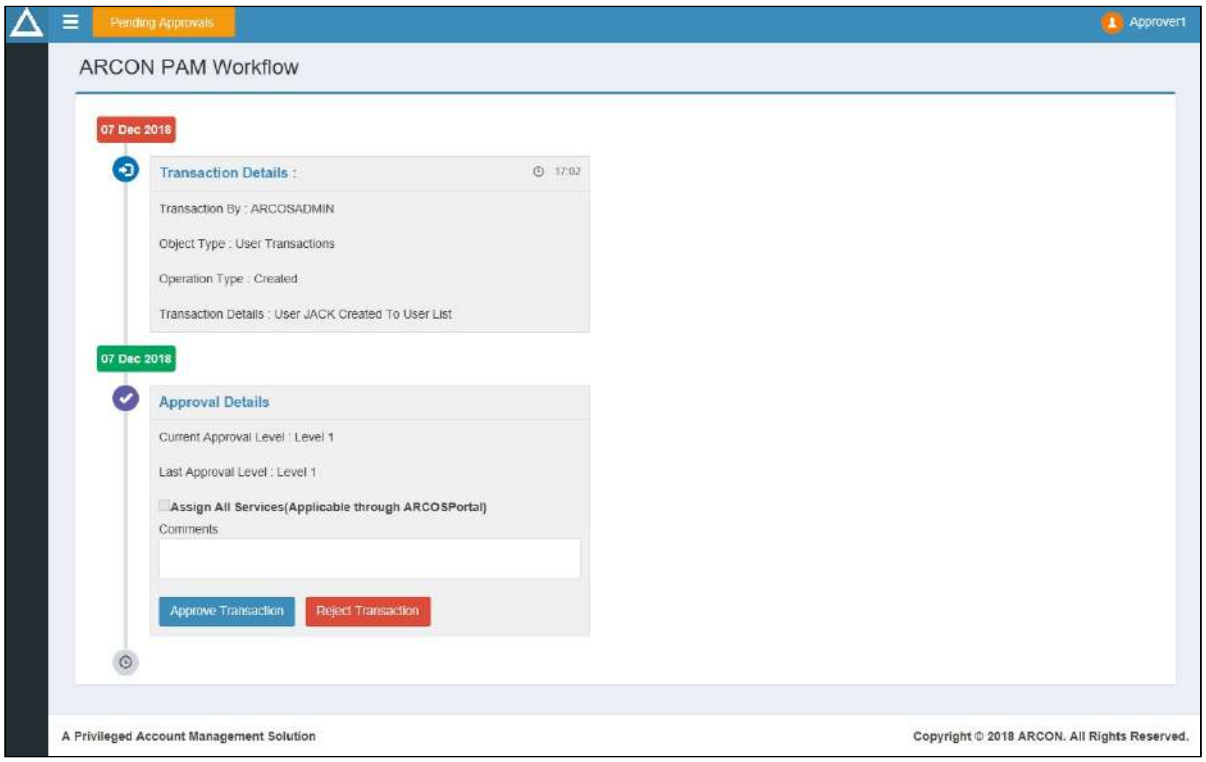


> ⚠ To approve/reject a request, the approver can click link given in email or can reply to the above mail received in their inbox. The approvers will have to reply with the content **#Approve#** or **#Reject#** to approve/reject the request.

- To approve/reject request using the link, click on the **Click here to Approve / Reject** link sent on email. The following login screen will be displayed.



- Login into ARCON PAM Workflow web console. Following details are displayed for approval.



- Enter comments and click **Approve Transaction** to approve User creation process.

> ⚠ Click **Reject Transaction** to reject User Creation.

- Similar email will be sent to all Approvers. The User will be created when all Approvers the transaction.

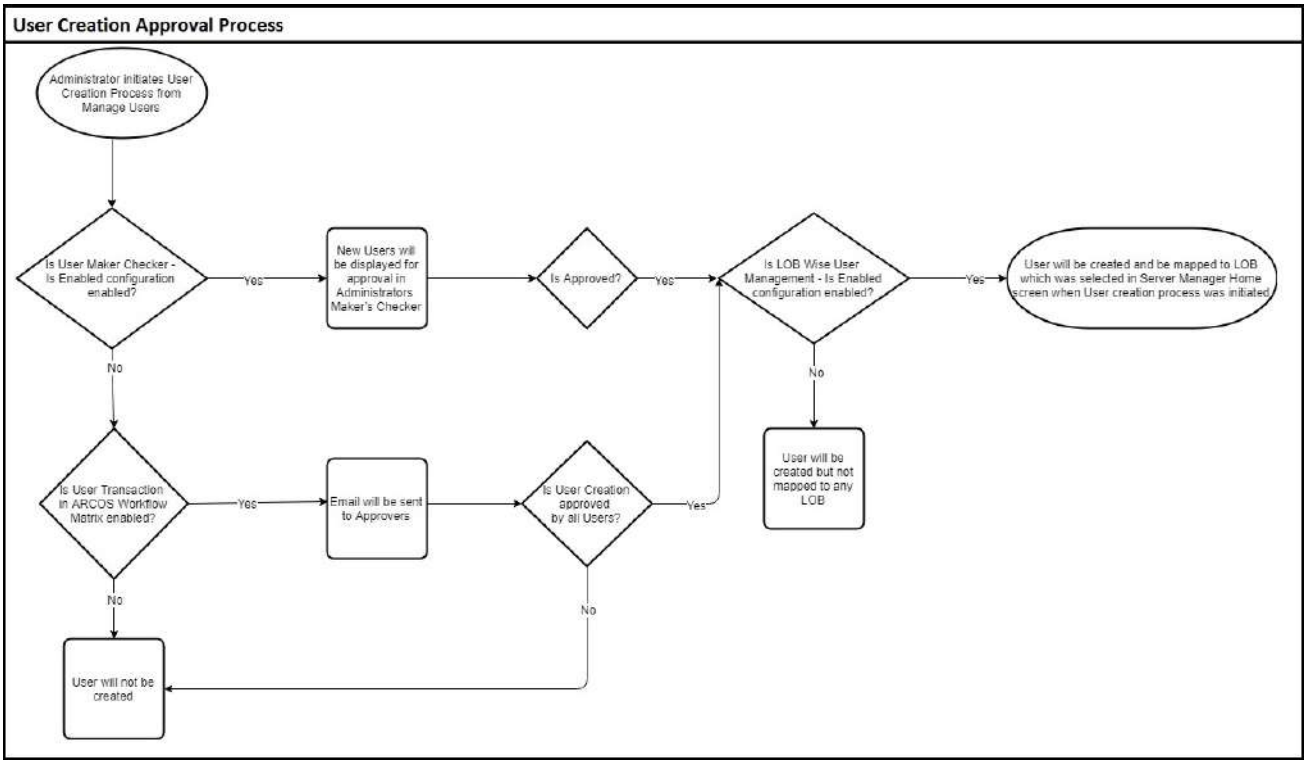
Once a User is successfully created, you need to then map the user to a particular LOB. In some cases, wherein an Administrator having **Settings** privileges has configured the value for **LOB Wise User Management** option, where

- **LOB Wise User Management - Is Enabled** toggle value is set to **Diabled**, it states that when a user is created, it will directly map the user to the selected LOB in **Select LOB/Profile** dropdown list, once it is created.
- **LOB Wise User Management - Is Enabled** toggle value is set to **Enabled**, it states that the user created needs to be mapped to a particular LOB in **LOB/Profile Master & Manager**.

By default, the toggle value is Enabled.

Process Flow Diagram

Following is the process flow diagram of User Creation Approval Process.



4.2.2 Modify details of User

This section helps you to modify the details of a particular user. You can modify the details of a particular user using the **Create/ Modify User** screen.

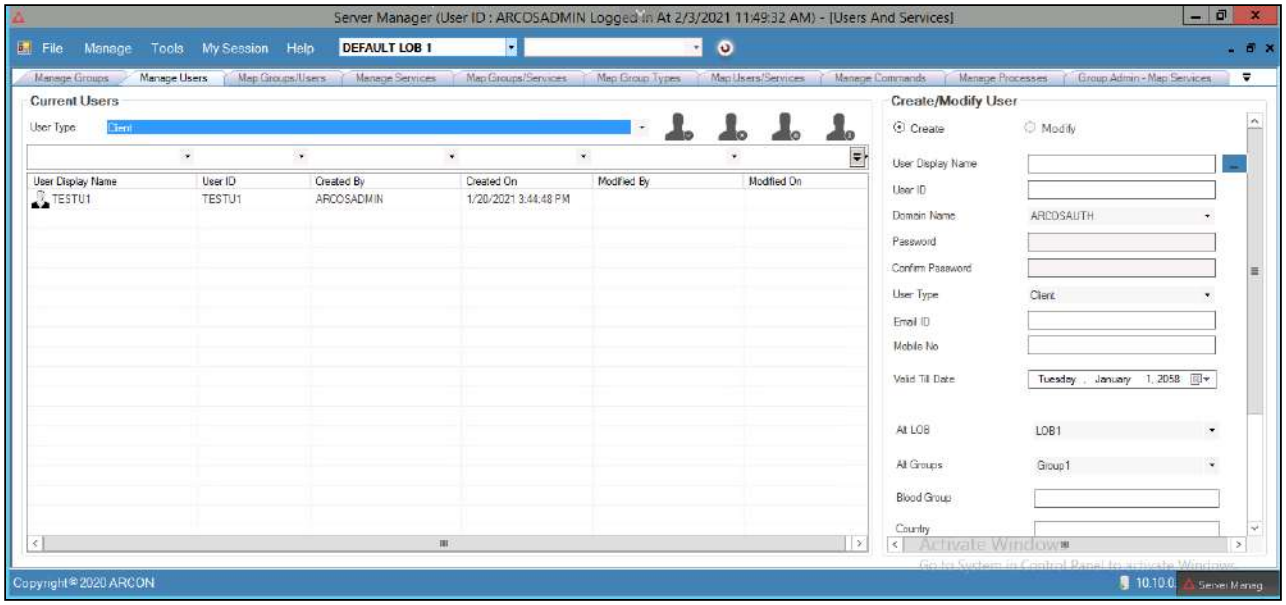
The Administrator having **Modify User** privilege shall only be able to modify User details.

To modify details of a User:

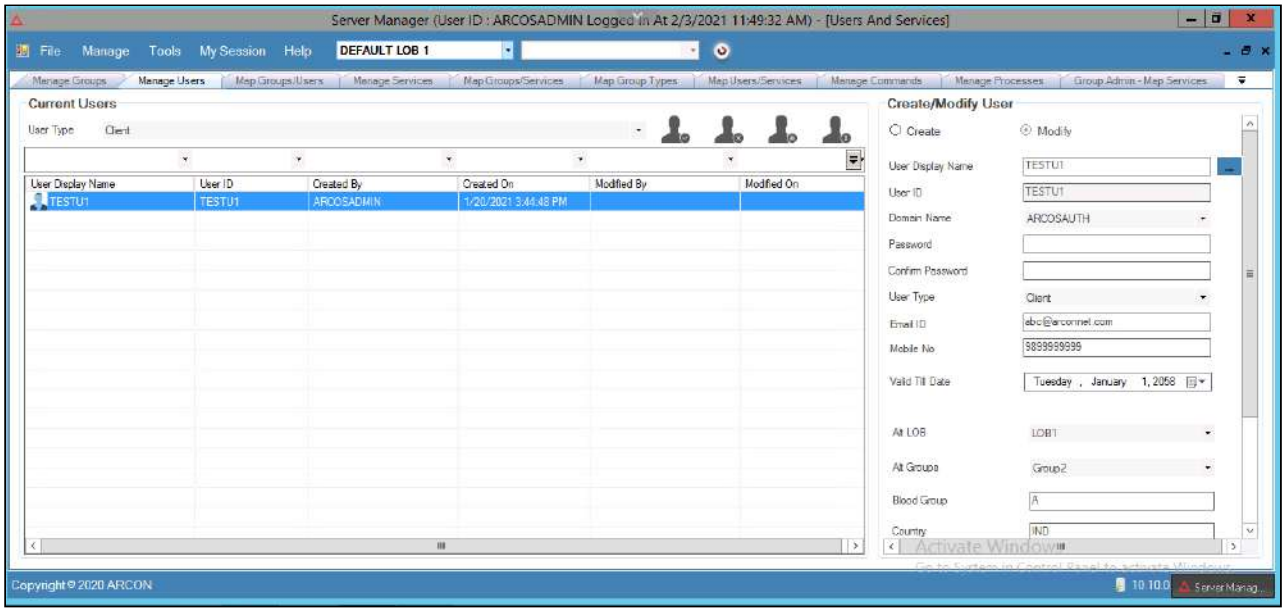
To modify details of a User use the following path:

Manage → Users and Services → Manage Users

1. Click the **Manage Users** sub menu. The **Create/Modify User** screen is displayed.



2. Select the LOB and type of User from the **Select LOB/Profile** and **User Type** dropdown list respectively. A list of active Users are displayed in the grid.



3. Select the User from the grid. The details are populated in the **Create/Modify User** fields.
4. Modify the required changes in the existing fields and click **Modify**. A window pops up with the following message:
   Selected User Updated.
5. Click **OK**. The details of the User are modified.

> ⚠ You can also modify details of Active Users, Disabled Users, Lockout Users, and Dormant Users of a particular LOB by selecting the icons besides the **User Type** dropdown.

4.2.3 User Access Control

Access control is a security technique that can be used to regulate who can view or use resources in a computing environment. Access control systems perform authorization identification, authentication, access approval, and accountability of entities through login credentials including passwords, personal identification numbers (PINs), biometric scans, and physical or electronic keys.

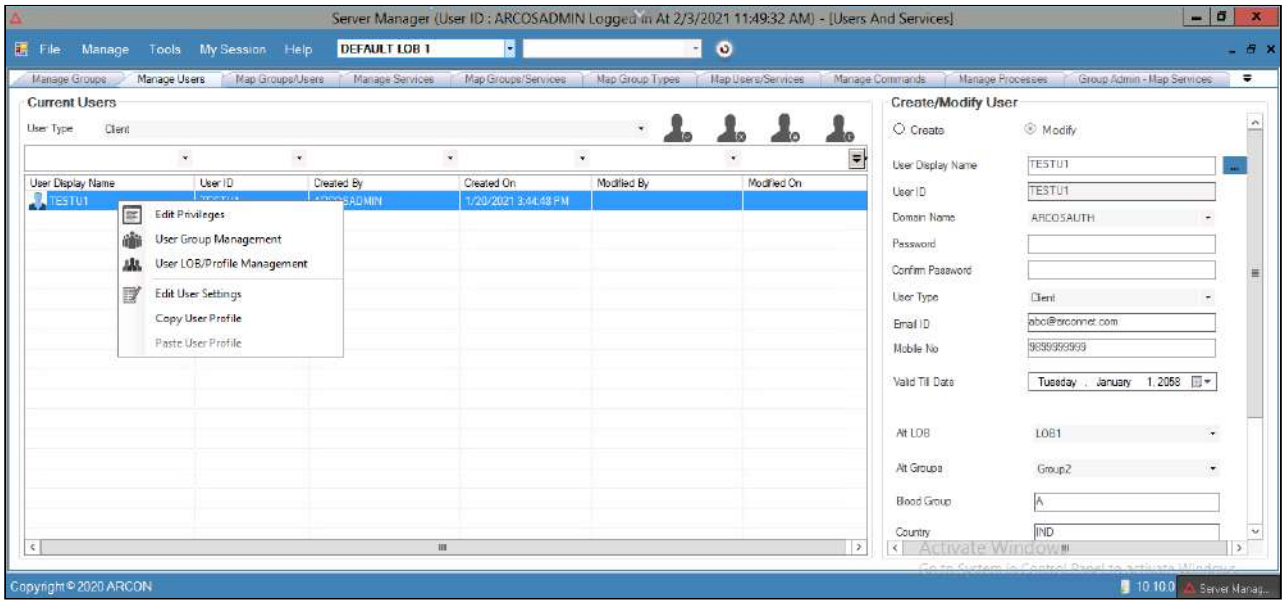
User Access Control is a security feature, which helps to prevent unauthorized changes to your computer. These changes can be initiated by applications, viruses or other users. User Access Control module makes sure that these changes are made only with approval from the Administrator. This section allows to enable the user logon period, disable the user logon, session lockout, endpoint based access, and to enable or disable the dual authorization factor for user(s).

> ⚠ The Administrator having **Edit User Settings** privilege shall only be able to edit User settings.

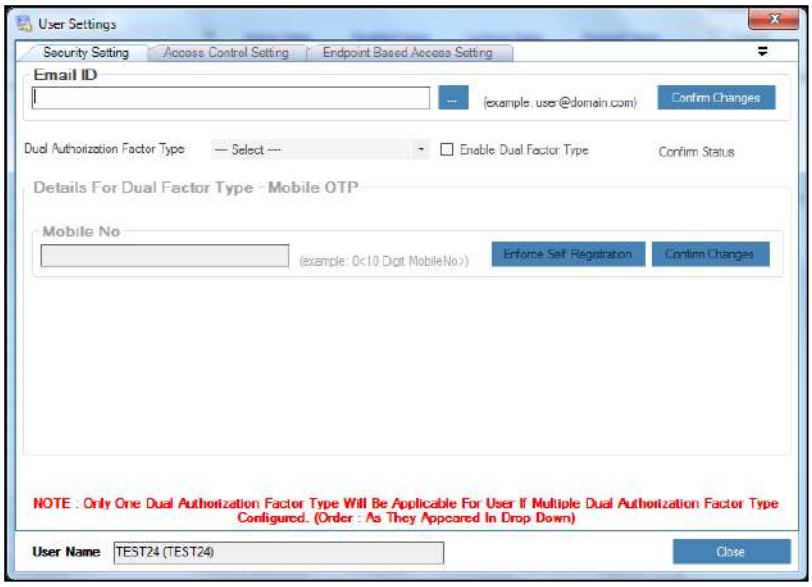
To navigate, use the following path:

Manage → Users and Services → Manage Users

1. Select a User and right click on the record. A dropdown list is displayed.



2. Click **Edit User Settings** option. The **User Settings** screen is displayed.



The **User Settings** screen contains the following tabs:

- Security Setting
- Access Control Setting
- Endpoint Based Access Setting

4.2.3.1 Security Settings

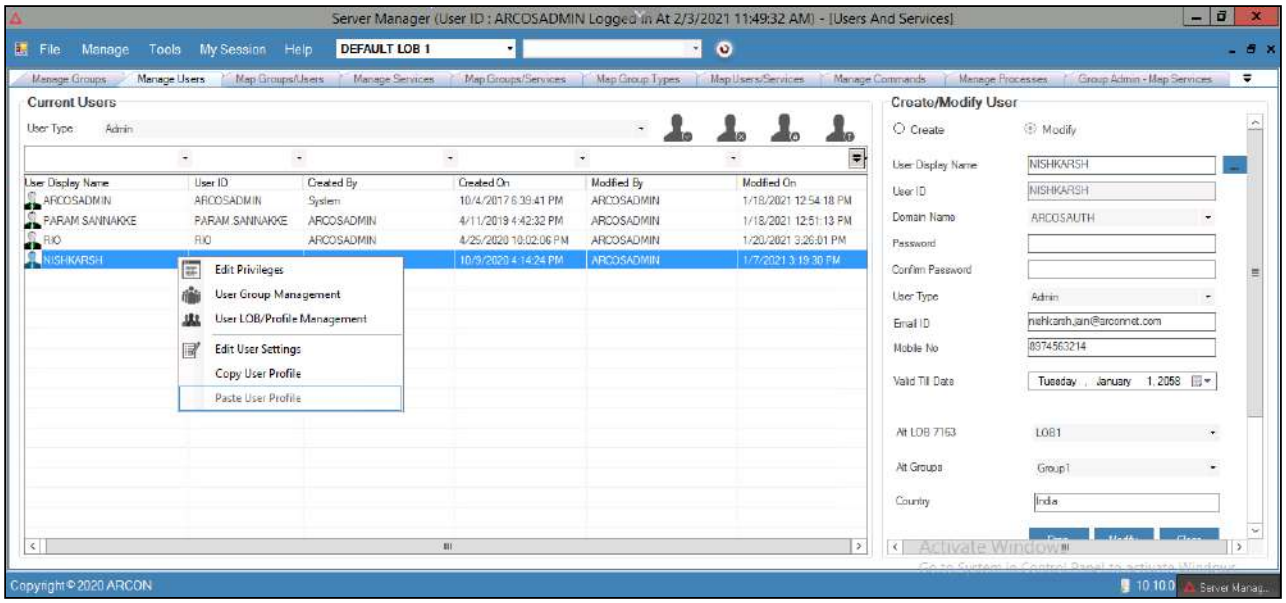
User Security Settings is a dual authentication process, wherein the user is authorized twice in ARCON PAM, after which the user can get access to the application, making it more secure.

To edit security settings:

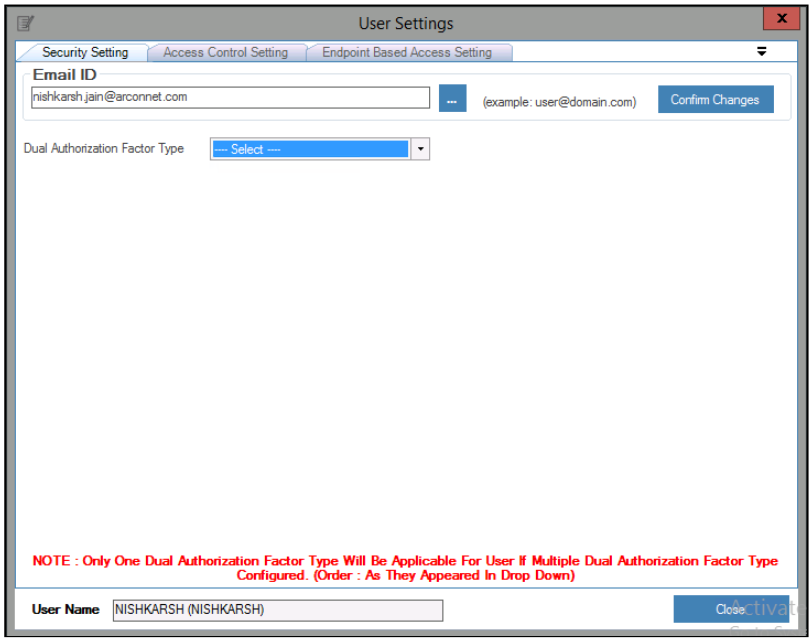
To edit user settings use the following path:

Manage → Users and Services → Manage Users

1. Right click on the User name from the **User Display Name** list. A multiple options list is popped up.



2. Click **Edit User Settings** option. The **User Settings** screen is displayed.



4.2.3.1.1 Configure Email Address

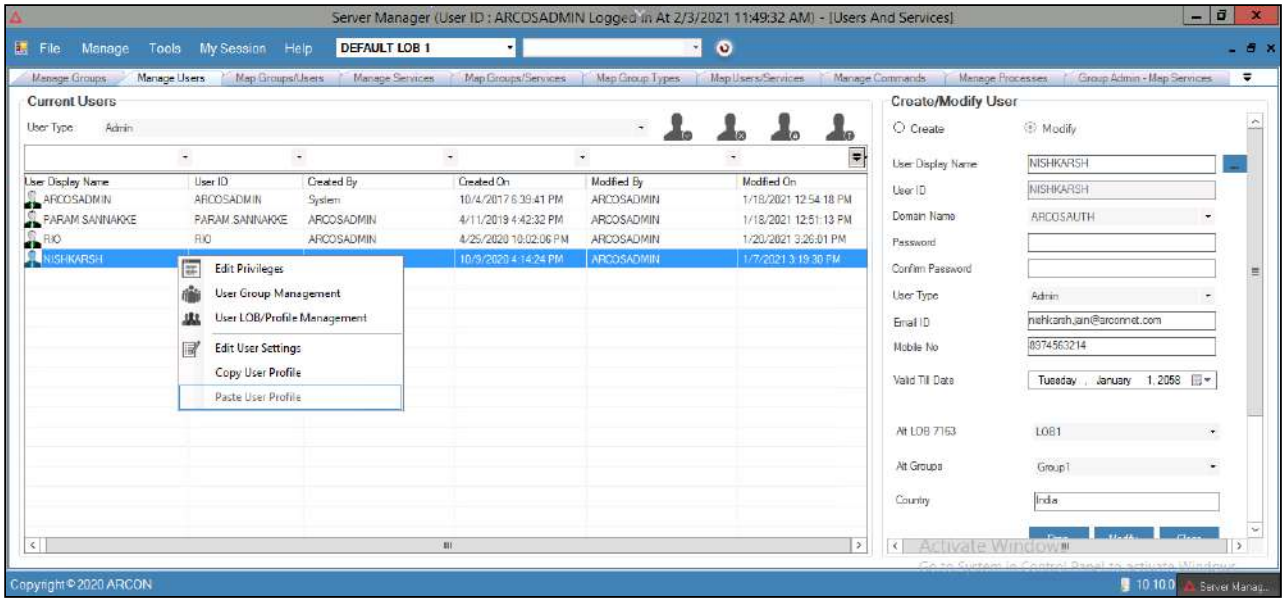
This section explains the steps to configure email address for the User. It helps the User to receive alert mails for the activities performed in ARCON PAM. For example, alert mails for Workflow Approval, Scheduled Reports, Scheduled Password Envelope, Service Access Request, Service Password Request, or Ticket Request.

To configure Email Address:

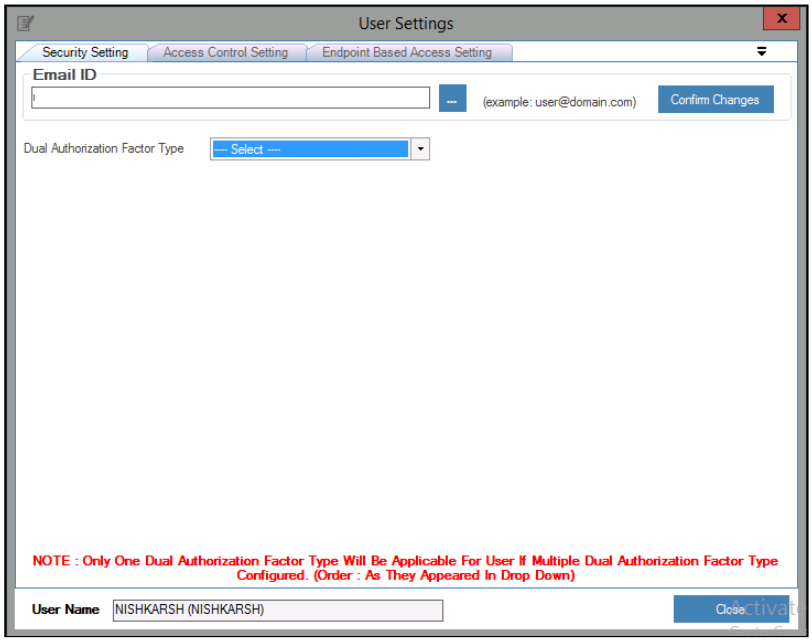
To configure Email Address use the following path:

Manage → Users and Services → Manage Users

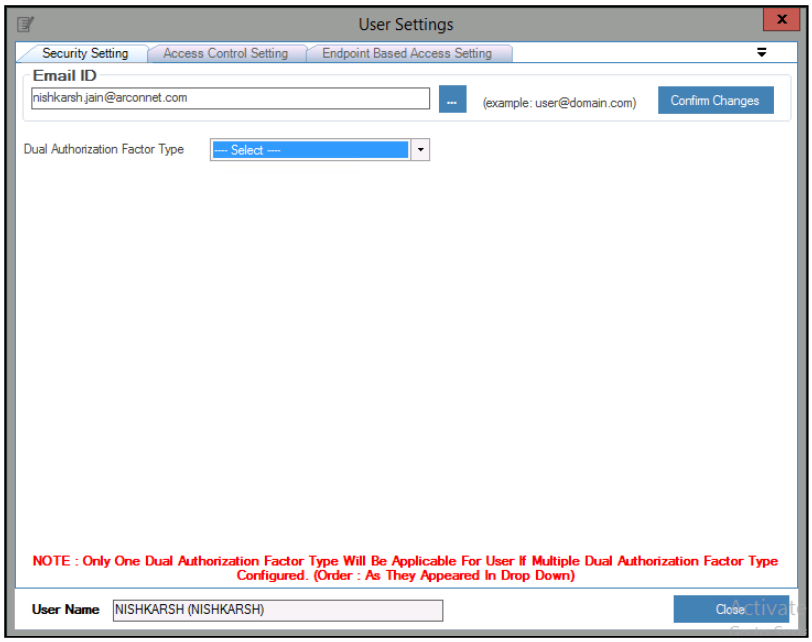
1. Right click on the user name from the **User Display Name** grid list. The **Edit User Settings** option is displayed.



2. Click the **Edit User Settings** option. The **User Settings** window is displayed.



3. In **Security Setting** tab, enter the email address of the user in the **Email ID** text field and click **Confirm Changes** to configure email address for the User.



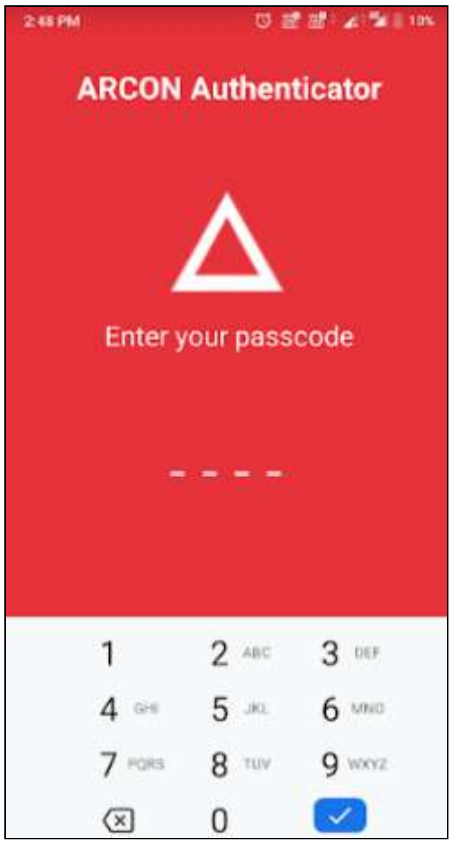
For Domain User, if Email Address is configured for the User on the Domain Server, then click ... icon to fetch the Email Address from the Domain Server.

4.2.3.1.2 Configure Mobile OTP

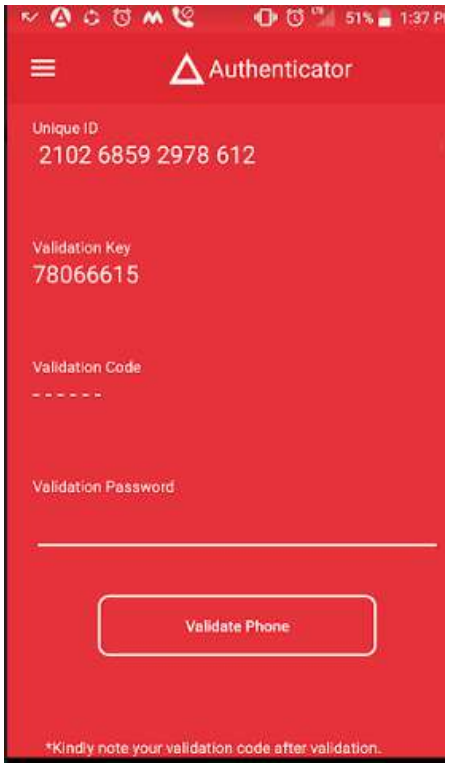
Static passwords for authentication has quite a few security drawbacks such as passwords can be guessed, forgotten, written down and stolen, eavesdropped or deliberately being told to other people. A better, more secure way of authentication is called "dual-factor" based on one time passwords. Mobile one time password (OTP) configuration is one of the dual factor authentication. It is used by mobile users by implementing the application on mobile, inorder to securely login into ARCON PAM.

4.2.3.1.2.1 Pre- requisite

1. Download and install **ARCON** App from **Google Play Store** on your mobile to configure mobile OTP dual factor authentication.



2. Enter a Passcode for first login attempt and re-enter passcode to confirm on your mobile device.



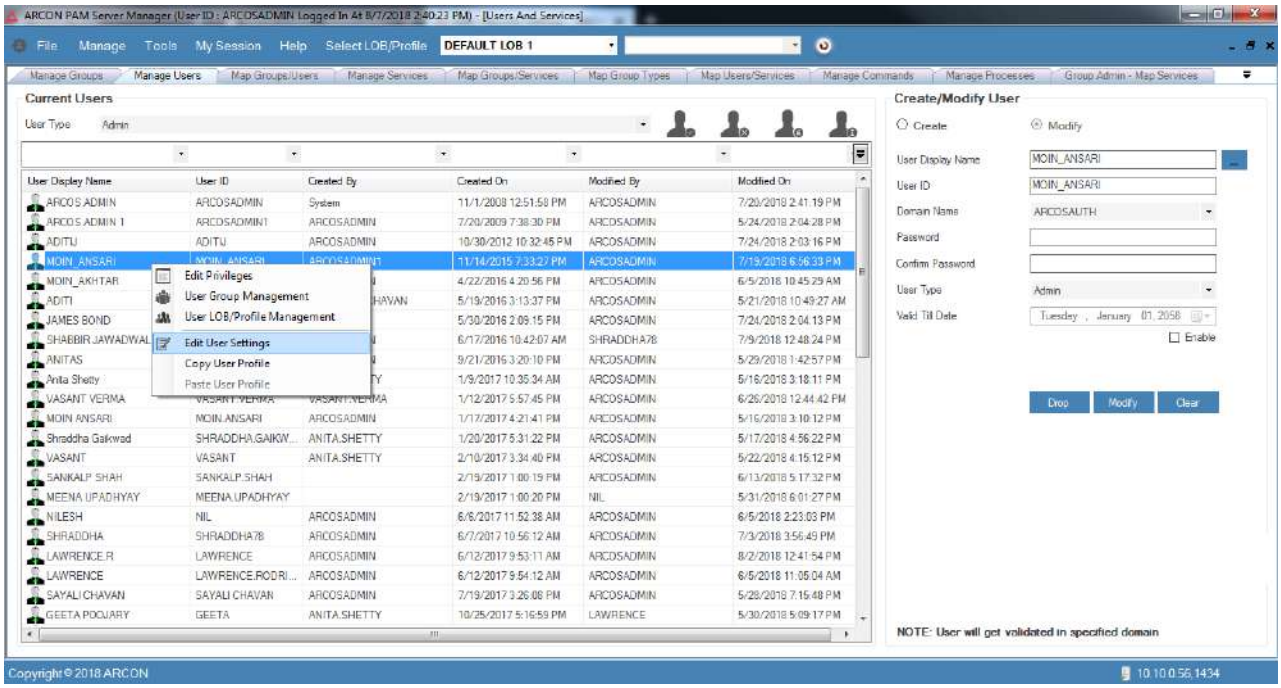
3. The above screen will be displayed on re-entering the password, the screen will have the following details
    a. Unique ID : To be entered in server manager
    b. Validation key: To be entered in Server Manager
    c. Validation code : Encrypted format
    d. Validation Password:

4.2.3.1.2.2 Enable Dual Factor Authentication - Mobile OTP

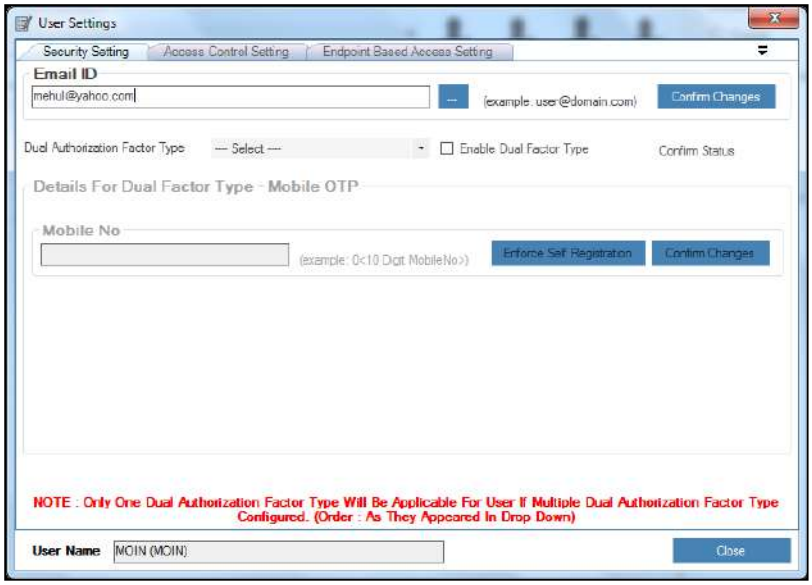
To enable dual factor authentication Mobile OTP use the following path on server manager:

Manage → Users and Services → Manage Users

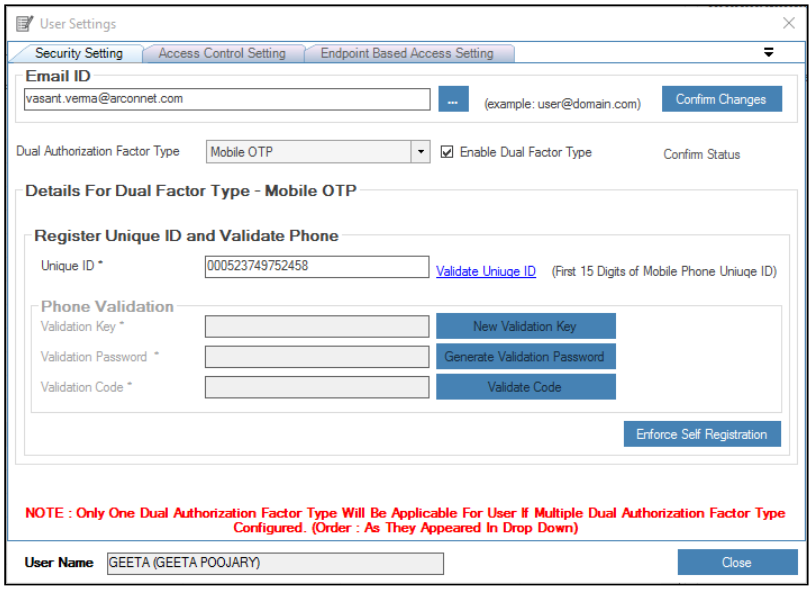
1. Right click on the User name from the **User Display Name** list. A multiple options list is popped up.



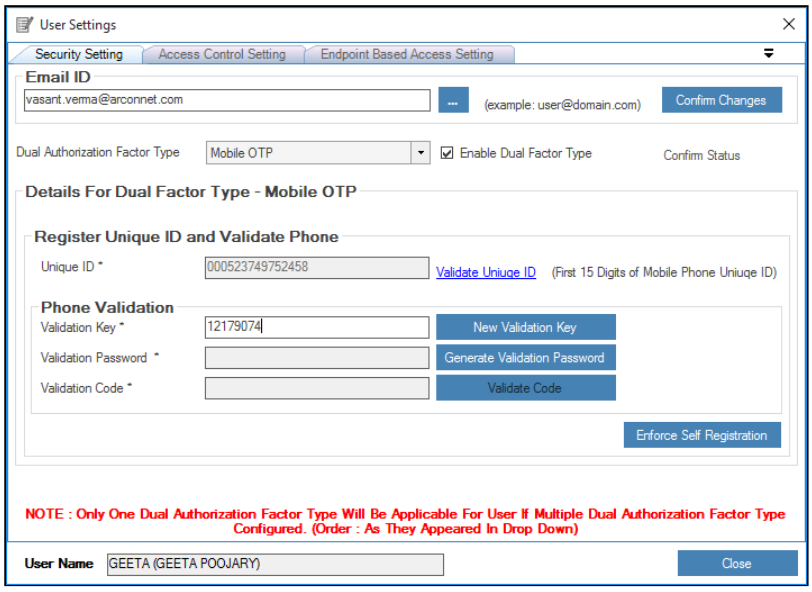
2. Click **Edit User Settings** option. The **User Settings** screen is displayed.



3. Select the Dual Authorization Factor Type as Mobile OTP and click the Enable Dual Factor Type checkbox.
4. Enter the Unique ID displayed on the App (explained in pre-requisite Step 3a) in the **Unique ID** text field.

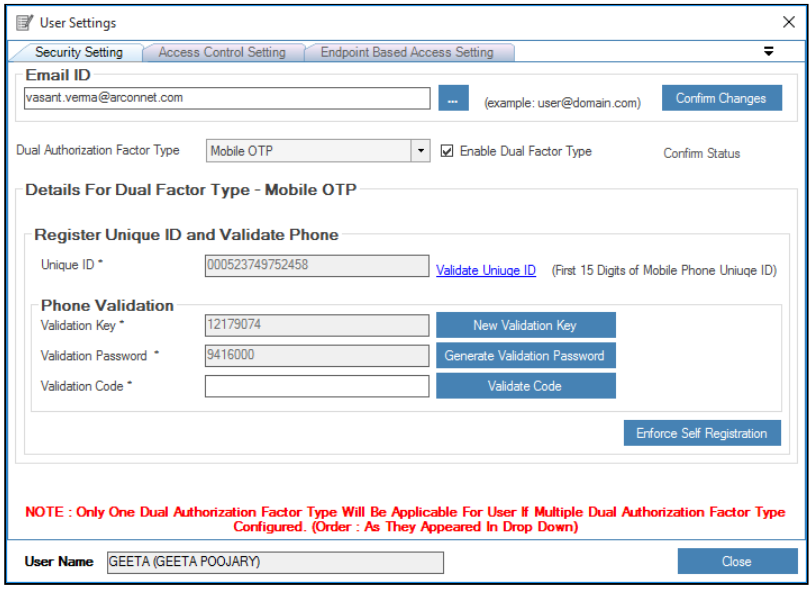


1. Click **Validate Unique ID** link to validate the Unique ID number.
2. If Unique ID is not valid, then it displays an error message **Unique ID Invalid**.
3. On successful validation, the Validation Key filed under Phone Validation will be enabled.
4. Enter the **Validation Key** displayed on the mobile screen (explained in pre-requisite Step 3b) .

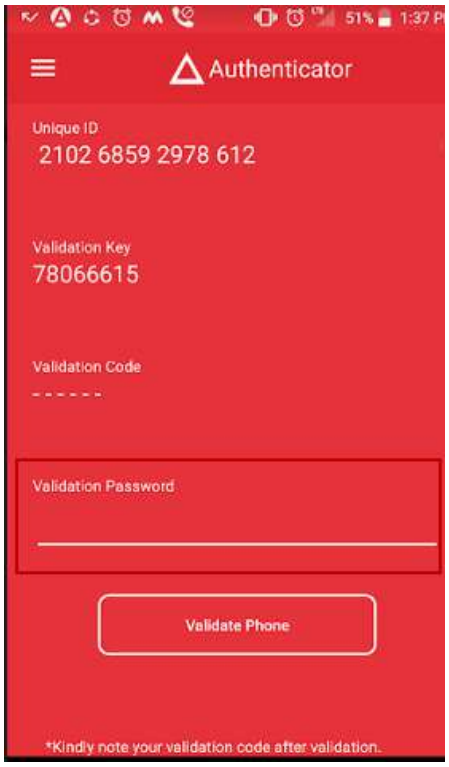


⚠ To enter new validation key, click on **New Validation Key** button.

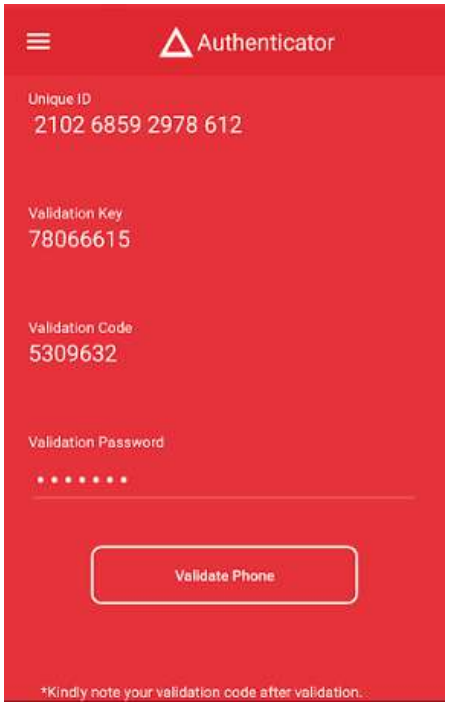
5. Click **Generate Validation Password** button. The validation password is displayed in the **Validation Password** text field.



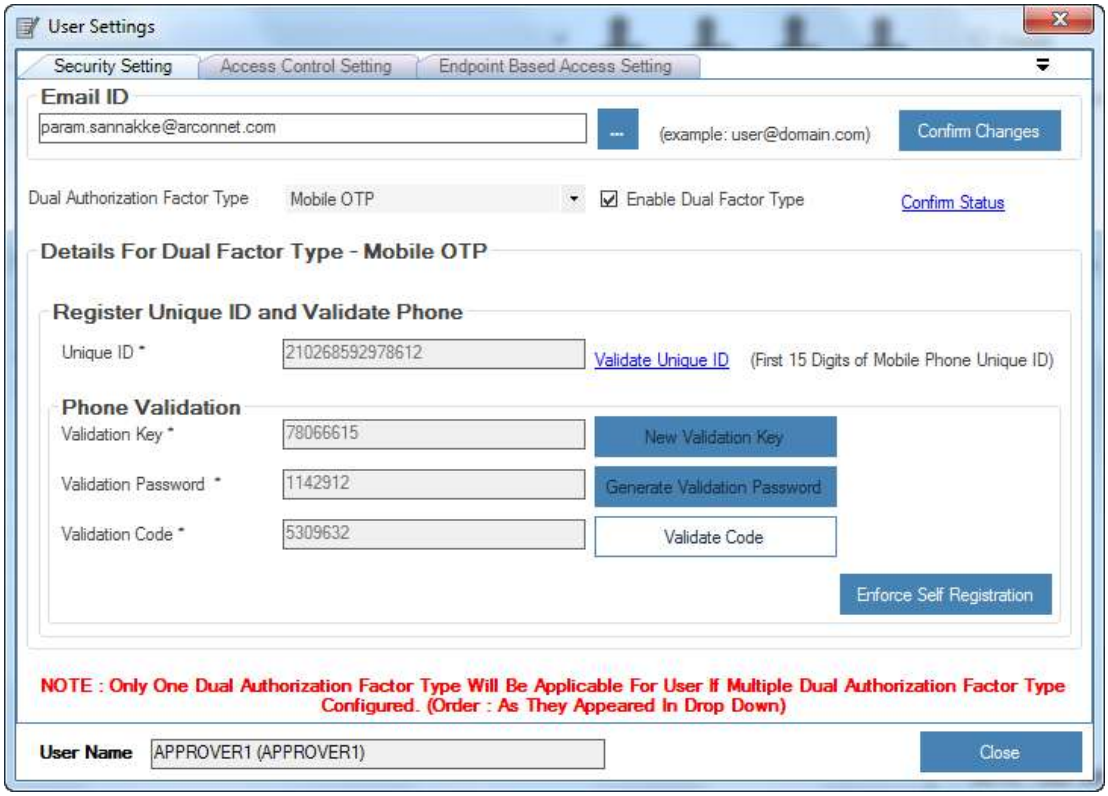
6. Enter the **Validation Password** displayed on the Server Manager in the Validation password field of the ARCOS Authenticator mobile app.



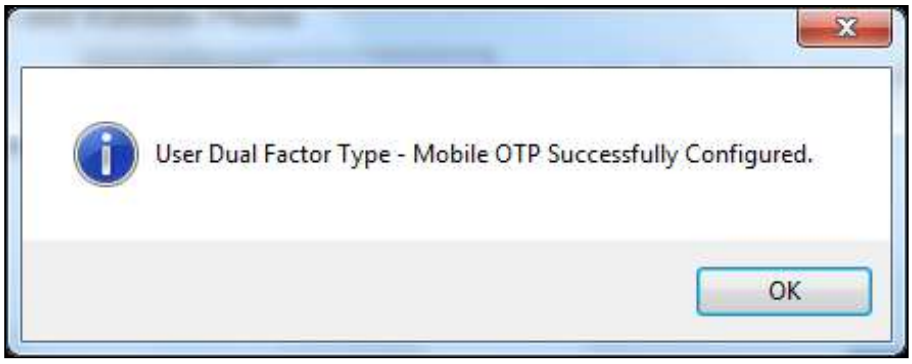
7. Click **Validate Phone** button.
8. On successful validation of the phone, the validate Code filed that was earlier in encrypted format will be displayed now.



9. Enter the Validation code displayed on the Mobile app in the Validation code filed on the Server Manager.



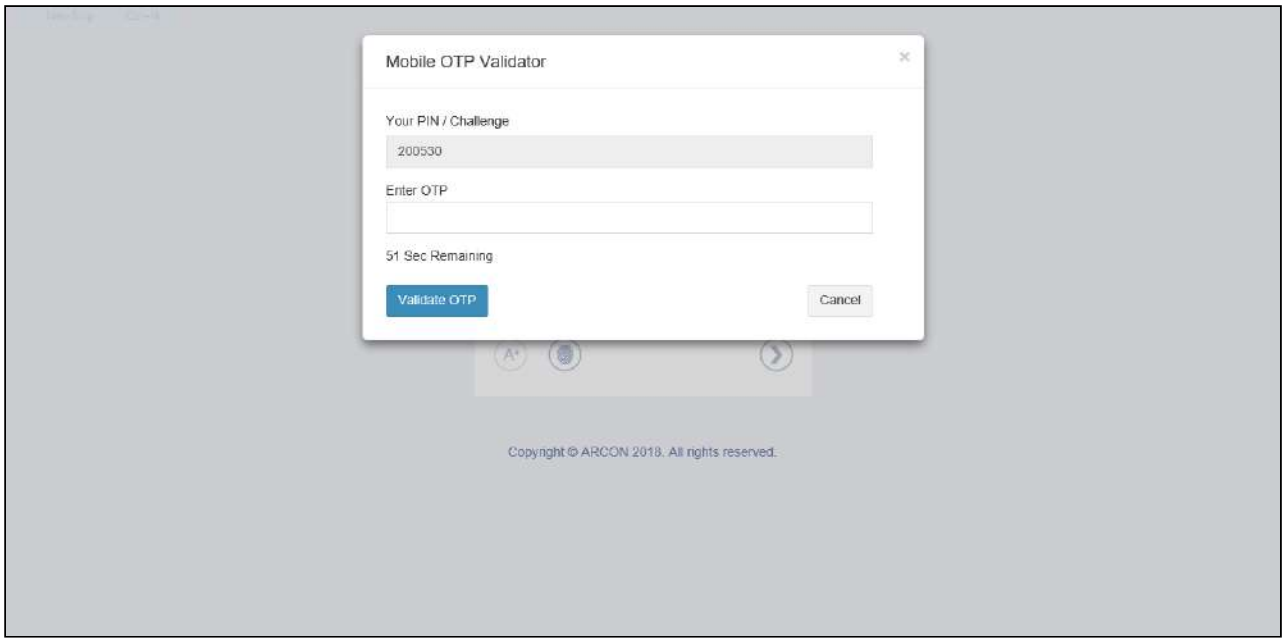
10. Click **Validate Code** button. A window pops up.



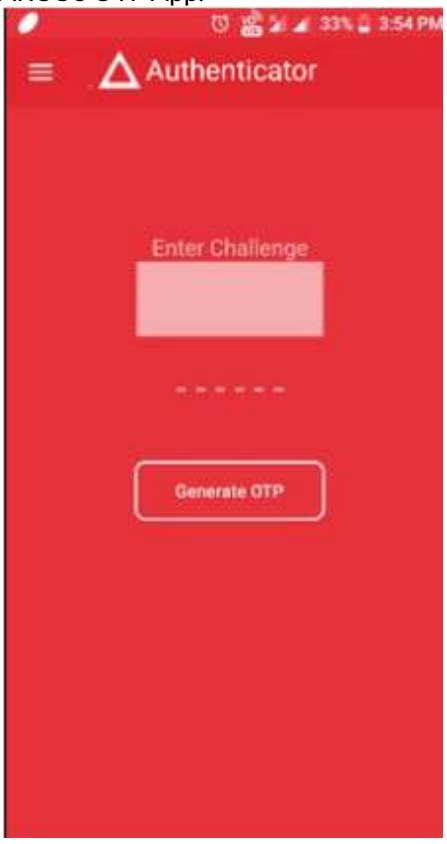
11. Click **OK** button. The mobile OTP is successfully configured.

4.2.3.1.2.3 Post Mobile OTP Configuration

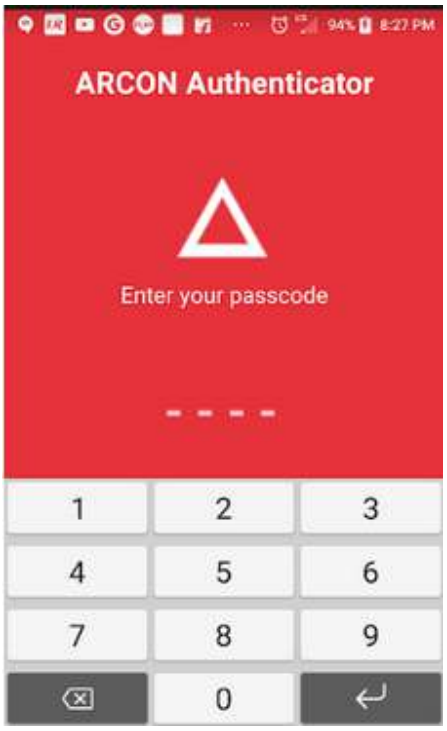
1. Enter the credentials in ARCON PAM Login screen and click on **Login** button, the **Mobile OTP Validator** pop up is displayed with **PIN/Challenge**.



2. User needs to enter the OTP. The OTP is generated in **ARCOS OTP** App.
3. The **Pin/Challenge** displayed in **Mobile OTP Validator** screen is entered in the **Enter Challenge** textfield in the ARCOS OTP App.

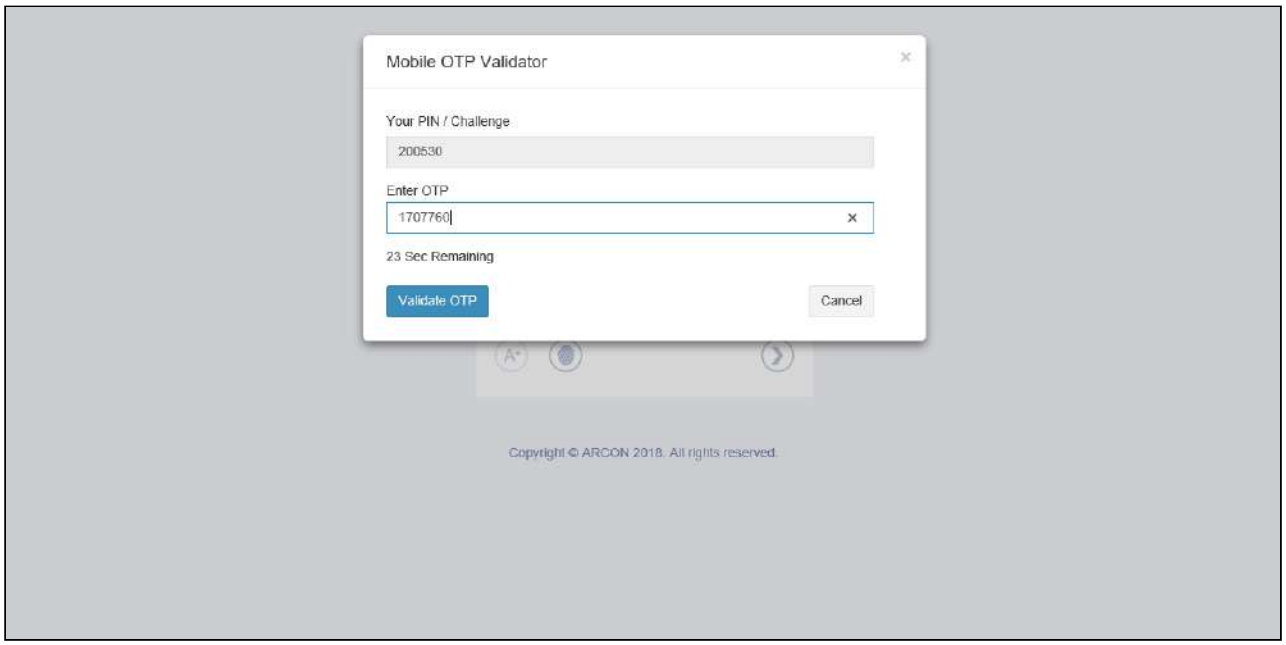


4. Click **Generate OTP** button to generate the OTP and enter the OTP in **Mobile OTP Validator** screen.



> ⚠ User needs to enter the OTP within 60 seconds for the given challenge or else the Pin/Challenge will change.

5. Click on **Validate OTP** button.



6. The user is allowed to successfully login to the application.

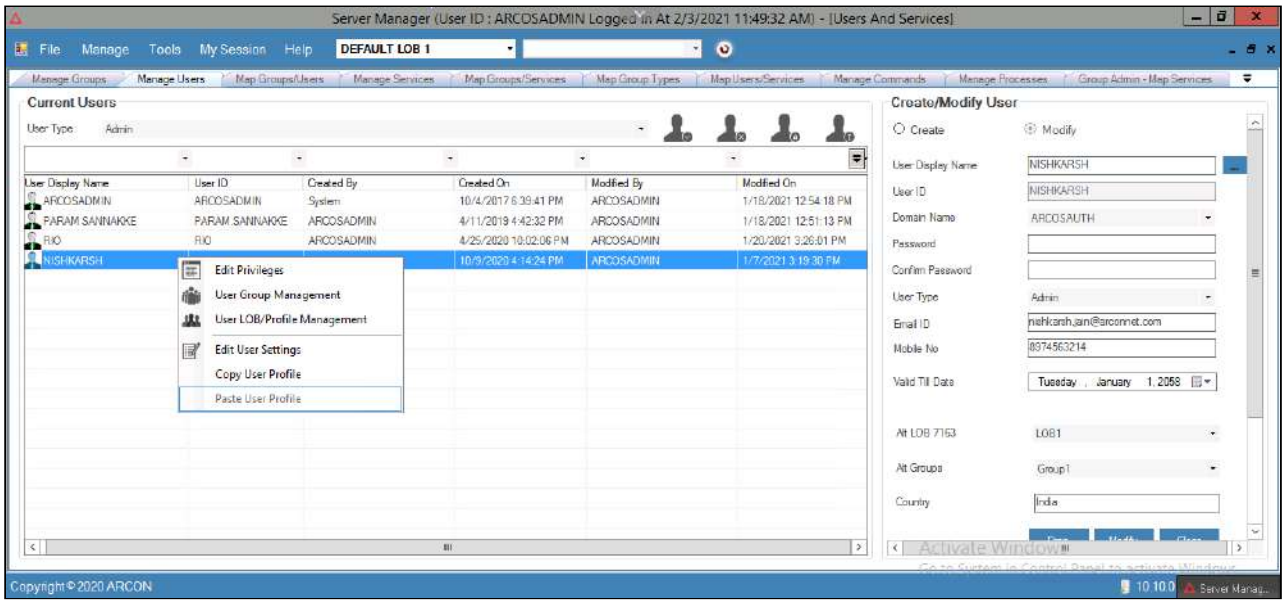
4.2.3.1.3 Configure SMS OTP

Dual-factor authentication makes the environment safer and more reliable. It helps to handle passwords in a secure way so authentication will only be available to authenticated people. Dual factor authentication means that during login the user has to provide two secure information such as his password and one time password he receives in SMS on his mobile phone. SMS OTP is one of the methods, wherein ARCON PAM user's receives OTP on registered mobile number.

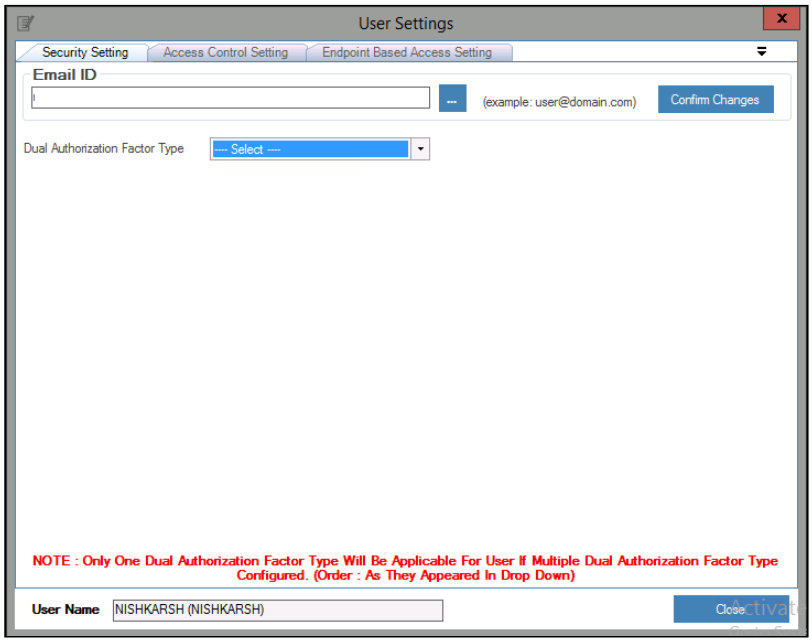
4.2.3.1.3.1 Configure SMS OTP

To configure SMS OTP, follow below steps:

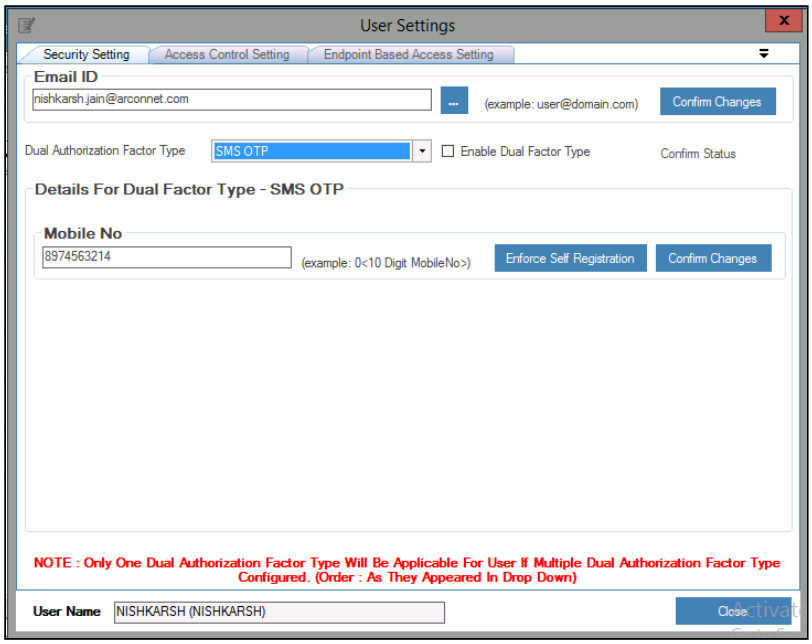
1. Right click on the user. A multiple options list is popped up.



2. Click on the **Edit User Settings** option. The **User Settings** screen is displayed.



3. Select the **Dual Authorization Factor Type** as **SMS OTP** from the dropdown list and then click on the **Enable Dual Factor Type** checkbox.

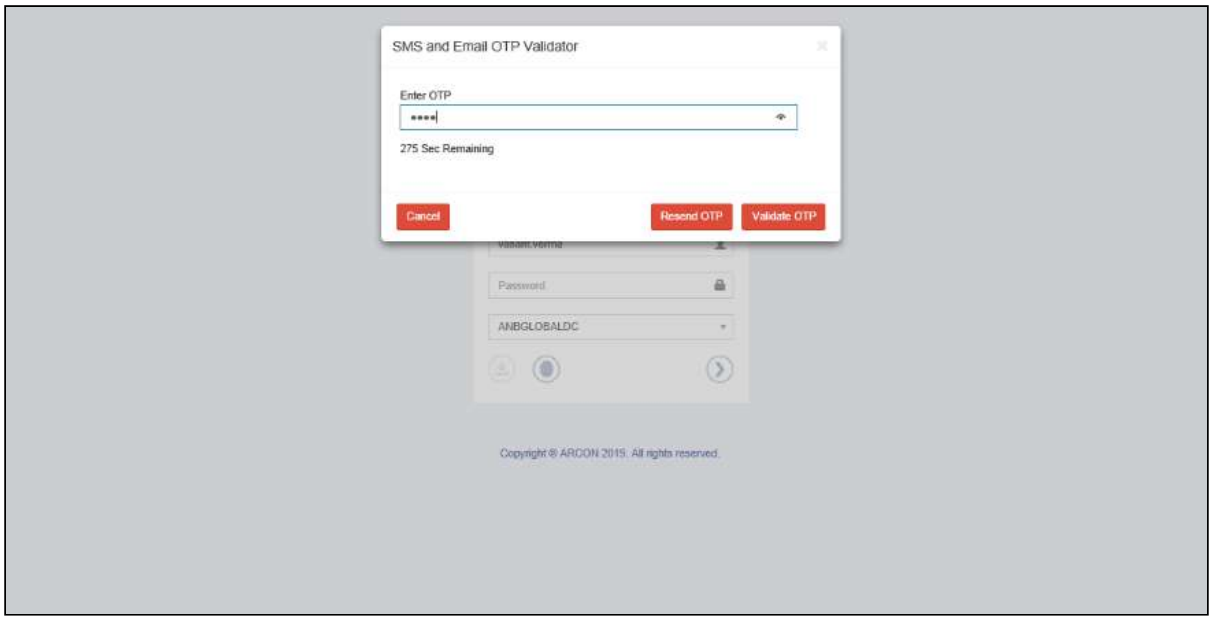


4. Click **Confirm Status** link then enter the 10 digit mobile number in **Mobile No** text field and click **Confirm Changes** button. A window pops up with the following message:
Do You Want To Change Dual Factor – SMS OTP Setting For Selected User?
5. Click **Yes** button, to confirm the changes.

⚠ Users will be locked out if wrong password is entered after the defined attempts. Settings for **SMS and Email OTP logout attempt** has been added to set a minimum and maximum value to consider for user lockout.

4.2.3.1.3.2 Post SMS OTP Configuration

1. Enter the credentials in ARCON PAM Login screen and click **Login**, the **SMS and Email OTP Validator** pop up is displayed.



2. Enter OTP received via SMS and click **Validate OTP**, to validate and login into ARCON PAM application.

> ⚠ **Resend OTP:** Click on **Resend OTP**, if OTP is not received via SMS for a long duration.

4.2.3.1.4 Configure Biometric Device

Biometric Device Configuration is a dual-factor authentication supported by ARCON PAM. It is performed by using biometric data (fingerprint) of the user. ARCON PAM acts as a strategic entry and identity management system for managing several system based user. It supports leading biometric devices such as 3M Cogent, Morpho, and Precision.

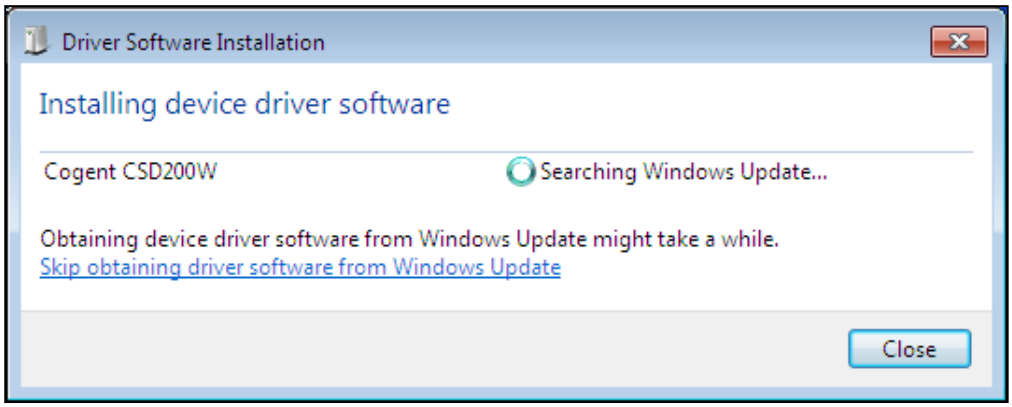
> ⚠ If the value in **Biometric – Finger Print – Minimum Match Score (Percentage)** is set between 0 to 100 in Settings, then the score of the fingerprint should be matched to the configured value while logging into the application.

4.2.3.1.4.1 Configure Biometric Device

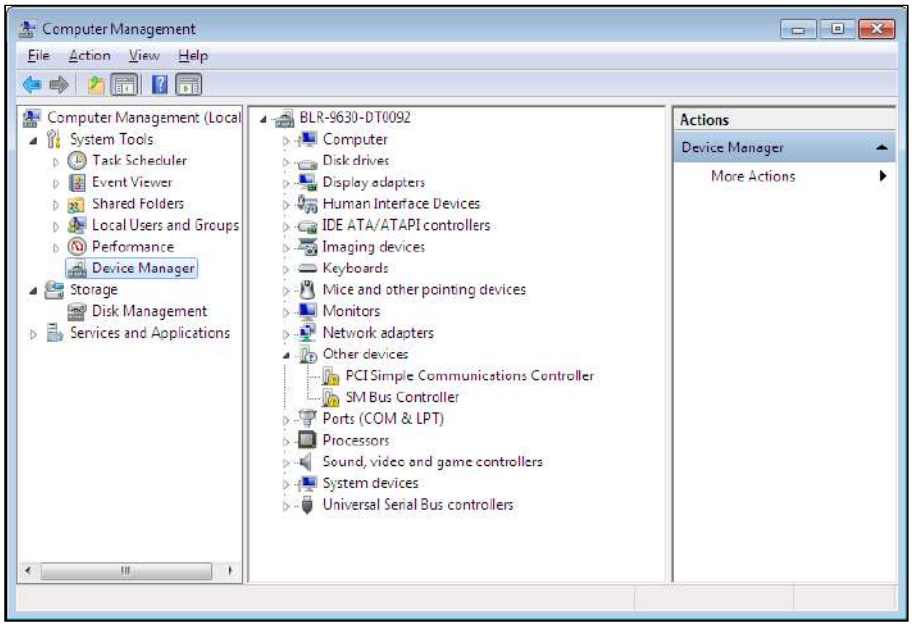
To configure the biometric device, you need to follow the below steps:

1. You need to install the driver of BIO Metrics in your local computer.

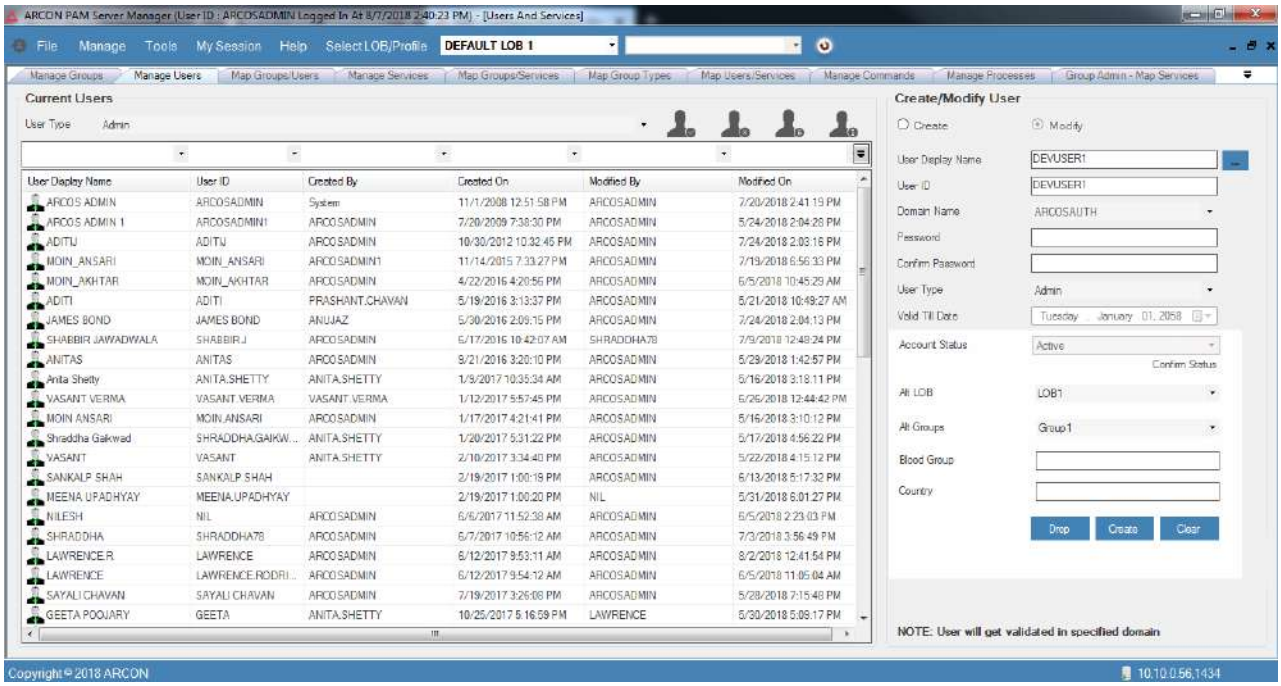
2. Install in local computer and then connect the device with local computer.



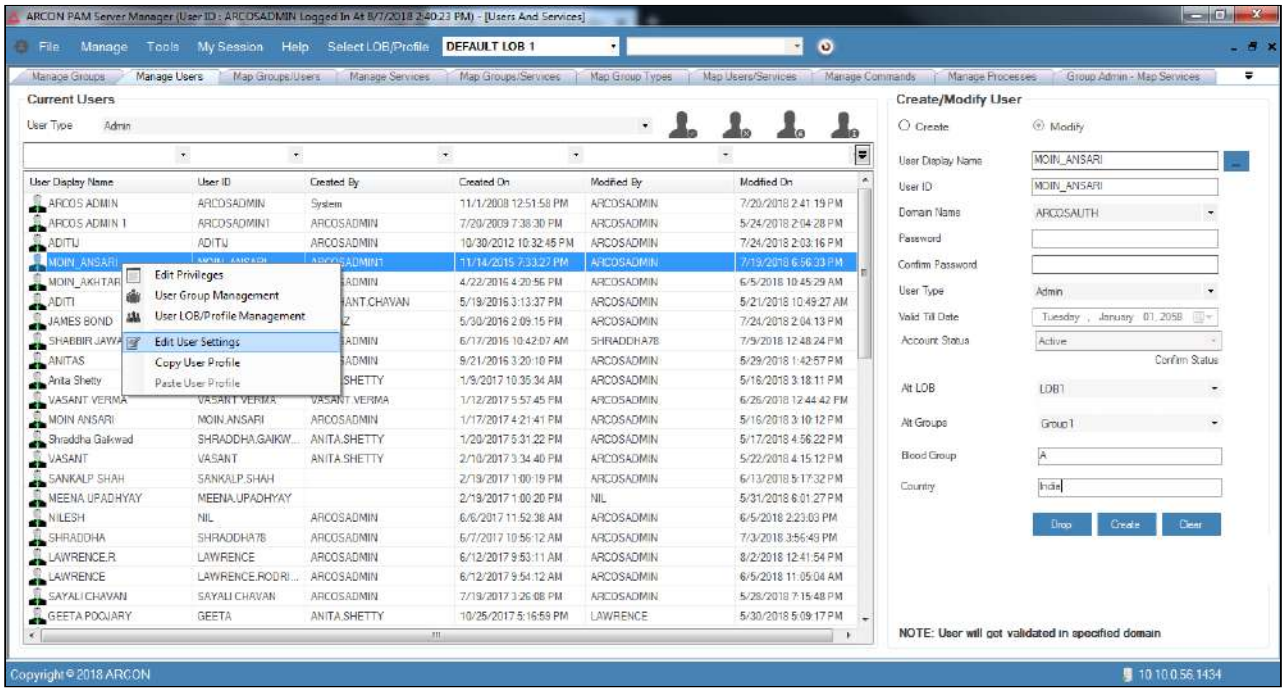
3. You need to check whether the device manager is installed in **Computer Management**.



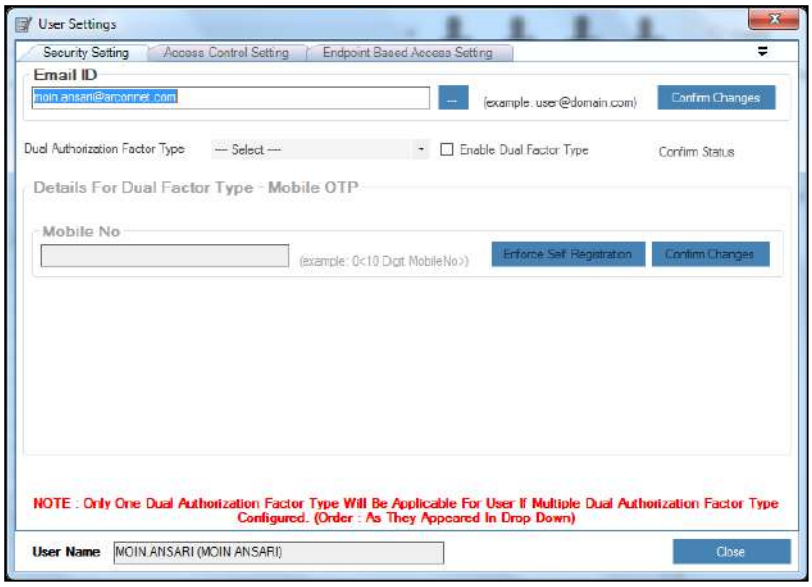
4. Check if the green light is displayed in the device.
5. Now configure the Biometric device on Server Manager for the individual user.



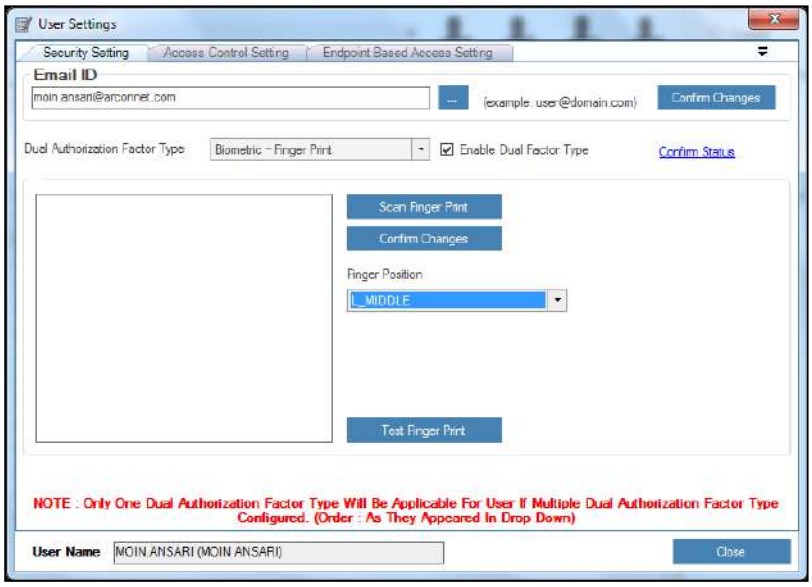
6. Right-click on the selected user. A multiple options list is popped up.



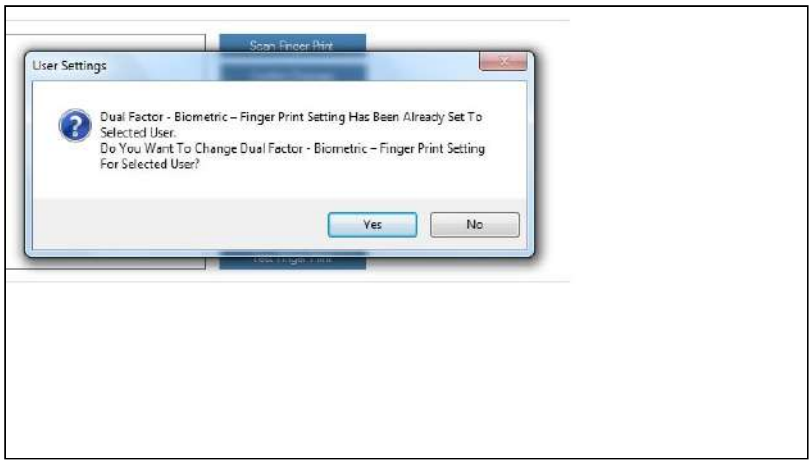
7. Click on the **Edit User Settings** option. The **User Settings** screen is displayed.



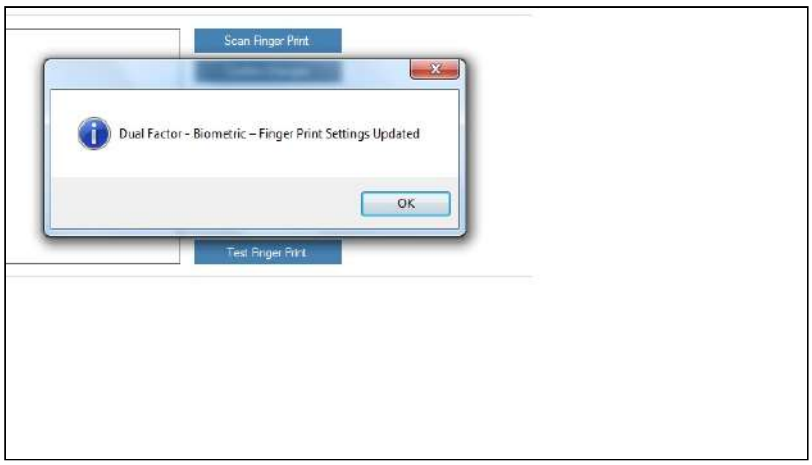
8. Select the **Dual Authorization Factor Type** as **Biometric – Finger Print** and then select the **Enable Dual Factor Type** checkbox.



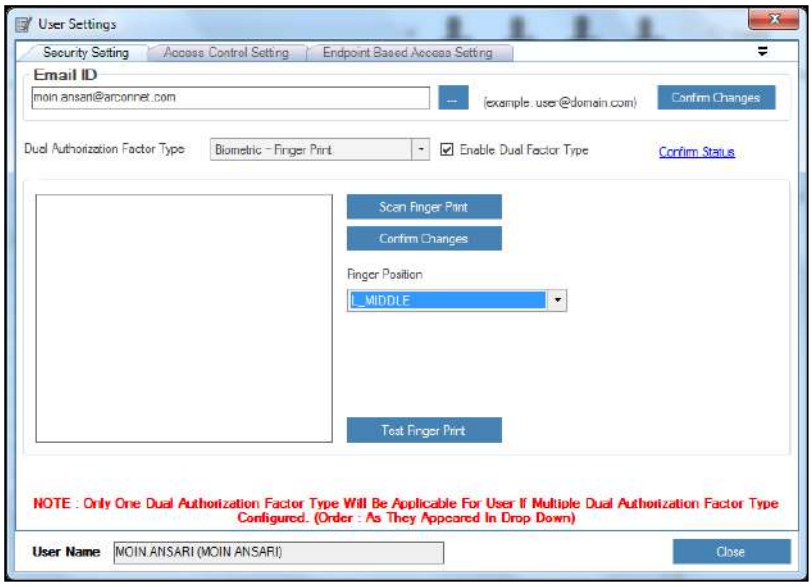
9. Click **Confirm Status** link. A window pops up.



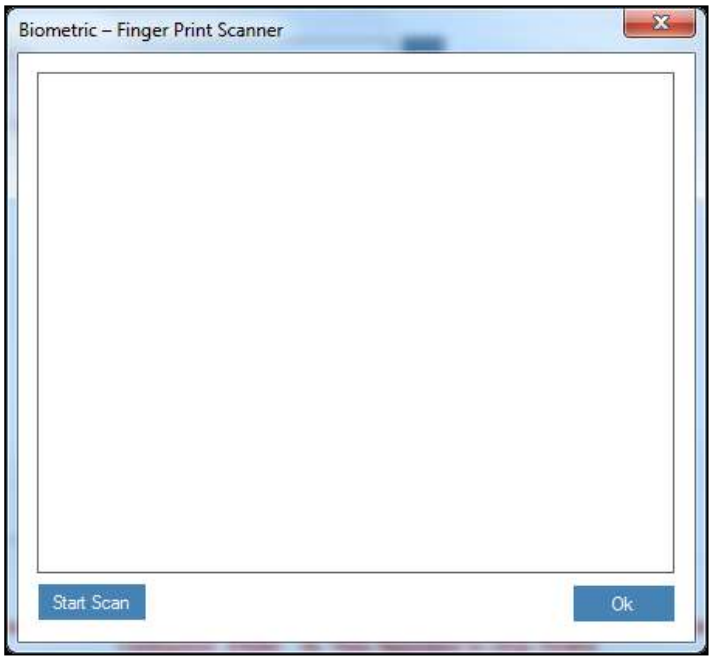
10. Click **Yes** button. Another window pops up.



11. Click **OK** button to enable the settings of dual-factor biometric fingerprint in ARCON PAM while logging into the application.

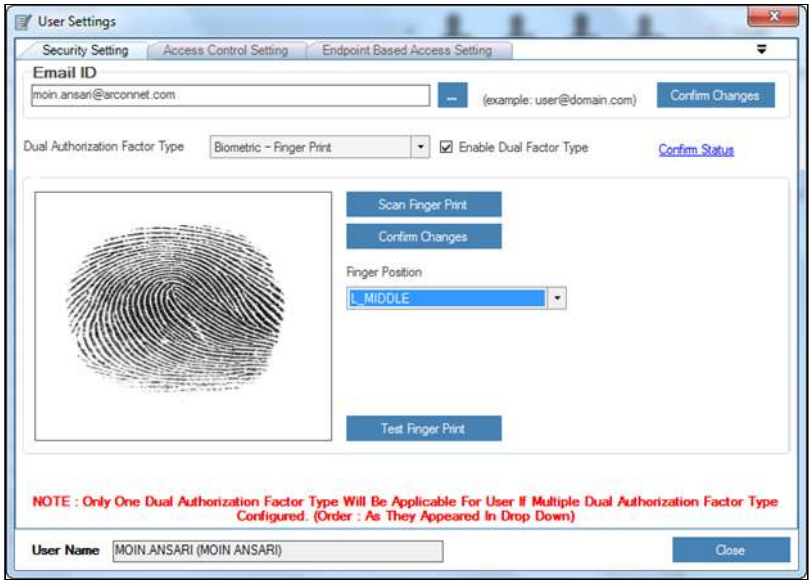


12. Select the finger position to be traced from **Finger Position** dropdown list and click **Scan Finger Print** button. A **Biometric – Finger Print Scanner** a window pops up.



13. Place the finger on the Biometric device and click **Start Scan** button, to scan the fingerprint. The fingerprint is traced on the **Biometric – Finger Print Scanner** screen.

14. Click **OK** button. The fingerprint is displayed in the Scanner.

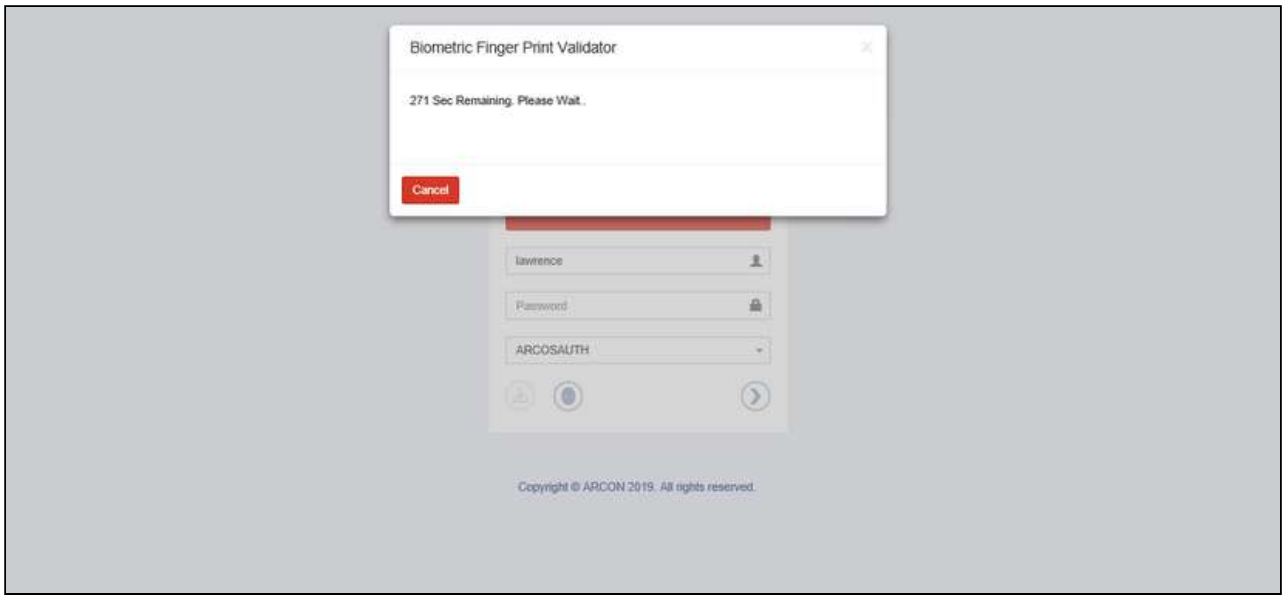


15. Click **Confirm Changes** button to save or enable the configuration.

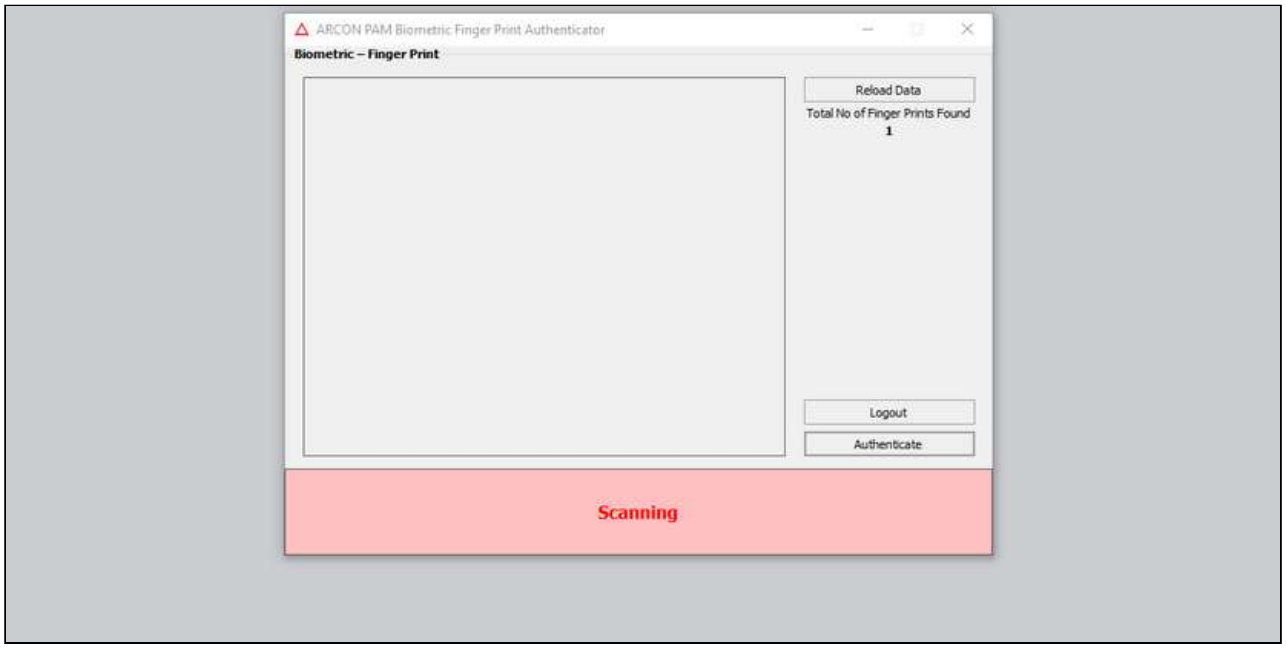
> ⚠ **Test Finger Print the** button is used to test the score of the fingerprint and if the score does not match with the configured value then an error message is displayed **Finger Print Does Not Match. Try Again.**

4.2.3.1.4.2 Post-Biometric Device Configuration

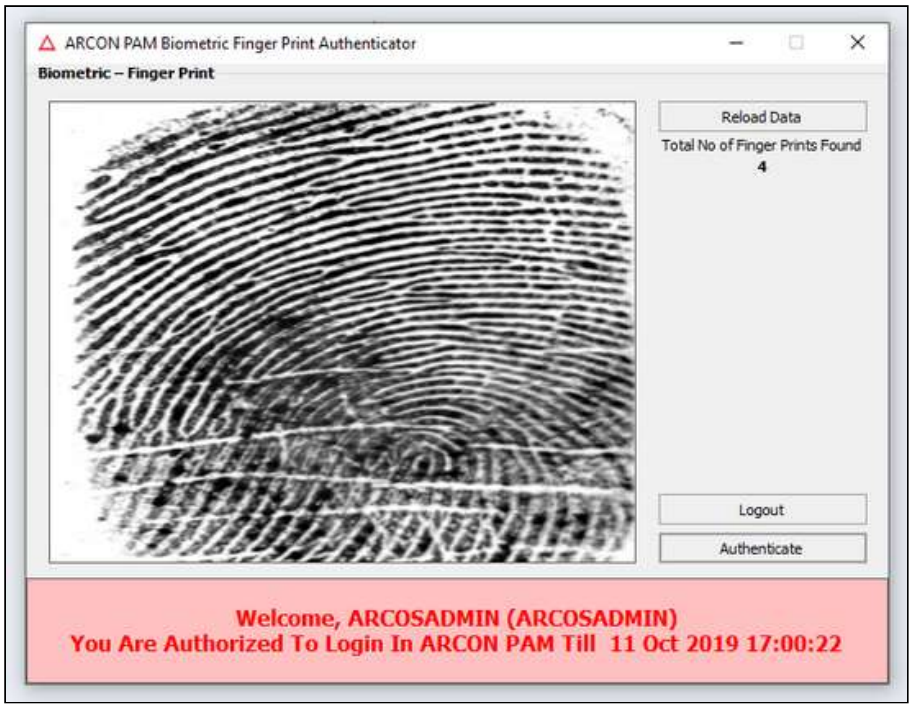
1. Enter the credentials in ARCON PAM Login screen and click **Login**, the **Biometric Finger Print Validator** pop up is displayed.



2. Within a few seconds, the **ARCON PAM Biometric Finger Print Authenticator** pop up is displayed.



3. Place the finger on the Biometric device. The fingerprint is traced on the **Biometric – Finger Print** screen as shown below:



4. The fingerprint is authenticated and User will be able to successfully login into ARCON PAM application.
5. If the traced fingerprint does not match, then you will view the following error message displayed in the below screen.

⚠ Configure **Biometric - Finger Print - Mode - Centralized Valid For (Minutes)** in Settings, to configure time in minutes for the validity of Finger Print.
If the value is Zero every time the user will have to identify through the biometric fingerprint.
If the value is 1 or above (minutes), it will bypass the biometric fingerprint for the defined time period after the first login.

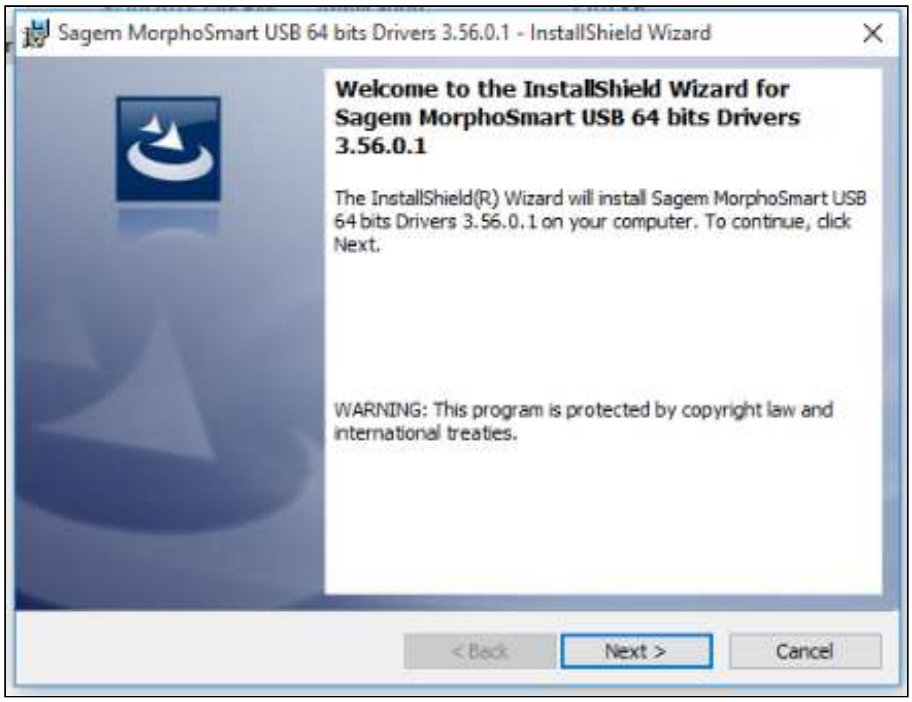
⚠ The following Settings can be configured to customize the requirements.

a. Biometric – Finger Print - Minimum Match Score (Percentage) - This configuration will allow setting, the percentage of minimum match score of Finger Print in Biometric Authentication. The minimum value is 0% and the maximum value is 100%
b. Biometric – Finger Print - Mode - This configuration sets the mode of Finger Print in Biometric Authentication.
    i. Desktop: In this mode, every ARCON PAM User should have an individual bio-metric device configured to their respective workstation, hence first the user login to the ARCON PAM portal with their respective credentials and then the biometric authentication is prompted.
    ii. Centralized: In this mode, the biometric device should be configured on a centralized location and every User will be authenticated with the centralized bio-metric device first and then are allowed to login into ARCON PAM Portal.
c. Biometric – Finger Print - Mode - Centralized Valid For (Minutes) - This configuration sets the time in minutes for the validity of Finger Print in Centralized Mode for Biometric Authentication. The minimum value is 1 minute and the maximum value is 480 minutes.
d. Biometric Devices - This configuration enables to set the type of biometric device that will be used. The value 1 is for Morpho, 2 for Precision, 3 for 3Mcognet/Gemalto, 4 for eikon Touch. 5 for Globalspace
e. Biometric Finger Print Authenticator Link On ACMO Login Page - Is Enabled -This configuration enables/disables Biometric Finger Print Authenticator Link on CM Login Page. Value '1' enables this link and '0' value disables it.

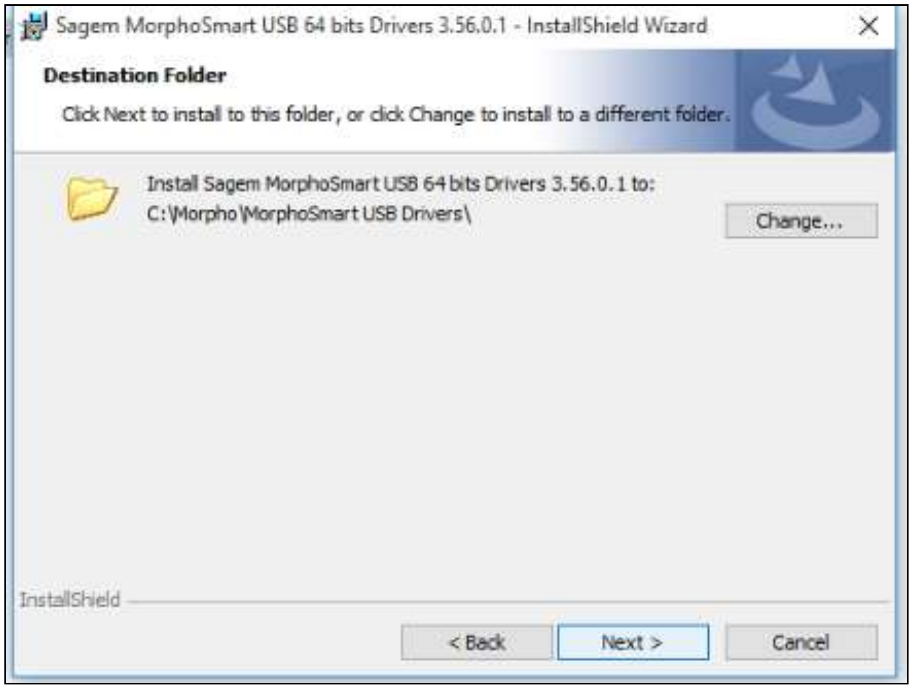
4.2.3.1.4.3 Morpho Biometric Device Installation

The steps for Morpho Biometric Device Installation are as follows:

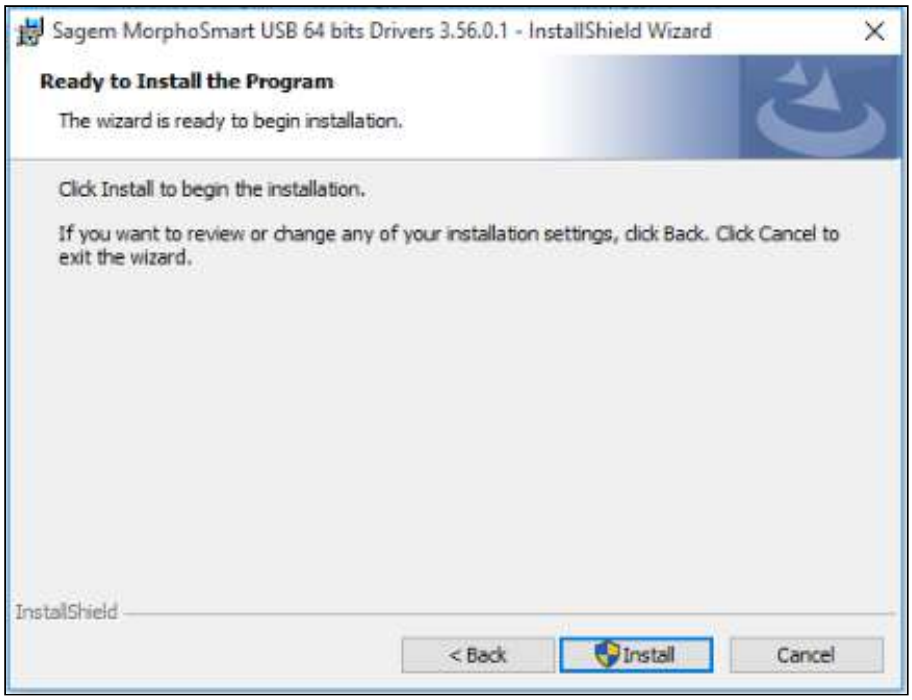
1. Double click on the **Morpho.**exe.



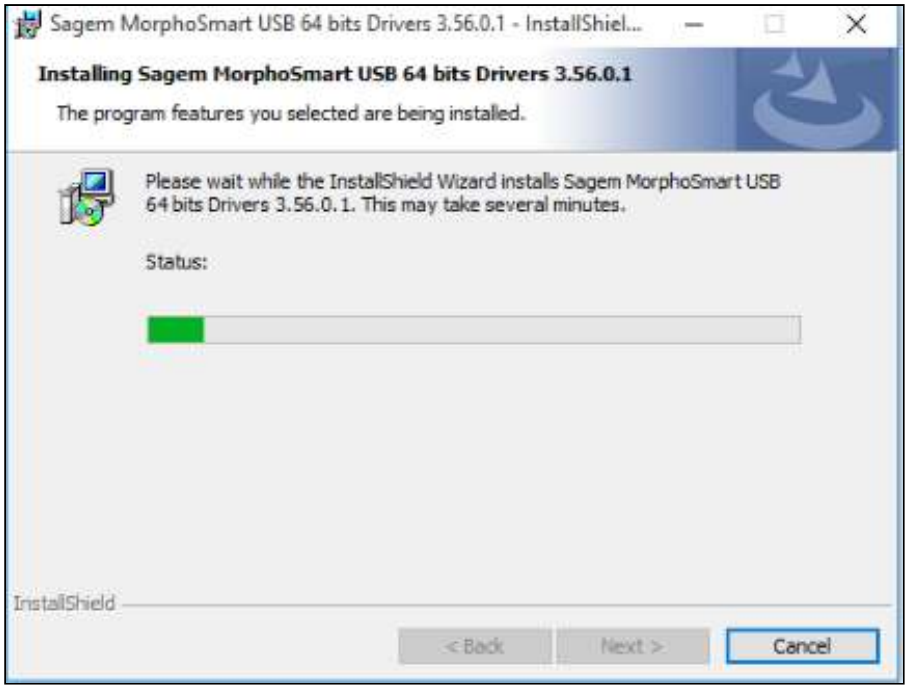
2. Click **Next**. Browse and select the required folder or location for installation.



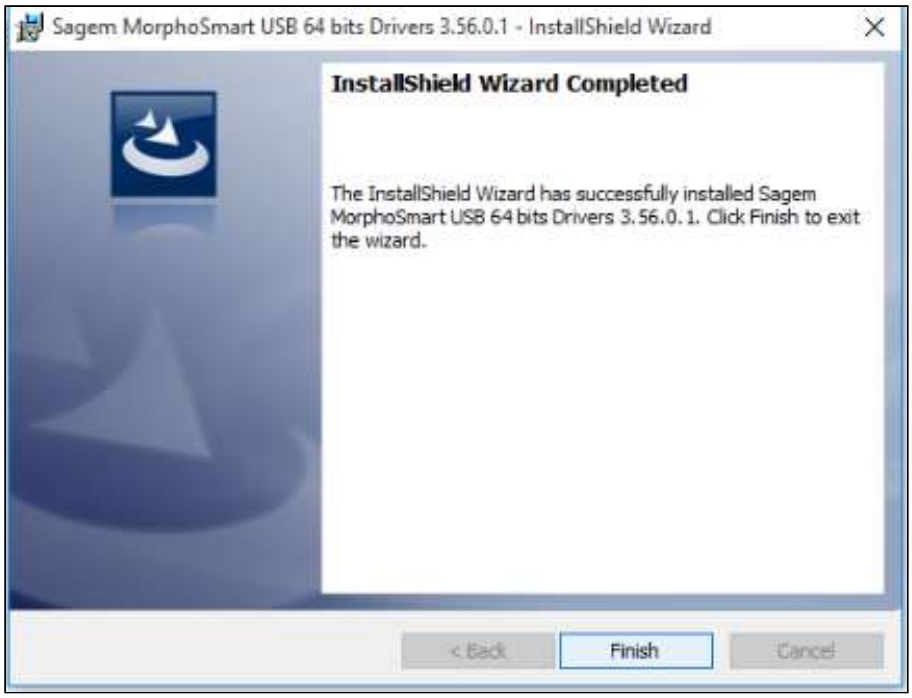
3. Click **Next**. The installer is ready to install the program on your computer.



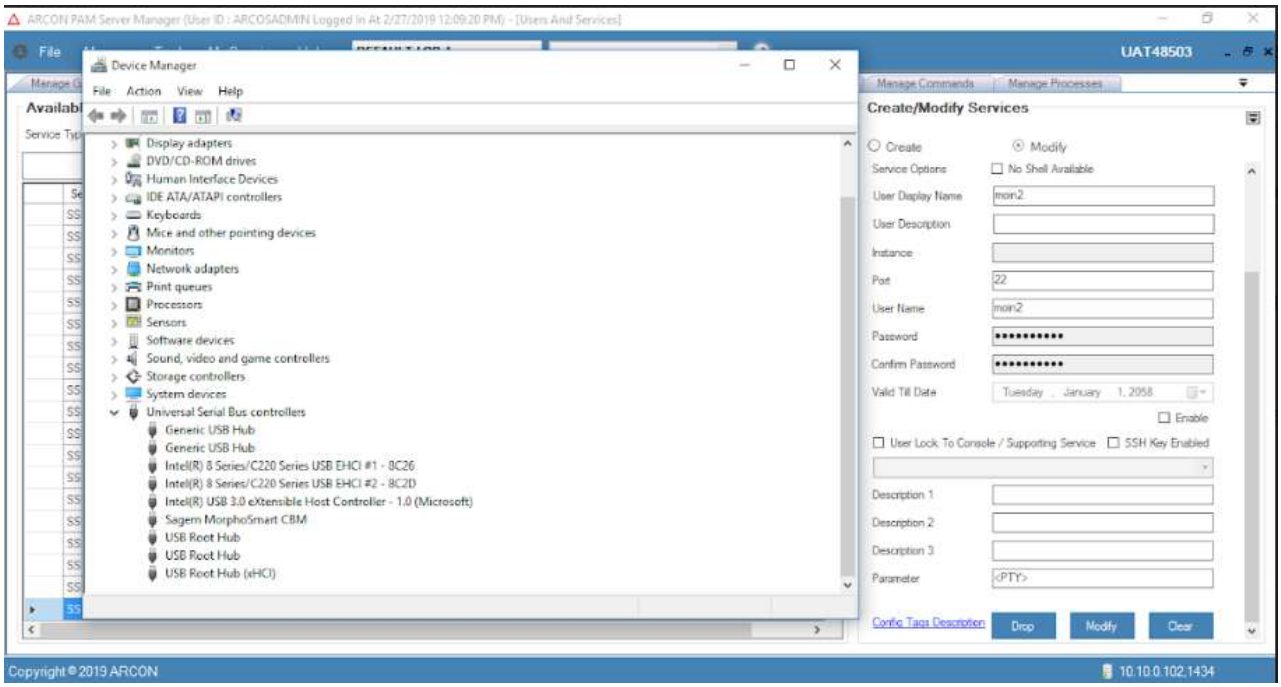
4. Click **Install** to start the installation.



5. The driver is being installed.



6. Click **Finish**, once the driver has been successfully installed, you need to check whether the driver is installed in the device manager.



7. Check if green light is displayed in the device. Now configure the Biometric device on Server Manager for individual user.

4.2.3.1.5 Configure Hardware Token

A Hardware token is a security token which may be a physical device that an authorized User of computer services is given, to ease authentication. It may be a small hardware device that the owner carries to authorize access to a

network service. In ARCON PAM, RADIUS servers are used for authentication of a RSA portal. RADIUS is a protocol similar to LDAP, DCPIP, and RDP protocol. Similarly, RADIUS is a kind of protocol that helps to communicate with another server.

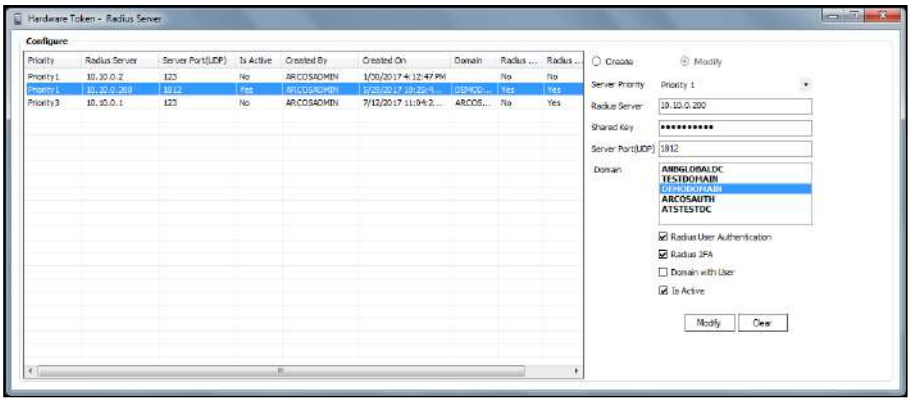
- The Administrator having **Hardware Token – RADIUS Server** privileges in Server's Privileges, will only be able to enable or configure values for Hardware Token.
- You need to configure values for **Hardware Token RADIUS Server** and **Dual Factor IP Range,** before enabling Hardware Tokens which work on RADIUS protocol as a second factor of authentication.

4.2.3.1.5.1 Configure Hardware Token

A. Hardware Token RADIUS Server Configuration:

To configure values for Hardware Token RADIUS Server, use the following path:

Tools → Advanced Configuration → Hardware Token – Radius Server



The **Hardware Token – RADIUS Servers** contains the following fields:

Field Name	Description
Create (radio button)	Configure new radius server details.
Modify (radio button)	Modify or update the radius server details.
Server Priority	Select the server priority. The server priority can be configured up to three servers, if those many servers are available in the environment as part of HA (High Availability).
Radius Server	Enter the IP address of the RADIUS Server.
Shared Key	Enter the shared key of the RADIUS Server.
Server Port (UDP)	Enter the port (UDP) number of the RADIUS Server.
Domain	Select the domain name of the RADIUS Server.

Field Name	Description
Radius User Authentication (checkbox)	If enabled will check whether the user is in **ActiveDirectory** of the **RADIUS Server**. ⚠ If **Radius User Authentication** is enabled, by default **Radius 2FA** will be enabled due to which while logging into the application, the user will be authenticated twice once for **ADauthentication** and then through **Dual FactorAuthentication**.
Radius 2FA	Enables Dual Factor Authentication. ARCON PAM supports two types of tokens, which are as follows: • **Hardware Token:** A random token is generated when you press the key in the Hardware Device, which is entered in 2FA prompt while logging into ARCON PAM. The token entered is authenticated with the RADIUS Server. Once authenticated, the User will be able to login into the application. • **Software Token:** A RADIUS Windows application available with the User on his/her local machine contains a random token, which is entered in 2FA prompt while logging into ARCON PAM. The token entered is authenticated with the RADIUS Server. Once authenticated, the User will be able to login into the application.
Domain with User	Select **Domain with User** checkbox, if multiple domains are configured on RADIUS Server. The User has to specify Domain Name with User Name while 2FA authentication.
Is Active	To enable the configuration in ARCON PAM.

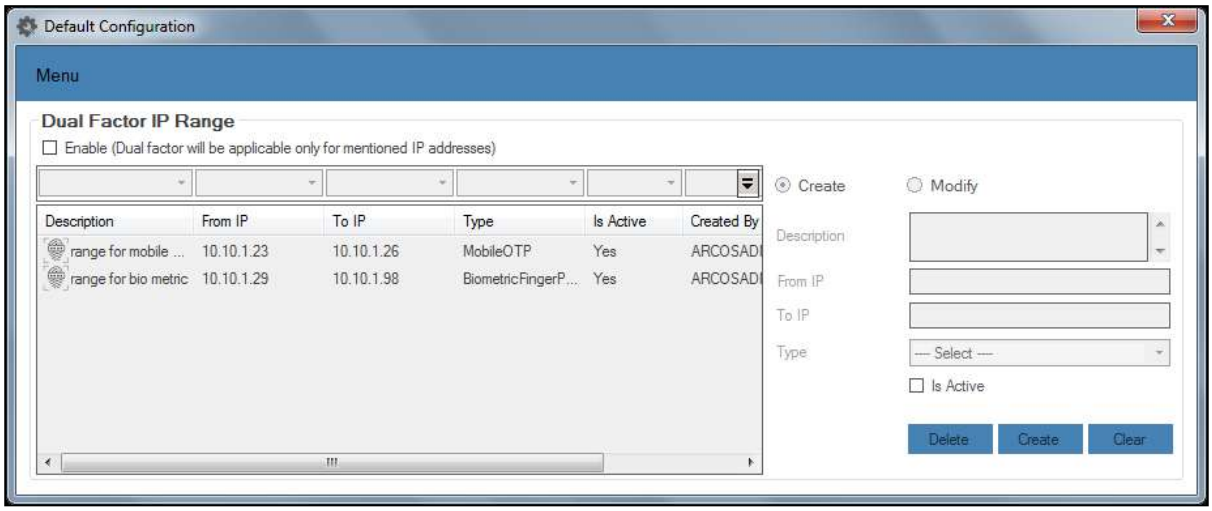
1. Select or Enter the details and click on **Create** button to configure the RADIUS Server.

B. Dual Factor IP Range Configuration:

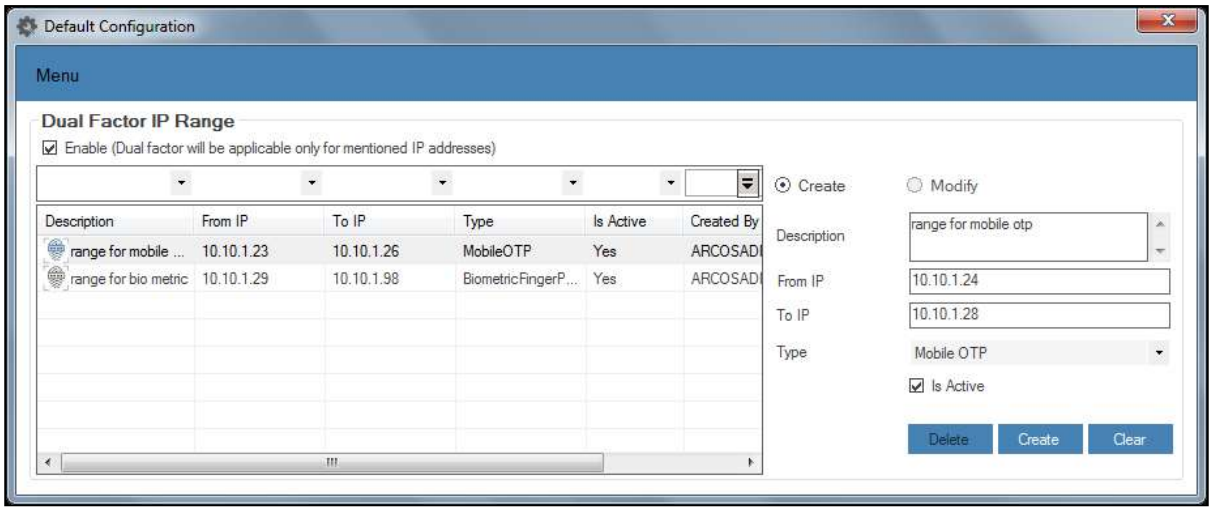
Dual Factor IP Range helps you to define the range of IP Address to be configured for the 'Dual Factor type'. Once configured, ARCON PAM will prompt for the second factor authentication to the End User only if the User is from the configured IP range.

⚠ The Administrator having **Default Configuration** and **Dual Factor IP Range** privileges in ARCON PAM Server's Privileges, will only be able to configure values for Dual Factor IP Range.

1. Select the **Enable** (Dual factor will be applicable only for mentioned IP addresses) checkbox.



2. A window pops up with the following message:
   Confirm Changes?
3. Click **Yes.** The fields are enabled to configure dual factor IP range.



The **Dual Factor IP Range** screen contains the following fields:

Field Name	Description
Create (radio button)	To create a dual factor IP range of machine.
Modify (radio button)	To modify or update an existing dual factor IP range. ⚠ To modify details of dual factor IP range, select the required dual factor IP range from the grid on the left pane. The details are displayed on the right side. Modify the required details and click **Modify** button, to update the IP address of the machines.
Description	Enter description for the dual factor IP range.
From IP	Enter IP address to set the start range for dual factor.

Field Name	Description
To IP	Enter IP address to set the end range for dual factor.
Type	Select the type of dual factor authentication.
Is Active	Click to enable the configuration in ARCON PAM.
Delete	Click **Delete**, to delete the configured dual factor IP Range. ⚠ To delete a dual factor IP range, select the required dual factor IP range from the grid on the left pane. The details are displayed on the right side. View the details and click **Delete** button, to delete the details.

4. Select/ Enter the details and click on **Create** button to define a dual factor IP range.

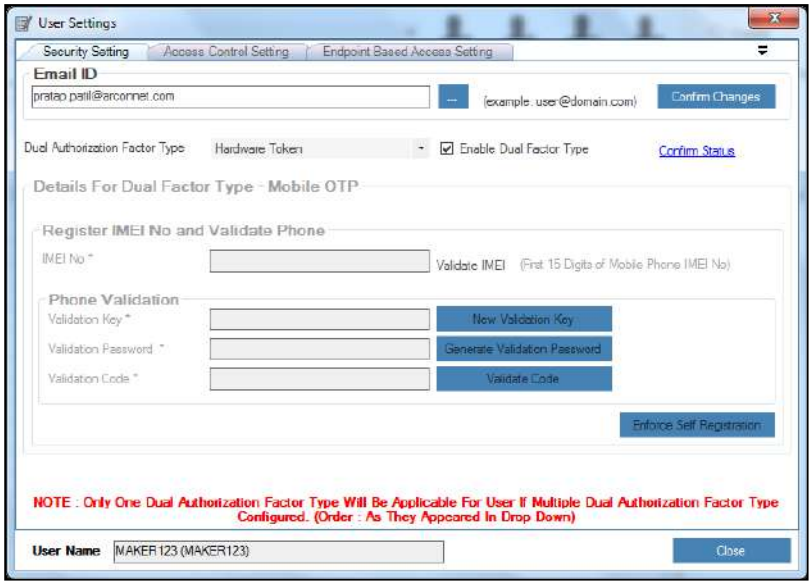
⚠
- The user is authenticated on login screen of **ARCON PAM Client Manager**, once the dual factor IP range is configured.
- Once both the values for **Hardware Token RADIUS Server** and **Dual Factor IP Range** are configured, you need to enable the configuration for **Hardware Token** in **User Settings** screen.

C. Enable Hardware Token Configuration:

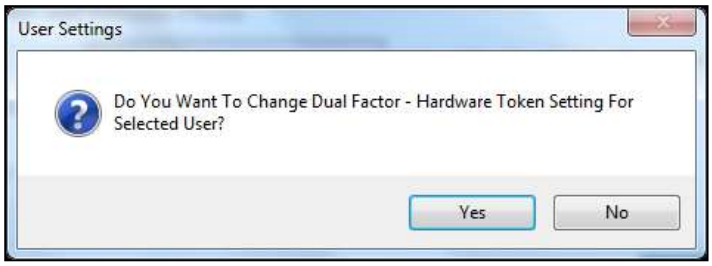
To enable the configuration for Hardware Token use the following path:

Manage → Users and Services → Manage Users → Right click on the User → Edit User Settings option.

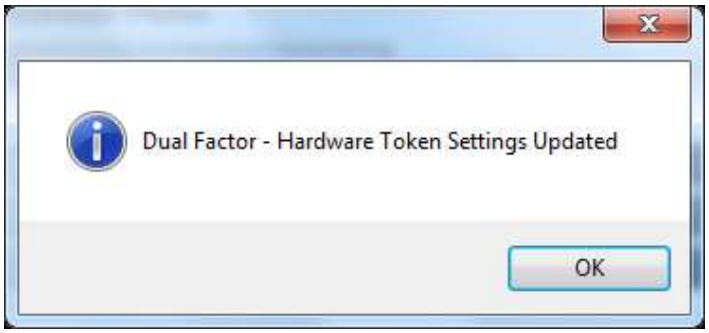
1. Select the **Dual Authorization Factor Type** as **Hardware Token** and then select the **Enable Dual Factor Type** checkbox.



2. Click **Confirm Status** link. A window pops up.



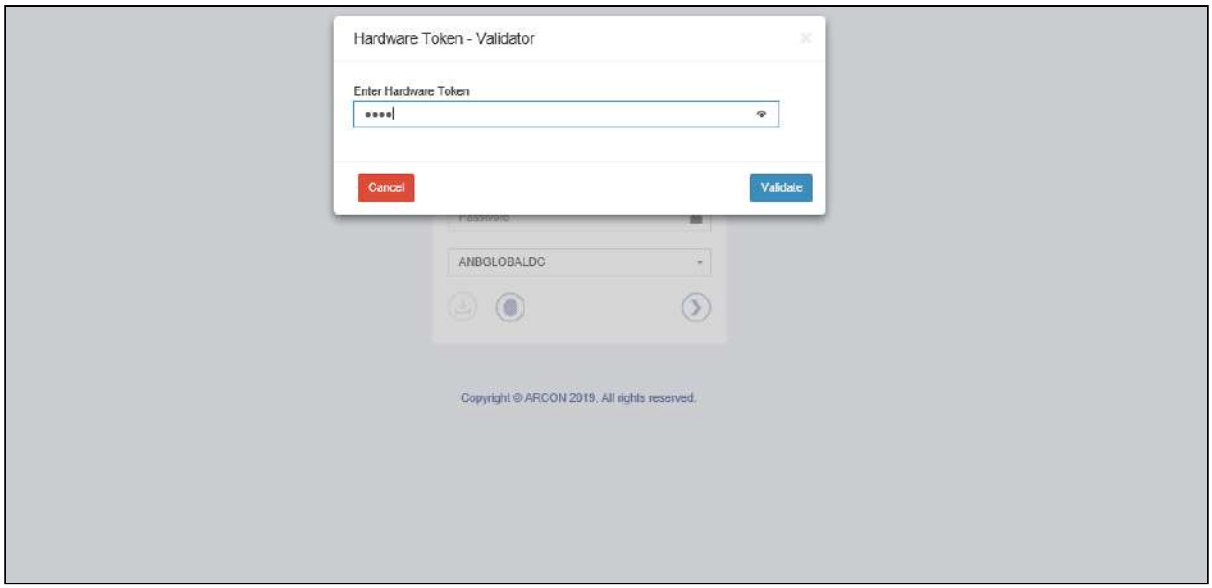
3. Click **Yes** button. Another window pops up.



4. Click **OK** button. The **Dual Factor Hardware Token** is enabled for the selected User.

4.2.3.1.5.2 Post Hardware Token Configuration

1. Enter the credentials in ARCON PAM Login screen and click **Login**, the **Hardware Token - Validator** pop up is displayed.



2. Enter OTP received via Email and click **Validate**, to validate and login into ARCON PAM application.

4.2.3.1.6 Configure Email OTP

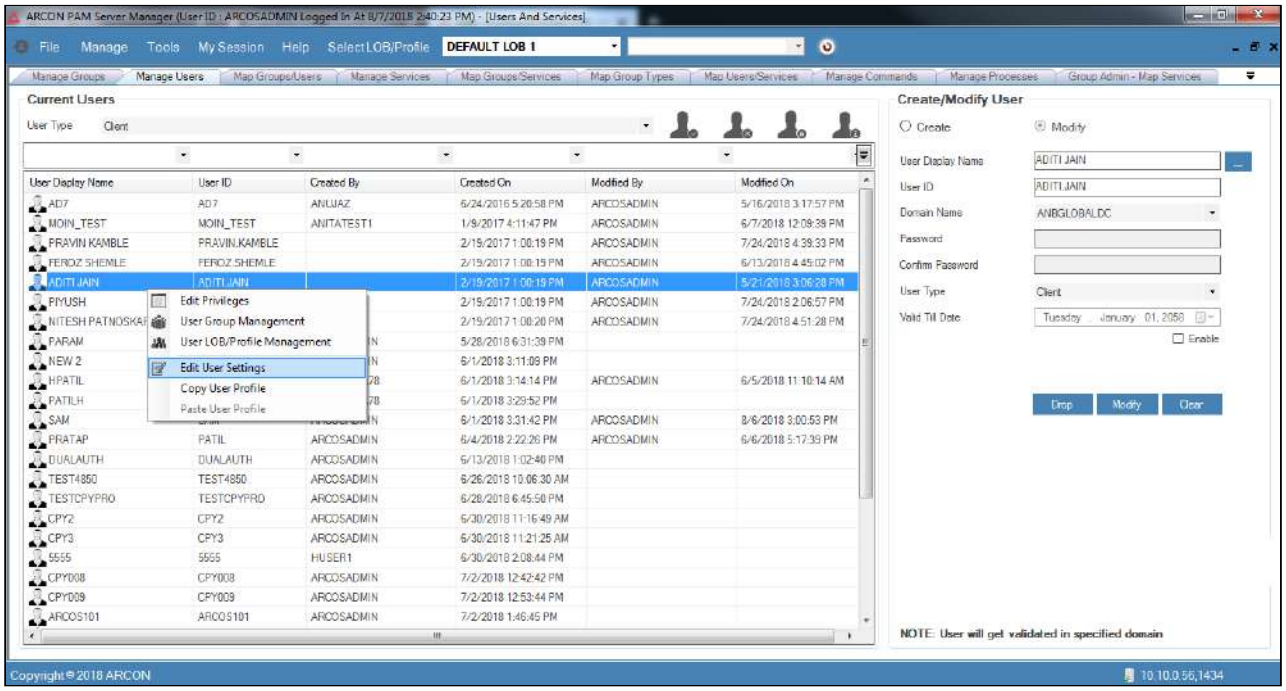
Dual-factor authentication makes the environment safer and more reliable. It helps to handle passwords in a secure way so authentication will only be available to authenticated people. Dual factor authentication means that during

login the user has to provide two secure information such as his password and one time password he receives in Email. Email OTP is one of the methods, wherein ARCON PAM user's receives OTP on registered email address.

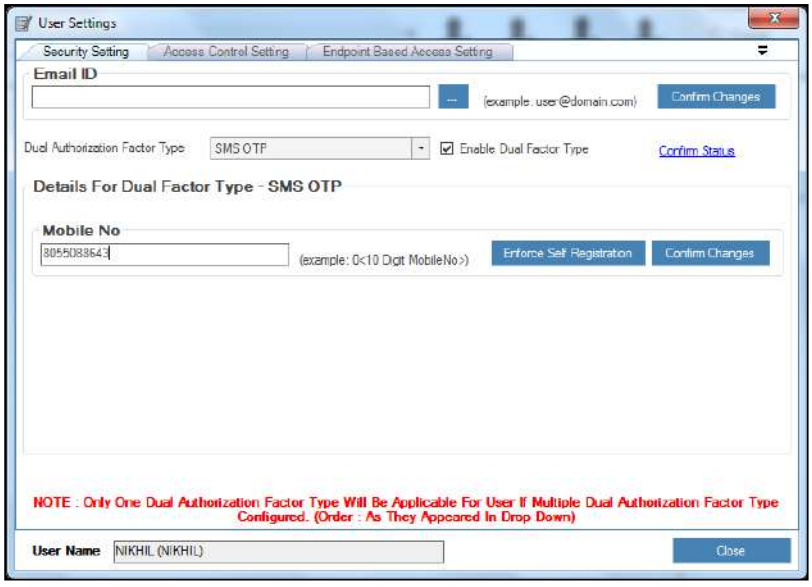
4.2.3.1.6.1 Configure Email OTP

To configure Email OTP, follow below steps:

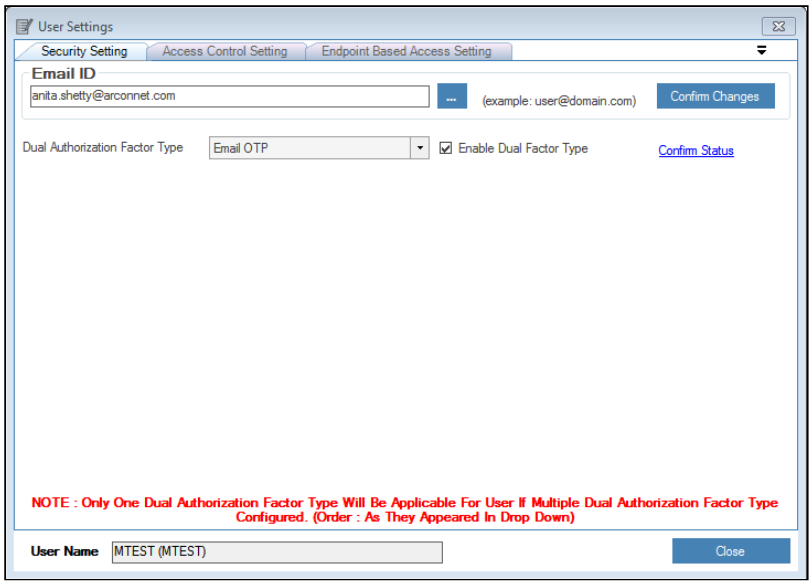
1. Right click on the user. A multiple options list is popped up.



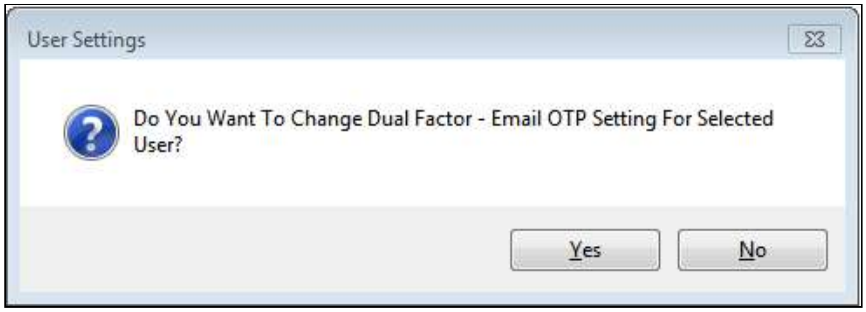
2. Click on the **Edit User Settings** option. The **User Settings** screen is displayed.



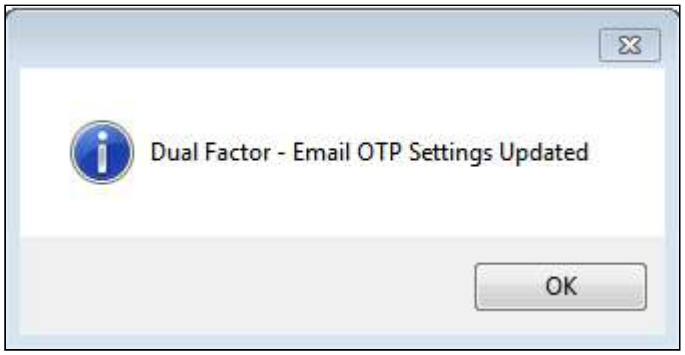
3. Select the **Dual Authorization Factor Type** as **Email OTP** from the drop down list and then click on the **Enable Dual Factor Type** checkbox.



4. Enter email address in the Email ID text field and click **Confirm Status link**. A window pops up with the following message will be displayed:



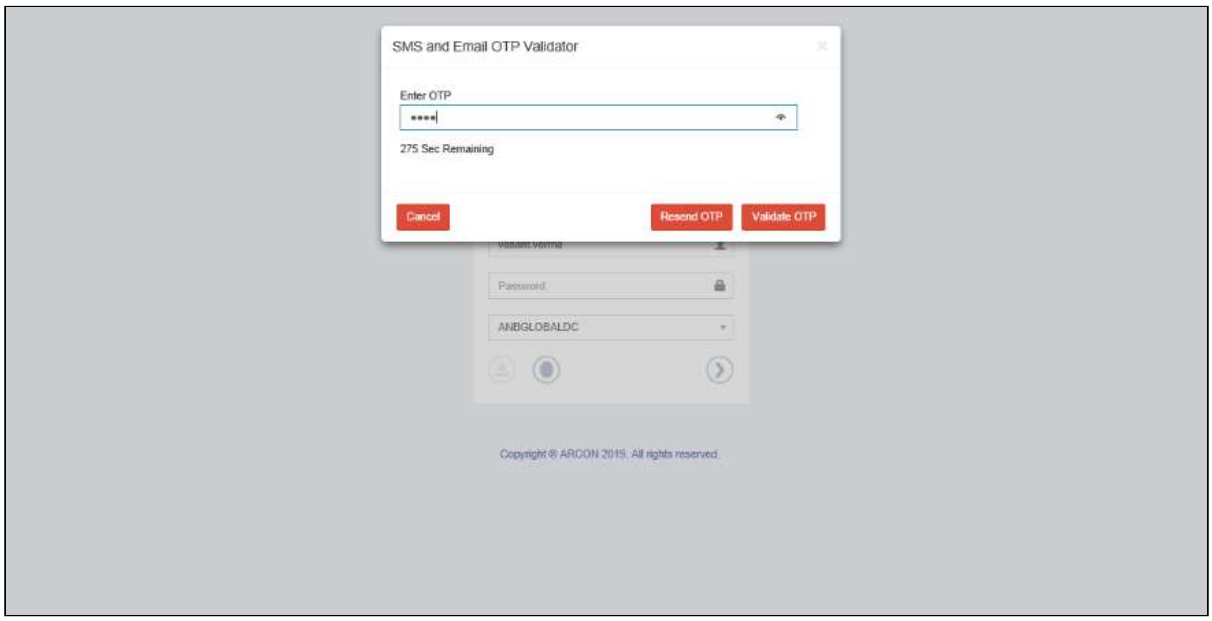
5. Click **Yes** button, to confirm the changes. The following message will be displayed on screen.



⚠ Users will be locked out if wrong password is entered after the defined attempts. Settings **SMS and Email OTP logout attempt** has been added to set a minimum and maximum value to consider for user lockout.

4.2.3.1.6.2 Post Email OTP Configuration

1. Enter the credentials in ARCON PAM Login screen and click **Login**, the **SMS and Email OTP Validator** pop up is displayed.



2. Enter OTP received via Email and click **Validate OTP**, to validate and login into ARCON PAM application.

> ⚠ **Resend OTP:** Click on **Resend OTP**, if OTP is not received via Email for a long duration.

4.2.3.1.7 Configure Voice Biometric

Voice Biometric Authentication is a type of Dual Factor Authentication which uses Web Service for authenticating user before logging into Client Manager. The predefined web service authentication is configured, which will authenticate the user through his voice and decide whether to allow the user to login or not.

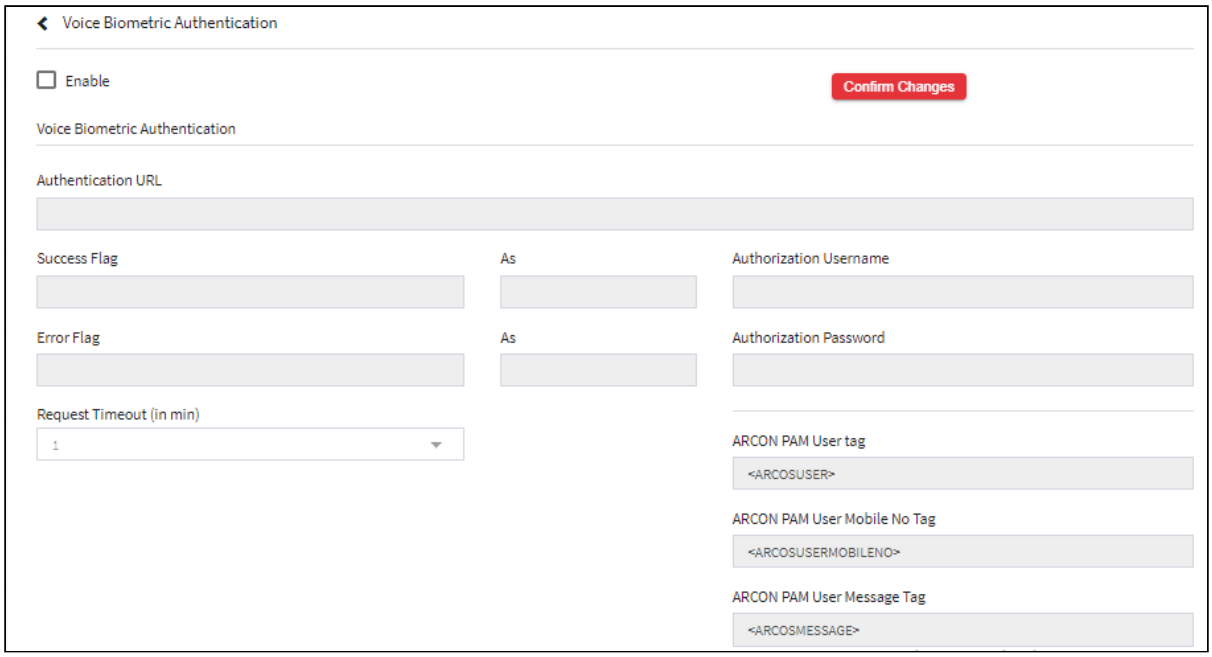
> ⚠
> - The Administrator having **Default Configuration** and **Voice Biometric Authentication** privileges in **Server's Privileges** will only be able to configure values for Voice Bio Metric Configuration.
> - You need to configure values for **Voice Biometric Authentication** and **Dual Factor IP Range,** before enabling Vioce Biomatric Authentication as a second factor of authentication.

A. Voice Biometric Authentication Configuration:

To Navigate use the following path:

Settings → Group → 2FA → BIOMETRIC

1. Select Voice Biometric Configuration
2. Select **Enable** checkbox. The fields are enabled to configure voice biometric authentication.



The **Voice Biometric Authentication** screen displays the following fields:

Field Name	Description
Authentication URL	It is in the predefined .xml format.
Success Flag	Configure success flag. The valid values are: ▪ True ▪ False
Error Flag	Configure error flag. The valid values are: ▪ True ▪ False
Authorization Username	Authorized user name used to access the specified URL.
Authorization Password	Password used to access the specified URL.
Request Timeout (in min)	Select the session timeout in minutes.

3. Few fields are customizable according to requirement. The ARCON PAM User Tag, ARCON PAM User Mobile No. Tag and ARCON PAM Message Tag can be configured with user details, user mobile number and message to be sent.
4. Select/Enter the details and click **Confirm Changes** to configure the details.

B. Dual Factor IP Range Configuration:

Dual Factor IP Range helps you to define the range of IP Address to be configured for the 'Dual Factor type'. Once configured, ARCON PAM will prompt for the second factor authentication to the End User only if the User is from the configured IP range.

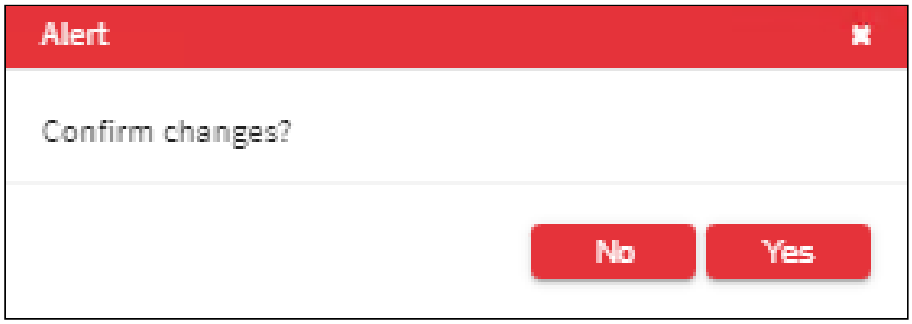
> The Administrator having **Default Configuration** and **Dual Factor IP Range** privileges in ARCON PAM Server's Privileges, will only be able to configure values for Dual Factor IP Range.

To Navigate use the following path:

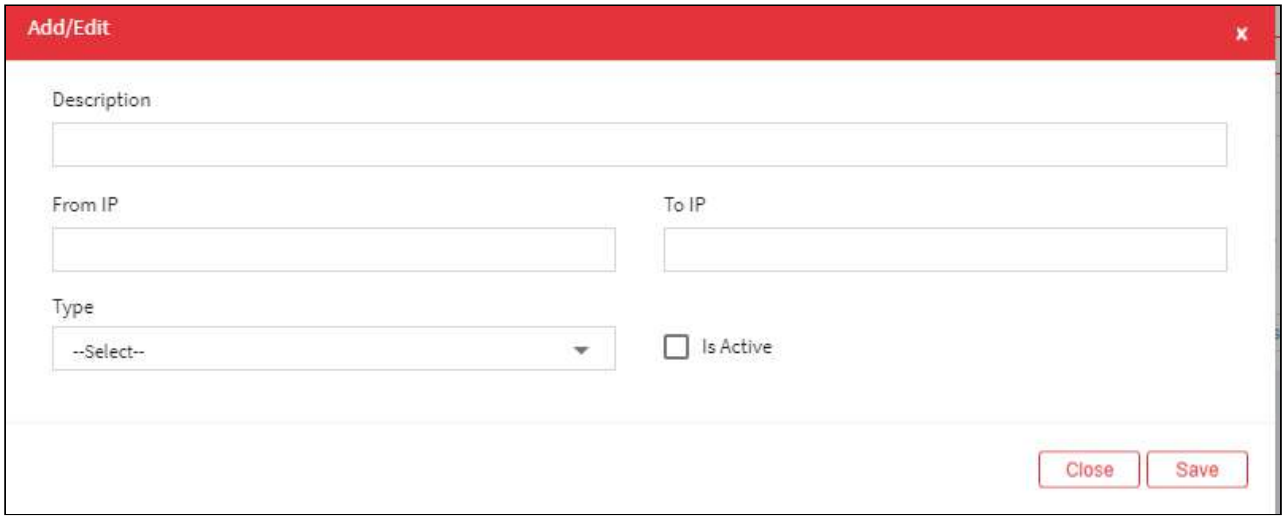
Settings → Group → 2FA

1. Select **Enable** (Dual factor will be applicable only for mentioned IP addresses) checkbox.

2. Select the **Enable** (Dual factor will be applicable only for mentioned IP addresses) checkbox. A window pops up with the following message: **Confirm Changes?**



3. Click **Yes.** The fields are enabled to configure the IP range.
4. Select the Add button to add a new Dual Factor.

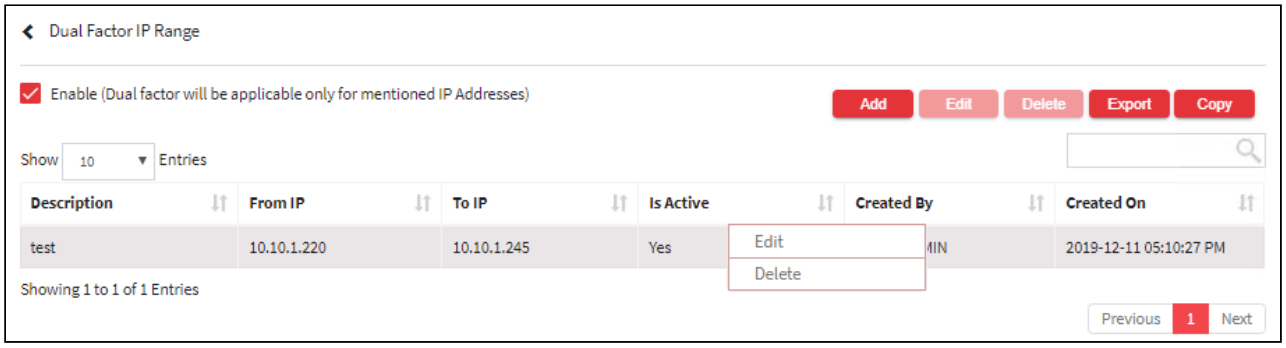


The **Dual Factor IP Range** screen contains the following fields:

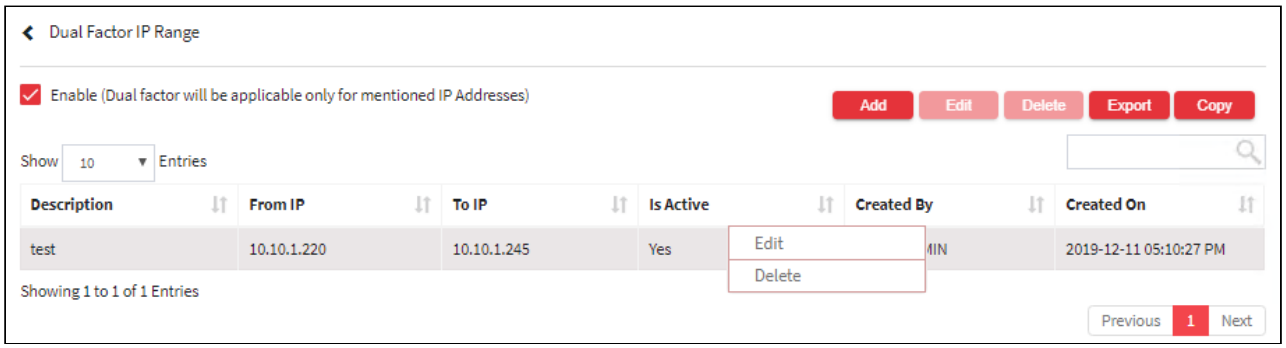
Field Name	Description
Description	Enter the description for the dual-factor IP range.
From IP	Enter IP address to set the start range for dual-factor.
To IP	Enter IP address to set the end range for dual-factor.
Type	Select the type of authentication.
Is Active	Click to enable the configuration.

⚠ The user is authenticated on login screen of **Client Manager**, once the dual factor IP range is configured.

5. For Editing the details of the existing Dual Factor IP Range click on the existing Dual Factor IP Range and select the Edit button at the top and make the required changes. Also, you can right-click on the domain and select Edit.



6. For Deleting the existing Dual Factor IP Range click on the existing Dual Factor IP Range and select the Delete button at the top and make the required changes. Also, you can right-click on the domain and select Delete.



7. The Export button will export all the Dual Factor IP Range details in the form .xlsx format. The Copy button will copy all the details of the table.

4.2.3.1.8 Configure TOTP Authentication

Time-based One-time Passwords (TOTP) Authentication is a robust multi-factor authentication type that adds a formidable layer of protection to your account. It works on a simple premise where the login tokens are formed by mixing a secret key with the current time interval to generate the OTP. So, it is necessary that the system times are synchronized. The generated OTP is validated by the server within the time frame, a successful validation will give to access ARCON PAM. If the validation is unsuccessful, a connection to ARCON PAM will not be established. **TOTP** authentication has an edge over others as it works without an internet connection and does not

rely on cell phone coverage and roaming. Moreover, it offers users the flexibility to choose from a range of **authentication** applications like Google Authenticator, Microsoft Authenticator, Symantec VIP Authenticator, etc.

4.2.3.1.8.1 Pre-requisites

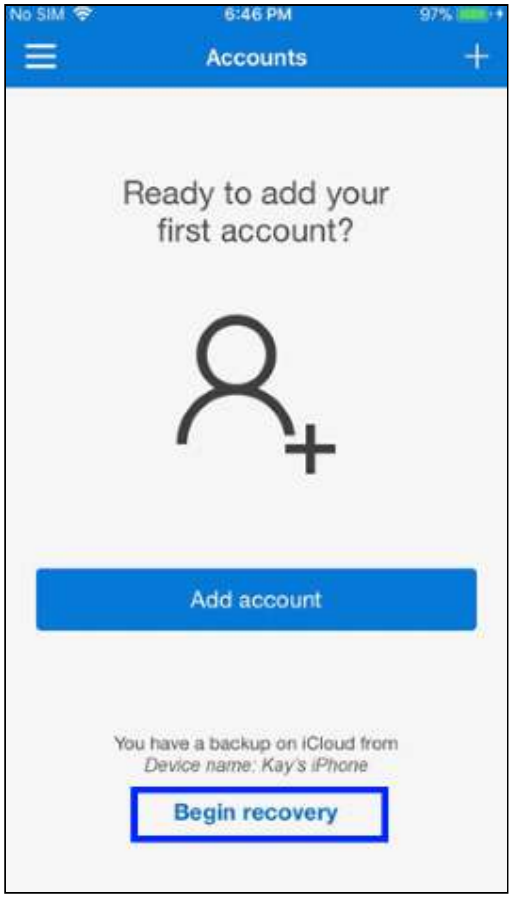
Access to smartphones that are capable of generating OTP. A smartphone is required because the users will have to download the TOTP generator app. Some of these apps are

- Google Authenticator
- Microsoft Authenticator
- Symantec VIP Authenticator

All of these work similarly so we will show you the configuration and working for one authenticator.

Let us consider Microsoft Authenticator.

- Download and install **Microsoft Authenticator** App from **Google Play Store** on your mobile to configure mobile TOTP dual-factor authentication.

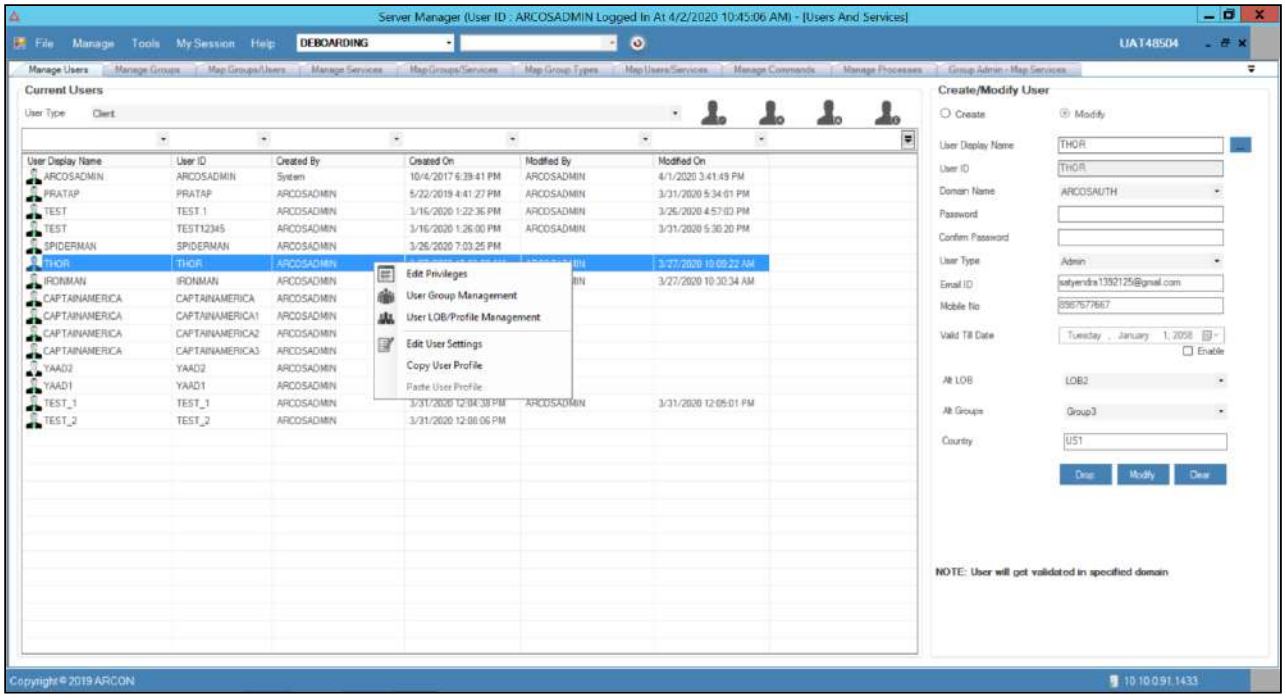


4.2.3.1.8.2 Enable Dual Factor Authentication - TOTP

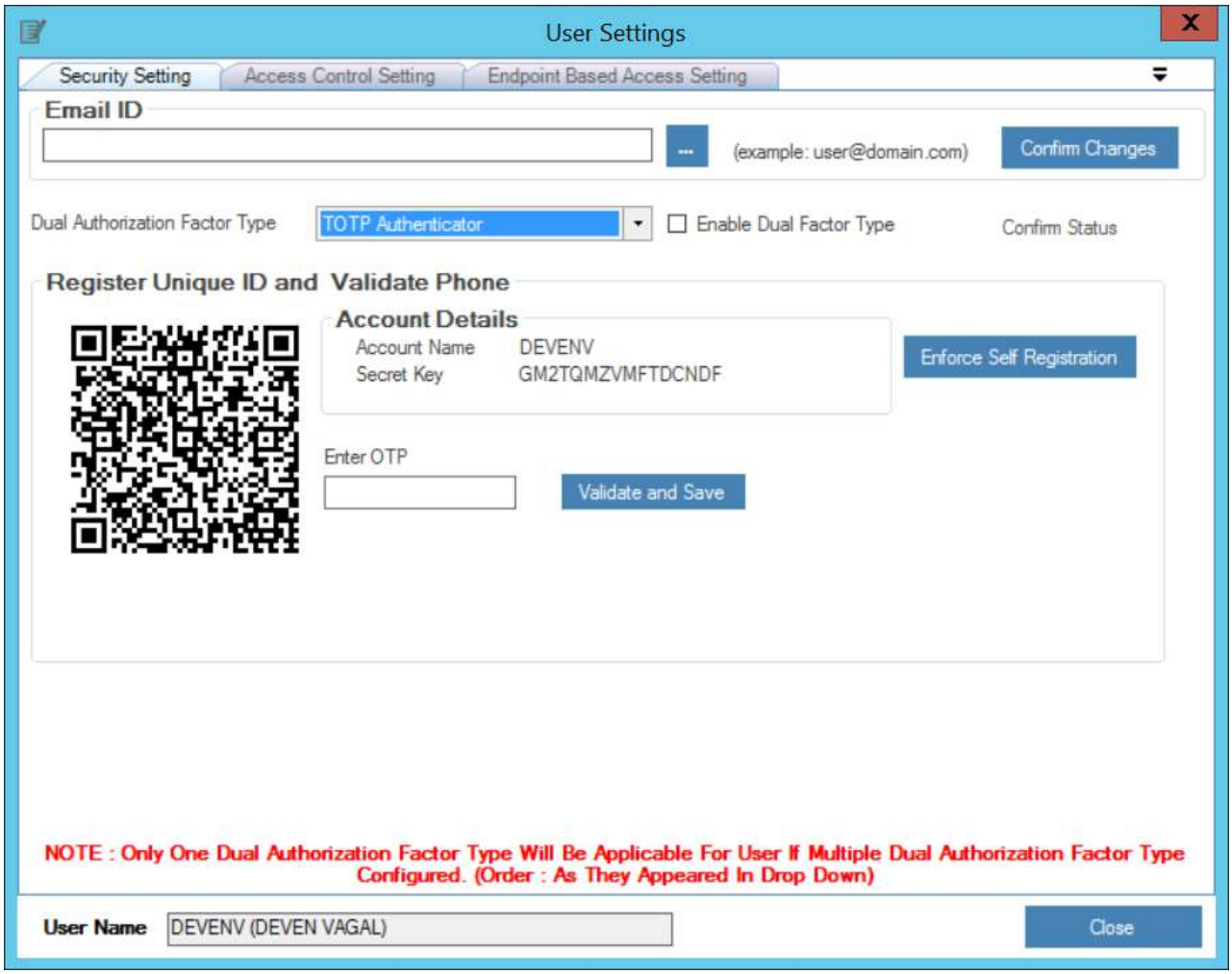
To enable TOTP dual-factor authentication perform the following steps on server manager for the following path :

Manage → Users and Services → Manage Users

1. Select the user for whom the TOTP Based authentication should be displayed during login from ACMO.
2. Right click on the User name from the **User Display Name** list. A multiple options list is popped up.

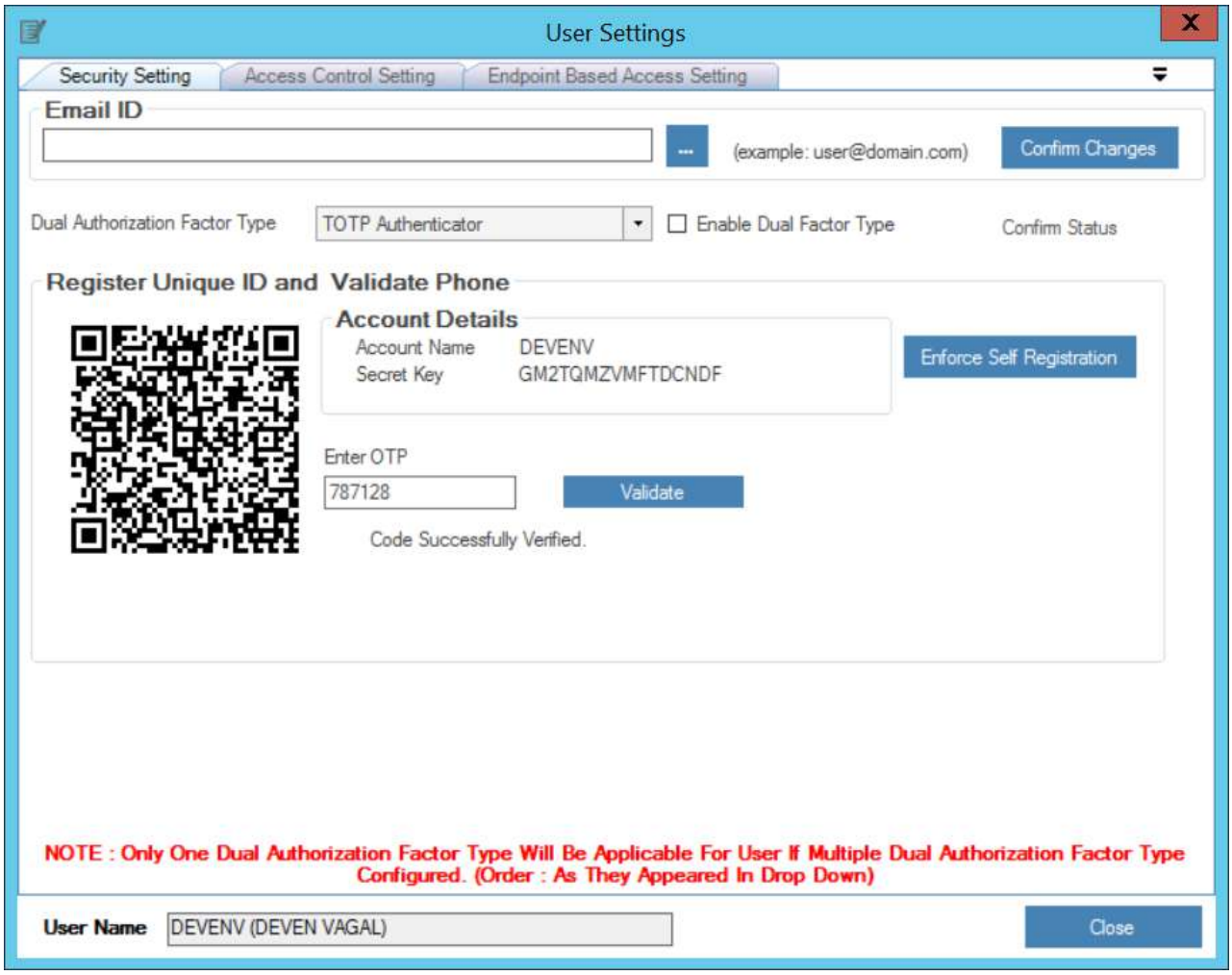


3. Click on **Edit User Settings** menu this will show a new window for User setting.
4. Click on the Dual Authorization Factor Type drop-down list this will populate list. At the end of the list, TOTP Authenticator list entry should be displayed.



5. Download Microsoft authenticator in your android phone. After downloading this application, open it, and scan the QR code. After scanning the new account gets added in your QR code application and respective time-based OTP is generated in your mobile application.

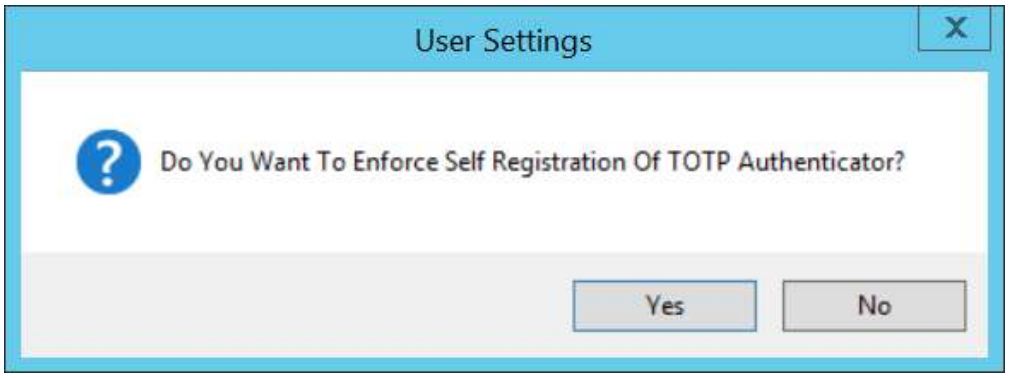
6. Enter this OTP in the textbox and click on the **validate** and **save** button after successful validation.
7. Select on Enable Dual Factor Type checkbox. It enables the Confirm Status button.



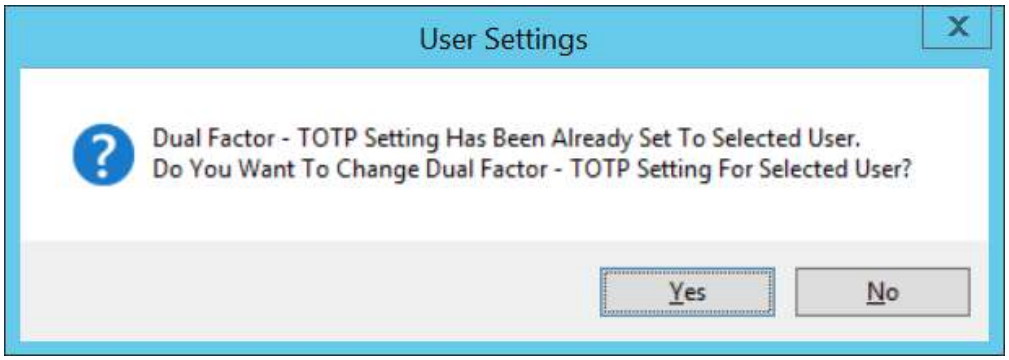
8. **Enforce Self Registration** button displays the **Account Details.**

- Only Admins have access to Enforce Self Registration.
- The enforce self registration the end user to register when accessing the first time post this MFA is applied by scanning the QR code and entering Secret Key. This reduces the Administrator overhead as the admin now needs to only enable the MFA and not perform any validation from the Server Manager module.

9. If you select Enforce Self Registration then the following popup appears.

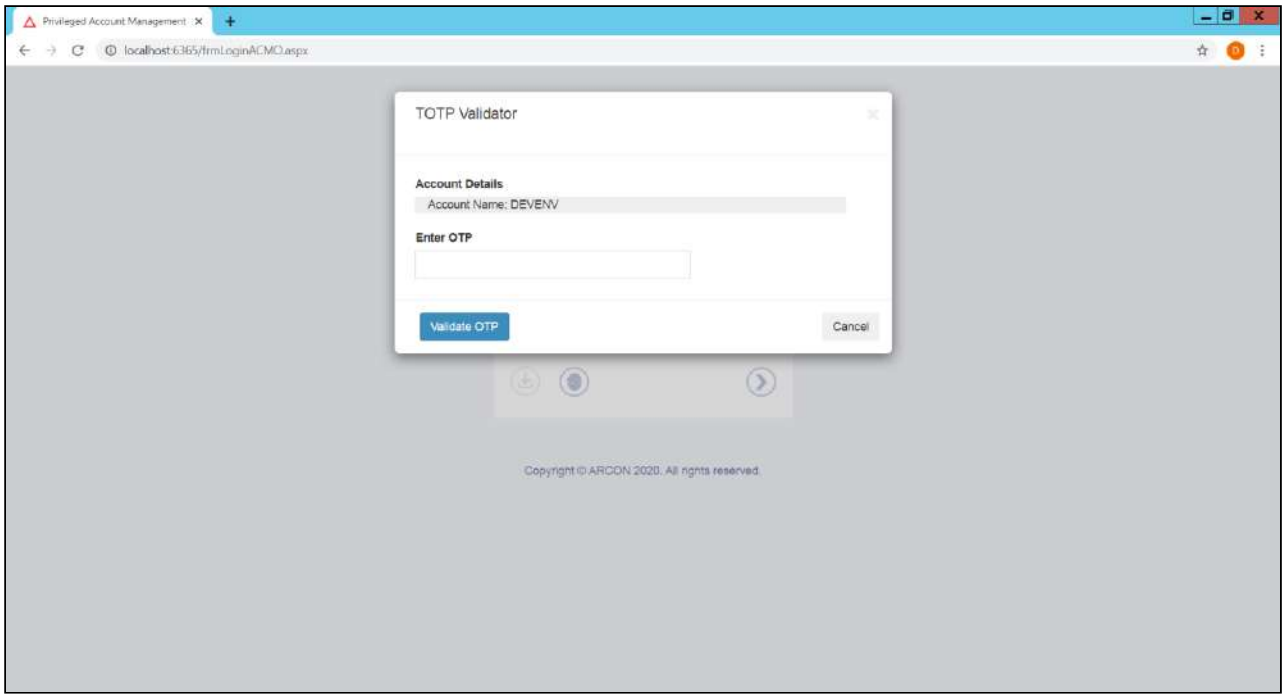


10. After clicking on the Confirm Changes button a confirmation dialog box appears with a yes/no option. Click on yes to save the settings.

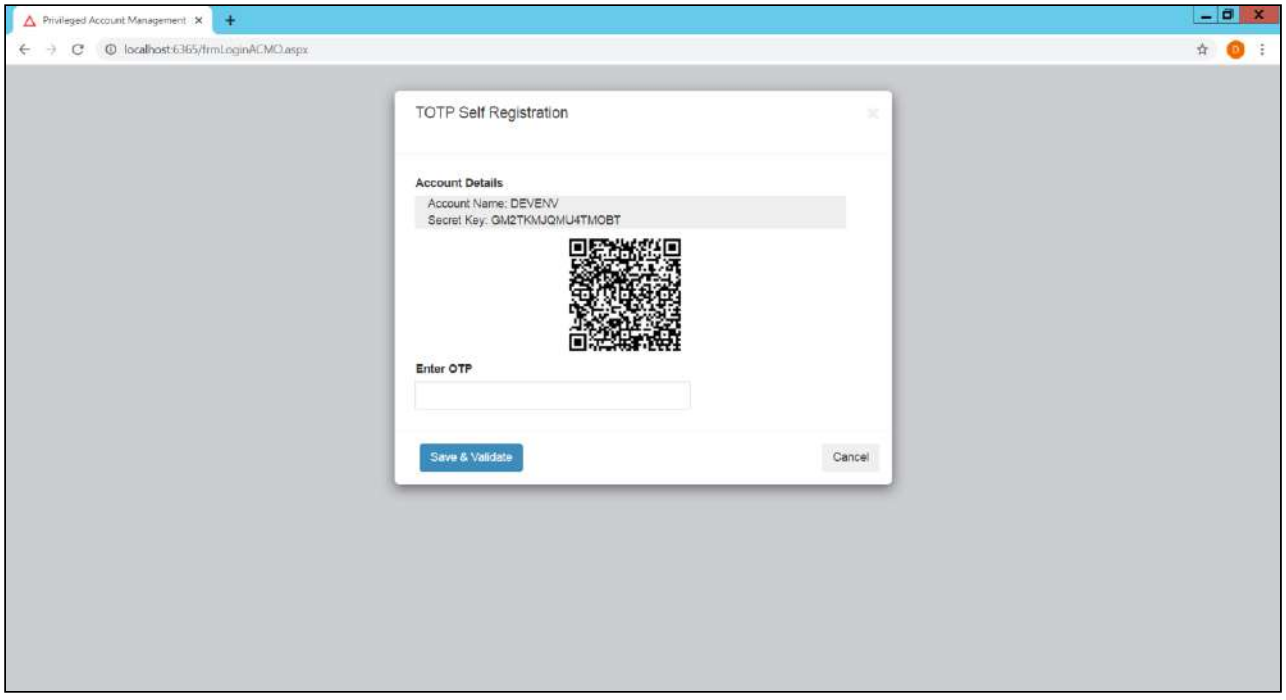


4.2.3.1.8.3 Post TOTP Configuration

1. Go to the ACMO Login page. Enter the credentials in ARCON PAM Login screen and click **Login**, The **TOTP Validator** pop up is displayed.
2. Enter the generated OTP from the configured Microsoft Authenticator application.



3. Users for whom the Enforce Self Registration was enabled, the **Account Name** and **Secret Key** are visible, after the user name and password are entered,
4. Scan the QR code and enter the TOTP which is generated in the Microsoft authenticator application.



5. Successful authentication will direct to the landing page.

If your OTP is correct but the password is wrong then the following message “Invalid User Name Or Password” is displayed and the user remains on the same page.

4.2.3.1.9 Passwordless Authentication

A drive towards complete automation is envisaged. With the evolving technology, the organization's security should be stronger than ever before and at the same time ensuring higher security standards. A new authentication has been introduced which frees the User from remembering passwords while logging into their systems.

ARCON PAM features a **Passwordless authentication** strategy where the Users can seamlessly logon to the application by just using MFA of their choice. The login details of the user are validated against the domain. Successful Validation lands the user on the Dual factor Authentication page if the admin has set one, else lands the user directly to the target page.

In order to achieve a passwordless authentication, it is recommended to enable Multifactor Authentication for the user as an additional security step. We have the following Multifactor solutions integrated with the ARCON PAM Solution:

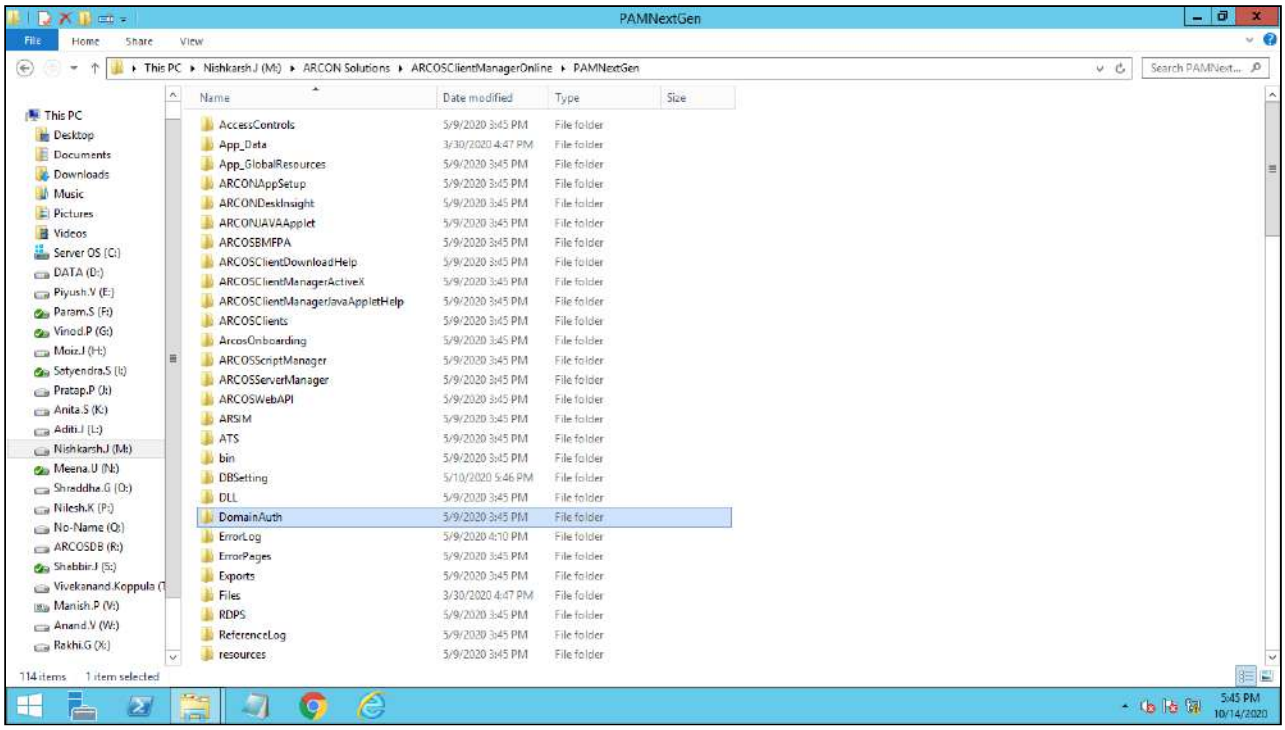
1. Leading **Biometric** devices such as 3M Cogent(Gemalto), Morpho, Precision, eikonTouch, Globalspace.
2. **Standard Protocols** based Authentication e.g. LDAP, RADIUS, OAUTH2.
3. **Email** and **SMS** based OTP.
4. **TOTP** based authenticators like Symantec VIP Access, Google Authenticator, and Microsoft Authenticator.
5. ARCON | PAM has it's own built Mobile OTP App called **ARCON AUTHENTICATOR.**
6. The solution integrates with **Facial recognition** solutions, as well as, has an in-built ARCON facial recognition module.

ARCON | PAM also gives the flexibility to a user to select the dual-factor he wants to when logging into the ARCON | PAM solution.

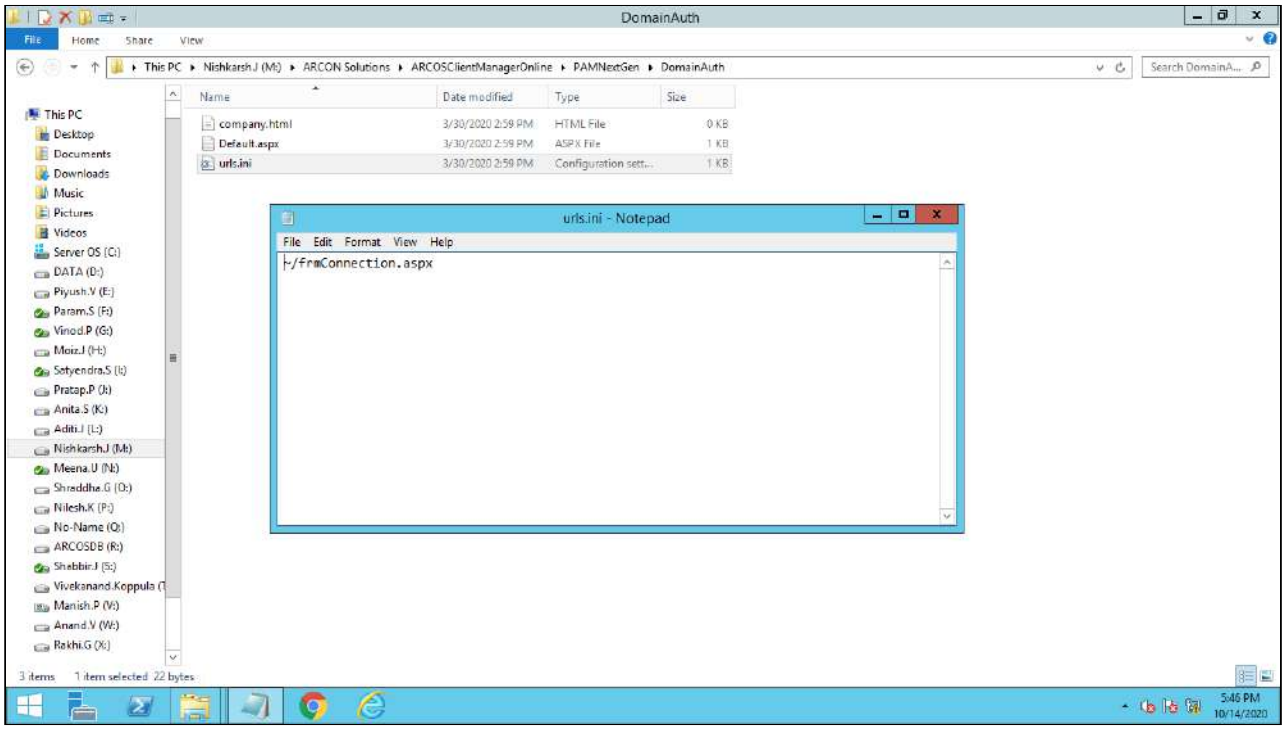
To support other Multi-Factor Authentications, Refer to their Configurations under Security Settings.

4.2.3.1.9.1 Application Configuration

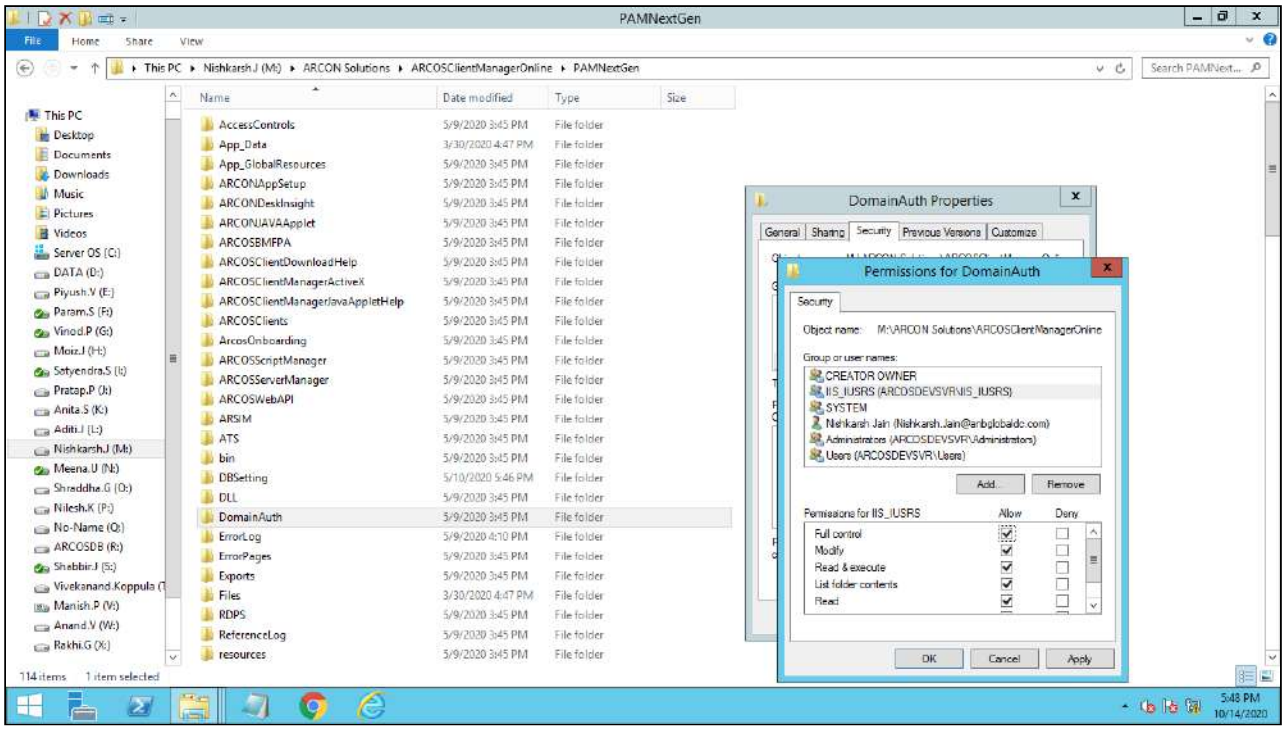
1. Go to the path: **Local Drive:\ARCON Solutions\ARCOSClientManagerOnline\PAMNextGen\DomainAuth** folder.



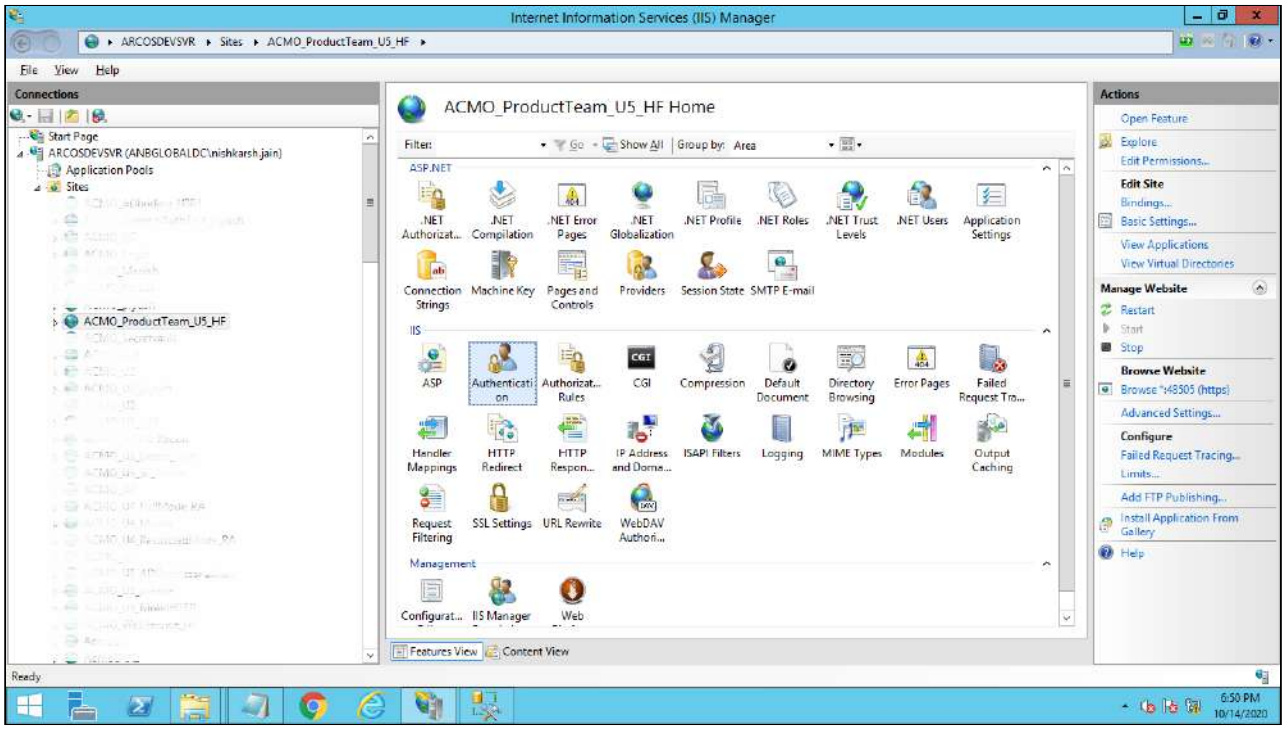
2. It should contain **urls.ini**, inside that it should contain below entry:
~/frmConnection.aspx



3. Right-click on the **DomainAuth** folder > Properties > Security Tab > Add a User > "IIS_IUSRS" with full rights (read, write, execute).

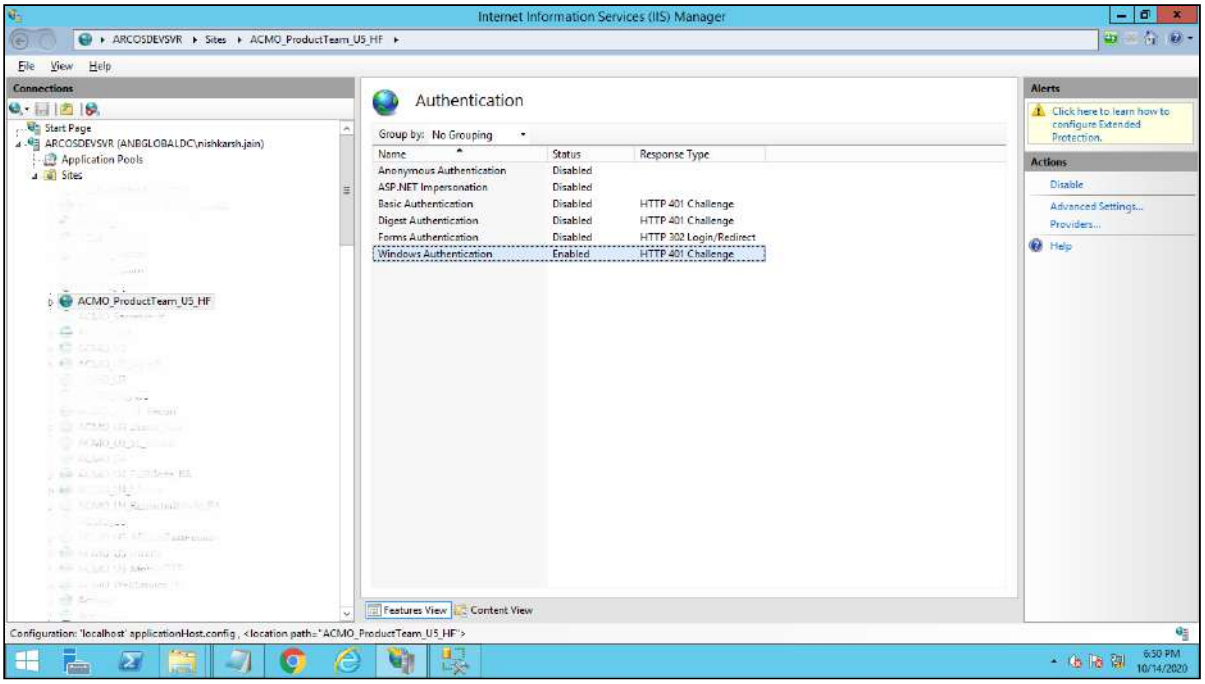


4. Open IIS and look for "Authentication" under the PAM hosted website.



5. Go to Sites > ARCOSClientManagerOnline > DomainAuth > Double Click > Authentication
    a. **Anonymous Logon** - Set it as Disabled

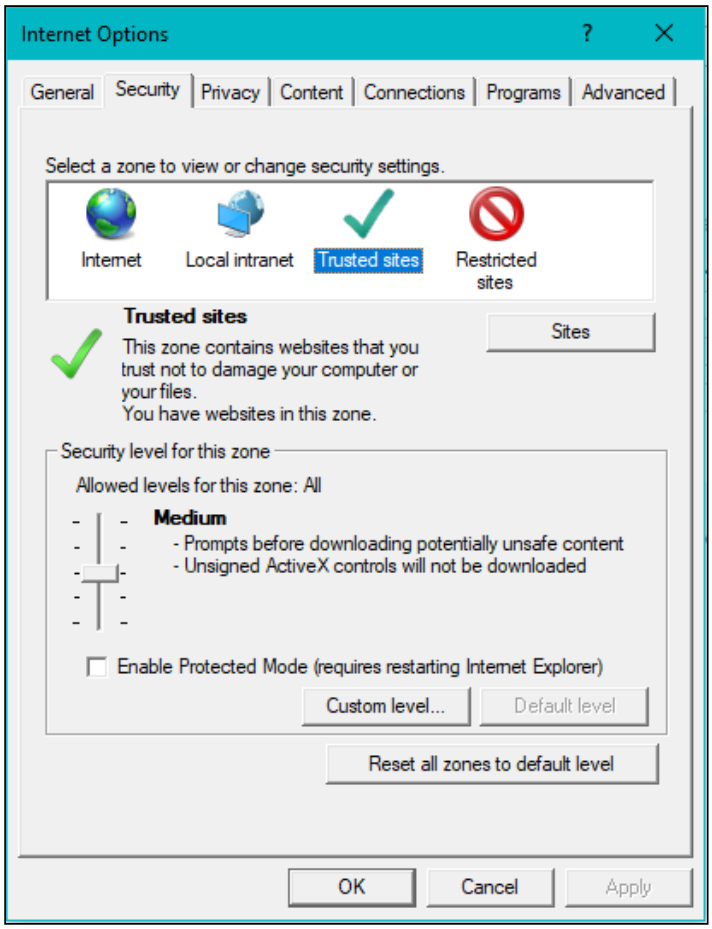
b. **Windows Authentication** - Set it as Enabled



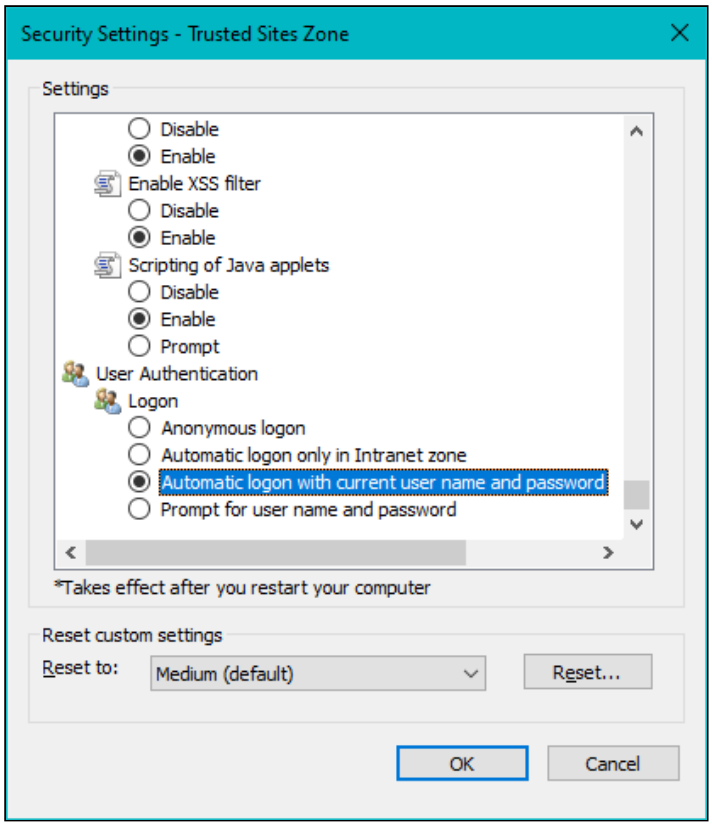
6. Restart IIS service.

4.2.3.1.9.2 Internet Explorer Configuration

1. Go to Internet Explorer > Tools (Menu) > Internet Options > Security > Custom Level button



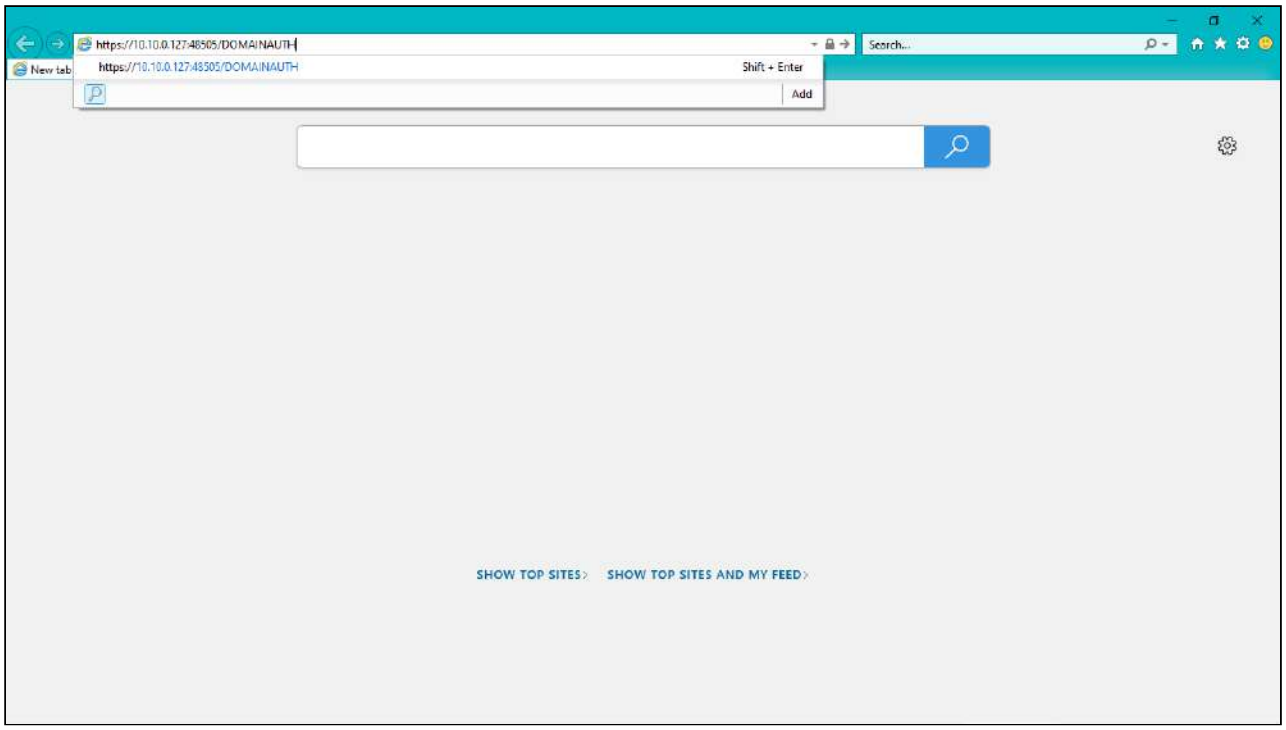
2. Under User Authentication > Logon > select radio button **"Automatically logon with current username and password".**



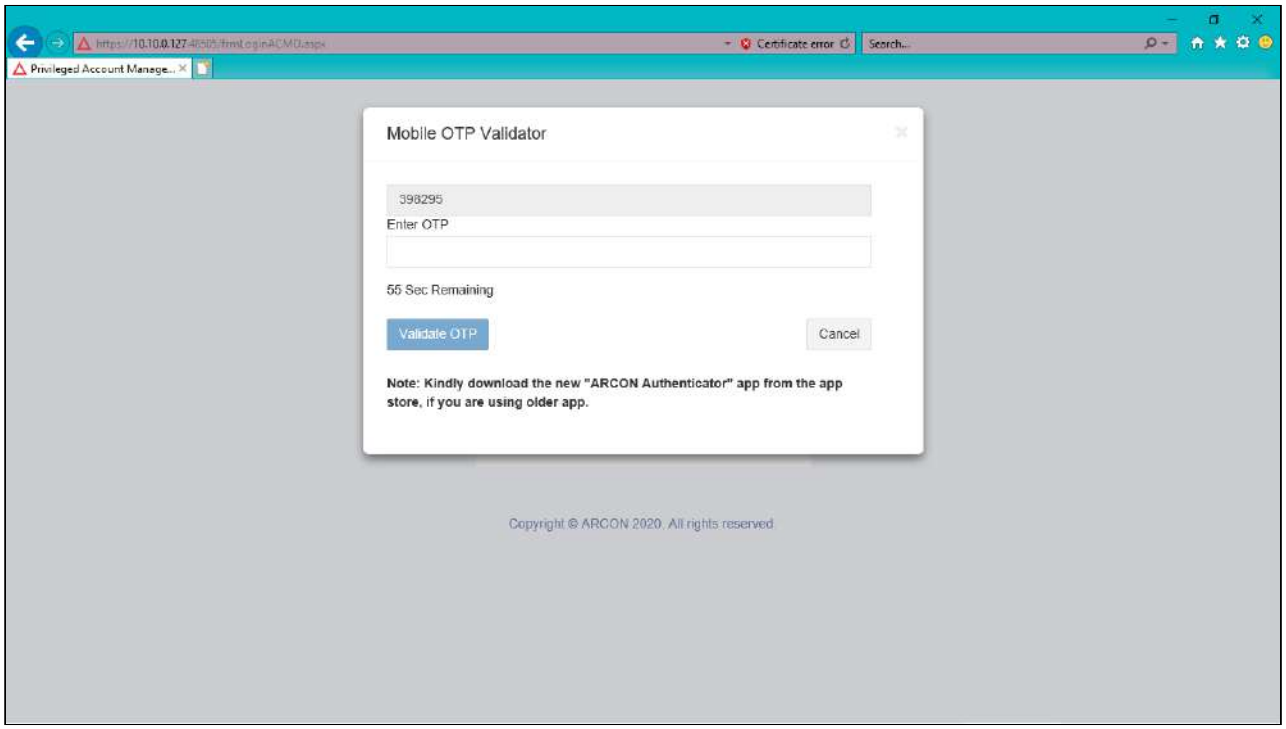
4.2.3.1.9.3 Accessing PAM

Once all the configuration for Passwordless Authentication is achieved, the end-user can login to Windows Domain Authenticated machine and open the PAM web application in the browser.
When the URL is accessed, Passwordless Authentication feature would automatically pick up the Authentication for the logged-in Domain User and provide only with the Multifactor Authentication. For example, if Mobile OTP(ARCON Authenticator), the below would be the process.

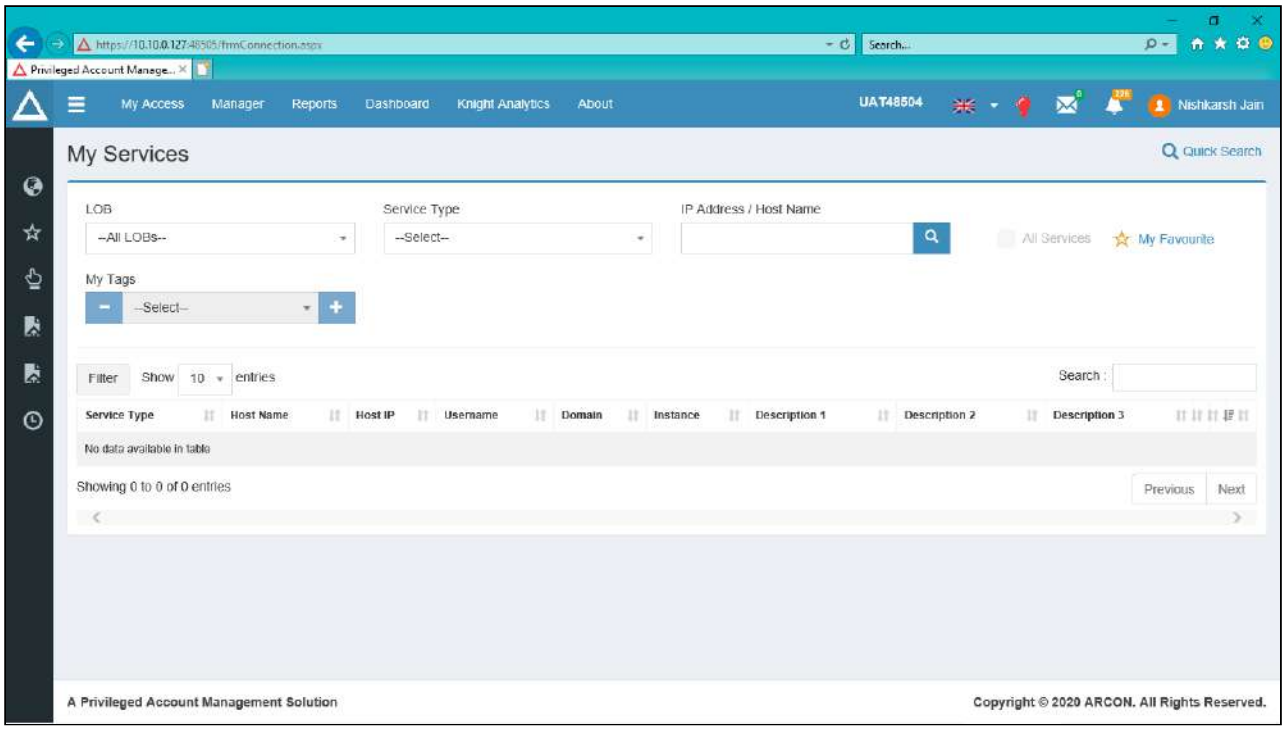
1. Enter the URL with **DOMAINAUTH** extension.



2. If Multifactor Authentication is enabled, the user will be asked for input to validate.



3. Post successful Multifactor Authentication validation, the user will be successfully logged into ARCON PAM Client Manager Online.



4.2.3.1.9.4 Domain Validation

Along with a seamless Passwordless authentication, ARCON PAM also provides additional security to control access for allowed domains in an organisation.

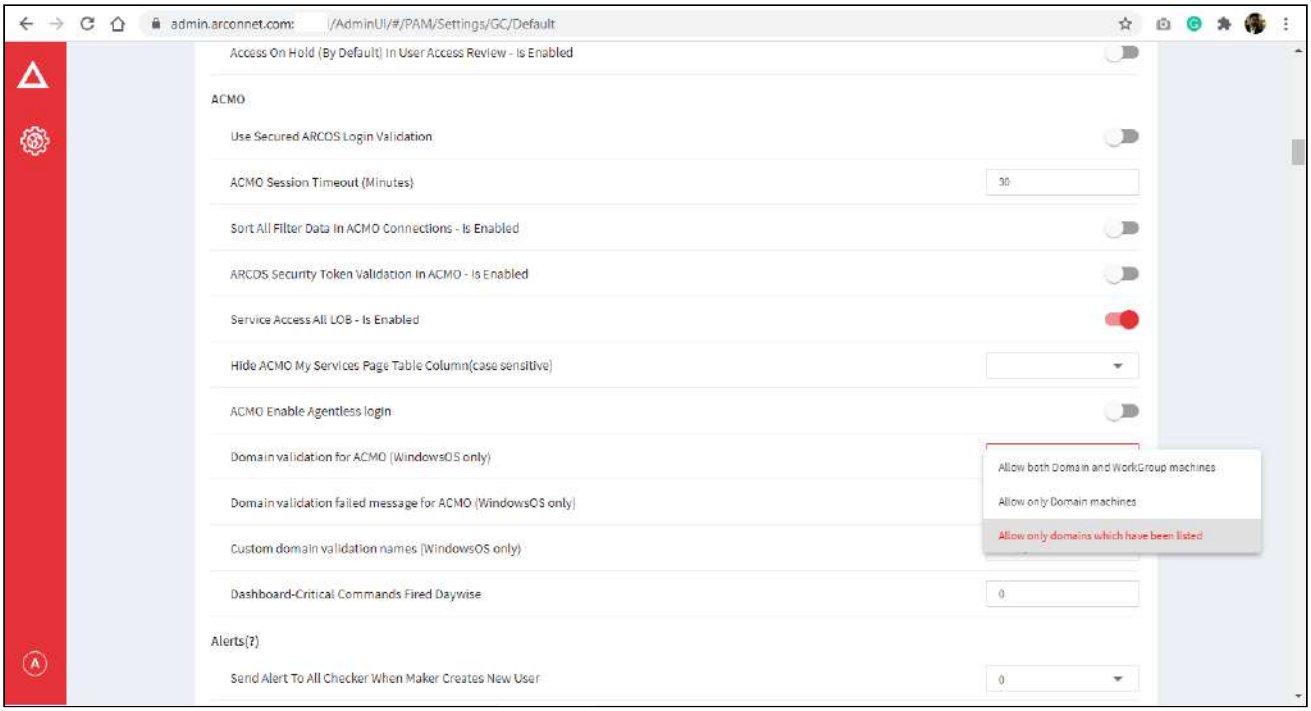
This can be achieved by enabling the following 3 configurations, using centralised PAM Settings. To navigate, use the following path:

Settings → Group → ACMO

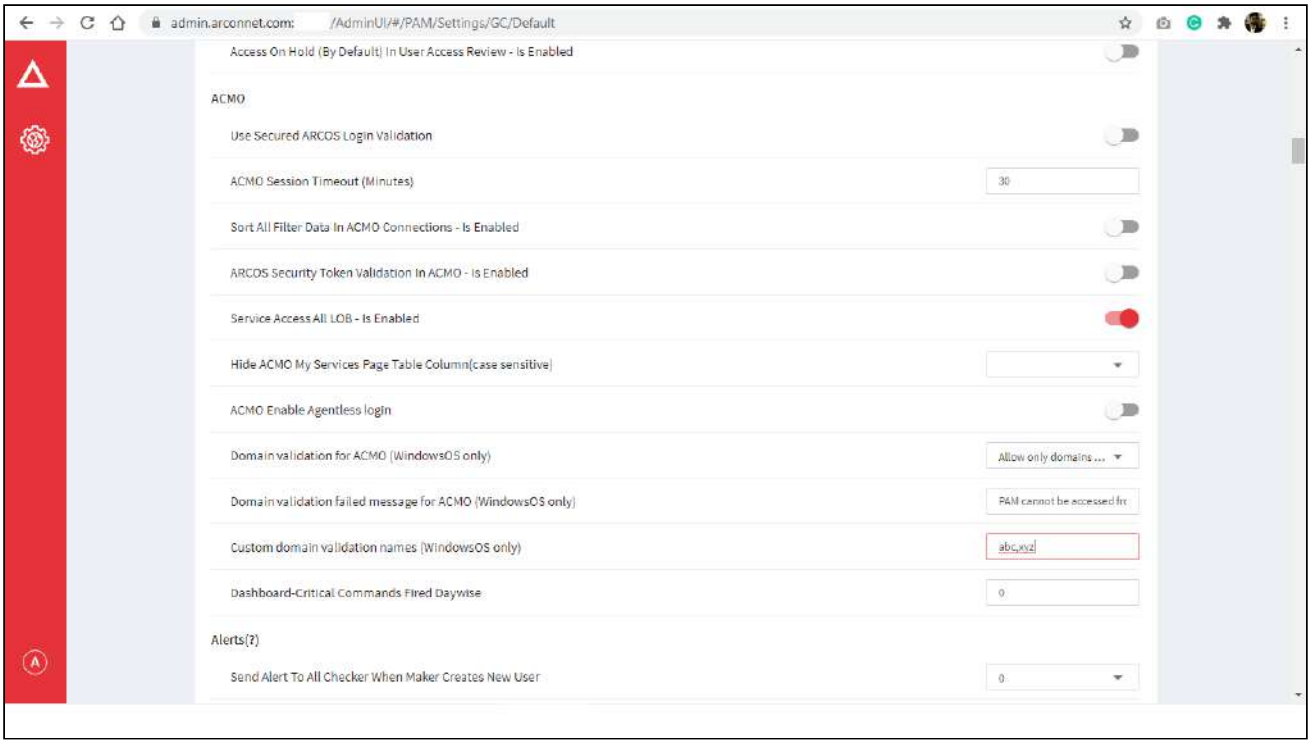
Field Name	Description
Domain Validation for ACMO (WindowsOS only)	This configuration sets restrictions for accessing PAM ACMO based on their domain and workgroup.
Valid Values	Allow both Domain and Workgroup machines, Allow only Domain machines, Allow only domain which have been listed
Domain validation failed message for ACMO (WindowsOS only)	Set a customized message for domain validation. For example- If my Domain validation for ACMO (WindowsOS only) is - Allow only Domain Machines, and a workgroup user tries to access it then the login is failed and the message set on Domain validation failed message for ACMO (WindowsOS only) appears on the ACMO user screen.
Valid Values	Enter the text message to be displayed on ACMO when the validation fails.

Field Name	Description
Custom Domain Validation names (WindowsOS only)	We write the Comma-separated domain names which verify the user's presence against that domain.
Valid Values	Enter the Domain names **Note: -** To enable **Custom Domain Validationnames (WindowsOS only),**the Domain validation for ACMO (WindowsOS only) value needs to set as **Allow only domain which have been listed.**

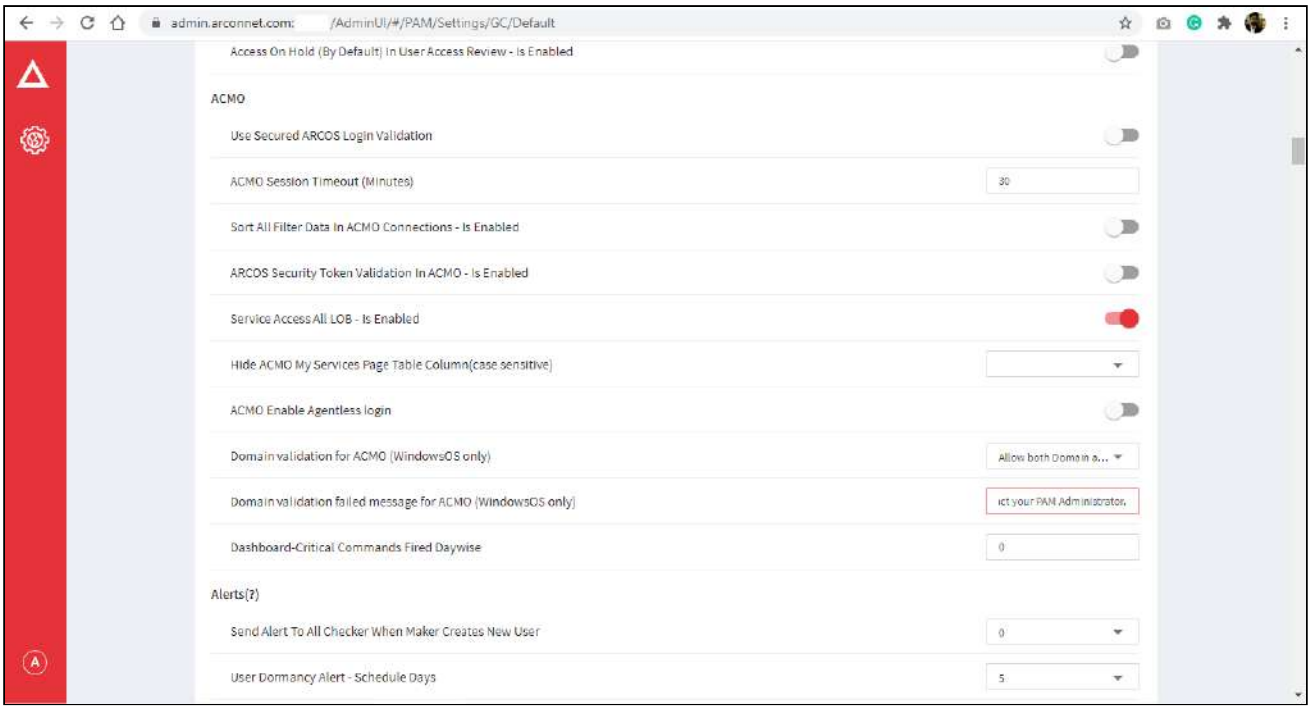
Domain Validation for ACMO (WindowsOS only)



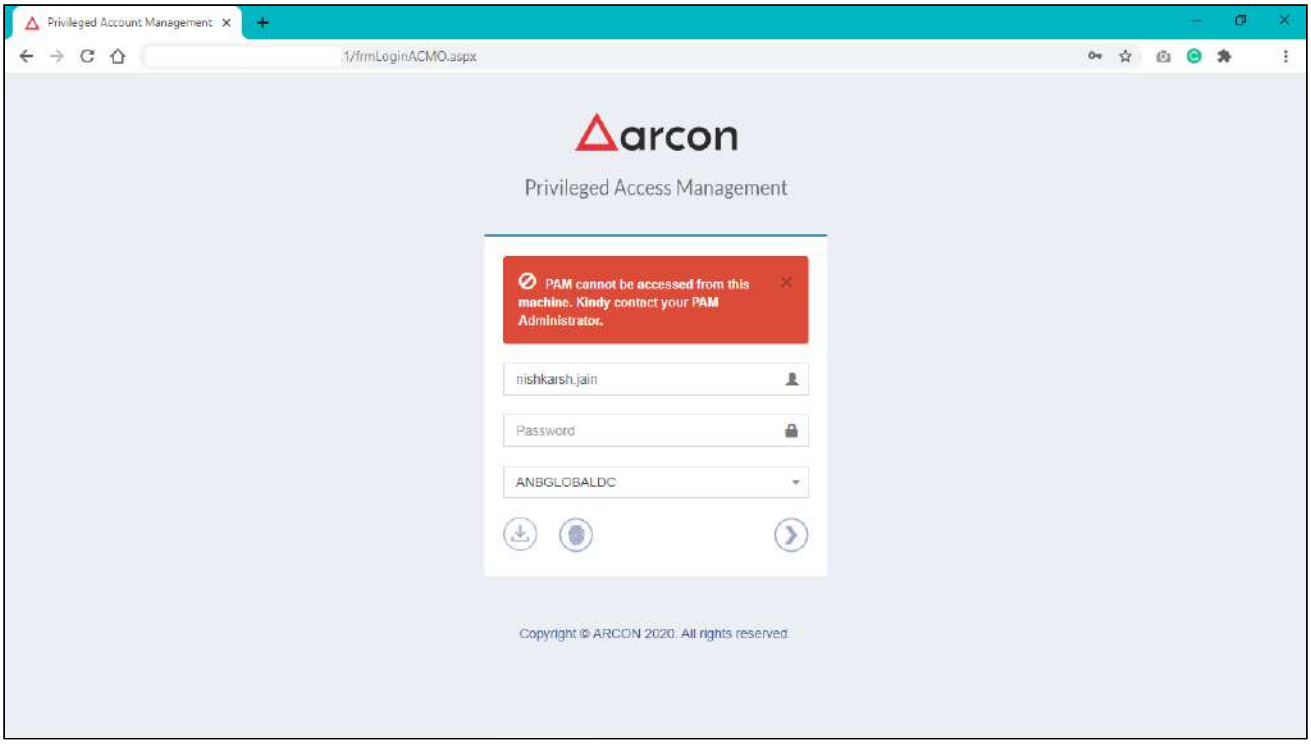
Domain validation failed message for ACMO (WindowsOS only)



Custom Domain Validation names (WindowsOS only)



If an unauthorized domain login happens, the custom defined message would be displayed.



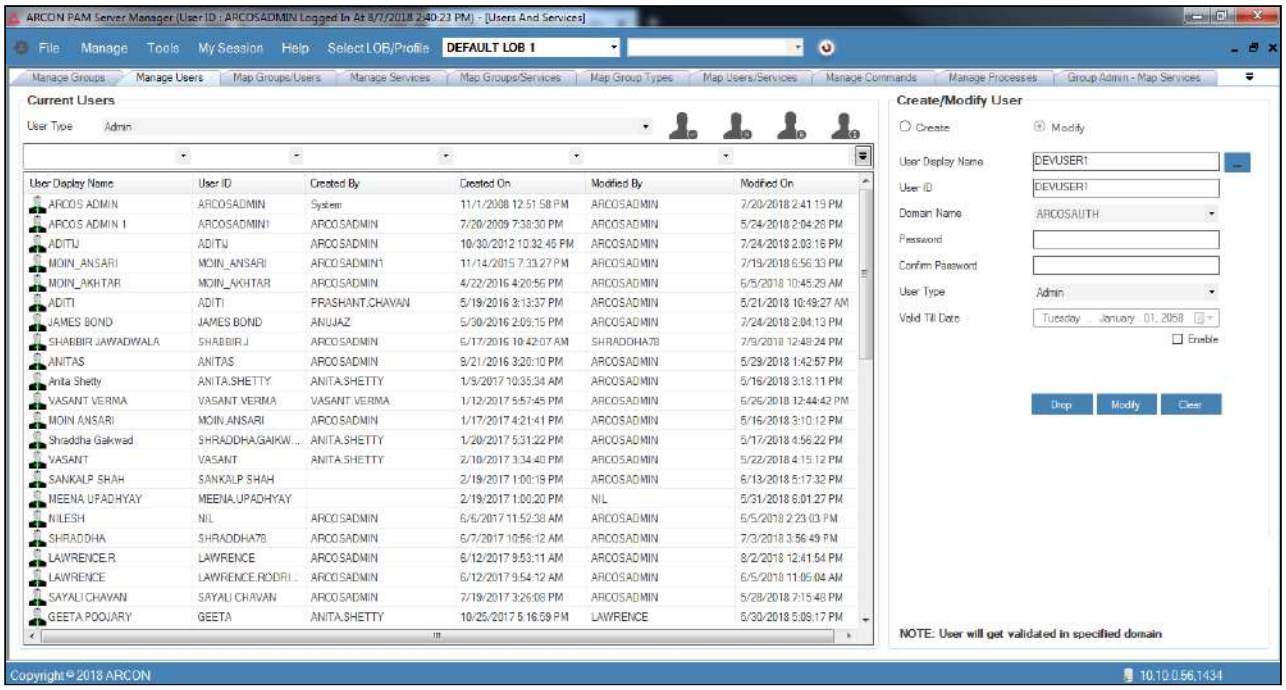
4.2.3.1.10 Configure Face Recognition

Face Recognition Configuration is a dual-factor authentication supported by ARCON PAM. It is performed by using the facial information captured from the webcam of the user's machine.

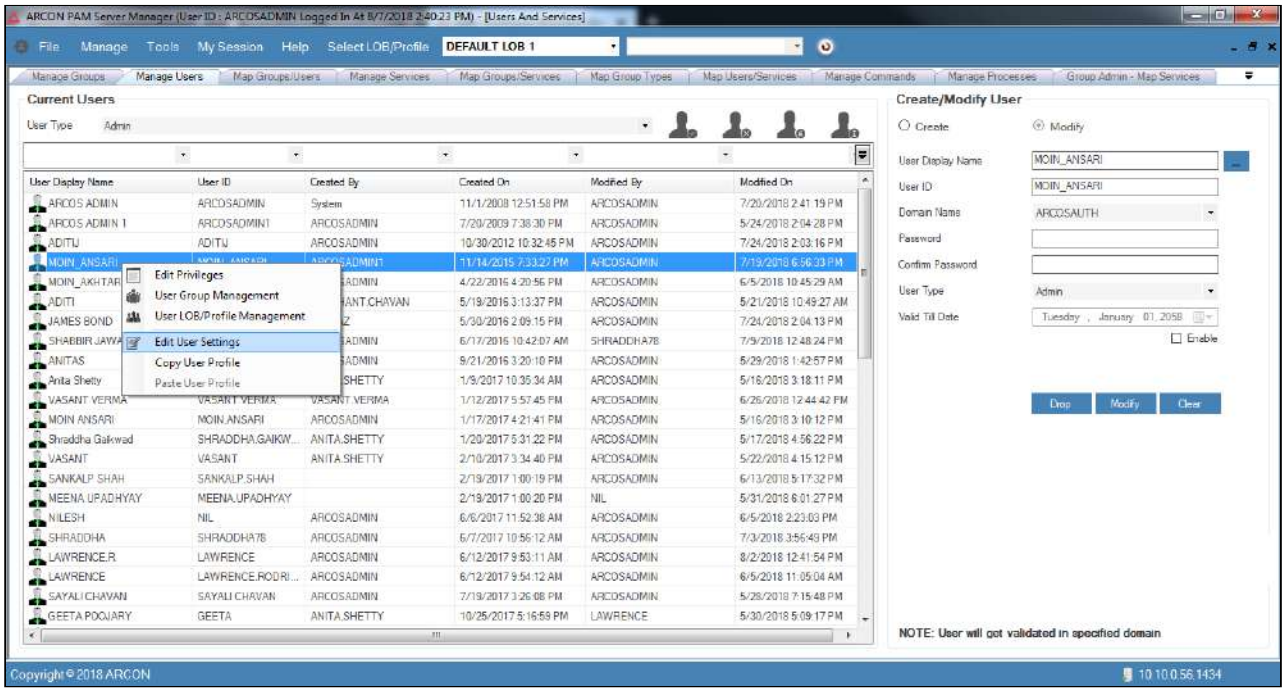
4.2.3.1.10.1 Configure Facial Information

To configure face recognition, you need to follow the below steps:

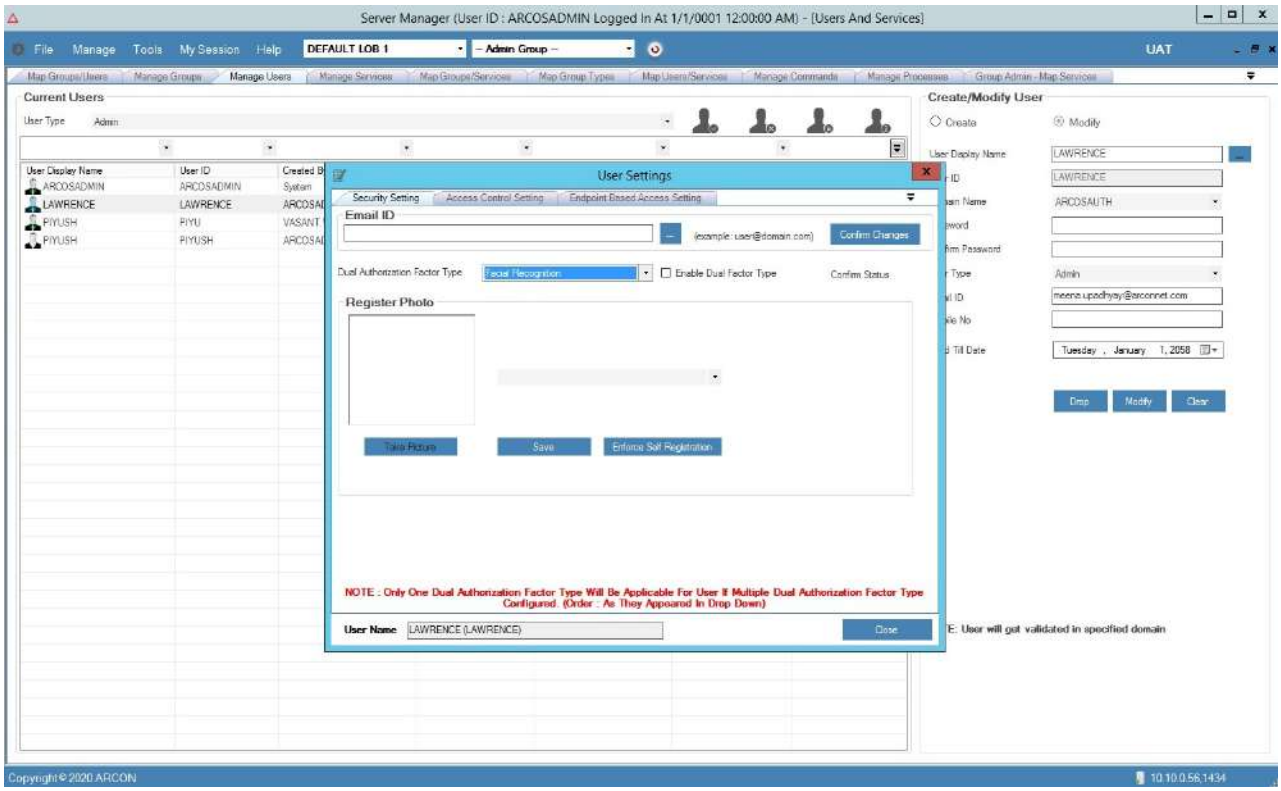
1. You need to configure the facial information on the Server Manager for the individual users.



2. Right-click on the selected user. A multiple options list is popped up.

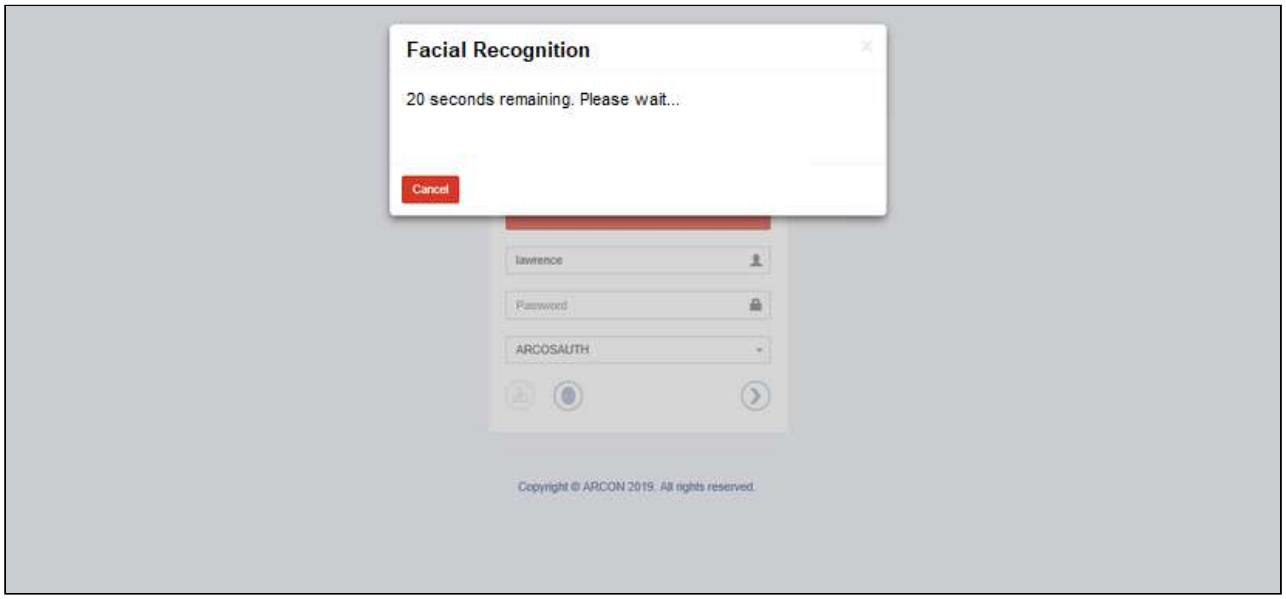


3. Click on the **Edit User Settings** option. The **User Settings the** screen is displayed.
4. Select the **Dual Authorization Factor Type** as **Face Recognition** and then select the **Enable Dual Factor Type** checkbox.
5. Click **OK** button to enable the settings of dual-factor facial recognition in ARCON PAM while logging into the application.

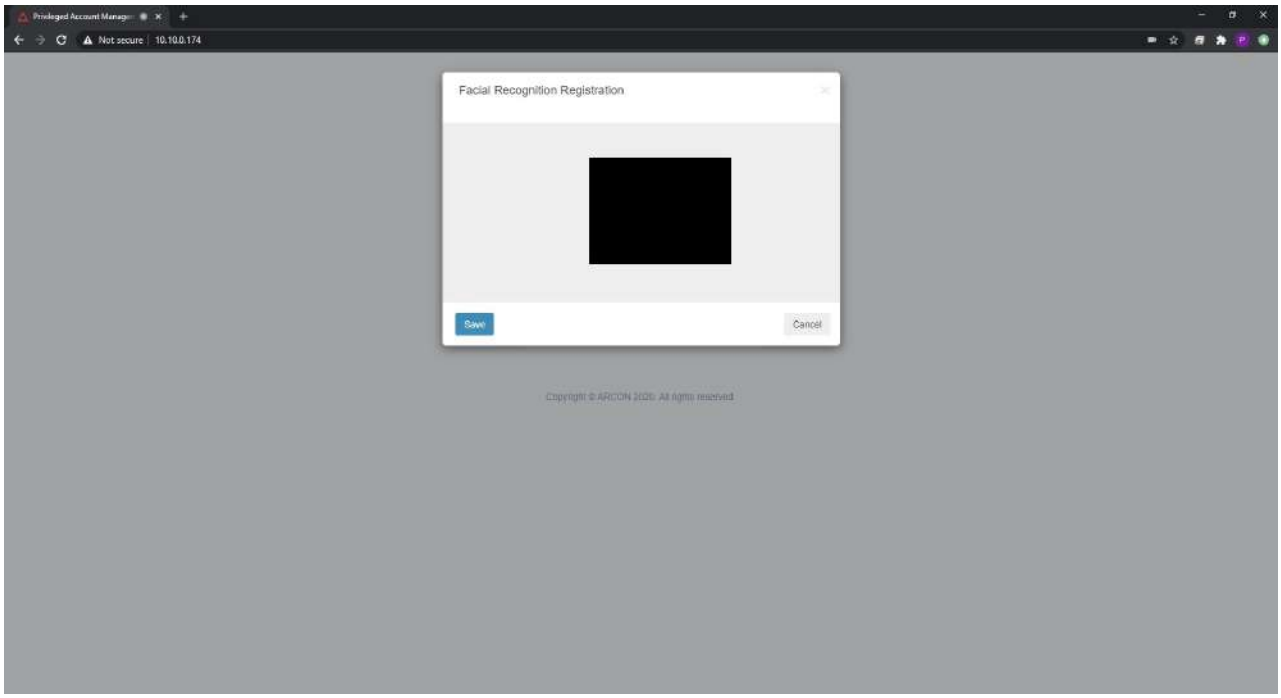


4.2.3.1.10.2 Post-Face Registration Configuration

1. Enter the credentials in ARCON PAM Login screen and click **Login**, the **Facial Recognition Validator** pop up is displayed.



2. Within a few seconds, the **ARCON PAM Facial Recognition Registration** pop up is displayed.



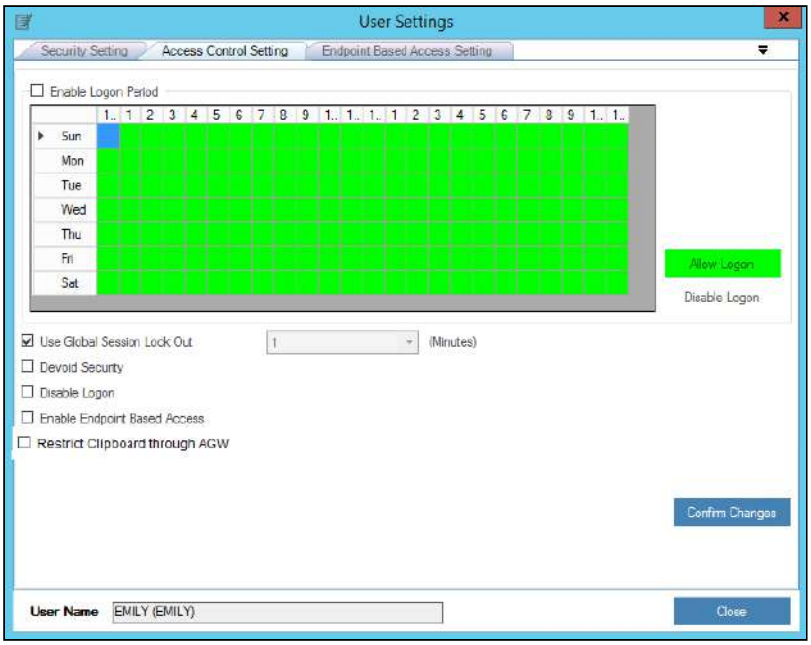
3. Place your face in front of the camera so that we can start scanning.
4. The facial data is authenticated from the database and Users will be able to successfully login into the ARCON PAM application.
5. If the facial data does not match, then you will not be able to log into the ARCON PAM application.

4.2.3.2 Access Control Setting

Access control is a security technique that can be used to regulate who can view or use resources in a computing environment. Access control systems performs authorization, identification, authentication, access approval, and accountability of entities through login credentials including passwords, personal identification numbers (PINs), biometric scans, and physical or electronic keys.

Access Control Setting helps to enable or disable the user logon period. In addition, it allows to decrease or increase the session lock out time, disable lockout attempts (Devoid Security), enable/disable user logon access, and enable the endpoint based access for user(s).

The **Access Control Setting** tab contains the following fields:



Field Name	Description
Enable Logon Period	Enable the number of days and hours for the selected user to access the application. ⚠ • If a user tries to login into ARCON PAM application after the set logon period is expired, then the user will receive an error message displaying "**Invalid User Name OR Password**". • Once the logon period is selected, click **Allow Logon**, to enable the logon period and click **Disable Logon** to disable the logon period.
Use Global Session Lock Out	Decrease or increase the session lock out time in minutes for the selected user. ⚠ By default, Use Global Session Lock Out is enabled.
Devoid Security	Disable lockout attempts for the selected user.
Disable Logon	Disable the logon access for the selected user.

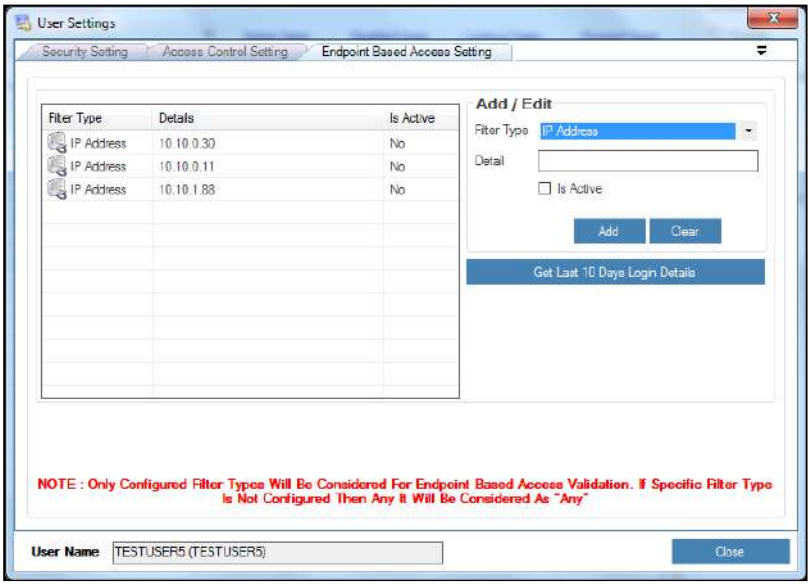
Field Name	Description
Enable Endpoint Based Access	Enable the endpoint based access, which allows access to the application through the specified desktop or laptop only. ⚠ If **Enable Endpoint Based Access** checkbox is selected, then you need to enter the IP or MAC address, Processor or BIOS Serial ID details of the laptop or desktop in the **Endpoint Based Access Setting** tab.
Restrict Clipboard through AGW	Enable or Disable the user from using the Copy-Paste Option through AGW.

1. Select the required access control settings and click **Confirm Changes** button. A window pops up with the following message:
   Access Control Setting Successfully Configured.
2. Click **OK** to configure the access control settings for the selected user.

4.2.3.3 Endpoint Based Access Setting

Endpoint Based Access Setting is an approach that helps to identify and manage the user's computer to gain access over the network. This involves the Administrator to restrict certain access to the user in order to maintain and comply with the organization's policies and standards. ARCON PAM binds the user(s) login to a particular system's IP address, MAC Address, Process ID, or BIOS Serial ID of a desktop or laptop. Hence, the users will be able to login into only those endpoint machines to which it is bind to.

The **Add/ Edit** frame contains the following fields:



Field Name	Description
Filter Type	Select the type for endpoint configuration. The valid values are: • IP Address • MAC Address • Processor ID • BIOS Serial ID
Detail	Specify the details based on the selected type of endpoint configuration.
Is Active (checkbox)	Enable the configuration for desktop or laptop who's details are specified.

1. Click **Add**. A window pops up with the following message:
   Endpoint Filter Added Successfully.
2. Click **OK**. The Endpoint Based Access setting for the specified desktop or laptop is added successfully.
3. Click **Get Last 10 Days Login Details**, to view the last 10 days login details of the User.

4.2.4 Copy User Profile

This section helps you to copy user profile of a particular User to another User. You can copy entities such as LOB, User Group, Services, Commands or Processes.

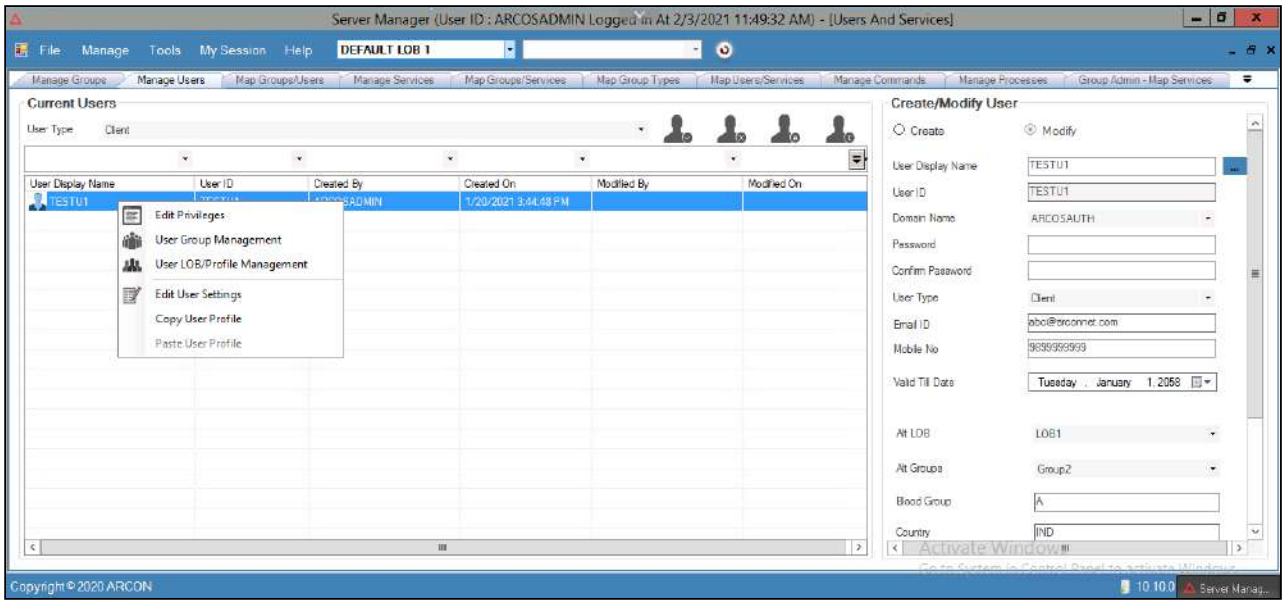
⚠ The Administrator having **Copy User Profile** privilege shall only be able to copy user profile from one User to another User.

To copy user profile:

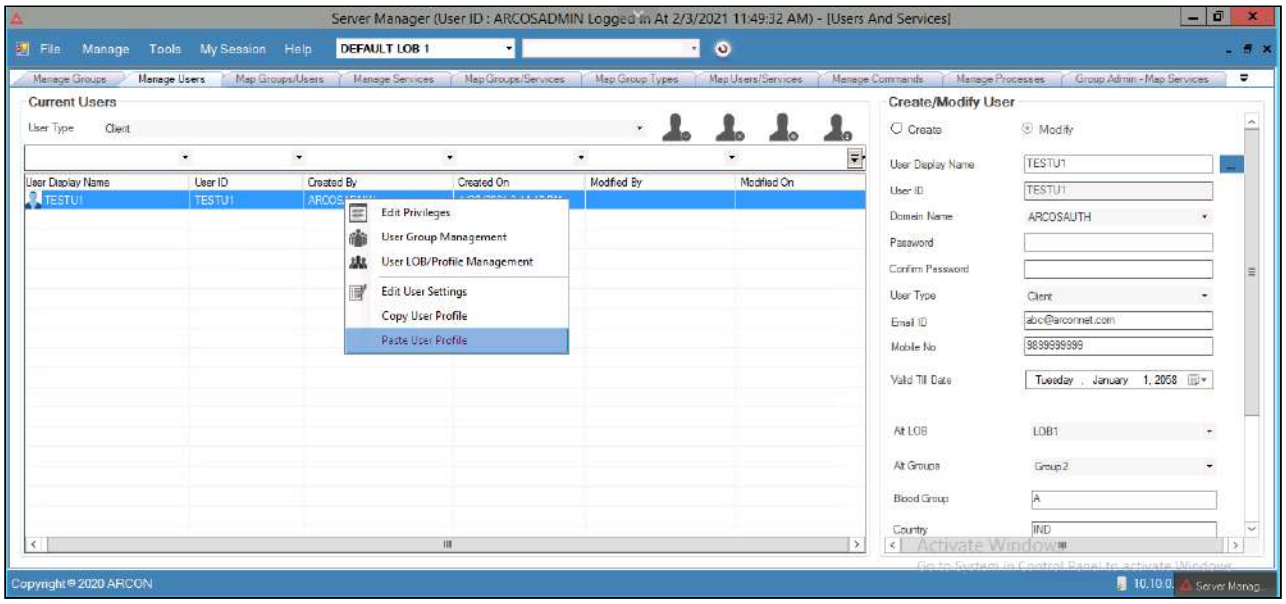
To copy user profile use the following path:

Manage → Users and Services → Manage Users

1. Right click on the User name from the **User Display Name** list. A multiple options list is popped up.



2. Click **Copy User Profile** option.
3. Now select another user to copy user profile.
4. Right click on the User name from the **User Display Name** list. A multiple options list is popped up.



5. Click **Paste User Profile** option. A confirmation box is displayed with the following message. **Do You Want To Perform this Operation?**
6. Click **Yes** button. The following **Copy Paste User Profile** screen is displayed.

7. Select the required check box against the options. The following entities can be selected on **Copy Paste User Profile** screen.
    - Copy LOB
    - Copy User Group
    - Copy Services
    - Copy Commands
    - Copy Process
8. Select the required options and click **Submit** button.

    ⚠ Click **Cancel** button to close window.
9. The following success message will be displayed.
   User Profile Copied Successfully...
10. Click **OK** button. The selected options will be copied to User.

4.3 Service

A service is an instance of server. In ARCON PAM, the routers, firewalls, switches, and databases are some of the services created to connect to the target server. These services needs to be mapped to users. The users mapped to the services will have the privilege to connect to the target server using these services.

For example, Suppose there are four users Admin, Client, TEST, and UAT on a windows server. Each user may have a unique requirement of service to perform on the server. Hence, the Administrator will create services for each of the users. These services are then grouped and mapped to each of the users which helps the Administrator to manage the services which are mapped to the user. Thereby, also helping the Administrator in user wise audit trail performed in ARCON PAM.

⚠ The Administrators having **Read Only Access** privilege (under **Manage Services**) can view details displayed under Manage Services and Map Groups/Services tab.

4.3.1 Create a Service

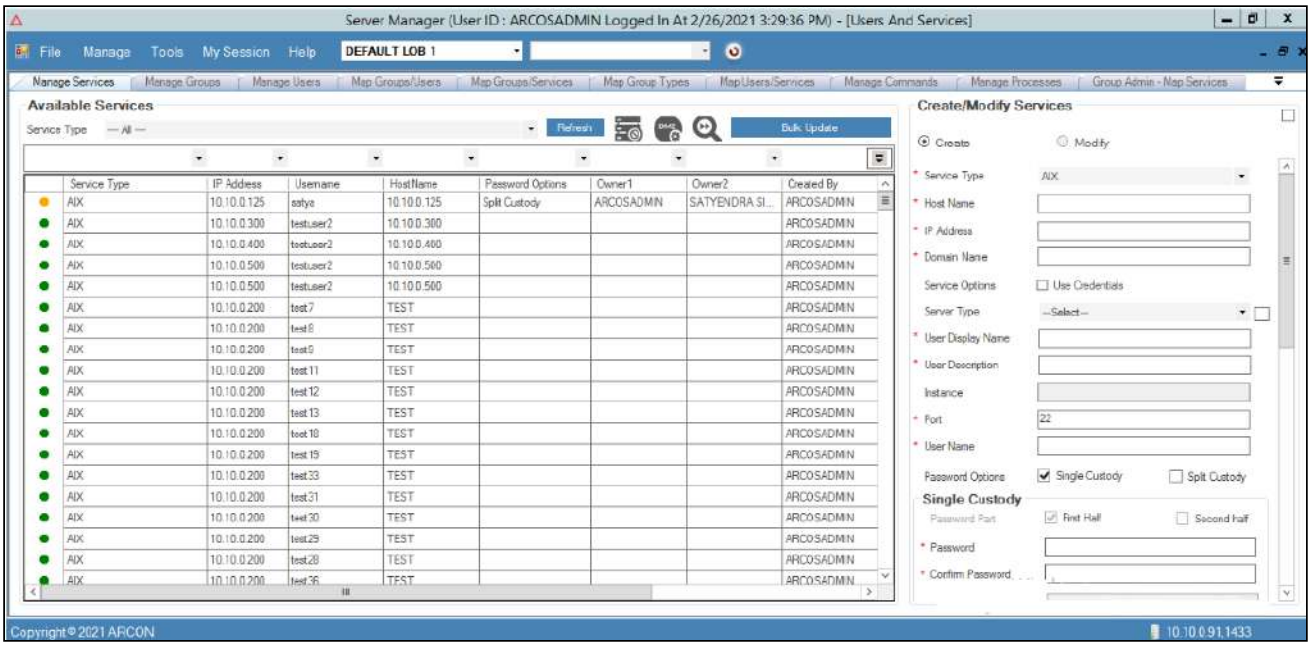
This section explains the steps to create services. The Administrators are responsible for managing services. In addition, the details of the services created shall also be modified or deleted.

⚠ The Administrator having **Add Service** privilege will only be able to create services.

To create a Service:

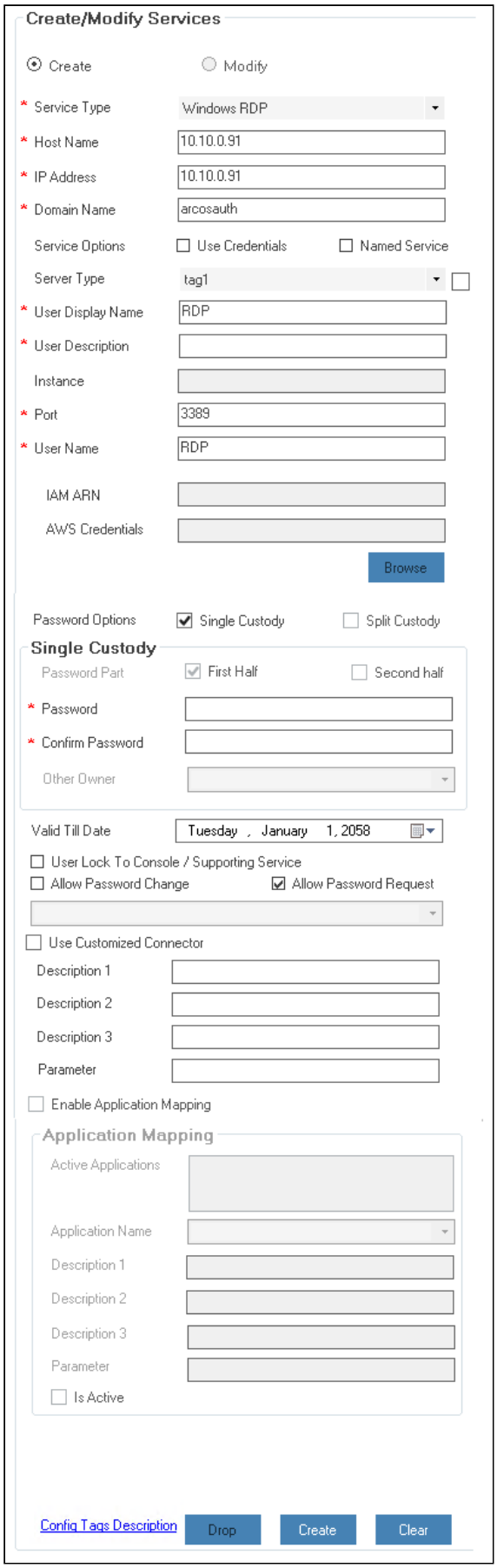
To create a service use the following path:

Manage → Users and Services → Manage Services



⚠ To search a specific set of rows, enter keywords (space separated) on the column's header, and the relevant rows are pulled out.

1. Click the **Manage Services** sub-menu. The **Create/Modify Services** screen is displayed.


Create/Modify Services
Create
Modify
* Service Type
Windows RDP
* Host Name
10.10.0.91
* IP Address
10.10.0.91
* Domain Name
arcosauth
Service Options
Use Credentials
Named Service
Server Type
tag1
* User Display Name
RDP
* User Description
Instance
* Port
3389
* User Name
RDP
IAM ARN
AWS Credentials
Browse
Password Options
Single Custody
Split Custody
Single Custody
Password Part
First Half
Second half
* Password
* Confirm Password
Other Owner
Valid Till Date
Tuesday , January 1, 2058
User Lock To Console / Supporting Service
Allow Password Change
Allow Password Request
Use Customized Connector
Description 1
Description 2
Description 3
Parameter
Enable Application Mapping
Application Mapping
Active Applications
Application Name
Description 1
Description 2
Description 3
Parameter
Is Active
Config Tags Description
Drop
Create
Clear

The **Create/ Modify Services** screen contains the following fields:

Field Name	Description
Create (radio button)	Select to create a service.
Modify (radio button)	Select to modify details of an existing service. ▪ The Administrator having **Modify Service** privilege will only be able to modify services. ▪ To modify details of Service, select the required Service from the grid on the left pane. The Service details are displayed under Create/Modify Services pane on the right side. Modify the required details and click **Modify**, to update the Service details.
Service Type	Select the type of service from the drop-down list.
Host Name	Specify the hostname of the Server.
IP Address	Specify the IP address of the Server.
Domain Name	Specify the domain name of the Server.
Service Options	**Use Credentials:** This field is enabled if you select the **Service Type** as **MS SQL EM – RDP**, to login to the server using the RDP credentials. **Dynamic Port:** Dynamic port can be enabled while connecting to **MS SQL QA Service**. While creating a service, if Administrator selects the Dymanic Port option, it is mandatory to pass the instance name of the server and user lock to console (supporting service) to connect to server. Therefore, the Administrator should enter the details in **Instance** field and select the **User Lock To Console or Supporting Service** from the dropdown. ▪ **Instance:** Enter the Instance name of the server to be connected. ▪ **User Lock To Console or Supporting Service:** Select the required supporting service having SQL Administrator rights. ◦ **User Lock To Console or Supporting Service** dropdown list will always display the active services list. Hence, the instance name and the supporting service will fetch the dynamic port number, and this port will connect to the target service. ◦ If Dynamic Port is enabled and the user does not select the supporting service, an error message **Please Select Service For → User Lock To Console/ Supporting Service** will be displayed.
Server Type	Select the type of Server.
User Display Name	Specify the User Display Name.
User Description	Specify the User Description.

Field Name	Description
Instance	Specify the instance name of the Server (if applicable).
Port	Displays the port number. ⚠ The data in this field is auto-populated based on the **Service Type** selected.
User Name	Specify the username.
IAM ARN	Each and every AWS Service can be uniquely identified with IAM ARN Text specified here. ⚠ This field will be visible for AWS Service Type.
AWS Credentials	Upload the CSV file that contains the Access Key and the Secret Key. ⚠ ▪ Both the keys will be stored in the database. ▪ This field will be visible for AWS Service Type
Password Options	▪ Single Custody- In this option, the Admin(Owner1 himself) assigns the password for the service and the service is created. ▪ Split Custody- In this option there are two owners of the password. Owner1 is the Admin himself who wants to create the service with his (first/second half) of the password and fills in the name of the second owner who will enter the other half of the password. The service will be created only when both the owners enter their part of passwords. ⚠ ◦ This checkbox can be selected only if **Store Passwords in Split custody** configuration is **Enabled** from **Settings.** ◦ The second owner receives an alert on ACMO and an email after the first owner has entered his part of the password for the service. After the second owner enters the other part the service is created, depending on the workflow.
Password Part	▪ First half- Select the checkbox to enter the first part of the password in the password field. ▪ Second half- Select the checkbox to enter the second part of the password in the password field. ⚠ Admin(Owner 1 himself) can select and enter either the first half or the second half of the password.
Password	Specify the password for the server.
Confirm Password	Re-enter the password and confirm.
Other Owner	Select the second owner's name who will enter the other half of the password and create the service.

Field Name	Description
Valid Till Date	Select the end date. This is the date from which the service will be inactive for the user. ⚠ This field is enabled, when you select the **Enable** checkbox.
Use Customized Connector	Used to select the customized connector.
User Lock To Console/ Supporting Service	Used for SSH Linux services to login to root and allow change of passwords.
Allow Password Change	To enable the password change process.
Allow Password Request	If the checkbox is enabled, then Users can raise a password request for that particular service. ⚠ By default the checkbox is **Enabled**.
Description 1	Specify the required description 1 (OS Version) for Service (if required).
Description 2	Specify the required description 2 (Server Description) for Service (if required).
Description 3	Specify the required description 3 (Location of Server) for Service (if required).
Parameter	Specify the parameter of Service (if applicable). ⚠ ▪ Refer configurations tag documents/or click Config tags Description for more details. ▪ ARCON supports multi sessions for SSH services. Multisession is configured in Server Manager→ Manage Service→ Select the service→ Add <MUTISESSION>tag in the parameter field.

Field Name	Description
Enable Application Mapping	Select this checkbox to have multiple connector options when taking the connection for the created service. ⚠ This can be enabled only for the following service types ▪ App Xshell ▪ App SecureCRT ▪ App MobaXterm ▪ App WinSCP ▪ App FileZilla ▪ App BMT ▪ App BSCLOGCOL ▪ App 3 HIT Tool ▪ App Win fiol ▪ Putty
Active Applications	It lists all the applications selected from the Application Name dropdown.
Application Name	Select the application names from the dropdown which should be available when taking the connection for the created service.
Description 1	Specify the required description 1 (OS Version) for Service (if required).
Description 2	Specify the required description 2 (Server Description) for Service (if required).
Description 3	Specify the required description 3 (Location of Server) for Service (if required).
Parameter	Specify the parameter of Service (if applicable).
Is Active	It enables all the applications set under Enable Application Mapping.
Config Tags Description	Click link to view configuration tags.
Drop button	Used to disable or delete the service from ARCON PAM. Click **Drop**, A pop up is displayed with two options: ▪ **Disable Service:** Used to disable the service in ARCON PAM. ▪ **Permanently Delete Service:** Used to permanently delete the service from ARCON PAM. ⚠ The Administrator having **Drop Service** privilege will only be able to disable or delete services.

2. Click **Create**. A window pops up with the following message:
New Server Instance Created

⚠ On creating Linux services, a pop-up window is displayed to confirm whether the password has to be vaulted.

3. Click **OK**. A new service is created for the user.

The new service created is displayed in **Manage Services** grid, once you have mapped it under a particular LOB.

⚠ Once a service is successfully created, you need to then map the service to a particular LOB. In some cases, wherein an administrator having **Settings** privileges has configured the value for the **LOB Wise Service Management - Is Enabled** option, where

- **LOB Wise Service Management - Is Enabled** toggle value is set to **Enabled**, then it states that when a service is created, it will directly map the service to the selected LOB from **Select LOB/ Profile** dropdown list, once it is created.
- **LOB Wise Service Management - Is Enabled** toggle value is set to **Disabled**, then it states that the service created needs to be mapped to a particular LOB in **LOB/Profile Master & Manager**.

⚠ While creating service and manually changing password of any existing service, a prompt will be displayed stating:
Do you want to Vault With New Password Immediately?
On User's confirmation, a new password will be generated by ARCON PAM. The new generated password will be vaulted in ARCON PAM and updated on Target Device.

⚠ To enable Password Change through Gateway Server, enable **Use Gateway Server (ARCON PAM - Firewall)** from **Password Change Defaults (Default Configuration)**.

On the topmost corner of the Create / Modify Service Page, Click the down arrow key and the following options will be displayed.

Options	Description
Paste Service Details	Directly paste the service details (the service details should already be copied to the clipboard)
Resolve Hostname	It will fetch for Hostname for a similar IP in the Database and automatically take up the hostname if there is an existing service in the same combination
Resolve IP Address	It will fetch for IP Address for a similar Hostname in the Database and automatically take up the IP Address if there is an existing service in the same combination
Resolve Hostname to DB	It will fetch for Hostname for a similar IP in the Database and automatically take up the hostname if there is an existing service in the same combination

4.3.1.1 App X-RDP

X-RDP service users can remotely connect to Windows Desktop and access files, applications and other network resources. If an X-RDP service type is assigned to user(s), when user(s) select the LOB and X-RDP Service type all the services will be listed.

1. To start RDP on second screen, configure **ARCOSAppExeTerminal_Config.ini** in ACM folder:
2. **ShowOnSecondaryMonitor** should be set to 1, If the value is set to 0, it will open on the same screen.
3. App X-RDP can be launched either directly or via Remote Desktop Plus too. For launching it with RDP Plus, tag <RDPPLUS> should be mentioned in field 4. else it will launch directly.

4. Port must be changed to **3389** while configuring App X-RDP in Server Manager.

4.3.1.2 ARCON DBeaver QA Connector

ARCON has extended the database integration by integrating DBeaver DBMS (Community Edition) which is a universal database management tool.

With DBeaver you are able to create analytical reports based on records from different data storages, export information in an appropriate format. For advanced database users DBeaver suggests a powerful SQL-editor, plenty of administration features, abilities of data and schema migration, monitoring database connection sessions, and a lot more.

Out-of-the box DBeaver supports more than 80 databases, but currently ARCON has tested the integration with MSSQL and Oracle.

This document will guide you through the steps involved in the deployment for the **ARCON Privileged Access Management (PAM) DBeaver QA Connector.** The following steps are to be followed for the successful deployment of ARCON PAM Datawarehouse in your environment.

4.3.1.2.1 Pre-requisites

Before configuring the ARCON PAM DBeaver QA Connector, you should read the **ARCON PAM connector Pre-requisite** document to ensure that your environments meets the minimum installation requirement for the ARCON PAM product.

- End-user machine should have access to below web components
    - ACMO (PAM Portal)
    - ARCON PAM API
- PAM Version: U10
- Java 8 (32/64 bit based on system) should be installed on the system to run DBeaver https://www.java.com/en/download/manual.jsp

4.3.1.2.2 Configuration:

4.3.1.2.2.1 Oracle QA Service.

Create a Oracle QA service and Parameter 4 of service needs to be **<dbeaverqa><ORACLE>**

4.3.1.2.2.2 MSSQL QA Service

Create an MSSQL QA Service and Parameter 4 of service needs to be **<dbeaverqa><MSSQL>**

4.3.1.2.3 Features

The following are the features of the DBeaver QA Connector:

- Single Sign On
- Command Restrictions
- Critical With Approval
- Alerts for Critical Commands
- Session Recording
    - Command logs
    - Video Logs
- Smart Session Monitoring
- Behavior Analytics

4.3.1.2.4 Issues Resolved

The Following issues are resolved with DBeaver QA Connector:

- Multiple Instances.

- Block popups for daily tips, Sample Database.
- Block Driver Download and set driver paths.
- Fixed command logging for multiple times execution of the same query.
- API Slowness.
- Restrict Dbeaver UI's editing options

4.3.1.3 App Corona Workbench

4.3.1.3.1 Overview

Corona is a Banking Tool that smart streams solution for effectively reconciling the following

- Nostro accounts
- Securities messages (settlements, statements of holdings, statements of transactions, and corporate actions)
- Forex, money market, derivative, and commodity confirmations
- Intra-day messages
- Cards-based transaction messages

It also includes the calculation module Corona Quantum which allows you to calculate positions for configurable periods by processing data from Corona Cards, Corona Cash, or external data sources. It also enables you to generate all types of Intraday Liquidity Reports according to the regulatory requirements of the Basel III agreement. Corona delivers complete transaction management and control and integrates a powerful module for the detection of exceptions, enabling institutions to reduce operational risk and cost through continual process improvement.

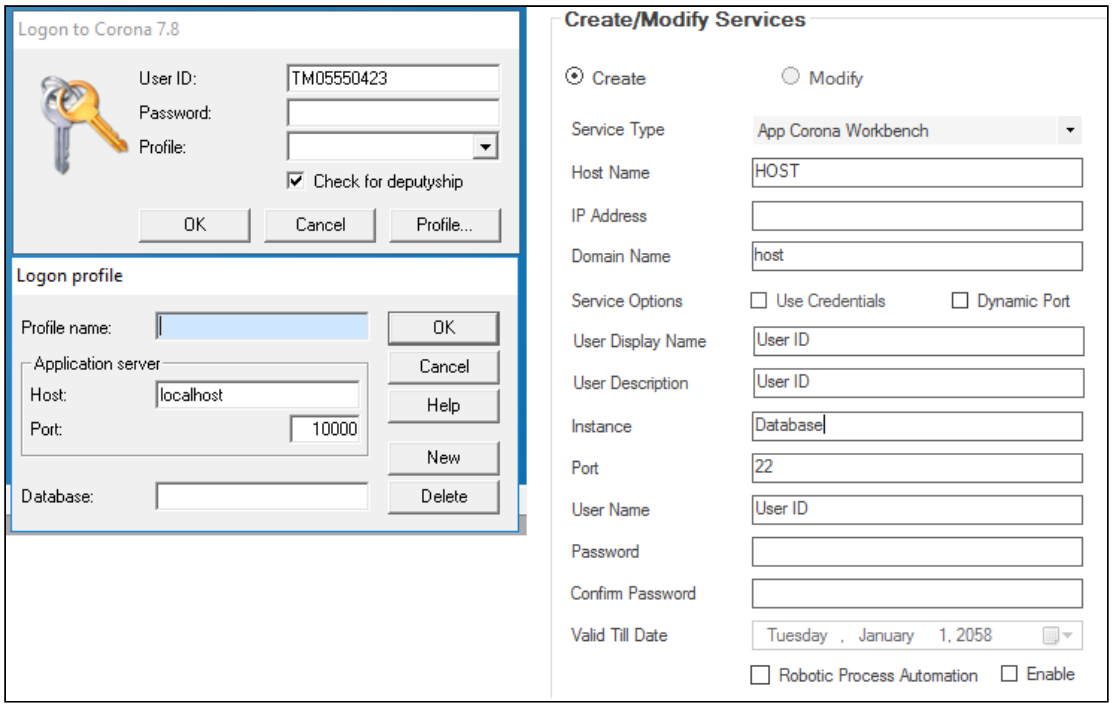
4.3.1.3.2 Pre-Requisite

Before configuring the ARCON PAM Corona Workbench Connector, you should read the **ARCON PAM connector Pre-requisite** document to ensure that your environment meets the minimum installation requirement for the ARCON PAM product.

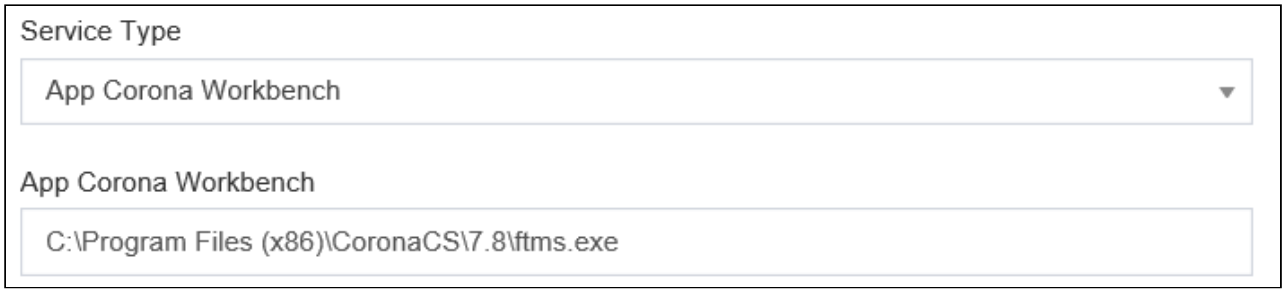
- The end-user machine should have access to the web component mentioned below
    - ACMO (PAM Portal)
- PAM Version: U10
- Exe Path: End user should have the corona application installed on the system (for eg.: C:\Program Files (x86)\CoronaCS\7.8\ftms.exe)
- Propertyfilepath: Folder hierarchy should be present at the end-user %APPDATA% \SmartStream Technologies\Corona\7.8

4.3.1.3.3 Configuration

1. Open Server Manager from ACMO.
2. Navigate **Manage → Users and Services → Manage Services.**
3. In the Manage Service screen, you can create the service type as App Corona Workbench by entering the Host Name, IP and Domain Name, and Port in the respected fields of the service.
4. Corona Database details need to be updated in the instance field of service



5. In the Parameter field,
    a. Property File Path **<DATA><CONFIGPATH>%APPDATA%\SmartStream Technologies\Corona\7.8\Logon Profiles.ini</CONFIGPATH></DATA>**
    b. Check for deputyship use **<deputyshipon>**
    c. Uncheck for deputyship use **<deputyshipoff>**
    d. Default tile is "Logon to Corona 7.8" for corona workbench. If the title is changed then include the title in the following format **<DATA><lwh>New title</lwh></DATA>.**
6. The path of this application should be copied and entered under the local path in My Preferences in ACMO.



7. Now, we can simply connect to the service from ACMO.

4.3.1.3.4 Features

The following features of ARCON PAM are supported by the App Corona Workbench Connector.

- Single Sign-On
- Session Recording
- SSM

4.3.2 Add Services in DMZ Supporting Server

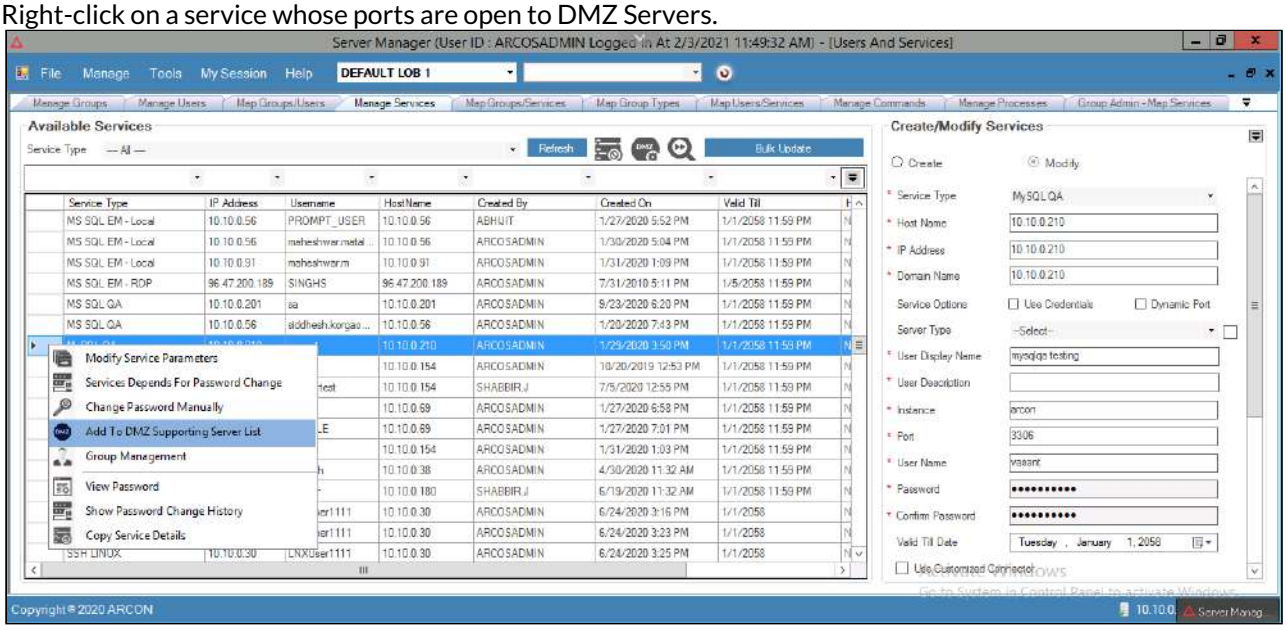
A DMZ or Demilitarized Zone is a secure server that adds an additional layer of security to a network and acts as a buffer between a local area network (LAN) and a less secure network which is the Internet. In computer security, a DMZ is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the Internet. Therefore, as a DMZ segments a network, security controls can be tuned specifically for each segment. This section helps you to add services to DMZ Server.

To add services in DMZ Supporting Server:

To add a services in DMZ Supporting Server, use the following path:

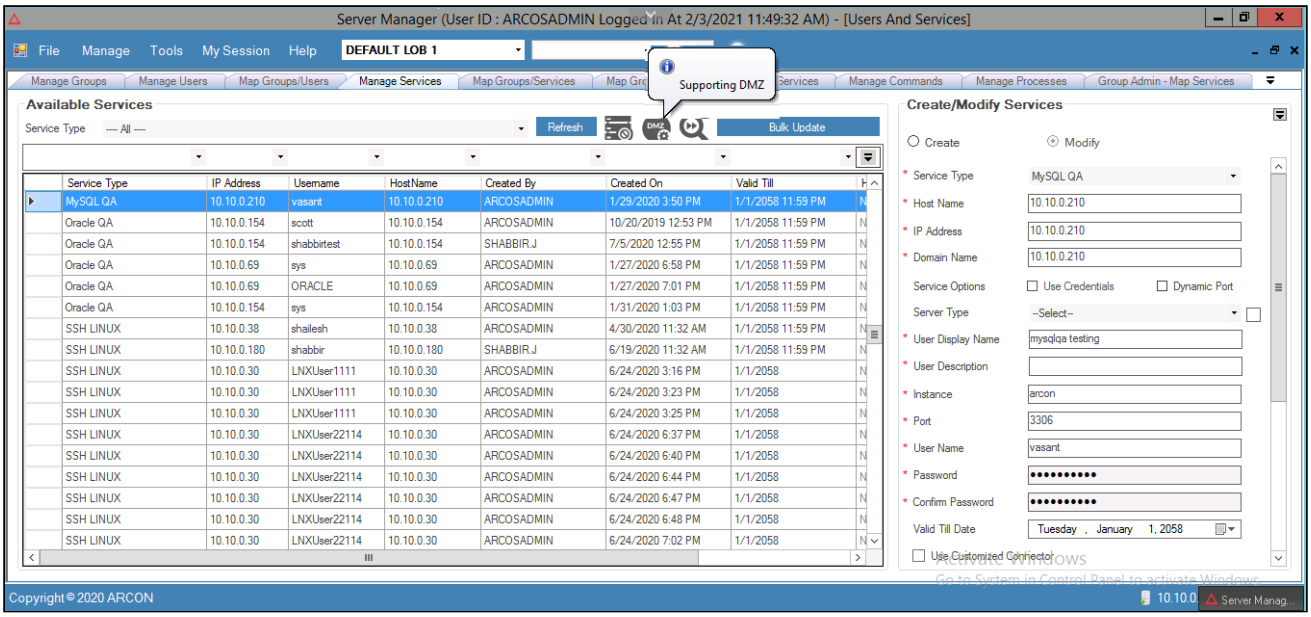
Manage → Users and Services → Manage Services

1. Right-click on a service whose ports are open to DMZ Servers.

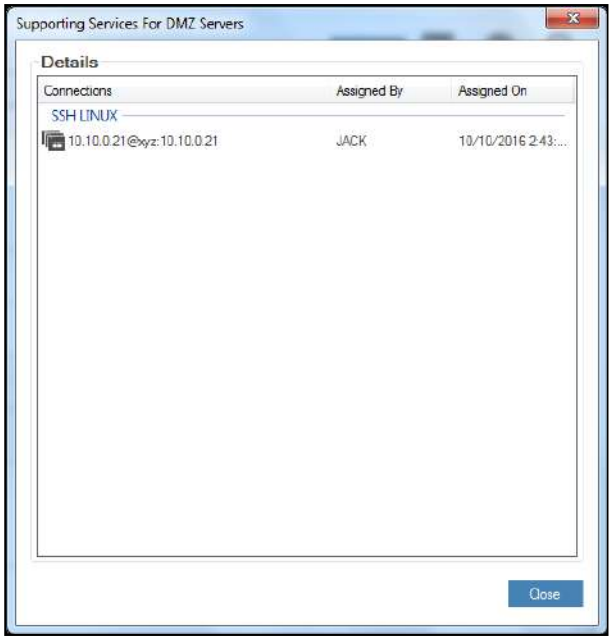


2. Choose **Add To DMZ Supporting Server List** option from the list. A window pops up with the following message:
   Are You Sure You Want To Add The Selected Service To Supporting Service(s) For DMZ Server List?
3. Click **Yes.** Another window pops up with the following message:
   Selected Services Has Been Added To Supporting Services For DMZ Servers List.
4. Click **OK**. The service is added to DMZ Server List.

To view the added services in DMZ Zone:



1. Click **Supporting DMZ** icon. The **Supporting Services For DMZ Servers** window pops up.



2. View the added services and click **Close**.

4.3.3 Service Quick Search

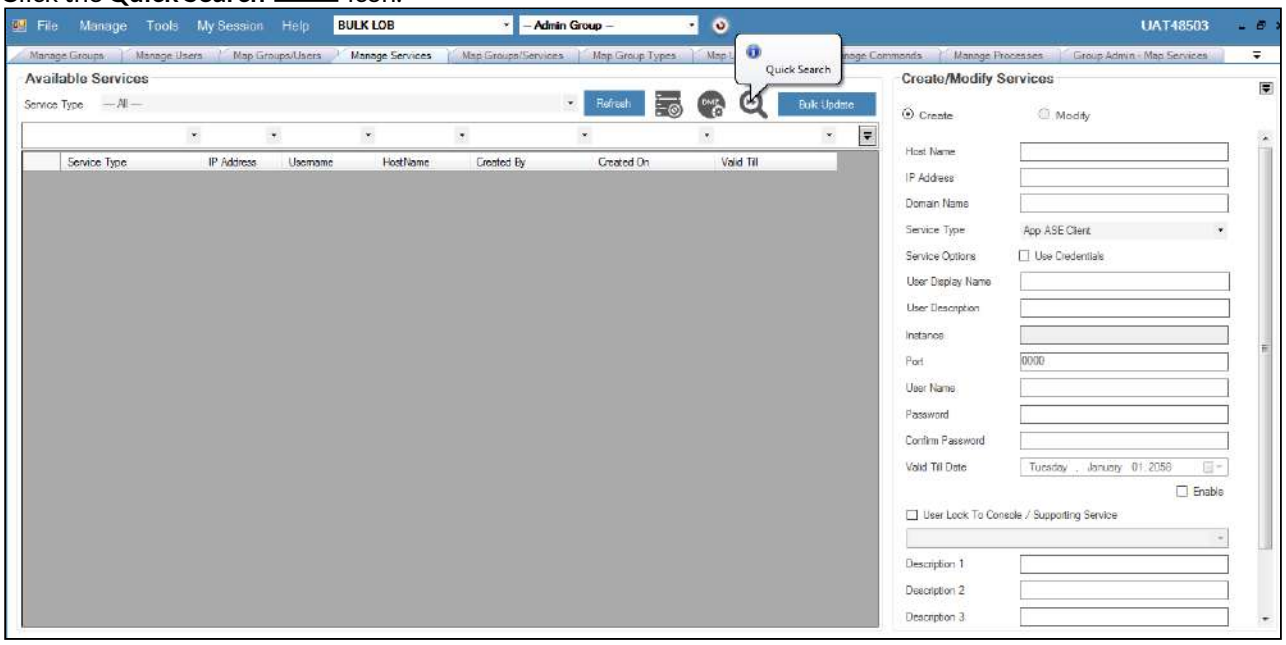
This section explains the steps to search for a service. The Administrator who knows details of service such as IP Address, Host name, name of Domain, user name of service, or type of service can search for a service using Quick Search option.

To search for a service using Quick Search:

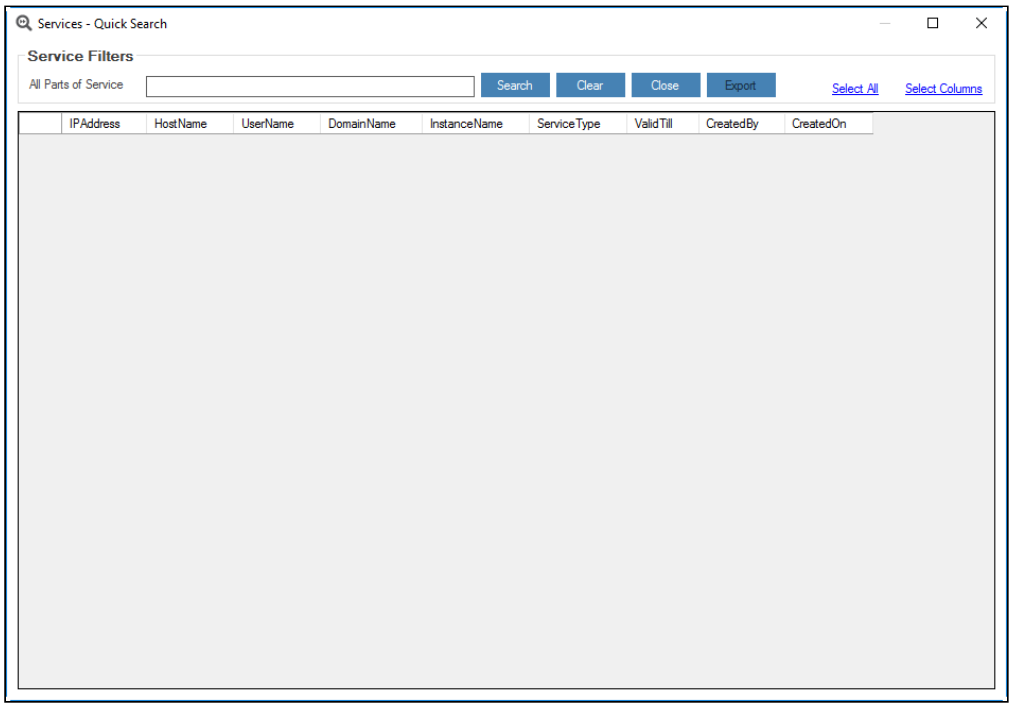
To search for a service using Quick Search, use the following path:

Manage → Users and Services → Manage Services

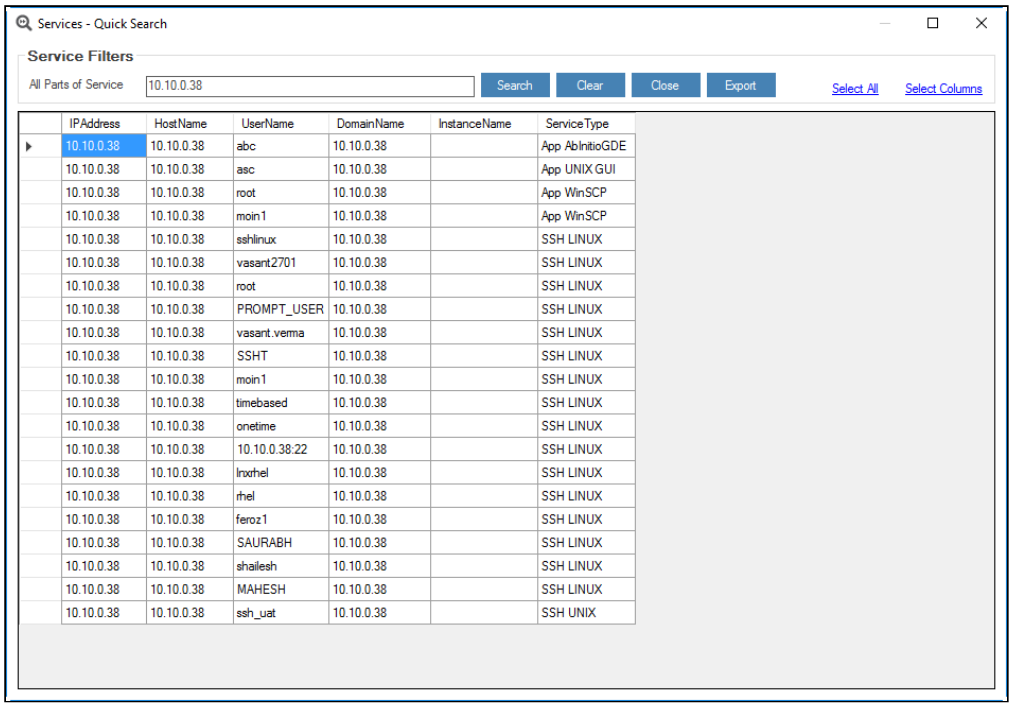
1. Click the **Quick Search**  icon.



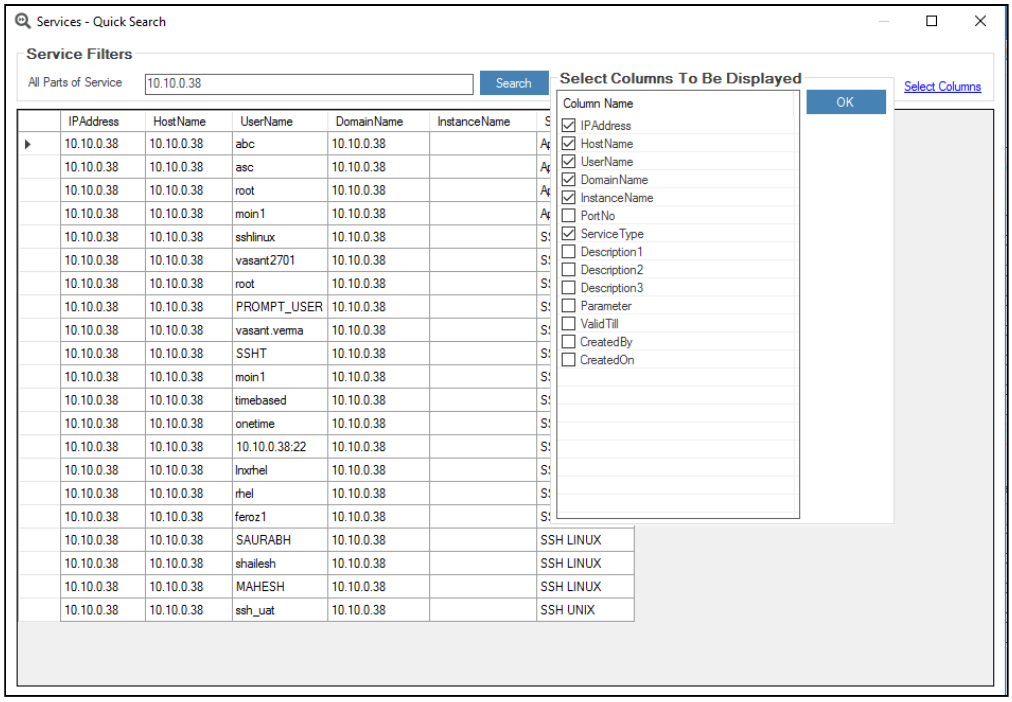
2. The **Services - Quick Search** window pops up.



3. You can enter part of Service in **All Parts of Service** field and click **Search** button. Details will be displayed in grid view.



4. Click **Export** button to export the service details.
5. Click **Select All** link to select details displayed in grid view.
6. Click **Select Column** link to select columns to be displayed.
7. Select the required Column Name and click **OK**.



8. Service details will be displayed in selected columns.

4.3.4 Define a Critical Command for a Service

Critical Commands are commands which are defined as highly critical for use. These commands when executed will have crucial impact on the target server or to the resources associated with it. When an attempt is made to execute a critical command, it will prompt for confirmation for executing the command.

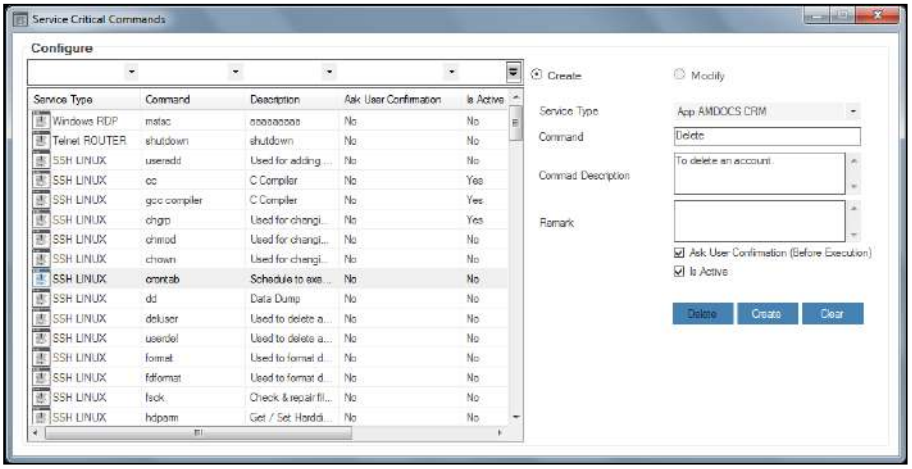
This section helps you to define a critical command for a service. In addition, you can modify or delete an existing defined critical command.

> ⚠ The Administrator having **Service Critical Commands** privilege in Server's Privileges will only be able to define a critical command for a service.

To define a critical command:

To define a critical command, use the following path:

Tools → Advanced Configuration → Service Critical Commands



The **Service Critical Commands** screen contains the following fields:

Field Name	Description
Create	Create a critical command for a service.
Modify	Modify an existing critical command defined for a service. ⚠ To modify a critical command, select the required command from the grid on the left pane. The Command details are displayed on the right side. Modify the required details and click **Modify** button, to update the Command details.
Service Type	Select the type of service.
Command	Define a command.
Command Description	Specify command description.
Remark	Specify the remark.

Field Name	Description
Ask User Confirmation (Before Execution)	Indicates that the user will be asked for confirmation before executing the command.
Is Active	Enables the configuration.
Delete button	Click **Delete**, to delete the selected critical command from ARCON PAM.

1. Select/Enter the details and click **Create**. A window pops up with the following message: **New Service Critical Commands Created.**
2. Click **OK**. The new critical command is defined.

> ⚠
> - To modify an existing defined critical command, select the command from the grid and modify the required changes and then click **Modify** to modify the changes.
> - To delete an existing command, select the critical command from the grid and click **Delete** to delete the details.

4.3.5 Service Classification

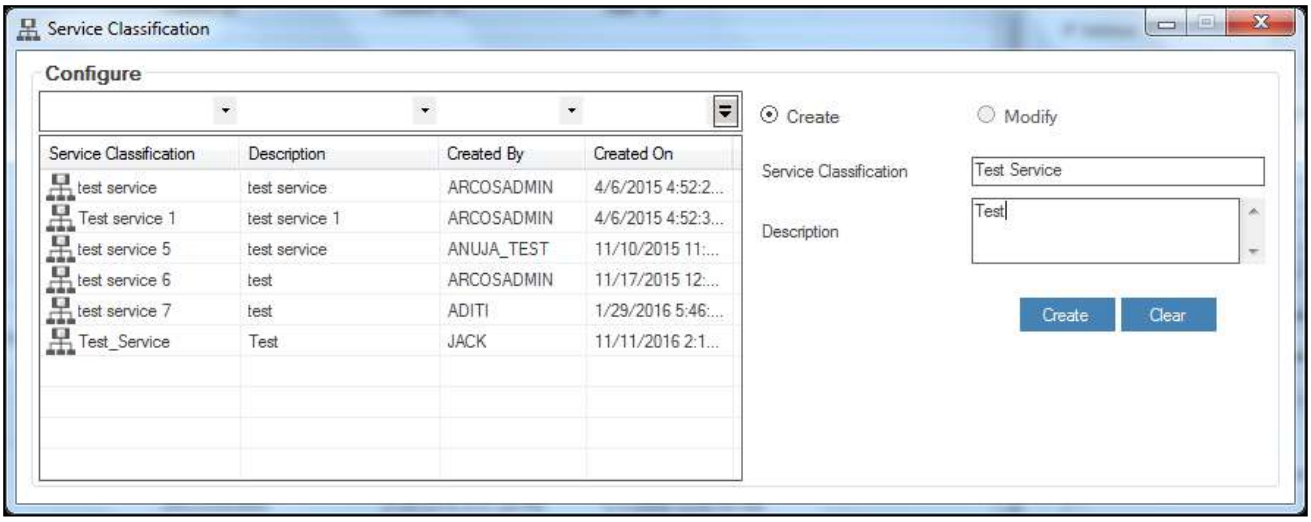
Service Classification defines the classification for a service such as critical, data, or antivirus server. In addition, you can modify the existing defined classification. Once the classification is defined, you can apply the classification while modifying parameters of a service.

> ⚠ The Administrator having **Service Classification** privilege in Server's Privileges will only be able to configure under Service Classification.

To define service classification:

To define service classification, use the following path:

Tools → Advanced Configuration → Service Classification



The **Service Classification** screen contains the following fields:

Field Name	Description
Create	Select to create a service classification.
Modify	Select to modify details of service classification. ⚠ To modify details of service classification, select the required service classification from the grid on the left pane. The details are displayed on the right side. Modify the required details and click **Modify** button, to update the service classification details
Service Classification	Specify the name for a service classification.
Description	Specify the description for a service classification.

1. Enter the details and click **Create** button. A window pops up with the following message: **New Service Classification Created.**
2. Click **OK**. The new service classification is created.
3. You can apply this service classification to service (s).

    a. **Apply to a single Service:**
    To apply Service Classification to single service, use the following path:
    Server Manager → Manage → Users and Services → Manage Services

        i. Select a service.
        ii. Right click and select **Modify Service Parameters**.
        iii. Select **Service Classification** from drop down.
        iv. Click **Modify**. The selected Service Classification will be applied to Service.

    b. Apply to a group of Services:
    To apply Service Classification to services, use the following path:
    Server Manager → Tools → Advanced Configuration → LOB / Profile Default Configuration → LOB / Profile - Password Policy

i. Select the LOB or profile from the **LOB/ Profile** dropdown list. A list of service groups are displayed in the grid.
ii. Select the checkbox from the **Service Group Name** list. It displays the count of services for that particular group under **Service Type** grid.
iii. Select a type of service from the **Service Type** list. This will enable you to set automated change passwords for that particular service type.
iv. To apply service classification, select **Allow** checkbox against **Service Classification** drop down. The drop down will be enabled.
v. Select the required service classification.
vi. Click **Confirm Changes** button. Service Classification will be applied to services under selected Service Group and Service Type.

4.3.6 Copy Service Details

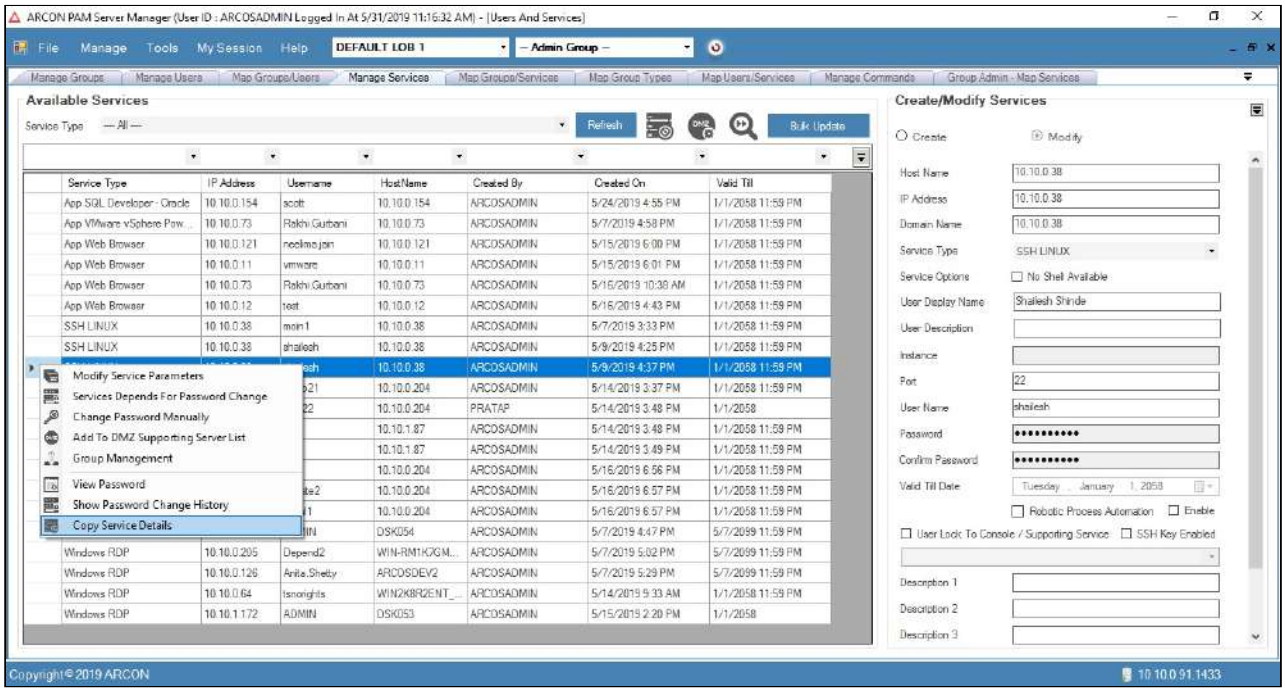
This section explains the steps to copy details of one service to another. You can copy all details displayed in **Create/ Modify Services** screen under **Manage Services**.

To copy details of Service

To copy details of Service, use the following path:

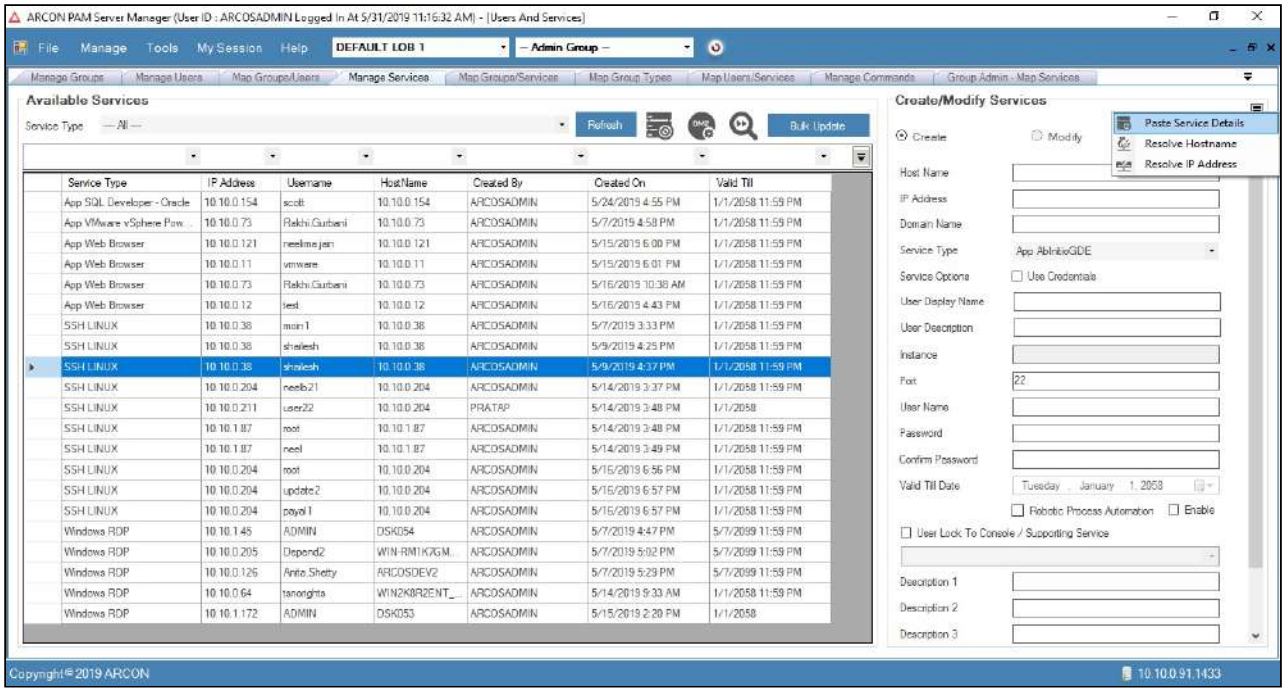
Manage → Users and Services → Manage Services

1. Right click on the Connections from the **Available Services** list. A multiple options list is popped up.

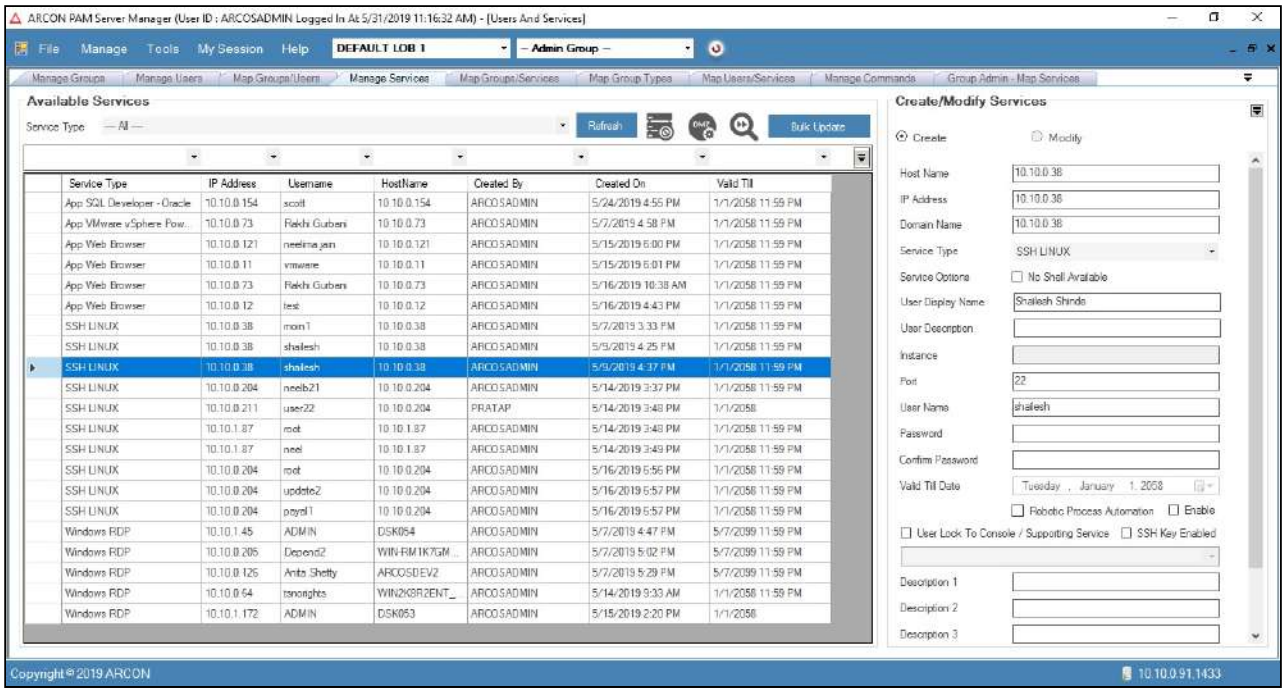


2. Click **Copy Service Details** option.
3. The following success message will be displayed.
   Service Details Copied To Clipboard
4. Click **OK**. The service details displayed in **Create/Modify Services** screen are copied to clipboard.
5. Select  icon displayed in top left under **Create/Modify Services** screen.

6. A multiple options list is popped up. Click **Paste Service Details** option.



7. Service Details will be copied in fields.



8. Edit required details and click **Create** button to create new Service.

4.3.7 Bulk Update

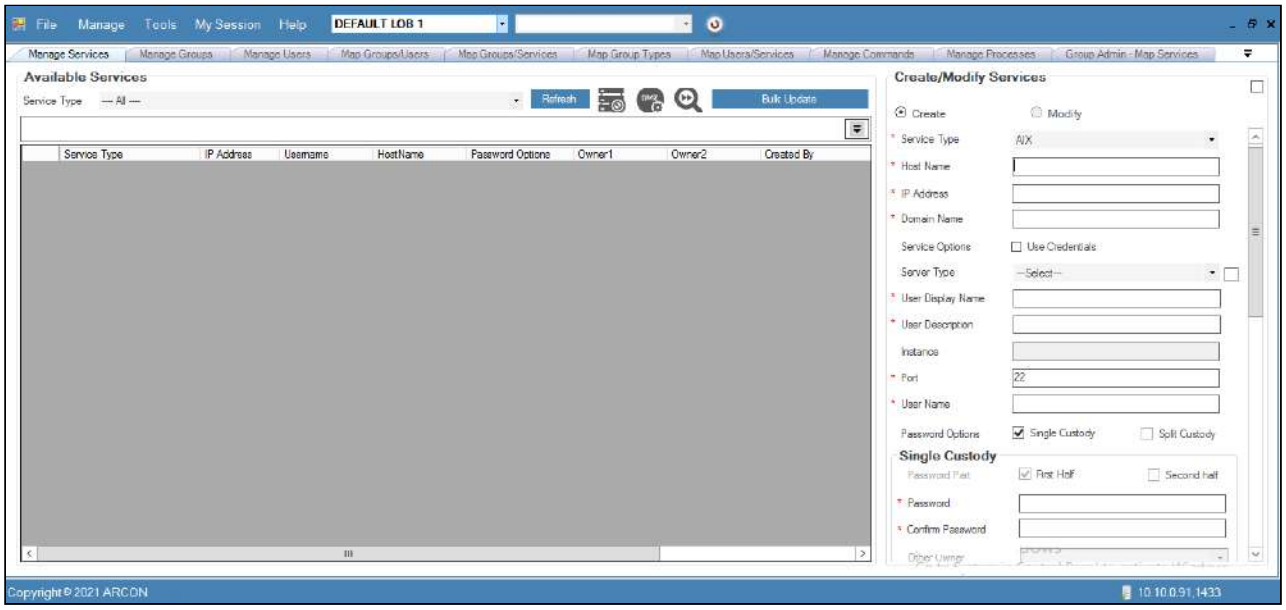
This section explains the steps to bulk update and delete services. The Administrators are responsible for updating and deleting services.

To Bulk Update or Delete Services:

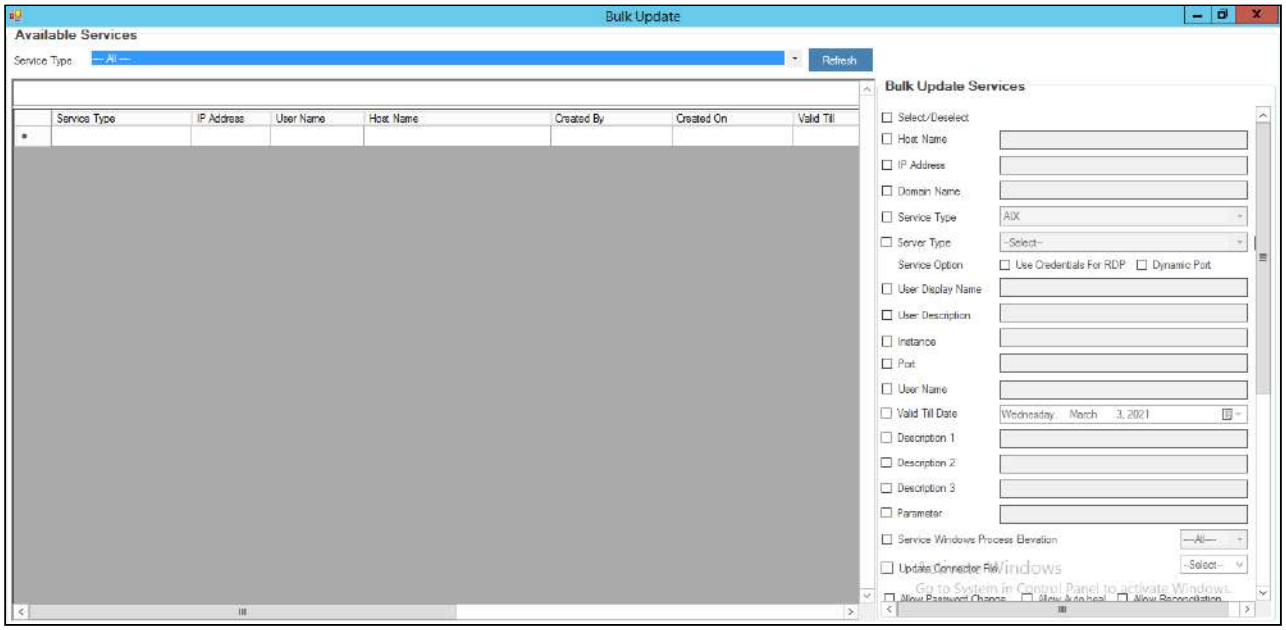
To Bulk Update or Delete Services, use the following path:

Manage → Users and Services → Manage Services

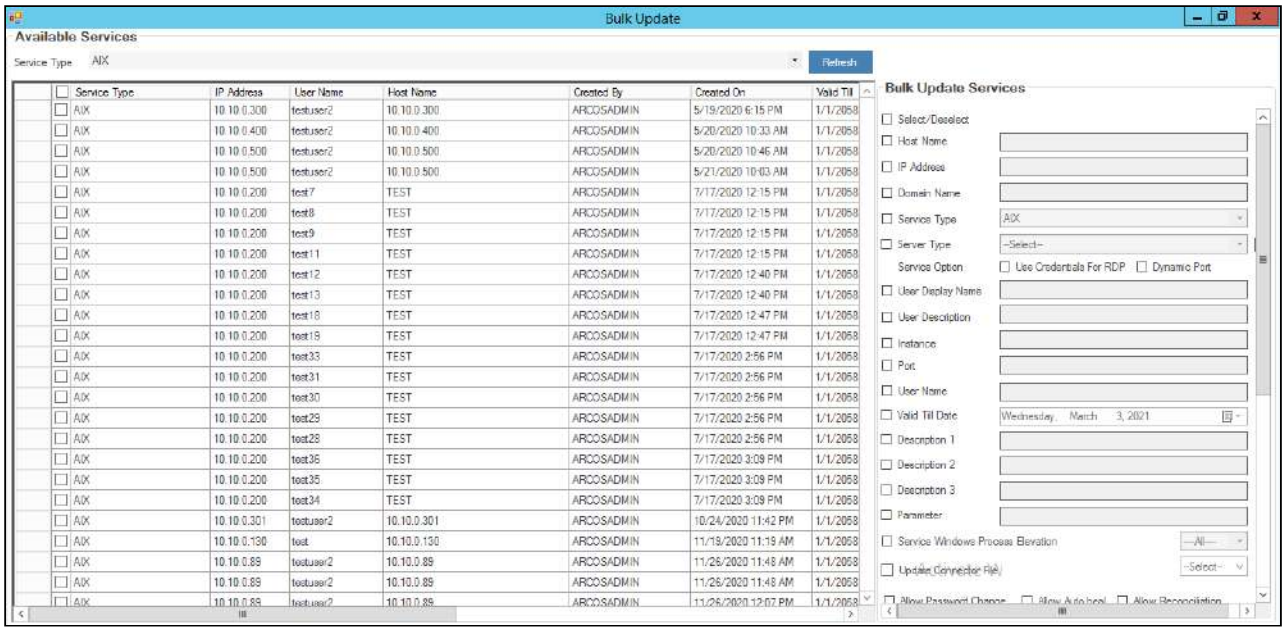
1. Select the particular LOB for which the Bulk Update or Delete has to be performed.



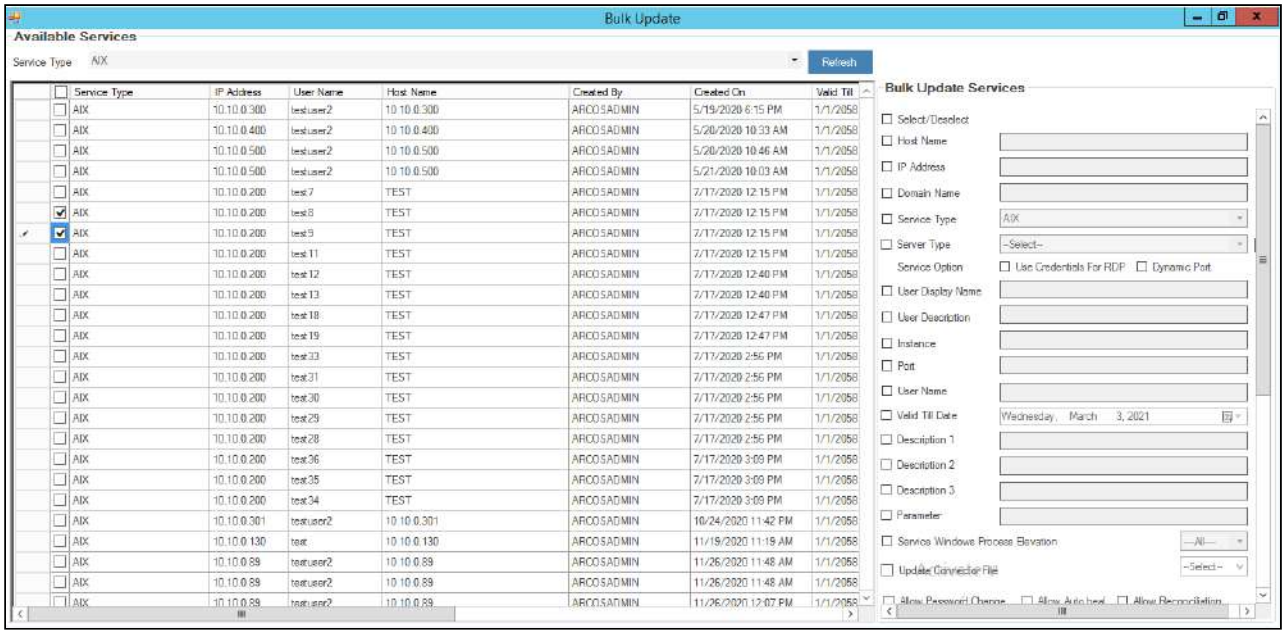
2. Click the Bulk Update option, the following window will be displayed.



3. Select the service type from the dropdown for which you want to do a bulk update or delete and click Refresh.
4. It will list all the services under the selected service type, select the services for which you want to do a bulk update or delete.



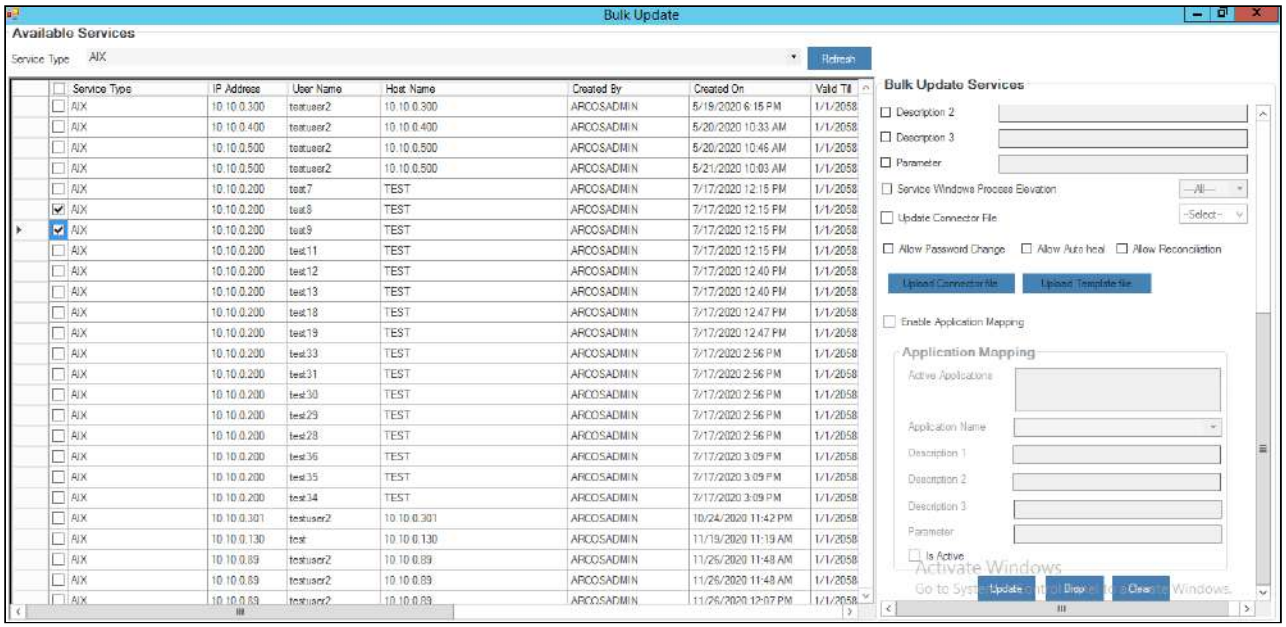
5. Select the checkboxes on the Bulk Update Services form on the right side.



6. Enter the changes that you want to make on the form and click Update to do a Bulk update of the selected services.
   For Example: If you want to change the port number for all the selected services, enter the new port number on the form and click update to bulk update the port number for all the selected services.
7. **For Bulk Delete** the above steps 1-4 should be followed.

> ⚠ If **Service Windows Process Elevation** checkbox is configured to **Yes,** then it will allow to elevate processes for selected services in bulk. In other words, it allows Users to elevate processes assigned to services.

8. Click the **Drop** button to delete the services, the following two options will be displayed.



a. **Disable Service:** Click this button to delete the service temporarily, the service will be listed under disabled services on the Managed Services page
b. **Permanently Delete Service:** Click this button to permanently delete all the selected services.

4.3.8 Modify Service Parameters

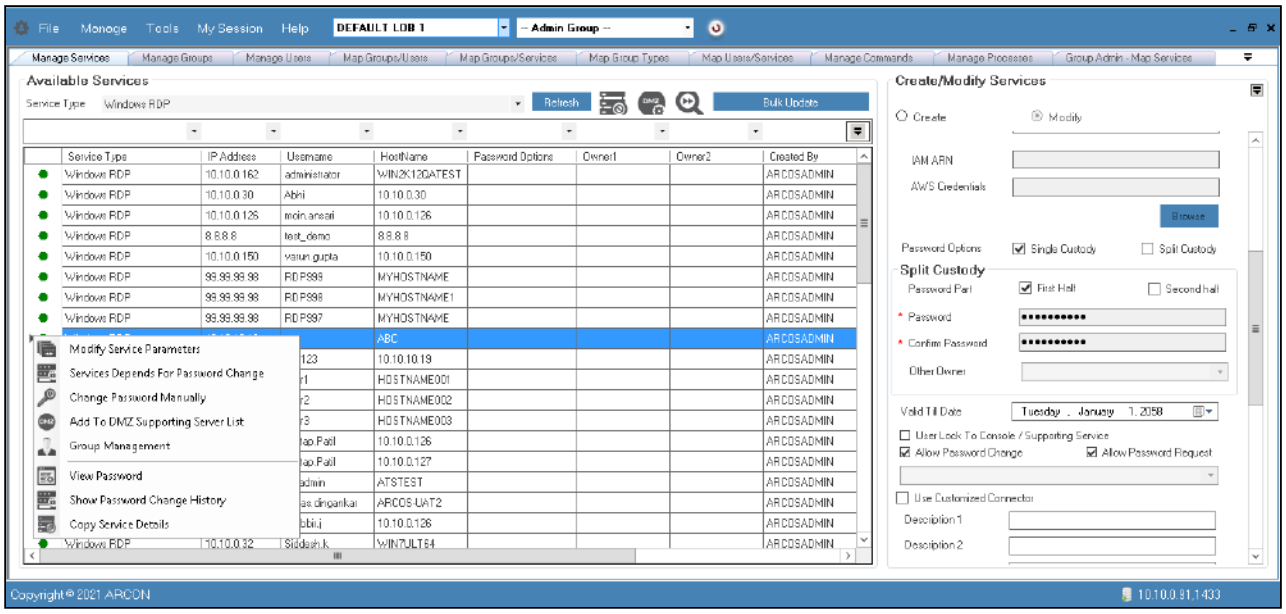
This section helps you to schedule password change process for a particular service.

To schedule password change process for a service:

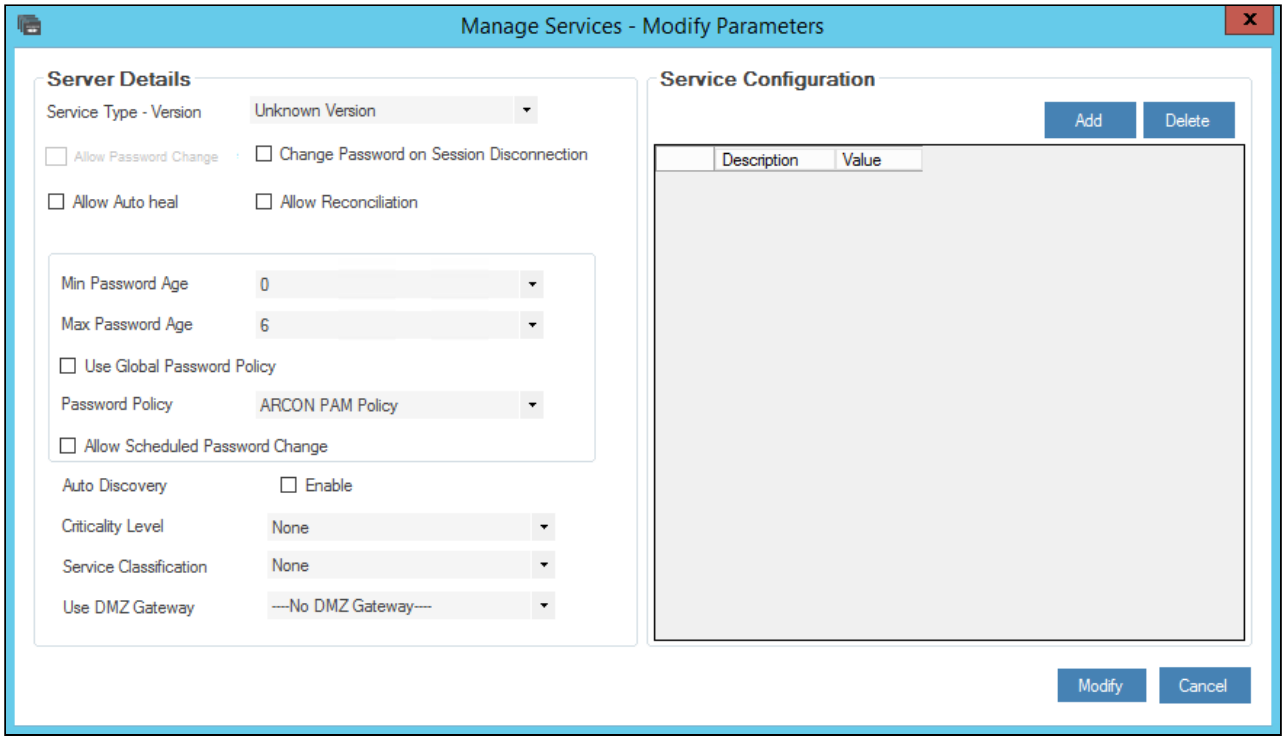
To schedule password change process for a particular service use the following path:

Manage → Users and Services → Manage Services

1. The services available in the grid are displayed based on the LOB and service type selected from the **Select LOB/Profile** drop-down list (in the home screen Server Manager) and **Service Type** drop-down list respectively. Click **Refresh** button after selecting the **LOB** and **Service Type.**
2. Right-click on the service for which you want to schedule the password change process and choose **Modify Service Parameters** option.



3. The **Manage Services - Modify Parameters** screen is displayed.



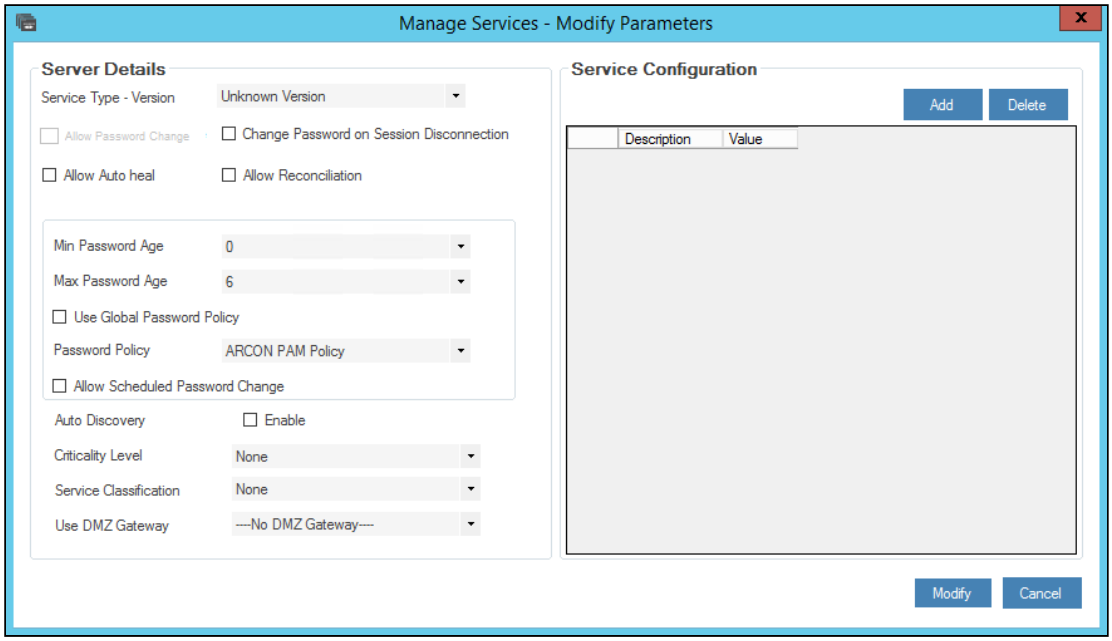
The **Manage Services – Modify Parameters** screen displays the following fields:

Field Name	Description
Service Type - Version	Select the service type version from the dropdown list. ⚠ • Commands are displayed in the dropdown list based on the selected Service Type. • The commands configured under **Custom Commands Configuration** screen is displayed in this dropdown.
Change Password on Session Disconnection	The password of the service changes after the session is closed from the PAM. On enabling the checkbox, the following popup window comes up- Enabling this option might affect existing sessions or immediate reconnection of the same service.? ⚠ The password change will happen for only those services which are configured in **ARCOSSPC- Supported Service Tyes** in **Settings**.
Allow Auto heal	To enable auto-healing for the service. Auto healing is supported by the following service types- • SSH Telnet ⚠ For SSH Telnet service En Account must be there in the Server Manager. • MS SQL EM - Local • MySQL QA • SSH LINUX • MS SQL QA • MS SQL EM - RDP • SSH Router • SSH Switch • SSH Firewall • SSH Unix • ORACLE QA
Allow Reconciliation	To enable reconciliation for the service. Reconciliation is supported by the following service types- • SSH Telnet • MS SQL EM - Local • MySQL QA • SSH LINUX • MS SQL QA • MS SQL EM - RDP • SSH Router • SSH Switch • SSH Unix • ORACLE QA

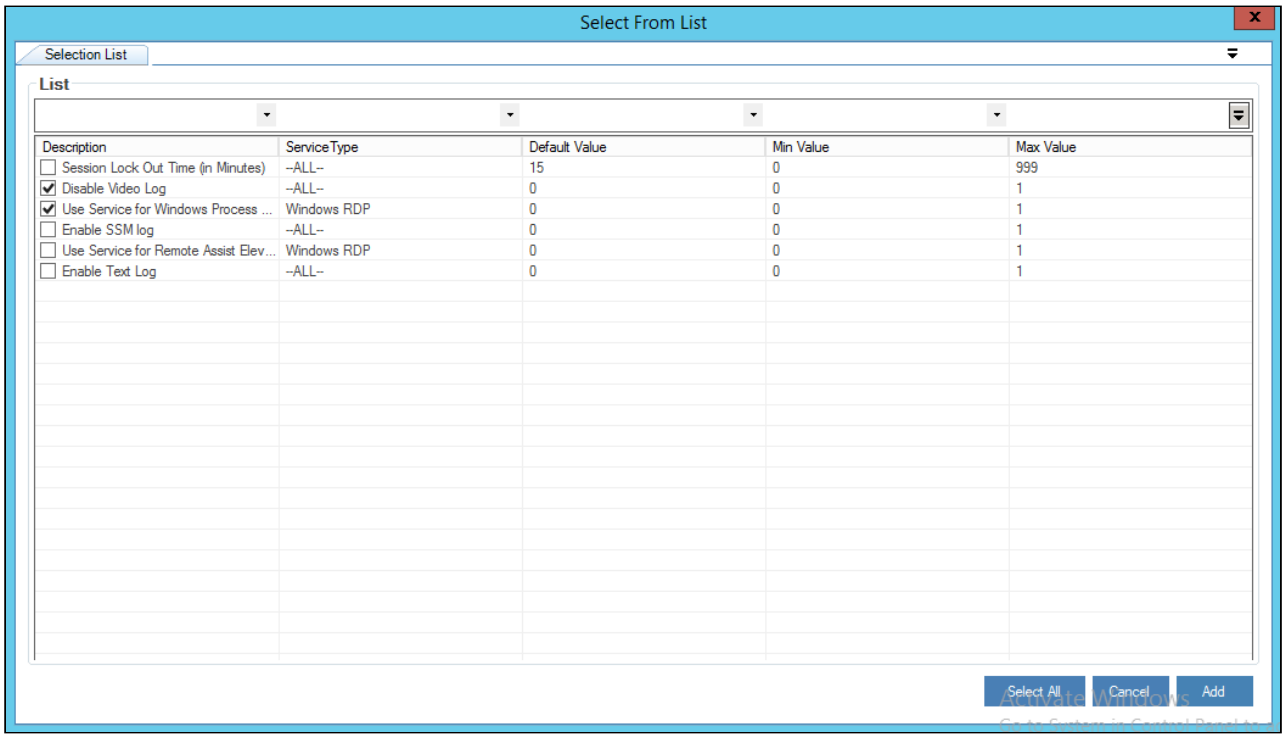
Field Name	Description
Min Password Age	Select minimum days for the scheduled password change process. ⚠ Password of Service will not be changed before the defined minimum days. Eg.: If you configure Minimum Password Age as 3; then the password change process cannot be performed before 3 days.
Max Password Age	Select maximum days for the scheduled password change process. ⚠ The password change process will be scheduled automatically depending on the selected max password age field.
Use Global Password Policy	Select to enable the global policy configured for the password change process.
Password Policy	Select the password policy. ⚠ By default, **Default Profile** is selected. You can create your own password policy, save it and select it in this field.
Allow Scheduled Password Change	Select to enable/configure the scheduled password change process. ⚠ By enabling this checkbox the password change process for the selected service will be scheduled according to the selected min and max password age and selected password policy or the global password policy.
Auto Discovery	Select this check box to enable Auto-Discovery of users on a particular server.
Criticality Level	Select the criticality level of the service. ⚠ This criticality level shall be considered while displaying reports.
Service Classification	Select the Service Classification. ⚠ • The value displayed here is the value that is configured in **Settings → Service → Service Modifications → Service Classification.** • This classification level shall be considered while displaying reports.

Service Configuration

1. To Add the Service Configuration details, Click Add on the top right side.



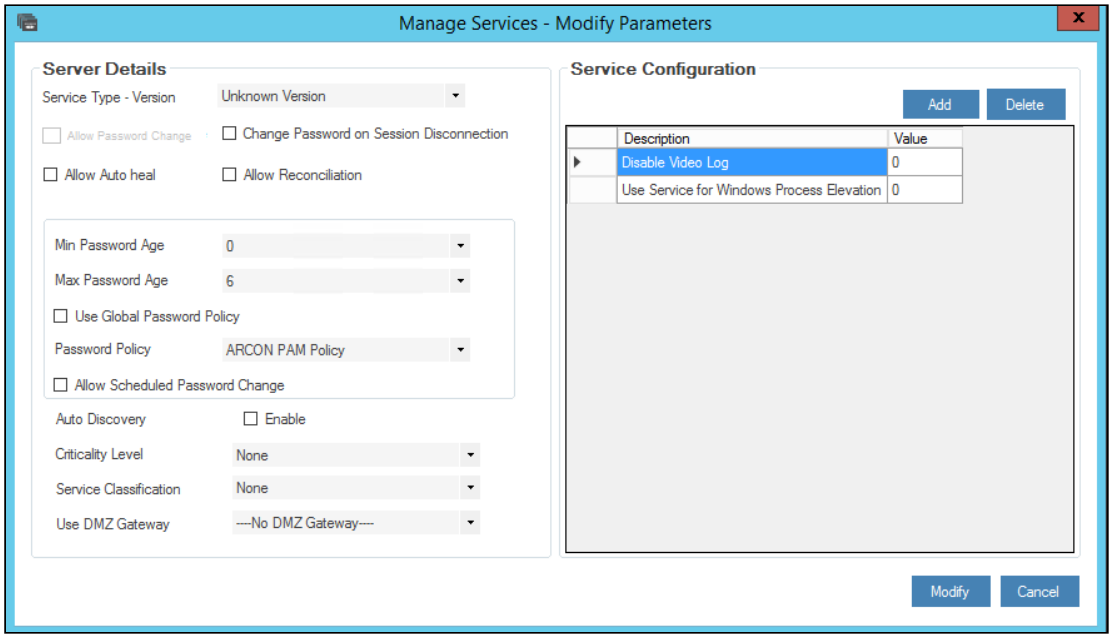
2. Select the checkboxes to configure that particular configuartion for the service.



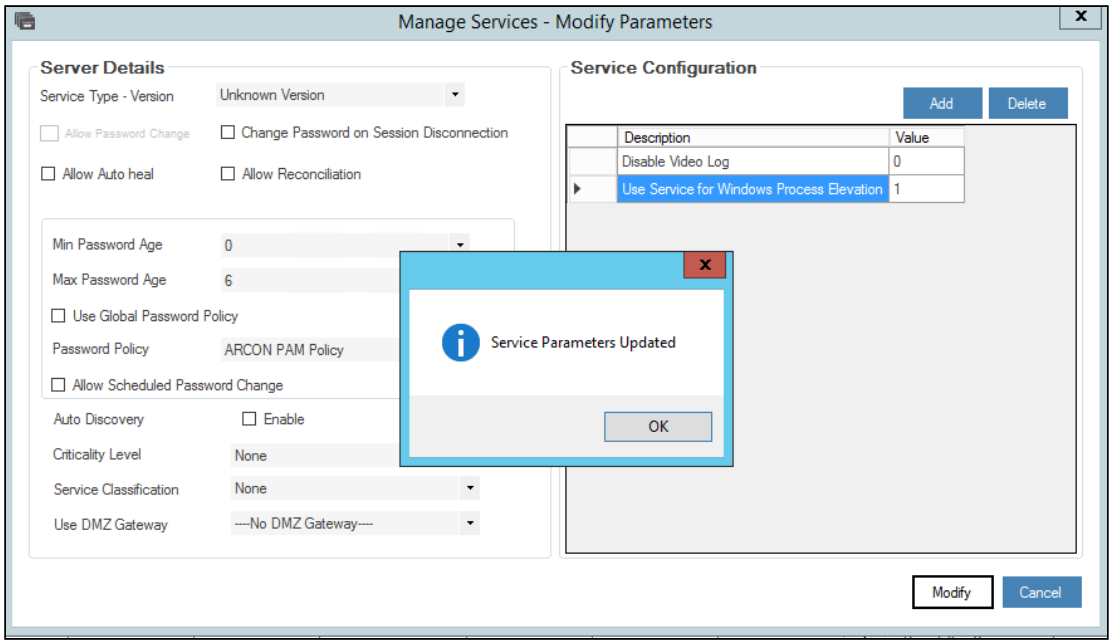
a. **Session Lock Out Time (in Minutes):** This option will set the duration after which an idle session should be locked out. Specify the time after which the session will be locked out if idle.
b. **Disable Video Log:** This configuration will check whether the images are to be captured during the session or not. If the value is 1, then it will not capture images. If the value is 0, then it will capture images.

c. **Enable Text Log:** This configuration will check whether the text logs are to be captured or not for a service. If the value is 1, then it will capture the text logs. If the value is 0, then it will not capture the text logs.
d. **Enable SSM Log:** This configuration will check whether the smart session monitoring logs are to be captured or not for a service. If the value is 1, then it will capture the smart session monitoring logs. If the value is 0, then it will not capture the smart session monitoring logs.
e. **Use Service for Windows Process Elevation**: This configuration will check whether the service can be used for Windows Process Elevation. If the value is 1, use the service for Windows Process Elevation. If the value is 0, then it will not use the service for Windows Process Elevation.
f. **Use Service for Remote Assist Elevation:** This configuration will check whether the service can be used for Remote Assist Elevation. If the value is 1, use the service for Remote Assist Elevation. If the value is 0, then it will not use the service for Remote Assist Elevation.

3. Click Add. The added configuration shall be displayed under service configuration, modify the value as per requirement

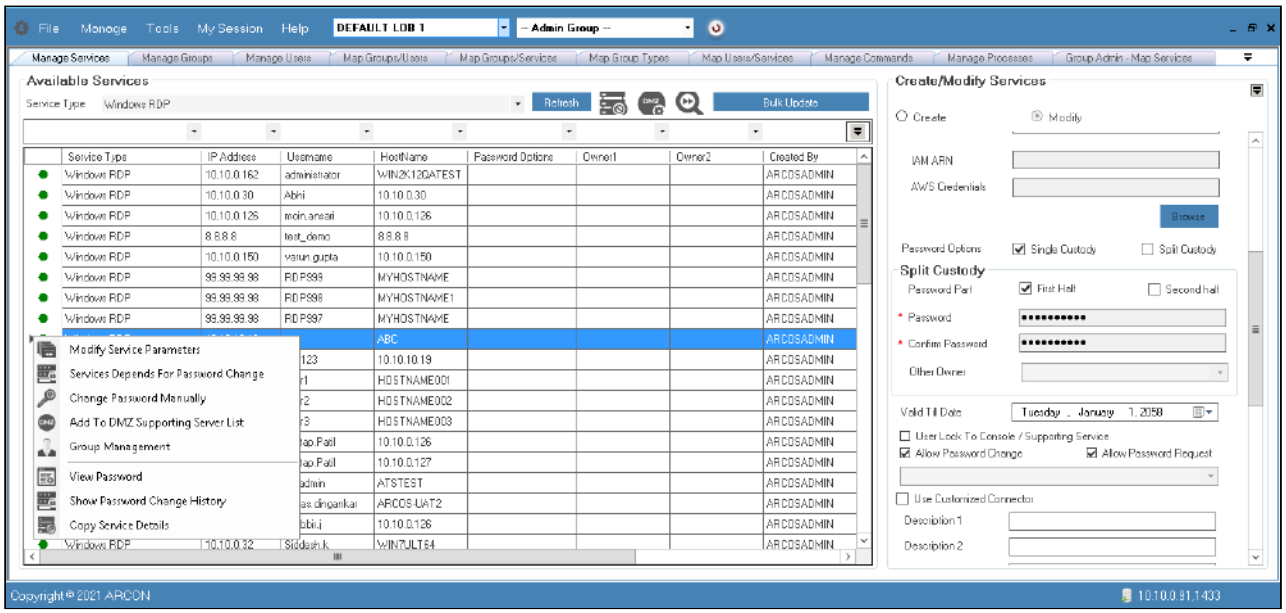


4. Click Modify, parameter updated screen shall be displayed

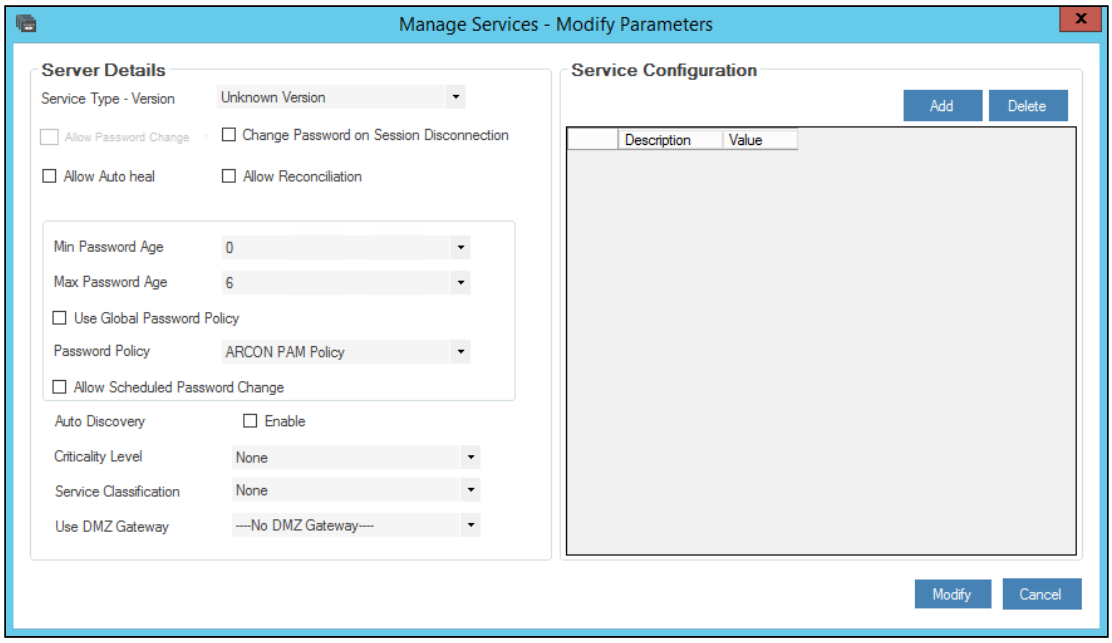


4.3.8.1 Windows Process Elevation

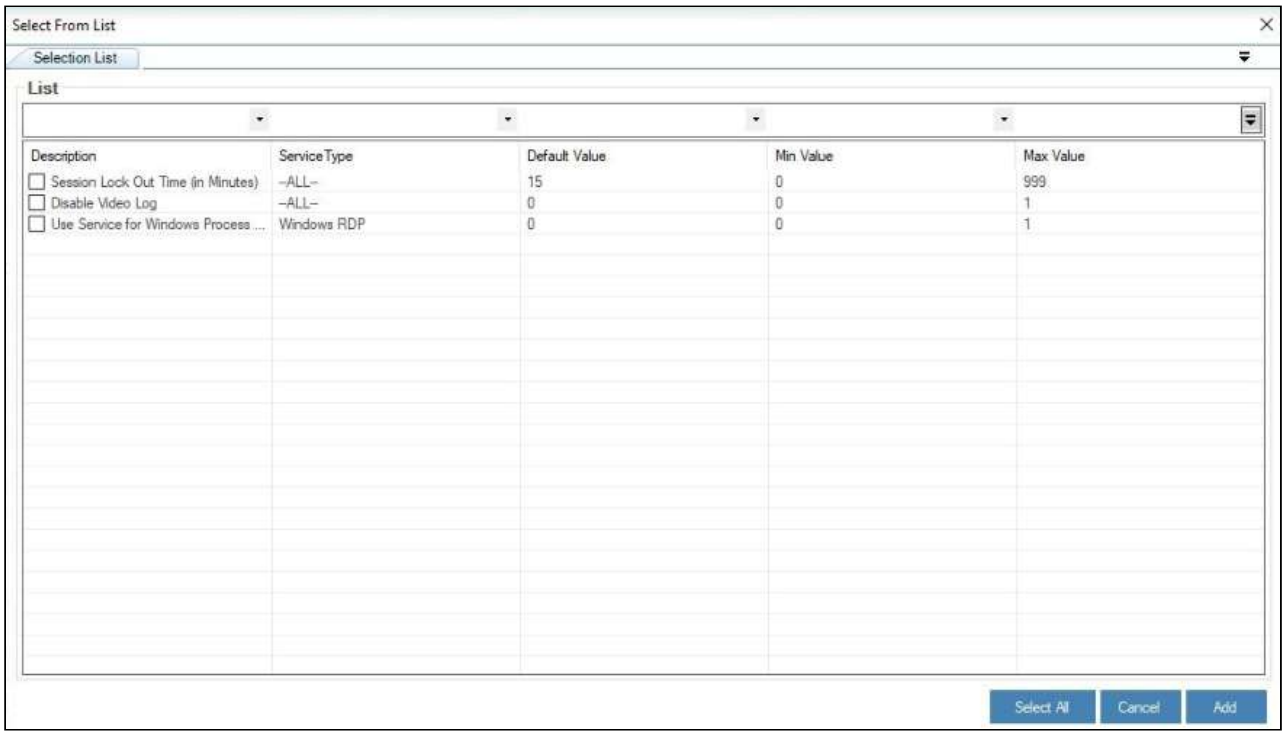
1. Right-click on the service for which you want to use for Windows Process Elevation and choose **Modify Service Parameters** option.



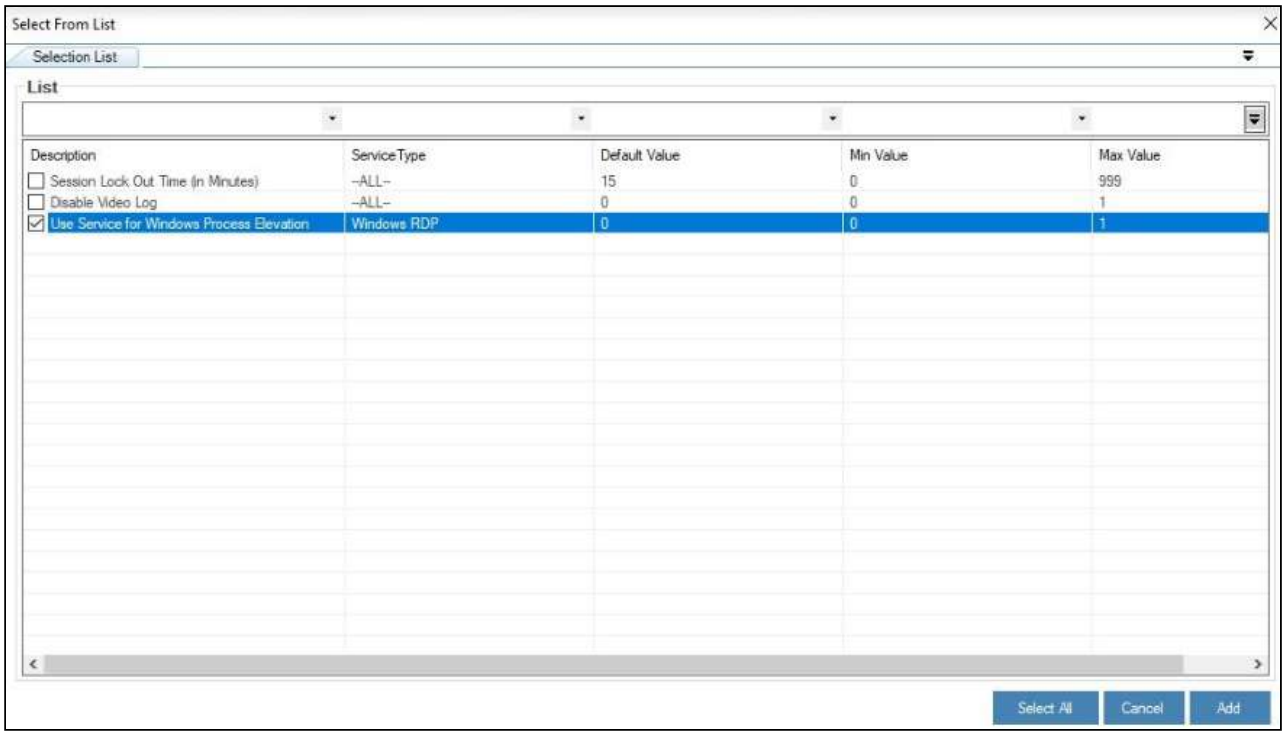
2. The **Manage Services - Modify Parameters** screen is displayed.



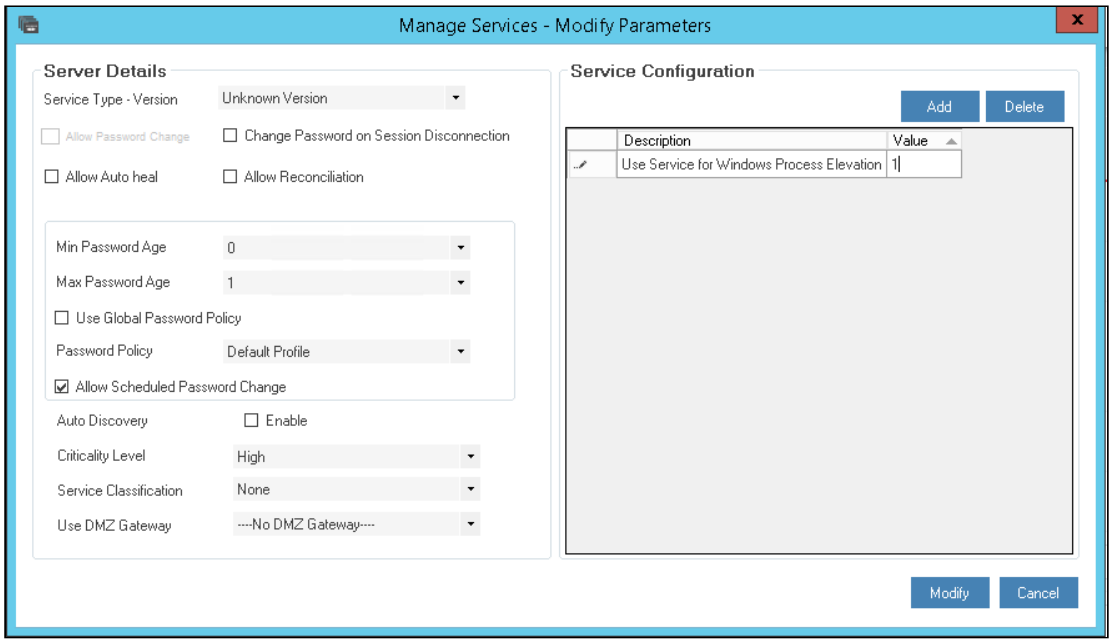
3. Now add the Process Elevation Service Configuration details, Click Add on the top right side, a new window shall be displayed.



4. Select Use Service for Windows Process Elevation and click Add

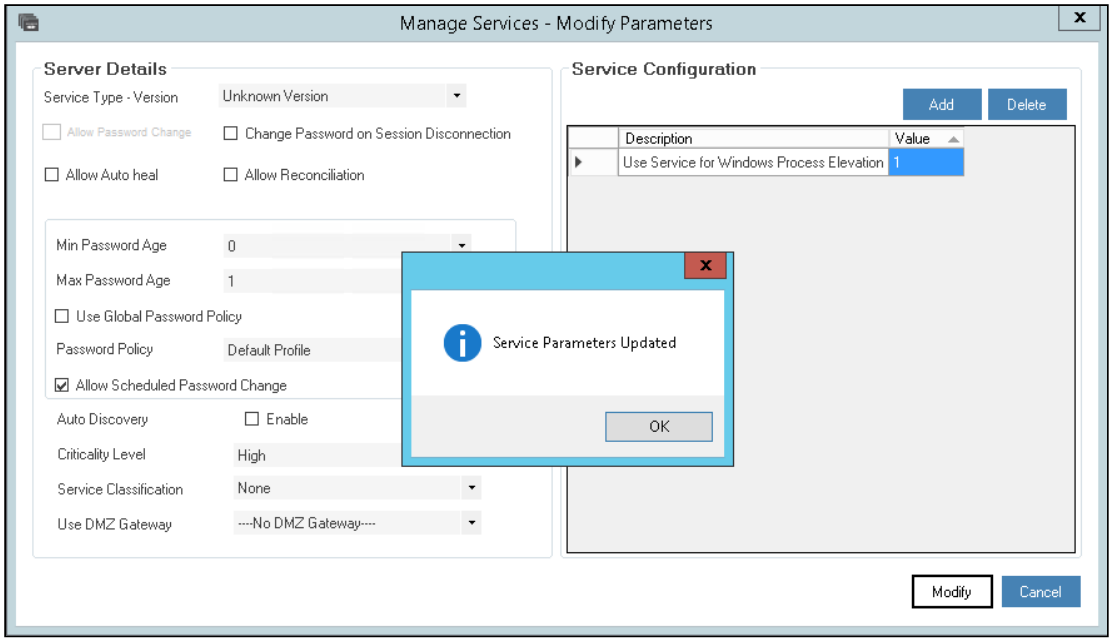


5. The added configuration shall be displayed under service configuration as follows:



6. By default, the value shall be 0, to enable Process Elevation modify the value to 1 and click Modify.

7. Parameter updated screen shall be displayed on successful modifying the parameters.



4.4 Groups

A Group is a collection of users or servers. The Users created are grouped such as Admin Users, Network Users, etc. Similarly, Server Group created are grouped according to the service provided on the server. For example, users accessing windows are grouped as Windows Admin, and Linux as Linux Admin. Similarly, services are grouped as Windows Services, Linux Services, etc.

For effective inventory management, services and users have been mapped. Therefore, to reduce the complication, we segregate them into two broad categories:

- User Group (based on users)
- Server Group (based on services)

⚠ The Administrators having **Read Only Access** privilege (under **Manage Group**) can view details displayed under Manage Groups, Manage Groups/Services and Manage Groups/Users.

This section includes the following topics:

- Create a User and Server Group
- Modify Details of a User/ Server Group
- Manage Group Utility

4.4.1 Create User and Server Group

A group is a collection of users or servers. For a user to access a service, user has to be part of at least one User Group and the user group has to be part of at least one Server Group. This section helps you to create groups such as User or Server Group. In addition, you can modify details of User or Server Group.

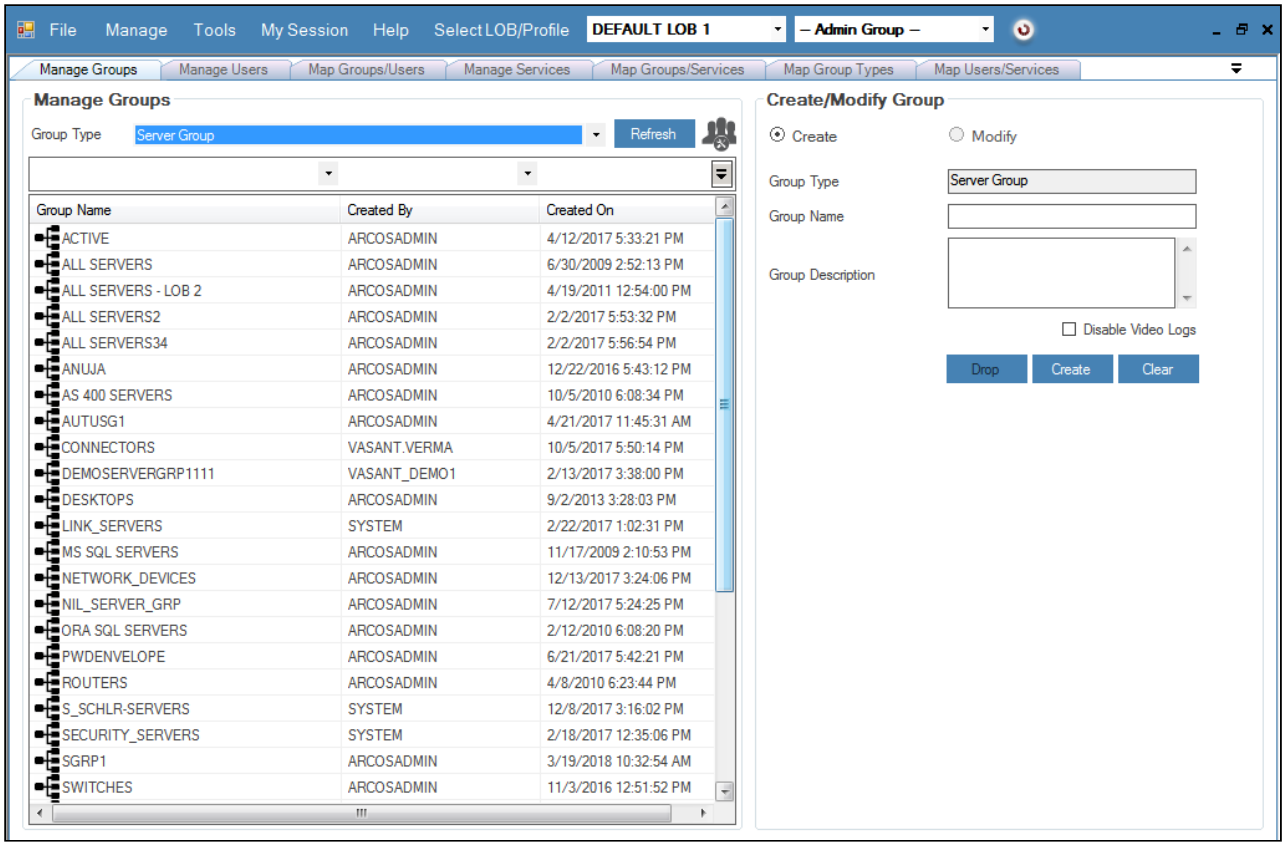
⚠ The Administrator having **Add Group** privilege shall only be able to create a User or Server Group.

To create groups:

To create groups use the following path:

Manage → Users and Services → Manage Groups

1. Click the **Manage Groups** sub menu. The **Create/Modify Group** screen is displayed.



> ⚠ To search a specific set of rows, enter keywords (space separated) on the column's header, and the relevant rows are pulled out.

The **Create/ Modify** screen contains the following fields:

Field Name	Description
Create (radio button)	Select to create a group.
Modify (radio button)	Select to modify details of an existing group. ⚠ To modify details of Group, select the required User or Server Group from the grid on the left pane. The Group details are displayed under Create/Modify Group pane on the right side. Modify the required details and click **Modify** button, to update the Group details.

Field Name	Description
Group Type	Displays the type of group. The valid values are: ▪ User Group ▪ Server Group ⚠ The data in this field is auto populated, once you select the **Group Type** under **Manage Groups** section.
Group Name	Specify the group name for users or services.
Group Description	Specify the description for the group.
Drop button	Click **Drop**, to delete group from ARCON PAM. ⚠ ▪ The Administrator having **Drop Group** privilege shall only be able to delete a User or Server Group. ▪ To drop a Group, select the required User or Server Group from the grid on the left pane. The Group details are displayed under Create/Modify Group pane on the right side. View the details and click **Drop**, to delete the Group from ARCON PAM.
Disable Video Logs	Select this Checkbox to Disable Video Logs for any particular Server Group. ⚠ This field is displayed, if **Disable Video Logs by Server Group** toggle value in **Settings** is **Enabled**.

2. Enter the fields and click **Create**. A window pops up with the following message:
   New Group Created
3. Click **OK**. A new user or service group is created.

⚠
- The new group created is displayed under **Manage Groups** grid, once you have mapped it under a particular LOB.
- Similarly, follow the above steps to create a Server Group by selecting **Group Type** as **Server Group**.

4.4.2 Modify details of User or Server Group

You can modify the details of a particular user or server group using the **Create/ Modify Group** screen.

⚠ The Administrator having **Modify Group** privilege shall only be able to modify User or Server Group details.

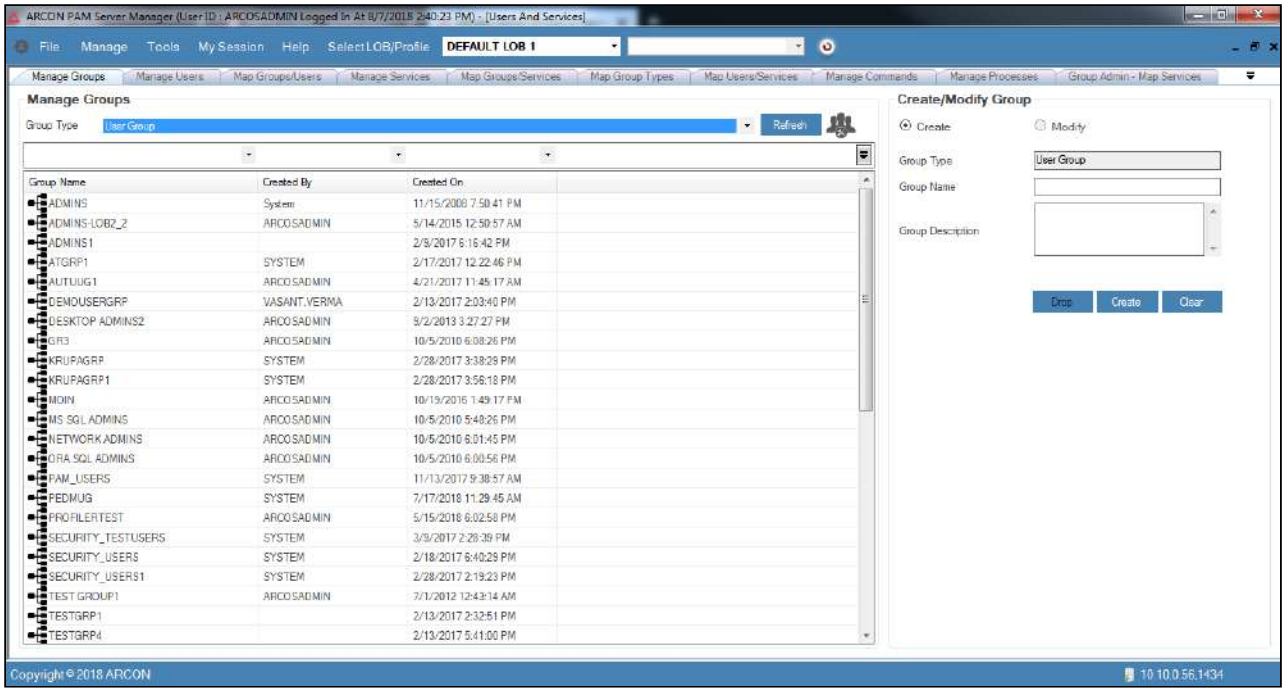
To modify details of a user group/ server group:

To modify details of a user/server group use the following path:

Manage → Users and Services → Manage Groups

1. Click the **Manage Groups** sub menu. The **Manage Groups** screen is displayed.

2. Select the LOB and type of group from the **Select LOB/Profile** and **Group Type** dropdown list respectively. A list of user or server groups are displayed in the grid.



3. Select a group name from the list of groups under **Manage Groups** grid. The details are populated in the **Create/Modify Group** fields.
4. Modify the required changes in the existing fields and click **Modify**. A window pops up with the following message:
   Selected Group Updated.
5. Click **OK**. The details of the group are modified.

4.4.3 Transfer Service Connections between Server Groups

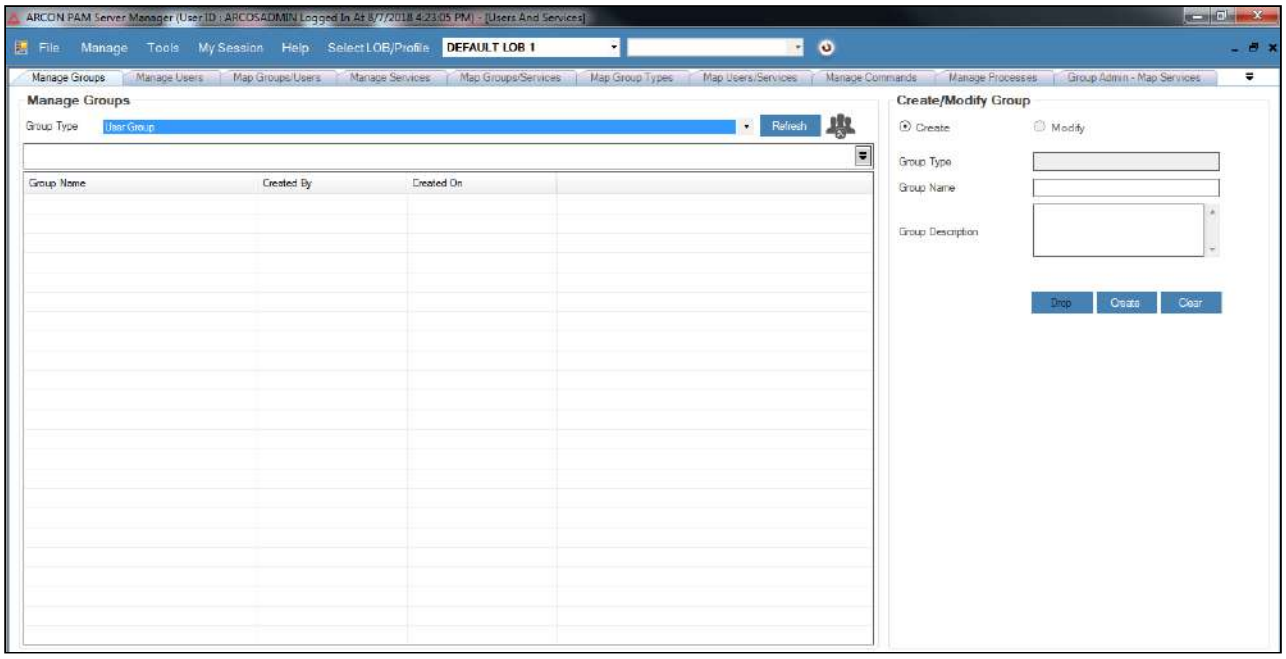
Manage Group Utility is used to transfer server connections from one Server Group to another Server Group. Suppose there are two server groups for example, Server Group 1 and Server Group 2. The Server Group 1 is mapped to User Group 1. However, through Manage Group Utility the connections from Server Group 1 is completely removed and transferred to Server Group 2. Then the User Group 1 will have all the connections of Server Group 2.

To transfer server connections:

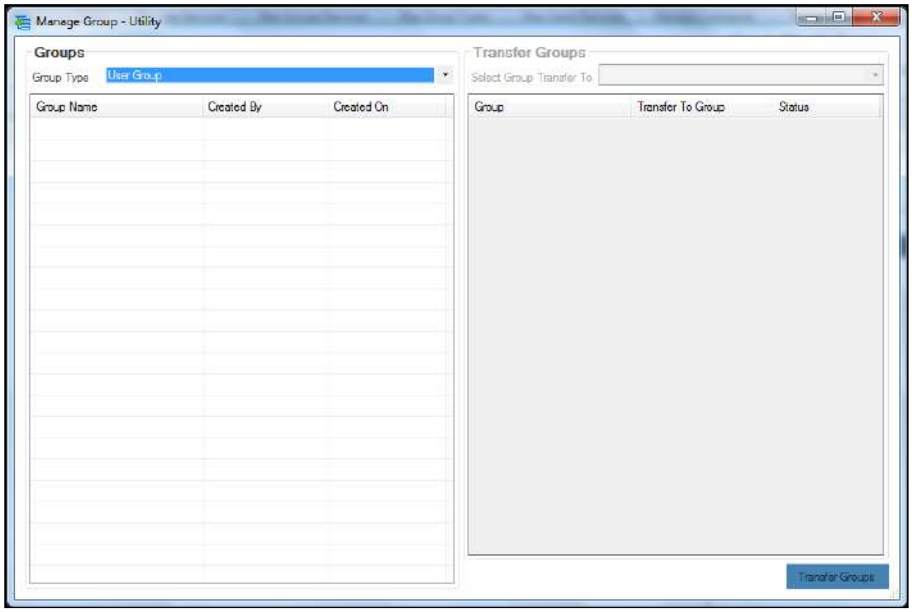
To transfer server connections use the following path:

Manage → Users and Services → Manage Groups

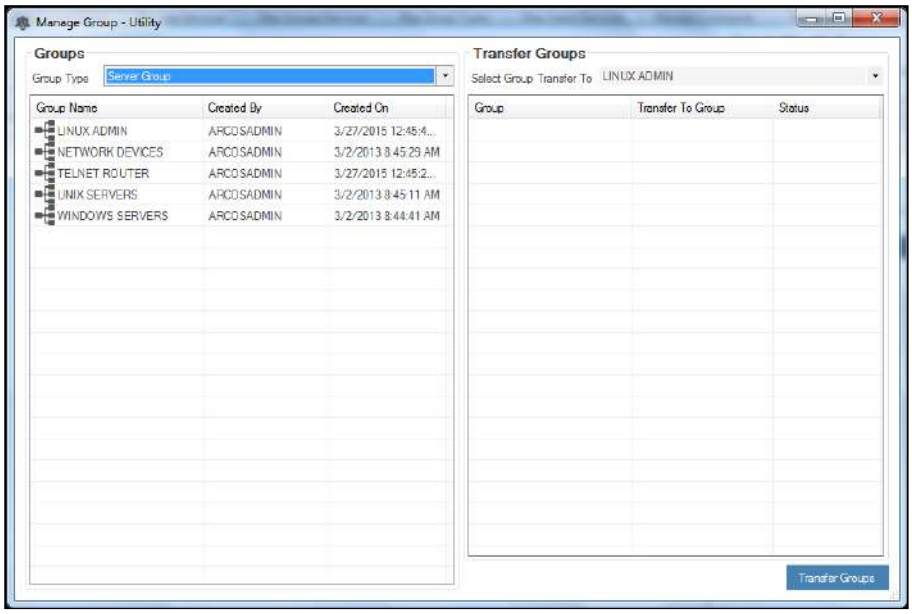
1. Click the **Manage Groups** sub menu. The **Create/Modify Group** screen is displayed.



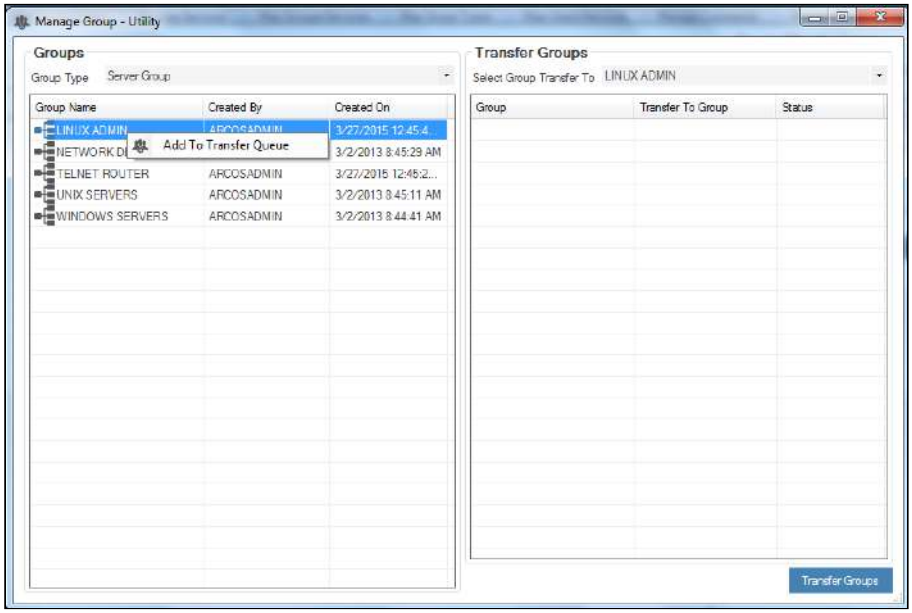
2. Select LOB from the **Select LOB/Profile** dropdown list and then click on the **Manage Group Utility**  icon. The **Manage Group – Utility** screen is displayed.



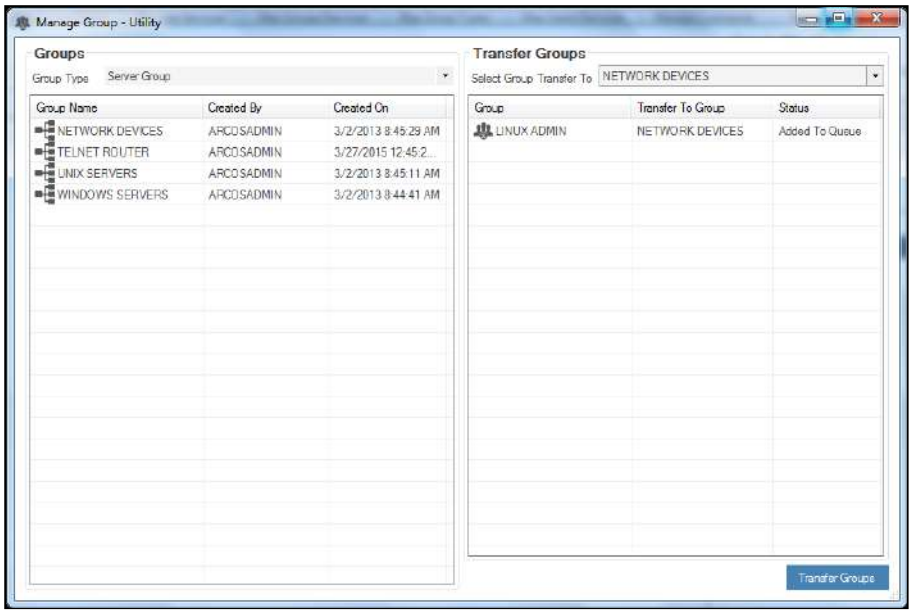
3. Select **Server Group** option from **Group Type** dropdown list. A list of services are displayed in the grid.



4. In **Transfer Groups** panel, select the server from the **Select Group Transfer To** dropdown list to which the connection is to be transferred.
5. Select the server group from the list on the left pane and right click on the selected server group.



6. Click **Add To Transfer Queue**. The selected server group is added to the Group list in **Transfer Groups** grid.



> ⚠ You cannot transfer the connections to the same server group. For example, if you select Network Admin as the server group, then you cannot transfer the connections to same Network Admin group.

7. Click **Transfer Groups** button to transfer the connections from one server group to another. A window pops up with the following message:
   Group Transfer Process Completed
8. Click **OK**. The connection is transferred to the server group.

4.5 Mapping

Mapping is the process, wherein the created entities such as LOB's, Users, Services, User Groups, and Server Groups are mapped with each other inorder to establish connection to the server. It is performed for effective management of entities in ARCON PAM.

This section includes the following topics:

- Map User to LOB
- Map Services to LOB
- Map User Groups to LOB
- Map Service Group to LOB
- Map Users to User Group
- Map Services to Server Group
- Map Server Group to User Group
- Map Services to Users
- Map Services to Multiple Users
- Automatically Map User to Service and Vice - Versa

4.5.1 Map Users to LOB

This section helps you to map Users to a particular LOB. You can map Users to a particular LOB using the **Map LOB/ Users** screen.

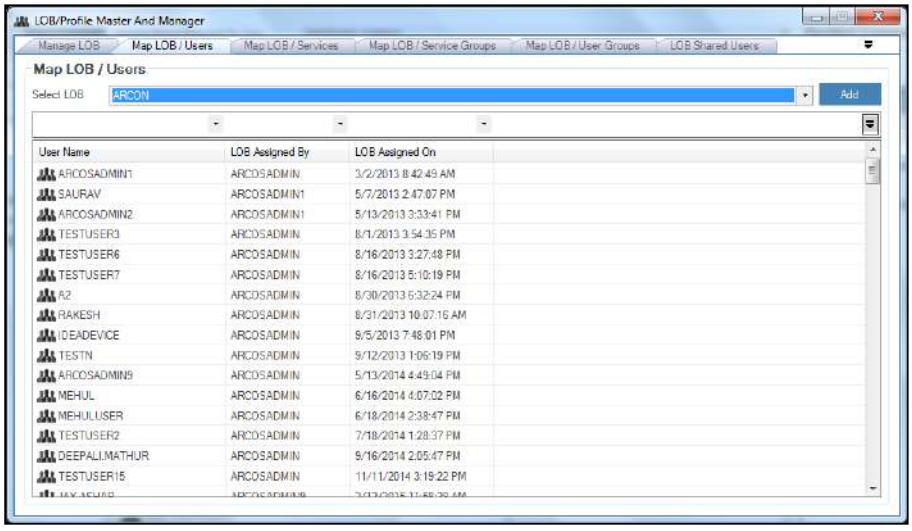
- The Administrator having **Assign LOB To User** privilege will only be able to map User to a particular LOB.
- If toggle value for **LOB - Share All Users** in **Settings** is **Enabled,** then the Users can be mapped to multiple LOB.

To map users to a particular LOB:

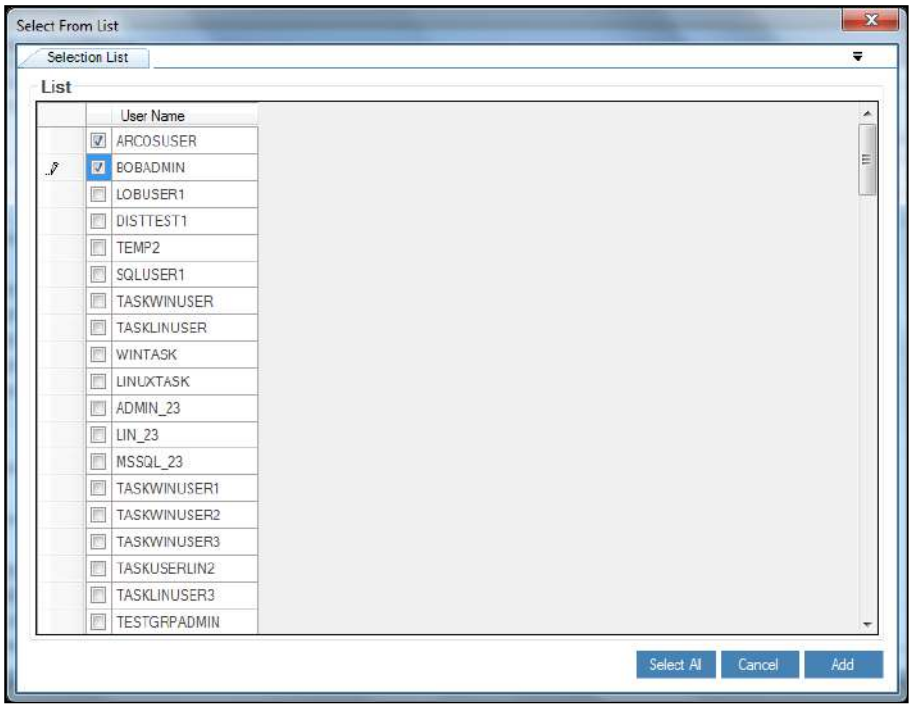
To map users to a particular LOB use the following path:

Manage → LOB/Profile Master and Manager → Map LOB/Users

1. Select the **LOB** from **Select LOB** field and click **Add** button.



2. The **Selection List** screen is displayed, then select the checkbox from the list and click **Add** button.



3. A window pops up with the following message:
   New User(s) Added To LOB
4. Click **OK**. The users are mapped to the particular LOB.

4.5.1.1 User LOB/Profile Management

You can map a User to multiple LOBs using **User LOB/Profile Management** option under **Manage Users** tab.

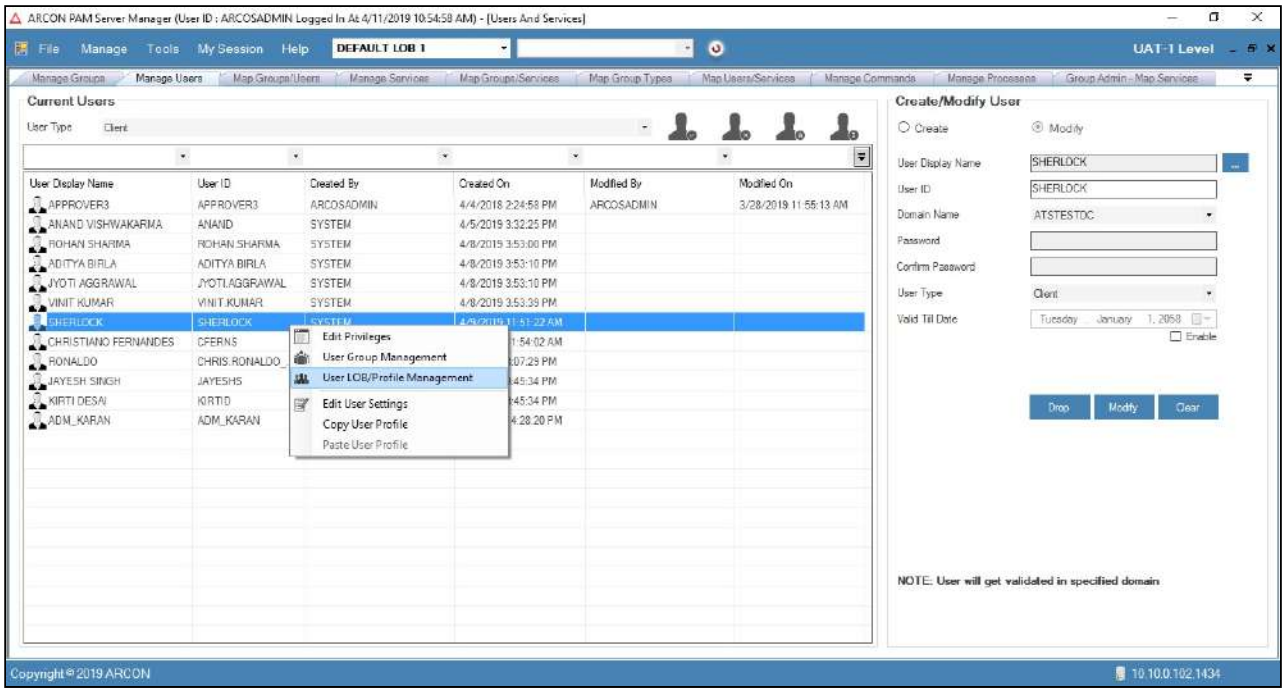
> ⚠ The toggle value for **LOB - Share All Users** in **Settings** should be **Enabled,** to map User to multiple LOBs using **User LOB/Profile Management** option.

To map User to LOB:

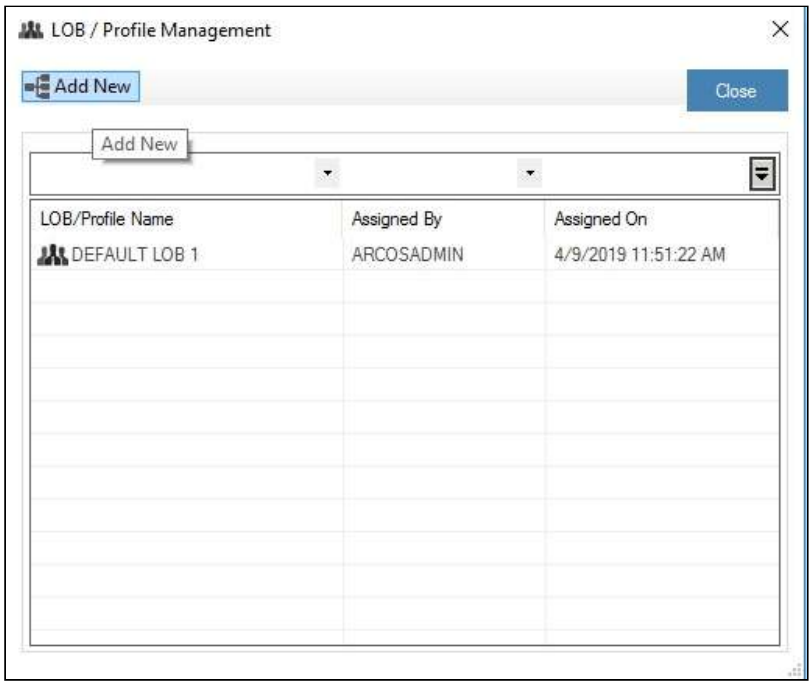
To map User to LOB use the following path:

Manage → Users and Services → Manage Users

1. Right-click on the User name from the **User Display Name** list. A multiple options list is popped up.

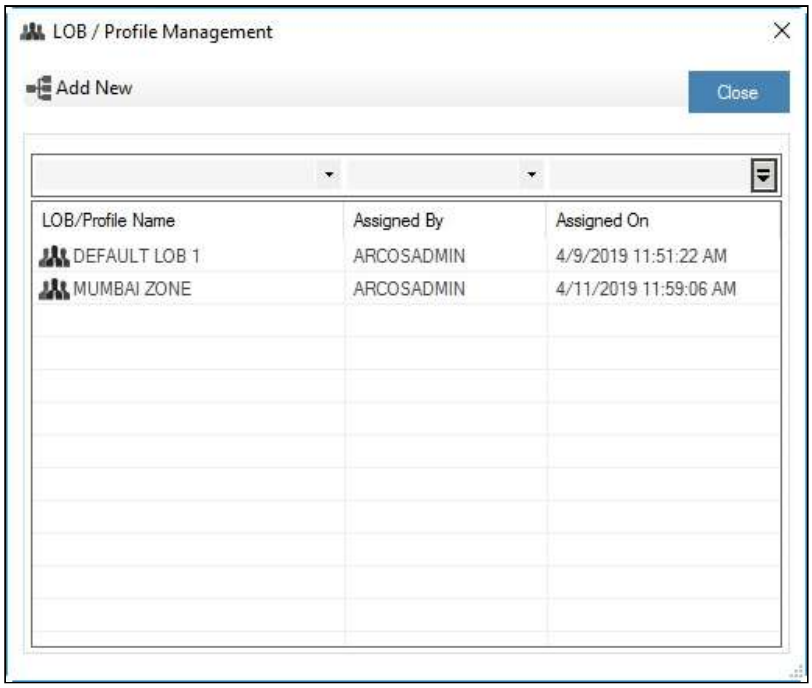


2. Click **User LOB/Profile Management** option. The **LOB / Profile Management** screen is displayed.



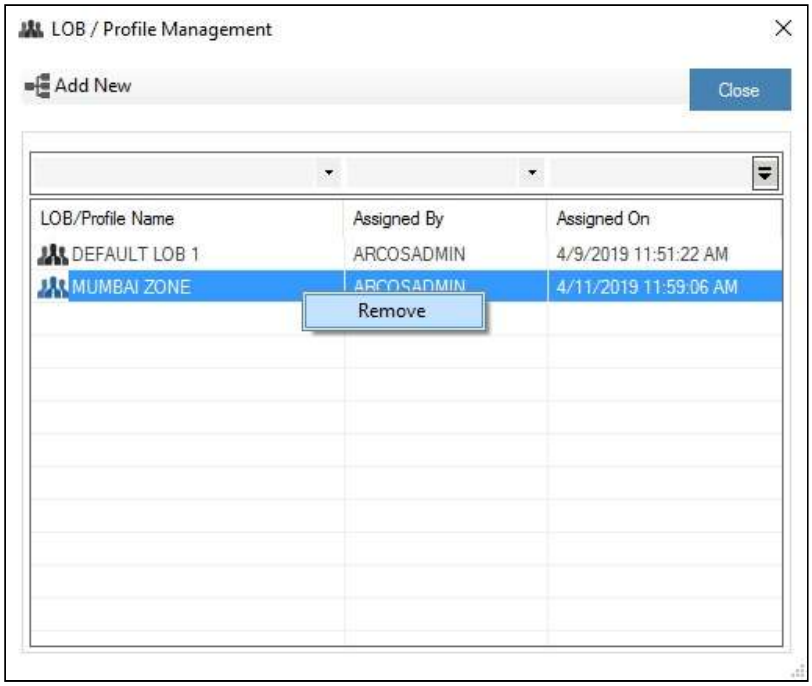
3. Click **Add New**. The **Selection List** screen is displayed, then select the LOB and double-click on the  icon.

4. The selected LOB is displayed in **LOB / Profile Management** screen.



⚠ To search a specific set of rows, enter keywords (space separated) on the column's header, and the relevant rows are pulled out

5. To remove User to LOB mapping, select the LOB, right-click and select **Remove**.



6. The selected LOB will be removed from **LOB / Profile Management** screen.

4.5.2 Map Services to LOB

This section helps you to map Services to a particular LOB. You can map Services to a particular LOB using the **Map LOB/Services** screen.

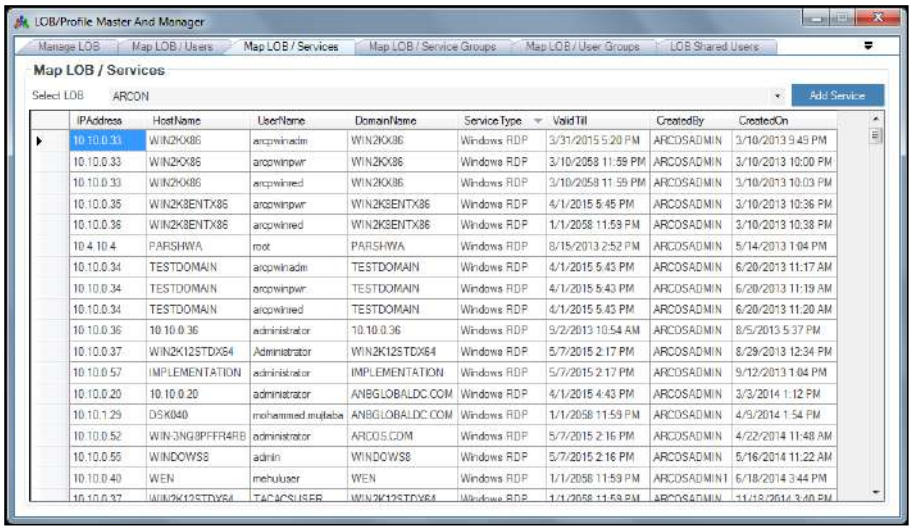
⚠ The Administrator having **Assign LOB To Service** privilege will only be able to map Services to LOB.

To Map a service to a particular LOB:

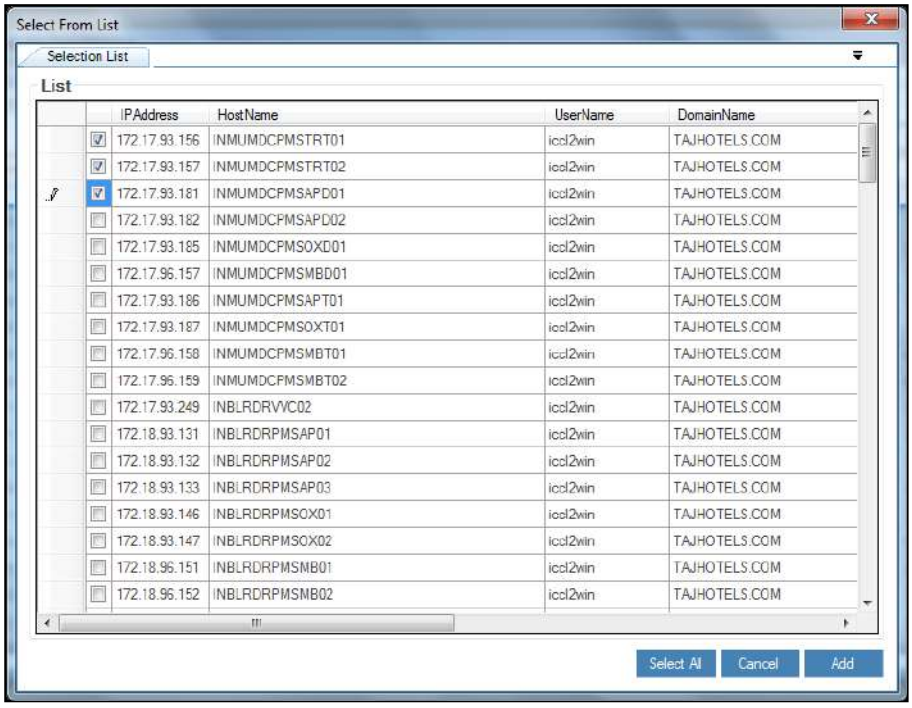
To map a service to a particular LOB use the following path:

Manage → LOB/Profile Master and Manager → Map LOB/Services

1. Select the LOB from the **Select LOB** dropdown list and click on the **Add Service** button.



2. The **Selection List** screen is displayed and then select the checkbox and click on **Add** button.



3. A window pops up with the following message:
   New Service(s) Added To LOB
4. Click **OK**. The new service is added to LOB.

4.5.3 Map User Group to LOB

This section helps you to map User Group to LOB. You can map User Group to a particular LOB using the **Map LOB/ User Groups** screen.

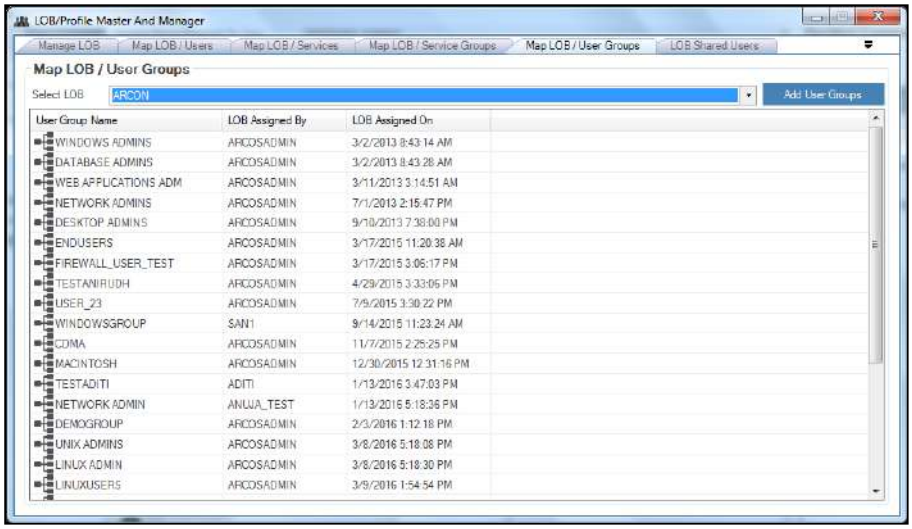
⚠ The Administrator having **Assign LOB To User Group** privilege will only be able to map User Group to a particular LOB.

To map user groups to a particular LOB:

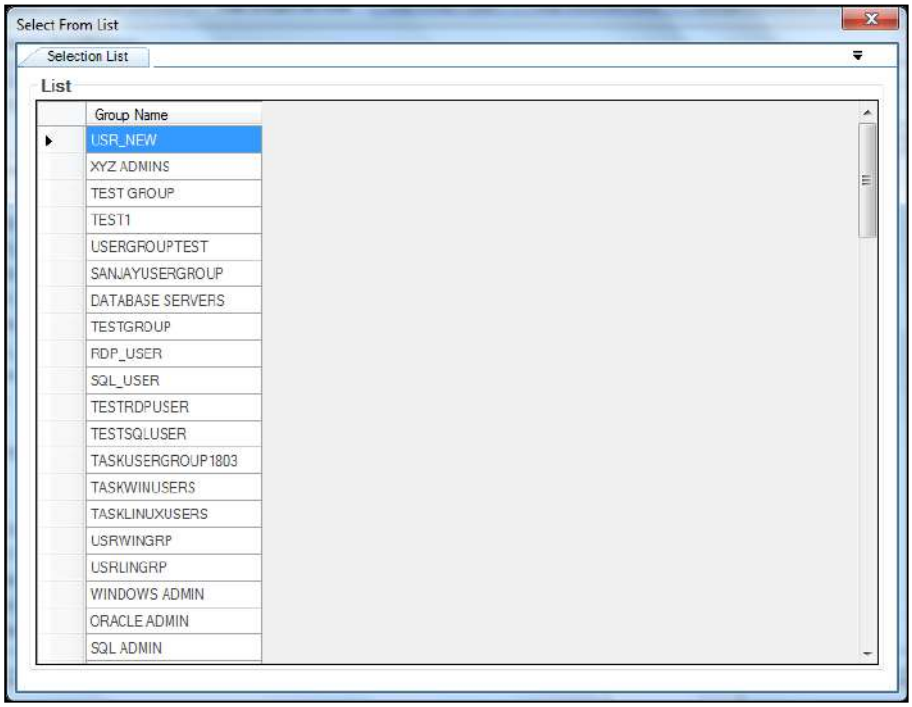
To map user groups to a particular LOB use the following path:

Manage → LOB/Profile Master and Manager → Map LOB/User Groups

1. Select the LOB from the **Select LOB** dropdown list and click on **Add User Groups** button.



2. The **Selection List** screen is displayed, then select the group name and double-click on the  icon.



3. A window pops up with the following message:
   New User Group Added To LOB
4. Click **OK**. The selected user group is mapped to a particular LOB.

4.5.4 Map Service Group to LOB

This section helps you to map Service Group to a particular LOB. You can map Service Group to a particular LOB using the **Map LOB/Service Groups** screen.

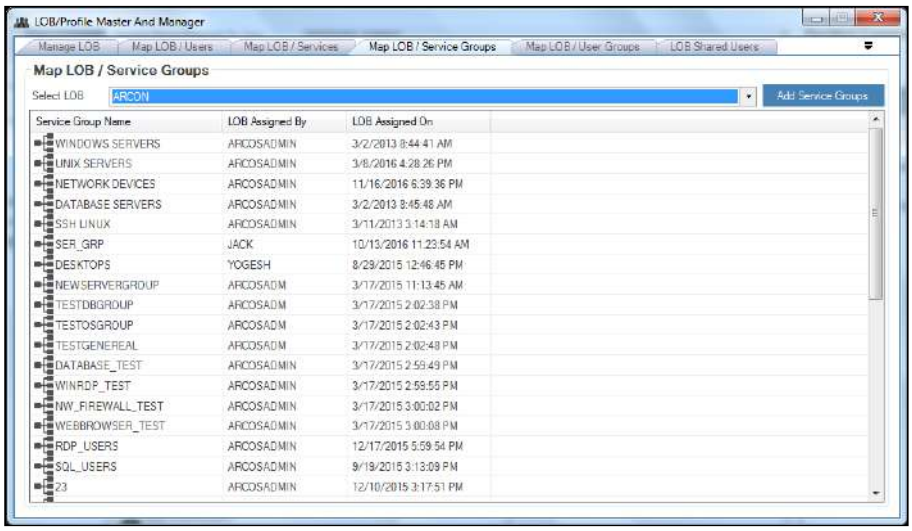
> ⚠ The Administrator having **Assign LOB To Service Group** privilege will only be able to map Service Group to a particular LOB.

To map Service Group to a particular LOB:

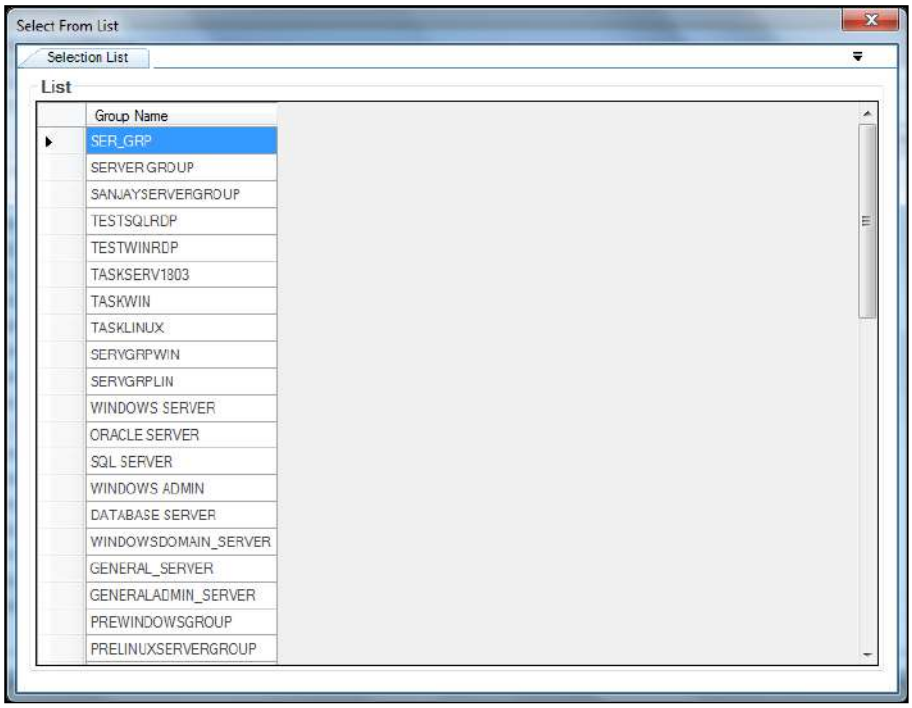
To map a service group to a particular LOB use the following path:

Manage → LOB/Profile Master and Manager → Map LOB/Service Groups

1. Select the LOB from the **Select LOB** drop down list and click the **Add Service Groups** button.



2. The **Select From List** screen is displayed, then select the service group and double click  icon.



3. A window pops up with the following message:
   New Service Group Added To LOB
4. Click **OK**. The Service Group is mapped to LOB.

4.5.5 Map Users to User Group

This section helps you to map Users to a particular User Group. Users can access the services belonging to a particular User Group, only when the services are mapped to the Users of that User Group.

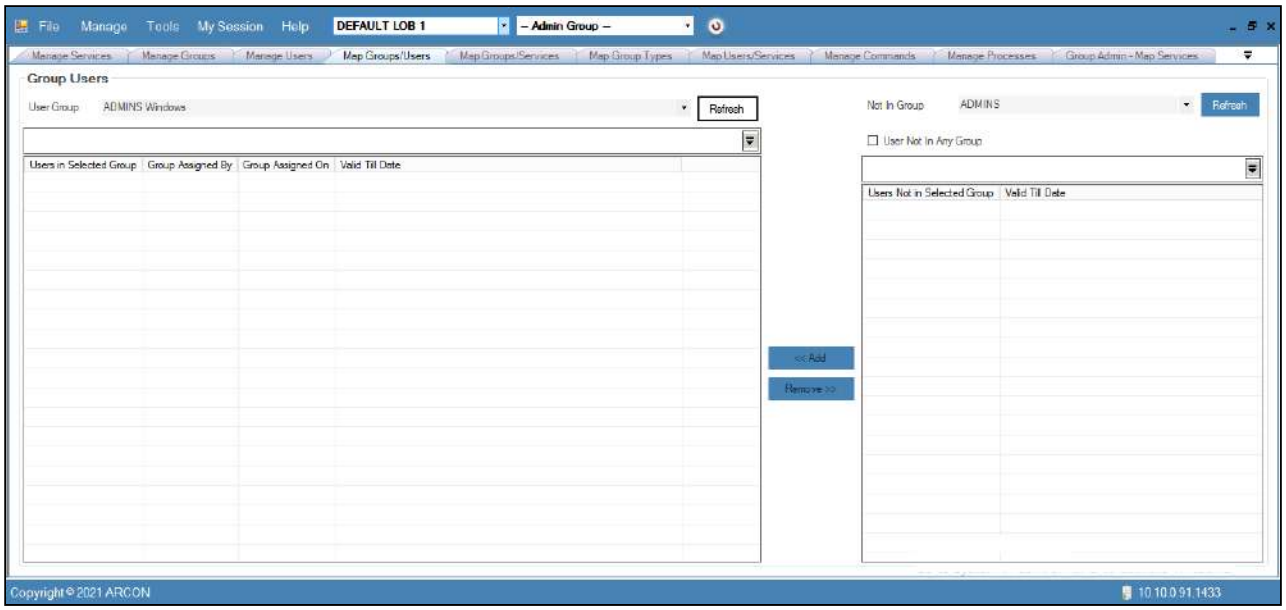
> ⚠ The Administrator having **Assign User Group** privilege will only be able to map Users to a particular User Group.

To map Users to User Group:

To map Users to a particular User Group use the following path:

Manage → Users and Services → Map Groups/Users

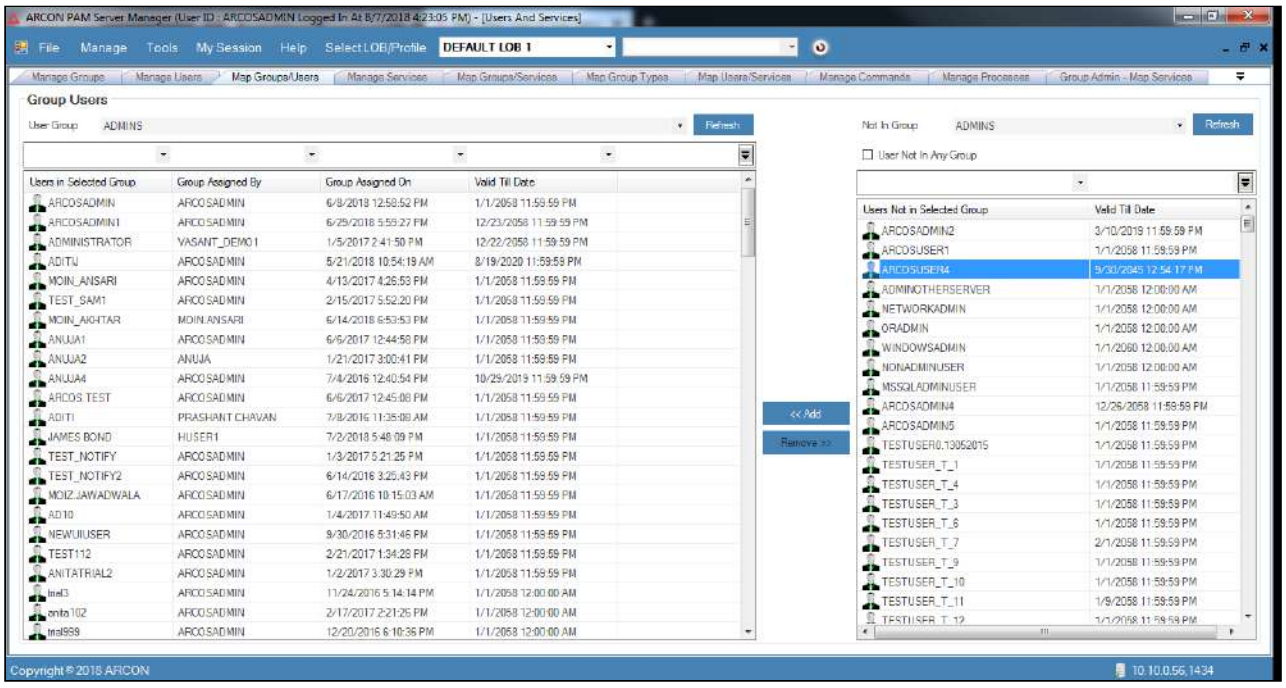
1. Click **Map Groups/Users** sub menu. The **Group Users** screen is displayed.



2. Select LOB and the user group from the **Select LOB/Profile** and **User Group** dropdown list respectively.

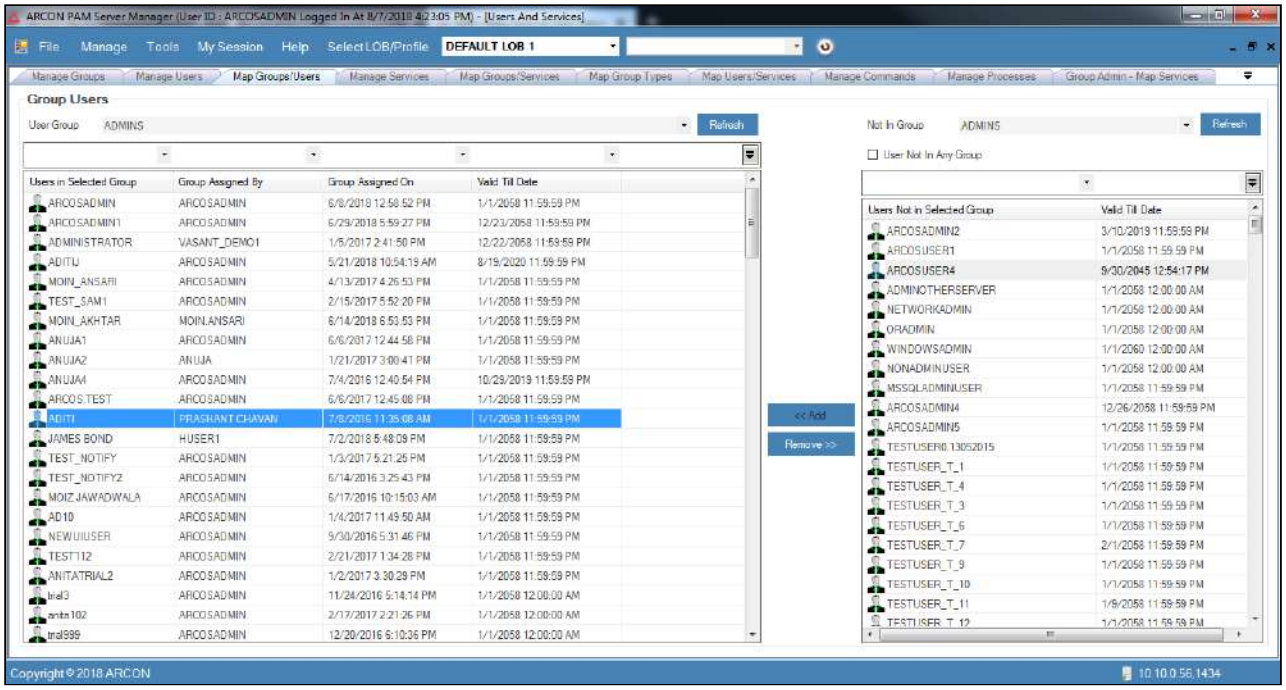
> ⚠ To search a specific set of rows, enter keywords(space separated) in the search text field of user group dropdown and the relevant rows are fetched.

3. Select the group name from the **Not In Group** dropdown list, wherein it displays all those users, which are not present in the selected user group.



- Select the **User Not In Any Group** checkbox, to display the list of all the users which are mapped to a particular LOB but are not present in any user group.
- To search a specific set of rows, enter keywords (space separated) on the column's header, and the relevant rows are pulled out.

4. Select the user from the **Users Not in Selected Group** grid list and click on **<< Add** button. The selected user is added on the left hand side, in **User in Selected Group** list.



5. Similarly, you can remove users from the particular user group by selecting the user from the list of **Users in Selected Group** and then click on the **Remove >>** button.

The Administrator having **Revoke User Group** privilege will only be able to remove Users mapped to User Group.

4.5.5.1 User Group Management

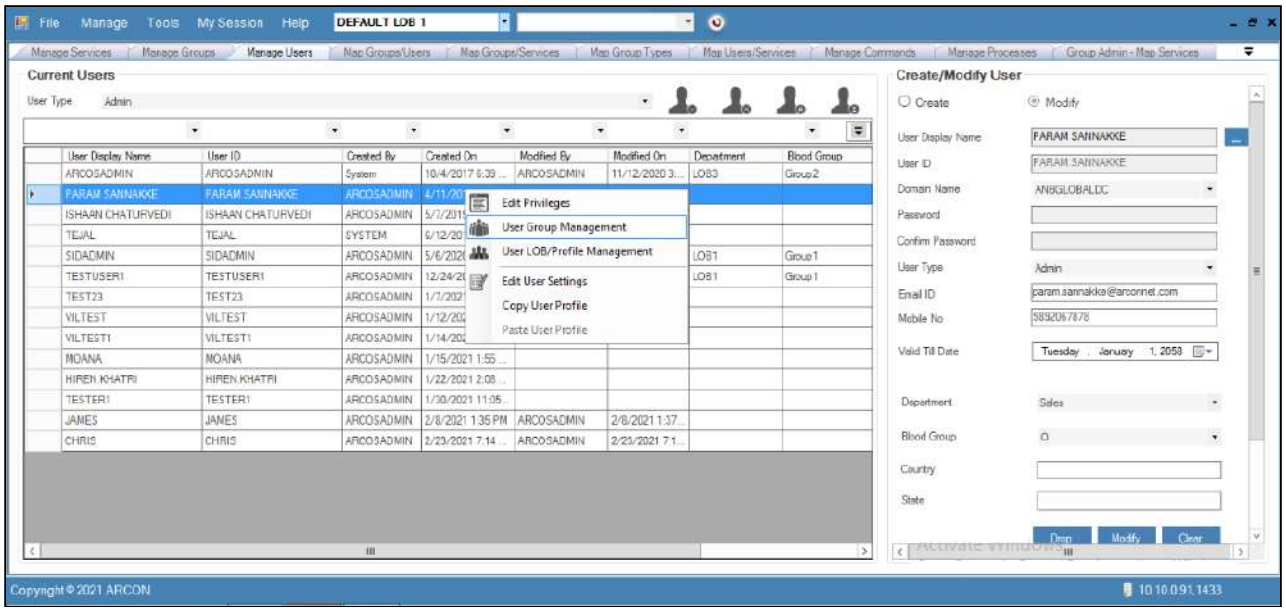
You can map a User to multiple User Groups using **User Group Management** option under **Manage Users** tab.

To map User to User Group:

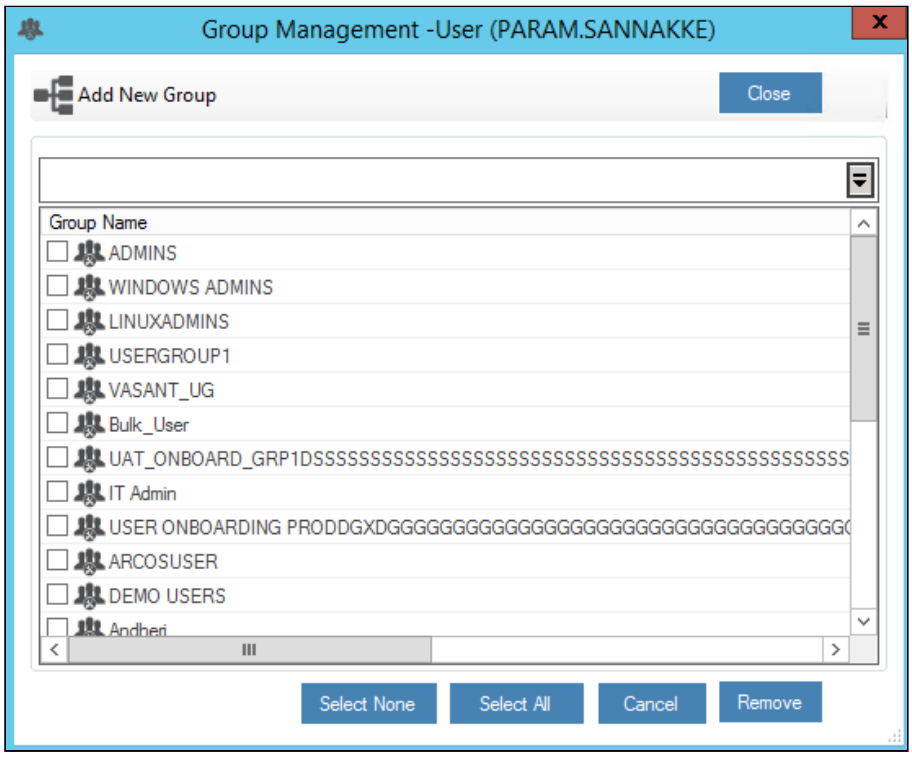
To map User to User Group use the following path:

Manage → Users and Services → Manage Users

1. Right-click on the User name from the **User Display Name** list. A multiple options list is popped up. Click **User Group Management** option.



2. The **Group Management** screen is displayed. It displays the list of User groups already mapped to the User.

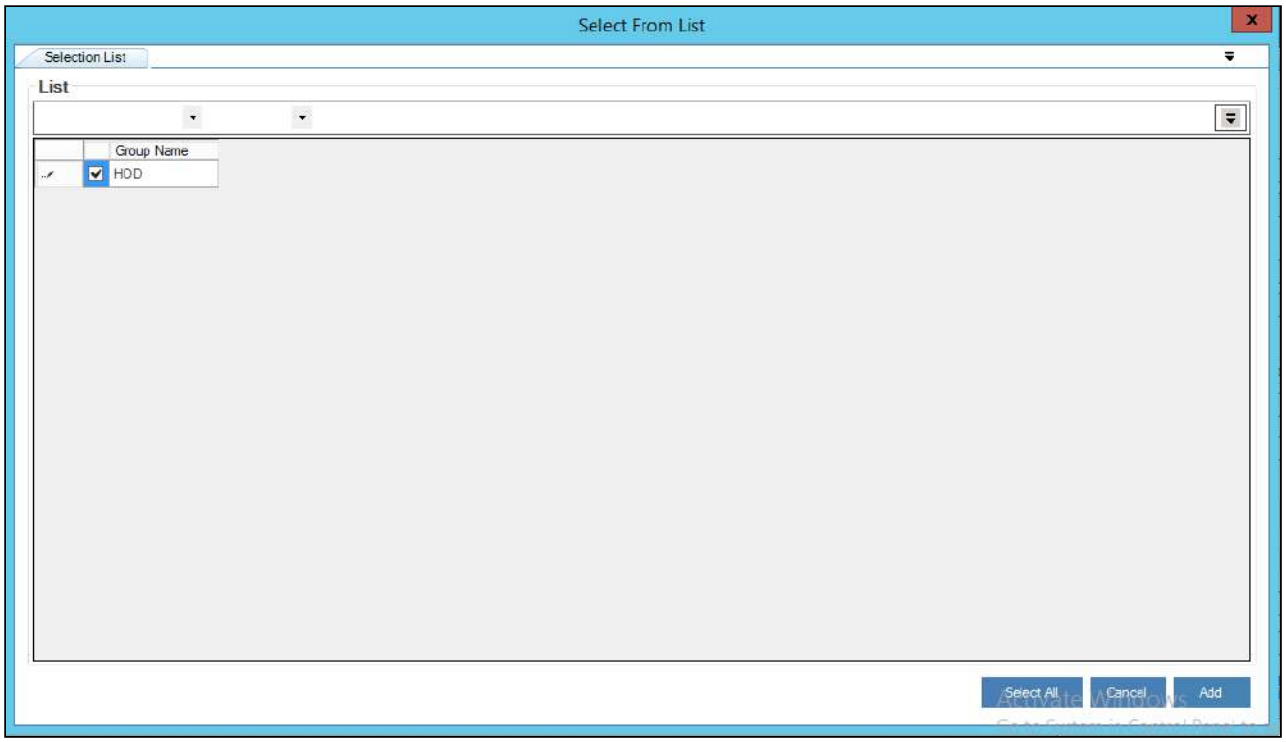


> ⚠ To search a specific set of rows, enter keywords (space separated) on the column's header, and the relevant rows are pulled out

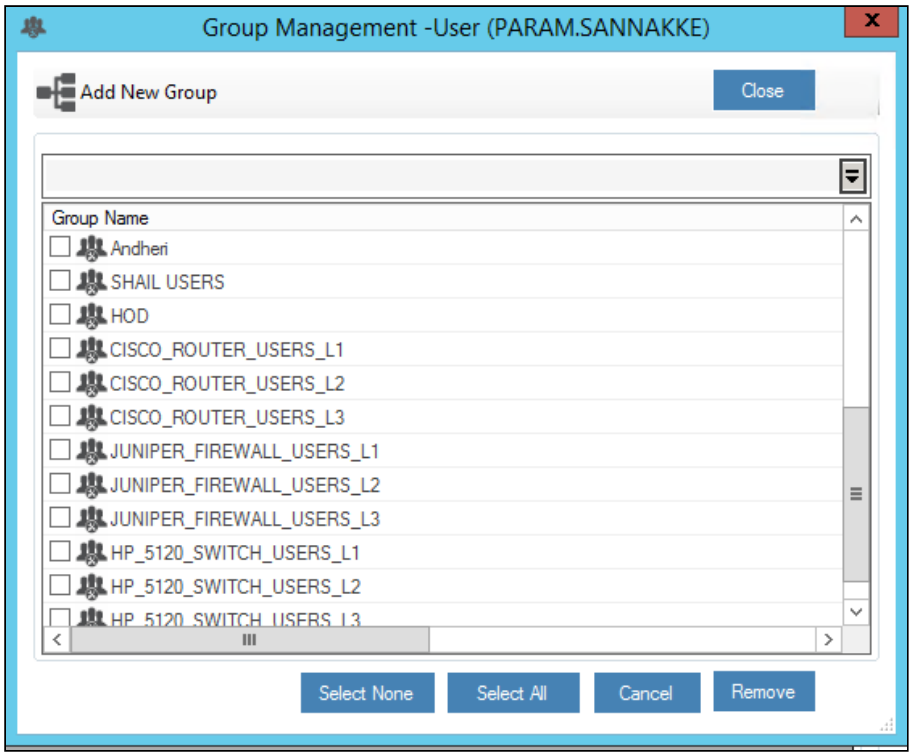
3. Click **Add New Group to map a new User Group to the User**. A pop up comes up- Do you want to perform this operation? Select Yes.

4. The **Selection List** screen is displayed, select the Server Groups checkbox to which the Service should be mapped and select **Add**.

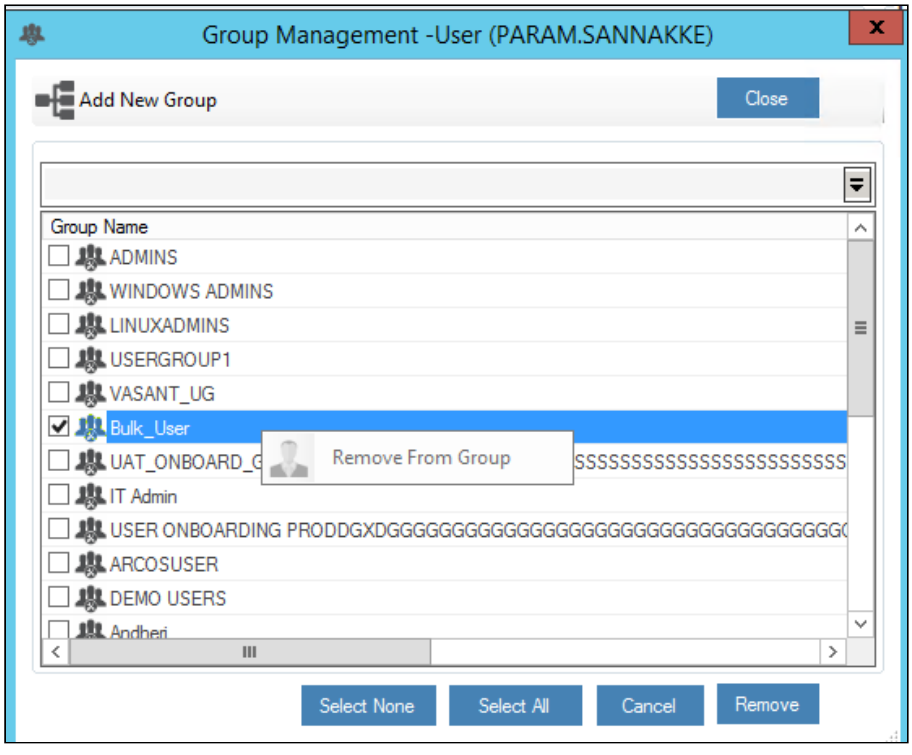
> ⚠ On clicking **Add** the User group is mapped to the User either directly or goes under approval to higher level admins depending on the workflow.



5. The selected User Group is displayed in **Group Management** screen.



6. To remove User Group from the User, select the User Group, right-click and select **Remove From Group** or select the checkbox beside the User Groups and select remove.



7. The selected User Group will be removed from **Group Management** screen.

> ⚠ On clicking **Remove**, the User group is revoked from the User either directly or goes under approval to higher level admins depending on the workflow.

4.5.6 Map Services to Server Group

This section helps you to map Services to a particular Server Group. You can map Services to a particular Server Group using the **Map Groups/Services** screen.

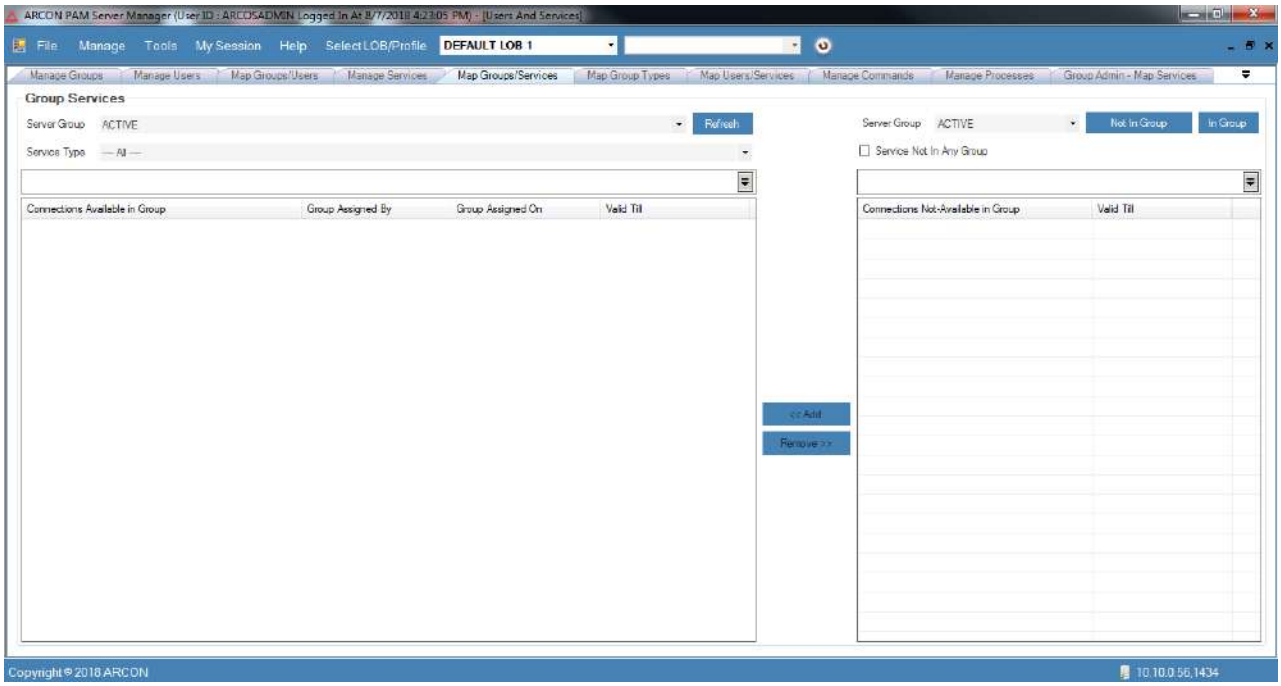
> ⚠ The Administrator having **Assign Service To Service Group** privilege will only be able to map services to a particular Service Group.

To map Services to Server Group:

To map services to a server group use the following path:

Manage → Users and Services → Map Groups/Services

1. Click **Map Groups/Services** sub menu. The **Groups Services** screen is displayed.

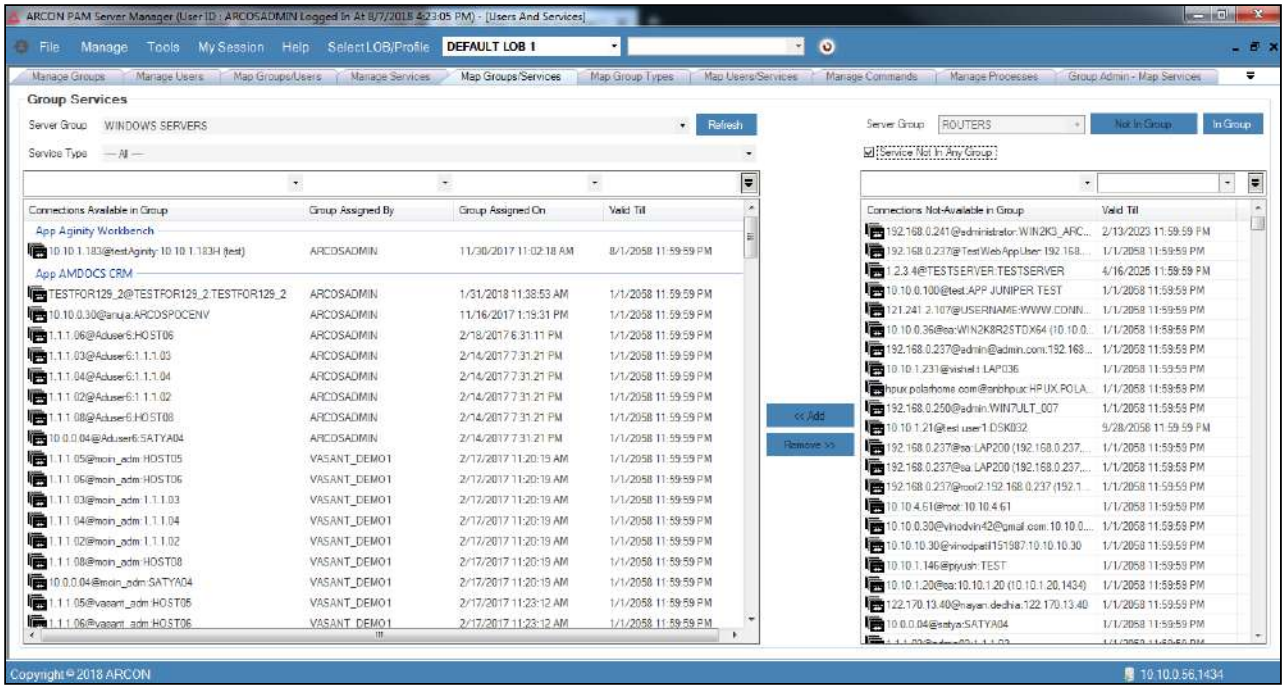


2. On the left pane, select/enter the server group from the **Server Group** dropdown list respectively and click on **Refresh** button, to view the services belonging to the selected server group.

> ⚠ To search a specific set of rows, enter keywords(space separated) in the search text field of service group dropdown and the relevant rows are fetched.

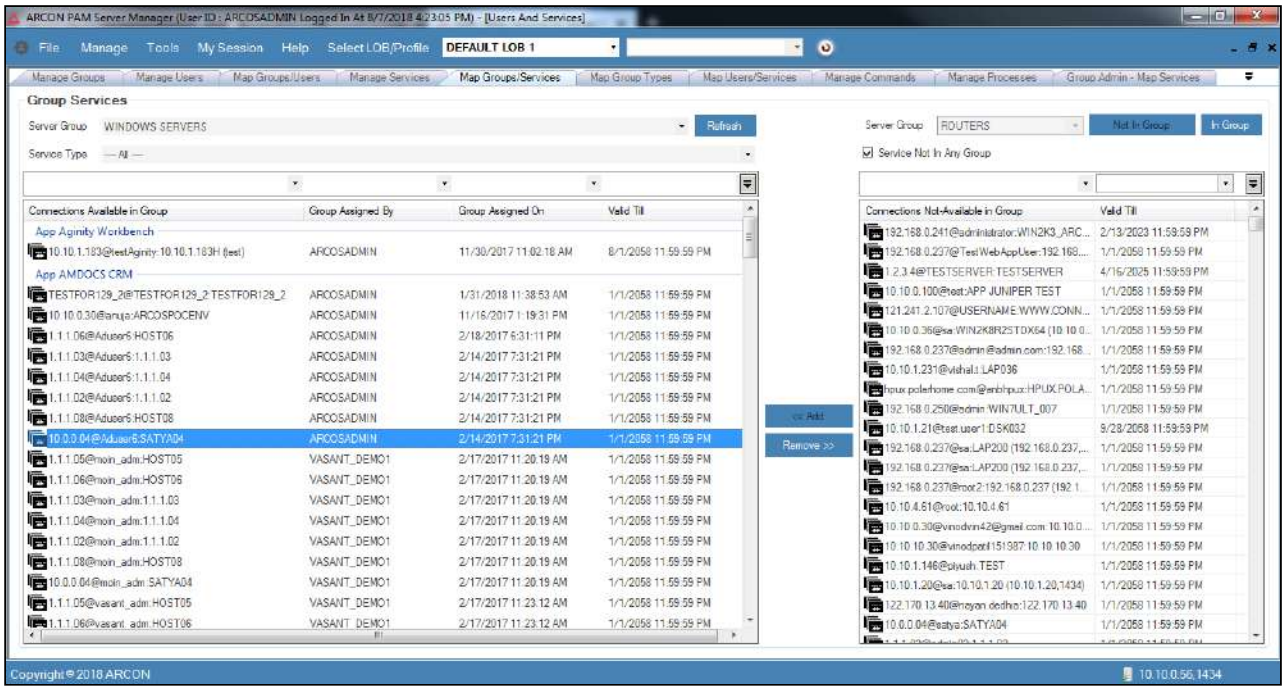
3. Select the Server Type from the server type dropdown list.

4. On the right pane, select the server group from the **Server Group** dropdown list and select the services which are to be added to the selected server group.



- Click **Not In Group** button, to view services which are not present in the selected server group.
- Click **In Group** button, to view services which are present in the selected server group.
- Select **Services Not in any Group** checkbox, to view services which are mapped to a particular LOB but not present in any server groups.
- To search a specific set of rows, enter keywords (space separated) on the column's header, and the relevant rows are pulled out.

5. Select the services from the **Connections Not Available in Group** list and click on **<< Add** button. The connection is added to the selected server group on the left pane.



6. Similarly, you can remove a service from a particular server group by selecting the service from the **Connections Available in Group** list and then click on the **Remove >>** button.

> ⚠ The Administrator having **Revoke Service From Service Group** privilege will only be able to remove Services mapped to Service Group.

4.5.6.1 Group Management

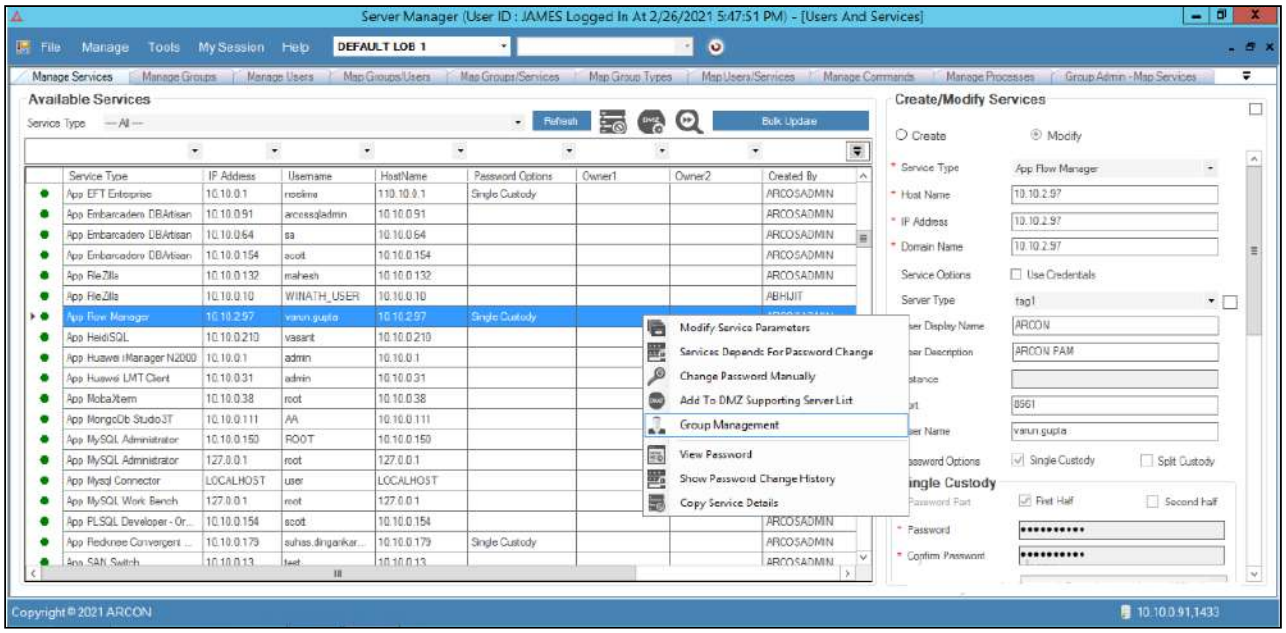
You can map service to multiple Server Groups using **Group Management** option under **Manage Service** tab.

To map Server to Server Group:

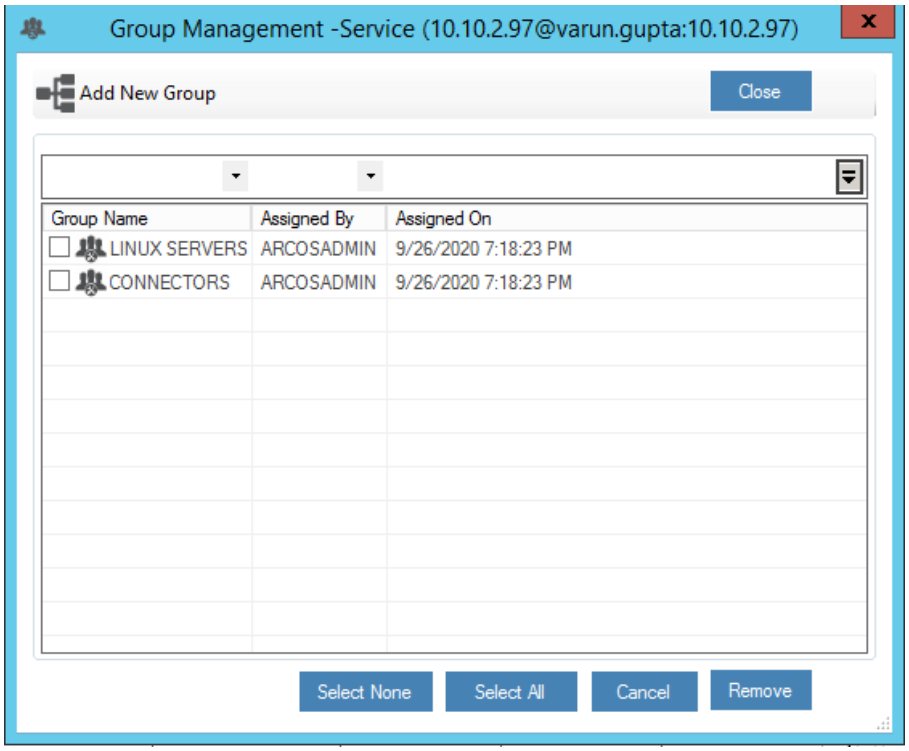
To map User to User Group use the following path:

Manage → Users and Services → Manage Service

1. Right-click on the User name from the **User Display Name** list. A multiple options list is popped up. Click **Group Management** option.



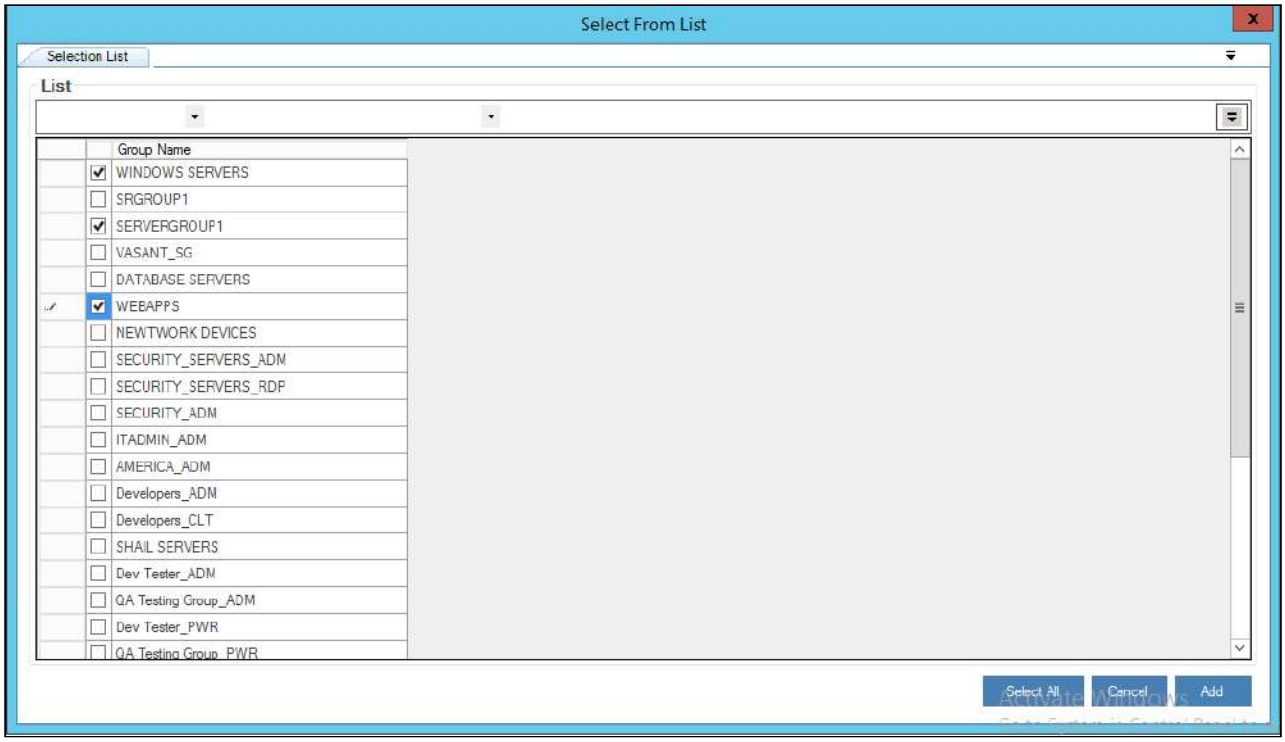
2. The **Group Management** screen is displayed. It displays the list of Server groups already mapped to the service.



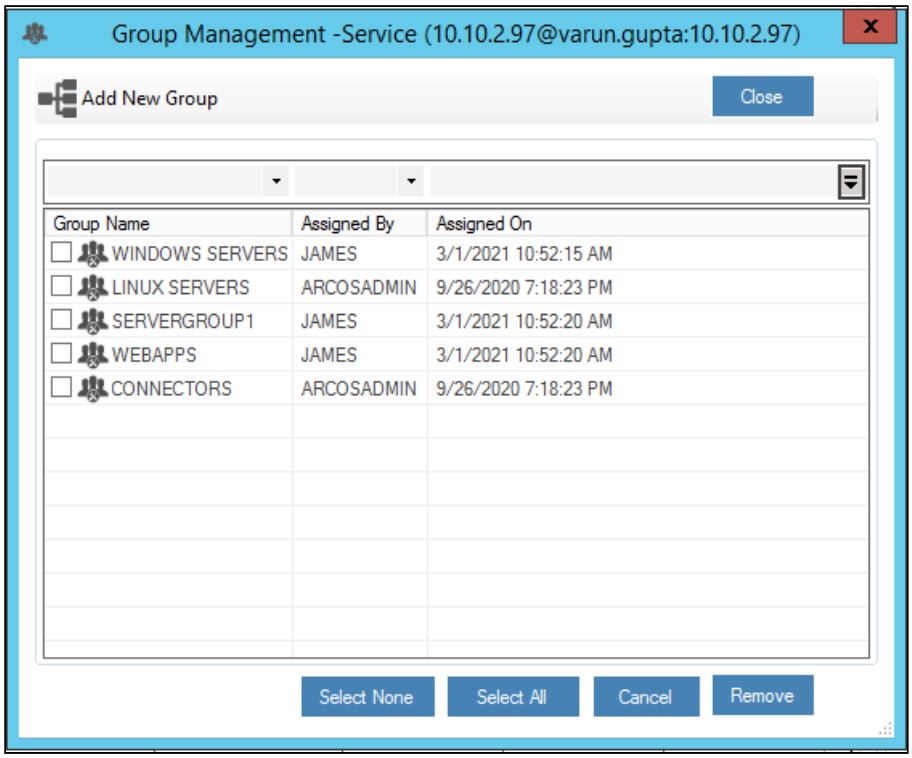
⚠ To search a specific set of rows, enter keywords (space separated) on the column's header, and the relevant rows are pulled out

3. Click **Add New Group to map a new Server Group to the Service**. A pop up comes up- Do you want to perform this operation? Select Yes.
4. The **Selection List** screen is displayed, select the User Groups checkbox to which the User should be mapped and select **Add**.

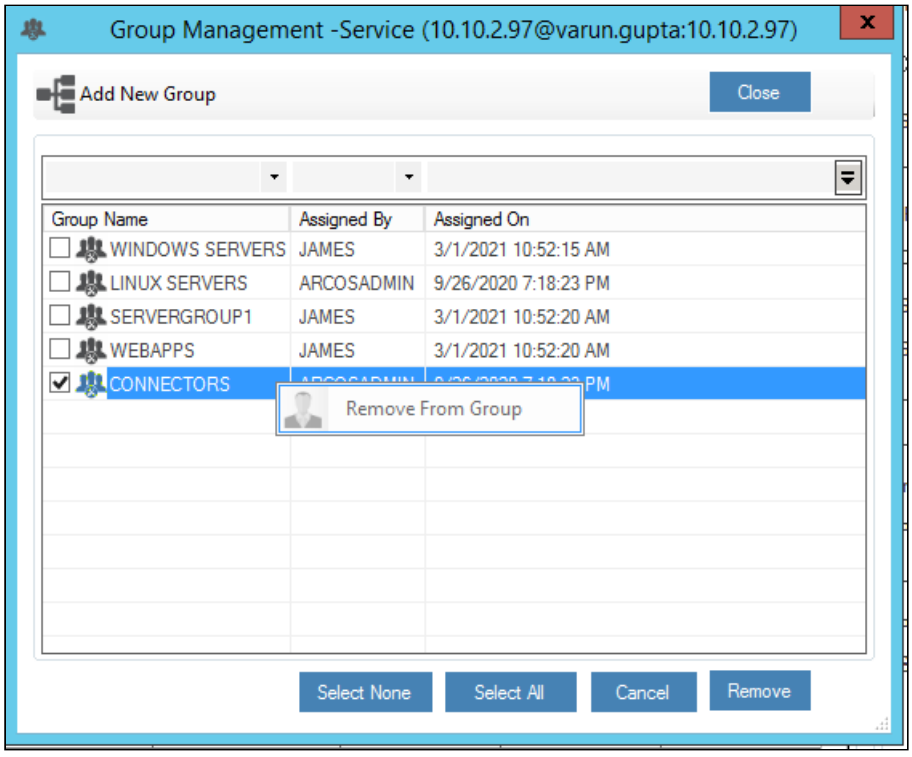
> ⚠ On clicking **Add** the User group is mapped to the User either directly or goes under approval to higher level admins depending on the workflow.



5. The selected User Group is displayed in **Group Management** screen.



6. To remove the Server Group from the Server, select the Server Group, right-click and select **Remove From Group** or select the checkbox beside the Server Group and select remove.



7. The selected Server Group will be removed from **Group Management** screen.

> ⚠ On clicking **Remove**, the Server group is revoked from the Server either directly or goes under approval to higher level admins depending on the workflow.

4.5.7 Map Server Group to User Group

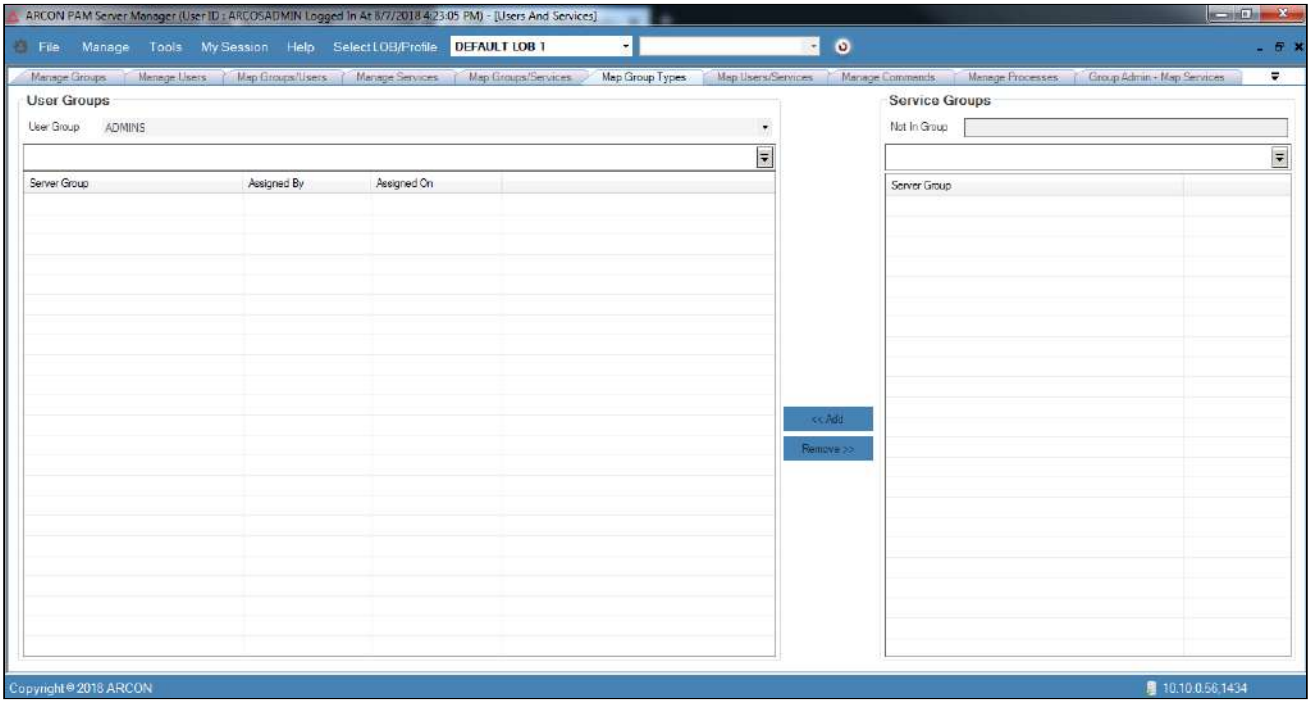
This section helps you to map Server Groups to User Groups. You can map Server Groups to User Groups using the **Map Group Types** screen.

> ⚠ The Administrator having **Assign Service Group To User Group** privilege will only be able to perform group mapping.

To map Server Group to User Group:

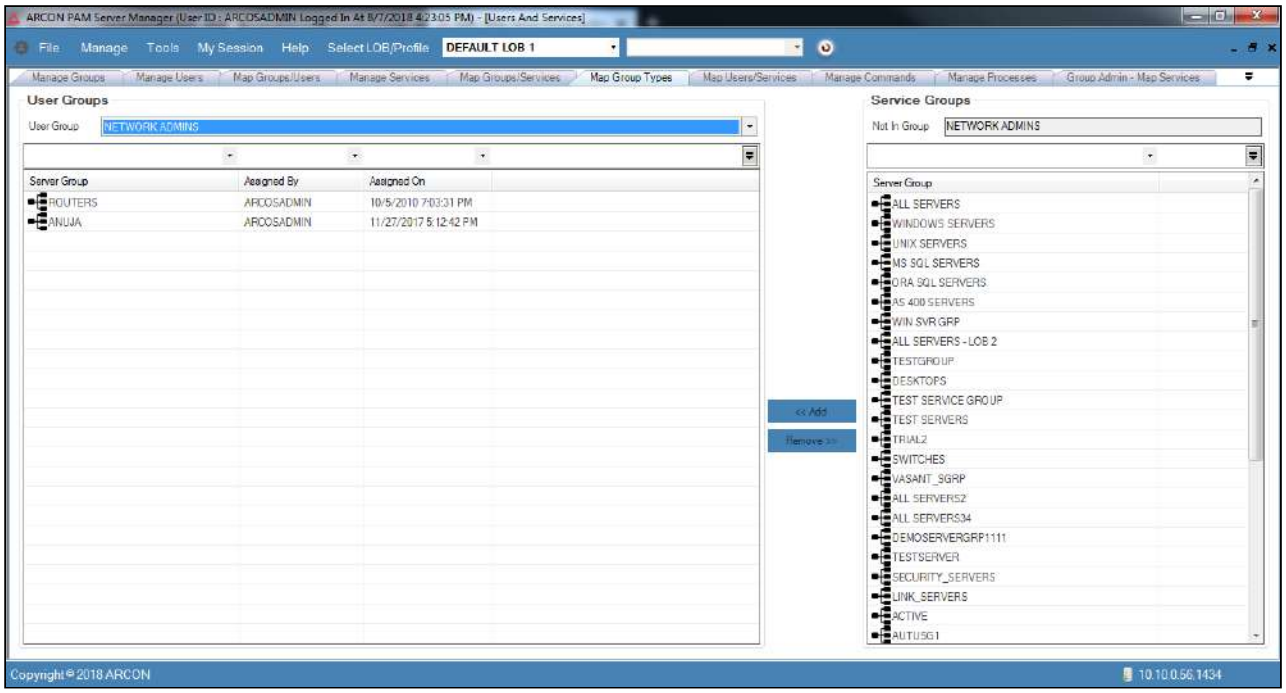
To map server group to user group use the following path:

Manage → Users and Services → Map Group Types

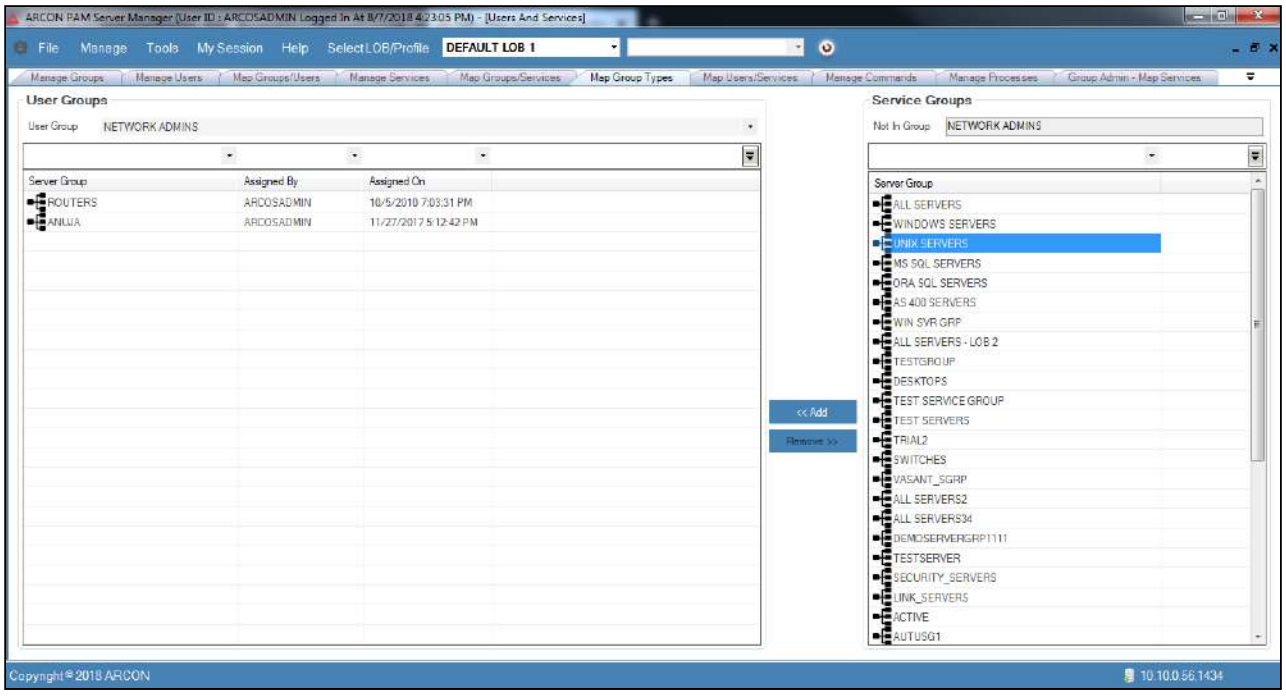


1. Select/Enter the user group from the **User Groups** dropdown list. The left pane displays all the server groups, which are already mapped with the user group, and the right pane displays all the server groups which are not yet mapped with the selected user group.

> ⚠
> - To search a specific set of rows, enter keywords(space separated) in the search text field of user group and service group dropdown and the relevant rows are fetched.
> - To search a specific set of rows, enter keywords (space separated) on the column's header, and the relevant rows are pulled out.



2. Select the server group from the right pane and click **<< Add** button. The server group is assigned to the user group on the left pane.



> ⚠ This will assign all the services of the selected server group to the selected user group.

3. Similarly, you can remove a server group assigned to a user group by selecting the server group from the **Server Group** list on the left pane and then click the **Remove >>** button.

> ⚠ The Administrator having **Revoke Service Group From User Group** privilege will only be able to revoke group mapping.

4.5.8 Map Services to a User

This section helps you to map Services to a particular User. The connections to the users are established in **Map Users / Services** screen. The Services are assigned to a User, based on the Services available in the User Group and the User shall be part of the User Group.

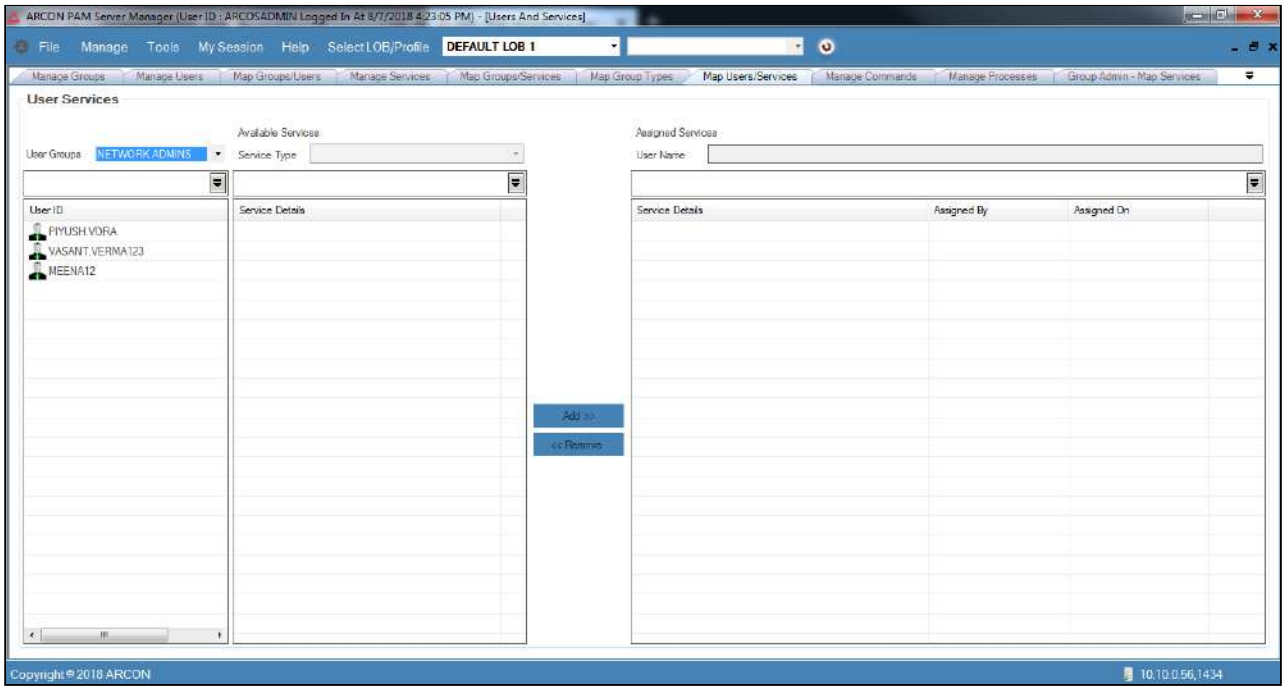
> ⚠
> - The Administrator having **Assign Service To User** privilege in Server's Privileges will only be able to map Services to a particular User.
> - If the Admin is Server Group Admin, then he should be assigned **Assign Service To User** privilege in Group Admin Privileges to map Services to a particular User.

To map Services to Users:

To map services to users use the following path:

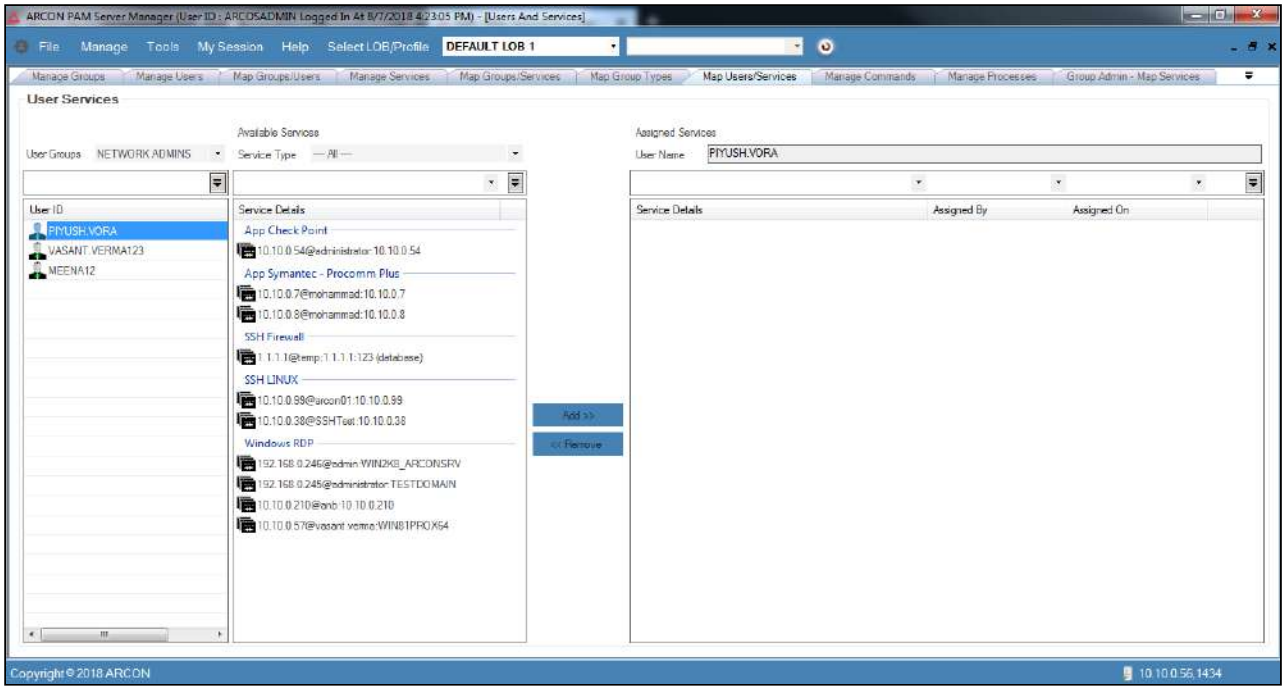
Manage → Users and Services → Map Users/ Services

1. Select the user group from the **User Groups** dropdown list on the left pane. A list of **User ID(s)** are displayed.



> ⚠ To search a specific set of rows, enter keywords (space separated) on the column's header, and the relevant rows are pulled out.

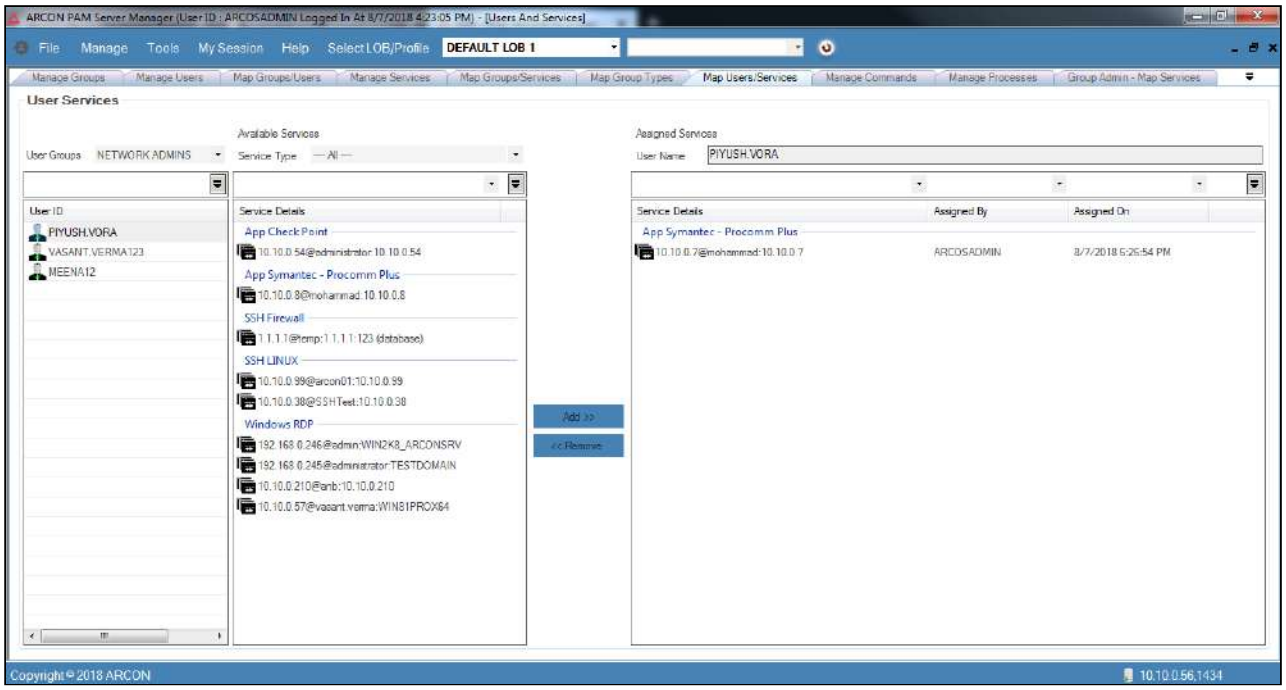
2. Select the user ID from the **User ID** list, wherein it displays all the service details available for that particular user ID.



3. Select the services from the **Service Details** list under **Available Services** section. On selection of the service, a popup appears requesting to select the access type(Time-based/one-time/permanent) of service for that user.

> ⚠ The popup will appear only if **Time Based Service Access Request From Server Manager - Is Enabled** in **Settings.**

4. Click **Add >>** button. The services are now assigned to that particular user.



5. You can view the services assigned to the user in the **Service Details** list under **Assigned Services** section.
6. Similarly, you can remove Services mapped to a particular User by selecting the user from the list of services in **Assigned Services** section and then click the **Remove >>** button.

> ⚠
>
> - The Administrator having **Revoke Service From User** privilege in Server's Privileges will only be able to remove Services mapped to a User.
> - If the Admin is Server Group Admin, then he should be assigned **Revoke Service From User** privilege in Group Admin Privileges will only be able to remove Services mapped to a User.

4.5.9 Map Service to Multiple Users

This section helps you to map Services to single or multiple Users. In addition, it also allows to restrict commands for a particular User.

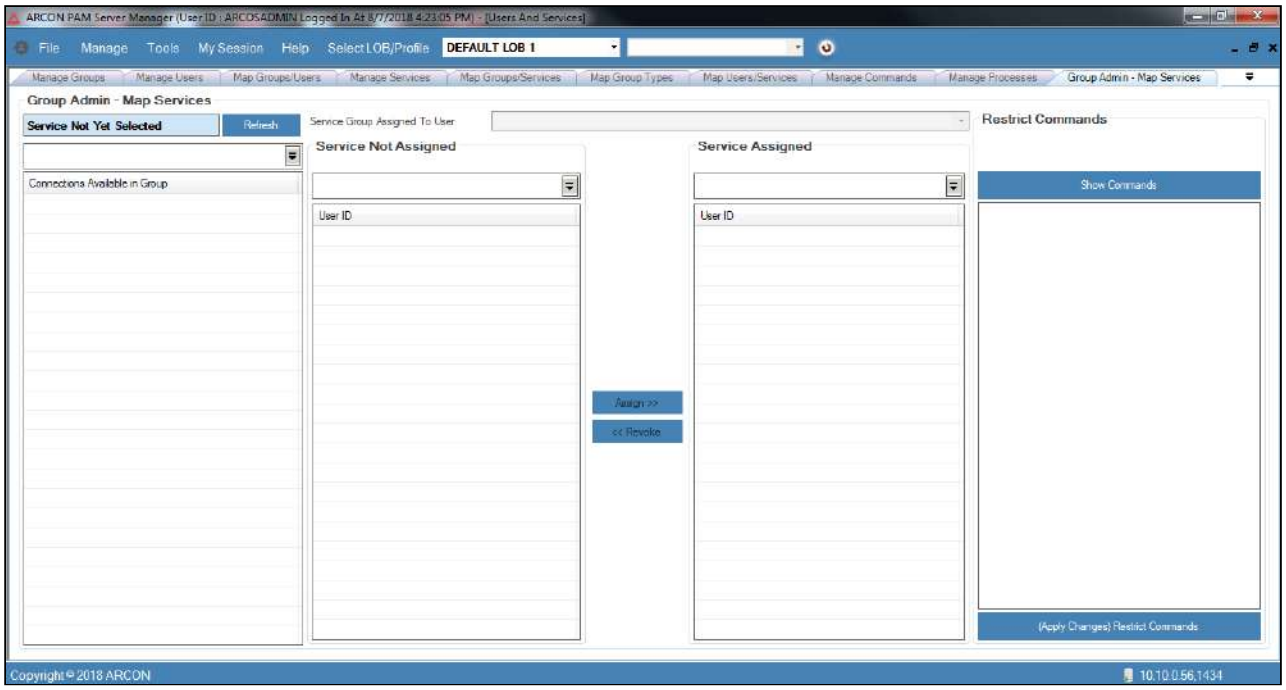
> ⚠ The Administrator having **Assign Service To User** privilege in **Group Admin** privileges will only be able to map Services to multiple Users.

To map Services to Multiple Users:

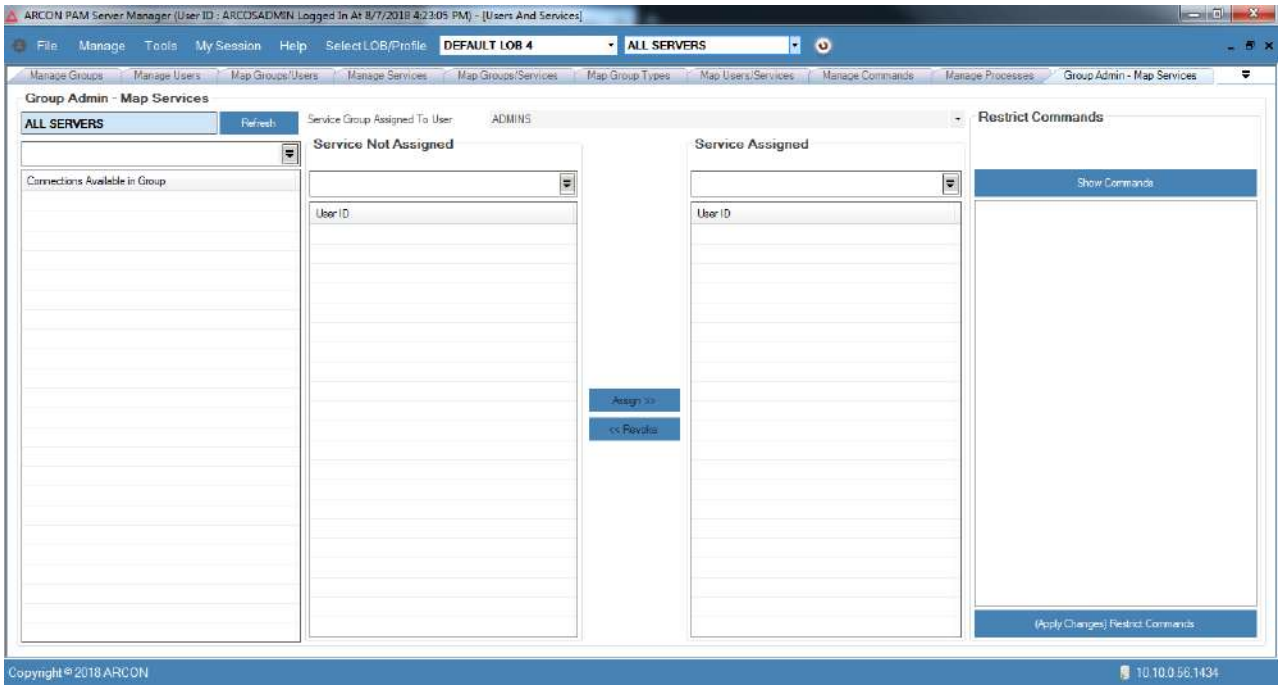
To map services to multiple users use the following path:

Manage → User and Services → Group Admin – Map Services

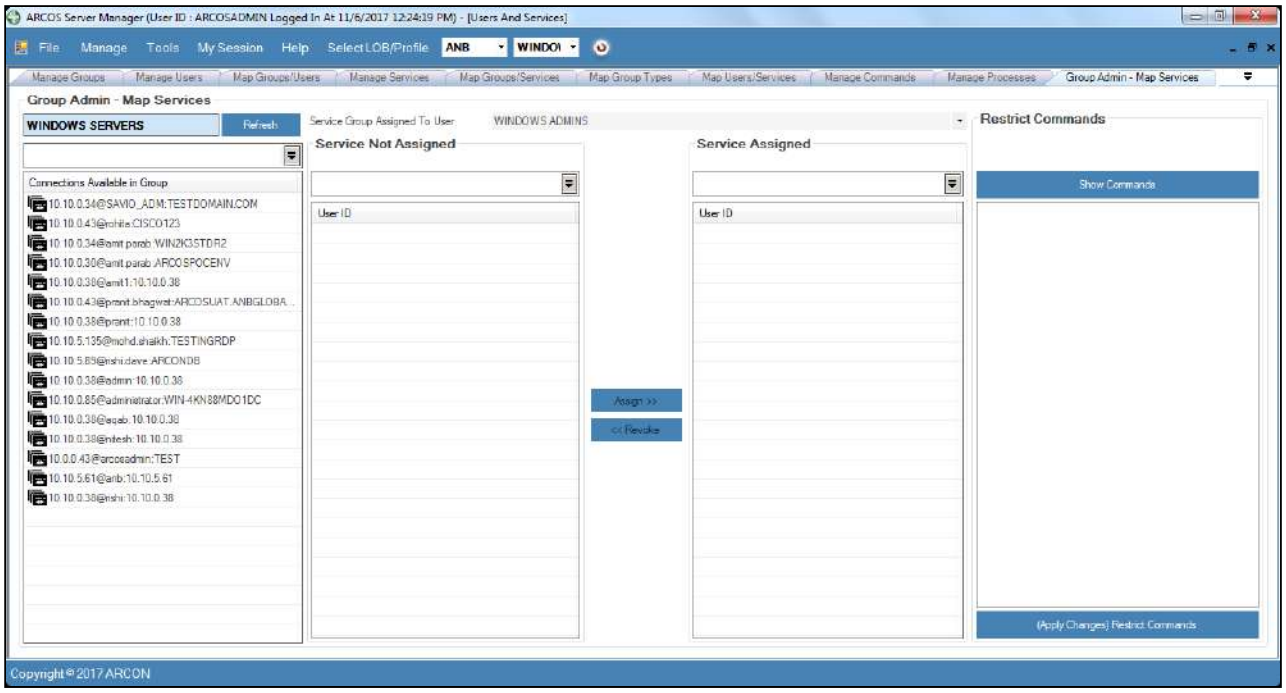
1. Select required **Service Group Admin** from the dropdown list in the menu bar.



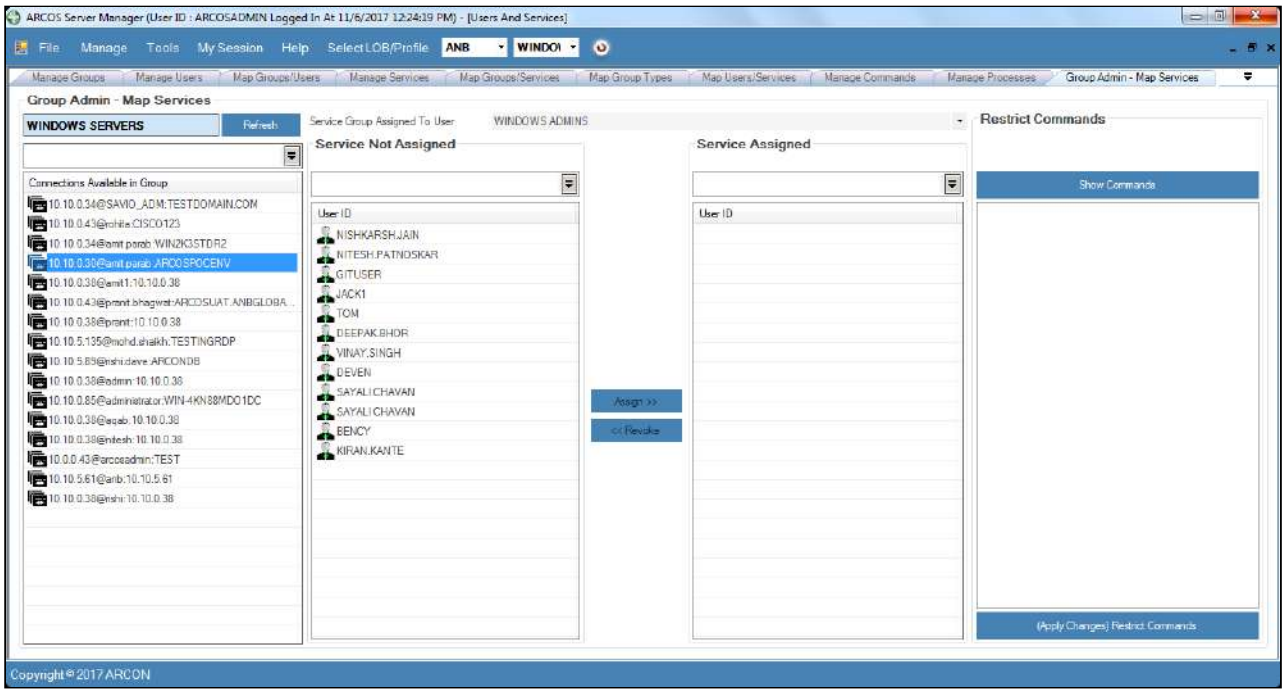
2. A window pops up with message: **Server Group Selected For Administration: Server Group Name**
3. Navigate through tabs to view the group name under **Group Admin – Map Services** text field.



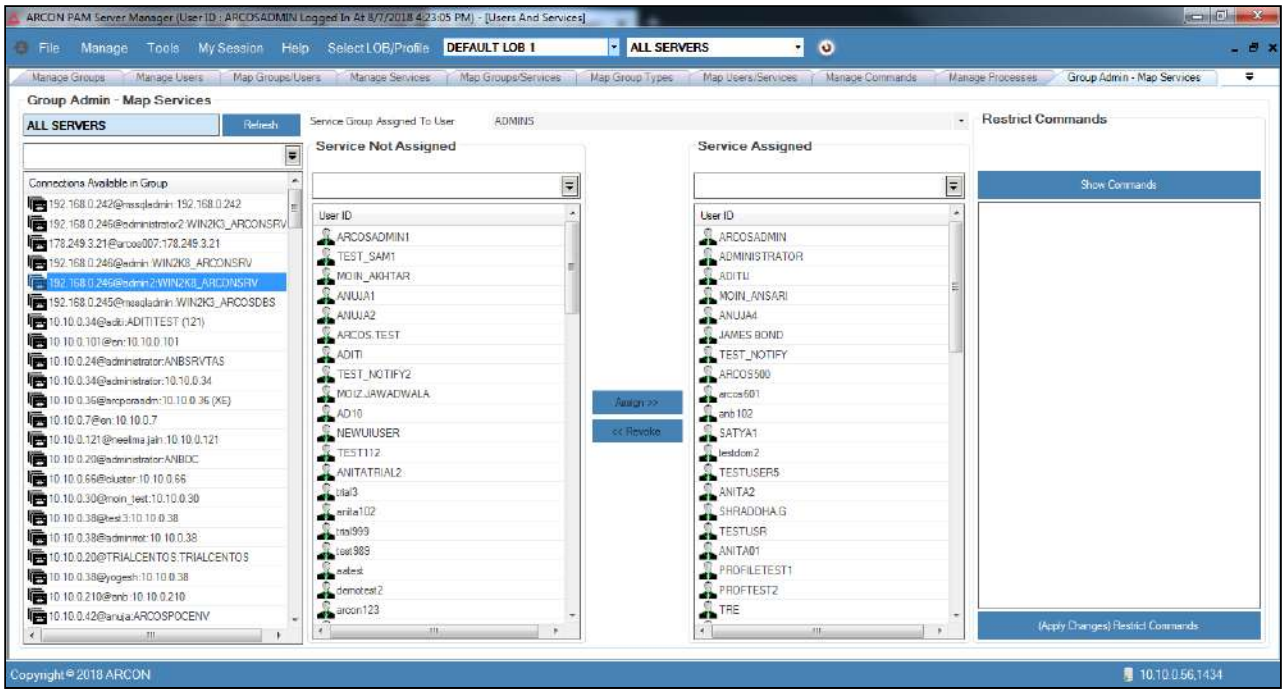
4. Click **Refresh** button. The services available in the server group and the service group assigned to user are displayed in the **Connections Available in Group** grid and **Service Group Assigned To User** text field respectively.



5. Select the service in **Connections Available in Group** grid. It displays a list of users to whom the services are not assigned and assigned in the **Service Not Assigned** grid and **Service Assigned** grid respectively.



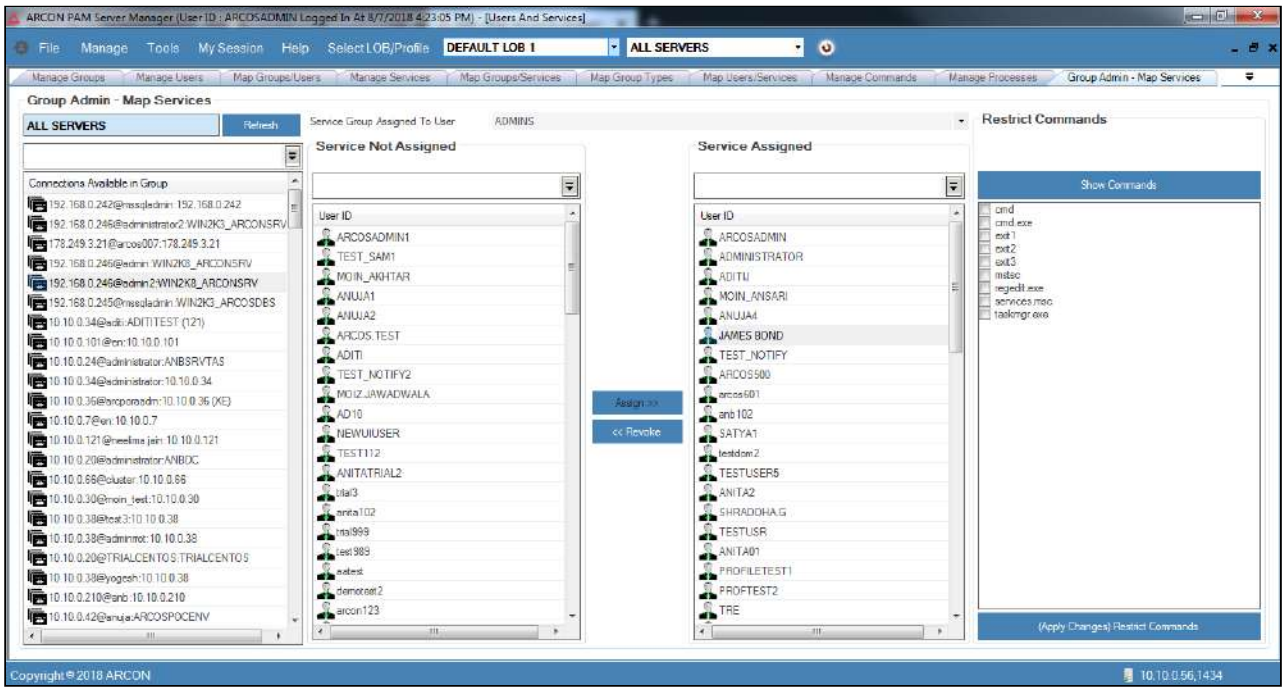
6. Select the user ID from the **Services Not Assigned** grid and click **Assign >>** button. The selected user ID is displayed in the **Service Assigned** grid.



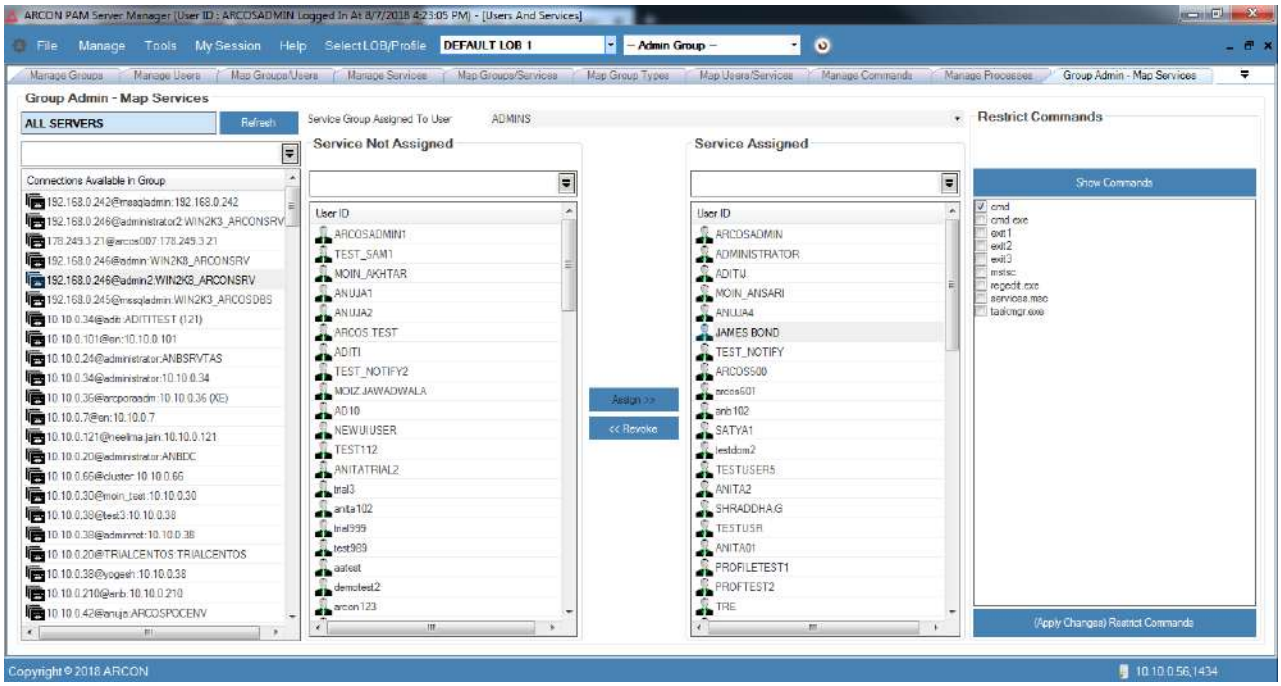
7. Similarly, you can revoke a user to whom a services are assigned by selecting the user from the **Service Assigned** grid and then click the **<< Revoke** button.

> ⚠ The Administrator having **Revoke Service From User** privilege in **Group Admin** privileges will only be able to remove Services mapped to multiple Users.

8. Select the User ID from the **Service Assigned** grid and then click **Show Commands** button. A list of commands assigned to the user are displayed in the **Show Commands** list.



9. Select the commands checkbox and click the **(Apply Changes) Restrict Commands** button to restrict the commands.



10. A window pops up with message: **Commands Restricted/ Applied Successfully For User.**

4.5.10 Automatically map User to Service and Vice Versa

The Automatically Map User to Server and vice-versa feature allows Administrator to automatically map Users to Services or Services to User which are mapped to their respective Groups. This feature can be applied at global level or LOB wise. To automate the feature at global level, the Administrator has to enable the configurations present in Settings.

Pre-requisites:

- The User Group should be present in the domain.
- The Server Group should be present in the domain.
- It is mandatory for the Administrator to map the User Group to the Server Group in the domain.

A. Automatically Assign Users to all Services

The Administrator has to enable the Settings to automatically assign all services to newly added Users in User Group. If the Settings value is Disabled and you add a User to User Group, then services are not assigned to the User. When the Settings value is configured as Enabled and you add a User to User group, the services are automatically assigned to this User. Whereas, services will not be assigned to Users who were added to User group before the Settings value was enabled.

⚠

- It is mandatory to map the User Group to Server Group before starting the automation of Users to Services or Services to Users

- To configure **Settings**, the Administrator should have **Default Configuration** and **Settings** privileges under Server's Privileges.

To automatically map User to Services, follow the below steps:

1. Click **Manager** → **Settings, Settings** window opens.
2. Search for **Automate User and Service Mapping When user added in UserGroup – Is Enabled.** You can Disable or Enable the feature using the toggle button in Settings.
3. Enable the toggle value and the settings Value will be updated Successfully.
4. The Settings to automate the user and service mapping when the user is added to User Group is configured successfully.
5. Click **Manage** → **Users and Services** → **Map Group/Users.**
6. Map User to User Group.

   For more information refer **Map User to UserGroup.**

7. On mapping the **User** to **User Group**, as the Settings for automation is **Enabled** the **User** is automatically assigned the **Services** present in the mapped **Server Group**.

B. Automatically Assign Services to All Users

The Administrator has to enable the Settings to automatically assign all Users to newly added Services in Server Group. If the Settings value is Diabled and you add a Service to Server Group, then Users are not assigned to the Service. When the Settings value is configured as Enabled and you add a Service to Server group, the Users are automatically assigned to this Service. Whereas, Users will not be assigned to Services which were added to Server group before the Settings value was enabled.

- It is mandatory to map the User Group to Server Group before starting the automation of Users to Services or Services to Users
- To configure **Settings**, the Administrator should have **Default Configuration** and **Settings** privileges under Server's Privileges.

To automatically assign Service to the Users, follow the below steps:

1. Click **Manager** → **Settings, Settings** window opens.
2. Search for **Automate User and Service Mapping When server added in ServerGroup – Is Enabled.** You can Disable or Enable the feature using the toggle button in Settings.
3. Enable the toggle value and the settings Value will be updated Successfully.
4. The Settings to automate the user and service mapping when the user is added to User Group is configured successfully.
5. Click **Manage** → **Users and Services** → **Map Group/Services.**
6. Map Service/s to Server Group.

   For more information refer **Map Services to Server Group**

7. On mapping the **Services** to **Server Group**, as the **Settings** or automation is **Enabled** the **Service/s** is automatically assigned to the **User** present in the mapped **User Group**.

4.6 Revoke and Share

ARCON PAM supports remove and share feature wherein an Administrator can remove users, user group, services, and server group from a particular LOB. An Administrator can use **Remove** function, when he does not want to allow any authorization to the users to access any services. In addition, an Administrator can share users between LOB's. A **Share** function is used, when a user is part of two different LOB's and he needs authorization to access the services belonging to those LOB's.

This section includes the following topics:

- Remove User from LOB
- Remove User Group from LOB
- Remove Services from LOB
- Remove Service Groups from LOB
- Share Users between LOB's

4.6.1 Remove Users from LOB

This section helps you to remove users from a particular LOB. You can remove users from a particular LOB using **Map LOB/Users** screen.

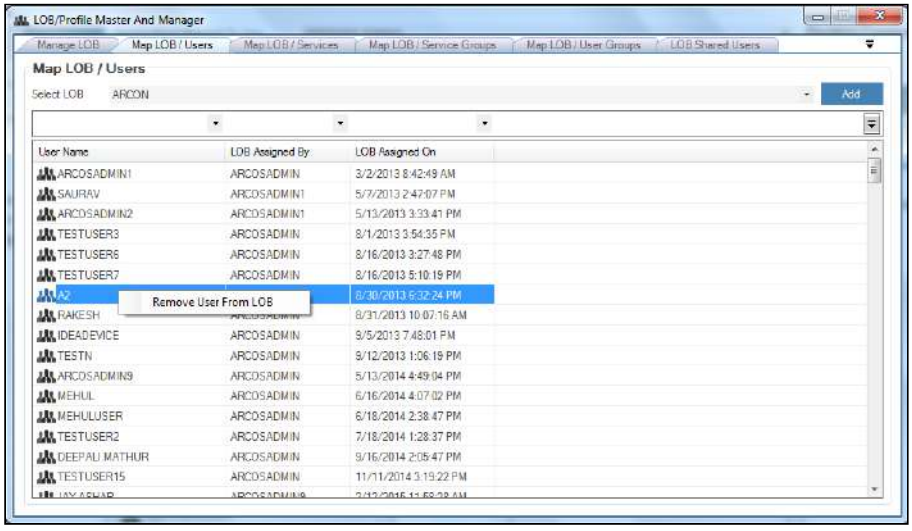
⚠ The Administrator having **Revoke LOB From User** privilege will only be able to revoke user from LOB.

To remove users from a particular LOB:

To remove users from a particular LOB use the following path:

Manage → LOB/Profile Master and Manager → Map LOB/Users

1. Select the required LOB. A list of Users mapped to the LOB are displayed.
2. Right click on the selected user. A **Remove User From LOB** option is popped up.



3. Click **Remove User From LOB**. A window pops up with the following message: **User(s) Removed From LOB**
4. Click **OK**. The selected user is removed from the LOB.

4.6.2 Remove User Groups from LOB

This section helps you to remove user groups from a particular LOB. You can revoke user groups from a particular LOB using the **Map LOB/User Groups** screen.

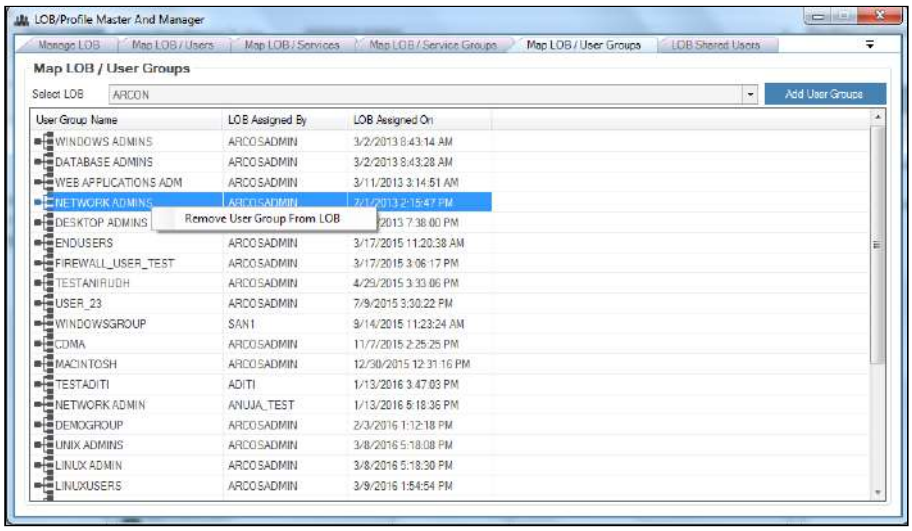
> ⚠ The Administrator having **Revoke LOB From User Group** privilege will only be able to revoke user group from a particular LOB.

To remove user groups from a particular LOB:

To remove user groups from a particular LOB use the following path:

Manage → LOB/Profile Master and Manager → Map LOB/User Groups

1. Select required LOB. A list of User Groups are displayed.
2. Right click on the selected user group. A **Remove User Group From LOB** option is popped up.



3. Click **Remove User Group From LOB**. A window pops up with the following message: **User Group Removed From LOB**
4. Click **OK**. The selected user group is removed from the LOB.

4.6.3 Remove Services from LOB

This section helps you to remove services from a particular LOB. You can revoke services from a particular LOB using the **Map LOB/Services** screen.

> ⚠ The Administrator having **Revoke LOB From Service** privilege will only be able to revoke services from a particular LOB.

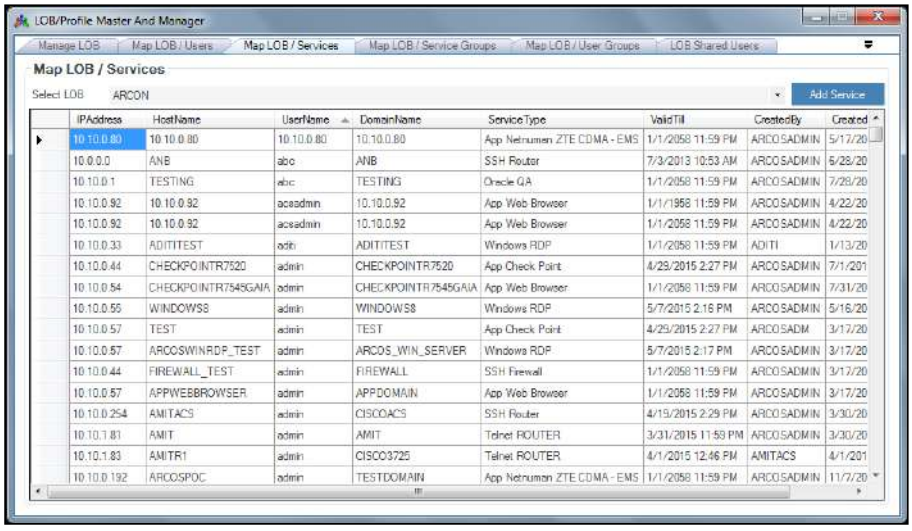
To remove services from a particular LOB:

To remove services from a particular LOB use the following path:

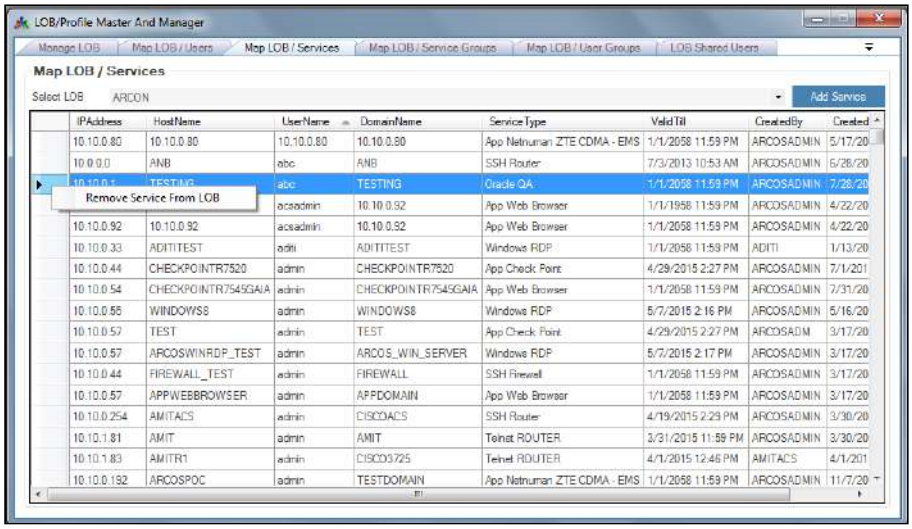
Manage → LOB/Profile Master and Manager → Map LOB/Services

1. Select required LOB. A list of services are displayed.

2. Select the service and click on the  icon to select the entire row.



3. Right click on the selected service. A **Remove Service From LOB** option is popped up.



4. Click **Remove Service From LOB**. A window pops up with the following message: **Services(s) Removed From LOB**
5. Click **OK**. The selected service is removed from the LOB.

4.6.4 Remove Service Groups from LOB

This section helps you to remove service groups from a particular LOB. You can revoke service groups from a particular LOB using the **Map LOB/Service Group** screen.

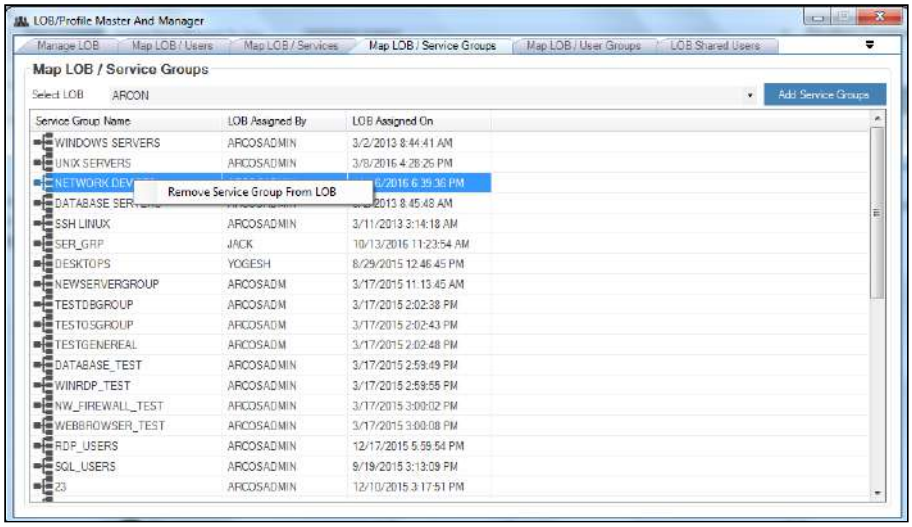
> ⚠ The Administrator having **Revoke LOB From Service Group** privilege will only be able to revoke service group from a particular LOB.

To remove service groups from a particular LOB:

To remove service groups from a particular LOB use the following path:

Manage → LOB/Profile Master and Manager → Map LOB/Services

1. Select the required LOB. A list of Service Groups are displayed.
2. Right click on the selected service group. A **Remove Service Group From LOB** option is popped up.



3. Click **Remove Service Group From LOB**. A window pops up with the following message: **Service Group Removed From LOB**
4. Click **OK**. The selected service group is removed from the LOB.

4.6.5 Share Users between LOB's

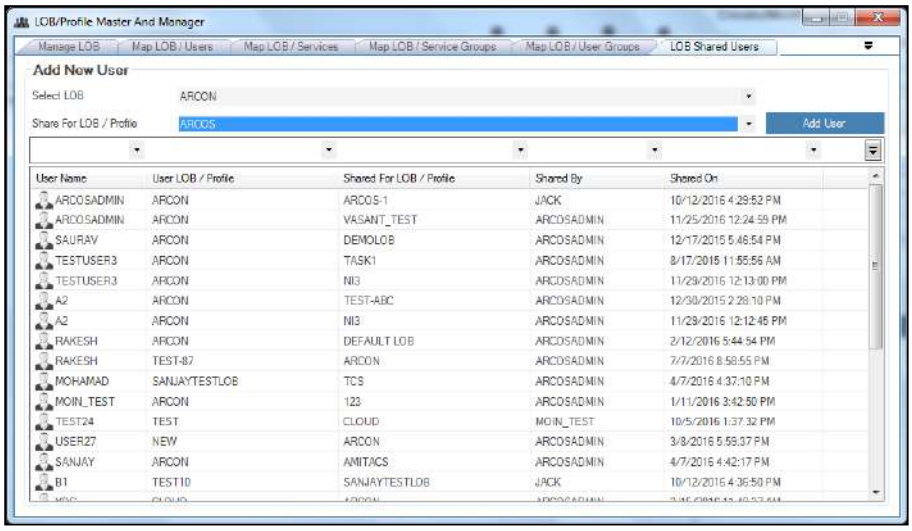
This section helps you to share users from one LOB to another LOB. Therefore, a user is able to access servers in multiple LOB(s).

To share users between LOB(s):

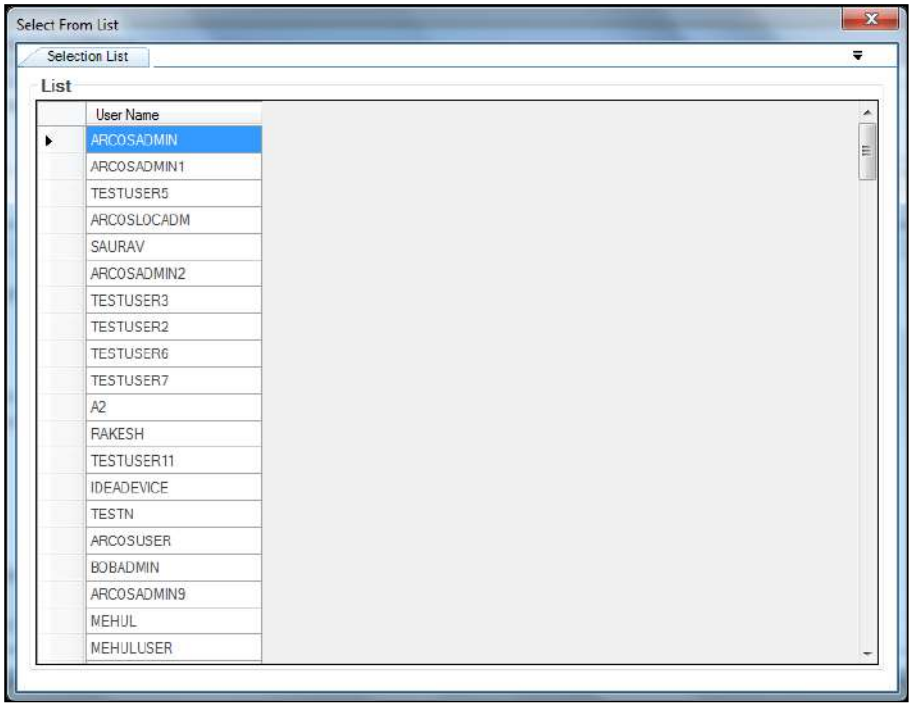
To share users between LOB(s) use the following path:

Manage → LOB/Profile Master and Manager → LOB Shared Users

1. Select the LOB from the **Select LOB** dropdown list.
2. Select the LOB from the **Shared For LOB/Profile** dropdown list, where a user has to be shared.



3. Click **Add User** button. The **Select From List** screen is displayed.



4. Select the username and double-click on the  icon. A window pops up with the following message: **New User Added To Shared User List**

5 Privilege Management

Privilege Management refers to the access or privileges assigned to an identity i.e. any user account that holds special or additional permissions within the enterprise systems. It involves managing privileged individual identities, their authentication, authorization, and privileges/permissions within or across systems and enterprise boundaries with the goal of increasing security and productivity while optimizing the downtime, repetitive tasks and the cost.

5.1 Assign or Revoke Privileges from Admin or Client Users

Privileges are special rights, advantage, or immunity granted or available only to a particular person or group. In ARCON PAM, there are two type of Users such as Client Users and Admin Users. Client Users are those Users who has access to only Client Manager whereas, Users who has access to both Client Manager and Server Manager are Admin type of User.

⚠ The Administrator having **Admin Privileges** will only be able to edit privilege settings assigned to Users or Group Admin.

The following options are available in **Edit Privilege Settings**:

- ARCON PAM User Privileges
- ARCON PAM Group Admin Privileges

A. ARCON PAM User Privileges:

In order to have limit on the user's accessibility, access rights to users are given in both Server Manager and Client Manager. These access rights are basically the privileges given to the users.

Client Manager or Server Manager privileges are assigned to Admin or Client Type users:

- **Client Manager Privileges:** API User Registration, ARCOS Applications, ARCOS Dashboard, ARCOS Delegation, ARCOS File Vault, Client Manager Log, Manager LOB/Profile, PAM Menu, Password Manager, Reports (Dashboard, Group Reports, LOB Reports, Logs, Performance Reports, Privilege Reports, Security Reports, Service Reports, User Reports, Vault Reports), and Script Manager.
- **Server Manager Privileges:**Application Password Change, Application Password Change – HP SiteScope, ARCOS Configuration, Command Profiler, Log Viewer, Manage Group, Manage LOB/ Profile, Manage Services, Manage Tab,Manage User, Password Manager and Tools Tab.

B. ARCON PAM Group Admin Privileges:

The Administrator can create number of groups for users and services. Each group can have their own Administrator. To manage these groups **Group Admin** privileges are assigned to the respective Group Administrator.

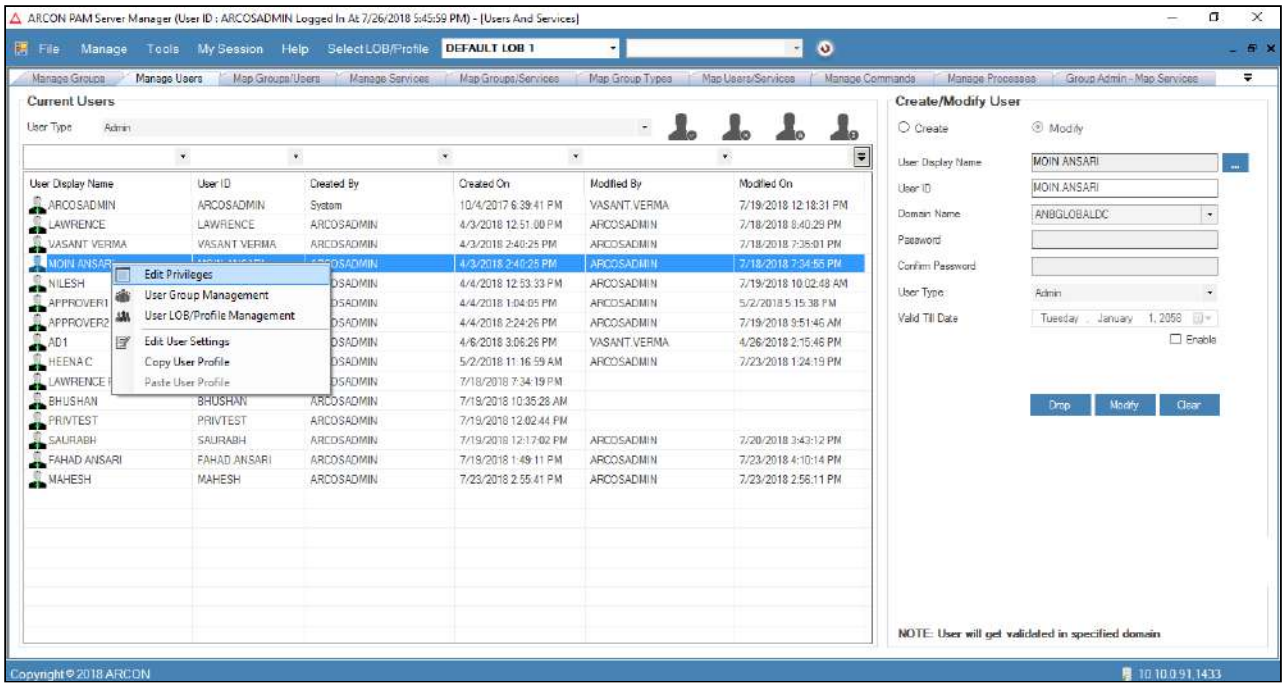
- **Group Admin privileges** such as Group Log Viewer, User Certification, Manage Services, and Manage User Request are only assigned to Admin type of users.

To edit privileges:

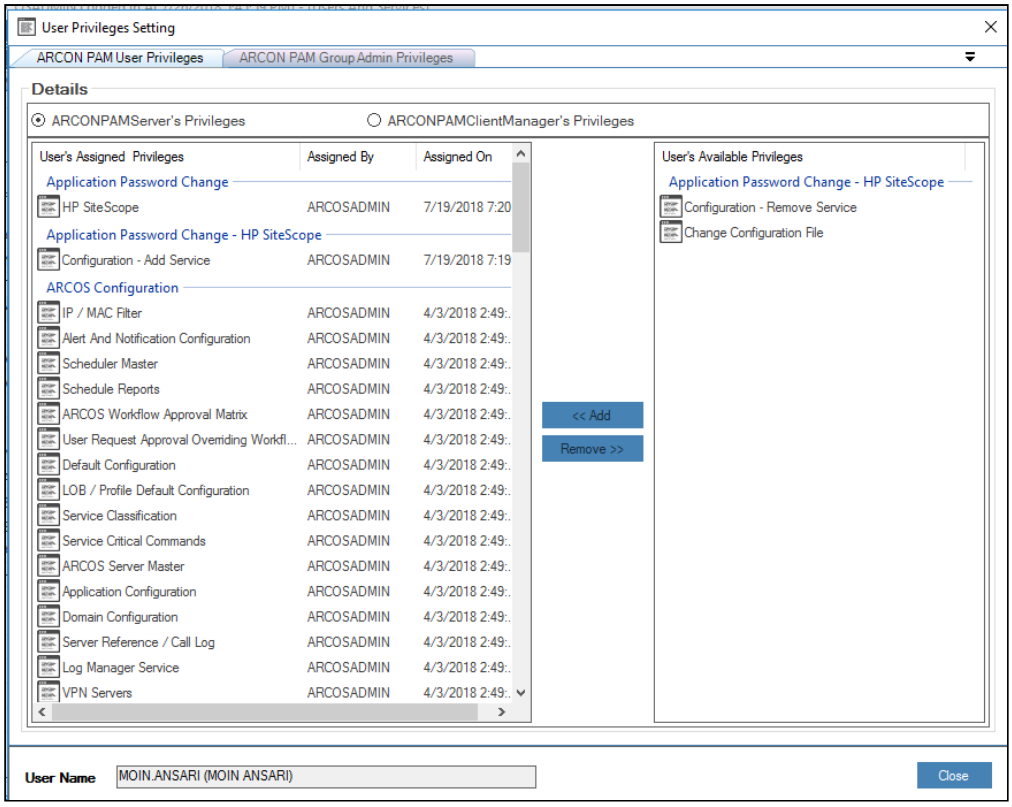
To edit privileges use the following path:

Manage → Users and Services → Manage Users

1. Right click on the user name from the **User Display Name** grid list. The **Edit Privileges** option is displayed.



2. Click the **Edit Privileges** option. The **User Privileges Setting** window is displayed.



3. Select the privileges from the list of **User's Available Privileges** and click the **<<Add** button. The selected privileges are displayed in the list of **User's Assigned Privileges**.

4. Similarly, you can remove the assigned privileges by selecting the privileges from the list of **User's Assigned Privileges** and then click on the **Remove>>** button to remove the assigned privileges.

> ⚠ You can follow the above steps to add or remove the available or assigned privileges for **ARCONPAMClientManager's Privileges** option and **ARCON PAM Group Admin Privileges** tab.

5.2 Server's Privileges

ARCON PAM Server's Privileges are assigned to Admin type of Users to grant special rights for User management, service management, group management, password management, accessing logs and other applications. Server privileges include Application Password Change, Application Password Change - HP SiteScope, ARCOS Configuration, Command Profiler, Log Viewer, Manage Group, Manage LOB / Profile, Manage Services, Manage Tab, Manage User, Password Manager and Tools Tab.

Following are the list of Server Privileges:

ARCON PAM Server Privilege		Description	Feature Navigation
Application Password Change	HP SiteScope	Administrator having this privilege can change configuration file process.	Server Manager > Tools > Application Password Change > HP SiteScope
Application Password Change - HP SiteScope	Configuration - Add Service	Administrator having this privilege can add service to configuration list.	Server Manager > Tools > Application Password Change > HP SiteScope > Configuration
	Configuration - Remove Service	Administrator having this privilege can remove service from configuration list.	Server Manager > Tools > Application Password Change > HP SiteScope > Configuration
	Change Configuration File	Administrator having this privilege can change Configuration file process.	Server Manager > Tools > Application Password Change > HP SiteScope > Change Password - Configuration File
ARCON PAM Configuration	IP / MAC Filter	Administrator having this privilege can configure all the IP address, MAC address, Processor ID, and BIOS Serial ID which have been blocked or allowed for desktop level access.	Server Manager > Tools > IP / MAC Filter
	Alert And Notification Configuration	Administrator having this privilege can configure alerts and Users who will receive alert notification.	Server Manager > Tools > Advanced Configuration > Alert & Notification Configuration
	Scheduler Master	Administrator having this privilege can configure a scheduler to send reports and password envelope through email.	Server Manager > Tools > Advanced Configuration > Scheduler Master

ARCON PAM Server Privilege		Description	Feature Navigation
	Schedule Reports	Administrator having this privilege can configure reports to be sent through email and saved on preferred path.	Server Manager > Tools > Advanced Configuration > Schedule Reports
	ARCOS Workflow Approval Matrix	Administrator having this privilege can configure approval levels for each transaction or operations performed by Administrator.	Server Manager > Tools > Advanced Configuration > ARCON PAM Workflow Approval Matrix
	User Request Approval Overriding Workflow	Administrator having this privilege can configure approval levels for the request raised by the User for service access, service password, service ticket, and critical command.	Server Manager > Tools > Advanced Configuration > User Request Approval Overriding Workflow
	Default Configuration	Administrator having this privilege and in addition having configuration privileges under Default Configuration such as Application Configuration, Domain Configuration, can create or modify the respective configuration.	Server Manager > Tools > Advanced Configuration > Default Configuration
	LOB / Profile Default Configuration	Administrator having this privilege can map different LOBs to a particular server, initiate schedule password change process, help to retain logs, and apply command profile to the services mapped under a particular User group.	Server Manager > Tools > Advanced Configuration > LOB / Profile Default Configuration
	Service Classification	Administrator having this privilege can define the classification for a service such as critical, data, or antivirus server.	Server Manager > Tools > Advanced Configuration > Service Classification
	Service Critical Commands	Administrator having this privilege can define a critical command for a service.	Server Manager > Tools > Advanced Configuration > Service Critical Commands
	ARCOS Server Master	Administrator having this privilege can add or modify servers such as application server, database server, gateway server, and DR servers.	Server Manager > Tools > Advanced Configuration > ARCOS Server Master
	Application Configuration	Administrator having Default Configuration and Application Configuration privileges can enable the Administrator to design local user account policy and manage User's login according to the policy.	Server Manager > Tools > Advanced Configuration > Default Configuration > Menu > Application Configuration
	Domain Configuration	Administrator having Default Configuration and Domain Configuration privileges can configure different domains.	Server Manager > Tools > Advanced Configuration > Default Configuration > Menu > Domain Configuration

ARCON PAM Server Privilege		Description	Feature Navigation
	Server Reference / Call Log	Administrator having Default Configuration and Server Reference / Call Log privileges can enable a confirmation message box, which prompts for the ticket number and the reason for accessing a particular service in Client Manager.	Server Manager > Tools > Advanced Configuration > Default Configuration > Menu > Server Reference / Call Log
	Log Manager Service	Administrator having Default Configuration and Log Manager Service privileges can configure Log Manager Service.	Server Manager > Tools > Advanced Configuration > Default Configuration > Menu > Log Manager Service
	VPN Servers	Administrator having Default Configuration and VPN Servers privileges can configure VPN Servers.	Server Manager > Tools > Advanced Configuration > Default Configuration > Menu > VPN Servers
	Service Reference Template	Administrator having Default Configuration and Service Reference Template privileges can configure templates which prompt User before accessing service from Client Manager.	Server Manager > Tools > Advanced Configuration > Default Configuration > Menu > Service Reference Template
	Advanced Utility	Administrator having Default Configuration and Advanced Utility privileges can convert the font of the Service Host Name and Service Domain Name to uppercase.	Server Manager > Tools > Advanced Configuration > Default Configuration > Menu > Advanced Utility
	Hardware Token - Radius Servers	Administrator having Hardware Token - Radius Servers privilege can configure values for authentication of a RSA portal.	Server Manager > Tools > Advanced Configuration > Hardware Token - Radius Servers
	Password Dictionary	Administrator having Default Configuration and Password Dictionary privileges can configure default passwords.	Server Manager > Tools > Advanced Configuration > Default Configuration > Menu > Password Dictionary
	SMTP Configuration	Administrator having Default Configuration and SMTP Configuration privileges can configure email settings to send alert and notification to approvers. Also Admin can configure IMAP Settings for approver to reply through email for approving or rejecting the raised request.	Server Manager > Tools > Advanced Configuration > Default Configuration > Menu > SMTP Configuration
	ARCOS Message Board	Administrator having Default Configuration and ARCOS Message Board privileges can configure messages to be displayed on pages after or before login.	Server Manager > Tools > Advanced Configuration > Default Configuration > Menu > ARCON PAM Message Board

ARCON PAM Server Privilege		Description	Feature Navigation
	Dual Factor IP Range	Administrator having Default Configuration and Dual Factor IP Range privileges can define the range of IP Address to be configured for the 'Dual Factor type'.	Server Manager > Tools > Advanced Configuration > Default Configuration > Menu > Dual Factor IP Range
	SMS Gateway Configuration	Administrator having Default Configuration and SMS Gateway Configuration privileges can configure SMS Gateway Server details.	Server Manager > Tools > Advanced Configuration > Default Configuration > Menu > SMS Gateway Configuration
	Server Monitoring System	Administrator having Default Configuration and Server Monitoring System privileges can configure details to validate whether the service or the server is already monitored by some monitoring system.	Server Manager > Tools > Advanced Configuration > Default Configuration > Menu > Server Monitoring System
	User Door Access Authentication	Administrator having Default Configuration and User Door Access Authentication privileges can enable and configure values for application to authenticate or check the User's physical presence within the premise.	Server Manager > Tools > Advanced Configuration > Default Configuration > Menu > User Door Access Authentication
	Password Change Defaults	Administrator having Default Configuration and Password Change Defaults privileges can configure settings of password change for different operating systems and service types such as Windows, Linux, and Oracle.	Server Manager > Tools > Advanced Configuration > Default Configuration > Menu > Password Change Defaults
	Voice Biometric Authentication	Administrator having Default Configuration and Voice Biometric Authentication privileges can configure web service for authentication before logging into Client Manager.	Server Manager > Tools > Advanced Configuration > Default Configuration > Menu > Voice Biometric Authentication
	ARCOS Staging Log Server	Administrator having Default Configuration and ARCOS Staging Log Server privileges can configure server details where logs will be stored before they are transferred to Database Server.	Server Manager > Tools > Advanced Configuration > Default Configuration > Menu > ARCON PAM Staging Log Server
	Web API Configuration	Administrator having Default Configuration and Web API Configuration privileges can configure number of configuration types such as URL, description, method, API ID, user name, and password.	Server Manager > Tools > Advanced Configuration > Default Configuration > Menu > Web API Configuration

ARCON PAM Server Privilege		Description	Feature Navigation
	Network Segments	Administrator having Default Configuration and Network Segments privileges can configure range of IP Address. The Network Segment Wise Logon report displays details based on this configuration.	Server Manager > Tools > Advanced Configuration > Default Configuration > Menu > Network Segments
	Settings	Administrator having Default Configuration and Settings privileges can configure critical configurations which affect the application at Global level.	Manager > Settings
	Schedule Password Envelope	Administrator having this privilege can configure password envelope to be sent through email.	Server Manager > Tools > Advanced Configuration > Schedule Password Envelope
	LOB wise Global Configuration	Administrator having this privilege can configure values to automate User to Service mapping when they are added in their respective User and Server group.	Manager > Settings > LOB
	ARCOS Server Configuration	Administrator having this privilege can configure Server details like UAT, Production, Application server which are displayed in About (Client Manager).	Server Manager > Tools > Advanced Configuration > Default Configuration > Menu > ARCON PAM Server Configuration
	ARCON PAM Web API Registration	Administrator having this privilege can configure machine details through which User can view password of Service.	Server Manager > Tools > Advanced Configuration > ARCON PAM Web API Registration
	API Reference Mapping	Administrator having this privilege can enable ARCON API to notify Third Party API about service password change in ARCON PAM.	Server Manager > Tools > Advanced Configuration > Default Configuration > Menu > API Reference Mapping
	Outside ARCON PAM Access Configuration	Administrator having this privilege can enable monitoring of Servers accessed outside ARCON PAM and configure actions such as send alert or block access.	Server Manager > Tools > Advanced Configuration > Outside ARCON PAM Access Configuration
	Generic Scheduler Settings	Administrator having this privilege can configure critical configurations which will be used by ARCON PAM Services and executable files.	Server Manager > Tools > Advanced Configuration > Default Configuration > Menu > Generic Scheduler Settings

ARCON PAM Server Privilege		Description	Feature Navigation
	Custom Commands Configuration	Administrator having this privilege can configure custom commands required for password change.	Server Manager > Tools > Advanced Configuration > Custom Commands Configuration
Command Profiler	Command Profiler	Administrator having this privilege can create, modify, or delete Elevate and Blacklist profiles.	Server Manager > Manage > Command Profiler
Log Viewer	View Command Log	Administrator having this privilege can view logs of the commands fired after connecting to the server.	Server Manager > Manage > Logs > Command Logs
	View ARCOS Log	Administrator having this privilege can view details for the activities performed in Server Manager.	Server Manager > Manage > Logs > ARCON PAM Logs
	View User Access Log	Administrator having this privilege can view login in and logout details of the user who has accessed the ARCON PAM application.	Server Manager > Manage > Logs > User Access Logs
	View Service Log	Administrator having this privilege can view detailed logs of the services accessed by the user in the ARCON PAM application.	Server Manager > Manage > Logs > Service Logs
	View User Validity Status	Administrator having this privilege can view details of all the users which are active or the ones who are deactivated by Administrator to access ARCON PAM application.	Server Manager > Manage > Logs > User Validity Status
	View Server Reference Log	Administrator having this privilege can view details of reference number used before accessing services by Users through ARCON PAM.	Server Manager > Manage > Logs > Service Reference Log
	View Process Log	Administrator having this privilege can view details of the processes executed on Windows Server when a service is accessed through ARCON PAM.	Server Manager > Manage > Logs > Process Logs
	View Service Password Status Log	Administrator having this privilege can view details of the service password status for the services in ARCON PAM.	Server Manager > Manage > Logs > Service Password Status
	Download Video Log	Administrator having this privilege can download video logs of Command logs, Process Logs and Service Logs.	Server Manager > Manage > Logs > Prcoess Logs (or Command Logs or Service Logs) > Video Log

ARCON PAM Server Privilege		Description	Feature Navigation
	View Application Logs	Administrator having this privilege can view error logs of Client Manager application.	Server Manager > Manage > Application Logs
	Real Time Session Monitoring	Administrator having this privilege can monitor real time sessions.	Server Manager > Tools > Real Time Session Monitoring
	User Activity Log	Administrator having this privilege can view SSM and File Watcher text and video logs.	Server Manager > Manage > Logs > User Activity Log
	View Envelope Log	Administrators having this privilege can view the print password envelope logs	Server Manager > Manage > Logs > Process Logs
Manage Group	Add Group	Administrator having this privilege can create User and Server groups.	Server Manager > Manage > User and Services > Manage Groups
	Modify Group	Administrator having this privilege can modify User and Server groups.	Server Manager > Manage > User and Services > Manage Groups
	Drop Group	Administrator having this privilege can delete a User and Server groups.	Server Manager > Manage > User and Services > Manage Groups
	Assign Service Group To User Group	Administrator having this privilege can perform User to Service group mapping.	Server Manager > Manage > User and Services > Map Group Types
	Revoke Service Group From User Group	Administrator having this privilege can revoke User to Service group mapping.	Server Manager > Manage > User and Services > Map Group Types
	Read Only Access	Administrator having this privilege can view details displayed under Manage Groups, Manage Groups/Services and Manage Groups/Users.	Server Manager > Manage > User and Services > Manage Groups (or Manage Groups/Services or Manage Groups/Users)
Manage LOB / Profile	Add New LOB	Administrator having this privilege can create new LOB and view all the LOB's in Select LOB/ Profile dropdown in Server Manager Home Page.	Server Manager > Manage > LOB/Profile Master & Manager > Manage LOB

ARCON PAM Server Privilege		Description	Feature Navigation
	Modify LOB	Administrator having this privilege can modify LOB name, description, address and Report Header of existing LOB.	Server Manager > Manage > LOB/Profile Master & Manager > Manage LOB
	Assign LOB To Service Group	Administrator having this privilege can map Service Group to a particular LOB.	Server Manager > Manage > LOB/Profile Master & Manager > Map LOB / Service Groups
	Revoke LOB From Service Group	Administrator having this privilege can remove service groups from a particular LOB.	Server Manager > Manage > LOB/Profile Master & Manager > Map LOB / Service Groups
	Assign LOB To User Group	Administrator having this privilege can map User Group to LOB.	Server Manager > Manage > LOB/Profile Master & Manager > Map LOB / User Groups
	Revoke LOB From User Group	Administrator having this privilege can remove user groups from a particular LOB.	Server Manager > Manage > LOB/Profile Master & Manager > Map LOB / User Groups
	Assign LOB To Service	Administrator having this privilege can map Services to a particular LOB.	Server Manager > Manage > LOB/Profile Master & Manager > Map LOB / Services
	Revoke LOB From Service	Administrator having this privilege can remove services from a particular LOB.	Server Manager > Manage > LOB/Profile Master & Manager > Map LOB / Services
	Assign LOB To User	Administrator having this privilege can map Users to a particular LOB.	Server Manager > Manage > LOB/Profile Master & Manager > Map LOB / Users
	Revoke LOB From User	Administrator having this privilege can remove users from a particular LOB.	Server Manager > Manage > LOB/Profile Master & Manager > Map LOB / Users
Manage Services	Modify Service Type	Administrator having this privilege can select service types to be displayed in ARCON PAM.	Server Manager > Manage > Modify Service Type

ARCON PAM Server Privilege		Description	Feature Navigation
	Add Service	Administrator having this privilege can create services.	Server Manager > Manage > User and Services > Manage Services
	Modify Service	Administrator having this privilege can modify services.	Server Manager > Manage > User and Services > Manage Services
	Drop Service	Administrator having this privilege can disable or delete services.	Server Manager > Manage > User and Services > Manage Services
	Assign Service To Service Group	Administrator having this privilege can map services to a particular Service Group.	Server Manager > Manage > User and Services > Map Groups/ Services
	Revoke Service From Service Group	Administrator having this privilege can remove services mapped to Service Group.	Server Manager > Manage > User and Services > Map Groups/ Services
	Assign Service To User	Administrator having this privilege can map Services to a particular User.	Server Manager > Manage > User and Services > Map Users/ Services
	Revoke Service From User	Administrator having this privilege can remove Services from a particular User.	Server Manager > Manage > User and Services > Map Users/ Services
	Windows Connection Service	Administrator having this privilege can add ARCON PAM Windows service to a service created in ARCON PAM, so if the password is changed for a particular service with Password Manager then the password of the dependent service is also changed.	Server Manager > Manage > Windows Connection Password Dependency > Windows Services
	Windows Connection DCOM	Administrator having this privilege can add DCOM service to a service created in ARCON PAM, so if the password is changed for a particular service with Password Manager then the password of the DCOM service is also changed.	Server Manager > Manage > Windows Connection Password Dependency > Windows DCOM

ARCON PAM Server Privilege		Description	Feature Navigation
	Windows Connection Task	Administrator having this privilege can add Windows service to a service created in ARCON PAM, so if the password is changed for a particular service with Password Manager then the password of the dependent task is also changed.	Server Manager > Manage > Windows Connection Password Dependency > Windows Task
	Read Only Access	Administrator having this privilege can view details displayed under Manage Services and Map Groups/Services tab.	Server Manager > Manage > User and Services > Manage Services (or Manage Groups/Services)
	Bulk /update Services	Administrators having this privilege can perform a bulk update of services	Server Manager Manage → Users and Services → Manage Services
Manage Tab	ARCON PAM Workflow Tracker	Administrator having this privilege can view workflow approval matrix logs, user request approval overriding workflow logs and ticket request workflow logs.	Server Manager > Manage > ARCON PAM Workflow Tracker
Manage User	Add User	Administrator having this privilege can create Users.	Server Manager > Manage > User and Services > Manage Users
	Modify User	Administrator having this privilege can modify User details.	Server Manager > Manage > User and Services > Manage Users
	Drop User	Administrator having this privilege can disable a User.	Server Manager > Manage > User and Services > Manage Users
	Assign User Group	Administrator having this privilege can map Users to a particular User Group.	Server Manager > Manage > User and Services > Map Groups/ Users
	Revoke User Group	Administrator having this privilege can remove Users mapped to User Groups.	Server Manager > Manage > User and Services > Map Groups/ Users
	Admin Privileges	Administrator having this privilege can edit privileges.	Server Manager > Manage > User and Services > Manage Users > Edit privileges
	Approve User (Checker)	Administrator having this privilege can approve or reject newly created Users.	Server Manager > Manage > Maker's Checker

ARCON PAM Server Privilege		Description	Feature Navigation
	Change User Restricted Commands	Administrator having this privilege can configure restricted commands, add critical commands for approval, apply Configuration Commands, Blacklist profile and Elevate profile to User and Service mapping.	Server Manager > Manage > User and Services > Manage Commands And Server Manager > Manage > User and Services > Manage Processes
	User Access Review Manager	Administrator having this privilege can configure User Access Review.	Server Manager > Tools > User Access Review
	Copy User Profile	Administrator having this privilege can copy entities such as LOB, User Group, Services, Commands or Processes assigned to one User to another User.	Server Manager > Manage > User and Services > Manage Users > Copy User Profile
	Read Only Access	Administrator having this privilege can view details displayed under Manage Users and Map Groups/Users tab.	Server Manager > Manage > User and Services > Manage Users (or Manage Groups/ Users)
	Receive Alert On User Creation By Maker	Administrator having this privilege along with Approve User (Checker) privilege will receive alert when Maker creates new User.	Server Manager > Manage > Maker's Checker
	Edit User Settings	The Administrator having this privilege shall only be able to edit User settings.	Server Manager > Manage > User and Services > Manage Users > Edit User Settings
Password Manager	Change Password	Administrator having this privilege can change password of a service.	Server Manager > Manage > Password Manager > Password Change And Server Manager > Manage > User and Services > Manage Services > Change Password Manually
	View Server Password	Administrator having this privilege can view password of a service.	Server Manager > Manage > User and Services > Manage Services > View Password

ARCON PAM Server Privilege		Description	Feature Navigation
	Generate Server Password Envelope	Administrator having this privilege can print password envelopes with Envelope Status as Generated.	Server Manager > Manage > Password Manager > Print Password Envelope
	Print Server Password Envelope	Administrator having this privilege can print password envelope in PDF or Pin Mailer format.	Server Manager > Manage > Password Manager > Print Password Envelope > Print Envelope(s)
	Reprint Server Password Envelope	Administrator having this privilege can print password envelopes with Envelope Status as Printed, First Reprint, Second Reprint, Third Reprint, Fourth Reprint, Fifth Reprint, Sixth Reprint, Seventh Reprint, Eighth Reprint, Ninth Reprint and Tenth Reprint.	Server Manager > Manage > Password Manager > Print Password Envelope > Print Envelope(s) And Server Manager > Manage > Password Manager > Print Password Envelope > Password Envelope(s) For APEM Tool
	Verify Reprint Server Password Envelope	Administrator having this privilege will be displayed as approver in dropdown list to authenticate password printing process.	Server Manager > Manage > Password Manager > Print Password Envelope > Print Envelope(s) And Server Manager > Manage > Password Manager > Print Password Envelope > Password Envelope(s) For APEM Tool
	Change Password Policy	Administrator having this privilege can set constraints for a password policy.	Server Manager > Manage > Password Manager > Password Policy Editor
	Show Password Change History	Administrator having this privilege can view the detailed history of the changed passwords for a service.	Server Manager > Manage > User and Services > Manage Commands > Manage Services > Show Password Change History

ARCON PAM Server Privilege		Description	Feature Navigation
	Password Change Process Approver	Administrator having this privilege can authorize password change process.	Server Manager > Manage > Password Manager > Password Change
	Windows Connection Password Dependency	Administrator having this privilege can map all the different Windows Services, Windows DCOM, and Windows Task that are depended on any service of a particular server.	Server Manager > Manage > Windows Connection Password Dependency
Tools Tab	Windows Utility	Administrator having this privilege can view version of ARCON PAM PWD service.	Server Manager > Tools > Windows Utility
	Import	Administrator having this privilege can import Users and Services in ARCON PAM database.	Server Manager > Tools > Import
	Password Reconciliation	Administrator having this privilege can compare entries in ARCON PAM repository and the target system.	Server Manager > Tools > Password Reconciliation
	ARCON PAM Object Counter	Administrator having this privilege can view and monitor different entities in ARCON PAM.	Server Manager > Tools > ARCON PAM Object Counter
	Privileged User Discovery & Reconciliation	Administrator having this privilege can view Users created on Server.	Server Manager > Tools > Privileged User Discovery & Reconciliation
HSM Device Configuration	HSM Device Configuration	Administrators having this privilege can configure HSM Devices in ARCON PAM	Server Manager > Tools > Advanced configuration > HSM Device Configuration

5.3 Client Manager's Privileges

ARCON PAM Client Manager's Privileges are assigned to Client or Admin type of Users to grant special rights for accessing reports, dashboard, logs and other applications. Client Manager privileges include API User Registration, ARCOS Applications, ARCOS Dashboard, ARCOS Delegation, ARCOS File Vault, Client Manager Log, Manager LOB/ Profile, PAM Menu, Password Manager, Report - Dashboard, Report - Group Reports, Report - LOB Reports, Report - Logs, Report - Performance Reports, Report - Privilege Reports, Report - Security Reports, Report - Service Reports, Report - User Reports, Report - Vault Reports and Script Manager.

Following are the list of Client Manager Privileges:

ARCON PAM Client Manager Privileges		Description	Feature Navigation
API User Registration	API User Registration	User having this privilege can register Users to login into API hosted in Client's environment.	Client Manager > Manager > Application Setting

ARCON PAM Client Manager Privileges		Description	Feature Navigation
ARCON PAM Applications	Privilege Elevation & Delegation Management	User having this privilege can configure processes to be restricted / elevated. This is an application which requires separate implementation. ⓘ Contact ARCON Team to implement and enable PEDM.	Client Manager > Manager > PEDMx`
	Smart Session Monitoring	User having this privilege can configure IP Address to monitor files and and log user activities using File Watcher and Smart Session Monitoring. ⓘ Contact ARCON Team to implement and enable Smart Session Monitoring.	Client Manager > Manager > Smart Session Monitoring
	File Vault	User having this privilege will be able to upload, download, view, or delete files in vault.	Client Manager > My Access > Preferences > My Vault
	AD Bridging	Users having this privilege will be able to view the AD Bridging App in ACMO	Client Manager > Manager
	Reporting Portal	Users having this privilege will only be able to view the reporting portal in ACMO	Client Manager > Manager
	User Governance Portal	User having this privilege will only be able to view and access User Governance Portal	
	Remote Assist	Users having this privilege will only be able to take remote sessions through Remote Assist	Client Manager > Manager
	Auto- On boarding	The Administrator/ User having this privilege will only be able to auto onboard and deboard Users and Services from ARCON PAM.	Client Manager > Manager
	PAM Logs	Users having this privilege will only be able to view the PAM Logs in ACMO	Client Manager > Manager
	ARCON Terminal Server	Users having this privilege will only be able to view and use ARCON Terminal Server.	Client Manager > Manager

ARCON PAM Client Manager Privileges		Description	Feature Navigation
ARCON PAM Configuration	Client Manager Privileges- View All LOB	Users having this privilege can view ALL LOB Option.	Client Manager > Reports, Settings > Scheduler >Schedule Reports, Client Manager > Reports > Dashboard, Client Manager > Dashboard
ARCON PAM Dashboard	Dashboard	User having this privilege can view useful graphical information about the various actions performed in ARCON PAM and can view pinned reports.	Client Manager > Dashboard
ARCON PAM Delegation	Delegation	User having this privilege can delegate his Service Access, Service Password or Service Ticket approval rights to another User.	Client Manager > My Access > Preferences > Delegation
Client Manager Log	View Server Access Log	User having this privilege will be able to view details of activity performed by User on services.	Client Manager > Manager > Access Logs
	View Server Access Log Details	User having this privilege will be able to view details of activity performed by User on services through video log.	Client Manager > Manager > Access Logs > Details
Manager LOB/ Profile	View Service Access Logs With Details	User having this privilege will be able to view various activities performed by him on services through video log.	Client Manager > My Access > My Activity
PAM Menu	Manager Menu Display	Client Users having this privilege will only be able to view Manager menu in Client Manager.	Client Manager > Manager
Password Manager	Support View Server Password	Administrator having this privilege along with Password Change Process Approver privilege (Server's Privileges) and Group Admin Privileges can authorize password change process as Authorising User 2. And Administrator having this privilege can authorize password view process as Authorizing User 2.	Server Manager > Manage > Password Manager > Password Change And Server Manager > Manage > Users and Services > Manage Services > View Password

ARCON PAM Client Manager Privileges		Description	Feature Navigation
Report - Dashboard	ARCOS Live	User having this privilege will be able to view the count and details of Users logging into the application, the servers accessed by the Users, critical and restricted commands fired by the Users.	Client Manager > Reports > Dashboard > ARCOS Live
	ARCOS PerfMonIT	User having this privilege will be able to view the percentage of CPU, RAM, and Disk Utilization of Application Server, Vault Server, and Gateway Server in ARCON PAM and the status of all the services installed on these Servers.	Client Manager > Reports > Dashboard > ARCOS PerfMonIT
	Enterprise Password	User having this privilege will be able to view Password Rotation Frequency, Password Policy Compliance Status, Password Security Status, Password Change Success- Failure Rate and Upcoming Password Review.	Client Manager > Reports > Dashboard > Enterprise Password
	Live Server Sessions	User having this privilege will be able to view list of live sessions taken through ARCON PAM.	Client Manager > Reports > Dashboard > Live Server Sessions
	User Access & Usage	User having this privilege will be able to view the count of number of times critical servers have been accessed, the same displayed in time-based manner and service-type wise, and the servers which are highly accessed.	Client Manager > Reports > Dashboard > User Access & Usage
Report - Group Reports	Servers In Server Group	User having this privilege will be able to view details of all the servers created in a Server Group irrespective of the LOB's. The details displayed in this report are based on IP Address of Server.	Client Manager > Reports > Group Reports > Servers In Server Group
	Service Group Report	User having this privilege will be able to view all the service groups created in ARCON PAM.	Client Manager > Reports > Group Reports > Service Group Report
	Services In Server Group	User having this privilege will be able to view details of all the services created in a Server Group irrespective of the LOB's. The details displayed in this report are based on Service Username of Server.	Client Manager > Reports > Group Reports > Services In Server Group

ARCON PAM Client Manager Privileges		Description	Feature Navigation
	User Group Report	User having this privilege will be able to view all the User Groups created in ARCON PAM.	Client Manager > Reports > Group Reports > User Group Report
	Users In User Group	User having this privilege will be able to view details of all the Users created in a User Group irrespective of the LOB's.	Client Manager > Reports > Group Reports > Users In User Group
Report - LOB Reports	Active Services Group Wise Report	User having this privilege will be able to view active services under a particular Service Group.	Client Manager > Reports > LOB Reports > Active Services Group Wise Report
	Service Count Report	User having this privilege will be able to view graphical representation of LOB wise status of unique IP address and services and status of Services LOB wise.	Client Manager > Reports > LOB Reports > Service Count Report
	Object Status Report	User having this privilege will be able to view graphical representation of LOB wise mapping of object and status of Users and Services LOB wise.	Client Manager > Reports > LOB Reports > Object Status Report
	Active Services Report	User having this privilege will be able to view details of all servers LOB wise which are active in ARCON PAM.	Client Manager > Reports > LOB Reports > Active Services Report
	Active Users Report	User having this privilege will be able to view details of all Users LOB wise who are active in ARCON PAM.	Client Manager > Reports > LOB Reports > Active Users Report
	Inactive Services Report	User having this privilege will be able to view details of all servers, which are inactive in ARCON PAM.	Client Manager > Reports > LOB Reports > Inactive Services Report
	LOB Details Report	User having this privilege will be able to view detailed description of all the LOB created in ARCON PAM	Client Manager > Reports > LOB Reports > LOB Details Report
Report - Logs	Service Request Workflow Logs	User having this privilege will be able to view details of all the service access requests raised by Users.	Client Manager > Reports > Logs > Service Request Workflow Logs

ARCON PAM Client Manager Privileges		Description	Feature Navigation
	Ticket Request Workflow Logs	User having this privilege will be able to view details of all the ticket request raised by Users in a LOB.	Client Manager > Reports > Logs > Ticket Request Workflow Logs
	Log Review Report	User having this privilege will be able to view details of all the Users who have accessed or viewed the logs generated in ARCON PAM.	Client Manager > Reports > Logs > Log Review Report
	Approval Delegation Report	User having this privilege will be able to view logs of delegation passed to/by, based on any particular LOB.	Client Manager > Reports > Logs > Approval Delegation Report
	Service Access Log	User having this privilege will be able to view details of all the services accessed by the Users.	Client Manager > Reports > Logs > Service Access Log
	Session Activity Log	User having this privilege will be able to view the reason why the current User switched to another User in on-going session.	Client Manager > Reports > Logs > Session Activity Log
	User Access Review Processes	User having this privilege will be able to view details of User access review processes.	Client Manager > Reports > Logs >User Access Review Processes
	Service Password Request Workflow Logs	User having this privilege will be able to view details of all the service password requests raised by Users.	Client Manager > Reports > Logs > Service Password Request Workflow Logs
	Day Wise Summary Report	User having this privilege will be able to view date and time wise count of activities performed on Server.	Client Manager > Reports > Logs > Day Wise Summary Report
	Session Wise Summary Report	User having this privilege will be able to view session wise count of activities performed on Server along with details of service. It displays details such as count of image logs, critical commands executed on Server, and restricted commands and restricted processes attempted to execute on Server.	Client Manager > Reports > Logs > Session Wise Summary Report

ARCON PAM Client Manager Privileges		Description	Feature Navigation
	My Vault Logs	User having this privilege will view list of all the activities performed in the File Vault. It displays details such as filename, extension, size, status, added by, addedon, sharedon, shared with, File Available till, Deleted by, Deleted on and Recorded on.	Client Manager > Reports > Logs > My Vault Logs
	SIEM Command Logs Report	User having this privilege will help you to view command logs fetched from SIEM service. It displays logs of commands executed on Linux service.	Client Manager > Reports > Logs > SIEM Command Logs Report
	APEM Logs	User having this privilege will help you to view logs of actions performed via APEM tool. Actions such as opening APEM application, reading file, and viewing password are captured in APEM logs.	Client Manager > Reports > Logs > APEM Logs
Report - Performance Reports	New ARCON DeskInsight Devices	User having this privilege will be able to view details of desktops integrated in ARCON PAM.	Client Manager > Reports > Performance Reports > New ARCON DeskInsight Devices
	MS SQL Connection Report	User having this privilege will be able to view details of all the Users connected to the MS SQL (Microsoft Sequel) instance on ARCON PAM database server.	Client Manager > Reports > Performance Reports > MS SQL Connection Report
Report - Privilege Reports	Client Manager Privilege Report	User having this privilege will be able to view count of client manager privileges and the privileges assigned to Users.	Client Manager > Reports > Privilege Reports > Client Manager Privilege Report
	Group Admin Privilege Report	User having this privilege will be able to view count of group admin privileges and the privileges assigned to Admin Users.	Client Manager > Reports > Privilege Reports > Group Admin Privilege Report
	Server Manager Privilege Report	User having this privilege will be able to view count of server manager privileges and the privileges assigned to Admin Users.	Client Manager > Reports > Privilege Reports > Server Manager Privilege Report

ARCON PAM Client Manager Privileges		Description	Feature Navigation
	User & Service Privileges - Windows RDP	User having this privilege will be able to view count of command privileges and list of privileges assigned to Client or Admin Users, which are mapped to Windows RDP (Remote Desktop Protocol) service type.	Client Manager > Reports > Privilege Reports > User & Service Privileges - Windows RDP
Report - Security Reports	Critical Commands Executed Report	User having this privilege will be able to view details of all the critical commands executed on servers.	Client Manager > Reports > Security Reports > Critical Commands Executed Report
	Restricted Commands Executed Report	User having this privilege will be able to view details of all the restricted commands executed by User.	Client Manager > Reports > Security Reports > Restricted Commands Executed Report
	High Usage (in hrs) Services Report	User having this privilege will be able to view count of services which are highly accessed.	Client Manager > Reports > Security Reports > High Usage (in hrs) Services Report
	Invalid Login Attempts Report	User having this privilege will be able to view count/number of invalid login attempts made by user.	Client Manager > Reports > Security Reports > Invalid Login Attempts Report
	Low Usage (in days) Services Report	User having this privilege will be able to view count/number of servers which are accessed rarely.	Client Manager > Reports > Security Reports > Low Usage (in days) Services Report
	Multiple Desktop Logon Report	User having this privilege will be able to view details of desktop IP used by Users to login in to ARCON PAM.	Client Manager > Reports > Security Reports > Multiple Desktop Logon Report
	Multiple User Logon Report	User having this privilege will be able to view details of Users who have logged into ARCON PAM from different IP/desktops.	Client Manager > Reports > Security Reports > Multiple User Logon Report
	Network Segment Wise Logon Report	User having this privilege will be able to view details of all the Users who have logged into ARCON PAM through any network device configured in Network Segments in Default Configuration.	Client Manager > Reports > Security Reports > Network Segment Wise Logon Report

ARCON PAM Client Manager Privileges		Description	Feature Navigation
	Service Accessed - Multiple Times Report	User having this privilege will be able to view details of services accessed multiple times by User.	Client Manager > Reports > Security Reports > Service Accessed - Multiple Times Report
	User Service Accessed - Multiple Times Report	User having this privilege will be able to view number of times User has accessed services between defined range.	Client Manager > Reports > Security Reports > User Service Accessed - Multiple Times Report
Report - Service Reports	Multiple Service Reference No. Report	User having this privilege will be able to view details of reference number provided by the User before accessing any Service.	Client Manager > Reports > Service Reports > Multiple Service Reference No. Report
	Unique Services IP Address Report	User having this privilege will be able to view details of all the Services having unique IP addresses.	Client Manager > Reports > Service Reports > Unique Services IP Address Report
	Active Services Report	User having this privilege will be able to view details of services that are active in ARCON PAM, irrespective of the LOB's.	Client Manager > Reports > Service Reports > Active Services Report
	Service Accessed Summary Report	User having this privilege will be able to view monthly summary report of all the services that are accessed by the User.	Client Manager > Reports > Service Reports > Service Accessed Summary Report
	Active Sessions Report	User having this privilege will be able to view details of all the service sessions that are currently active in ARCON PAM.	Client Manager > Reports > Service Reports > Active Sessions Report
	Scheduled Password Change Services	User having this privilege will be able to view details of all the services that are scheduled for password change process.	Client Manager > Reports > Service Reports > Scheduled Password Change Services
	Service Accessed Summary Days Wise Report	User having this privilege will be able to view total count of the services accessed on daily basis.	Client Manager > Reports > Service Reports > Service Accessed Summary Days Wise Report

ARCON PAM Client Manager Privileges		Description	Feature Navigation
	Password Envelope Print Report	User having this privilege will be able to view details of Users who have printed password envelope and those who have verified the process.	Client Manager > Reports > Service Reports > Password Envelope Print Report
	Service Dependency Report	User having this privilege will be able to view details of all the services that have dependent services.	Client Manager > Reports > Service Reports > Service Dependency Report
	Servers in Domain	User having this privilege will be able to view details of all the servers in a domain irrespective of the LOB's. The details displayed in this report are based on IP Address of Server.	Client Manager > Reports > Service Reports > Servers in Domain
	Services in Domain	User having this privilege will be able to view details of all the services in a domain irrespective of the LOB's. The details displayed in this report are based on Service Username.	Client Manager > Reports > Service Reports > Services in Domain
	Service Group wise Service Type Report	User having this privilege will be able to view Service Types of Services assigned to Service Group.	Client Manager > Reports > Service Reports > Service Group wise Service Type Report
	Service Creation Deletion Summary Report		
	Service Timeline Report		
	Service Creation Deletion Details Report		

ARCON PAM Client Manager Privileges		Description	Feature Navigation
Report - User Reports	Idle Users Report	User having this privilege will be able to view details of all the users who are idle for the selected LOB.	Client Manager > Reports > User Reports > Idle Users Report
	User & Service Mapping Report	User having this privilege will be able to view LOB wise User and Service mapping details.	Client Manager > Reports > User Reports > User & Service Mapping Report
	User Last Logon Report	User having this privilege will be able to view User's last logon details into ARCON PAM application.	Client Manager > Reports > User Reports > User Last Logon Report
	User Biometric Auth Report	User having this privilege will be able to view details of Users who have configured only the bio-metric authorization to make the login process more secure.	Client Manager > Reports > User Reports > User Biometric Auth Report
	User Biometric Auth Report - All LOB		
	User Mobile OTP Auth Report	User having this privilege will be able to view details of Users who have configured mobile authorization, to make the login process more secure.	Client Manager > Reports > User Reports > User Mobile OTP Auth Report
	User Hardware Auth Report	User having this privilege will be able to view details of the Users who have configured Hardware Token authorization, to make the login process more secure.	Client Manager > Reports > User Reports > User Hardware Auth Report
	User SMS OTP Auth Report	User having this privilege will be able to view details of the Users who have configured SMS OTP authorization, to make the login process more secure.	Client Manager > Reports > User Reports > User SMS OTP Auth Report
	Active Users Report	User having this privilege will be able to view details of all Users who are active in ARCON PAM irrespective of the LOB's.	Client Manager > Reports > User Reports > Active Users Report
	Inactive Users Report	User having this privilege will be able to view details of all Users who are inactive in ARCON PAM irrespective of the LOB's.	Client Manager > Reports > User Reports > Inactive Users Report

ARCON PAM Client Manager Privileges		Description	Feature Navigation
	Dual Factor Auth Configuration Report	User having this privilege will be able to view details of Users who have configured the dual factor authorization to make the login process more secure.	Client Manager > Reports > User Reports > Dual Factor Auth Configuration Report
	Locked Out User Report	User having this privilege will be able to view details of Users who have tried to login using invalid password and exceeded the value configured in lockout attempts in Application Configuration (Default Configuration).	Client Manager > Reports > User Reports > Locked Out User Report
	Dormant User Report	User having this privilege will be able to view details of Users who have not used their account for the configured number of dormancy days in Application Configuration (Default Configuration).	Client Manager > Reports > User Reports > Dormant User Report
	Last Service Accessed Report	User having this privilege will be able to view details of last service accessed by users.	Client Manager > Reports > User Reports > Last Service Accessed Report
	Consolidated User & Service Mapping Report	User having this privilege will be able to view total count of all the services mapped to users.	Client Manager > Reports > User Reports > Consolidated User & Service Mapping Report
	User Dormant in next 5 day Report	User having this privilege will be able to view details of Users whose account will be dormant in next 5 days.	Client Manager > Reports > User Reports > User Dormant in next 5 day Report
	User Creation Deletion Summary Report		
Report - Vault Reports	Service Password Envelope Print Status Report	User having this privilege will be able to view details of all the services for which the password envelope has been generated.	Client Manager > Reports > Vault Reports > Service Password Envelope Print Status Report
	Restore Service Password Option Used	User having this privilege will be able to view the list of users who used the Restore Service Password option.	Client Manager > Reports > Vault Reports > Restore Service Password Option Used

ARCON PAM Client Manager Privileges		Description	Feature Navigation
	Service Password Age Report	User having this privilege will be able to view the age of the service password i.e. for the number of days the password of the service is active in ARCON PAM.	Client Manager > Reports > Vault Reports > Service Password Age Report
	Service Password Change Failed (Server Unavailable) Report	User having this privilege will be able to view details of all the services whose password change has failed due to server downtime.	Client Manager > Reports > Vault Reports > Service Password Change Failed (Server Unavailable) Report
	Service Password Changed Status Report	User having this privilege will be able to view details of all the services whose password have been successfully changed since the service was created.	Client Manager > Reports > Vault Reports > Service Password Changed Status Report
	Service Password Expires In 5 Days Report	User having this privilege will be able to view details of those services whose passwords will be expired in 5 days.	Client Manager > Reports > Vault Reports > Service Password Expires In 5 Days Report
	Service Password Manually Changed Report	User having this privilege will be able to view details of all the services whose password are changed manually.	Client Manager > Reports > Vault Reports > Service Password Manually Changed Report
	Service Password Never Changed Report	User having this privilege will be able to view details of all the services whose passwords are never changed both manually or through password change process.	Client Manager > Reports > Vault Reports > Service Password Never Changed Report
	Service Password Check Out Report	User having this privilege will be able to view details of the Users requested to view the service password for a desired number of hours.	Client Manager > Reports > Vault Reports > Service Password Check Out Report
	Service Password Changed Success-Failed Report	User having this privilege will be able to view password change status for the services.	Client Manager > Reports > Vault Reports > Service Password Changed Success-Failed Report

ARCON PAM Client Manager Privileges		Description	Feature Navigation
	Service Password Security Status	User having this privilege will be able to view details of all the services whose password are in open or closed state.	Client Manager > Reports > Vault Reports > Service Password Security Status
	Service Password Vaulting Summary Report	User having this privilege will be able to view the LOB wise summary of all the services whose password have been changed.	Client Manager > Reports > Vault Reports > Service Password Vaulting Summary Report
	Current Password Status Report	User having this privilege will be able to view current status of service password and other password change details.	Client Manager > Reports > Vault Reports > Current Password Status Report
	SPC not Configured Report	User having this privilege will be able to view details of services for whom SPC has not been configured.	Client Manager > Reports > Vault Reports > SPC not Configured Report
	SPC Success and Failed Report	User having this privilege will be able to view details of service password change through SPC service.	Client Manager > Reports > Vault Reports > SPC Success and Failed Report
	Users Extracting Password Envelope	User having this privilege will be able to view details of Users, who have printed Password Envelopes.	Client Manager > Reports > Vault Reports > Users Extracting Password Envelope
	Service Password Enevelope Print Status Report		
	Service Reconcile Status Report		
	Mobile OTP Auth Status Report		
	Services Scheduled for SPC		
	Users Extracting Password Envelope		

ARCON PAM Client Manager Privileges		Description	Feature Navigation
	Service Password Never Changed Report - All LOB		
	Service Password Changed Status Report - All LOB		
Notifications_Service	Service Password Change Scheduled	Users having this privilege will be notified prior to the configured number of days in Settings Service Password Change Scheduled Days (number of days). For example, if the configured value is set to 5, then User will be notified 5 days prior to password expiry.	Client Manager > Notifications
	Service Expiry Due	Users having this privilege will be notified prior to the configured number of days in **Settings Service Expiry Days** (number of days). For example, if the configured value is set to 5, then User will be notified 5 days prior to service expiry.	Client Manager > Notifications
Script Manager	Create New Script	User having this privilege will be able to create a new script.	Client Manager > Manager > Script Manager > Add New Script
	Edit Script	User having this privilege will be able to edit an existing script.	Client Manager > Manager > Script Manager > Edit Script
	Run Script	User having this privilege will be able to run a script.	Client Manager > Manager > Script Manager > Run Script
About	Edit Contact	Users having this privilege Edit/Add contact details on the ACMO about page.	Client Manager > About

5.4 Group Admin Privileges

ARCON PAM Group Admin Privileges are assigned to Server Group Admins to grant special rights for assigning services, viewing logs and review User access. Group Admin privileges include Group Log Viewer, Manage Services and Manage User Request.

Following are the list of Client Manager Privileges:

ARCON PAM Group Admin Privileges		Description	Feature Navigation
Group Log Viewer	View Command Log	Group Admin having this privilege can view Command Logs and Process Logs. ⚠ You should also be assigned View Command Log and View Process Log privileges under Server's Privileges.	Server Manager > Manage > Logs > Command Logs And Server Manager > Manage > Logs > Process Logs
	View Service Log	Group Admin having this privilege can view Service Logs. ⚠ You should also be assigned View Service Log privilege under Server's Privileges.	Server Manager > Manage > Logs > Service Logs
Manage Services	Assign Service To User	Group Admin having this privilege can map Services to a particular User.	Server Manager > Manage > User and Services > Map Users/ Services And Server Manager > Manage > User and Services > Group Admin - Map Services
	Revoke Service From User	Group Admin having this privilege can remove Services from a particular User.	Server Manager > Manage > User and Services > Map Users/ Services And Server Manager > Manage > User and Services > Group Admin - Map Services
	Change User Restricted Command	Group Admin having this privilege can configure restricted commands, add critical commands for approval, apply Configuration Commands to User and Service mapping.	Server Manager > Manage > User and Services > Manage Commands

ARCON PAM Group Admin Privileges		Description	Feature Navigation
	Change Password	Group Admin having this privilege can change password of a service. ⚠ Group Admin shall be assigned **Change Password** privilege only if the toggle value for **Only Server Group Admin Can Perform Password Change - Is Enabled** is **Enbaled** in Settings.	Server Manager > Manage > Password Manager > Password Change And Server Manager > Manage > User and Services > Manage Services > Change Password Manually
Manage User Request	Service Access Approver	Group Admin having this privilege can approve Service Access Request. ⚠ The requested service access should be assigned to Approver.	Workflow Manager And Client Manager > Server Manager > Service Access Request
	User Access Reviewer	Group Admin having this privilege can review the services mapped to User.	Server Manager > Tools > User Access Review

6 Command Profiler

6.1 Overview

Command Profiler is used to restrict or elevate processes or commands. You can assign commands with **Critical With Approval** property, wherein an email notification will be sent to the Approver for approval. Once approved, the command will be allowed for execution. This feature is used by Administrator who is responsible for keeping a track of unwanted or critical commands or processes that should/should not be executed by the user on the server. Multiple profiles can be created for each service type.

Following are the two types of profiles created: Blacklist and Elevate

- **Blacklist:** Blacklist is a method for adding processes or commands that are required to be blocked.
- **Elevate:** Elevate is a method to allow the user to execute certain processes.

Also new processes or commands can be added to the existing set of processes and commands. In addition, you can modify and delete a command profiler. To Blacklist or Elevate the processes or commands for the service type the Administrator has to check the checkbox beside the processes or commands listed.

⚠

- For Windows Services we can use blacklist and elevate as profile type whereas, for Linux services only blacklist profile type can be used.
- The Administrator having **Command Profiler** privilege will only be able to create, modify, or delete multiple profiles. The Administrator can also create, delete commands or restrict commands and processes available for User.

6.2 Manage Commands

6.2.1 Overview

This section helps you to restrict commands. In addition, the critical commands can also be sent for approval based on the configuration done in the Workflow Approval Matrix. On authorizing, the User will be able to execute the command. If the Approver has rejected the request, then the command will not be allowed for execution. You can restrict commands or add critical commands for approval under **Manage Commands** tab.

Restricting commands will disallow the user from further usage of the commands. Adding critical commands for approval will disallow user from executing critical command until approved.

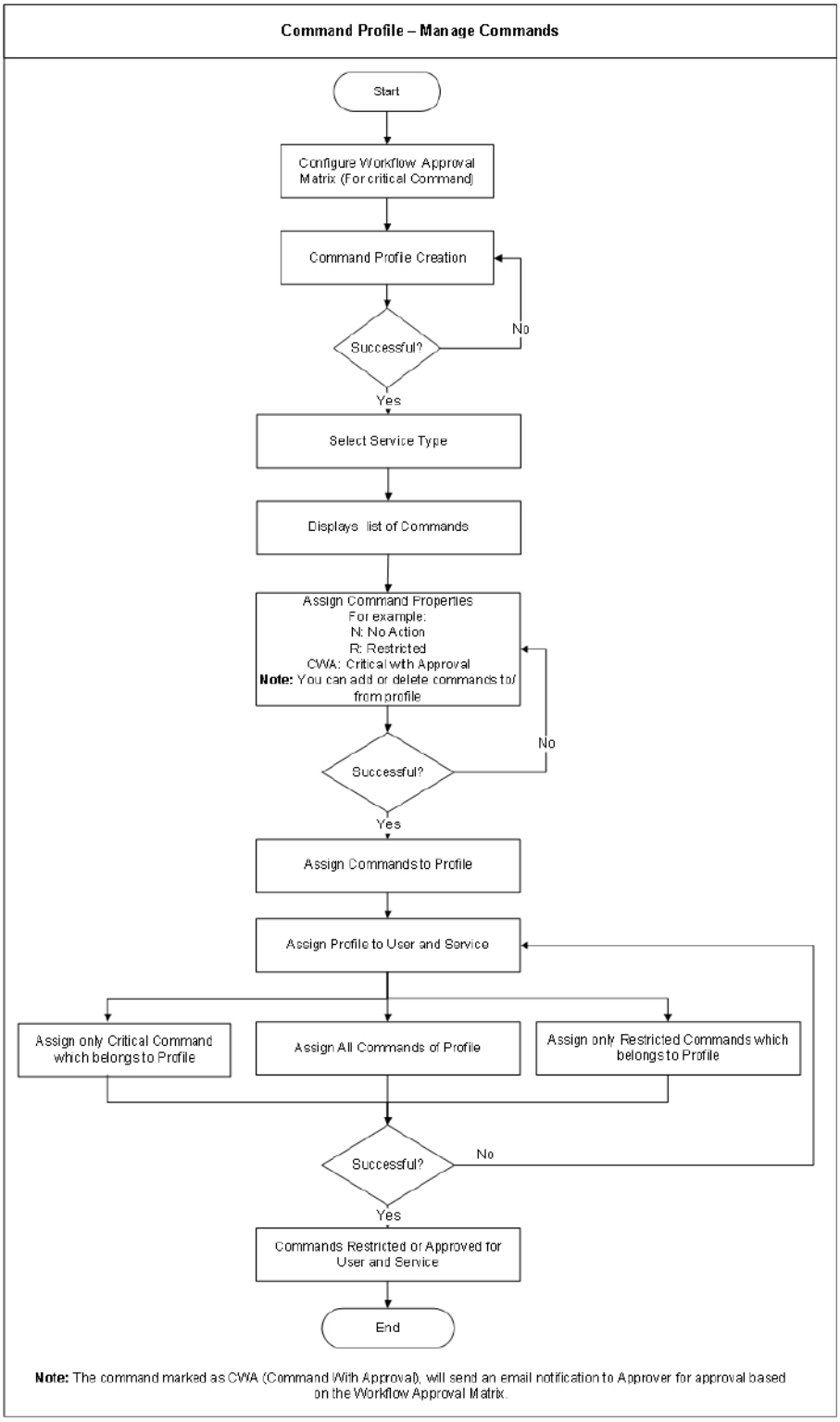
⚠

- The **Administrator** having **Change User Restricted Commands** privilege in **Server's Privileges** shall only be able to configure restricted commands, add critical commands for approval and apply Configuration Commands to User and Service mapping.
- The **Server Group Admin** having **Change User Restricted Command privilege** in **Group Admin Privileges**, shall only be able to configure restricted commands, add critical commands for approval and apply Configuration Commands to User and Service mapping.

To manage commands, follow the below steps:

1. Configure Workflow Approval Matrix
2. Create Command Profile
3. Assign Profile To User

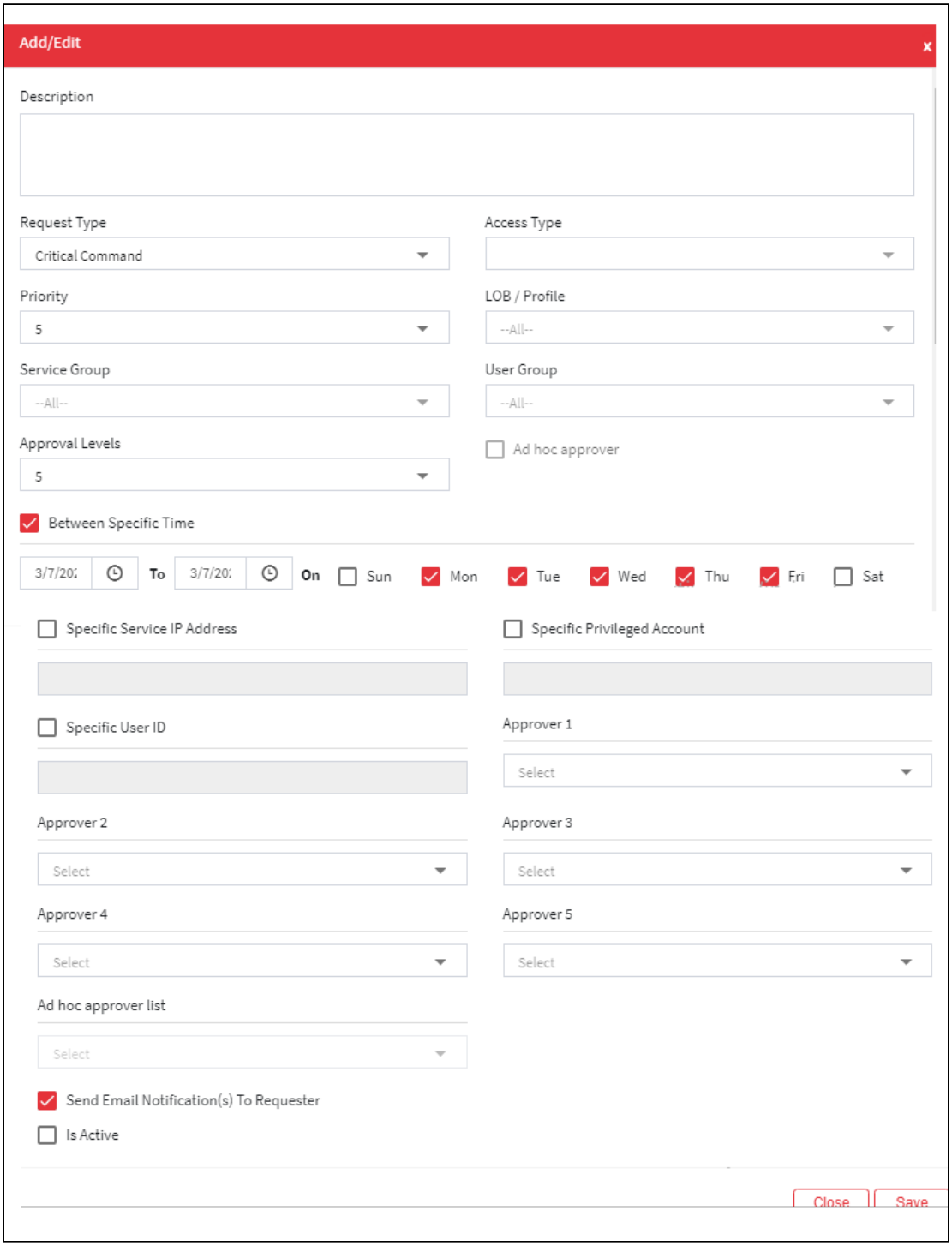
6.2.2 Process Flow Diagram



6.2.3 Configure Workflow Approval Matrix

The Administrator shall configure Critical Command Workflow using the following path:

Settings → Workflow → Raise Request



The **User Request Approval Workflow** screen contains the following fields:

Field Name	Description
Description	Specify the name or details of the approval matrix to be created.

Field Name	Description
Request Type	Select **Critical Command** as the type of request.
LOB/ Profile	Select the LOB or profile.
Service Group	Select the service group.
User Group	Select the user group.
Approval Levels	Select the number of approval levels to approve the request. ⚠ It can be set to maximum of 5 levels and minimum of 1 level.
Between Specific Time	Select the specific time with hours and days, to enable the matrix between the selected time.
Specific Service IP Address	Select and specify the service IP address to apply the created matrix to the specific IP only. ⚠ The IP refers to the destination server/service accessed via ARCON PAM.
Specific Privileged Account	Select and specify the privileged account to apply the created matrix to the specific privilege account only. ⚠ The account refers to the destination server user account accessed via ARCON PAM.
Specific User ID	Select and specify the user ID to apply the created matrix to the specific user ID only. ⚠ The user ID refers to the user's login in ARCON PAM.
Approvers	Select the name of the approver to approve the request. ⚠ • For the User ID's to appear for selection in the dropbox, the Users in ARCON PAM needs to have email ID's configured in user settings. • Multiple approvers can be chosen at each level of approval.

Field Name	Description
Send Email Notification(s) To Requester	Send email notification to the User who has raised request from CM. ⚠ For the mails, SMTP configuration under ARCON PAM has to be configured prior and ARCOS Alert Service has to be running on ARCON PAM server.
Send SMS Notification(s) To Approver	Send SMS notification to the approver. ⚠ For sending SMS notification, it is mandatory to define SMS Gateway configuration prior in ARCON PAM.
Is Active	Enable the matrix.

1. Select **Any** or **Critical Command** in **Request Type** dropdown list and enter or select the required details.
2. Click **Create**, to create the Workflow Matrix for Critical Command.

⚠ You can create only one **Critical Command** workflow. This workflow is configured by default for All LOB/ Profile, All User Groups and All Service Groups.

6.2.4 Create Command Profile

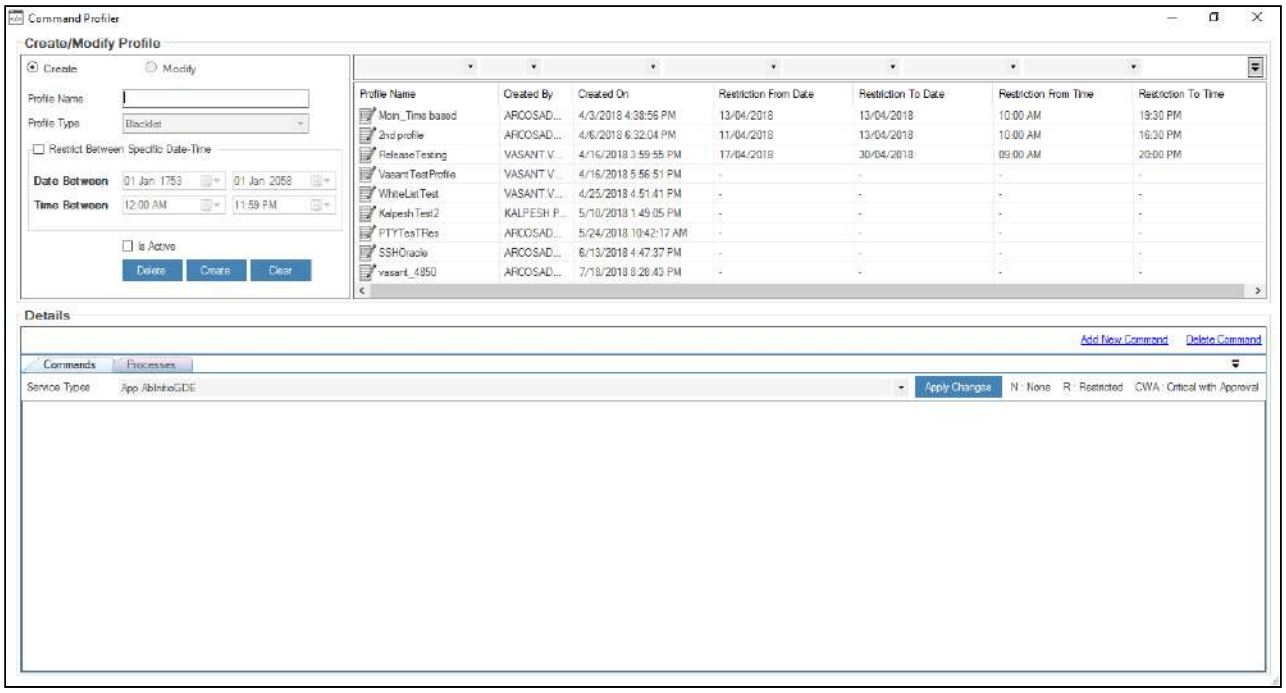
This section explains the steps to create a command profile.

⚠ Administrators can also assign Windows configuration commands to user groups.

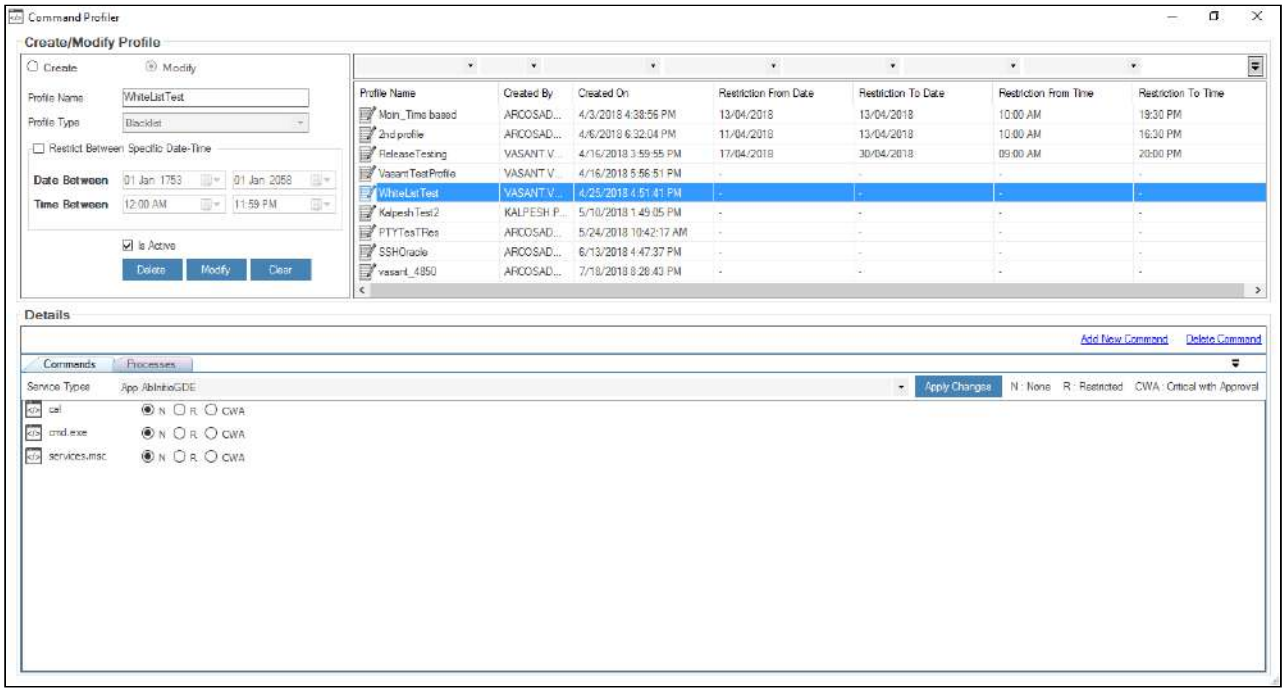
To create a command profiler use the following path:

Manage → Command Profiler

1. Enter the name of the profile in the **Profile Name** text field.

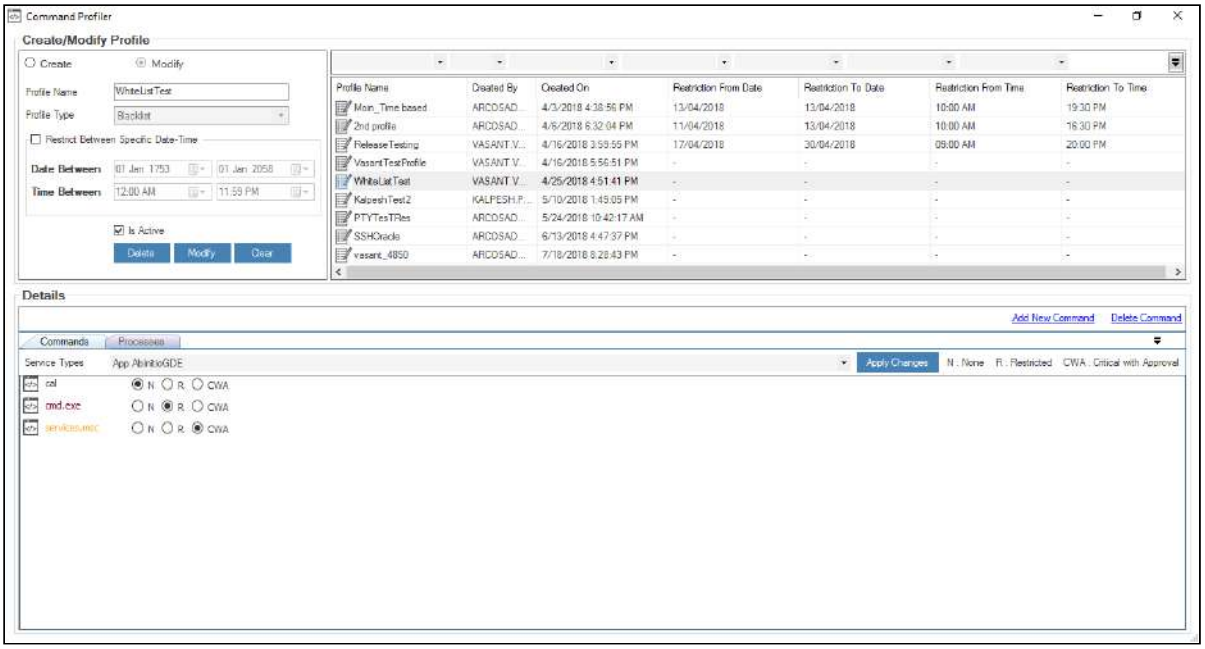


2. Select the **Is Active** checkbox and click on the **Create** button. A window pops up with the following message: **Command Profile Added Into List**
3. Select the profile from the **Profile Name** list and then select the required service type from the **Service Types** dropdown. It displays the list of commands commonly used by the particular servers.



4. Assign command properties to the commands displayed in list.
   Following are the command properties:

- **N:** None <Displayed in Black Colour>
  The command marked as None, will allow the user to execute the command without any restriction or approval process.
- **R:** Restricted <Displayed in Maroon Colour>
  The command marked as Restricted, will not allow the User to execute the command.
- **CWA:** Critical With Approval <Displayed in Orange Colour>
  The command marked as Critical With Approval will allow the User to execute the command only after approval. An email notification will be sent to Approver for approval or rejection. Once approved, the User will be able to execute the command.

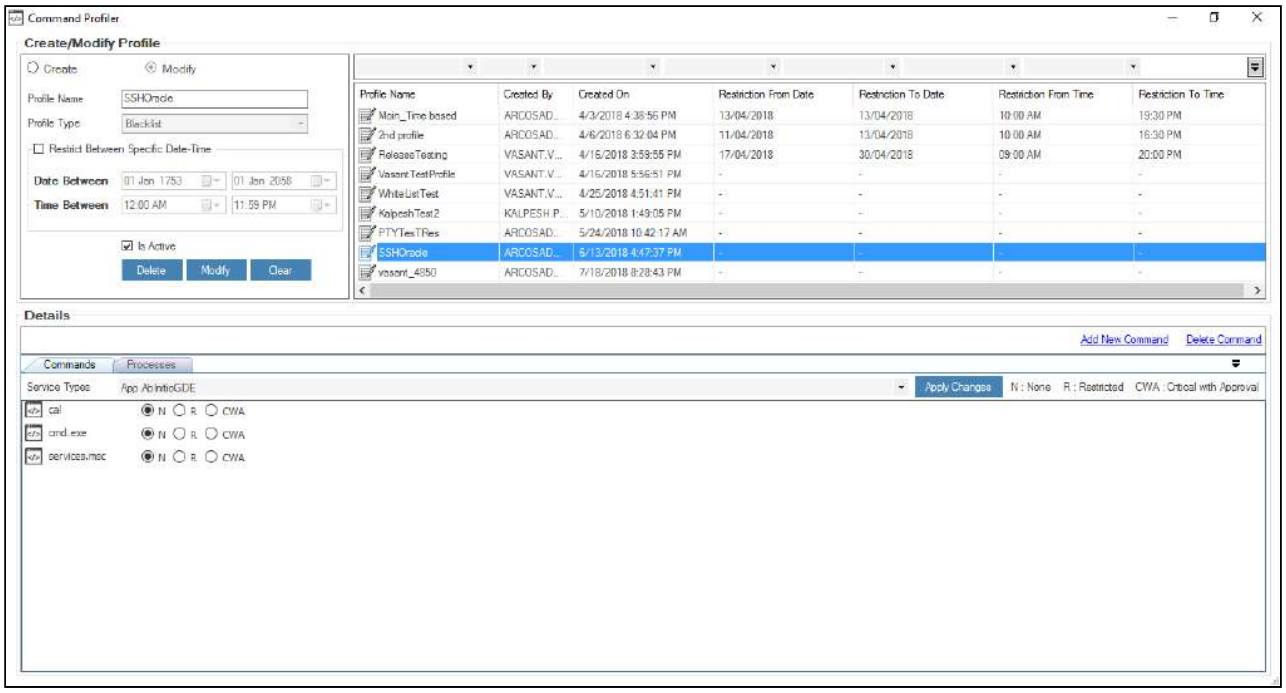


5. Click **Apply Changes**,to assign commands to profile. A window pops up with the following message: **Command Profile Updated**
6. Click **OK.** The profile is created.

6.2.4.1 Delete Command Profile

This section explains the steps to delete a command profile.

1. Select the name of the profile from the **Profile Name** list and click **Delete**.

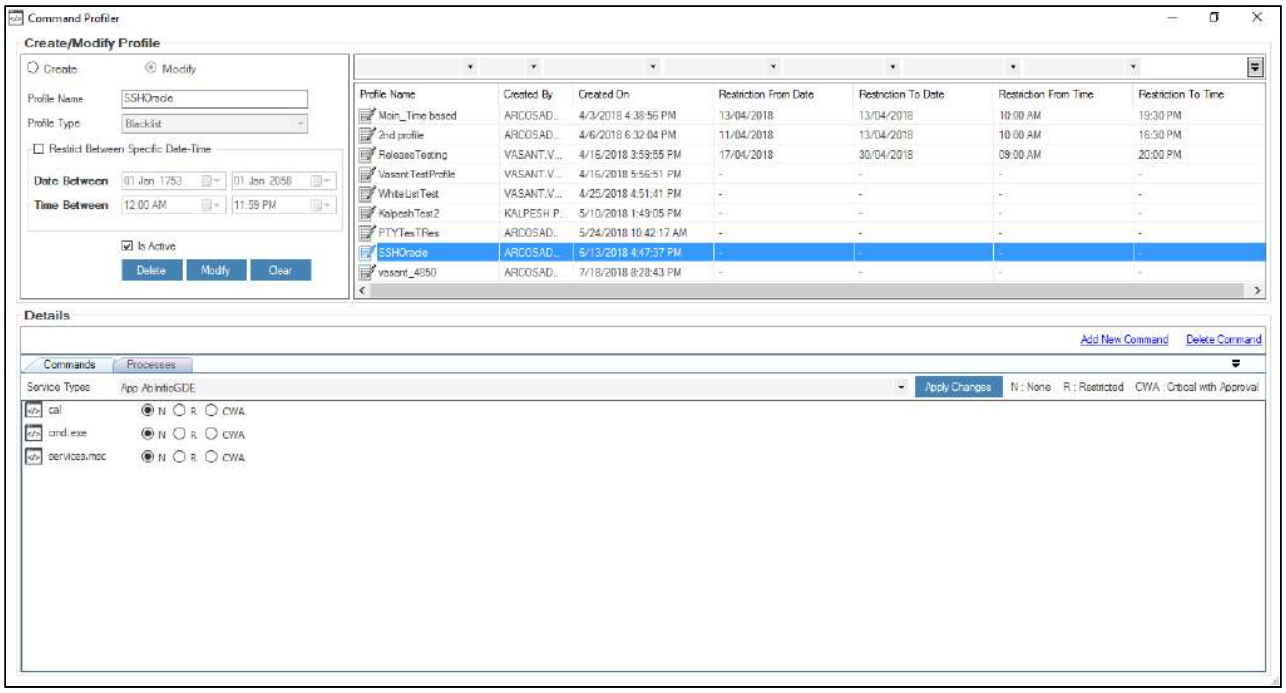


2. A window pops up with the following message:
   Are You Sure You Want To Delete The Selected Command Profile?
3. Click **Yes.** Another window pops up with the following message
   Command Profile Deleted From List.

6.2.4.2 Modify Details of Command Profile

This section explains the steps to modify details of an command profile.

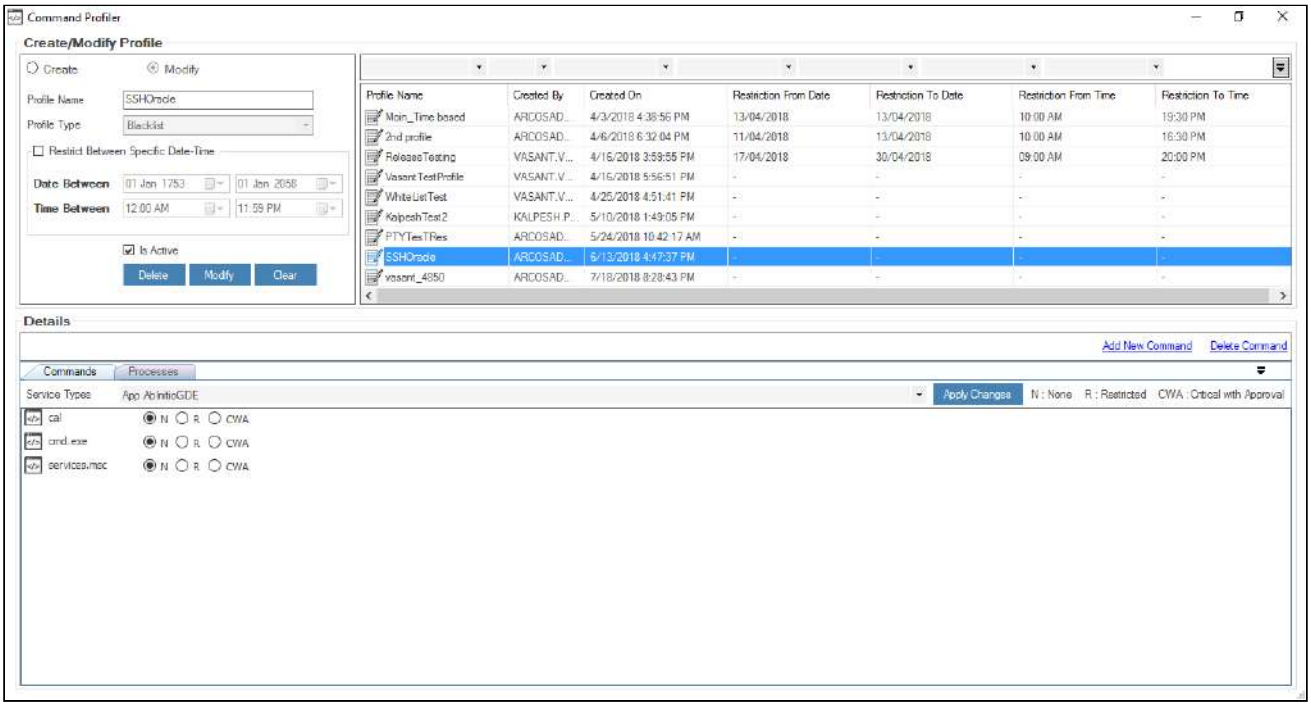
1. Select the required name of the profile from the **Profile Name** gridlist. The details are displayed in the **Profile Name** and **Profile Type** fields.



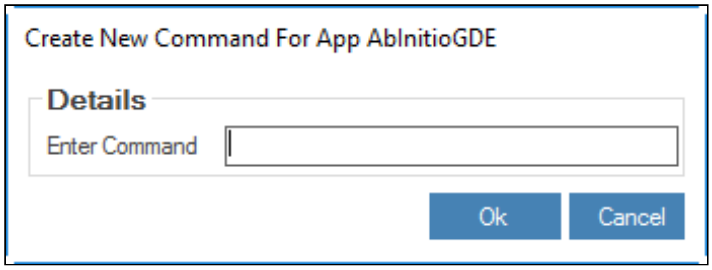
2. Modify the required details and click **Modify**, to update the details.
3. A window pops up with the following message:
   Command Profile Updated.

6.2.4.3 Create New Command

A command is a specific instruction executed on the Server to perform some kind of task or function. This section explains the steps to create a command.



1. Select the required Profile and Service Type from the **Service Type** dropdown.
2. Click **Add New Command** link. A **Create New Command For <Service Type name>** window pops up.

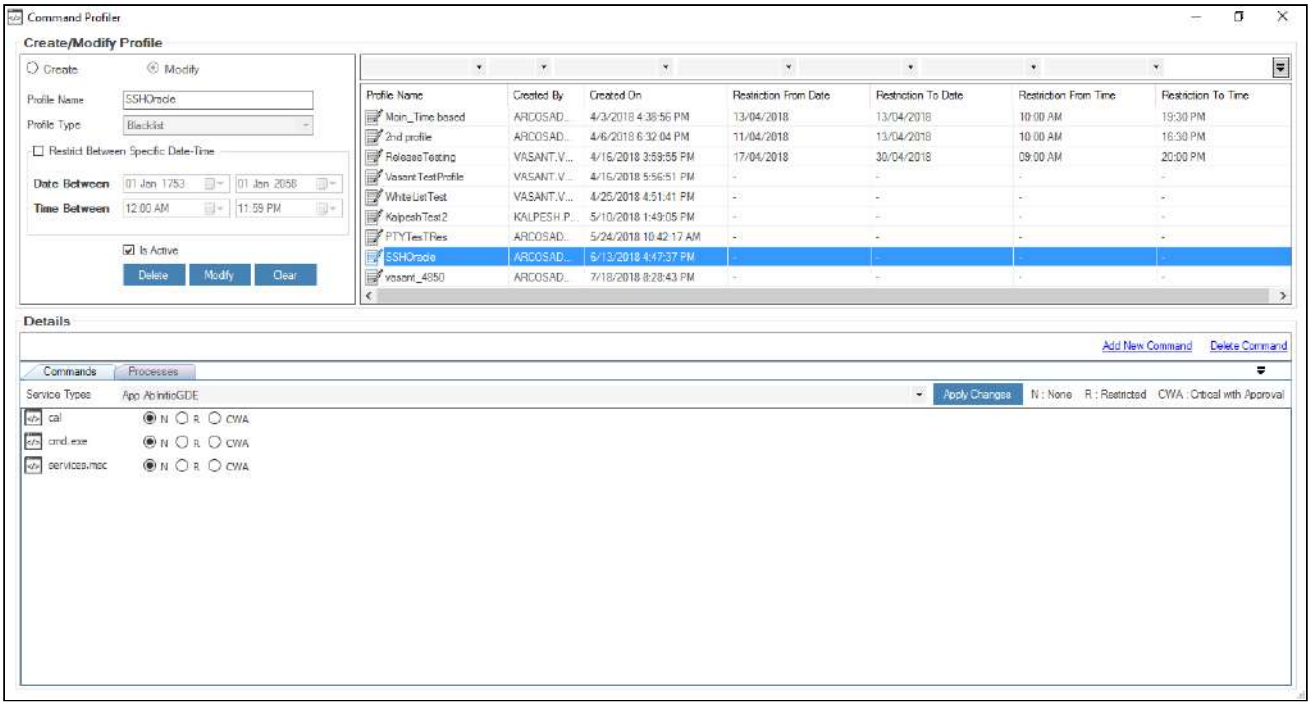


3. Enter command in **Enter Command** text field and click **OK**. A window pops up with the following message: **New Command For Selected Service Type Added.**

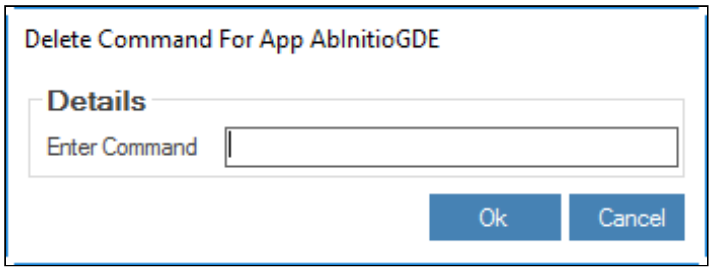
> ⚠ The character limit for Add New Command window is increased from 50 to 1000 characters for restricting or blacklisting commands.

6.2.4.4 Delete Command

This section explains the steps to delete a command.



1. Select the required Profile and Service Type from the **Service Type** dropdown.
2. Click **Delete Command** link. A **Delete Command for App** window pops up.



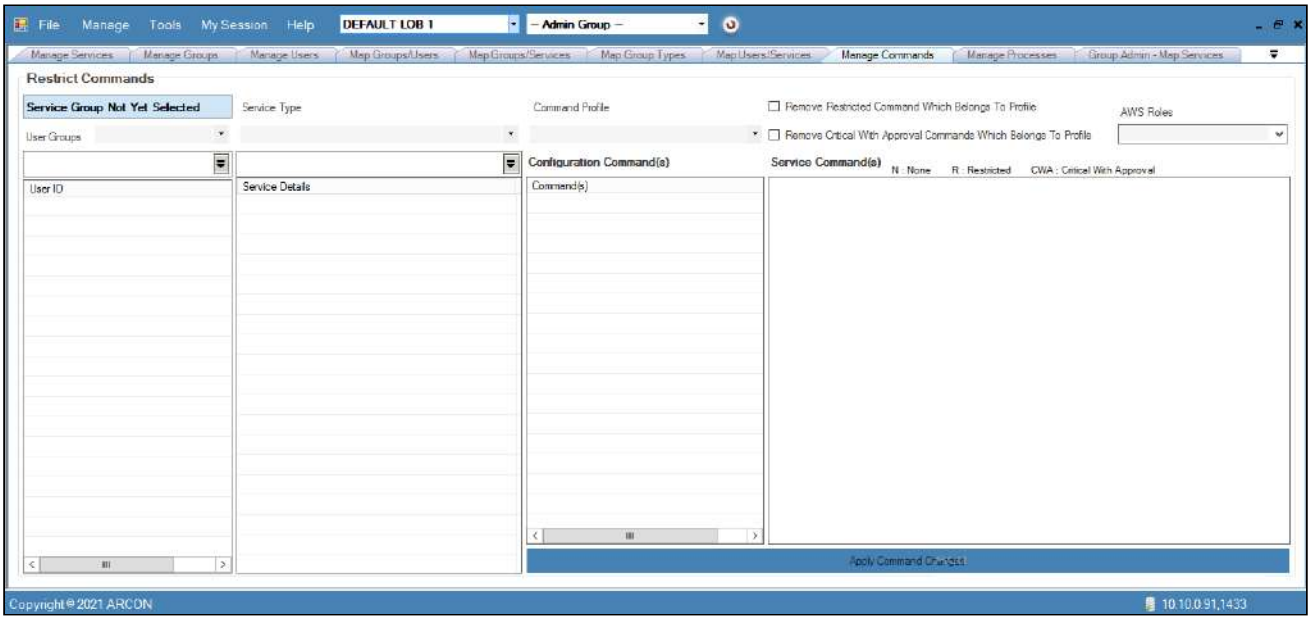
3. Enter the existing data or command in the **Enter Data** text field and click **Delete** button. A window pops up with the following message:
Command Deleted From Selected Service Type.

6.2.5 Assign Profile to User

This section explains the steps to assign a profile to a User and Service.

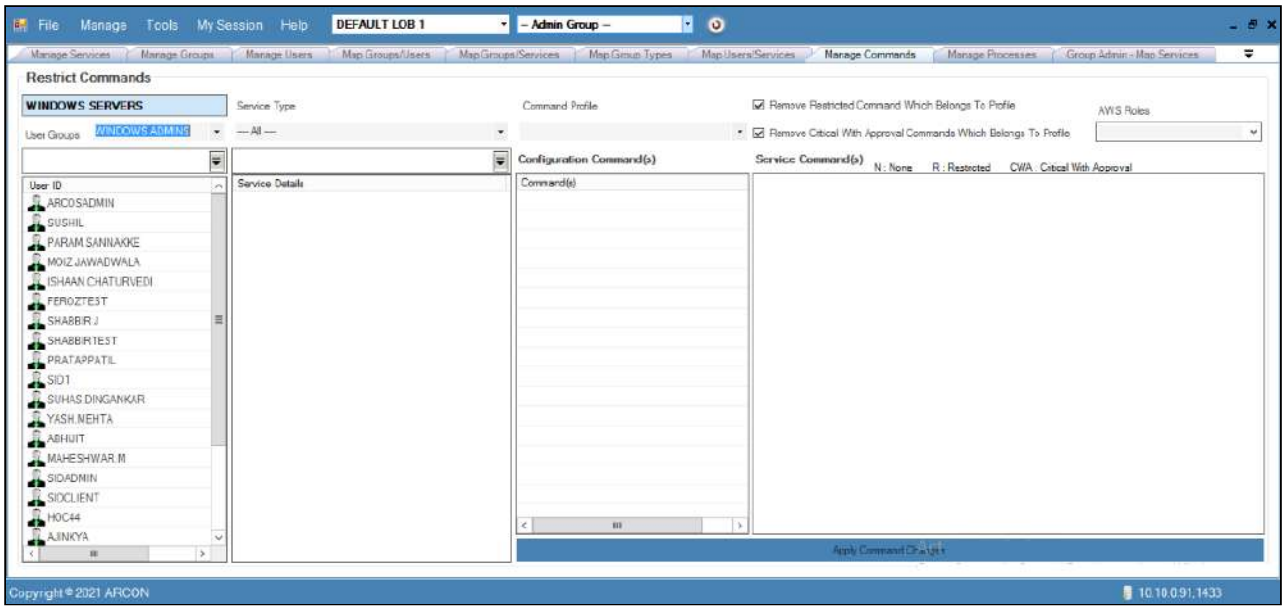
To assign a profile to a User use the following path:

Manage → Users and Services → Manage Commands

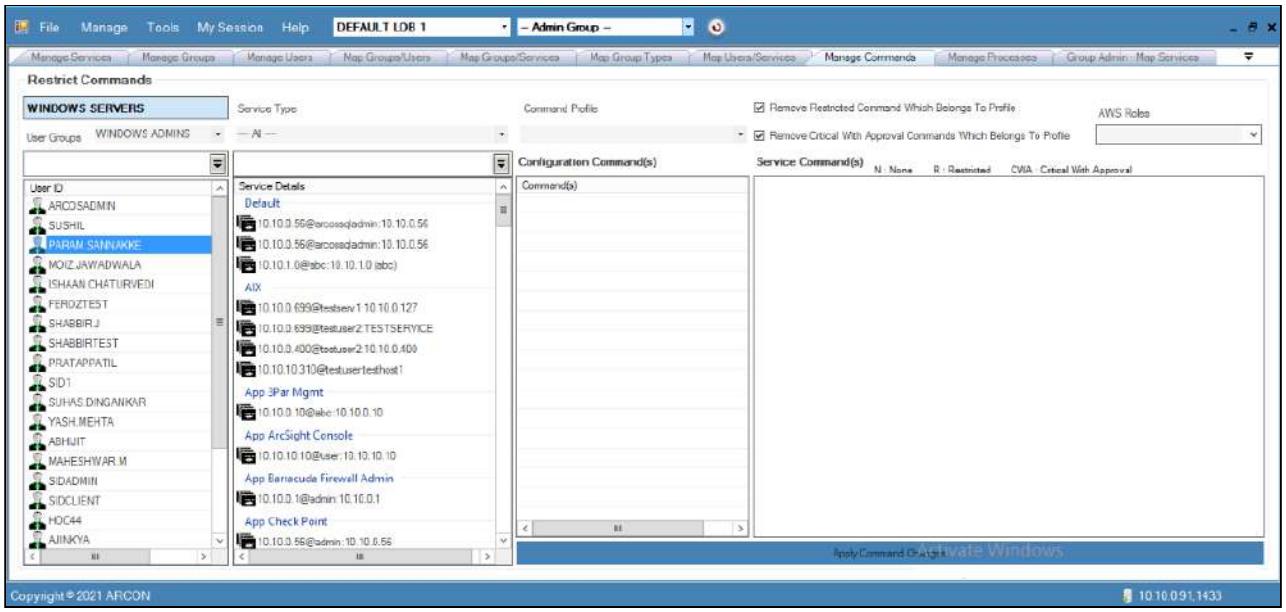


1. Select/Enter the user group from the **User Groups** dropdown list on the left pane. A list of **User ID(s)** are displayed.

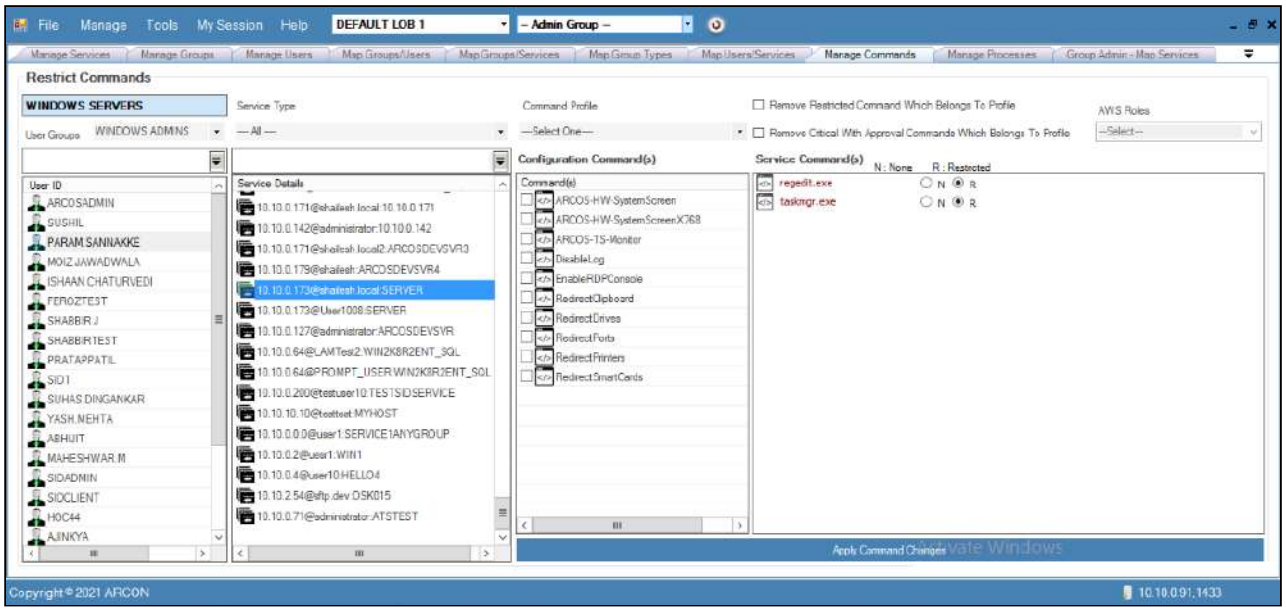
> ⚠ To search a specific set of rows, enter keywords(space separated) in the search text field of the user group, service type, Command Profile dropdown and the relevant rows are fetched.



2. Select the user ID from the **User ID** list, wherein it displays all the service details available for that particular user ID.



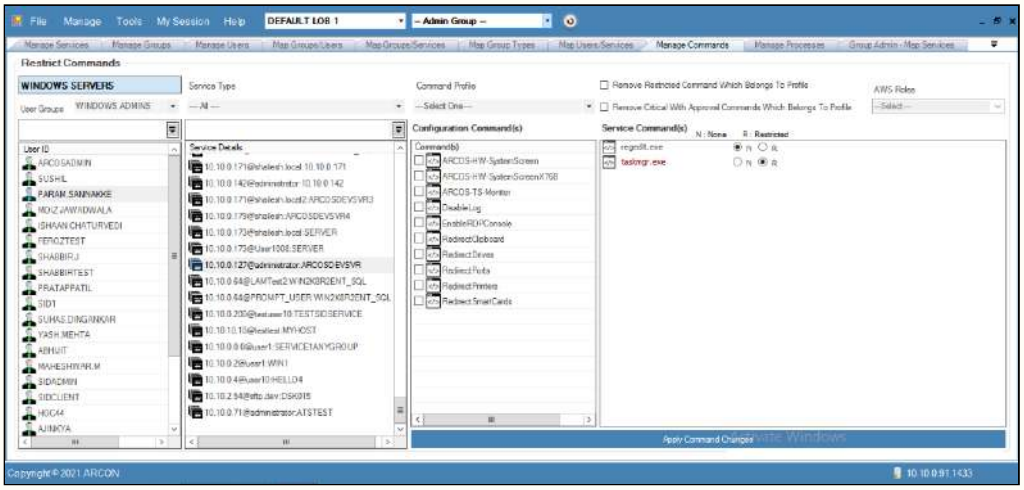
3. Select the service from the list of **Service Details** in **Service Type** section.
4. You can view all the commands in **ARCON PAM Configuration Command(s)** and **Service Command(s)** section.



5. Select the commands from **ARCON PAM Configuration Command(s)** and **Service Command(s)** grid and click **Apply Command Changes**. A window pops up with the following message:
   Commands Restricted/ Applied Successfully For User
6. Click **OK**. The commands are restricted for that particular user.

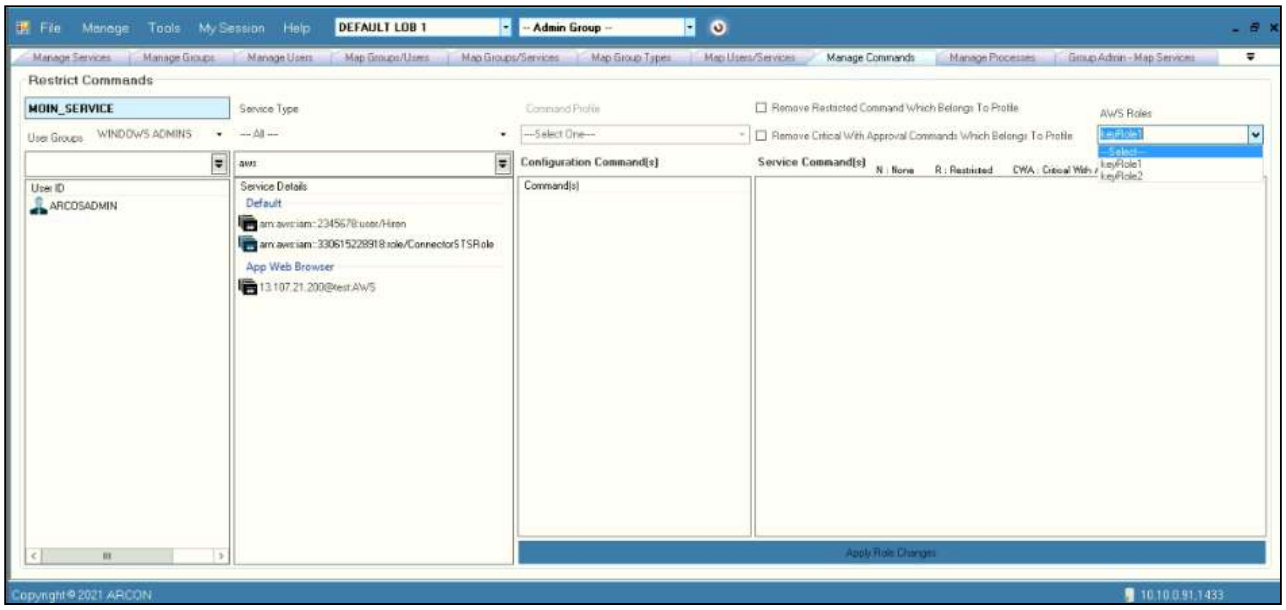
a.

- If you want to restrict only those commands that belong to the selected Command Profile, then you need to select the **Select only Restricted command which belongs to profile** checkbox.
- If you want to select only those critical commands that belong to the selected Command Profile, then you need to select the **Select only Critical command which belongs to profile** checkbox.
- If **Profile Duration** is configured for selected profile then from and to date and time will be displayed.



- To verify, whether the commands are restricted or approved for execution, open a session from Client Manager and execute the command on server. It will either allow to execute the command or an error prompt will be displayed for restricted commands.
- The **CWA** (**Critical With Approval**) command property is not applicable for SFTP Commands of SSH Linux Service Type.
- You can whitelist configuration commands for services of SSH Firewall, SSH Router and SSH Switch Service Type.
- Redirect clipboard option can be disabled for individual users even if the clipboard option is globally enabled.

7. Users can assign AWS Roles after selecting the AWS service type from the dropdown.



6.3 Manage Processes

6.3.1 Overview

This section helps you know about TS Plugin service and how this service is used to blacklist and elevate windows processes in ARCON. This service is installed on servers having 2003, 2008, 2008 R2, and 2012 R2 windows operating system. A process restricted to you will not be allowed for access whereas an elevated process will be made available to perform any action. This plugin can also help you to capture process logs.

⚠

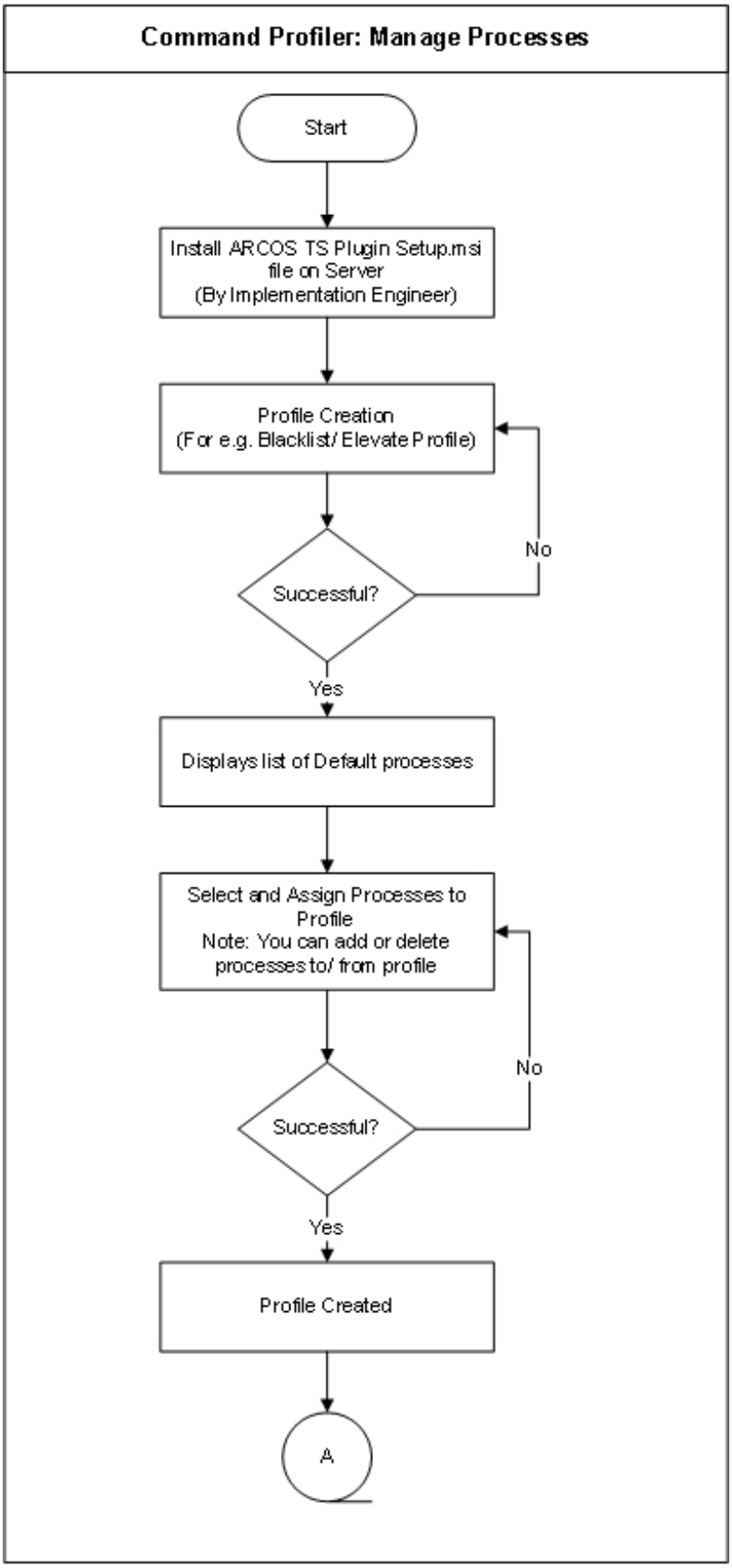
- The Administrator having **Change User Restricted Commands** in **Server's Privileges** privilege shall only be able to apply Blacklist and Elevate profiles.
- You will be able to install **TS Plugin** only if you have **Administrator** level privileges.

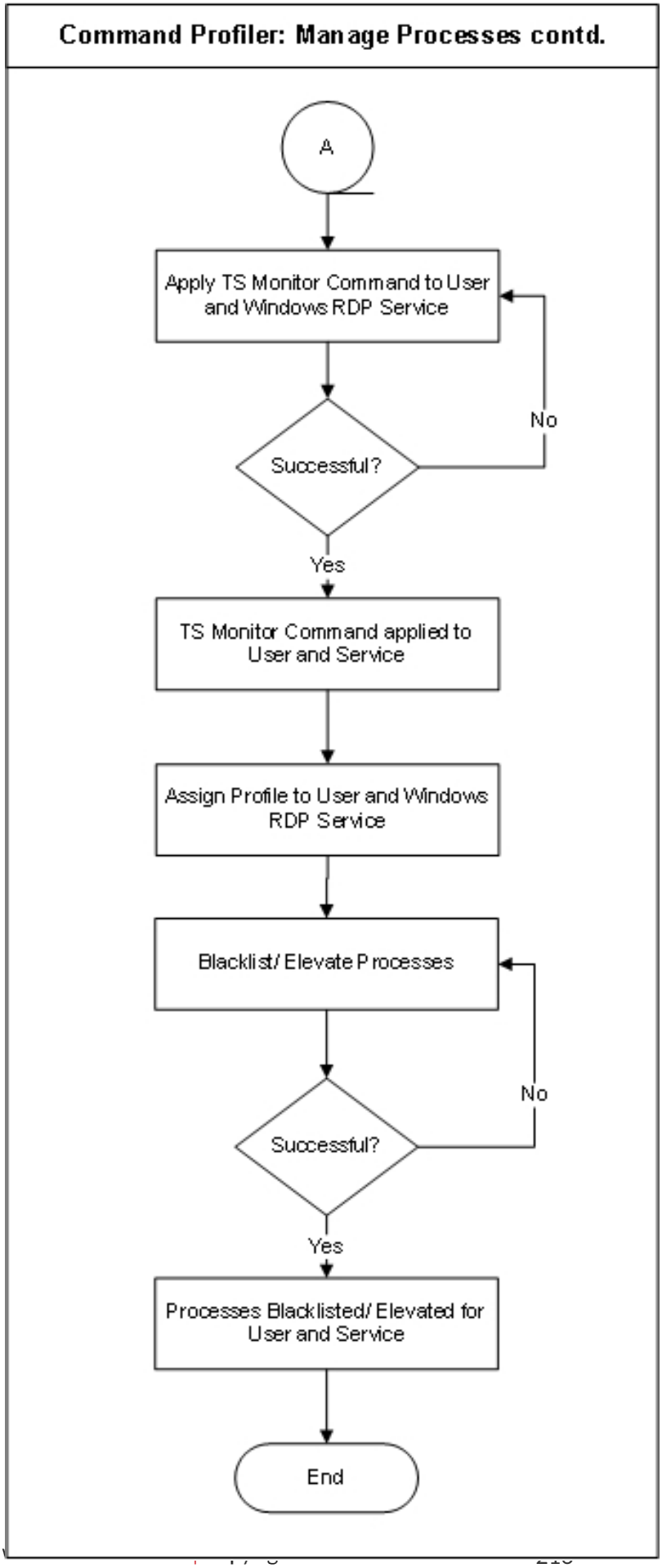
To manage processes, follow the below steps:

1. TS Plugin Installation
2. Create Profile
3. Assign TS Monitor Command To Service

4. Assign Profile and Restrict or Elevate Processes

6.3.2 Process Flow Diagram

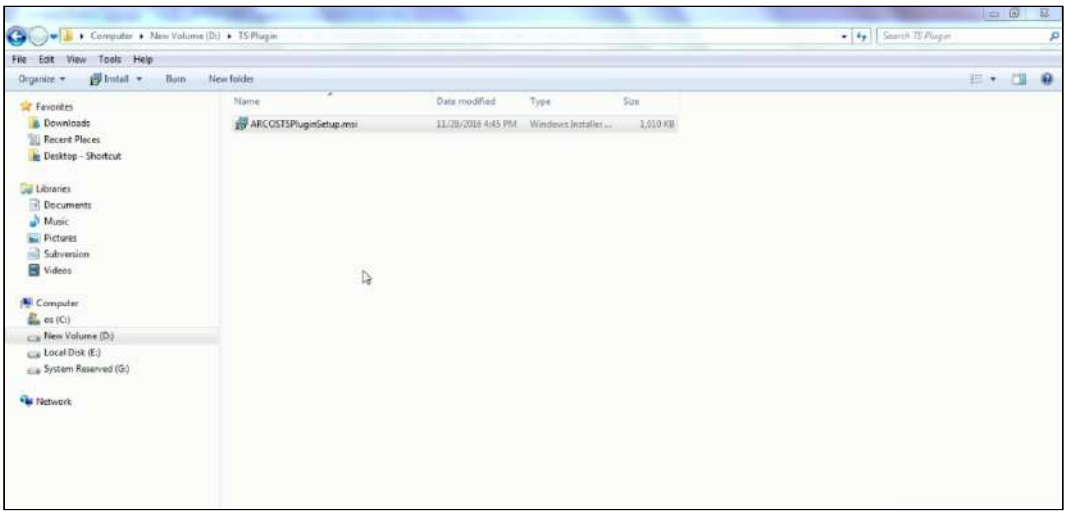

Command Profiler: Manage Processes
Start
Install ARCOS TS Plugin Setup.msi file on Server (By Implementation Engineer)
Profile Creation (For e.g. Blacklist/ Elevate Profile)
Successful?
No
Yes
Displays list of Default processes
Select and Assign Processes to Profile Note: You can add or delete processes to/ from profile
Successful?
No
Yes
Profile Created
A


Command Profiler: Manage Processes contd.
A
Apply TS Monitor Command to User and Windows RDP Service
Successful?
No
Yes
TS Monitor Command applied to User and Service
Assign Profile to User and Windows RDP Service
Blacklist/ Elevate Processes
Successful?
No
Yes
Processes Blacklisted/ Elevated for User and Service
End

6.3.3 TS Plugin Installation

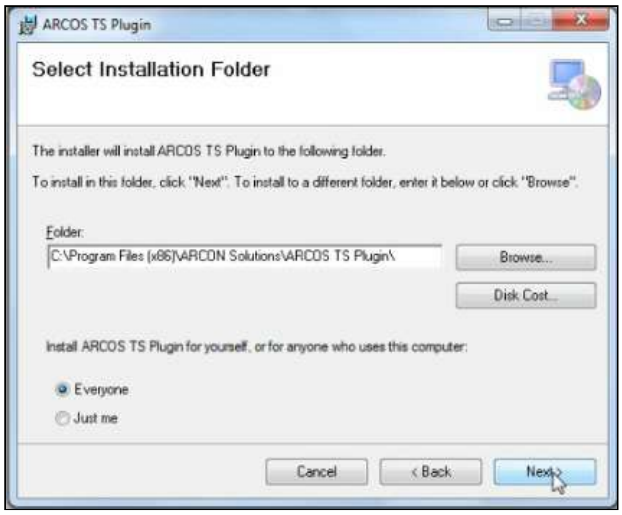
This section helps you to install TS Plugin.

> ⚠ You need to have ARCOS TS Plugin Setup.msi file on the server.

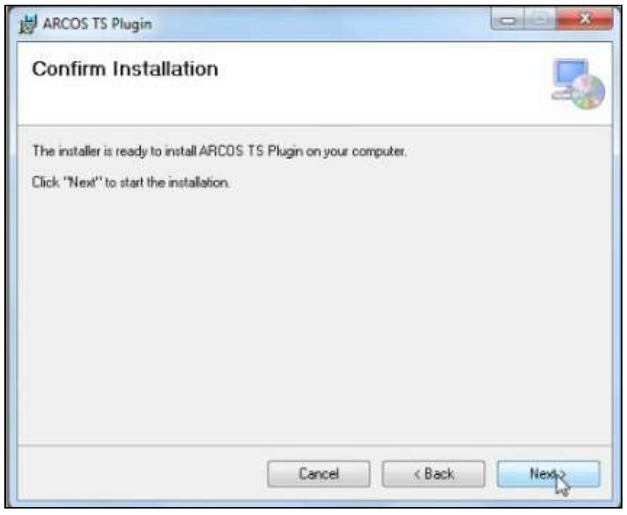


1. Double click on the setup file. The following screen is displayed.

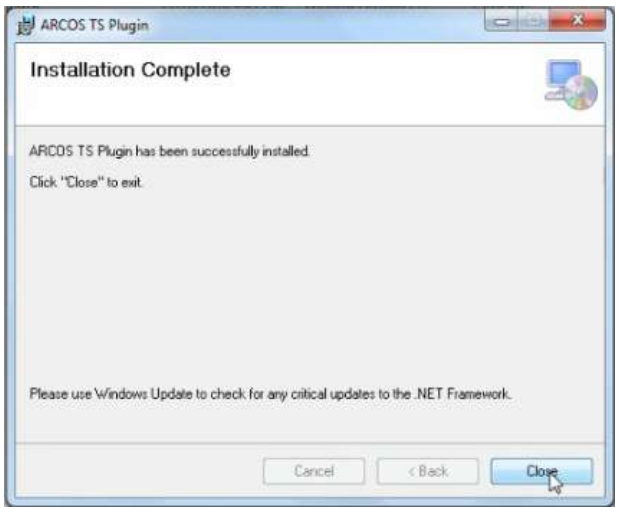
2. Click **Next.** The following screen is displayed.



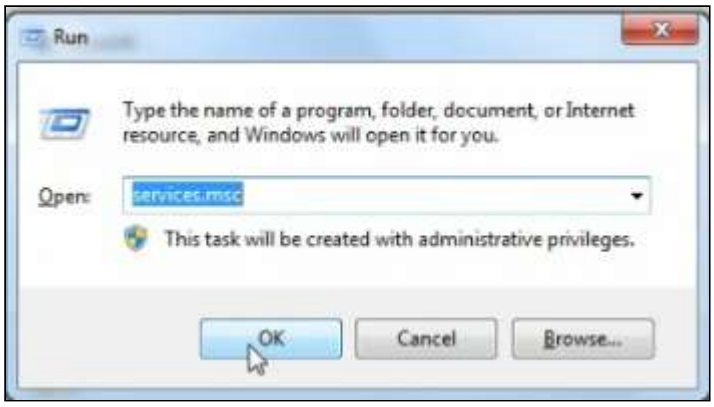
3. Browse and select the folder for installation and click **Next.**



4. Confirm the installation and click **Next**. You can see that the installation process is completed.



5. Click **Close**. Once TS Plugin is installed on server, you can check that the service is running on services.msc console.
6. Go to **Run** (Windows R) and enter services.msc.



7. Click **OK** to view TS Plugin service running on server.

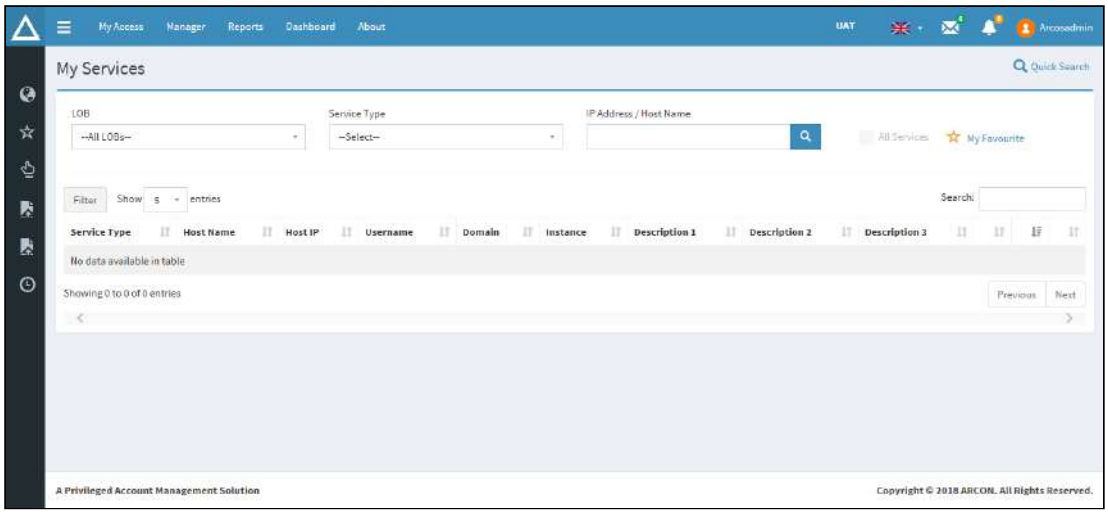
6.3.4 Create Profile

This section helps you to create profiles and then assign processes to the profile.For example, we will create two profiles Blacklist and Elevate.

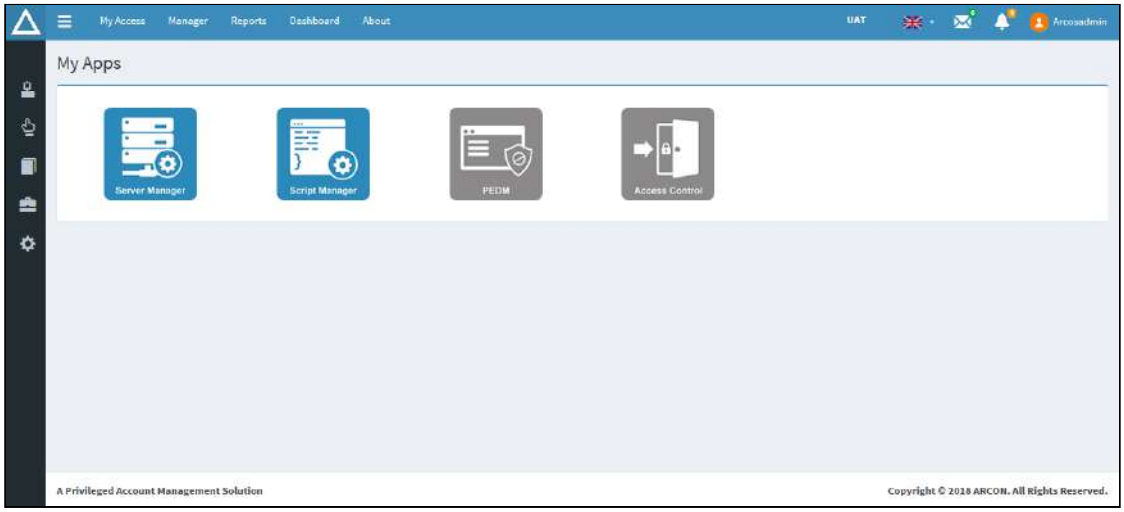
To create Profiles, follow the below steps:

1. Login to ARCON PAM Application using valid credentials.

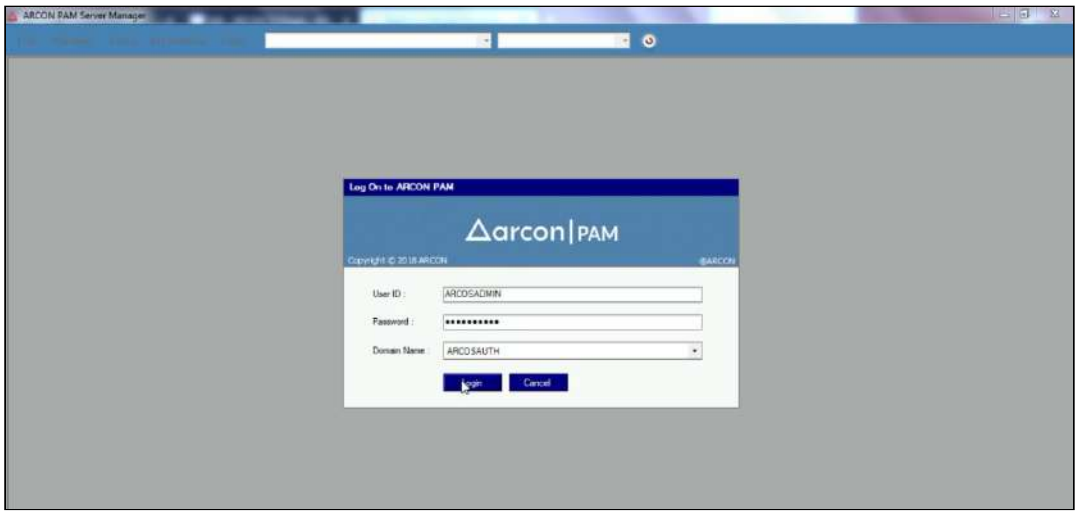
2. Click **Login**. The following screen is displayed.



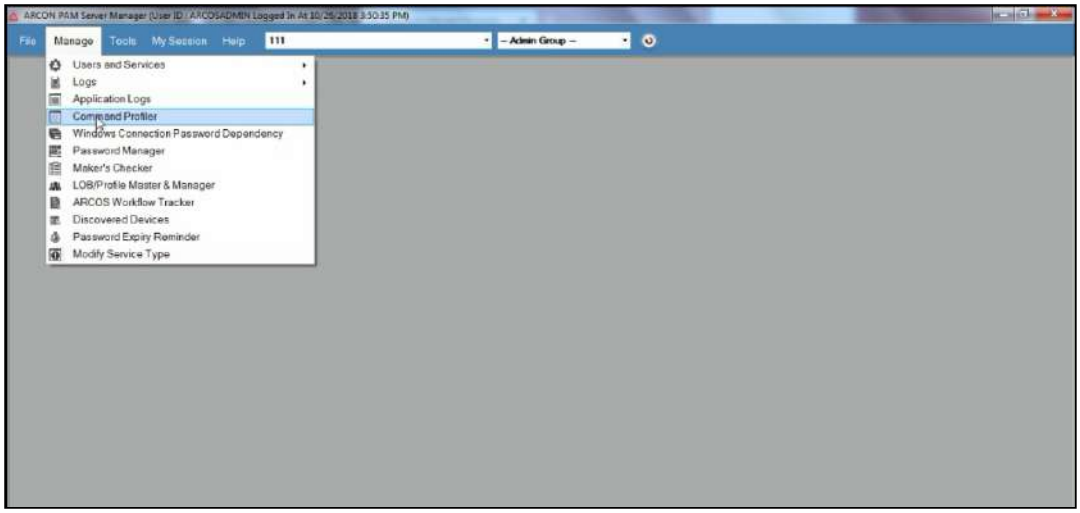
3. Click **Manager**. The following screen is displayed.



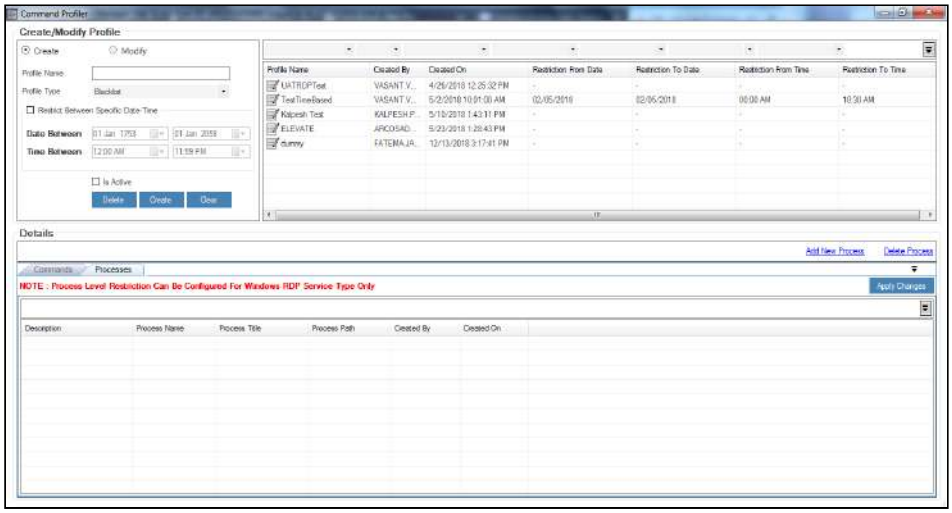
4. Click **Server Manager**. You can view the **Server Manager** login screen.



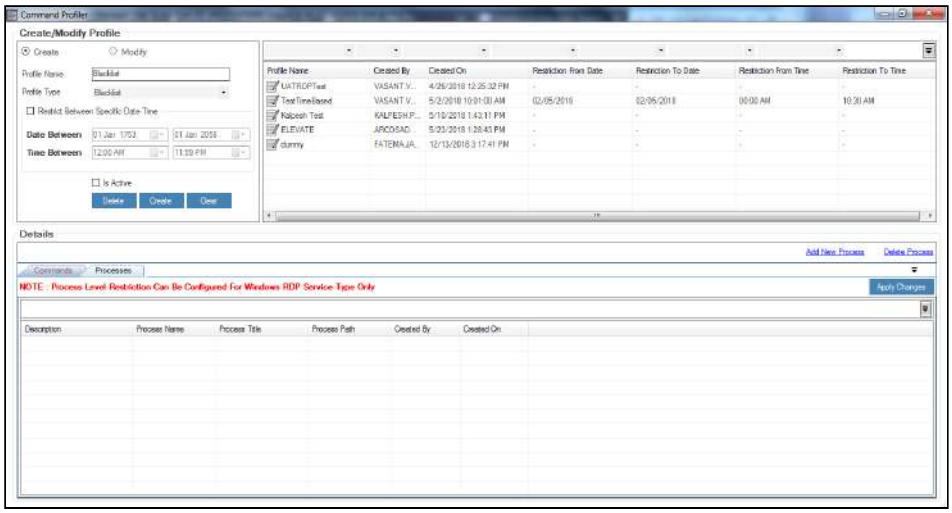
5. Enter valid credentials and click on **Login**.



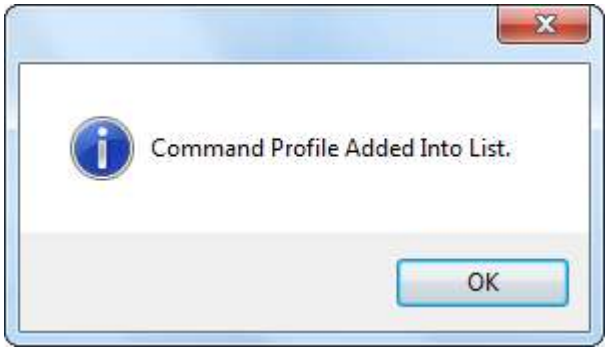
6. Click **Manage** and then go to **Command Profiler**. The **Command Profiler** screen is displayed.



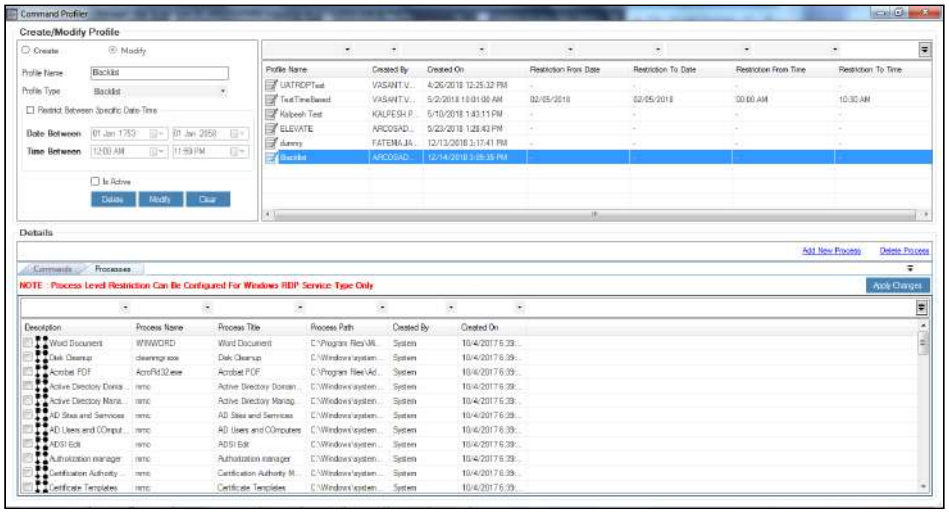
7. Go to **Processes** tab and click **Create** radio button.



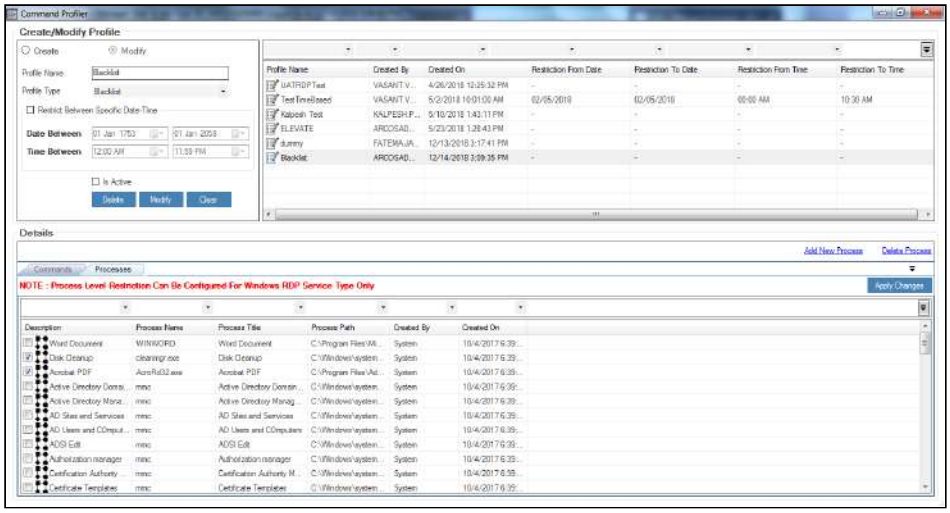
8. Enter Profile Name For example, Blacklist
9. Select Profile Type as Blacklist
10. Select Is Active checkbox, and then Click **Create**. The following pop up screen is displayed.



11. Confirm and click **OK,** you can view the profile created in the grid view.



12. Select the profile created, you can view list of default processes available for the profile.



13. Select the required processes to be assigned to the profile and click **Apply Changes**, to create a profile.
14. Similarly, you can create another profile for Elevate.

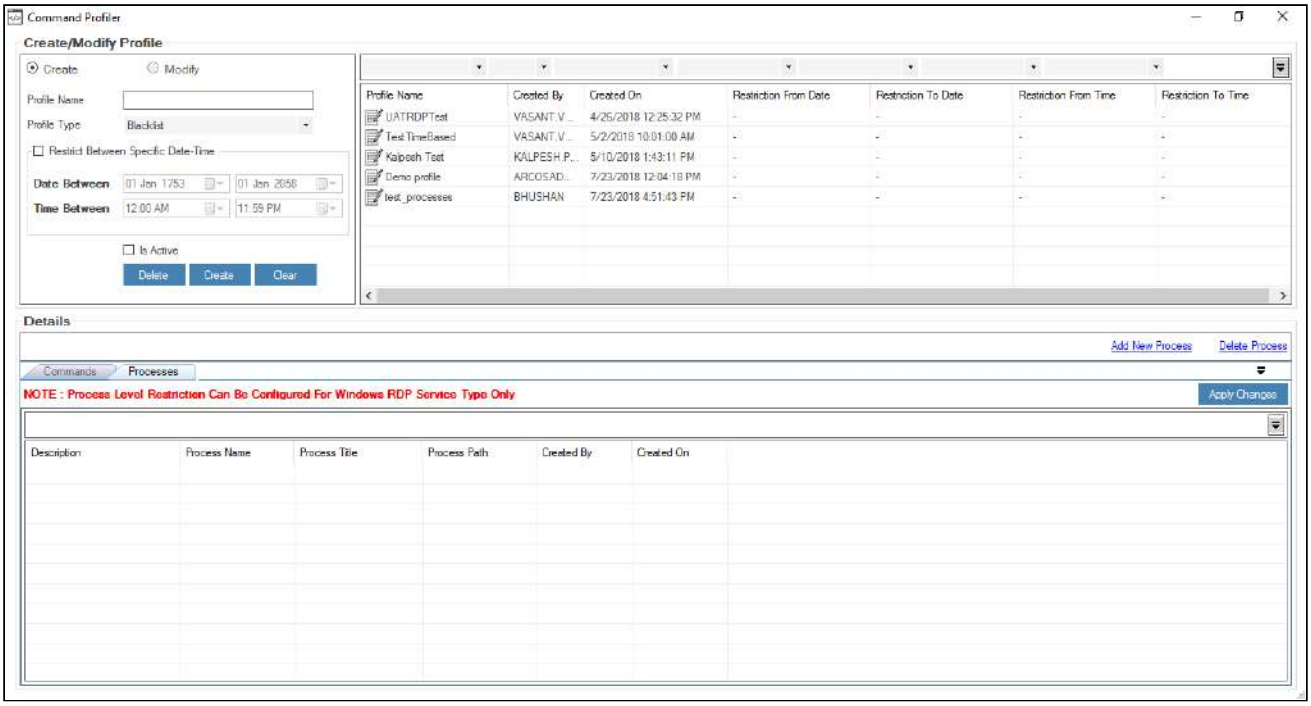
6.3.4.1 Add New Process

This section helps you to add processes to a profile.

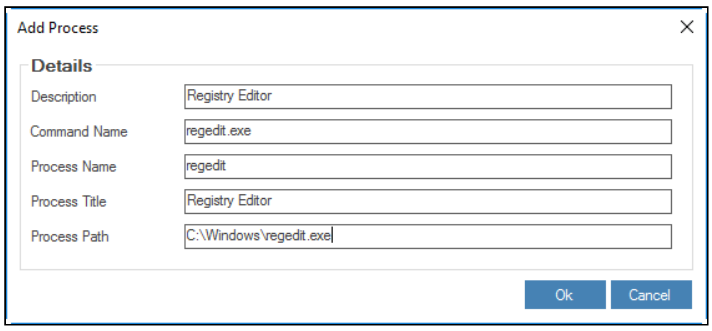
To add new process:

To add new process, use the following path:

Manage → Command Profiler



1. Select **Processes** tab and click **Add New Process** link. The **Add Process** window is displayed.



The **Add New Process** contains the following fields:

Field Name	Description
Description	Enter short description for the process.
Command Name	Enter name of the command.
Process Name	Specify process name.
Process Title	Specify title for a process.
Process Path	Specify path of the process. ⚠ The character limit for **Process Path** field in **Add Process** window is increased to 150 characters.

2. Enter the details and click **Ok** button, to add a process to the default list of processes.

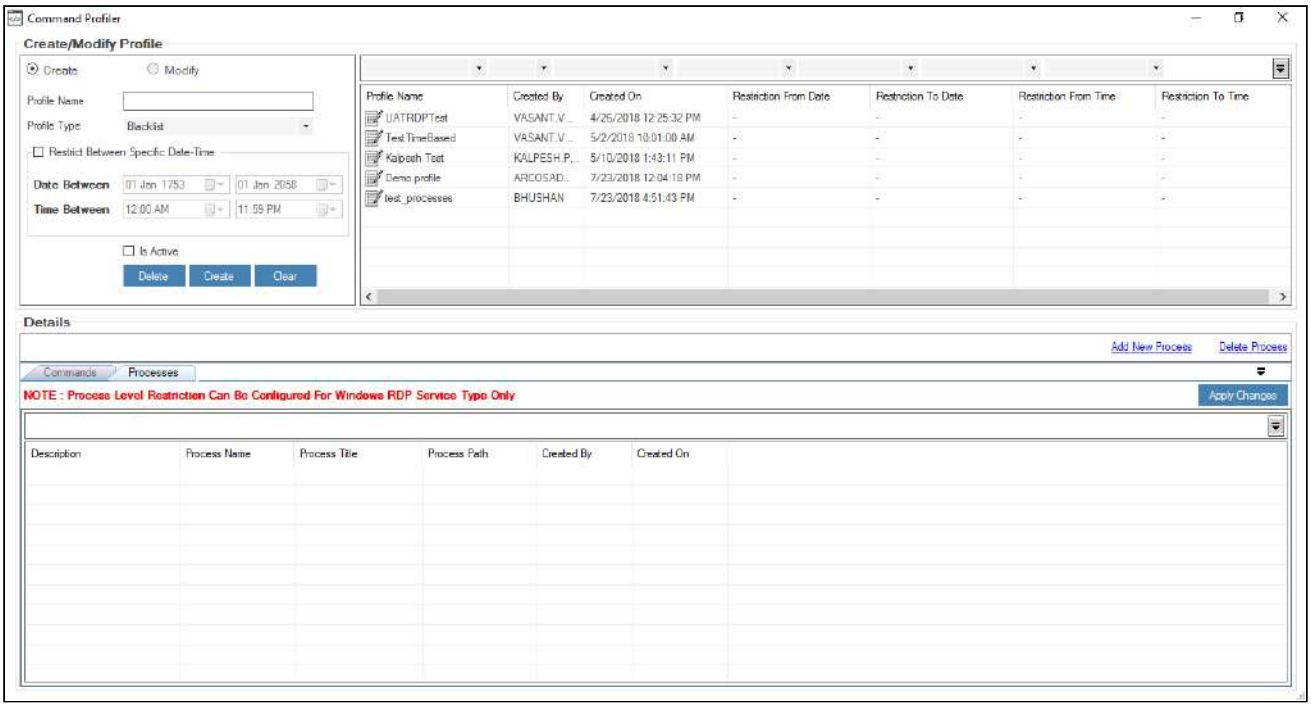
6.3.4.2 Modify Details of Process

This section helps you to modify details of a process.

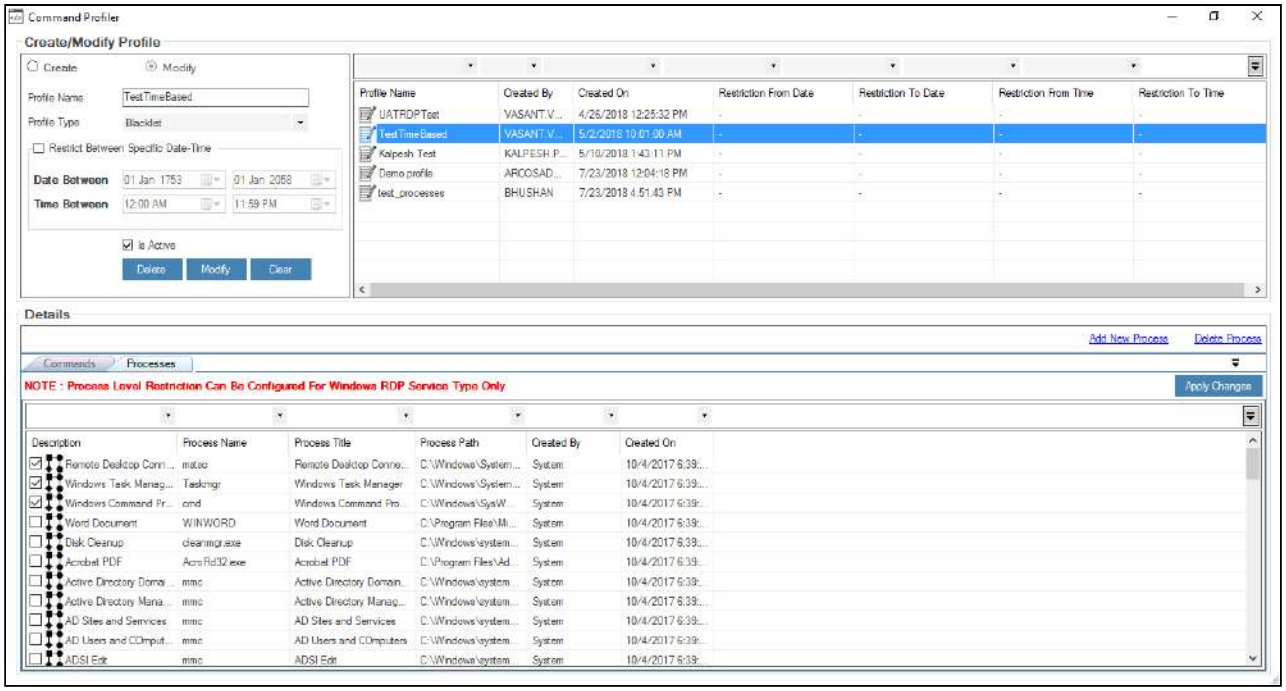
To modify details of a Process:

To modify details of a process, use the following path:

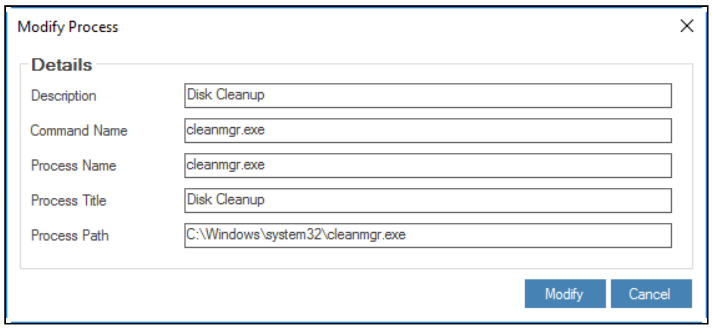
Manage → Command Profiler



1. Select **Processes** tab. The Profiles created in Command Profiler are displayed.
2. Select required Profile Name. The processes belonging to the particular profile are displayed.



3. Double click on the required process. The **Modify Process** pop up screen is displayed.



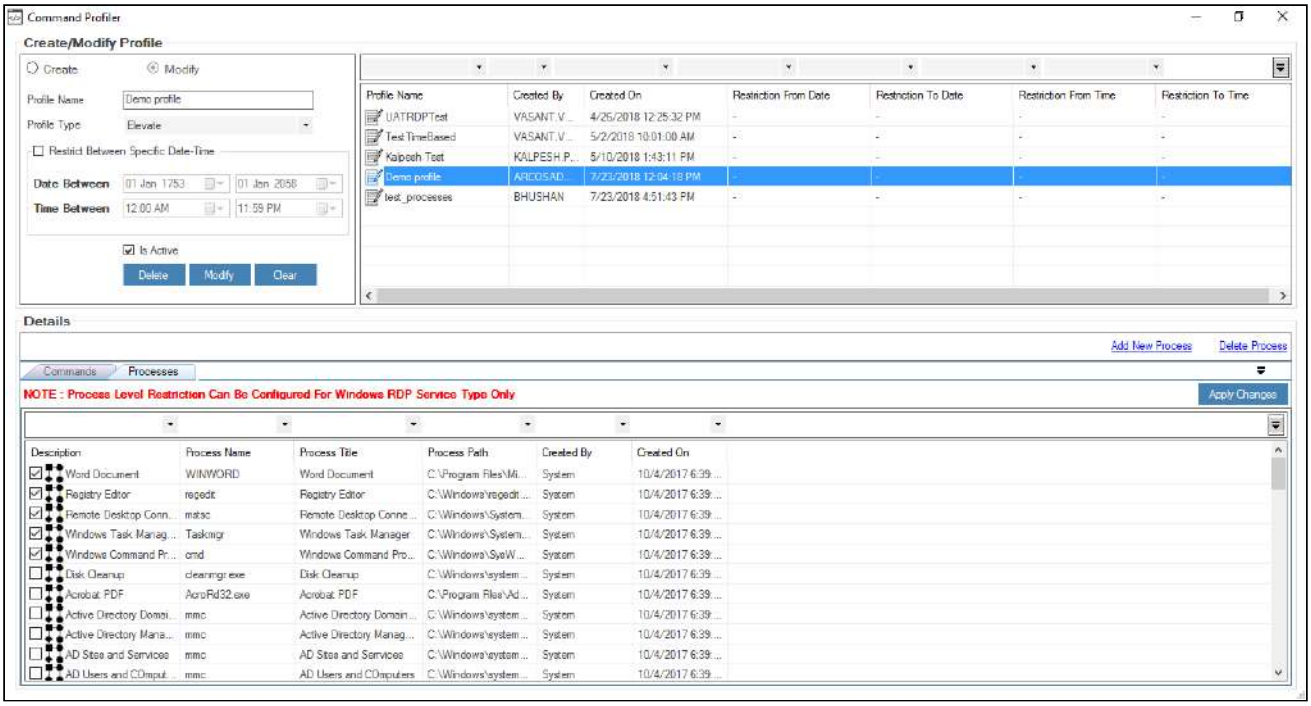
4. Modify the required details and click **Modify**, to update the details.

6.3.4.3 Delete a Process

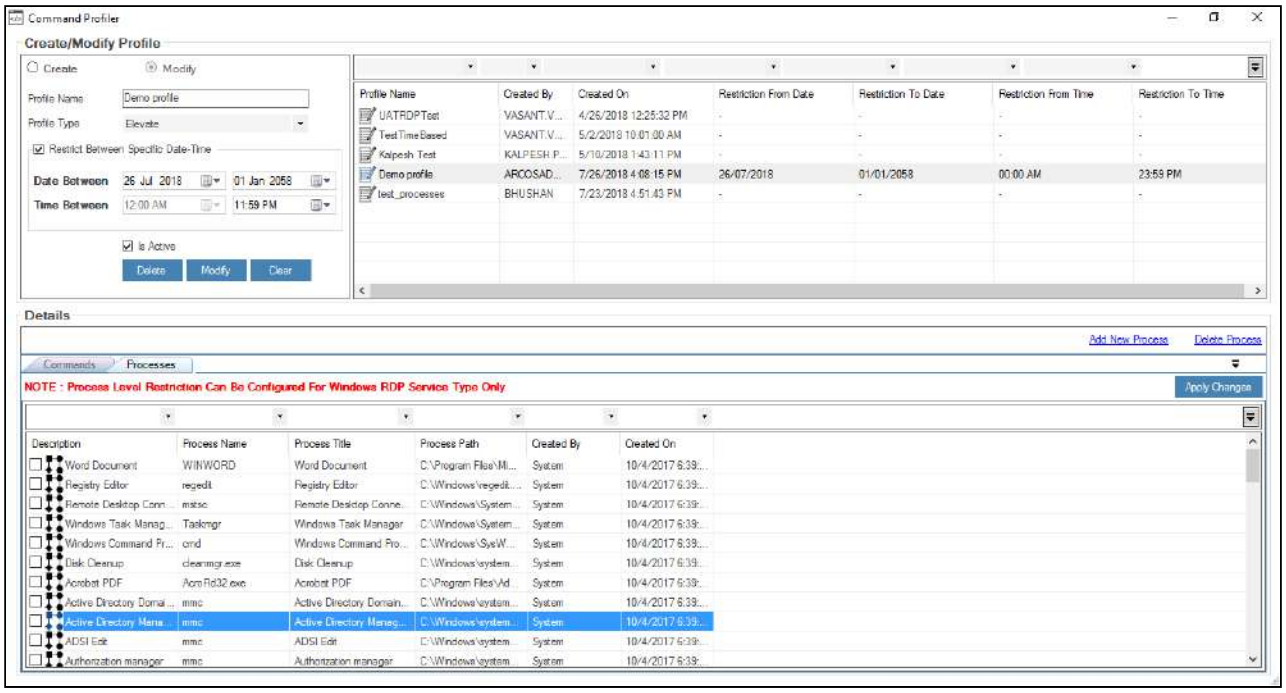
This section helps you know how to delete a process.

To delete a Process, use the following path:

Manage → Command Profiler



1. Select required **Profile Name**. The processes belonging to the particular profile are displayed in the grid on the bottom pane.

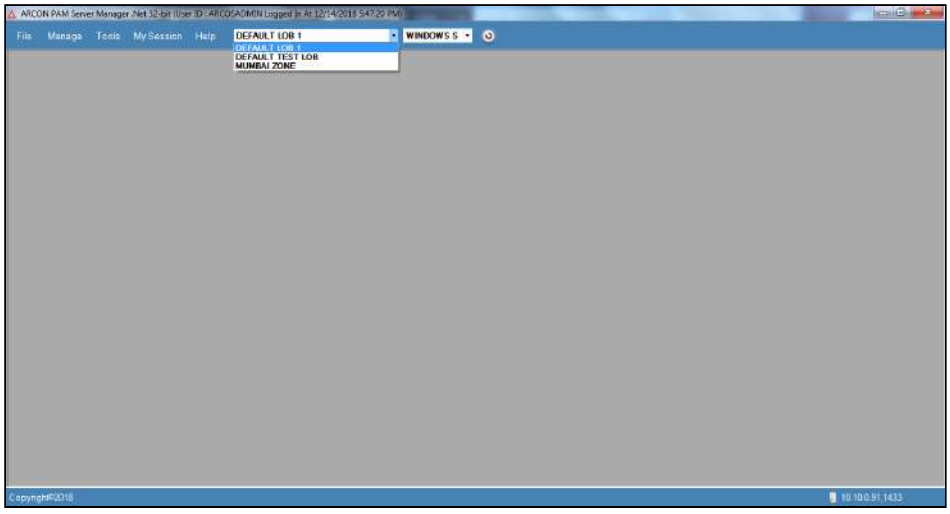


2. Select the required process to be deleted and click **Delete Process** link, to delete the process successfully.

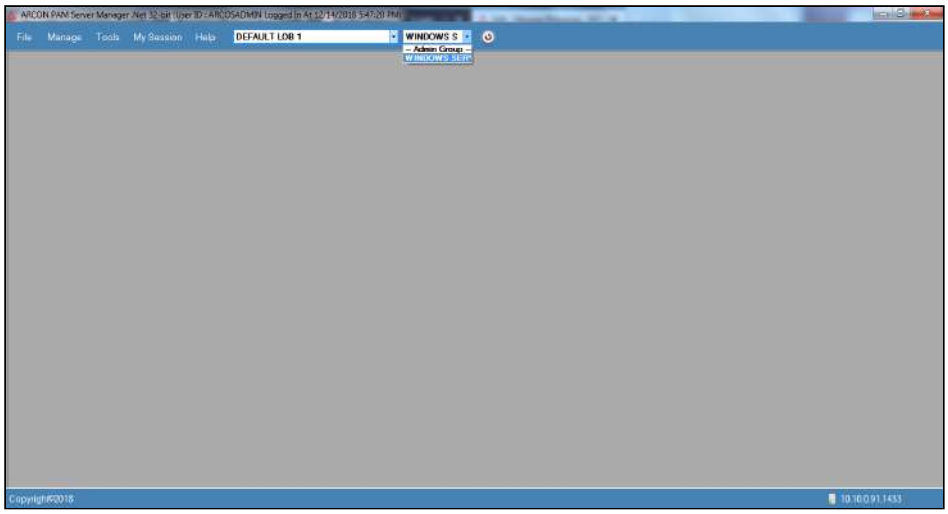
6.3.5 Assign TS Monitor Command to Service

This section helps you to assign TS Monitor Command to service. Once the profile is created then it is mandatory to assign ARCOS TS Monitor Command to a particular service. Processes shall only be restricted or elevated only once the TS Monitor Command is assigned to a particular service.

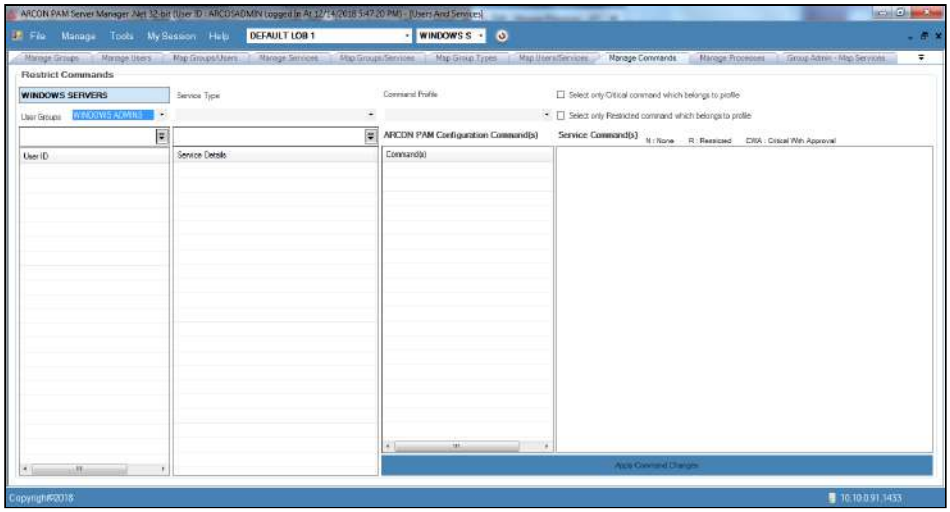
1. To assign TS Monitor, select the required LOB mapped to the service.



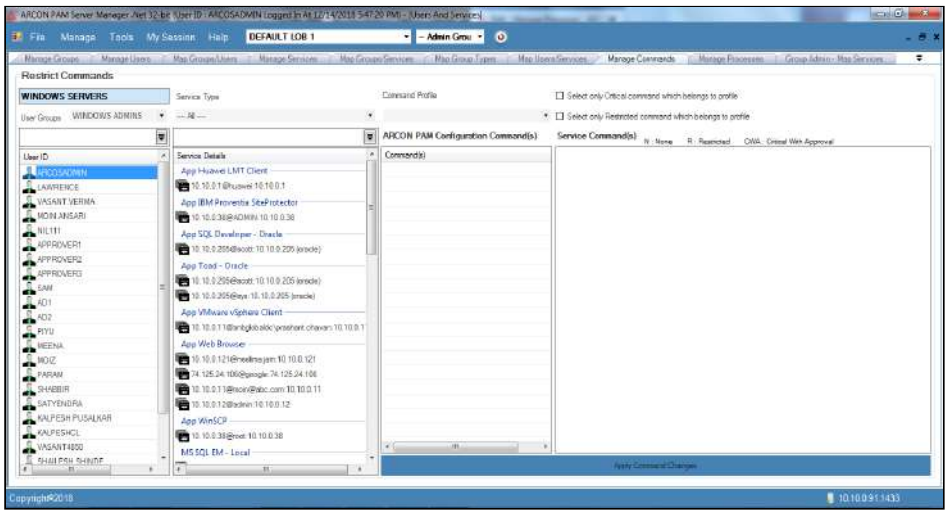
2. Select **Windows Server** group if you are a Group Admin.



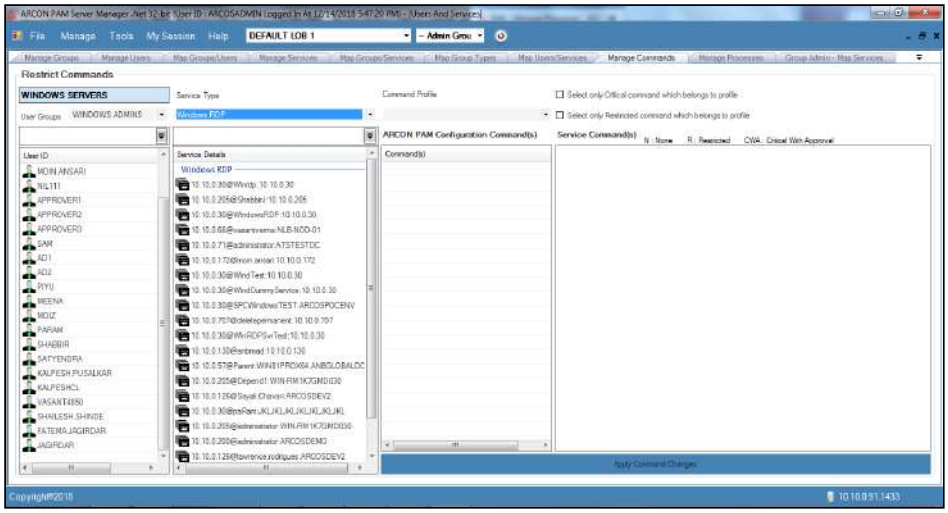
3. Go to Manage → Users and Services → Manage Commands



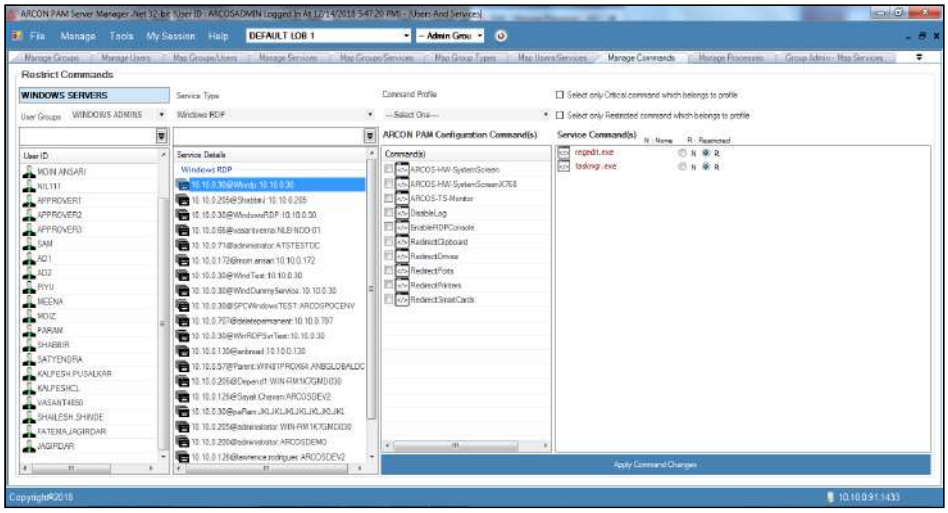
4. Select **Windows Admin User** Group. You can view the list of User ID's assigned to the group.



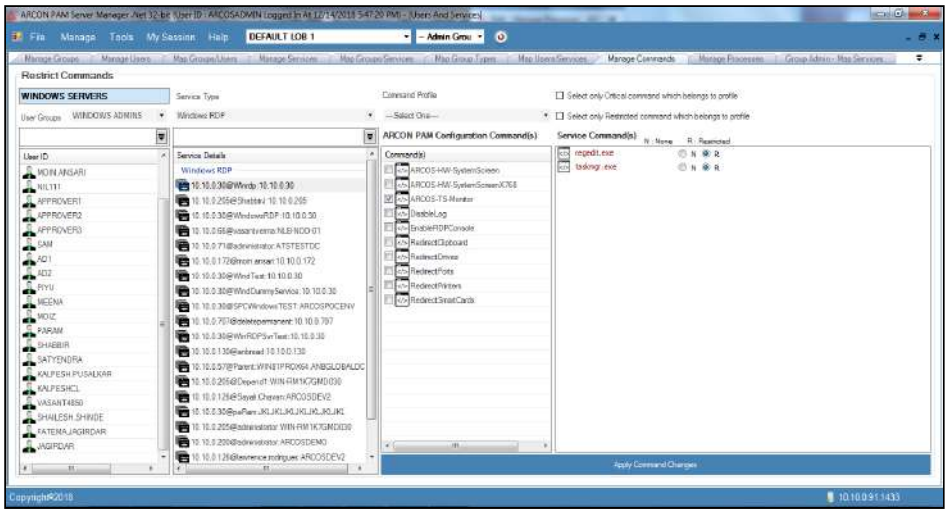
5. Select required USER ID (E.g. ARCOSADMIN) from list of User ID's.



6. Select **Windows RDP** Service Type. A list of services are displayed.



7. Select **Windows RDP** Service. The configuration commands are displayed.

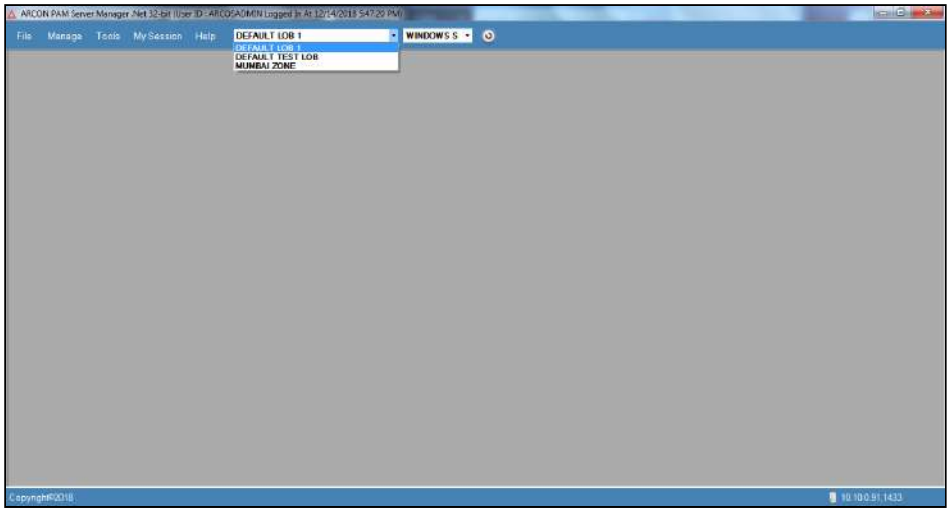


8. Select **ARCOS-TS Monitor** command and click **Apply Command Changes** to apply TS Monitor command to the Windows service.

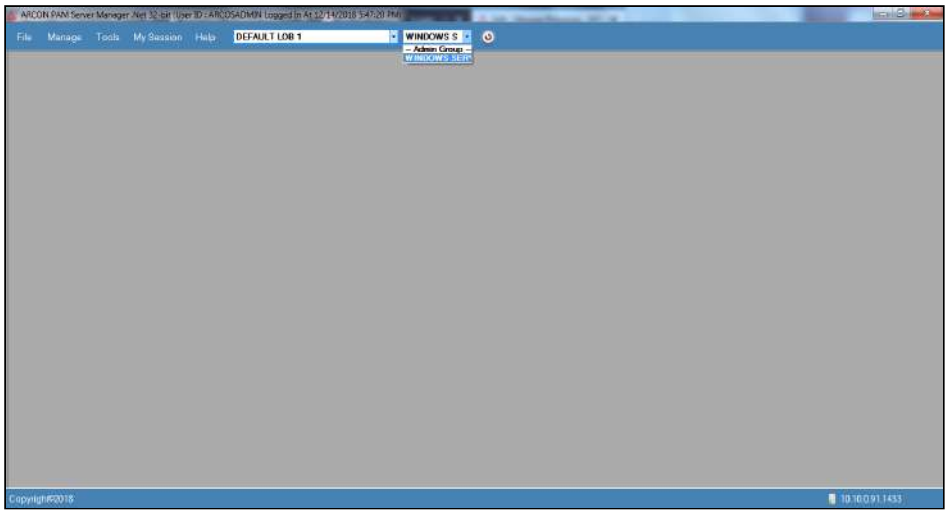
6.3.6 Assign Profile and Restrict or Elevate Processes

This section helps you to assign profile to a User. In addition, you can restrict or elevate processes available for a particular user. You can restrict or elevate processes under **Manage Processes** tab. Restricting processes will disallow the user from further usage of the processes.

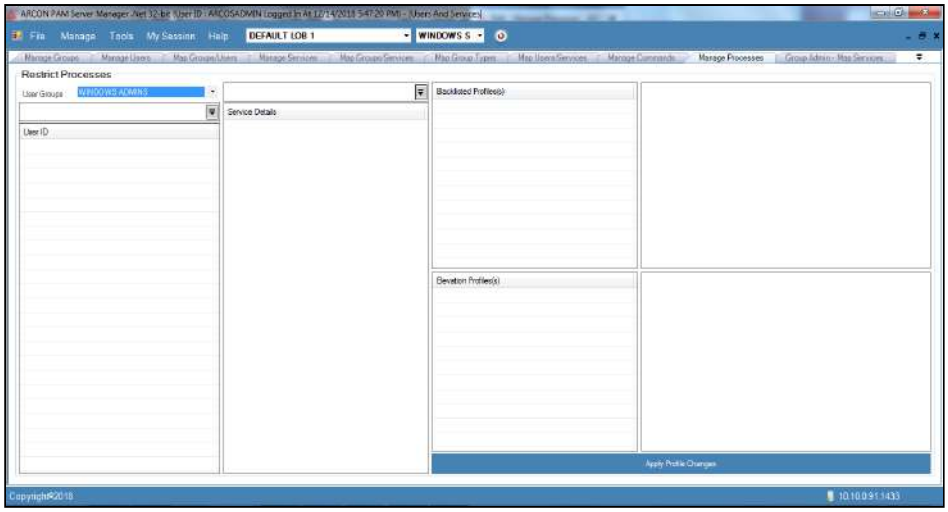
1. To assign profile and restrict or elevate processes, select the required LOB mapped to the service.



2. Select **Windows Server** group if you are a Group Admin.

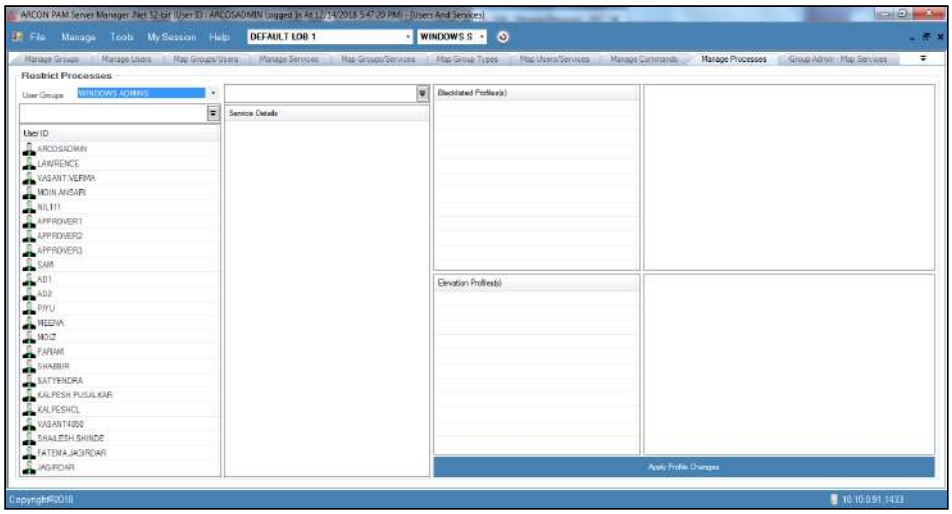


3. Go to Manage → Users and Services → Manage Processes. The following screen is displayed.

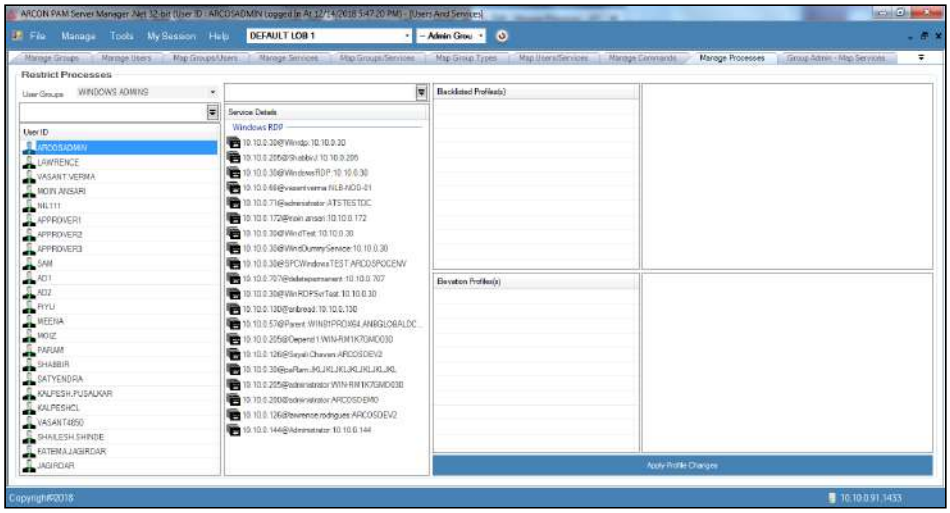


4. Select/Enter **Windows Admin User Group**. You can view a list of User Ids mapped to the User Group.

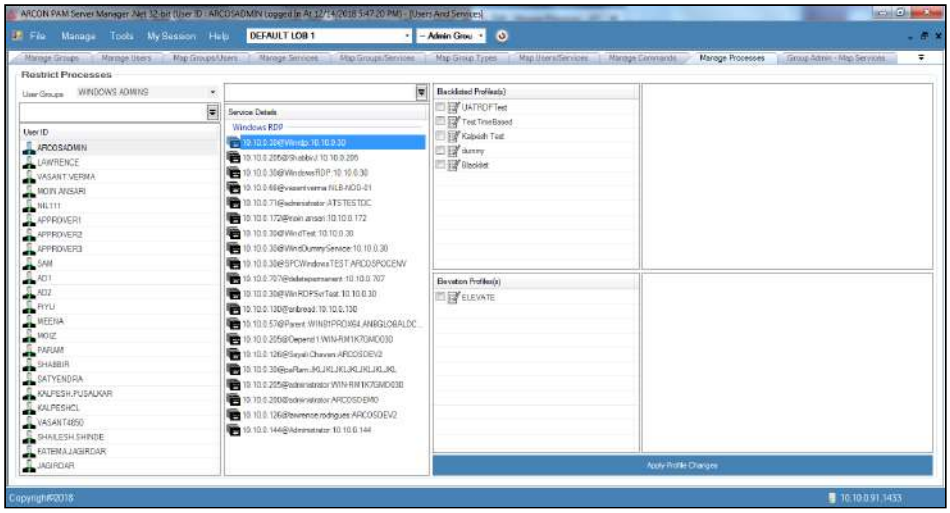
> ⚠ To search a specific set of rows, enter keywords(space separated) in the search text field of the user group, and service detail dropdown, and the relevant rows are fetched.



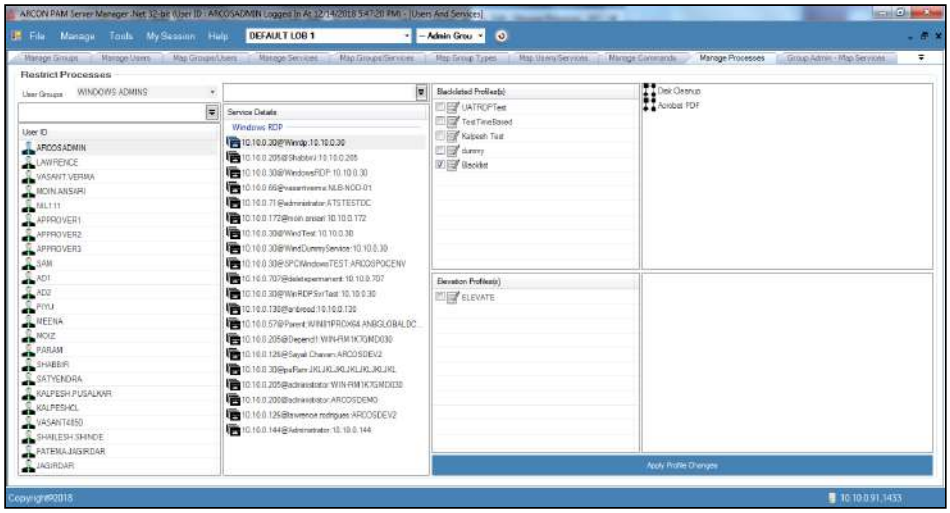
5. Select required USER ID (E.g. ARCOSADMIN) from list of User ID's.



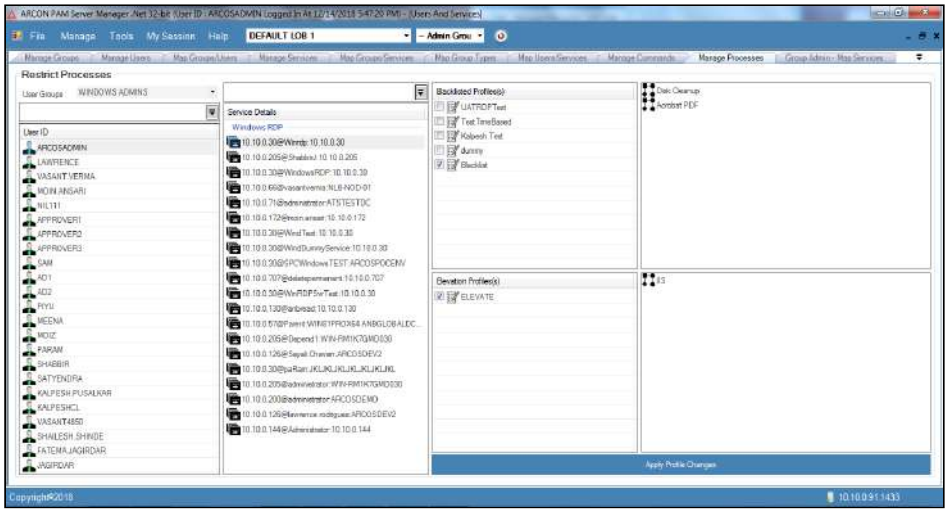
6. Select Windows RDP Service. You can view the profiles created.



7. Select the profile **Blacklist.** On right side, blacklisted processes are displayed.



8. Similarly select **Elevate** Profile, you can view the processes assigned to the profile.

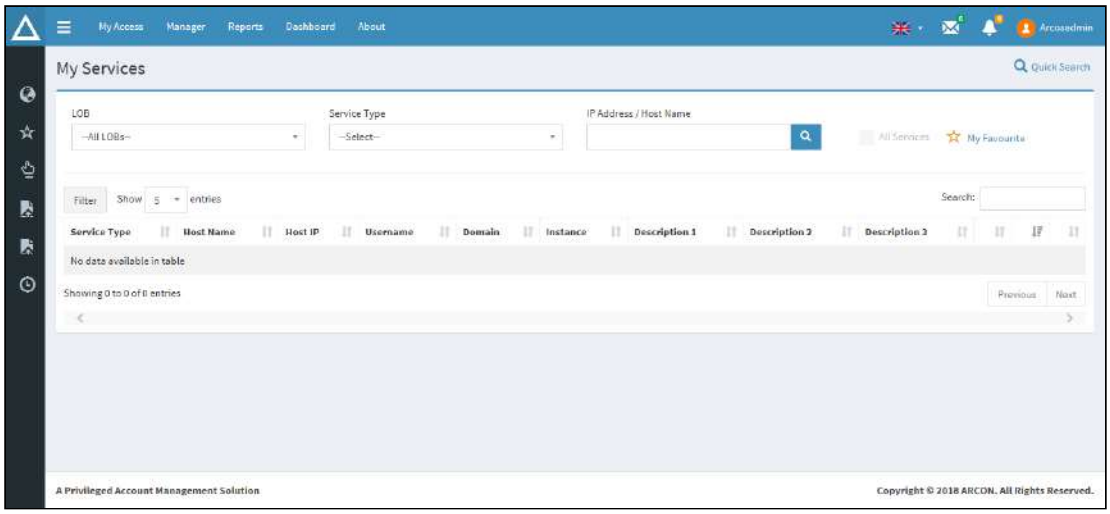


9. Click **Apply Profile Changes** to restrict or elevate processes for a windows service.

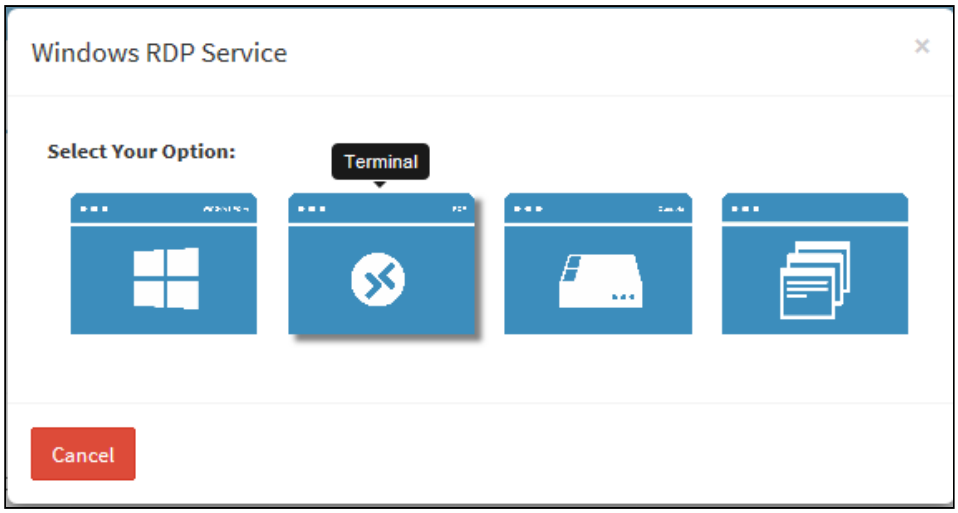
> ⚠ If a process is assigned in both Blacklist and Elevate profiles, then that process will be considered as **Blacklisted** as a rule.

After restricting Processes, follow the below steps in Client Manager

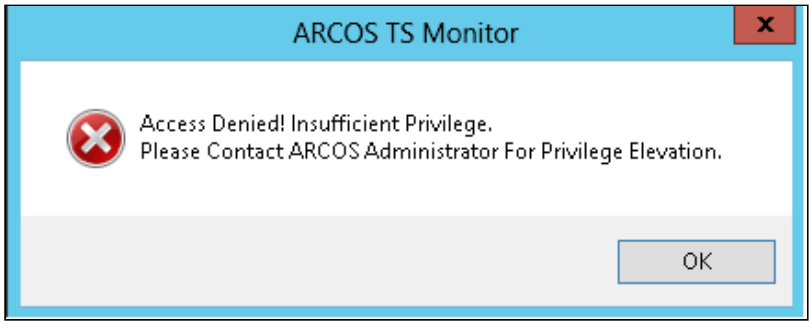
1. Select the LOB and select Windows RDP option from Service Type dropdown list.



2. Click on the service for which settings were saved in Manage Command Tab.
3. Select Terminal option to access server.



4. On selected Server, click **Run** from Start Menu.
5. Enter Blacklisted Process name and click **OK** to execute process. An error prompt for restricted command will be displayed.



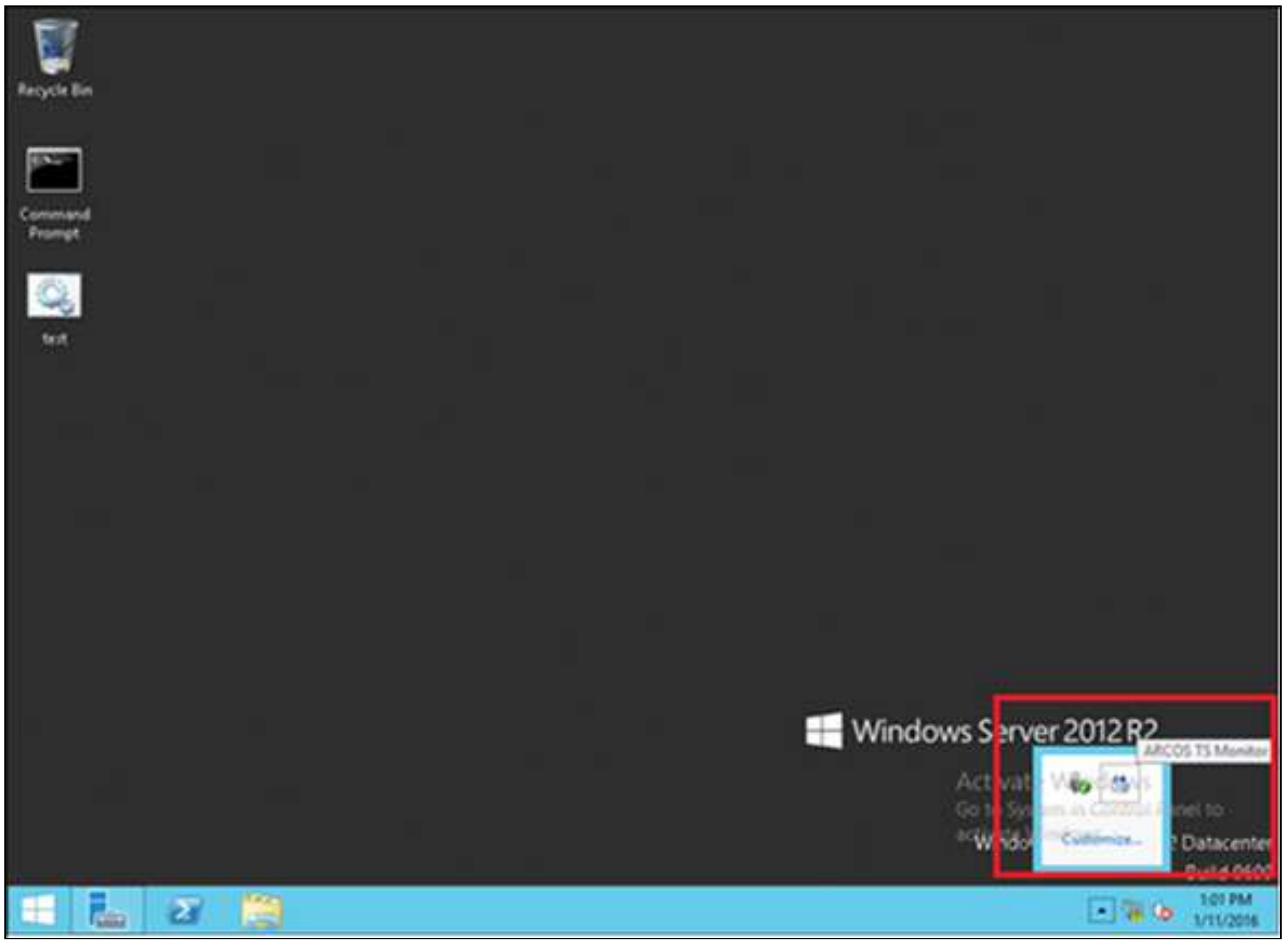
Similarly, follow the above steps to **Elevate Processes.**

On Elevating Processes follow the below steps in Client Manager:

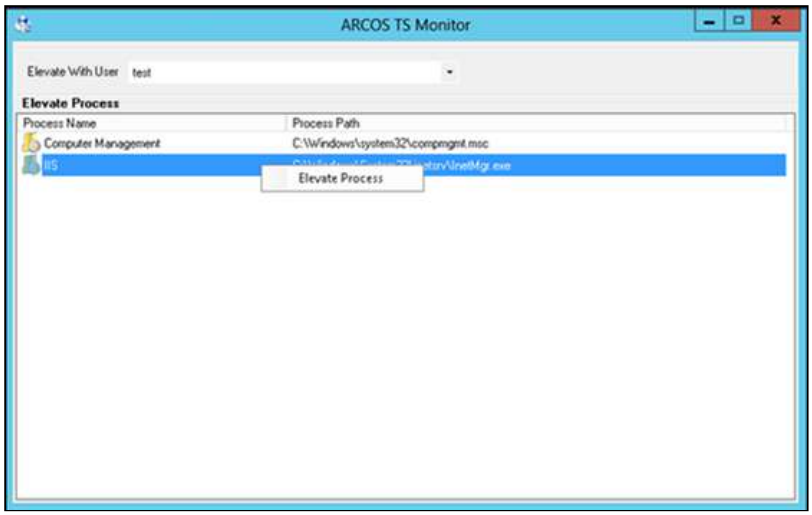
1. Select the LOB and select Windows RDP option from Service Type dropdown list.
2. Click on the service for which settings were saved in Manage Command tab.
3. Select Terminal Tab to access server.

On Server follow below steps

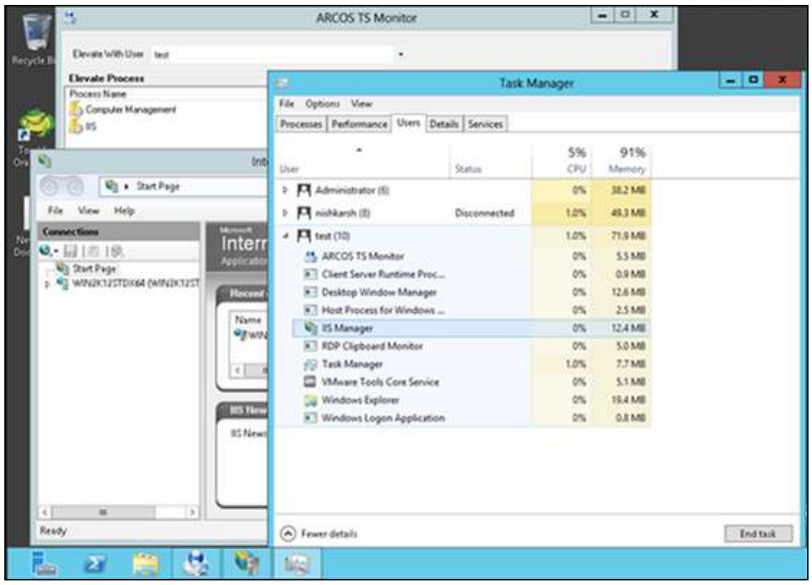
1. Select ARCOS TS Monitor window.



2. In **ARCOS TS Monitor** select **User** from drop down.



3. Select a process (E.g. Notepad).
4. Right-click and click **Elevate Process** option.
5. The selected process will be displayed (Elevated).



7 Password Management

Mismanagement of Privileged Users and their passwords is a major cause of security breaches and one of the top reasons for passwords unavailability that leads to a long recovery processes from IT failures.

ARCON PAM performs password management for privileged accounts. The following ways are used to change passwords:

- **Central Password Change:** Central Password Change Service Configuration is required while configuring agentless approach to change domain/ local accounts passwords on windows devices.
- **Manual Password Change:** Passwords can be changed manually only by Administrators who has password change privileges and should have group admin privileges for those services.
- **Automatic Password Change:** Automatic password change process refers to schedule password change service. Schedule password change service helps to change password on the target device, based on the scheduled configuration.

Password Management helps a user store and organize passwords. Password Manager offers a readily configurable password policy profiler and a password generator, where the passwords generated are unique from each other. The passwords generated are fired on the end devices including dependencies if any, such as services, task, scripts etc. The password vault is an electronic vault, which stores the privileged passwords in a highly secured manner. The vault is AES-256 bit encrypted, which is further wrapped with a proprietary encryption algorithm. The electronic vault requires authorization of users for secured printing.

The password vault secures all the passwords with its proprietary encryption methodology. Further, it provides dynamic password generation facility, which incorporates the following:

- The Vault can enforce a password policy to avoid usage of passwords that can be easily guessed.
- The password policy defines rules for the password content such as the length, combination of different types of characters, and password history.
- The password configuration is parameterized such that the user can select the appropriate parameters based on the IT Security Policy of your organization.
- Further password management module enables Administrator to perform bulk password changes on scheduled intervals.

The password management module also offers the following:

- Automated password change for various systems viz Unix, Linux, Solaris, AIX, Win2K3, Win2K8, Oracle, MS SQL, Services, DCOM etc.
- The password connectors available are both agent based and agent less. The agent less connectors offer scalability and the agent based connectors offer control on the password management activity and better error trapping.
- There are features to set password dependencies for all the systems and services which ensure that passwords on multiple systems can be common and changed at the same time. In addition, the passwords can be sequentially changed for dependent systems and services.
- The password communication between the ARCON PAM Client and Server is in encrypted form.
- There is a password request mechanism for electronically releasing the password in case hard console access is required.
- In a scenario where domain resources, services and Active Directory become unavailable, ARCON Password management offers a solution by following an agent-based approach in Windows. So for password management of local administrator account on windows server which are part of workgroup the pre-requisite is to install 'WinPWD Service' on all the respective workgroup servers. Port no 45045 is required to be opened from ARCOS SGS (Secured Gateway Server) to respective windows servers to manage Local Administrator accounts password. This WinPWD service is run as a windows service which should be running under a non interactive account (like service account-set to never expire) which holds the rights to reset the other privilege account password on domain & local. Delegate Domain User Account "write" property on attribute

''Reset Password'' and change "Change Password". This ensures password and post password actions to be performed even at the loss of connection with domain services.

7.1 Password Policy

7.1.1 Overview

Password Policy Editor allows the authorized Administrator to set the policy for password, wherein the policy complies with the standards followed by the organization. The constraints that can be set include the characters that improves the complexity of the password. In addition, the Administrator can set the positions and other settings which helps in increasing the strength of a password.

⚠ The Administrator having **Change Password Policy** privilege in Server's Privilege will only be able to set constraints for a password policy.

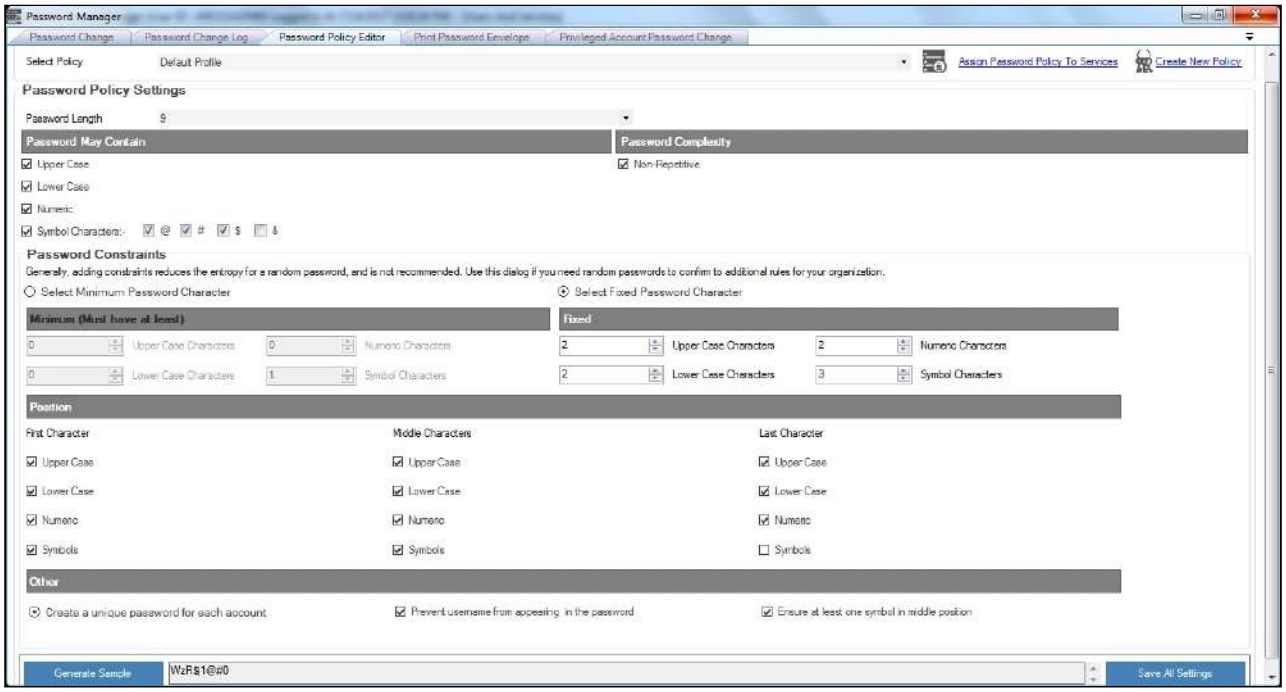
7.1.1.1 Password Policy Configuration

The process of configuring Password Policy and applying it to a Service or group of Services is explained below.

Configuring Password Policy

The following steps are followed to configure Password Policy and create new policy:

1. To configure password policy editor use the following path:
   Server Manager → Manage → Password Manager → Password Policy Editor



The **Password Policy Editor** screen displays the following fields:

Field Name	Description
Select Profile	Select to modify an existing password policy profile.
Password Policy Settings	

Password Length	Select the length for the password.
Password May Contain	
Upper Case	Use uppercase characters in password.
Lower Case	Use lowercase characters in password.
Numeric	Use numeric characters in password.
Symbol Characters	Use symbolic characters in password.
Password Complexity	
Non-Repetitive	Ensures that the characters selected for the password are unique from each other.
Password Constraints (Min must have at least)	
Select Minimum Password Character	
Upper Case	Set minimum uppercase characters in password.
Lower Case Characters	Set minimum lowercase characters in password.
Numeric Characters	Set minimum numeric characters in password.
Symbol Characters	Use symbolic characters in password.
Select Fixed Password Character	
Upper Case Characters	Set fixed uppercase characters in password.
Lower Case Characters	Set fixed lowercase characters in password.
Numeric	Set fixed numeric characters in password.
Symbol Characters	Set fixed symbolic characters in password.
Position	
First Character	Set the position of first character.
Middle Character	Set the position of middle character.
Last Character	Set the position of last character.
Other	
Create a unique password for each account	Select to create a unique password for each account.
Prevent username from appearing in the password	Select to prevent username from appearing in the password.
Ensure at least one symbol in middle position	Select to ensure at least one symbol in the middle position.

2. The **Password Policy Editor** screen allows to set the password constraints as per the company's password policy. You can set the password length, complexity, position, and other constraints. Select the required details and click **Save All Settings** button. A window pops up with the following message:
Password Policy Updated Successfully.

> ⚠ The **Generate Sample** button is used to generate a sample of the password, depending on the selected password policy settings. For example: $6#Y#&@2

3. To create new policy, click **Create New Policy** link available next to **Select Profile** dropdown list.
4. A **Create New Password Profile** window pops up.

5. Enter the name of the policy and click **Ok**. Another window pops up displaying the following message: **New Password Policy Created.**
6. Click **OK**. The new password policy is created.

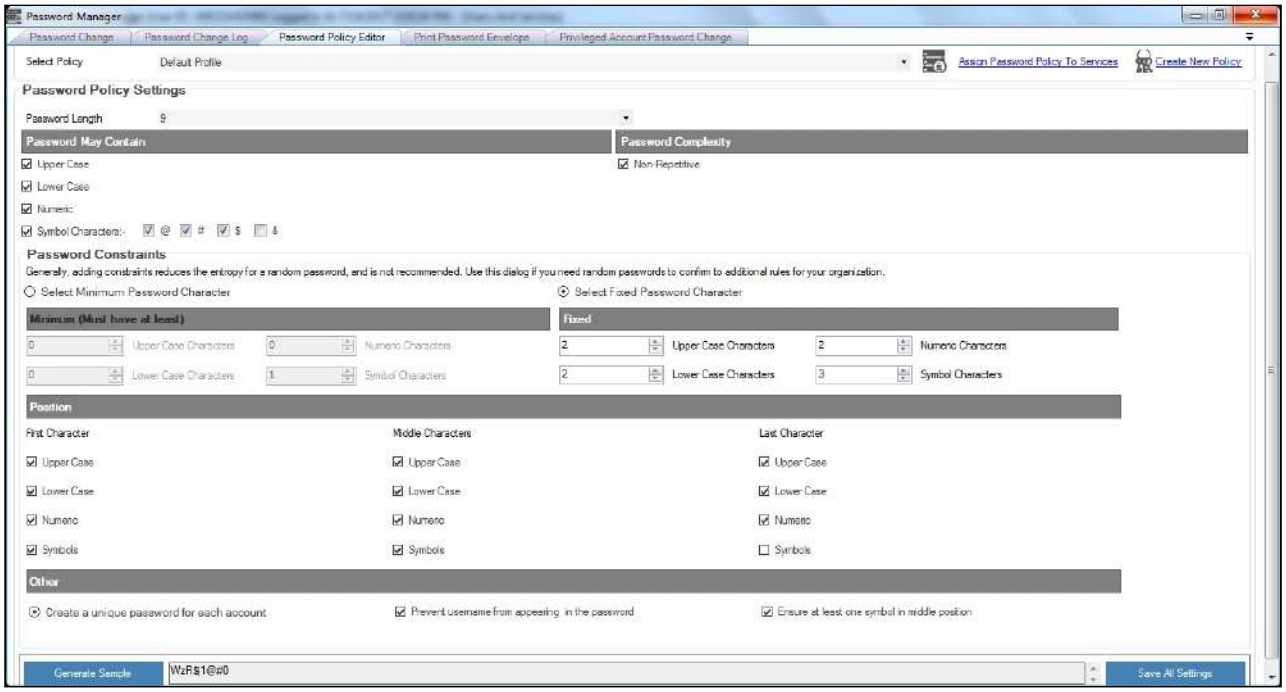
7.1.1.2 Assign Password Policy

Assigning Password Policy to a Service or Group of Services

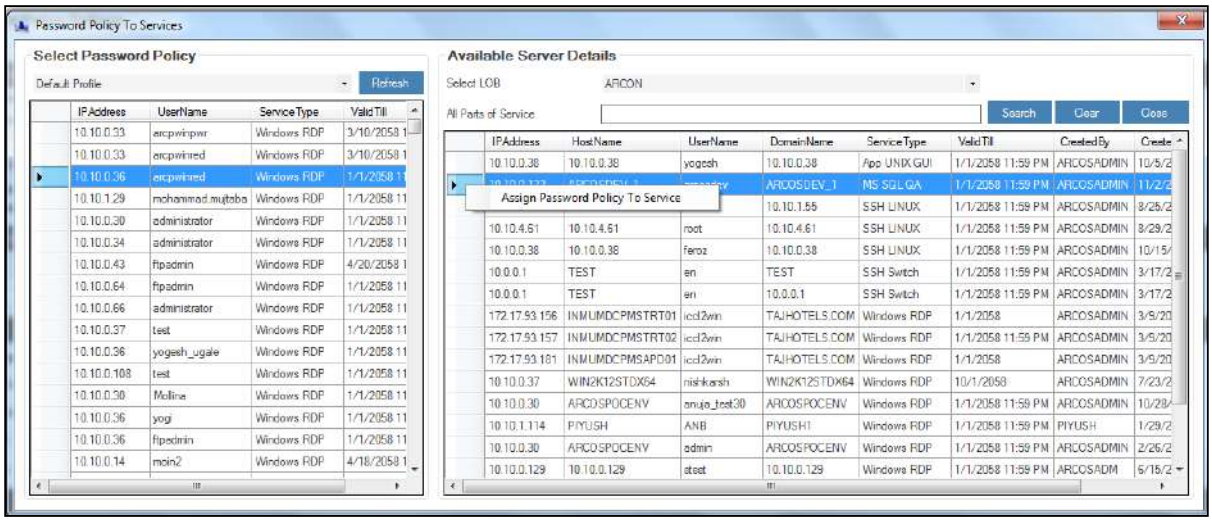
A. Assign password policy to services using **Assign Password Policy To Services** link.

The following steps are used to assign Password Policy to Services from **Password Manager**:

1. To assign password policy, use the following path:
   Server Manager → Manage → Password Manager → Password Policy Editor



2. Click **Assign Password Policy To Services** link available next to **Select Profile** drop down list.
3. The **Password Policy To Services** screen is displayed. On **Select Password Policy** pane, select policy from the **Select Password Policy** dropdown list and click **Refresh**.
4. On **Available Server Details** pane, select LOB from the **Select LOB** dropdown list and click **Search**. The available services in the selected LOB will be displayed.
5. Right click on the service and click **Assign Password Policy To Service**.

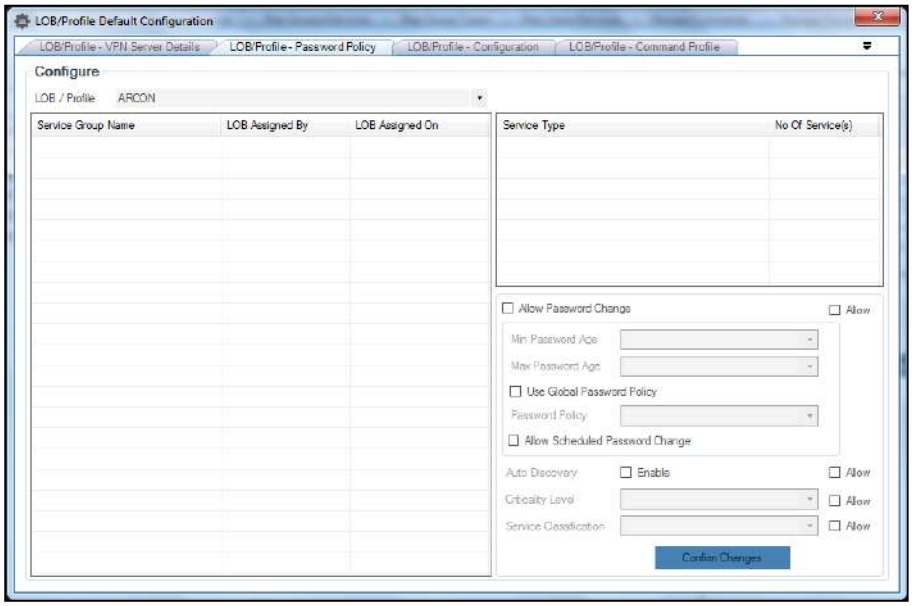


6. A window pops up displaying the following message:
   Password Policy Assigned To Selected Service.
7. Click **OK**. The password policy is assigned to the selected service.

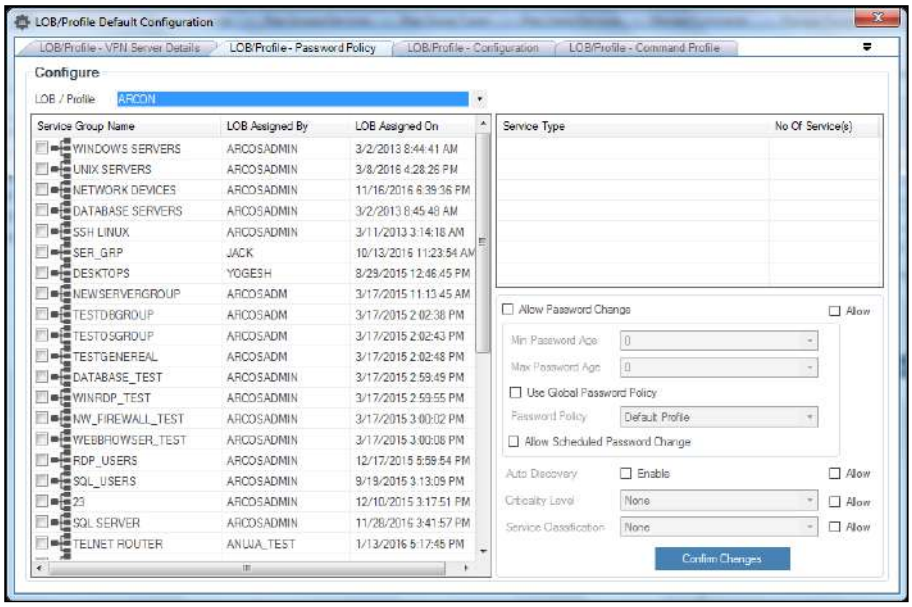
B. Assign password policy to Services using **LOB/Profile Default Configuration**.

The following steps are used to assign Password Policy to Group of Services:

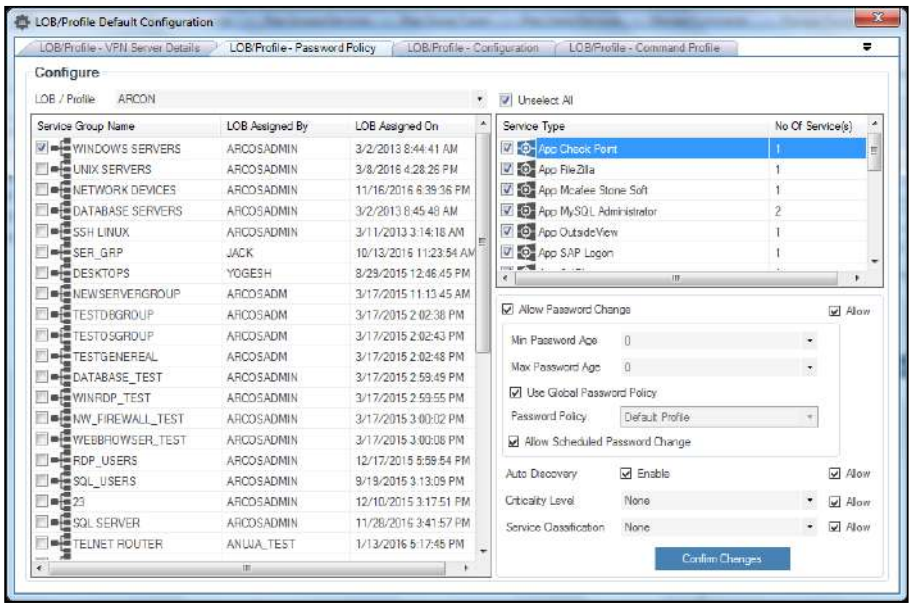
1. To assign password policy, use the following path:
   Server Manager → Tools → Advanced Configuration → LOB/Profile Default Configuration → LOB/Profile – Password Policy
2. Select the LOB or profile from the **LOB/ Profile** dropdown list.



3. A list of service groups are displayed in the grid.



4. Select the checkbox from the **Service Group Name** list. It displays the list of services for that particular group under **Service Type** grid.

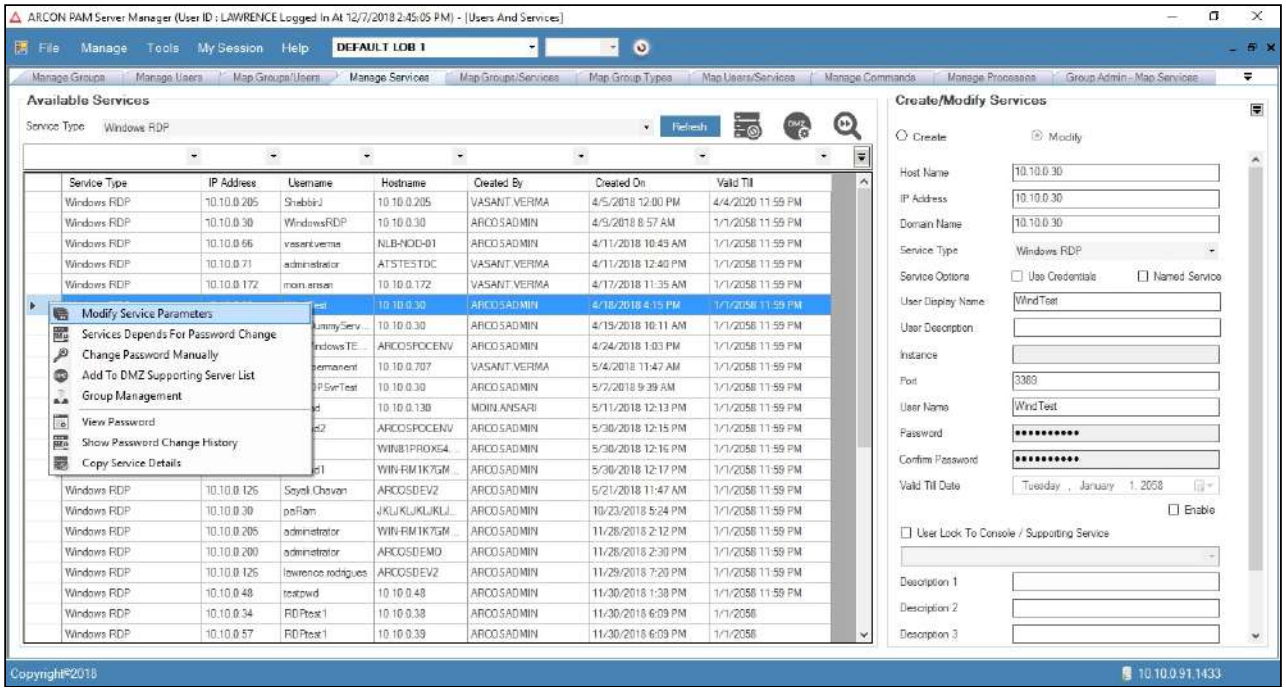


5. Select a type of service from the **Service Type** list. This will enable you to set automated change passwords for that particular service type. It will also allow you to set the password policy and you can also set auto discovery, criticality level, and service classification for the password change process.
6. Select required details and click **Confirm Changes** to apply configuration to Services.

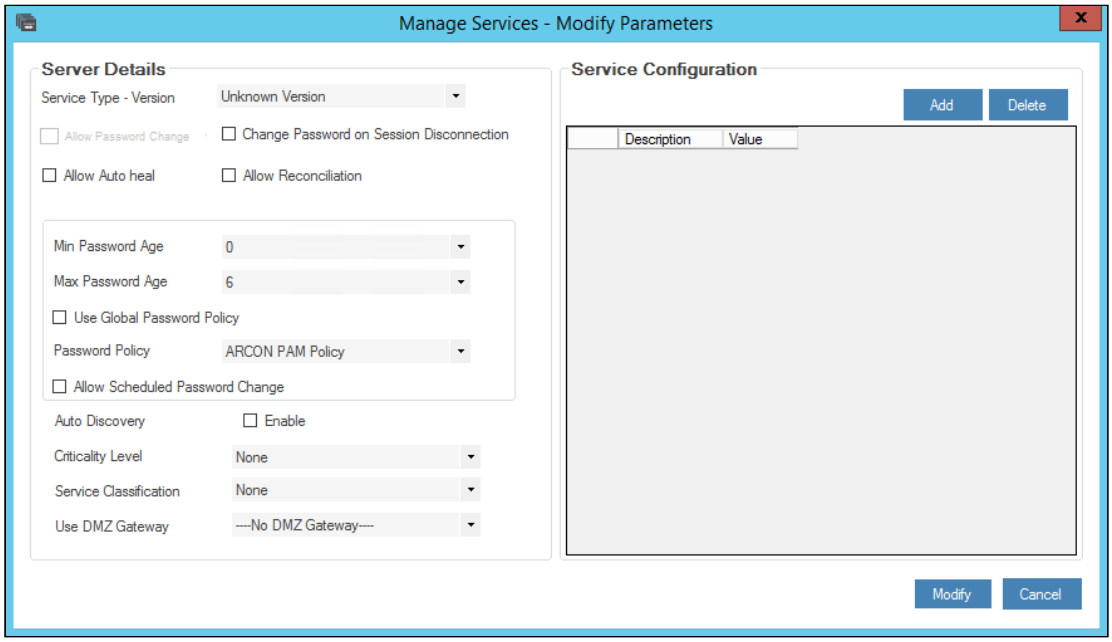
C. Assign password policy to a particular Service from **Manage Services**

The following steps are used to assign Password Policy to a particular Service:

1. To assign password policy, use the following path:
   Server Manager → Manage → Users and Services → Manage Services
2. Right click on the service for which you want to schedule the password change process and choose **Modify Service Parameters** option.



3. The **Manage Services - Modify Parameters** screen is displayed.



> ⚠ The services available in the grid are displayed based on the LOB and service type selected from the **Select LOB/Profile** drop down list (in the home screen Server Manager) and **Service Type** drop down list respectively. Click **Refresh** button after selecting the **LOB** and **Service Type**.

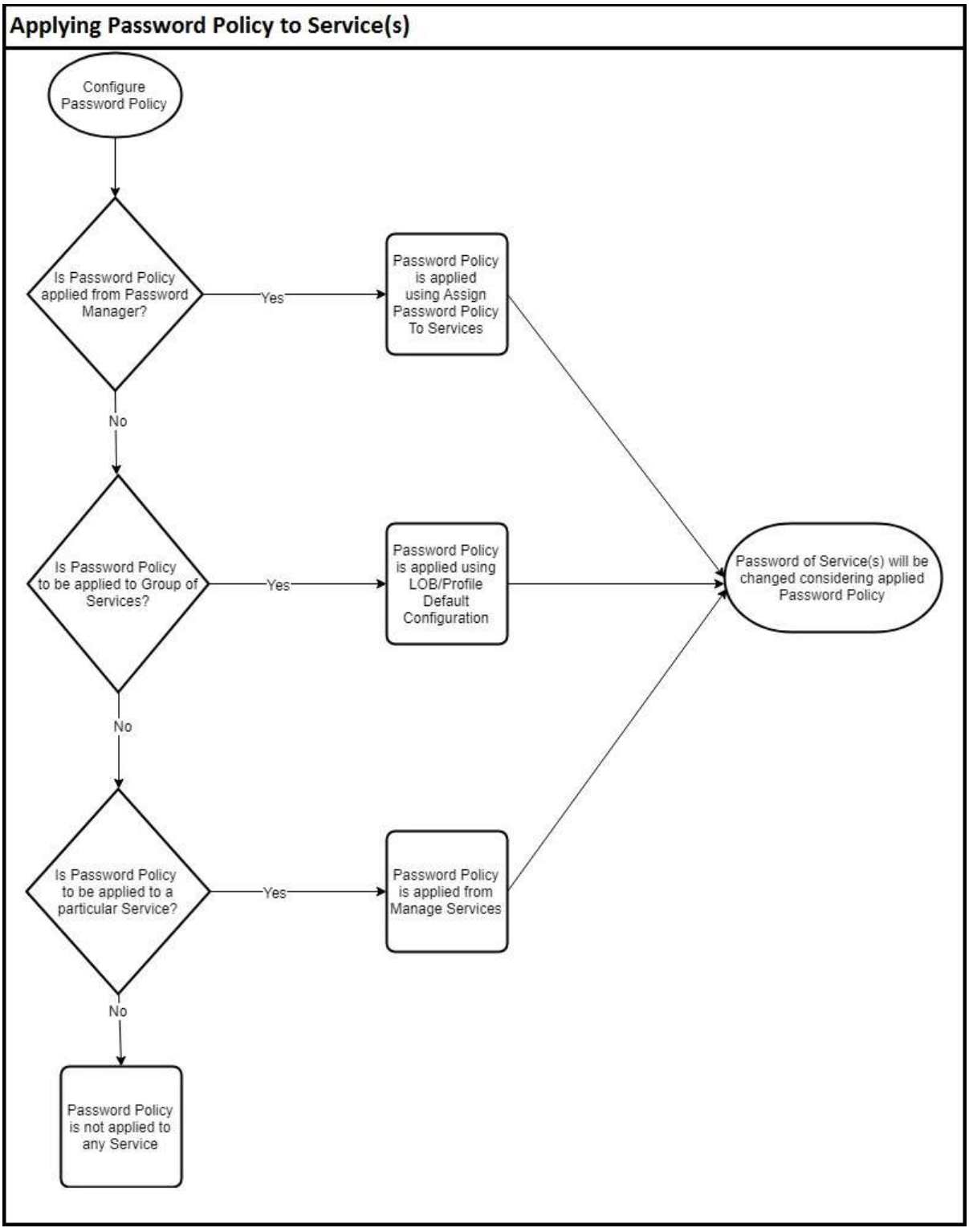
The **Manage Services – Modify Parameters** screen displays the following fields:

Field Name	Description
Change Password on Session Disconnection	The password of the service changes after the session is closed from the PAM.
Allow Auto heal	To enable auto-healing for the service.
Allow Reconciliation	To enable reconciliation for the service.
Min Password Age	Select minimum days for scheduled password change process. ⚠ Password of Service will not be changed before the defined minimum days. Eg.:If you configure Minimum Password Age as 3; then password change process cannot be performed before 3 days.
Max Password Age	Select maximum days for scheduled password change process. ⚠ The password change process will be scheduled automatically depending on the selected max password age field.
Use Global Password Policy	Select to enable the global policy configured for password change process.
Password Policy	Select the password policy. ⚠ By default, **Default Profile** is selected. You can create your own password policy, save it and select it in this field.
Allow Scheduled Password Change	Select to enable/configure scheduled password change process. ⚠ By enabling this checkbox the password change process for the selected service will be scheduled according to the selected min and max password age and selected password policy or the global password policy.

4. Select the details and click **Modify**. A window pops up displaying the following message: **Service Parameters Updated**
5. Click **OK**. The password change process for the selected service is scheduled and the password will changed according to configured password policy.

7.1.1.3 Process Flow Diagram

Following is the process flow diagram for configuring Password Policy.



7.2 Manually change password for single or multiple services

Password Change is a process where you can change password of all the services in a group or a particular service from a service group. A user is authenticated before trying to change password of a service. Authentication is performed based on the configuration value set in **Settings**.

If the configuration value for **Change Password – No of User(s) Authentication** in **Settings** is set to:

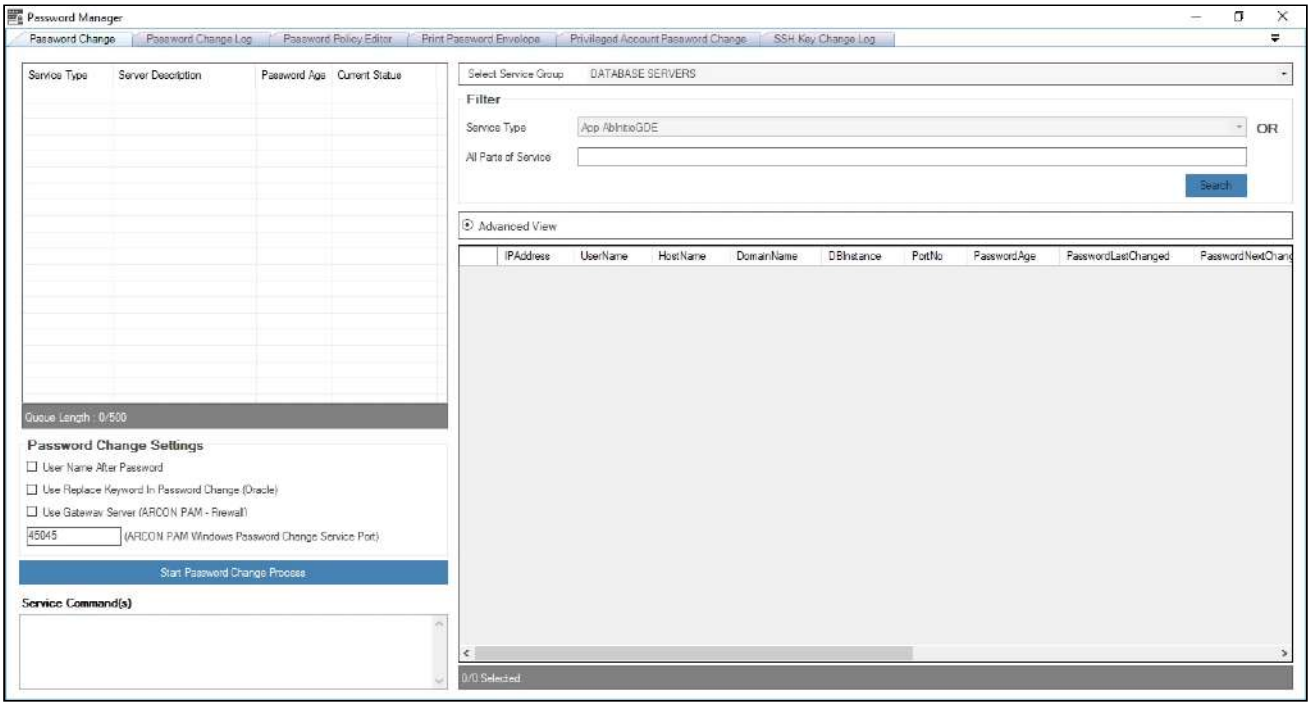
- 1: A user is authenticated only once.
- 2: A user is authenticated twice.

- The Administrator having **Change Password** privilege in Server's privileges will only be able to perform password change process.
- The **Authorising User 1** should have **Password Change Process Approver** privilege in Server's Privileges, to approve the user trying to perform password change process.
- The **Authorising User 2** should have **Password Change Process Approver** privilege in Server's Privileges and **Support View Server Password** privilege in Client Manager's Privileges, to approve the user trying to perform password change process.
- The **Authorising User 2** should be a **Group Admin** of the service group which has been selected for password change process.
- If value for **Only Server Group Admin Can Perform Password Change - Is Enabled** in **Settings** is **Enabled,** then **Change Password** privilege under **ARCON PAM Group Admin Privileges** should be assigned to Administrators along with above mentioned privileges to change password of service.

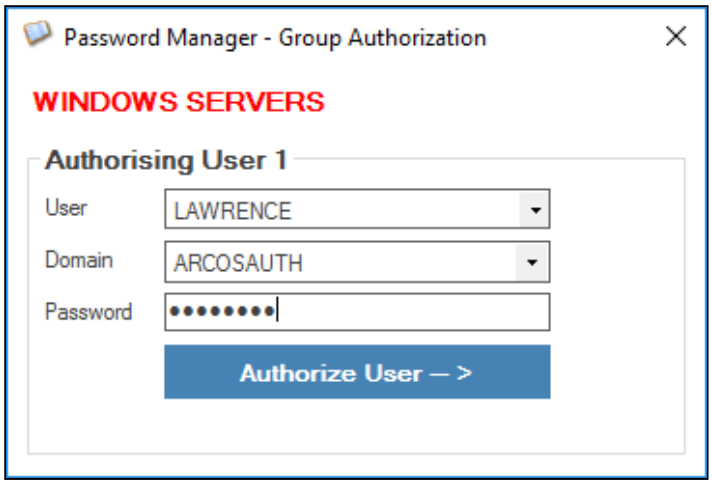
To manually change password for multiple services:

To manually change password for multiple services use the following path:

Manage → Password Manager → Password Change

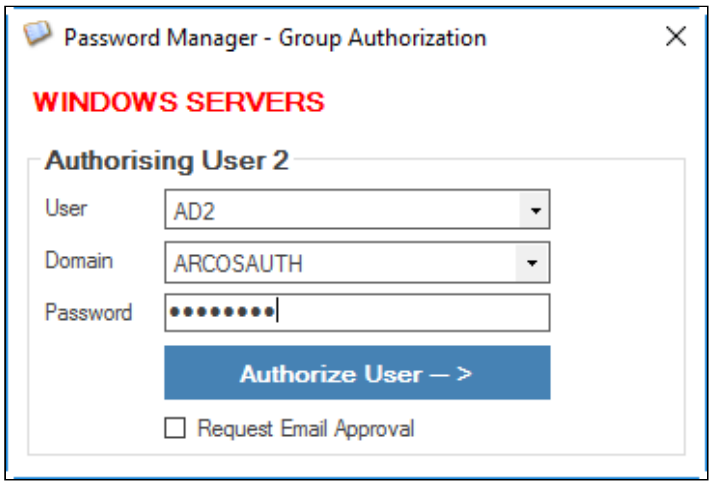


1. Select the service group from the **Select Service Group** dropdown list. A **Password Manager – Group Authorization** window pops up to authorize the user.

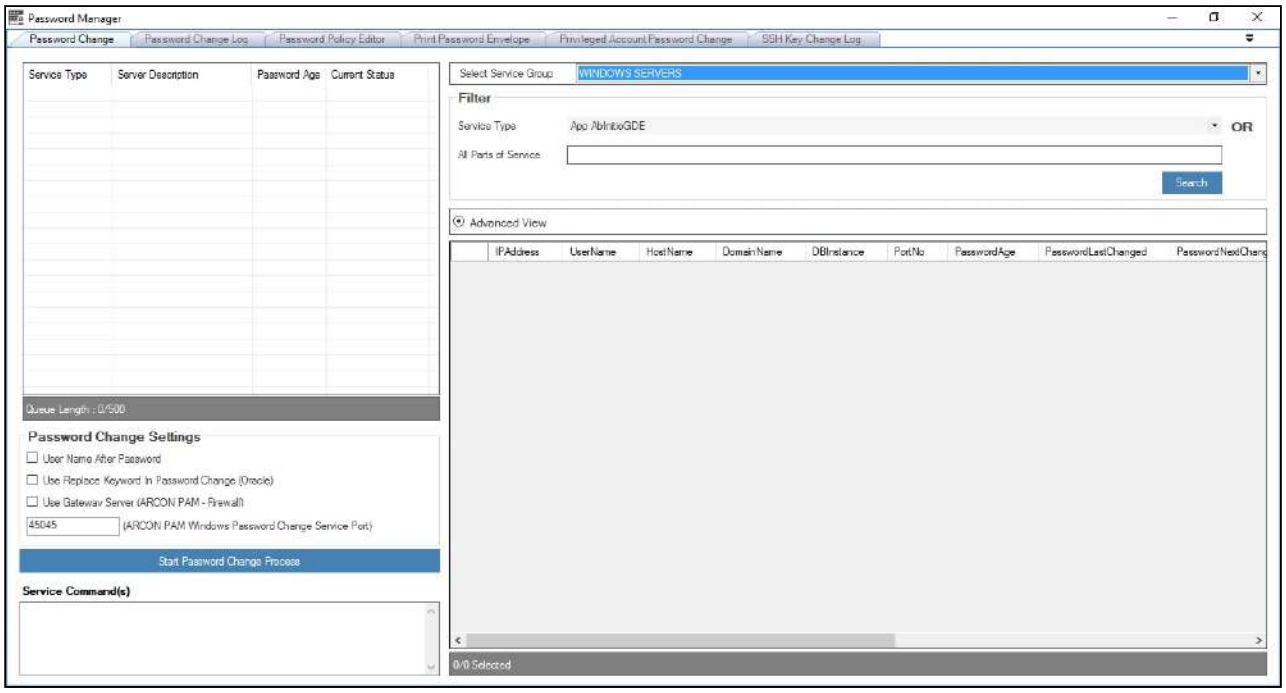


⚠ The service groups available in the **Select Service Group** dropdown list are displayed based on the LOB selected from the **Select LOB/Profile** dropdown list available in the home screen (Server Manager).

2. The **Authorising User 1** should select the username and domain from the **User** and **Domain** dropdown list respectively and enter password in the **Password** text field.
3. Click **Authorize User** → button, to approve the user trying to change the password. Another **Password Manager – Group Authorization** window pops up for second level authorization.

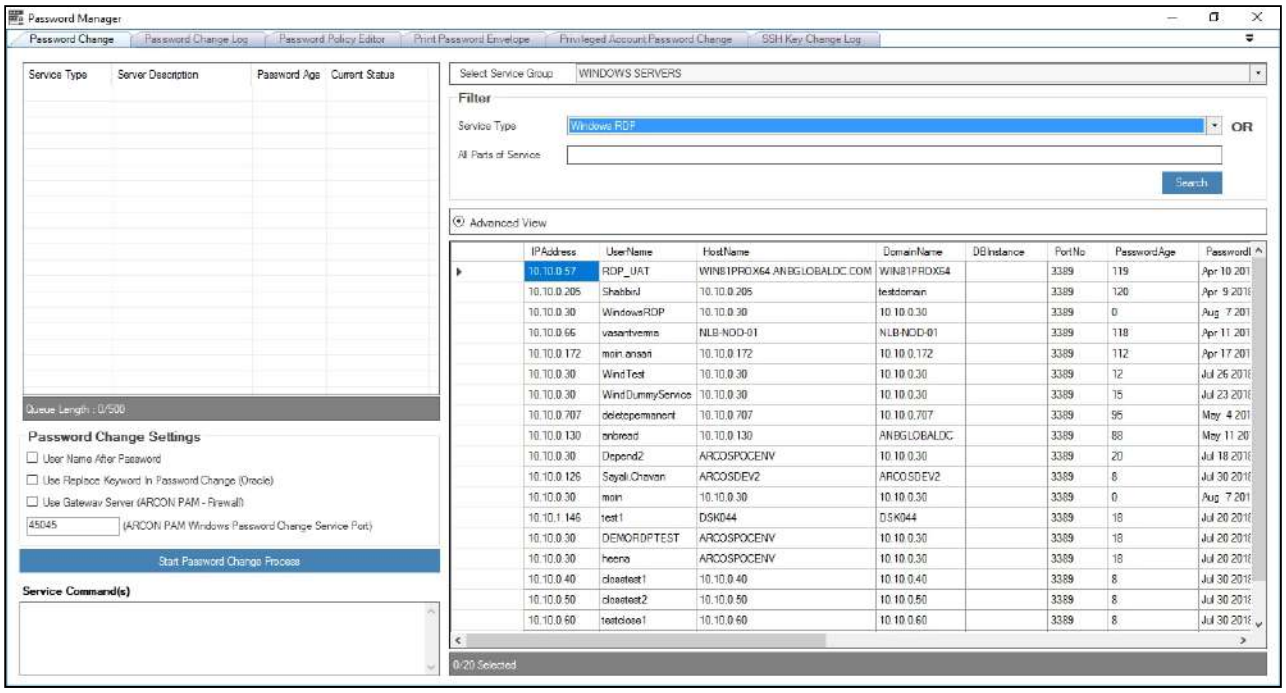


4. The **Authorising User 2** should select the username, domain, and enter the password and then click on **Authorize User** → button. The **Service Type** filter is enabled after two levels of authorization.

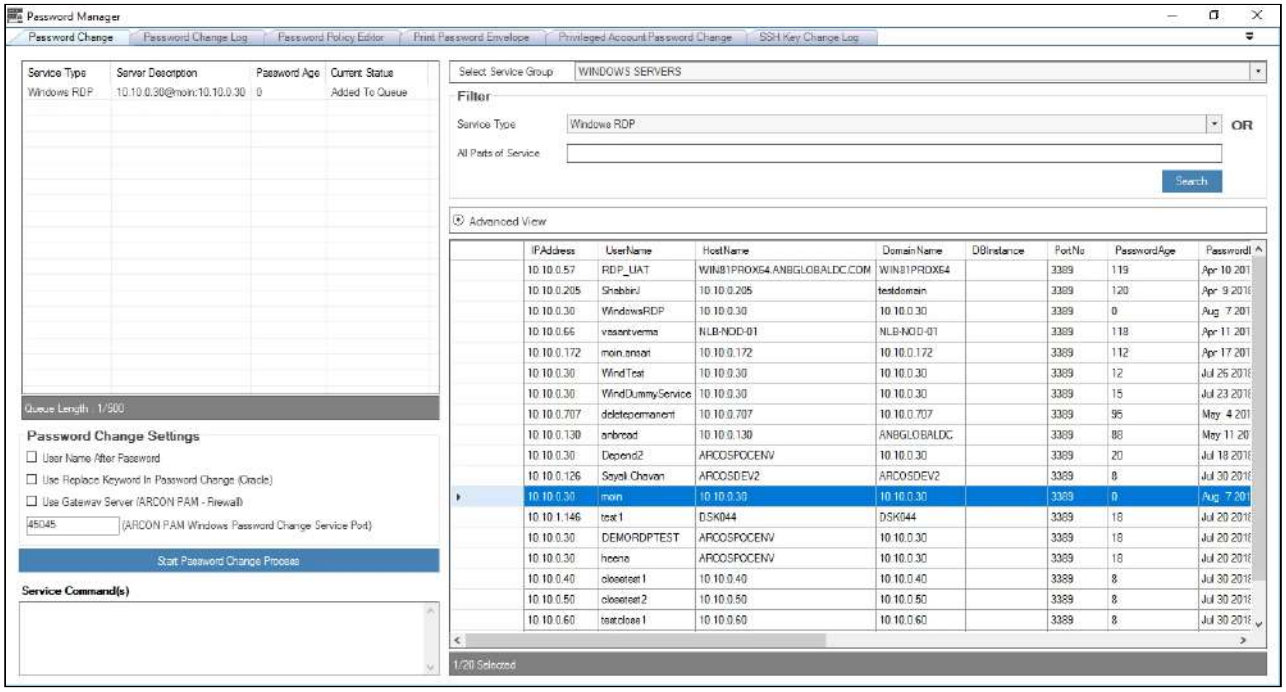


- In some cases, wherein an **Authorising User 2** is not available to approve the user trying to change the password, then **Request Email Approval** checkbox can be selected which will display the email id of the **Authorising User 2**. Once the email ID of the approver is displayed, click **Request Approval** button, an email is send to the approver, where he can approve or reject the password change request.
- You can only view the **Request Email Approval** option, if you set the configuration value for **Password Manager – Group Authorization (Request Email Approval) – Is Enabled** option **Enabled** in **Settings**. By default, the value is **Disbaled**.

5. Select the type of service from the **Service Type** dropdown list. A list of service instance(s) for the selected service type are displayed.
6. Alternatively, Enter IP address in **All Parts of Service** text field and click **Search** button.



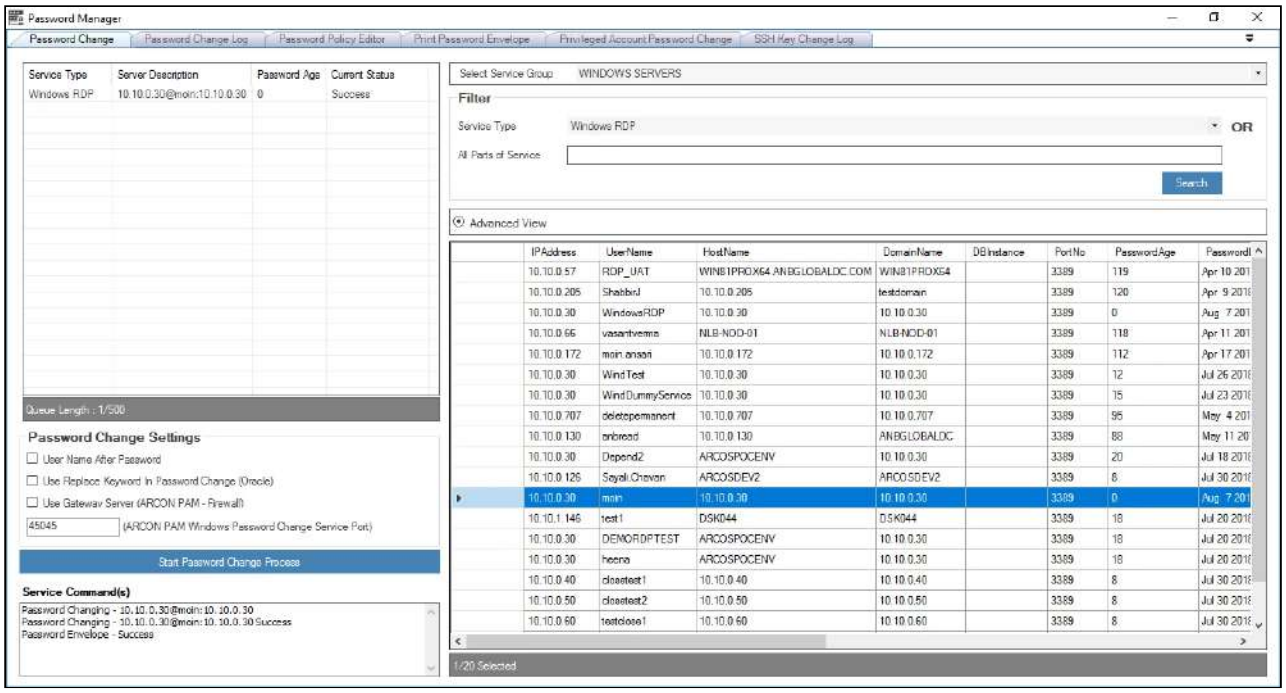
7. Double click the  icon, displayed on the left side of the selected record in the grid. The selected service is displayed in the queue on the left pane.



8. Alternatively, select and right click on the record from the grid, you can view two options to add the record in the queue on the left pane.

- **Add To Password Changing Queue**: To add the selected service from the grid in the queue on the left pane.
- **Add To Password Changing Queue & Delete From List:** To add the selected service in the queue on the left pane and delete the record from the grid list.

9. Click **Start Password Change Process** button to start the password change process for all the records in the queue. On successful completion of password change process, a message is displayed in **Service Command(s)** field.



⚠

- You can configure the necessary options in Password Change Settings, before you start the password change process.
- The following options can be configured:
  - **User Name After Password:** Enable User Name After Password, to use username after password while configuring password.
  - **Use Replace Keyword in Password Change (Oracle):** Enable Use Replace keyword in Password Change (Oracle), to use Replace keyword in Password change process.
  - **Use Gateway Server (ARCON PAM – Firewall):** Enable Use Gateway Server (ARCON PAM Firewall), to route the password change process through gateway server.
  - **ARCON PAM Windows Password Change Service Port:** Enable ARCON PAM Windows Password Change Service Port, when you require port for windows password change process. The default value is 45045.

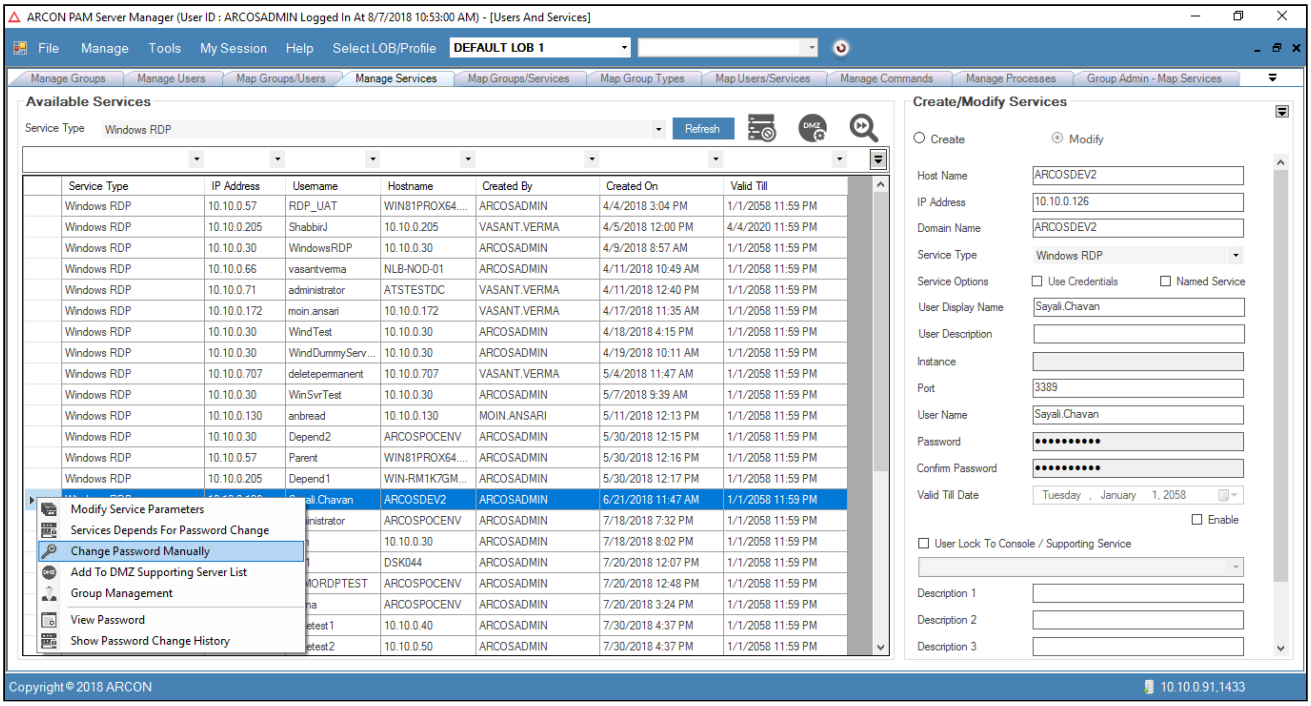
Alternative, for Manual Password Change process for Single Service:

This section helps to manually change the password for a particular service.

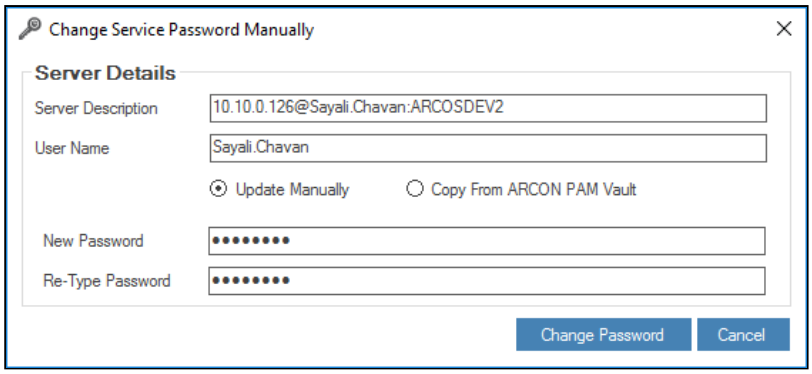
To manually change password for a particular service:

To manually change the password for a particular service use the following path:

Manage → Users and Services → Manage Services



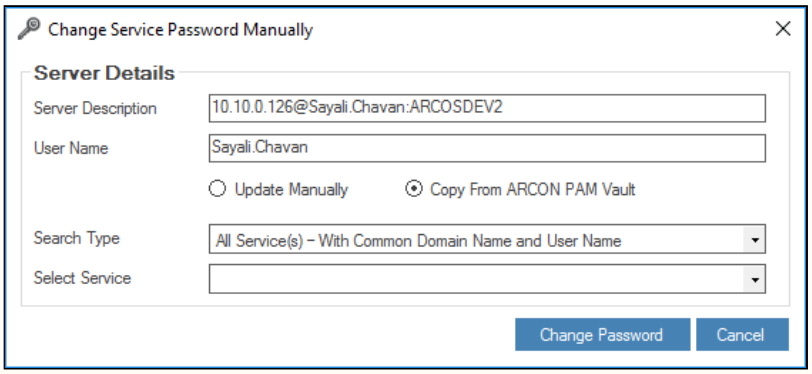
1. Right click on the service. A multiple options list is popped up. Click on the **Change Password Manually** option. The **Change Service Password Manually** window pops up.



> ⚠ The services available in the grid are displayed based on the LOB and service type selected from the **Select LOB/Profile** dropdown list (in the home screen Server Manager) and **Service Type** dropdown list respectively and then click **Refresh**.

2. Enter the password details and click **Change Password** to change the password.

> ⚠
> - To update the passwords manually, select **Update Manually** radio button.
> - To update the password using existing service for **All Service(s) – With Common Domain Name and User Name** or **All Service(s) – With Common IP Address**, select **Copy From ARCON PAM Vault** radio button.



⚠ While creating service and manually changing password of any existing service, a prompt will be displayed stating:
Do you want to Vault With New Password Immediately?
On User's confirmation, a new password will be generated by ARCON PAM. The new generated password will be vaulted in ARCON PAM and updated on Target Device.

⚠ To enable Password Change through Gateway Server, enable **Use Gateway Server (ARCON PAM - Firewall)** from **Password Change Defaults (Default Configuration)**.

7.3 Windows Connection Password Dependency

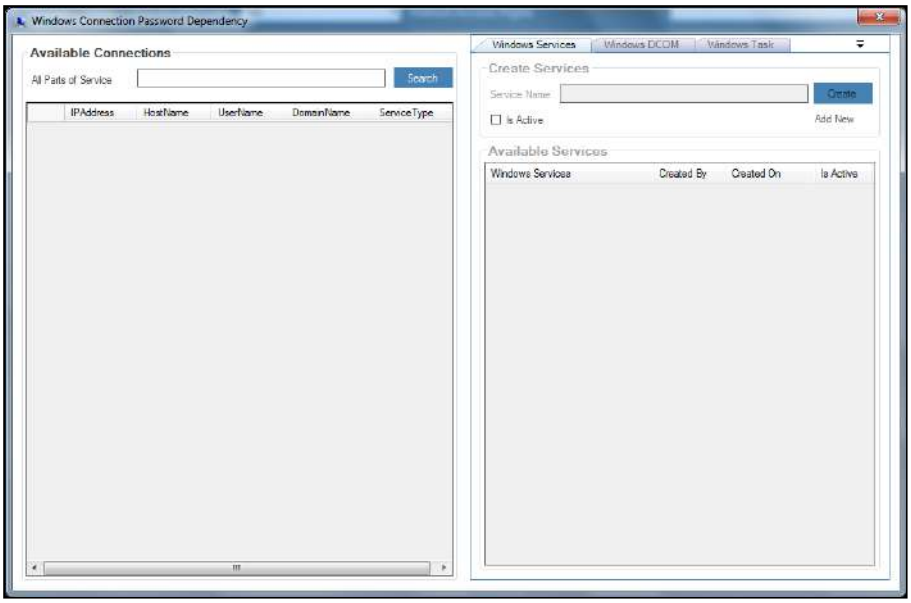
This feature helps you to map all the different Windows Services, Windows DCOM, and Windows Task that are depended on any service of a particular server, so if the password is changed for a particular service with Password Manager then the password of the dependent services, DCOM and tasks are also changed.

⚠

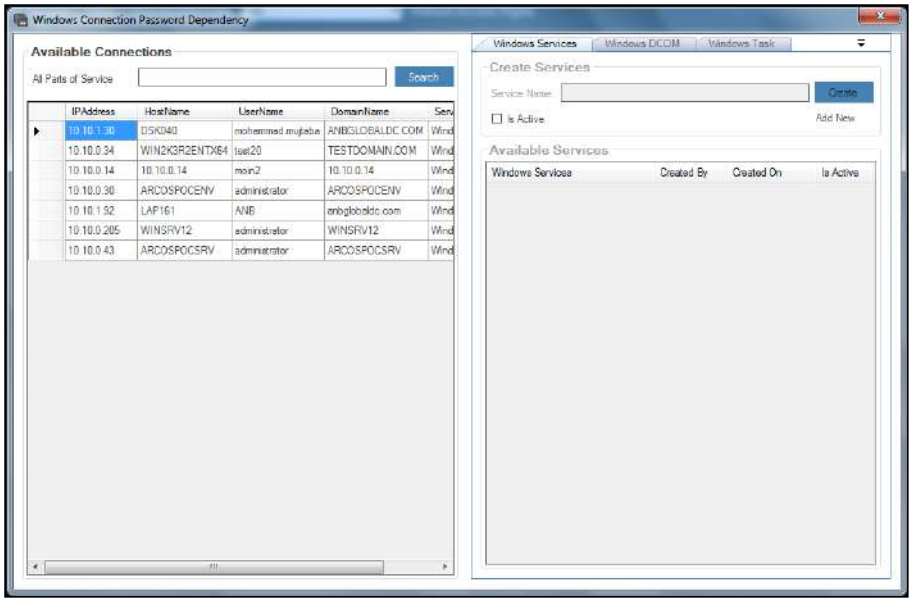
- The Administrator having **Windows Connection Password Dependency** privilege will only be add Windows services and DCOM to ARCON PAM services.
- The Administrator having **Windows Connection Service** privilege will only be add ARCON PAM Windows service to a service created in ARCON PAM.
- The Administrator having **Windows Connection DCOM** privilege will only be add DCOM service to a service created in ARCON PAM.
- The Administrator having **Windows Connection Task** privilege will only be add Windows service to a service created in ARCON PAM.

The following path is used for Windows Connection Password Dependency:

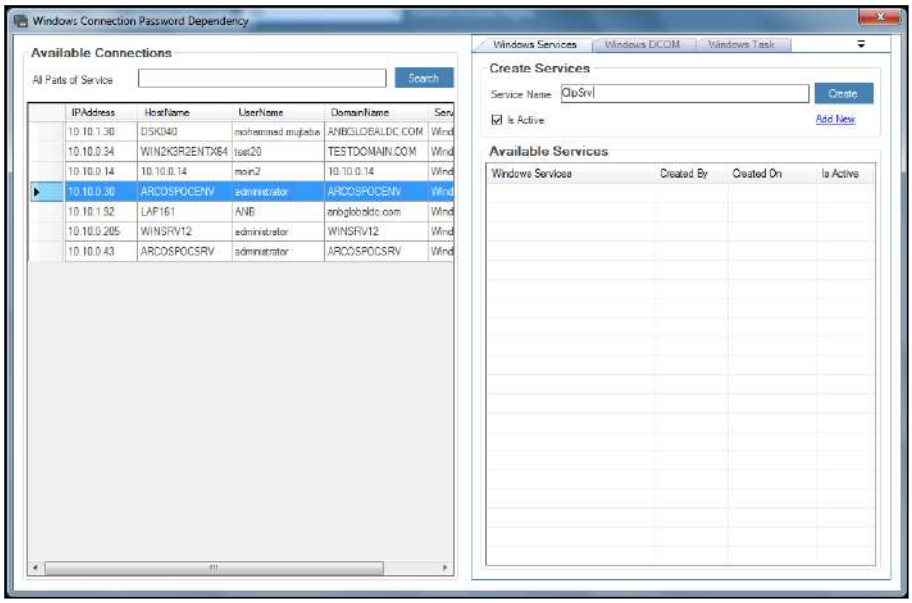
Manage → Windows Connection Password Dependency



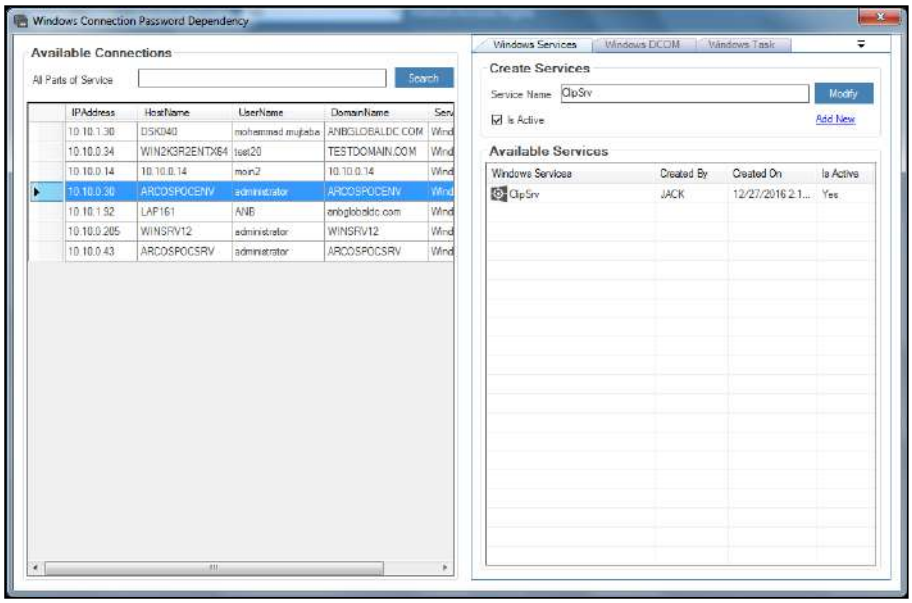
1. Click **Search** button to search for a particular IP address. It displays all the available Windows services.



2. Select and double click on  icon. This will enable the **Create Services** section.



3. Enter the service name in the **Service Name** text field and click on **Create** button. A window pops up with the following message:
   New Service Created
4. Click **OK** button. You can view the service in the **Available Services** grid.



- The **Is Active** checkbox is used to enable or disable the selected Windows Services, DCOM or Task dependency on the selected service of a server.
- Similarly, you can follow the above steps for Windows DCOM and Windows Task.
- The **Add New** link allows to add new services.

7.4 View Password of Service

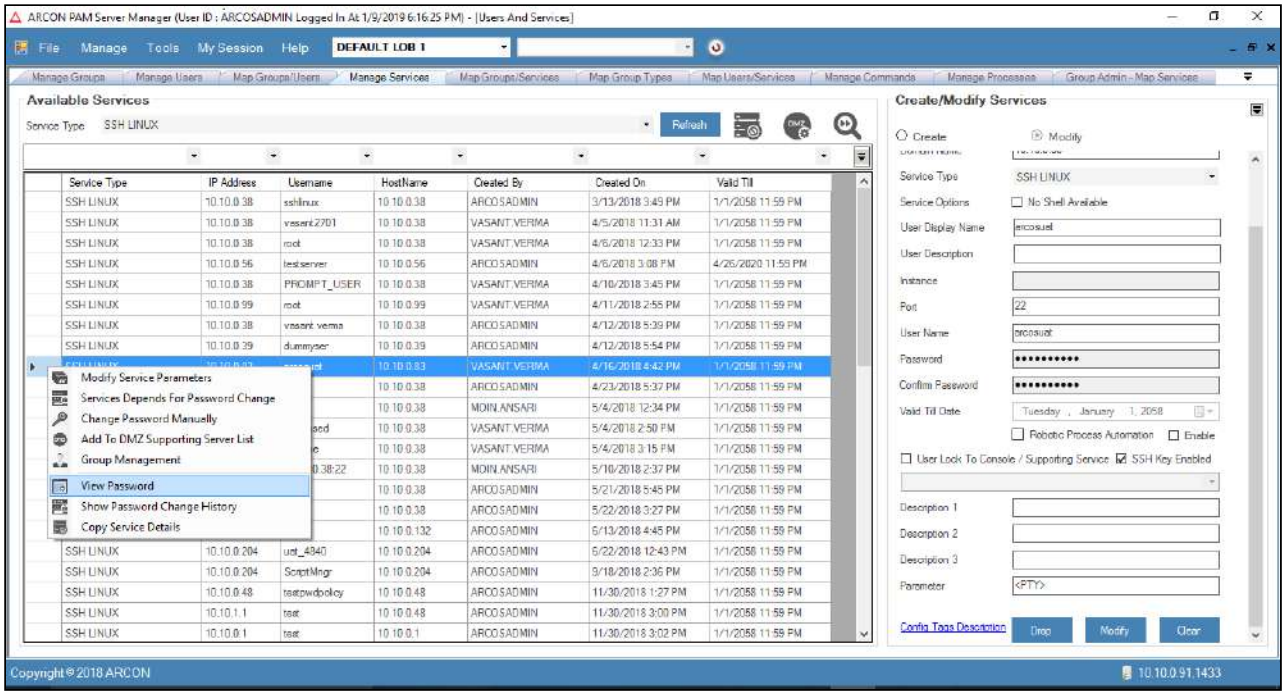
This section helps you to view the password of any services configured in ARCON PAM.

⚠ The Administrator having **View Server Password** privilege in Server's Privileges will only be able to view password / SSH Key of services.

To view the password / SSH Key use the following path:

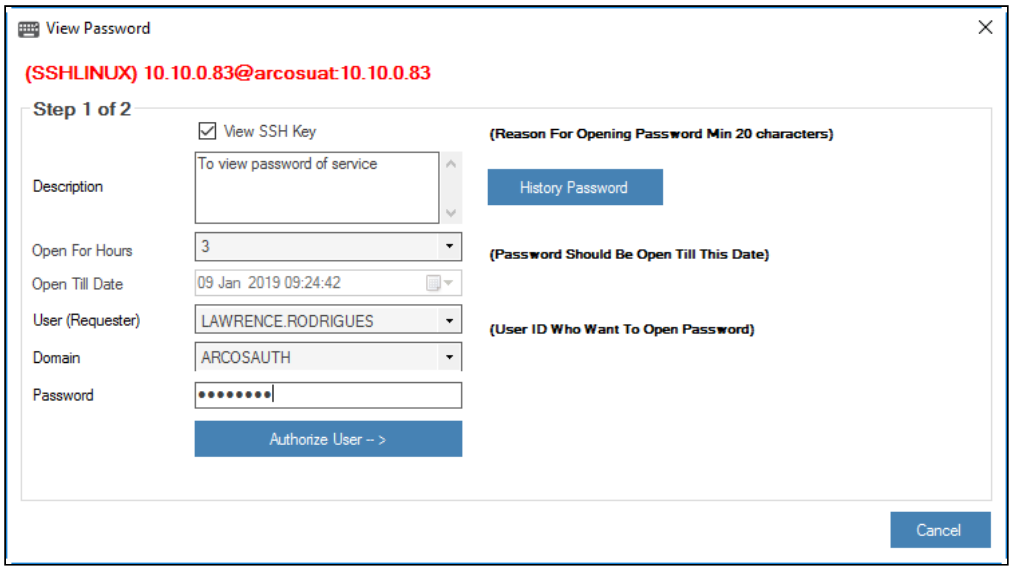
Manage → Users and Services → Manage Services

1. Right click on the service. A multiple options list is popped up.



⚠ The services available in the grid are displayed based on the LOB and service type selected from the **Select LOB/Profile** dropdown list available in the home screen (Server Manager) and from the **Service Type** dropdown list respectively.

2. Click **View Password** option. The **View Password** screen is displayed.



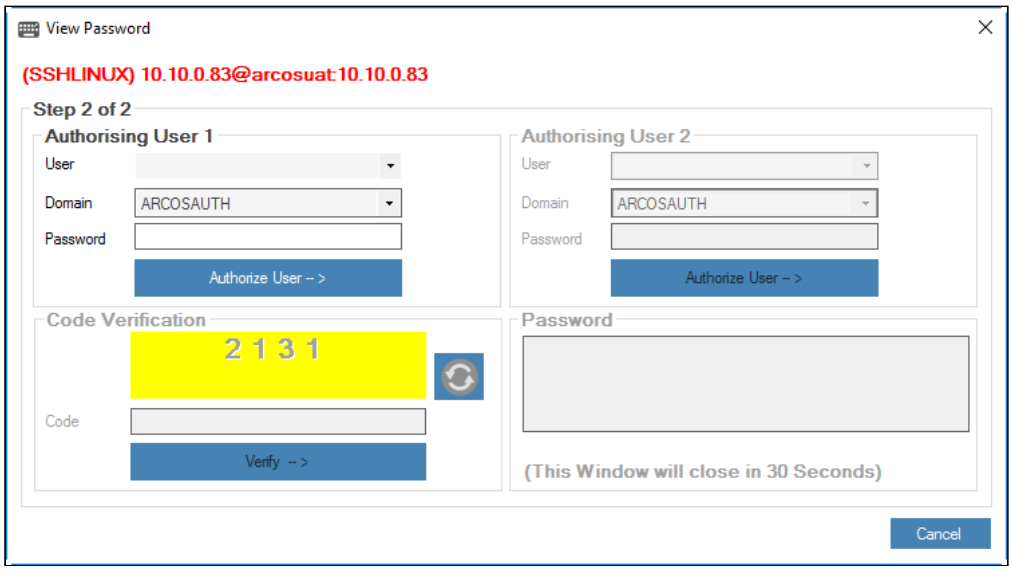
The **View Password** screen displays the following fields:

Field Name	Description
View SSH Key	Select to request SSH Key. ⚠ This checkbox is displayed if you select **SSH Linux** service to view password.
Description	Enter description or reason to view password / SSH Key.
Open For Hours	Select the number of hours, until when the password / SSH Key will be open for use. ⚠ If the **Min Password Age** is configured other then 0, then **VPC Service** will check minimum configured days before changing password of Service. ⓘ To know more about **Min Password Age** and **Max Password Age** read **Schedule Password Change Process for a Service** from **Password Manager** section.
Open Till Date	Displays the date and time, until when the password / SSH Key is open for use. ⚠ The data in this field is auto populated based on the **Open For Hours** selected.
User (Requester)	Select name of the user/requestor who requests to view password / SSH Key.
Domain	Select domain of the user/requestor who requests to view password / SSH Key.

Field Name	Description
Password	Enter password of the user who requests to view password / SSH Key.

⚠ **History Password** checks whether the service password exists in ARCON PAM database.

3. Select and enter the details and click **Authorize User** → button. The following screen is displayed.



4. The **Authorising User 1** should select the username and domain from the **User** and **Domain** dropdown list respectively and enter password in the **Password** text field.
5. Click **Authorize User** → button, to approve the user trying to view the password/ SSH key. On authorization, the **Authorising User 2** is enabled.
6. The **Authorising User 2** should select username and domain from the **User** and **Domain** dropdown list respectively and enter password in the **Password** text field.
7. Click on **Authorizer User** → button. On authorization, the **Code Verification** is enabled.
8. Enter the code in the **Code** text field and click **Verify** button. On verifying, the password/ SSH key is sent to the verified User in ARCON PAM mail box (Messages) and the **Password** field is enabled displaying the following notification:
Dear ARCONPAMLOCADM, Please Check Your ARCON PAM Mailbox For Requested Password (/SSH Key)

⚠
- **Requestor:** A Requestor is any Administrator with View Server Password privilege.
- **Authorizing User 1:** The Authorizing User 1 is an Administrator with View Server Password privilege.
- **Authorizing User 2:** The Authorizing User 2 is an ARCON PAM Client with Support View Server Password privilege. The Administrator can also have Support View Server Password privilege.

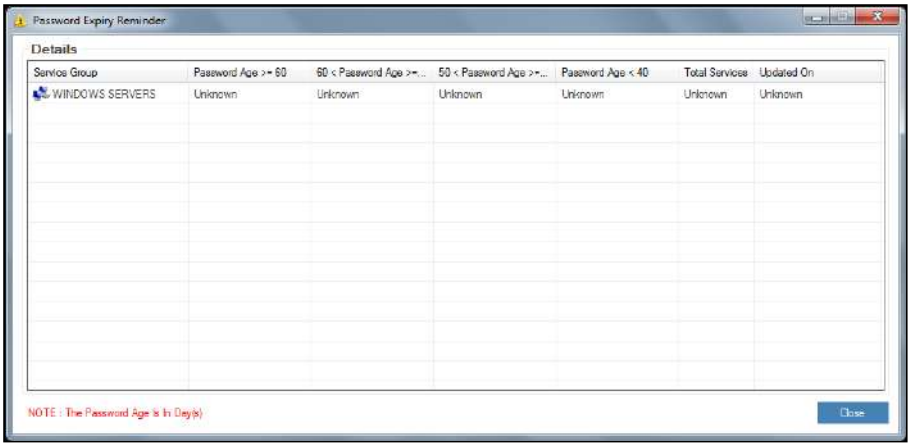
7.5 View Password Expiry Details

Password Expiry Reminder displays the expiry reminder details of the password for the selected service group. It mainly displays the age of the password, which helps the user to configure the scheduler of password change process.

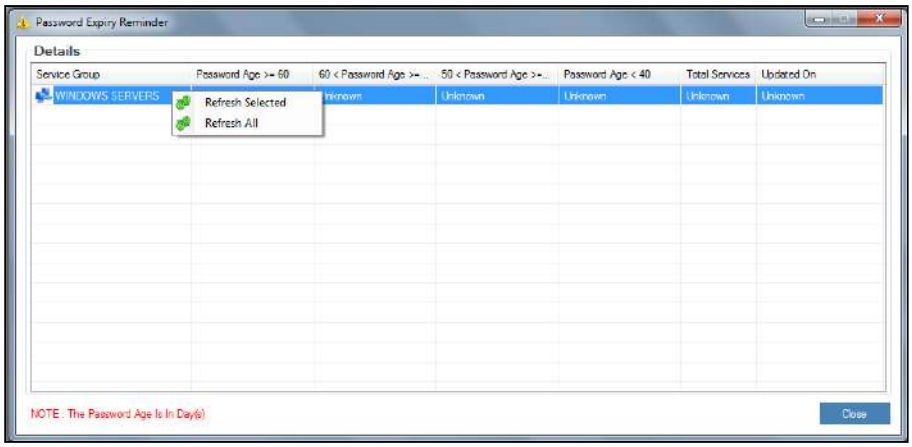
To view password expiry reminder:

To view password expiry reminder use the following path:

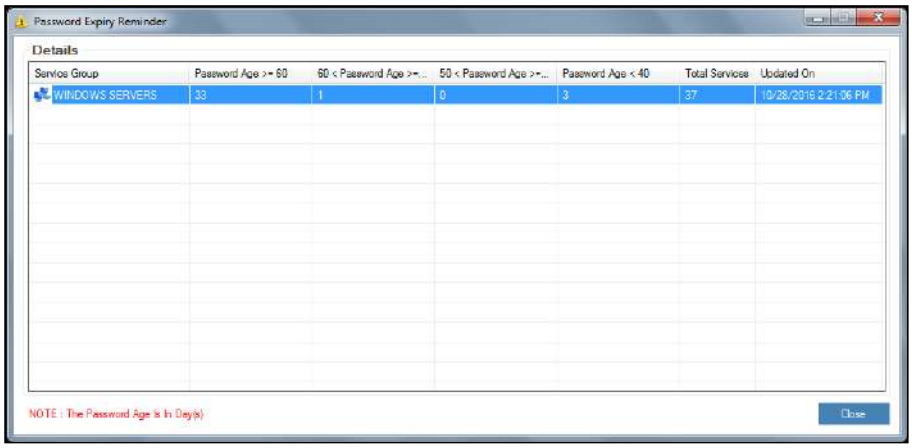
Manage → Password Expiry Reminder



1. Right click on the service group detail. The multiple options list is popped up.



2. Click **Refresh Selected** option to refresh the selected service group. It displays the expiry reminder details of the password for the selected record.
3. Click **Refresh All** option to refresh all the service groups in the list. It displays the expiry reminder details of the password for all the records.
4. On refreshing, you can see the detailed screen.



5. View the expiry reminder details of the password.

7.6 Password Change Dependency

Services Dependencies for Password Change feature adds dependent child services to the parent service. In addition, you can view the parent service for the selected child service and configure pre or post actions to be performed before or after password change process.

This section includes the following topics:

- Adding Dependent Servers
- Viewing details of Dependent Servers
- Configuring Pre or Post Password Change Actions
- App-to-App Password Change

7.6.1 Add Dependent Servers

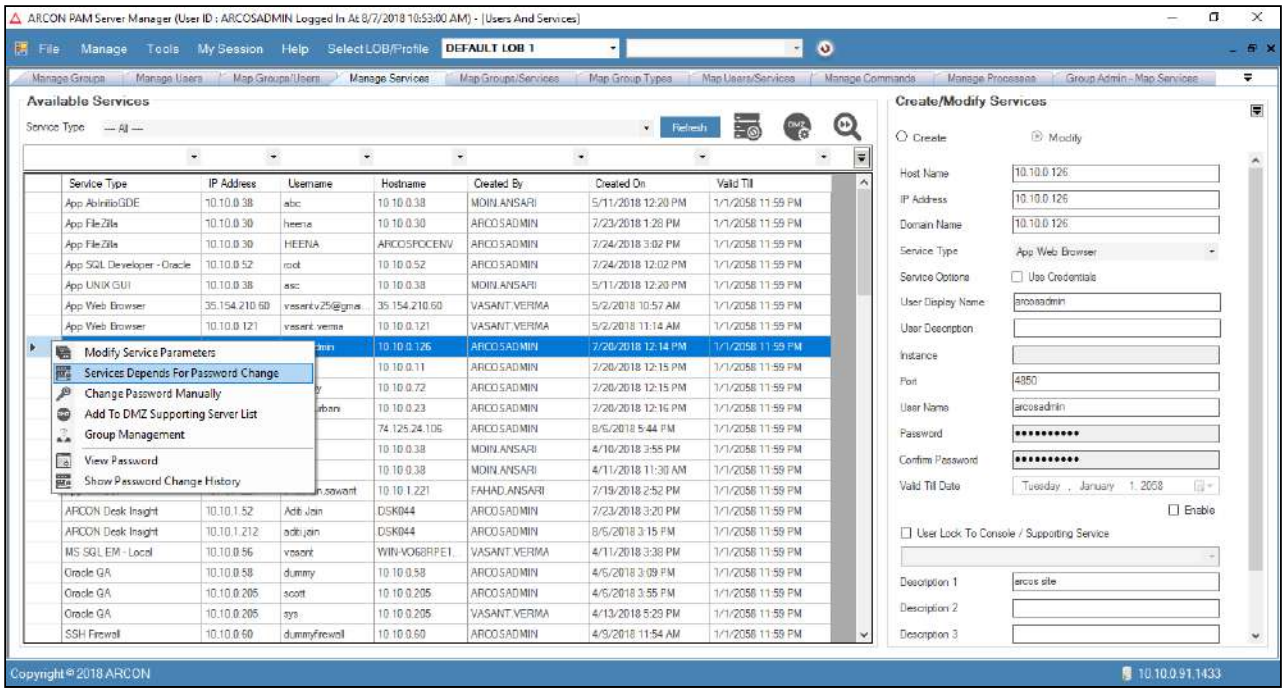
This section helps you to add dependent child services to the parent service, wherein when the password of the parent service is changed then the password of the child service is automatically changed.

To add depending servers:

To add the depending servers use the following path:

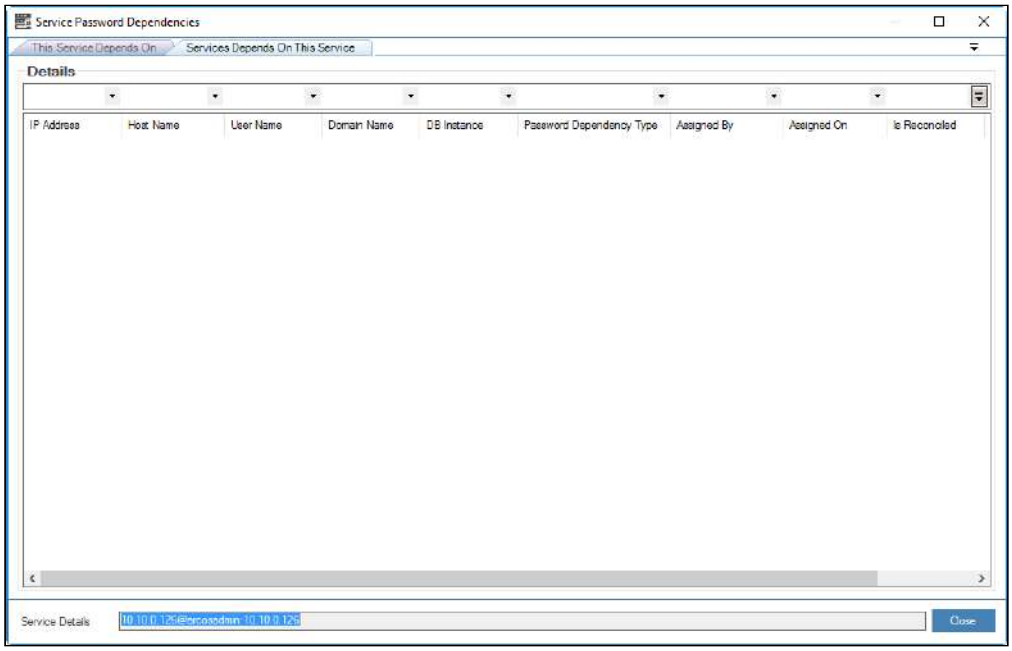
Manage → Users and Services → Manage Services

1. Right click on the service. The multiple options list is popped up.

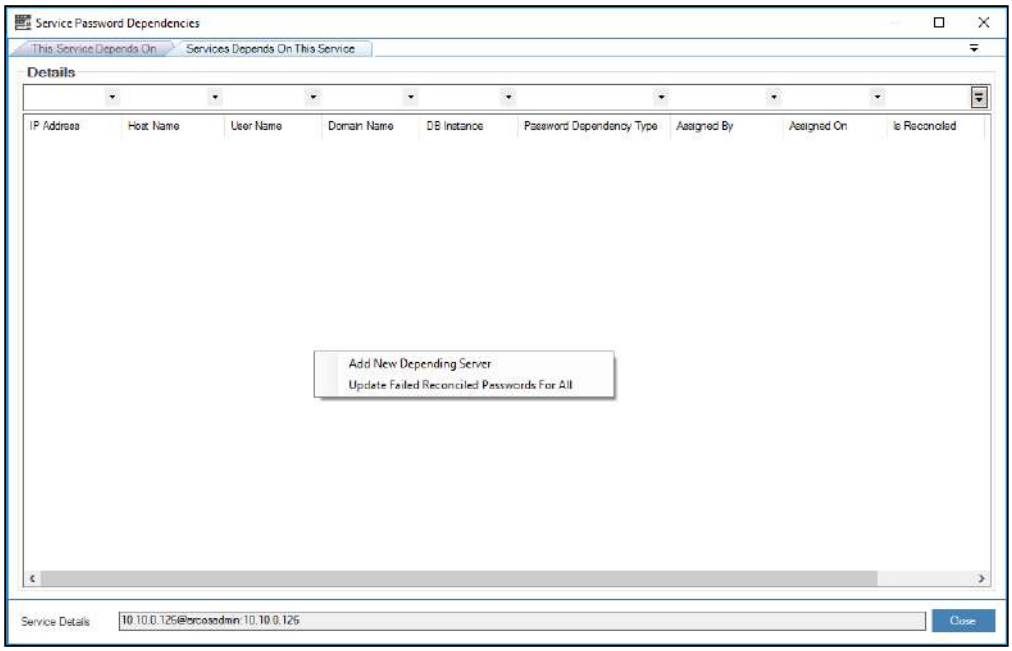


⚠ The services available in the grid are displayed based on the LOB and service type selected from the **Select LOB/Profile** dropdown list (in the home screen Server Manager) and **Service Type** dropdown list respectively and then click on **Refresh** button.

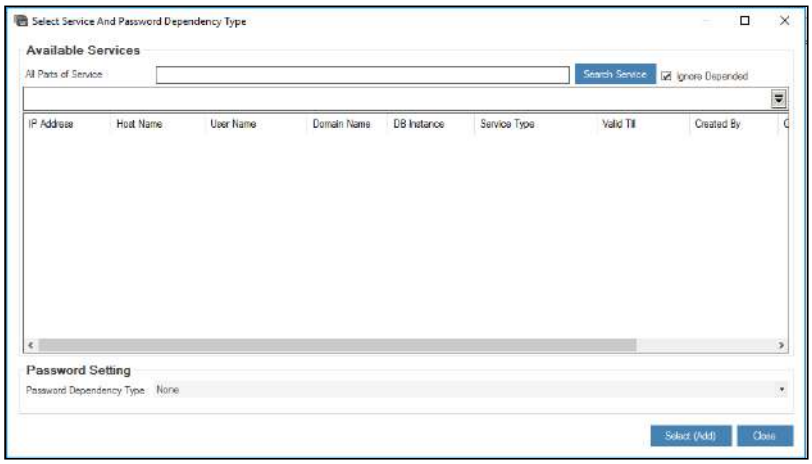
2. Click **Services Depends For Password Change** option. The **Service Password Dependencies** screen is displayed. By default, **Service Depends On This Service** tab is viewed.



3. Right click inside the window. A multiple options list is popped up.

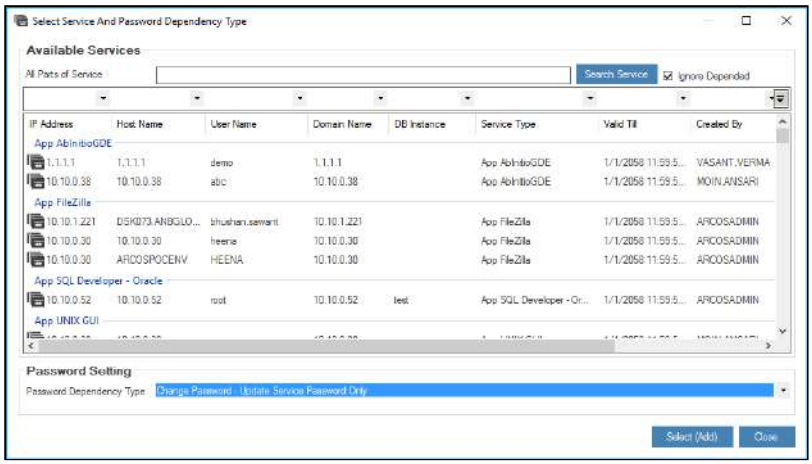


4. Click **Add New Depending Server** option. The **Select Service And Password Dependency Type** screen is displayed.



5. To search for a particular IP address, enter the IP address in the **All Parts of Service** text field and click **Search Service** button or simply click **Search Service** button. The available service details are displayed.

> ⚠ If the Settings **Allow Dependency From Across the LOB is Enabled**, If the Toggle value is 'Disabled', then it will not allow Services across LOB to be added for Service Password dependencies. If the Toggle value is 'Enabled', then it will allow Services across LOB to be added for Service Password dependencies.



6. Select the child service and then select the type of password dependency from the **Password Dependency Type** drop down list and click on **Select (Add)** button to add the selected service to the dependency list.

   The following are the different types of **Password Dependency**:

   - **Process With Same Password:** It will change the password of the depending service with the same password of parent service.
   - **Process with New Password:** It will change the password of the depending service with the different (new) password as that of parent service.
   - **Update Service Password Only:** It will update the password of the depending service with the same password of parent service only in ARCON PAM database.

7.6.2 View details of Dependent Servers

This section helps you to view the details of the parent service for the selected child service.

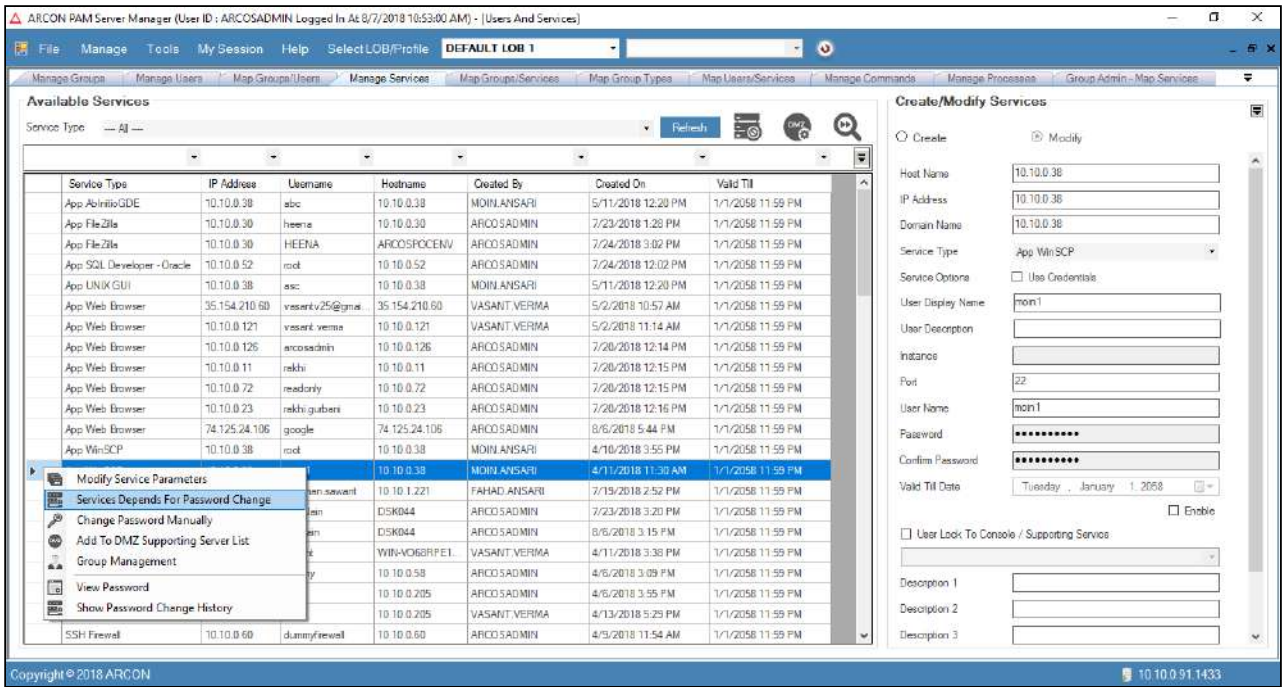
> ⚠ If the toggle value for **Allow Dependency From Across LOB is Enabled** is Disabled in **Settings**, it will not display Services across LOB. If the toggle value is Enabled services across LOB will be displayed.

To view details of depending servers:

To view details of depending servers use the following path:

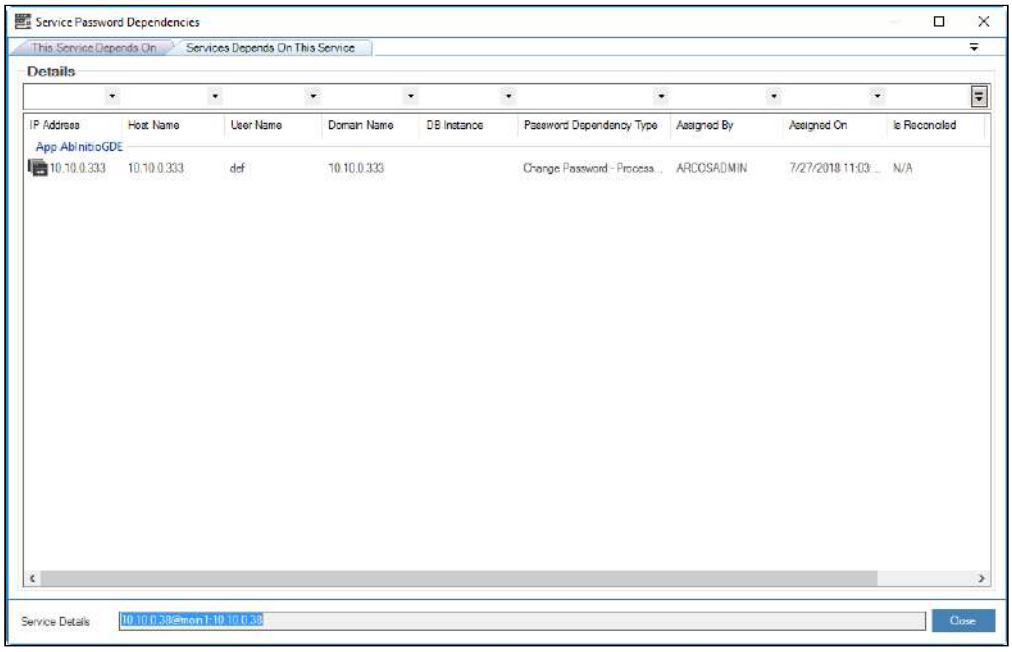
Manage → Users and Services → Manage Services

1. Right click on the service. A multiple options list is popped up.

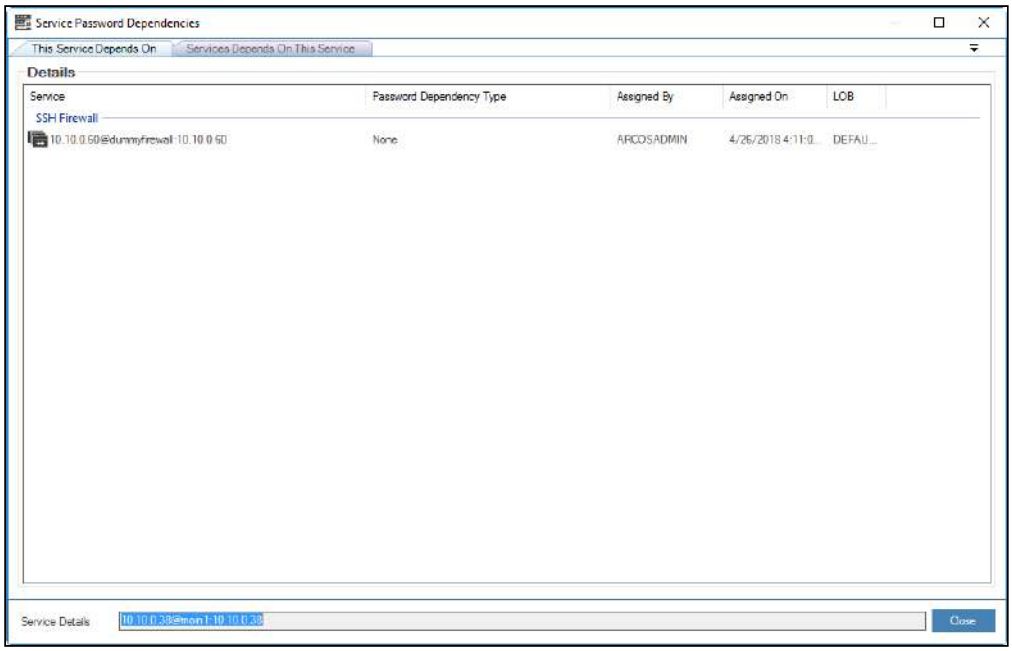


> ⚠ The services available in the grid are displayed based on the LOB and service type selected from the **Select LOB/Profile** dropdown list (in the home screen Server Manager) and **Service Type** dropdown list respectively and then click **Refresh.**

2. Click **Service Depends For Password Change** option. The **Service Password Dependencies** screen is displayed.



3. Click **This Service Depends On** tab. The details for the selected service is displayed.



For Example:
The service displayed in **Service Details** textfield is a child of Windows RDP service displayed in the grid. In other words, 10.10.0.30@shared_service:10.10.0.30 service is a child of 10.10.0.43@nishkarsh:arcosUAT parent service.

7.6.3 Configure Pre or Post Password Change Actions

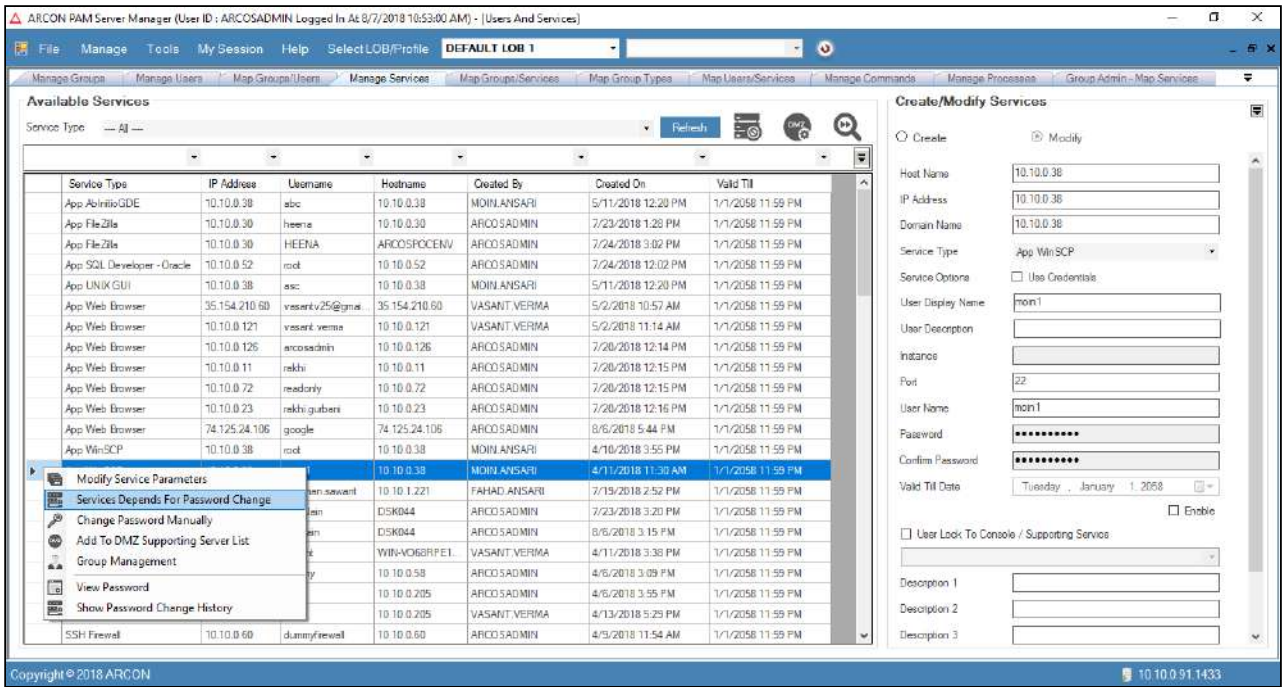
This section helps you to configure the actions to be performed before or after the password change process.

To configure pre or post password change actions:

To configure pre or post password change actions use the following path:

Manage → Users and Services → Manage Services

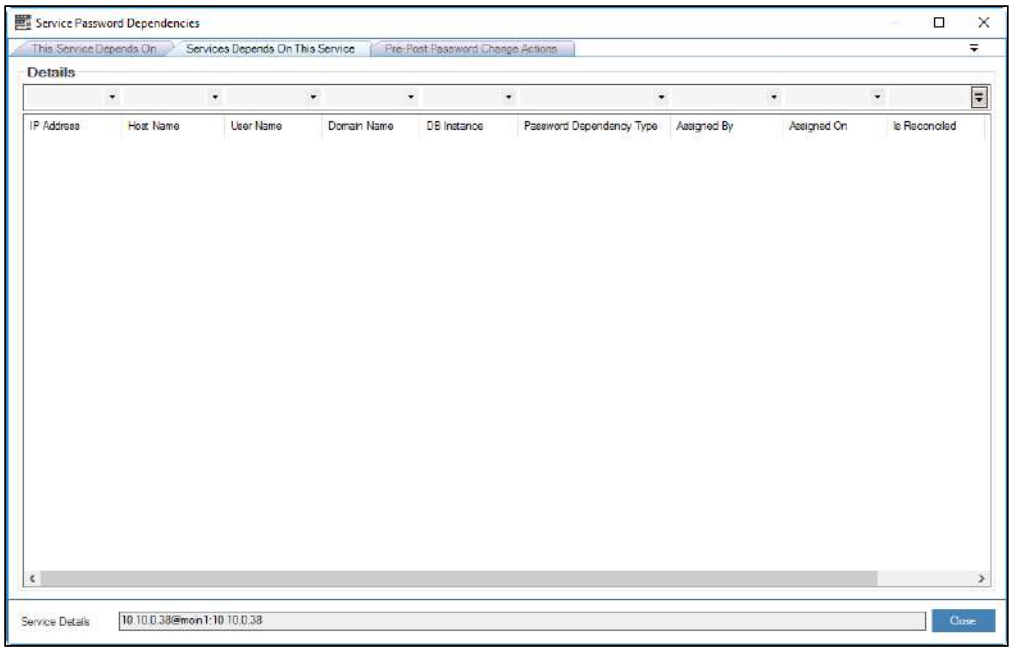
1. Right click on the service. A multiple options list is popped up.



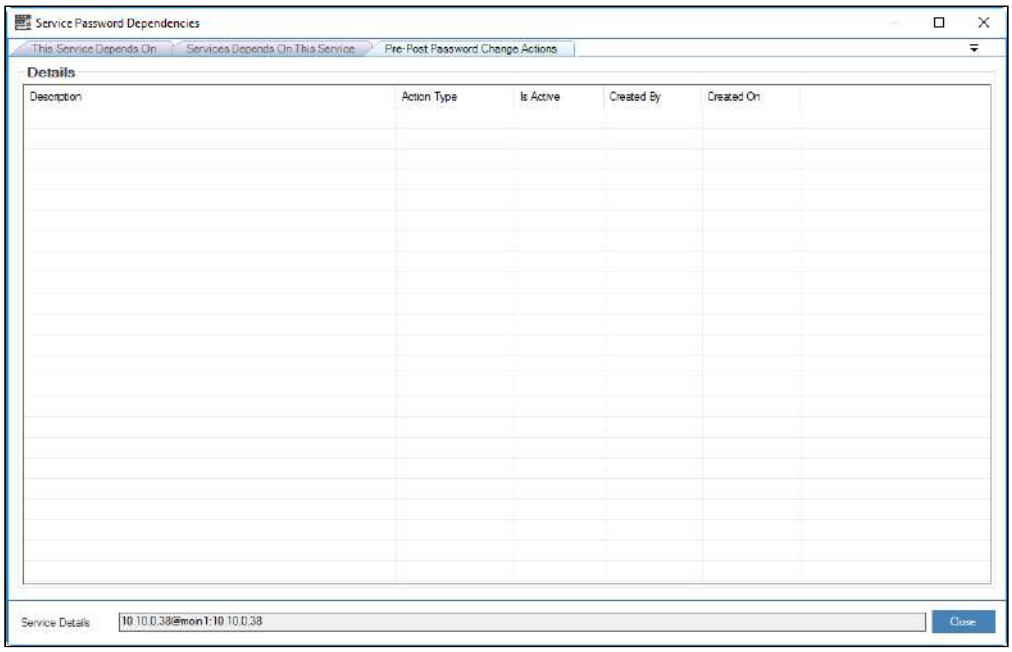
> ⚠ The services available in the grid are displayed based on the LOB and service type selected from the **Select LOB/Profile** dropdown list (in the home screen Server Manager) and **Service Type** dropdown list respectively and then click on **Refresh** button.

2. Click **Services Depends For Password Change** option. The **Service Password Dependencies** screen is displayed.

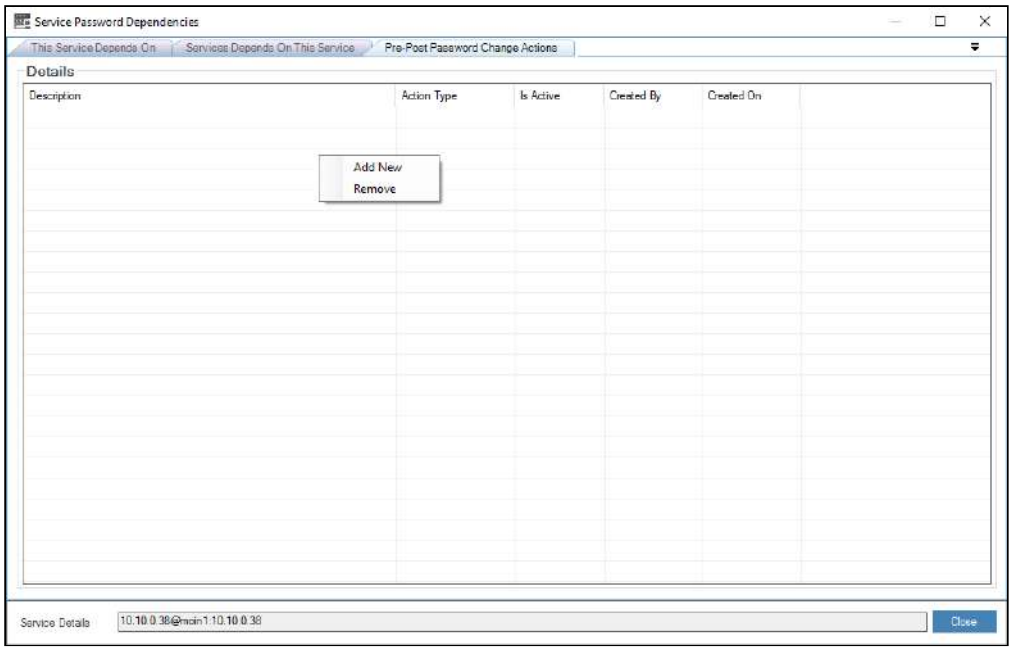
> ⚠ If the toggle value for **Post Password Change Actions - Is Enabled** in **Settings** is **Enabled,** then **Pre-Post Password Change Actions** tab will be displayed to configure pre-post password change actions.



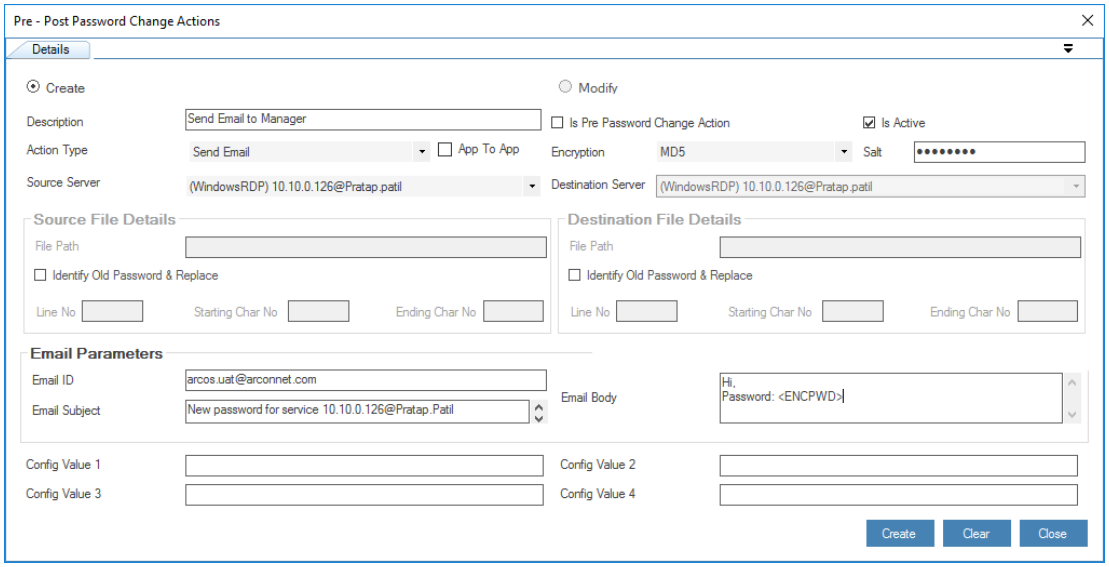
3. Click **Pre-Post Password Change Actions** tab. The following screen is displayed.



4. Right – click on the screen. A multiple options list is popped up.



5. Click **Add New** option. The **Pre-Post Password Change Actions** screen is displayed.



The **Pre-Post Password Change Actions** screen displays the following fields:

Field Name	Description
Create	Creates a new pre or post action.
Modify	Modify an existing pre or post action.
Description	Enter the description to perform the action.

Action Type	Select the type of action. The valid values are: ▪ **Transfer File:** Transfer files from the source server to the destination server. ▪ **Update Password In File:** Updates the password changed in VB script and Batch processing file. ▪ **Execute Command:** Executes the command. ▪ **Send Email:** Sends Email to the client. ▪ **Linked Server:** Updates the password of linked server user. ▪ **Update through API:** Updates the password using the supported third-party APIs ⚠ The below fields are enabled based on the **Action Type** selected.
Source Server	Select IP address of the source server.
Is Pre Password Change Action	Select to configure Pre Password Change Action.
Encryption	Select the hashing algorithm method for encryption.
Salt	Enter the salt value used for encryption.
Destination Server	Select the IP address of destination server.
Source File Details	
File Path	Enter the file path of the source file.
Identify Old Password & Replace	Identifies the old password and then replace it from the source file.
Line No	Enter the line number from the script file.
Starting Char No	Enter the starting character number from the script file.
Ending Char No	Enter the ending character number from the script file.
Destination File Details	
File Path	Enter the file path of the destination file.
Identify Old Password & Replace	Identifies the old password and then replace it from the destination file.
Line No	Enter the line number from the script file.
Starting Char No	Enter the starting character number from the script file.
Ending Char No	Enter the ending character number from the script file.
Email Parameters	
Email ID	Specify the email ID of the user.
Email Subject	Specify the subject title for the email.
Email Body	Specify the description for the email.

6. Enter or select the fields and click **Create** to create a pre or post password change action.

⚠ Post - Password actions can be performed on Windows Services

7.6.3.1 Action Type Parameters

Action Type parameter is an important parameter which defines 4 major types of ways in which ARCON PAM can further cause password change in the required dependent servers. To configure this parameter, following is a list of instances and scenarios that ARCON PAM can induce the passwords for.

Inducing passwords through Microsoft Windows-based services, APIs, Powershell, and VB scripting scripts:

Category	Device/ OEM	OEM Service/ Feature Type (If applicable)	Operation Type	Version / Type	ARCON PAM Post Password Action/ Navigation Type
OS	Microsoft Windows	Server	File Transfer from Server to Server	2008, 2012 R2	Action Type- Execute Command
OS	Microsoft Windows	Active Directory Domain Account	Domain Account Password Change Dependency	2008, 2012 R2	Password Dependency Type-Change Password- Update Service Password Only
OS	Microsoft Windows	Configuration	Auto Logon	2008, 2012 R2	Action Type-Execute Powershell Command
OS	Microsoft Windows	System Center Operation Manager (SCOM)	Password Change Dependency	2008, 2012 R2	Action Type-Execute Powershell Command
OS	Microsoft Windows	Server	Network Cluster Failover Process	2008, 2012 R2	Action Type-Update Through API
OS	Microsoft Windows	SharePoint	SharePoint Domain Account Password Change	2008, 2012 R2	Password Dependency Type-Change Password- Update Service Password Only
OS	Microsoft Windows	SharePoint	SharePoint Local Account Password Change	2008, 2012 R2	Action Type- Update Password In File
OS	Microsoft Windows	Server	Scheduled Tasks	2008, 2012 R2	Windows Password Dependency
OS	Microsoft Windows	Server	COM, DCOM	2008, 2012 R2	Action Type-Execute Powershell Command
OS	SSH Linux	Configuration	Auto Logon	Ubuntu	Action Type- Execute Command
Database	Microsoft Windows	SQL Server	Dependent Database Password Change	2008, 2012	Action Type- Linked Server

Category	Device/ OEM	OEM Service/ Feature Type (If applicable)	Operation Type	Version / Type	ARCON PAM Post Password Action/ Navigation Type
Database	Microsoft Windows	SQL Server Auditing	Dependent Database Password Change	2008, 2012	Action Type- Linked Server
Web/ Application Server	Oracle WebLogic	WebLogic Application Server	Dependent Server Password Change	11g, 12c	Action Type- Update Password In File
Web/ Application Server	Apache Tomcat	Tomcat Application Server	Dependent Server Password Change	7.0, 8.5	Action Type- Update Password In File
Web/ Application Server	Microsoft Windows	Internet Information Service	Anonymous, Application Pool Password Change	2008, 2012 R2	Action Type-Update Password in IIS App Pool
Driver-based	Microsoft	JDBC driver	Configuration	6.0	Action Type - Execute Command
Driver-based	Microsoft	ODBC driver	Configuration	13.1	Action Type - Execute Command

7.6.4 App-to-App Password Change

It is clear that the privileged user-ids, which are hardcoded carry a high degree of risk from being compromised as these user-ids and passwords are known to be in clear text in various files on the application servers or are known to the support team as they insert this in the application configuration files during any application implementation.

Also, this creates administrative overhead as any change in such passwords have to be replicated in the applications as well as the operating system or databases as the case may be. There are several cases wherein these passwords are in services that need to be restarted again on updation.

7.6.4.1 Pre-requisites

Install **ARCON PAM Windows Vaulting Service** on the Windows Servers where the application is installed.

Port number **45045** is required to be opened from **ARCOS SGS (Secured Gateway Server)** to respective Windows Servers.

Powershell must be installed on the target Windows Servers.

7.6.4.2 ARCON Approaches

ARCON PAM has a comprehensive framework to deal with various scenarios such that applications can connect seamlessly with data sources/systems by requesting privileged passwords from the PAM vault.

The following methodologies are available:

- In cases where the application provides an API/input methods, ARCON PAM through its "ARCON SPC Service" installed on the ARCON PAM Application server connects to the vault and fetches the passwords on a defined frequency or on-demand (similar to the password change process used for other systems) and

provides the same to the target operating system. The supported operating systems are Windows and All flavors of Unix.

- On Windows the Windows Password Change Service (ARCON Windows Vaulting Service) will receive the various parameters described above and also the password, similarly, on Unix flavors, these parameters will be passed on through script which gets executed once the ARCON PAM logs on using the privileged user account already integrated or available with it. This method works even if there are multiple applications/scripts on the same application server.
- There are pre and post-events, which will get executed based on the application requirements. These are useful depending on how applications input the new passwords.

7.6.4.3 Use-cases

ARCON PAM Windows Vaulting Service inserts the password input and simultaneously encrypt the same and store it in a particular path in **.ini** or **.config** files or similar other files.

Sometimes, ARCON PAM has to insert the password inputs in clear text, and thereafter the service needs to be restarted so that the password is encrypted. The service restart can be triggered by either ARCON PAM (as configured in the **Pre-Post Password Change Actions**) or by the application API.

In case the passwords are to be inserted in the scripts, ARCON PAM will push the passwords to the "ARCON SPC Service" or through scripts (depending on the operating system) and thereafter they are updated in the scripts, etc.

The approach used above is useful to carry out scheduled password change activity triggered through ARCON PAM. The passwords of the applications can also be scheduled to be changed at regular intervals say 30/60/90 days. This approach also takes away the dependency on the ARCON PAM system once the activity is carried out.

Moreover, in the post actions, Admin can configure to trigger a mail notifying other Admins about the password change success status.

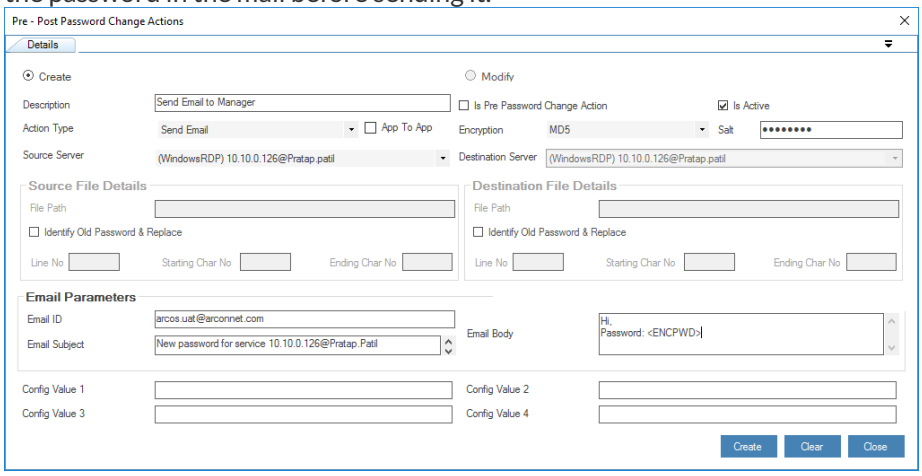
Use-cases - Fulfilled	
Service Accounts For a service instance that logs on with a user account, rather than the LocalSystem account, the Service Control Manager (SCM) on the host computer stores the account password, which it uses to log on the service when the service starts. As with any user account, you must change the password periodically to maintain security.	**Stop Services on Application Server** Stops the service running on Application Server using the Service Name.
	Start Services on Application Server Starts the service running on Application Server using the Service Name.
	Update the Password in Service Accounts When you change the password on a service account, it is required that the password stored by the Service Control Manager must also be updated.
Database Accounts Generally, in order to provide your connection information to a particular Database account, a connection string is used.	**Change Password of Database** Changing the password of a Database user using a database query.
	Make Changes to ODBC Drivers Updating the new password of the database user used in the connection string of the ODBC Driver. A manual restart of the ODBC Driver is required.

Use-cases - Fulfilled

Credentials in Web.config files
There are a number of important settings that can be stored in the configuration file. Some of the most frequently used configurations, stored conveniently inside Web.config file are:
1. Database connections
2. Caching settings
3. Session States
4. Error Handling
5. Security
	Update the Password in Web.config
	Update the new password of the database user in the connection string web setting
	
	Update a string in configuration files using keyword
	Update the new password in a particular string inside the config files with a specific keyword.
	For example, cred=”pass@123” (a string in the config file) then by mentioning “cred” as the keyword, the new password will be updated in the place of “pass@123”.
	
	Update password in the Batch file
	This will update the password in the file (batch file) and execute the same.
	For example, assuming the CP.bat file containing the following command.
	`sc config "TEST Plugin" password=%1`
	`echo success`
	Select the Execute Commands option from the Action Types dropdown and mention the file path and the password tag following it in the Source File section. “C:\CP.bat <AUSRNP>”

Website Accounts In order to ensure security isolation of Websites in a shared hosting environment, using a dedicated user account as an identity for the application pool is recommended.	**Restart the Website in IIS** Stop and Start the Website in IIS using the Website name. **Update the Password in Application Pools** Update the new password for the account associated with the Application Pool Identity in the Application Pools.
Execute Commands with the new password	**Execute PowerShell Commands** Perform advanced tasks to be performed on the server with the updated password using <AUSRNP> tag wherever required. Following are the list of tags that can be used in the command.

Tag	Description
<AIPADD>	IP Address of the service
<AHSTNM>	Host Name of the service
<ADOMNM>	Domain Name of the service
<ADBINS>	DB Instance of the service

Use-cases - Fulfilled		
	<AUSRID>	User Id of the service
	<AUROP>	User Original Password of the service
	<AUSRNP>	User New Password of the service
Network Drive User Accounts Applications use Drive maps to simply associate a single drive letter to files and folders that reside on file servers.	**Reconnect Network Drive** To save a mapped drive in the user's settings and attempt to restore it at each subsequent logon, reconnecting to the Network Drive is necessary. Otherwise, the drive is mapped, but not saved in the user's settings.	
	Reconnect Network Drive with User Credentials To implement a drive mapping using the credentials of the privileged account.	
File Transfer	**Transfer Files from Linux to Windows & Citrix Servers** Copy files from the source server to the destination server. This can be done on SSH Linux and Windows RDP.	
Notify Admins	**Send Email** This function will trigger a mail as per configuration. This can be done to trigger a mail pre or post password change as per requirement. We can also encrypt the password in the mail before sending it. 	

Use-cases - Under Development		
Update password using User Interface	Execute utility to prompt for Password	
	Update UI of Management Consoles	
	Update the Passwords in UI based .exe locations	
Encrypted Credentials	Execute commands to decrypt-update-encrypt .config files	
	Execute a utility to encrypt new password in a string	

	Use Encrypted Passwords to update files
Others	Update Password for COM+ Components
	Make Changes in Regedit
	Update the Password in Linux Management consoles

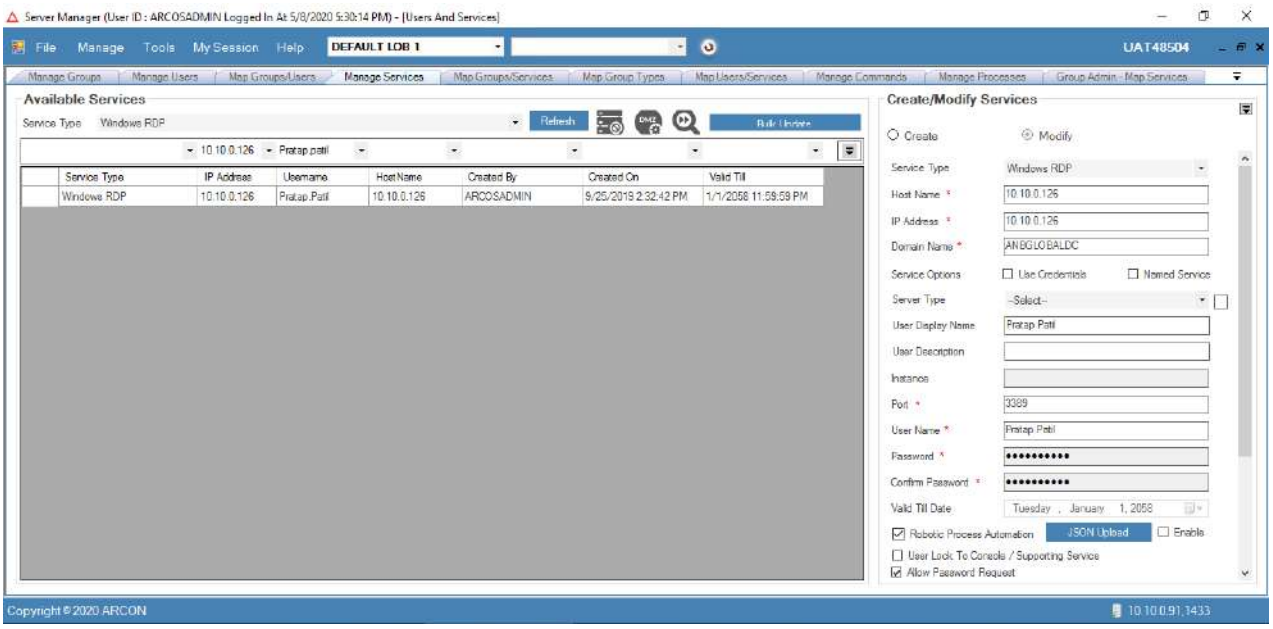
7.6.4.4 Sample Applications

7.6.4.4.1 Microsoft Sharepoint

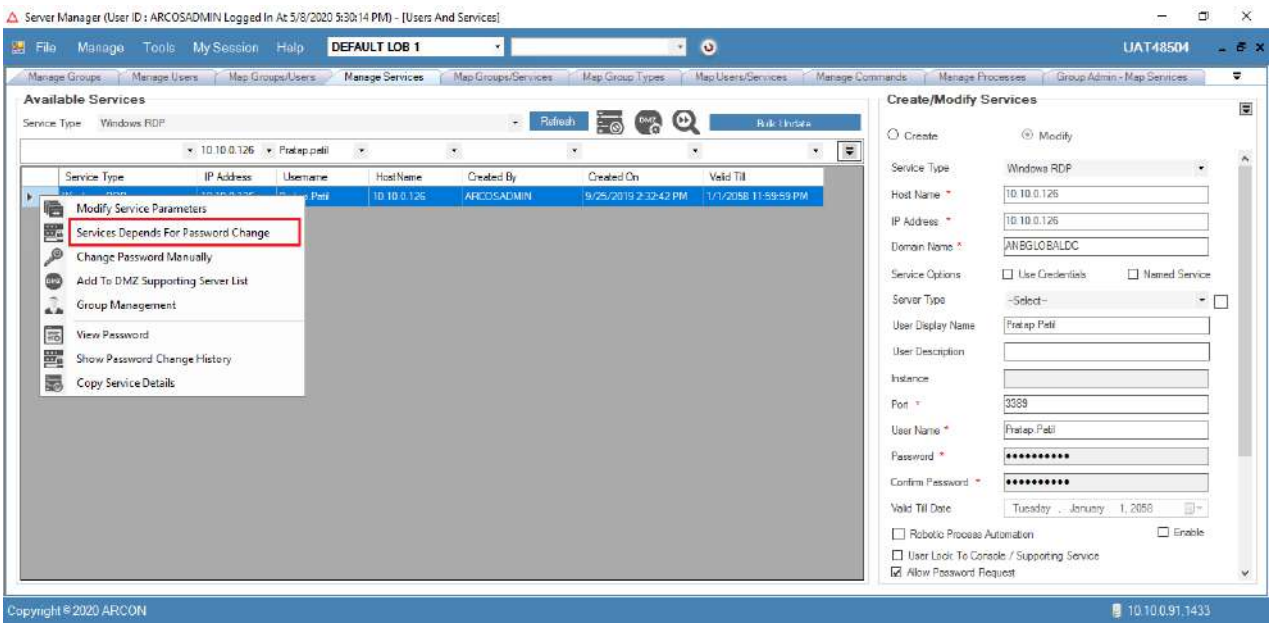
Assuming the Microsoft Sharepoint is installed on server 10.10.0.126. Moreover, the Microsoft Sharepoint service is running under the user "ANBGLOBALDC\Pratap.Patil". When the password rotation triggers due to Scheduled Password Change Service the password will be rotated on the Microsoft Active Directory Server. In order to update this password in the Service Account Post password change action must be configured.

To configure pre or post password change actions use the following path:

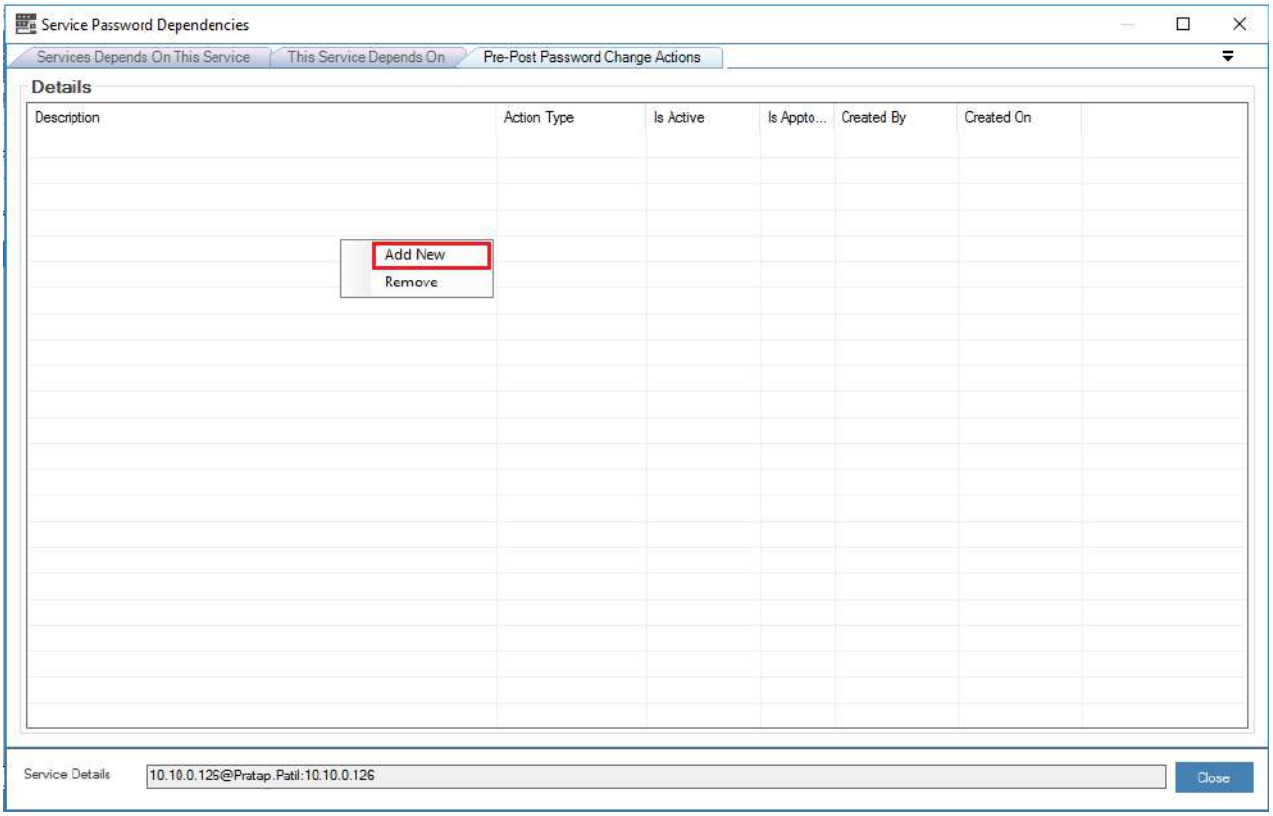
1. In **Manage → Users and Services → Manage Services**, select the ARCON PAM Domain Service under which the Microsoft Sharepoint is running on 10.10.0.126



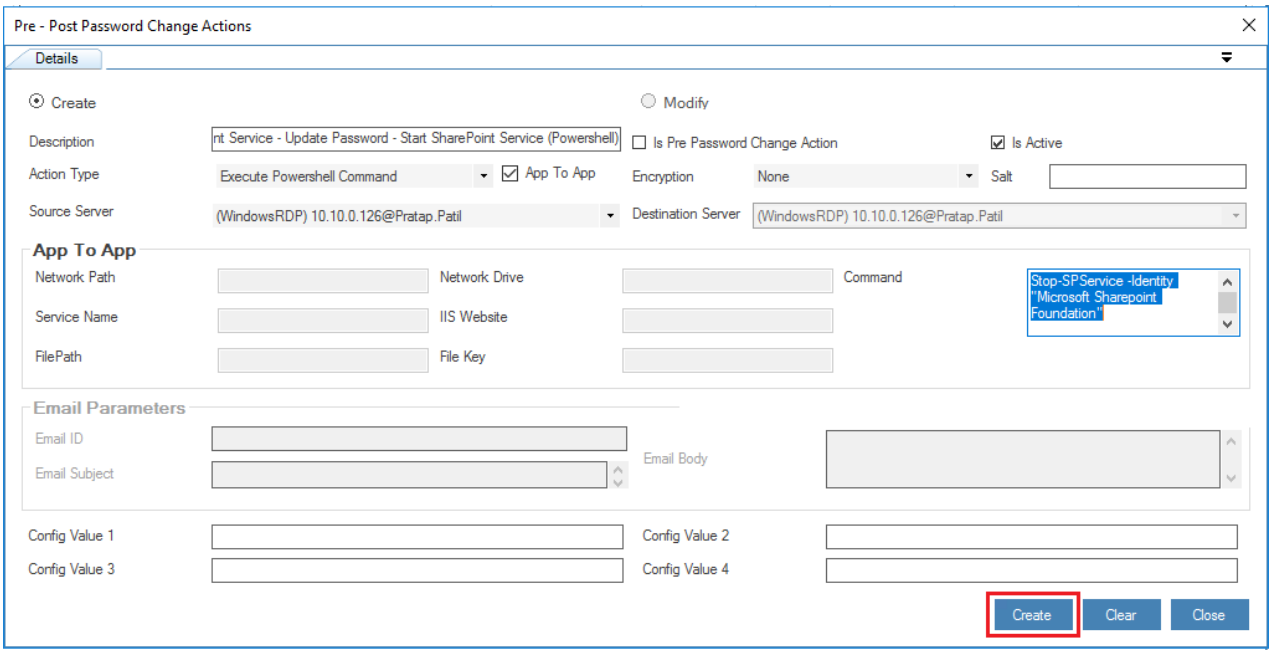
2. Right-click on the service and select "**Service Depends for Password Change**"



3. Click on the "**Pre-Post Password Change Actions**" tab and right-click on the grid view.



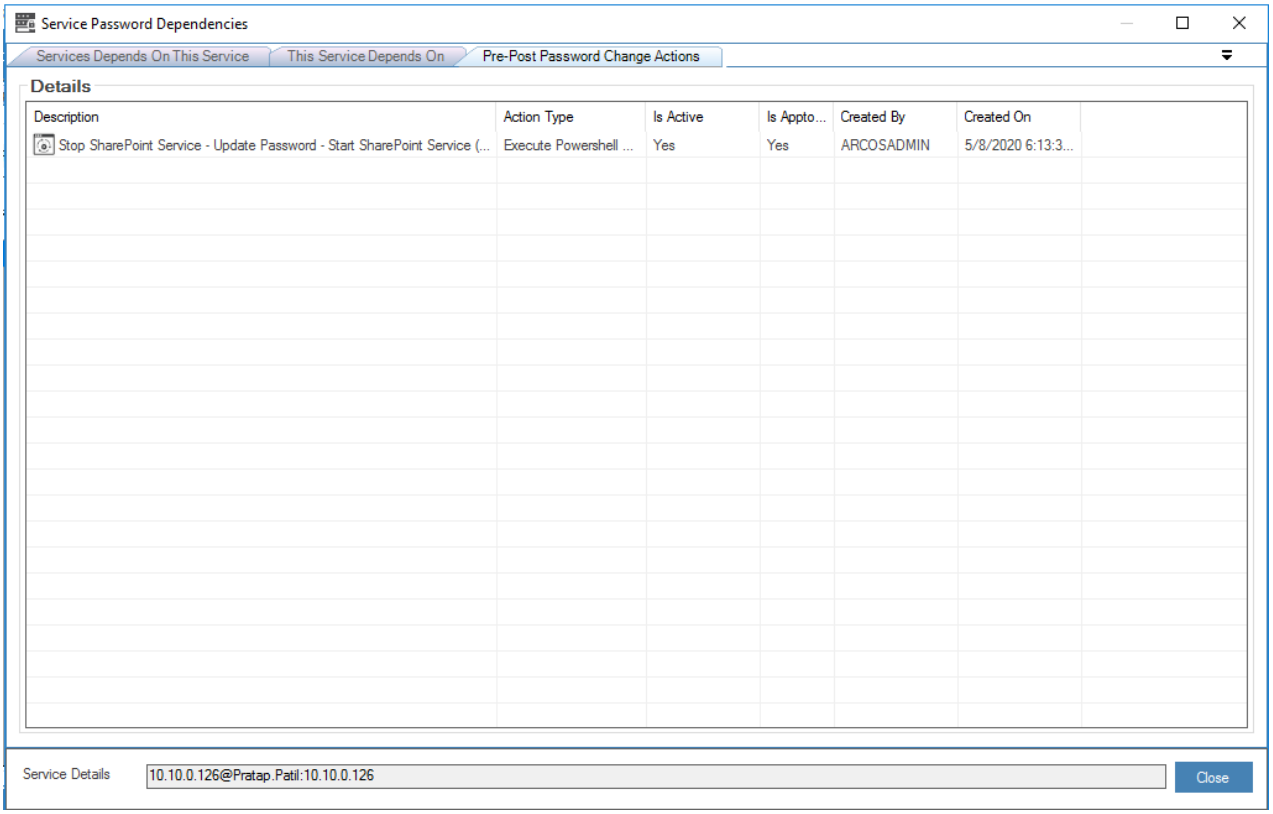
4. Click **Add New** option. The **Pre-Post Password Change Actions** screen is displayed



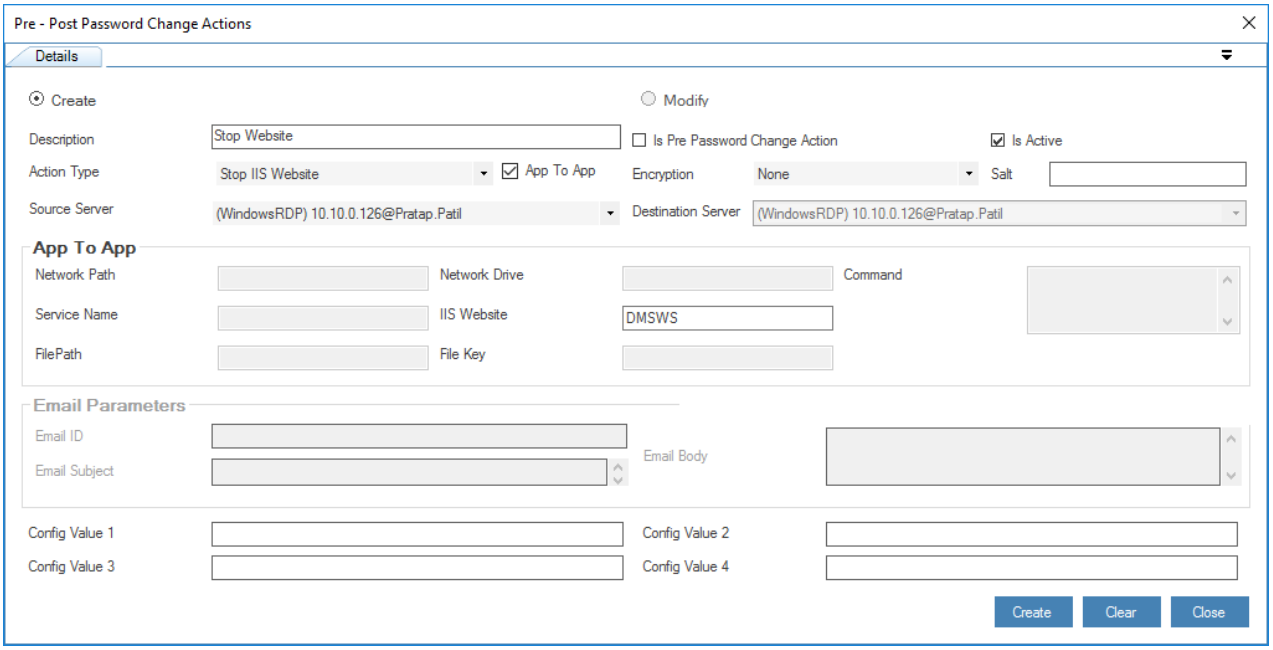
i. Give a description to this action.
ii. Check the "Is Active" checkbox
iii. Check the "App To App" checkbox. This will populate App-to-App related action types.
iv. Select "Execute Powershell Command" as the action type. Selecting this will enable Command textbox in the App To App section.
v. Place the following command to achieve updation of the service account password.
vi. Click on Create button

```
#####Powershell Script Starts#####
Stop-SPService -Identity "Microsoft Sharepoint Foundation" ##Stop the Microsoft Sharepoint Service
$m = Get-SPManagedAccount -Identity "ANBGLOBALDC\Pratap.Patil"
Set-SPManagedAccount -Identity $m -NewPassword <AUSRNP> -ConfirmPassword <AUSRNP>
## Update the password
Start-SPService -Identity "Microsoft Sharepoint Foundation" ##Start the Microsoft Sharepoint Service
#####Powershell Script Ends#####
```

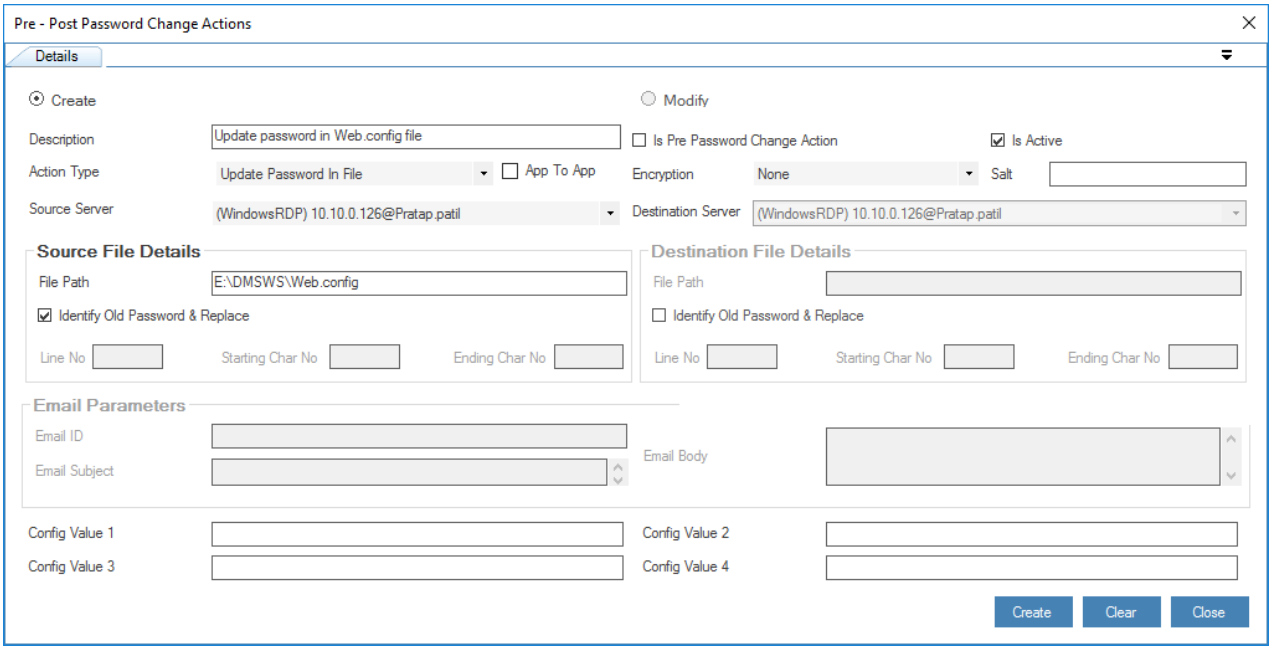
5. Post Password change action has been successfully configured.



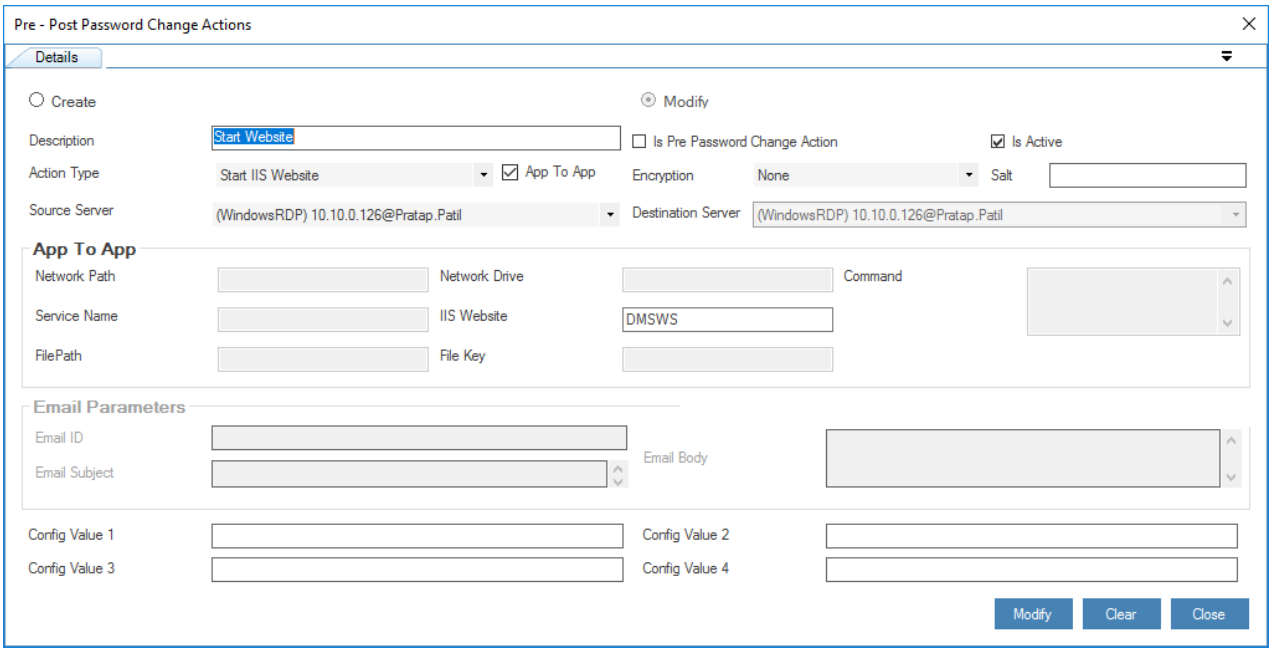
6. **Stop Website** - Select the **Stop IIS Website** from the **Action Type** dropdown. Provide the **Website Name** of the service that should get stopped.



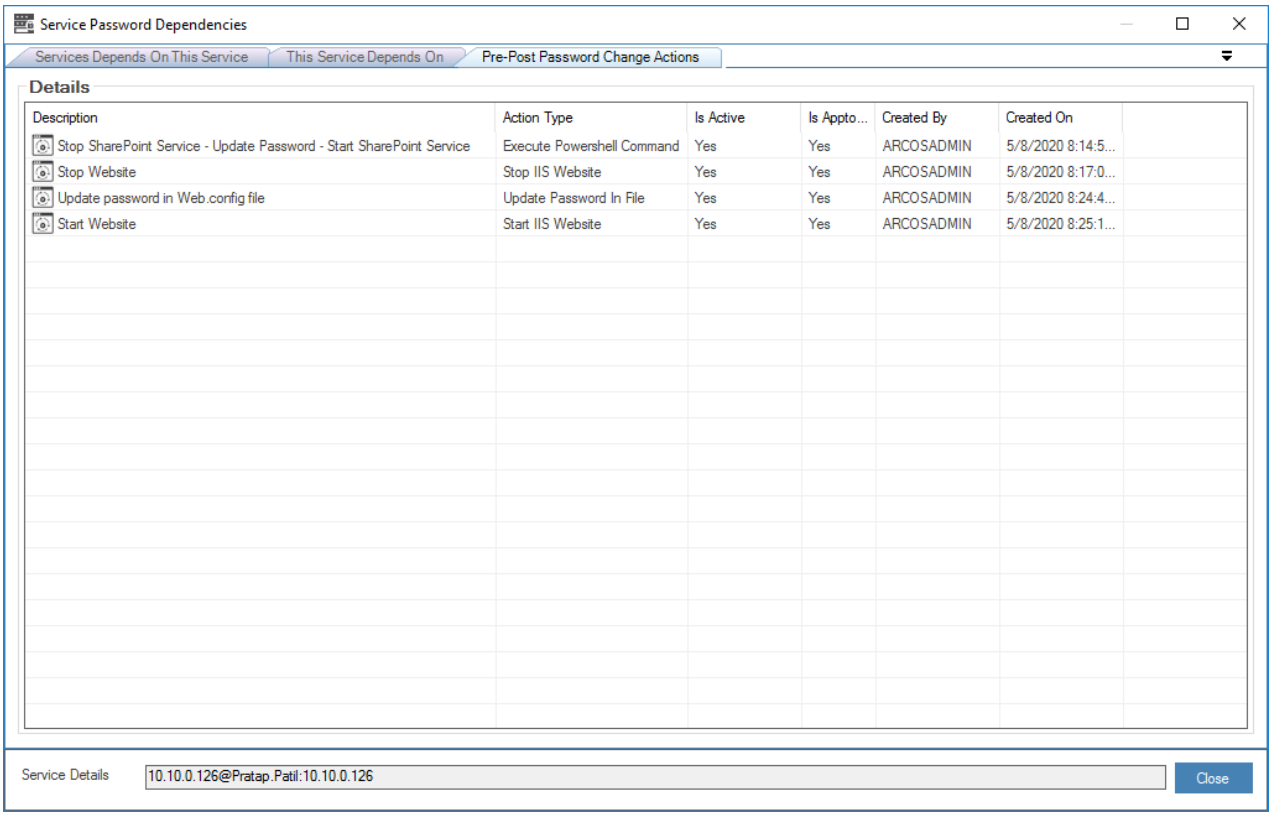
7. **Update password in file** - Select the **Update Password in File** from the **Action Type** dropdown. Provide the **File Path** of the file that should be updated.



8. **Start Website** - Select the **Start IIS Website** from the **Action Type** dropdown. Provide the **Website Name** of the website that should get started.



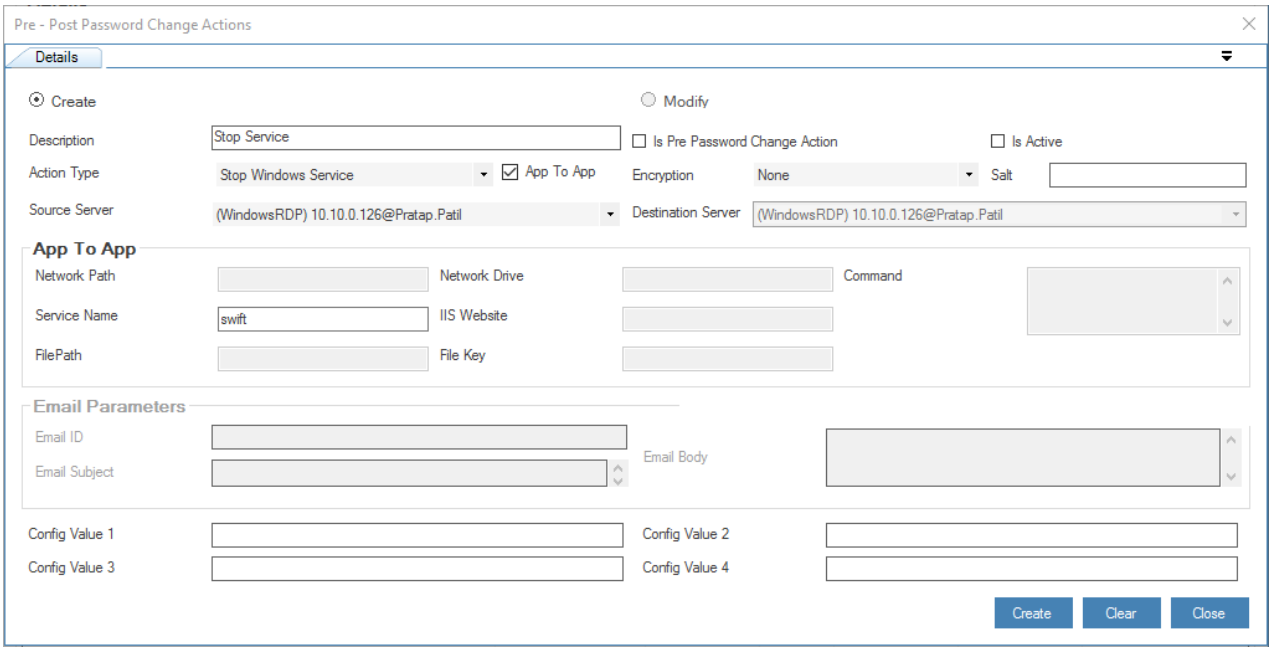
9. On the following screen, you can see all the pre actions and post actions configured for this service.



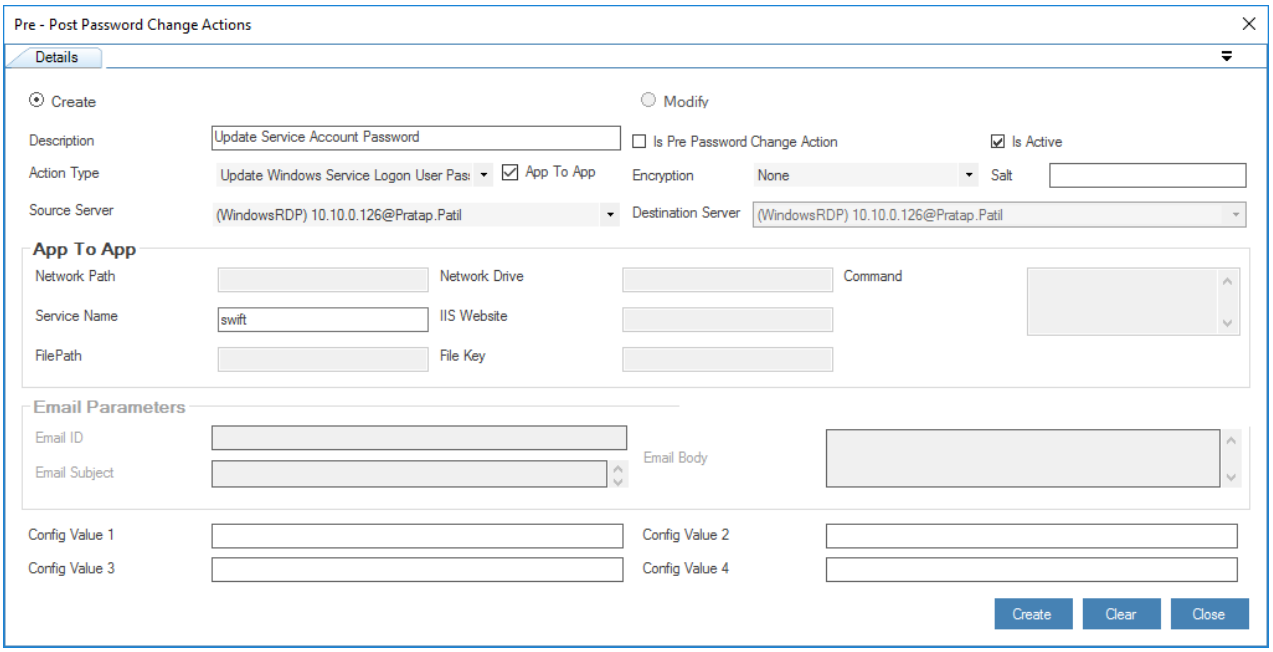
7.6.4.4.2 Swift

The Swift application runs a service under a Domain account. Password will have to be updated on the AD server and also for the Swift service and restart the service post password change. Because Swift uses file storage mapped as a network drive with the same credentials, re-mapping of network drives on the servers must also be configured in Pre-Post Password Change Actions.

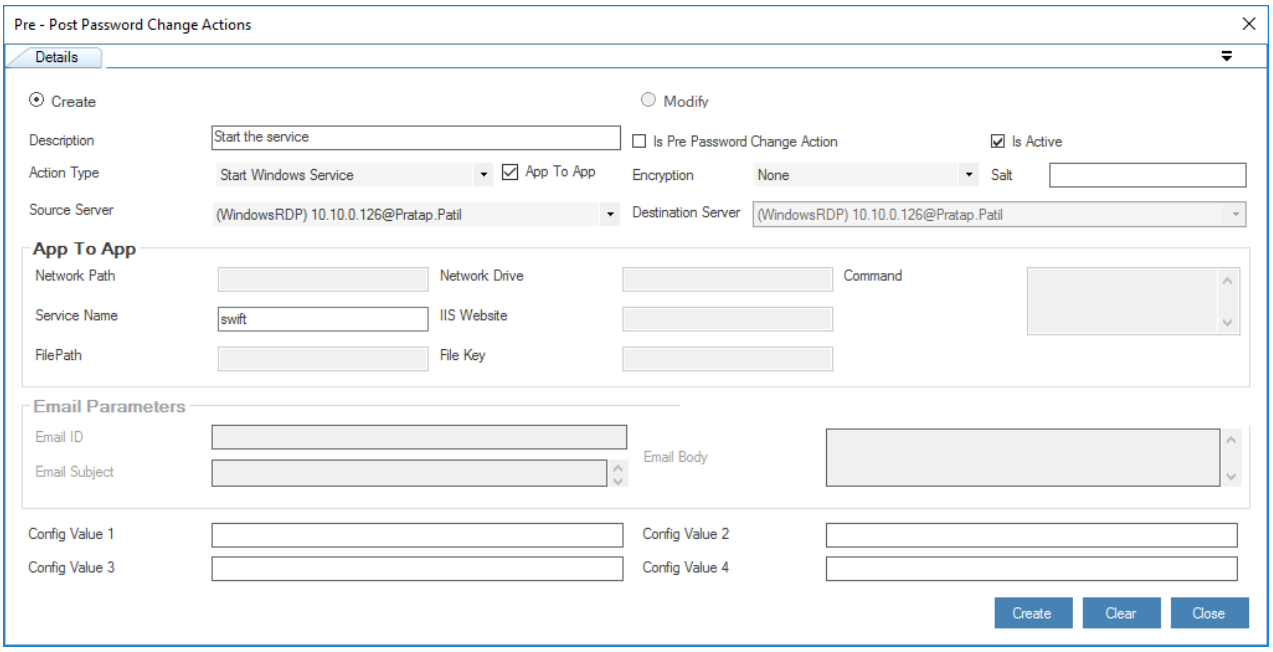
1. **Stop Service** - Select the **Stop Windows Service** from the **Action Type** dropdown. Provide the **Service Name** of the service that should get stopped.



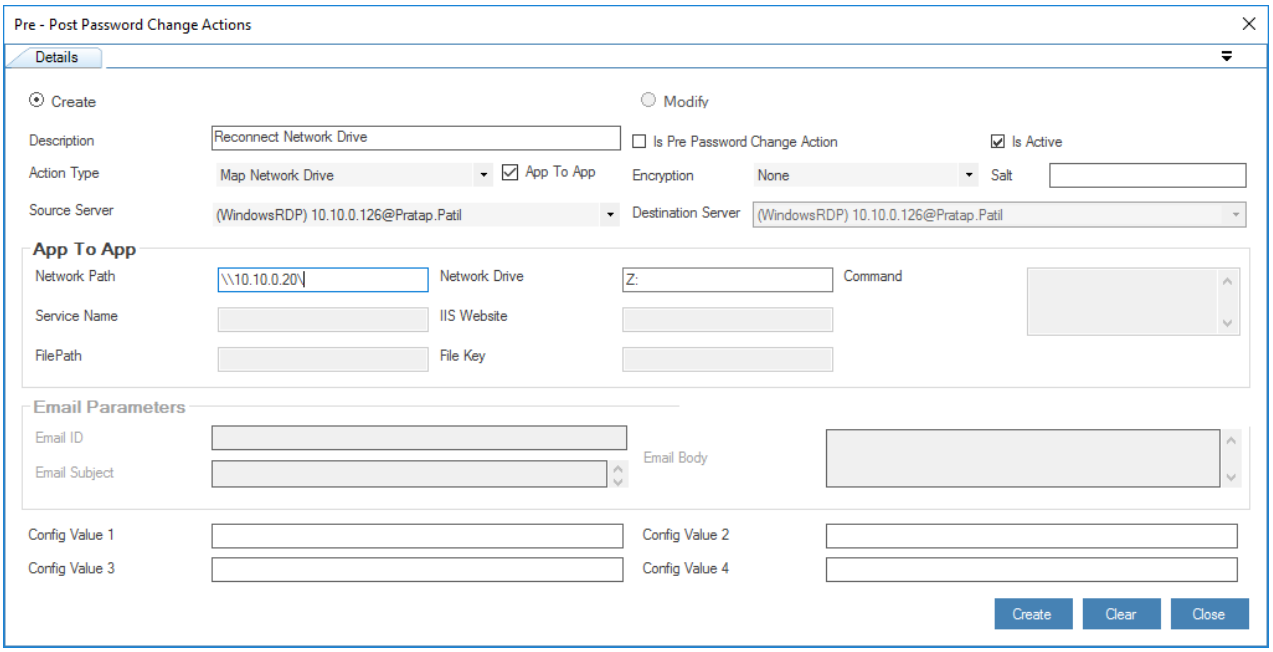
2. **Update Service Account Password** - Select the **Update Windows Service Logon User Password** from the **Action Type** dropdown. Provide the **Service Name**.



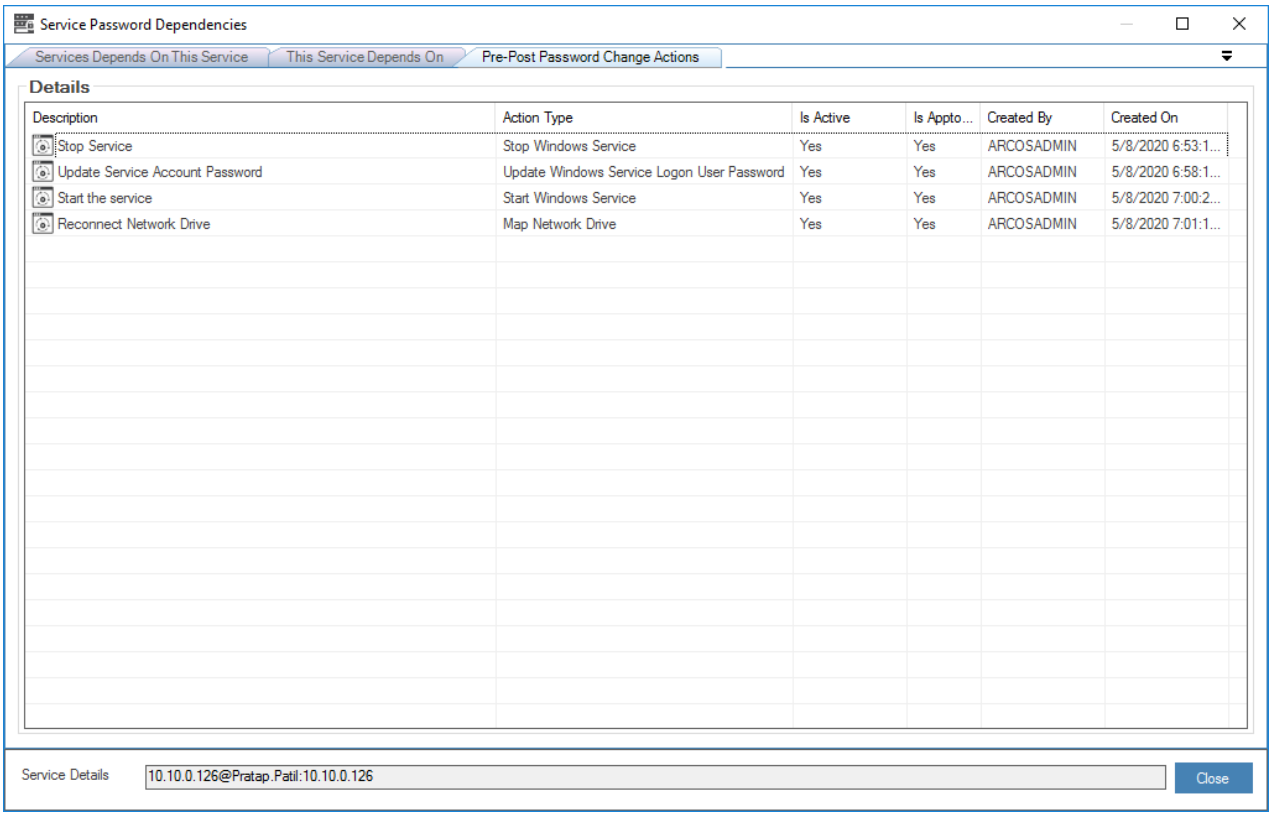
3. **Start Service** - Select the **Start Windows Service** from the **Action Type** dropdown. Provide the **Service Name** of the service that should get started.



4. **Reconnect Network Drive** - Select the **Map Network Drive** from the **Action Type** dropdown. Provide the **Network Path** and **Network Drive** to map it to.



5. On the following screen, you can see all the pre actions and post actions configured for this service.



7.6.4.4.2.1 WSB2BAutomation

SQL and Oracle are the Databases for this Application. On the password change of the database, it must be updated with the new password in the web.config file in cleartext. Moreover, also update the DSN settings of the respective application server.

7.6.4.5 Other Applications

- TERMS
- Fircosoft
- Trans_Rep
- BBprosysy
- IPLA
- IPO system
- CES

7.7 Print Password Envelope

7.7.1 Overview

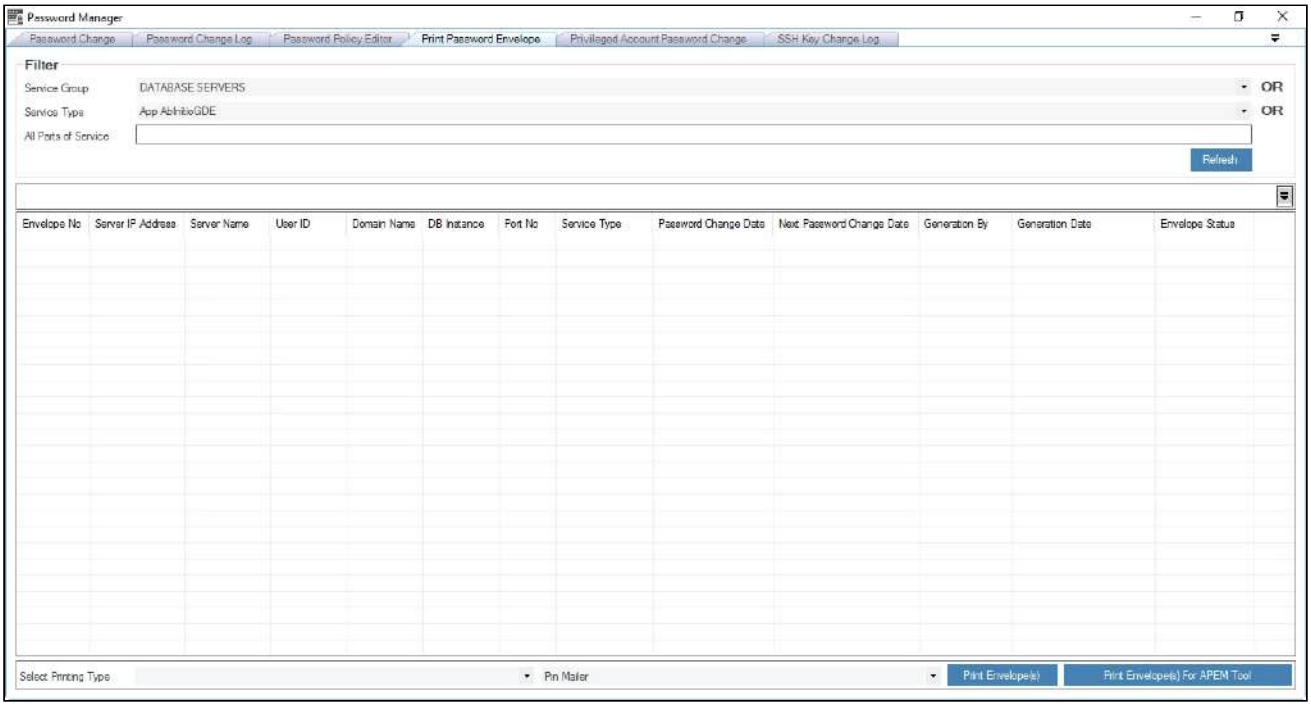
A password envelope containing the password is generated whenever the password of any service is changed. The password envelope can be printed in different forms such as Pin Mailer, pdf and APEM tool. This section helps you to print password envelope using the **Print Password Envelope** screen. The password envelopes are printed by selecting all the service connections whose passwords are to be printed. Logs are generated for all the actions performed via APEM tool.

- The Administrator having **Print Password Envelope** privilege in Server's Privileges will only be able to print Password Envelope in Pin Mailer or PDF format.
- The Administrator having **Generate Server Password Envelope** privilege in Server's Privileges will only be able to print password envelope with Envelope Status as Generated.
- The Administrator having **Reprint Server Password Envelope** privilege in Server's Privileges will only be able to print password envelope with Envelope Status as Printed, First Reprint, Second Reprint, Third Reprint, Fourth Reprint, Fifth Reprint, Sixth Reprint, Seventh Reprint, Eighth Reprint and Ninth Reprint.
- The Administrator having **Verify Reprint Server Password Envelope** privilege in Server's Privileges will only be displayed as approver in drop down list to authenticate password printing process.
- The service groups or service types available in the **Service Group** and **Service Type** drop down list are displayed based on the LOB selected from the **Select LOB/Profile** drop down list available in the home screen (Server Manager).
- Crystal Reports can also be used to generate Password Envelopes.
- To generate a Unique Password Envelope for similar Domain ID's, configure the toggle value in **Generate Envelope By Domain IDs** configuration as **Enabled** in **Settings**. This configuration is used to generate and send a unique password envelope for similar Domain IDs based on the scheduled time in **Schedule Master**.

7.7.1.1 Print Password Envelope - Pin Mailer/Pin Mailer A4

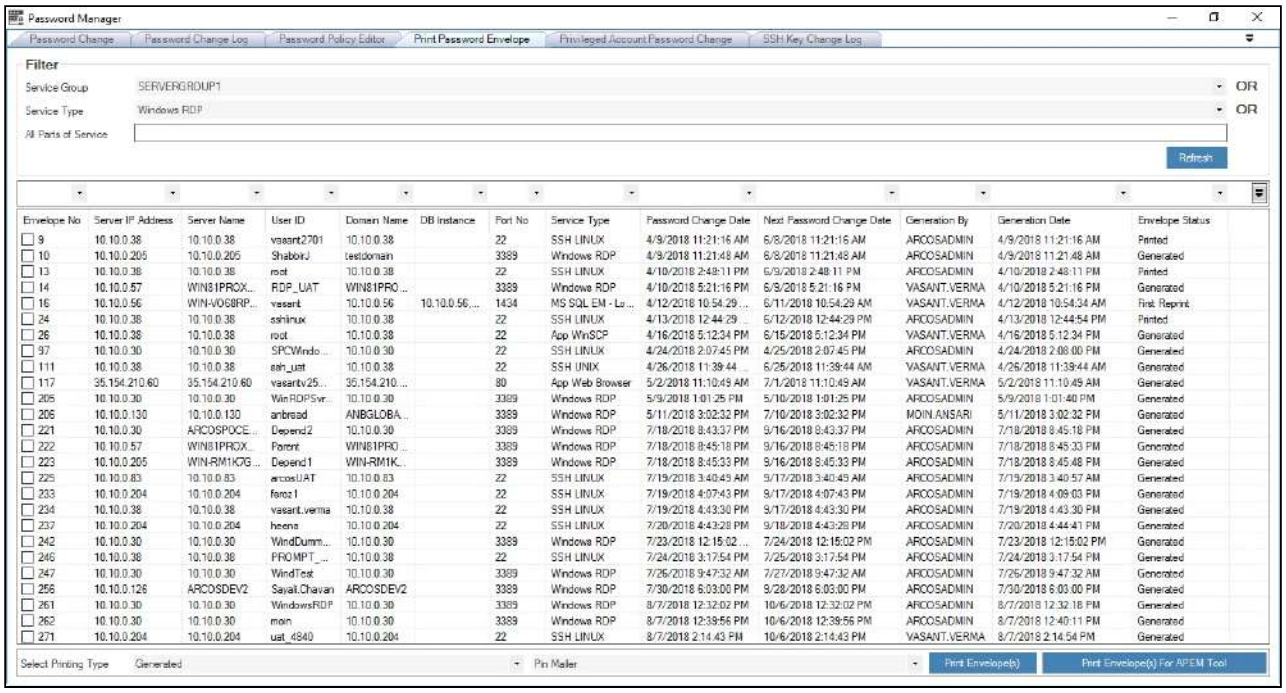
To print password envelope use the following path:

Manage → Password Manager → Print Password Envelope

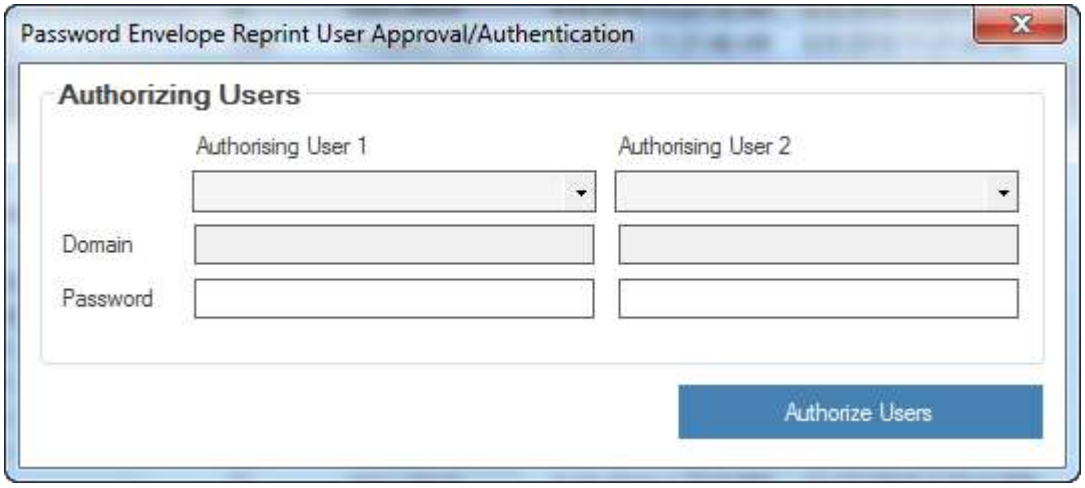


1. Select value from **Service Group** drop down to display password envelope details of services assigned to selected service group.

2. Select value from **Service Type** drop down to display password envelope details of services of selected service type.
3. Click **Refresh** to display password envelope details of all services, the services will be displayed as follows



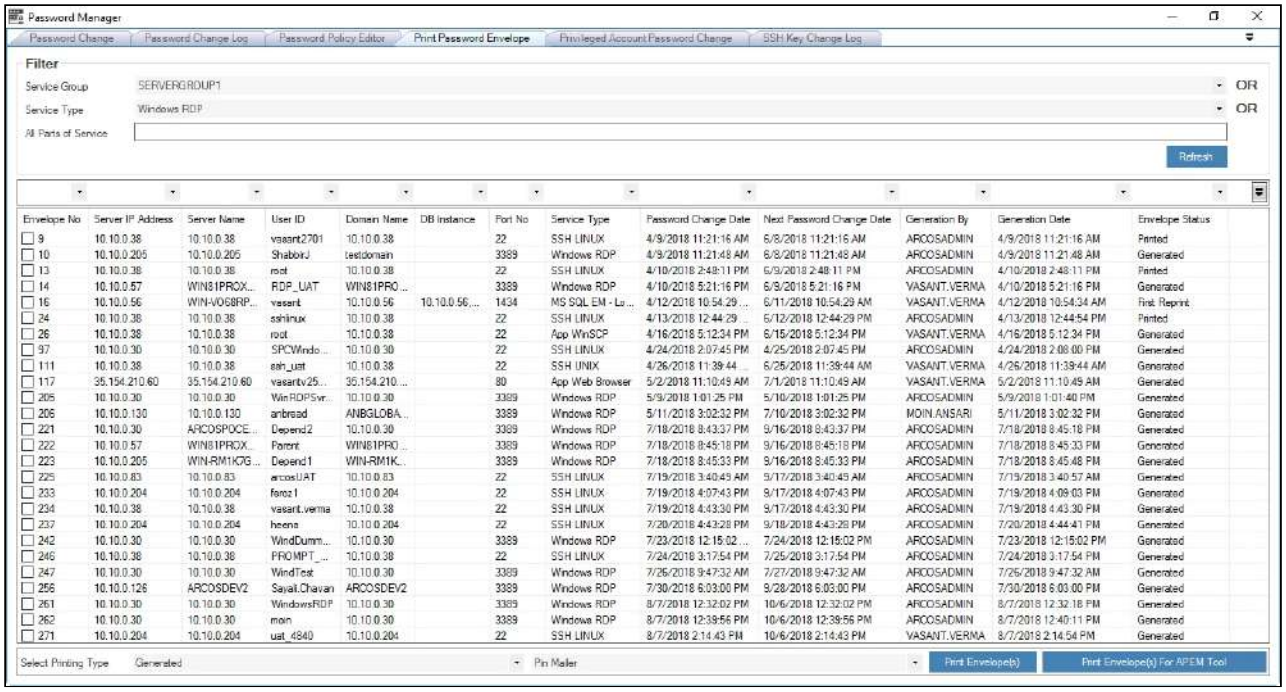
4. The above screen displays all details of the services for which the password has been generated.
5. Now select the envelope status of the password that should be printed such as Generated, Printed, First Reprint, Second Reprint and so on.
6. Select the Printing type such as Pin Mailer or Pin Mailer A4 and click Print Envelope



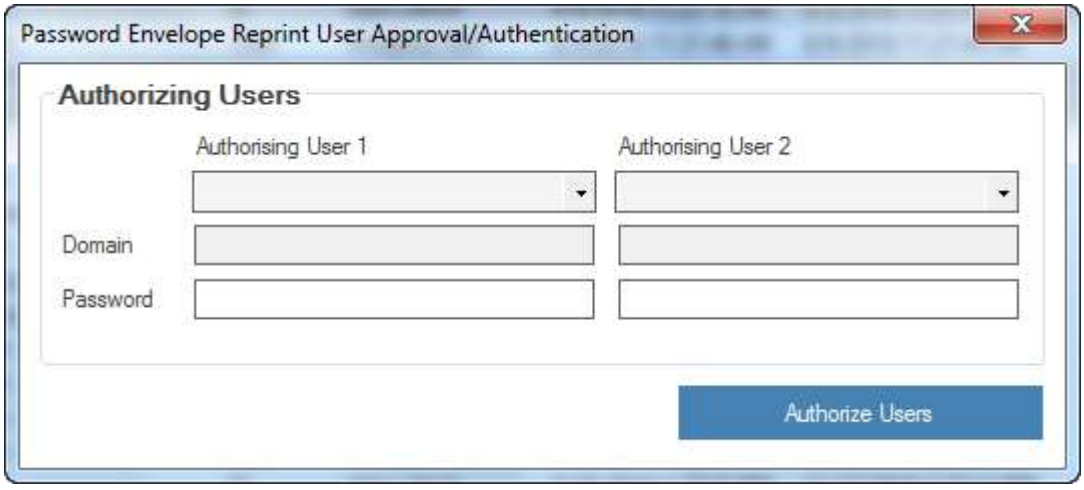
7. The Authorizing users screen will be displayed, two users with the privilege "**Verify Reprint Server Password Envelope**" will have to authorize the user to print or reprint the Password.
8. Select the Pin mailer printer and click Print; the password shall be printed.

7.7.1.2 Print Password Envelope - .Pdf/Pdf A4

1. Select value from **Service Group** drop down to display password envelope details of services assigned to selected service group.
2. Select value from **Service Type** drop down to display password envelope details of services of selected service type.
3. Click **Refresh** to display password envelope details of all services, the services will be displayed as follows



4. The above screen displays all details of the services for which the password has been generated.
5. Now select the envelope status of the password that should be printed such as Generated, Printed, First Reprint, Second Reprint and so on.
6. Select the Printing type such as .pdf or .pdf A4 and click Print Envelope

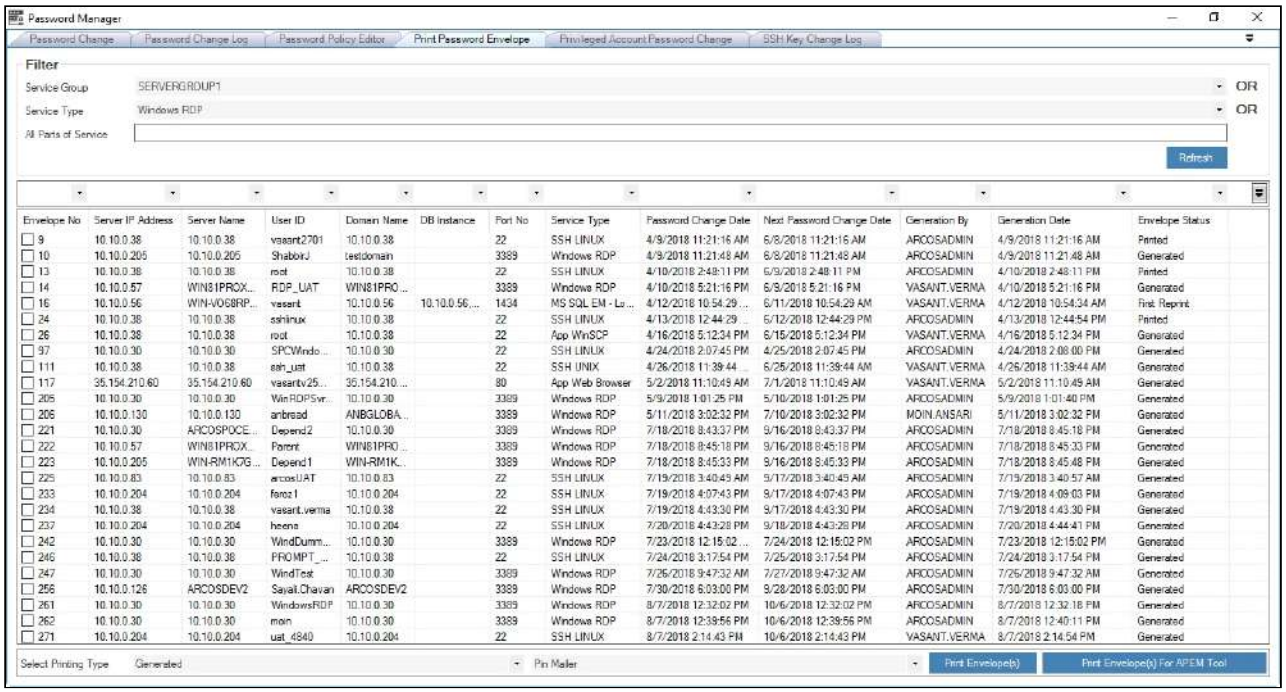


7. The Authorizing users screen will be displayed, two users with the privilege "**Verify Reprint Server Password Envelope**" will have to authorize the user to print or reprint the Password.

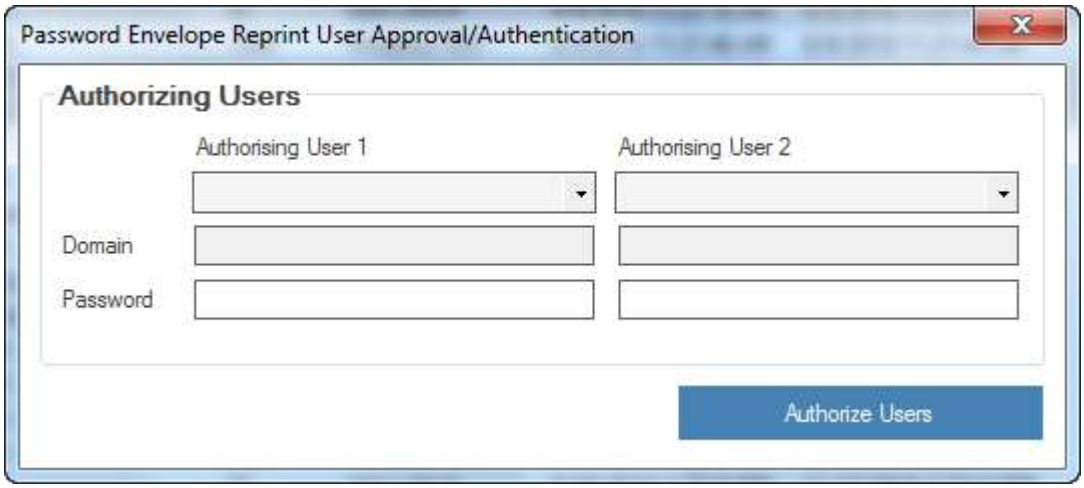
8. Set a 12 character password for the .pdf document and save the document to a secured location.
9. Open the .pdf file that you just created, it will prompt for a password, enter the same password you set before saving the pdf file.
10. View the password

7.7.1.3 Print Password Envelope - APEM Tool

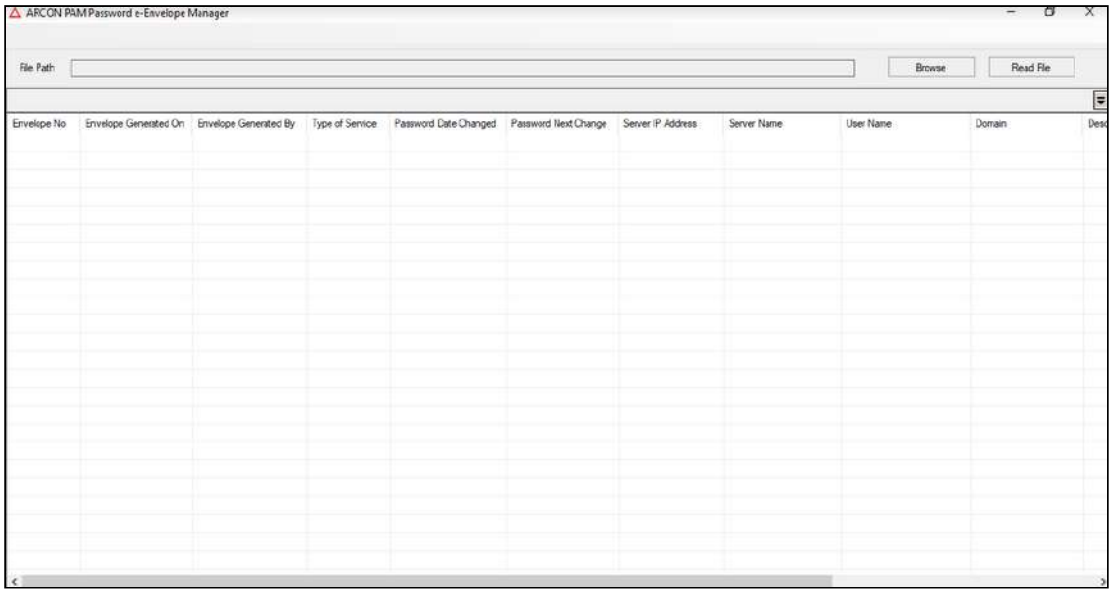
1. Select value from **Service Group** drop down to display password envelope details of services assigned to selected service group.
2. Select value from **Service Type** drop down to display password envelope details of services of selected service type.
3. Click **Refresh** to display password envelope details of all services, the services will be displayed as follows



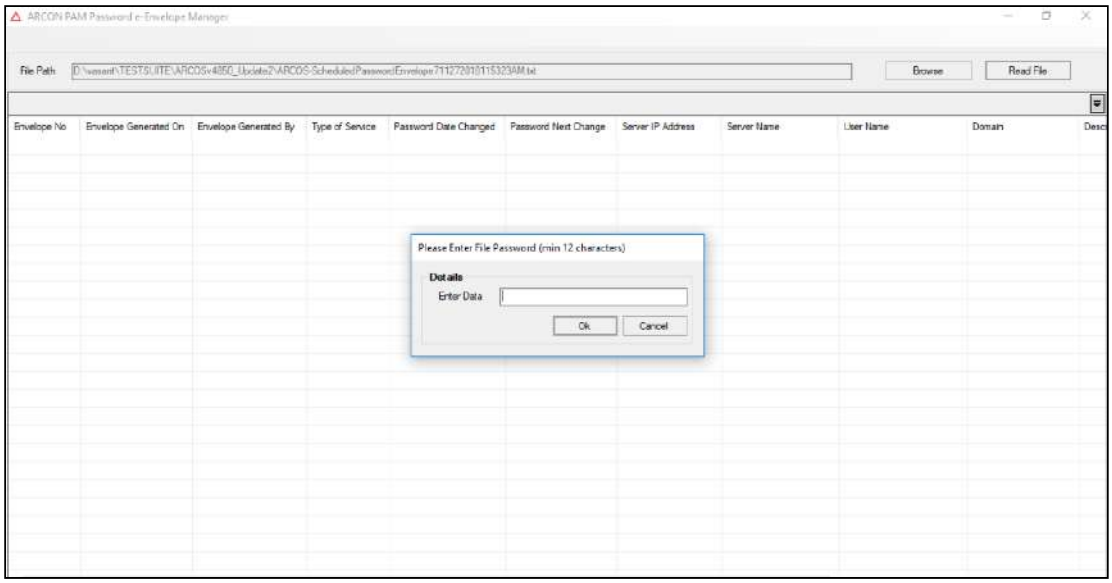
4. The above screen displays all details of the services for which the password has been generated.
5. Now select the envelope status of the password that should be printed such as Generated, Printed, First Reprint, Second Reprint and so on.
6. Click Print Envelope for APEM tool



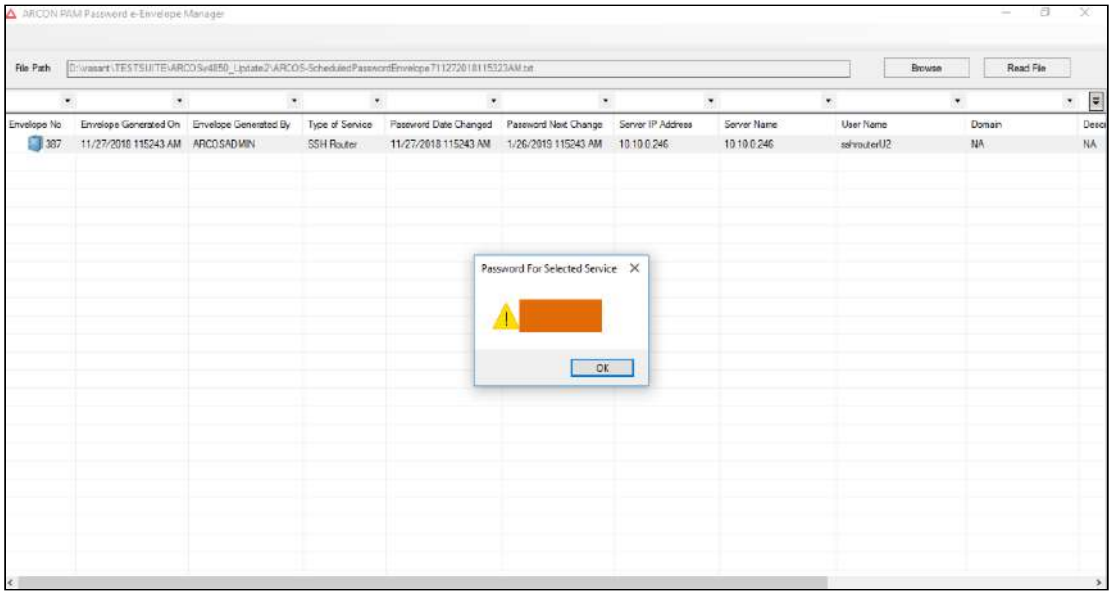
7. The Authorizing users screen will be displayed, two users with the privilege "**Verify Reprint Server Password Envelope"** will have to authorize the user to print or reprint the Password.
8. Set a 12 character password for the .txt document and save the document to a secured location.
9. To view the password, Open APEM tool



10. Browse the .txt file generated and click Read file, it will prompt for a password, enter the same password you set before saving the txt file.



11. The password envelope will be listed as follows, Double click on the password envelope row to view the password.



- If the toggle value for **Generate Password Envelope For New Service - Is Enabled** in **Settings** is **Enabled**, then newly created services are displayed in Print Password Envelope tab for printing whereas if the value is set to 0, then only those services are displayed for printing whose passwords have been changed.
- If the toggle value for **Password Envelope Protected File** in **Settings** is **Enabled,** then the password envelopes (printed on clicking **Print Envelope(s) For APEM Tool** button) will be in .zip format whereas if the value is set to 0, then password envelope will be in .txt format.

7.7.1.3.1 APEM Tool

Follow these steps to use APEM (ARCON PASSWORD ENVELOPE MANAGER) tool

1. Go to Help page in Server Manger, click About option
2. On the About page, a Desktop Finger Print ID shall be listed, send this ID to ARCON team.
3. ARCON team shall generate a customized APEM tool exe based on the to Desktop Finger Print ID provided
4. Run the .exe

> ⚠
> - Users can run the ARCOSPasswordeEnvelopeManager.exe only on the system from where desktop finger print Id was provided
> - The Password envelope status does not change when printed through APEM tool.

7.7.1.3.2 APEM Logs

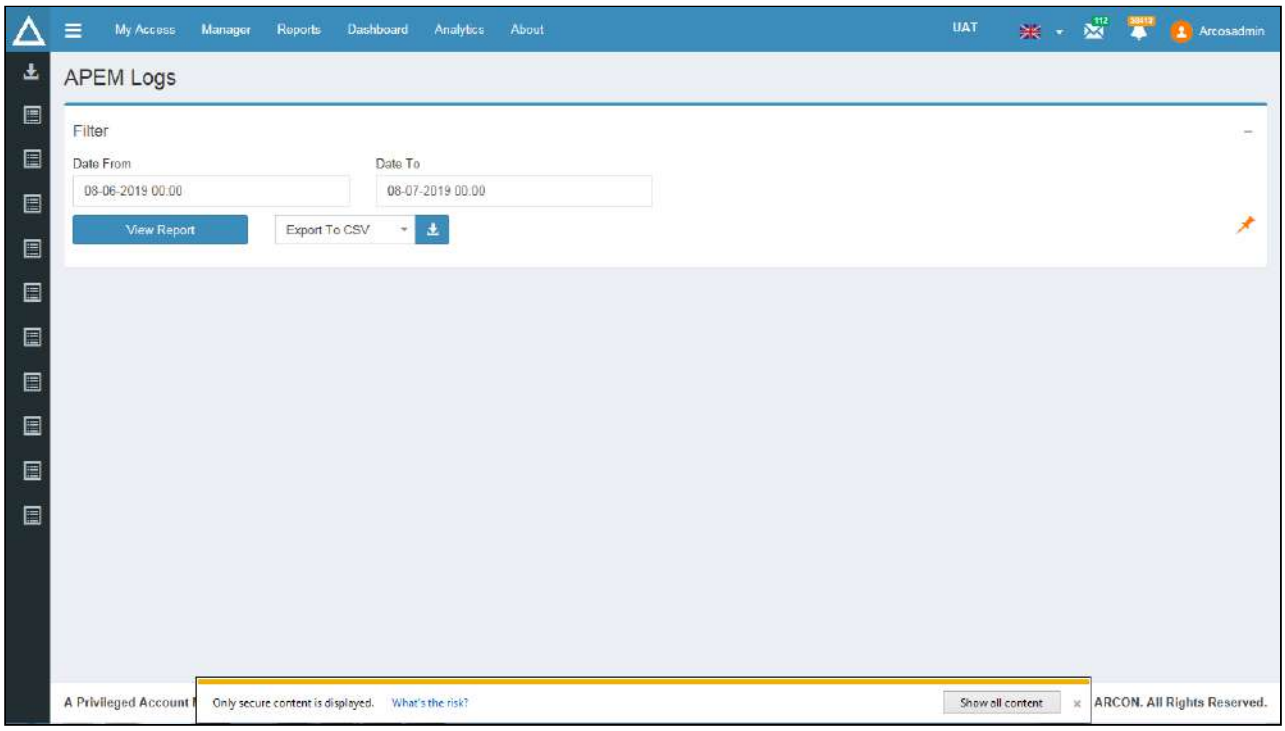
APEM logs displays logs of actions performed via APEM tool. Actions such as opening APEM application, reading file, and viewing password are captured in APEM logs.

> ⚠ User having **APEM Logs** privilege will be able to view **APEM Logs**.

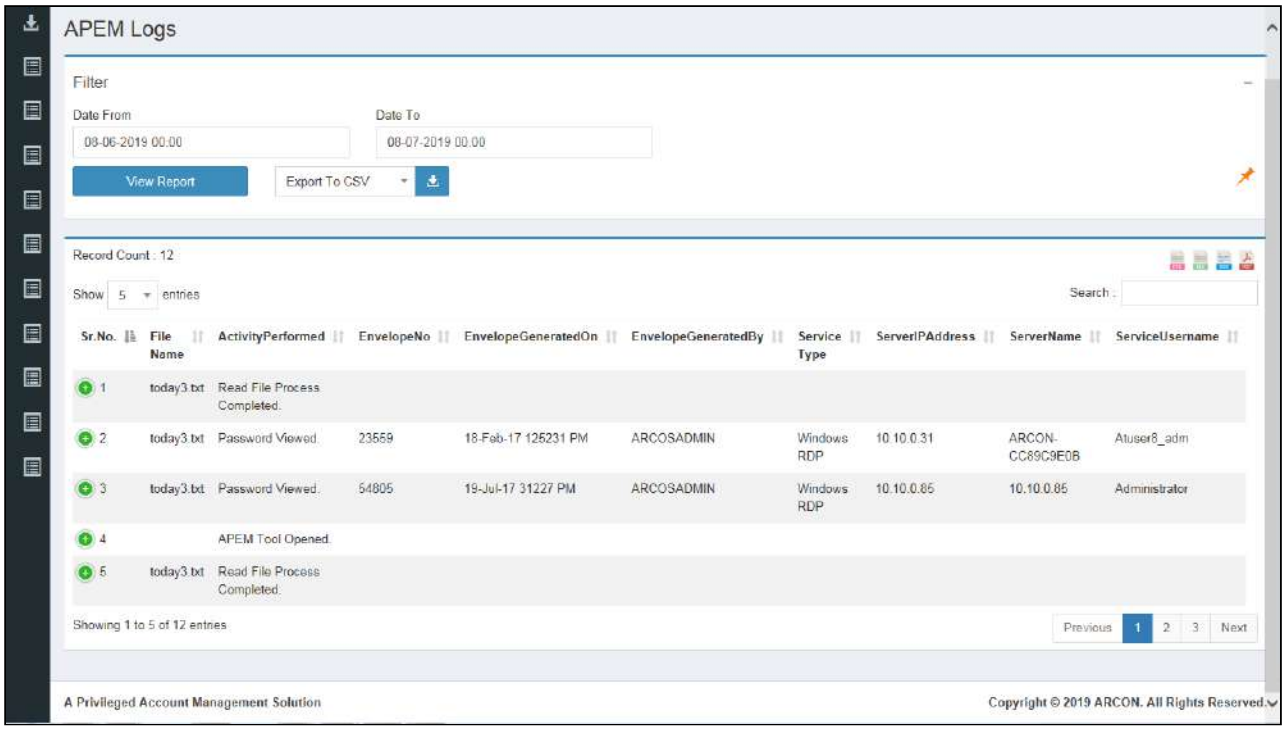
To navigate to APEM Logs, use the following path:

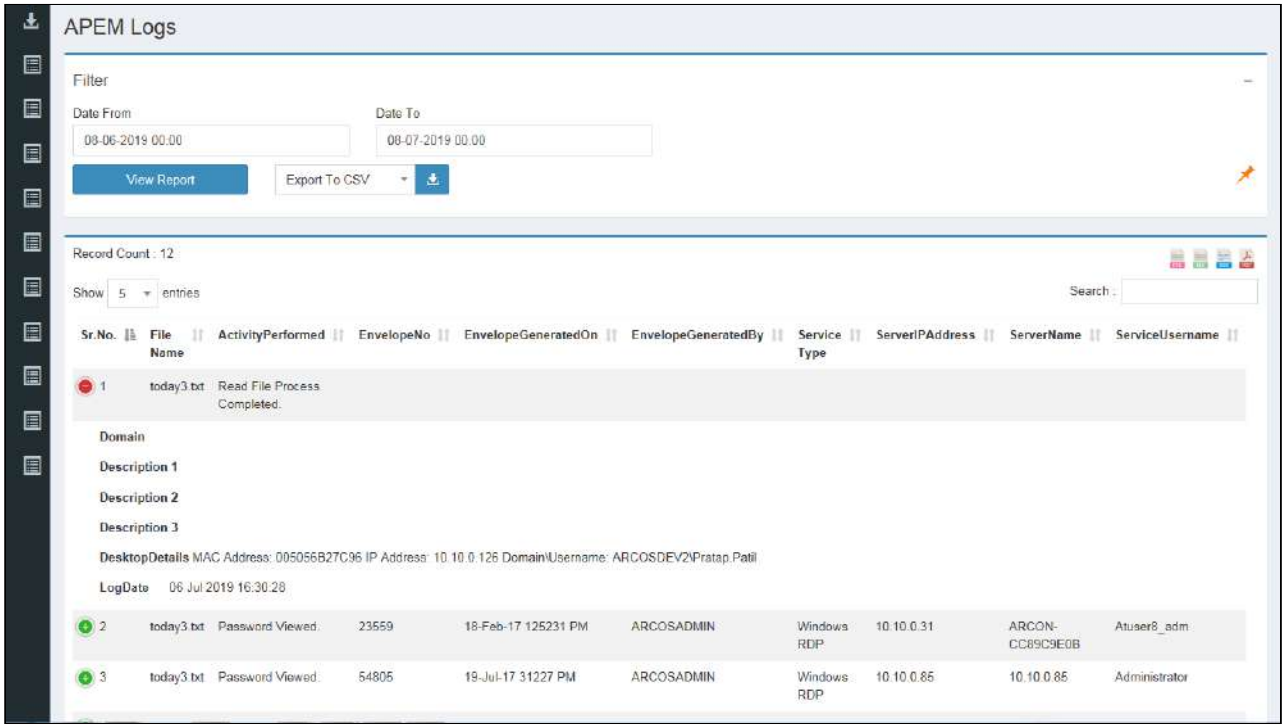
Client Manager → Reports → Logs → APEM Logs

1. Click **APEM Logs**. The following screen is displayed.



2. Select Start Date and End Date from the **Date From** and **Date To** fields respectively and click **View Report**. It displays details such as Name of the File, Activity Status, Envelope Number, Date and Time on which the envelope was generated, Name of the User trying to generate envelope, Type of Service, Server IP address, Server Name, and Service Username.





3. Select the number of entries from the **Show entries** drop down list, to display only those numbers of records in the grid.
4. To search for a particular record, enter the required search filter in the **Search** text field, on the right hand side of the screen.

5. Click  icon, to view details of desktop and log date and timestamp details.
6. To pin the report to Dashboard, click  icon.
7. Click  icons displayed on the right side corner of the screen to select the file type for exported reports. The download request will be processed and will be available for download in Exported Reports screen.

   ⚠ For downloaded reports, refer **Exported Reports** section in **Client Manager Guide**.

7.8 Schedule Password Change Process

Automatic password change process is performed by scheduled password change service. This service allows the Administrator to change the passwords of the target device automatically based on the scheduled date every month. Based on LOB/Profile Default Configuration configured in ARCON PAM, the automatic password change refers to the password change policy. It fulfils basic requirements of compliance such as, the number of upper case and lower case characters in the password, the length of the password, special characters used in the password, and so on. Based on the organization's policy and compliance requirements, one can configure the type of passwords that ARCON PAM should generate and update it on the devices.

Example, on the Windows servers and in ARCON PAM, the password change is set to 30 days then this service will change all the Windows passwords as configured.

⚠ Henceforth, we will call the Schedule Password Change as SPC service.

This section includes the following topics:

- SPC for Single Service
- SPC for Group Services

7.8.1 Schedule Password Change Process for a Service

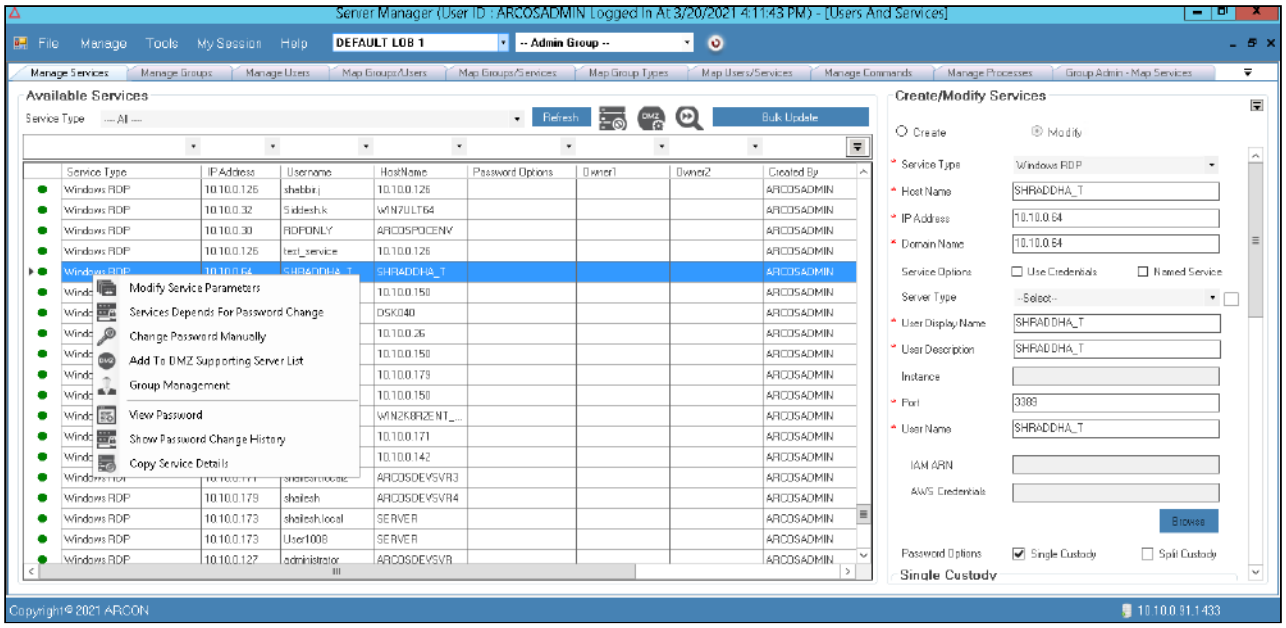
This section helps you to schedule password change process for a particular service.

To schedule password change process for a service:

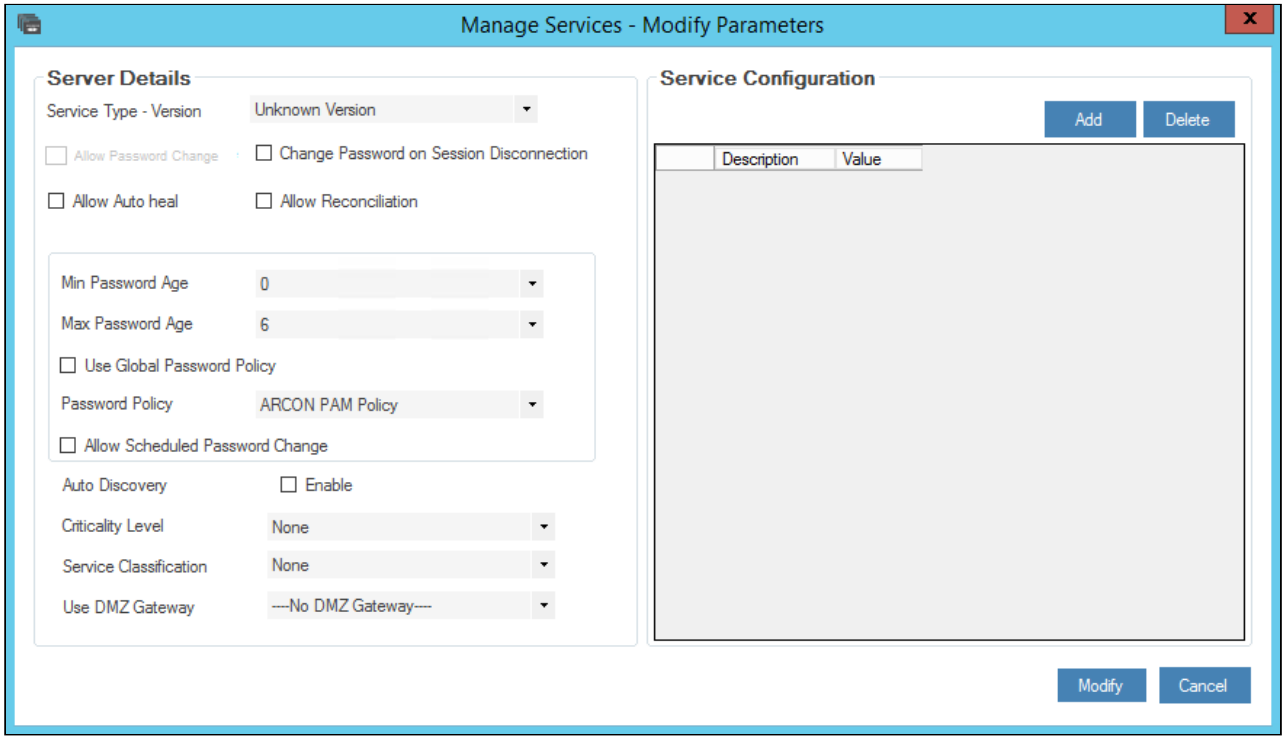
To schedule password change process for a particular service use the following path:

Manage → Users and Services → Manage Services

1. Right click on the service for which you want to schedule the password change process and choose **Modify Service Parameters** option.



2. The **Manage Services - Modify Parameters** screen is displayed.



> ⚠ The services available in the grid are displayed based on the LOB and service type selected from the **Select LOB/Profile** drop down list (in the home screen Server Manager) and **Service Type** drop down list respectively. Click **Refresh** button after selecting the **LOB** and **Service Type.**

The **Manage Services – Modify Parameters** screen displays the following fields:

Field Name	Description
Change Password on Session Disconnection	The password of the service changes after the session is closed from the PAM.
Allow Auto heal	To enable auto-healing for the service.
Allow Reconciliation	To enable reconciliation for the service.
Min Password Age	Select minimum days for scheduled password change process. ⚠ Password of Service will not be changed before the defined minimum days. Eg.:If you configure Minimum Password Age as 3; then password change process cannot be performed before 3 days.
Max Password Age	Select maximum days for scheduled password change process. ⚠ The password change process will be scheduled automatically depending on the selected max password age field.
Use Global Password Policy	Select to enable the global policy configured for password change process.
Password Policy	Select the password policy. ⚠ By default, **Default Profile** is selected. You can create your own password policy, save it and select it in this field.
Allow Scheduled Password Change	Select to enable/configure scheduled password change process. ⚠ By enabling this checkbox the password change process for the selected service will be scheduled according to the selected min and max password age and selected password policy or the global password policy.

3. Select the details and click **Modify** button. A window pops up displaying the following message: **Service Parameters Updated**
4. Click **OK**. The password change process for the selected service is scheduled.

⚠ In case of SPC password failure, SPC password change can be attempted at a pre-defined interval.

The **Settings SPC failed services Interval (Hours)** has been added. The value minimum can be 1, the password change shall be attempted every one hour. The maximum value can be set as per requirement, the password change shall be attempted after the specified hours.

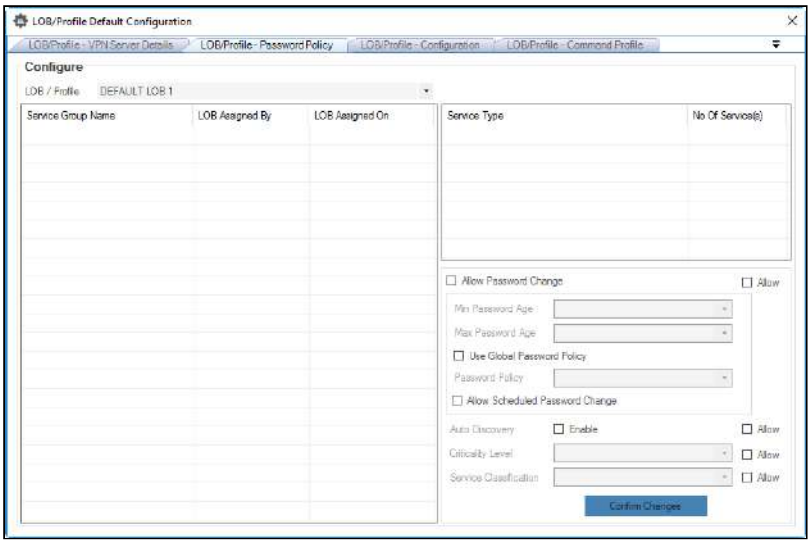
7.8.2 Schedule Password Change for Multiple Services

This section helps you to schedule password change process for multiple services.

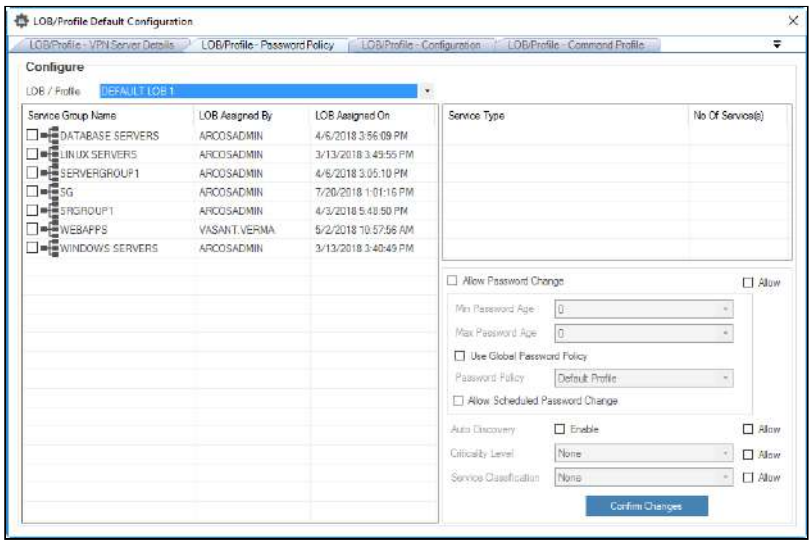
To schedule password change process for multiple services:

To schedule password change process for multiple services use the following path:

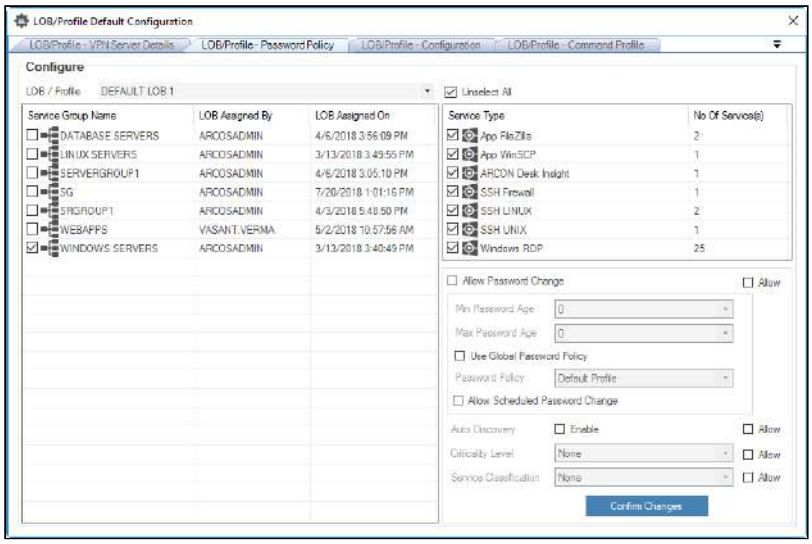
Tools → Advanced Configuration → LOB/ Profile Default Configuration → LOB/ Profile – Password Policy tab



1. Select LOB from **LOB/ Profile** dropdown list. The service groups are displayed in the grid.

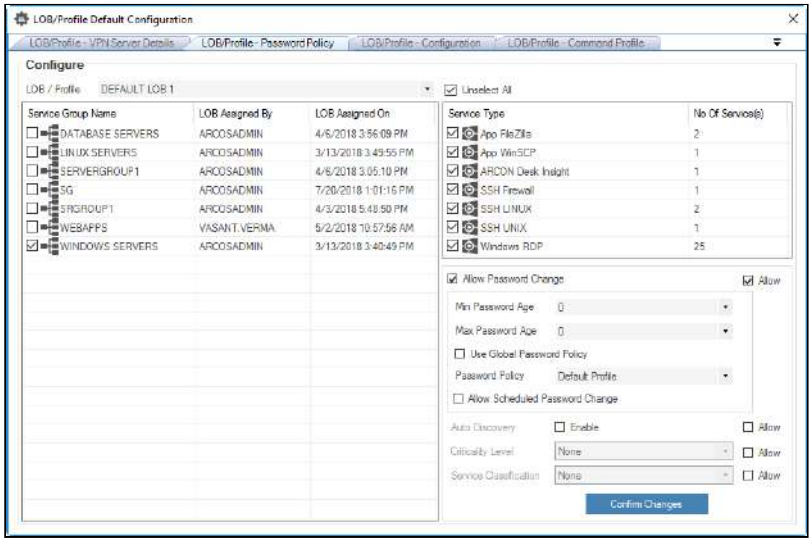


2. Select the service group from the list of service groups. The services mapped to the service group are displayed in the **Service Type** grid on the right side.



⚠ By default, all the services are selected and can be scheduled for password change process.

3. Select **Allow** checkbox and then select **Allow Password Change** checkbox to enable the fields for updating.



The **Manage Services – Modify Parameters** screen displays the following fields:

Field Name	Description
Allow Password Change	Select to enable the fields for password change process.
Min Password Age	Select minimum age for scheduling password change process.
Max Password Age	Select maximum age for scheduling password change process. ⚠ The password change process will be scheduled automatically depending on the selected max password age field.

Field Name	Description
Use Global Password Policy	Select to enable global policy configured for password change process.
Password Policy	Select the password policy. ⚠ By default, it's the **Default Profile**. You can create your own password policy, save it and select it in this field.
Allow Scheduled Password Change	Select to enable/configure scheduled password change process. ⚠ By enabling this checkbox the password change process for the selected service will be scheduled according to the selected min and max password age and selected password policy or the global password policy.

4. Select the details and click **Confirm Changes** button. A window pops up displaying the following message:
   Are You Sure You Want To Apply LOB/Profile – Password Policy To Selected Service Group(s)
5. Click **Yes**. Another window pops up displaying the following message:
   LOB/Profile – Password Policy Applied Successfully
   No Of Services Updated: (Number)
6. Click **OK**. The schedule password change process is configured for the selected group.

⚠ In case of SPC password failure, SPC password change can be attempted at a pre-defined interval.

The **Settings SPC failed services Interval (Hours)** has been added. The value minimum can be 1, the password change shall be attempted every one hour. The maximum value can be set as per requirement, the password change shall be attempted after the specified hours.

7.9 View Password Change History

This section helps you to view the detailed history of the changed passwords for a selected service. It displays details such as type of service, description of server, user ID of service, date & time on which the password is changed, name of the user or service through which password is changed, and status of the changed password.

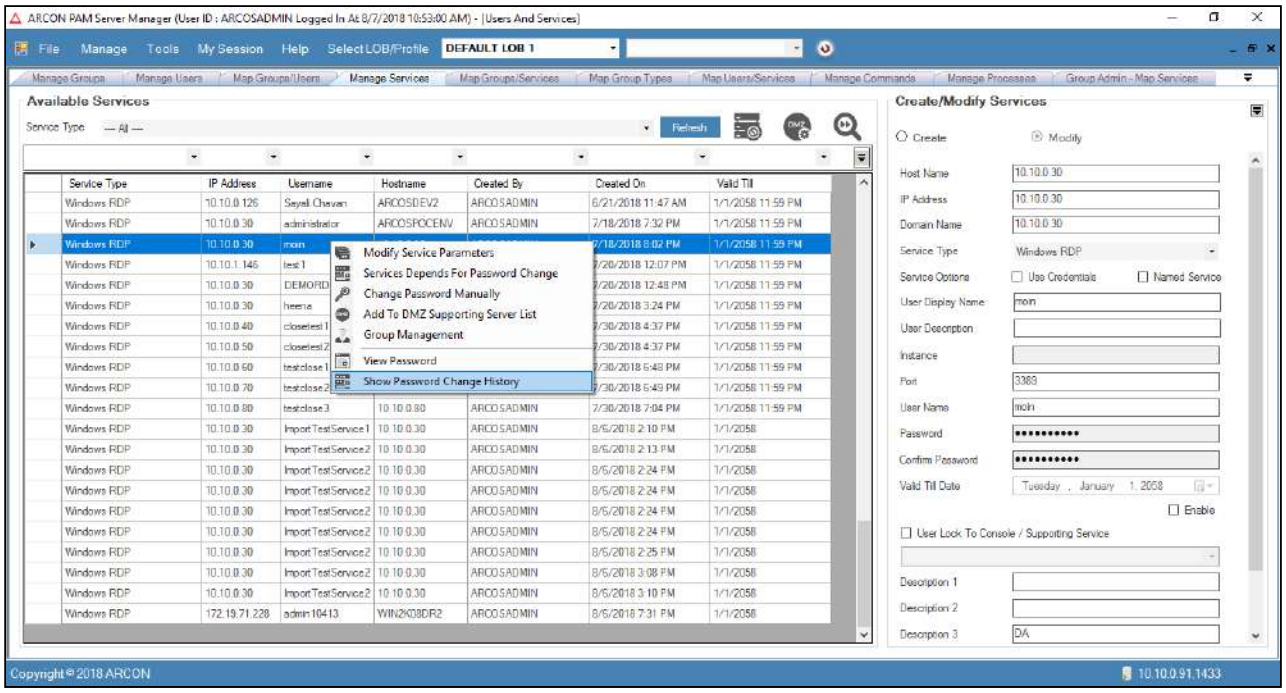
⚠ The Administrator having **Show Password Change History** privilege in Server's Privilege will only be able to view detailed history of the changed password of a service.

To view Password Change History:

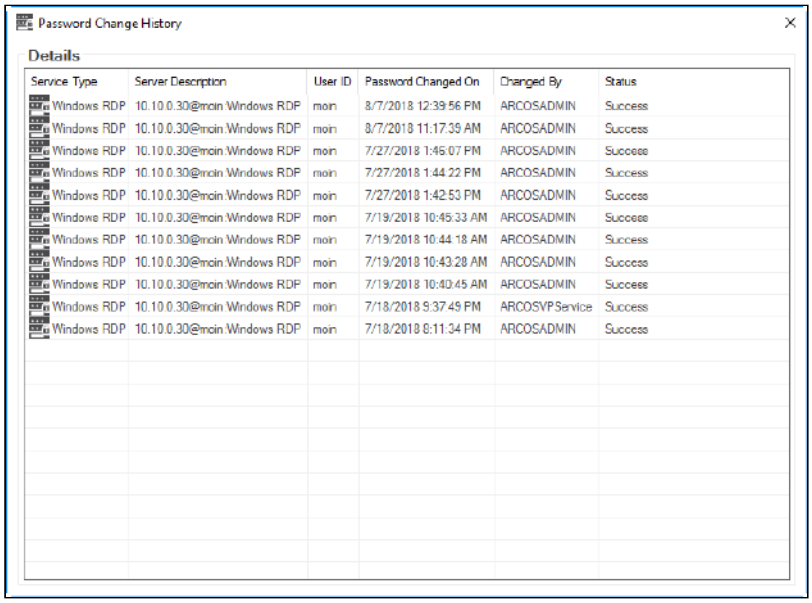
To view password change history use the following path:

Manage → Users and Services → Manage Services

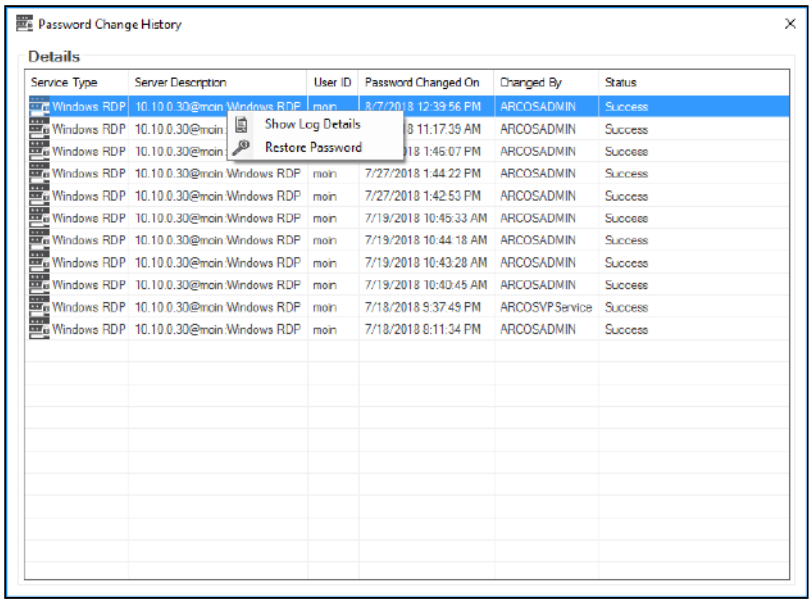
1. Right click on the service. A multiple options list is popped up.



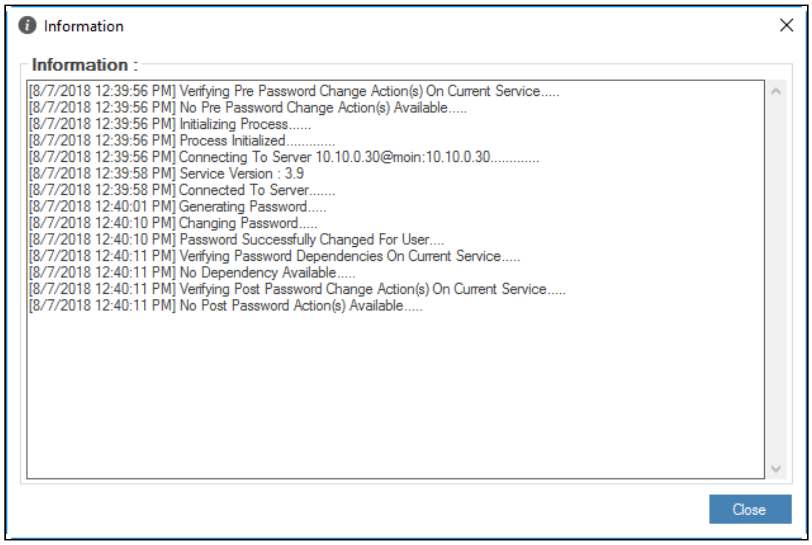
2. Click **Show Password Change History** option. The **Password Change History** screen is displayed which displays details such as type of service, description of server, user ID of service, date & time on which the password is changed, name of the user or service through which password is changed, and status of the changed password.



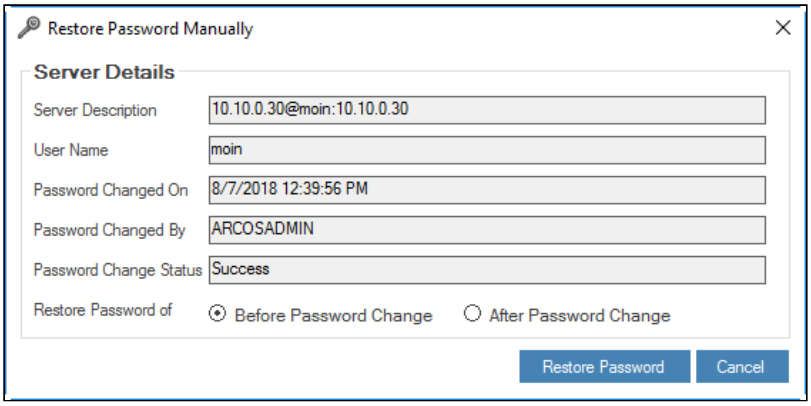
3. View the password history details.
4. Right click on the required password history detail. A pop up is displayed with two options:



- **Show Log Details:** Displays the password change log details.



- **Restore Password:** Helps to restore password both in ARCON PAM and Target Device.



To Restore Password of selected Service:
Passwords can be restored on Target Server/ARCON PAM Vault before or after Password Change Process.

- **Before Password Change:** If password is changed only on Target Server after password change process, then select **Before Password Change** radio button and click **Restore Password** button, to restore the password.
- **After Password Change:** If password is changed only in ARCON PAM Vault after password change process, then select **After Password Change** radio button and click **Restore Password** button, to restore the password.

> ⚠ If the toggle value for **Restore Password - Is Enabled** is **Enabled** in **Settings**, then only you will be able to view the **Restore Password** option in the **Password Change History** screen whereas if the toggle value is **Disabled** then the option will not be available for use.

To Restore Password of Dependent Service:
The password of Dependent Service is restored when password of parent service is restored to previous password. This is only achieved for services whose dependency type is configured as **Update Service Password Only** in **Select Service And Password Dependency Type** screen.

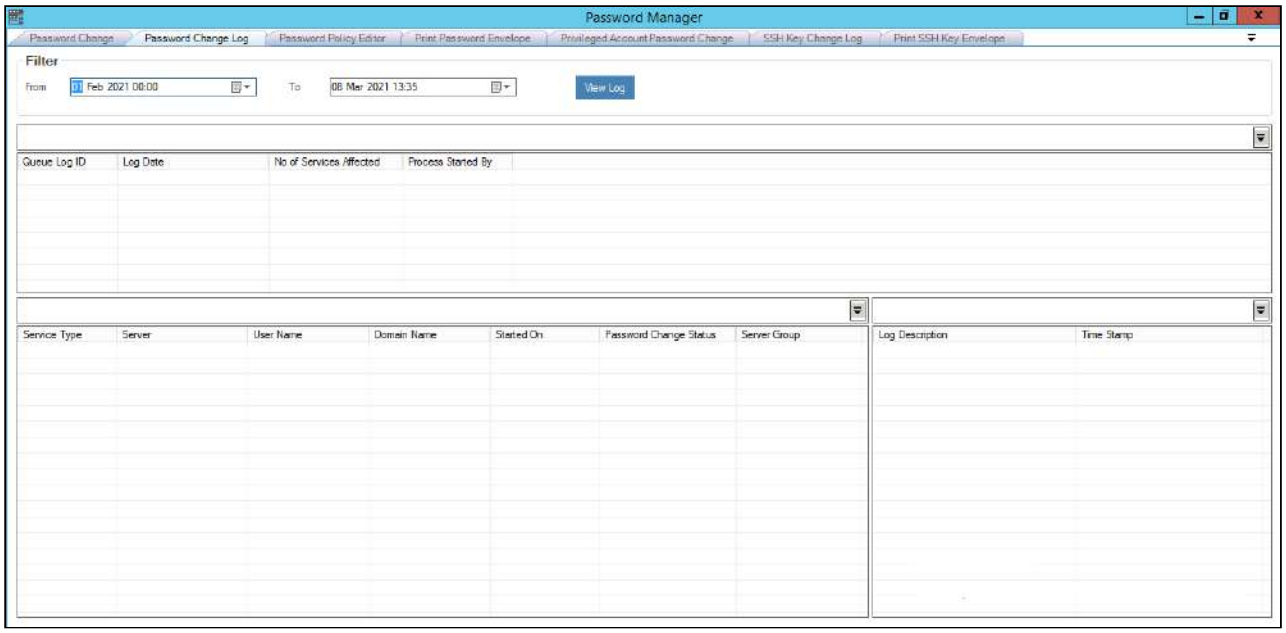
> ⓘ To know more about **Password Dependency** refer **Add Dependent Servers** from **Password Change Dependency** section.

7.10 View Password Change Log

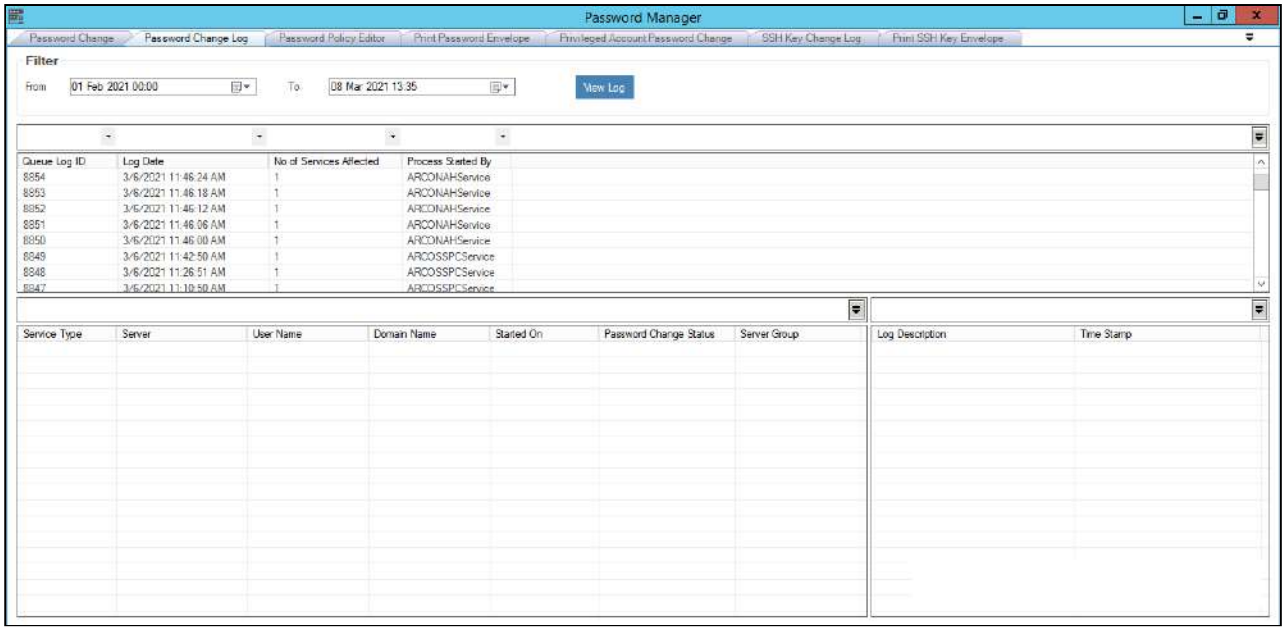
Password Change Log tracks the details of all the services whose passwords have been changed. This feature is used to view all the password change and auto-heal queue logs that are generated. It displays details such as queue log ID, date on which the log was generated, number of servers affected for password change process, and name of the user who initiated the password change process or name of the service through which the password change process is initiated.
The Administrator can view the log details for every queue log such as type of service, IP address of the server, username of the service, domain name of the service, date and time on which the password change process is initiated, status of the process, group of server, description of log and timestamp. In addition, you can export all the log data to .xls format.
To view the password change log use the following path:

Manage → Password Manager → Password Change Log

1. The **Password Change Log** displays the password change queue log. The queue log displays details such as the queue log ID, log date, number of services affected, and the name of the user who has initiated the process or name of the service through which the password change process is initiated.



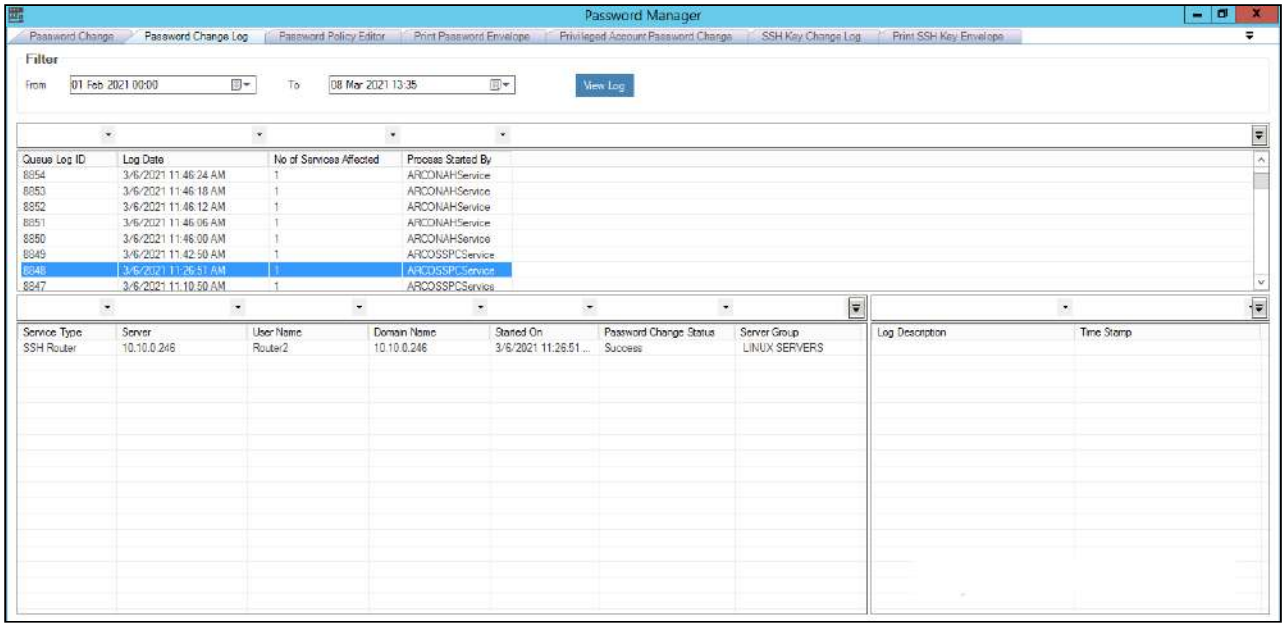
2. Select date from the **From** and **To** filters and click **View Log**.



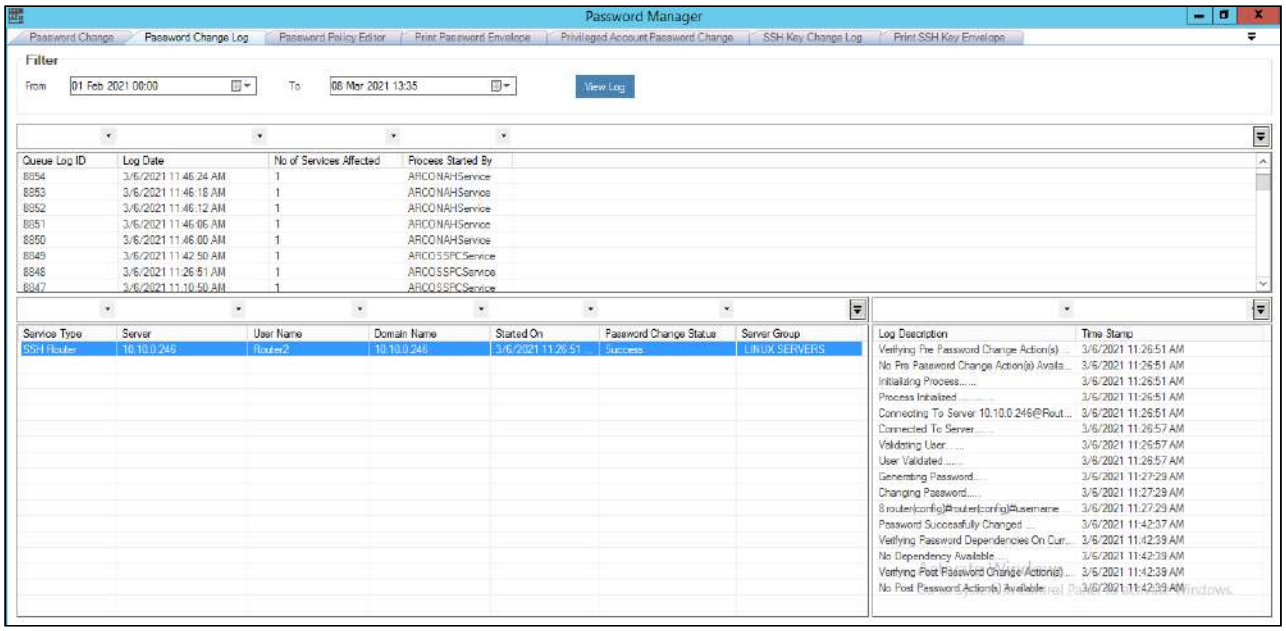
> ⚠ The details can be fetched for maximum 90 days (3 months). By default, current date is selected in **From** and **To** date field.

3. Click the queue log ID. The service details such as type of service, IP address of server, username of service, domain name of the service, date and time on which the password change process is initiated, status of

the process, and group of server are displayed in the grid.



4. Click the type of service from the grid. The service log details are displayed in the **Log Description** grid.



5. View the service password change details along with Terminal Details in **Log Description** grid. Terminal details displays detailed information of password change process at terminal end.

⚠

a. It is recommended to add **<PTY>** tag in **Parameter** field (Field 4) of Network Devices and SSH Linux/Unix services for capturing Terminal Details in Password Change Log.

b. ARCON PAM supports SSH Linux server hardened with following ciphers for password vaulting (Add **<PTY>** tag in Parameter field of service):

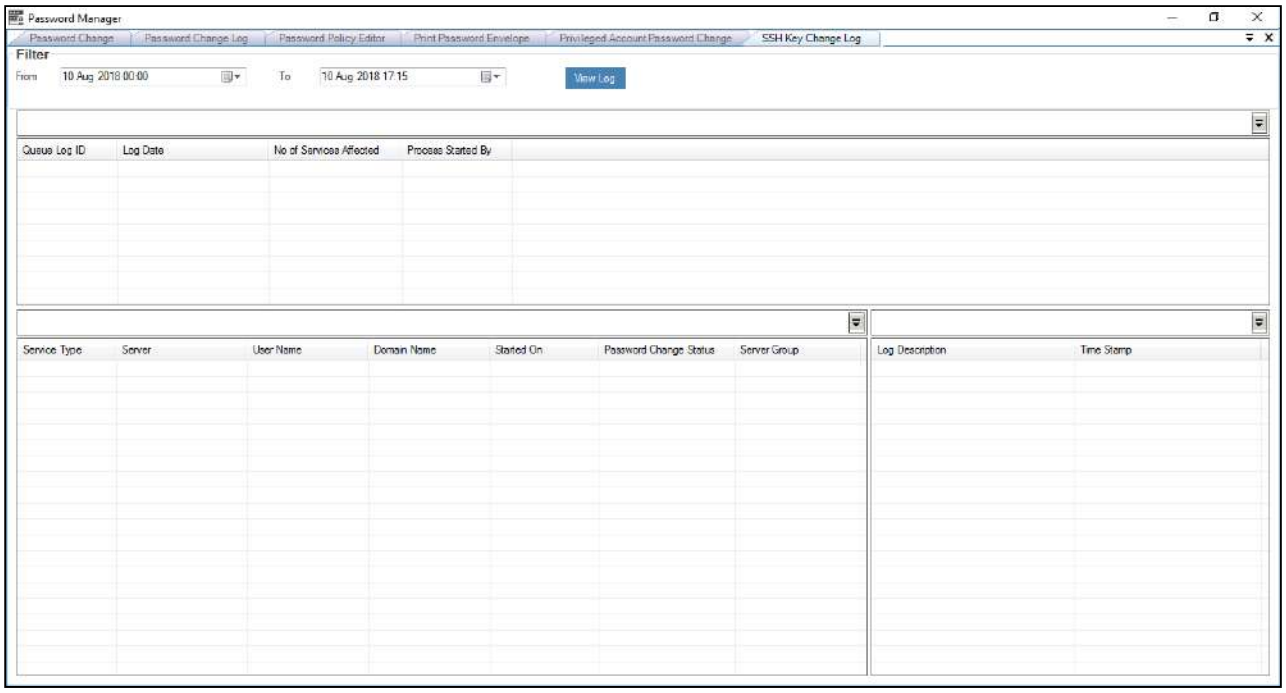
- **Cipher's supported by Component-Pro:-**
  - RSA_WITH_3DES_EDE_CBC_SHA
  - RSA_WITH_AES_128_CBC_SHA
  - RSA_WITH_AES_256_CBC_SHA
  - RSA_WITH_AES_128_CBC_SHA256
  - RSA_WITH_AES_256_CBC_SHA256
  - DHE_DSS_WITH_3DES_EDE_CBC_SHA
  - DHE_DSS_WITH_AES_128_CBC_SHA
  - DHE_DSS_WITH_AES_256_CBC_SHA
  - DHE_DSS_WITH_AES_128_CBC_SHA256
  - DHE_DSS_WITH_AES_256_CBC_SHA256
  - DHE_RSA_WITH_3DES_EDE_CBC_SHA
  - DHE_RSA_WITH_AES_128_CBC_SHA
  - DHE_RSA_WITH_AES_256_CBC_SHA
  - DHE_RSA_WITH_AES_128_CBC_SHA256
  - DHE_RSA_WITH_AES_256_CBC_SHA256
- **Host Key Algorithm**
  - RSA
  - DSS
  - X509 certificate.
- **Key Exchange Algorithm**
  - DiffieHellmanGroup1SHA1
  - DiffieHellmanGroup14SHA1
  - DiffieHellmanGroupExchangeSHA1
  - DiffieHellmanGroupExchangeSHA256

7.11 View SSH Key Change Log

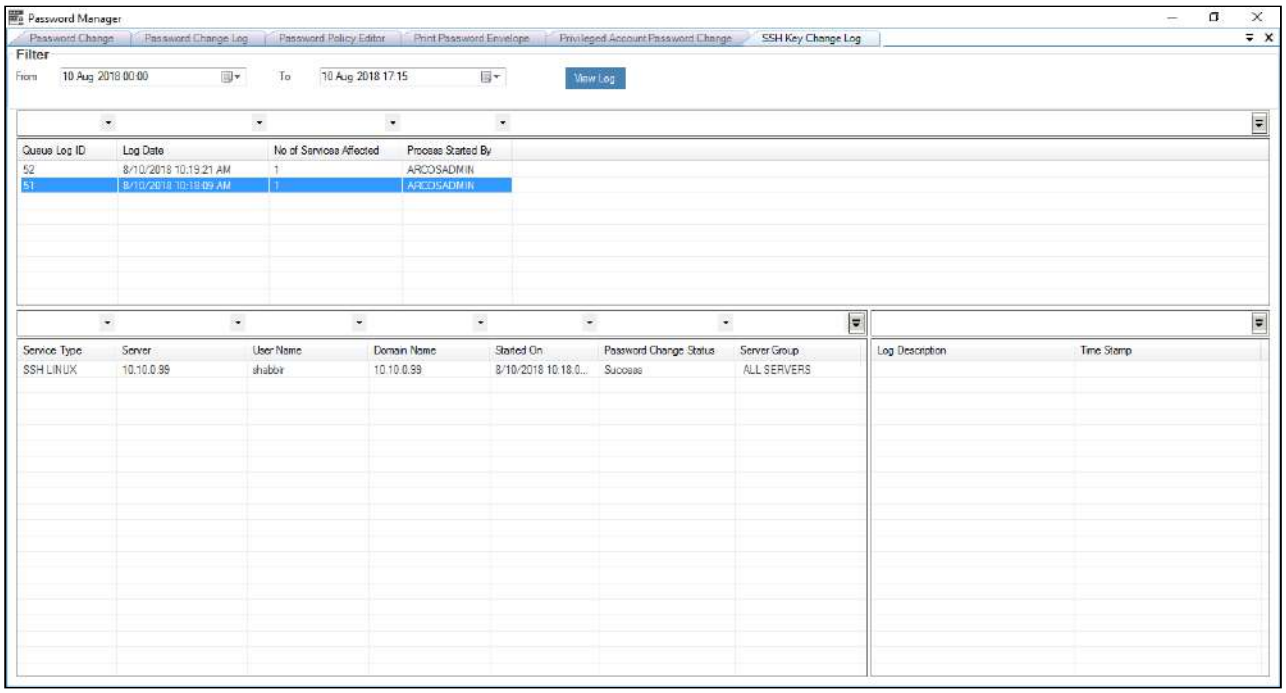
SSH Key Change Log tracks the details of SSH Linux services whose key has been changed. SSH key is only changed for those SSH Linux services for whom SSH Key Enabled option is configured.
This feature is used to view all the Key Rotation queue logs that are generated. It displays details such as queue log ID, date on which the log was generated, number of servers affected for key rotation process, and name of the user who initiated the key rotation process or name of the service through which the key rotation process is initiated.
The Administrator can view the log details for every queue log such as type of service, IP address of the server, username of the service, domain name of the service, date and time on which the key rotation process is initiated, status of the process, group of server, description of log and timestamp. In addition, you can export all the log data to .xls format.
To view the key rotation log use the following path:

Manage → Password Manager → SSH Key Change Log

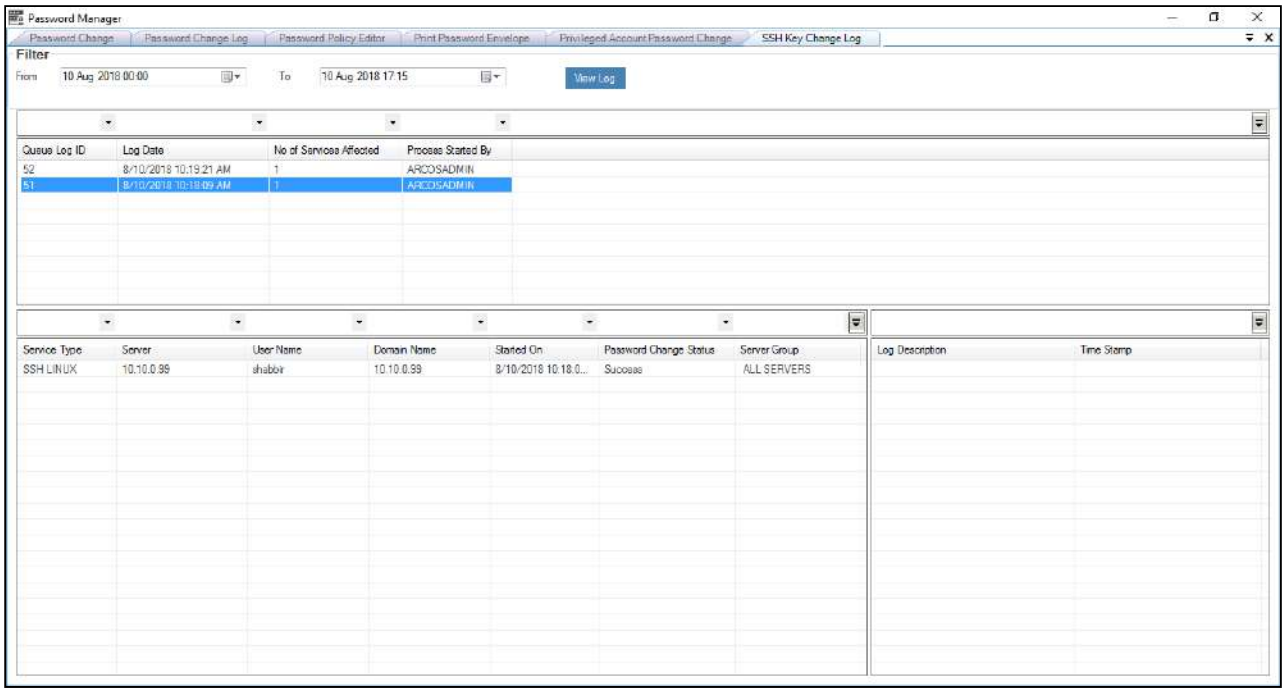
1. The **SSH Key Change Log** displays the key rotation queue log. The queue log displays details such as the queue log ID, log date, number of services affected, and the name of the user who has initiated the process or name of the service through which the process is initiated.



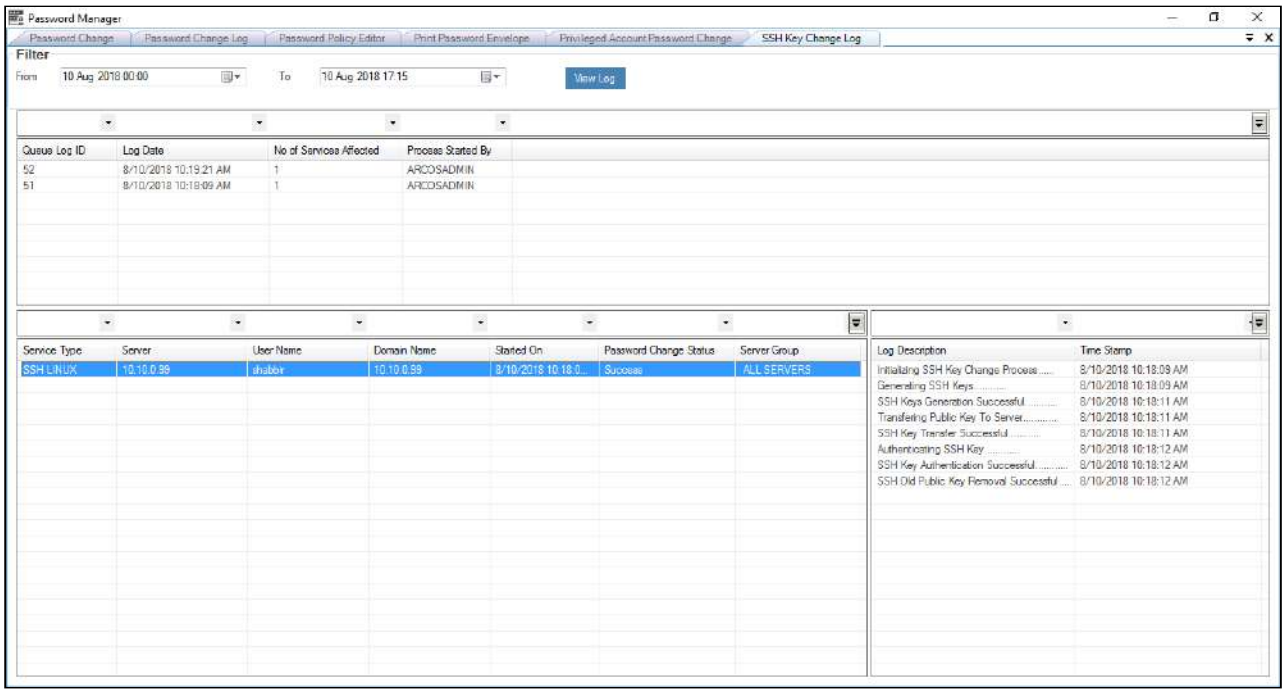
2. Select date from the **From** and **To** filters and click on **View Log** button.



3. Click the queue log ID. The service details such as type of service, IP address of server, username of service, domain name of service, date and time on which the key rotation process is initiated, status of the process, and group of server are displayed in the grid.



4. Click the type of service from the grid. The service log details are displayed in the **Log Description** grid.



5. View the service key rotation details along in **Log Description** grid.

7.12 Password Reconciliation

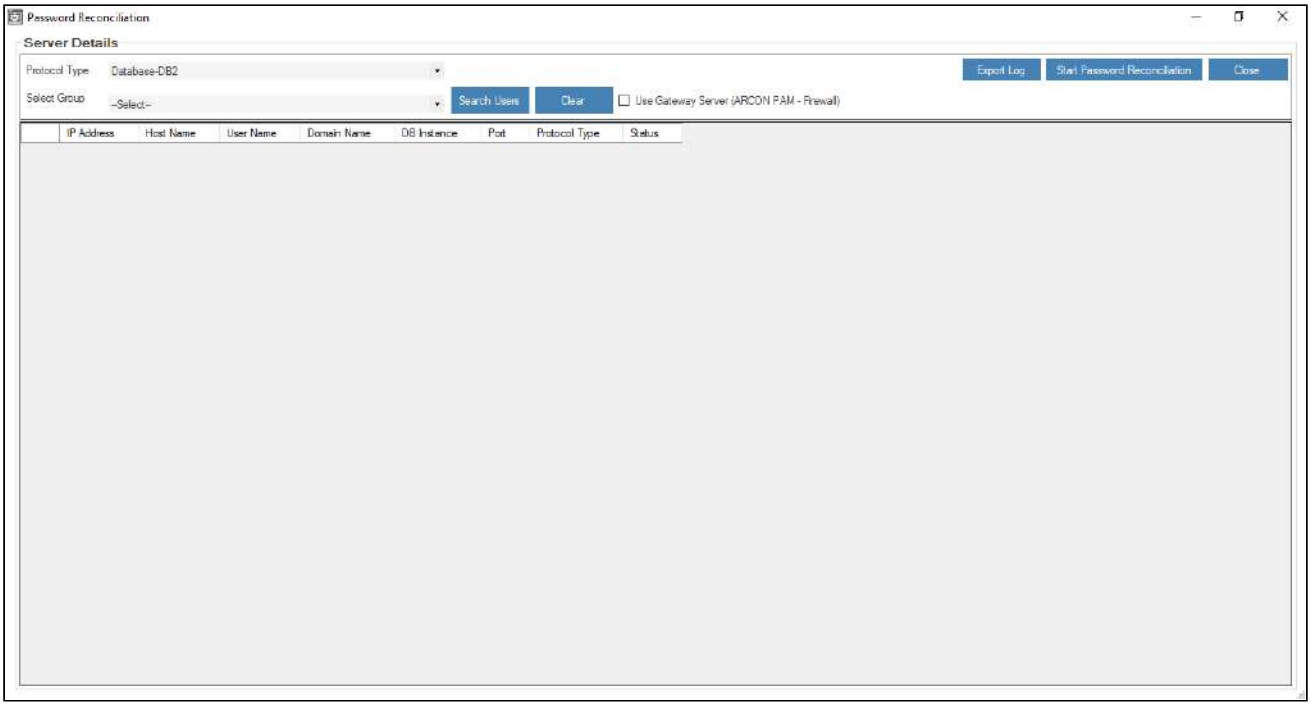
The reconciliation process compares the entries in ARCON PAM repository and the target system repository, determining the difference between the two repositories. When you run reconciliation for the first time on a target

system, all users and accounts on the target system are reconciled into ARCON PAM. This is called full reconciliation. To perform full reconciliation, the connector sends the reconciliation events for each entity in the target system. At the end of full reconciliation, the connector typically sets the last execution time parameter to the time when the reconciliation run ends. For the next reconciliation run, only the entity records that have been added, modified, or deleted after the first reconciliation run ended are fetched for reconciliation.

⚠ The Administrator having **Password Reconciliation** privilege in **Server's Privileges** will only be able to compare entries in ARCON PAM repository and the target system.

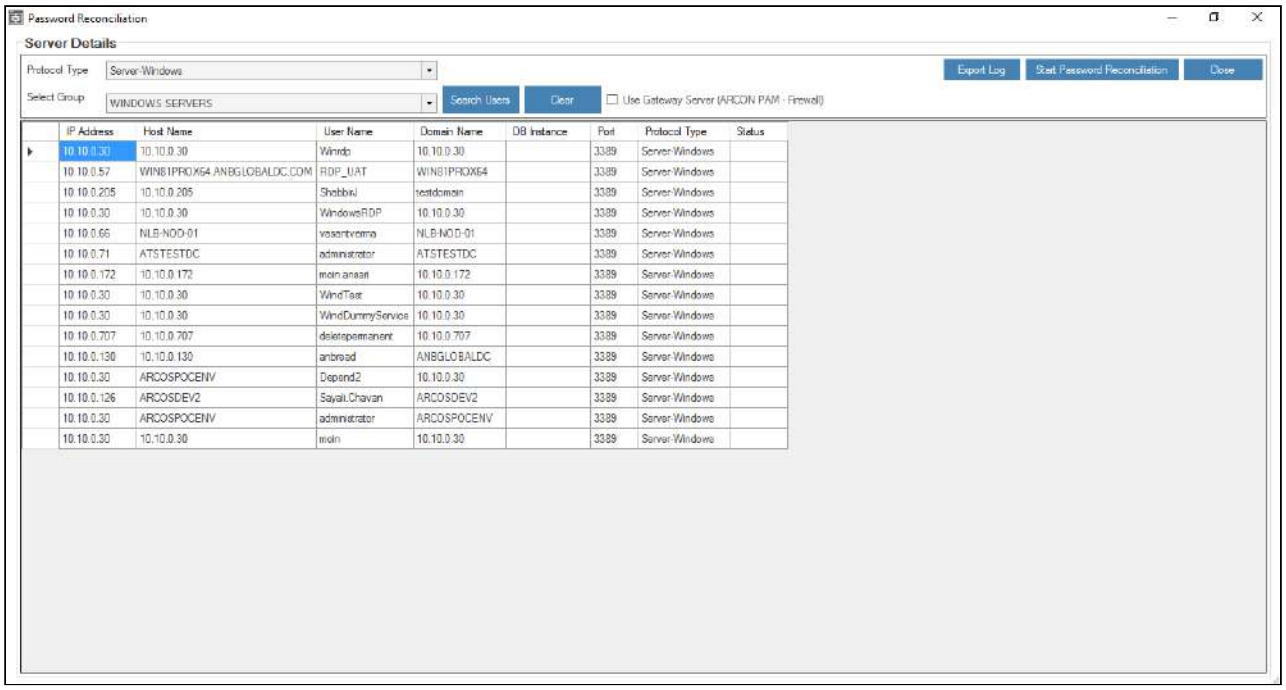
To navigate to password reconciliation, use the following path:

Tools → Password Reconciliation



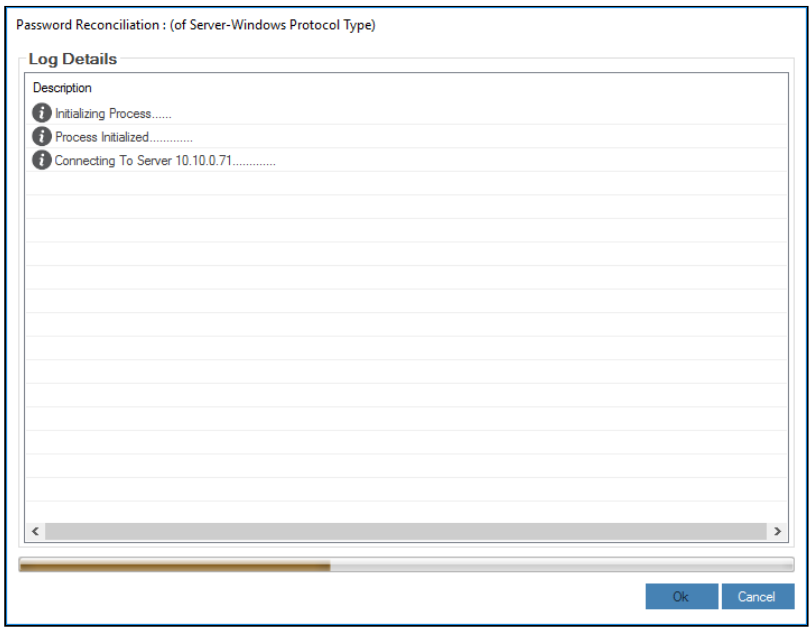
1. Select the protocol type from the **Protocol Type** dropdown list.
   The following protocol types are displayed in the dropdown list:
   - Database-DB2
   - Database-MSSQL
   - Database-Oracle
   - Desktop-Windows
   - Network-Telnet
   - Server-Unix-SSH
   - Server-Windows
   - SSH-Telnet
   - Server-UNIX-SSH Keys

2. Select the service group from **Select Group** dropdown list and click on **Search Users** button. The server details are displayed in the grid.



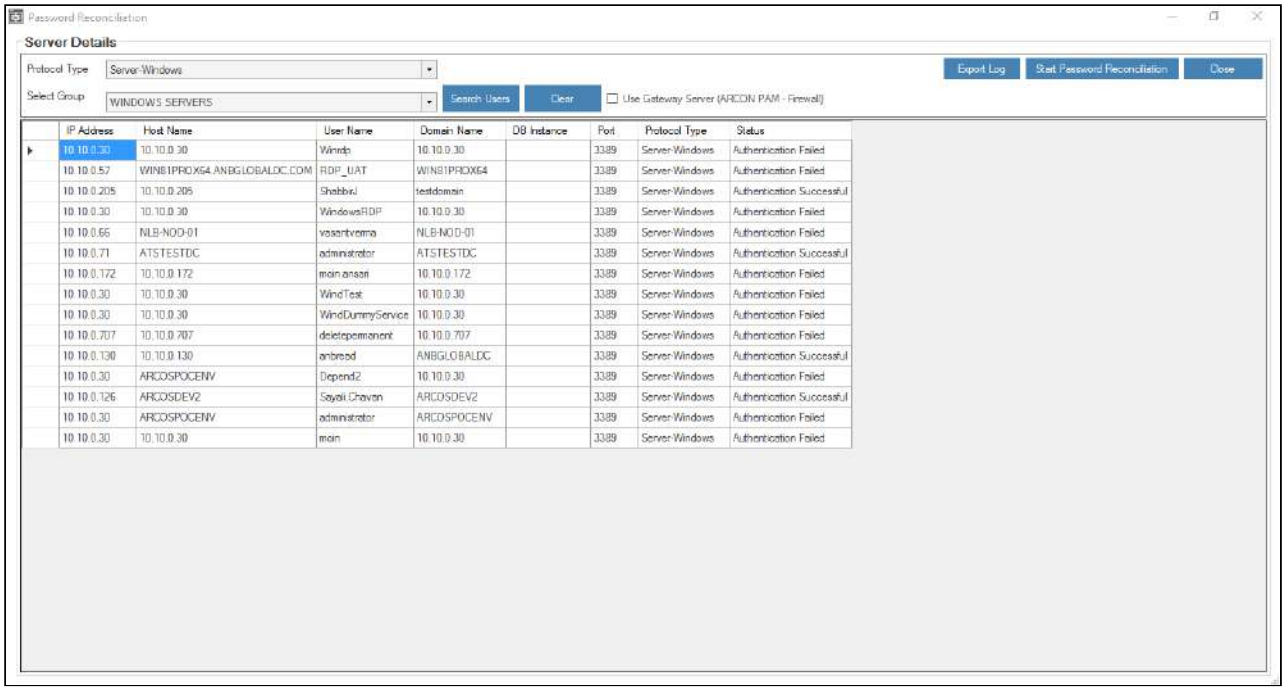
> ⚠ You can perform reconciliation process via gateway by selecting **Use Gateway Server (ARCON PAM - Firewall)** checkbox.

3. Click **Start Password Reconciliation** button once all services are displayed. The **Password Reconciliation: (Protocol Type Name)** screen is displayed once reconciliation is initiated.



> ⚠ If you do not want to reconcile all services, select the service which you want to delete and click **Delete** button on the keyboard or right click on service and select **Remove From List** option. Similarly, user can reconcile for a single service by right clicking on it and select **Start Password Reconciliation** option.

4. Click **Ok**. The status field is updated in the grid.



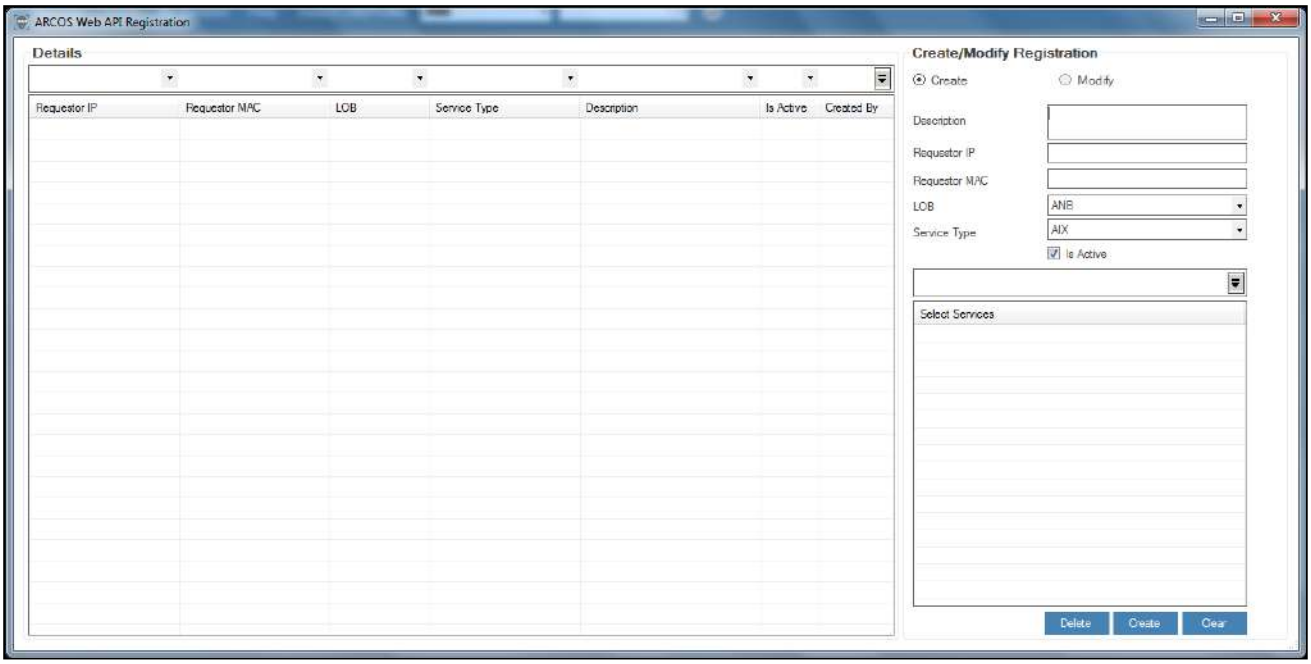
> ⚠
> - If status is displayed as **Authentication Successful**, then it means that the username and password for the particular service is correct.
> - If status is displayed as **Authentication Unsuccessful** or **A connection attempt failed**, then it means the connectivity to the destination server is not possible or has some issue reaching the server.
> - **Export Log** button saves or downloads the generated logs in .csv format.
> - As of now, direct port access/connectivity is required for this feature. For example, source system 3389 would be required for using this feature.
> - Port 445 should be open for Local Windows server.

7.13 Web API Registration

Web API Registration helps you to register the user's machine IP address, where the user can view the password from the registered machine or laptop.

To navigate to ARCOS Web API Registration, use the following path:

Tools → Advanced Configuration → ARCOS Web API Registration

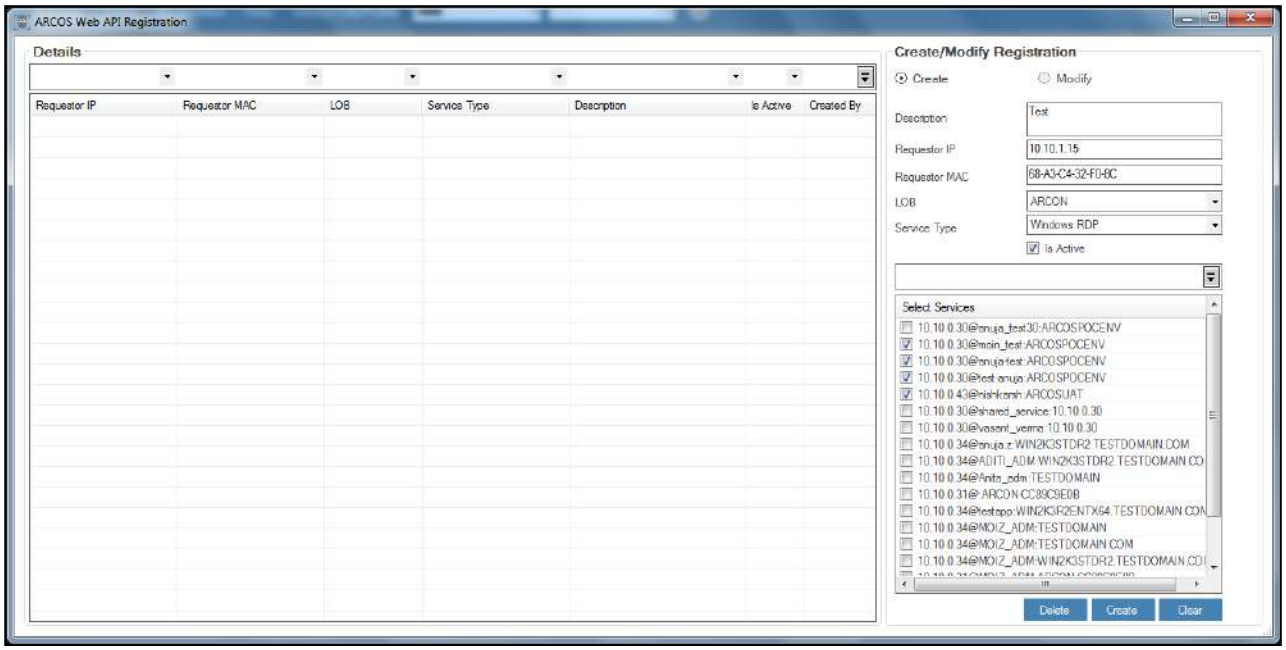


The **ARCOS Web API Registration** screen contains the following fields:

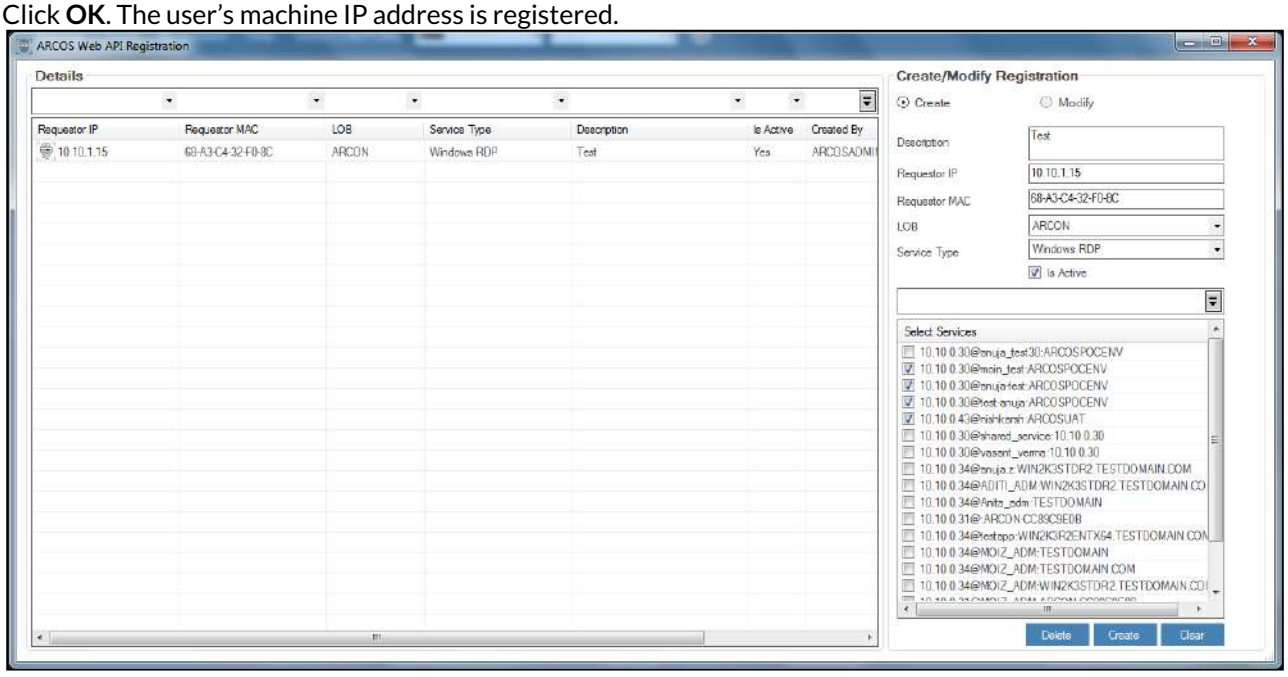
Field Name	Description
Description	Specify description for registration.
Requestor IP	Specify IP address of the requestor.
Requestor MAC	Specify MAC address of the requestor.
LOB	Select LOB.
Service Type	Select type of service.
Is Active	Enable the configuration.

1. Enter/ Select the details.

> ⚠ The list of services are displayed in the **Select Services** grid, once you select the service type from the **Service Type** dropdown list.



2. Select the services from the list of services and click on **Create** button. A window pops up with the following message:
   New Web API Registration Created.
3. Click **OK**. The user's machine IP address is registered.



⚠

- If the toggle value of **ARCOSAPI(Password Retrieval)RequestorValidator – Is Enabled** in **Settings** is **Enabled**, then the user can view the password of the service from any machine.
- If the toggle value of **ARCOSAPI(Password Retrieval)RequestorValidator – Is Enabled** in **Settings** is **Disbaled**, then the user can view the password of the service from only the registered machine.

- For API Restriction to work the Settings **ARCOSAPI(Password Retrieval)RequestorValidator** should be Disabled. It works only if both the Requestor Machine and API Server is in the same Vlan/Subnet.
- On enabling this settings it will restrict all API Access and will allow only those API Requests for which IP address and MAC address is registered in API registration.

7.14 Network Connectivity to Target Systems

7.14.1 Overview

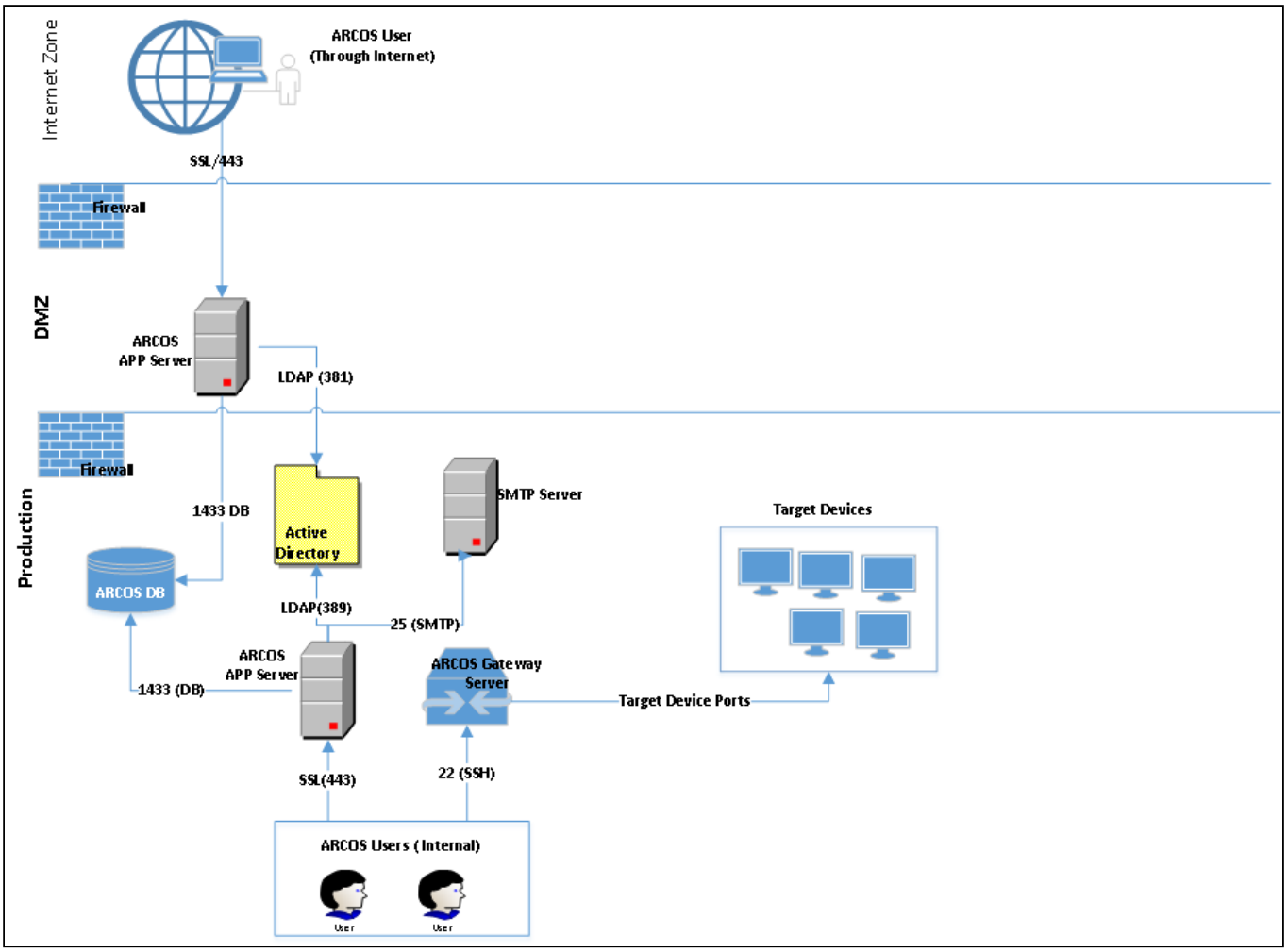
There are multiple scenarios that have to be handled when the network connectivity to the target systems becomes a great concern. These network connectivity scenarios arise at multiple occasions in terms of infrastructural, logistics and operational challenges faced in the everyday functioning of an organization. Despite these challenges, ARCON PAM enables you to manage your critical credentials with the help of a highly secured and steadfast vaulting and password management mechanism. Major scenarios that our client's face are as follows. To handle the respective challenging scenarios gracefully, ARCON PAM ensures the following mechanisms to handle each one.

7.14.2 Demilitarized Zone (DMZ)

A DMZ or Demilitarized Zone is a secure server that adds an additional layer of security to a network and acts as a buffer between a local area network (LAN) and a less secure network which is the Internet. In computer security, a DMZ is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the Internet. Therefore, as a DMZ segment a network, security controls can be tuned specifically for each segment. This document includes a brief description of LDAP authentication is done via DMZ, data flow for DMZ to APP and DB server and Approval Workflow.

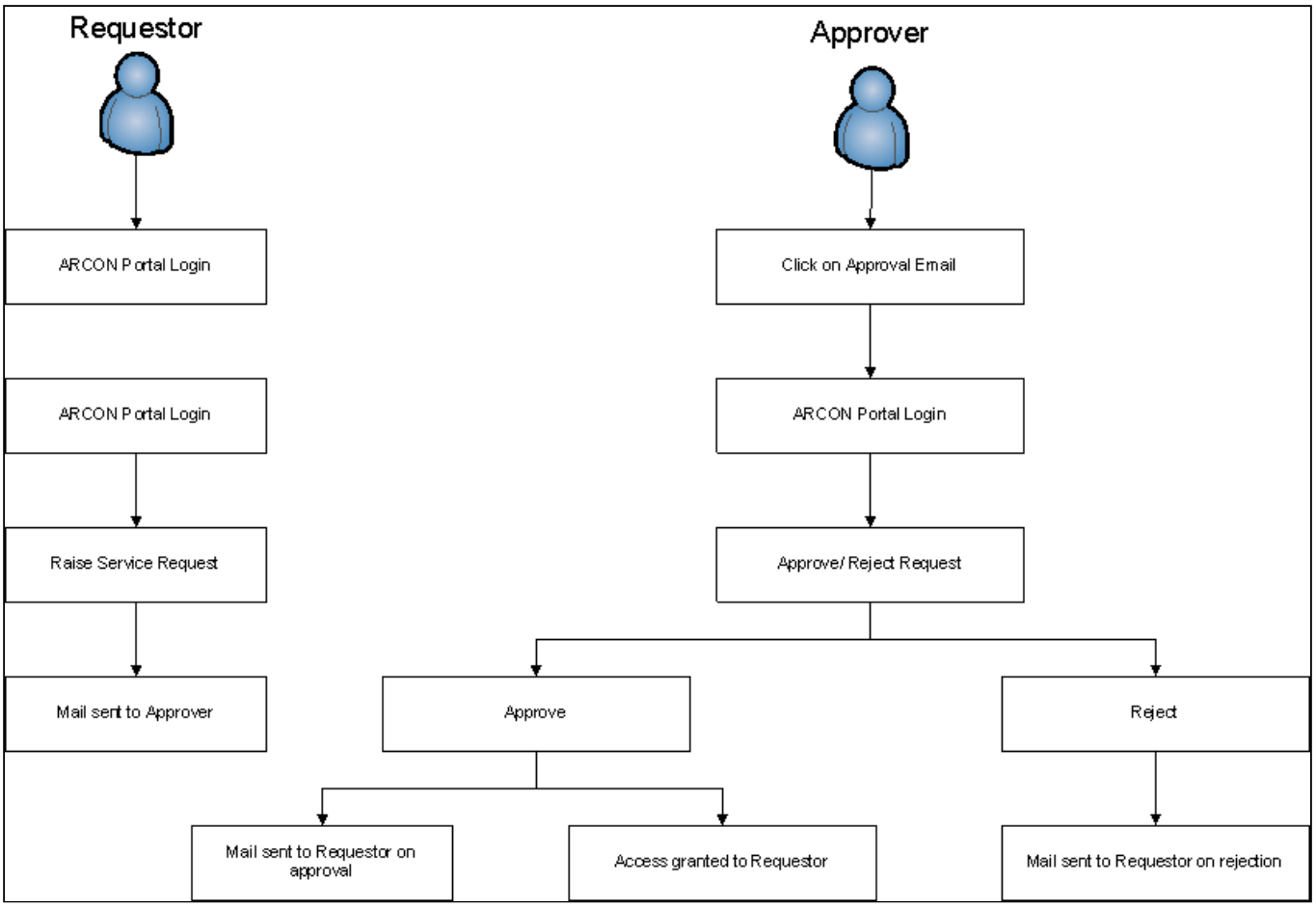
7.14.2.1 LDAP Authentication via DMZ

All the ARCON PAM Components (App, DB, and Gateway) would be initially hosted within the data center in the production zone. To facilitate authentication via AD, ARCON PAM should be internally integrated with the AD Domain. This allows ARCON PAM to authenticate users against AD and then allow access on ARCON PAM. In a similar way, ARCON PAM APP Server in the DMZ would authenticate the user against AD and this happens using the AD Integration already configured in ARCON PAM for which the settings are stored in ARCON DB. Appropriate port opening as depicted below should be allowed for.



7.14.3 Approval Workflow

If an ARCON PAM user needs access to an unassigned server; the user will have to log in to ARCON PAM and raise a service request, the user will have to select the service (server), mention the duration for which the access is required and raise request. On every request raised, ARCON PAM will send out an email to the approver(s) for their approval as ARCON PAM is integrated with the mail server of the user. Approver will have to click on the link in the email and it would open the ARCOS Portal on which the approver has to login using the AD Credentials. AD authentication happens as explained above. Once logged in the Approver can Approve/Reject the request and a response email is sent to the requestor confirming the approval/rejection of the request.



7.14.4 Clustering of Services

If an organization has multiple clustering of services and cluster nodes in a single network. There is a cluster node manager in an organization that manages all the cluster nodes together. The password change and post password change, in this case, has been handled by communicating with the Microsoft Windows inbuilt clustering service facility. The cases of password propagation during fail-over cluster is handled by communicating with the Windows APIs. For more information on the same, please refer to "Configure Post Password Actions".

Clustering is only available on certain Windows Operating Systems:

1. Microsoft Windows server v2012
2. Microsoft Windows server v2014
3. Microsoft Windows server v2016

Following parameter to be modified in the config.ini file:

```
IsServiceOutSideCluster=Yes
```

7.14.5 Disconnected Infrastructure

When an organization has a disconnected architecture and infrastructure needs, this type of solution is suggested to them. Disconnected infrastructure is nothing but a combination of disconnected endpoints and client-server architecture. The servers could be hosted on-premise or on the cloud. For managing password change here, ARCON LocalVault service is utilized here. For more information, please refer to the Password Management document.

7.14.6 LOB-wise Vault Processors - Segmented Networks

When a multinational organization wants to secure it's various geographically divided zones all across the globe, it becomes necessary to centrally manage the zonal instances of ARCON PAM central Vault for password management. ARCON handles this scenario efficiently by managing Line Of Business (LOBs) in ARCON PAM.

This LOB-wise distribution is possible using independent Secured Gateway Server (SGW) or ARCON PAM ARCON Terminal Server(ATS). ARCON PAM Vault uses a Gateway Server (SGW) or ARCON PAM ARCON Terminal Server(ATS) that can be placed in different locations of the Target Devices if there is no direct connectivity i.e. only the Vault and SGW hosts, ports are trusted.

While the Gateway Server/ARCON Terminal Server ports can be open to the end devices within the segmented network. ARCON PAM also provides a Vault Processor (LOB-wise) which means we could install 'N' number of Vault Processors on various devices and these processors could be used to multiplex as well as connect to only their local networks. The only connectivity should be between the PAM Vault and the Vault Processors. These vault processors act like a normal vault and can provide all features that are provided by the vault, for example, the complex ones like propagating passwords in scripts, executables, API calls, etc.

Following parameter to be modified in the config.ini file:

```
DefaultLOBs= <Required_LOB_ID>
```

8 Workflow Management

ARCON PAM supports Workflow Tracker feature, wherein it tracks details of a workflow. It also tracks the service access request, service password request, and ticket request raised by users. Therefore, tracking helps to monitor and maintain the details of the workflow.

8.1 Workflow Logs

Workflow Tracker displays logs generated for transactions such as User creation, service creation, service access, ticket and service password request raised by User. In addition, it displays workflow approval details for the requests raised.

> ⚠ The Administrator having **ARCON PAM Workflow Tracker** privilege under **Server's Privileges** shall only be able to view workflow approval matrix logs, user service request workflow logs, ticket request workflow logs and service password request workflow logs.

Following are the list of logs generated in Workflow Tracker:

- ARCOS Workflow Tracker
- User Service Request Workflow Tracker
- Ticket Request Workflow Tracker
- Service Password Request Workflow Tracker

> ⚠ If the value for **LOB Wise Workflow Tracker – Is Enabled** in **Settings** is set to:
>
> - **Disabled:** The Service Access Request, Ticket Request and Service Password Request logs are filtered based on the selected LOB from the **LOB/Profile** dropdown list.
> - **Enabled:** The Service Access Request, Ticket Request and Service Password Request logs are filtered for all the LOBs. By default, the value is set to **All** in **LOB/Profile** dropdown list.

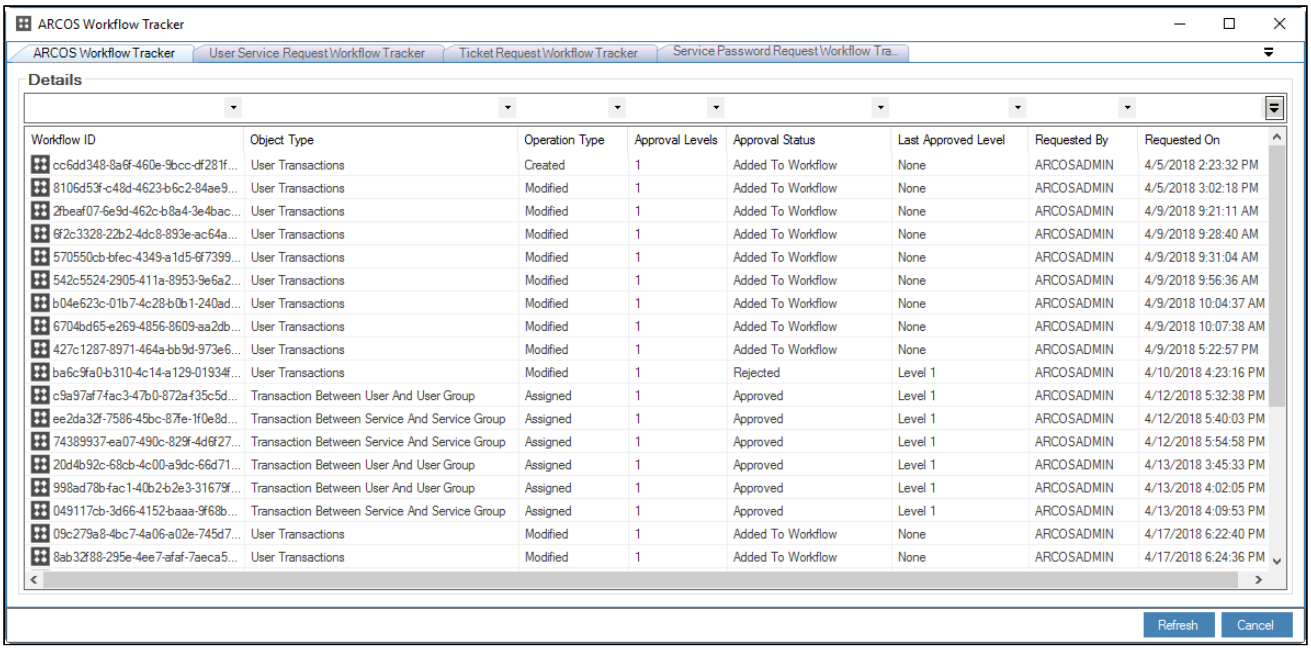
8.1.1 View Workflow Approval Matrix Logs

ARCOS Workflow Tracker displays workflow approval matrix details for transactions such as User creation, service creation. It displays details such as the workflow ID, type of object, type of operation, levels of approval, and status of approval, last approved level, name of the user who has initiated the request, and date & time on which the request was initiated.

To view logs of workflow:

To view logs of workflow use the following path:

Manage → ARCOS Workflow Tracker



Workflow ID	Object Type	Operation Type	Approval Levels	Approval Status	Last Approved Level	Requested By	Requested On
cc6dd348-8a6f-460e-9bcc-df281f...	User Transactions	Created	1	Added To Workflow	None	ARCOSADMIN	4/5/2018 2:23:32 PM
8106d53f-c48d-4623-b6c2-84ae9...	User Transactions	Modified	1	Added To Workflow	None	ARCOSADMIN	4/5/2018 3:02:18 PM
2fbeaf07-6e9d-462c-b8a4-3e4bac...	User Transactions	Modified	1	Added To Workflow	None	ARCOSADMIN	4/9/2018 9:21:11 AM
6f2c3328-22b2-4dc8-893e-ac64a...	User Transactions	Modified	1	Added To Workflow	None	ARCOSADMIN	4/9/2018 9:28:40 AM
570550cb-bfec-4349-a1d5-6f7399...	User Transactions	Modified	1	Added To Workflow	None	ARCOSADMIN	4/9/2018 9:31:04 AM
542c5524-2905-411a-8953-9e6a2...	User Transactions	Modified	1	Added To Workflow	None	ARCOSADMIN	4/9/2018 9:56:36 AM
b04e623c-01b7-4c28-b0b1-240ad...	User Transactions	Modified	1	Added To Workflow	None	ARCOSADMIN	4/9/2018 10:04:37 AM
6704bd65-e269-4856-8609-aa2db...	User Transactions	Modified	1	Added To Workflow	None	ARCOSADMIN	4/9/2018 10:07:38 AM
427c1287-8971-464a-bb9d-973e6...	User Transactions	Modified	1	Added To Workflow	None	ARCOSADMIN	4/9/2018 5:22:57 PM
ba6c9fa0-b310-4c14-a129-01934f...	User Transactions	Modified	1	Rejected	Level 1	ARCOSADMIN	4/10/2018 4:23:16 PM
c9a97af7-fac3-47b0-872a-f35c5d...	Transaction Between User And User Group	Assigned	1	Approved	Level 1	ARCOSADMIN	4/12/2018 5:32:38 PM
ee2da32f-7586-45bc-87fe-1f0e8d...	Transaction Between Service And Service Group	Assigned	1	Approved	Level 1	ARCOSADMIN	4/12/2018 5:40:03 PM
74389937-ea07-490c-829f-4d6f27...	Transaction Between Service And Service Group	Assigned	1	Approved	Level 1	ARCOSADMIN	4/12/2018 5:54:58 PM
20d4b92c-68cb-4c00-a9dc-66d71...	Transaction Between User And User Group	Assigned	1	Approved	Level 1	ARCOSADMIN	4/13/2018 3:45:33 PM
998ad78b-fac1-40b2-b2e3-31679f...	Transaction Between User And User Group	Assigned	1	Approved	Level 1	ARCOSADMIN	4/13/2018 4:02:05 PM
049117cb-3d66-4152-baaa-9f68b...	Transaction Between Service And Service Group	Assigned	1	Approved	Level 1	ARCOSADMIN	4/13/2018 4:09:53 PM
09c279a8-4bc7-4a06-a02e-745d7...	User Transactions	Modified	1	Added To Workflow	None	ARCOSADMIN	4/17/2018 6:22:40 PM
8ab32f88-295e-4ee7-afaf-7aeca5...	User Transactions	Modified	1	Added To Workflow	None	ARCOSADMIN	4/17/2018 6:24:36 PM

1. View the logs generated in **ARCOS Workflow Tracker**.

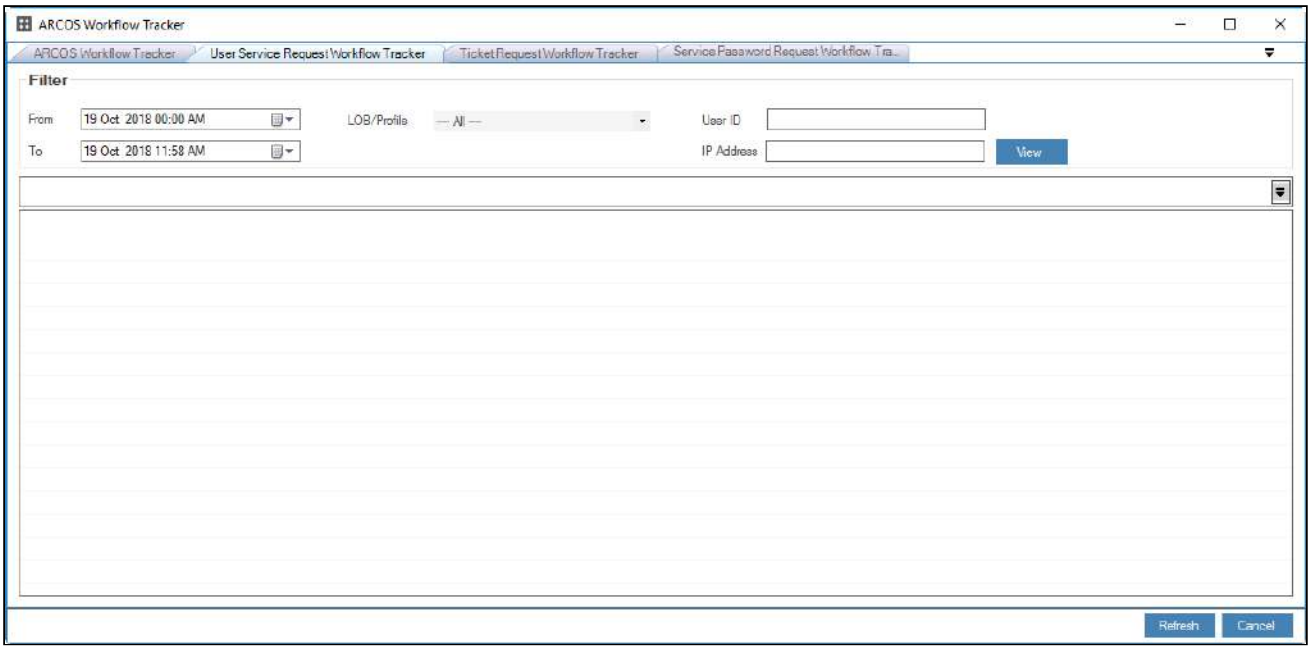
8.1.2 View User Service Request Workflow Logs

This section helps you to view details of the user service requests raised by Users. You can filter the logs based on the selected LOB, User ID and IP address. It displays details such as the name of the LOB, name of the User who has raised the request, date & time on which the request was raised, description of the request, requested type of access, type of service, service IP address, domain name, username of service and date & time on which the access was requested.

To view logs of user service request workflow:

To view logs of user service request workflow use the following path:

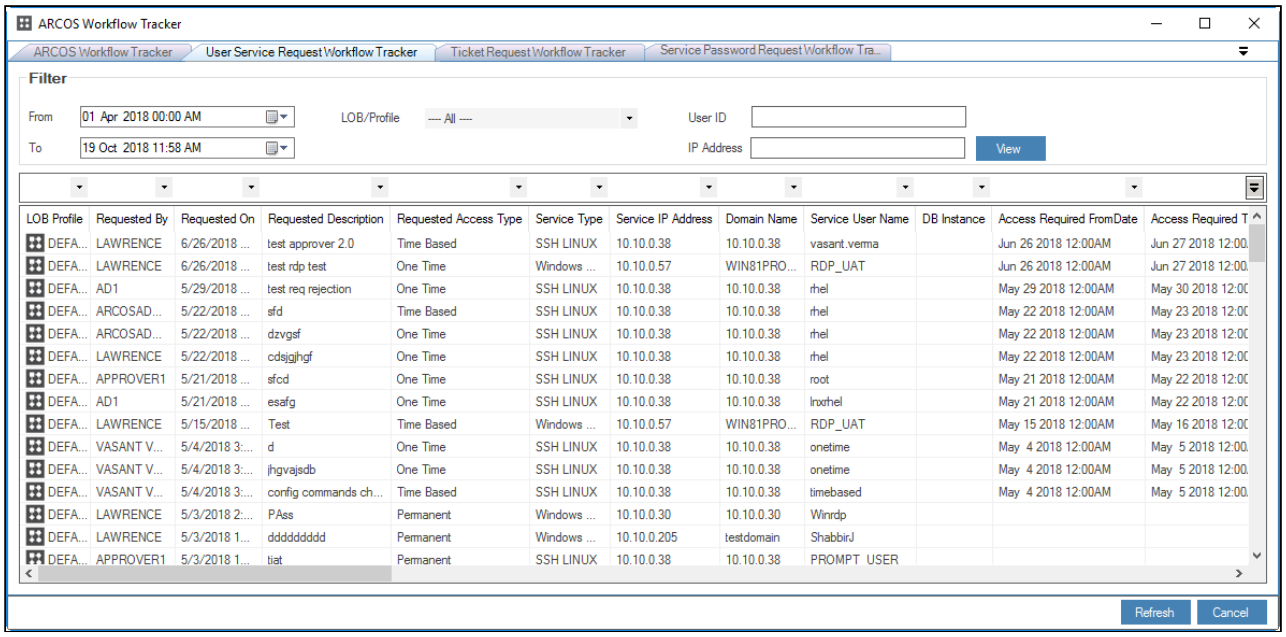
Manage → ARCOS Workflow Tracker → User Service Request Workflow Tracker



The **User Service Request Workflow Tracker** screen contains the following fields:

Field Name	Description
From	Select the start date to filter logs.
To	Select the end date to filter logs.
LOB/ Profile	Select the LOB.
User ID	Specify the User ID, to filter the logs based on the particular User ID.
IP Address	Specify the IP address.

1. Select/ Enter the fields and click **View**. The details of the user service requests raised by users are displayed in the grid.



2. View the user service request workflow details.

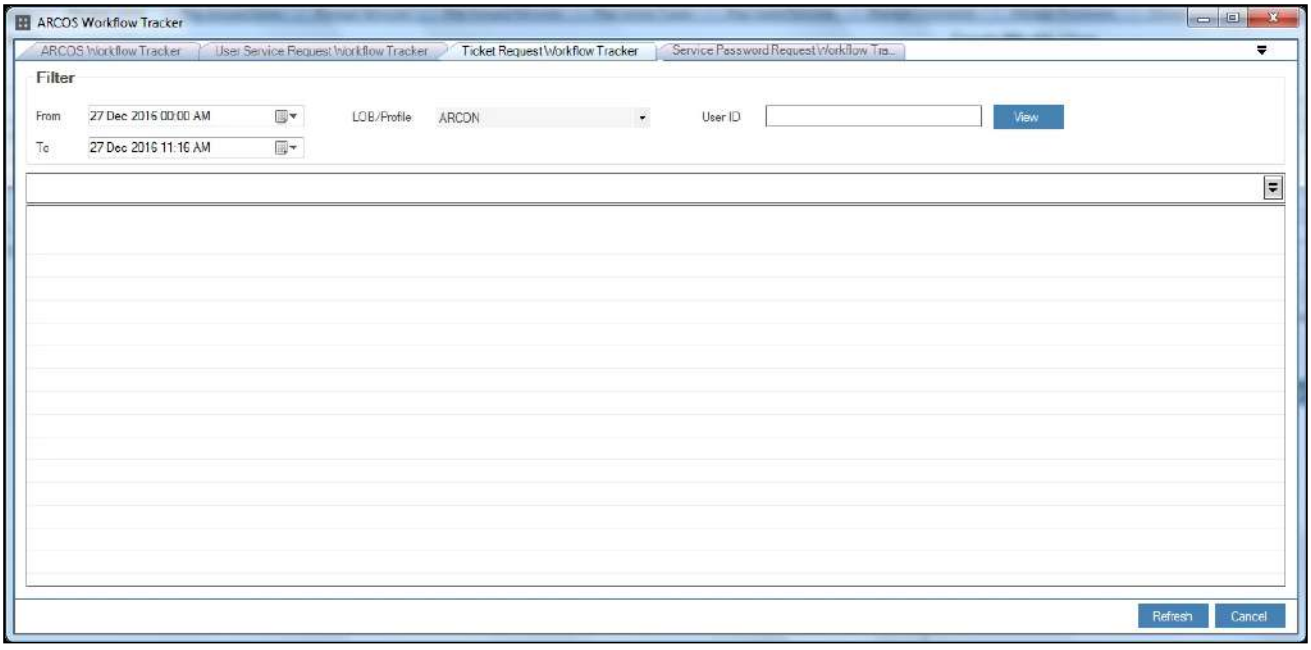
8.1.3 View Ticket Request Workflow Logs

This section helps you to view the details of ticket request raised by Users. You can filter the logs based on the selected LOB and User ID. It displays details such as the name of the LOB, ticket ID, ticket number, type of ticket, type of activity, server group, domain name of server, and port number of server.

To view logs of ticket request workflow:

To view logs of ticket request workflow use the following path:

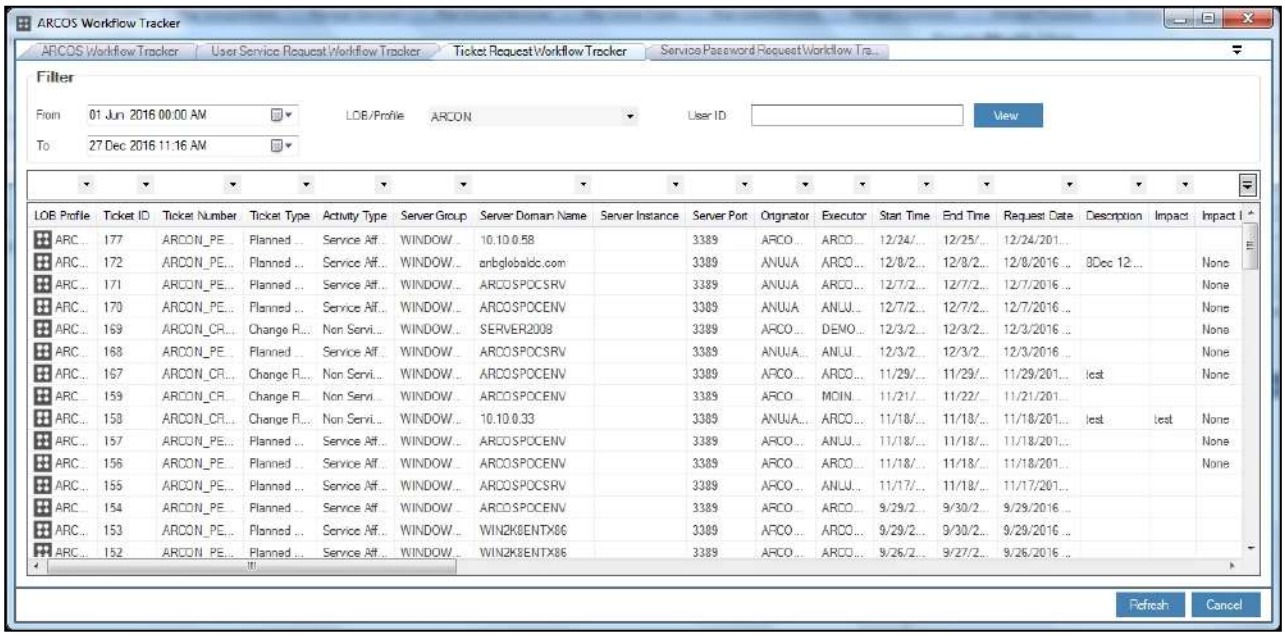
Manage → ARCOS Workflow Tracker → Ticket Request Workflow Tracker



The **Ticket Request Workflow Tracker** screen contains the following fields:

Field Name	Description
From	Select the start date to filter logs.
To	Select the end date to filter logs.
LOB/ Profile	Select the LOB.
User ID	Specify the User ID, to filter the logs based on the particular user ID.

1. Select/ Enter the fields and click **View**. The details of ticket request raised by Users are displayed in the grid.



2. View the ticket request workflow details.

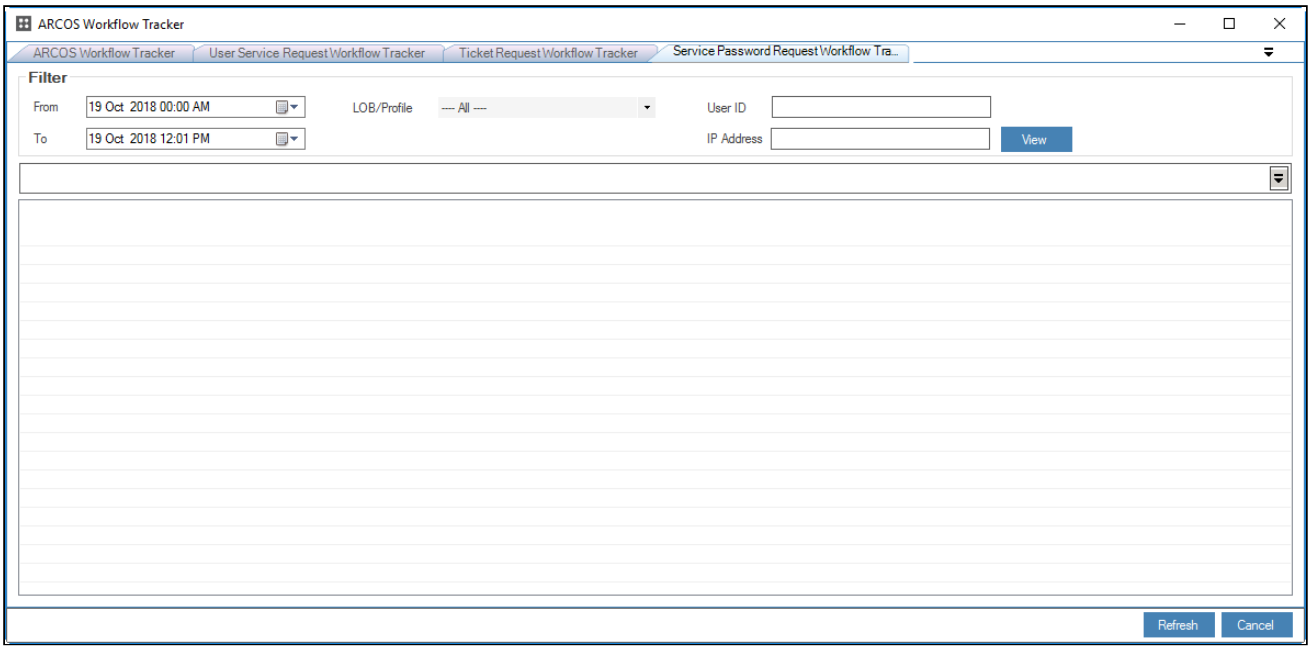
8.1.4 View Service Password Request Workflow Logs

This section helps you to view details of the service password requests raised by Users. You can filter the logs based on the selected LOB, User ID and IP address. It displays details such as the name of the LOB, name of the User who has raised the request, date & time on which the request was raised, description of the request, type of service, service IP address, domain name, username of service, DB instance, date and time when password will be sent to User's mailbox, number of hours password will be open, date and time till when password will be open, current approval level, number of configured approval levels, the configured approver's username, approval status, status updated date and time, and the final approval status.

To view logs of service password request workflow:

To view logs of service password request workflow use the following path:

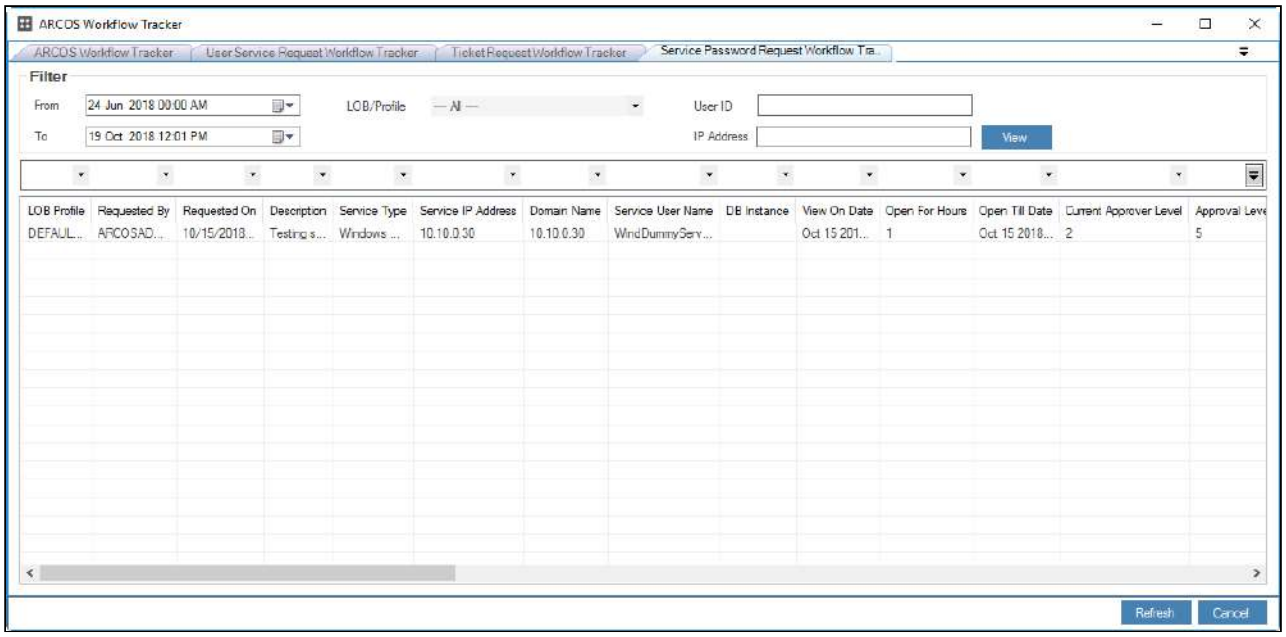
Manage → ARCOS Workflow Tracker → Service Password Request Workflow Tracker



The **Service Password Request Workflow Tracker** screen contains the following fields:

Field Name	Description
From	Select the start date to filter logs.
To	Select the end date to filter logs.
LOB/ Profile	Select the LOB.
User ID	Specify the User ID, to filter the logs based on the particular User ID.
IP Address	Specify the IP address.

1. Select/ Enter the fields and click **View**. The details of the service password requests raised by Users are displayed in the grid.



2. View the service password request workflow details.

9 Log Management

Logs capture all the activities performed in ARCON PAM with detailed information. It provides audit trial for transactions performed in Server Manager. It also provides detailed information of services accessed through ARCON PAM. The Administrator can view them using **View Logs** option.

⚠ The Administrator, who is assigned privileges listed in **Log Viewer** in **Server's Privileges**, can view logs.

This section includes the following topics:

- Process Logs
- Command Logs
- ARCON PAM Logs
- User Access Logs
- Service Logs
- User Validity Status
- Service Password Status
- Service Reference Logs
- User Activity Logs
- Envelope Logs
- Import Service Logs
- Service Password Request Logs
- Application Logs

9.1 Process Logs

Process Logs helps you to view details of the processes executed on Windows Server when a service is accessed through ARCON PAM. The processes executed on Windows Server are only viewed in Process Logs. It displays details such as ID of the user who has logged in application, machine's IP [MAC address], type of service, service description, log type, timestamp, name of the process, and process title executed on server. The generated logs can be exported to .xls format.

⚠
- The Administrator having **View Process Log** privilege in Server's Privileges will only be able to view Process logs. In addition, the Administrator should have **Download Video Log** privilege, to download video logs.
- The Server Group Admin having **View Command Log** privilege in Group Admin Privileges, will only be able to view Process Logs.

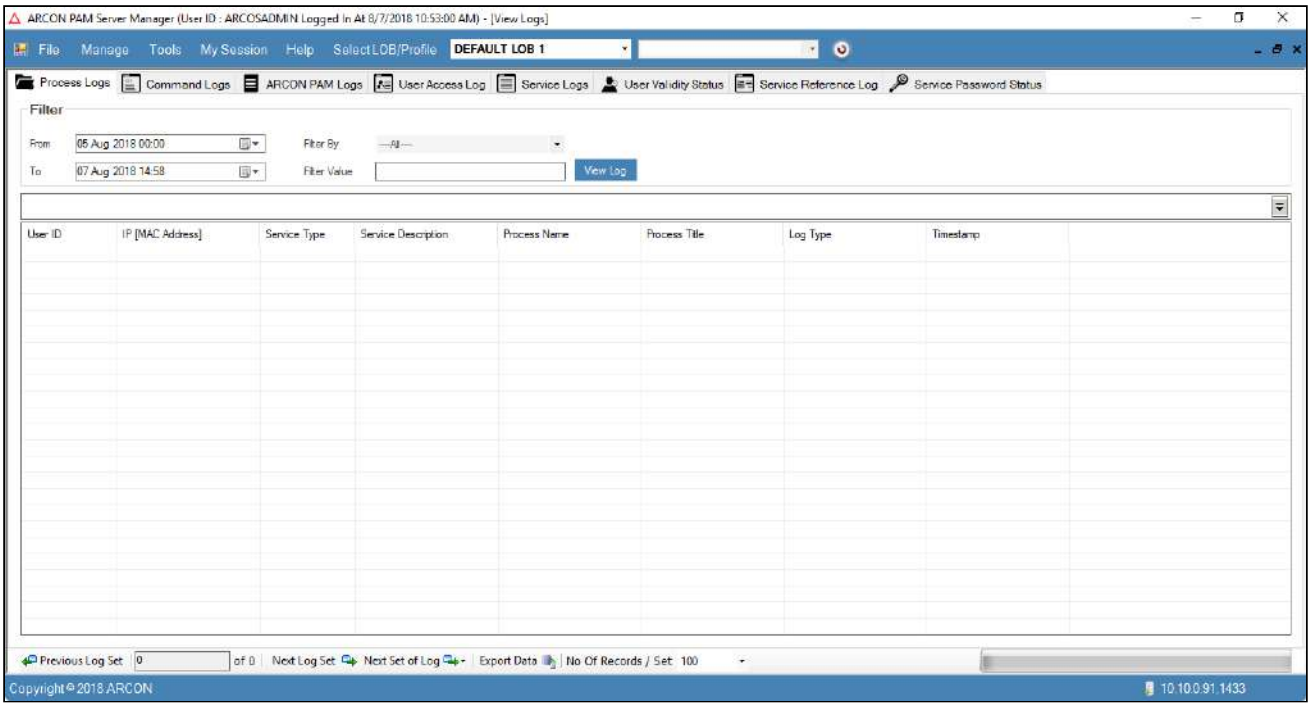
If type of the log is displayed as:

- Activated: Session is active.
- Inactivated: Session is closed.
- Minimized: Session is minimized by user.
- Maximized: Session is maximized by user.

To generate process logs:

To generate process logs use the following path:

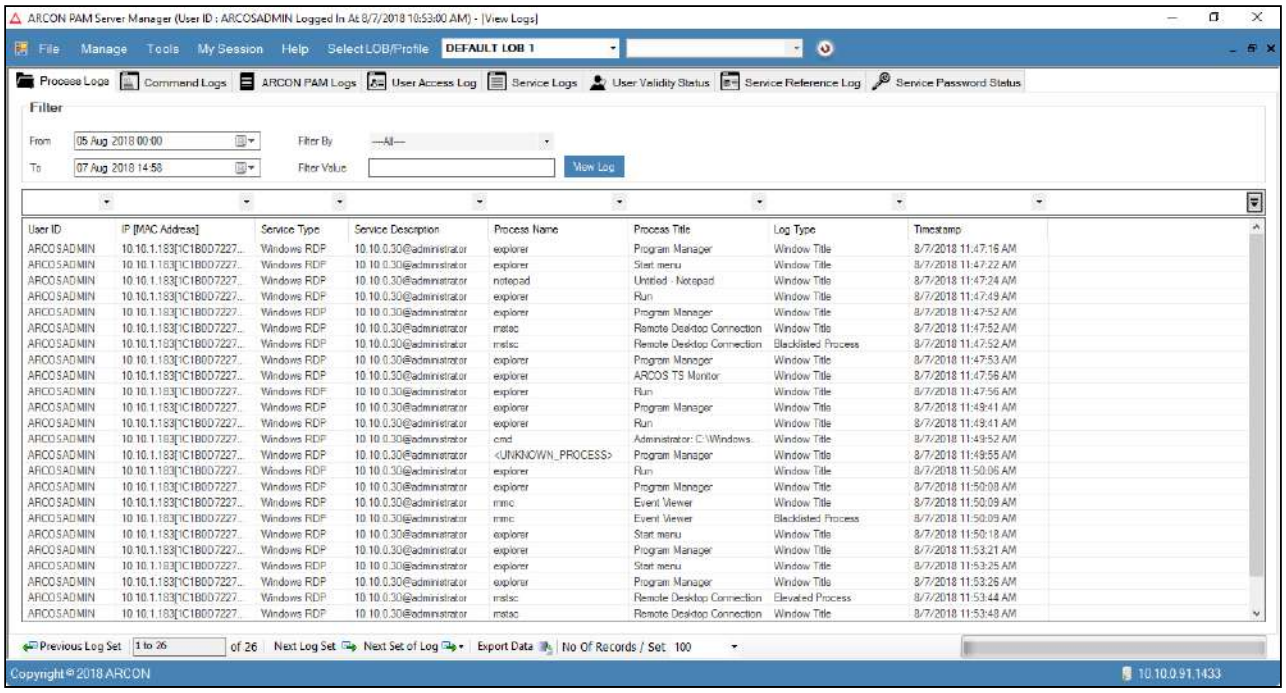
Manage → Logs → Process Logs



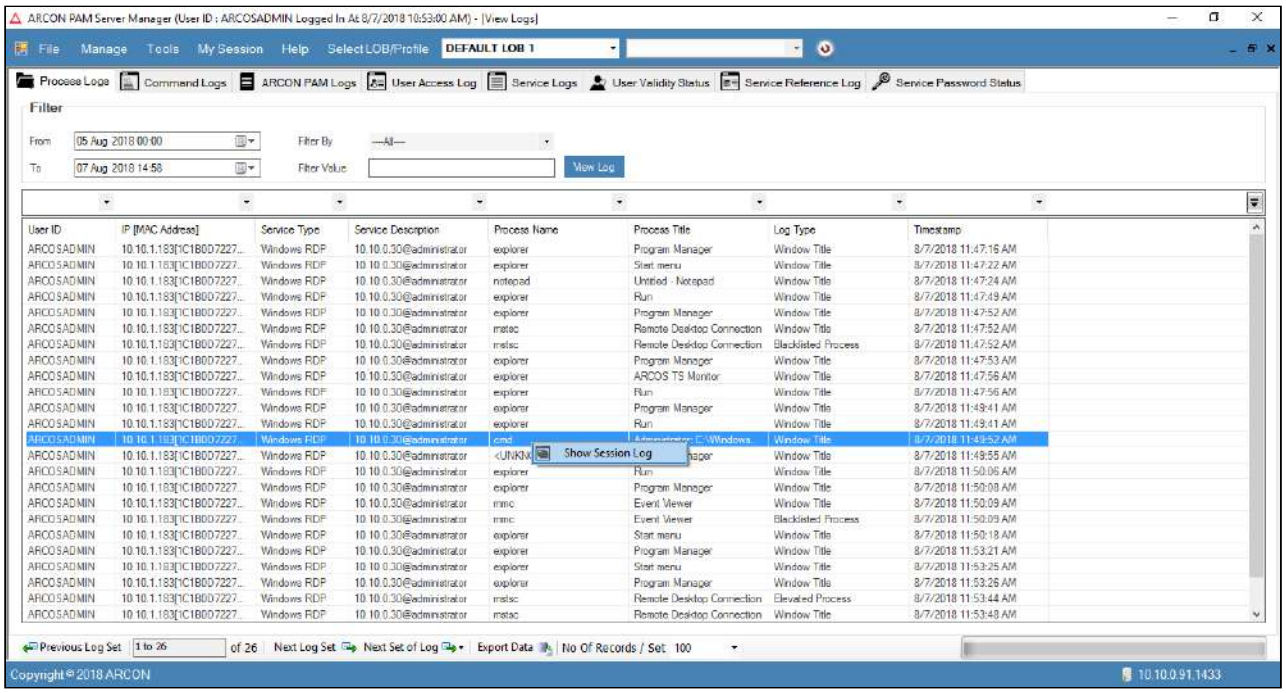
The **Filter** screen contains the following fields:

Field Name	Description
From	Select the start date, to generate logs.
To	Select the end date, till when you want to generate logs.
Filter By	Select the type of filter. The valid values are: • User Name • User IP (MAC) Address • Server IP Address • Process Name • Process Title
Filter Value	Specify the value, to filter the logs.

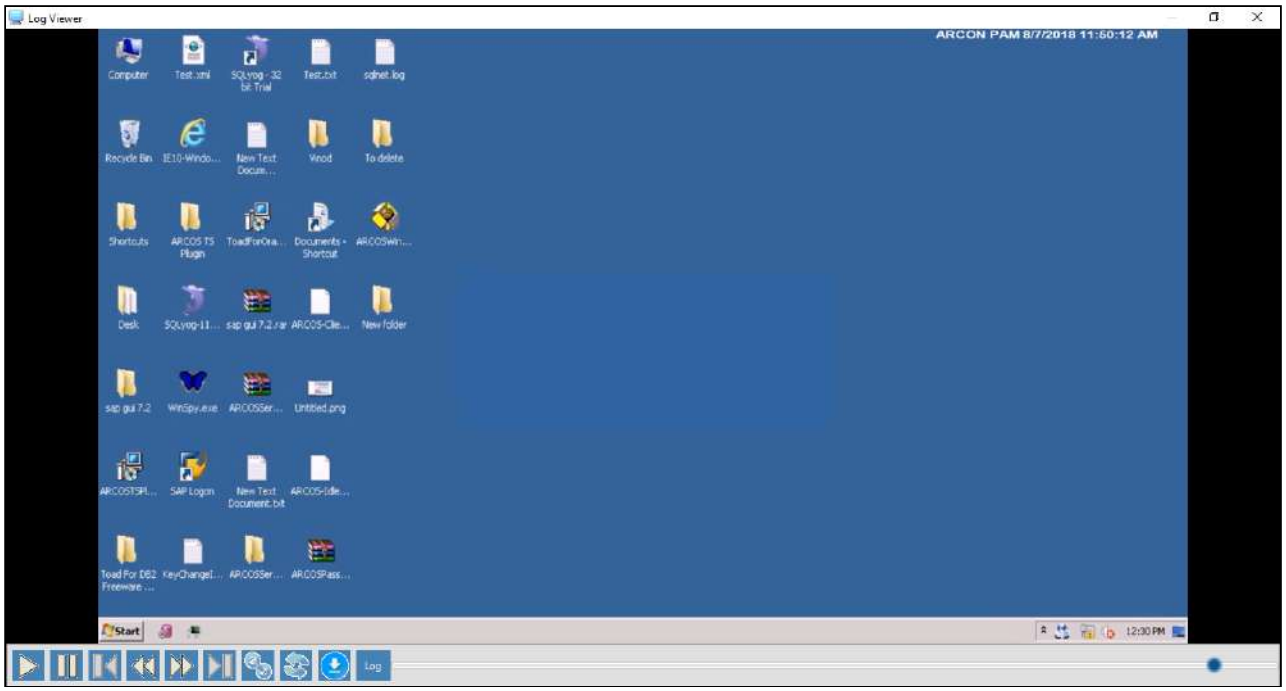
1. Select/Enter the fields and click on **View Log** button. The logs are generated based on the selected filters.



2. Right click on the windows service and choose **Show Session Log** option, to view video log.



3. Click **Show Session Log** option. The **Log Viewer** screen is displayed.



4. View the video log.

> ⚠
>
> - To export logs into .xls format, click on **Export Data** button, which is present in the bottom of the screen.
> - Click Previous Log Set, to view set of previous logs.
> - Click Next Log Set, to view next set of logs.
> - Click Next Set of Log, to view particular set of logs. Select the particular set from the **Next Set of Log** dropdown list.
> - Select the number of records from **No of Records/Set** dropdown list, wherein it will display those many records in the grid.

9.2 Command Logs

This section helps you to view the logs of the commands fired after connecting to the server. It displays details such as User ID of the User who has logged in ARCON PAM, User Display Name, User Machine's IP [MAC address], type of Service, Service Description, Session Log ID, Command fired, Command Response, Command Logged in and out timestamp. The generated logs can be exported to .xls format. For enhancing the security in the session management of the logs, we make sure that whenever critical commands like "passwd" are typed on the terminal it does not maintain the value of it in the logs. The password is consumed from the Vault for validating the session and is discarded once the session authentication is completed.

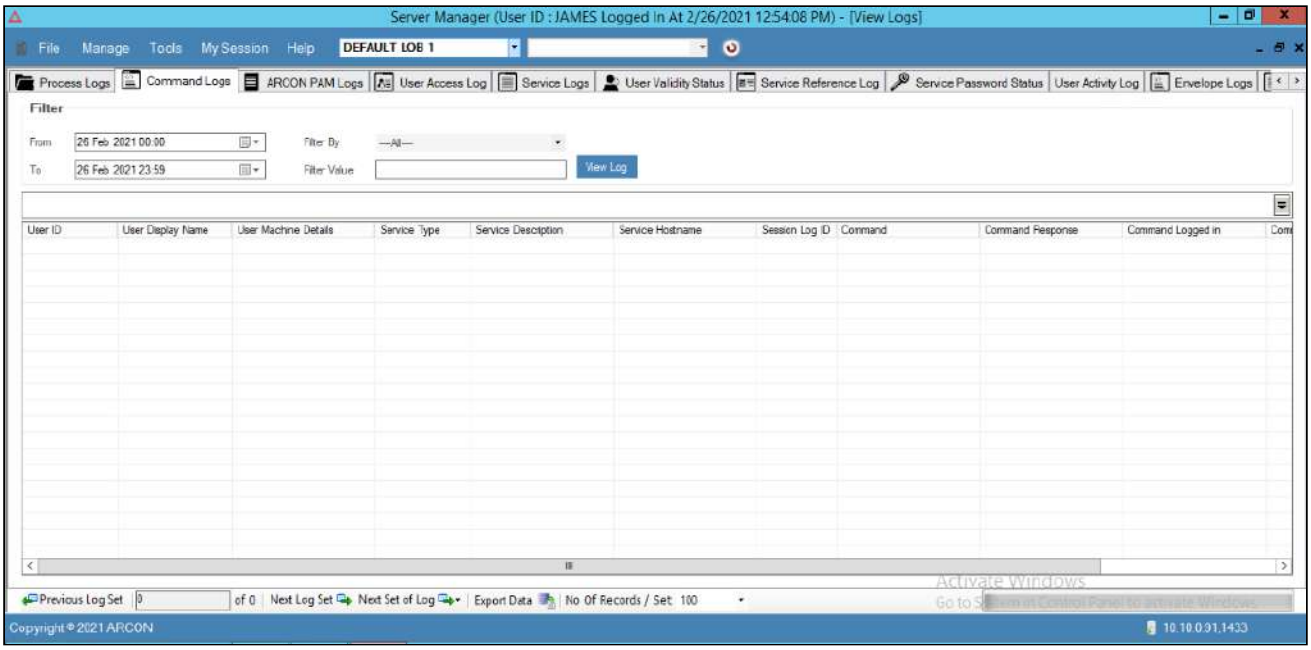
> ⚠
>
> - The Administrator having **View Command Log** privilege in Server's Privilege will only be able to view Command logs. In addition, the Administrator should have **Download Video Log** privilege, to download video logs.
> - The Server Group Admin having **View Command Log** privilege in Group Admin Privileges, will only be able to view Command Logs.

- To generate video logs for SSH services (Firewall, Switch, LINUX, Telnet etc.), configure the toggle value for **SSH Video Log - Is Enabled For All** as **Enabled** in **Settings**. The storage capacity shall be maximum on the Server, where logs are generated.
- Any inputs such as password, username, IP address, credit card number can be masked in logs.

To generate command logs:

To generate command logs use the following path:

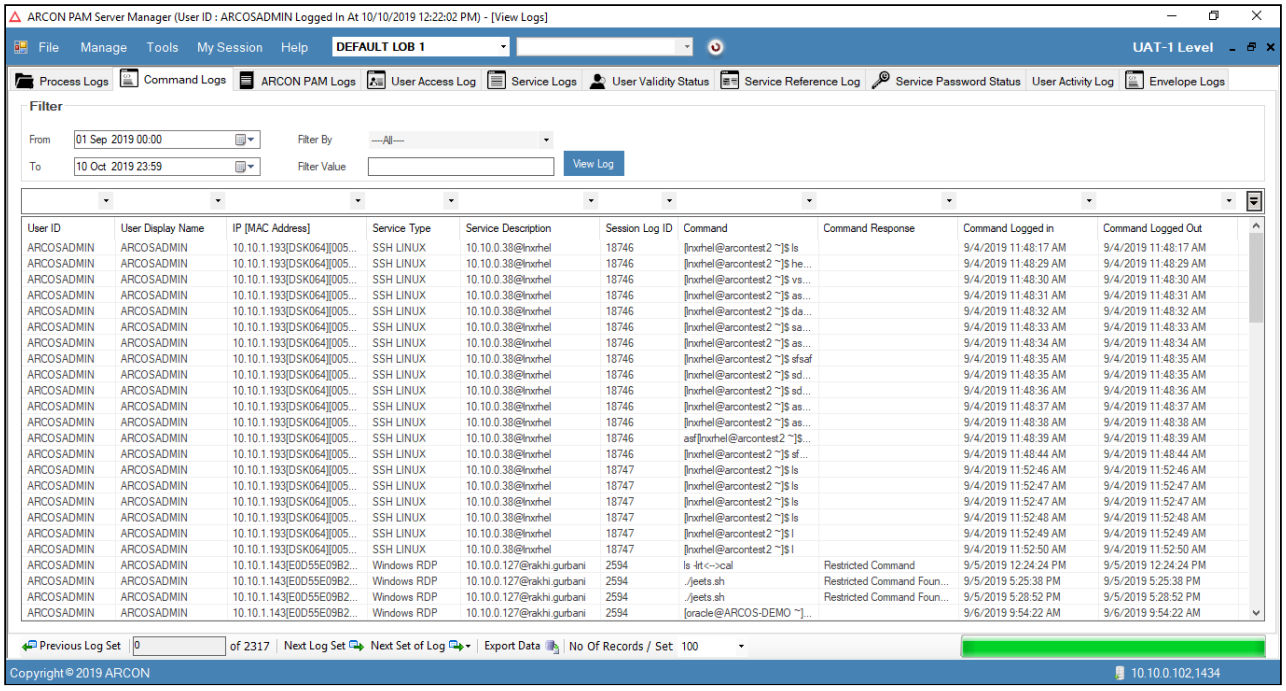
Manage → Logs → Command Logs



The **Filter** screen contains the following fields:

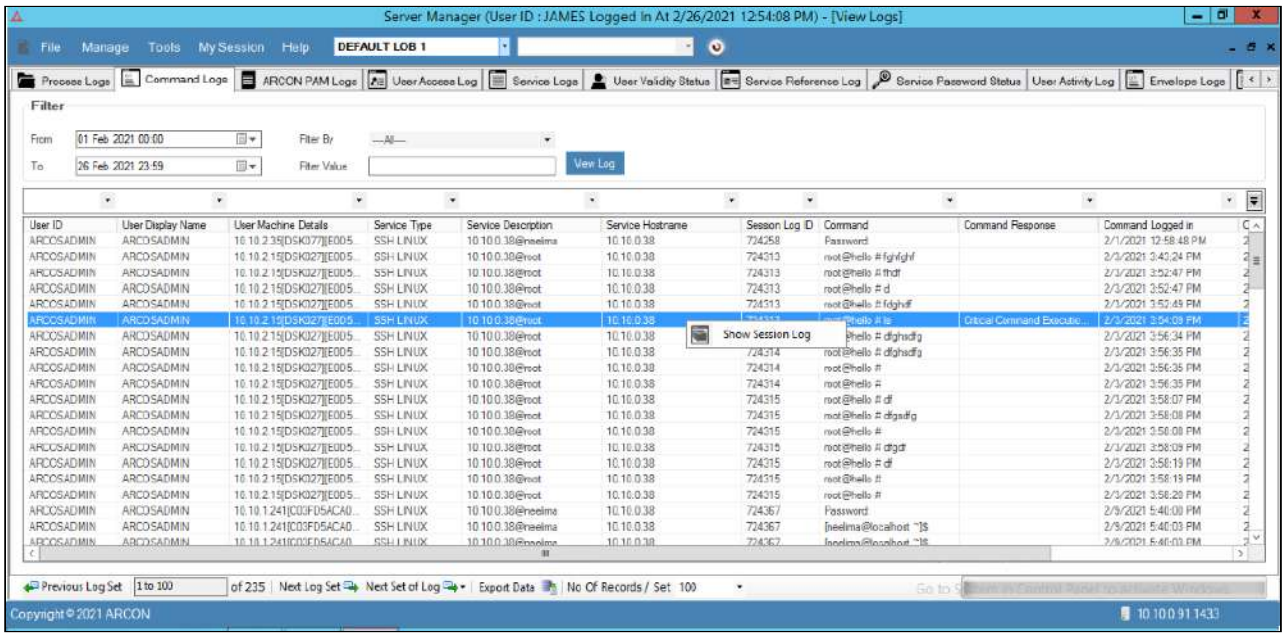
Field Name	Description
From	Select the start date, to generate logs.
To	Select the end date, until when you want to generate logs.
Filter By	Select the type of filter. The valid values are: • User Name • Server IP Address • User IP (MAC) Address • Command Fired • Command Response • User Groups • Service Groups
Filter Value	Specify the value, to filter the logs.

1. Select/Enter the fields and click on **View Log** button. The logs are generated based on the selected filters.

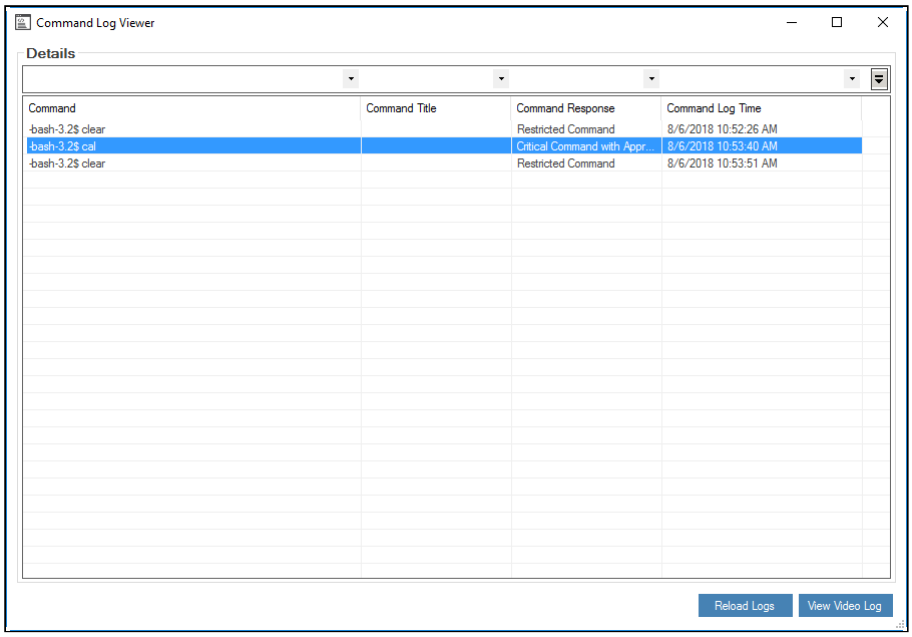


To view video of command logs:

1. Right-click on the command log, to view the video log. A **Show Session Log** option is popped up.

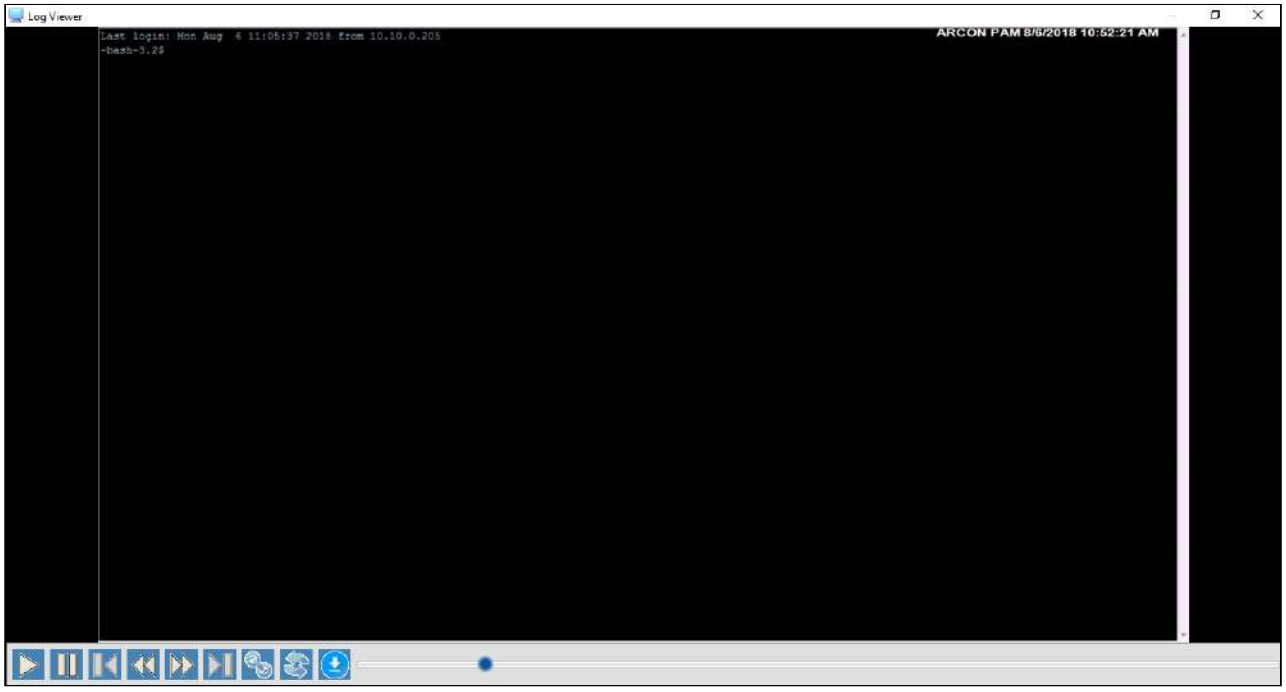


2. Click **Show Session Log** option. A window pops up.



⚠ You can view **Video Logs** for the selected set of commands. In **Command Log Viewer** screen, select the required command and click **View Video Log** button. The video will start from the selected command till the end of the session.

3. Click **View Video Log** button. The **Log Viewer** screen is displayed.



4. View the video log.

- To export logs into .xls format, click on **Export Data** button, which is present in the bottom of the screen.
- Click Previous Log Set, to view set of previous logs.
- Click Next Log Set, to view next set of logs.
- Click Next Set of Log, to view particular set of logs. Select the particular set from the **Next Set of Log** dropdown list.
- Select the number of records from **No of Records/Set** dropdown list, wherein it will display those many records in the grid.

9.3 ARCON PAM Logs

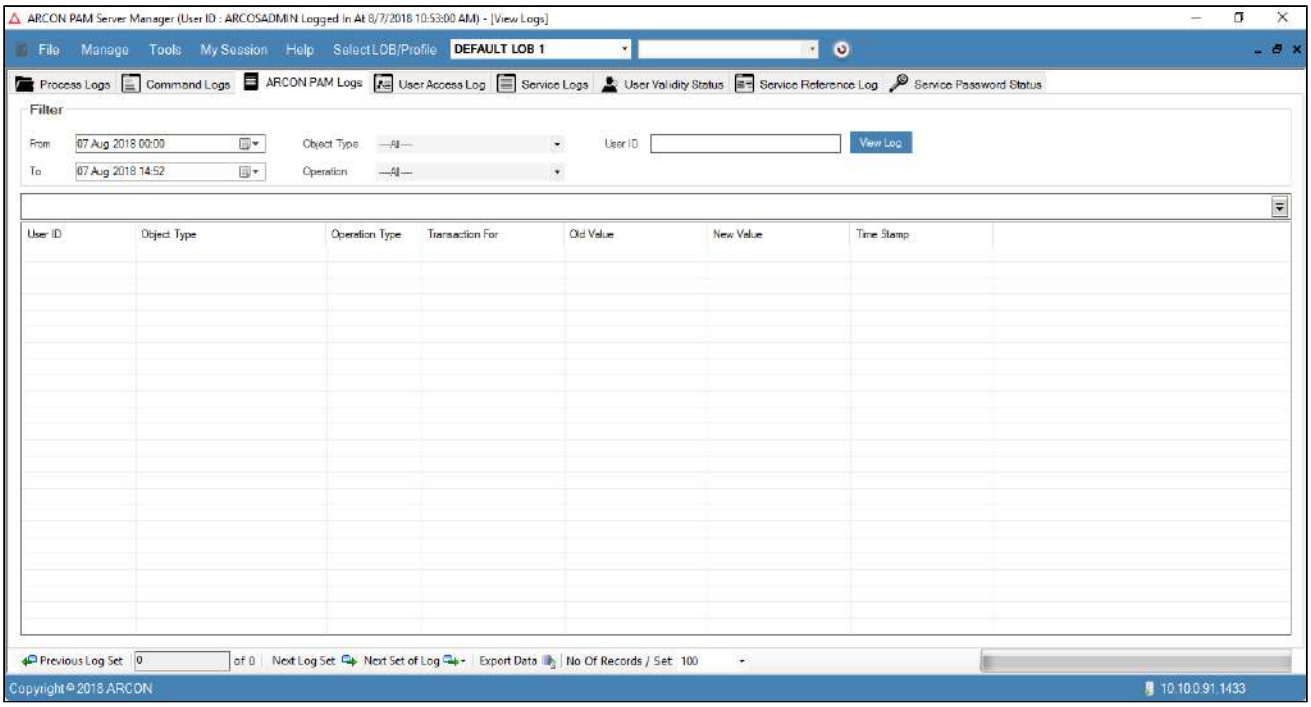
ARCON PAM Logs provides audit trail details for the activities performed in Server Manager. It generates logs for all the activities performed by the users while using the application. The logs can be filtered based on the type of object such as Group Transactions, User and Services Transactions, Transactions between User/User Group, Service/ Service Group, User/Service, User Group/Service Group, and User/Restrict Commands based on the date. In addition, the logs can also be filtered based on the type of operations such as Created, Modified, Deleted, Assigned, Revoked, Checker Approved, and Checker Not Approved. It displays details such as User ID of the User, type of object, type of operation, transaction for, old value, new value, and time stamp. The generated logs can be exported to .xls format.

- The Administrator having **View ARCOS Log** privilege in Server's Privileges will only be able to view ARCON PAM logs.
- When **Server** is added to **ServerGroup** through **workflow** and the **Settings** for bulk mapping is enabled then ARCON PAM Logs for transaction between **User** and **Service** will be generated.
- Administrators having **PAM Logs** privilege can view ARCON PAM Logs in ACMO under Manager tab (My Apps)

To generate ARCON PAM Logs:

To generate ARCON PAM logs use the following path:

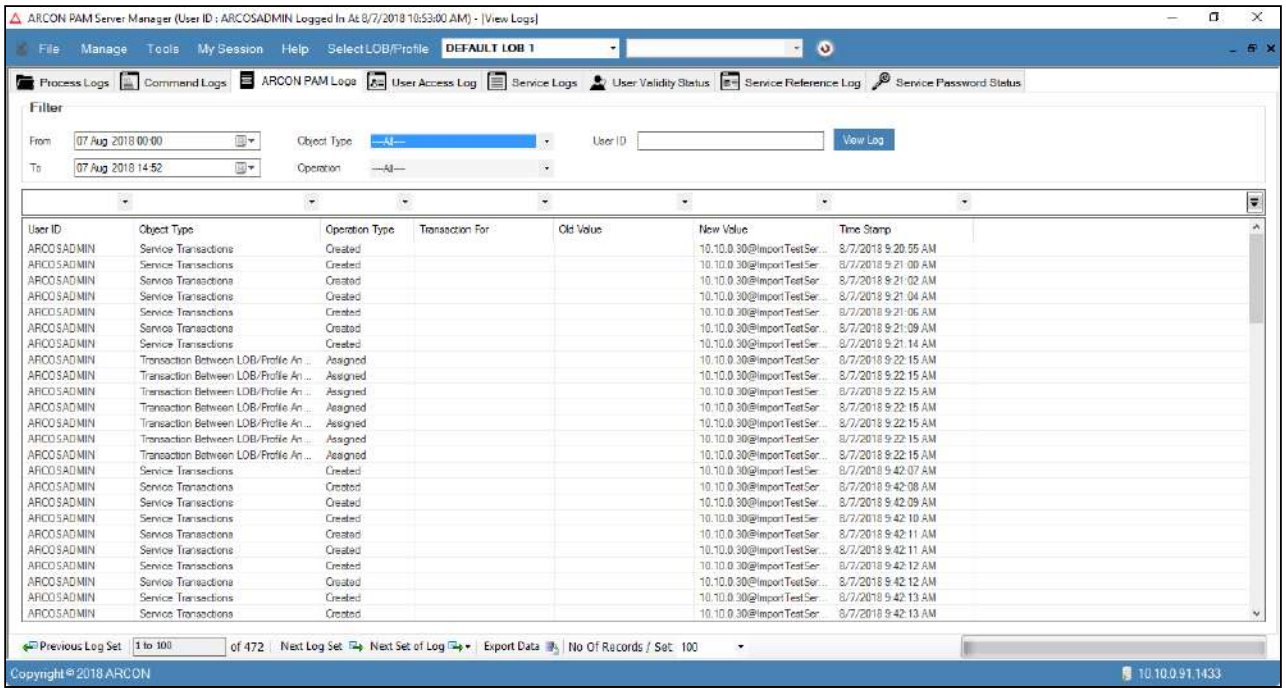
Manage → Logs → ARCON PAM Logs



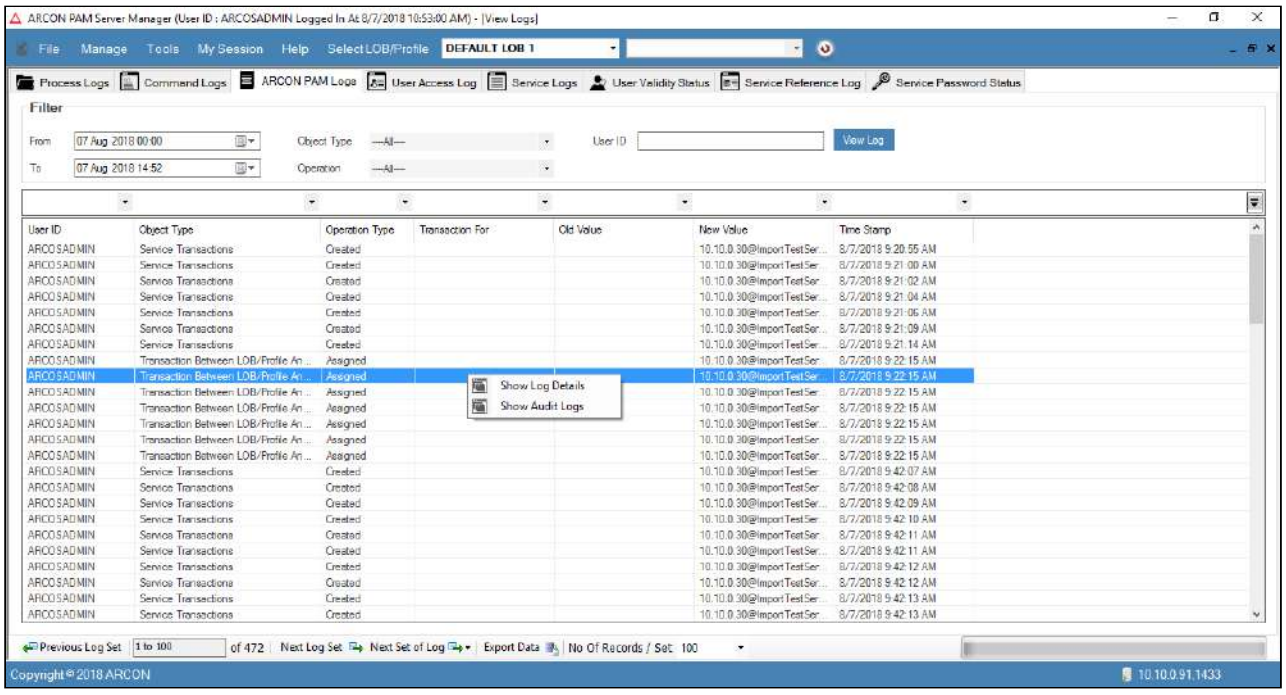
The **Filter** screen contains the following fields:

Field Name	Description
From	Select the start date, to generate logs.
To	Select the end date, until when you want to generate logs.
Object Type	Select the type of object from the dropdown list.
Operation	Select the type of operation from the dropdown list.
User ID	Specify the user ID, to filter the logs. ⚠ The logs are filtered based on the user ID.

1. Select/Enter the fields and click on the **View Log** button. The logs are generated based on the selected filters.



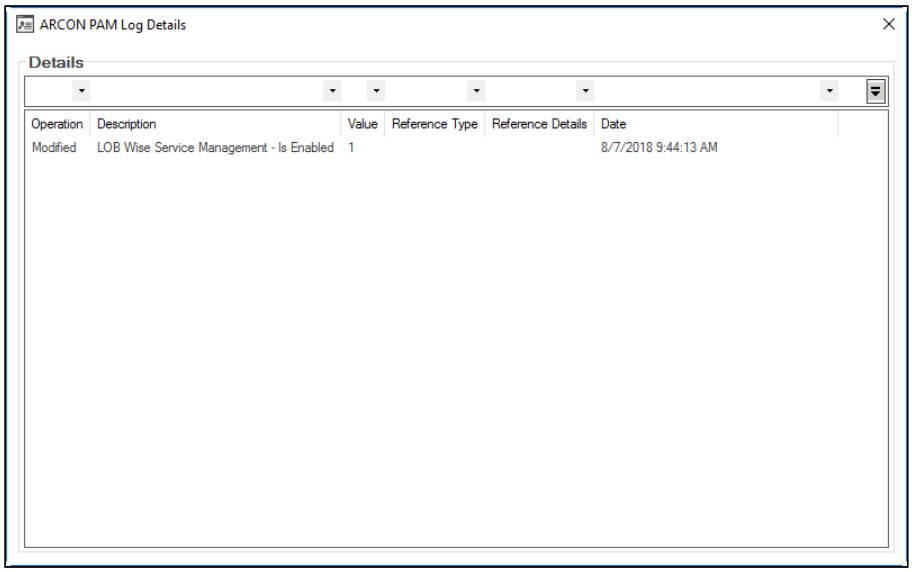
2. Right click on the log. A **Show Log Details** and **Show Audit Logs** options are displayed.



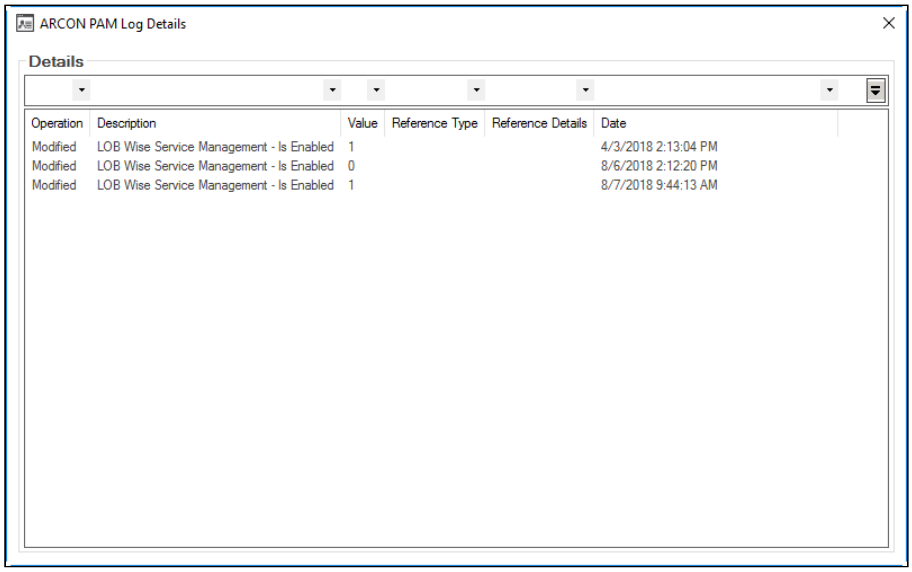
The following are the two options:

- **Show Log Details:** Displays details of the log selected.
- **Show Audit Details:** Displays details of all the actions performed.

3. Click the **Show Log Details** option. The log details screen is displayed.



4. Click **Show Audit Logs** option. The audit details screen is displayed.



5. View the audit log details.

⚠

- To export logs into .xls format, click on **Export Data** button, which is present in the bottom of the screen.
- Click Previous Log Set, to view set of previous logs.
- Click Next Log Set, to view next set of logs.
- Click Next Set of Log, to view particular set of logs. Select the particular set from the **Next Set of Log** dropdown list.
- Select the number of records from **No of Records/Set** dropdown list, wherein it will display those many records in the grid.
- ARCON PAM Logs can be viewed only for a maximum of 180 days at a time.

9.3.1 Reference Detail for Audit Trail

You can enable reference details for transactions performed in Advanced Configuration and User and Service Management. These details help you to track reference for transactions performed in ARCON PAM under ARCON PAM Logs.

A **Configuration Reference Details** window is prompted to User when he performs any transaction in ARCON PAM. You need to select type of reference and enter its details. These details will be displayed in ARCON PAM Logs along with the transaction details.

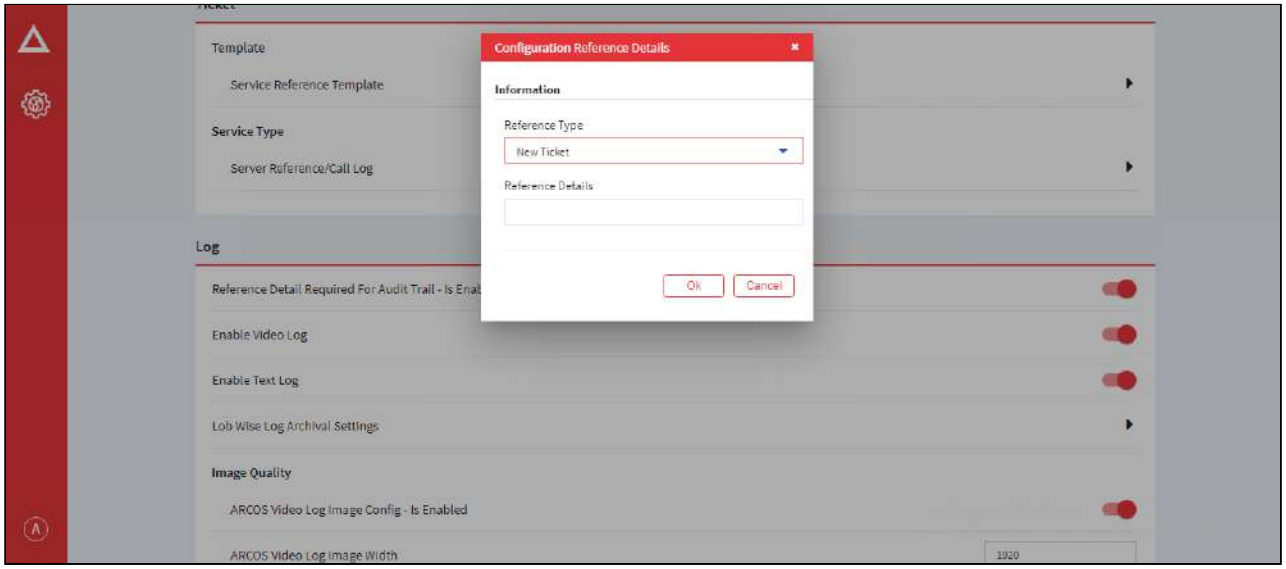
> ⚠ Thetoggle value for **Reference Detail Required For Audit Trail - Is Enabled** under **Settings** should **Enabled** for ARCON PAM to prompt **Configuration Reference Details** window to Administrator.

Configure reference details and view in ARCON PAM Logs.

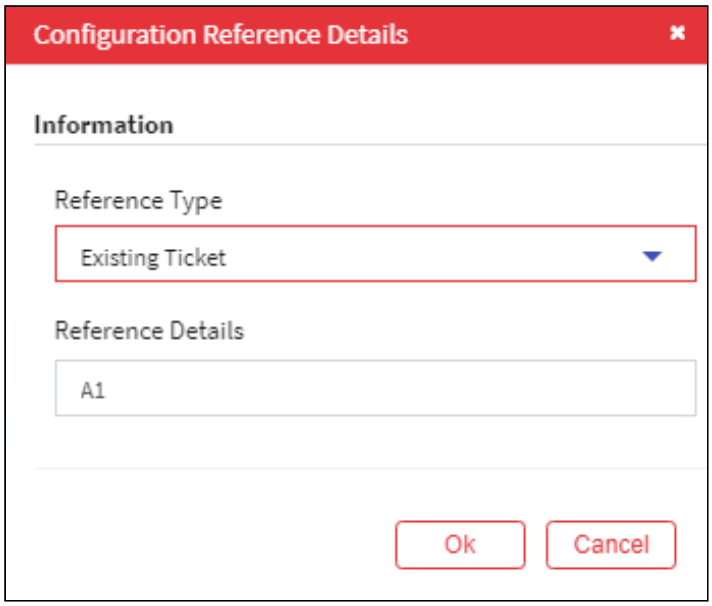
To configure reference details, use following path:

Settings → Log

1. Enable the toggle value for **Reference Detail Required For Audit Trail - Is Enabled** configuration.
2. The **Configuration Reference Details** window will be prompted.



3. Select the **Reference Type** as New Ticket, Existing Ticket or Other. Enter details in **Reference Details** text field.

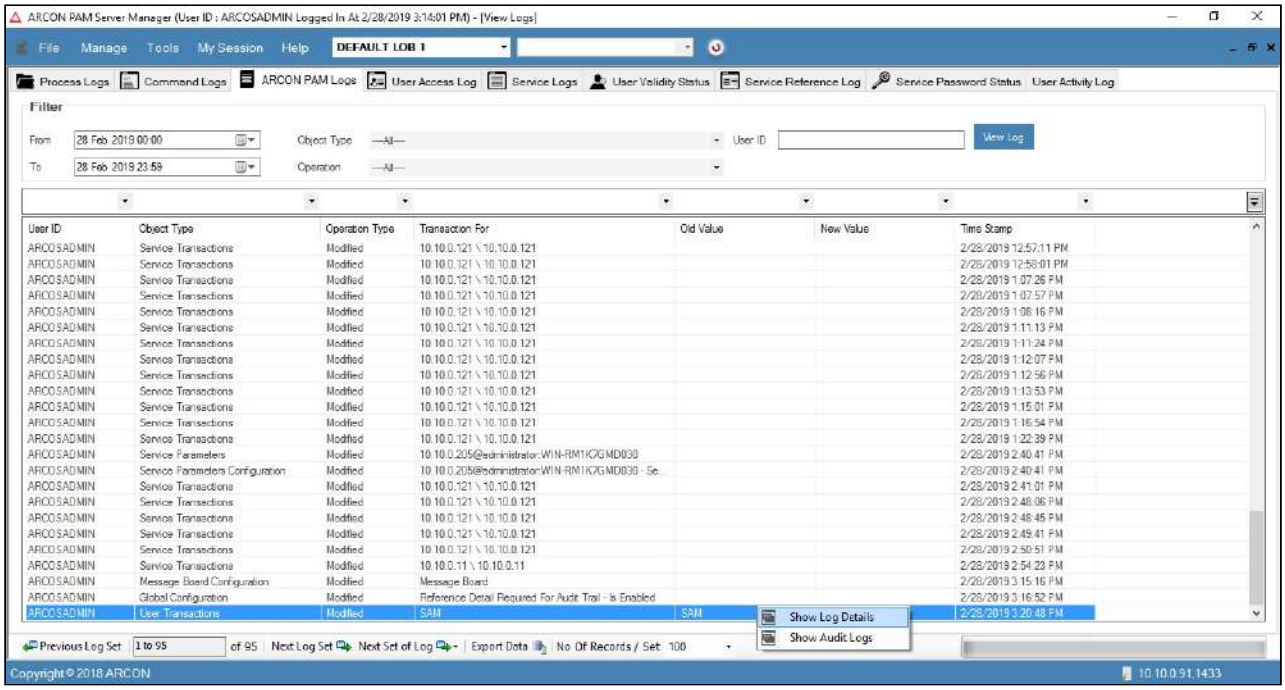


4. Click **OK**. The transaction will be completed and transaction details along with reference details will be captured in **ARCON PAM Logs**.

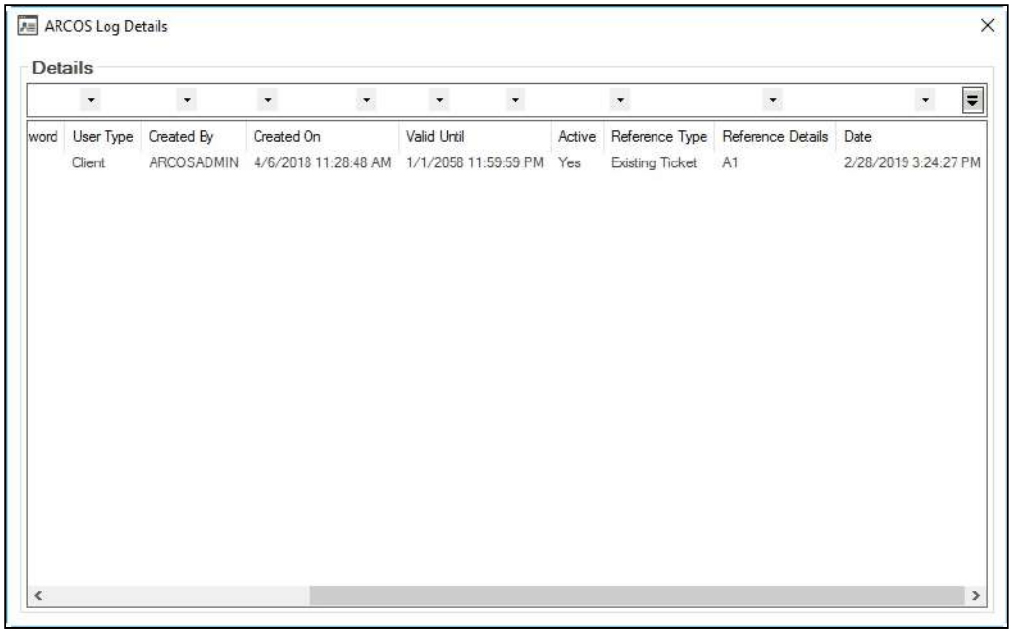
To view details in ARCON PAM Logs, use the following path:

Manage → Logs → ARCON PAM Logs

1. Select or enter details in filters and click **View Log**.
2. Right click on the log for which you had performed transaction. A **Show Log Details** and **Show Audit Logs** options are displayed.



3. Click the **Show Log Details** option. The log details screen is displayed.



4. Click **Show Audit Logs** option. The audit details screen is displayed.
5. View the reference details displayed under **Reference Type** and **Reference Details** in **ARCOS Log Details** window.

9.4 User Access Logs

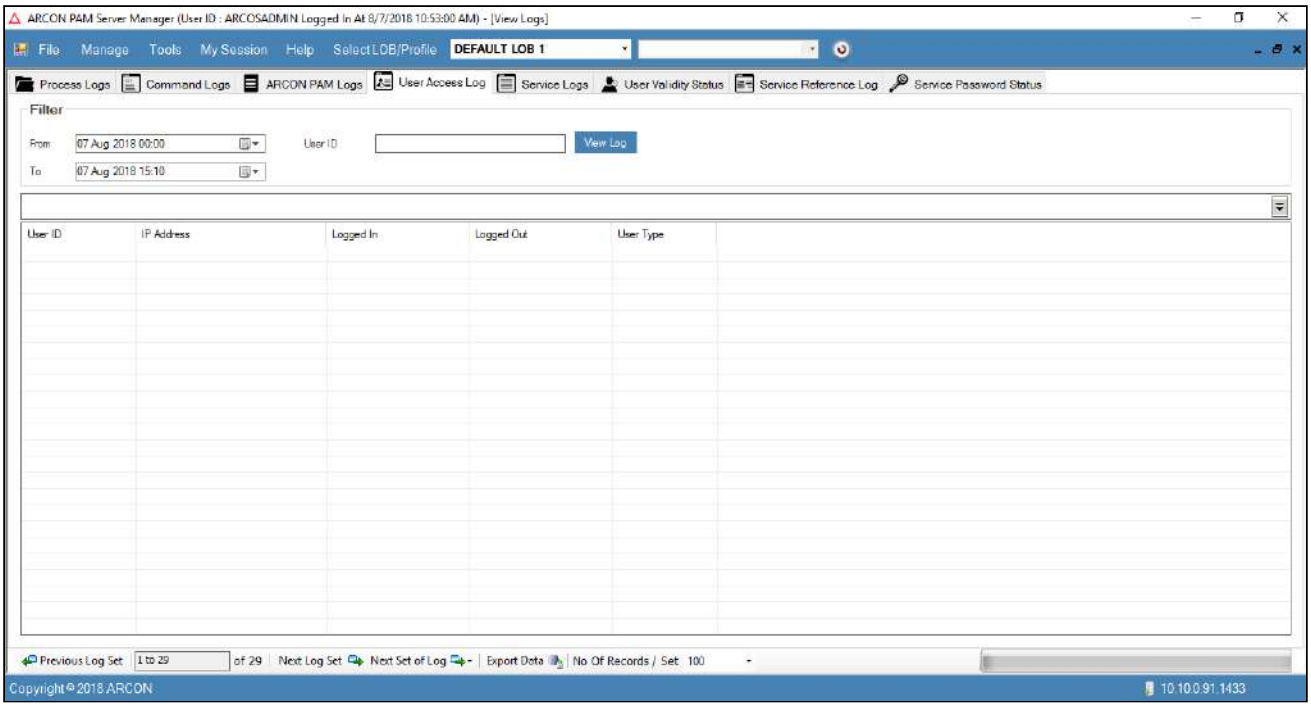
User Access Logs helps you to generate the login and logout details of the user who has accessed the ARCON PAM application. It displays details such as User ID, User Display Name, User Machine Details, Logged in and out time, and type of user.

> ⚠ The Administrator having **View User Access Log** privilege in Server's Privileges will only be able to view User Access logs.

To generate User Access Logs:

To generate User Access Logs use the following path:

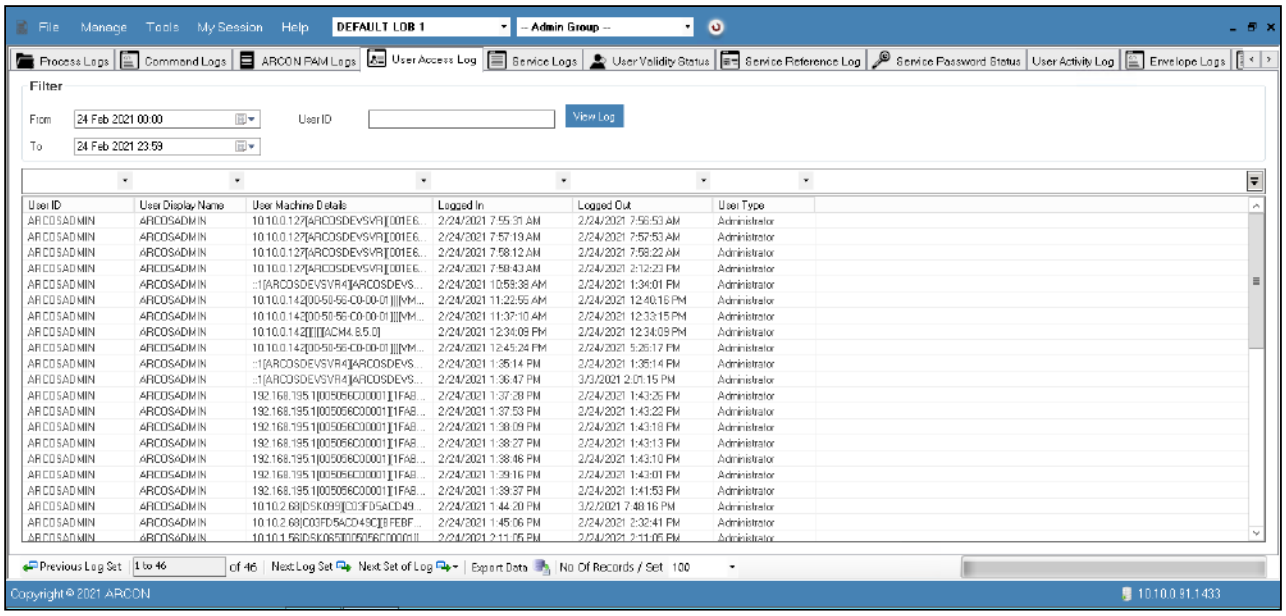
Manage → Logs → User Access Logs



The **Filter** screen contains the following fields:

Field Name	Description
From	Select the start date, to generate logs.
To	Select the end date, until when you want to generate logs.
User ID	Specify the user ID, to filter the logs. ⚠ The logs are filtered based on the user ID.

1. Select/Enter the fields and click the **View Log** button. The logs are generated based on the selected filters.



- To export logs into .xls format, click on **Export Data** button, which is present in the bottom of the screen.
- Click Previous Log Set, to view set of previous logs.
- Click Next Log Set, to view next set of logs.
- Click Next Set of Log, to view particular set of logs. Select the particular set from the **Next Set of Log** dropdown list.
- Select the number of records from **No of Records/Set** dropdown list, wherein it will display those many records in the grid.

9.5 Service Logs

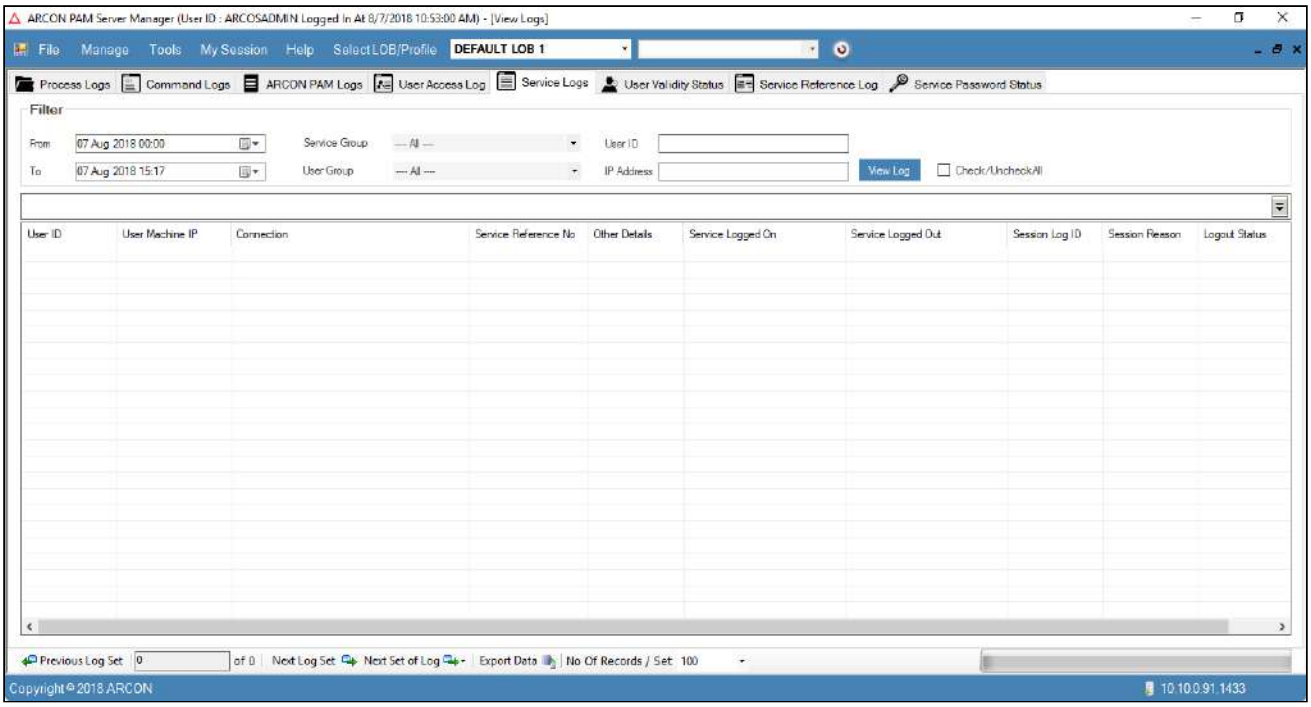
Service logs help you to generate detailed logs of the services accessed by the user in the ARCON PAM application. It displays details such as User ID, User Machine ID, Connection details, Service Reference Number, other details, log in and logout details of the service, session Log ID, reason for accessing session and log out status (reason for session termination). Users can export these logs to the desired location if required.

- The Administrator having **View Service Log** privilege in Server's Privileges will only be able to view Service logs. In addition, the Administrator should have **Download Video Log** privilege, to download video logs.
- The Server Group Admin having **View Command Log** privilege in Group Admin Privileges, will only be able to view Service Logs.

To generate Service Logs:

To generate service logs use the following path:

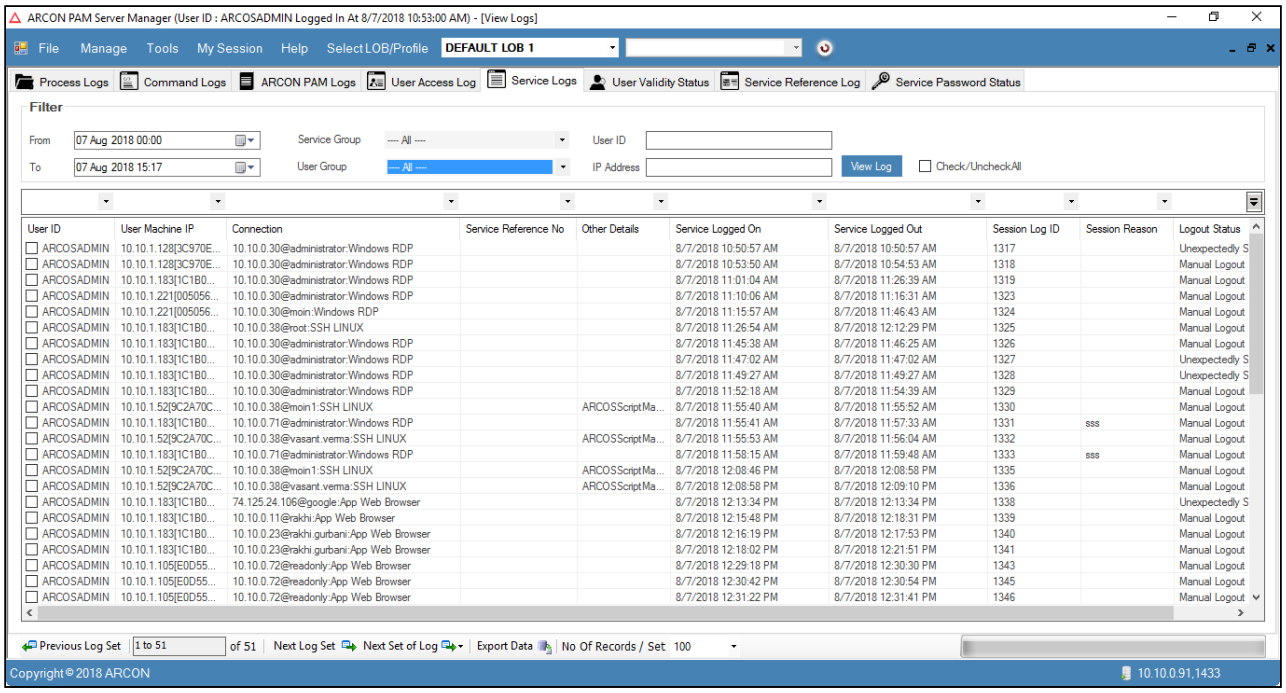
Manage → Logs → Service Logs



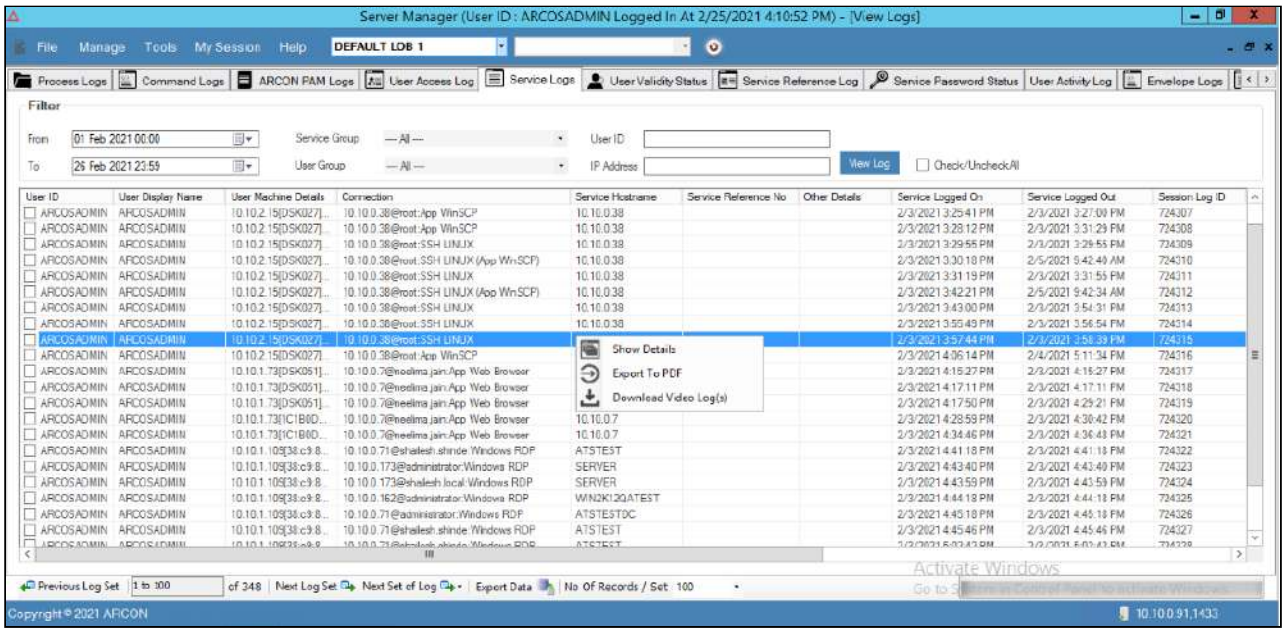
The **Filter** screen contains the following fields:

Field Name	Description
From	Select the start date, to generate logs.
To	Select the end date, until when you want to generate logs.
Service Group	Select the service group from the dropdown list.
User Group	Select the user group from the dropdown list.
User ID	Specify the user ID, to filter the logs. ⚠ The logs are filtered based on the user ID.
IP Address	Specify the IP address, to filter the logs. ⚠ The logs are filtered based on the IP address.

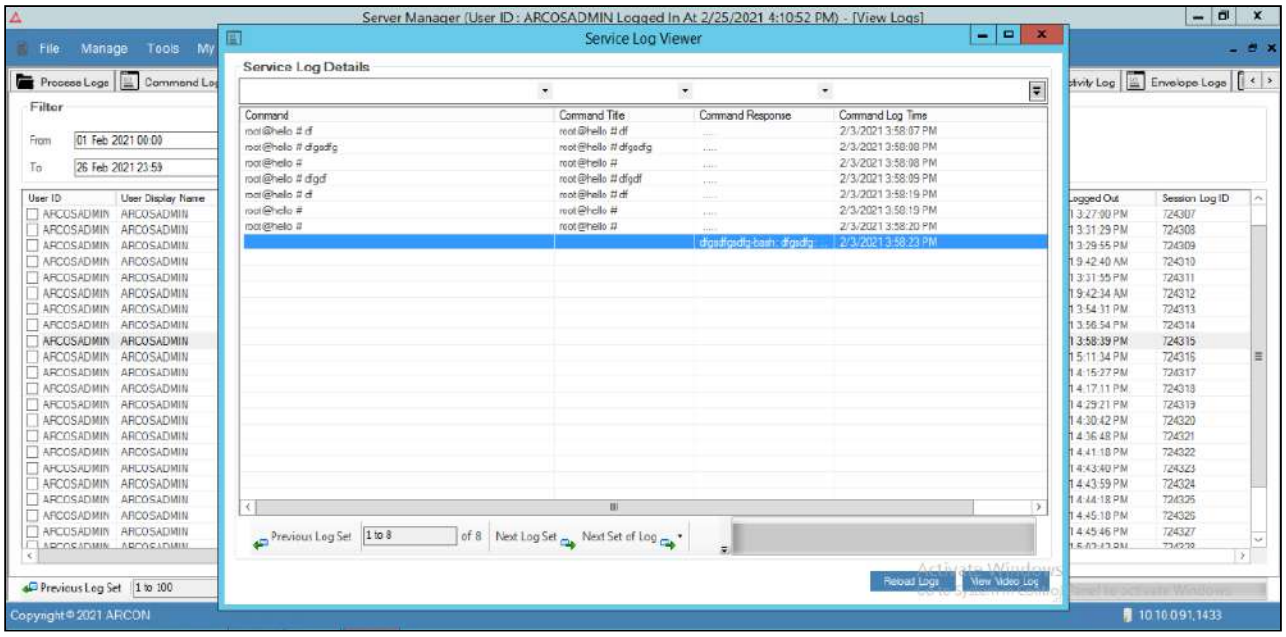
1. Select/Enter the fields and click on the **View Log** button. The logs get generated based on the selected filters.



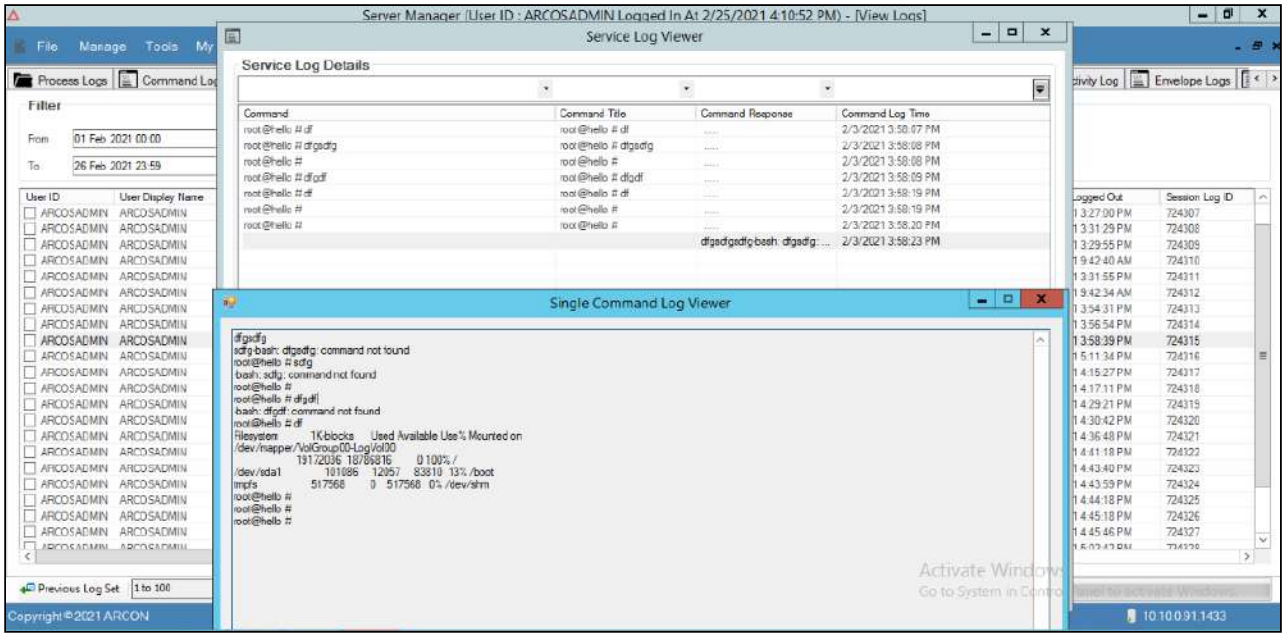
2. Select the **Check/UncheckAll** checkbox to select/deselect all the details in grid view.
3. Right-click on the selected service detail and choose **Show Details** option, to view video log.



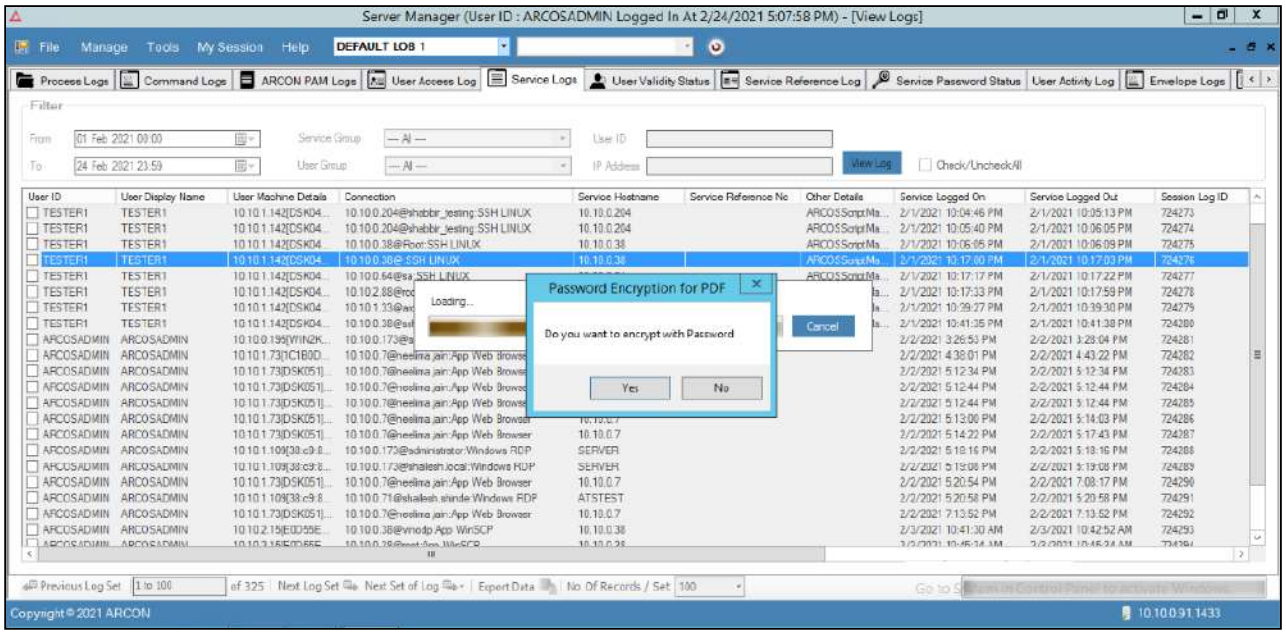
4. Click **Show Details** option. The **Service Log Viewer** screen is displayed. To view the video logs, click the view video log button.



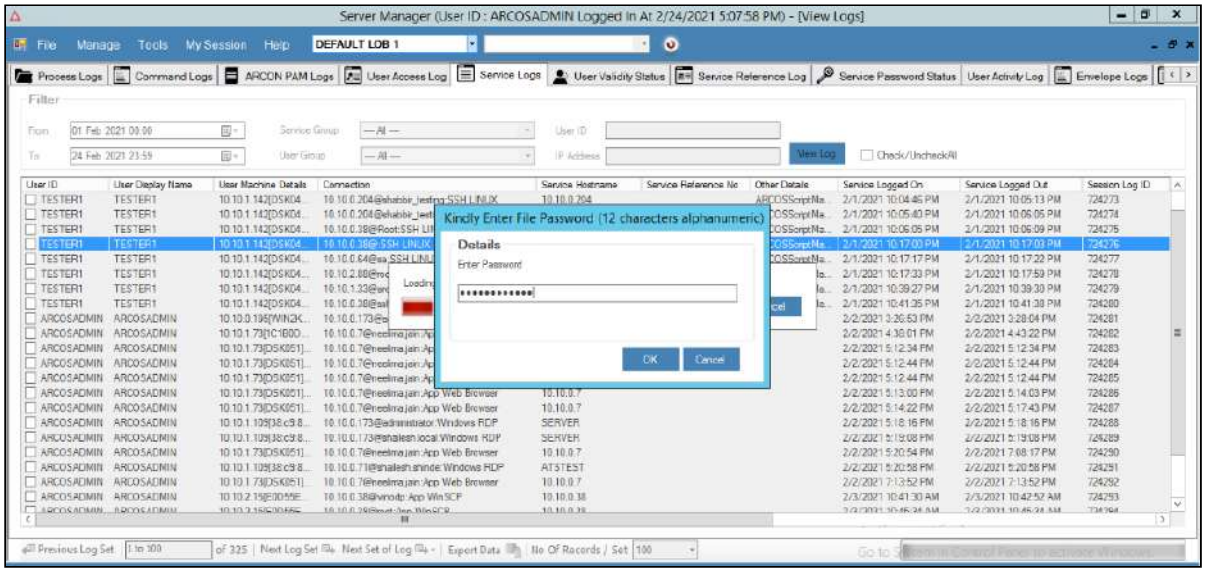
5. To view the response of the command, right-click on the command response- Single command log viewer opens.



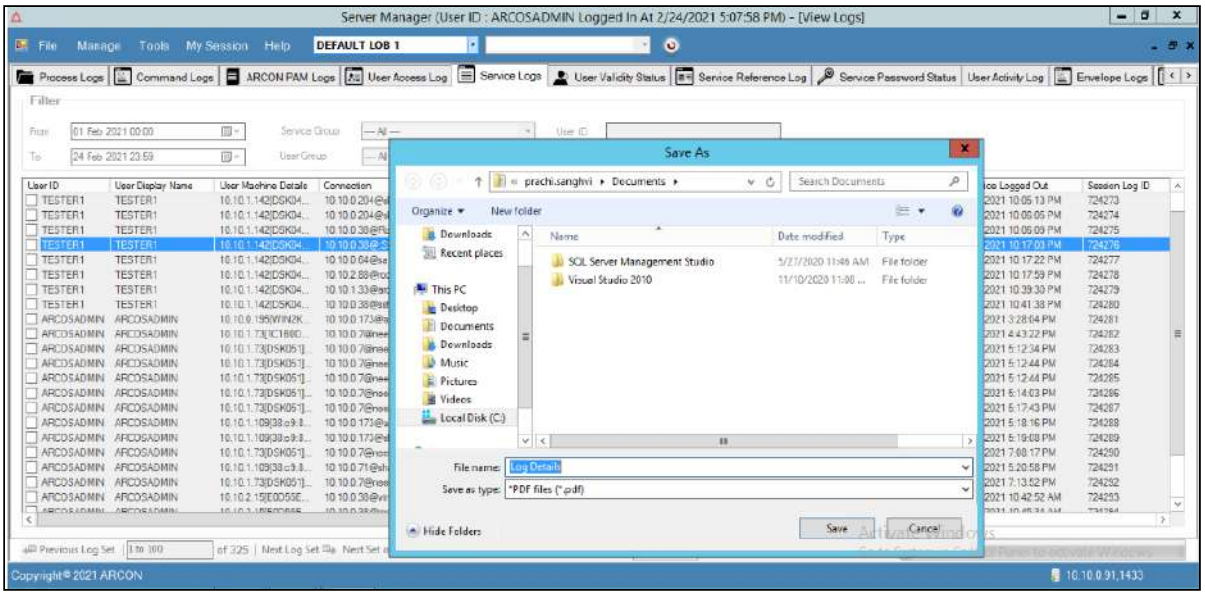
6. Select the checkboxes beside the service details, right-click, and select **Export To PDF** option, to export logs to PDF document.
7. A prompt appears on the screen- Do you want to encrypt with Password.



a. Select **Yes** if the file you want to export should be password encrypted. It will then ask to enter twelve character Alphanumeric password.



b. Select **Ok** and select where you'd like your **files** to be saved.



8. Select the checkboxes beside the service details, right-click, and select **Download Video Log(s)** option, to download multiple video logs.
9. View the video log.

- To export logs into .xls format, click on **Export Data** button, which is present at the bottom of the screen.
- Click Previous Log Set, to view the set of previous logs.
- Click Next Log Set, to view the next set of logs.
- Click Next Set of Log, to view particular set of logs. Select the particular set from the **Next Set of Log** dropdown list.
- Select the number of records from **No of Records/Set** dropdown list, wherein it will display those many records in the grid.

9.6 User Validity Status

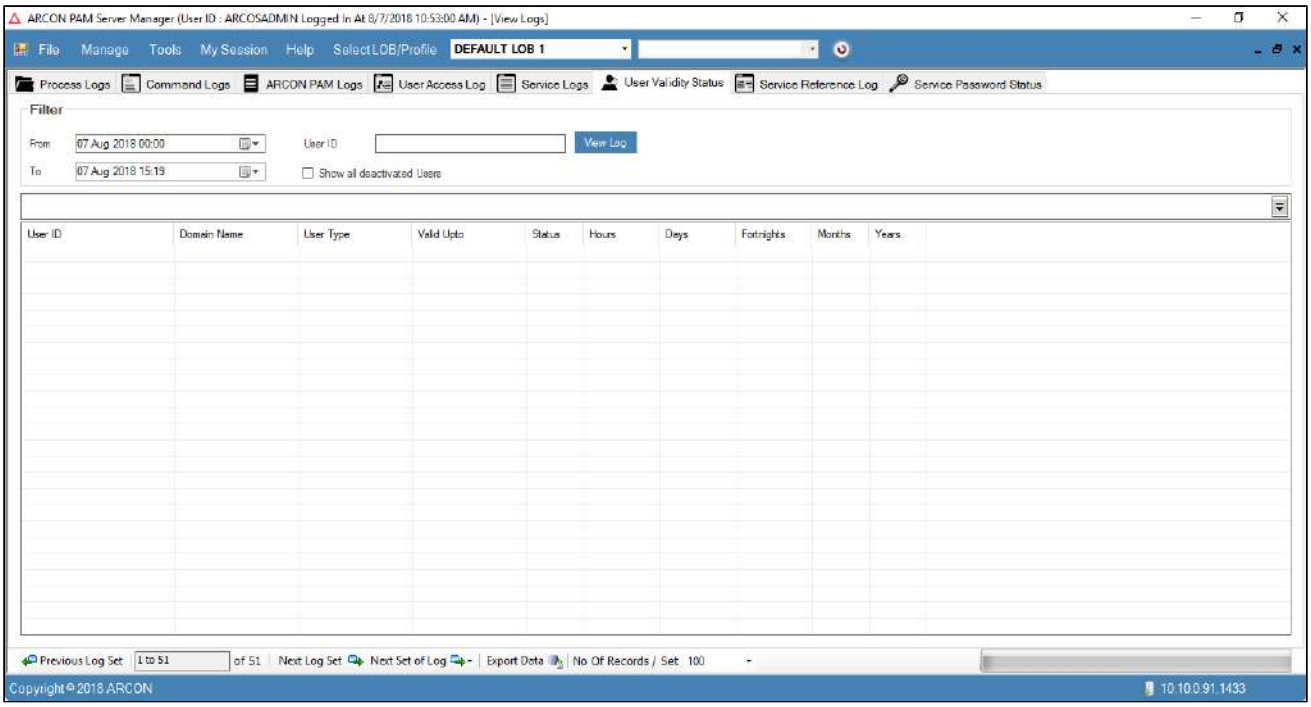
User Validity Status helps you to generate details of all the users which are active or the ones who are deactivated by Administrator to access ARCON PAM application. This helps the Administrator to visually perceive all the details of the users. It gives the total time [in hours, days, forth nights and years] the user is active and the time he has been de-activated to access the application. It displays details such as User ID, domain name, type of user, valid date and time with hours, days, forth nights and years to access the application, and status of the user.

The Administrator having **View User Validity Status** privilege in Server's Privileges will only be able to view User Validity Status logs.

To generate User Validity Status:

To generate User Validity Status use the following path:

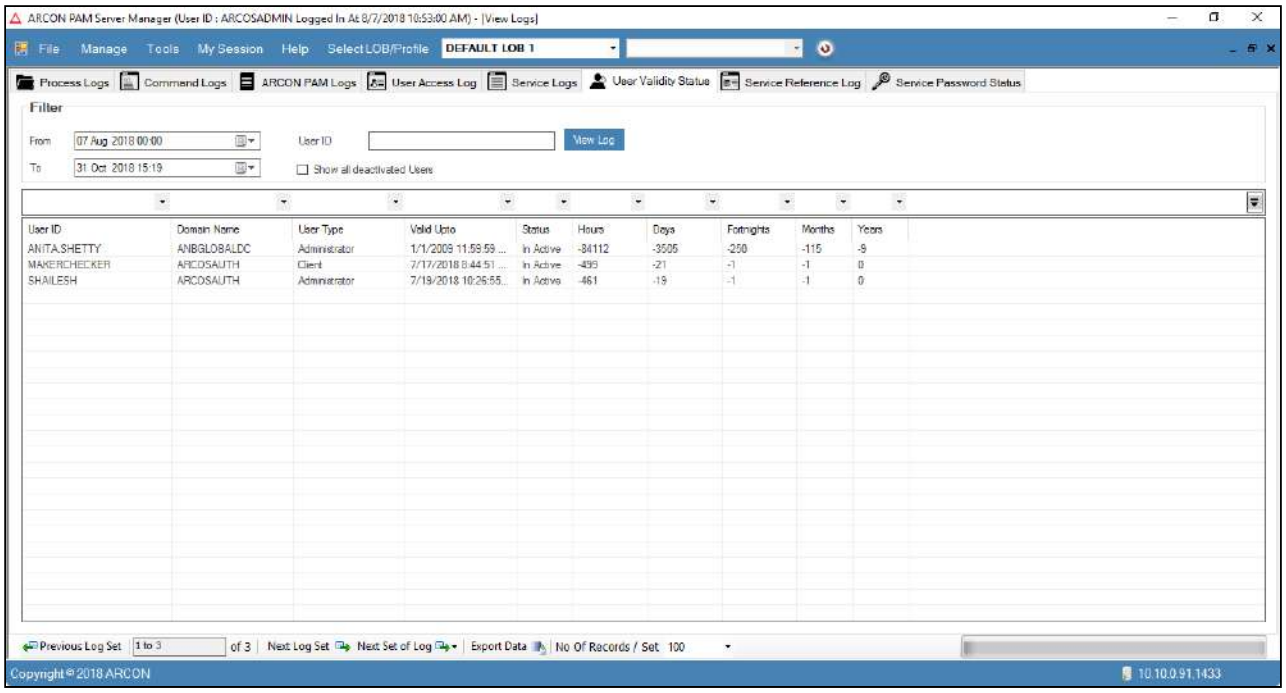
Manage → Logs → User Validity Status



The **Filter** screen contains the following fields:

Field Name	Description
From	Select the start date, to generate logs.
To	Select the end date, until when you want to generate logs.
User ID	Specify the user ID, to filter the logs. ⚠ The logs are filtered based on the user ID.
Show all deactivated Users (checkbox)	Filter the logs of all the deactivated (inactive) users.

1. Select/Enter the fields and click the **View Log** button. The logs are generated based on the selected filters.



- Select **Show all deactivated Users** and click **View Log** button to display inactive users.
- To export logs into .xls format, click on **Export Data** button, which is present in the bottom of the screen.
- Click Previous Log Set, to view set of previous logs.
- Click Next Log Set, to view next set of logs.
- Click Next Set of Log, to view particular set of logs. Select the particular set from the **Next Set of Log** dropdown list.
- Select the number of records from **No of Records/Set** dropdown list, wherein it will display those many records in the grid.

9.7 Service Password Status

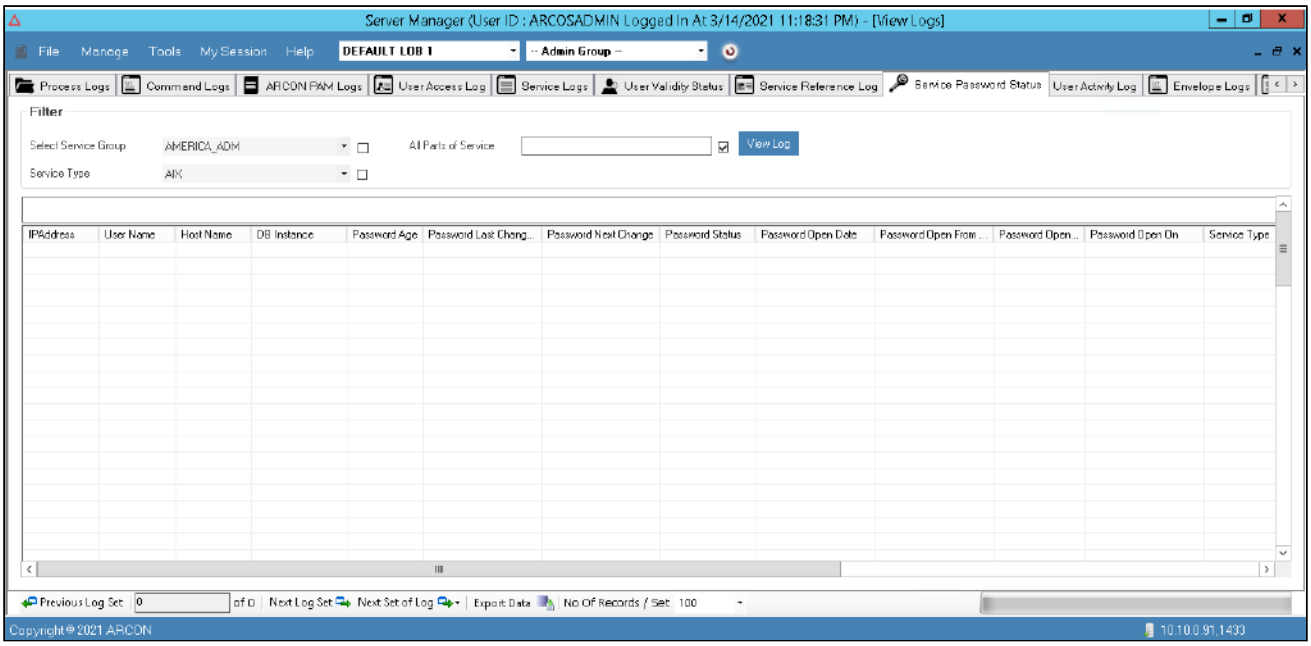
Service Password Status Logs helps you to view the details of the service password status for the services in ARCON PAM. It displays details such as the age of the password, last modified date of the password, the next date to change the password, and the status of the password. In addition, if the status of the password is Open then it also displays the details such as the date and time on which the password is opened, the days from when the password is active, the name of the user who has viewed the password, and the type of the service.

The Administrator having **View Service Password Status Log** privilege in Server's Privileges will only be able to view Service Password Status logs.

To generate Service Password Status log:

To generate the service password status log use the following path:

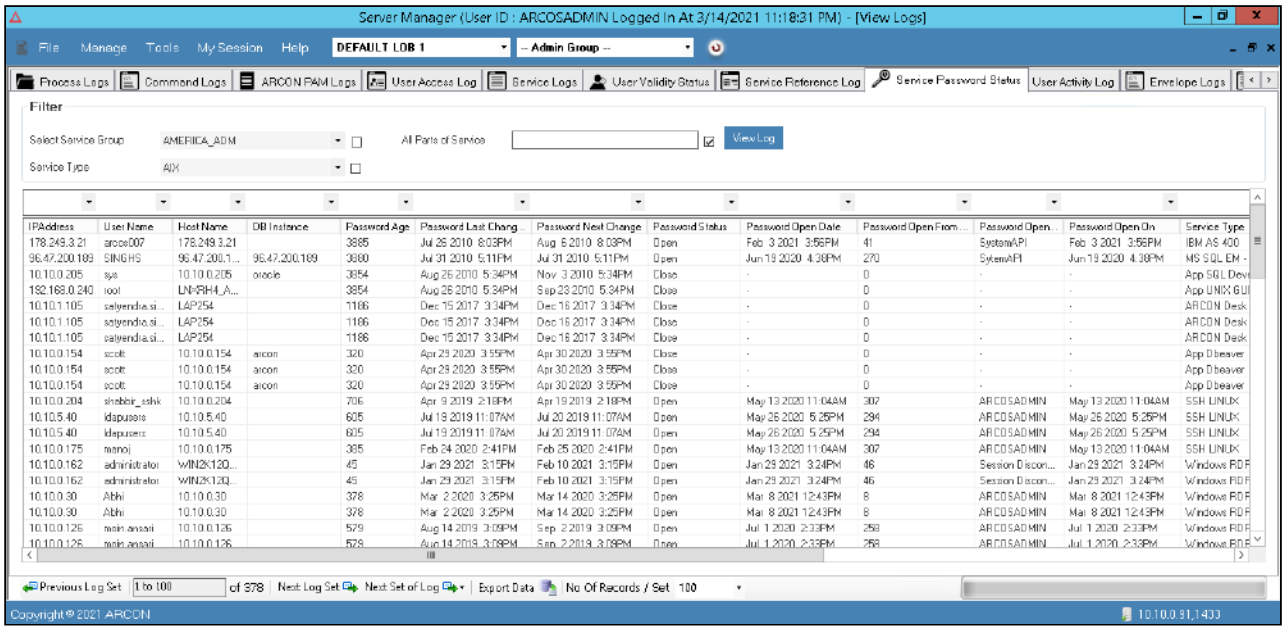
Manage → Logs → Service Password Status



The **Filter** screen contains the following fields:

Field Name	Description
Select Service Group	Select the service group. ⚠ To filter logs for a specific service group, select **Select Service Group** checkbox.
Service Type	Select the type of service. ⚠ To filter logs for a specific service type, select **Service Type** checkbox.
All Parts of Service	Specify a keyword to search the available service type. For example, To search for a service type like WINDOWS RDP, specify the keyword as WIN, RDP or NDO. ⚠ If you want to filter details of all the services then you need to select **All Parts of Service** checkbox. By default, **All Parts of Service** checkbox is selected.

1. Select/Enter the fields and click the **View Log** button. The logs are generated based on the selected filters.



- To export logs into .xls format, click on **Export Data** button, which is present in the bottom of the screen.
- Click Previous Log Set, to view set of previous logs.
- Click Next Log Set, to view next set of logs.
- Click Next Set of Log, to view particular set of logs. Select the particular set from the **Next Set of Log** dropdown list.
- Select the number of records from **No of Records/Set** dropdown list, wherein it will display those many records in the grid.

9.8 Service Reference Logs

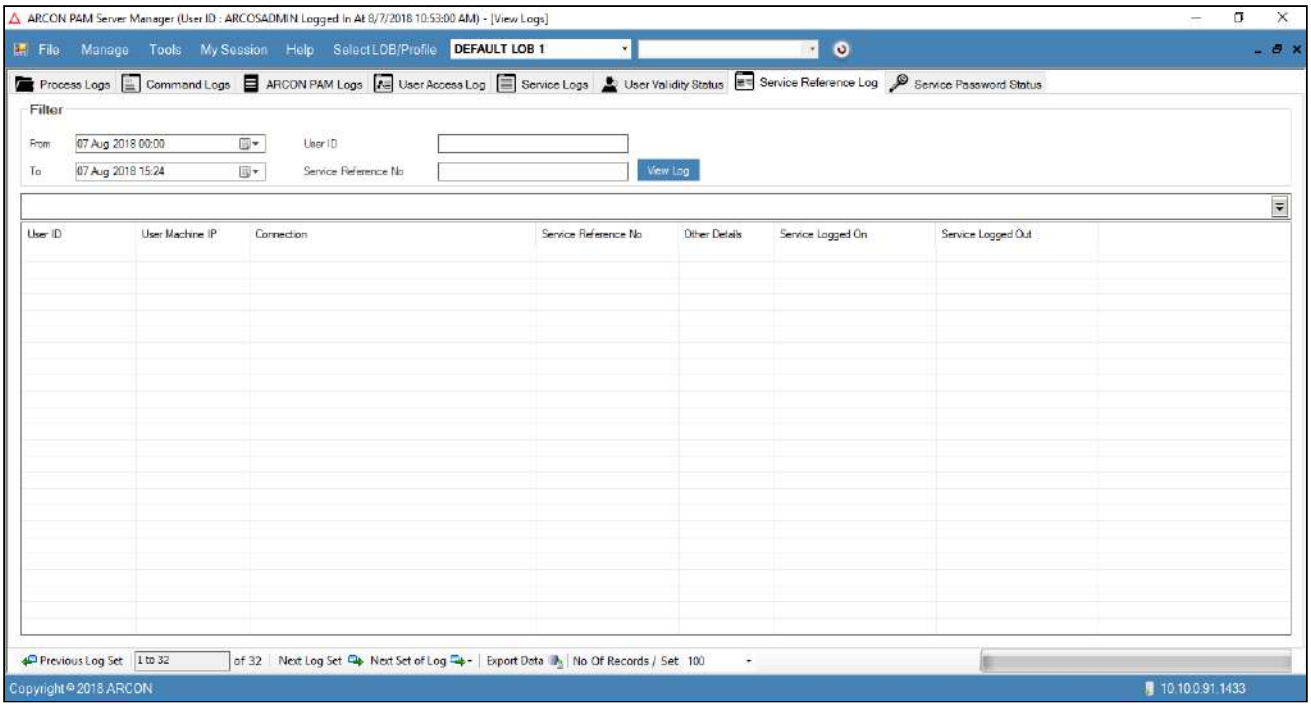
Service Reference Logs helps you to generate details of reference number used before accessing services by Users through ARCON PAM. It displays details of the User such as the ID of the User, machine IP, the type of connection, service reference number, and the login – logout details of the service used.

The Administrator having **View Server Reference Log** privilege in Server's Privileges will only be able to view Service Reference logs.

To generate Service Reference Logs:

To generate Service Reference Logs use the following path:

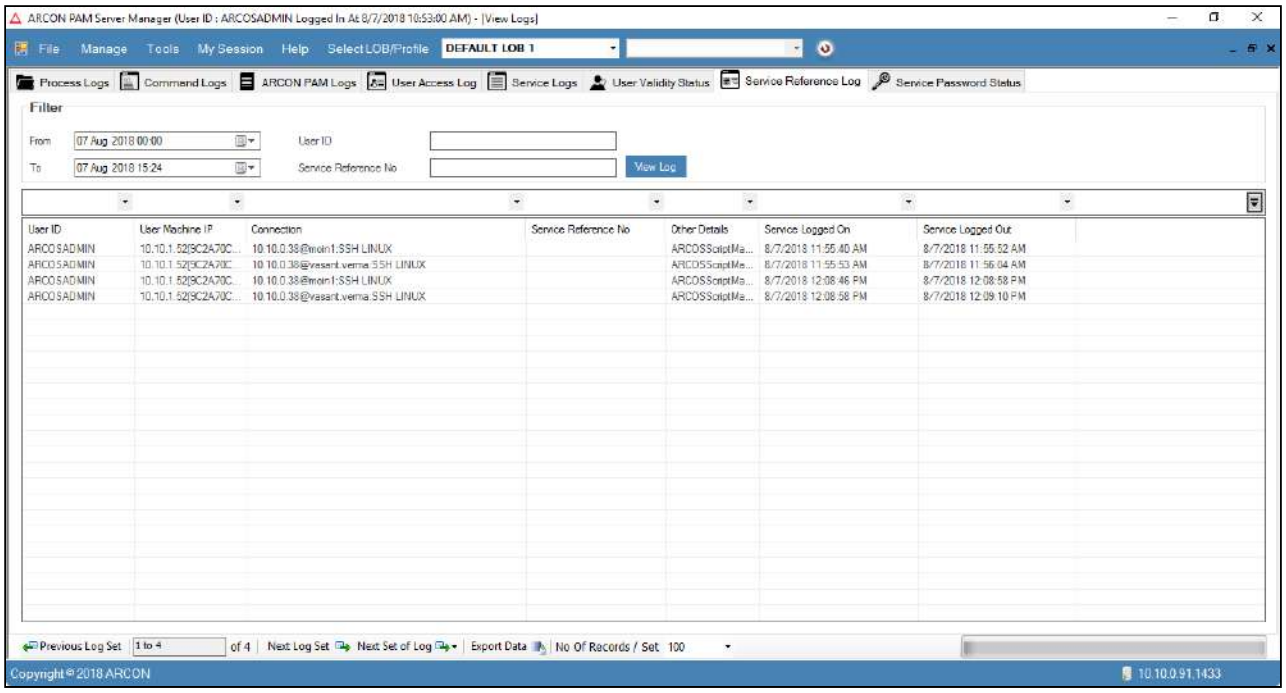
Manage → Logs → Service Reference Logs



The **Filter** screen contains the following fields:

Field Name	Description
From	Select the start date, to generate logs.
To	Select the end date, until when you want to generate logs.
User ID	Specify the user ID, to filter the logs. ⚠ The logs are filtered based on the user ID.
Service Reference Number	Specify the service reference number, to filter the logs. ⚠ The logs are filtered based on the reference number of a service.

1. Select/Enter the fields and click on the **View Log** button. The logs are generated based on the selected filters.



- To export logs into .xls format, click on **Export Data** button, which is present in the bottom of the screen.
- Click Previous Log Set, to view set of previous logs.
- Click Next Log Set, to view next set of logs.
- Click Next Set of Log, to view particular set of logs. Select the particular set from the **Next Set of Log** dropdown list.
- Select the number of records from **No of Records/Set** dropdown list, wherein it will display those many records in the grid.

9.9 User Activity Log

User Activity Log displays text and video logs for File Watcher or Smart Session Monitoring (SSM). The user activities such as creation, modification or deletion of files and User activities are captured under these logs.

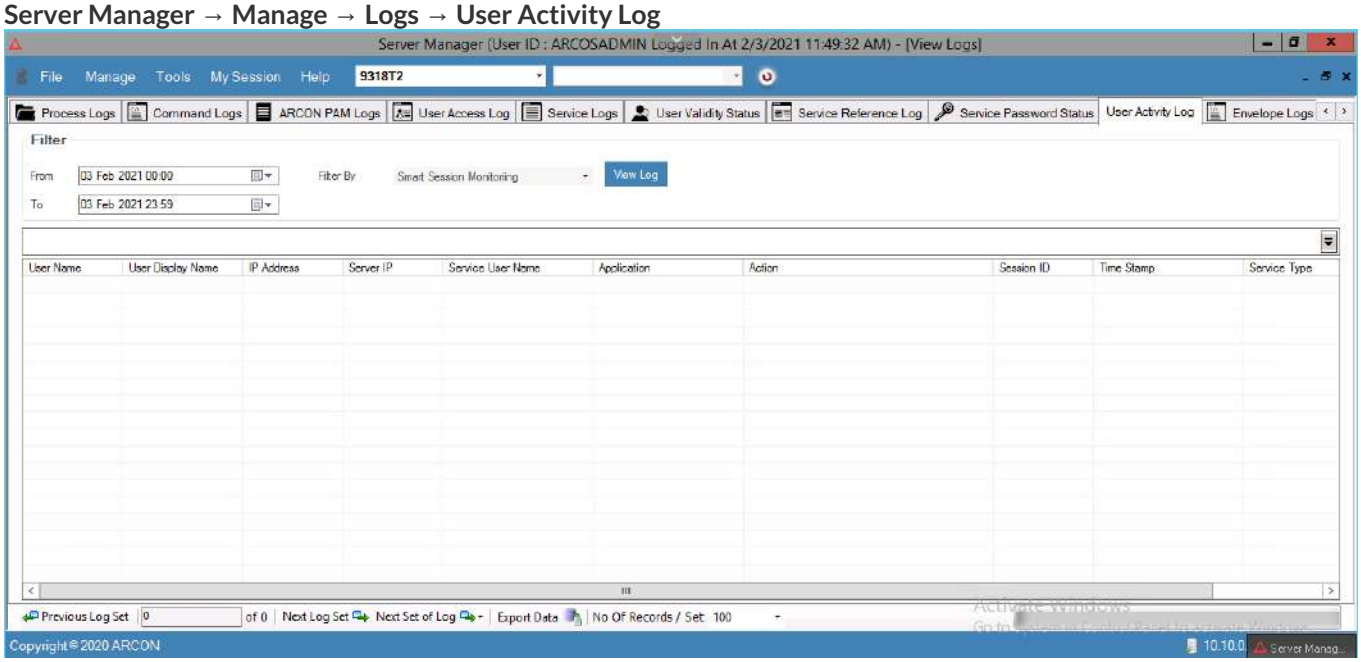
These logs display details such as name of User, machine details of User, IP Address of configured Server, application started on Server, action performed on Server, session ID, and date and time details of activity performed on Server.

- The Administrator having User Activity Log privilege in Server's Privileges will only be able to view User Activity Log under Logs (Server Manager > Manage > Logs > User Activity Logs)
- User having Smart Session Monitoring privilege in Client Manager's Privileges will be able to view User Activity Logs under File & SSM Profiles (CM > Manager > Smart Session Monitoring > File & SSM Profiles > User Activity Logs)

To generate User Activity Log in Server Manager:

To generate User Activity Log use the following path:

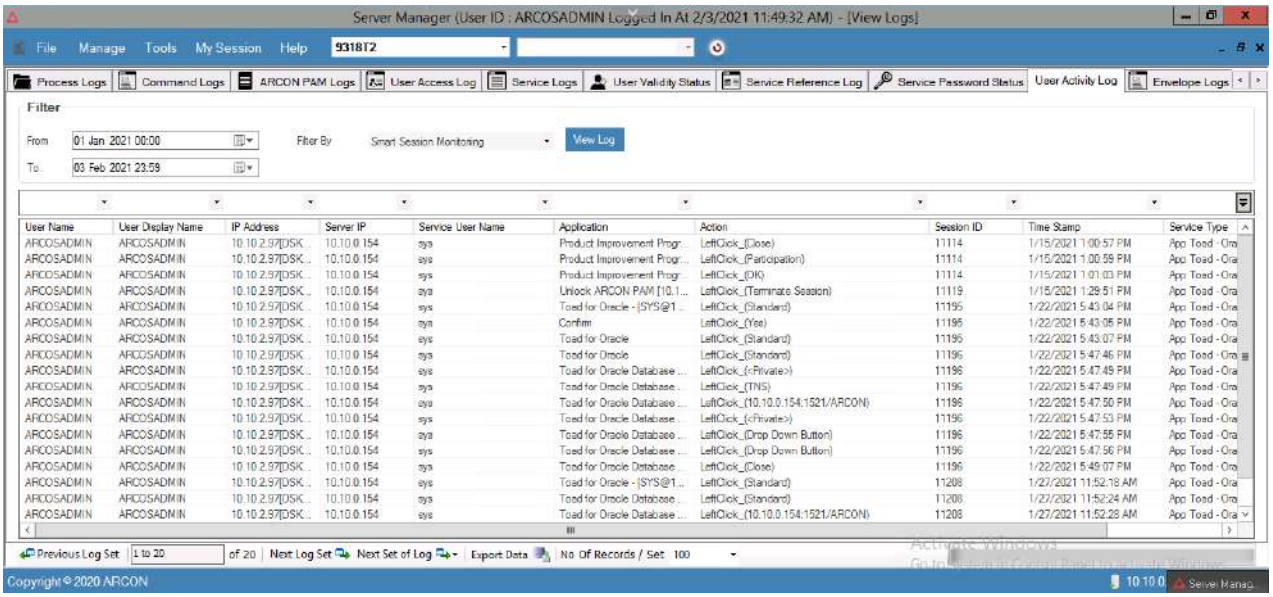
Server Manager → Manage → Logs → User Activity Log



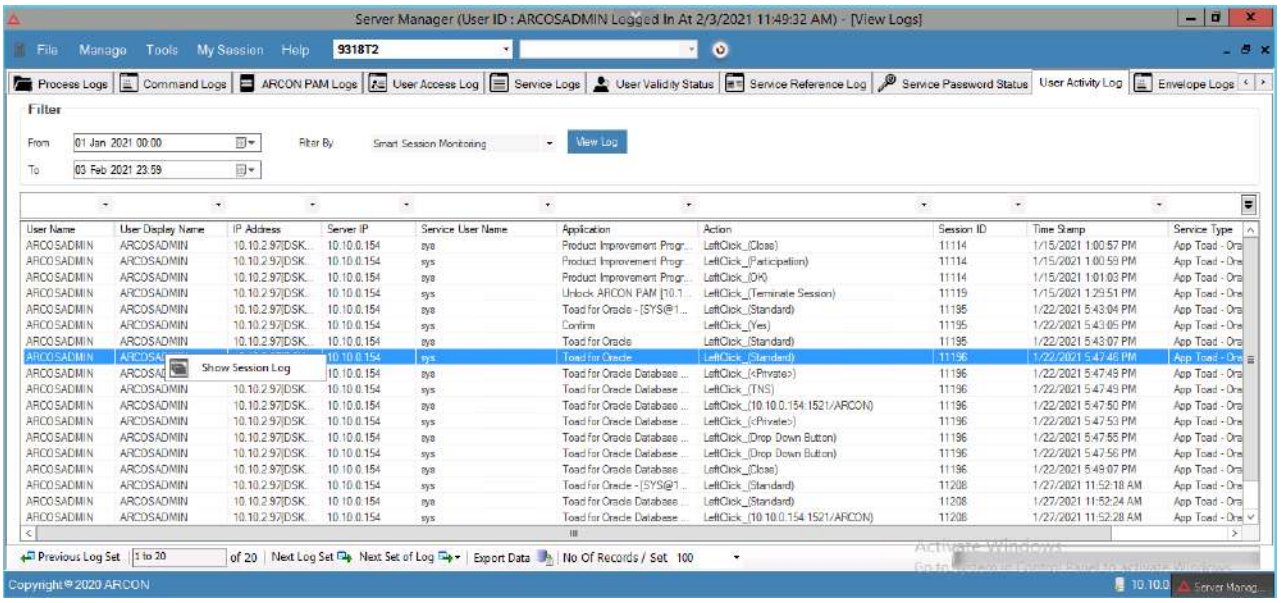
The **Filter** screen contains the following fields:

Field Name	Description
From	Select the start date, to generate logs.
To	Select the end date, until when you want to generate logs.
Filter By	Select the required option.

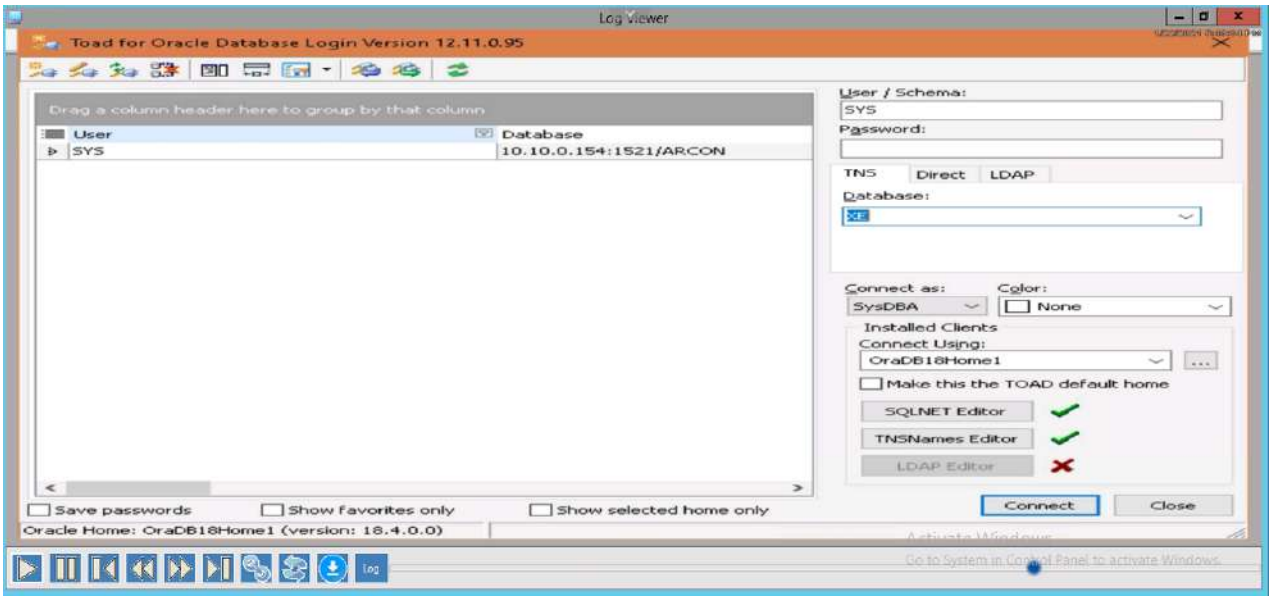
1. Select/Enter the fields and click **View Log** button. The logs are generated based on the selected filters.00 You can view either Smart Session Monitoring or File Watcher logs at a time.



2. Right click on the user activity log, to view video log. A **Show Session Log** option is popped up.



3. Click **Show Session Log** option. The **Log Viewer** screen is displayed to view video log.



The mouse click activities performed by User on Server are highlighted in red when you view video logs.

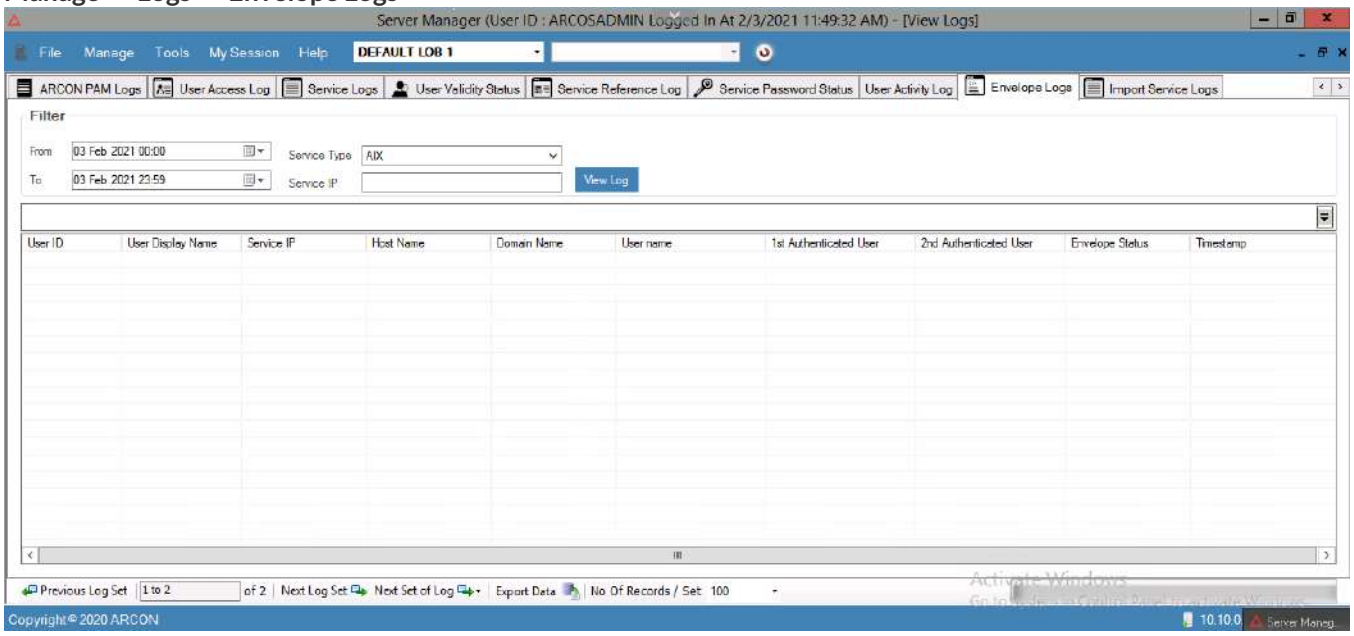
9.10 Envelope Logs

The Envelope Logs helps you to generate the detailed logs of the password generated for the authorized users. It displays details such as the User ID, User Display Name, Service IP, Host Name, Domain Name, User Name, 1st Authenticate User, 2nd Authenticated User, Envelope Status and Timestamp.

To generate the Envelope Logs:

To generate the envelope logs use the following path:

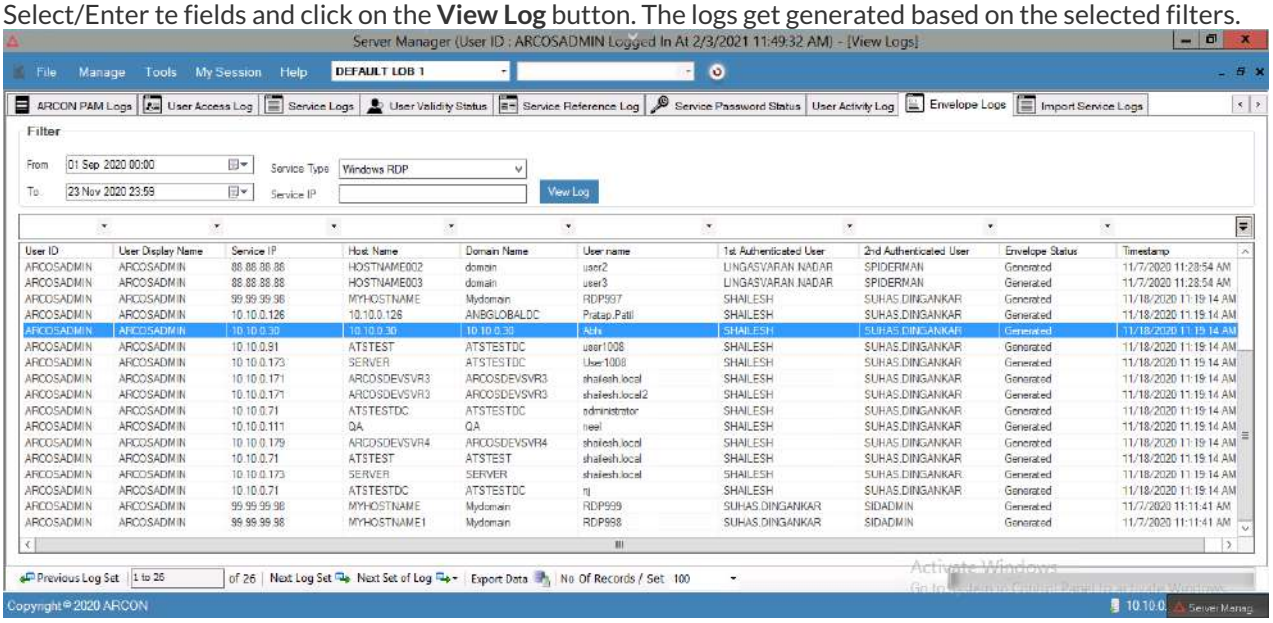
Manage → Logs → Envelope Logs



The filter screen contains the following fields:

Field Name	Description
From	Select the start date, to generate the logs.
To	Select the end date, until when you want to generate the logs.
Service Type	Select the service type from the dropdown list.
Service IP	Specify the Service IP, to filter the logs

1. Select/Enter te fields and click on the **View Log** button. The logs get generated based on the selected filters.



- To export logs into .xls format, click on Export Data button, which is present in the bottom of the screen.
- Click Previous Log Set, to view set of previous logs.
- Click Next Log Set, to view next set of logs.
- Click Next Set of Log, to view particular set of logs. Select the particular set from the Next Set of Log dropdown list.
- Select the number of records from No of Records/Set dropdown list, wherein it will display those many records in the grid.

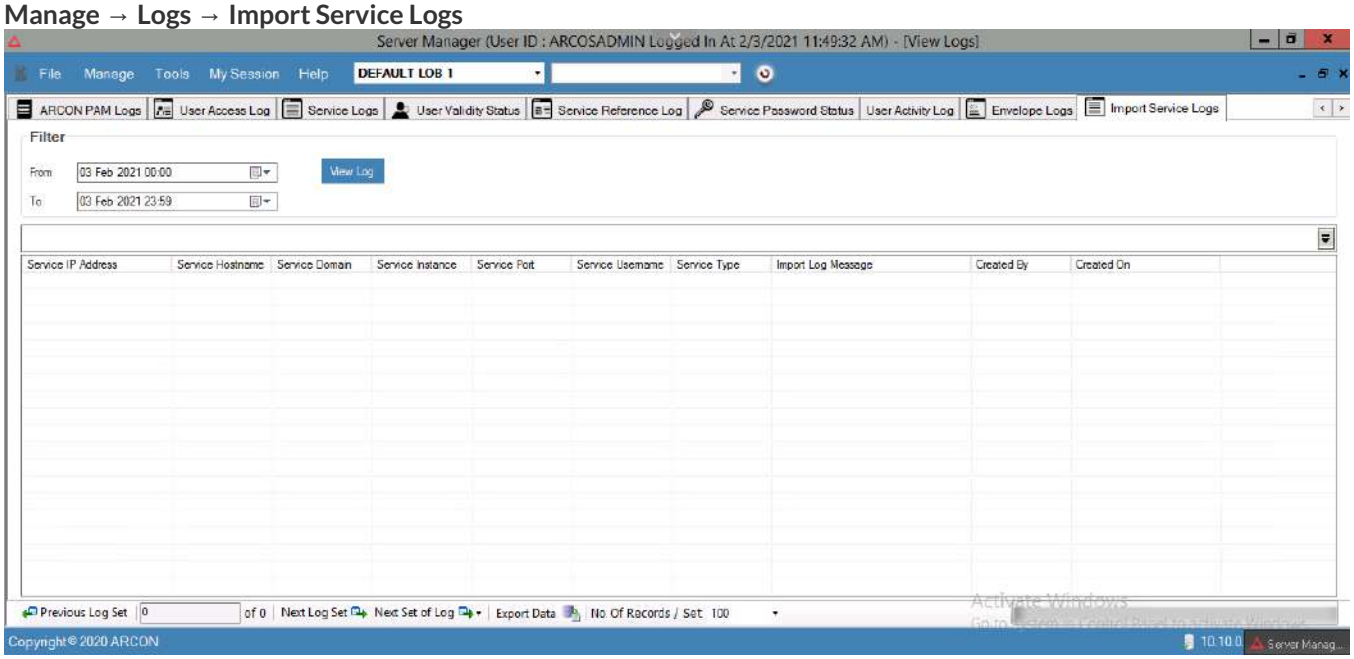
9.11 Import Service Logs

The Import Service Logs helps to generate the detailed logs of the imported services in the ARCON PAM Application. It displays the details such as Service IP Address, Service Hostname, Service Domain, Service Instance, Service Port, Service Username, Service type, Import Log Message, Created by and Created on.

To generate Import Service Logs:

To generate Import service logs use the following path:

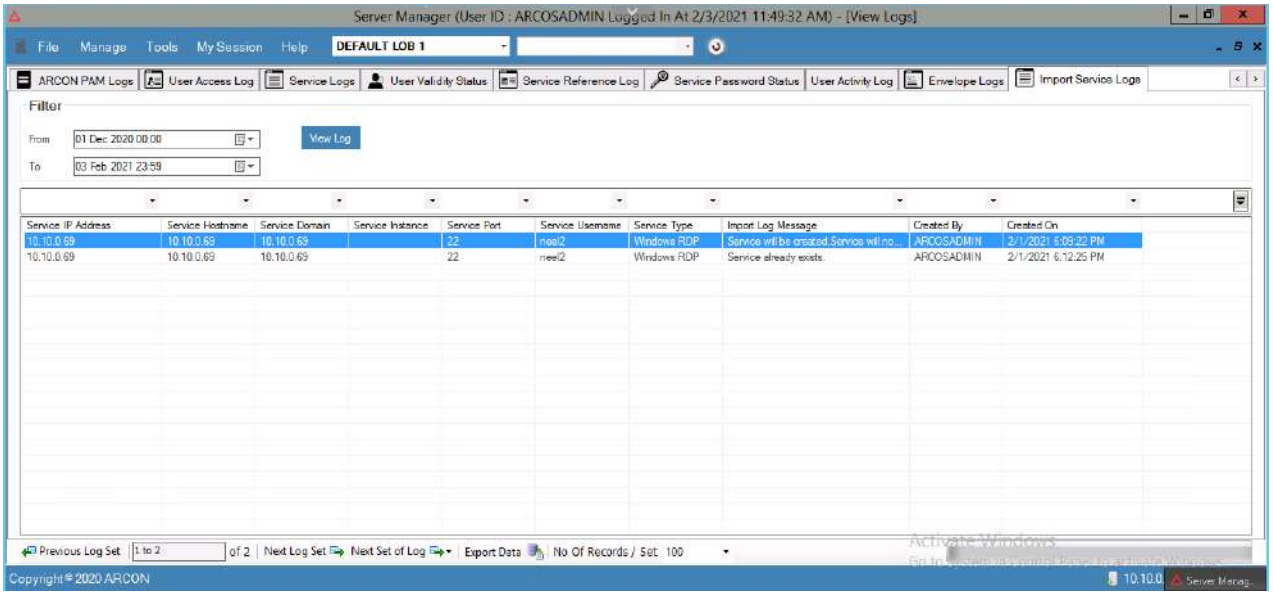
Manage → Logs → Import Service Logs



The **Filter** screen contains the following fields:

Field Name	Description
From	Select the start date, to generate logs.
To	Select the end date, until when you want to generate logs.

1. Select/Enter the fields and click on the **View Log** button. The logs gets generated based on the selected filters.



- To export logs into .xls format, click on Export Data button, which is present in the bottom of the screen.
- Click Previous Log Set, to view set of previous logs.
- Click Next Log Set, to view next set of logs.
- Click Next Set of Log, to view particular set of logs. Select the particular set from the Next Set of Log dropdown list.
- Select the number of records from No of Records/Set dropdown list, wherein it will display those many records in the grid.

9.12 Service Password Request Log

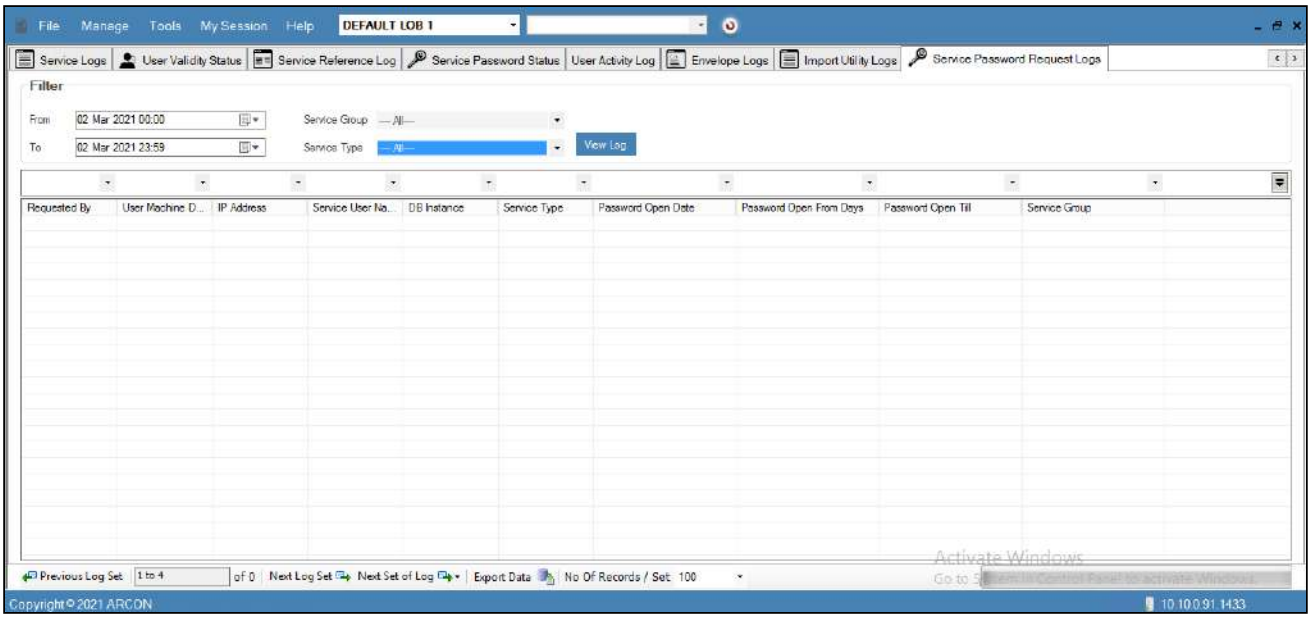
Service Password request log keeps a track of all the service password requests. It displays details like from where was the password requested(from ACMO, API, Server Manager, etc), User Machine Details(only in case when the request is made from API), IP Address, Service User Name, DB Instance, Service Type, Password Open Date, Password Open from days, Password open till, Service Group(comma separated values in case service is attached to multiple Service Groups).

The Administrator having **Service Password Request Log** privilege in Server's Privileges will only be able to view Service Password Request logs.

To generate Service Password Request log:

To generate the service password status log use the following path:

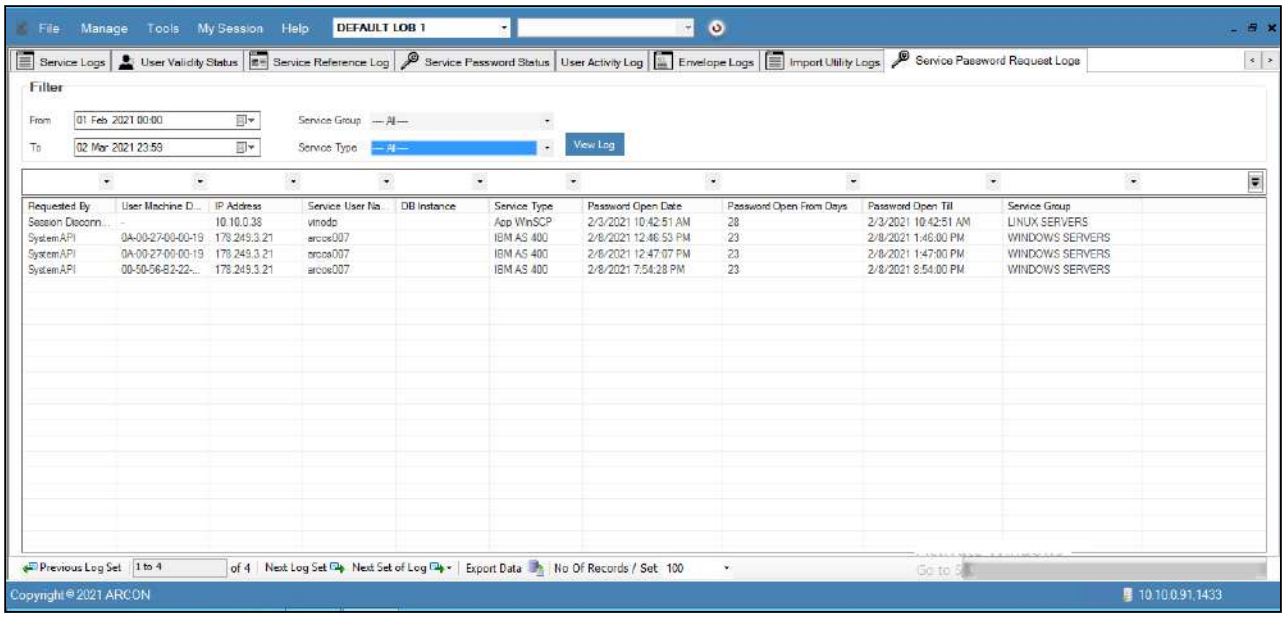
Manage → Logs → Service Password Request Logs



The **Filter** screen contains the following fields:

Field Name	Description
From	Select the start date, to generate logs.
To	Select the end date, till when you want to generate logs.
Service Group	Select the service group.
Service Type	Select the type of service.

1. Select/Enter the fields and click the **View Log** button. The logs are generated based on the selected filters.



- To export logs into .xls format, click on **Export Data** button, which is present in the bottom of the screen.
- Click Previous Log Set, to view the set of previous logs.
- Click Next Log Set, to view the next set of logs.
- Click Next Set of Log, to view a particular set of logs. Select the particular set from the **Next Set of Log** dropdown list.
- Select the number of records from **No of Records/Set** dropdown list, wherein it will display those many records in the grid.

9.13 Application Logs

Application Logs helps you to generate error logs of Client Manager application. In other words, it generates logs of invalid login attempts made by the user in Client Manager (CM) application. It displays details such as date and time, type of log, log data, information of log, log message, name of logger, name of logger machine, and version number.

The Administrator having **View Application Logs** privilege in Server's Privileges will only be able to view Application logs.

To generate Application Logs:

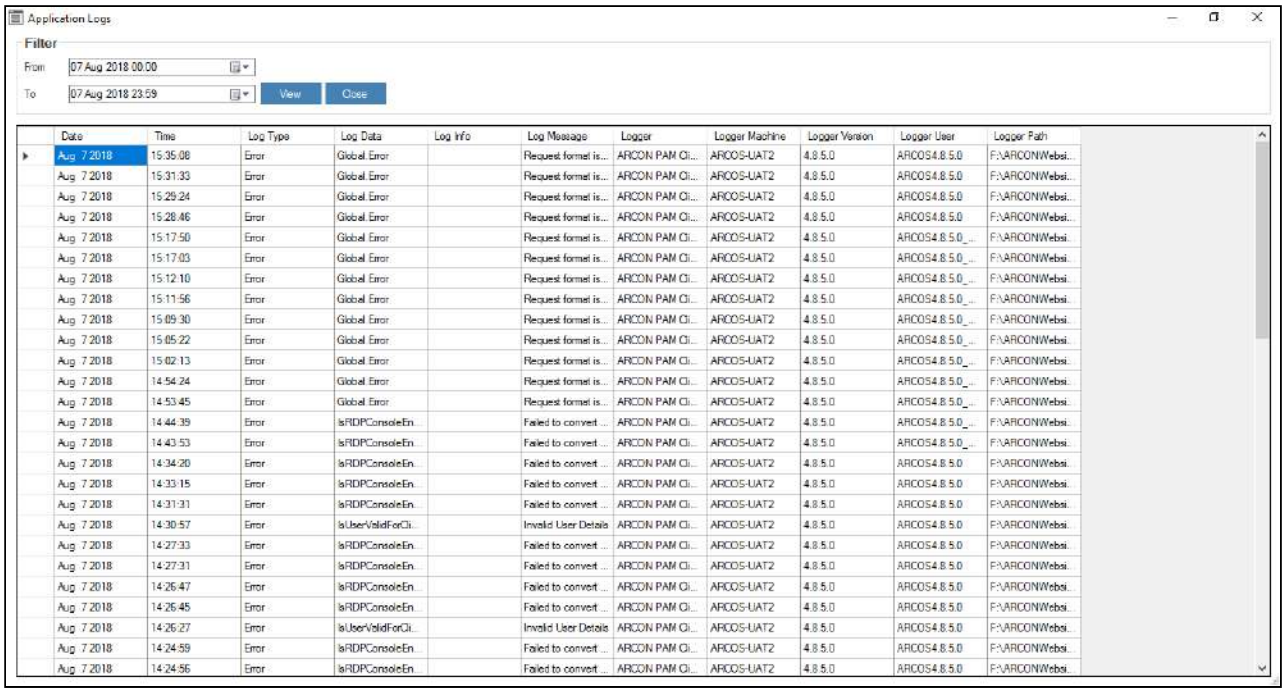
To generate application logs use the following path:

Manage → Application Logs

The **Filter** screen contains the following fields:

Field Name	Description
From	Select the start date, to generate logs.
To	Select the end date, until when you want to generate logs.

1. Select the fields and click **View** button. The logs are generated based on the selected filters.



Date	Time	Log Type	Log Data	Log Info	Log Message	Logger	Logger Machine	Logger Version	Logger User	Logger Path
Aug 7 2018	15:35:08	Error	Global.Error		Request format is...	ARCON PAM Cli...	ARCOS-UAT2	4.8.5.0	ARCOS4.8.5.0	F:\ARCONWebsi...
Aug 7 2018	15:31:33	Error	Global.Error		Request format is...	ARCON PAM Cli...	ARCOS-UAT2	4.8.5.0	ARCOS4.8.5.0	F:\ARCONWebsi...
Aug 7 2018	15:29:24	Error	Global.Error		Request format is...	ARCON PAM Cli...	ARCOS-UAT2	4.8.5.0	ARCOS4.8.5.0	F:\ARCONWebsi...
Aug 7 2018	15:28:46	Error	Global.Error		Request format is...	ARCON PAM Cli...	ARCOS-UAT2	4.8.5.0	ARCOS4.8.5.0	F:\ARCONWebsi...
Aug 7 2018	15:17:50	Error	Global.Error		Request format is...	ARCON PAM Cli...	ARCOS-UAT2	4.8.5.0	ARCOS4.8.5.0_...	F:\ARCONWebsi...
Aug 7 2018	15:17:03	Error	Global.Error		Request format is...	ARCON PAM Cli...	ARCOS-UAT2	4.8.5.0	ARCOS4.8.5.0_...	F:\ARCONWebsi...
Aug 7 2018	15:12:10	Error	Global.Error		Request format is...	ARCON PAM Cli...	ARCOS-UAT2	4.8.5.0	ARCOS4.8.5.0_...	F:\ARCONWebsi...
Aug 7 2018	15:11:56	Error	Global.Error		Request format is...	ARCON PAM Cli...	ARCOS-UAT2	4.8.5.0	ARCOS4.8.5.0_...	F:\ARCONWebsi...
Aug 7 2018	15:09:30	Error	Global.Error		Request format is...	ARCON PAM Cli...	ARCOS-UAT2	4.8.5.0	ARCOS4.8.5.0_...	F:\ARCONWebsi...
Aug 7 2018	15:05:22	Error	Global.Error		Request format is...	ARCON PAM Cli...	ARCOS-UAT2	4.8.5.0	ARCOS4.8.5.0_...	F:\ARCONWebsi...
Aug 7 2018	15:02:13	Error	Global.Error		Request format is...	ARCON PAM Cli...	ARCOS-UAT2	4.8.5.0	ARCOS4.8.5.0_...	F:\ARCONWebsi...
Aug 7 2018	14:54:24	Error	Global.Error		Request format is...	ARCON PAM Cli...	ARCOS-UAT2	4.8.5.0	ARCOS4.8.5.0_...	F:\ARCONWebsi...
Aug 7 2018	14:53:45	Error	Global.Error		Request format is...	ARCON PAM Cli...	ARCOS-UAT2	4.8.5.0	ARCOS4.8.5.0_...	F:\ARCONWebsi...
Aug 7 2018	14:44:39	Error	isRDPConsoleEn...		Failed to convert ...	ARCON PAM Cli...	ARCOS-UAT2	4.8.5.0	ARCOS4.8.5.0_...	F:\ARCONWebsi...
Aug 7 2018	14:43:53	Error	isRDPConsoleEn...		Failed to convert ...	ARCON PAM Cli...	ARCOS-UAT2	4.8.5.0	ARCOS4.8.5.0_...	F:\ARCONWebsi...
Aug 7 2018	14:34:20	Error	isRDPConsoleEn...		Failed to convert ...	ARCON PAM Cli...	ARCOS-UAT2	4.8.5.0	ARCOS4.8.5.0	F:\ARCONWebsi...
Aug 7 2018	14:33:15	Error	isRDPConsoleEn...		Failed to convert ...	ARCON PAM Cli...	ARCOS-UAT2	4.8.5.0	ARCOS4.8.5.0	F:\ARCONWebsi...
Aug 7 2018	14:31:31	Error	isRDPConsoleEn...		Failed to convert ...	ARCON PAM Cli...	ARCOS-UAT2	4.8.5.0	ARCOS4.8.5.0	F:\ARCONWebsi...
Aug 7 2018	14:30:57	Error	isUserValidForCli...		Invalid User Details	ARCON PAM Cli...	ARCOS-UAT2	4.8.5.0	ARCOS4.8.5.0	F:\ARCONWebsi...
Aug 7 2018	14:27:33	Error	isRDPConsoleEn...		Failed to convert ...	ARCON PAM Cli...	ARCOS-UAT2	4.8.5.0	ARCOS4.8.5.0	F:\ARCONWebsi...
Aug 7 2018	14:27:31	Error	isRDPConsoleEn...		Failed to convert ...	ARCON PAM Cli...	ARCOS-UAT2	4.8.5.0	ARCOS4.8.5.0	F:\ARCONWebsi...
Aug 7 2018	14:26:47	Error	isRDPConsoleEn...		Failed to convert ...	ARCON PAM Cli...	ARCOS-UAT2	4.8.5.0	ARCOS4.8.5.0	F:\ARCONWebsi...
Aug 7 2018	14:26:45	Error	isRDPConsoleEn...		Failed to convert ...	ARCON PAM Cli...	ARCOS-UAT2	4.8.5.0	ARCOS4.8.5.0	F:\ARCONWebsi...
Aug 7 2018	14:26:27	Error	isUserValidForCli...		Invalid User Details	ARCON PAM Cli...	ARCOS-UAT2	4.8.5.0	ARCOS4.8.5.0	F:\ARCONWebsi...
Aug 7 2018	14:24:59	Error	isRDPConsoleEn...		Failed to convert ...	ARCON PAM Cli...	ARCOS-UAT2	4.8.5.0	ARCOS4.8.5.0	F:\ARCONWebsi...
Aug 7 2018	14:24:56	Error	isRDPConsoleEn...		Failed to convert ...	ARCON PAM Cli...	ARCOS-UAT2	4.8.5.0	ARCOS4.8.5.0	F:\ARCONWebsi...

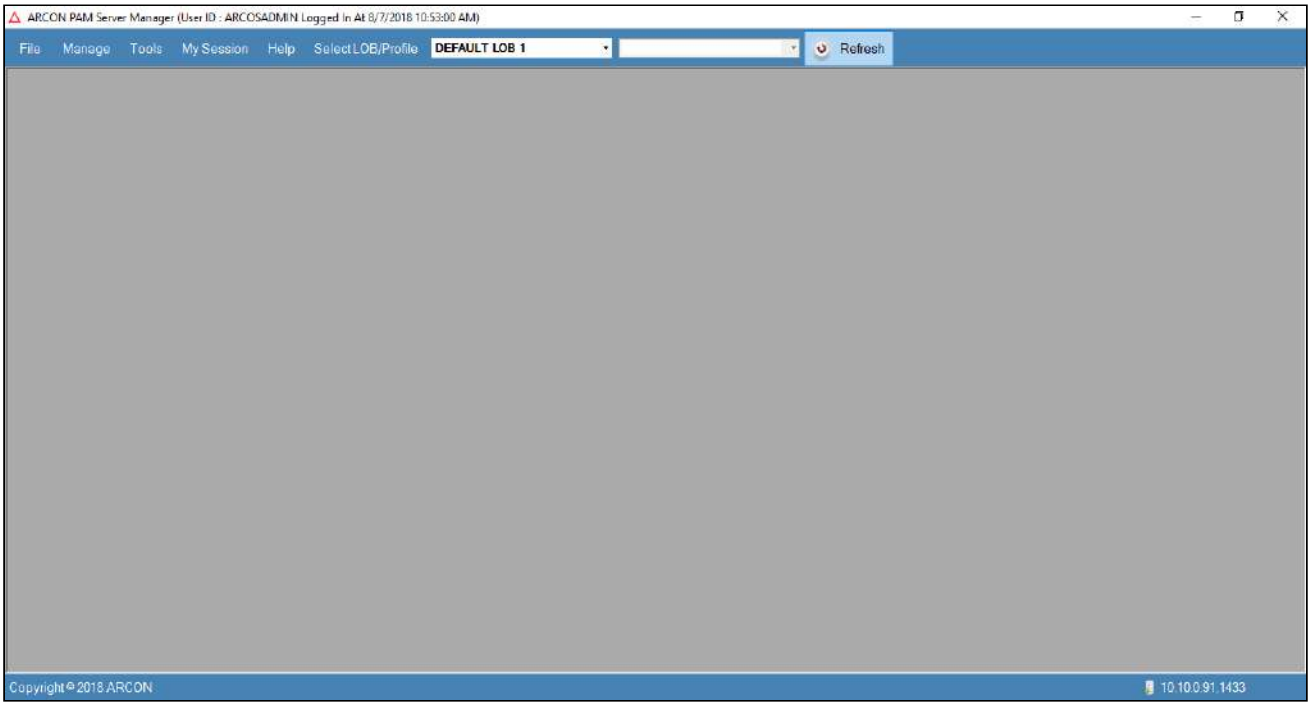
2. View the logs generated.

10 Refresh Access Rights

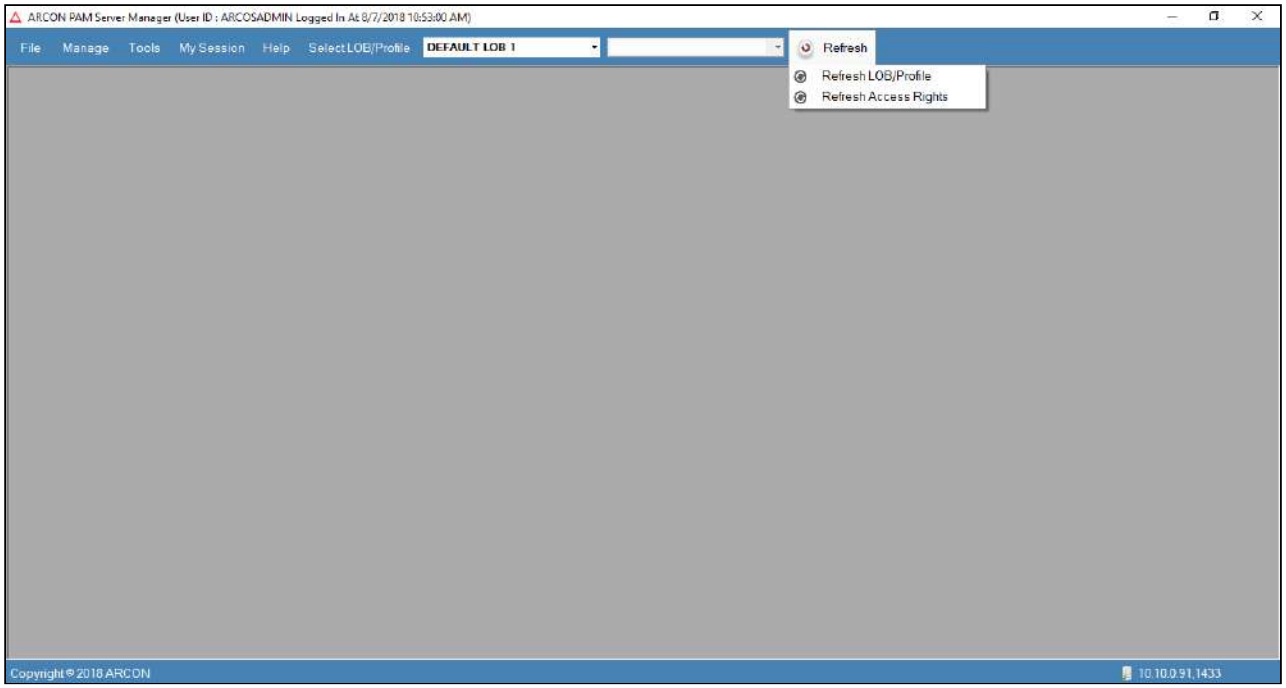
Refresh feature is used to refresh the settings configured by the Admin User. It can be used when the changes modified by the Administrator are not reflected in the system or to refresh LOB/Profile.

To navigate to Refresh menu, use the following path:

Server Manager → Refresh



1. Click **Refresh** to display **Refresh LOB/Profile** and **Refresh Access Rights** options.



- Select **Refresh LOB/Profile** to display Default LOB in **Select LOB/Profile** drop down.
- Select **Refresh Access Rights** to refresh settings configured by Administrator.

11 Tool Management

Server Manager provides various tools from where the Admin user can perform different types of activities.

This section includes the following topics:

- ARCOS Object Counter
- Import Utility
- Privilege User Discovery and Reconciliation
- ARCOS PerfMonIT Configuration
- Discovered Devices
- Real Time Session Monitoring
- Windows Utility
- Refresh
- My Session Menu
- About
- Registration Form

11.1 Import Utility

Import Utility allows bulk import of users and services into ARCON PAM database. ARCON PAM provides templates for defining data related to users and services for uploading through Import Utility. Import Utility reads data from the .txt file and imports it into ARCON PAM.

> ⚠ The Administrator having **Import** privilege in Server's Privilege will only be able to import Users and Services in ARCON PAM database.

The Import Utility provides following options:

- Import Server Connections
- Update Server Connections
- Import Windows Services
- Change DMZ Gateway
- Import Users
- User Server Mapping
- Import User Groups
- Import Service Groups
- Import User Group Server Group

The following path is used to import users and services:

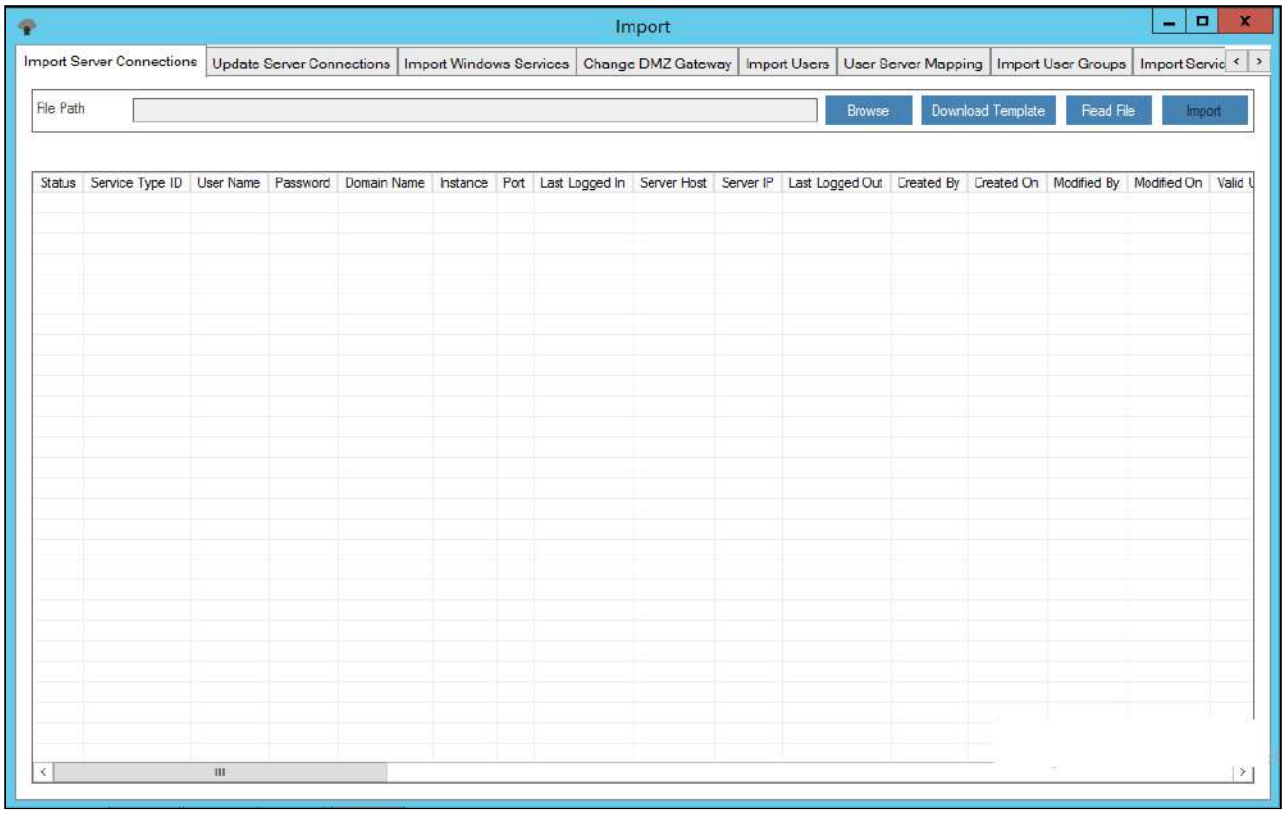
Tools → Import

11.1.1 Import Server Connections

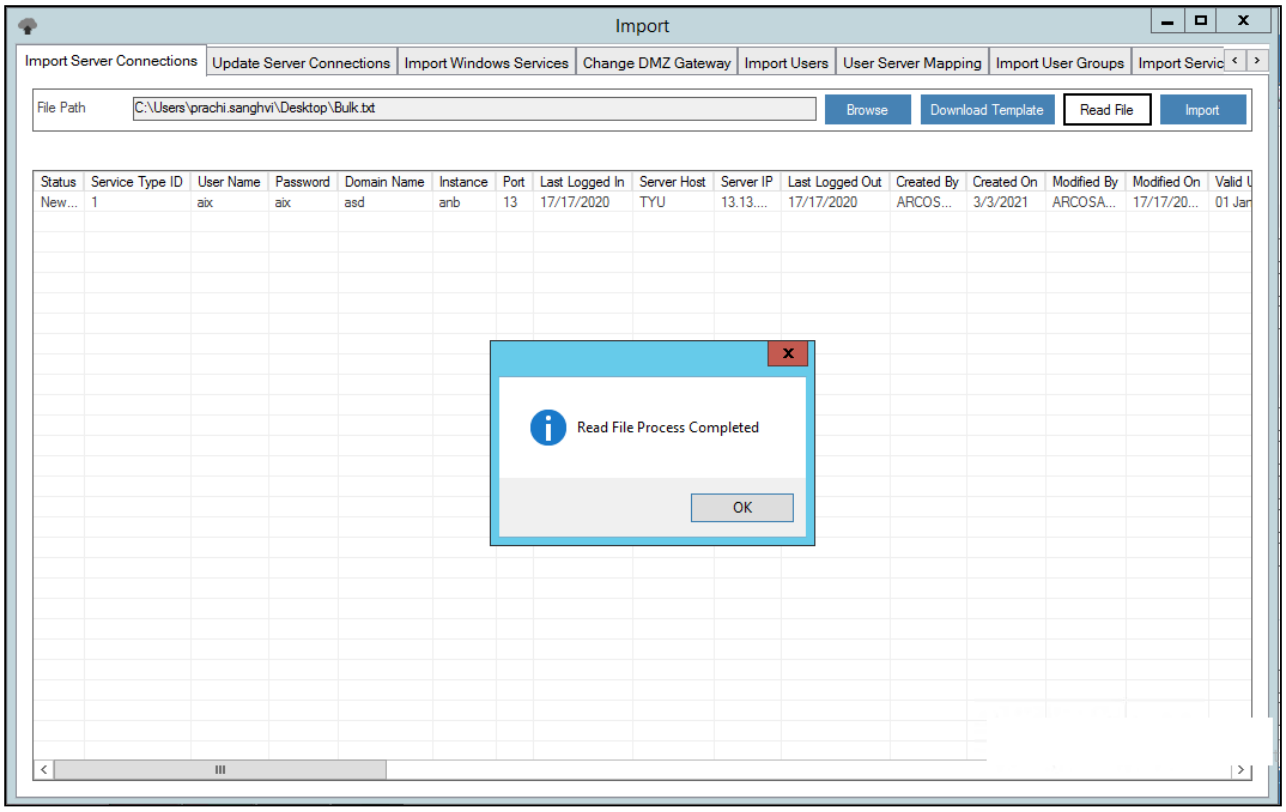
Import Server Connections tab is used for importing new services in ARCON PAM. These services will be reflected under Manage Services in Server Manager after they are assigned to the required LOB.

Process for Importing Users :

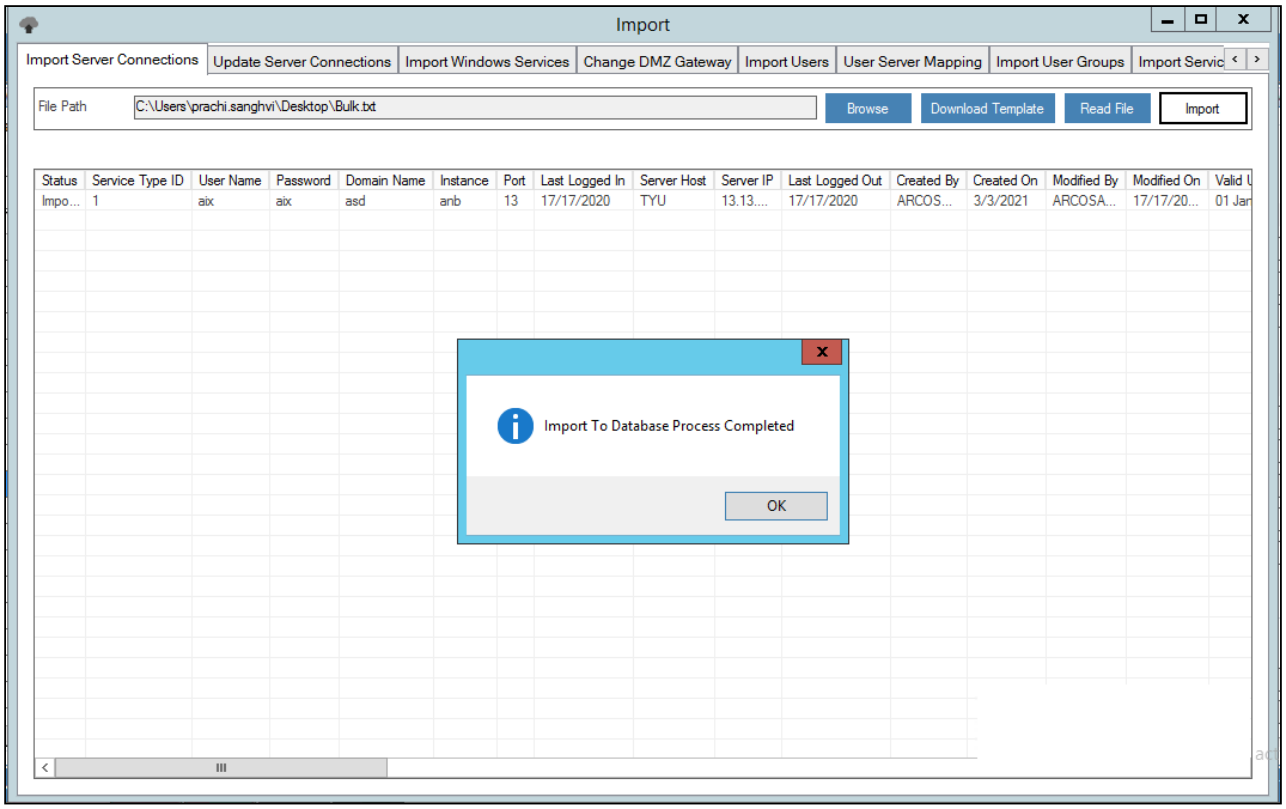
1. Login to **Server Manager → Tools → Import → Import Server connection** tab is opened.



2. Now, the data should be imported in the .txt format in the following manner.
    a. Click **Download Template Button.**
    b. The Admin user has to enter the desired data into a predefined excel template.
    c. The data entered in the excel template should be left-aligned.
    d. The data from the excel template is copied to the text file.
    e. The text file is then used to import the desired data into ARCON PAM.
3. Select **Browse** tab → browse for the .txt file → click **Read File** button. This will read all the services details from the .txt file and is displayed in the grid.



4. Verify the details and click **Import** button. The service is imported into the ARCON PAM database.
5. Check the status in the first column, it shows **Import Success**.



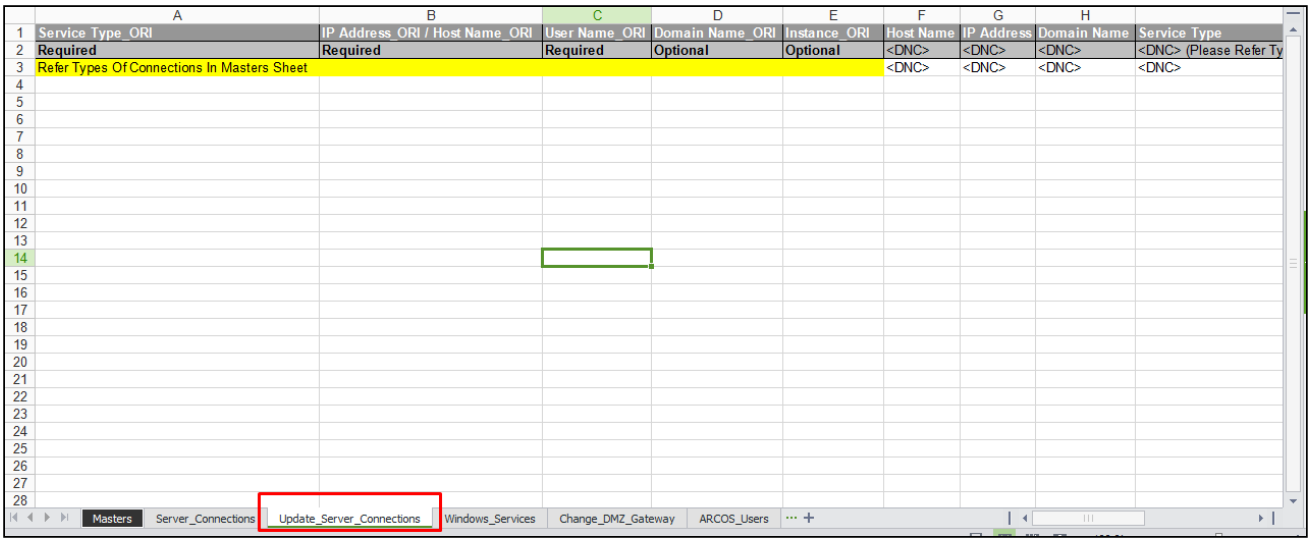
6. Map the imported services to a particular LOB and you will view the services under **Manage Services** tab.

> ⚠ Once a service is successfully imported, you need to then map the service to a particular LOB. In some cases, wherein an Administrator having Settings privileges has configured the value for the **LOB Wise Service Management - Is Enabled** option, where
>
> - **LOB Wise Service Management - Is Enabled** toggle value is **Enabled**, then it states that when a service is imported, it will directly map the service to the selected LOB from Select **LOB/ Profile** drop-down list, once it is imported.
> - **LOB Wise Service Management - Is Enabled** toggle value is **Disabled**, then it states that the service imported needs to be mapped to a particular LOB in **LOB/Profile Master & Manager**.
>
> By default, the value is Disabled.

11.1.2 Update Server Connections

Update Server Connections is used for updating details of existing services configured in ARCON PAM such as username, IP Address, Hostname, Domain Name, Service Type, and Description. The updated details are reflected under Manage Services screen.

A predefined MS-Excel template for gathering data is provided.



	A	B	C	D	E	F	G	H	
1	Service Type_ORI	IP Address_ORI / Host Name_ORI	User Name_ORI	Domain Name_ORI	Instance_ORI	Host Name	IP Address	Domain Name	Service Type
2	Required	Required	Required	Optional	Optional	<DNC>	<DNC>	<DNC>	<DNC> (Please Refer Ty
3	Refer Types Of Connections In Masters Sheet					<DNC>	<DNC>	<DNC>	<DNC>

Masters | Server_Connections | Update_Server_Connections | Windows_Services | Change_DMZ_Gateway | ARCOS_Users

Process for Updating Services is as follows:

1. The sheet Update_Server_Connections is used for Updating Services.
2. Enter Original Service details under Service Type_ORI, IP Address_ORI / Host Name_ORI, User Name_ORI columns. Using these parameters, service is recognized by ARCON PAM.
3. <DNC> tag stands for "Do Not Change". Enter revised details only under those columns in which respective parameters of the service need to be changed. For columns where there no change is required enter <DNC> tag. The cells with <DNC> tag will not change the value of the respective parameters of the service. Description of column headers are as follows:

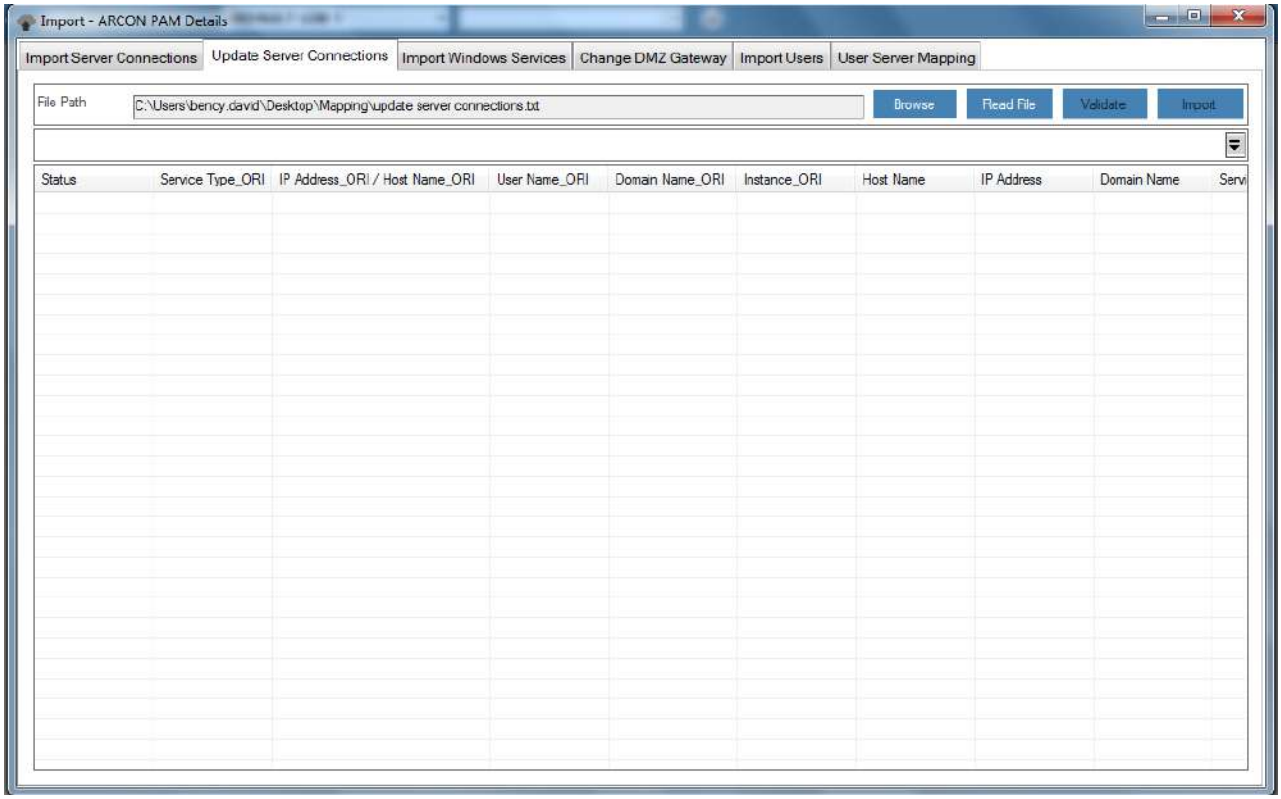
Field Name	Description
*Service Type_ORI	Enter Service Type ID referring to Masters sheet.
*IP Address_ORI / Host Name_ORI	Enter original IP Address / HostName of service to be updated.
*User Name_ORI	Enter original User Name of service to be updated.
Domain Name_ORI	Enter Original Domain Name details in this field or keep it blank. This is optional field.
Instance_ORI	Enter Original Instance details in this field or keep it blank. This is optional field.
Host Name	Enter new Host Name for Service or enter <DNC> in this field.
IP Address	Enter new IP Address for Service or enter <DNC> in this field.
Domain Name	Enter new Domain Name for Service or enter <DNC> in this field.
Service Type	Enter Service Type for Service or enter <DNC> in this field.
Service Options	Enter Service Options (True or False) for Service or enter <DNC> in this field.
Instance	Enter new Instance for Service or enter <DNC> in this field.
Port No	Enter new Port no. for Service or enter <DNC> in this field.

Field Name	Description
User Name	Enter new User Name for Service or enter <DNC> in this field.
Password	Enter new Password for Service or enter <DNC> in this field.
Valid Till Date	Enter new Valid Till Date for Service or enter <DNC> in this field.
Description 1	Enter new Description 1 (OS Version) for Service or enter <DNC> in this field.
Description 2	Enter new Description 2 (Server Description) for Service or enter <DNC> in this field.
Description 3	Enter new Description 3 (Location of Server) for Service or enter <DNC> in this field.
Parameter	Enter Tags for Service or enter <DNC> in this field.

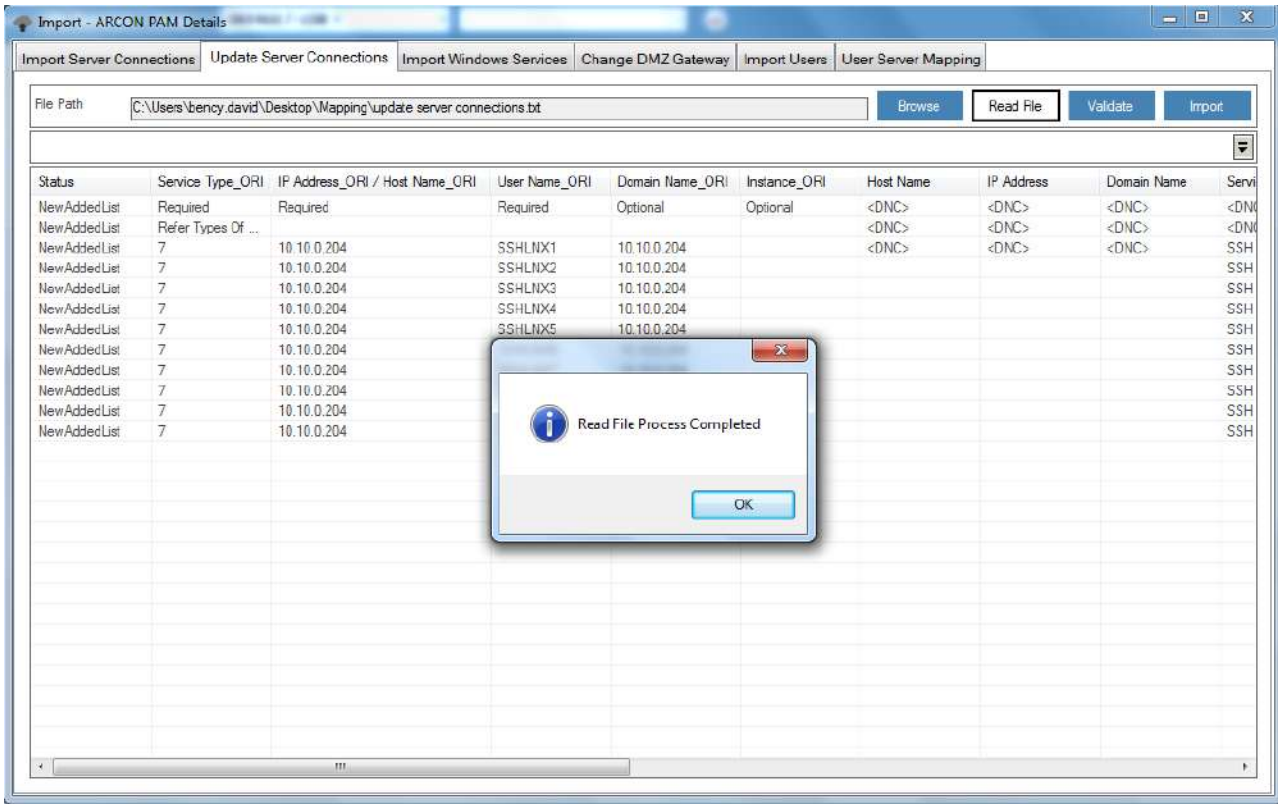
4. The details entered in Template should not contain space or special characters.
5. Copy the details from Master Sheet to notepad and save it to .txt format.
6. The text file is then used to import the desired data into ARCON PAM.

Import Text file into ARCON PAM

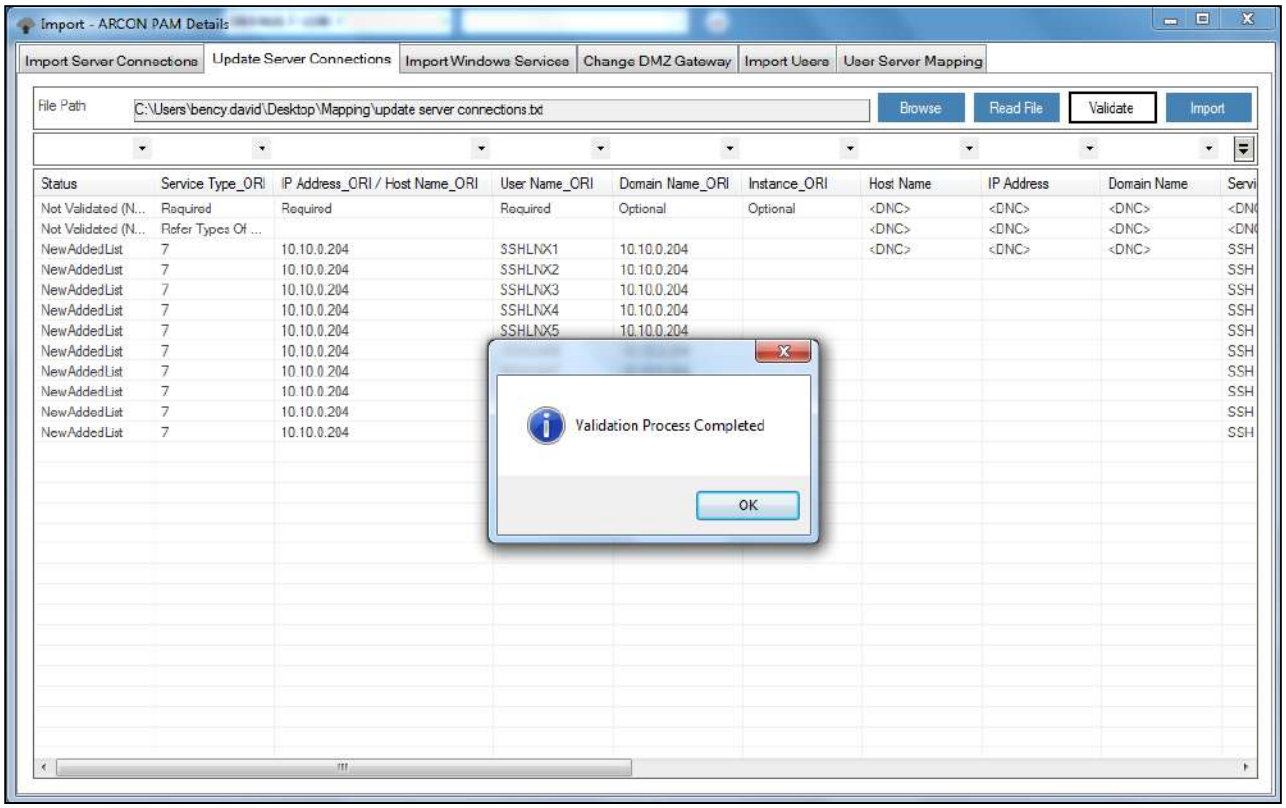
1. Login to **Server Manager** → **Tools** → **Import** → Select **Update Server Connections** tab → Click **Browse** → Select the location of the .txt file.



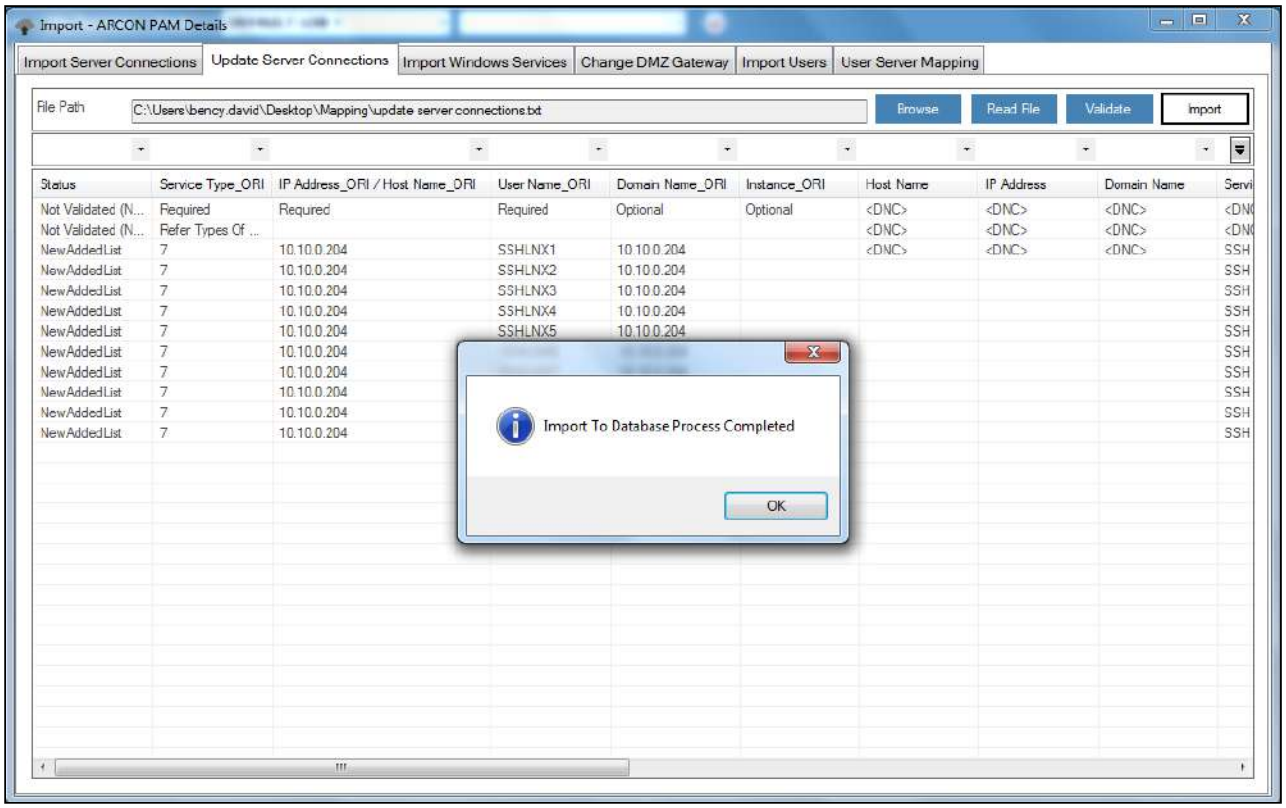
2. Click **Read File** button. A window pops up with the following message:
   Read File Process Completed
3. Click **OK**. The details are displayed in the grid.



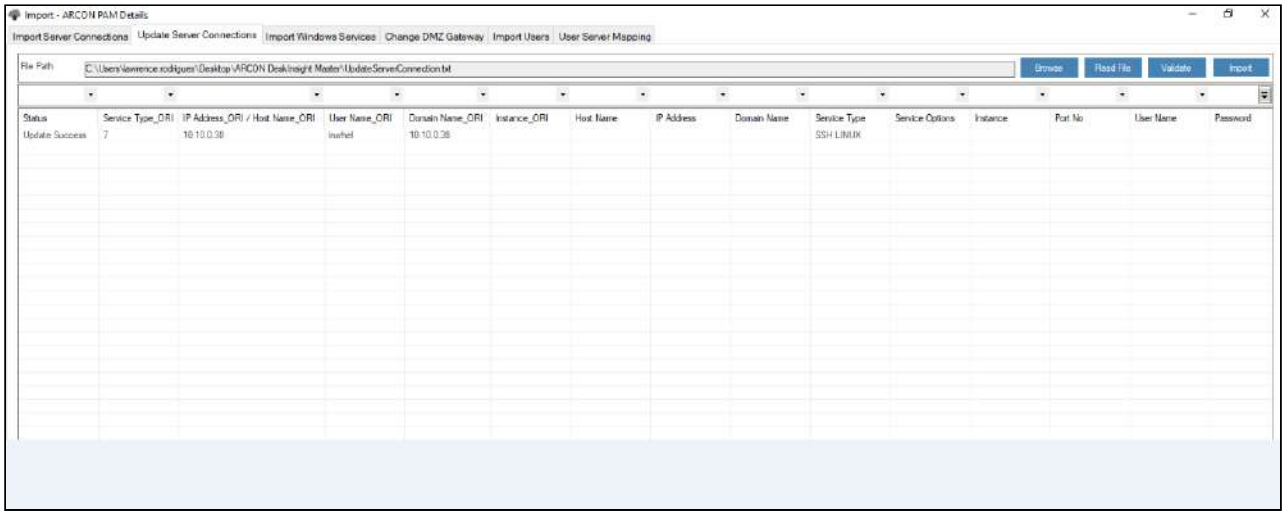
4. Click **Validate** button to validate whether the imported service exists in ARCON PAM or not. A window pops up with the following message:
   Validation Process Completed.
5. Click **OK** button. The status is updated to **Validated**.



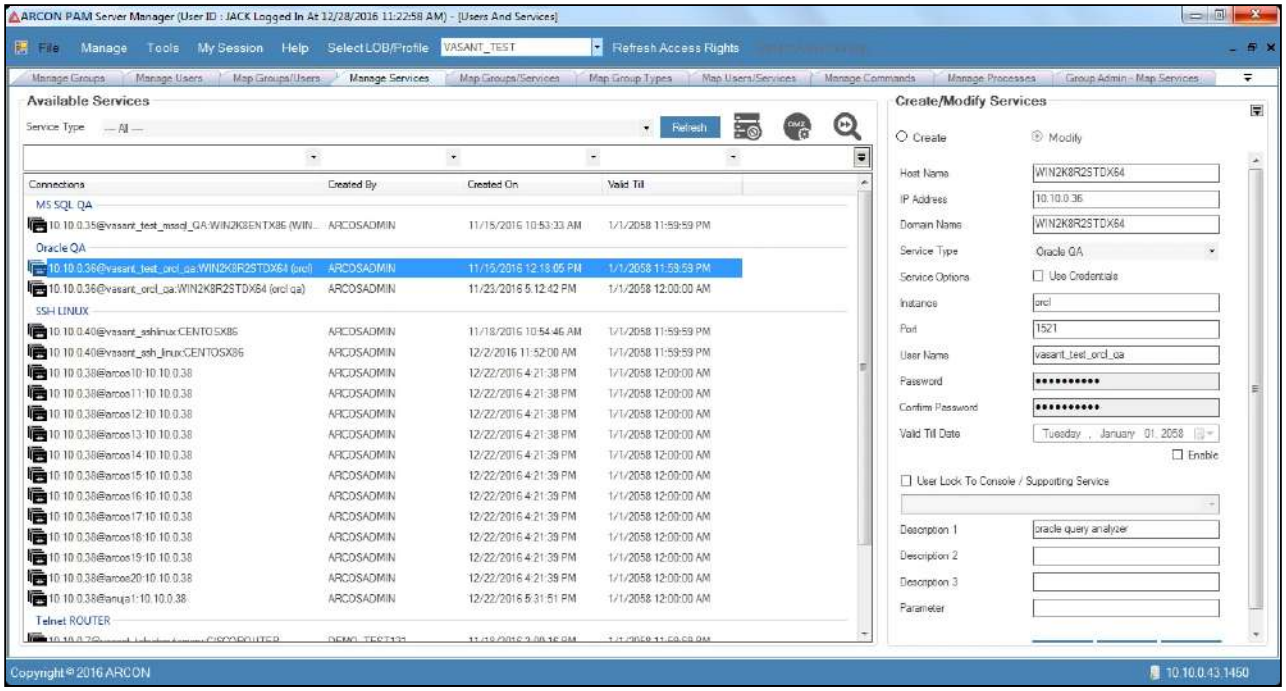
6. Click **Import** button. A window pops up with the following message:
   Import To Database Process Completed.



7. Click **OK**. The status is updated to **Update Success**.



8. The updated service will be displayed in **Manage Services** screen.

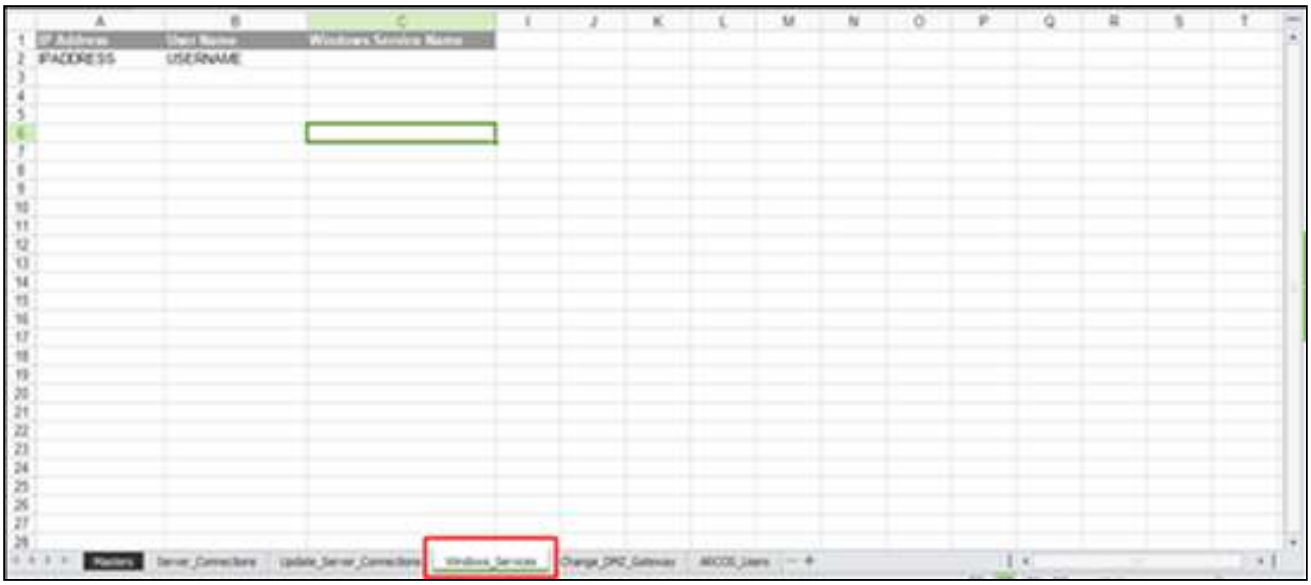


> ⚠ If toggle value for **Bulk Update Server Password** in **Settings** is **Enabled**, then you can update the password of Services whereas if the value is **Disabled**, then you cannot update the password of Services. Bulk update excel supports across LOBs using bulk Import Utility in a single excel upload.

11.1.3 Import Windows Services

Import Windows Services is used to import multiple Windows Services that are dependent on a particular privileged account and are integrated into ARCON PAM. This reduces the tedious job of creating Windows Services one-by-one in 'Windows Connection Password Dependency' option.

A predefined MS-Excel template for gathering data is provided.

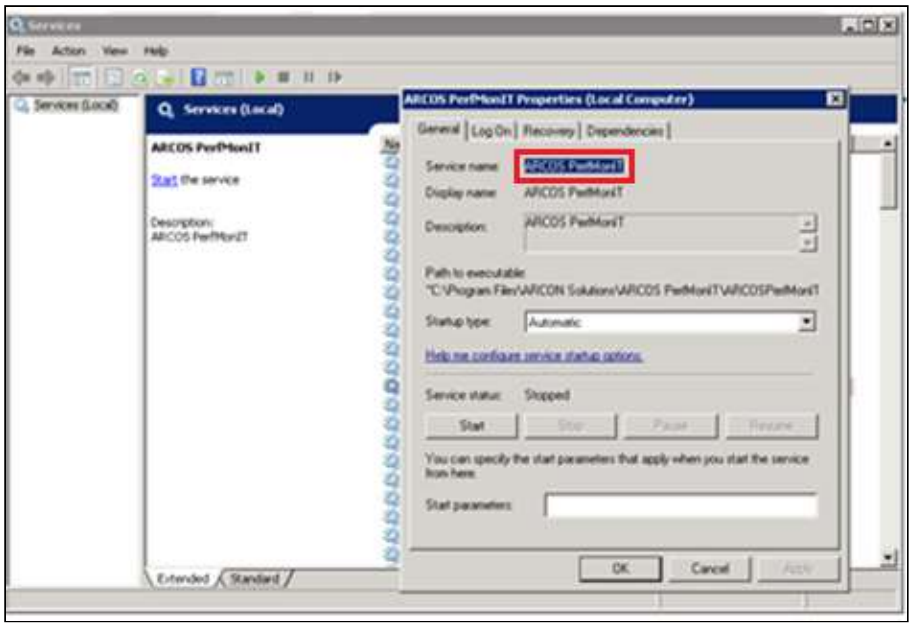


The description of column headers are as follows:

Field Name	Description
IP Address	Enter IP Address of Existing Service.
Username	Enter Username of Existing Service.
Windows Service Name	Enter Windows Service Name.

Process for Importing Windows Service are as follows:

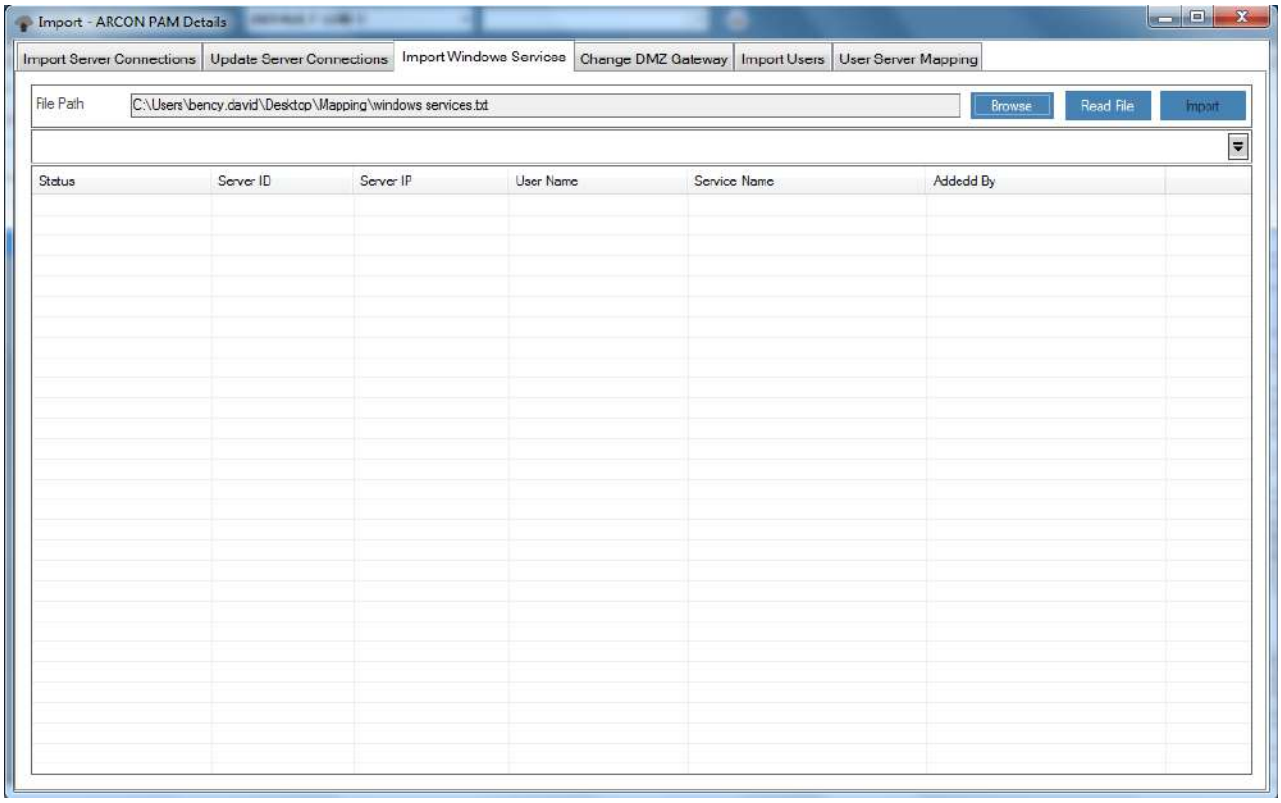
1. For Windows Service Name, login to Server where service is installed.
2. Go to “Services.msc”. Select the service, right click on select Properties.
3. Enter the Service Name displayed in properties under WindowsServiceName column in Template.



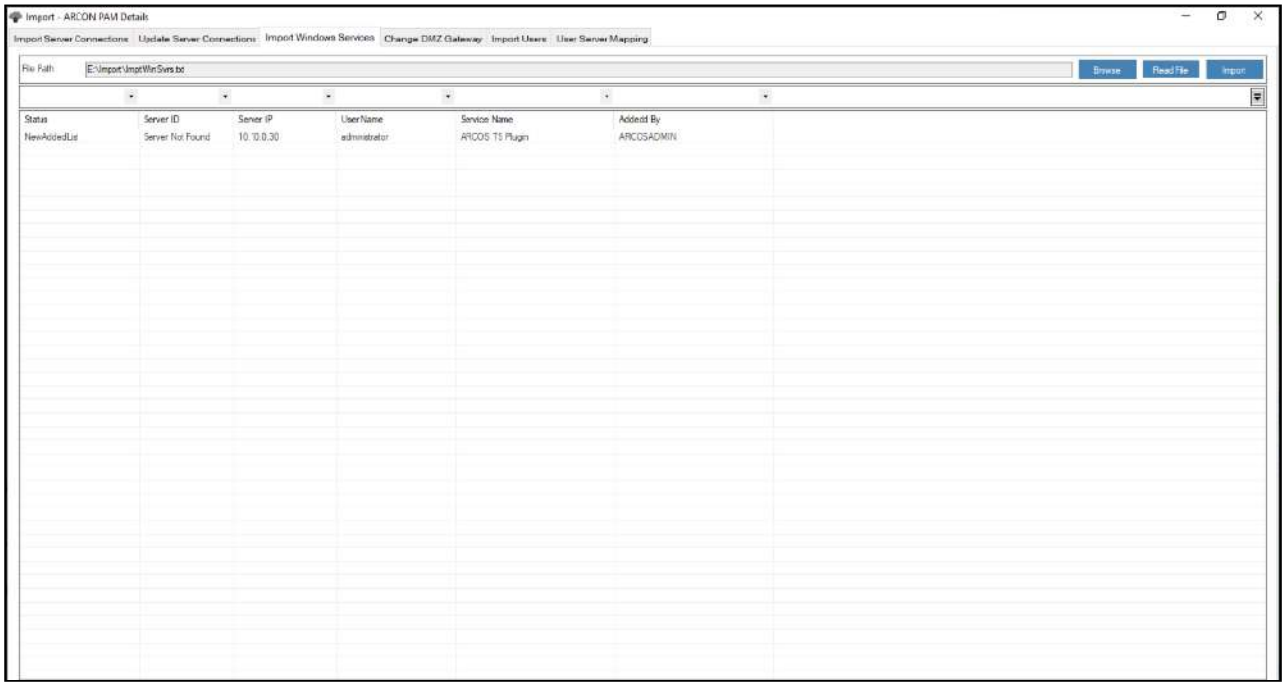
4. The details entered in Template should not contain space or special characters.
5. Copy the details from Master Sheet to notepad and save the file to .txt format.
6. The text file is then used to import the desired data into ARCON PAM.

Import Text File into ARCON PAM:

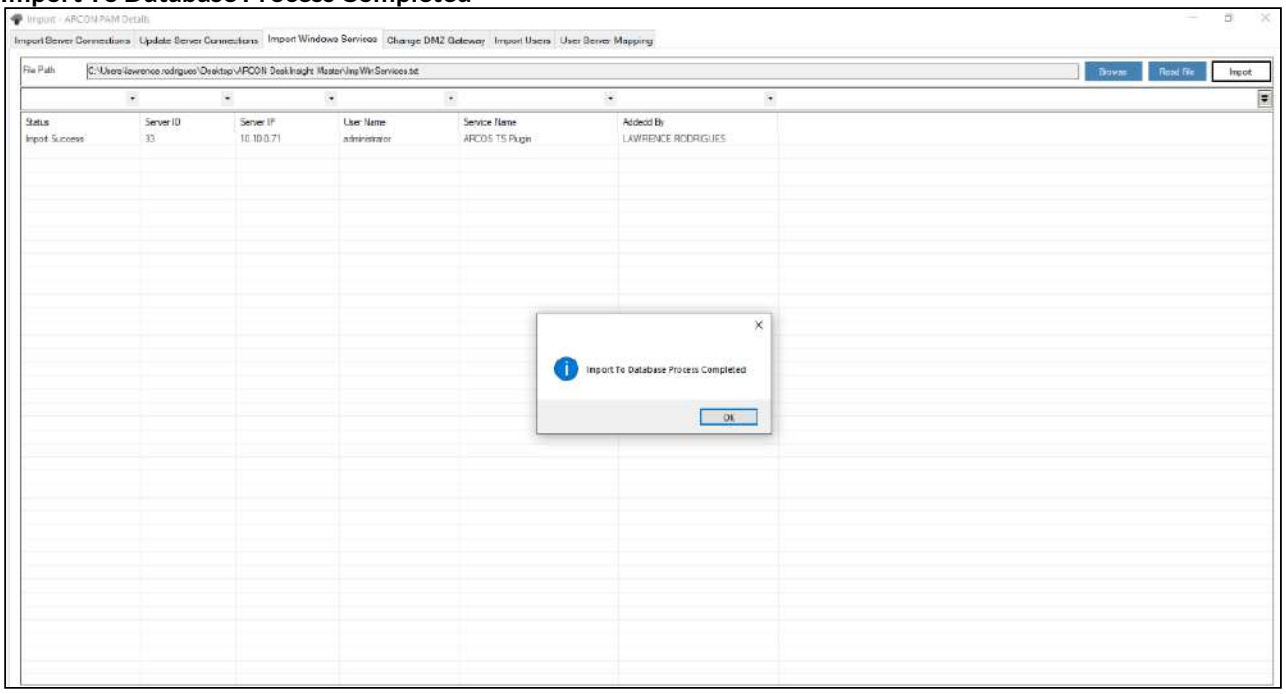
1. Login to **Server Manager** → **Tools** → **Import** → Select **Import Windows Services** tab → Click **Browse** → Select the location of .txt file.



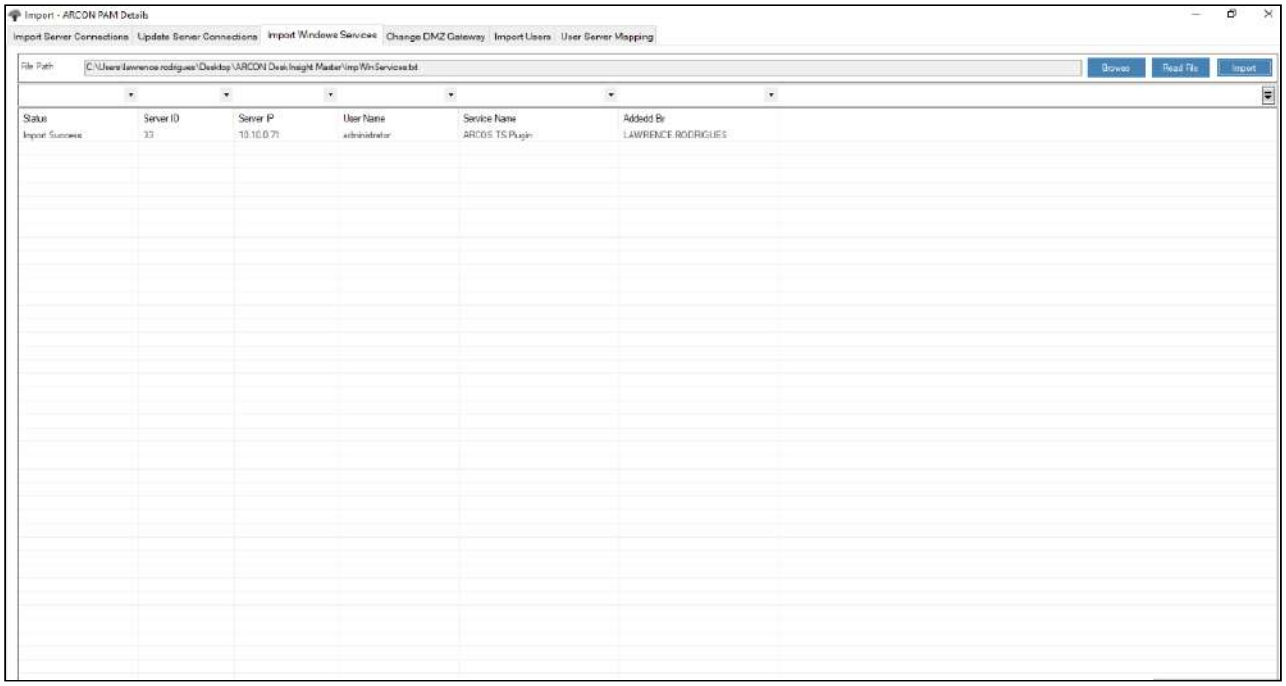
2. Click **Read File** button. A window pops up with the following message:
   Read File Process Completed
3. Click **OK**. The details are displayed in the grid.



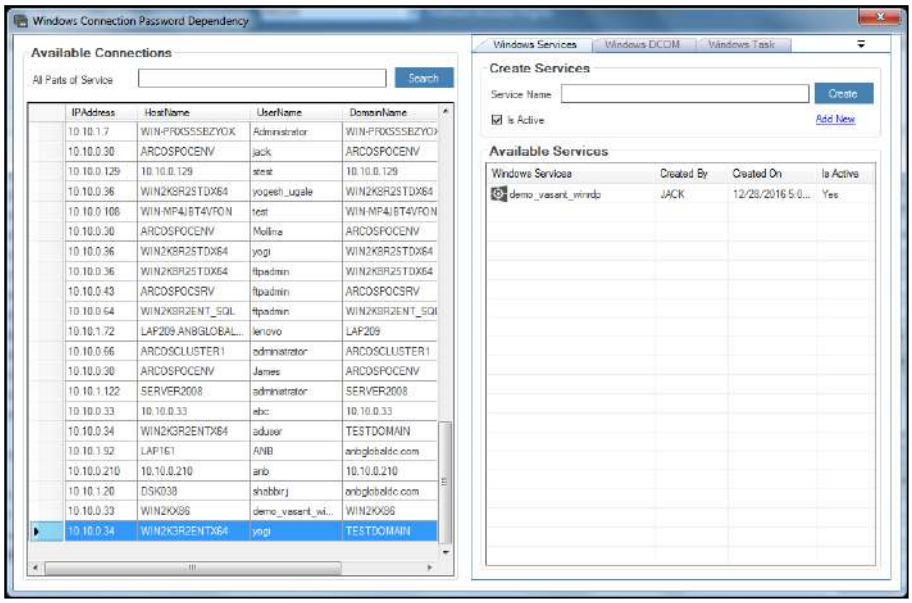
4. Click **Import** button. A window pops up with the following message:
   Import To Database Process Completed



5. Click **OK**. The status is updated to **Import Success**.



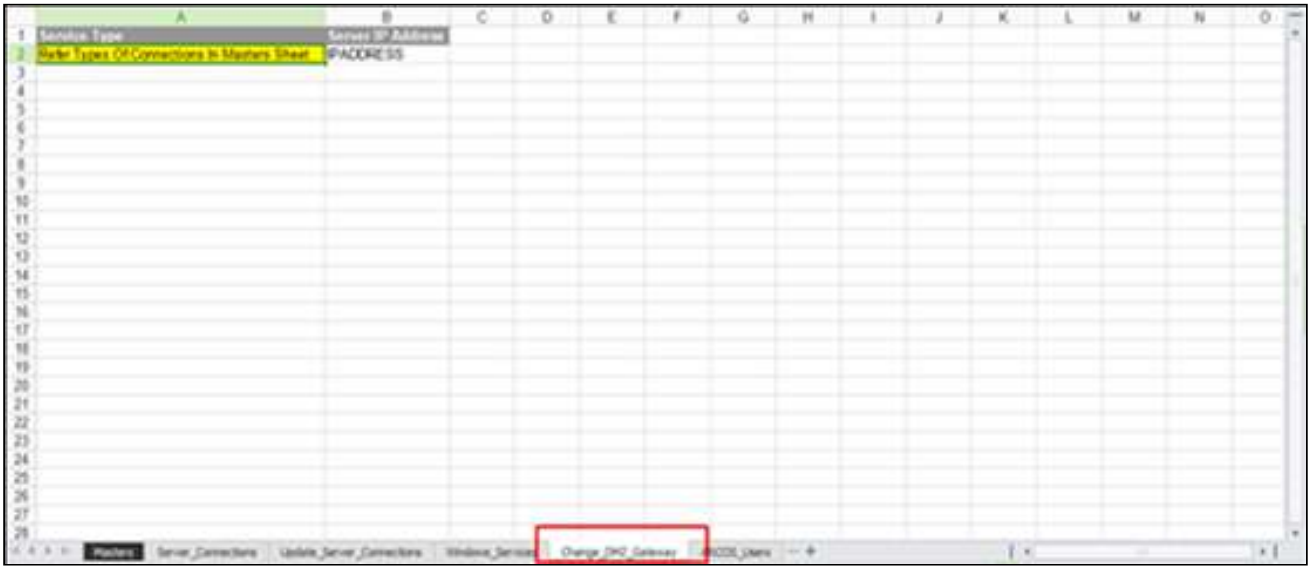
6. The imported service will be displayed for entered IP Address in **Windows Connection Password Dependency** screen in **Manage** menu.



11.1.4 Change DMZ Gateway

Secure Gateway Server (SGS) acts as a PAM Firewall, as any connection initiated by end-user through PAM is routed through SGS. ARCON|PAM Secured Gateway Server (SGS) runs proprietary components to securely manage all traffic directly from a user machine to the target devices. Native clients can be used for multiple active sessions for all Unix/Linux target systems. If any server is isolated in a separate network zone such as DMZ server, which is not reachable through SGS configured for a specific LOB in ARCON PAM then the 'Change DMZ Gateway' option provides a way to take an exception or change SGS for these isolated servers from where the communication is enabled for connecting to it. To configure multiple such SGS for multiple isolated servers integrated in ARCON PAM in bulk, Change DMZ Gateway is used.

A predefined MS-Excel template for gathering data is provided.



The description of column headers are as follows:

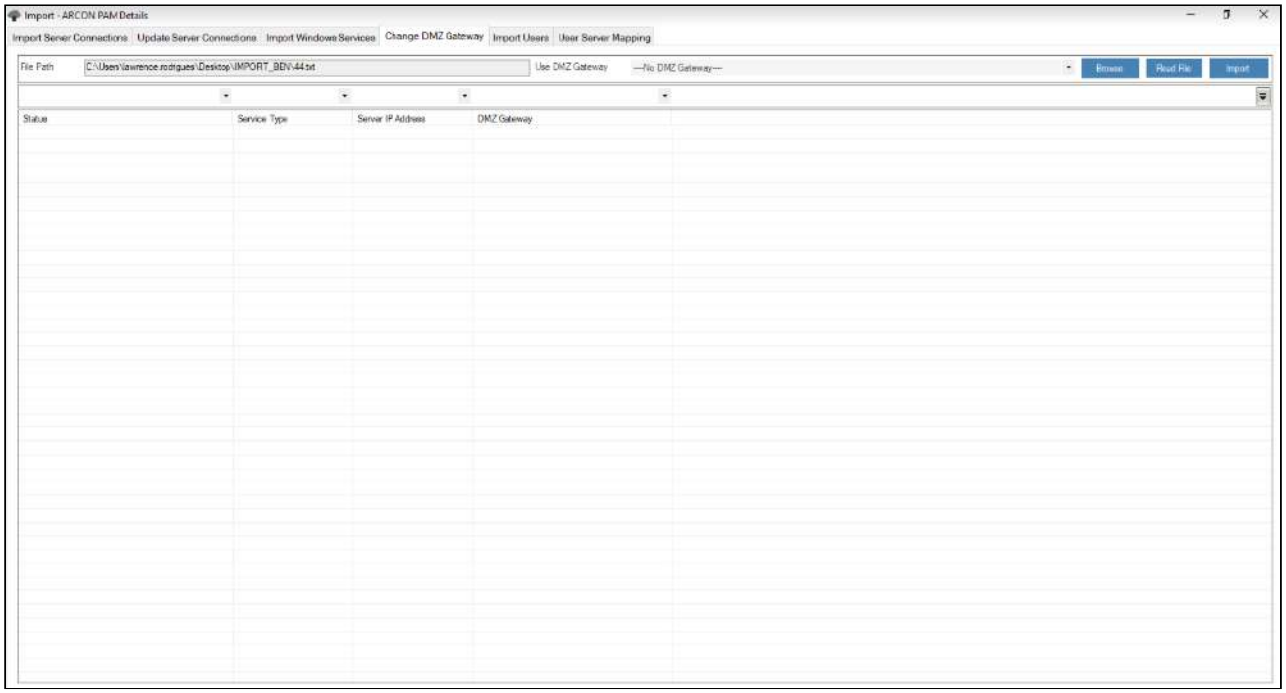
Field Name	Description
Service Type	Enter Service Type ID of service referring Master Sheet
Server IP Address	Enter Server IP Address of service to be added in DMZ zone

Process to configure SGS for multiple Servers are as follows:

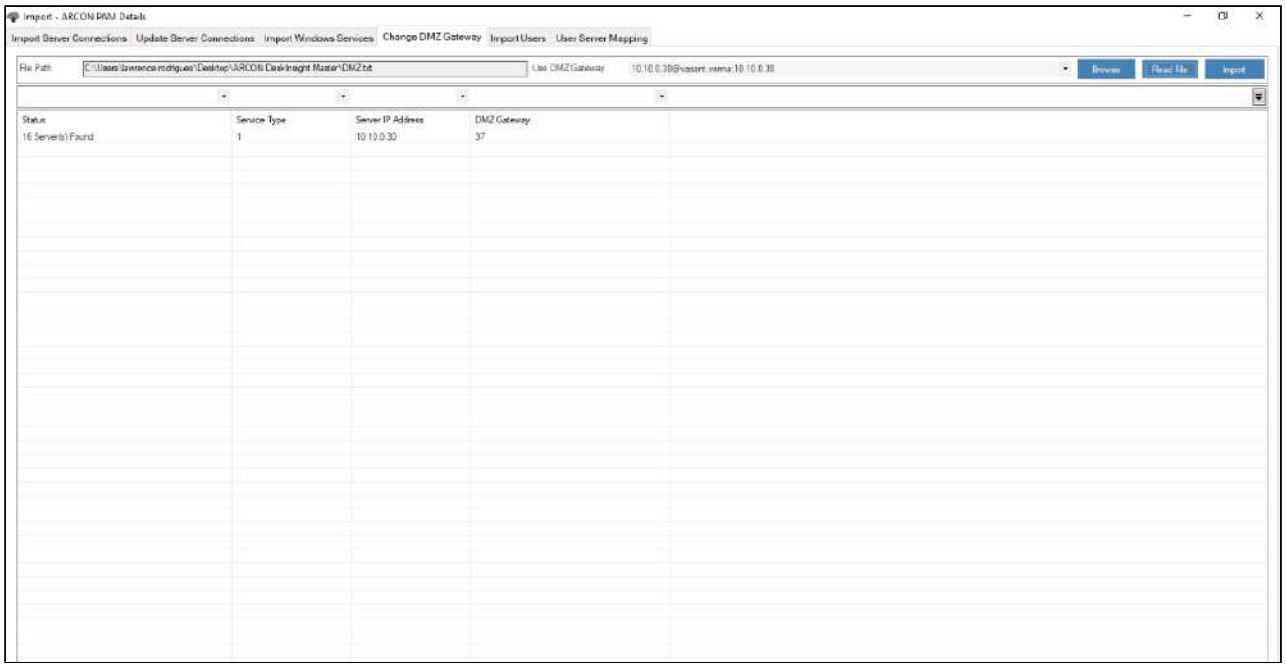
1. The details entered in the template should not contain space or special characters.
2. Copy the details from Master Sheet to notepad and save it to .txt format.
3. The text file is then used to import the desired data into ARCON PAM.

Import Text file into ARCON PAM:

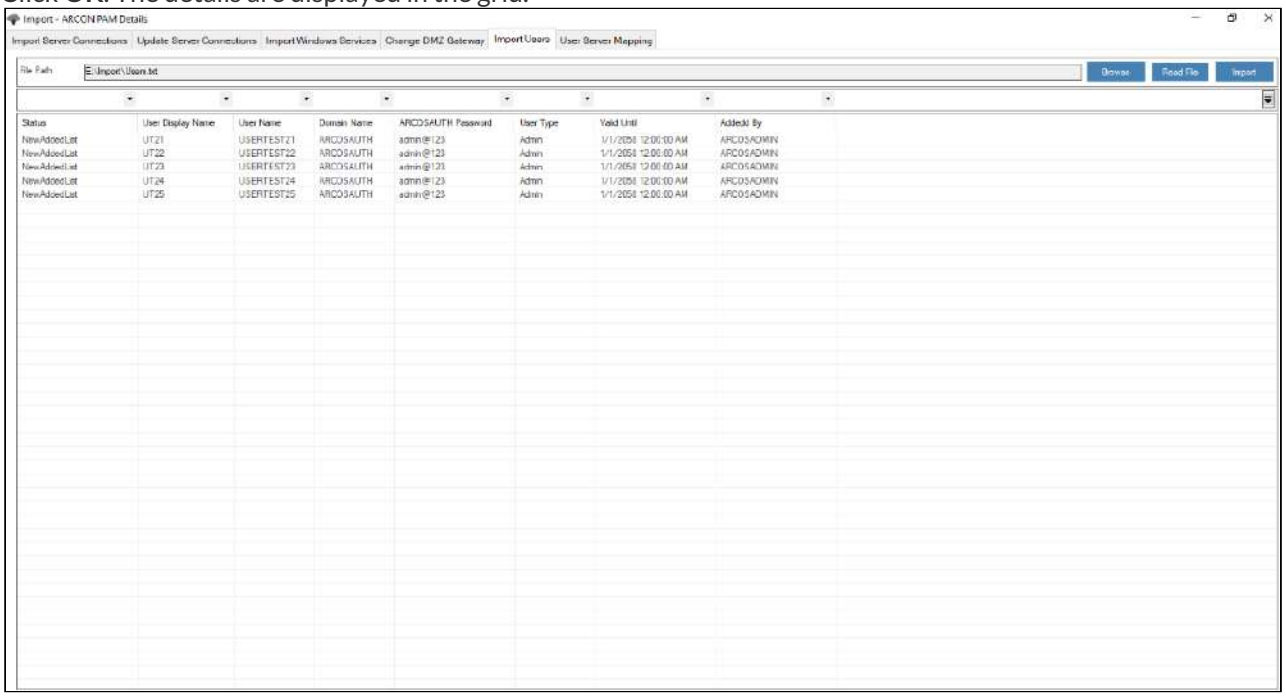
1. Login to **Server Manager** → **Tools** → **Import** → Select **Change DMZ Gateway** tab → Click **Browse** → Select the location of .txt file.



2. Select DMZ Server from **Use DMZ Gateway** dropdown.

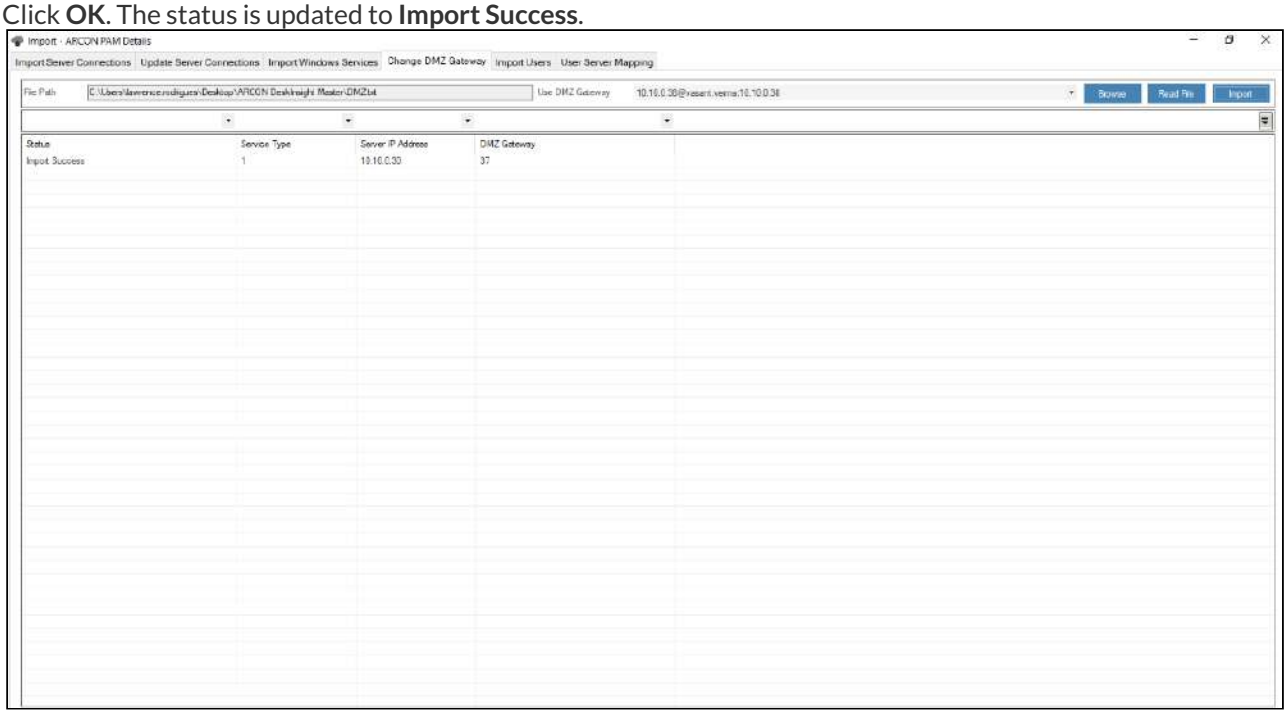


3. Click **Read File** button. A window pops up with the following message:
   Read File Process Completed
4. Click **OK**. The details are displayed in the grid.



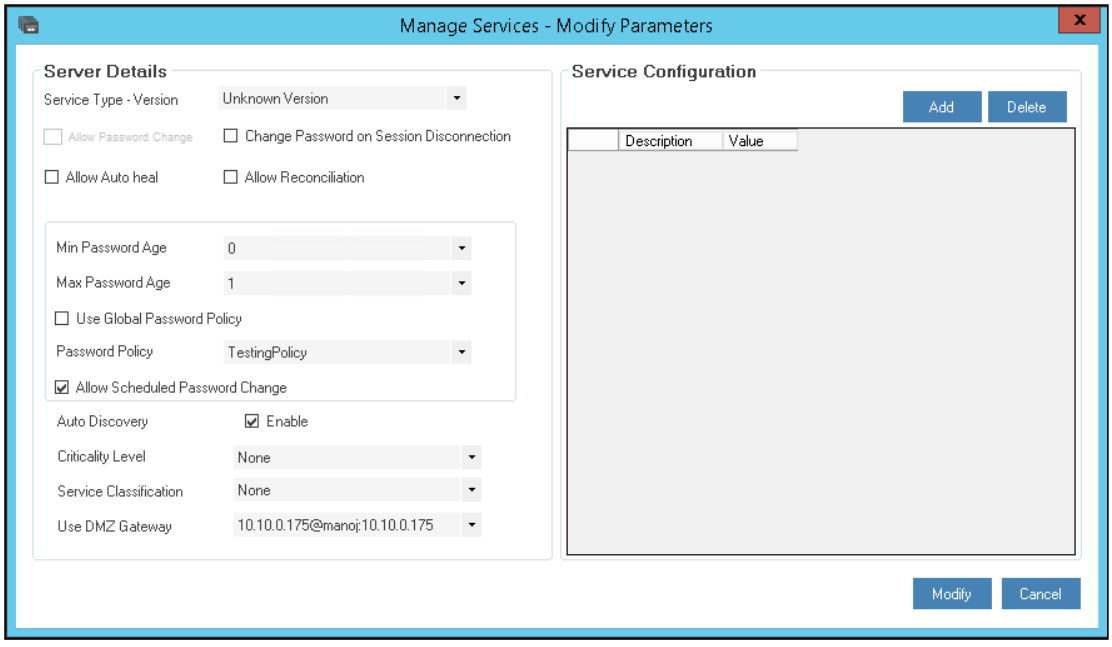
5. Click **Import** button. A window pops up with the following message:
   Import to Database Process Completed

6. Click **OK**. The status is updated to **Import Success**.



To view the configured DMZ Gateway:

1. Login to **Server Manager → Manage → Users and Services → Manage Services**
2. Select the service for which DMZ Gateway was changed. Right-click and choose **Modify Service Parameters** option.
3. The selected DMZ Gateway will be displayed in **Use DMZ Gateway** drop-down list.

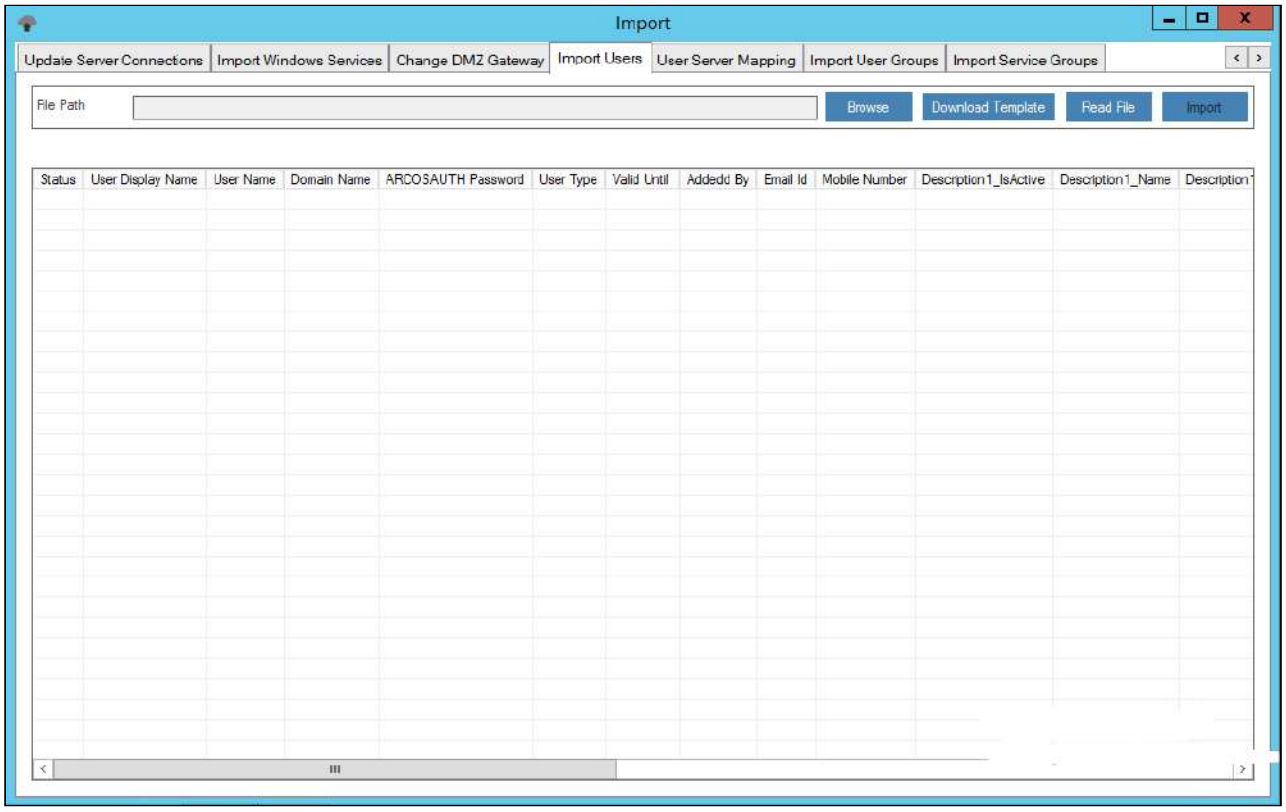


11.1.5 Import Users

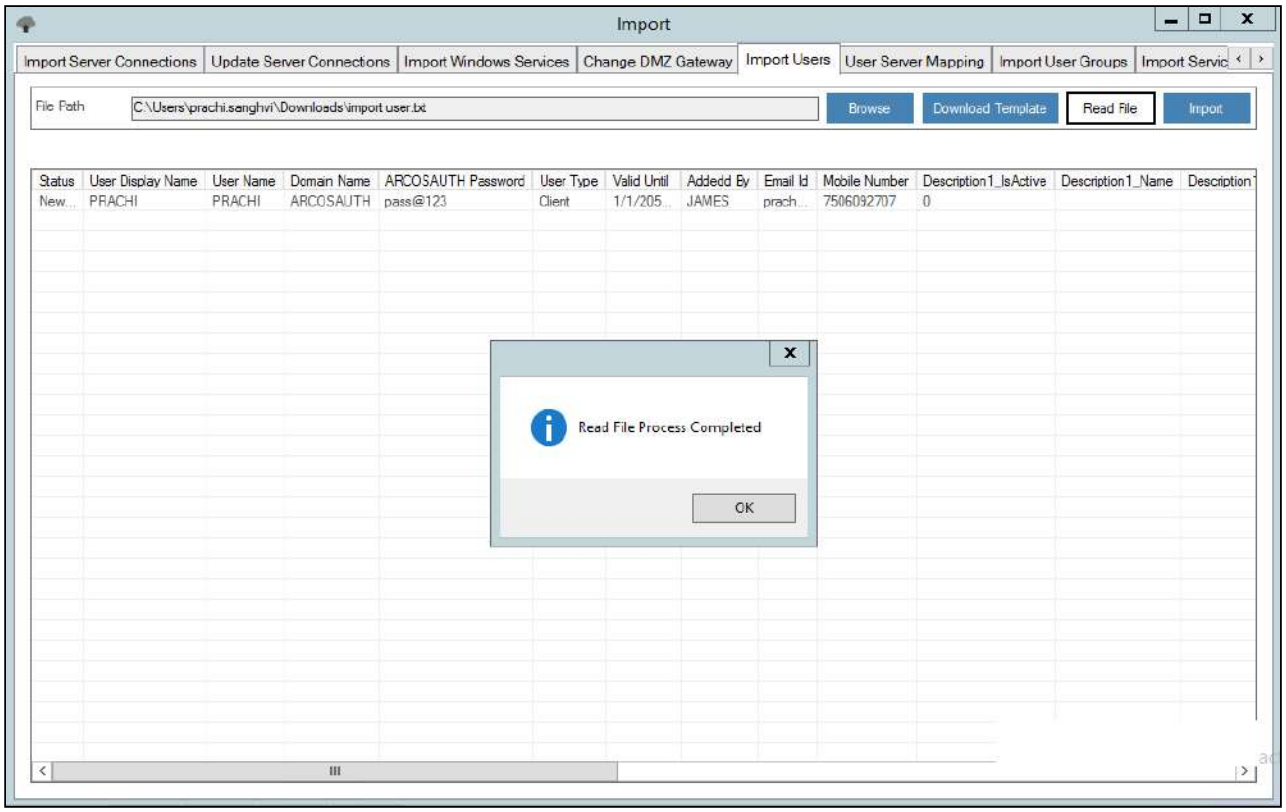
Import Users is used to Import Users in bulk. The imported users will be displayed under Manage Users in Server Manager after they are checked by Admin ID other than the one who Imported Users from Maker's Checker option (Server Manager > Manage > Maker's Checker). After being checked or approved, this user should be added to LOB from the LOB/Profile Master & Manager option (Server Manager > Manage > LOB/Profile Master & Manager > Map LOB / Users).

Process for Importing Users :

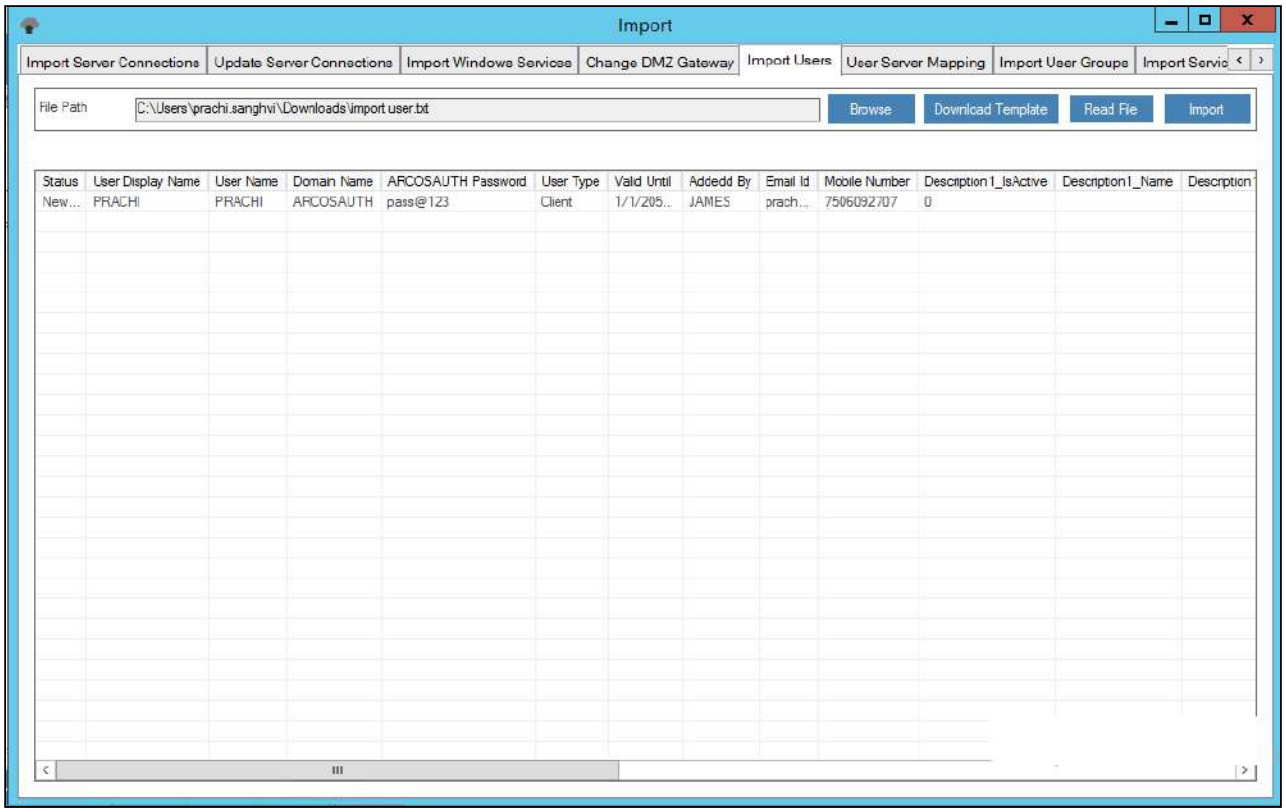
1. Login to **Server Manager** → **Tools** → **Import** → Select **Import Users** tab



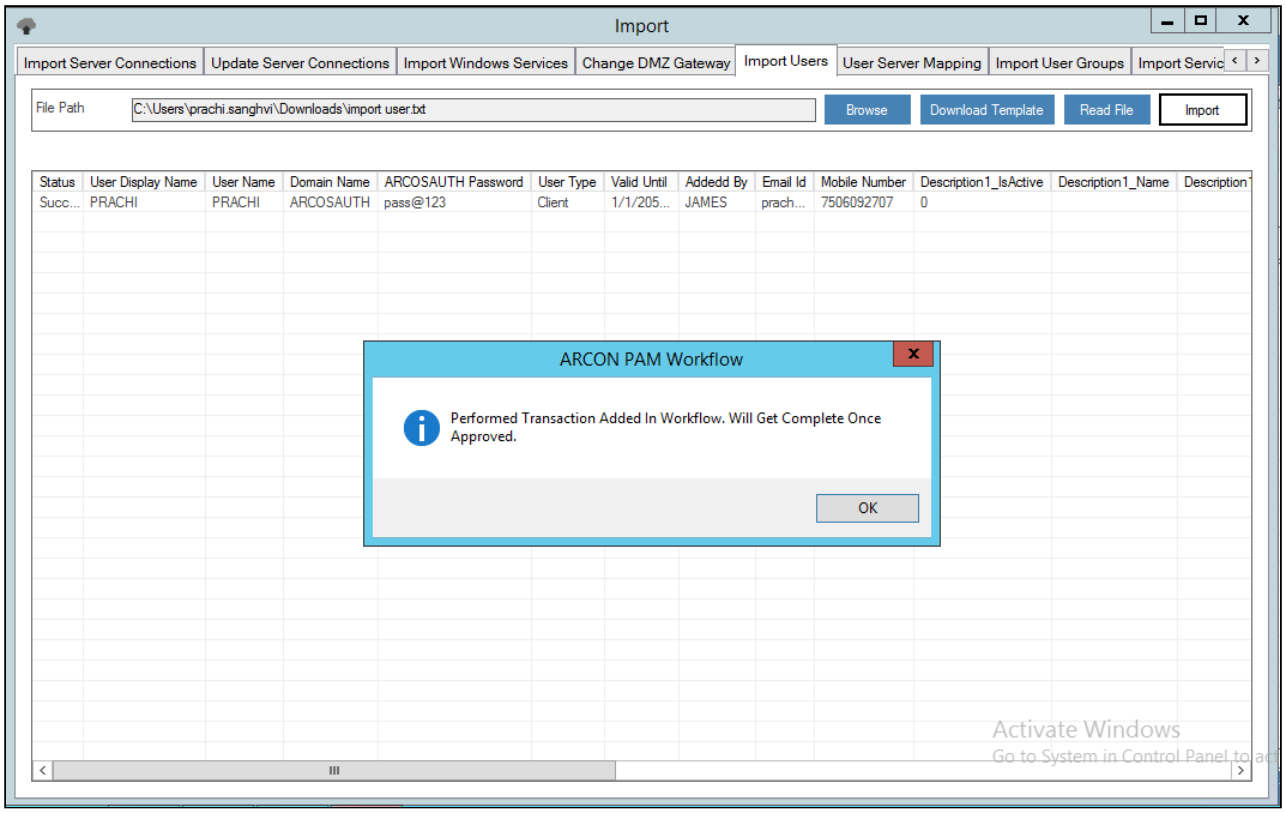
2. Now, the data should be imported in the .txt format in the following manner.
    a. Click **Download Template Button,** Save the file on your local machine.
    b. The Admin user has to enter the desired data into a predefined excel template.
    c. The data entered in the excel template should be left-aligned.
    d. The data from the excel template is copied to the text file.
    e. The text file is then used to import the desired data into ARCON PAM.
3. Select **Browse** tab → browse for the .txt file → click **Read File** button. A window pops up with the following message: **Read File Process Completed.**



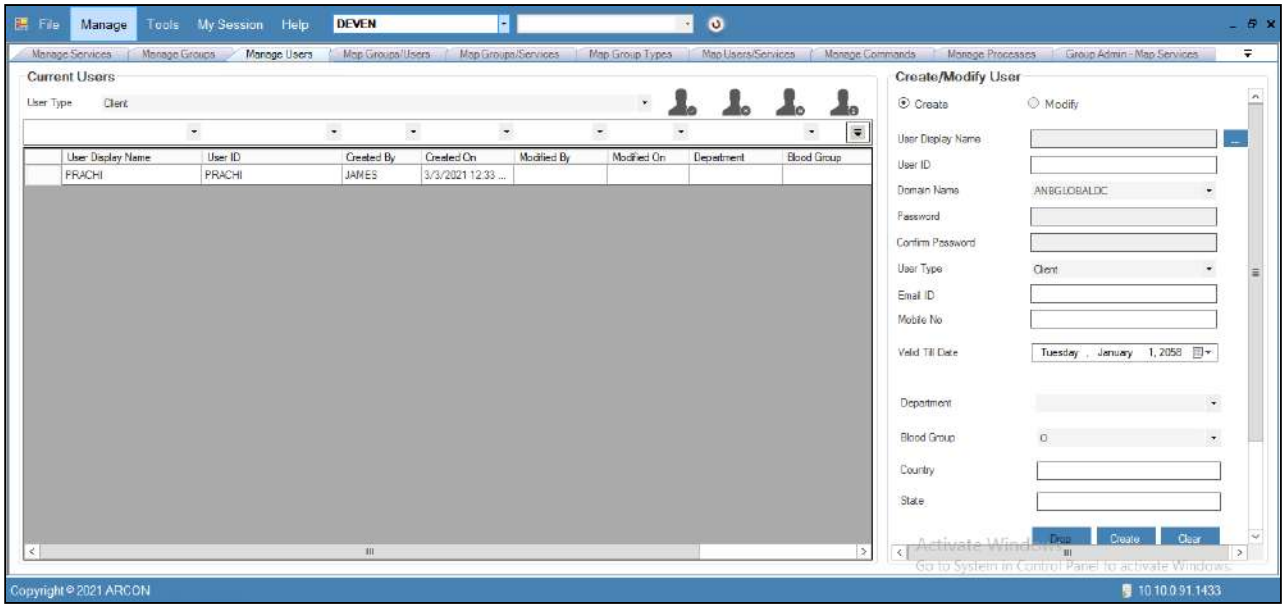
4. Click **OK**. The details from the .txt file are displayed in the grid.



5. Click **Import** button. A window pops up with the following message: **Performed Transaction Added in Workflow. Will get Complete once approved.** Click **Ok.**



6. The imported users will be displayed in Manage Users in Server Manager after they are approved by Admin ID. After being approved by the checker, the users should be mapped to LOB from LOB/Profile Master & Manager.



⚠ Once a user is successfully imported, you need to then map the user to a particular LOB. In some cases, wherein an Administrator having **Settings** privileges have configured the toggle value for **LOB Wise User Management - Is Enabled** option, where

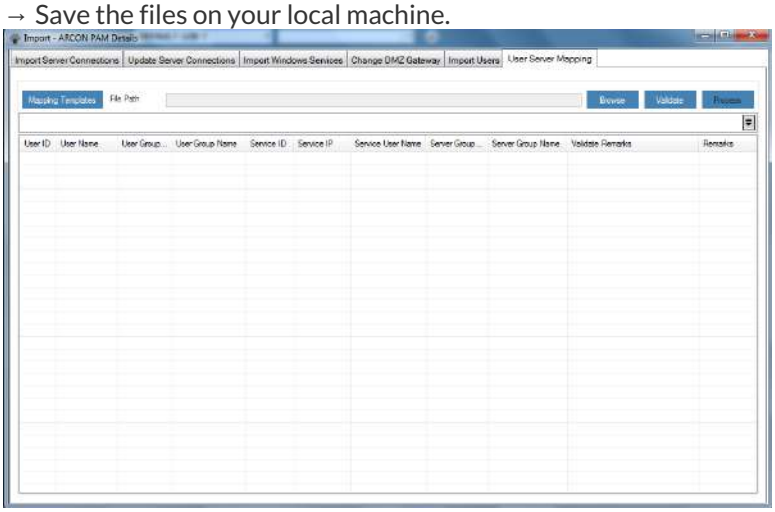
- **LOB Wise User Management - Is Enabled** toggle value is **Enabled** then it states that when a user is imported, it will directly map the user to the selected LOB from **Select LOB/ Profile** dropdown list, once it is imported.
- **LOB Wise User Management - Is Enabled** value is **Disabled**, then it states that the user imported needs to be mapped to a particular LOB in **LOB/Profile Master & Manager**.

11.1.6 User Server Mapping

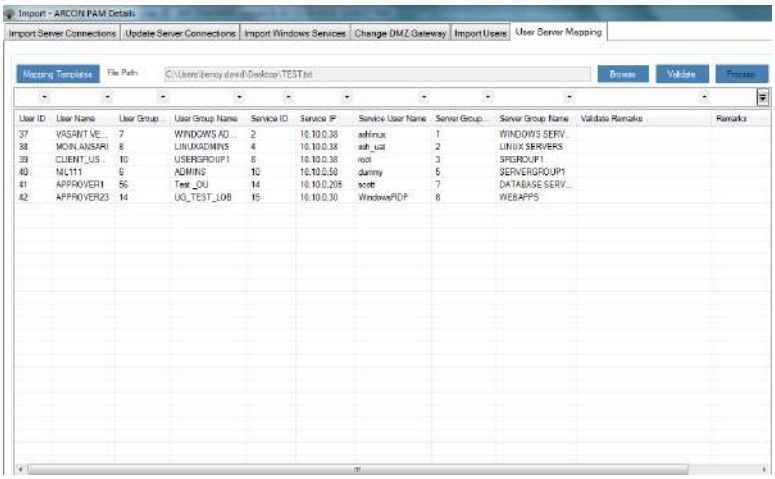
Mapping is the process, wherein the created entities such as LOB's, Users, Services, User Groups, and Server Groups are mapped with each other in order to establish a connection to the server. The mapping process shall be automated and is performed for effective management of entities in ARCON PAM.

Process for User Server Mapping

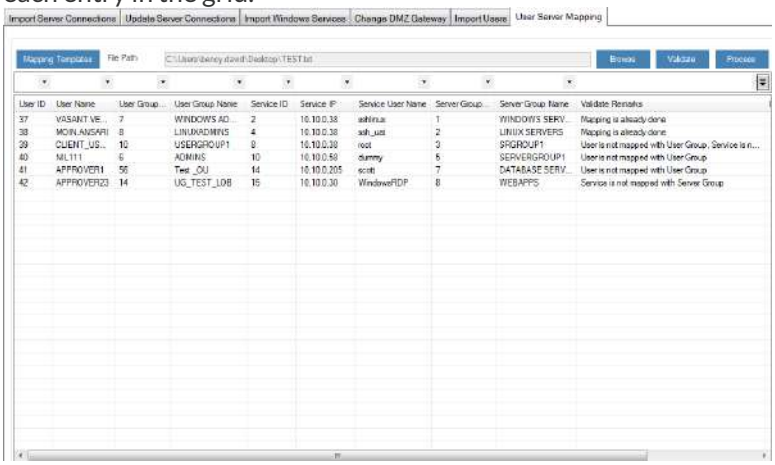
1. Login to **Server Manager** → **Tools** → **Import** → Select **User Server Mapping** tab → Click **Mapping Templates** → Save the files on your local machine.



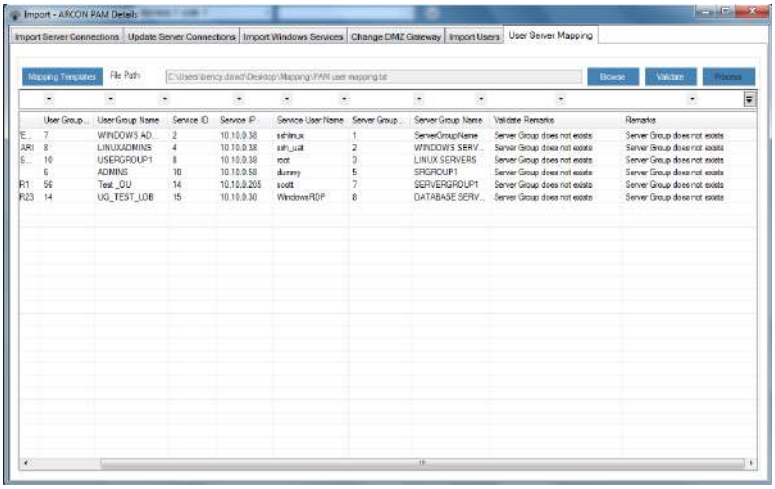
2. Five excel files will be downloaded on to your system, Open the excel file by the name ARCON_PAM_SampleFile, copy paste the data from the other excel files in to the respective columns of this file.
3. Copy the data from **ARCON_PAM_SampleFile** and paste it into a notepad and save this .txt file.
4. On the **User Server Mapping** tab click Browse and open the .txt file with the data, the data will be displayed in the grid.



5. Click **Validate** button to validate whether the imported data. Validation remarks would be displayed against each entry in the grid.



6. Once the data is validated successfully, the process button will be enabled.
7. Click **Process** to automate the mapping process, it will automatically do the mapping process as per the validation remarks.



8. The remarks column will be updated as per the mapping process completed

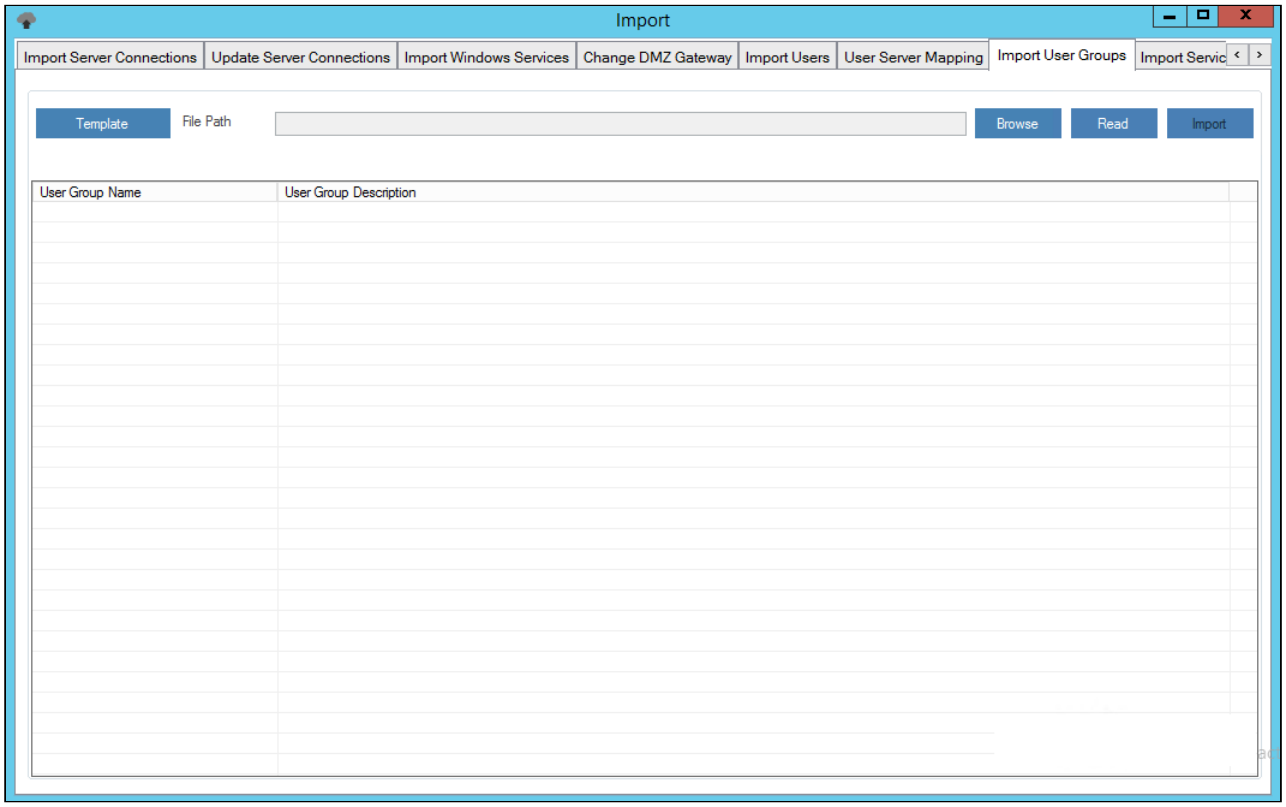
.

11.1.7 Import User Group

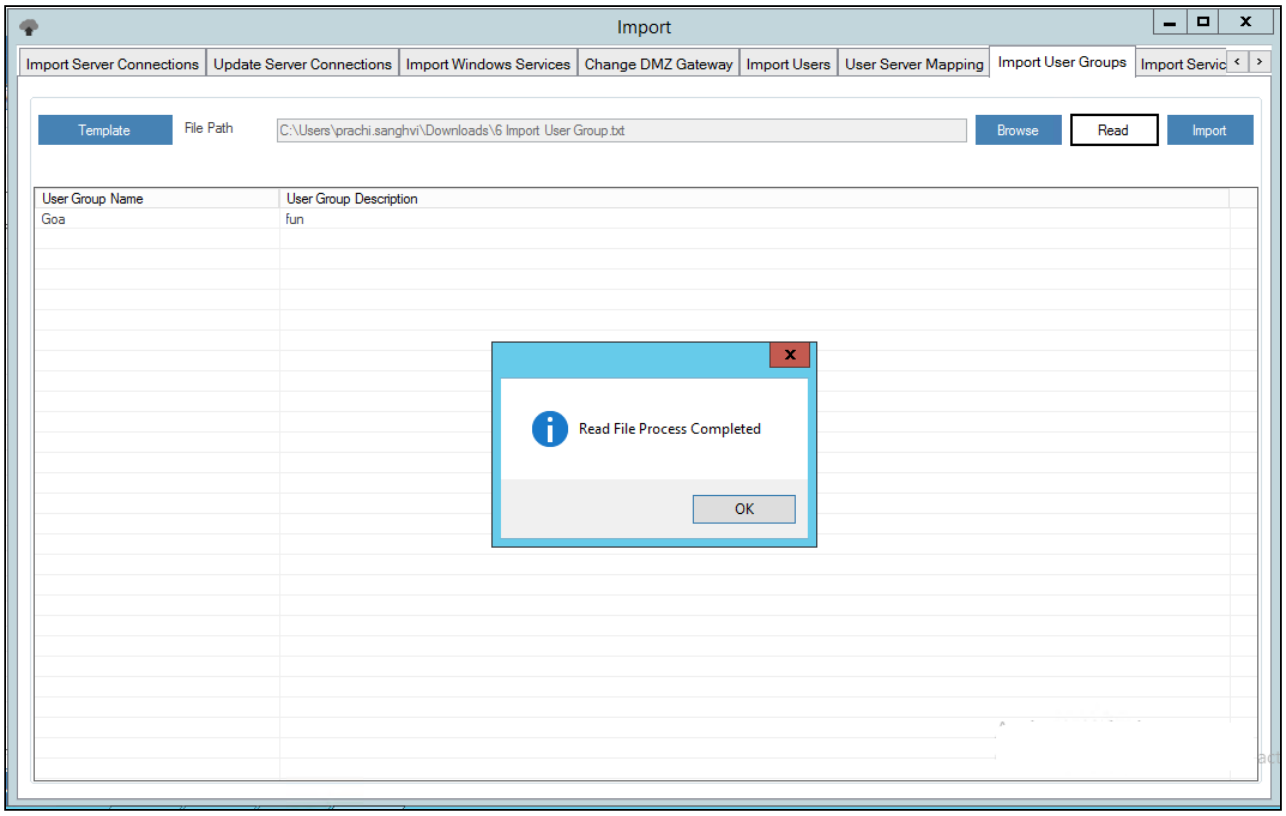
Import user group is used to Import User Groups in bulk. The imported user groups will be displayed under Manage Groups.

Process for Importing User Groups :

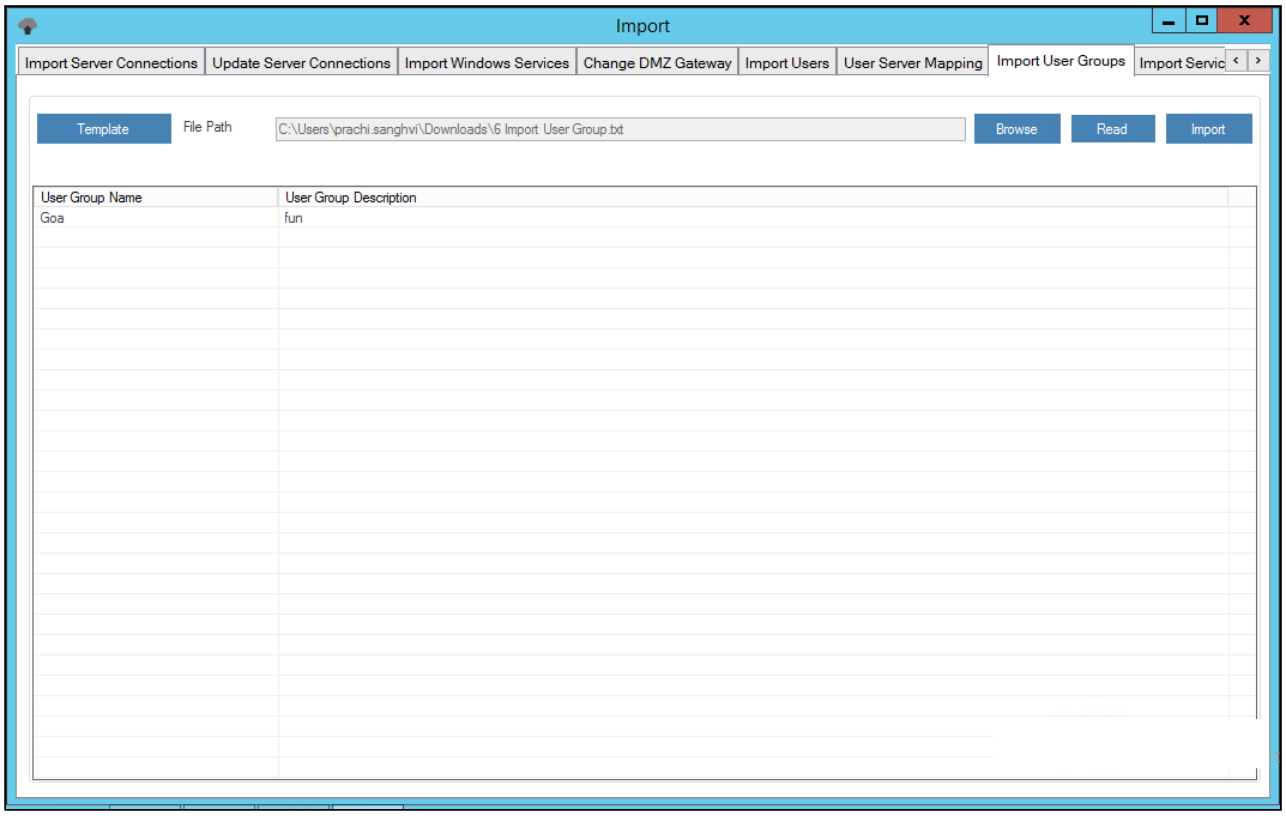
1. Login to **Server Manager** → **Tools** → **Import** → Select **Import User Group** tab.



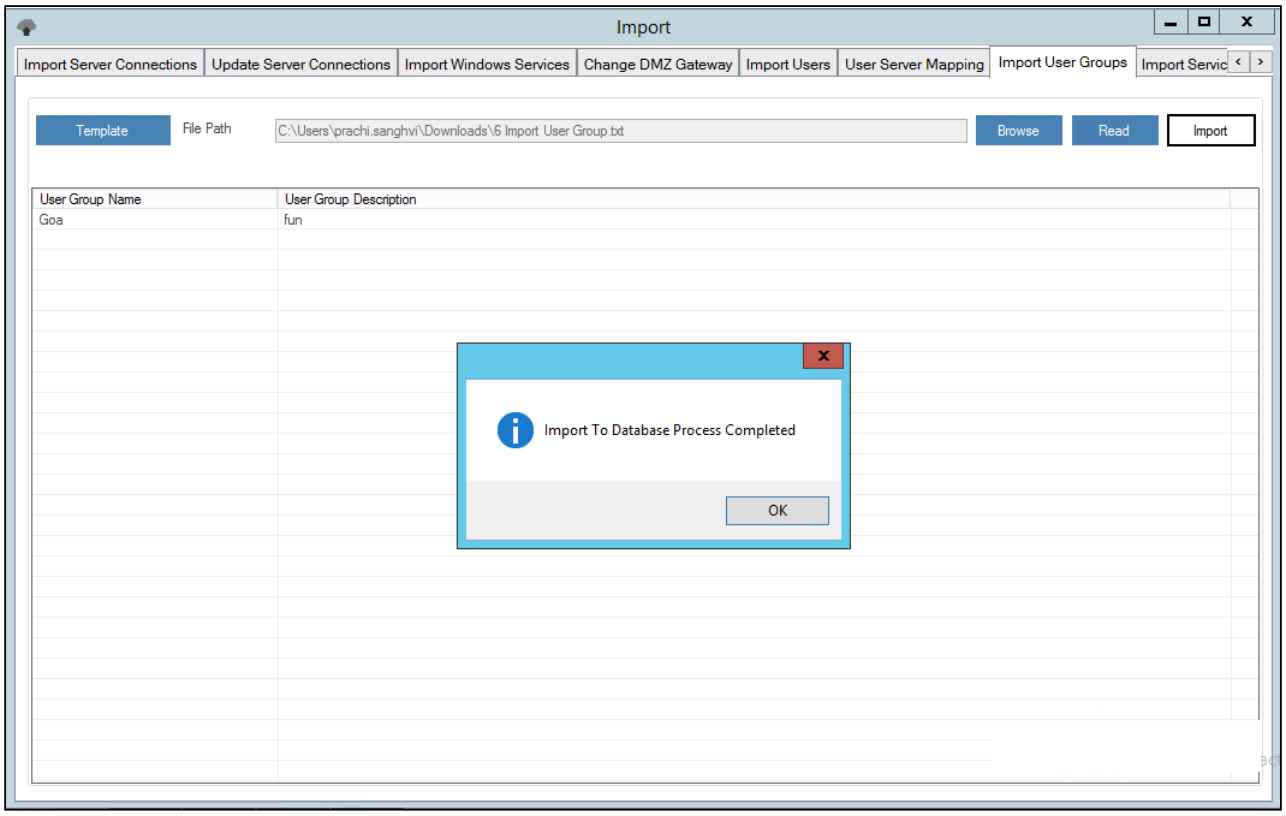
2. Now, the data should be imported in the .txt format in the following manner.
    a. Click **Template Button,** Save the file on your local machine.
    b. The Admin user has to enter the desired data into a predefined excel template.
    c. The data entered in the excel template should be left-aligned.
    d. The data from the excel template is copied to the text file.
    e. The text file is then used to import the desired data into ARCON PAM.
3. Select **Browse** tab → browse for the .txt file → click **Read File** button. A window pops up with the following message: **Read File Process Completed.**



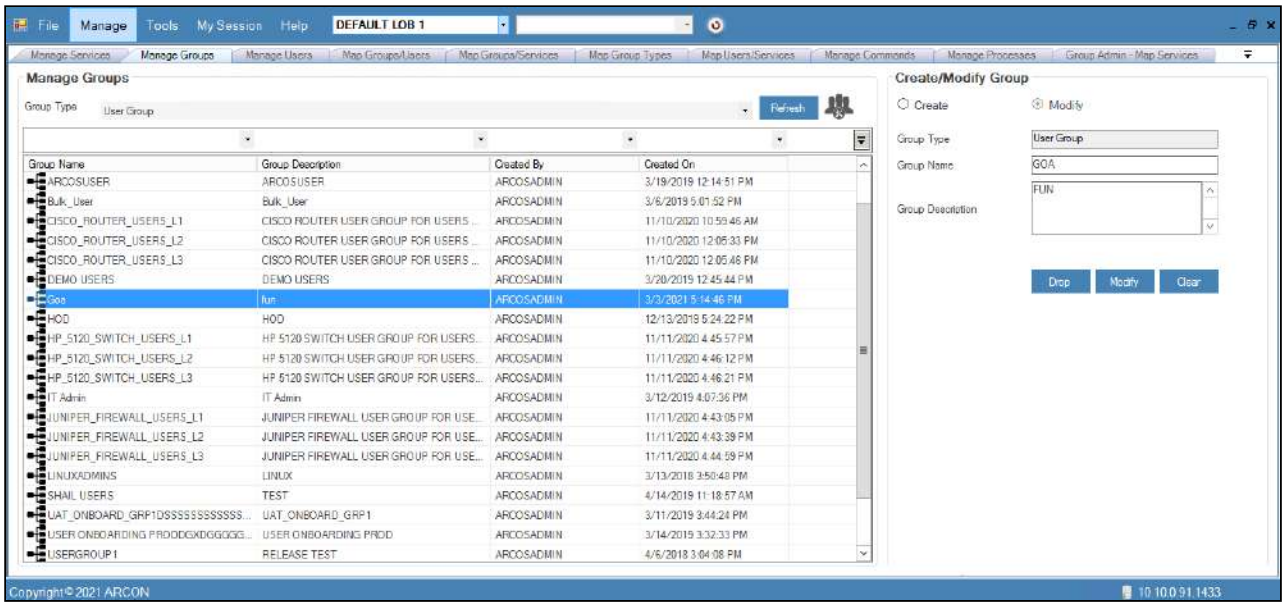
4. Click **OK**. The details from the .txt file are displayed in the grid.



5. Verify the details and click **Import** button. The service is imported into the ARCON PAM database.



6. The imported user group will be displayed under Manage Groups in Server Manager after they are mapped to LOB from LOB/Profile Master & Manager.



⚠ Once a user is successfully imported, you need to then map the user to a particular LOB. In some cases, wherein an Administrator having **Settings** privileges have configured the toggle value for **LOB Wise User Management - Is Enabled** option, where

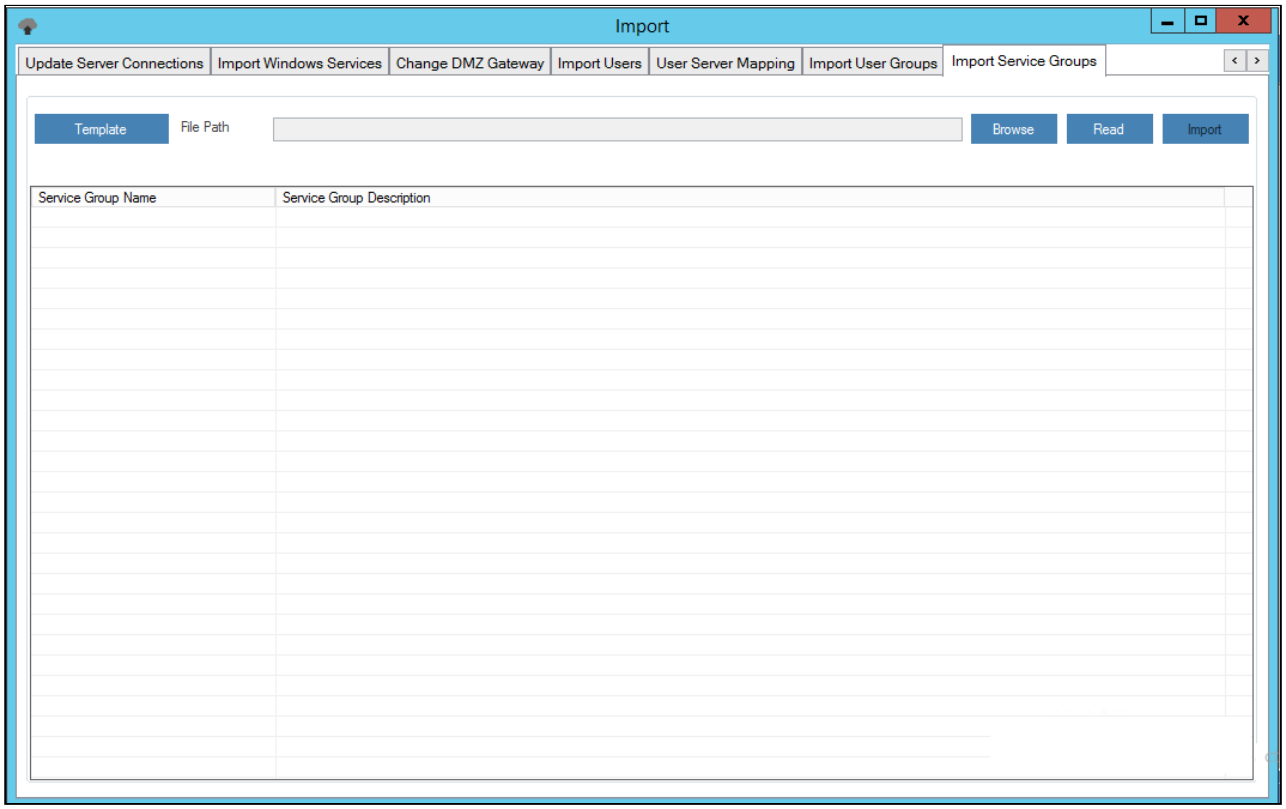
- **LOB Wise User Management - Is Enabled** toggle value is **Enabled** then it states that when a user is imported, it will directly map the user to the selected LOB from **Select LOB/ Profile** dropdown list, once it is imported.
- **LOB Wise User Management - Is Enabled** value is **Disabled**, then it states that the user imported needs to be mapped to a particular LOB in **LOB/Profile Master & Manager**.

11.1.8 Import Server Group

Import server group is used to Import Server Groups in bulk. The imported server groups will be displayed under Manage Groups.

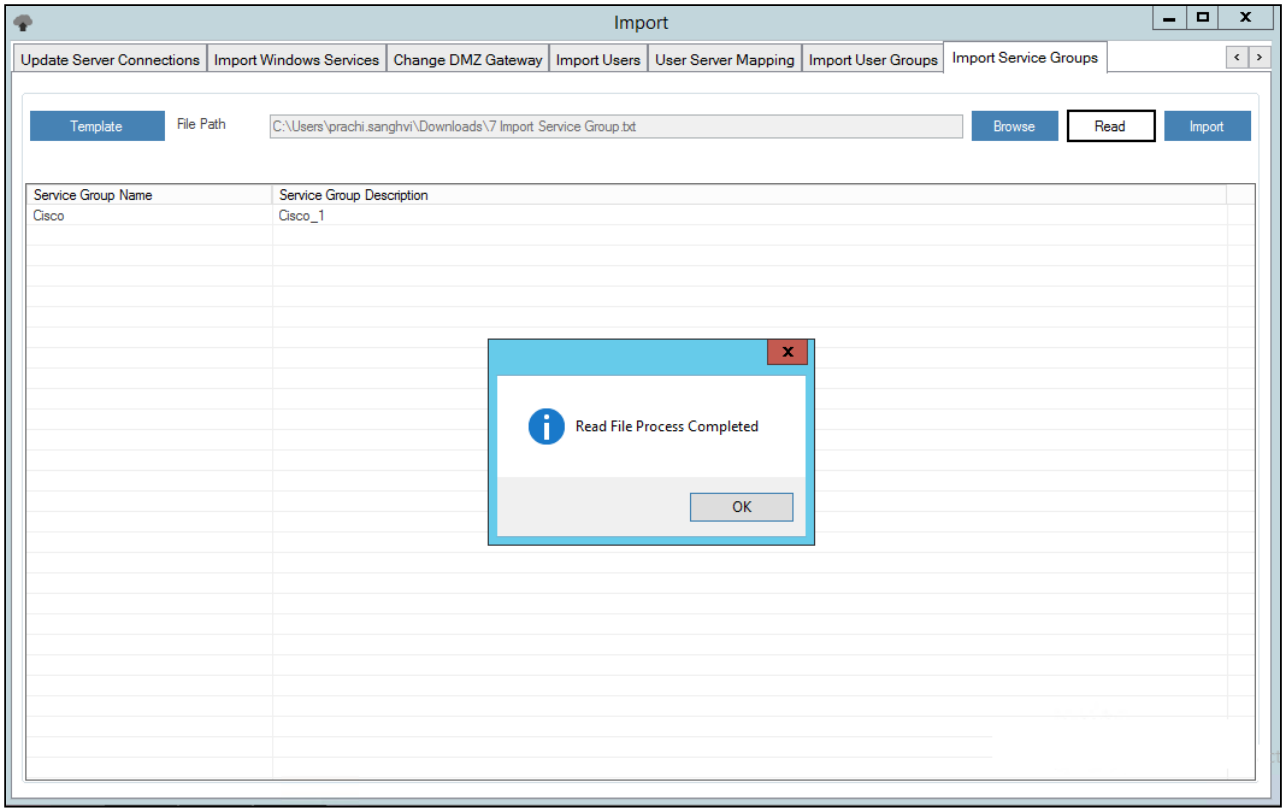
Process for Importing Server Groups :

1. Login to **Server Manager** → **Tools** → **Import** → Select **Import Server Group** tab.

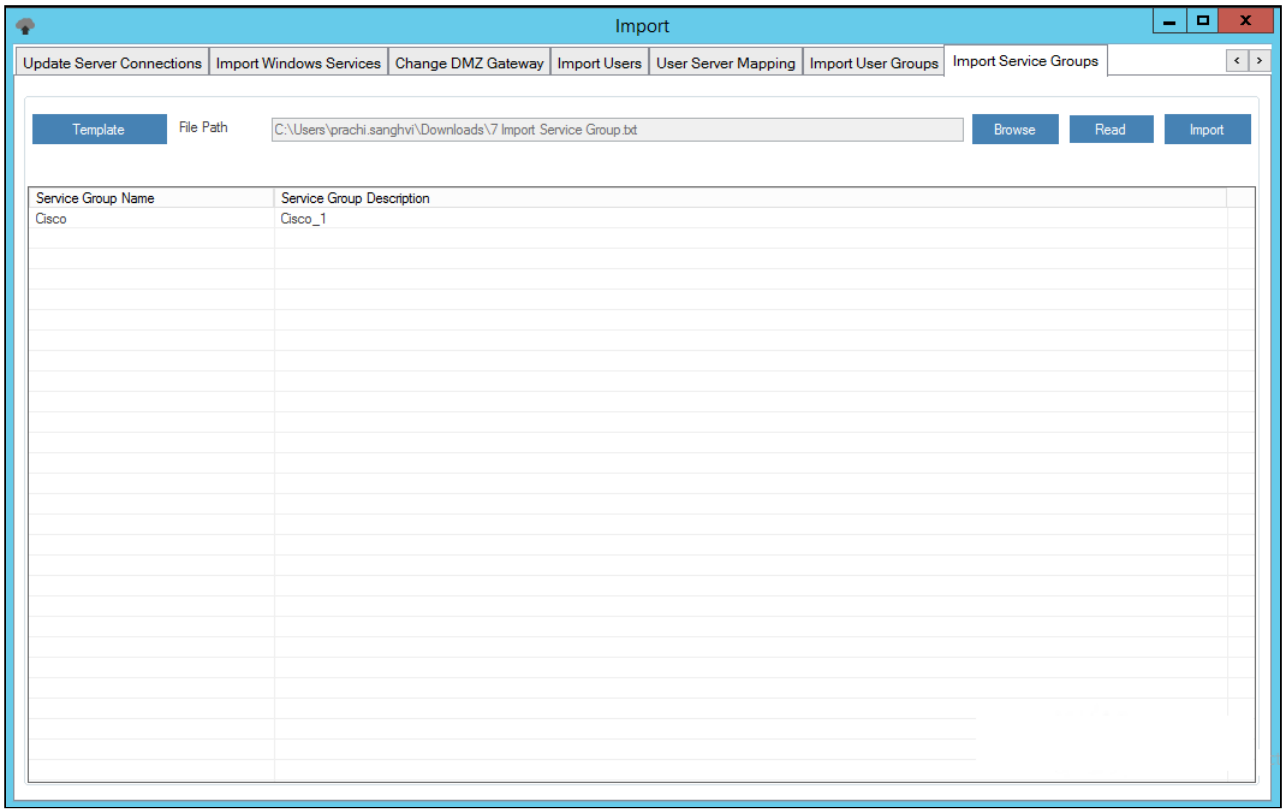


2. Now, the data should be imported in the .txt format in the following manner.
   a. Click **Template Button,** Save the file on your local machine.
   b. The Admin user has to enter the desired data into a predefined excel template.
   c. The data entered in the excel template should be left-aligned.
   d. The data from the excel template is copied to the text file.
   e. The text file is then used to import the desired data into ARCON PAM.

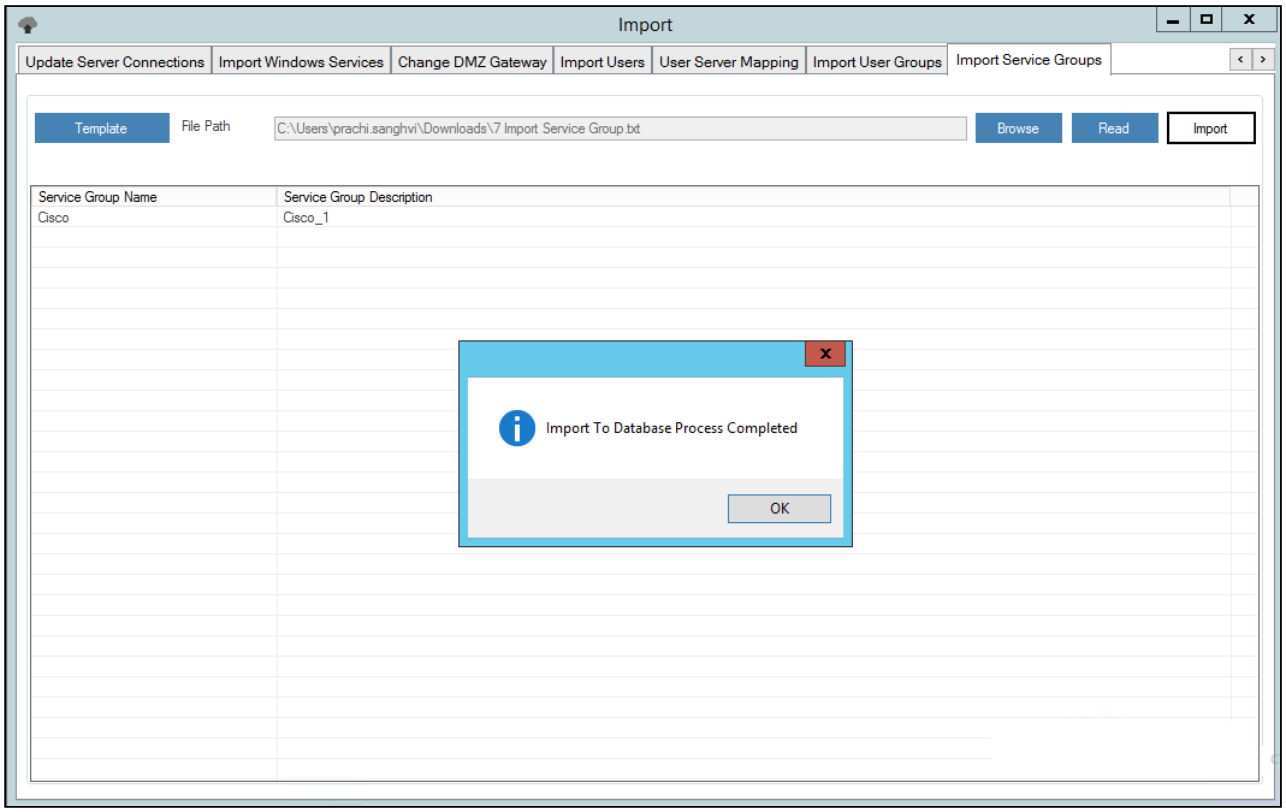
3. Select **Browse** tab → browse for the .txt file → click **Read File** button. A window pops up with the following message: **Read File Process Completed.**



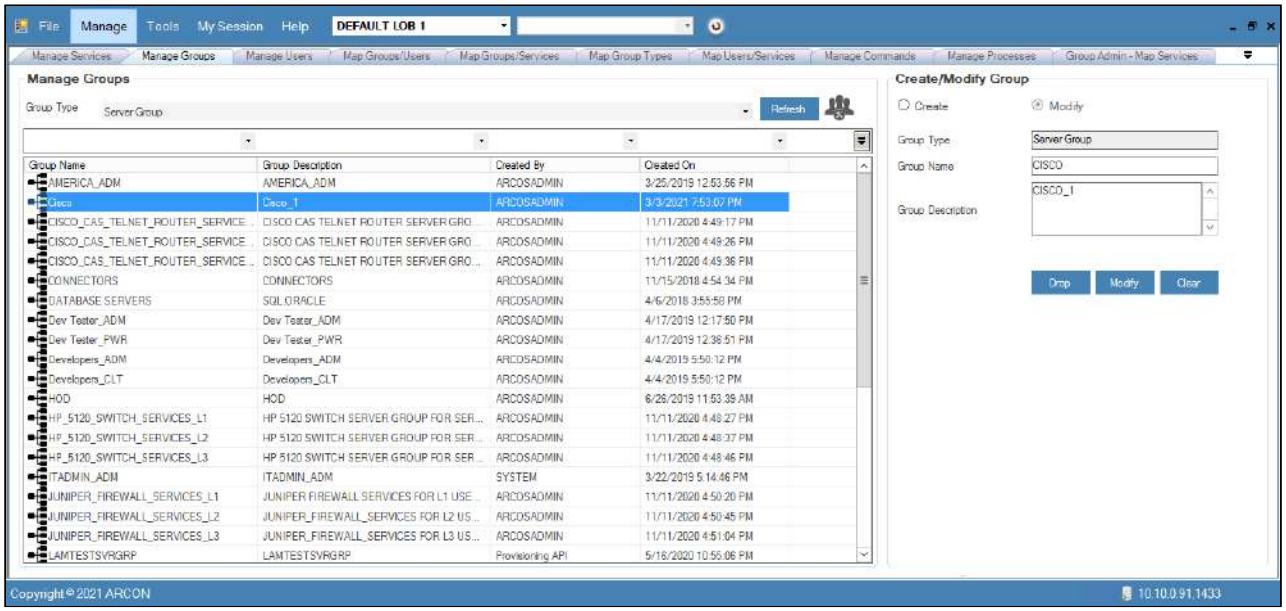
4. Click **OK**. The details from the .txt file are displayed in the grid.



5. Verify the details and click **Import** button. The service is imported into the ARCON PAM database.



6. The imported server group will be displayed under Manage Groups in Server Manager after they are mapped to LOB from LOB/Profile Master & Manager.



⚠ Once a user is successfully imported, you need to then map the user to a particular LOB. In some cases, wherein an Administrator having **Settings** privileges have configured the toggle value for **LOB Wise User Management - Is Enabled** option, where

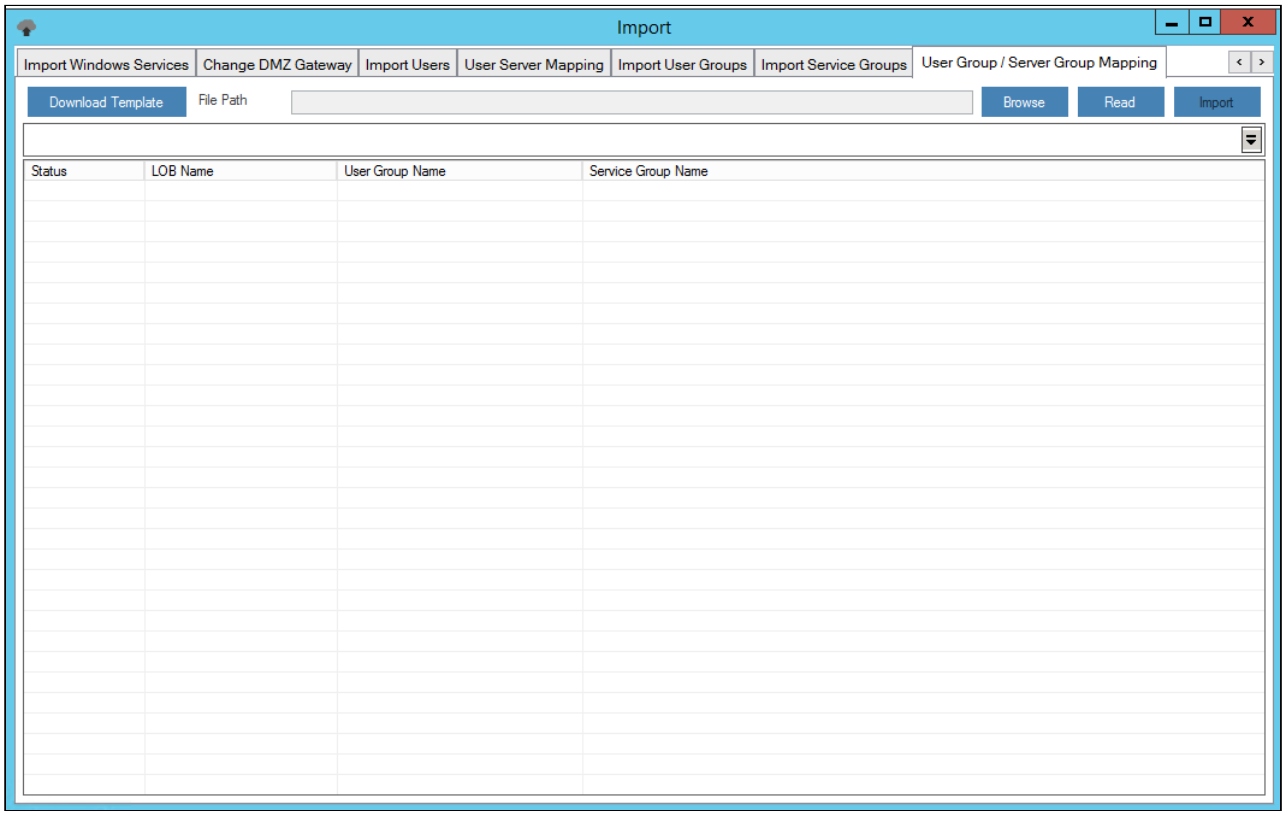
- **LOB Wise User Management - Is Enabled** toggle value is **Enabled** then it states that when a user is imported, it will directly map the user to the selected LOB from **Select LOB/ Profile** dropdown list, once it is imported.
- **LOB Wise User Management - Is Enabled** value is **Disabled**, then it states that the user imported needs to be mapped to a particular LOB in **LOB/Profile Master & Manager**.

11.1.9 Import User Group Server Group

Import user group server group is used to Import and map user group server groups in bulk. The imported groups will be displayed under Map Group Types.

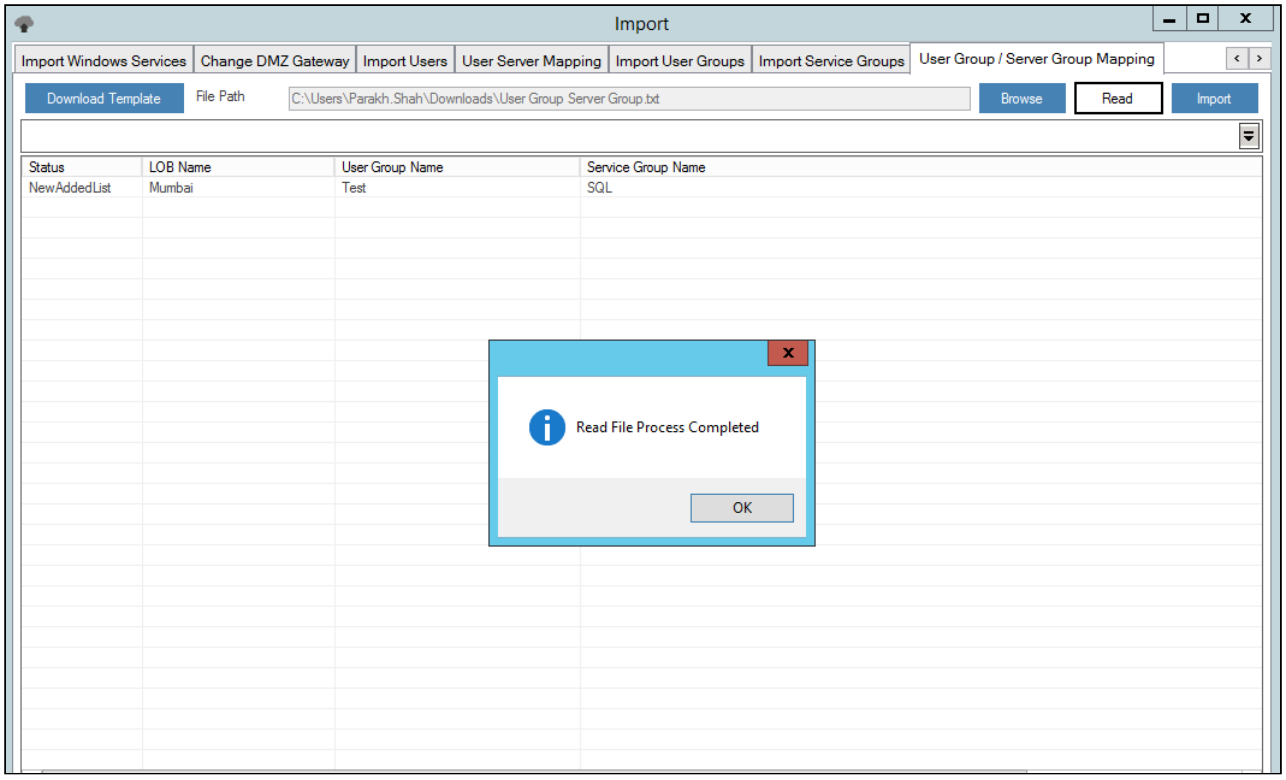
Process for Importing User Group/Server Group:

1. Login to **Server Manager** → **Tools** → **Import** → Select **Import User Group/Server Group Mapping** tab.

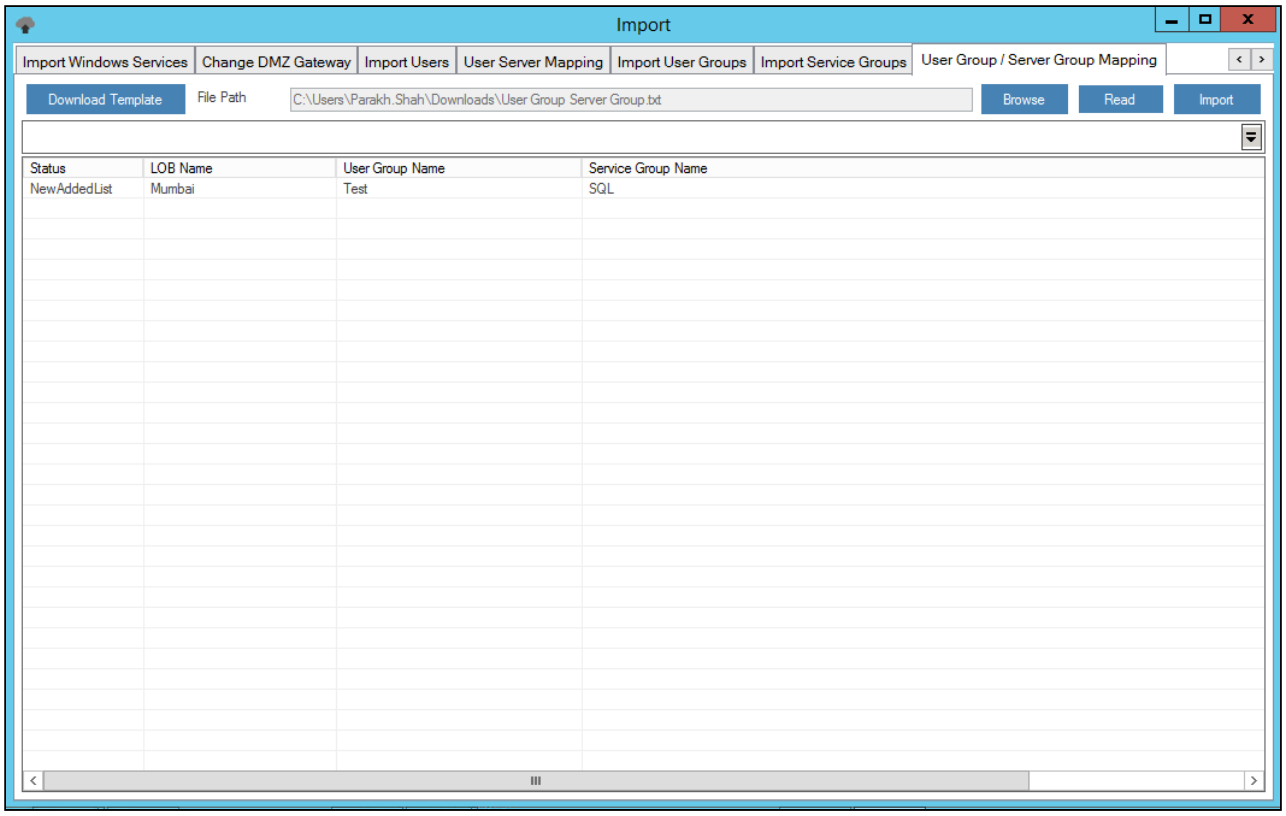


2. Now, the data should be imported in the .txt format in the following manner.
   a. Click **Template Button,** Save the file on your local machine.
   b. The Admin user has to enter the desired data into a predefined excel template.
   c. The data entered in the excel template should be left-aligned.
   d. The data from the excel template is copied to the text file.
   e. The text file is then used to import the desired data into ARCON PAM.

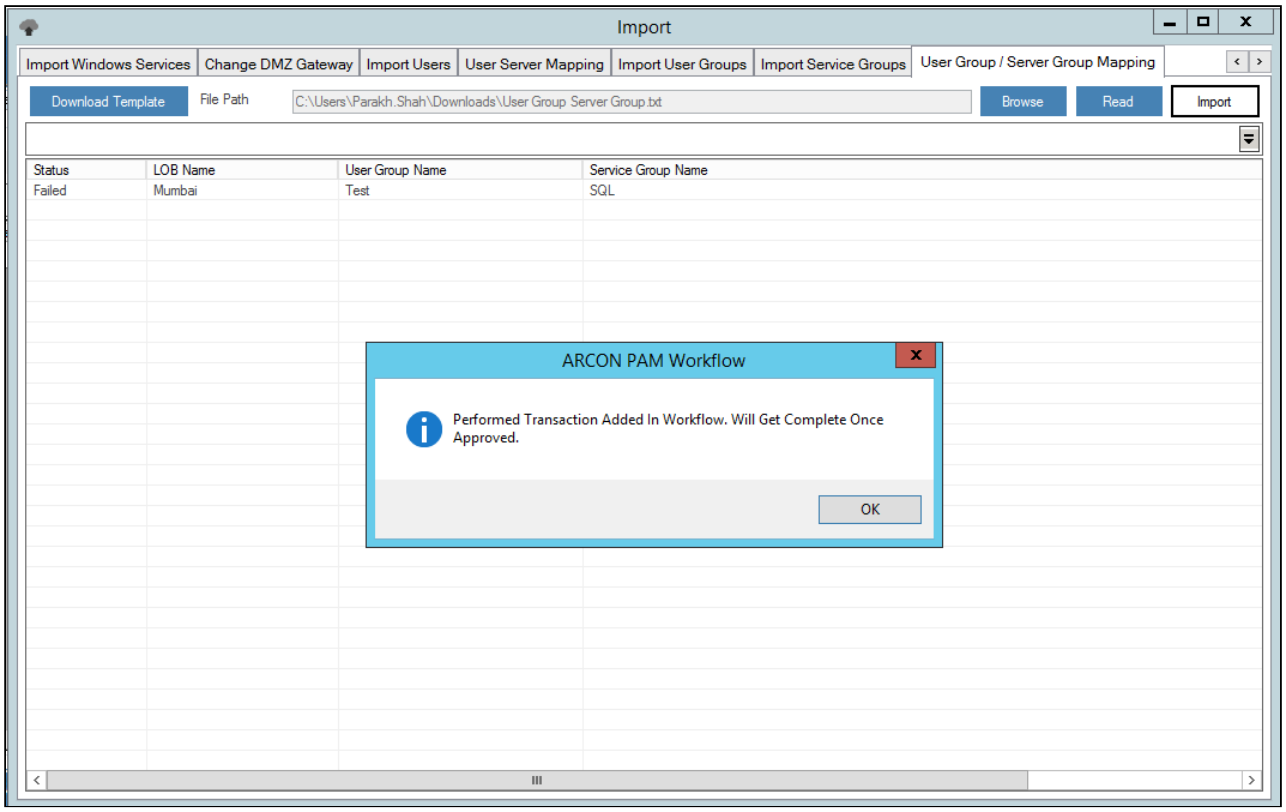
3. Select **Browse** tab → browse for the .txt file → click **Read File** button. A window pops up with the following message: **Read File Process Completed.**



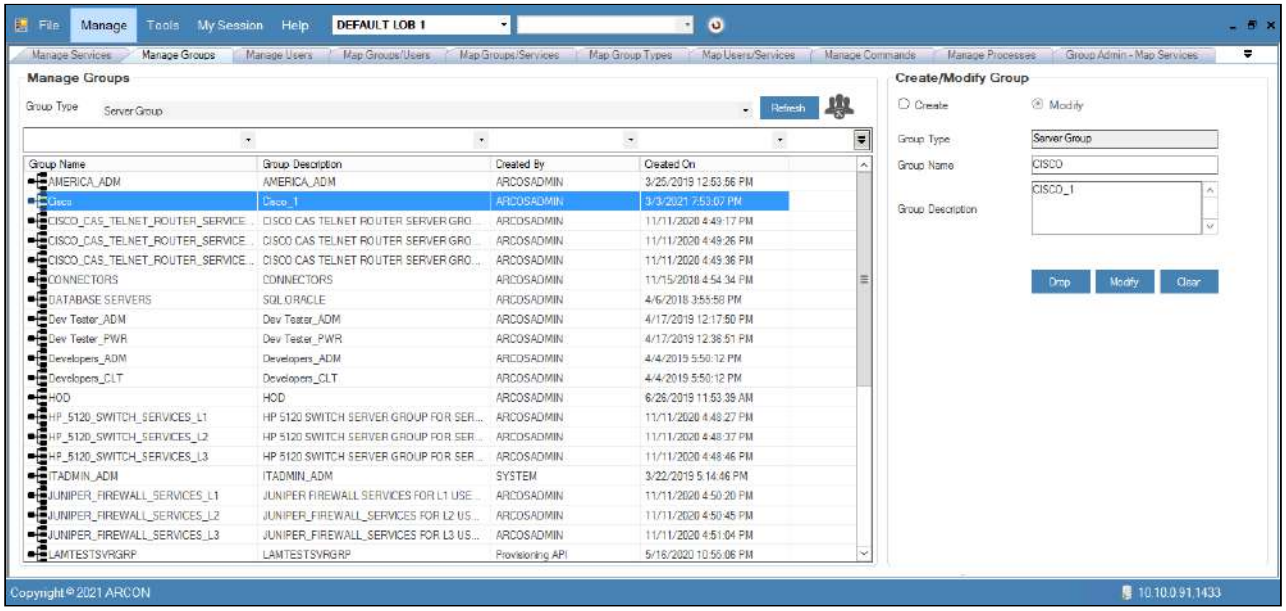
4. Click **OK**. The details from the .txt file are displayed in the grid.



5. Verify the details and click **Import** button. The service is imported into the ARCON PAM database after approval.



6. The imported server group will be displayed under Map Group Types in Server Manager after they are mapped to LOB from LOB/Profile Master & Manager.



⚠ Once a user is successfully imported, you need to then map the user to a particular LOB. In some cases, wherein an Administrator having **Settings** privileges have configured the toggle value for **LOB Wise User Management - Is Enabled** option, where

- **LOB Wise User Management - Is Enabled** toggle value is **Enabled** then it states that when a user is imported, it will directly map the user to the selected LOB from **Select LOB/ Profile** dropdown list, once it is imported.
- **LOB Wise User Management - Is Enabled** value is **Disabled**, then it states that the user imported needs to be mapped to a particular LOB in **LOB/Profile Master & Manager**.

11.2 Privilege User Discovery and Reconciliation

The discovery processes are designed to be used when a resource is being deployed for the first time. It provides a means to load account information into ARCON PAM quickly. For example, the discovery process does not add entries to ARCON PAM nor can you run workflows before or after discovery. However, the discovery processes allows you to determine more quickly whether the users are present or are to be added in ARCON PAM.

When you begin a discovery process, ARCON PAM determines whether an input account matches (or correlates with) an existing user. If it does, the discovery process uses the account to discover other users on the same server. Reconciliation compares the contents of the account index to what each resource currently contains. Reconciliation can perform the following functions:

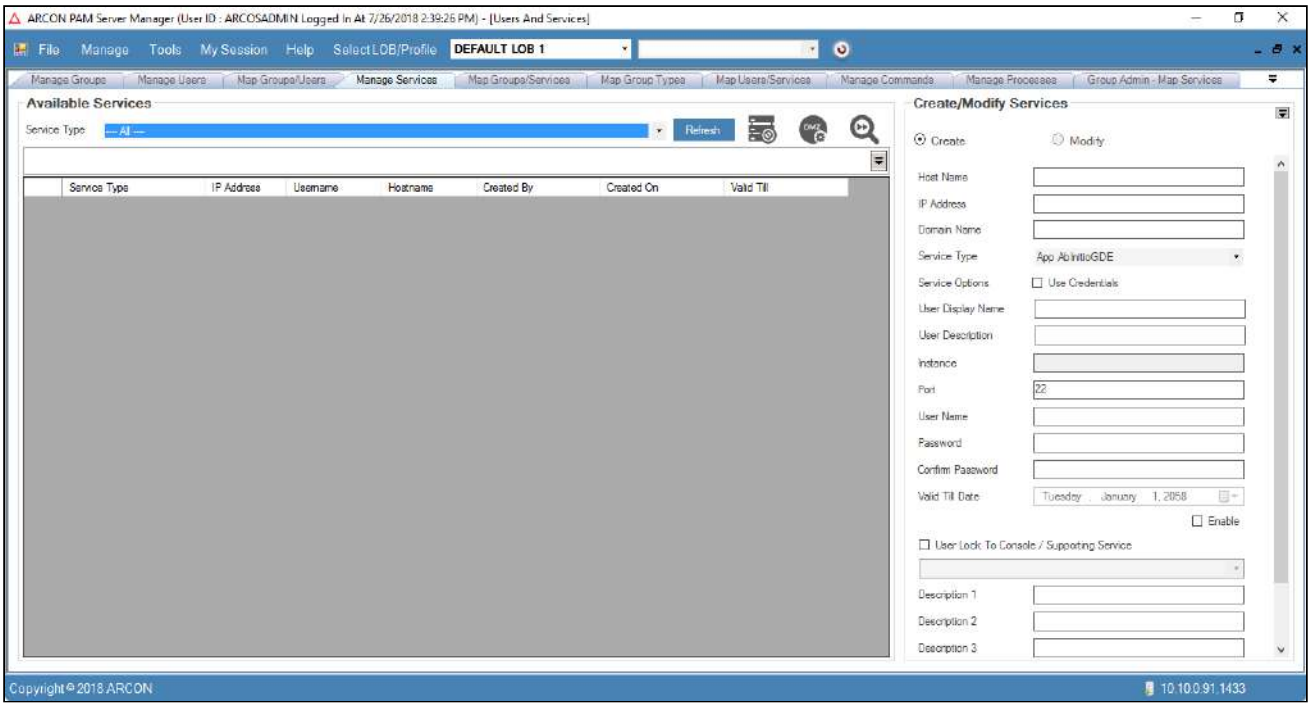
- Detect new accounts
- Correlate accounts with ARCON PAM users
- Detect accounts that are not associated with ARCON PAM users

Users Auto – Discovery is used to automatically discover all the users on all the target servers (server level users only) such as Linux, Windows, and Database.

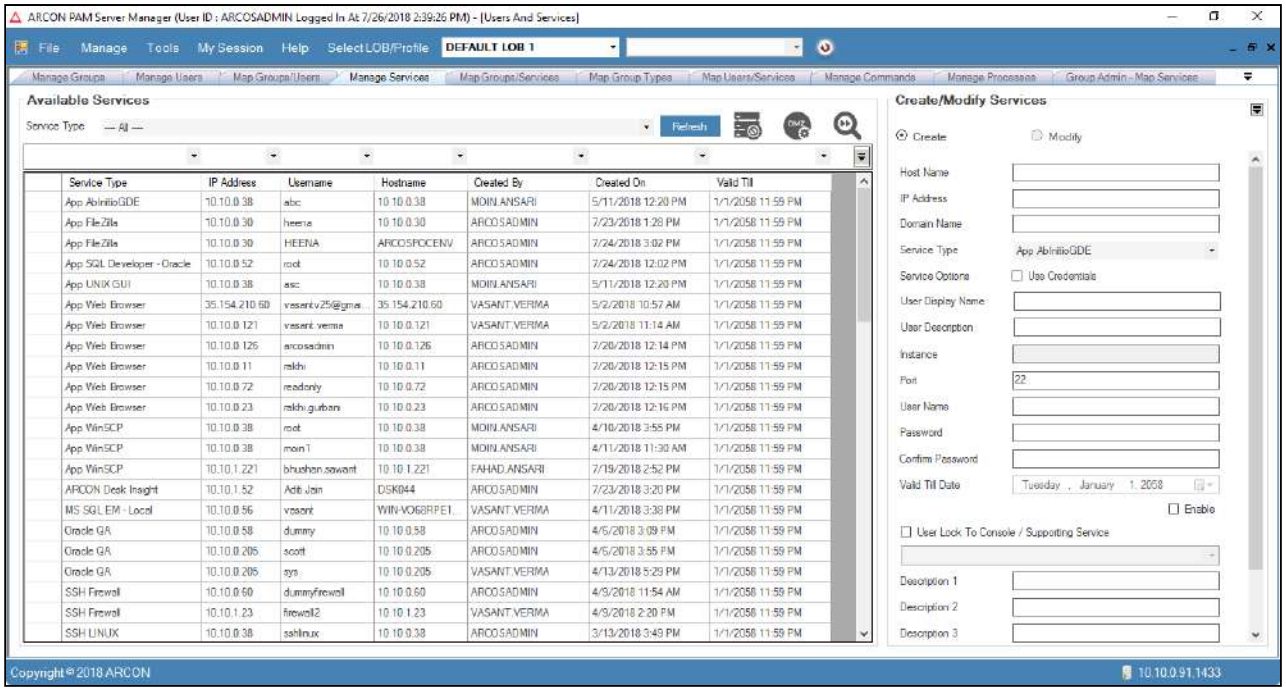
⚠ The Administrator having **Privileged User Discovery & Reconciliation** privilege in Server's Privilege will only be able to view Users created on Server.

To configure Auto Discovery use the following path:

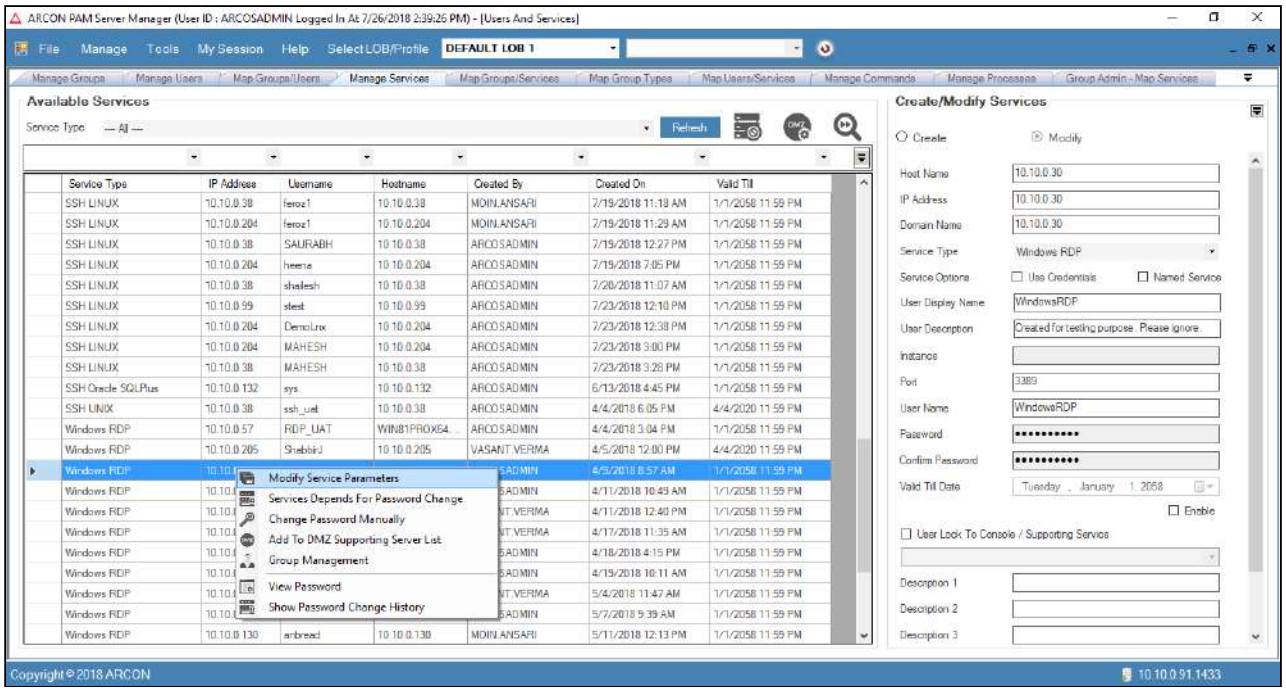
Manage → Users and Services → Manage Services



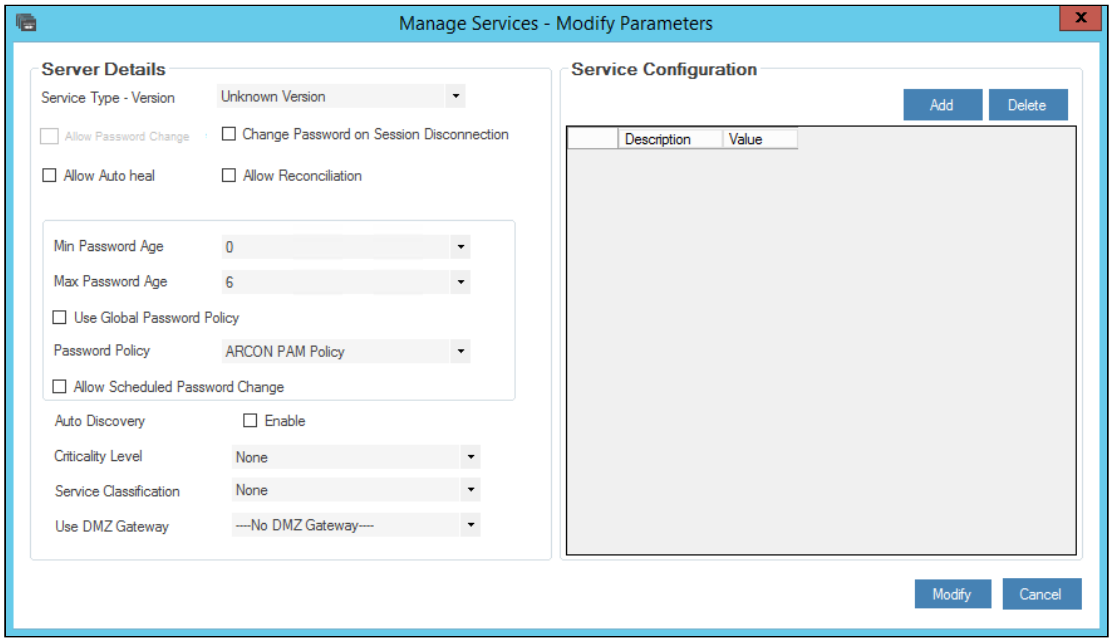
1. Select the type of service such as SSH Linux, or Window RDP from **Service Type** dropdown list and click on **Refresh** button. The services are displayed in the grid.



2. Right click on the service and choose **Modify Service Parameters** option.



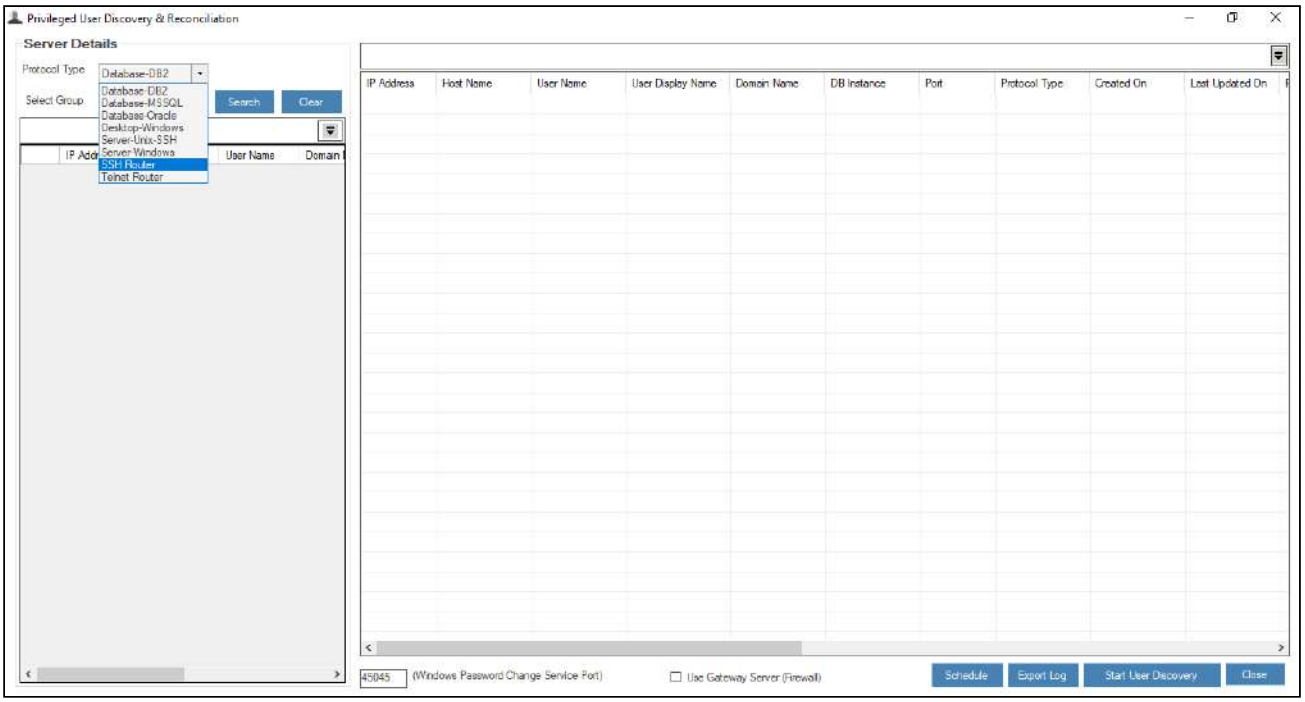
3. Click **Modify Service Parameters** option. The **Manage Services – Modify Parameters** window pops up.



4. Select the **Enable** checkbox besides **Auto Discovery** field and click on **Modify** button to auto discover all the users.

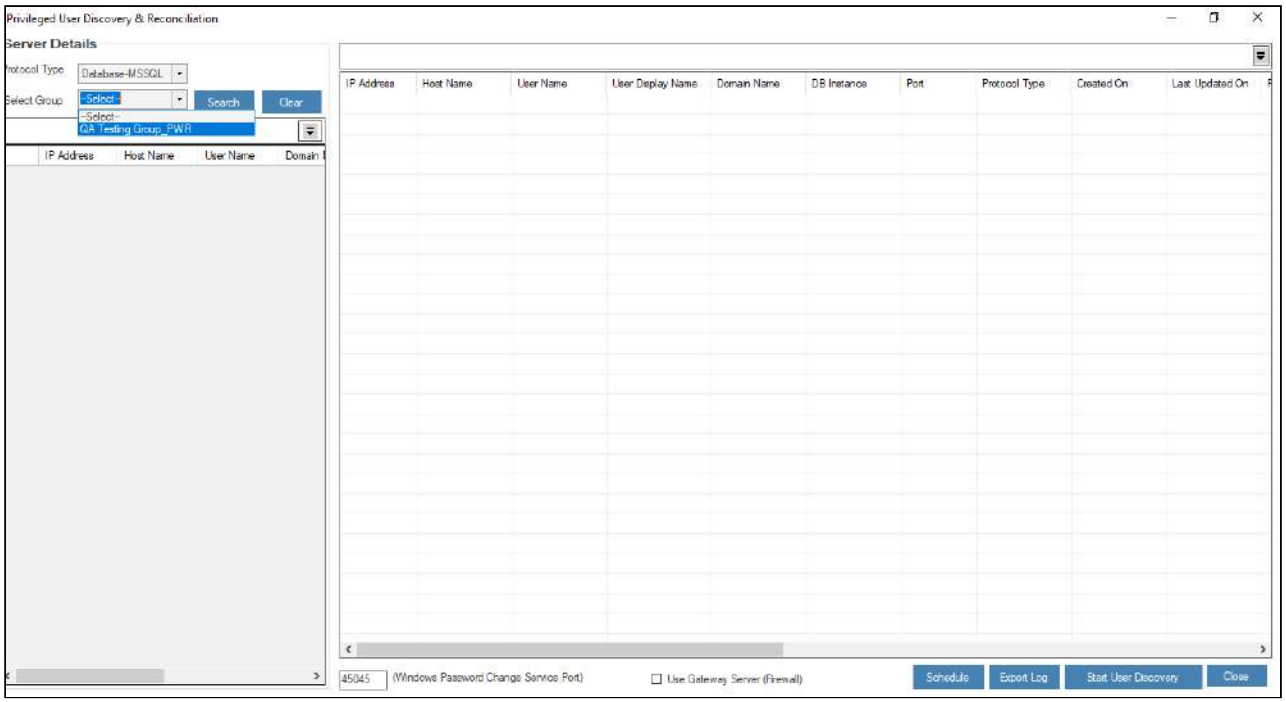
To validate the process use the following path:

Tools → Privileged User Discovery & Reconciliation



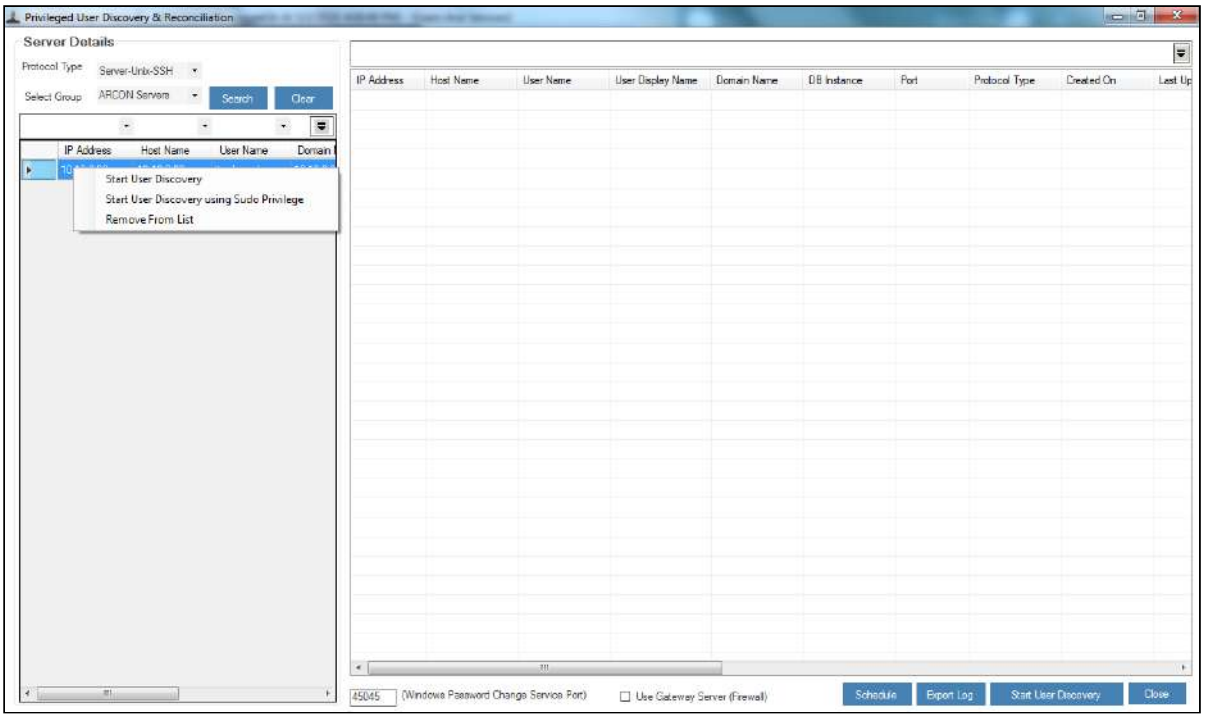
1. Select the type of protocol from **Protocol Type** dropdown list.The following protocol types are displayed in the drop down list:
    a. Database-DB2
    b. Database-MSSQL
    c. Database-Oracle
    d. Desktop-Windows
    e. Server-Unix-SSH
    f. Server-Windows
    g. SSH Router
    h. Telnet Router
2. Select the service group from **Select Group** drop down list and click **Search**. The services which have been enabled for Auto Discovery will be displayed.

> ⚠ To search for a particular service, enter the required details in the **Search** filter field.

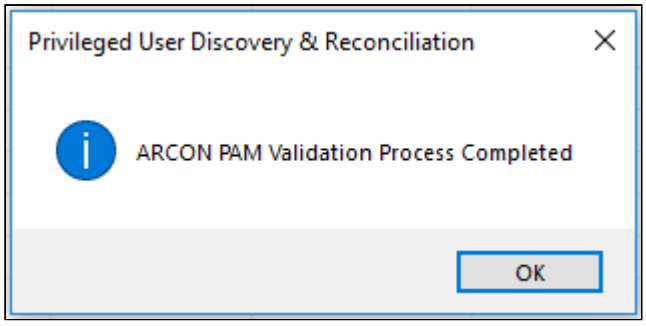


3. Right click on the Service,
    a. Select **Start User Discovery** option to discover users for selected service.
    b. Select **Start User Discovery using Sudo Privilege** option when sudo command is required.

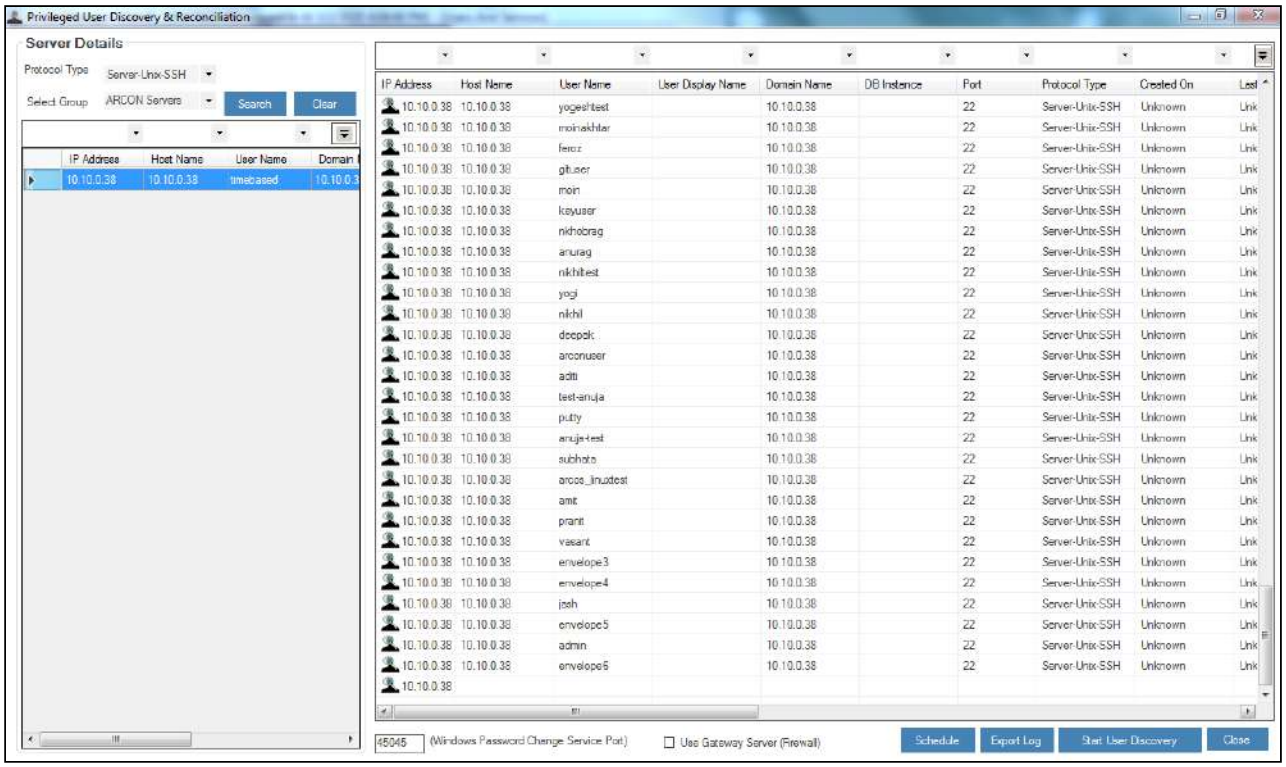
> ⚠ If you do not want to discover users for all services, select the service which you want to delete and click **Delete** button on the keyboard or right click on service and select **Remove From List** option.



4. Click **Start User Discovery** option. A window pops - up with the following message **ARCON PAM Validation Process Completed**.



5. Click **OK** to view the list of all the users belonging to the particular server.

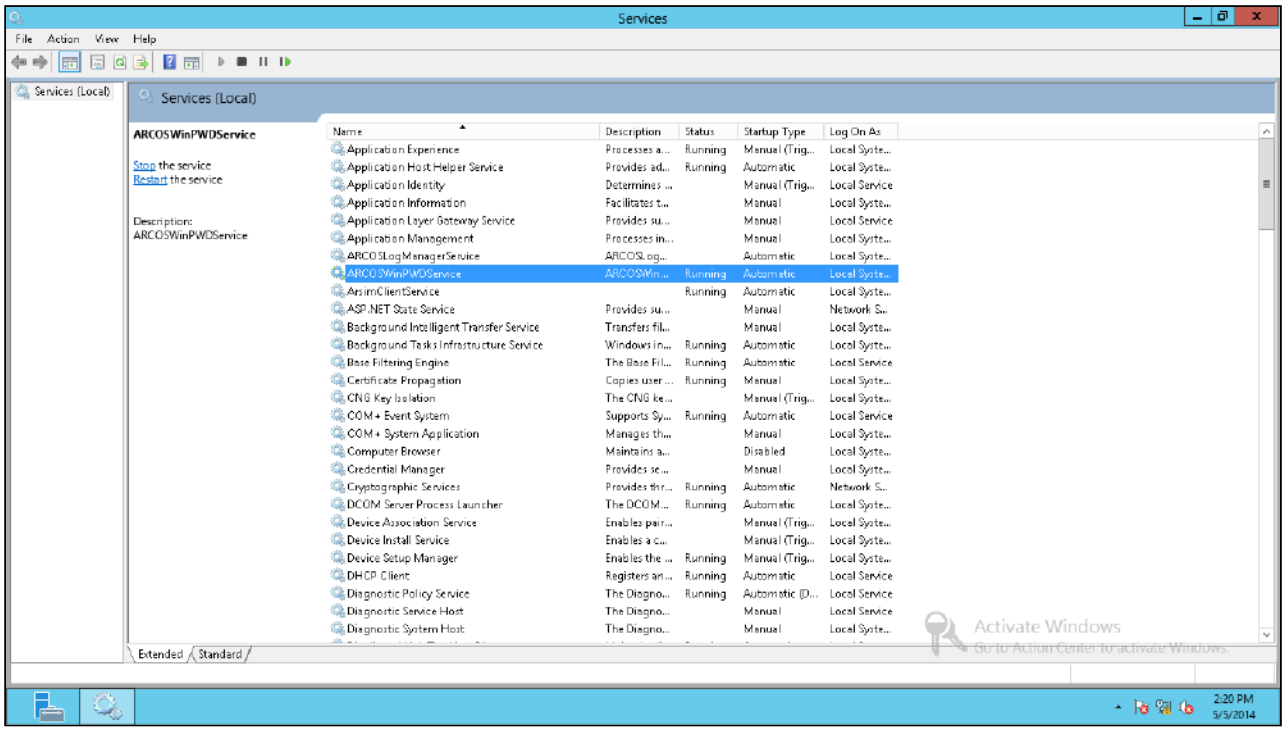


- The port number for Windows RDP based services is 45045.
- **Export Log** button saves or downloads the generated logs in .csv format.
- **Start User Discovery** button allows you auto discover all the users in a sequence on all the target servers.
- **Use Gateway Server (ARCON PAM – Firewall)** routes you to a service through a gateway server.

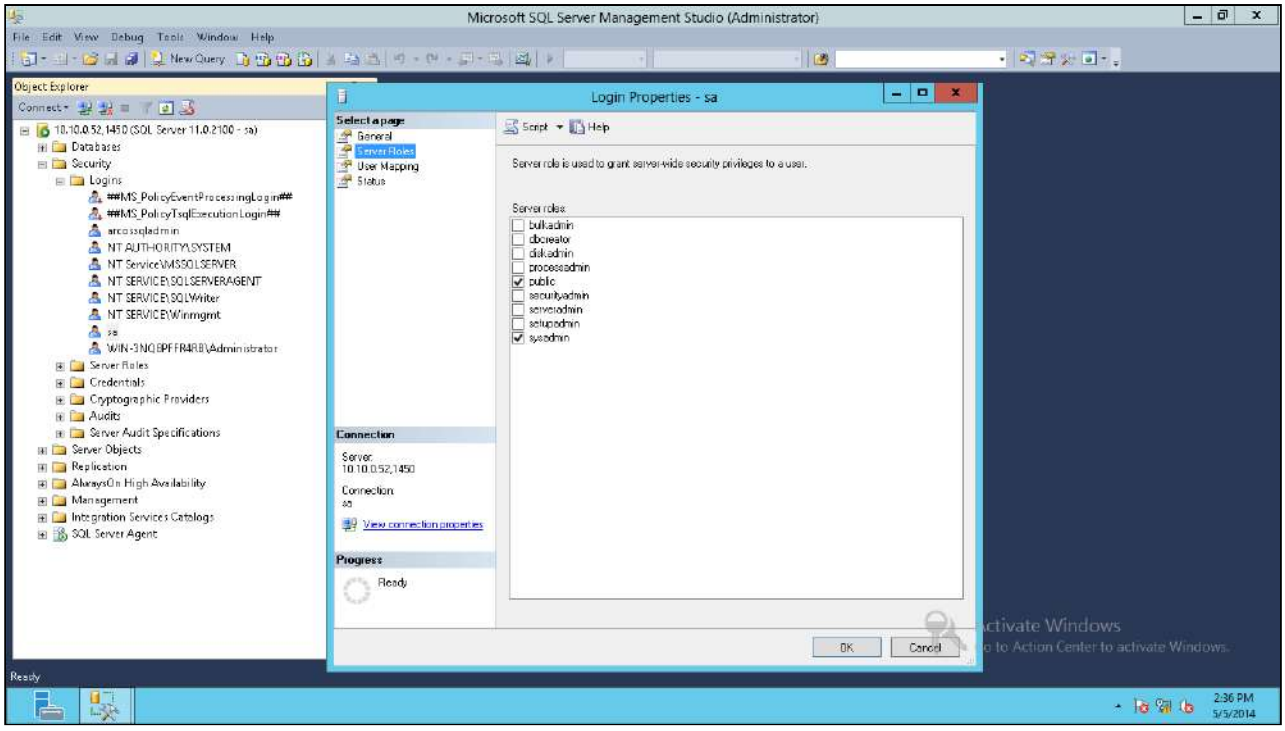
Auto Discovery for particular Service Types:

The auto discovery for a particular service type are as follows:

- **For SSH Based Services:** You need to have "root" account in ARCON PAM for fetching the details.
- **For Windows Based Services:** For windows servers you need to install "**ARCOS win PWD service**" and port"**45045**"should be open from ARCON PAM secured server.



- **For Databases:** MS SQL / SQL QA, For MS-SQL users auto discovery, the sql user should have "sysadmin" rights.



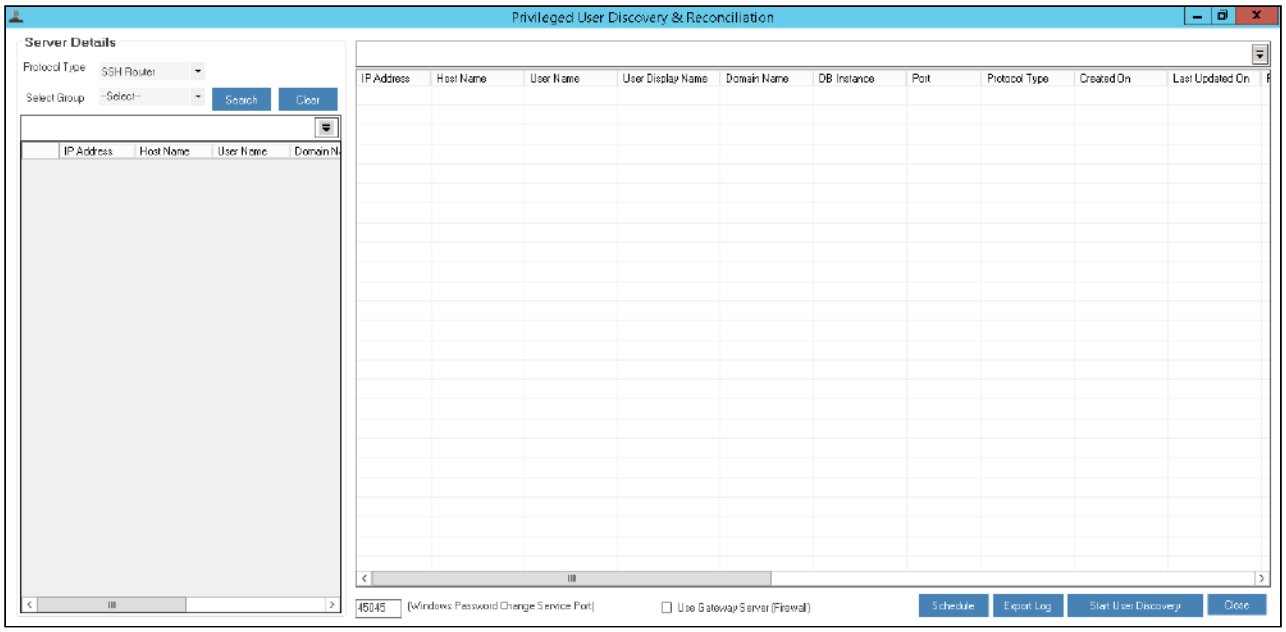
- **SSH Oracle SQL Plus:** You need to have "**Oracle**" user access.

Schedule User Discovery

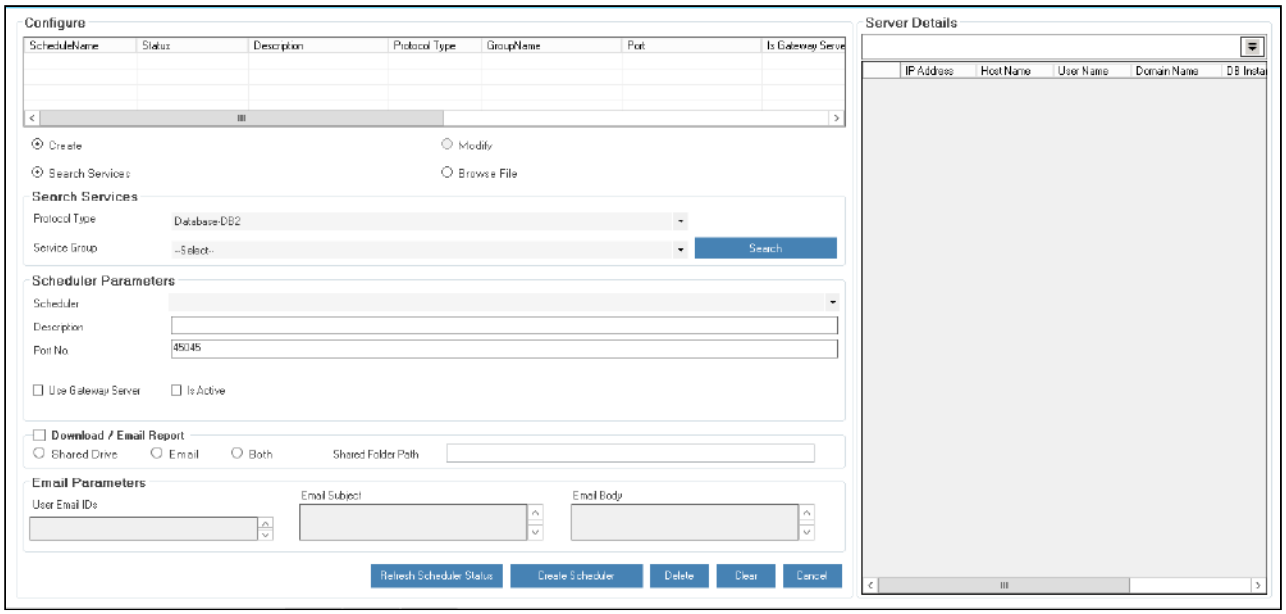
The PAM admin can schedule the Privilege User Discovery using the scheduling option.

To schedule the Privilege user Discovery use the following steps:

1. A schedule option is provided to schedule the "Privilege User Discovery".



2. After clicking on the Schedule option, A Service can either be searched for or can be uploaded for privilege user discovery.



The **Schedule Privilege User Discovery** screen contains the following fields:

Field Name	Description

Create (radio button)	Create a new Privilege User Discovery scheduler.
Modify (radio button)	Modify details of an existing Privilege User Discovery scheduler.
Search Services	A Section Search Services will be displayed on selecting this radio button. a. Select the type of protocol from **Protocol Type** drop down list.The following protocol types are displayed in the drop down list: i. Database-DB2 ii. Database-MSSQL iii. Database-Oracle iv. Desktop-Windows v. Server-Unix-SSH vi. Server-Windows b. Select the service group from **Select Group** drop down list and click **Search**. The services which have been enabled for Auto Discovery will be displayed.
Browse File	Browse File to Upload Services section will be displayed on selecting this radio button. Steps to upload a file. ▪ Click Download file template and save the file to a preferred location on to your local machine. ▪ Open the saved template and enter the required details and save the file. ▪ Copy all the file content in to .txt file and save it. ▪ On the Schedule Privilege User Discovery screen, Browse the .txt file ▪ Click Validate.
Scheduler Parameters	Enter a description for the specific scheduler
Port No.	This field will be displayed automatically
Use Gateway Server	Select this radio button to **(ARCON PAM – Firewall)** routes you to a service through a gateway server.
Is Active	Select this radio button to enable the scheduler to start processing.
Download/ Email Report	Select this radio button to download/ email the user discovery report. ▪ Shared Drive: Select this radio button to share the report on a shared drive ▪ Email: Select this radio button to share the report via email, enter the email address in the field provided. ▪ Both: Select this option to receive the files through email and in shared path. ▪ Shared Folder path: Enter the shared folder path/ email id where the file are to be placed/shared.
Email Parameters	
User Email ID	Specify the email id of the user to whom the email is to be sent.
Email Subject	Specify the subject for the email.
Email Body	Specify the description for the mail.

3. ARCON Privilege User Discovery Windows Service will therefore start user discovery as per the selected scheduler.
4. The discovered data can be viewed and exported.

5. The data can also be sent on email or shared path, which is to be provided while scheduling the privilege user discovery.

11.3 Performance Monitoring Configuration

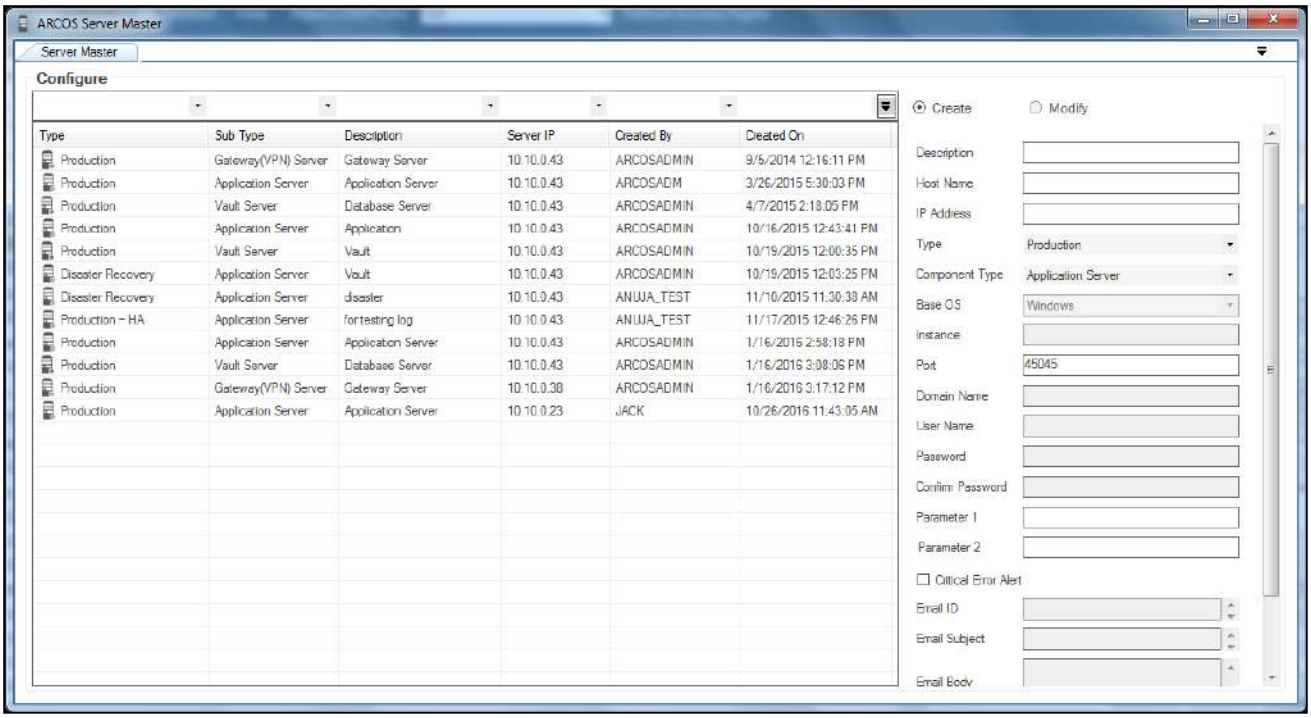
This section monitors the performance of ARCON PAM servers. In addition, it allows adding or modifying servers such as application server, database server, gateway server, and DR servers.

> ⚠ The Administrator having **ARCOS Server Master** privilege in Server's Privileges will only be able to configure details in ARCOS Server Master.

To configure Performance Monitoring:

To configure Performance Monitoring use the following path:

Tools → Advanced Configuration → ARCOS Server Master



The **Server Master** screen contains the following fields:

Field Name	Description
Description	Specify the type of server such as application server, or database server.
Host Name	Specify the hostname of the server.
IP Address	Specify the IP address of the server.

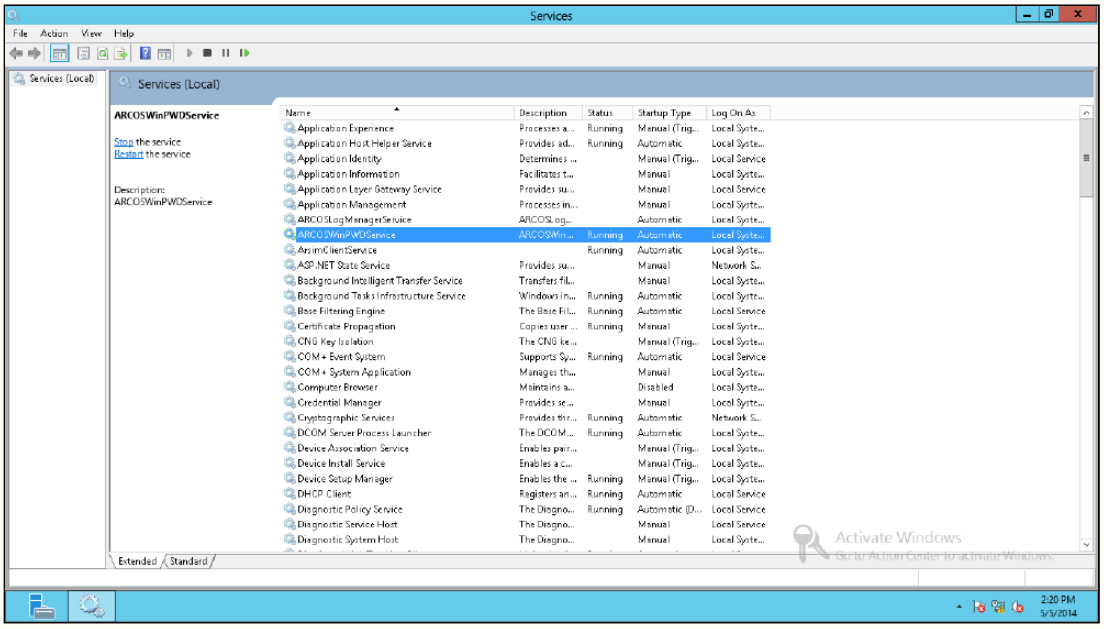
Field Name	Description
Type	Select the type of server. The valid values are: • Production • Production – HA • Disaster Recovery • Disaster Recovery - HA
Component Type	Select the type of component (sub type server). The valid values are: • Application Server • Vault Server • Gateway (VPN) Server
Base OS	Displays the base OS used.
Instance	Specify the instance.(if applicable)
Port	Specify the standard port number.
Domain Name	Specify the domain name.
User Name	Specify the username. ⚠ The data in this field is auto populated, if you select the **Component Type** as **Vault Server**.
Password	Specify the password.
Confirm Password	Re-enter the password and confirm.
Parameter 1	Specify the parameter.(if applicable) ⚠ The data in this field is auto populated, if you select the **Component Type** as **Vault Server**.
Parameter 2	Specify the parameter.(if applicable) ⚠ The data in this field is auto populated, if you select the **Component Type** as **Vault Server**.
Critical Error Alert (checkbox)	Enable the Email ID, Email Subject, and Email Body text field.
Email ID	Specify the email ID of the user.
Email Subject	Specify the subject title for the email.

Field Name	Description
Email Body	Specify the description for the email.
Is Active (checkbox)	Enable the configuration in ARCON PAM.

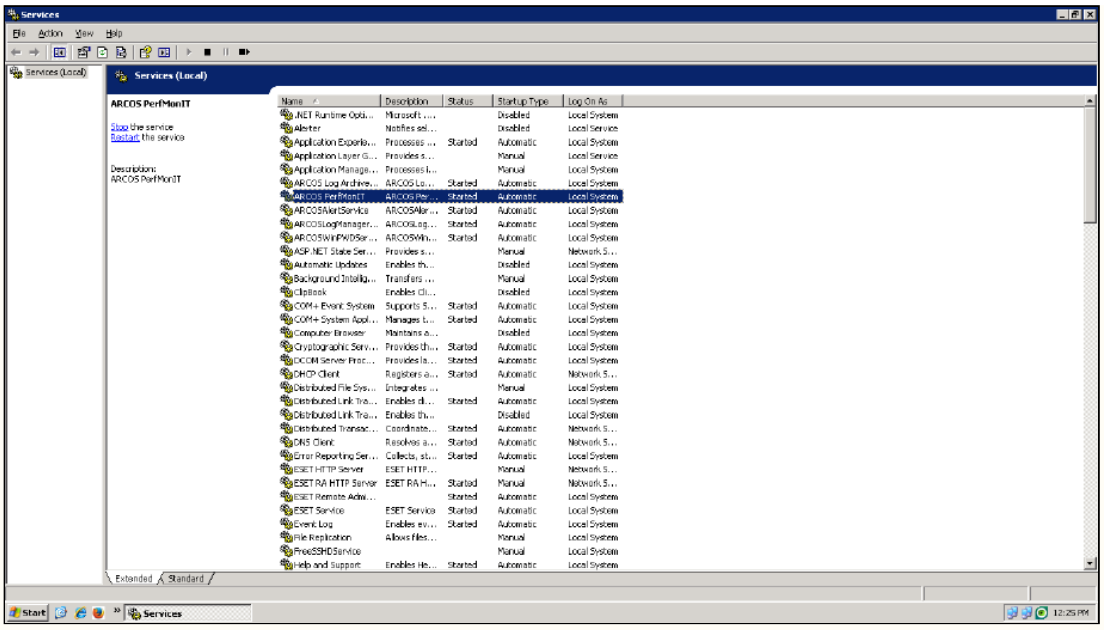
1. Enter/Select the details and click **Create** button. A window pops up with the following message: **New ARCOS Server Created**
2. Click **OK**. The new sever is created.
3. Select the configuration from grid, edit details and click **Modify** to updated the configuration.
4. Select the configuration from grid and click **Delete** to delete the configuration.

⚠

- The win PWD service.exe should be installed on ARCON PAM Servers which is Windows based.
- Port 45045 should be opened from Database Server to all windows based servers (i.e. App and DB servers).
- Port 22 (SSH) should be opened from Database Server to all UNIX based servers (i.e. Secured servers).



- PerformIT service should be installed and running on Application or Database server of ARCON PAM.



11.4 Discovered Devices

This feature helps you to view all the newly discovered devices running in the system. It displays details such as type of service, host name, type of device, name of the windows service, and date/time on which the device was discovered.

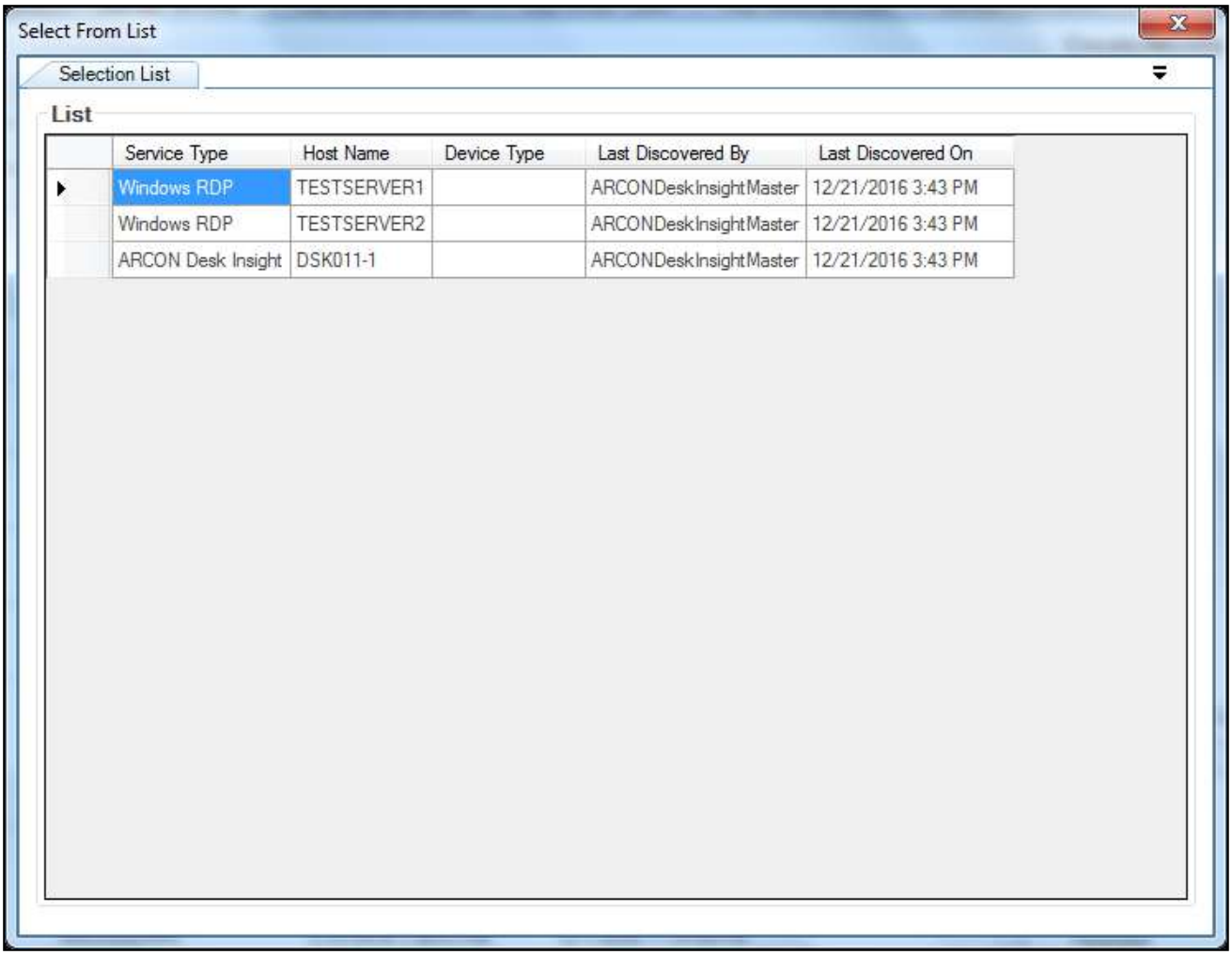
ARCON DeskInsight Master service should be installed on Database Server. Configure device details in **ARCONDeskInsightMaster.ini** file (ARCONDeskInsightMaster.ini file is available in folder on Domain/Application Server where the service has been installed).

⚠ Configure toggle value of **Show List Of Newly Discovered Devices In Server Manager - Is Enabled** as **Enabled** in **Settings** to enable Discovered Devices in Server Manager under the Manage menu.

To view discovered services:

To view discovered services use the following path:

Manage → Discovered Devices



11.5 Real-Time Session Monitoring

Administrative users require privileged account access in their day-to-day roles to maintain systems, perform upgrades and troubleshoot issues. However, these users can also misuse their privileges to gain unauthorized access to sensitive information or cause damage to the IT environment. To deter the misuse of privileges by authorized users, as well as detect malicious activity, organizations should proactively record and monitor all privileged session activity.

Real Time Session Monitoring monitors the live feed of a session. ARCON|PAM Real Time Session Monitoring feature enables monitoring, suspending and terminating activities. You can quickly freeze, unfreeze or logout the session to minimize any potential damage. It increases the control over user's activity.

⚠ The Administrator having **Real Time Session Monitoring** privilege will be able to monitor real time sessions.

Pre-requisites for RTSM configuring in different VLAN

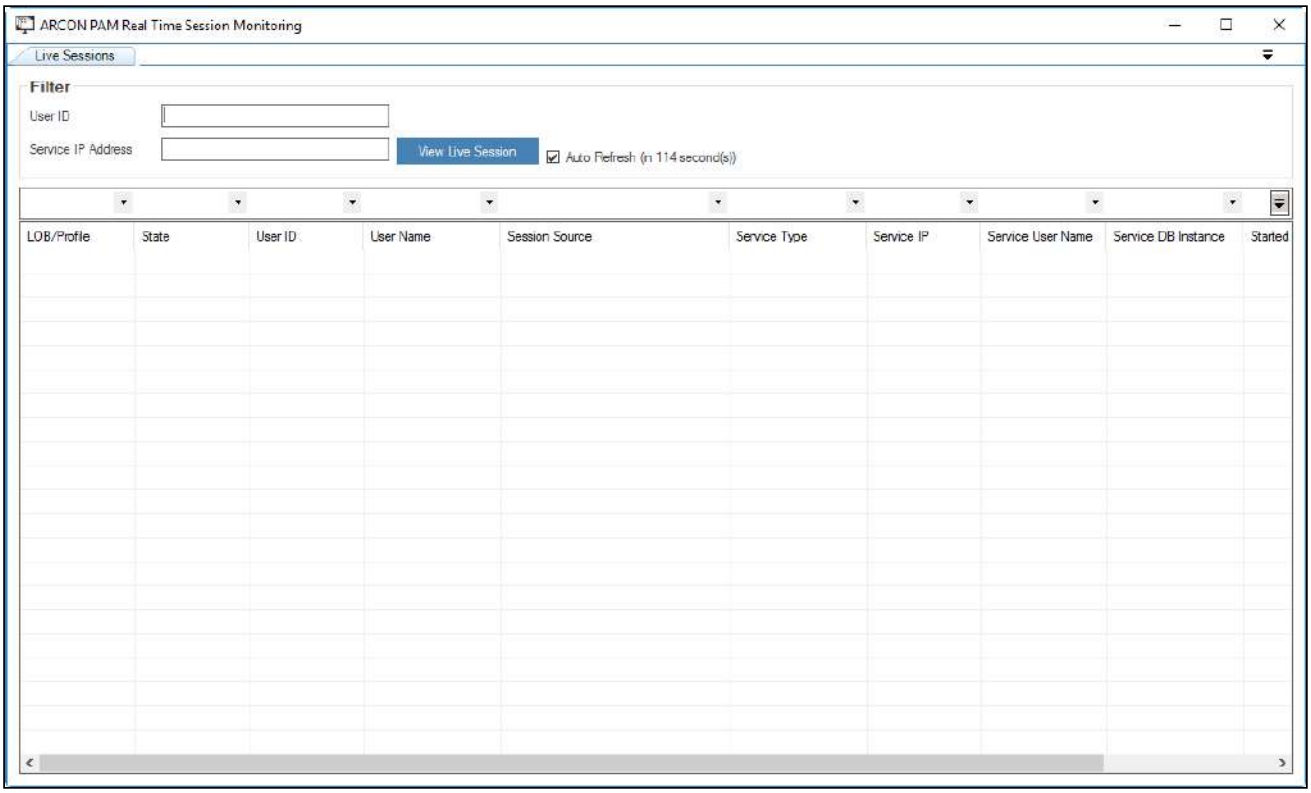
- Ports to be opened- They belong in the range of 12000-13000 which are unidirectional in nature.
- Communication
    - Source: End Machine of ADMIN who wants to see the session

- Destination: Target Machine of PAM user who is initiating the session

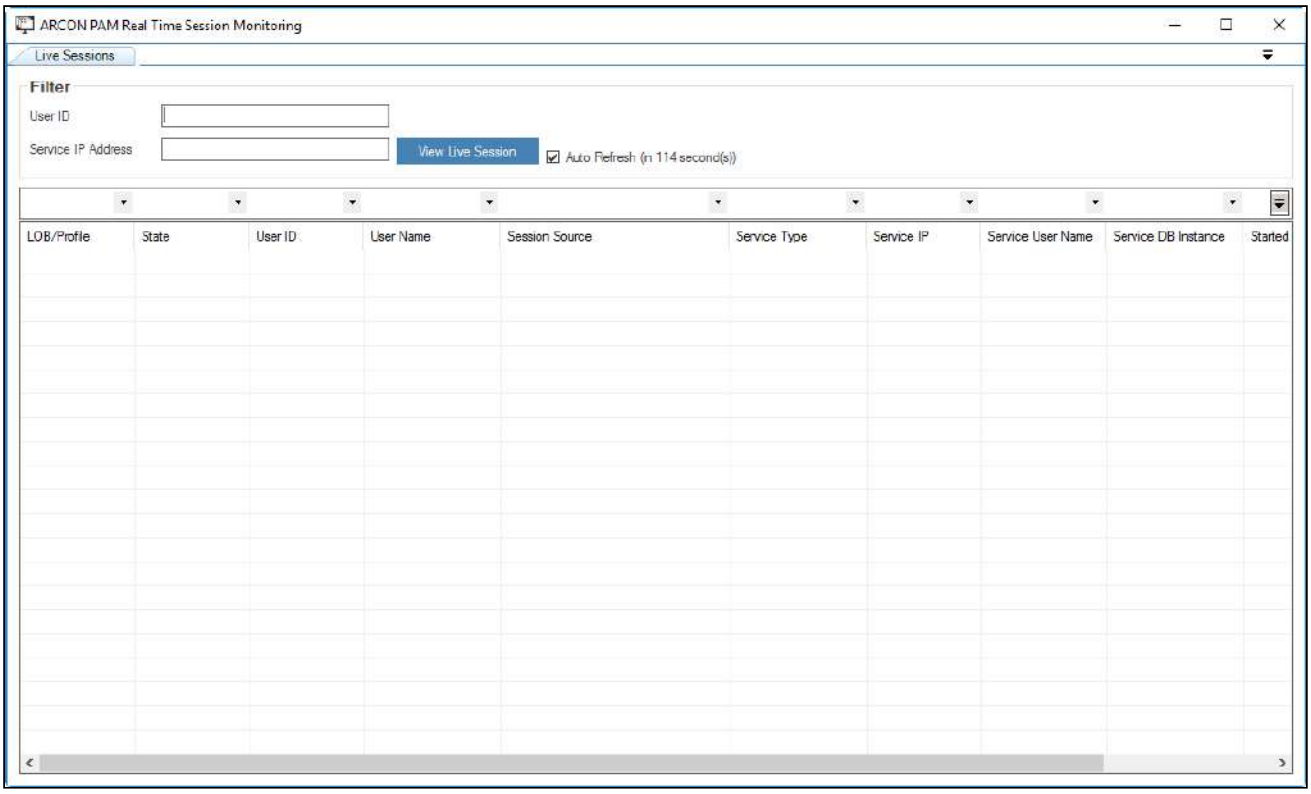
To monitor real time session:

To monitor real time session, use the following path:

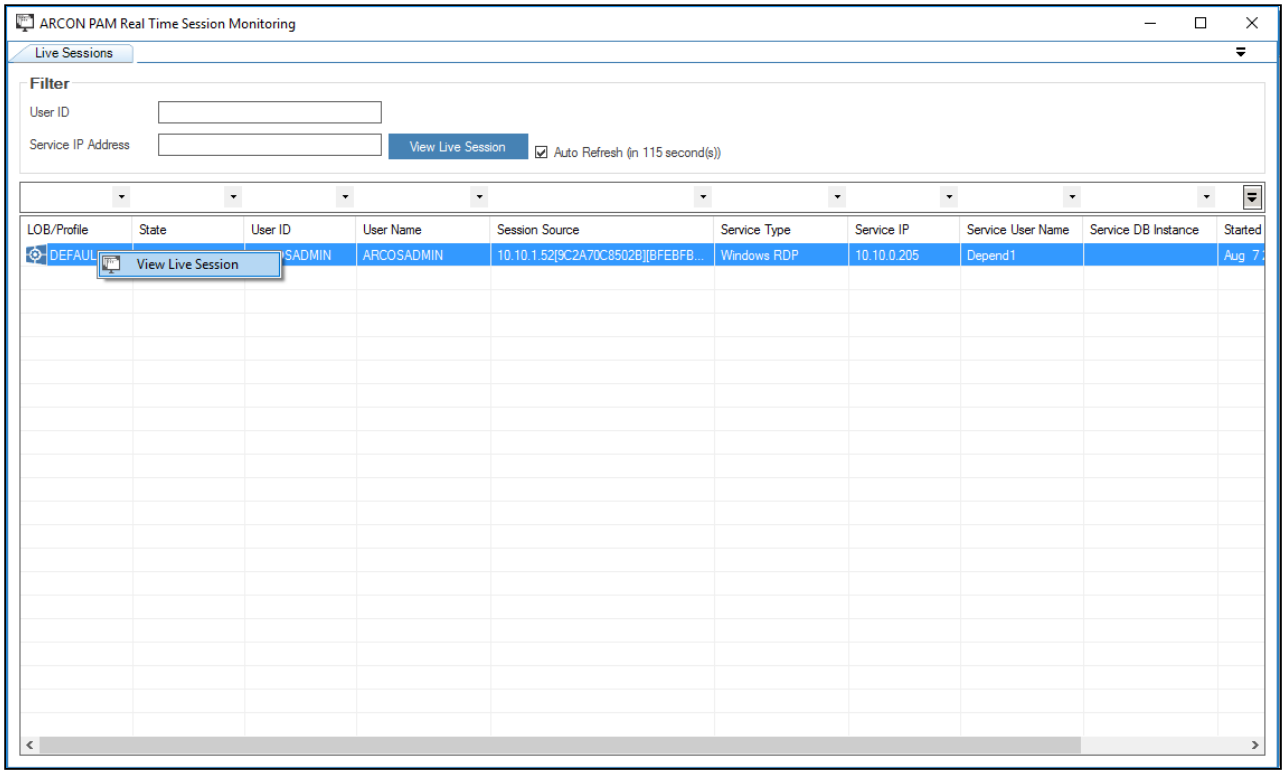
Tools → Real Time Session Monitoring



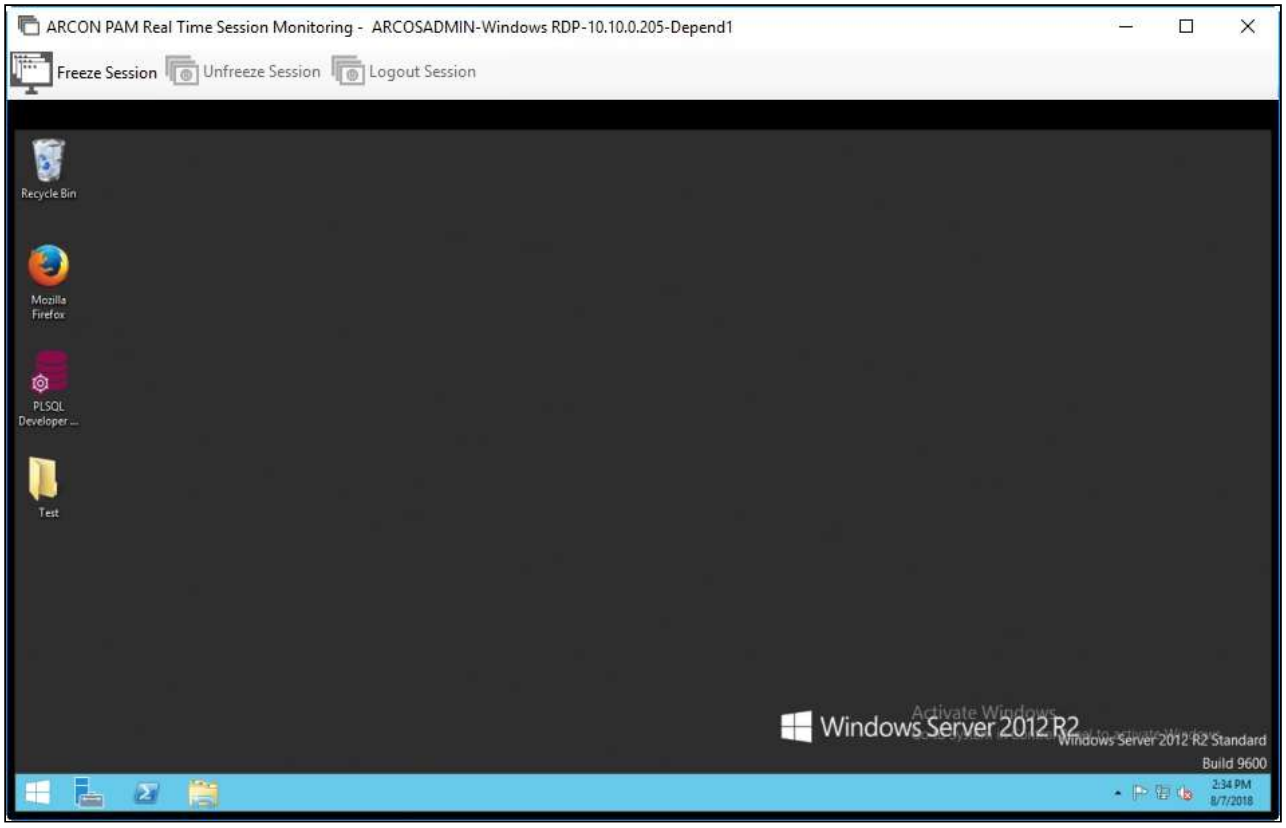
⚠ By default, you can view all the live sessions in the grid. If you want to view live session of a particular user, then enter the User ID or Service IP Address and click **View Live Session** to view the live session of a particular user.



1. Right click on the session and choose **View Live Session** option.



2. Click **View Live Session** option. The live session screen is displayed.



⚠ The Administrator has the privilege to Freeze, Unfreeze or Logout the session.

- **Freeze Session:** It allows to freeze the session being used by the user.

  ⚠ The User shall specify the reason while freezing any session.

- **Unfreeze Session:** It allows to unfreeze the freezed session being used by the user.
- **Logout Session:** It allows to logout the session being used by the user.

  ⚠ The User shall specify the reason while logging out any session.

11.6 Windows Utility

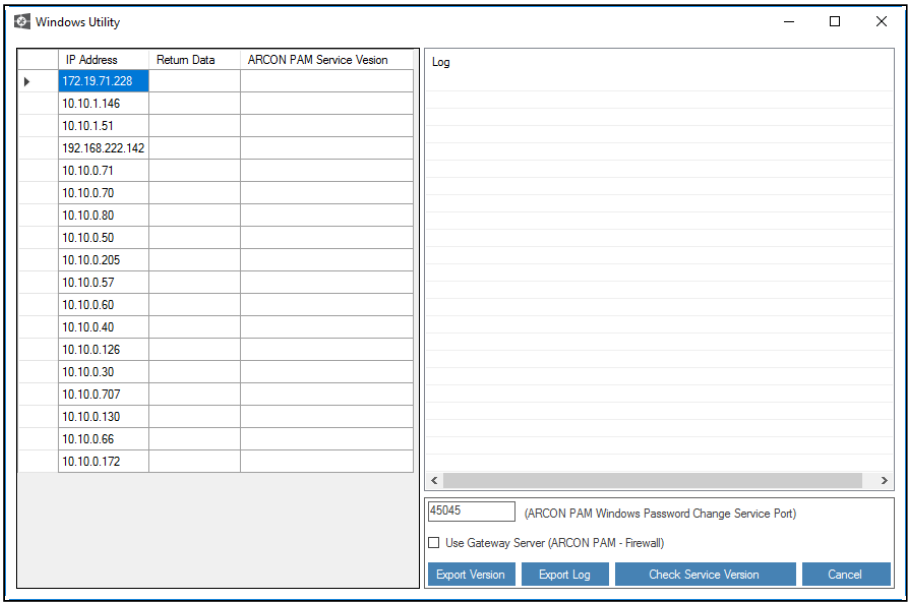
Windows Utility is used to monitor the ARCON PAM PWD service. It checks if the service is running on the windows servers which are defined for password change via ARCON PAM.

Windows Utility will only check whether a password change service is installed or not. This utility is only for Windows connections. If all the servers are equipped with password change service and there is a need to check whether the password change service is installed or not, you can run this utility to validate.

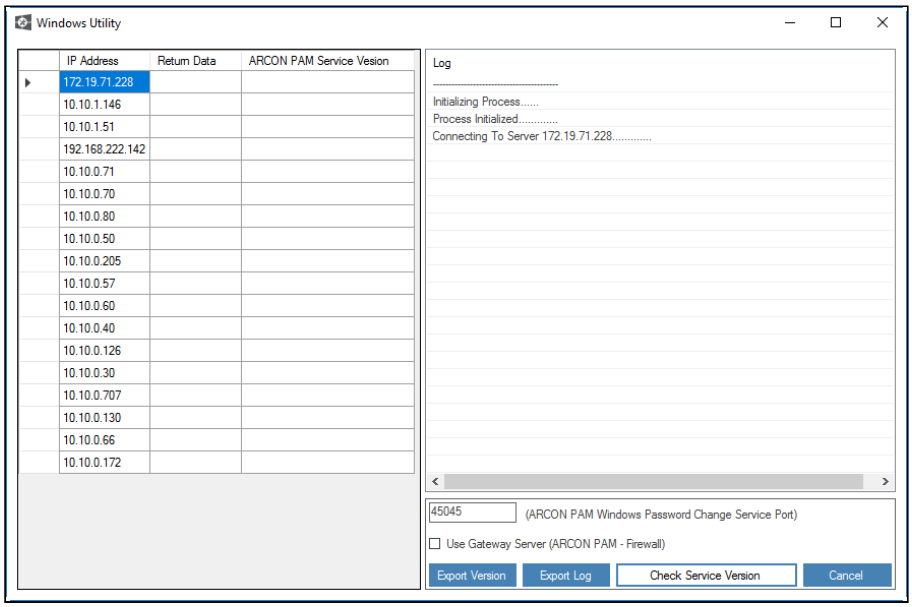
⚠ The Administrator having **Windows Utility** privilege in Server's Privilege will only be able to view version of service.

To navigate to Windows Utility, use the following path:

Tools → Windows Utility



1. Click **Check Service Version**. The status of the log are displayed on the right pane and the services that are connected will display the version on the left pane.



2. If user does not want to gather version information for all services, click on the required service and click **Delete** button on the keyboard or right click on the service and click **Delete** or user can select and drag using mouse and click delete to remove from the list. Similarly, user can check version for a single service by right clicking on it and click **Check Service Version** option.

Status for final output screen:

- Output Status displaying **Service Version** describes that ARCON PAM PWD service is installed on server and its version details are captured.
- Output Status displaying **A Connection Attempt Failed** describes that the connectivity to the destination server is not possible or has some issue reaching the server.

3. **Export Version** button exports version details in excel format and **Export Log** button exports log details in text format.

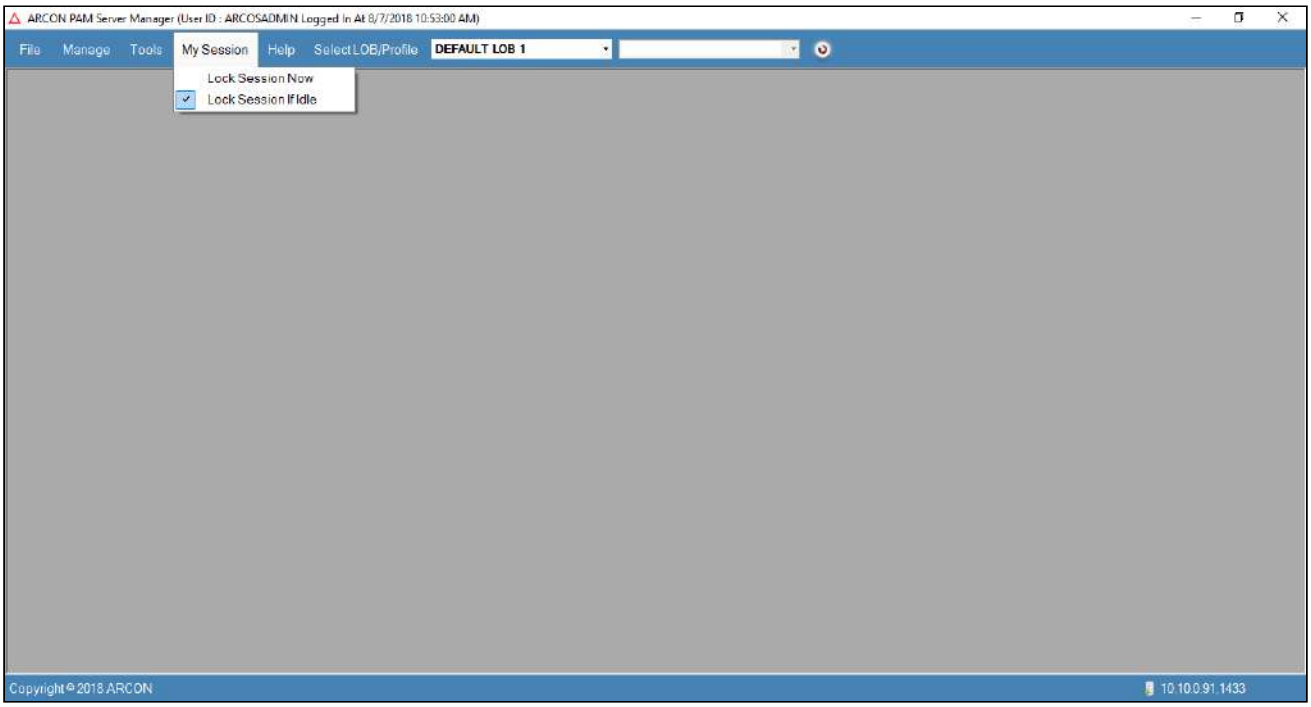
- The password change port number 45045 is displayed in text box against **ARCON PAM Windows Password Change Service Port**.
- You can check the WinPWD Services version via gateway by selecting **Use Gateway Server (ARCON PAM - Firewall)** checkbox.

12 My Session

The Session menu is used to lock the current or active session of Server Manager.

To navigate to **My Session** menu, use the following path:

Server Manager → My Session



The **Session** menu has two features:

- Lock Session Now
- Lock Session If Idle

1. **Lock Session Now** feature is used to immediately lock the current user session.
2. **Lock Session If Idle** feature automatically locks the current user session after a specified time period, if kept idle. If the option is un-checked then the current user session will never get lock.

13 Settings

13.1 Overview

Settings is a prebuilt system with standard specifications, it mainly consists of the preset settings. This was previously a part of the server manager and has been moved independently onto the web. ARCON PAM Settings supports the multilingual feature that displays the settings in many languages like French, German, Arabic, Spanish, Japanese and Korean.

To change the language of Settings select the User Profile icon and select the language.

ARCON PAM Settings help you to know about the configurations in detail. This section includes the following configuration topics:

- LOB
- Group
- User
- Service
- Password
- Alerts and Notification
- Workflow
- Session
- Domain
- Ticket
- Log
- Network/Connection
- API
- General
- My Vault

To Navigate to Settings use the following path:

Manager → Settings

13.2 LOB

This section includes the followings topics:

- Assigned Gateway(s)
- Log Retention
- Service Configuration
- LOB Wise Global Configuration

13.2.1 Assigned Gateway(s)

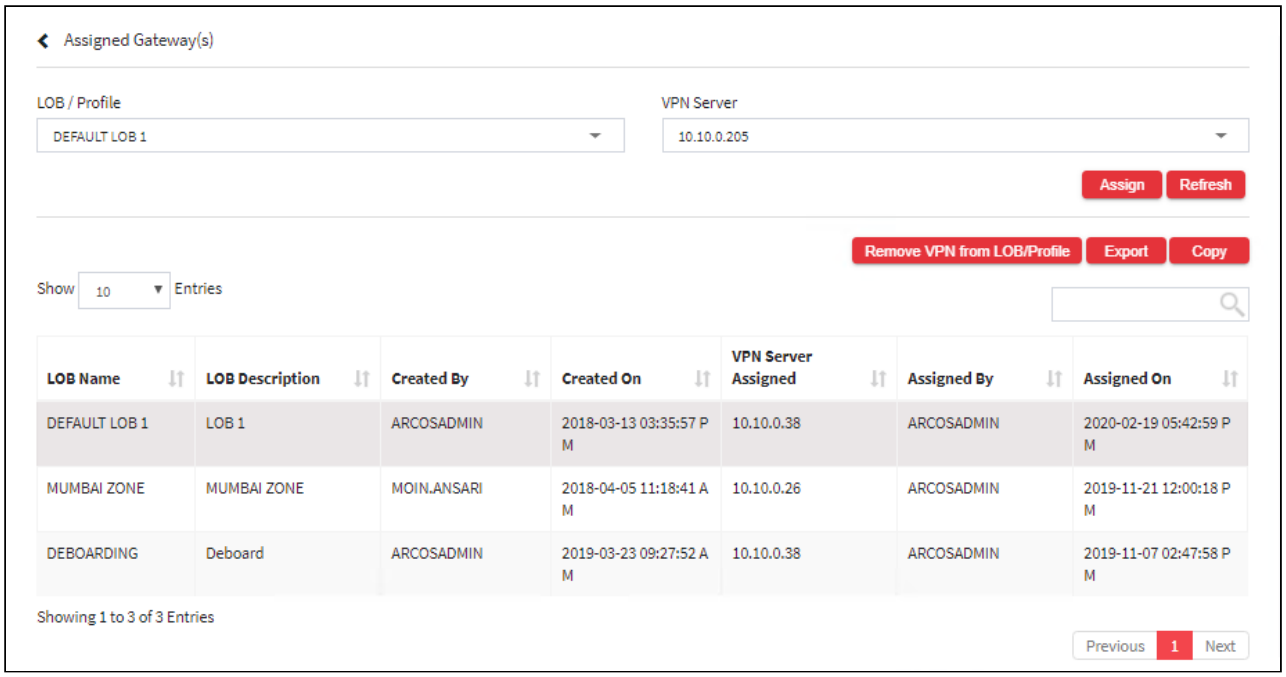
This section helps you to map different LOBs to a particular VPN Server.

The Administrator having **LOB / Profile Default Configuration** privilege in Server's Privileges will only be able to do configurations under LOB / Profile Default Configuration.

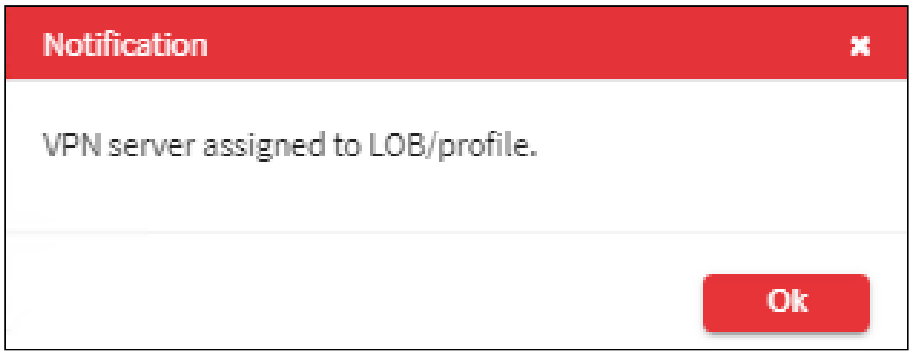
To navigate, use the following path:

Settings → LOB

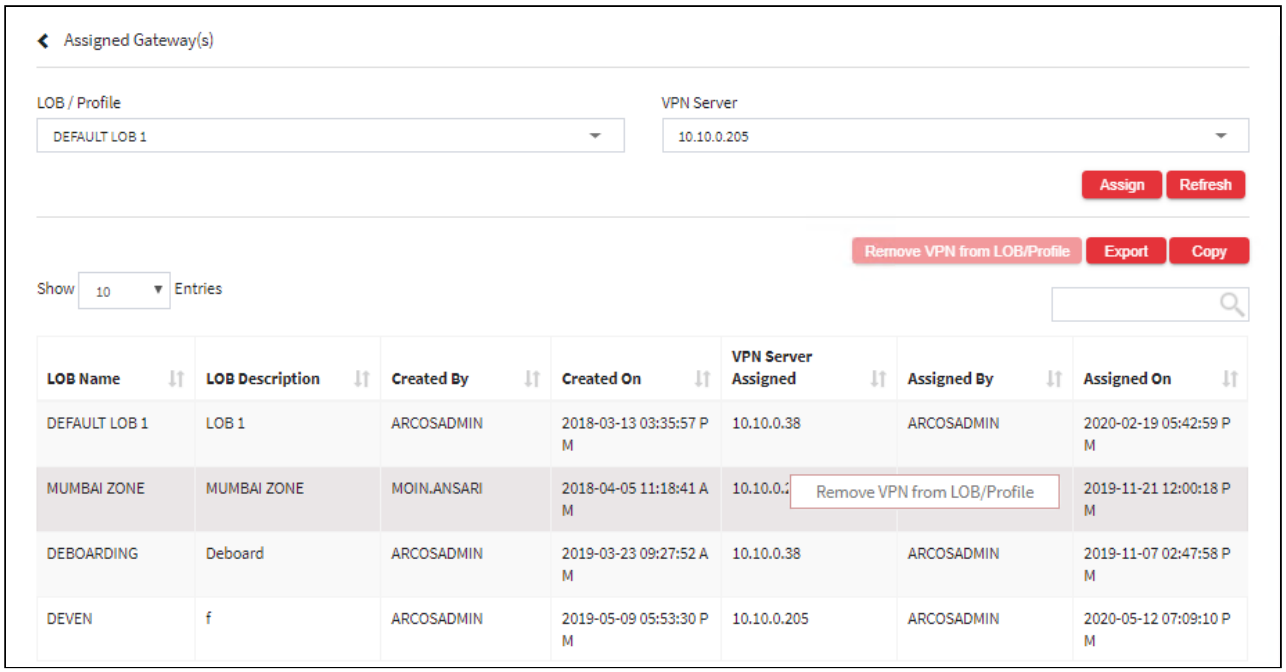
1. Select Assigned Gateway(s).



2. Select the VPN Server from the **VPN Server** dropdown list and click Assign Button.
3. A window pops up with the following message:
   VPN Server Assigned To LOB/ Profile



4. Click **OK**. The LOB is mapped to the particular VPN Server.
5. To remove the VPN server from LOB Profile select the row and click Remove VPN server from LOB Profile. Also, you can right-click on the row and select Remove VPN server from LOB Profile.



6. The Export button will export all the Assigned Gateway(s) details in the form .xlsx format. The Copy button will copy all the details of the table.

13.2.2 Log Retention

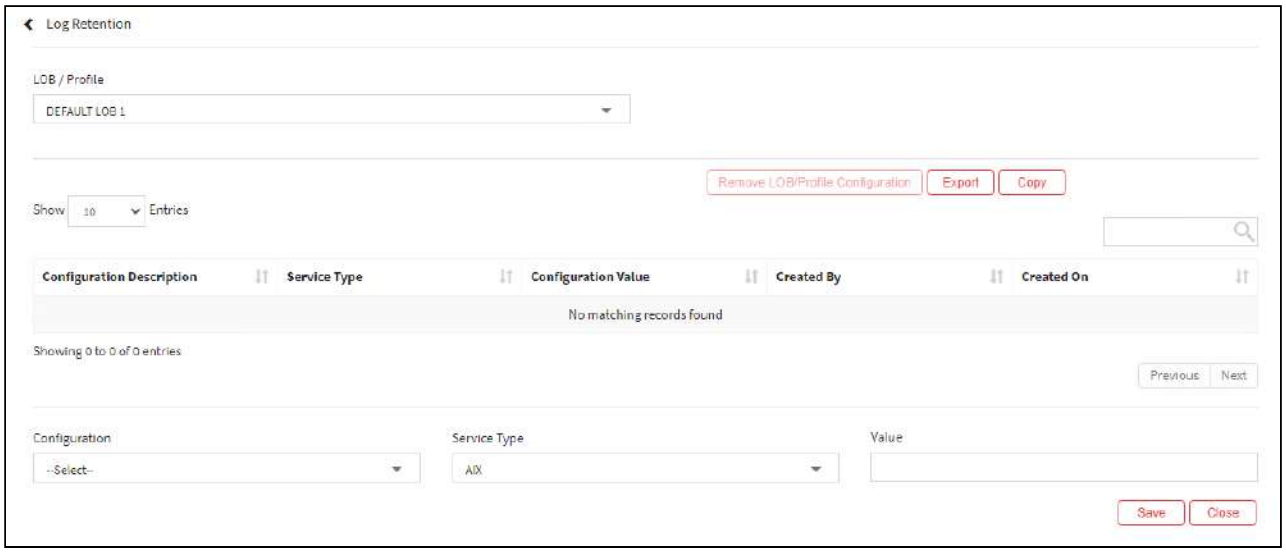
Log Retention helps you to retain command and session logs. You can enable or disable these logs for particular number of days.

> ⚠ The Administrator having **LOB / Profile Default Configuration** privilege in Server's Privileges will only be able to do configurations under LOB / Profile Default Configuration

To navigate, use the following path:

Settings → LOB

1. Select Log Retention.



The **LOB/ Profile Configuration** screen contains the following fields:

Field Name	Description
LOB/ Profile	Select the LOB.
Configuration	Select the configuration, to configure command and session logs. User can enable or disable these logs for particular number of days. The valid values are: **Command Log Retention – Enable:** To specify how long activity log information is kept in the database. Select this command to manage the activity log records by date or size. The activity log contains normal activity messages generated by the server. These messages include information about server and client operations, such as the start time of sessions or device I/O errors. Activity log information includes messages, such as the following: ▪ Client session starts and ends ▪ Migration starts and ends ▪ Diagnostic error messages ▪ Scheduled administrative command output User can choose to adjust the length of time that the activity log retains messages to avoid insufficient or outdated data. The server automatically removes the messages from the activity log after the retention period ends. **Command Log Retention – Days**: Number of days to retain entries in the change log. The default value is 90 days. **Session Log Retention – Enable**: Used to retain session log. It works as same as command logs the only difference is that it generates video logs of user activities captured by ARCON PAM. **Session Log Retention – Days**: User can retain session logs days as much as user want. By default, the value is 90 days.
Service Type	User can also retain command and session logs for particular type of service.

Field Name	Description
Value	Used to set value to enable or disable command or session log retention. The valid values are: ▪ 0: Disable ▪ 1: Enable User can also set days in this field for both the logs as much as user want. By default, the value is 90days.

2. Enter the details and click **Save** button. A window pops up with the following message: **LOB/Profile Configuration Saved Successfully**

3. Click **OK**. The settings are successfully configured.

13.2.3 Service Configuration

To navigate, use the following path:

Settings → LOB->Service Configuration

Field Name	Description
LOB - Share All Users	**This configuration enables/disables the sharing of users between LOBs.**
Disable	If Toggle value is 'Disabled', then it disables the sharing of users between LOBs.
Enable	If Toggle value is 'Enabled', then it enables the sharing of users between LOBs.
Remove From User Group If User Removed From LOB/Profile - Is Enabled	**This configuration enables/disables the removal of User Group Mapping if the User is removed from LOB.**
Disable	If Toggle value is 'Disabled', and the user is removed from LOB then User Group mapping for that particular LOB will be retained.
Enable	If Toggle value is 'Enabled', and the user is removed from LOB then User Group mapping for that particular LOB will be removed.

Field Name	Description
Remove Service Mapping If User Removed From LOB/Profile - Is Enabled	**This configuration enables/disables removal of Service Mapping if User is removed from LOB.**
Disable	If Toggle value is 'Disabled', and the user is removed from LOB then service mapping for that LOB will be retained from the backend.
Enable	If Toggle value is 'Enabled', and the user is removed from LOB then service mapping for that particular LOB will be removed.
Service Access Expiry Reminder to User (Hours)	**This configuration sends an email notification to the User prior to the number of hours set here stating that his time based or one time service access is going to expire.**
Valid Values	The range is from 0-100 hours. By default value is 0. If '0' is set then no email will be sent.
Shift Start Time	**This Configuration sets the start time value. It means any service which critically high and is accessed before this time will be captured in Service Access Off Production Hrs Report in ACMO.**
Valid Values	Enter the start time.
Shift End Time	**This Configuration sets the end time value. It means any service which critically high and is accessed after this time will be captured in Service Access Off Production Hrs Report in ACMO.**
Valid Values	Enter the end time.
Display All Option for LOB	**This configuration enables/disables LOB dropdown for Scheduled Report master and for all the reports in ACMO.**
Disable	If Toggle value is 'Disabled', then LOB dropdown is not visible in Scheduled Report master.
Enable	If Toggle value is 'Enabled', then LOB dropdown is visible in Scheduled Report master
Auto Revoking of User-Service Mapping	**This configuration revokes the services of the user based on the number of days configured in this configuration.**
Valid Values	Enter the number of days after which the service will be revoked.

Field Name	Description
Auto Revoking of User-Service Mapping LOB Wise- Is Enabled	**This configuration revokes the services of the user LOB Wise.**
Disable	If Toggle value is 'Disabled', then the number of days cannot be configured under LOB Wise Global configuration
Enable	If Toggle value is 'Enabled', then configure the number of days of Auto Revoking of User-Service Mapping LOB Wise under LOB Wise Global configuration. Its value ranges from 0-999.

13.2.4 LOB Wise Global Configuration

LOB Wise Global Configuration screen helps in setting the configuration at a global level. The following settings can be configured directly at the LOB level

- Windows RDP- Allow Clipboard to All
- Automate User and service mapping when User added in User Group- Is Enabled
- Automate User and Service mapping when Service added in Service Group- Is Enabled
- Auto Revoking of User-Service Mapping Lob Wise- Is Enabled

A. Windows RDP- Allow Clipboard to All

This configuration enables/disables Clipboard by default for all the Windows RDP session taken through ARCON PAM at LOB level.

B. Automatically Assign Users to all Services

The Administrator has to enable the **LOB wise Global Configuration** to automatically assign all services to newly added Users in the User Group. If the LOB wise Global Configuration is disabled and you add a User to User Group, then services are not assigned to the User. When the LOB wise Global Configuration value is enabled and you add a User to the User group, the services are automatically assigned to the User only for configured LOB. Whereas, services will not be assigned to Users who were added to User group before the LOB wise Global Configuration value was enabled.

Pre-requisites:

- The User Group should be present in the domain.
- The Server Group should be present in the domain.
- It is mandatory for the Administrator to map the User Group to the Server Group in the domain.

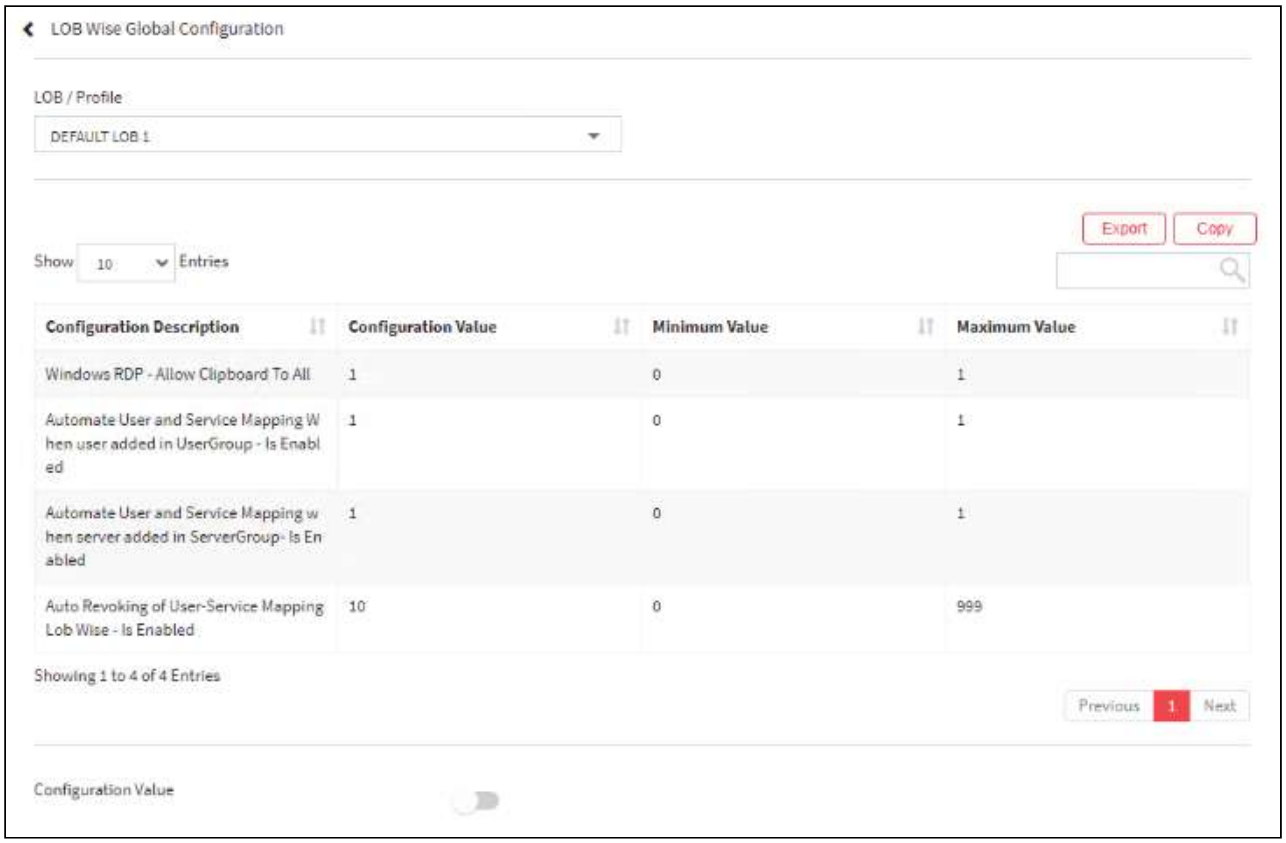
⚠

- Services will not be mapped to User in other than configured LOB.
- It is mandatory to map the User Group to Server Group before starting the automation of Users to Services or Services to Users.
- To configure **LOB wise Global Configuration**, the Administrator should have **LOB wise Global Configuration** privileges under Server's Privileges.

To automatically map User to Services, follow the below steps:
To navigate, use the following path:

Settings → LOB

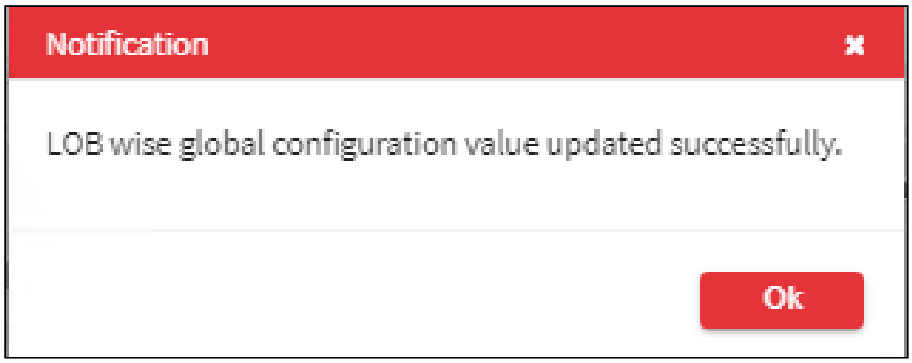
1. Select LOB wise Global Configuration.
2. Select the LOB from **LOB/Profile** dropdown list for which you want to automate mapping.



3. For changing the details of **Automate User and Service Mapping When user added in UserGroup – Is Enabled** click on the existing row and change the Configuration value via the toggle button.

> ⚠ By default, the **Configuration Value** is disabled, enable the toggle to enable LOB wise global configuration.

4. A window pops up with the following message: **LOB Wise Global Configuration Value Updated Successfully.**



5. Click **OK**. The LOB wise global configuration to automate the user and service mapping when user is added in User Group is configured successfully.
6. Click **Close** button to close the **LOB Wise Global Configuration** window.
7. In the Server Manager, click **Manage → Users and Services → Map Group/Users .**
8. Map User to User Group.

   ⚠ For more information refer **Map User to User Group.**

9. On mapping the **User** to **User Group**, as the **LOB wise Global Configuration** for automation is enabled, the **User** in configured LOB is automatically assigned the **Services** present in the mapped **Server Group.**

C. Automatically Assign Services to All Users

The Administrator has to enable the LOB wise Global Configuration to automatically assign all Users to newly added Services in Server Group. If the LOB wise Global Configuration value is disabled and you add a Service to Server Group, then Users are not assigned to the Service. When the LOB wise Global Configuration is enabled and you add a Service to Server group, the Users are automatically assigned to the Service only for configured LOB. Whereas, Users will not be assigned to Services which were added to Server group before the LOB wise Global Configuration value was enabled.

Pre-requisites:

- The User Group should be present in the domain.
- The Server Group should be present in the domain.
- It is mandatory for the Administrator to map the User Group to the Server Group in the domain.

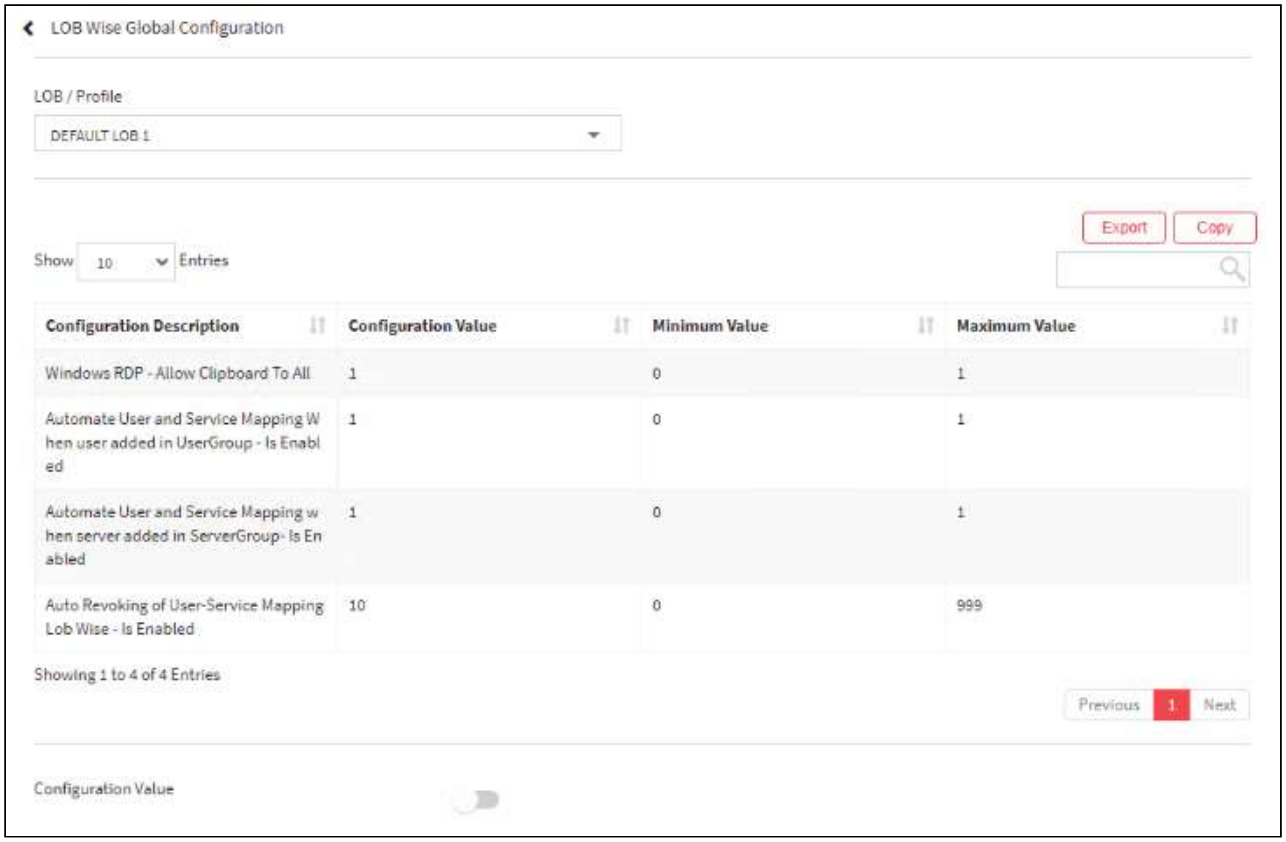
⚠

- Users will not be mapped to Service in other than configured LOB.
- It is mandatory to map the User Group to Server Group before starting the automation of Users to Services or Services to Users.
- To configure **LOB wise Global Configuration**, the Administrator should have **LOB wise Global Configuration** privileges under Server's Privileges.

To automatically map User to Services, follow the below steps:
To navigate, use the following path:

Settings → LOB

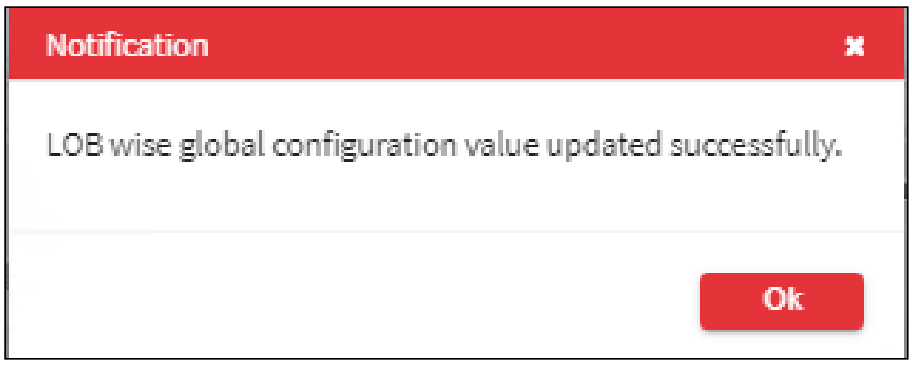
1. Select LOB wise Global Configuration.
2. Select the LOB from **LOB/Profile** dropdown list for which you want to automate mapping.



3. For changing the details of **Automate User and Service Mapping When server added in ServerGroup – Is Enabled.** Click on the existing row and change the Configuration value via the toggle button.

> ⚠ By default, the **Configuration Value** is disabled, enable the toggle to enable LOB wise global configuration.

4. A window pops up with the following message: **LOB Wise Global Configuration Value Updated Successfully.**



5. Click **OK**. The LOB wise global configuration to automate the user and service mapping when a user is added in User Group is configured successfully.

6. Click **Close** button to close the **LOB Wise Global Configuration** window.
7. In the Server Manager, Click **Manage → Users and Services → Map Group/Services.**
8. Map Service/s to Server Group.

   ⚠ For more information refer **Map Services to Server Group.**

9. On mapping the **Services** to **Server Group**, as the **LOB wise Global Configuration** for automation is enabled, the **Service/s** in configured LOB is automatically assigned to the **User** present in the mapped **User Group.**

D. Auto Revoking of User-Service Mapping Lob Wise- Is Enabled

This configuration revokes the services of the user LOB Wise after the number of days set here.

⚠ **Auto Revoking of User-Service Mapping LOB Wise- Is Enabled** in Service Configuration **in Settings** should be **enabled** first.

13.3 Group

This section includes the following topics:

- Apply Password Settings
- Apply Command Profile
- 2FA
  - USER DOOR ACCESS
  - BIOMETRIC
- Machine Control
- ACMO
- Alerts
- Mapping

13.3.1 Apply Password Settings

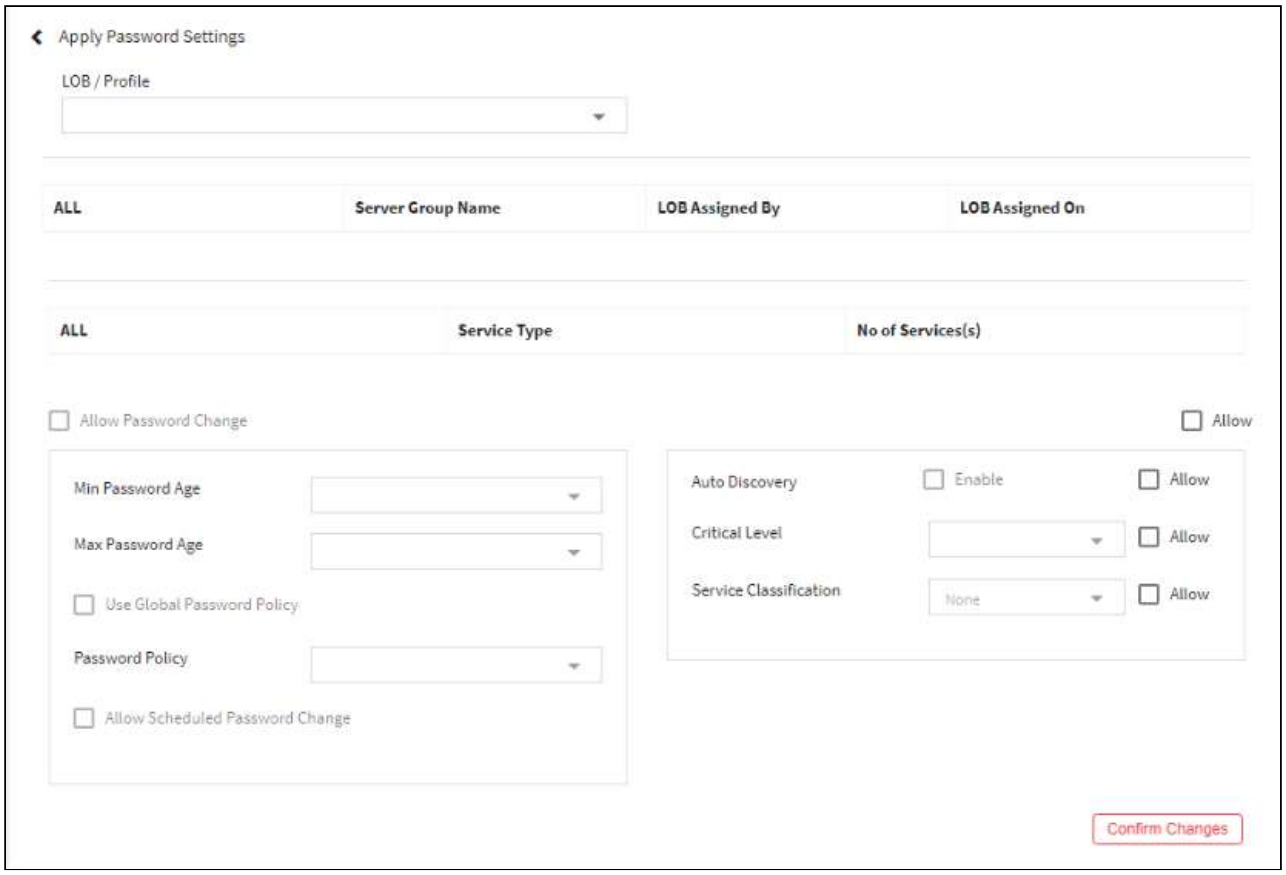
This section helps you to configure the settings for password, wherein you can define a policy at a group level, you can configure the minimum or maximum age of the password, and also schedule the password change process.

⚠ The Administrator having **LOB / Profile Default Configuration** privilege in Server's Privileges will only be able to do configurations under LOB / Profile Default Configuration.

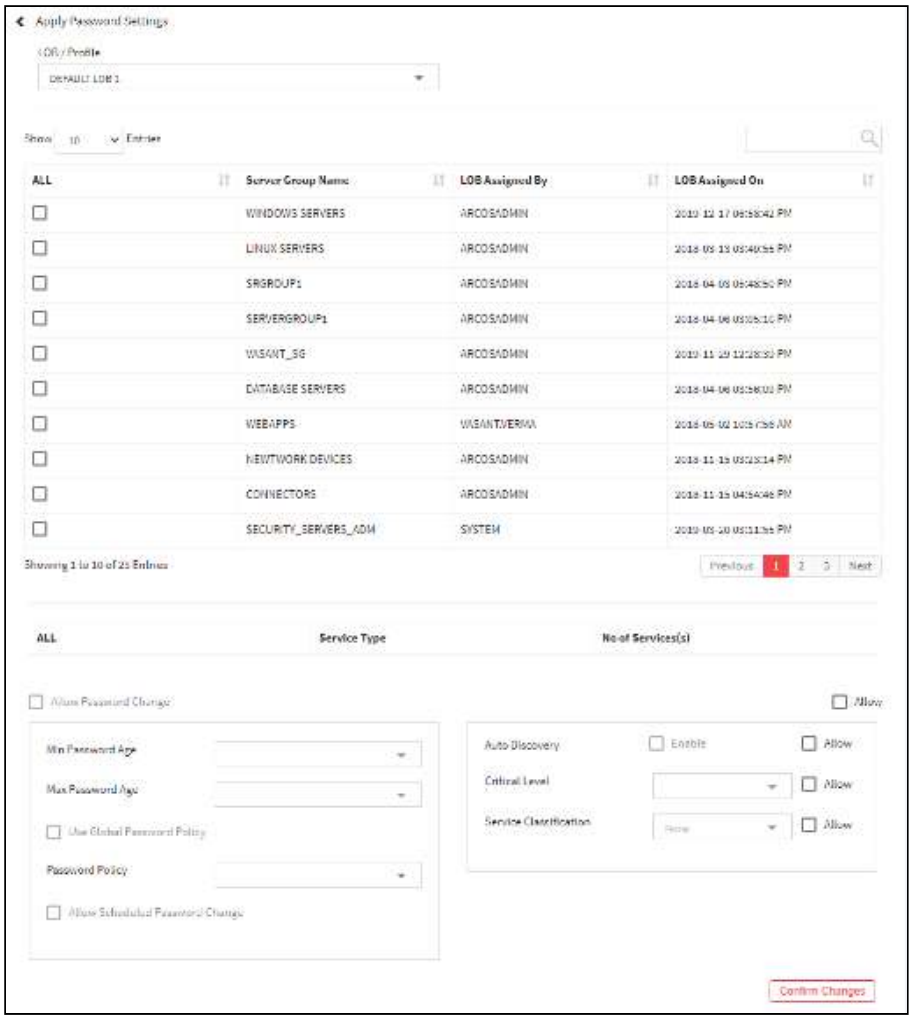
To navigate, use the following path:

Settings → Group

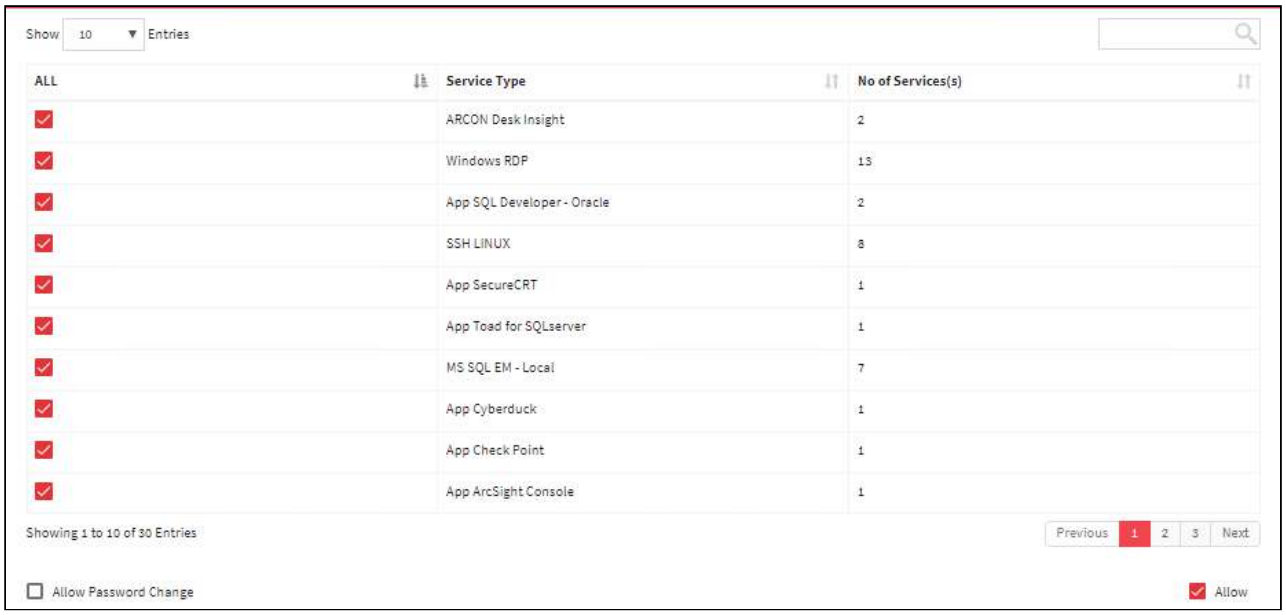
1. Select Apply Password Settings.



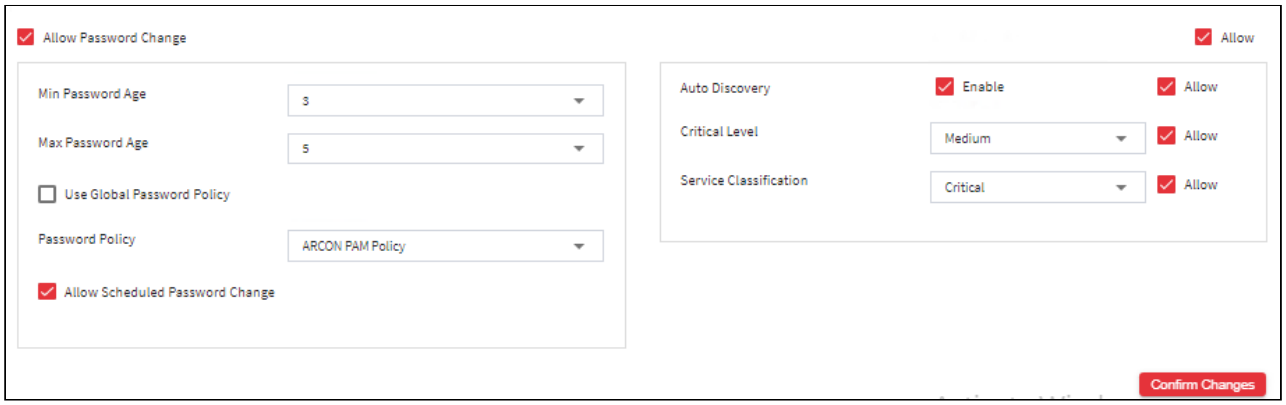
2. Select the LOB from the **LOB/Profile** dropdown list. A list of server groups are displayed in the grid.



3. Select the checkbox from the **Service Group Name** list. Select a type of service from the **Service Type** list which displays the count of services.



4. Enable **Allow** to set automated change passwords for that particular service type. It will also allow you to set the password policy and you can also set auto-discovery, criticality level, and service classification for the password change process.



Field Name	Description
Allow Password Change	To enable the password change process. ⚠ By default, the **Allow Password Change the** checkbox is selected. If you uncheck it, all the fields are disabled and you cannot change the password for the selected service both manually and automatically.

Field Name	Description
Min Password Age	Select minimum days for the scheduled password change process. ⚠ Password of Service will not be changed before the defined minimum days. Eg.: If you configure Minimum Password Age as 3; then the password change process cannot be performed before 3 days.
Max Password Age	Select maximum days for the scheduled password change process. ⚠ The password change process will be scheduled automatically depending on the selected max password age field.
Use Global Password Policy	Select to enable the global policy configured for the password change process.
Password Policy	Select the password policy. ⚠ By default, **Default Profile** is selected. You can create your own password policy, save it, and select it in this field.
Allow Scheduled Password Change	Select to enable/configure the scheduled password change process. ⚠ By enabling this checkbox the password change process for the selected service will be scheduled according to the selected min and max password age and selected password policy or the global password policy.
Allow (Checkbox)	Enable **Allow** to set automated change passwords for that particular service type
Auto Discovery	To enable Auto Discovery
Critical Level	Enable the Critical level and select from the dropdown to assign the critical level. • Low • Medium • High
Service Classification	Enable Service Classification and select from the dropdown to assign the service classification. • Critical

⚠ If **Automatically Apply Password Policy When Service is added in Server Group** Configuration is **enabled**, then Password Policy will be applied to Services newly mapped in Server Group whereas if it is set to disabled, then Password Policy will not be applied to Services newly mapped in Server Group.

13.3.2 Apply Command Profile

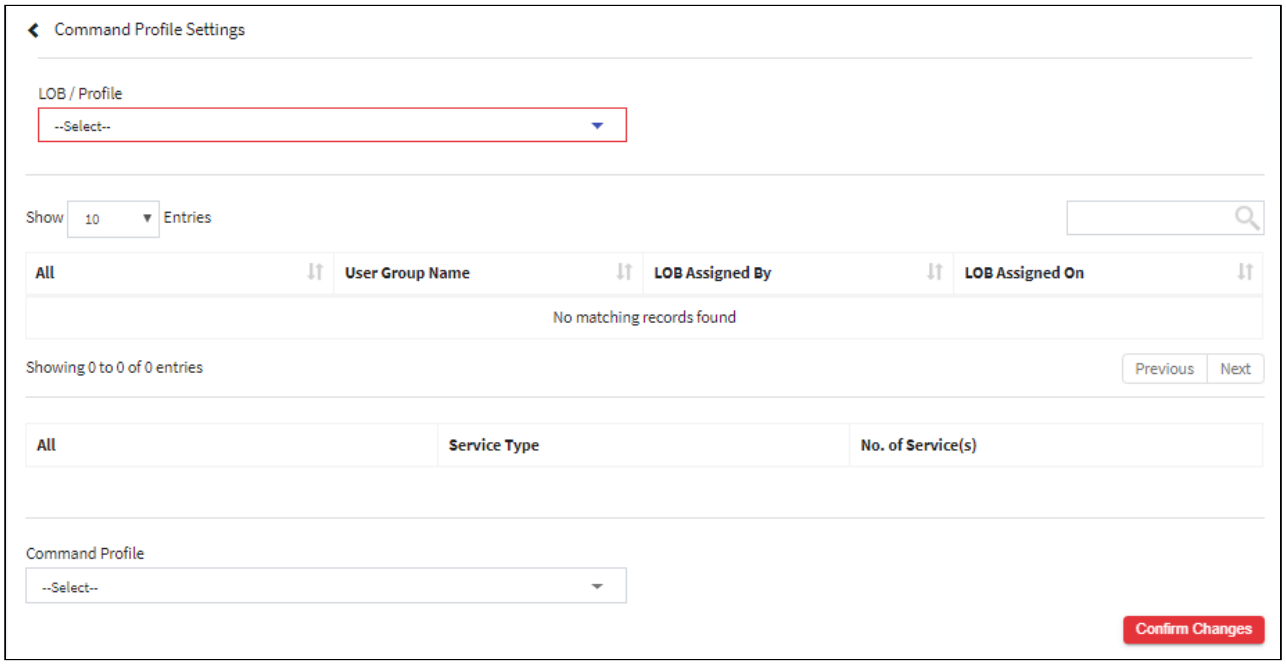
Command Profile helps you to assign a command profile to the services mapped under a particular user group. For example, if the user is using drive sharing command frequently, then he can create a "command profile" for that particular command to reduce workload.

> ⚠ The Administrator having **LOB / Profile Default Configuration** privilege in Server's Privileges will only be able to do configurations under LOB / Profile Default Configuration.

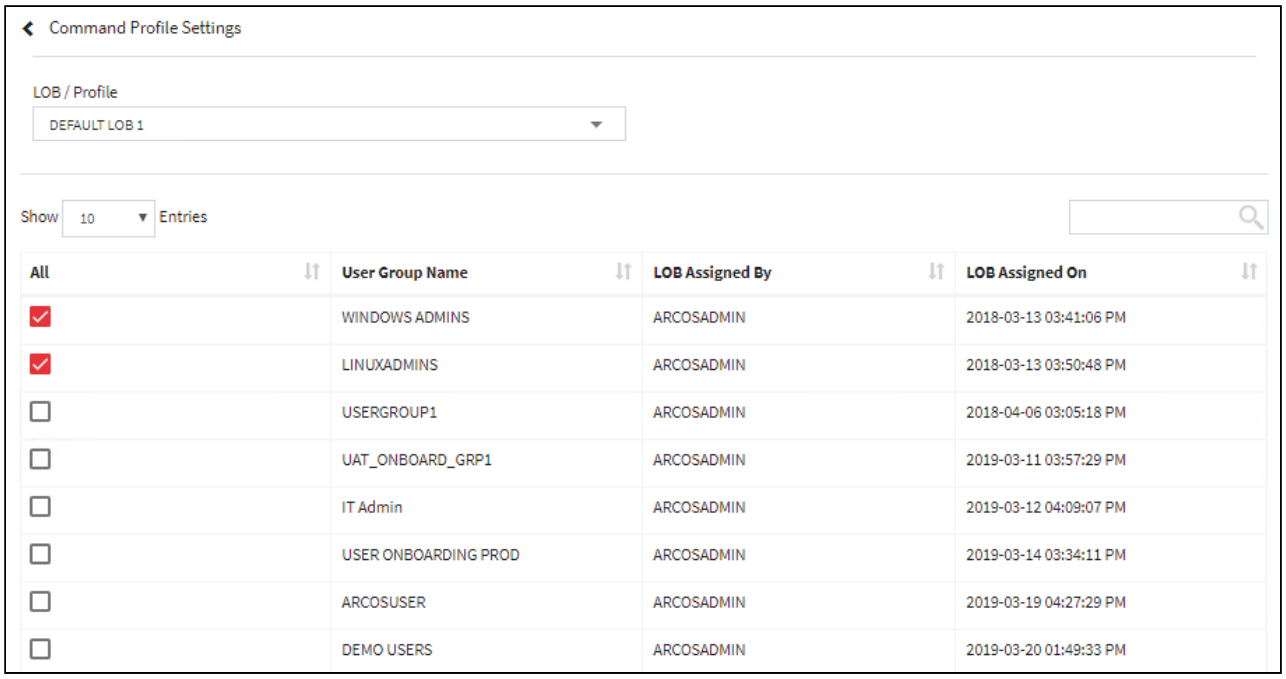
To navigate, use the following path:

Settings → Group

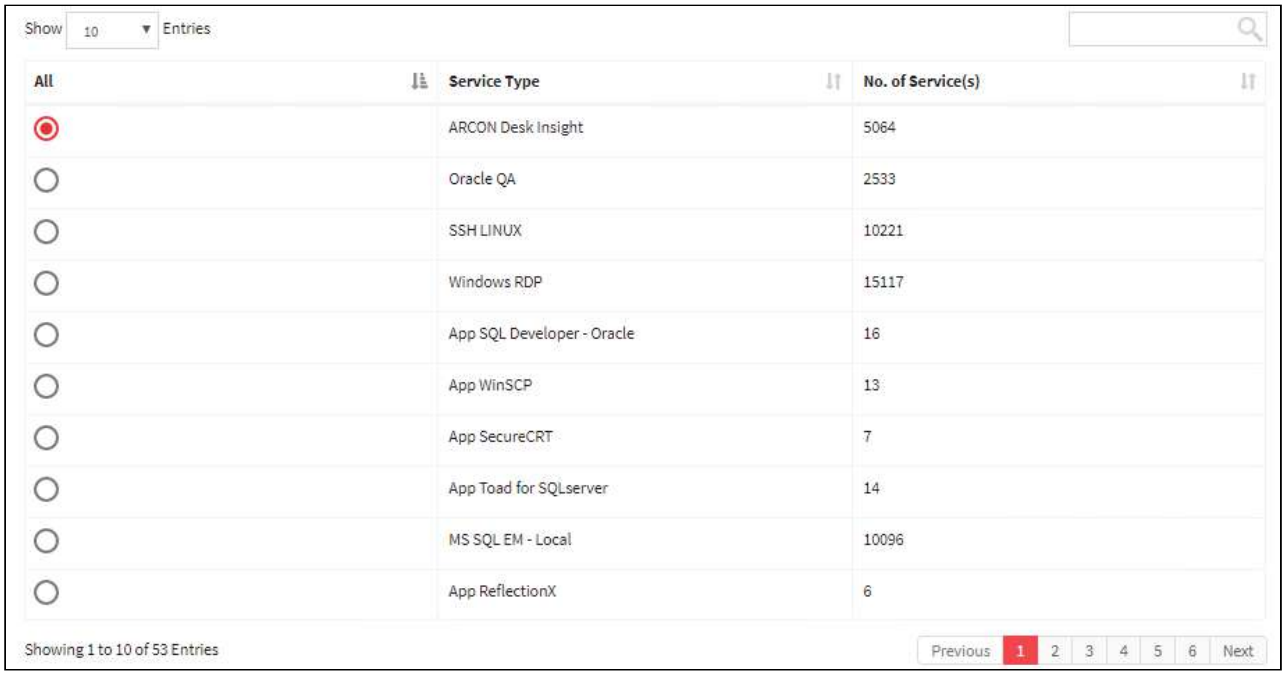
1. Select Apply Command Profile.



2. Select the LOB from the **LOB/Profile** dropdown list. Select the user group from the list of User Groups in the grid



3. The service types are displayed belonging to that particular user group.



4. Select the profile from the **Command Profile** dropdown list and click on **Confirm Changes** button. A window pops up displaying the following message:
   Are You Sure You Want To Apply LOB/Profile – Command Policy To Selected User Group(s)

5. Click **Yes**. Another window pops up displaying the following message: **LOB/Profile – Command Policy Applied Successfully**
   No Of Users Affected: (Total Number)

13.3.3 2FA

13.3.3.1 Dual Factor IP Range

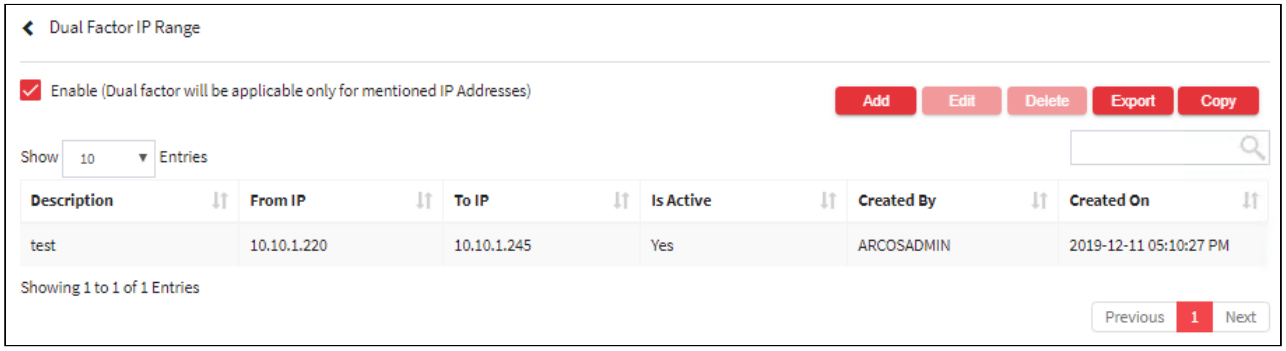
In Dual Factor IP Range, you can define the range of IP Address to be configured for the 'Dual Factor type'. Once configured, ARCON PAM will prompt for the second authentication to the End User only if the User is from the configured IP range.

> ⚠ The Administrator having **Dual Factor IP Range** privileges in Server's Privileges will only be able to configure values for Dual Factor IP Range.

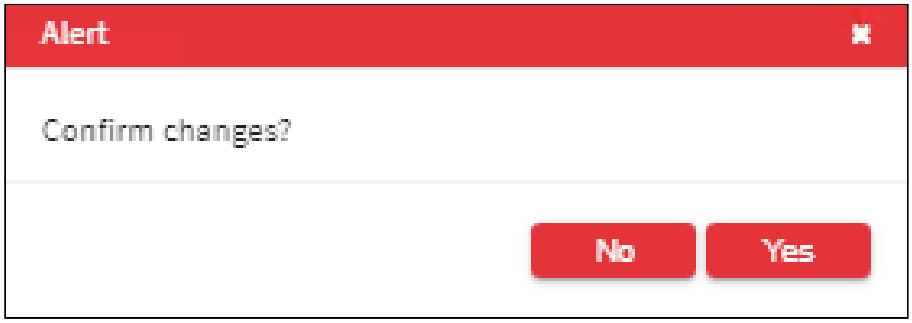
To navigate, use the following path:

Settings → Group → 2FA

1. Select Dual Factor IP Range under 2FA.



2. Select the **Enable** (Dual factor will be applicable only for mentioned IP addresses) checkbox. A window pops up with the following message: **Confirm Changes?**



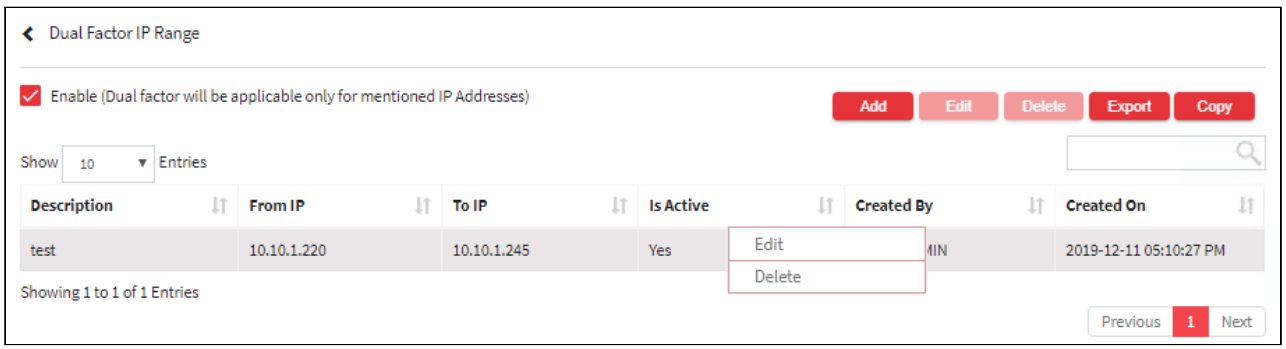
3. Click **Yes**. The fields are enabled to configure the IP range.
4. Select the Add button to add a new Dual Factor.

The **Dual Factor IP Range** screen contains the following fields:

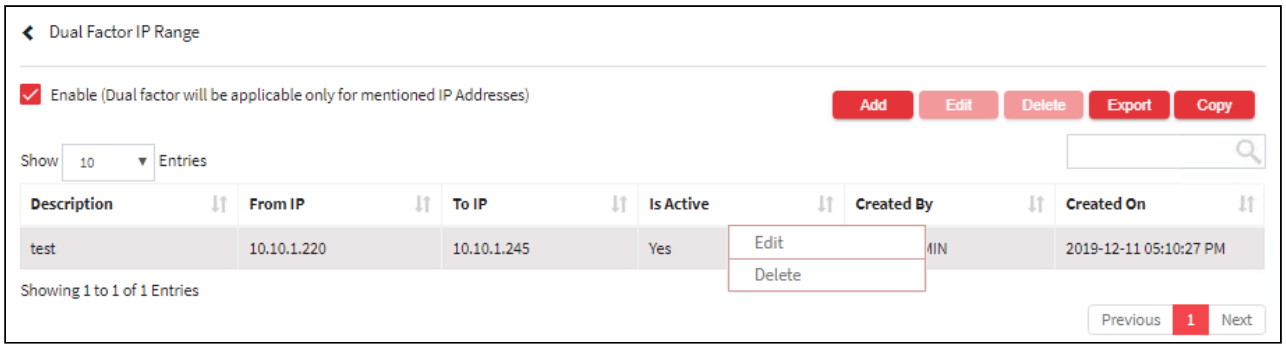
Field Name	Description
Description	Enter the description for the dual-factor IP range.
From IP	Enter IP address to set the start range for dual-factor.
To IP	Enter IP address to set the end range for dual-factor.
Type	Select the type of authentication.
Is Active	Click to enable the configuration.

⚠ The user is authenticated on login screen of **Client Manager**, once the dual factor IP range is configured.

5. For Editing the details of the existing Dual Factor IP Range click on the existing Dual Factor IP Range and select the Edit button at the top and make the required changes. Also, you can right-click on the domain and select Edit.



6. For Deleting the existing Dual Factor IP Range click on the existing Dual Factor IP Range and select the Delete button at the top and make the required changes. Also, you can right-click on the domain and select Delete.



7. The Export button will export all the Dual Factor IP Range details in the form .xlsx format. The Copy button will copy all the details of the table.

13.3.3.2 2FA Configurations

To navigate, use the following path:

Settings → Group → 2FA

Field Name	Description
User Door Access Authentication - Error Message	**Allows to configure the Message to be displayed by ARCON PAM when User Door Access Authentication fails.**
Valid Values	If Toggle value is 'Enabled', then it enables Restoration of last Password based on the password history.
Biometric Device	**This configuration sets which Biometric device is to be enabled for Biometric Authentication.**
Valid Values	The valid values are Morpho, Precision, 3M Cogent/Gemalto, eikonTouch, Globalspace
SMS OTP - Enforce Self Registration for all Users	**This configuration will allow administrators to enable/disable SMS OTP**
Disable	If Toggle value is 'Disabled', then SMS OTP-Enforce Self Registration will be disabled for All Users.
Enable	If Toggle value is 'Enabled', then SMS OTP-Enforce Self Registration will be enabled for All Users. Note- **SMS OTP -Enforce Self Registration for All User** and **Mobile OTP -Enforce Self Registration for All User** cannot be enabled at the same time.

Field Name	Description
Mobile OTP - Enforce Self Registration for all Users	**This configuration will allow administrators to enable/disable Mobile OTP - Enforce Self Registration.**
Disable	If Toggle value is 'Disabled', then Mobile OTP-Enforce Self Registration will be disabled for All Users.
Enable	If Toggle value is 'Enabled', then Mobile OTP-Enforce Self Registration will be enabled for All Users. Note- **SMS OTP -Enforce Self Registration for All User** and **Mobile OTP -Enforce Self Registration for All User** cannot be enabled at the same time.
Enable Mobile OTP Registration on Multiple Instances	**This configuration enables/disables Mobile OTP on multiple instances with the same user.**
Disable	If Toggle value is 'Disabled', then this feature is disabled. Note- If Mobile OTP is disabled in the first instance it will be disabled in the following instances too.
Enable	If Toggle value is 'Enabled', then this feature is enabled.
Disable Hardware Token - for All User	**This configuration enables/disables Hardware tokens OTP for all users.**
Disable	If Toggle value is 'Disabled', then this feature is disabled.
Enable	If Toggle value is 'Enabled', then this feature is enabled.

13.3.3.3 User Door Access

13.3.3.3.1 User Door Access Authentication

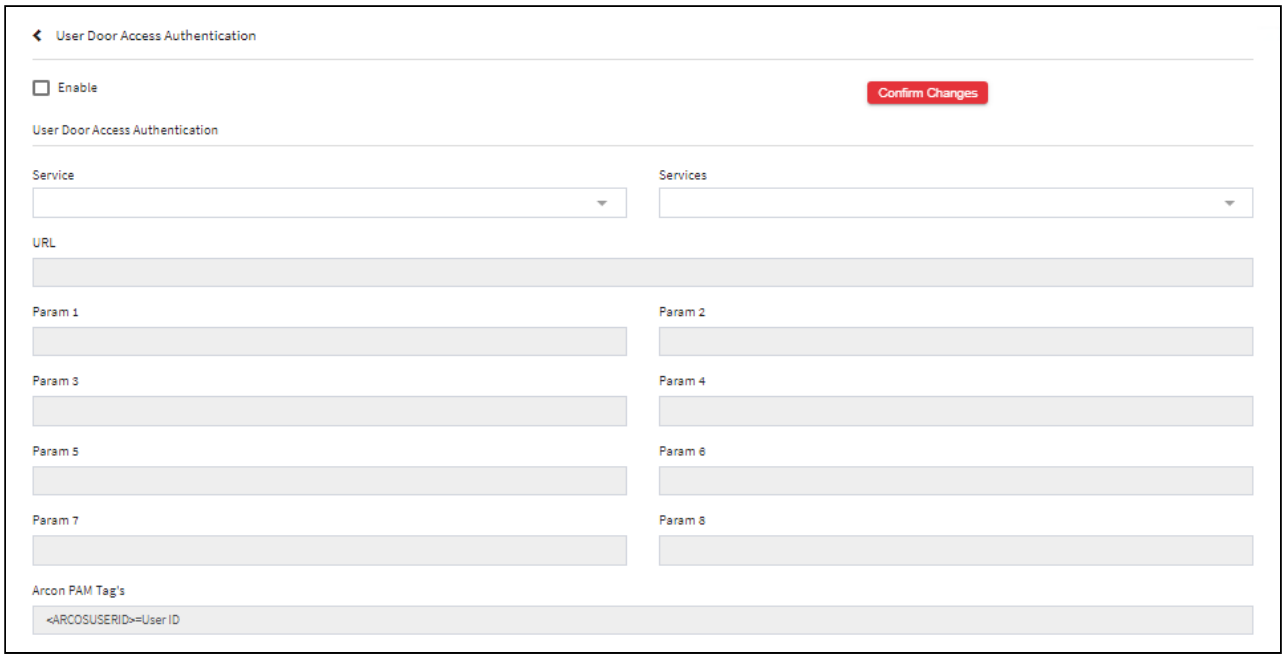
User Door Access Authentication mechanism is used when the user wants the application to authenticate or check the User's physical presence within the premise. This can be done by communicating with the Door Access Management System to check if the User has swiped the door to check in the premise, this information can be monitored by ARCON PAM to get the status of the user and only then allow to login into the application. For such communication with Door Access Management, a framework is available in ARCON PAM.

⚠ The Administrator having **User Door Access Authentication** privileges in Server's Privileges will only be able to configure values for User Door Access Authentication.

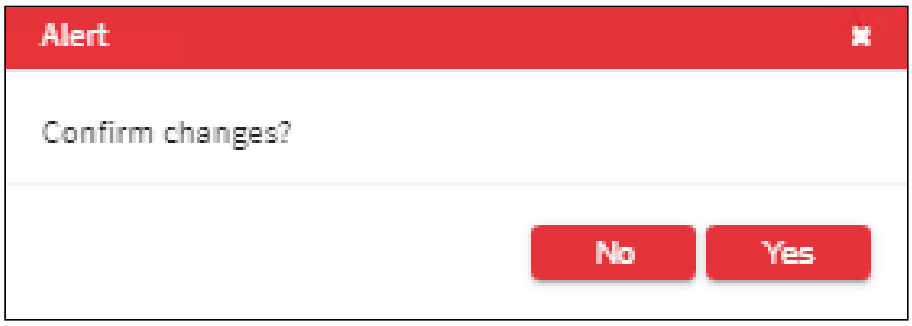
To navigate, use the following path:

Settings → Group → 2FA → USER DOOR ACCESS

1. Select User Door Access Authentication under USER DOOR ACCESS.



2. Click Enable. A User Door Access Authentication window pops up with the following message. **Confirm Changes?**



3. Click **Yes.** The fields are enabled to configure user door access authentication.

The **User Door Access Authentication** screen displays the following fields:

Field Name	Description
Service	Select the service. Predefined service types are available in ARCON PAM. To add a service in Service drop-down, right-click the service from manage services and select add it to DMZ supported services. Only supported services will be available in the drop-down list. The User Door Access Authentication section has eight different parameters. Based on the selected service, these parameters get utilized. **Example:** In the Service list, select the service. Based on this, from the Service list, a database is selected on the User Door Access Authentication screen. ARCON PAM will now connect to the Info Bridge.

Field Name	Description
Services	ARCON PAM will pass the details of the server, to the Info Bridge. Info Bridge will fire the query provided in the Parameter field to the database selected in the Service list and check whether User 1 has checked in or not. ARCON PAM knows the type of database, the type of connectivity needs to be established. If there is a web service, configure a web service parameter and it will customize the Info Bridge accordingly so that it can connect to any type of access card system or door access system.
URL	It is an Info Bridge. This is one of the web services in the Info Bridge. **Example:** One application using the Microsoft SQL database has created a view. This is a temporary table where ARCON PAM can query data. User 1 tries to access ARCON PAM from the office but he has not swiped his card at the main entrance. Now, according to the swipe mechanism User 1 has not entered the office. When User 1 tries to access ARCON PAM, it will communicate with the Info Bridge. ARCON PAM will check whether User 1 has swiped his card in or not. When it communicates with the Info Bridge, Info Bridge will take the details such as server details to the database. ARCON PAM will directly query the database whether User 1 has checked in or not. If User 1 has checked in, ARCON PAM will allow him to log in.

4. Enter the details and click **Confirm Changes** button to configure the details.

13.3.3.3.1.1 User Door Access Configuration

To navigate, use the following path:

Settings → Group → 2FA → USER DOOR ACCESS

Field Name	Description
RADIUS Server Connection Timeout	**This configuration sets the time for Radius Server Connection Timeout.** **If the user selects the default RADIUS Server Connection Timeout value to 5000, it refers to 5 seconds/minute.**
Valid Values	The valid range is 1-100000.

13.3.3.3.2 Hardware Token-Radius Servers

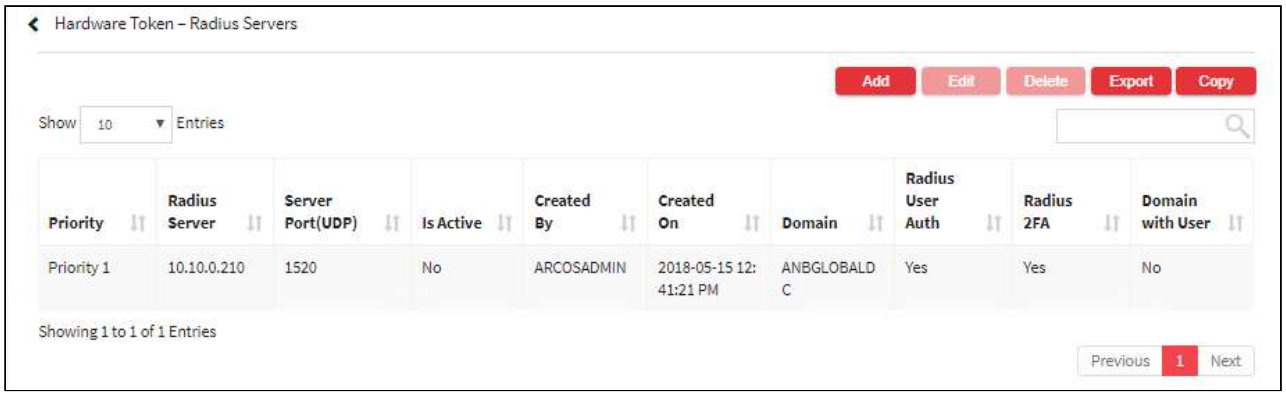
The RADIUS servers are used for the authentication of the RSA portal. RADIUS is a protocol similar to LDAP, DCPIP, and RDP protocol. Similarly, RADIUS is a kind of protocol that helps to communicate with another server. When you want to enable the Hardware / Software Tokens which works on the RADIUS protocol as the second factor of authentication in ARCON PAM, then the configuration of the RADIUS server is done here.

⚠ The Administrator having **Hardware Token – RADIUS Servers** privilege in Server's Privileges will only be able to configure values for Hardware Token – Radius Servers.

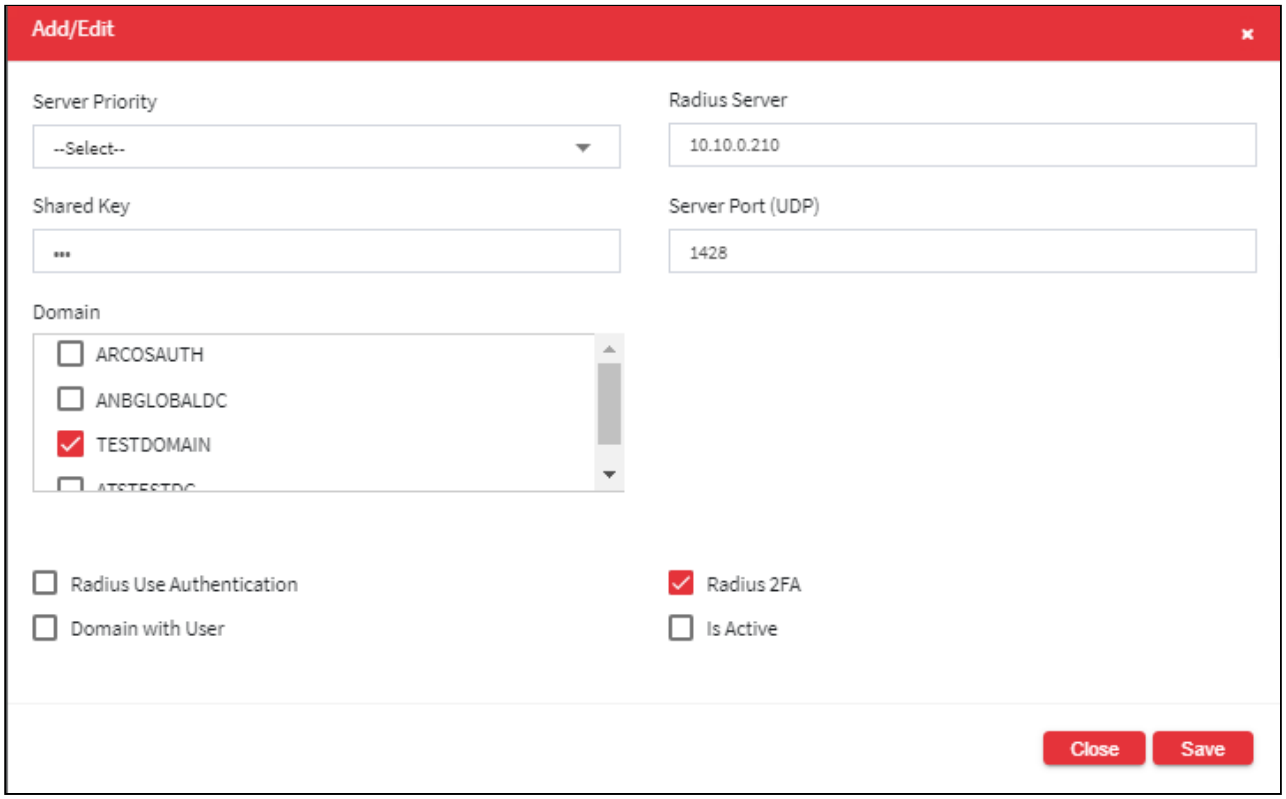
To navigate, use the following path:

Settings → Group → 2FA → USER DOOR ACCESS

1. Select Hardware Token – Radius Servers under USER DOOR ACCESS.



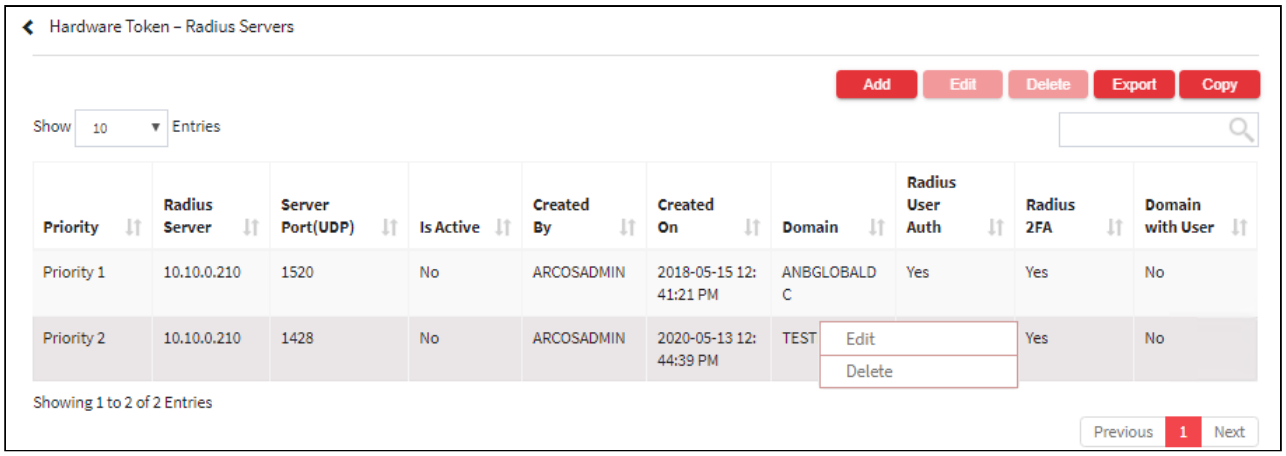
2. Select Add to add a new token.



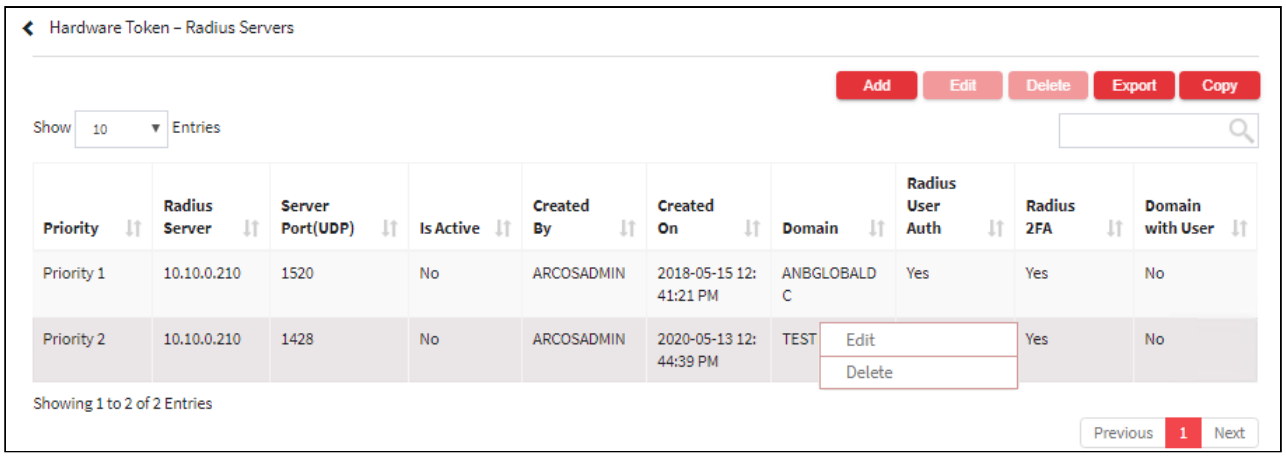
Field Name	Description
Server Priority	Select the server priority. ⚠ The priority up to three servers can be configured if those many servers are available in the environment as part of HA (High Availability).
Radius Server	Enter the radius server.
Shared Key	Enter the shared key.

Field Name	Description
Server Port (UDP)	Enter the server port (UDP) number.
Domain	Select the Domain name.
Radius User Authentication	Enable Radius User Authentication for User Authentication
Radius 2FA	Enable Radius 2FA for 2FA
Domain with User	Enables all the users within the domain
Is Active	Enable the server in ARCON PAM.

3. Enter the details and click **Save** button to configure the radius server details.
4. For Editing, the details of the existing Hardware Token- Radius servers click on the existing row and select the Edit button at the top and make the required changes. Also, you can right-click on the row and select Edit.



5. For Deleting the existing Hardware Token- Radius servers click on the existing row and select the Delete button at the top and make the required changes. Also, you can right-click on the row and select Delete.



6. The Export button will export all the Hardware Token- Radius servers details in the form .xlsx format. The Copy button will copy all the details of the table.

13.3.3.4 Biometric

13.3.3.4.1 Voice Biometric Configuration

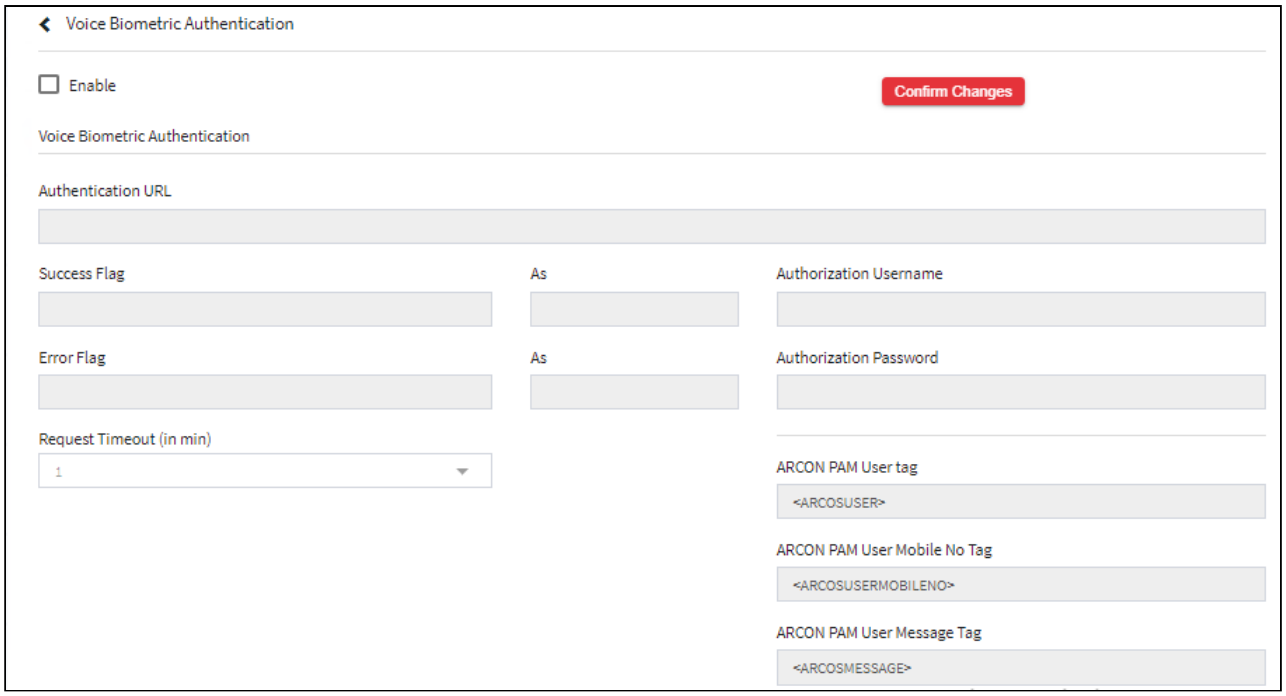
Voice Biometric Authentication is a type of Dual Factor Authentication which uses Web Service for authenticating user before logging into Client Manager. The predefined web service authentication is configured, which will authenticate the user through his voice and decide whether to allow the user to login or not.

> ⚠ The Administrator having **Voice Biometric Authentication** privileges in **Server's Privileges** will only be able to configure values for Voice Bio Metric Configuration.

To navigate, use the following path:

Settings → Group → 2FA → BIOMETRIC

1. Select Voice Bio Metric Configuration.



2. **Enable** checkbox. The fields are enabled to configure voice biometric authentication

Field Name	Description
Authentication URL	It is in the predefined .xml format.
Success Flag	Configure the success flag. The valid values are: ▪ True ▪ False
Error Flag	Configure the error flag. The valid values are: ▪ True ▪ False

Field Name	Description
Authorization Username	Authorized user name used to access the specified URL.
Authorization Password	Password used to access the specified URL.
Request Timeout (in min)	Select the session timeout in minutes.

3. Few fields are customizable according to requirements. The ARCON PAM User Tag, ARCON PAM User Mobile No. Tag and ARCON PAM Message Tag can be configured with user details, user mobile number and message to be sent.
4. Enter the details and click **Confirm Changes** to configure the details.

13.3.3.4.2 Biometric Configurations

To navigate, use the following path:

Settings → Group → 2FA → BIOMETRIC

Field Name	Description
Biometric – Finger Print - Mode	**This configuration sets mode of Finger Print in Biometric Authentication.**
Valid Values	The two modes are- **Desktop:** In this mode, every ARCON PAM User should have an individual bio-metric device configured to their respective workstation, hence first the user login to the ARCON PAM portal with their respective credentials and then the biometric authentication is prompted. **Centralized:** In this mode, the biometric device should be configured on a centralized location and every user will be authenticated with the centralized bio-metric device first and then are allowed to login to ARCON PAM Portal.
Biometric – Finger Print - Mode - Centralized Valid For (Minutes)	**This configuration sets time in minutes for the validity of Finger Print in Centralized Mode for Biometric Authentication.**
Valid Values	The range is from 1-480. If the value is Zero every time the user will have to identify through the bio-metric fingerprint.
Biometric Finger Print Authenticator Link On ACMO Login Page - Is Enabled	**This configuration enables/disables Biometric Finger Print Authenticator Link on CM Login Page.**
Disable	If Toggle value is 'Disabled', then this feature will be disabled.
Enable	If Toggle value is 'Enabled', then this feature will be enabled.

Field Name	Description
Biometric-Finger Print- Minimum Match Score (Percentage)	**This configuration sets the percentage of minimum match score of Finger Print in Biometric Authentication.**
Valid Values	The range is 0-100.

13.3.4 Machine Control

13.3.4.1 Network Segments

Network Segments configuration is used to pull Network Segment Wise Logon Report from Client Manager. The range of IP Address is set under a Network Segment. The report will display details based on the configuration. The Network Segment Wise Logon report displays the details of the User who has logged into the application by any network device with User IP address and desktop details.

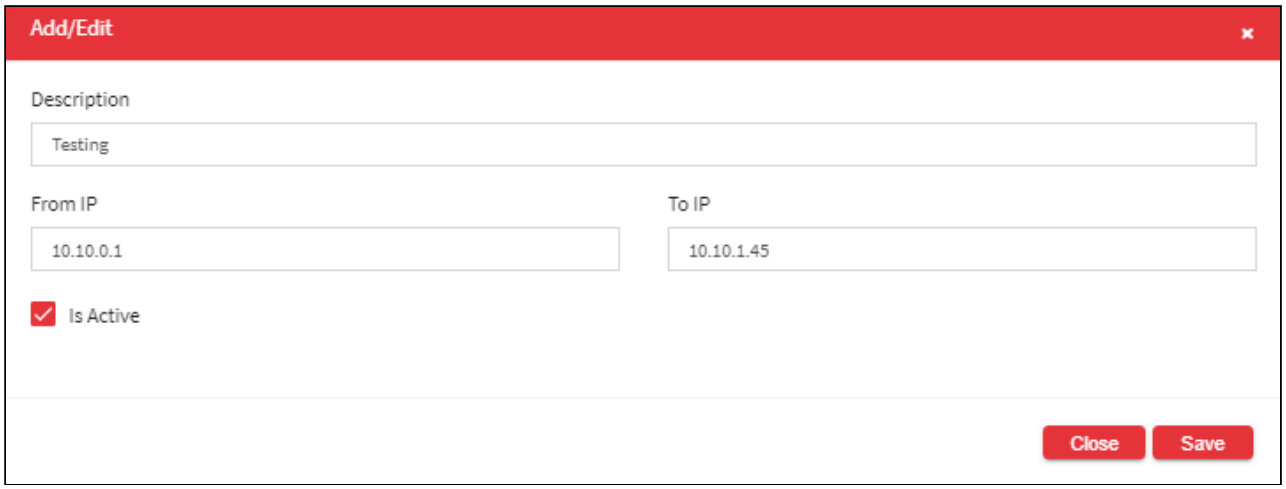
⚠ The Administrator having **Network Segments** privileges in Server's Privileges will only be able to configure values for Network Segments.

To navigate, use the following path:

Settings → Group → Machine Control

1. Select Network Segments under Machine Control

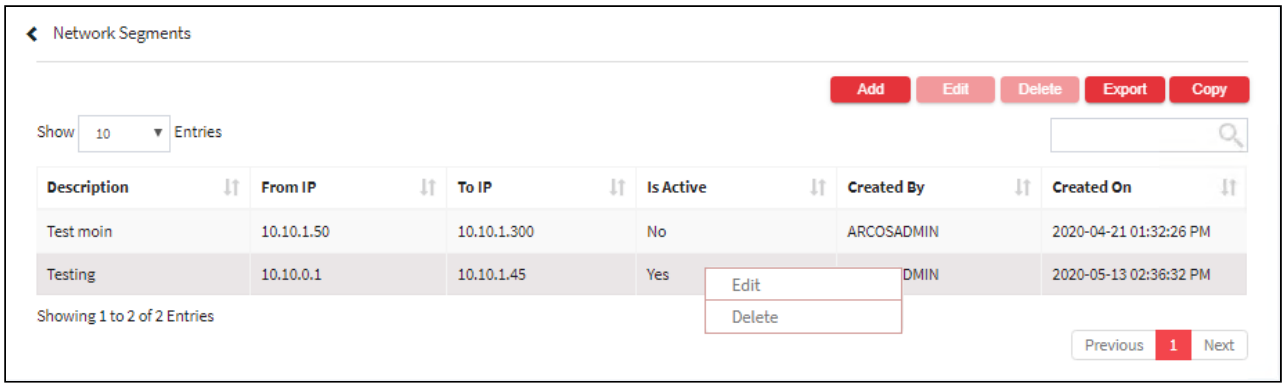
2. Select the Add button to add a new Network segment.



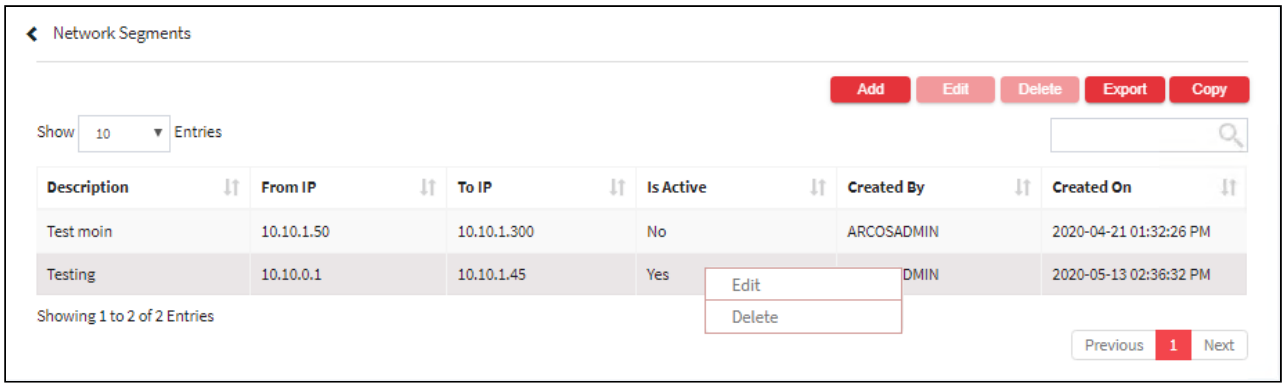
Network segment fields are described as below

Field Name	Description
Description	Enter the description for network segment.
From IP	Enter the IP address, from where the network range starts.
To IP	Enter the IP address, where the network range ends.
Is Active	To enable the configuration.

3. Enter the details and click **Save** button to create a new network segment.
4. For Editing the details of the existing Network Segment click on the existing row and select the Edit button at the top and make the required changes. Also, you can right-click on the domain and select Edit.



5. For Deleting the existing Network Segment click on the existing row and select the Delete button at the top and make the required changes. Also, you can right-click on the domain and select Delete.



6. The Export button will export all the Network Segment details in the form .xlsx format. The Copy button will copy all the details of the table.

13.3.4.2 Machine Controls Global Configurations

To navigate, use the following path:

Settings → Group → Machine Control

Field Name	Description
Desktop Level Access Control - MAC/IP Filter	**This configuration sets whether Desktop Level Access will block devices from connecting to ARCON PAM or not.**
Valid Values	The range is from 0-2 • If the value is set to '0', it refers to everything is allowed. It means all the devices are allowed to connect to ARCON PAM. The menu is not visible because no configuration is required. • If the value is set to '1', it refers to Block Only value. It means the listed workstations are blocked and rest are allowed to connect to ARCON PAM. • If the value is set to '2', it refers to Allow Defined Only. It means only the defined Workstations are allowed to connect to ARCON PAM.
Common Temp Parent Folder For ARCOS ActiveX	**This configuration sets the name of Common Temp Parent Folder for ActiveX.**
Valid Values	Set the name of Common Temp Parent Folder for ActiveX. By default value is 'ARCON PAM'.
Access On Hold (By Default) In User Access Review - Is Enabled	**This configuration sets whether old reviews kept on hold will be displayed under CM > Server Manager > Reviews > User Access.**

Field Name	Description
Disable	If Toggle value is 'Disabled', then recently added to Hold list reviews will be displayed under CM > Server Manager > Reviews > User Access > Access On Hold tab.
Enable	If Toggle value is 'Enabled', then old reviews kept on Hold will be displayed under CM > Server Manager > Reviews > User Access > Access On Hold tab.
Biometric-Finger Print- Minimum Match Score (Percentage)	**This configuration sets the percentage of minimum match score of Finger Print in Biometric Authentication.**
Valid Values	The range is 0-100.

13.3.5 ACMO

To navigate, use the following path:

Settings → Group → ACMO

Field Name	Description
Use Secured ARCOS Login Validation	**This configuration enables/disables capturing of details of the user who tries to log in to ARCON PAM without ActiveX.**
Disable	If Toggle value is 'Disabled', then this feature is disabled.
Enable	If Toggle value is 'Enabled', then this feature is enabled.
ACMO Session Timeout (Minutes)	**This configuration sets the time in minutes which is considered to logout the user if the ACMO session is idle for that duration.**
Valid Values	The range is from 1-9999.
Sort All Filter Data In ACMO Connections - Is Enabled	**This configuration sets whether service details displayed in the grid view under My Services (Client Manager > My Access > My Services) should be sorted or not. By default, ARCON PAM only sorts by the IP address.**
Disable	If Toggle value is 'Disabled', then it displays data sorted by IP address.
Enable	If Toggle value is 'Enabled', and under Server Manager > Settings > Service > Security > Service Critical Command > Configure a command and tick Ask User Confirmation (Before Execution). Execute this critical command on the server. A confirmation message will be displayed.

Field Name	Description
ARCOS Security Token Validation In ACMO - Is Enabled	**This configuration will enable or disable ARCON PAM Security Token Validation in Client Manager.**
Disable	If Toggle value is 'Disabled', then this feature is disabled.
Enable	If Toggle value is 'Enabled', then this feature is enabled.
Service Access All LOB - Is Enabled	**This configuration enables/disabled All LOBs option in the LOB drop-down list in My Services (Client Manager).**
Disable	If Toggle value is 'Disabled', then it displays Services LOB wise.
Enable	If Toggle value is 'Enabled', then it displays All LOBs option. Enable this configuration if you want to display services for particular IP Address or Hostname from all LOBs.
Hide ACMO My Services Page Table Column (Case sensitive)	**This configuration hides the selected column from ACMO -> My Services.**
Valid Values	Select the column name: Service Type, Host Name, Host IP, Username, Domain, Instance
ACMO Enable Agentless Login	
Disable	
Enable	
Domain Validation for ACMO (WindowsOS only)	**This configuration sets restrictions for accessing PAM ACMO based on their domain and workgroup.**
Valid Values	Allow both Domain and Workgroup machines, Allow only Domain machines, Allow only domain which have been listed
Domain validation failed message for ACMO (WindowsOS only)	**Set a customized message for domain validation.** **For example- If my Domain validation for ACMO (WindowsOS only) is - Allow only Domain Machines, and a workgroup user tries to access it then the login is failed and the message set on Domain validation failed message for ACMO (WindowsOS only) appears on the ACMO user screen.**
Valid Values	Enter the text message to be displayed on ACMO when the validation fails.

Field Name	Description
Custom Domain Validation names (WindowsOS only)	**We write the Comma-separated domain names which verify the user's presence against that domain.**
Valid Values	Enter the Domain names. Note:- To enable **Custom Domain Validationnames (WindowsOS only)**, the Domain validation for ACMO (WindowsOS only) value needs to set as **Allow only domain which have been listed.**
Dashboard-Critical Commands Fired Daywise	**This configuration will display data in ACMO → Dashboard → Critical Commands fired.**
Disable	If Toggle value is 'Disabled', then it will display 30 days records in critical command fired.
Enable	If Toggle value is 'Disabled', then it will display 1 day record in critical command fired.

13.3.6 Alerts

To navigate, use the following path:

Settings → Group → Alerts(?)

Field Name	Description
Send Alert To All Checker When Maker Creates New User	**This configuration sets whether the alert will be sent to all Checkers when Maker creates new User.**
Valid Values	The range is 0-2. • If '0' value is set then alert will not be sent to any Administrator, but the request will be displayed in **Maker's Checker** screen of Admins having **Approve User (Checker)** privilege. • If '1' value is set then alert will be sent to Administrators having **Receive Alert On User Creation By Maker** and **Approve User (Checker)** privilege. • If '2' value is set then alert will be sent to Administrators having **Approve User (Checker)** privilege.

Field Name	Description
User Dormancy Alert - Schedule Days	**This configuration sets the number of days for the alert to be sent to User prior to his ID is added in the Dormant User list.** ⚠ The Dormant User Alert configuration should be enabled for this configuration. **Eg: If the value is configured as 4, the User will be notified 4 days prior to the day his ID will be added in the Dormant User List.**
Valid Values	The range is from 1-5.
Dormant User Alert	**This configuration sets whether alert is sent to User that he will be added in Dormant User list.**
Disable	If Toggle value is 'Disabled', then an alert will not be sent to User.
Enable	If Toggle value is 'Enabled', then an alert will be sent to User.

13.3.7 Mapping- settings

To navigate, use the following path:

Settings → Group→Mapping

Field Name	Description
Automate UserGroup And ServerGroup Mapping (AD OnBoarding) - Is Enabled	**This configuration when enabled will map the User Group with Server Group once they are scanned from Active Directory. If User Group is mapped to respective Server Group then only named and vault Services will be created for the Users present in the User Group.**
Disable	If Toggle value is 'Disabled', then this feature is disabled.
Enable	If Toggle value is 'Enabled', then this feature is enabled.
Automate User and Service Mapping When user added in UserGroup - Is Enabled	**All services that are mapped to the Server Groups which is itself mapped to User Group will be assigned to the user that has been newly added in User Group.**
Disable	If Toggle value is 'Disabled', then this feature is disabled.
Enable	If Toggle value is 'Enabled', then this feature is enabled.

Field Name	Description
Automate User and Service Mapping when server added in ServerGroup- Is Enabled	**Service that has been newly added to the Service Group which is itself mapped to User Group will get assigned to all the Users present in the User Groups.**
Disable	If Toggle value is 'Disabled', then this feature is disabled.
Enable	If Toggle value is 'Enabled', then this feature is enabled.

13.4 User

13.4.1 Mac or IP Filter

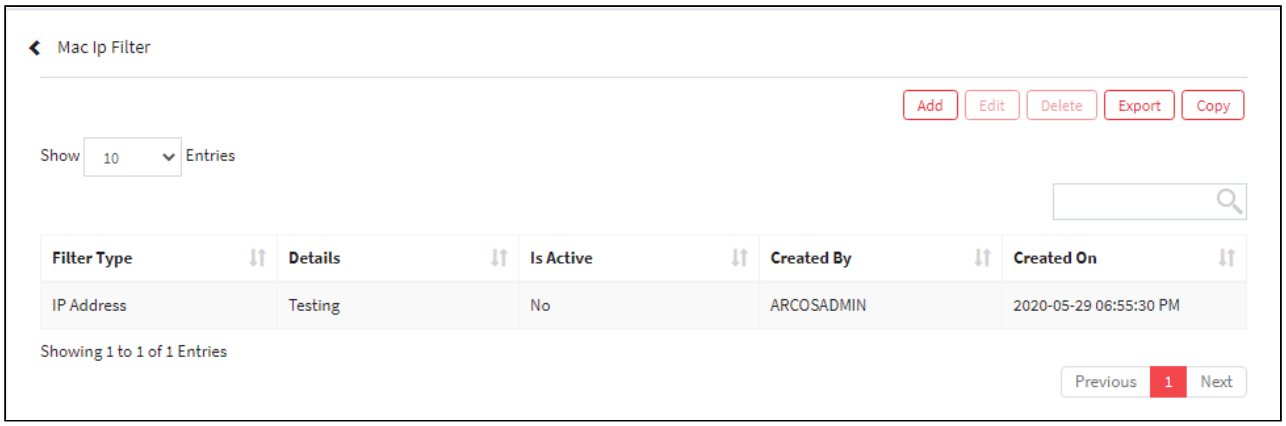
This section helps you to define or view all the IP address, MAC address, Processor ID, and BIOS Serial ID which have been blocked or allowed for desktop level access.

- The **Desktop Level Access Control - MAC/IP Filter** Configuration sets whether Desktop Level Access will block devices from connecting to ARCON PAM or not.
  - If value **0** is configured, it refers to everything is allowed and all the devices are allowed to connect to ARCON PAM. The **MAC/IP Filter** option will not be visible under **Tools** menu as no configuration is required.
  - If value **1** is configured, it refers to Block Only value. It means the workstations listed in **MAC/IP Filter** option will be blocked and rest are allowed to connect to ARCON PAM.
  - If value **2** is configured, it refers to Allow Defined Only. It means only the workstations listed in **MAC/IP Filter** option are allowed to connect to ARCON PAM.
- The Administrator having **IP / MAC Filter** privileges in Server's Privileges will only be able configure values in IP/MAC Filter.

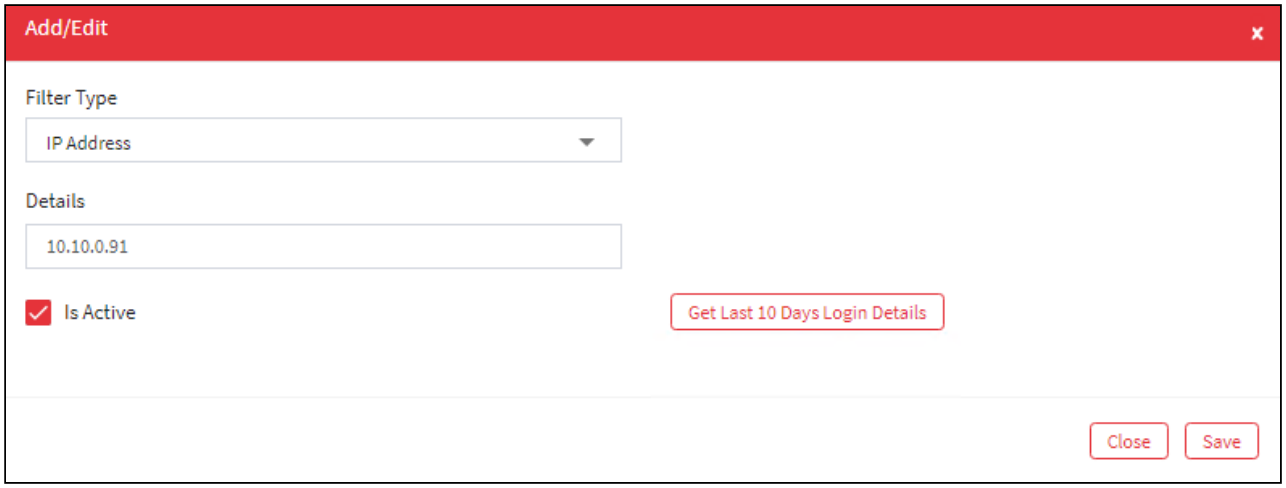
To navigate, use the following path:

Settings → Users

1. Select Mac/IP Filter.



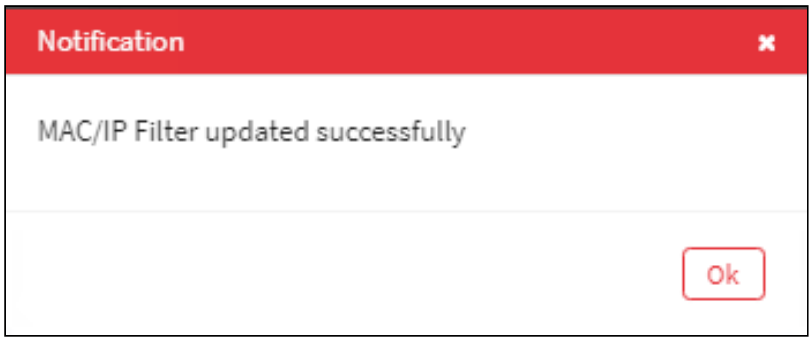
2. Select the Add button to add a new Mac/IP Filter.



The **Mac/IP filter** screen contains the following fields:

Field Name	Description
Filter Type	Select the type of filter. The valid values are: ▪ IP Address ▪ MAC Address ▪ Processor ID ▪ BIOS Serial ID
Detail	Specify the detail based on the filter type.
Is Active (checkbox)	Enable the configuration.

3. Click **Get Last 10 Days Login Details**, to view the last 10 days login details in the application.
4. Click on Save to save all the changes and the Mac/IP Filter has been set. A window pops up with the following message: **MAC/IP Filter updated successfully**.



5. For Editing, the details of the existing Mac/IP Filter click on the existing row and select the Edit button at the top and make the required changes.

6. For Deleting the existing Mac/IP Filter Click on the existing row and select the Delete button at the top and make the required changes.

7. The Export button will export all the Mac/IP Filter details in the form .xlsx format. The Copy button will copy all the details of the table.

13.4.2 User Security

This section helps you to with configurations to view passwords.
To navigate, use the following path:

Settings → Users → User Security

Field Name	Description
Instance Is Checked By Default	**This configuration enables/disables the availability of Instance option in grid view in CM > Connections.**
Disable	If Toggle value is 'Disabled', then it disables it.
Enable	If Toggle value is 'Enabled', then it enables it.

13.4.3 User Modification

This section helps you to with configurations to view passwords.
To navigate, use the following path:

Settings → Users → User Modification

Field Name	Description
Allow User Enabling Once Disabled - Is Enabled	**This configuration enables/disables User Enabling Once Disabled.**
Disable	If Toggle value is 'Disabled', then it disables the feature.
Enable	If Toggle value is 'Enabled', then it enables the feature.
Editable Display Name For Domain User - Is Enabled	**This configuration sets permission to edit the display name of users integrated in ARCON PAM with Domain validation.**
Disable	If Toggle value is 'Disabled', then the name cannot be modified.
Enable	If Toggle value is 'Enabled', then user display name can be modified.
User Display Name Properties In LDAP (Separated With ~)	**This configuration sets User Properties separated by ~, which will allow the application to fetch configured values from AD (LDAP) and display it in the User Display Name field. This is applicable only for Domain Users.**
Valid Values	displayName

Field Name	Description
User Valid Till Date	**The user will be valid for the specified number of days.**
Valid Values	If the minimum value is 0 (default value), the date will be displayed as 2058 (the default ARCON PAM Date). If the maximum value is set to specified days, the user will be valid for the specified number of days.
Display username along with userId on all Mapping screen	**This configuration will display the User Display name along with User ID (Example-If user ID is Satyendra.s and User Display name in Satyendra Singh then it should be seen as** **Satyendra.s (Satyendra Singh) under the following screens** **ACMO-> Manage -> Server Manager** **Map Group/Users** **Map Users/Services** **Manage Commands** **Manage Processes** **GroupAdmin - Map Services**
Disable	If Toggle value is 'Disabled', then only the User ID is visible on all the screens mentioned above.
Enable	If Toggle value is 'Enabled', then User ID(User Display name) is visible on all the screens mentioned above.

13.4.4 Configure User Tags

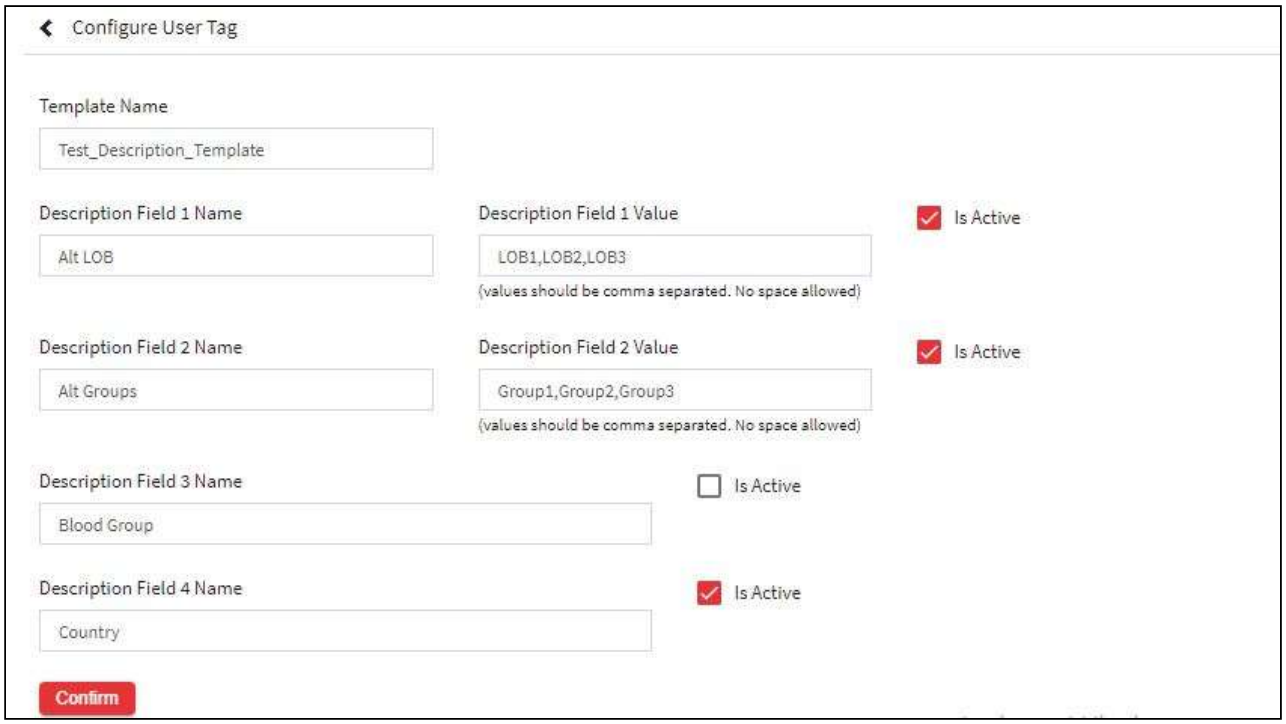
The Configure User Tags are the critical configurations given to the ARCON PAM Services. User Tags give control over what users of your site have access. Admin can arrange users into these groups by assigning them the appropriate tag.

⚠ To configure the values Administrator should be assigned **Configure User Tags** privileges from the Administrator under Server's Privileges.

To navigate, use the following path:

Settings → Others/Unsorted → Configure User Tags

1. Select Configure User Tag under Configure.



2. Enter the details, make sure that template name must be unique.
3. **Description Field 1 Name**: Enter the name of the Description Field. This entered value will be the field name displayed in **Manage Users**. Display an information icon with the following message - “This is a dropdown field".
4. Enter the name of the Description Field. This entered value will be the field name displayed in **Manage Users**. Enter comma-separated to display in the dropdown. Display an information icon with the following message - “Enter comma separated values. Admin can import values from LDAP”.

> ⚠ LDAP Value is a checkbox. If this value is selected, “Description Field 1 Value” field will be disabled and a text box beside this checkbox will be enabled along with the LDAP Path text field.

5. **Description Field 1 Value**: Enter comma-separated to display in the dropdown.

> ⚠ Click on the checkbox will enable this field. If not then the checkbox will not be enabled.

6. Similarly, Description Field 2 Name will be similar to Description Field 1 Name and Description Field 2 Value will be similar to Description Field 1 Value.
7. Description Field 3 and 4 will be text fields.

> ⚠ If Description Field Name is kept blank then it will be displayed as Description Field 1 (2/3/4) in Manage Users screen.

13.5 Service

This section includes the following topics:

- Security
- SSH

- Windows
- Request
- Service Modifications

13.5.1 Security

13.5.1.1 Service Critical Command

Critical Commands are commands which are defined as highly critical for use. These commands when executed will have a crucial impact on the target server or to the resources associated with it. When an attempt is made to execute a critical command, it will prompt for confirmation for executing the command.

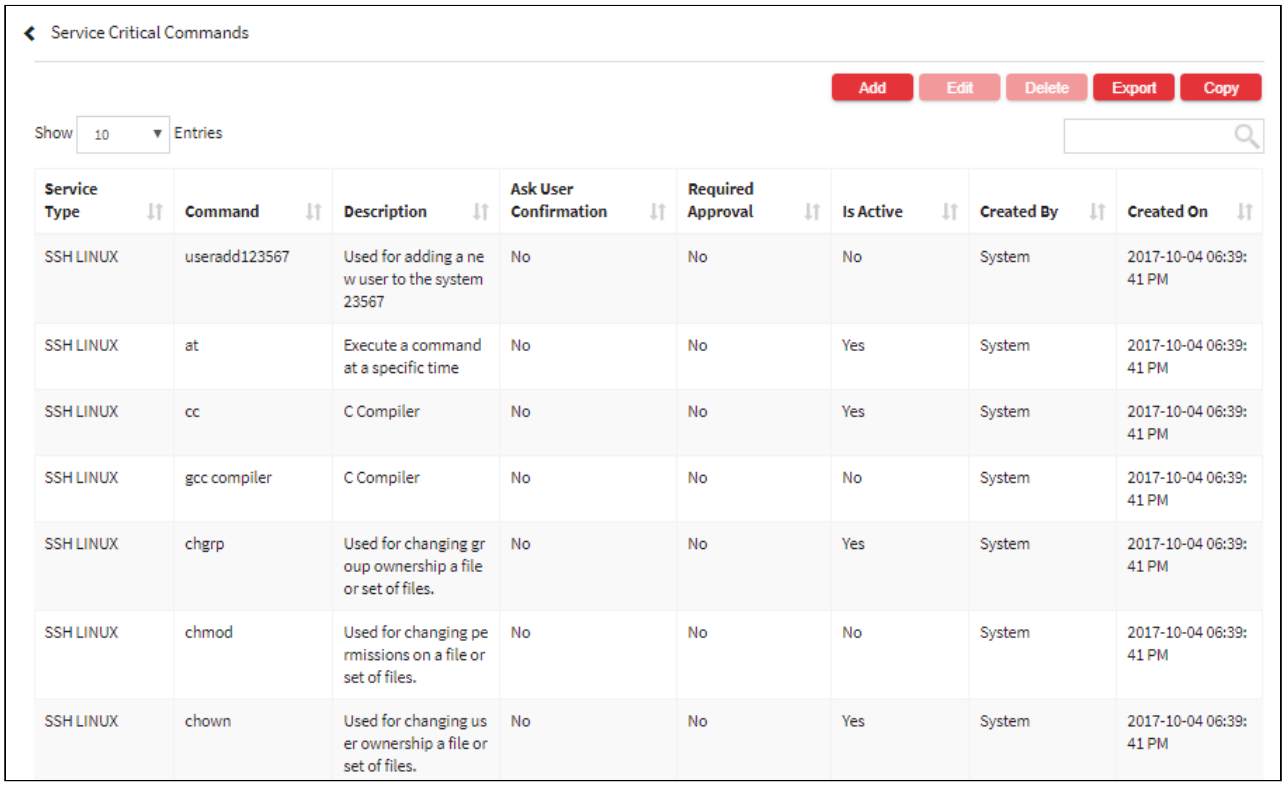
This section helps you to define a critical command for a service. In addition, you can modify or delete an existing defined critical command.

> ⚠ The Administrator having **Service Critical Commands** privilege in Server's Privileges will only be able to define a critical command for a service.

To navigate, use the following path:

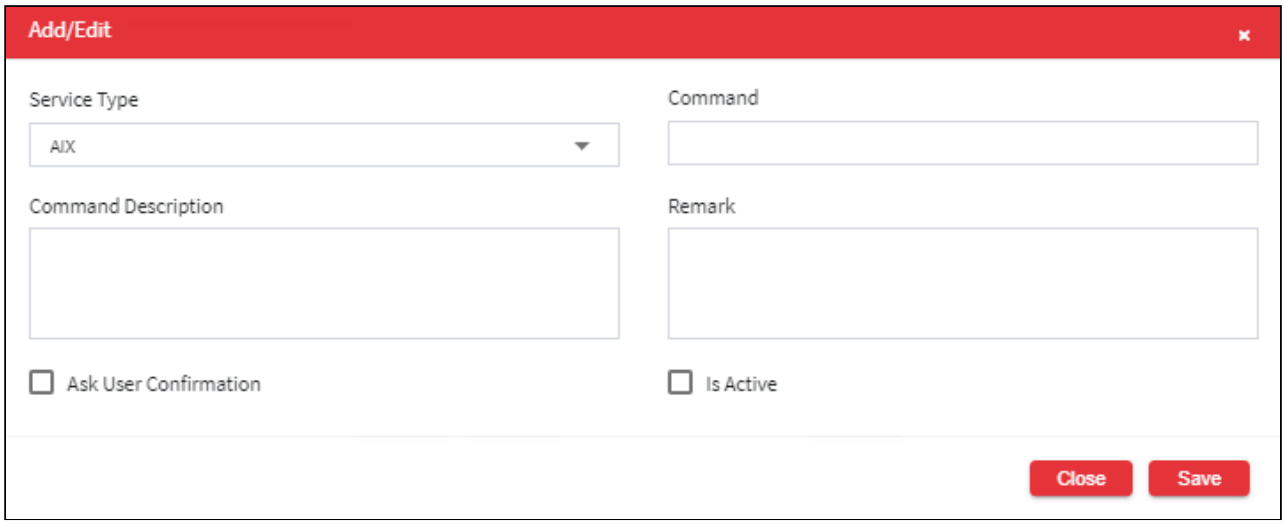
Settings → Service → Security

1. Select the Service Critical Commands under Security.



Service Type	Command	Description	Ask User Confirmation	Required Approval	Is Active	Created By	Created On
SSH LINUX	useradd123567	Used for adding a new user to the system 23567	No	No	No	System	2017-10-04 06:39:41 PM
SSH LINUX	at	Execute a command at a specific time	No	No	Yes	System	2017-10-04 06:39:41 PM
SSH LINUX	cc	C Compiler	No	No	Yes	System	2017-10-04 06:39:41 PM
SSH LINUX	gcc compiler	C Compiler	No	No	No	System	2017-10-04 06:39:41 PM
SSH LINUX	chgrp	Used for changing group ownership a file or set of files.	No	No	Yes	System	2017-10-04 06:39:41 PM
SSH LINUX	chmod	Used for changing permissions on a file or set of files.	No	No	No	System	2017-10-04 06:39:41 PM
SSH LINUX	chown	Used for changing user ownership a file or set of files.	No	No	Yes	System	2017-10-04 06:39:41 PM

2. Select the Add button to add a new service critical command.



The **Service Critical Commands** screen contains the following fields:

Field Name	Description
Service Type	Select the type of service.
Command	Define a command.
Command Description	Specify the command description.
Remark	Specify the remark.
Ask User Confirmation (Before Execution)	Indicates that the user will be asked for confirmation before executing the command.
Is Active	Enables the configuration.
Delete button	Click **Delete**, to delete the selected critical command from ARCON PAM.

3. Click on Save to save all the changes and the service critical command has been set. A window pops up with the following message: **New Service Critical Commands Created.**

4. For Editing, the details of the existing service critical command click on the existing row and select the Edit button at the top and make the required changes. Also, you can right-click on the row and select Edit.

Service Type	Command	Description	Ask User Confirmation	Required Approval	Is Active	Created By	Created On
SSH LINUX	useradd123567	Used for adding a new user to the system 23567	No	No	No	System	2017-10-04 06:39:41 PM
SSH LINUX	at	Execute a command at a specific time	No	No	Yes	System	2017-10-04 06:39:41 PM
SSH LINUX	cc	C Compiler	No	No	Yes	System	2017-10-04 06:39:41 PM
SSH LINUX	gcc compiler	C Compiler	No	No	No	System	2017-10-04 06:39:41 PM
SSH LINUX	chgrp	Used for changing group ownership a file or set of files.	No	No	Yes	System	2017-10-04 06:39:41 PM
SSH LINUX	chmod	Used for changing permissions on a file or set of files.	No	No	No	System	2017-10-04 06:39:41 PM

5. For Deleting the existing service critical command click on the existing row and select the Delete button at the top and make the required changes. Also, you can right-click on the row and select Delete.

Service Type	Command	Description	Ask User Confirmation	Required Approval	Is Active	Created By	Created On
SSH LINUX	useradd123567	Used for adding a new user to the system 23567	No	No	No	System	2017-10-04 06:39:41 PM
SSH LINUX	at	Execute a command at a specific time	No	No	Yes	System	2017-10-04 06:39:41 PM
SSH LINUX	cc	C Compiler	No	No	Yes	System	2017-10-04 06:39:41 PM
SSH LINUX	gcc compiler	C Compiler	No	No	No	System	2017-10-04 06:39:41 PM
SSH LINUX	chgrp	Used for changing group ownership a file or set of files.	No	No	Yes	System	2017-10-04 06:39:41 PM
SSH LINUX	chmod	Used for changing permissions on a file or set of files.	No	No	No	System	2017-10-04 06:39:41 PM

6. The Export button will export all the service critical command details in the form .xlsx format. The Copy button will copy all the details of the table.

13.5.1.2 Service Security Configurations

To navigate, use the following path:

Settings → Service → Security

Field Name	Description
Restricted Command Error Message	**This configuration sets the Message that should be displayed by ARCON PAM when an attempt is made to execute any Restricted Command.**
Valid Values	Contact ARCON PAM Administrator To Get Access to the Restricted Command.
Resolve IP Address Before Connecting (If Direct Access) - Is Enabled	**This configuration enables/disables resolving of IP Address before Connecting to target server if Direct Access (this is applied only in an environment without secured)**
Disable	If Toggle value is 'Disabled', then it disables the feature.
Enable	If Toggle value is 'Enabled', then it enables the feature.
Toolbar In App Attachmate Reflection - Is Enabled	**This configuration will allow users to access the SFTP connection of the App Attachmate Reflection application. By default ARCON PAM disables the toolbar.**
Disable	If Toggle value is 'Disabled', then this feature is disabled.
Enable	If Toggle value is 'Enabled', then this feature is enabled.
Remove Sign On Menu In App PLSQL Developer Oracle - Is Enabled	**This configuration will allow users to remove LogOn menu from PLSQL Developer Oracle Application. By default ARCON PAM enables the LogOn menu.**
Disable	If Toggle value is 'Disabled', then this feature is disabled.
Enable	If Toggle value is 'Enabled', then this feature is enabled.
ARCON PAM MultiTab Option	**This configuration enables/disables Users to open multiple Windows RDP and SSH Linux connections in multiple tabs (single window).**
Disable	If Toggle value is 'Disabled', then multiple connections can be opened but in different windows.
Enable	If Toggle value is 'Enabled', then **MultiTab** option will be displayed before establishing Windows RDP connection and **SSH MultiTab** option will be displayed before establishing the SSH Linux connection.

Field Name	Description
Oracle Virtual RAC IPs	**It will display the list of the IPs for the Oracle Virtual RAC**
Valid Values	The value ranges from 1-999.
Service Health Status	**It will display the health status of the services being monitored**
Disable	If Toggle value is 'Disabled', then this feature is disabled.
Enable	If Toggle value is 'Enabled', then this feature is enabled.
Days For Server Last Accepted On	**It will display the list of idle servers for the configured value or more for Server Last Accessed Report. Example: If the configured value is 10, the server Last Accessed Report will display all the servers that were idle for 10 days.**
Valid Values	The value ranges from 1-999.

13.5.1.3 Outside ARCON PAM Access Configuration

ARCON PAM monitors Servers that are accessed from outside ARCON PAM. You can configure actions such as send alert to configured user or block access to Server from outside ARCON PAM.

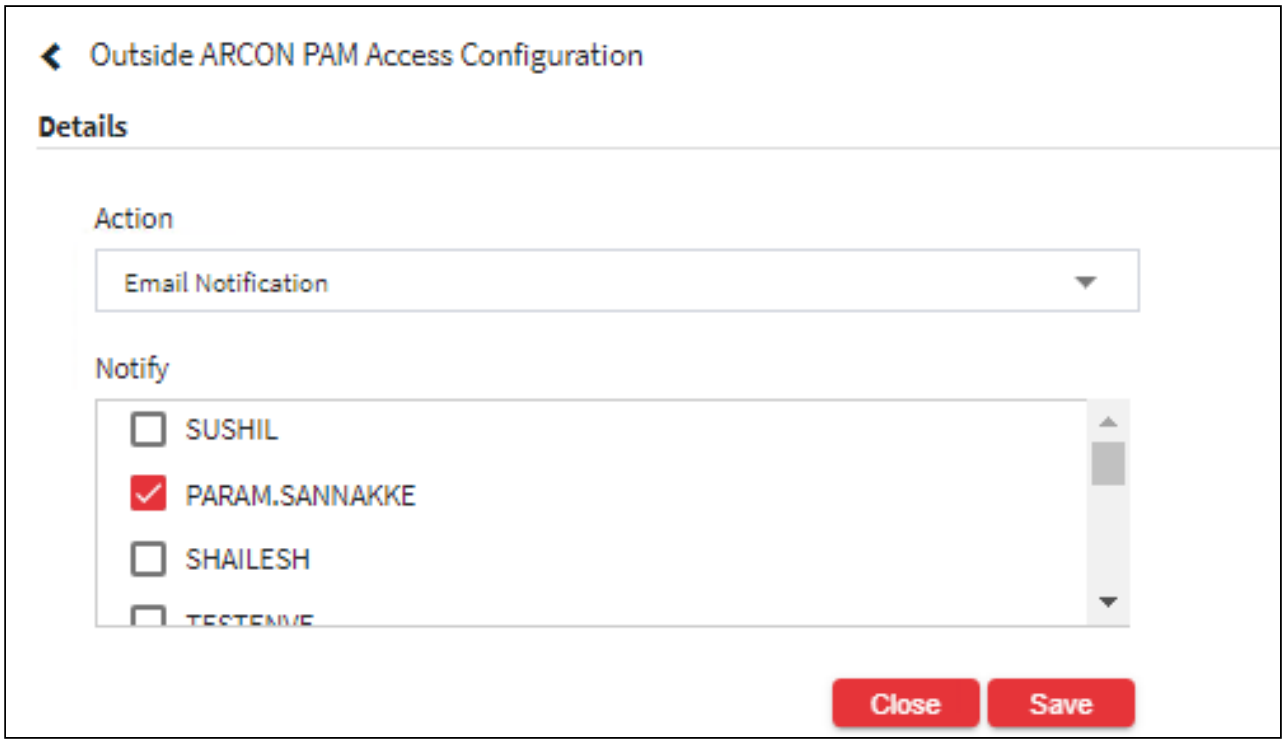
Pre-requisite: ARCOS TSPlugin service should be installed on server, for monitoring users trying to access the server.

> ⚠ The Administrator having **Outside ARCON PAM Access Configuration** privileges in **Server's Privileges** will only be able to configure action to be performed under Outside ARCON PAM Access Configuration.

To navigate, use the following path:

Settings → Service → Security

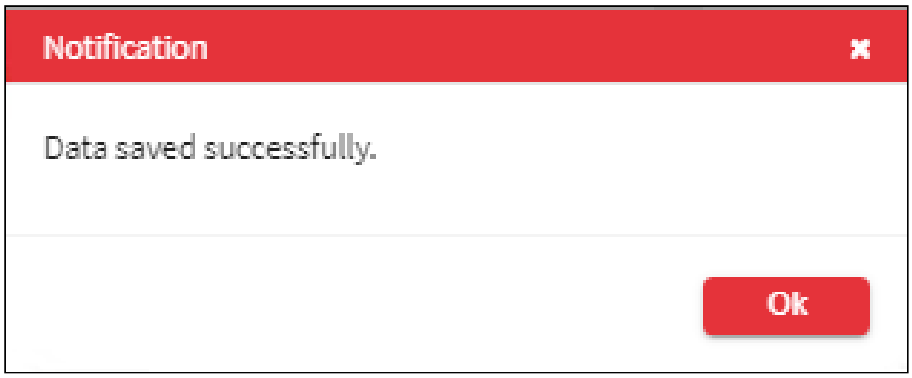
1. Select Outside ARCON PAM Access Configuration under Security.



The **Outside ARCON PAM Access Configuration** screen contains the following fields:

Field Name	Description
Action	Select the action to be taken. The valid values are: ▪ **No Action:** Perform no action on access. ▪ **Email Notification:** Send email notification to Users, necessary to be intimated during access. ▪ **Block:** Block access to server ▪ **Email Notification & Block:** Send email notification to Users and block access to server.
Notify To	Select the Users to send email notification. Email ID should be configured in **Edit User Settings** under **Manage Users** to list Users in **Notify To** selection list.

2. Select the required details and click **Save**. The following success message will be displayed : **Data Saved Successfully.**



3. Click **OK**. The details will be saved and configured action will be performed when the server is accessed outside ARCON PAM.

13.5.2 SSH

To navigate, use the following path:

Settings → Service→ SSH

Field Name	Description
Use SFTP Privileges	**This configuration sets whether SFTP Privileges should be allowed to all users or not.**
Disable	If Toggle value is 'Disabled', then this privilege is by default given to all users.
Enable	If Toggle value is 'Enabled', then Admin ID needs to give this privilege for an individual user under the Server Manager > Manage Commands tab.
ARCOS Default SSH Terminal	**This configuration sets which SSh Terminal to be used. There are two different SSh terminal interchangeably used with different sets of functions being delivered.**
Valid Values	It can be either 1 or 2. Value '1' – With this value SSh terminal will have all the standard functionality of a PuTTY client but no function key mapping. Value '2' – With this value SSh terminal will have function key mapping along with standard functionality of a PuTTY client.
SYSADM Account For Root User 7 & 16 (With Comma)	**This configuration sets SYSADM Account for Root User 7 & 16 (IP - 7 for SSH Linux and IP- 16 for DMZ SSH Linux). SYSADM is required to login to switch to Root. Multiple values are separated by Comma.**
Valid Values	The valid strings are arcon,sysadm,sysadmin,netadmin.

Field Name	Description
Root Account For IP Service Type 7 & 16 (With Comma)	**This configuration sets Root Account for IP Service Type 7 & 16 (IP - 7 for SSH Linux and IP- 16 for DMZ SSH Linux). Multiple values are separated by Comma. These accounts are used for changing password.**
Valid Values	The Valid strings are arcon,root,test.
Domain Validation For SSH Based Connections - Is Enabled	**This configuration enables/disables Domain Validation for SSH Based Connections.**
Disable	If Toggle value is 'Disabled', then it disables validation.
Enable	If Toggle value is 'Enabled', then it enables validation.
Service Critical Commands - Ask User Confirmation (Before Execution) - Is Enabled	**This configuration enables/disables the working of Ask User Confirmation (Before Execution) option of Service Critical Command.**
Disable	If Toggle value is 'Disabled', then the steps below are carried out then confirmation message will not be displayed.
Enable	If Toggle value is 'Enabled', and under Server Manager >Settings > Service >Security > Service Critical Command > Configure a command and tick Ask User Confirmation (Before Execution). Execute this critical command on the server. A confirmation message will be displayed.
ARCOS SSH Terminal (2) SSH Authentication Methods Type	**This configuration will set SSH Authentication Method for ARCON PAM SSH type 2 Terminal ("suse").**
Valid Values	Select from the dropdown where the values are 0,1,2,15.
ARCOS Switch User Reason Popup Box	**This configuration when enabled will raise a popup box when a switch user attempt is made during a service session. User needs to enter the reason for switching to another user in the popup box and click on submit button. This will effect the configured Service Type.**
Valid Values	Select from the dropdown where the values are SSH, TELNET, SQLPLUS.
ARCOS SFTP Latest Ciphers Is Enabled	**This configuration will enable/disable the latest ciphers.**
Valid Values	It ranges from 5-99.

Field Name	Description
ARCOS Putty WebService CLURL	**This configuration is used to configure web API URL for ARCON PAM API. This API can be used in PAM Client Multi-type Utility for RDP and SSH Linux Connections.**
Valid Values	Configure web API URL for ARCON API URL
Execute Network Command With Credential	**This configuration is used to configure commands for which you want ARCON PAM to enter credentials on Server before executing commands.**
Valid Values	The Configuration Value shall be Command_Name. Multiple commands can be configured separated by a comma. Eg: sudo, passwd.
Enforce Login to EN Account	**This configuration enables/disables Network Device services (Telnet Router, Telnet Switch, SSH Router, SSH Switch, SSH Telnet) to switch to configuration mode.**
Disable	If Toggle value is 'Disabled', then User needs to access service and then switch to EN service.
Enable	If Toggle value is 'Enabled', then User is switched to configuration mode.
Stop SSHOracleSqlplus Auto Login	**This configuration sets whether the Database list will be displayed to User when SSH Oracle SQL Plus connection is established from Client Manager.**
Disable	If Toggle value is 'Disabled', Service will connect to the default Database.
Enable	If Toggle value is 'Enabled', you have multiple database on the Server and you want to login into a particular DB.
Enable/Disable Copy Paste in Putty	**This Configuration restricts the Copy Paste option in putty.**
Valid Values	The valid values are Enable Copy Paste everywhere, Enable Copy Paste only in Putty window, Disable Copy Paste everywhere. **Enable Copy Paste everywhere**- This Configuration allows copy-paste functionality inside putty session window as well as outside putty eg- in notepad. **Enable Copy Paste only in Putty window**- This configuration allows copy-paste functionality only inside putty session window. **Disable Copy Paste everywhere**- This configuration disables copy-paste functionality everywhere i.e both inside and outside putty.

Field Name	Description
Disable copy to all option in ARCOSPutty	**This configuration restricts the Copy to all option in ARCOSputty.**
Disable	If the Toggle value is 'Disabled', the users can access copy to all option everywhere.
Enable	If the Toggle value is 'Enabled', the users cannot access copy to all option from ARCOSputty.

13.5.3 Windows

To navigate, use the following path:

Settings → Service → Windows

Field Name	Description
Show VNC Button	**This configuration shows/hides the VNC button on RDP Service Type.**
Disable	If Toggle value is 'Disabled', then it hides the button.
Enable	If Toggle value is 'Enabled', then it shows the button.
Windows RDP - Use Console Privileges	**This configuration enables/disables the Console Privileges button for Windows RDP.**
Disable	If Toggle value is 'Disabled', then this privilege is by default given to all users.
Enable	If Toggle value is 'Enabled', then Admin ID needs to assign this privilege for individual users under the Server Manager > Manage Commands tab.
Windows RDP - Allow Clipboard To All	**This configuration enables/disables Clipboard by default for Windows RDP session taken through ARCON PAM.**
Disable	If Toggle value is 'Disabled', then this feature is disabled.
Enable	If Toggle value is 'Enabled', then this feature is enabled.
Windows App Option For Windows RDP - Is Enabled	**This configuration enables/disables display of Windows App option before accessing Windows RDP service in CM > Connections > Select Windows RDP option from Service Type drop-down > Click Open.**
Disable	If Toggle value is 'Disabled', then this feature is disabled.
Enable	If Toggle value is 'Enabled', then this feature is enabled.

Field Name	Description
Process Level Restriction - Is Enabled	**This configuration enables/disables process restriction on Windows Server.**
Disable	If Toggle value is 'Disabled', then processes will not be restricted. Also 'Manage Processes' tab will not be available under Server Manager > User and Services and 'Process Logs' will not be available under View Logs.
Enable	If Toggle value is 'Enabled', then processes will be restricted on Windows Server.
ARCOS TS Monitor Keep Alive Max Value	**This configuration sets the number of attempts to connect to the ARCOS TS Monitor plug-in on Server for the Session taken through ARCON PAM. If ARCOS TS Monitor plug-in is not connected in these attempts then the session is terminated.**
Valid Values	It ranges from 1-99
ARCOS TS Monitor Connection Timeout (Seconds)	**This configuration is a timeout value for RDP Terminal to determine whether ARCON PAM TS Monitor has started on target server (if configured for particular RDP session).**
Valid Values	It ranges from 30-999
Allow RDP Connection Without TS-Monitor	**This configuration enables/disables session termination if ARCOS TSPlugin service is not installed on Server but ARCOS TS-Monitor is enabled for User and Service mapping under Manage Commands(Server Manager).**
Disable	If Toggle value is 'Disabled', then the session will be terminated.
Windows Terminal Option For Windows RDP - Is Enabled	**This configuration enables/disables display of Terminal option before accessing Windows RDP service in CM > Connections > Select Windows RDP option from Service Type drop down > Click Open.**
Disable	If Toggle value is 'Disabled', then this feature is disabled.
Enable	If Toggle value is 'Enabled', then this feature is enabled.

13.5.4 Request

To navigate, use the following path:

Settings → Service→ Request

Field Name	Description
Time Based Request Service Access - Is Enabled	**This configuration sets availability for Time Based Service Access Request under CM > Connections > Raise Request > Service Access > Access Type drop-down.**
Disable	If Toggle value is 'Disabled', then it disables availability.
Enable	If Toggle value is 'Enabled', then it enables availability.
Hide Configuration Command for Service Request	**This configuration will hide/display the configuration command field on the Service Access Request form (Client Manager > My Access > Raise Request > Service Access).**
Disable	If Toggle value is 'Disabled', then it will display the Configuration Command field
Enable	If Toggle value is 'Enabled', then it will hide the Configuration Command field on the Service Access Request form.
ARCOS Service Password - Is Enabled	**It enables/disables Service Password requests.**
Disable	If Toggle value is 'Disabled', then users won't be able to raise a service password request.
Enable	If Toggle value is 'Enabled',(default value) then the users shall be able to raise a service password request.
ARCOS Service Access - Is Enabled	**This configuration will enable or disable Service Access option under Raise Request (My Access > Raise Request) in Client Manager**
Disable	If Toggle value is 'Disabled', then it disables the feature.
Enable	If Toggle value is 'Enabled', then it enables the feature.
Access Duration For Service Access Request(in days)	**The users can raise a service access request for specified number of days.**
Valid Values	It ranges from 1-90 days. The minimum value is 1 (default value), the users shall be able to raise a service access request only for a day. The maximum value is 90, the users shall be able to raise a service access request for 90 days.

Field Name	Description
Permanent Request Service Access - Is Enabled	**This configuration enables/disables the users to raise a permanent service access request.**
Disable	If Toggle value is 'Disabled', then the users won't be able to raise a permanent service access request.
Enable	If Toggle value is 'Enabled', then the users shall be able to raise a permanent service access request.
Time Based Service Access Request From Server Manager - Is Enabled	**This configuration enables/disables the pop-up which asks for Service level access, whether, OneTime, Time Based or Permanent under Server Manager > Manager> Manage User/Service.**
Disable	If Toggle value is 'Disabled', then users won't be able to see the popup on selecting the service.
Enable	If Toggle value is 'Enabled', then users will be able to see the popup on selecting the service.
One Time Service Access Request- Is Enabled	**This configuration sets availability for One Time Service Access Request under CM > Connections > Raise Request > Service Access > Access Type drop-down.**
Disable	If Toggle value is 'Disabled', then the users won't be able to raise a one time service access request.
Enable	If Toggle value is 'Enabled', then the users shall be able to raise a one time service access request.

13.5.5 Service Modification

13.5.5.1 Service Mandatory Field Configuration

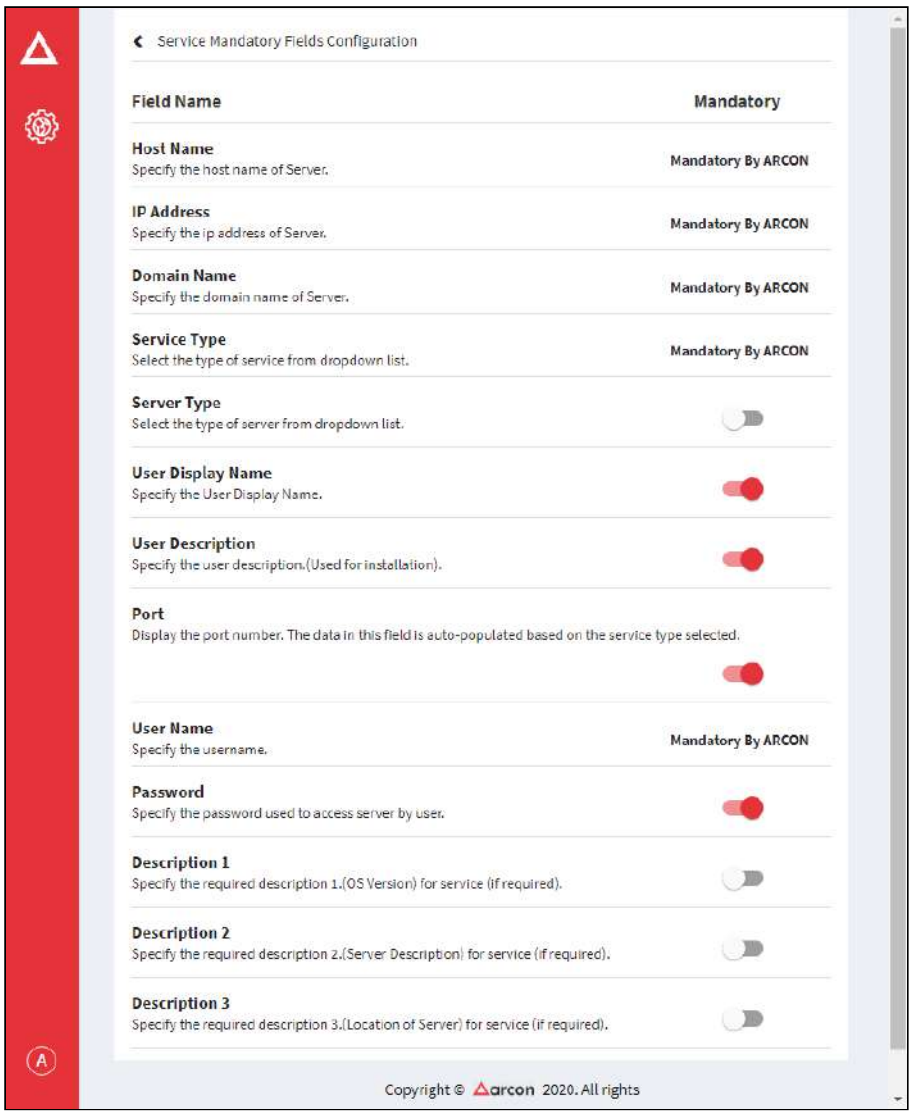
The Service mandatory field configurations sets the mandatory configurations which helps an organization in reviewing and auditing. ARCON has few proprietary mandatory configurations, however, the admins too can set their own mandatory configurations. These settings are reflected with an asterisk mark while creating/ modifying the service, or using the quick search functionality to find a service and then modify it, or when the user uses bulk update, all under the Manager Service Section. It is also reflected while importing server connections under the import section and while setting service details in ARCON PAM API.

⚠ The Administrator having **Service Mandatory Fields Configuration** privilege in Server's Privileges will only be able to configure details in SService mandatory field configurations.

To navigate, use the following path:

Settings → Service → Service Modifications

1. Select Service Mandatory Field Configuration under Service Modifications.



2. Configurations enabled here are set as mandatory fields in the Server Manager.

13.5.5.2 Advanced Utility

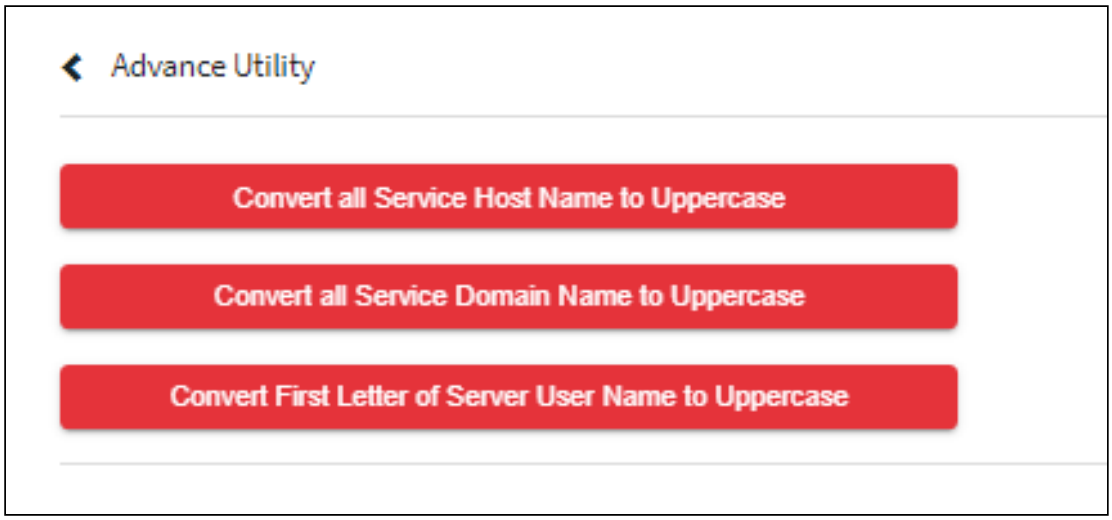
Advanced Utility is used to convert the font of the Service Host Name and Service Domain Name to uppercase.

> ⚠ The Administrator having **Advanced Utility** privileges in Server's Privileges will only be able to convert the font.

To navigate, use the following path:

Settings → Service → Modification

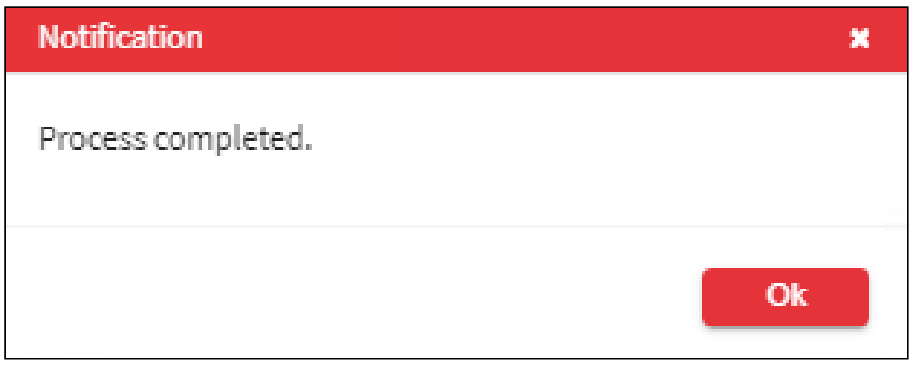
1. Select Advanced Utility under Modification



The **Advance Utility screen** contains the following buttons:

Field Name	Description
Convert All Service Host Name to Uppercase	It converts the font of all service hostname to uppercase.
Convert All Service Domain Name To Uppercase	It converts the font of all service domain name to uppercase.
Convert First Letter of Server User Name To Uppercase	It converts the font of the first letter of Server username to uppercase.

2. A window pops up with the following message: **Process completed.**



13.5.5.3 Service Classifications

Service Classification defines the classification for a service such as critical, data, or antivirus server. In addition, you can modify the existing defined classification. Once the classification is defined, you can apply the classification while modifying the parameters of a service.

⚠ The Administrator having **Service Classification** privilege in Server's Privileges will only be able to configure under Service Classification.

To navigate, use the following path:

Settings → Service → Modification

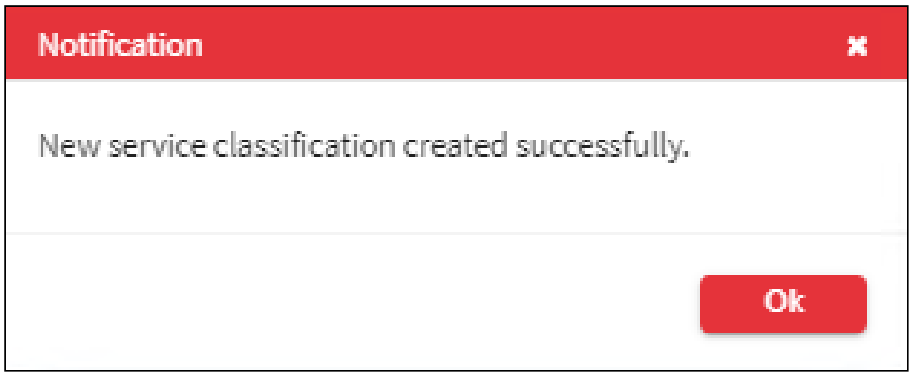
1. Select Service Classification under Modification

2. Select the Add button to add a new service classification.

The **Service Classification** screen contains the following fields:

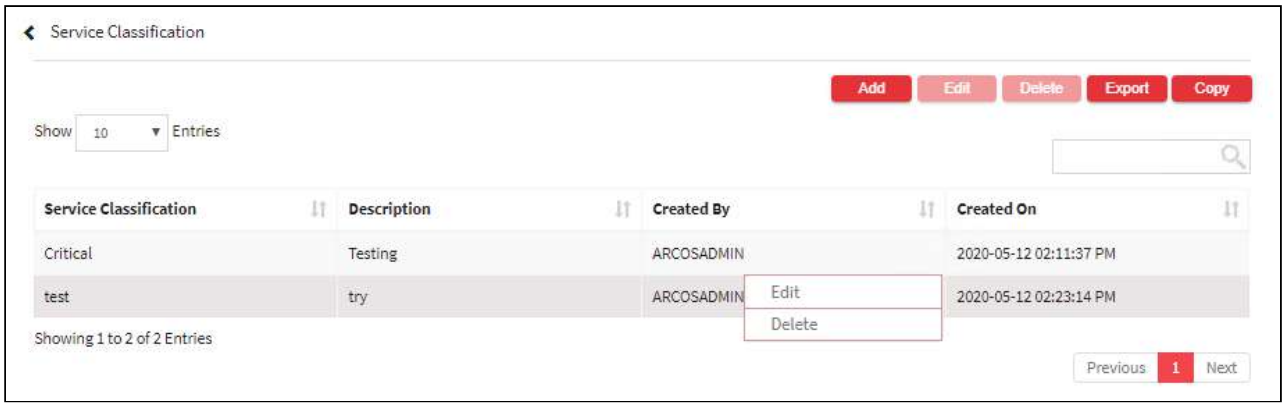
Field Name	Description
Service Classification	Specify the name for a service classification.
Description	Specify the description for a service classification.

3. Click on Save to save all the changes and the service critical command has been set. A window pops up with the following message: **New service classification created. successfully.**



4. For Editing, the details of the existing service classification click on the existing row and select the Edit button at the top and make the required changes. Also, you can right-click on the row and select Edit.

5. For Deleting the existing service classification click on the existing row and select the Delete button at the top and make the required changes. Also, you can right-click on the row and select Delete.



6. The Export button will export all the service critical command details in the form .xlsx format. The Copy button will copy all the details of the table.

1. You can apply this service classification to service (s).

a. **Apply to a single Service:**
To apply Service Classification to single service, use the following path:
Server Manager → Manage → Users and Services → Manage Services

i. Select a service.
ii. Right click and select **Modify Service Parameters**.
iii. Select **Service Classification** from drop down.
iv. Click **Modify**. The selected Service Classification will be applied to Service.

b. Apply to a group of Services:
To apply Service Classification to services, use the following path:
Server Manager → Tools → Settings → Groups→ Apply Password Settings

i. Select the LOB or profile from the **LOB/ Profile** dropdown list. A list of service groups are displayed in the grid.
ii. Select the checkbox from the **Service Group Name** list. It displays the count of services for that particular group under **Service Type** grid.
iii. Select a type of service from the **Service Type** list. This will enable you to set automated change passwords for that particular service type.
iv. To apply service classification, select **Allow** checkbox against **Service Classification** drop down. The drop down will be enabled.
v. Select the required service classification.
vi. Click **Confirm Changes** button. Service Classification will be applied to services under selected Service Group and Service Type.

13.5.5.4 Service Modifications Configurations

To navigate, use the following path:

Settings → Service → Modification

Field Name	Description
Description 1 New Name	**This configuration sets the new name for Description 1 in Manage Services.**
Valid Values	It sets the value for Description 1.
Description 2 New Name	**This configuration sets the new name for Description 2 in Manage Services.**
Valid Values	It sets the value for Description 2.
Description 3 New Name	**This configuration sets the new name for Description 3 in Manage Services.**
Valid Values	It sets the value for Description 3.

Field Name	Description
Description 1 Is Checked By Default	**This configuration enables/disables Description 1 in Manage Services.**
Disable	If Toggle value is 'Disabled', then it enables Description 1.
Enable	If Toggle value is 'Enabled', then it disables Description 1.
Description 2 Is Checked By Default	**This configuration enables/disables Description 2 in Mo Services**
Disable	If Toggle value is 'Disabled', then it enables Description 2.
Enable	If Toggle value is 'Enabled', then it disables Description 2.
Description 3 Is Checked By Default	**This configuration enables/disables Description 3.**
Disable	If Toggle value is 'Disabled', then it enables Description 3.
Enable	If Toggle value is 'Enabled', then it disables Description 3.
Confirmation Box For Mapping Operations In ARCOS Server Manager - Is Enabled	**This configuration sets whether the Confirmation box should be displayed when mapping Operations are performed in Server Manager between entities.**
Disable	If Toggle value is 'Disabled', then it disables the appearance of box.
Enable	If Toggle value is 'Enabled', then it enables the appearance of box.
Allow Permanently Service Deletion - Is Enabled	**This configuration enables/disables permanent service deletion from ARCON PAM database including, the logs, mapping, and so on. It deletes everything except the audit trail.**
Disables	If Toggle value is 'Disabled', then it disables the feature.
Enable	If Toggle value is 'Enabled', then it enables the feature.
Service Display Configuration	**This configuration sets which Service details are to be displayed in following fields:** • **Service (CM > My Access > Raise Request > Service Access)** • **Service (CM > My Access > Raise Request > Service Password)** • **Service / IP Address (CM > My Access > Raise Request > Ticket)**

Field Name	Description
Valid Values	IPADDRESS,USERNAME,DOMAIN,DBINSTANCE,HOSTNAME,USERDISPLAYNAME,USERDESCRIPTION
Service Creation - Force Host Name check from DB	**This configuration is explained below.**
Disable	If Toggle value is 'Disabled', while creating a service the combination of service type and IP address, and the Host Name is different then it will display a prompt Yes/No. If yes, the service will be created, and If No, the service will not be created.
Enable	If Toggle value is 'Enabled', while creating a service it ensures that the combination of service type and IP address, the Host Name has to be the same every time for the service to be created. It will not create a service if the hostname is different.
Service Expiry Days	**If the value is set to 5 an alert notification shall be sent 5 days before the service expiry and so on. An alert notification shall be displayed in ACMO notifications before the Service Validity expires (before the days configured) so that the Administrators can extend the validity period of the service if required. Users with the Privilege Service Expiry Due will only be able to view this notification.**
Valid Values	It ranges from 5-99 days.

13.6 Password

This section includes the following topics:

- HSM configuration
- Generic Scheduler Setting
- Password Dashboard
- View Password
- Password Change
- Reconciliation
- Debug Mode
- Miscellaneous

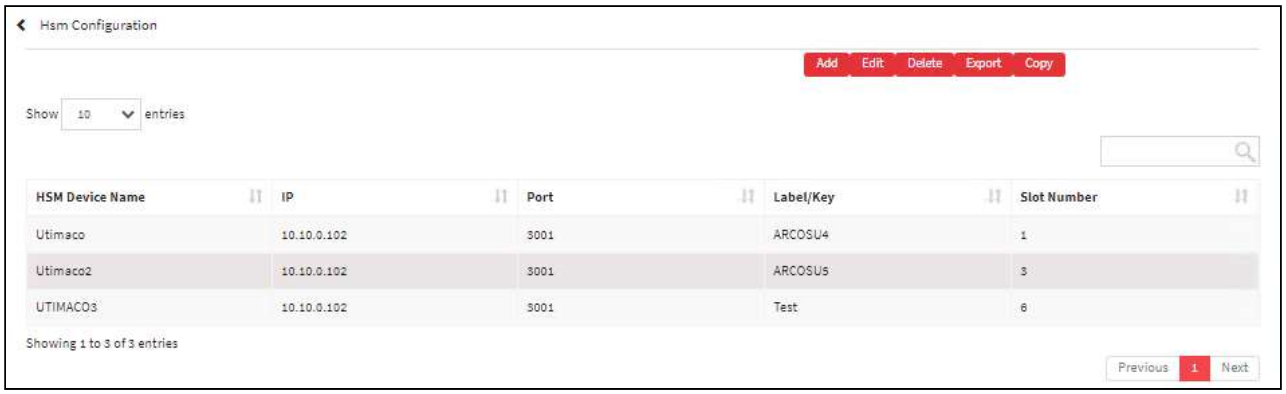
13.6.1 HSM Configuration

The Hardware Secure Module (HSM) feature is used to verify sensitive data by provisioning encryption and decryption. This feature can be enabled for a service. ARCON PAM will use HSM for verifying details. The Administrator responsible for modifying a service can enable this feature.

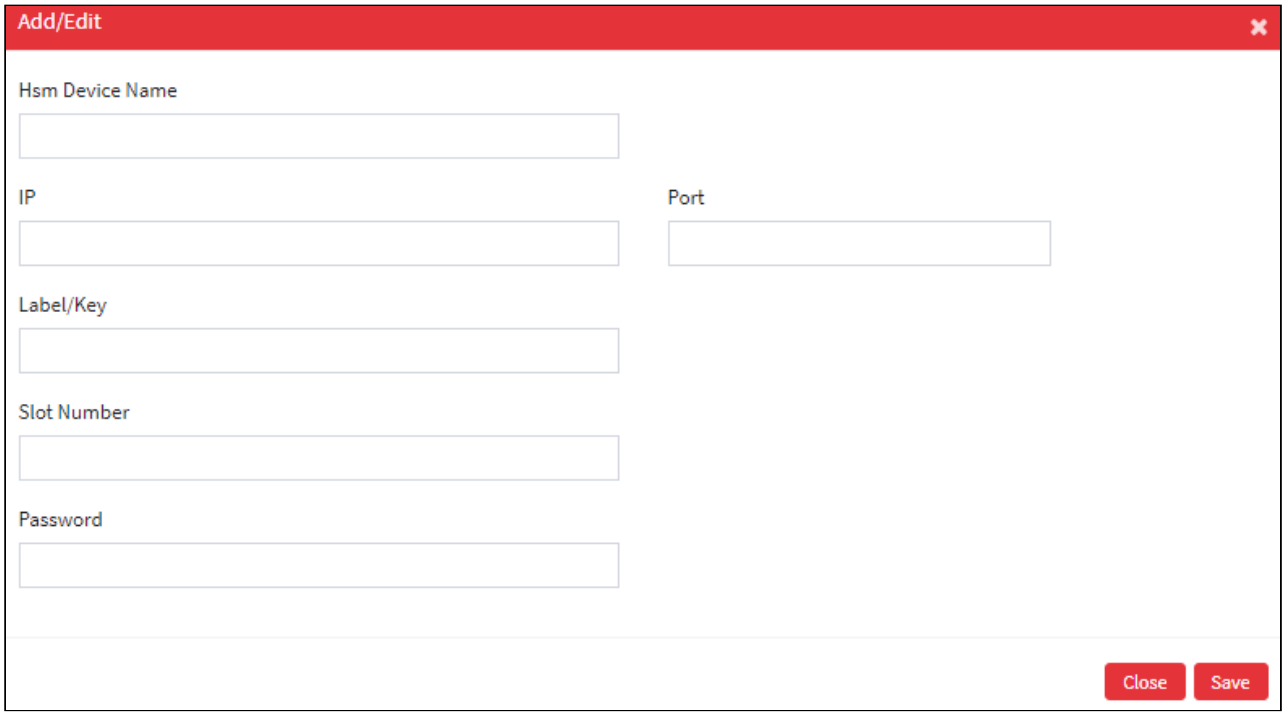
To navigate, use the following path:

Settings → Password

1. Select Hardware Secure Module under Configure.



2. Select the Add button to add a new Hardware Secure Module.

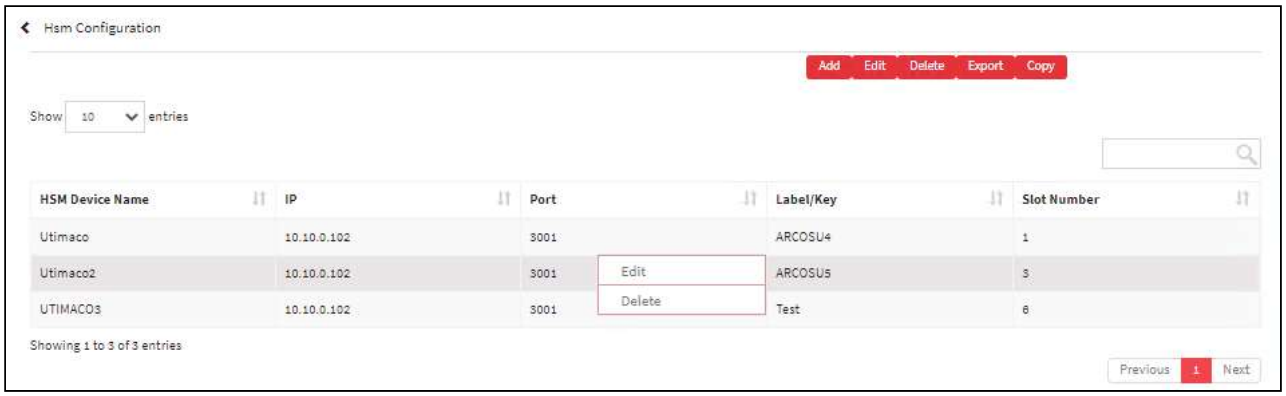


The **Hardware Secure Module Configuration** screen contains the following fields:

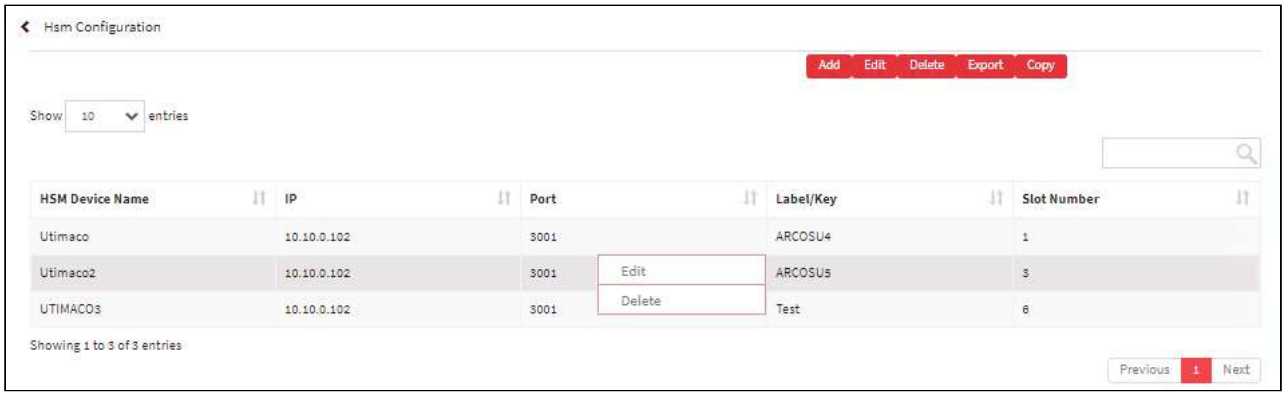
Field Name	Description
HSM Device Name	Enter the HSM device name.
IP Address	Enter the IP Address of HSM.
Port	Enter the port number.
Label/Key	Enter the Key
Slot Number	Enter the slot number
Password	Enter the password.

3. Enter the details and click Save button to create a new Hardware Secure Module Configuration.

4. For Editing, the details of the existing Hardware Secure Module Configuration click on the existing row and select the Edit button at the top and make the required changes. Also, you can right-click on the row and select Edit.



5. For Deleting the existing Hardware Secure Module Configuration click on the existing row and select the Delete button at the top and make the required changes. Also, you can right-click on the row and select Delete.



6. The Export button will export all the Hardware Secure Module Configuration details in the form .xlsx format. The Copy button will copy all the details of the table.

⚠

- You need to enable Precision Biometric for fingerprint authentication over API from the back end.
- The Precision Authentication API URL will be provided by the Client. Enter this URL in the **URL** text field and configure details in **Web API Configuration** window.

13.6.2 Generic Scheduler Settings

The Generic Scheduler Settings are the critical configurations given to the ARCON PAM Services and executable files. In this configuration the Settings Values are configured. The executable files such as ARCOS Generic Scheduler, ARCOS Provisioning Scheduler, and so on, consider these settings for running the files. ARCON PAM Services such as ARCOS Alert Service, ARCOS Log Manager Service, and so on, consider these settings for running the services.

⚠ To configure the values Administrator should be assigned **Default Configuration** and **Generic Scheduler Setting** privileges from the Administrator under Server's Privileges.

Assign Generic Scheduler Setting

To assign these privileges follow the below steps:

1. Open **Server Manager**.
2. On the menu bar, click **Manage > Users and Services > Manage Users**.
3. On the **Users Type**, select admin from the dropdown list. All admin users will be displayed.
4. Select the user present in the **User Display Name** column.
5. Right click on the admin user to whom you want to give the **Generic Scheduler Setting** privileges and select **Edit Privileges**. **User Privileges Settings** windows open.

   ⚠ Be sure that the Server Privileges radio button is selected as we are assigning these privileges to the Admin users.

6. On the **User's Available Privileges** frame, select the **Default Configuration** and **Generic Scheduler Setting** and click the **<< Add** button.
7. The **Default Configuration** and **Generic Scheduler Setting** privileges will be added on the **User's Assigned Privileges** frame.

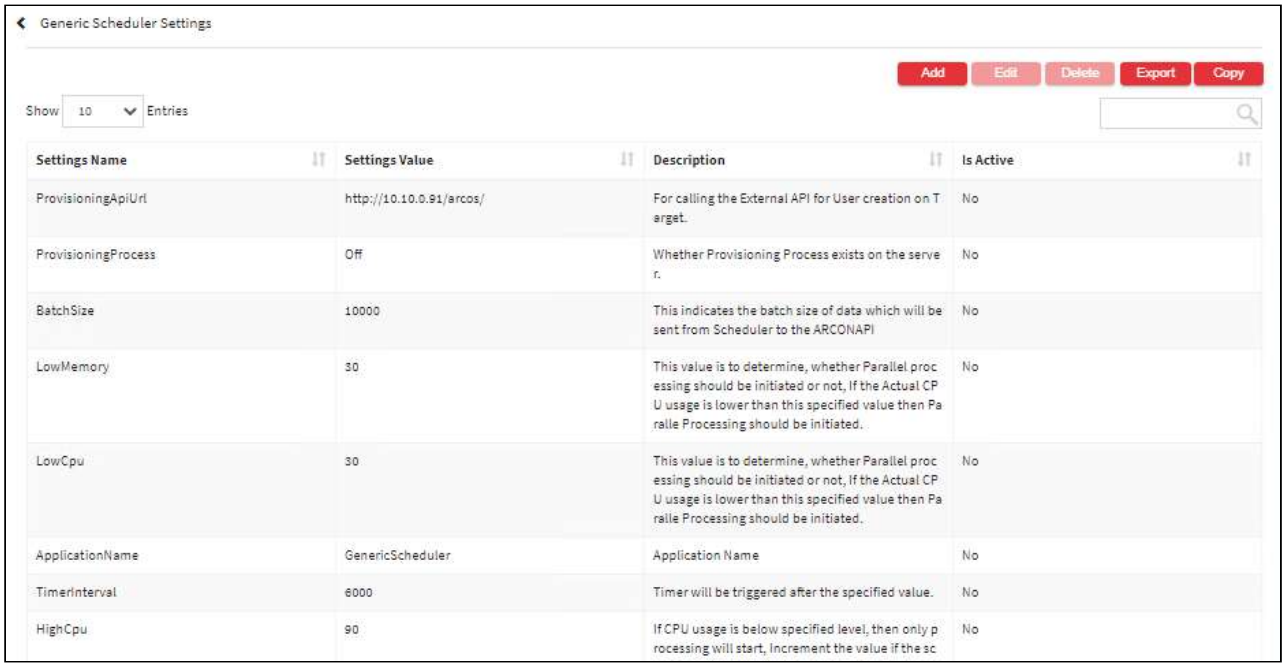
Configure Generic Scheduler Settings

To configure Generic Scheduler Settings follow the below steps:

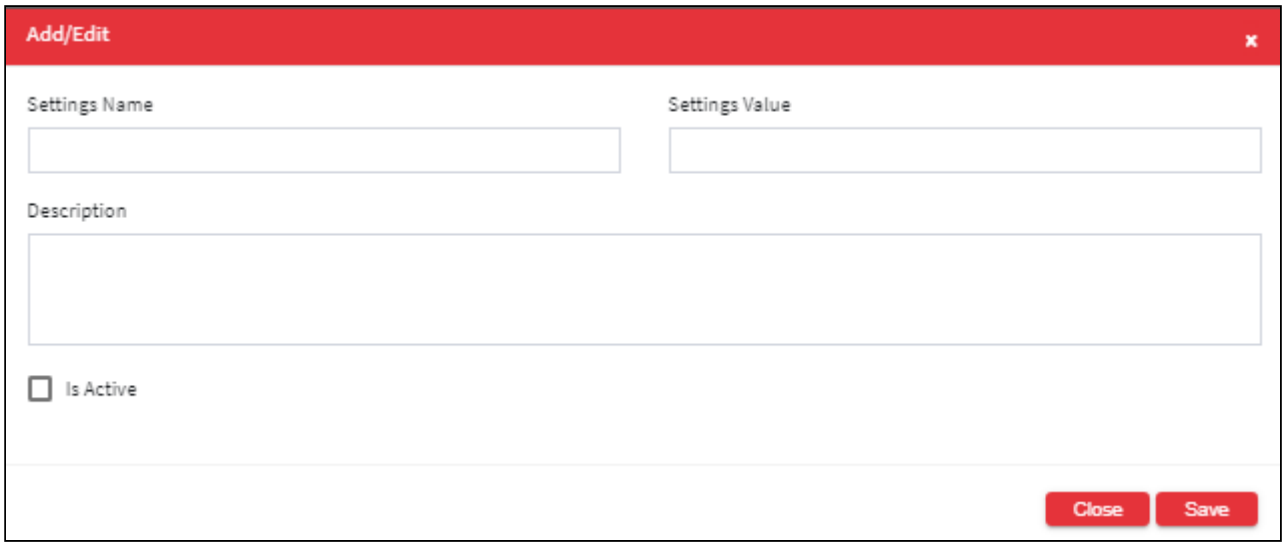
To navigate, use the following path:

Settings → Password

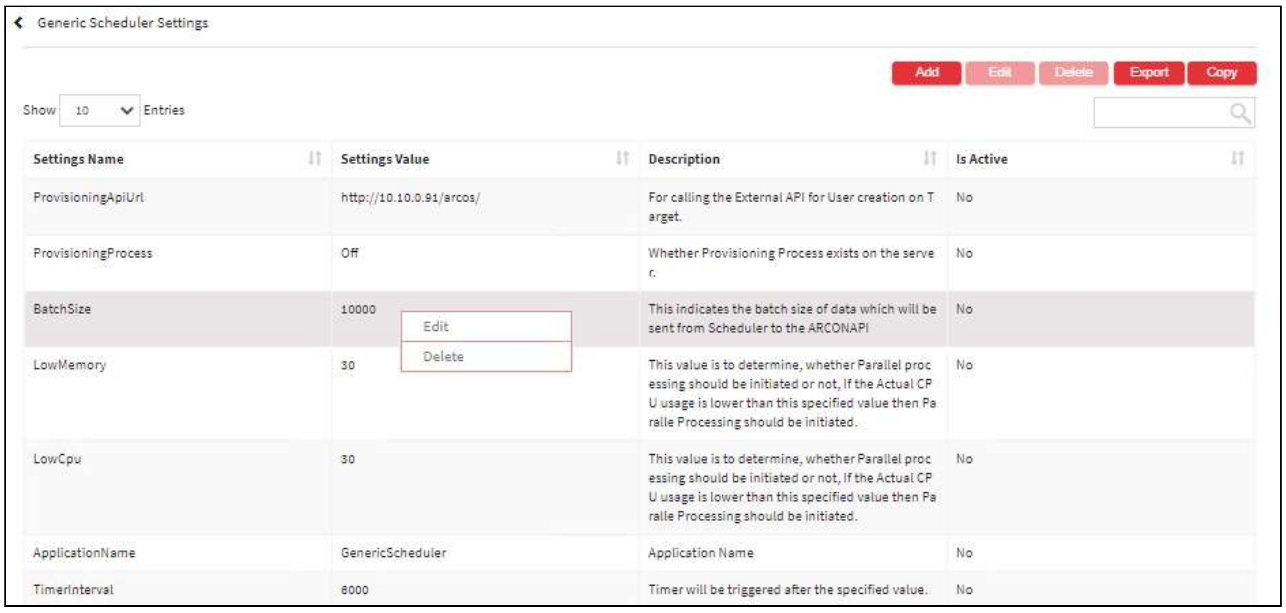
1. Select Generic Scheduler settings.



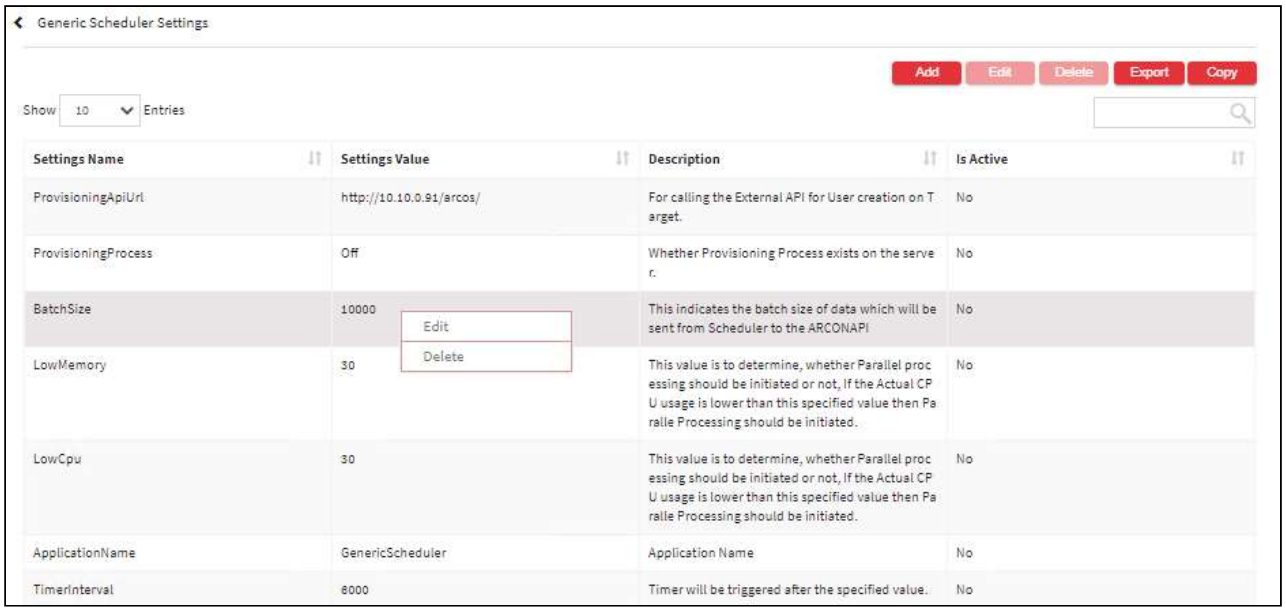
2. Select the add button to configure a new Generic Scheduler Settings



3. Enter name of settings, value of settings and its description in **Settings Name**, **Settings Value** and **Description** text field respectively.
4. Select **Is Active** checkbox to enable this settings.
5. Enter the details and click **Save** to create a new Generic Scheduler Settings.
6. For Editing, the details of the existing Generic Scheduler Settings click on the existing row and select the Edit button at the top and make the required changes. Also, you can right-click on the row and select Edit.



7. For Deleting the existing Generic Scheduler Settings click on the existing row and select the Delete button at the top and make the required changes. Also, you can right-click on the row and select Delete.



8. The Export button will export all the Generic Scheduler Settings details in the form .xlsx format. The Copy button will copy all the details of the table.
   The settings given in below table are used by executable files and services. Following is the categorization:

   - Provisioning Scheduler: This is used for LAM.
   - ARCOS Generic Scheduler: This is responsible for transferring the data from ARCON PAM DB to the Data warehouse DB via ARCON PAM API. This is used in Data Warehouse.
   - ARCONPAMVaultApp: This service is responsible for reconciliation of each service present in ARCON PAM Services.

   The settings name along with its usage and default settings value are as follows:

Sr. No.	Settings Name	Settings Value	Description	Usage
1.	ProvisioningApiUrl	http://IP/arcos/	This value is used for calling External API for User creation on Target Server.	Used for Provisioning Scheduler
2.	ProvisioningProcess	Off	This value is used to check whether Provisioning Process exists on the server or not.	Used for Provisioning Scheduler
3.	BatchSize	10000	This value indicates the batch size of data which will be sent from Scheduler to the ARCON API.	Used for ARCOS Generic Scheduler

Sr. No.	Settings Name	Settings Value	Description	Usage
4.	LowMemory	30	-This value is used to determine, whether Parallel processing should be initiated or not. - If the Actual CPU usage is lower than this specified value then Parallel Processing should be initiated.	Used for Provisioning Scheduler, ARCOS Generic Scheduler and ARCONPAMVaultApp
5.	LowCpu	30	-This value is used to determine, whether Parallel processing should be initiated or not. -If the Actual CPU usage is lower than this specified value then Parallel Processing should be initiated.	Used for Provisioning Scheduler, ARCOS Generic Scheduler and ARCONPAMVaultApp
6.	ApplicationName	GenericScheduler	This value indicates the name of the application.	Used for ARCOS Generic Scheduler
7.	TimerInterval	6000	This value indicates the Timer to be triggered after the specified value.	Used for Provisioning Scheduler, ARCOS Generic Scheduler and ARCONPAMVaultApp
8.	HighCpu	90	-The value indicates the high limit of CPU usage. -If CPU usage is below specified level, then only processing will start. Increment the value if the scheduler is not running.	Used for Provisioning Scheduler, ARCOS Generic Scheduler and ARCONPAMVaultApp
9.	ParallelProcessing	N	-This value indicates whether Parallel Processing should start or not. -Irrespective of low usage, if the value is N, then parallel processing wont start. -Possible value for this setting are: Y or N.	Used for Provisioning Scheduler, ARCOS Generic Scheduler and ARCONPAMVaultApp
10.	SiteName	Site Name (Eg. Site1)	This value indicates the site name used in Data Warehouse.	Used for ARCOS Generic Scheduler
11.	DWHAPIUrl	http://IP:Port/api/	This value indicates URL of API for dumping data into the Data Warehouse Database.	Used for ARCOS Generic Scheduler

Sr. No.	Settings Name	Settings Value	Description	Usage
12.	OffPeakTime	NightTime	This value indicates the time other than peak time. Possible Values for this setting are: NightTime, DayTime and Both.	Used for ARCOS Generic Scheduler
13.	DecryptDataLimit	50000	This value indicates the decryption limit used for Data Warehouse Application for decrypting data at a single time.	Used for ARCOS Generic Scheduler
14.	DatawareHouseProcess	On	This value indicates whether Data Warehouse Process exists on the Server.	Used for ARCOS Generic Scheduler
15.	HighMemory	90	This value indicates the Timer to be triggered after the specified value.	Used for Provisioning Scheduler, ARCOS Generic Scheduler and ARCONPAMVaultApp
16.	StartTime	9:00:00	-This value indicates the start time of service password change password. -Enter value in 24 hour format.	Used for ARCONPAMVaultApp
17.	EndTime	22:00:00	-This value indicates the end time of service password change process. -Enter value in 24 hour format.	Used for ARCONPAMVaultApp
18.	PasswordChangeProcess	On	This value is used for turning On/ Off password change process.	Used for ARCONPAMVaultApp
19.	MaxPasswordAgeRange	10	-This value indicates the number of hours to be considered by password change vault service. -The password of service will get changed before the specified number of hours of the password expiry. Eg. Password of service will be changed 10 hours before the password expiry time. -The default value for this setting is 10.	Used for ARCONPAMVaultApp
20.	MonthCount	2	This value indicates the number of months for fetching data.	Used for ARCOS Generic Scheduler

Sr. No.	Settings Name	Settings Value	Description	Usage
21.	IsRunIncrementalData	0	This value indicates whether to run increment data instead of checking firstrun. The value '0' stands for 'No' and '1' stands for 'Yes'. ⚠ This is considered only for DWH Log tables.	Used for ARCOS Generic Scheduler
22.	TillDate	05/01/2018	This value indicates upto which back date data should be pushed to DWH.	Used for ARCOS Generic Scheduler
23.	MaxDegreeOfParallelism	1000	This value indicates the number of parallel threads running at a time. More number might increase the CPU percentage of the Server.	Used for ARCONPAMVaultApp
24.	TelnetTimeout	0	This value is used for telnet the server for connectivity. The value is in milliseconds.	Used for ARCONPAMVaultApp
25.	BatchSizeForReconciliation	50	This value indicates the batch size used for reconciliation of services parallelly. ⚠ If the batch size is increased then check for Out Of Memory exception.	Used for ARCONPAMVaultApp

13.6.3 Password Dashboard

Password Dashboard provides the necessary information for password related activities in the form of cards and graphs. The cards display the count of open passwords, success and failure rate of services in SPC and VPC, the number of passwords auto healed, password checkouts, and the count of envelopes printed. The graphs are dynamic and display password age, password expiry for services (Scheduled and Disabled), password reconciliation, and envelope status over the chosen time range.

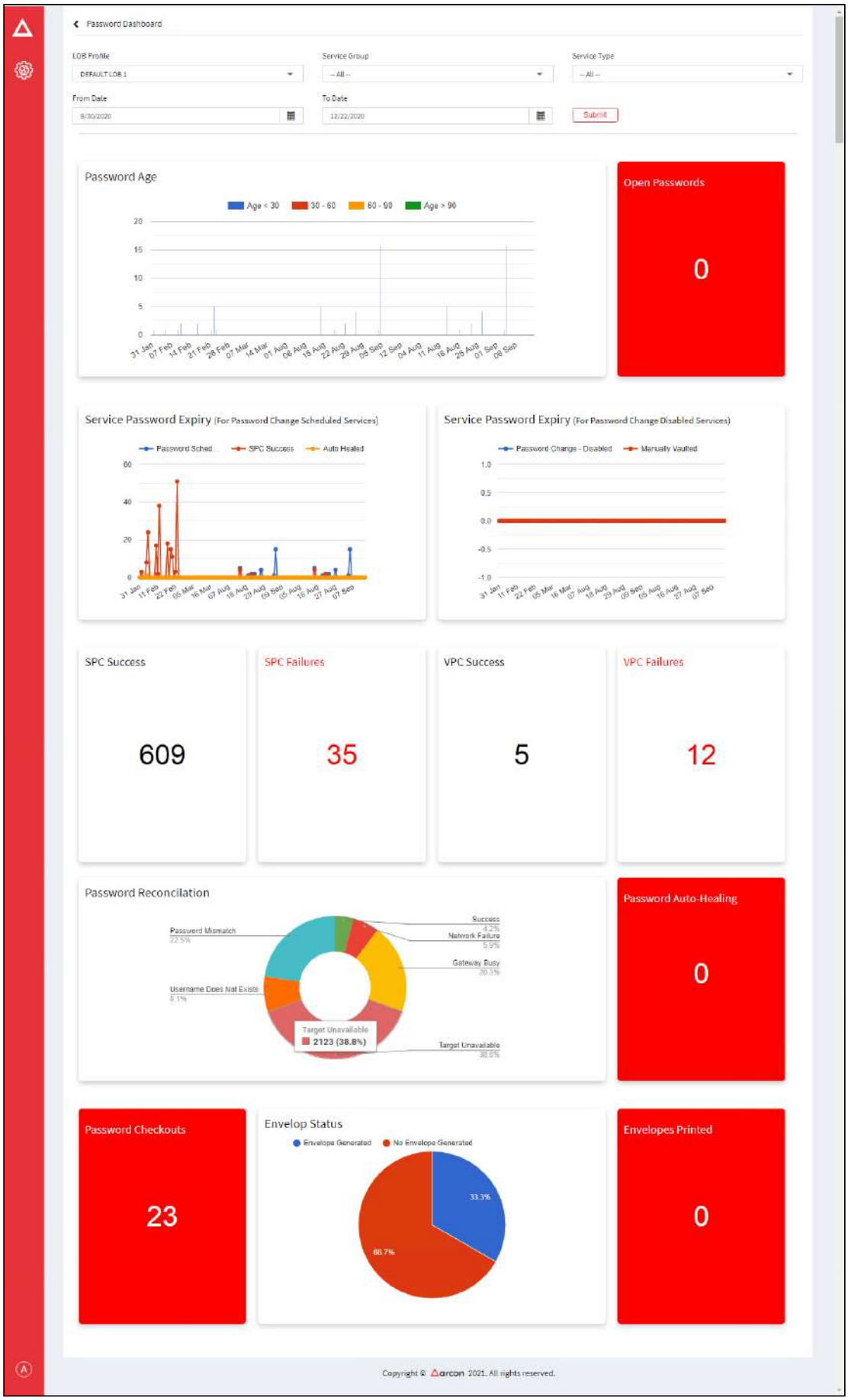
⚠ The Administrator having **Password Dashboard** privileges in Server's Privileges will only be able to do configurations under Password Dashboard.

To navigate, use the following path:

Settings → Password

1. Select **Password Dashboard**.

2. Select the LOB/Profile, Service Group, Service Type, From Date, and To Date, filters to view the Password Dashboard.

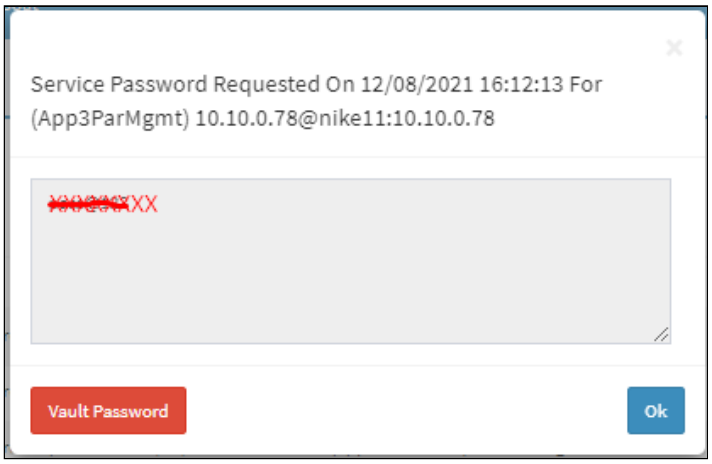

Password Dashboard
LOB Profile
DEFAULT LOB 1
Service Group
-- All --
Service Type
-- All --
From Date
9/30/2020
To Date
12/22/2020
Submit
Password Age
Age < 30
30 - 60
60 - 90
Age > 90
Open Passwords
0
Service Password Expiry (For Password Change Scheduled Services)
Password Sched...
SPC Success
Auto Healed
Service Password Expiry (For Password Change Disabled Services)
Password Change - Disabled
Manually Vaulted
SPC Success
609
SPC Failures
35
VPC Success
5
VPC Failures
12
Password Reconcilation
Password Mismatch
22.5%
Username Does Not Exists
8.1%
Success
1.2%
Network Failure
9.9%
Gateway Busy
20.3%
Target Unavailable
2123 (38.8%)
Target Unavailable
38.8%
Password Auto-Healing
0
Password Checkouts
23
Envelop Status
Envelope Generated
No Envelope Generated
33.3%
66.7%
Envelopes Printed
0
Copyright © arcon 2021. All rights reserved.

13.6.4 View Password

This section helps you to with configurations to view passwords.
To navigate, use the following path:

Settings → Password → View Password

Field Name	Description
View Password - No of Authentication Users	**This configuration sets the number of users to be enabled to authenticate on View Password window under Server Manager > Manage Services > Select a service > Right-click and select View Password.**
Valid Values	It is either 1 or 2.
Allow Password Request Of Dependent Services - Is Enabled	**This configuration enables/disables users to request password for services that are dependent on other services for password change.**
Disable	If Toggle value is 'Disabled', then the user can request password for only parent service.
Enable	If Toggle value is 'Enabled', then the user can request password for both parent and dependent service.
Allow Multiple Users to Request to open Service Password	**This will allow the Administrators to define the settings to allow/deny multiple users to work on a particular Service.**
Disable	If Toggle value is 'Disabled', it will not allow multiple users to open an already requested/opened Service Password.
Enable	If Toggle value is 'Enabled', it will allow multiple users to open an already requested/opened Service Password.
Max Hours for Service Password Duration	**This configuration sets maximum hours to be displayed in Open for Hours drop-down under Service Password Request (Client Manager).**
Valid Values	It ranges from 0-999.

Field Name	Description
Display Vault Password button	**This configuration displays the Vault password button under ACMO → Mailbox.** 
Disable	If Toggle value is 'Disabled', the Vault Password button is not visible in the ACMO→Mailbox.
Enable	If Toggle value is 'Enabled', the Vault Password button is visible in the ACMO→Mailbox.
Auto clear closed passwords from Mail Box older than days	**This Configuration clears the closed password from Mailbox post the configured days.**

13.6.5 Password Change

13.6.5.1 Password Dictionary

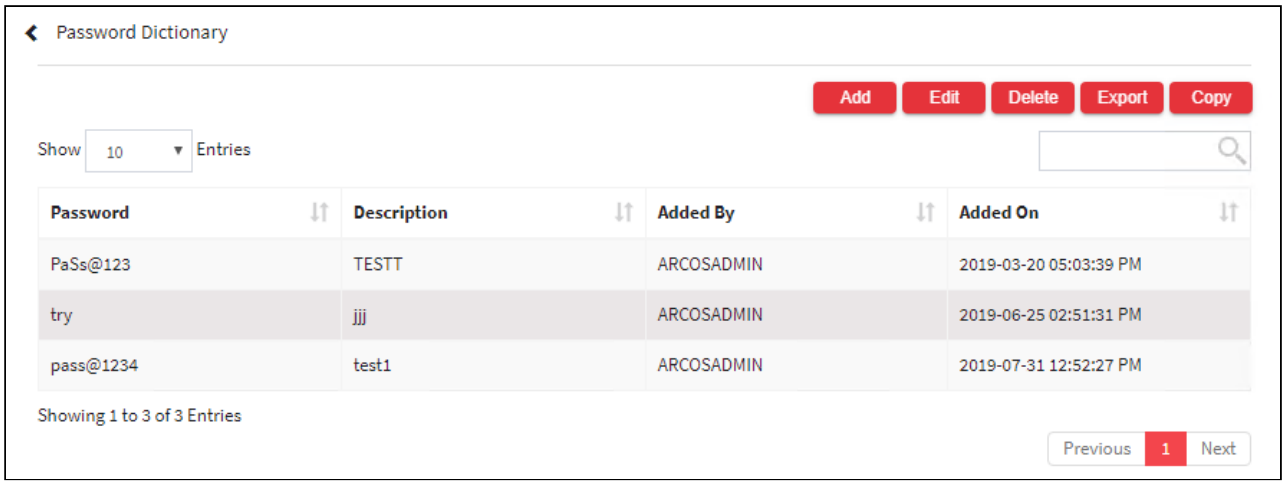
The password dictionary is the repository of default passwords. In ARCON PAM, a set of default passwords are added that are used in the Password Dictionary of the organization.

> ⚠ The Administrator having **Password Dictionary** privileges in **Server's Privileges** will only be able to configure the password dictionary.

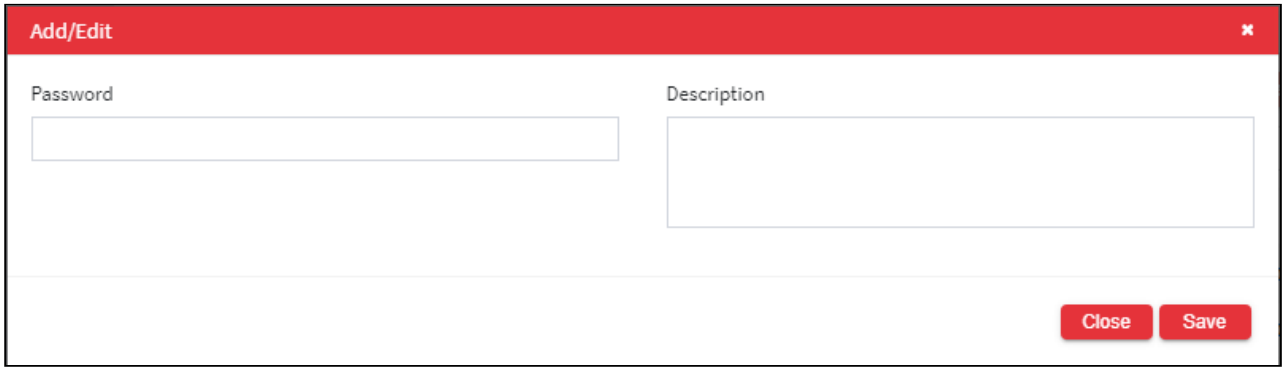
To navigate, use the following path:

Settings → Password → Password Change

1. Select Password Dictionary under Password Change.



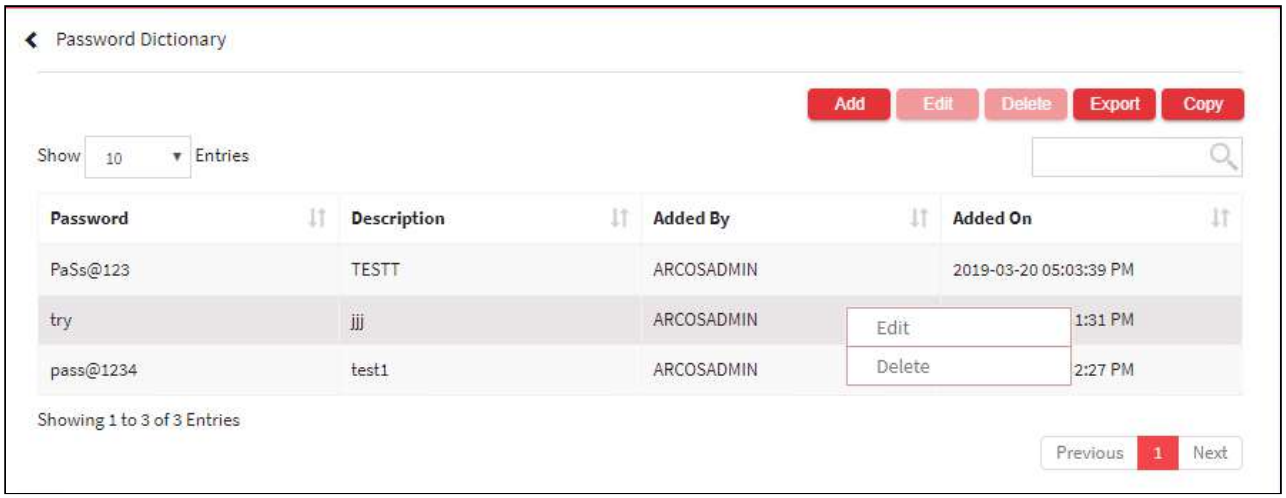
2. Select the Add button to add a new default password.



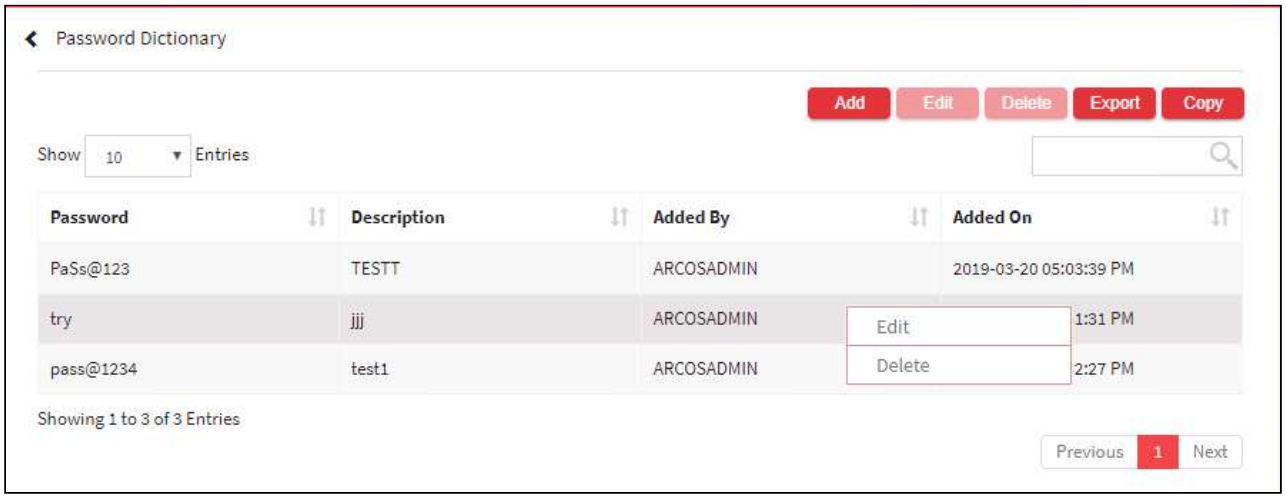
The **Password Dictionary** screen contains the following fields:

Field Name	Description
Description	Enter the description for the password
Password	Enter the default password.

3. Enter the details and click Save button to create a default password.
4. For Editing, the details of the existing password dictionary click on the existing row and select the Edit button at the top and make the required changes. Also, you can right-click on the row and select Edit.



5. For Deleting the existing password dictionary click on the existing row and select the Delete button at the top and make the required changes. Also, you can right-click on the row and select Delete.



6. The Export button will export all the password dictionary details in the form .xlsx format. The Copy button will copy all the details of the table.

13.6.5.2 Password Change Defaults

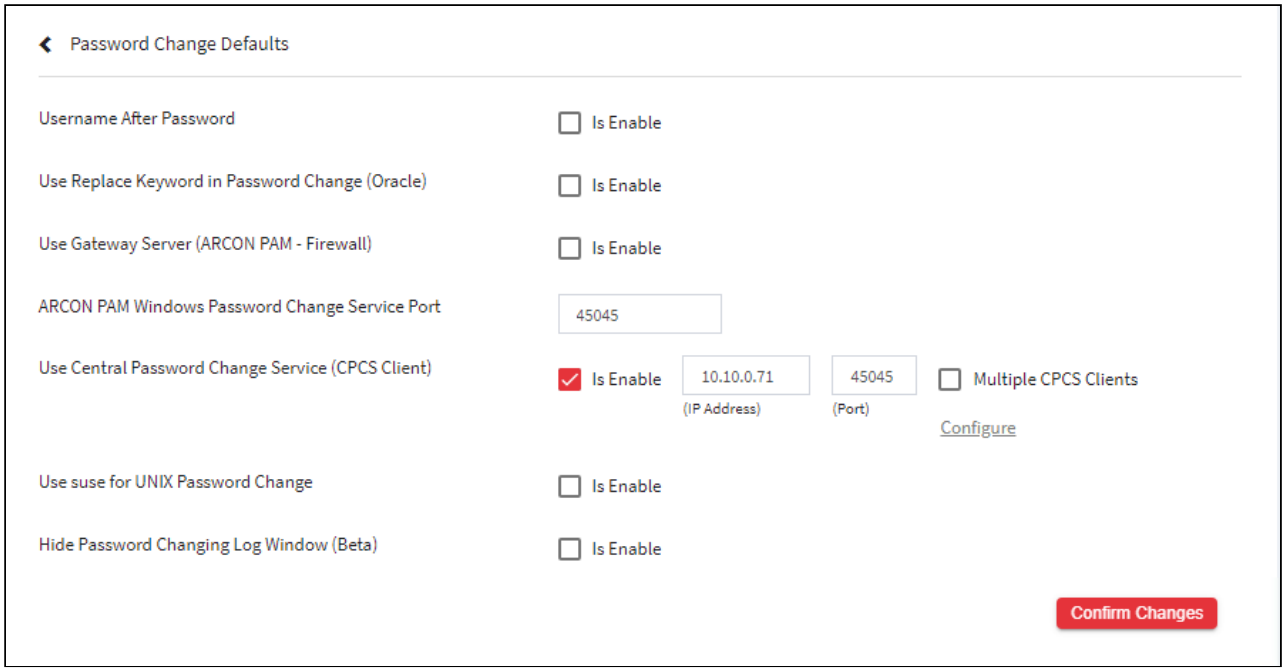
Password Change Defaults is a default setting of password change for different operating systems and service types such as Windows, Linux, and Oracle.

> ⚠ The Administrator having **Password Change Defaults** privileges in Server's Privileges will only be able to configure values for Password Change Defaults.

To navigate, use the following path:

Settings → Password → Password Change

1. Select Password Change Defaults under Password Change.



The **Password Change Defaults** screen contains the following fields:

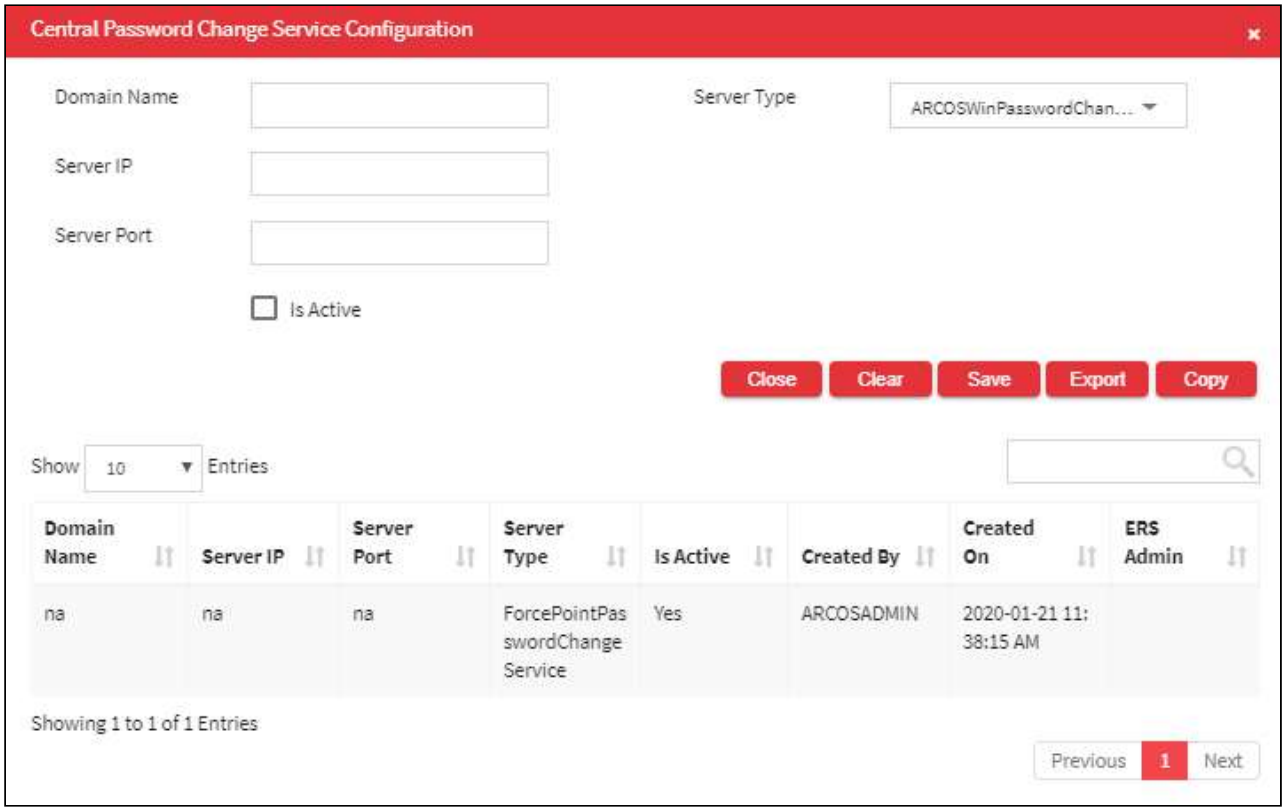
Field Name	Description
Username After Password	Enable User Name After Password, to use username after password while configuring password.
Use Replace Keyword in Password Change (Oracle)	Enable Use Replace keyword in Password Change (Oracle), to use Replace keyword in the Password change process.
Use Gateway Server (ARCON PAM – Firewall)	Enable Use Gateway Server (ARCON PAM Firewall), to route the password change process through the gateway server.
ARCON PAM Windows Password Change Service Port	Enable ARCON PAM Windows Password Change Service Port, when you require port for windows password change process. The default value is 45045.
Use Central Password Change Service (CPCS Client)	Enable the Central Password Change Service (CPCS Client), to initiate the password change process through a centralized domain server (ARCON PAM Server). Note: • **WinPwd** service needs to be installed on the centralized server, to initiate the password change process. • To configure multiple centralized servers, select **Multiple CPCS Clients** checkbox and click on **Configure** link, this will initiate the password change process through multiple domain servers.

Field Name	Description
Use “suse” For UNIX Password Change	Enable “suse” for UNIX Password Change, to change the password through suse putty.
Hide Password Changing Log Window (Beta)	Enable Hide Password Changing Log window (Beta), to disable the password log details window in Password Change Log screen.

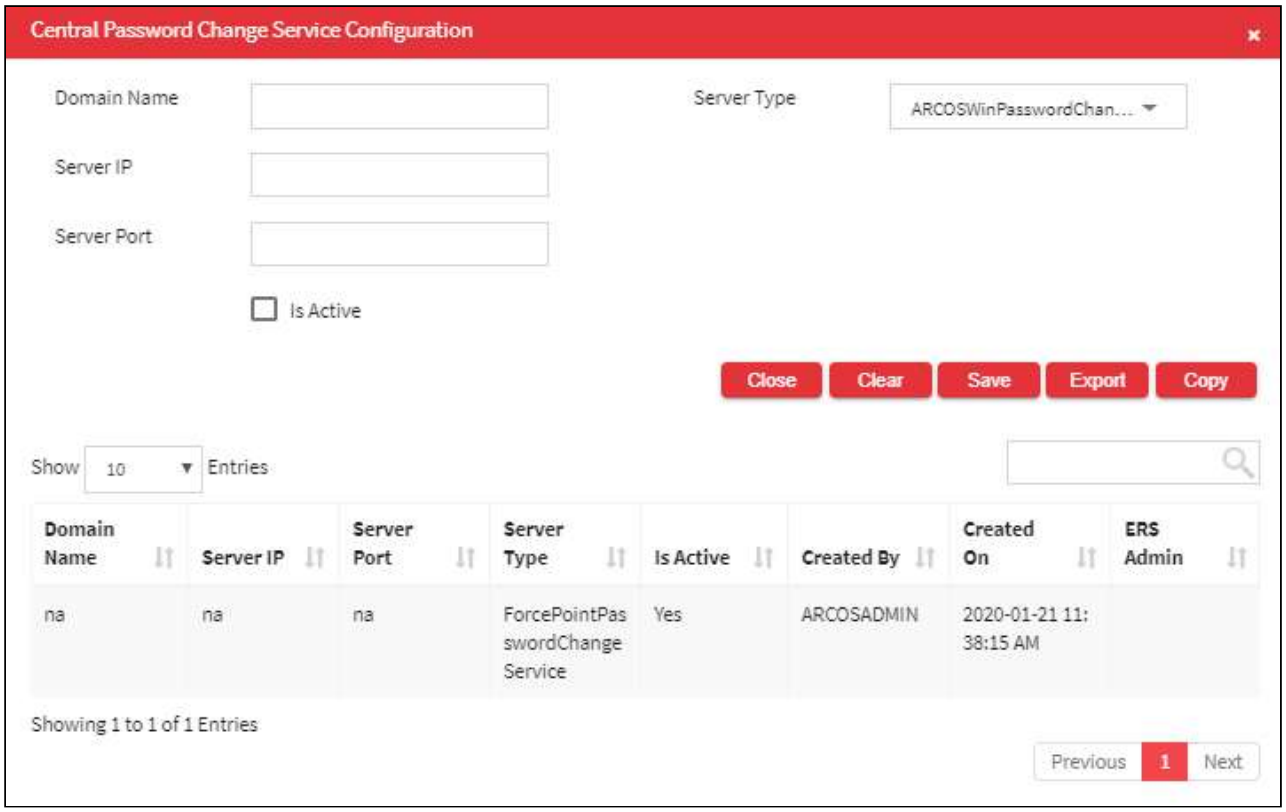
3. Select the details and click **Confirm Changes** to save the configuration details.

Configure Multiple CPCS Clients

1. To configure multiple centralized servers, select **Multiple CPCS Clients** checkbox and click on **Configure** link, this will initiate the password change process through multiple domain servers.



2. Click **Configure**, the following screen is displayed.



The **Central Password Change Service Configuration** screen contains the following fields:

Field Name	Description
Domain Name	Enter Domain Name
Server IP	Enter the IP Address of Server
Server Port	Enter Port Number of Server
Server Type	Select the type of Server. The valid values are: • ARCOSWinPasswordChangeService • CiscoACSPasswordChangeService • CiscoISEPasswordChange Service • ForcePointPasswordChangeService
Is Active	Enable the configuration

Based on the **Server Type**, the details are to be entered:

ARCOSWinPasswordChangeService: Enter Domain Name, IP Address, and Port Number of the server, where ARCOSWinPasswordChangeService (service provided by ARCON Team) is installed.

CiscoACSPasswordChangeService: Enter Domain Name, IP Address, and Port Number of the server, where CiscoACSPasswordChangeService (API provided by Third Party Client) is installed.

CiscoISEPasswordChange Service: Enter Domain Name, IP Address, and Port Number of the server, where CiscoISEPasswordChange Service (API provided by Third Party Client) is installed.

ForcePointPasswordChangeService: Enter Domain Name, IP Address, and Port Number of the server, where ForcePointPasswordChangeService (API provided by Third Party Client) is installed.

3. The Export button will export all the password dictionary details in the form .xlsx format. The Copy button will copy all the details of the table.

13.6.5.3 Custom Command Configuration

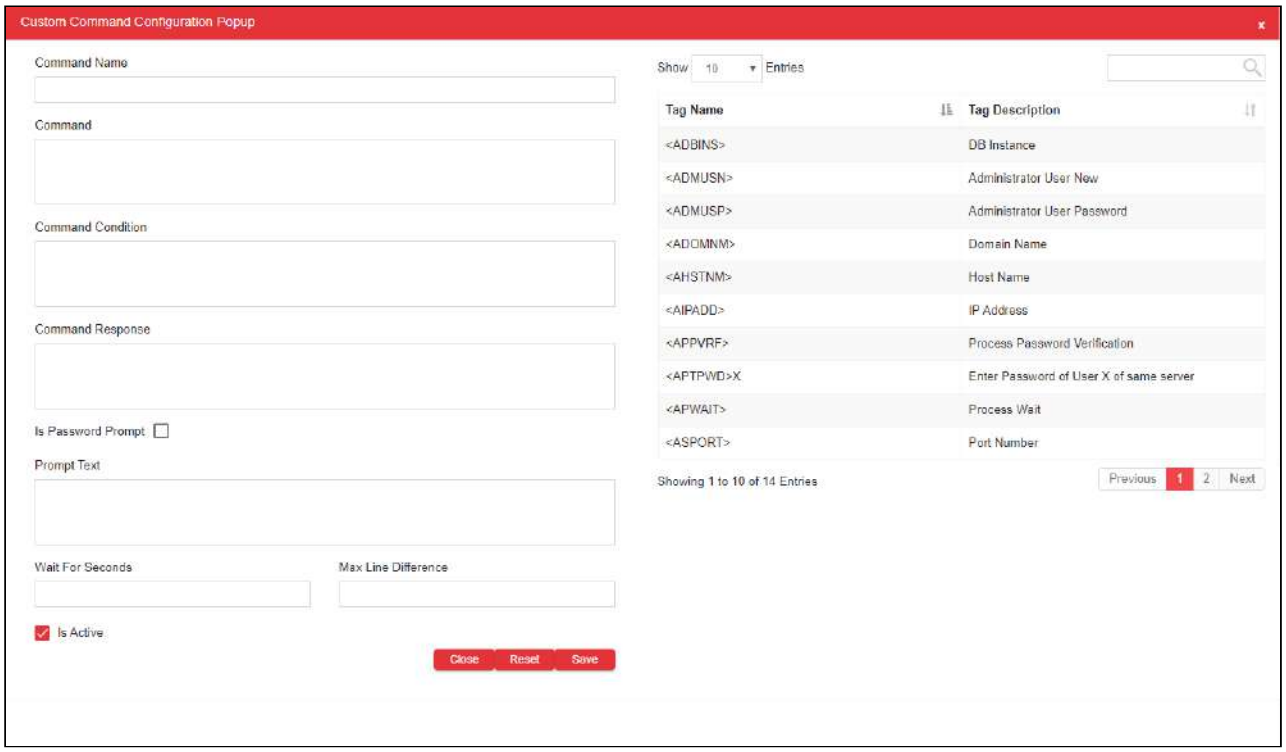
Custom Command Configuration is used to configure commands required for password change. This will remove the dependency on developers to create database script for every password change commands request which is required to change the password of the router, switch, and network devices.

> ⚠ The Administrator having **Custom command Configuration** privileges in Server's Privileges will only be able to configure custom commands.

To navigate, use the following path:

Settings → Password → Password Change

1. Select Custom Command Configuration under Password Change.

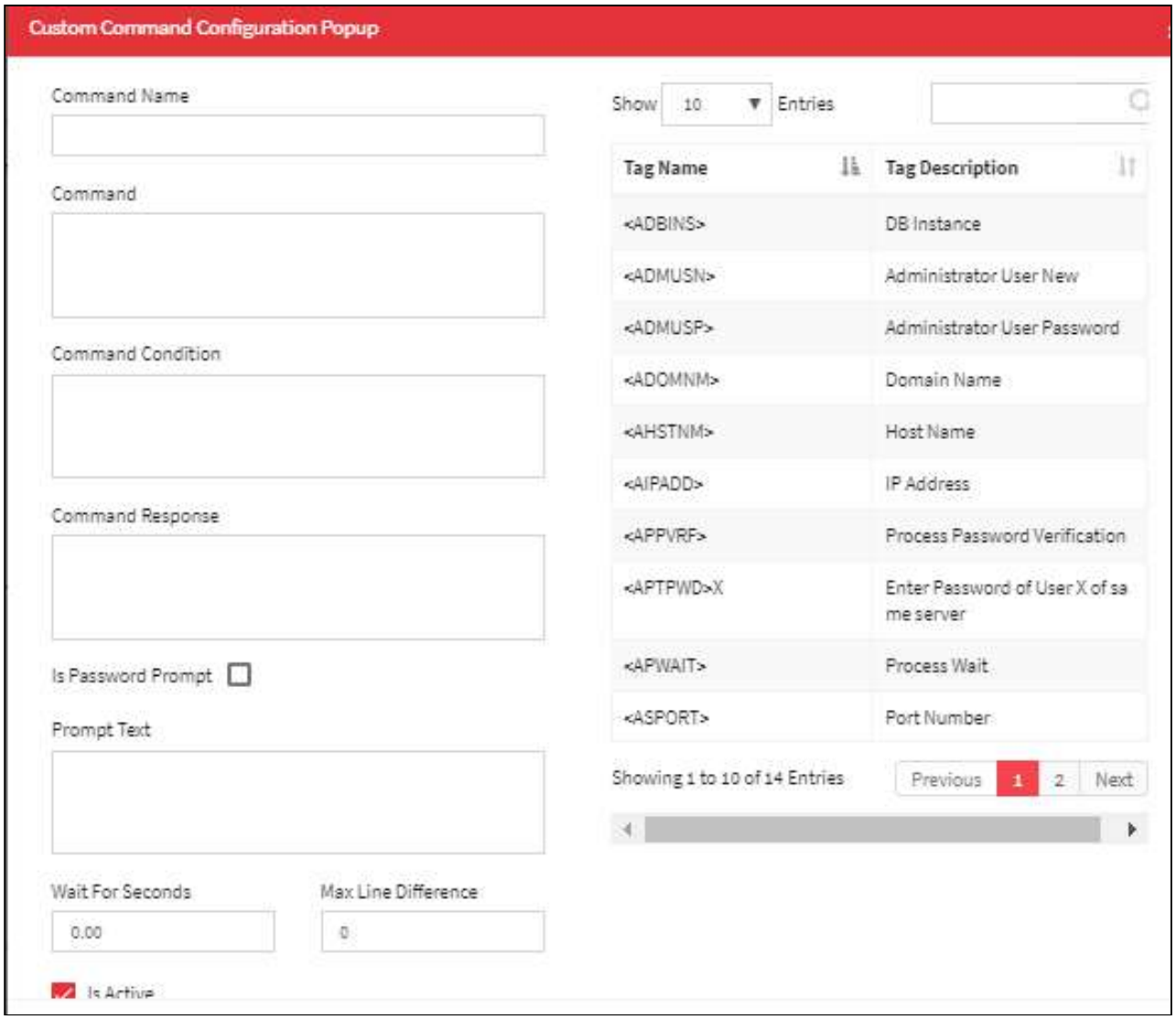


The **Custom Command Configuration popup screen** contains the following fields:

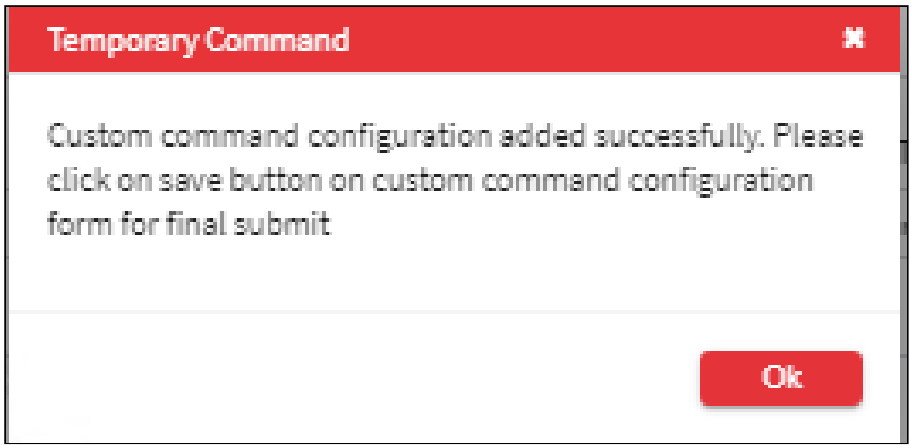
Field Name	Description
Command Name	Enter name for command
Command	Enter Command

Field Name	Description
Command Condition	NA
Command Response	NA
Is Password Prompt	NA
Prompt Test	NA
Wait For Seconds	Duration to execute the command
Is Active	Enable command for execution

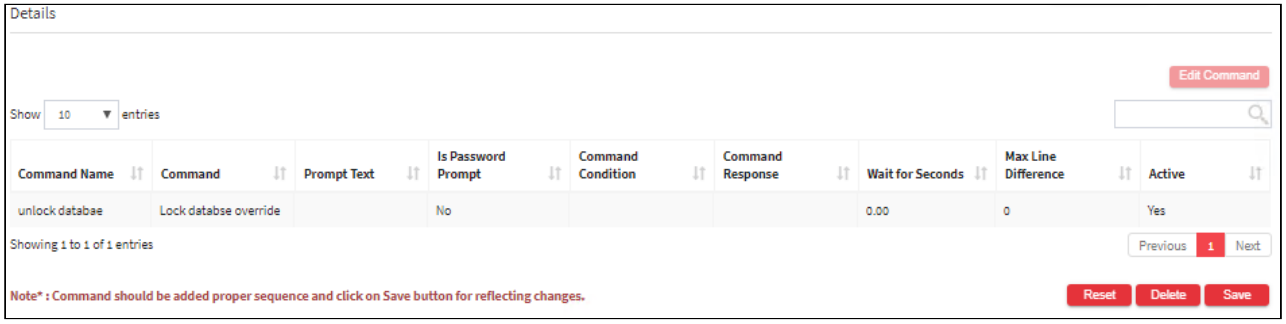
2. Enter the details and click **Add Command**, to add custom commands. The **Custom Command Configuration** popup is displayed.



3. Enter the command details and click **Save**. A window pops up displaying the following message:



4. Click **OK**. The commands are displayed in the **Custom Command Configuration** grid.



- The commands are executed in the order in which they are added for password change. Therefore, commands shall be added in a proper sequence.
- Multiple commands shall be added using **Add Command** button.

5. Click **Save**. A window pops up with the following message: **New Custom Command Configuration added Successfully.**
6. The Export button will export all the custom command configuration details in the form .xlsx format. The Copy button will copy all the details of the table.

13.6.5.4 Password change Configurations

To navigate, use the following path:

Settings → Password → Password Change

Field Name	Description
Default Password Age For New Service	**This configuration sets the default Password Age for a new service created.**
Valid Values	It ranges from 0-100.

Field Name	Description
Password Manager - Group Authorization (Request Email Approval) - Is Enabled	**This configuration enables/disables Password Manager - Group Authorization.**
Disable	If Toggle value is 'Disabled', then it disables Password Manager - Group Authorization.
Enable	If Toggle value is 'Enabled', then it enables Password Manager - Group Authorization.
Change Password - No of User(s) Authentication	**This configuration sets the number of users either 1 or 2 to authenticate before the password of service is changed under Server Manager > Manage > Password Manager.**
Valid Values	It is either 1 or 2.
ARCOSSPCService - Supported Service Types	This configuration triggers the Service Password Change for specified Service Ids.
Valid Values	Enter comma-separated service IDs to start Service Password change. Eg:1,7 In the above example, SPC will trigger password change only for Service Type ID 1 & 7.
Scheduled Password Change - Maximum Failed Attempts	**This configuration will exclude the service from changing the password by SPC Service if the maximum password change failed attempt reached.**
Valid Values	It ranges from 3-9.
Allow Dependency From Across LOB Is Enabled	**This will allow services across LOB to be added for Service Password dependencies.**
Disable	If Toggle value is 'Disabled', then it will not allow Services across LOB to be added for Service Password dependencies.
Enable	If Toggle value is 'Enabled', then it will allow Services across LOB to be added for Service Password dependencies.

Field Name	Description
Only Server Group Admin Can Perform Password Change-Is Enabled	**This configuration enables/disables service password change rights to Server Group Administrators.** **Note:** **To know more about Password Change privileges refer Manually change the password for single or multiple services topics from Password Management section.**
Disable	If Toggle value is 'Disabled', then Administrators having required privileges can change the password of a service.
Enabled	If Toggle value is 'Enabled', then only Server Group Admins can change the password of service manually for single (Manage > User and Services > Manage Services) or multiple services (Manage > Password Manager > Password Change). Administrators should be assigned Change Password privilege under ARCON PAM Group Admin Privileges along with other privileges required for changing the password of service.
SPC Failed Services Interval (Hours)	**The password change can be attempted after the specified hours.**
Valid Values	It ranges from 1-999. The default value is 1.
Service Password change scheduled days	**If the value is set to 5 an alert notification shall be sent 5 days before the service expiry and so on. An alert notification shall be displayed in ACMO notifications before the Service Password change. Users with the Privilege Service Password Change Scheduled will only be able to view this notification.**
Valid Values	It ranges from 5-99.

13.6.6 Reconciliation

To navigate, use the following path:

Settings → Password → Reconciliation

Field Name	Description
Application Password Change (ASM) - Is Enabled	**This configuration enables or disables Application Password Change – HP SiteScope.**
Disable	If Toggle value is 'Disabled', then it disables Application Password Change-HP SiteScope.
Enable	If Toggle value is 'Enabled', then it enables the Application Password Change-HP SiteScope.

Field Name	Description
Password Reconciliation - Is Enabled	**This configuration enables/disables Password Reconciliation.**
Disable	If Toggle value is 'Disabled', then it disables Password Reconciliation.
Enable	If Toggle value is 'Enabled', then it enables Password Reconciliation.
Root account for MSSQL Database Users Passwords Auto Heal	This configuration sets the ROOT accounts for Auto healing Note- For Auto Healing ROOT Account is required.
Valid Values	In this, we add comma separated root usernames. Eg: If we have MSSQL Service as below 1. 10.10.0.180@user1 2. 10.10.0.280@user1 3. 10.10.0.180@user2 As there are 2 Server IPs mentioned above which will have 2 different root account as follows 10.10.0.180@root, 10.10.0.180@admin Then you have to configure as shown below **root,admin** Note: If 2 Servers have the same root username then add username only once. root,root is wrong **only add root**
Root account for Oracle Database Users Passwords Auto Heal	This configuration sets the ROOT accounts for Auto healing Note- For Auto Healing ROOT Account is required.
Valid Values	In this, we add comma separated root usernames. Eg: If we have Oracle Service as below 1. 10.10.0.180@user1 2. 10.10.0.280@user1 3. 10.10.0.180@user2 As there are 2 Server IPs mentioned above which will have 2 different root account as follows 10.10.0.180@root, 10.10.0.180@admin Then you have to configure as shown below **root,admin** Note: If 2 Servers have the same root username then add username only once. root,root is wrong **only add root**

13.6.7 Fail Safe(Envelope)

To navigate, use the following path:

Settings → Password → Fail Safe(Envelope)

Field Name	Description
Pin Mailer - Auto Generate Password For PDF - Is Enabled	**This configuration enables/disables sending passwords to User's Mailbox who has printed Password for service. This password is used to open PDF files generated by the user from Server Manager > Manage > Password Manager > Print Password Envelope > Select Printing Type.**
Disable	If Toggle value is 'Disabled', then the user needs to enter the password manually while generating PDF. User needs to use this password to open the PDF file.
Enable	If Toggle value is 'Enabled', then ARCON PAM will Auto-Generate password to password protect the generated PDF file. The user needs to use this password sent to his Mailbox to open the PDF file.
Generate Password Envelope For New Service - Is Enabled	**This configuration enables/disables the generation of Password Envelope for new Service created.**
Disable	If Toggle value is 'Disabled', it disables the generation of Password Envelope for new service.
Enable	If Toggle value is 'Enabled', it enables the generation of Password Envelope for new service.
Schedule Password Envelope - Is Enabled	**This configuration sets availability of Schedule Password Envelope under Settings → Logs → Scheduler → Schedule Password Envelope**
Disable	If Toggle value is 'Disabled', then this option is not available.
Enable	If Toggle value is 'Enabled', then this option is available.
Password Envelope Protected File	**This configuration enables/disables sending password envelope through email or printing it in .zip format. This file can be decrypted by APEM Tool.** ⚠ • Print password envelope from ARCON PAM Server Manager > Manage > Password Manager > Print Password Envelope > Print Password For APEM Tool. • **Password envelope is sent through email when you schedule it from ARCON PAM Server Manager > Settings > Logs > Scheduler > Schedule Password Envelope.**
Disable	If Toggle value is 'Disabled', the configured password envelope will be sent in .txt format.

Field Name	Description
Enable	If Toggle value is 'Enabled', the configured password envelope will be sent in .zip format.

13.6.8 Debug Mode

To navigate, use the following path:

Settings → Password → Debug Mode

Field Name	Description
ARCOS Password Change Log In Debug Mode - Is Enabled	**This configuration enables/disables ARCOS Password Change Log in debug mode.**
Disable	If Toggle value is 'Disabled', then it disables ARCOS Password Change Log in debug mode.
Enable	If Toggle value is 'Enabled', then it enables ARCOS Password Change Log in debug mode.
ARCOS Password Change Log File Path In Debug Mode	**This configuration is used to specify the file path for the password change log generated in debug mode. Log file generated is saved at that location under the DebugLogs folder.**
Valid Values	The default value is C;\ and can browse till any drive of the client machine.

13.6.9 Miscellaneous

To navigate, use the following path:

Settings → Password → Miscellaneous

Field Name	Description
Restore Password - Is Enabled	**This configuration enables/disables Restoration of the last Password based on the password history.**
Disable	If Toggle value is 'Disabled', then it disables Restoration of last Password based on the password history.
Enable	If Toggle value is 'Enabled', then it enables Restoration of last Password based on the password history.
View History Password - Is Enabled	**This configuration enables/disables display of "History Password" button on View Password window under Server Manager > Manage Services > Select a service > Right click and select View Password.**
Disable	If Toggle value is 'Disabled', it disables this button.

Field Name	Description
Enable	If Toggle value is 'Enabled', it enables this button.
Post Password Change Actions - Is Enabled	**This configuration enables/disables the option of Actions after Password is Changed done for a service.**
Disable	If Toggle value is 'Disabled', then it disables the feature.
Enable	If Toggle value is 'Enabled', then it enables the feature.
Auto Detect Dependent Service With Common Domain Name and User Name (For Update Service Password Only) - Is Enabled	**This configuration will enable or disable, auto detection of depended services based on common Domain Name and User Name of Service and will update the service password after successfully changing the password of same user account.**
Disable	If Toggle value is 'Disabled', then it disables the feature.
Enable	If Toggle value is 'Enabled', then it enables the feature.
ARCOSAPI (Password Retrieval) Requestor Validation - Is Enabled	**This configuration when enabled will validate the user(requestor) for viewing the password of the services.** **The first step will be the registration of the User(Requestor) through ARCON PAM Web API Registration option in Server Manager.** **The second step will be enabling this configuration in order to validate the requestor.** **The final step will be viewing the password of the services that has been registered for the User.**
Disable	If Toggle value is 'Disabled', then it disables the feature.
Enable	If Toggle value is 'Enabled', then it enables the feature.
Bulk Update Server Password	**This configuration enables/disables updating Password of Services under Import > Update Server Connections option.**
Disable	If Toggle value is 'Disabled', then you cannot update Password of Services under **Import**.
Enable	If Toggle value is 'Enabled', then you can update Password of Services under **Import**.

Field Name	Description
Automatically Apply Password Policy When Service is added in Server Group	**This configuration sets whether Password Policy is applied to Services newly mapped in Service Group.** **Password policy is applied to Services of particular Service Type in a Server Group under LOB/Profile - Default Configuration > LOB/Profile – Password Policy.**
Disable	If Toggle value is 'Disabled', the Password Policy is not applied to **Services** newly mapped in **Server Group**.
Enable	If Toggle value is 'Enabled', the Password Policy is applied to **Services** newly mapped in **Server Group**.
Enable Robotic Automation Process	**This configuration enables/disables the Robotic Automation.**
Disable	If Toggle value is 'Disabled', the Robotic Automation will be disabled.
Enable	If Toggle value is 'Enabled', the Robotic Automation will be enabled.
Admin Account for IP Service Type 1 (with Comma)	**This Configuration sets the admin account for IP Service Type 1. Multiple values are separated by commas.**
Valid Values	The valid strings are administrator, admin, root1.
Store passwords in Split Custody	**This Configuration enables/disables the Split Custody option under password options in Manage Services.**
Disable	If Toggle value is 'Disabled', the split custody option will be disabled in Manage Sevices.
Enable	If Toggle value is 'enabled', the split custody option will be enabled in Manage Sevices.

13.7 Alert & Notifications

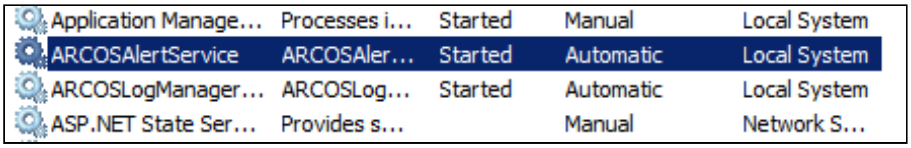
Alert and Notification feature provides you alert notification on email for activities performed in ARCON PAM. It provides alerts for New User Approved, New Service Created, New User Added in group, Command executed on SSH, Invalid Login Attempt, ARCOS Logs, Service Password Manually Changed, Process started on Windows, Process title on Windows, Critical Service(s) accessed in Service Group, Failed SMS OTP Authentication, Successful login and logout alert, Password reset failure, and Failed User Door Access Authentication. The following two modules come under Alert and Notification

- Alert and Notification Configuration
- Alert Email Template
- ARCON PAM Message Board
- Configure

Pre Requisite for Alert & Notification

Alert service should be installed and configured in ARCON PAM to receive alerts on email. Alert Service is installed and configured in ARCON PAM Application or Database Server (EPAM) for sending notifications to users.

Primarily, before starting Alert configuration, you need to install **ARCOS Alert Service** on application or database server.

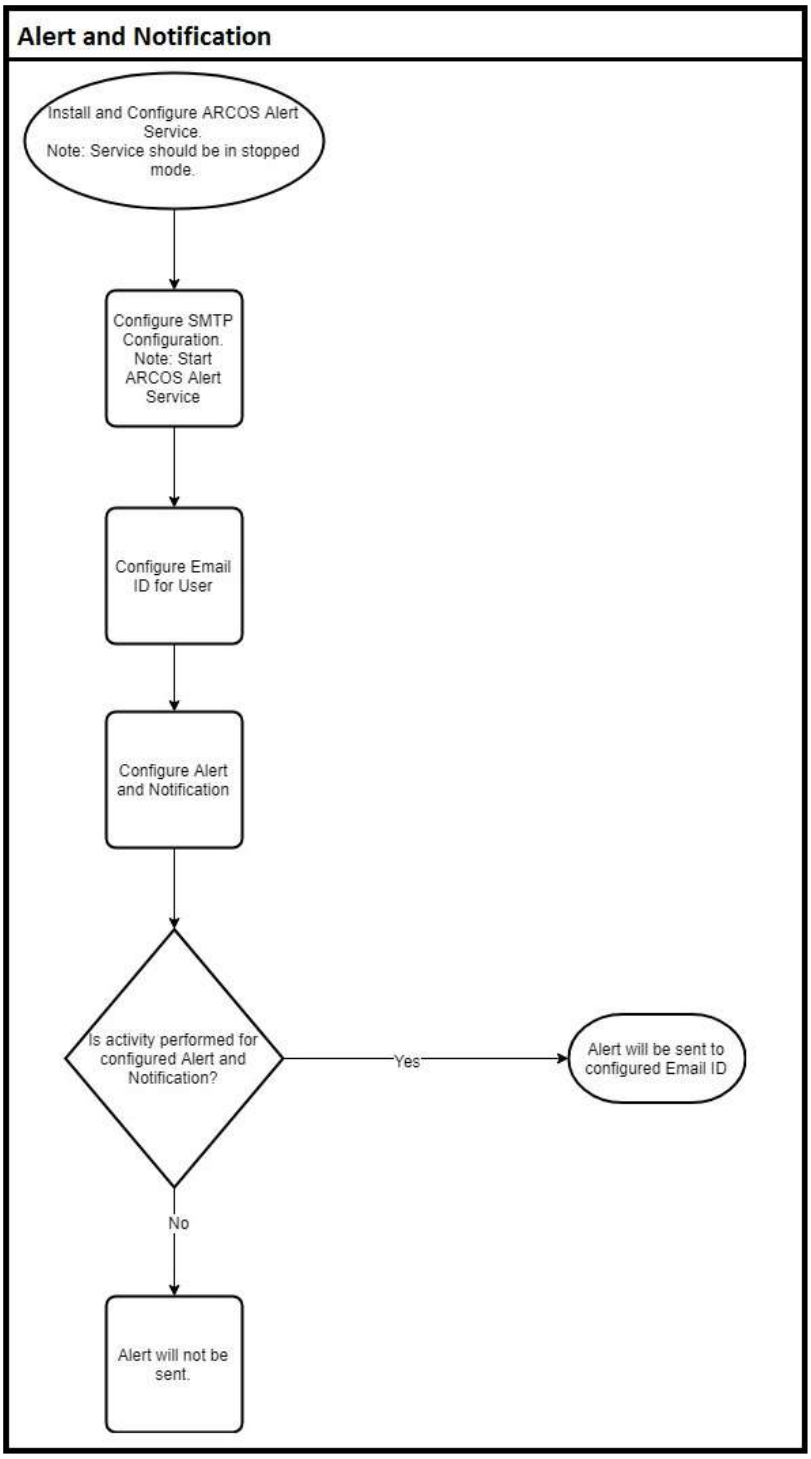


⚠

- The Administrator having **Alert And Notification Configuration** privilege will be able to configure alerts and Users who will receive an alert notification.
- It is mandatory to configure SMTP details in ARCON PAM in order to receive an alert notification.

Process Flow Diagram

Following is the process flow diagram for receiving Alerts and Notification.



13.7.1 Alert & Notification Configuration

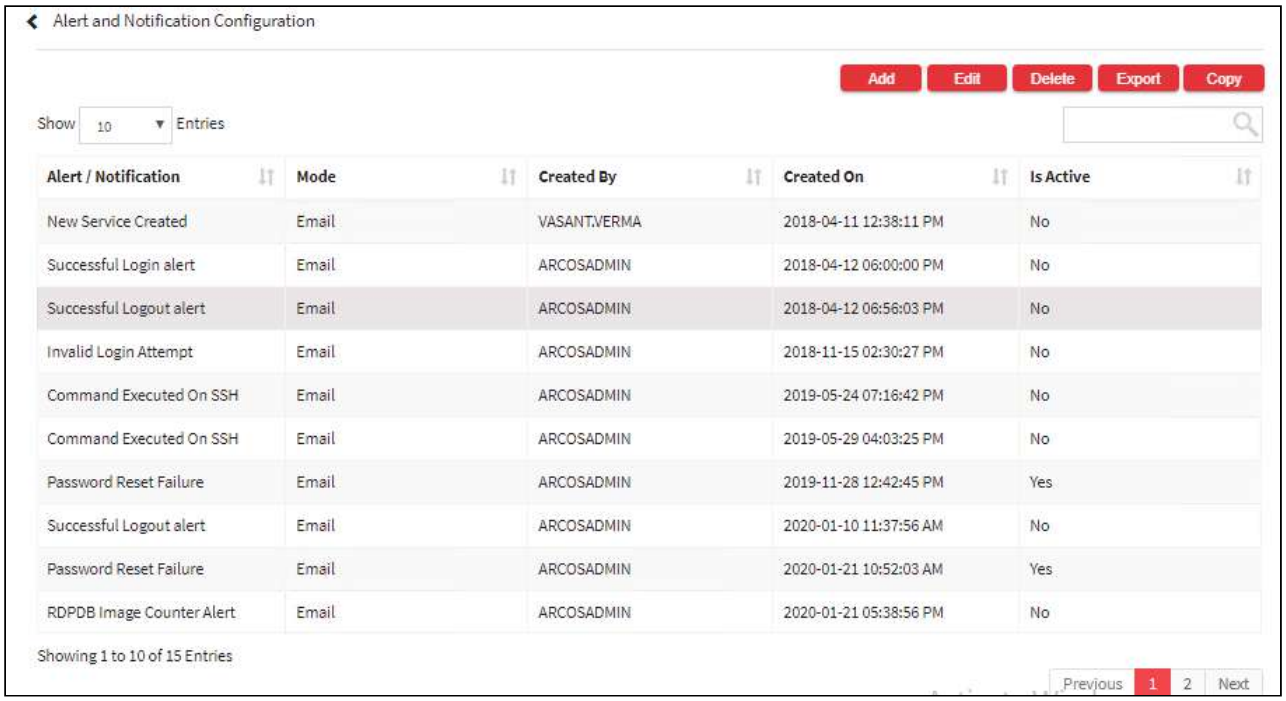
The process to configure a new Alert and Notification Configuration is explained below.

⚠ The Administrator having **Alert and Notification Configuration** privileges in Server's Privileges will only be able to configure Alert and notification.

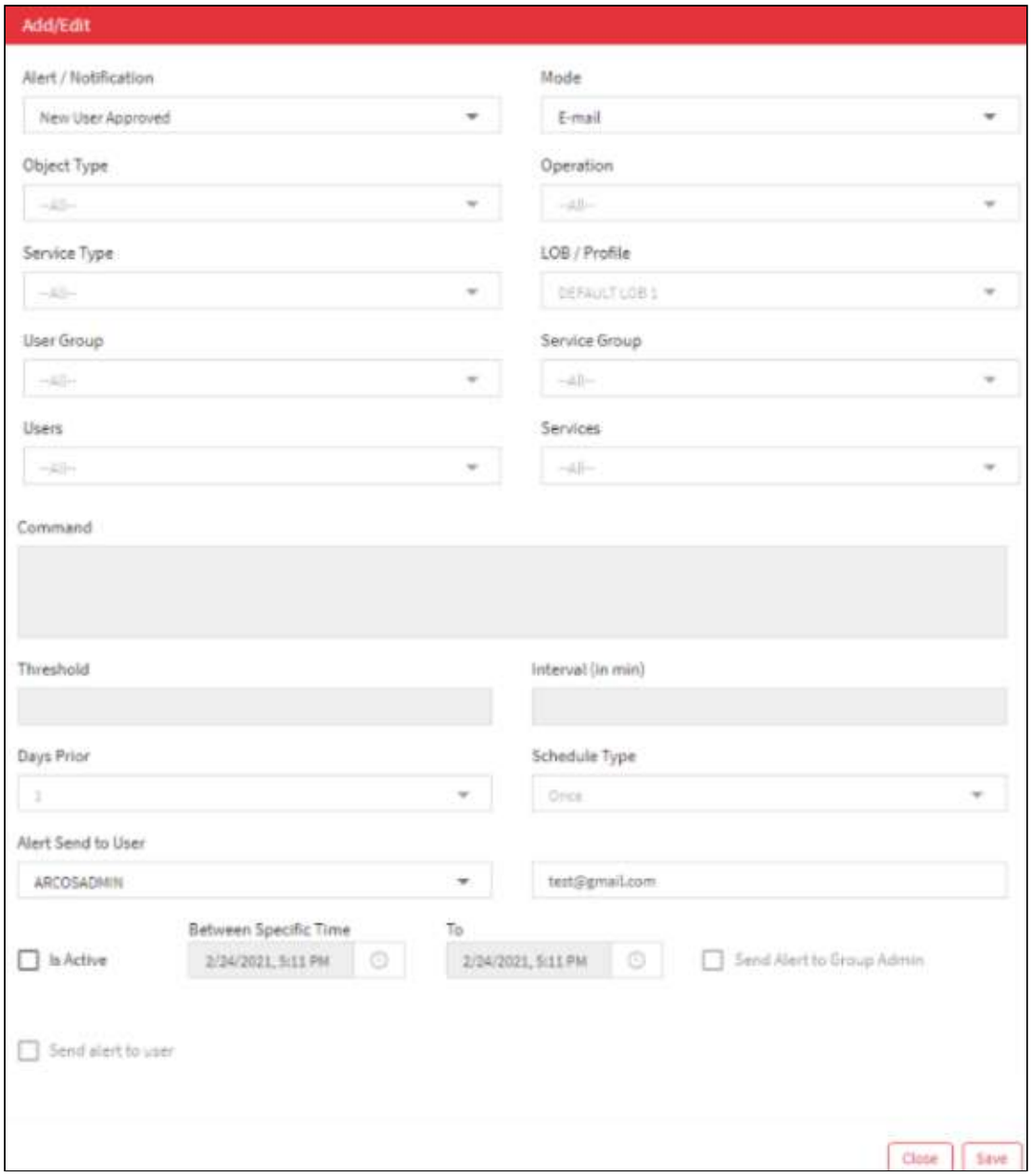
To navigate, use the following path:

Settings → Alert & Notifications

1. Select Alert and Notification configuration.



2. Select the add button to add a new Alert and Notification configuration.



From here, we can configure the following Alerts/Notification-

- **New User Approved:** Notification for the recently approved new user in ARCON PAM.
- **New Service Created:** Notification for every new service created in ARCON PAM.
- **User Added In Group:** Notification for every new user added in the group.
- **Command executed on SSH:** Notification for command executed on SSH-based service (command needs to be defined).
- **Invalid Login Attempt:** Notification for every invalid attempt to login to the application.
- **ARCOS Logs:** Notification for logs viewed.
- **Service Password Manually Changed:** Notification for every service whose password is manually changed.
- **Process Started On Windows:** Notification for the process started on windows.
- **Process Title On Windows:** Notification for process title on windows.

- **Critical Service(s) Accessed In Service Group:** Notification for critical services accessed in the service group.
- **Failed SMS OTP Authentication:** Notification for failed SMS OTP authentication.
- **Failed User Door Access Authentication:** Notification for failed user door access authentication.
- **Successful Login Alert:** Notification for every successful login.
- **Successful logout Alert:** Notification for every successful logout.
- **Password Reset Failure:** Notification for every Password Reset Failure.
- **Critical Command Executed on Server:** Notification for critical commands executed on server.
- **RDPDB Image Counter Alert:** Notification when the RDPDB image count exceeds the threshold value in the specified time interval.
- **Service Revoked from User:** Notification for revoking of service.
- **Service Password Expiry Reminder:** Notification when the service password is going to expire.
- **Services Accessed from User Group:** Notification when any user from that User Group accesses service assigned to them.

The **Alerts and Configuration** screen contains the following fields:

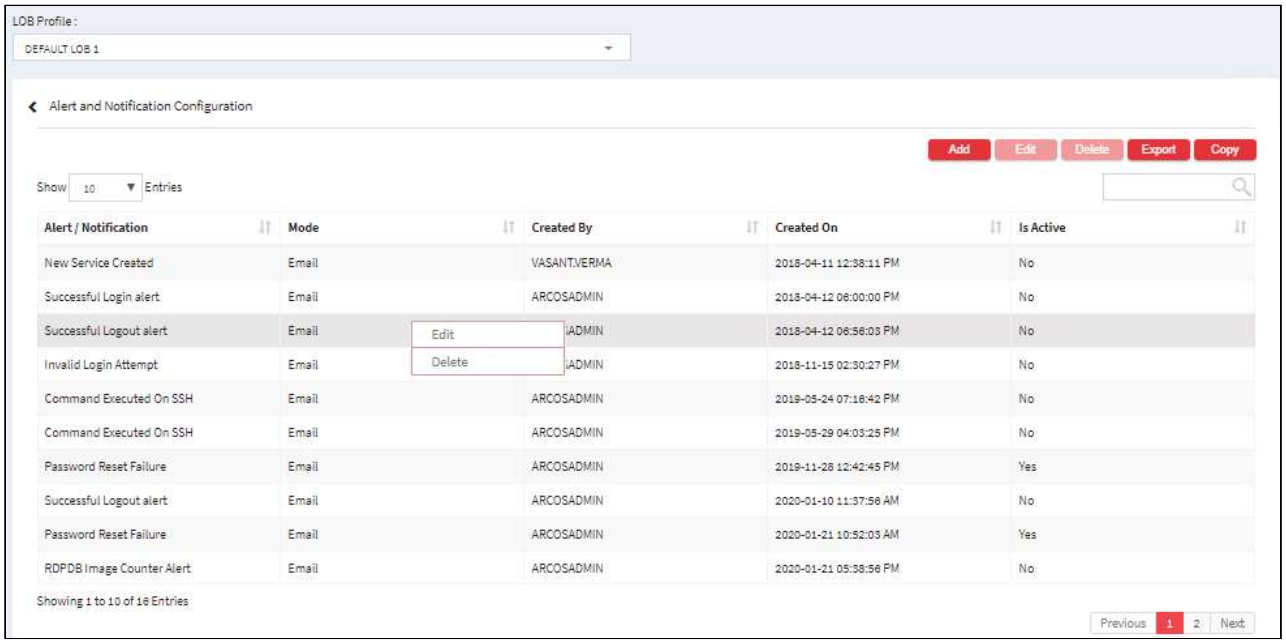
Field Name	Description
Alert/ Notification	Select the type of alert or notification.
Mode	Select the type of mode used for notification i.e. email.
Object Type	Select the type of object. ⚠ This field is enabled if you select the Alert/ Notification as ARCOS Logs.
Operation	Select the type of operation. ⚠ This field is enabled if you select the Alert/ Notification as ARCOS Logs.
Service Type	Select the type of service.
LOB/ Profile	Select the LOB/ profile.
User Group	Select the group name of the user. ⚠ This field is enabled if you select the Alert/ Notification as User Added In Group.
Service Group	Select the service group. ⚠ This field is enabled if you select the Alert/ Notification as Critical Service(s) Accessed In Service Group and Password Reset Failure.
Users	Select the name of the user.
Services	Select the name of the service.

Field Name	Description
Command	Define the command in SSH. ⚠ This field is enabled if you select the Alert/ Notification as Command Executed On SSH, Process Started On Windows, and Process Title On Windows.
Threshold	Set the threshold value for the alert. ⚠ This field is enabled if you select the Alert/ Notification as Command Executed On SSH, Process Started On Windows, and Process Title On Windows.
Interval (in min)	Set the alert interval in minutes.
Days Prior	Set the days prior to which the user will receive the alert ⚠ This field is enabled if you select the Alert/ Notification as Service Password Expiry.
Schedule type	Select the schedule type. ▪ Run Once- If the password of the service is going to expire on 6th of April at 4:00 pm and the Days prior is 5 and scheduler is Run Once, then the alert will be sent once on 1st April at 4:00 pm. ▪ Daily- If the password of the service is going to expire on 6th of April at 4:00 pm and the Days prior is 5 and scheduler is Daily, then the alert will be sent from 1st April at 4:00 pm till the time the password is not changed; keeping a difference of 24 hours. ⚠ This field is enabled if you select the Alert/ Notification as Service Password Expiry.
Alert Send To User	Select the name of the user to whom the alert has to be sent. After selecting the user from the **Alert Send To User** dropdown list, it will display the mail ID of the respective user in the text field beside the **Alert Send To User** dropdown. ⚠ For the users to appear in the Alert Send To User list, their e-mail ID must be configured.
Is Active (checkbox)	To enable the alerts.
Between specific time	Set the time and date between which alert and notification shall be received.

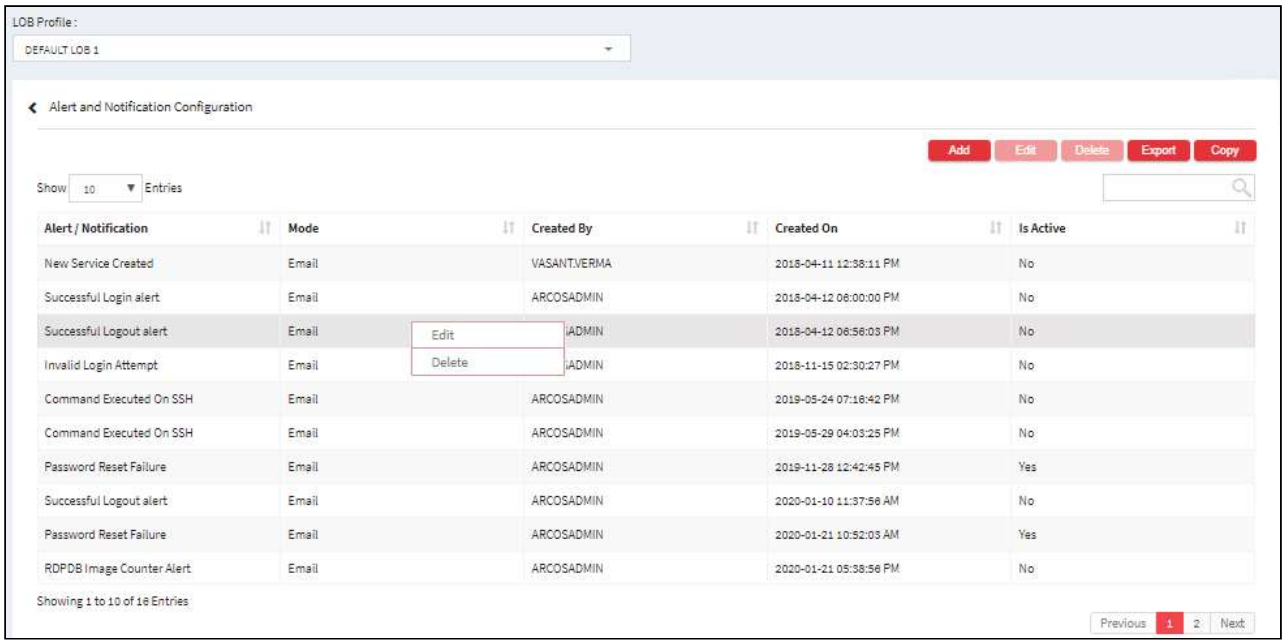
Field Name	Description
Send Alert to Group Admin	To send Alert to the Group Admin. ⚠ This field is enabled if you select the Alert/ Notification as Password Reset Failure, Service Password Expiry Reminder, Critical Service(s) Accessed In Service Group, and Critical Command Executed on Server.

⚠ Start the **ARCOS Alert Service** in **services.msc** for getting e-mail alerts.

3. Click on Save to configure Alert and Notification.
4. For Editing, the details of the existing Alert and Notification configuration click on the existing row and select the Edit button at the top and make the required changes. Also, you can right-click on the row and select Edit.



5. For Deleting the existing Alert and Notification configuration click on the existing row and select the Delete button at the top and make the required changes. Also, you can right-click on the row and select Delete.



6. The Export button will export all the Alert and Notification configuration details in the form .xlsx format. The Copy button will copy all the details of the table.

13.7.2 Alert Email Template

Alert Email Template feature provides users to notify on email for activities performed in ARCON PAM. The email template contains basic details about the requests. This feature has a Business Email ID and Business Mobile Number field in the Manage Users screen. When a new user is created, an email is sent to the user on a configured email ID.

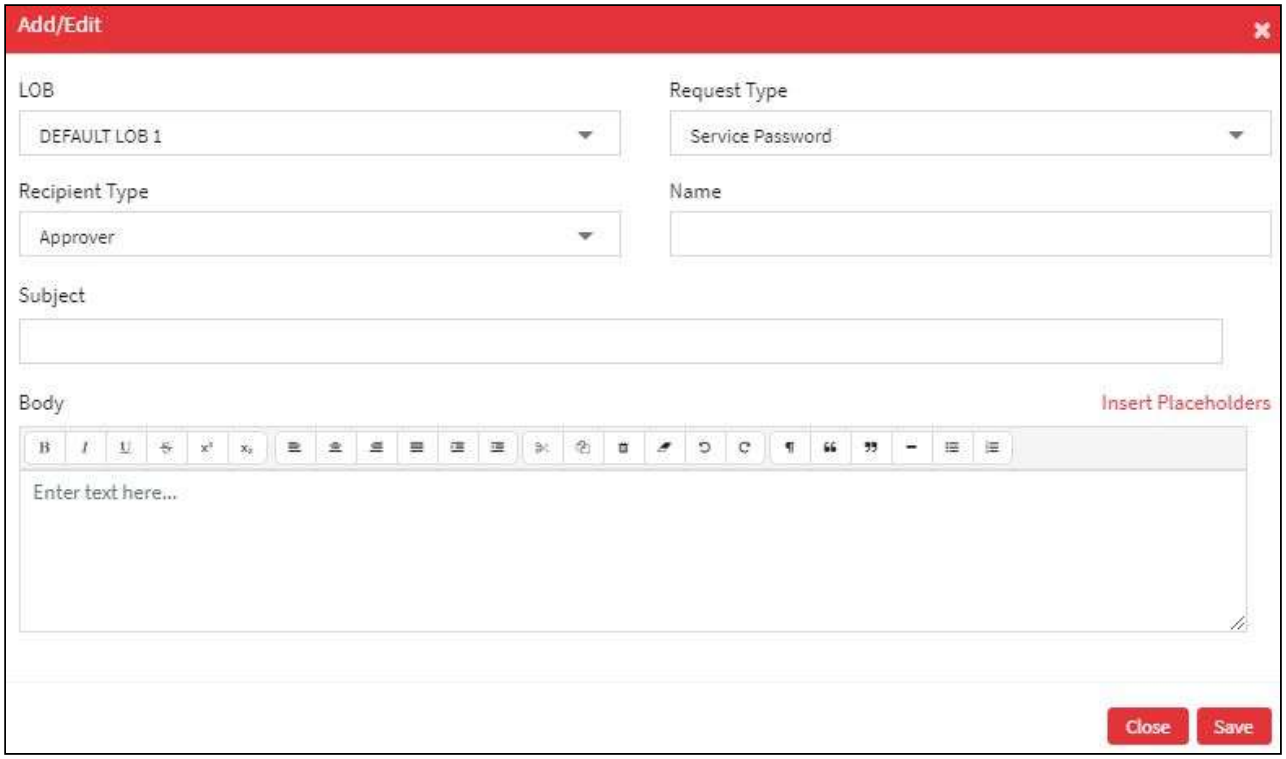
⚠ The Administrator having **Alert Email Template** privileges in Server's Privileges will only be able to do configurations under Alert Email Template.

To navigate, use the following path:

Settings → Alert & Notifications

1. Select **Alert Email Template**.

2. Select the add button to add a new **Alert Email Template**.



The **Alert Email Template** screen contains the following fields:

Field Name	Description
LOB	User has access to make LOB specific templates. Configurations in ARCON PAM that include LOBs will be sent using this template. User can select LOB from the dropdown. User can also select more than one LOB for the template.
Request Type	User has to select a module for which the template is been created. Whenever this module is configured in Server Manager then Email is sent to the respective receiver (Approver/Requestor/End-User/ Executor) User can select below actions under Request Type: ▪ Service Password Request ▪ Service Access ▪ Service Ticket ▪ Critical With Approval

Field Name	Description
Recipient Type	Select Recipient Type: **Approver** The approver is the one who will decide to accept or reject the request based on the information provided in the email. **Requestor** The requestor is one who requests for accessing a particular entity.
Name	Assign a unique name to this template.
Body	The user can enter a customized message. This message will be delivered to the respective receiver. The body contains features to edit and style the message. From left to right the icons specification are as follows: Bold, Italic, Underline, Strike Out Text, Colour Text, Colour Background, Fonts, Text Size, Left Align Right Align, Adjust, Center Align, Bullets, Numbered Bullets, Indent, and Dedent.

3. After updating all the required details click **Save** so that the template created in the **Alert Email Template**.
4. For Editing, the details of the existing **Alert Email Template,** click on the existing row and select the Edit button at the top and make the required changes. Also, you can right-click on the row and select Edit.

5. For Deleting the existing **Alert Email Template,** click on the existing row and select the Delete button at the top and make the required changes. Also, you can right-click on the row and select Delete.

6. The Export button will export all the **Alert Email Template** details in the form .xlsx format. The Copy button will copy all the details of the table.

13.7.3 ARCON PAM Message Board

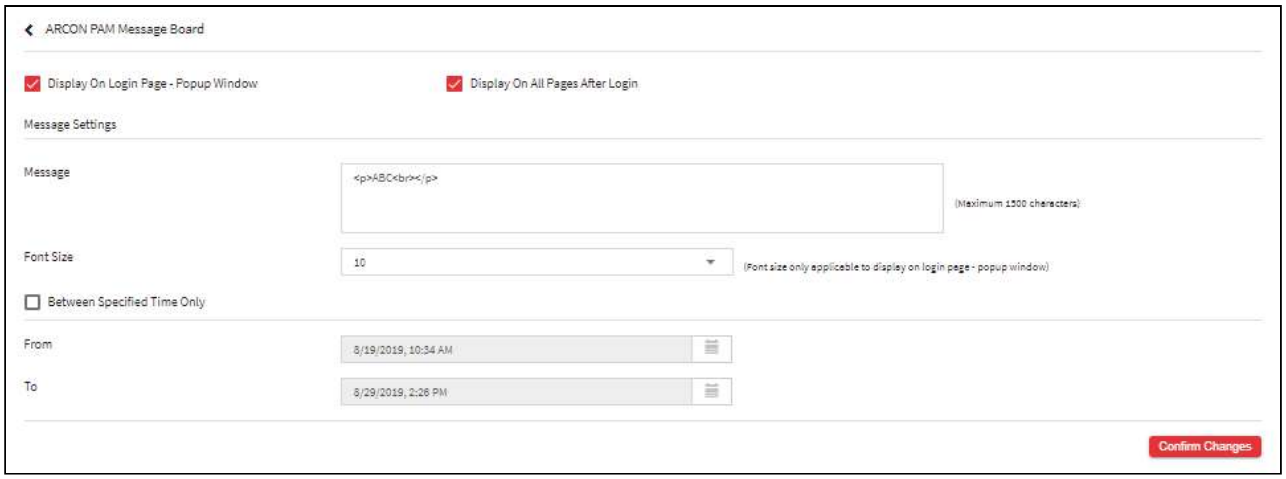
ARCON PAM Message Board allows, to configure messages to be displayed on pages after or before login.

> ⚠ The Administrator having **ARCOS Message Board** privileges in Server's Privileges will only be able to do configuration under the message board.

To navigate, use the following path:

Settings → Alert & Notifications

1. Select ARCON PAM Message Board.

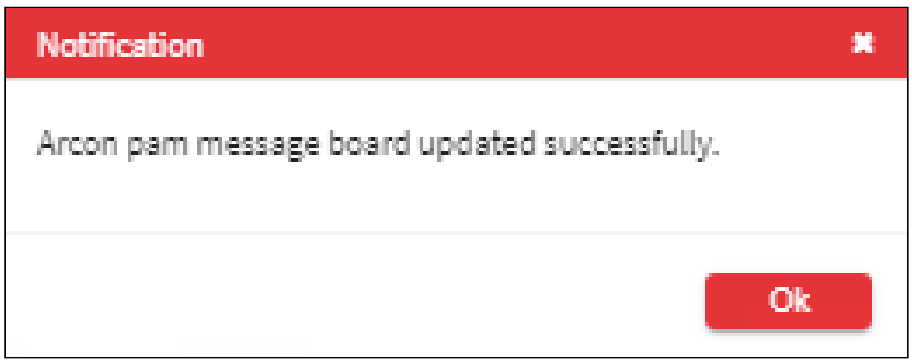


The **ARCON PAM Message Board** screen contains the following fields:

Field Name	Description
Display On Login Page-Popup Window	Enable checkbox to receive the message that will be displayed on Login Page after login.

Display On All Pages After Login	Enable checkbox to receive the message that will be displayed on all pages after login.
Message Settings	
Message	Enter the message in the **Message** text field. ⚠ The maximum text length of ARCON PAM Message Board is 1500 characters.
Font Size	Set the font size of the message.
Between specific time	Set the time and date between which message shall be received.

2. Select the details and click **Confirm Changes** button to configure the details. The following message appears: Arcon pam message board updated successfully.



13.7.4 Configure

The two major configurations required for Alerts and Notifications are

- SMTP Configuration
- SMS gateway

13.7.4.1 SMTP Configuration

The Email Configuration to send Alerts and Notifications to users is done using SMTP Configuration.

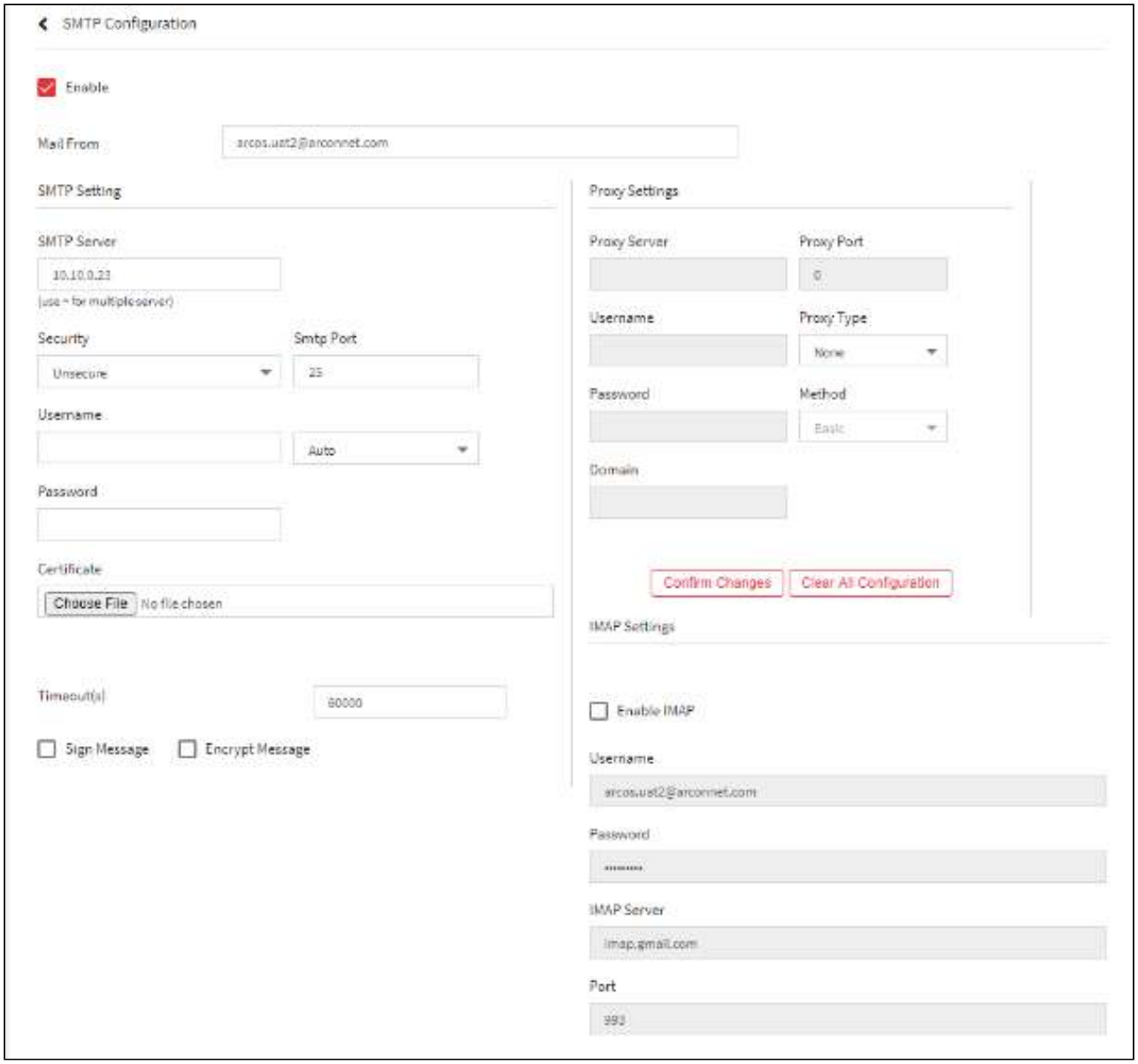
ARCON PAM provides alerts for New User Approved, New Service Created, New User Added in group, Command executed on SSH, Invalid Login Attempt, ARCOS Logs, Service Password Manually Changed, Process started on Windows, Process title on Windows, Critical Service(s) accessed in Service Group, Failed SMS OTP Authentication, and Failed User Door Access Authentication.

⚠
- Start the ARCOS Alert Service in services.msc for getting e-mail alerts.
- The Administrator having **SMS Gateway Configuration** privileges in Server's Privileges will only be able to configure values for SMS Gateway Configuration.

To navigate, use the following path:

Settings → Alert & Notifications → Configure

1. Select SMTP configuration under Configure.



The **SMTP Configuration** screen displays the following fields:

Field Name	Description
Enable (checkbox)	To enable the configuration.
Mail From	Enter the sender's email id.
SMTP Settings	

Smtp Server	Enter server DNS / IP of the SMTP server.
Security	Select the security of the SMTP server.
Smtp Port	Enter the port number of the SMTP server.
Username	Username for the mail ID mentioned in Mail From (if applicable as per SMTP Configuration)
Password	Password for the mail ID mentioned in Mail From (if applicable as per SMTP Configuration)
Certificate	Enter/Select the certificate details.
Timeout(s)	Duration of receiving mail in seconds.
Sign Message	Select to send the message digitally signed, to verify the identity as the sender.
Encrypt Message	Select to send message in an encrypted format.
Proxy Setting:	
Applicable only if proxy server is present	
Proxy Server	Enter the proxy server details.
User Name	Enter the username of the proxy server.
Password	Enter the password of the proxy server.
Domain	Enter the domain of the proxy server.
Proxy Port	Enter the port number of the proxy server.
Proxy Type	Select the type of proxy server.
Method	Select the method based on the selected type in the **Proxy Type** field.
IMAP Setting	
Enable IMAP (checkbox)	To enable the IMAP configuration
Username	Username for the mail ID mentioned in Mail From.
Password	Password for the mail ID mentioned in Mail From.
IMAP Server	Enter the IMAP server details
Port	Enter the port number of the IMAP server

2. Select the details and click **Confirm Changes** button. The **Clear All Configuration** button allows to reset the details i.e. clear the data from the fields.

13.7.4.2 SMS Gateway Configuration

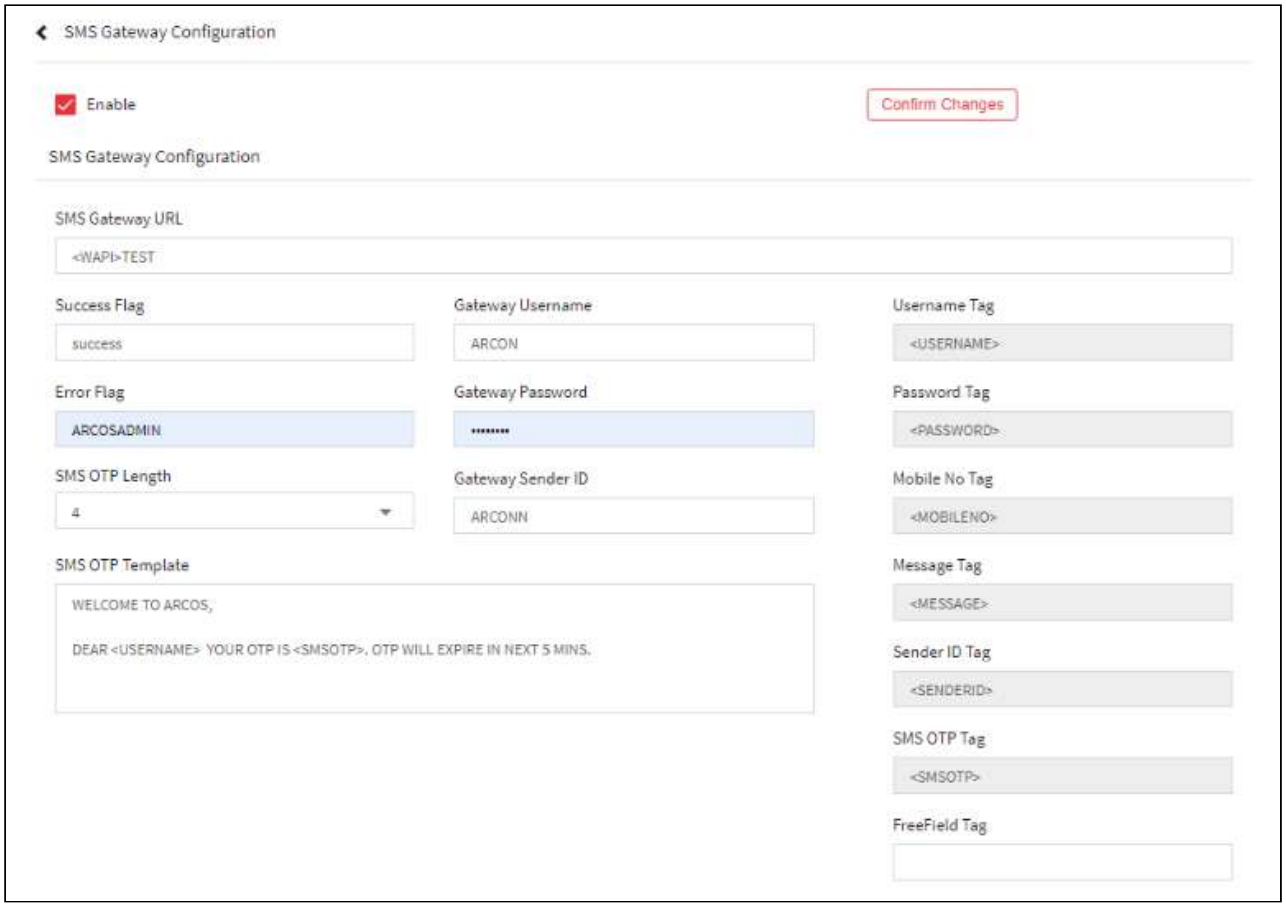
ARCON SMS gateway server details are used when the notification is sent to approvers for service, ticket, and password requests. ARCON PAM provides Dual Factor Authentication when the user logs in Client Manager. SMS OTP is one of the methods wherein User receives OTP on the registered mobile number. OTP is the second factor of authentication.

⚠ The Administrator having **SMS Gateway Configuration** privileges in Server's Privileges will only be able to configure values for SMS Gateway Configuration.

The SMS gateway configuration allows receiving alerts or notification messages via SMS on the configured Mobile devices in the following way.
To navigate, use the following path:

Settings → Alert & Notifications → Configure

1. Select SMS gateway configuration under Configure.



The **SMS Gateway Configuration** screen contains the following fields:

Field Name	Description
Enable (checkbox)	To enable the configuration.
SMS Gateway URL	Define the main URL for SMS gateway.
Success Flag	Defines the success flag. It can either be 1, 0, or success depending on the gateway. It can also be different characters or variables.
Error Flag	Defines the error flag. It can either be Error or Invalid Entry. This field is variable depending on the gateway.

Field Name	Description
SMS OTP Length	Set the Length of the OTP. The valid values are from 2 to 9.
Gateway Username	Enter the gateway Username
Gateway Password	Enter the gateway Password
Gateway Sender ID	Enter the Gateway Sender ID
SMS OTP Template	Set the template message to be displayed.
Username Tag	The Tag used in the URL will be replaced by the Gateway's Username, which is configured under 'SMS Gateway Configuration'.
Password Tag	The Tag used in the URL will be replaced by the Gateway's Password, which is configured under 'SMS Gateway Configuration'.
Mobile No Tag	The Tag used in the URL will be replaced by the User's Mobile Number, which is configured in User's Security Setting under 'Manage User'.
Message Tag	The Tag used in the URL will be replaced by the SMS OTP Template, which is configured in 'SMS Gateway Configuration'.
Sender ID Tag	The Tag used in the URL will be replaced by the Gateway's Sender ID, which is configured in 'SMS Gateway Configuration'.
SMS OTP Tag	Used in configuring OTP Message under SMS OTP Template, which will be replaced by the randomly generated OTP.

3. Select the details and Click **Confirm Changes** button to configure the settings.

13.7.4.3 Configurations

To navigate, use the following path:

Settings → Alert & Notifications → Configure

Field Name	Description
SMS and Email OTP Logout Attempt	**SMS and Email OTP Logout Attempt**
Valid Values	It ranges from 3-100.
Alert Service Email/SMS Failed Attempts	**This configuration sets the number of times Alert Service shall attempt to send an alert on Email or SMS.**
Valid Values	It ranges from 1-10.
Send Password of ARCOSAUTH Users in Email Notification	**This configuration will send the URL, password, and other guidelines for the first-time login users in ARCOSAUTH Domain over an email.**

Field Name	Description
Disable	If the Toggle value is 'Disabled', then the first time ARCOSAUTH user will not receive an email with URL, Password, and guidelines.
Enable	If the Toggle value is 'Enabled', then then the first time ARCOSAUTH user will receive an email with URL, Password, and guidelines.

13.8 Workflow

Workflow is an approval process where one or more Admins will approve the changes that have been made in ARCON PAM. The transactions between users, services, user groups, and service groups can undergo approval before any action in ARCON PAM. For this, you should configure workflow in **Workflow Approval Matrix**. The request raised by User for service access, service password, ticket, and executing a critical command on Server can undergo an approval process. For this, you need to **Raise Request** and configure workflow in the User Request Approval Workflow. The following two sections come under the workflow module

- Configure Holidays
- Raise Request
- Admin Activities

13.8.1 Configure Holiday

This section monitors the performance of ARCON PAM servers. Using this feature an organization can define a list of Holidays by selecting Month, Date, and describing the holiday by adding Name of the Holiday.

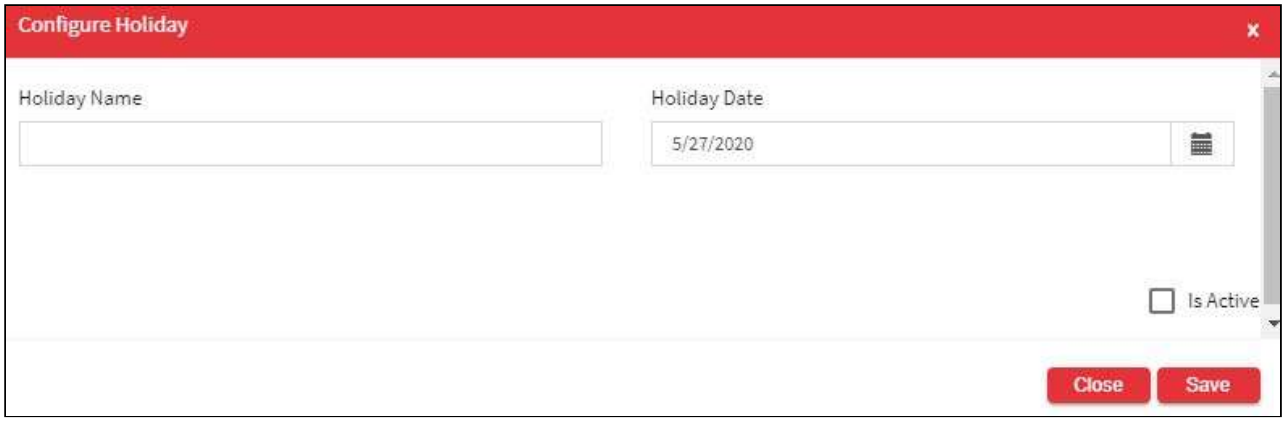
⚠ The Administrator having **Configure Holiday** privilege in Server's Privileges will only be able to do configurations under Configure holiday screen.

To navigate, use the following path:

Settings → Workflow

1. Select Configure Holiday.

2. Select the add button to add a new **Configure Holiday**.



3. The **Configure Holiday** screen contains the following fields:

Field Name	Description
Holiday Name	Specify the Holiday Name.
Holiday Date	Select the Holiday date.
Is Active	If selected, then the command profile will be applicable only between the time range. If left unselected, then the commands profile will be applicable for the complete day. ⚠ Holidays will have a validity of one year and need to be defined manually each year. For Example: **Scenario 1:** The defined holidays will only by-pass the time and not the days (Monday to Friday) which are configured. So, if a public holiday falls on a Saturday or Sunday, the end user will have full access as stated in Scenario 2. **Scenario 2:** This configuration has to be set from 12:00 AM to 5:00 PM in order to restrict commands. So starting 5:00 PM and the next day, being a working day, restrictions will start from 8:00 AM as defined in Scenario 1.

4. Enter the details and click **Save,** new holiday Is created in **Configure Holiday**.
5. For Editing, the details of the existing **Configure Holiday,** click on the existing row and select the Edit button at the top and make the required changes. Also, you can right-click on the row and select Edit.

6. For Deleting the existing **Configure Holiday,** click on the existing row and select the Delete button at the top and make the required changes. Also, you can right-click on the row and select Delete.

7. The Export button will export all the **Configure Holiday** details in the form .xlsx format. The Copy button will copy all the details of the table.

13.8.2 Raise Request

To navigate, use the following path:

Settings → Workflow → Raise Request

Field Name	Description
ARCOS Workflow - Is Enabled	**This configuration sets the availability of Workflow Approval Matrix under ACMO > Settings > Workflow.**
Disable	If the Toggle value is 'Disabled', then this option will not be available for configuration.
Enable	If the Toggle value is 'Enabled', then this option will be available for workflow configuration.
Reference Details Mandate while raising Service Access Request- Is Enable	**This configuration helps in setting the reference parameters that will be visible on ACMO → Raise Request → Service Access Request screen.**
Disable	If the Toggle value is 'Disabled', then Reference type and Reference Detail fields will not be visible in Settings.
Enable	If the Toggle value is 'Enabled', then the User can set Reference type and Reference Details fields in Settings which will reflect on ACMO → Raise Request → Service Access Request screen.

13.8.2.1 User Request Approval Workflow

This section helps you to configure approval levels for the request raised by the User for service access, service password, service ticket, and critical command. The request raised by Users from Client Manager shall be sent for

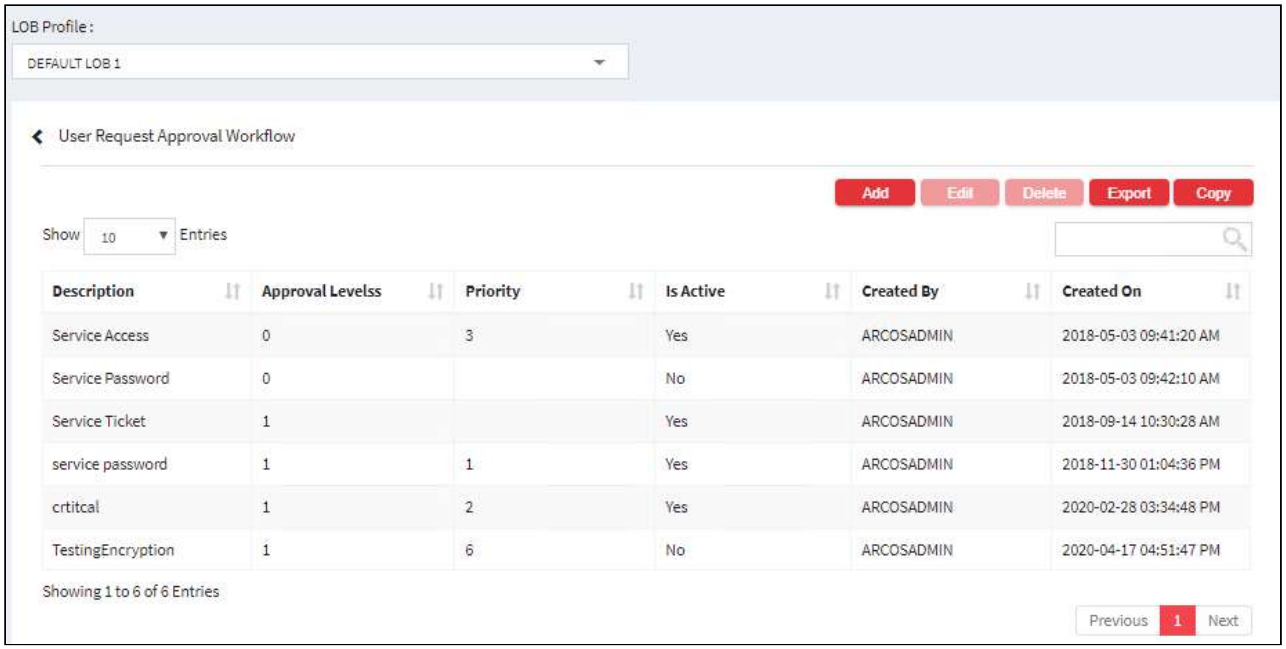
approval based on the approval levels configured in the workflow matrix. Therefore, it provides a definite audit trail and proper flow of events, which are required to be monitored closely.

⚠ The Administrator having **User Request Approval Workflow** privileges in Server's Privileges will only be able to configure user request approval Workflow

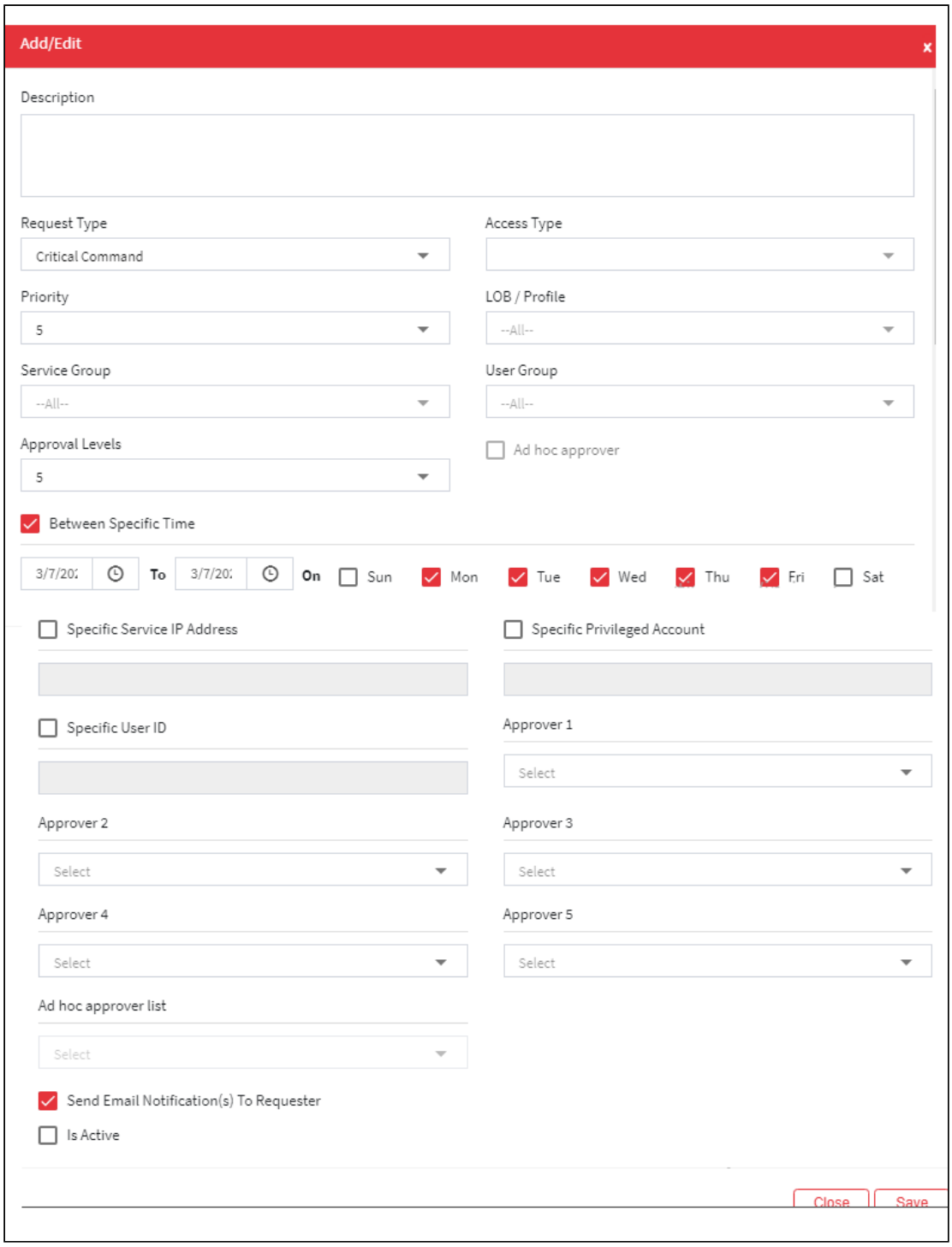
To navigate, use the following path:

Settings → Workflow → Raise Request

1. Select User Request Approval workflow under Raise Request.



2. Select the Add button to raise a new request.



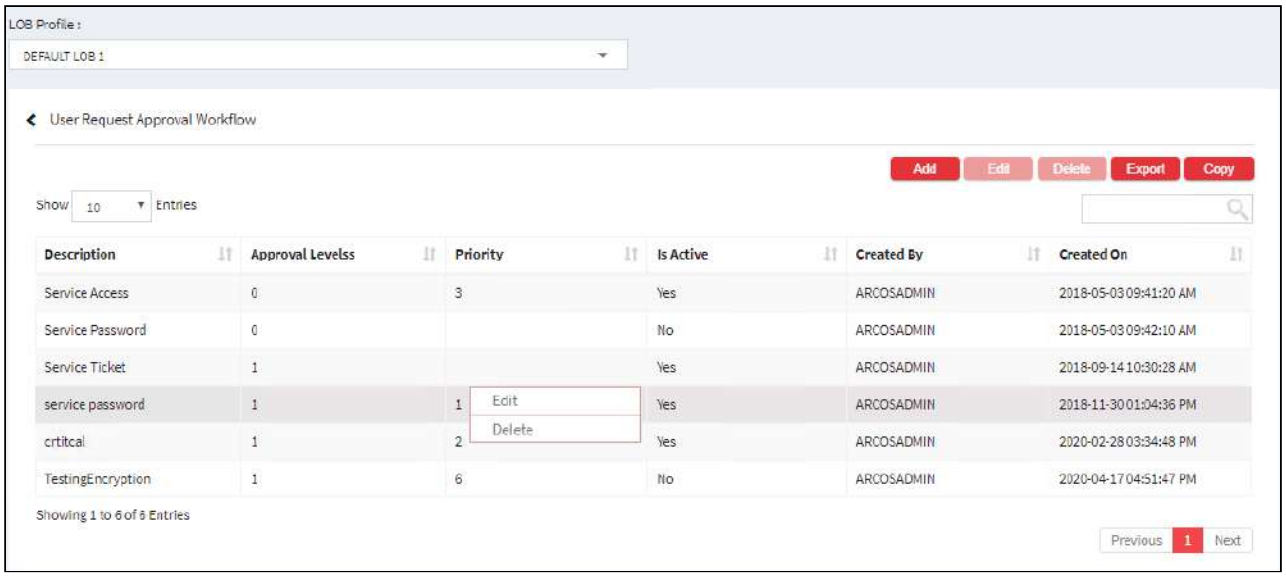
The **User Request Approval workflow** contains the following fields:

Field Name	Description
Description	Specify the name or details of the approval matrix to be created.

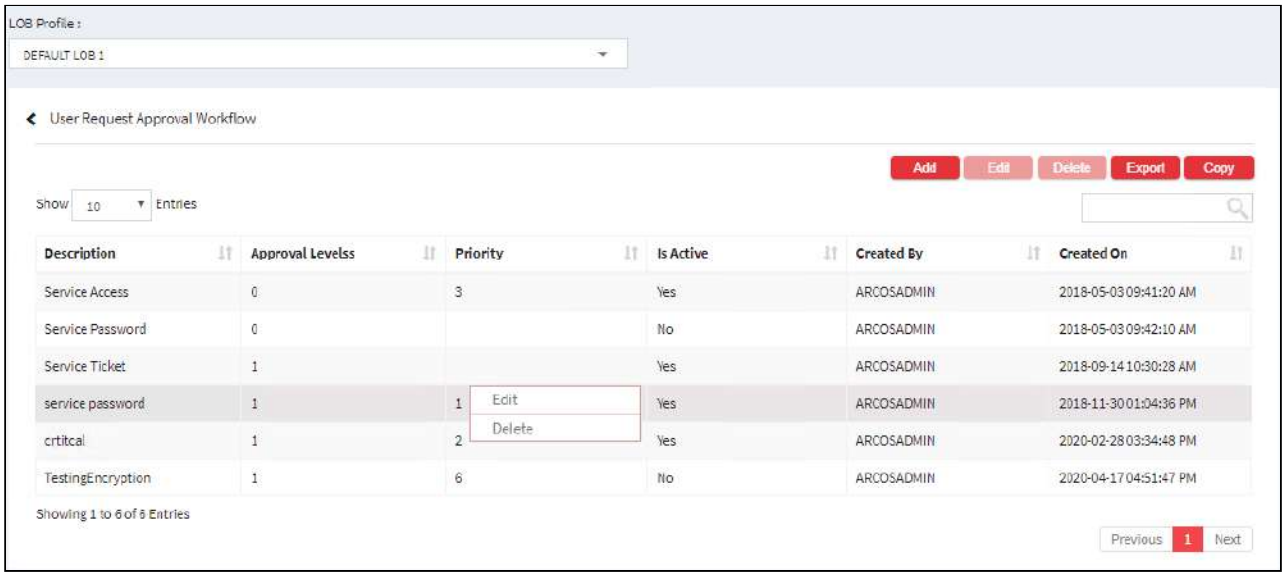
Field Name	Description
Request type	Select the type of request to be raised ▪ **Service Password:**It raises a request to view the password of a particular service. ▪ **Service Access:** It raises a request to access a particular service. ▪ **Service Ticket:** It raises a ticket request which states the requested services. ▪ **Critical Command:** It raises a request to fire a critical command. ▪ **Script Execution:** It raises a request to execute a script.
Access type	Select the Access type ▪ **Permanent:**It raises Permanent and full access request of the service to the user. ▪ **One time:** It raises One time request of the service to the user. ▪ **Time Based:**It raises requests based on a specified duration of the time by the user.
Priority	Configure **Priority Levels** for Workflow. Based on the priority configured, the Workflow would be applied. **For Example**, if User 1 raises a Service Access Request, now User 1 belongs to both Group 1 and Group 2, mapped to Workflow 1 and Workflow 2 respectively. However, since the priority that is set for Workflow 2 is higher, the highest priority level workflow would be applied.
LOB/ Profile	Select the LOB/Profile. ⚠ If LOB Wise Workflow Configuration - Is Enabledconfiguration is enabled in Settings, then only LOB/Profile will be displayed in LOB/Profile drop-down list. Whereas, if it is disabled, then the All LOB option will be displayed along with LOBs in the drop-down list.
Service Group	Select the Service group from the drop-down.
User Group	Select the user group from the drop-down.
Approval Levels	Select the number of approval levels to approve the request. ⚠ ▪ It can be set to a maximum of 5 users and a minimum of 0 users. ▪ 0 Approval Level can be configured only for Service Password and Service Access Requests. If the Approval level is configured to 0, then it is mandatory to specify an email Id for notification. For any service password and service access request by User, a service details notification will be sent to the configured email id. ◦ Enter the email ID in Notify Email Only for 0 Approval Level text box.

Field Name	Description
Ad hoc approver	If the Request type is **Service access** and the approval level is **more than 0**, ad hoc approver checkbox will be visible. Clicking this checkbox ad hoc approval list is populated at the bottom where the admin can set Ad hoc approvers. The purpose of this configuration is that approvers can simply **forward** the service access request if they are not sure of approving or rejecting the request on ACMO. ⓘ The Ad hoc approvers which are configured here by the Admin will be visible under ACMO to the approvers when they select the Forward option.
Between Specific time	Select the specific time with hours and days, to enable the workflow matrix between the selected time.
Specific Service IP address	Select and specify the service IP address to apply the created matrix to the specific IP only. ⚠ The IP refers to the destination server/service accessed via ARCON PAM.
Specific Privileged Account	Select and specify the service IP address to apply the created matrix to the specific IP only. ⚠ The account refers to the destination server user account accessed via ARCON PAM.
Specific User ID	Select and specify the user ID to apply the created matrix to the specific user ID only. ⚠ The user ID refers to the user's login in ARCON PAM.
Approvers	Search and select the approvers for the workflow.
Send SMS notification to Approver	Enabling the checkbox SMS is sent to the approver for the request.
Show password on request window	Enable the checkbox to see the password on the request window
Send Email Notification(s) to Requester	Enable the checkbox to get an email notification for the raised request. ⚠ For the mails, SMTP configuration under ARCON PAM has to be configured prior and ARCOS Alert Service has to be running on ARCON PAM server.
Is Active	Enable the matrix.

3. Click on Save to save all the changes and the user request approval workflow has been set.
4. For Editing, the details of the existing approval workflow click on the existing row and select the Edit button at the top and make the required changes. Also, you can right-click on the row and select Edit.



5. For Deleting the existing request approval workflow click on the existing row and select the Delete button at the top and make the required changes. Also, you can right-click on the row and select Delete.



6. The Export button will export all the user request approval workflow details in the form .xlsx format. The Copy button will copy all the details of the table.

13.8.3 Admin Activies

13.8.3.1 Workflow Approval Matrix

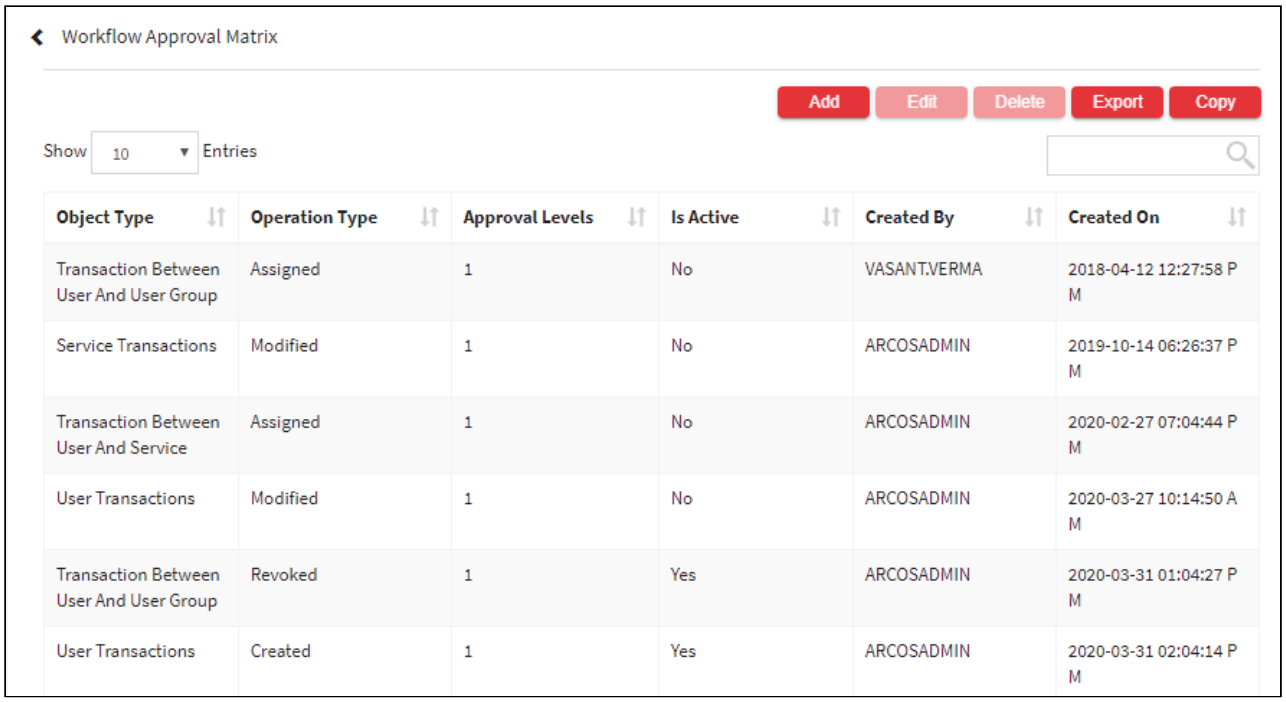
This section helps you to configure approval levels for each transaction or operation performed by Administrator. The transactions between Users, services, User group, and service group shall be sent for approval based on the approval levels configured in workflow matrix. Therefore, it provides a definite audit trail and proper flow of events, which are required to be monitored closely.

⚠ The Administrator having **ARCOS Workflow Approval Matrix** privilege in Server's Privileges will only be able to configure workflow approval matrix.

To navigate, use the following path:

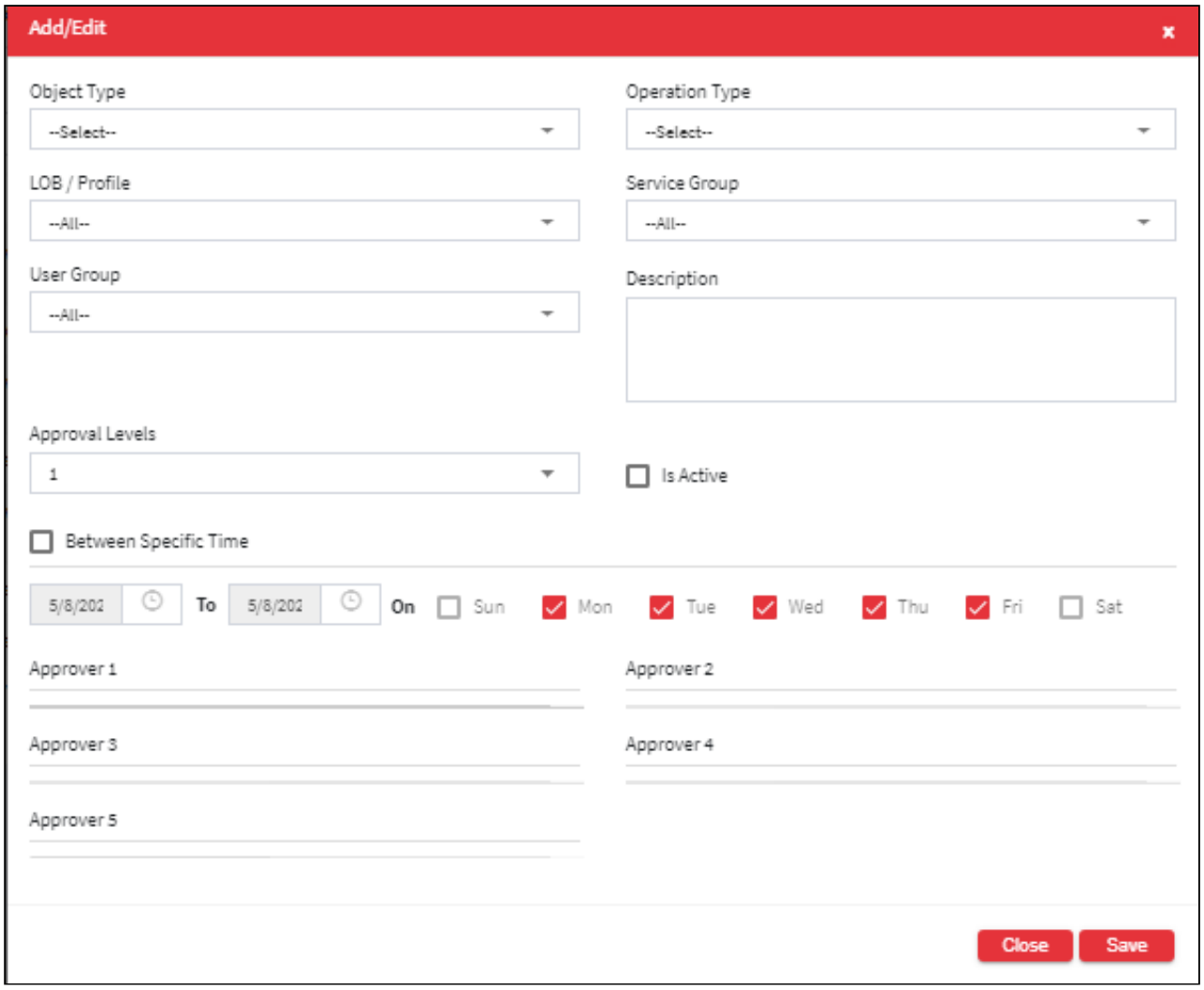
Settings → Workflow → Admin Activities

1. Select Workflow Approval Matrix under Admin Activities.



Object Type	Operation Type	Approval Levels	Is Active	Created By	Created On
Transaction Between User And User Group	Assigned	1	No	VASANT.VERMA	2018-04-12 12:27:58 PM
Service Transactions	Modified	1	No	ARCOSADMIN	2019-10-14 06:26:37 PM
Transaction Between User And Service	Assigned	1	No	ARCOSADMIN	2020-02-27 07:04:44 PM
User Transactions	Modified	1	No	ARCOSADMIN	2020-03-27 10:14:50 AM
Transaction Between User And User Group	Revoked	1	Yes	ARCOSADMIN	2020-03-31 01:04:27 PM
User Transactions	Created	1	Yes	ARCOSADMIN	2020-03-31 02:04:14 PM

2. Select the Add button to create a new matrix.

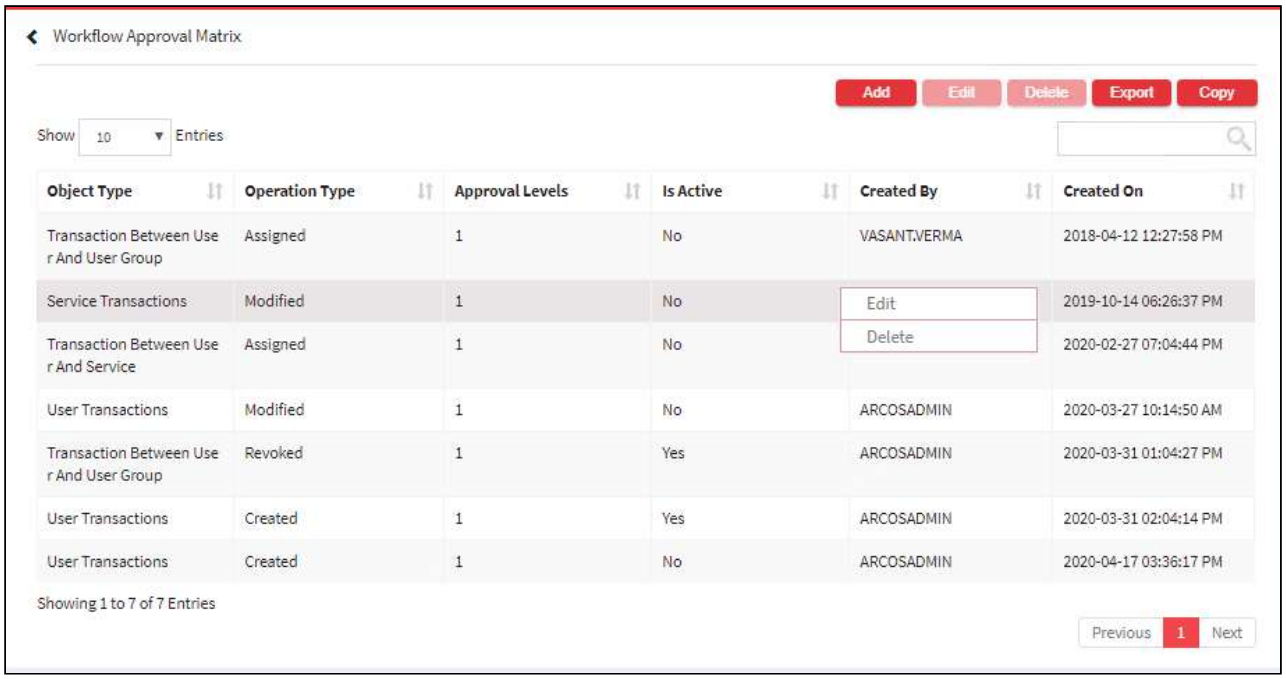


The **Approval Matrix** screen contains the following fields:

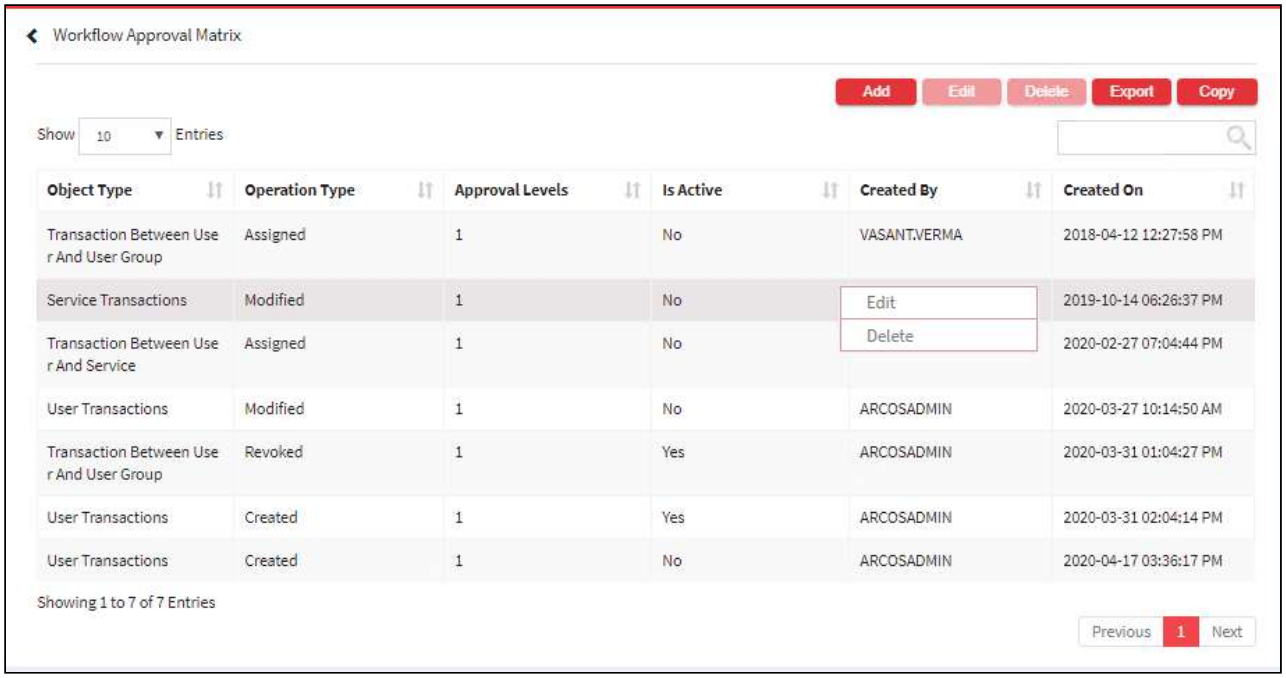
Field Name	Description
Object Type	Select the type of object. The valid values are: ▪ **User Transactions:** Used for the creation, deletion, modification of Users. ▪ **Service Transactions:** Used for the creation, deletion, modification of Services. ▪ **Transaction Between User and User Group:** To map User(s) with their respective User Groups. ▪ **Transaction Between Service and Service Group:**To add or remove services to/from their respective Server Group. ▪ **Transaction between User And Service:** To assign or revoke Services to/from Users. ▪ **Transaction Between User Group And Service:**To map or remove User Group to/from Service Group and vice versa.

Field Name	Description
Operation Type	Select the type of operation. The valid values are: ▪ Created ▪ Modified ▪ Deleted ▪ Assigned ▪ Revoked
LOB/ Profile	Select the LOB/Profile.
Service Group	Select the service group.
User Group	Select the user group.
Description	Specify the description for the selected object type.
Approver Levels	Select the levels of approval for the selected object type. The valid values are: ▪ 1 ▪ 2 ▪ 3 ▪ 4 ▪ 5 ⚠ You can select up to 5 levels of approval.
Is Active	Enable the configuration for approval.
Between Specific Time	To set the specific time for approval.
Approvers	Search and select the approvers for the workflow.

3. Click on Save to save all the changes.
4. For Editing, the details of the existing workflow matrix click on the existing row and select the Edit button at the top and make the required changes. Also, you can right-click on the row and select Edit.



5. For Deleting the existing workflow matrix click on the existing row and select the Delete button at the top and make the required changes. Also, you can right-click on the row and select Delete.



6. The Export button will export all the workflow approval matrix details in the form .xlsx format. The Copy button will copy all the details of the table.

- Once the workflow is created as per **Workflow Approval Matrix**, the request is sent to the approver(s) through email for approval.

Approve/Reject new users created

On raising a request by the user, the approvers will get the following mail in their inbox.

1. To approve/reject a request, the approver can reply to the above mail received in their inbox.
2. The approvers will have to reply with the content **#Approve#** or **#Reject#** to approve/reject the request.

13.8.3.2 Admin Activities Global Configurations

To navigate, use the following path:

Settings → Workflow → Admin Activities

Field Name	Description
User Request Approval Workflow - Is Enabled	**This configuration sets the availability of User Request Approval Workflow option.**
Disabled	If Toggle value is 'Disabled', this option will not be available for configuration.
Enabled	If Toggle value is 'Enabled', this option will be available for workflow configuration.
CAPTCHA Validation In ACMO Service Access And Password Request - Is Enabled	**This configuration enables/disables Captcha Validation in CM while raising Service Access and Password View Request.**
Disable	If Toggle value is 'Disabled', then it disables Captcha
Enable	If Toggle value is 'Enabled', then it enables Captcha

Field Name	Description
User Access Review Workflow - Is Enabled	**This configuration sets the availability of User Access Review under Server Manager.**
Disable	If Toggle value is 'Disabled', this option will be available.
Enable	If Toggle value is 'Enabled', this option will not be available.
Minimum Length of Comment Field While Rejecting Any Workflow	**This configuration sets the minimum length of characters under the comment field which is mandatory to be entered by Admin ID while rejecting Service Access, View Password requests, or any Workflow.**
Valid Values	It ranges from 0-99.
Minimum Length of Comment Field While Approving Any Workflow	**This configuration sets the minimum length of characters under the comment field which is mandatory to be entered by Admin ID while rejecting Service Access, View Password requests, or any Workflow.**
Valid Values	It ranges from 0-99.
LOB Wise Workflow Tracker - Is Enabled	**This configuration sets whether Workflow details should be displayed LOB wise or for all.**
Disable	If Toggle value is 'Disabled', then the “All” option will be available in LOB/Profile drop-down.
Enable	If Toggle value is 'Enabled', then only LOBs will be available for selection in LOB/Profile drop-down in Server Manager > Manage > Workflow Tracker > User Service Request Workflow Tracker tab.
Critical With Approval (Minutes)	**This configuration sets the time in minutes post which critical command execution request would auto terminate when the defined duration is expired.** **When the user tries to execute a critical command on the Server accessed from CM > Connections, count down for approval process is displayed. That count downtime is defined in this configuration**
Valid Values	It ranges from 5-30.

13.9 Session

13.9.1 Time Control

13.9.1.1 Application Configuration

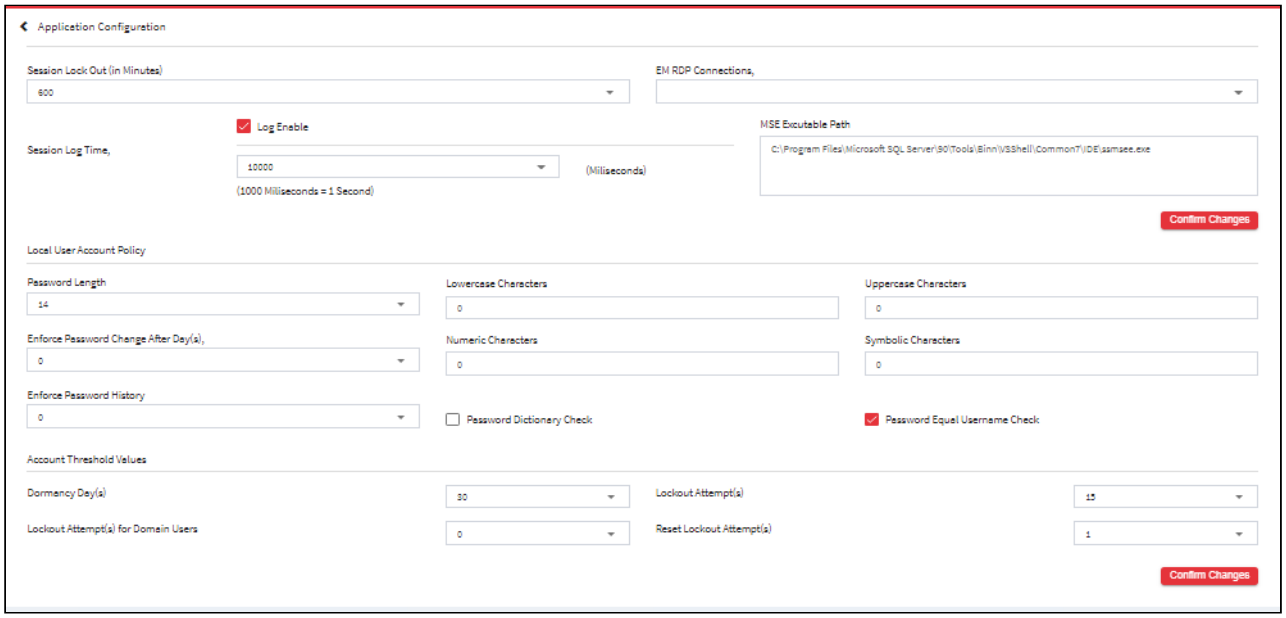
Application Configuration on the web enables the Administrator to design local and domain user account policy. The password policy and account threshold values configured are applicable to users created in ARCON PAM. The user's login can be managed according to the policy designed here. This configuration helps to set the session time out for the Target Server session, define session log time to capture images, set the password policy for the local users, and set the accessibility control for User's ids and hence this resides under the Session tab.

⚠ The Administrator having **Application Configuration** privilege in Server's Privileges will only be able to configure values.

To navigate, use the following path:

Settings → Session → Time Control

1. Select the Application Configuration under Time Control.



The **Application Configuration screen** contains the following buttons:

Field Name	Description
Session Lock Out (Minutes)	It is a Global Session Lockout time in minutes. If the value is set to 30 minutes and a user's RDP session remains idle for 30 minutes, it will get locked.

Log Enable	Enables the video log globally. ARCON PAM checks for every 250 milliseconds for the new screen. If it is set to 1000 milliseconds, it will check for a new screen after every 1 second. Note: By default, Log is enabled.
Session Log Time	Select the time interval in minutes to capture images of the Target Server session.
Local User Account Policy:	
Select the password policy for the ARCON PAM Local Users.	
Password Length	Set the length of the password.
Lower Case Characters	Select the number of lower case characters in the password.
Numeric Characters	Select the number of numeric characters in the password.
Enforce password Change After Day(s)	Users can apply similar policies as used in their Organization's Active Directory. Set the number of days after which the password should be changed.
Upper Case Characters	Select the number of upper case characters in the password.
Symbol Characters	Select the set number of symbol characters in the password.
Enforce Password History	The value set in this field applies that Users cannot use the same password for the next time. If the value in this field is set to 6, the user cannot use the passwords for the next 6 times. Every time a new password should be used for the defined number of times.
Password Dictionary Check	Select this value for ARCON PAM to check Password Dictionary while changing the password of Local User or creating new local User in ARCON PAM.
Password Equal Username Check	Select this option if you do not want to set the same username and password.
Account Threshold values	
Sets accessibility control for all active User IDs in ARCON PAM. The Admin ID can set the maximum number of days an account will be in an enable state, set lockout attempts, and reset lockout time.	
Dormancy Days(s)	A User ID is added to the Dormancy Days list if the user does not login to ARCON PAM for the configured number of days. **Example:** If the dormancy period is set to 30 days and a user did not log into the application during this period, then ARCON PAM will become dormant to that user and the user will be added in the dormant list under Manage Users. The Users in Dormant List are not allowed to login until the Administrator does not change Account Status to Active for that user.
Lockout Attempt(s)	The value set in Lockout Attempts is considered to Lock local User ID's in ARCON PAM. **Example:** If Lockout Attempts is set as 3 and User makes 3 Invalid Attempts to login into Client Manager Online; then his ID gets locked and it is added to Lockout Users List under Manage Users. Such users will not be able to Login into ARCON PAM even with the correct password.

Lockout Attempt(s) for Domain Users	The value set in Lockout Attempts for Domain Users is considered to Lock domain User ID's in ARCON PAM. **Example:** If Lockout Attempts for Domain Users is set as 3 and User makes 3 Invalid Attempts to login into Client Manager Online; then his ID gets locked and it is added to Lockout Users List under Manage Users. Such domain users will not be able to Login into ARCON PAM even with the correct password.
Reset Lockout Minute(s)	The value set in Reset Lockout Minutes is considered to Reset Locked User IDs in ARCON PAM. **Example:** If the value in Reset Lockout Minute(s) field is set as 15, after 15 Minutes User ID will be unlocked. This user can then login to ARCON PAM. If the value in this field is set to zero, ARCON PAM will not reset locked users. In this case, the Administrator of ARCON PAM needs to change Account Status to Active for that user under Manage Users.

3. Select/Enter the details and click **Confirm Changes** to enable the configuration.

13.9.1.2 Time Control Configuration

To navigate, use the following path:

Settings → Session → Time Control

Field Name	Description
Max Session(s) Per User (0 Is Unlimited)	**This configuration sets the maximum number of CM sessions that can be taken by a User ID at a time.**
Valid Values	The valid range is 0-999.
Min Time Wait For New User Session - If Exceeds	**This configuration sets the minimum time to wait before initiating a new CM session when other than zero value is defined in Max Session(s) Per User (0 Is Unlimited) configuration.** **If value defined in Max Session(s) Per User (0 Is Unlimited) is '1' and user logs in into CM and without logging out closes the browser, then he cannot log in to CM with same User ID from another system until the time defined in Min Time Wait For New User Session - If Exceeds has expired.**
Valid Values	It ranges from 0-999.
AWM Session Timeout (Minutes)	**This configuration sets the time in minutes for Workflow Manager Session Timeout. The Workflow Manager will log out if keep idle for the configured number of minute** **Note: The Workflow Manager link is sent to Approver's email for approving/rejecting requests such as service access, service password, user transaction, and so on.**
Valid Values	It ranges from 0-9999.

Field Name	Description
Max Hours For Service Session Duration	**This configuration sets the time in hours to be made available for selection while raising a request for Service Access.**
Valid Values	It ranges from 0-999.
Auto Terminate Session If Session Duration Expired (Minutes)	**This configuration sets time in minutes post which Session would auto terminate when defined duration in service access request has expired.** **When a Time Based or One Time session is accessed from My Services (Client Manager > My Access > My Services) and defined duration in request has expired, a window is displayed for requesting session extension. This window is displayed for a defined time which displays as a count down. The maximum minutes to be displayed as count down are configured in this configuration.**
Valid Values	It ranges from 0-999.

13.9.2 UI Control

We also need to set the UI features for capturing the sessions.

To navigate, use the following path:

Settings → Session → UI Control

Field Name	Description
ARCOS Window Min Width	**This configuration sets minimum Width of ARCON PAM window.**
Valid Values	It ranges from 600-800.
ARCOS Window Min Height	**This configuration sets minimum Height of ARCON PAM window.**
Valid Values	It ranges from 450-600.
Terminate Session Button On Unlock Session - Is Enabled	**This configuration enables/disables the display of “Terminate Session” button on the Unlock Session window.**
Disable	If Toggle value is 'Disabled', then it disables the button.
Enable	If Toggle value is 'Enabled', then it displays the button.

Field Name	Description
Client Session Window Title Order	**This configuration will allow users to rearrange name in the title bar for service session.**
Valid Values	One can mention at least these fields IP Address, User, Service Type and a maximum of IP Address, User, Hostname, DBInstance, Service Type
Disable Snipping Tool - Is Enable	**This configuration enables/disables Snipping Tool on the Windows RDP connection established from Client Manager.**
Disable	If Toggle value is 'Disabled', then enable the snipping tool on Server.
Enable	If Toggle value is 'Enabled', then it disables the snipping tool on Server.
Launch Putty FullScreen Mode - Is Enabled	**This configuration sets whether putty will open in full screen or minimized mode when you connect from Client Manager.** **Note: This configuration is applicable to SSH Linux services with <PTY> tag in the Parameter field (field 4).**
Disable	If Toggle value is 'Disabled', then putty will be opened in minimized mode.
Enable	If Toggle value is 'Enabled', then putty will be opened in full screen.

13.10 Domain

13.10.1 Configure

13.10.1.1 Domain Configuration

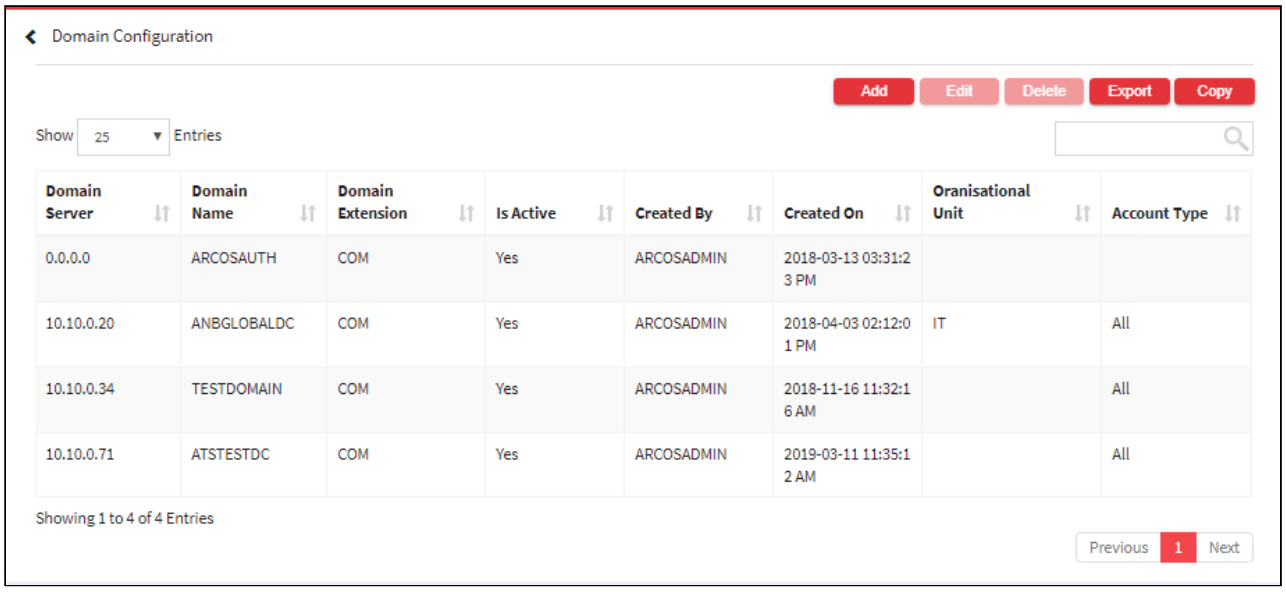
Domain Configuration allows in configuring different domains. A particular domain will only be visible on the login screen if it is active. The configured domain can be disabled. To disable all the logins for a particular domain, the configuration has to be disabled. Once the configuration is disabled, users will not be allowed to login to ARCON PAM. User authentication is done by validating details in the domain server. ARCON PAM can also authenticate users using multiple domain servers.

⚠ The Administrator having **Domain Configuration** privileges in Server's Privileges will only be able to configure values for the domain.

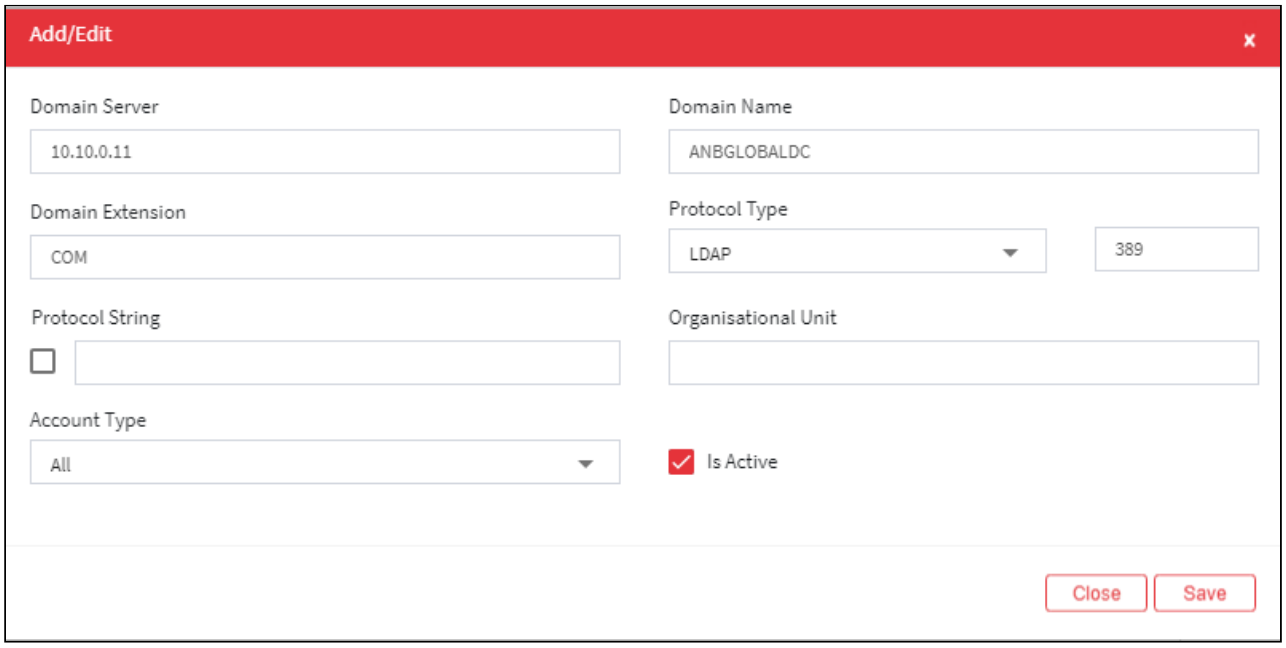
To navigate, use the following path:

Settings → Domain → Configure

1. Select Domain configuration and the following screen is displayed.



2. For adding a new domain select the Add button.

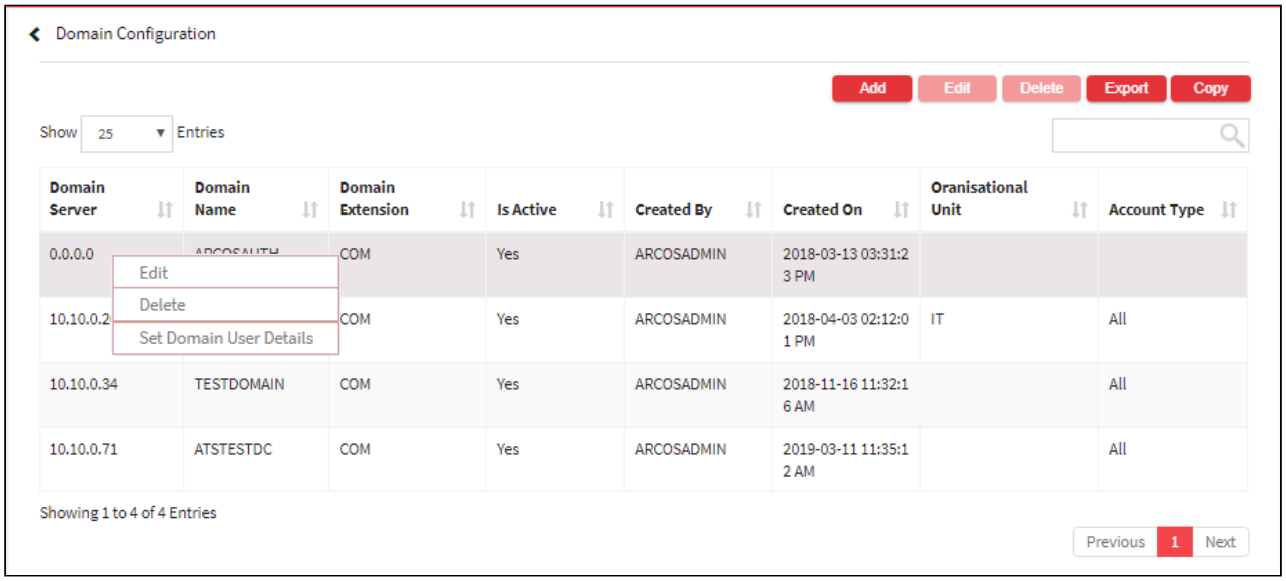


The **Domain configuration screen** contains the following fields:

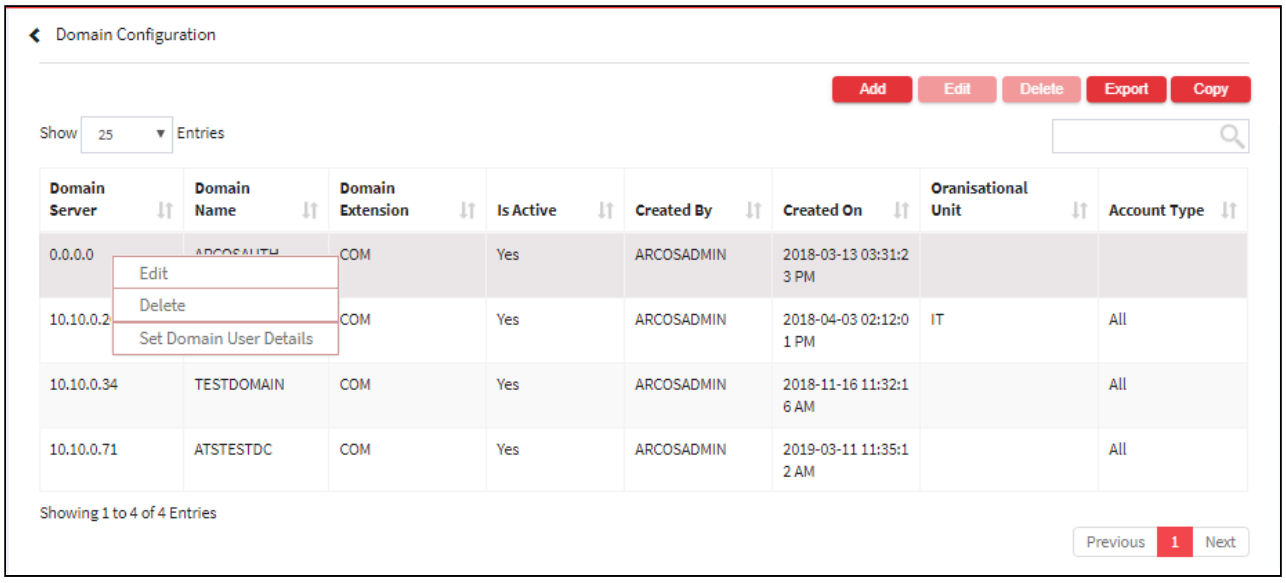
Field Name	Description
Domain Server	Enter the Domain Server IP Address. If there are multiple AD accounts in an organization, use ~ to separate multiple IP addresses.
Domain Name	Enter the Domain Name.
Domain Extension	Enter the extension of Domain.
Protocol Type	Select authentication type as ARCOSAUTH, LDAP OR LDAP SSL as available in the dropdown list.

Field Name	Description
Protocol String	In LDAP, the LDAP string can be configured. If the LDAP string is enabled, ARCON PAM will use the configured Protocol String, such as Domain Server, Domain Name and Domain Extension to communicate the Domain Server.
Organizational Unit	Enter the name of the Organization Unit to which it shall belong.
Account Type	Select the type of account for which the domain is configured i.e Privileged account or Login account
Is Active	Enable the configuration.

3. Enter the details and click **Save,** a domain is configured in **Domain Configuration**.
4. For Editing the details of the existing Domain click on the existing domain and select the Edit button at the top and make the required changes. Also, you can right-click on the domain and select Edit.



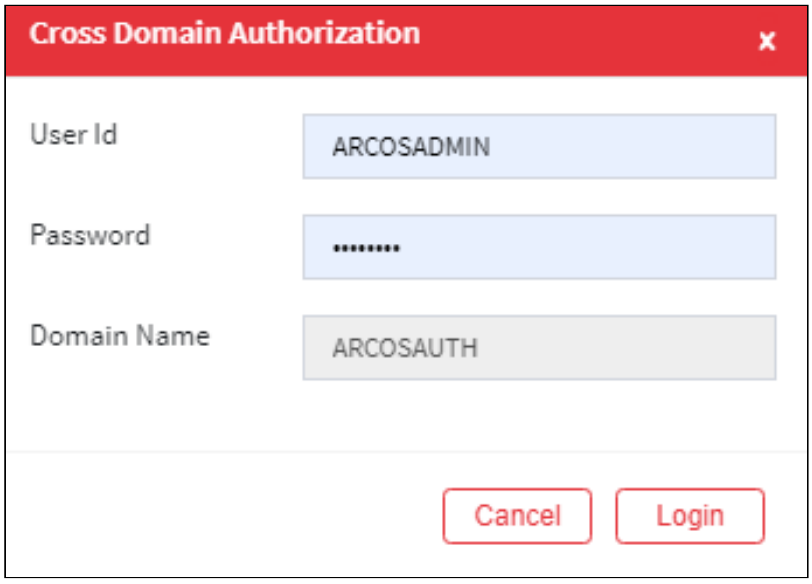
5. For Deleting the existing Domain click on the existing domain and select the Delete button at the top and make the required changes. Also, you can right-click on the domain and select Delete.



6. Right-click the domain and click **Set Domain User Details**. The **Cross Domain Authorization** dialog box appears.

> Cross Domain authorization is set when users have to be created belonging to ARCOS domain, with some credentials to authenticate with another domain. The user using for Cross-Domain Authentication should be a part of the domain and should not have a password expiry. It is recommended to be a service account.

The **Domain configuration screen** contains the following fileds:



The **Cross Domain Authorization** dialog box appears.

Field Name	Description
User ID	Enter the User ID.

Field Name	Description
Password	Enter the Password.
Domain Name	Enter the Domain Name.

7. The User ID and Password to be entered once. When validating a user or creating a new user of that particular domain, it will not prompt for the password.
8. The Export button will export all the template details in the form .xlsx format. The Copy button will copy all the details of the table.

13.11 Ticket

This section includes the following topics:

- Template
- Service Type

13.11.1 Template

13.11.1.1 Service Reference Template

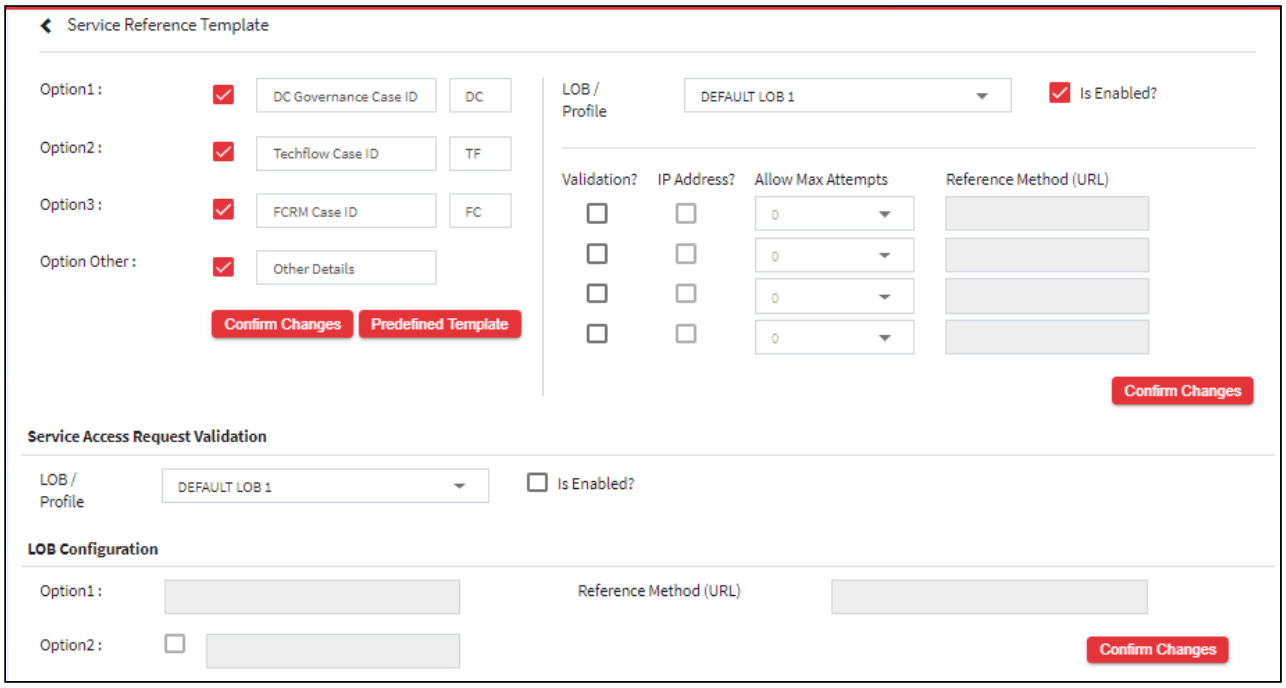
Service Reference Template is used to configure templates. Once the service reference template is configured, the user will be asked for the reference to access any service such as Ticket Number, DC Governance Case ID, Techflow Case ID, or Form Case ID. The template can be modified as per the admin's requirement. The DC, TF, and FC are the prefix defined by the admin and it will be displayed in Audit Trails to identify which type of reference details the log is referring to. You can also define **Predefined Templates** Service Type wise. The details captured while accessing any service are displayed in 'Service Logs' as a part of a comprehensive audit trail to have a correlation with the integrated CMS/TS Tool.

The Administrator having **Service Reference Template** privileges in Server's Privileges will only be able to configure templates.

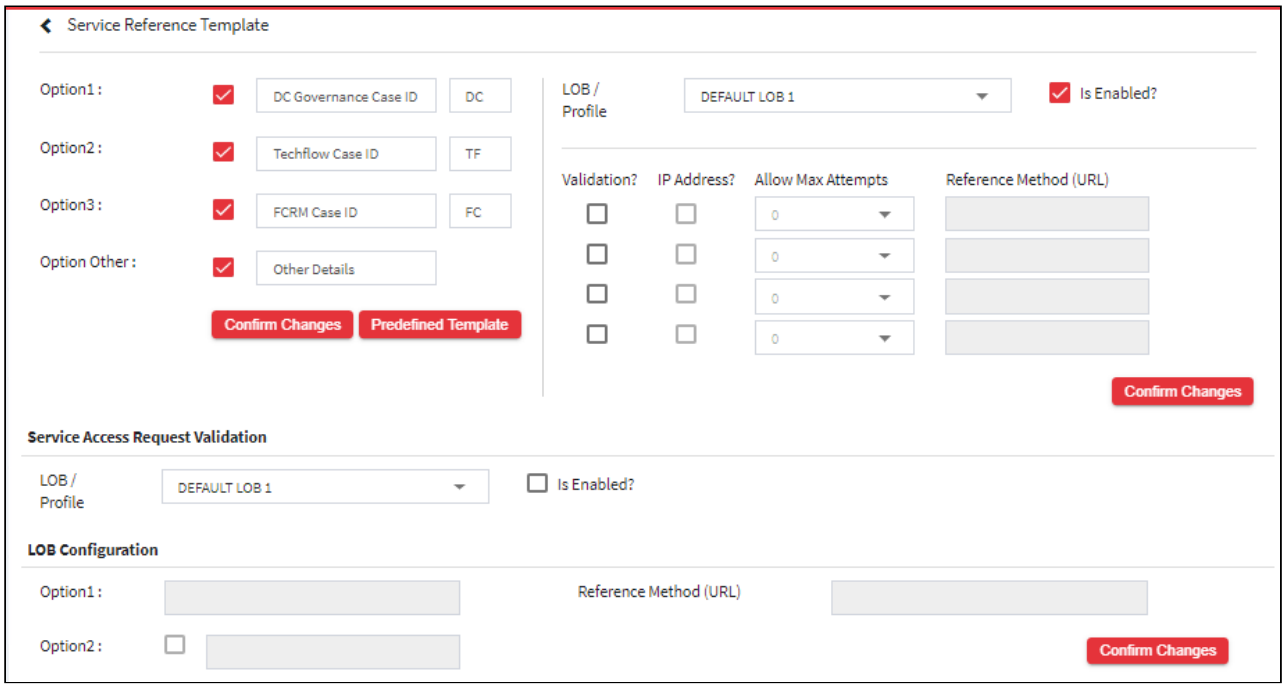
To navigate, use the following path:

Settings → Ticket → Template

1. Select Service Reference Template under the template and the following screen is displayed.
2. Select the required option from the left pane and click **Confirm Changes**. The selected options will be displayed while accessing the Service.



3. Select the LOB/Profile from the **LOB/Profile** drop-down list and select **Is Enabled?** checkbox to enable the Service Reference Template.



4. Below is the detail description of fields under **LOB/Profile Configuration** and action invoked with it:

Field Name	Description
Validation	If 'Validation?' is enabled, ARCON PAM will send the UserId, Reference Ticket Number to the CMS/TS for validation. On successful validation, it will further give access to the target server, or else it will display the appropriate message send by the CMS/TS.
IP Address	If 'IP Address?' is enabled, ARCON PAM sends the UserId, Reference Ticket No. & Requested Server IP Address to the CMS/TS for validation. On successful validation, it further gives access to the target server or else displays the appropriate message sent by the CMS/TS.
Allow Max Attempts	If the attempts are set to a particular value it allows the end-user to use the Reference Ticket Number only for the number of times it is set.
Reference Method (URL)	Enter the URL (Web Service Call), so that ARCON PAM can communicate to the CMS/TS.

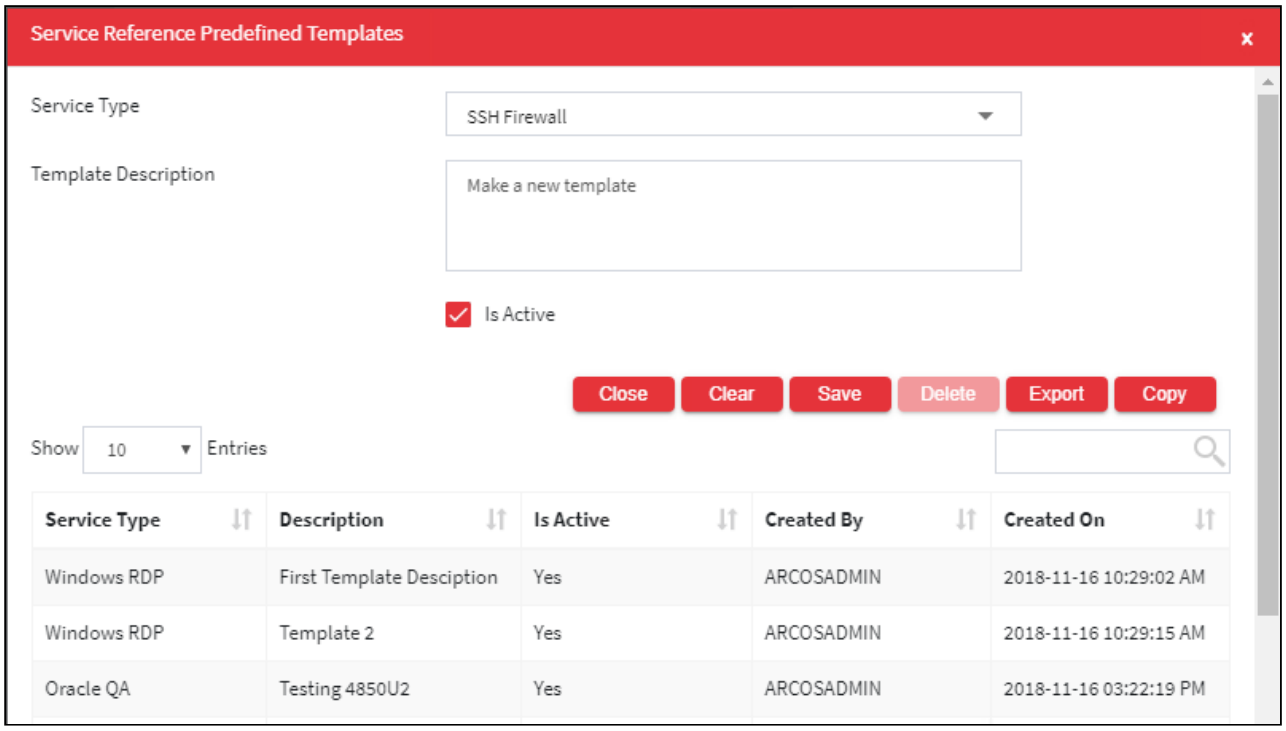
5. Click **Confirm Changes** to save settings.

   Example: When the Administrator enables this validation and User tries to access any Service, ARCON PAM sends User ID, the Ticket / Reference Details entered by User, IP Address of Server being accessed to Change Management System / Ticketing System by calling the Reference URL configured above. If validation is successful, the user gets access to the server. If not successful then appropriate Error Message from Change Management System will be populated to the End User.

6. Click **Predefined Template** to configure templates Service Type wise.

   ⚠ You need to select **Option Other** checkbox and click **Confirm Template**. The details configured in the predefined template option will be displayed in **Option Other** field viewed while accessing Service from Client Manager.

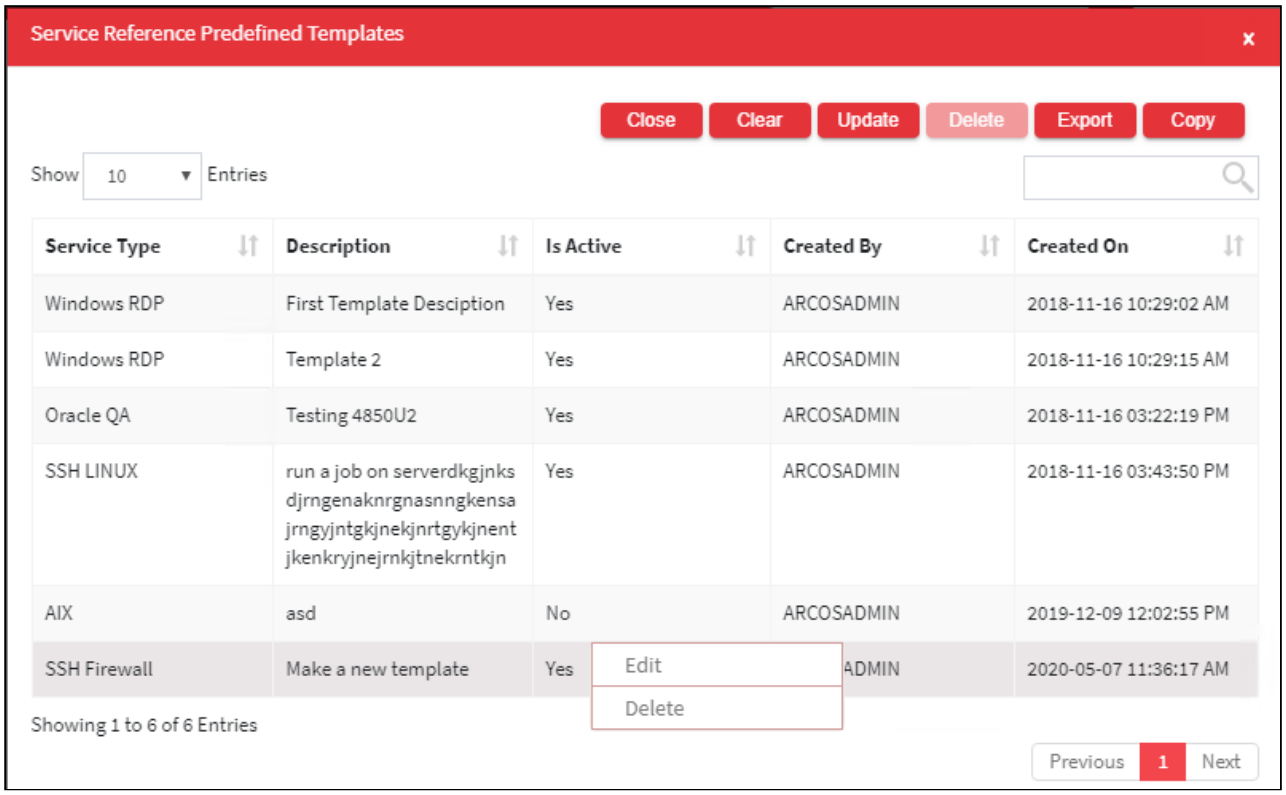
7. The following screen is displayed when you click **Predefined Template**. It displays the list of existing Predefined templates.
8. For adding a new template select the service type, add the Template Description, and select Is Active and click on Save to add the template and Clear to clear all the details.



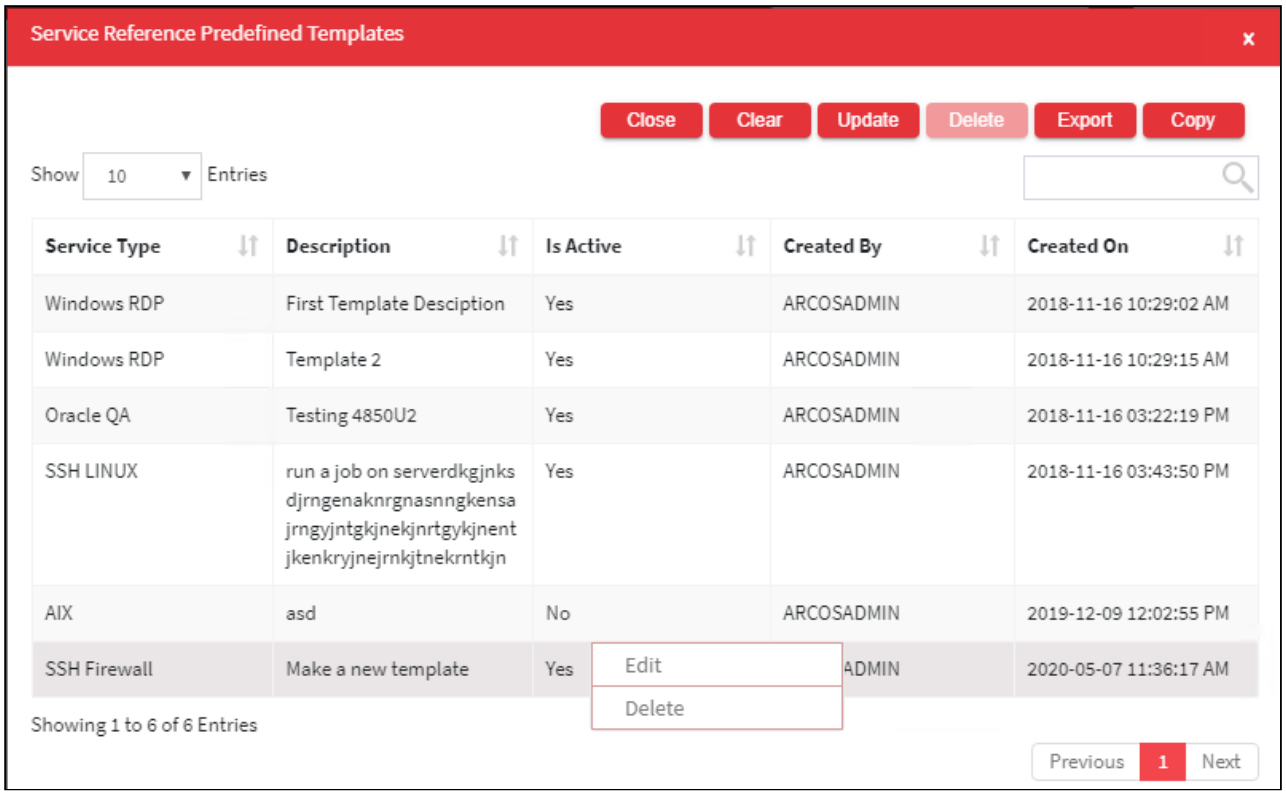
Below is the detail description of fields under **Service Reference Predefined Templates**:

Field Name	Description
Service Type	Select the Service Type.
Template Description	Enter the template description.
Is Active	Select the checkbox to enable visibility of this template.

9. For Editing, the details of the existing predefined templates click on the existing predefined templates and select the Update button at the top and make the required changes. Also, you can right-click on the row and select Edit.



10. For Deleting the predefined templates select on the predefined templates and select the Delete button at the top and make the required changes. Also, you can right-click on the row and select Delete.



11. The Close button closes the page and returns to the former page.
12. The Export button will export all the server template details in the form .xlsx format. The Copy button will copy all the details of the table.

13.11.2 Service Type

13.11.2.1 Server Reference / Call log

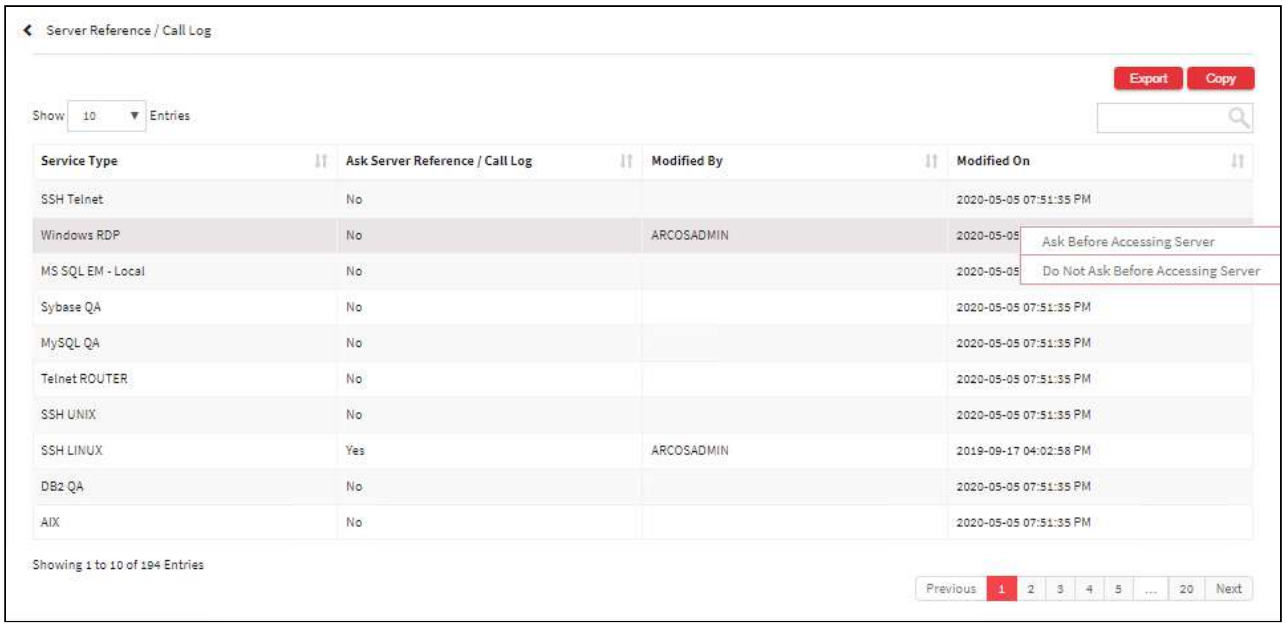
The Server Reference / Call Log feature on the web enables a confirmation message box, which prompts for the ticket number and the reason for accessing a particular service in Client Manager.

⚠ The Administrator having **Server Reference / Call Log** privileges in Server's Privileges will only be able to enable confirmation message box.

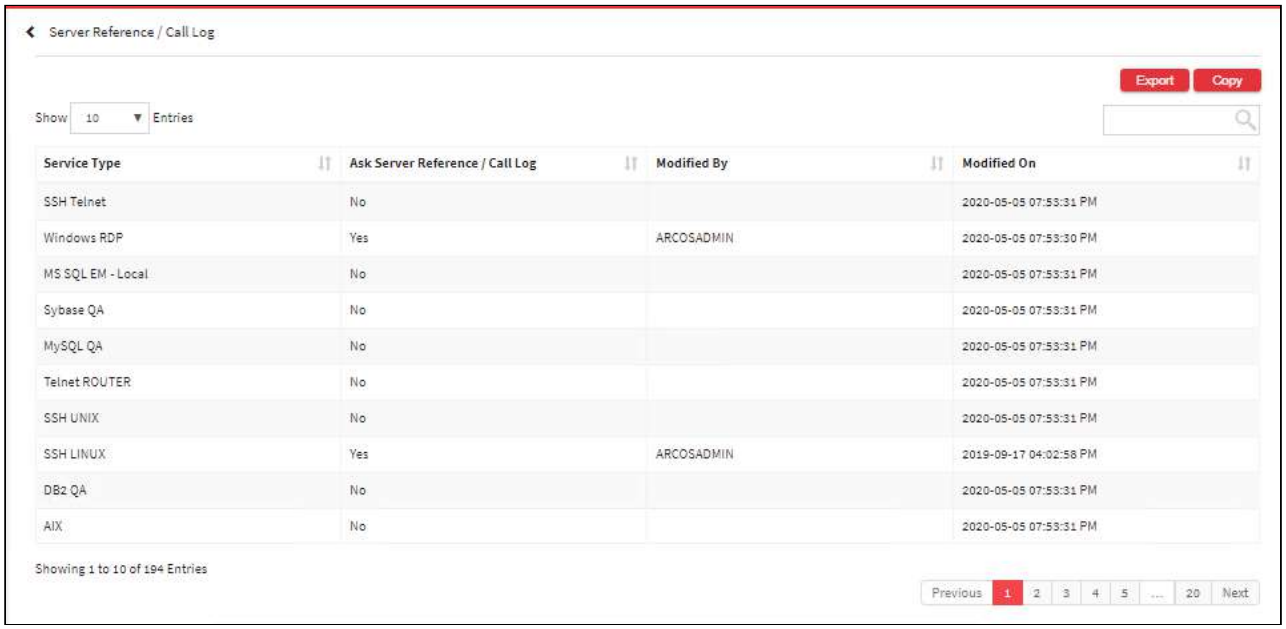
To navigate, use the following path:

Settings → Ticket → Service Type

1. Select service Reference/ Call log under Service type.
2. Right-Click on a particular **Service Type** then choose **Ask Before Accessing Server** option.



3. The **Ask Server Reference / Call Log?** column status will change from **No** to **Yes**.



4. The Export button will export all the Service Reference or Call Log details in the form .xlsx format. The Copy button will copy all the details of the table.

13.12 Logs

Logs capture all the activities performed in ARCON PAM with detailed information. It provides an audit trail for transactions performed in Server Manager. It also provides detailed information about services accessed through ARCON PAM.

This section includes the following topics:

- Image Quality
- Capture
- Archival Service
- Scheduler

To navigate, use the following path:

Settings → Log

Field Name	Description
Reference Detail Required For Audit Trail - Is Enabled	**This configuration enables/disables prompting Admin User to enter reference details for transactions performed in Advanced Configuration and User and Service Management.**
Disable	If Toggle value is 'Disabled', then ARCON PAM will not prompt Admin User for reference details against which the change is being performed.
Enable	If Toggle value is 'Enabled', then ARCON PAM will prompt Admin User for reference details against which the change is being performed.
Enable Video Log	This configuration enables/disables video logs for all service types under Settings → Log → Capture→ Modify Service type→ Enable/Disable service parameter field.
Disable	If Toggle value is 'Disabled', then video logs for all service types are disabled.
Enable	If Toggle value is 'Enabled', then video logs for all service types are enabled.
Enable Text Log	This configuration enables/disables text logs for all service types under Settings → Log → Capture→ Modify Service type→ Enable/Disable service parameter field.
Disable	If Toggle value is 'Disabled', then text logs for all service types are disabled.
Enable	If Toggle value is 'Enabled', then text logs for all service types are enabled.

13.12.1 LOB Wise Log Archival Settings

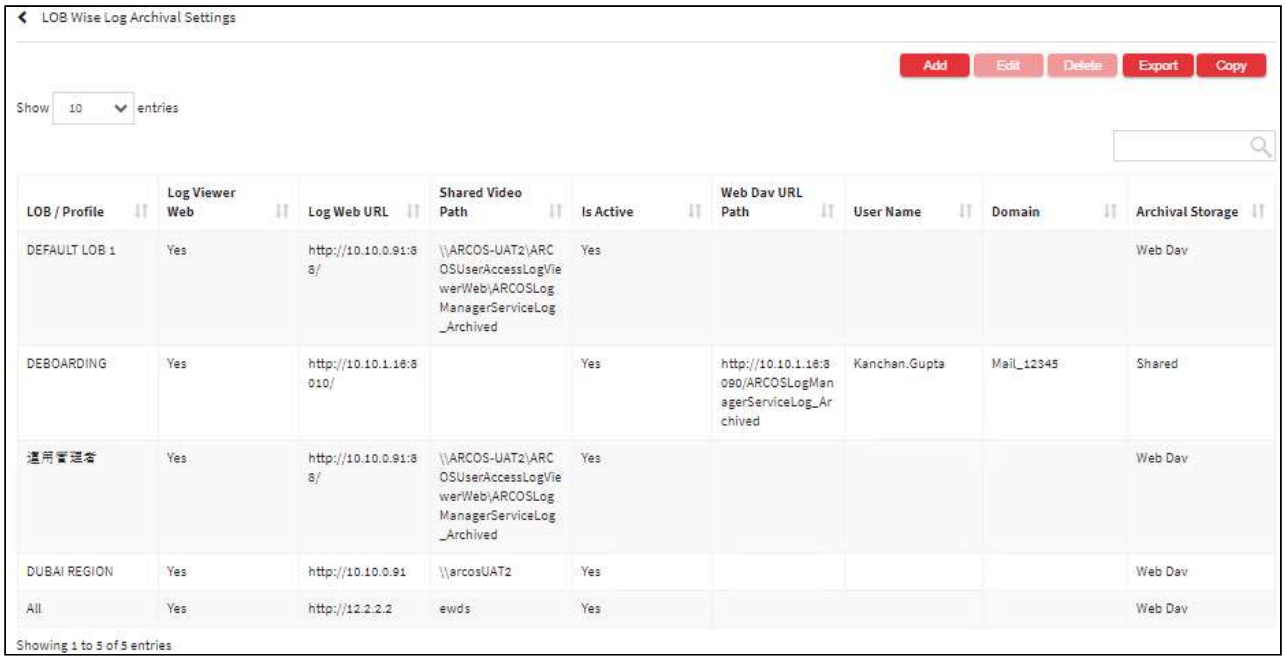
LOB Wise Log Archival Settings will enable users to store the video logs LOB wise. The videos can be stored on a shared folder or on Web Dav.

⚠ The Administrator having **LOB Wise Log Archival Setting** privilege in Server's Privileges will only be able to configure details in LOB Wise Log Archival Setting section.

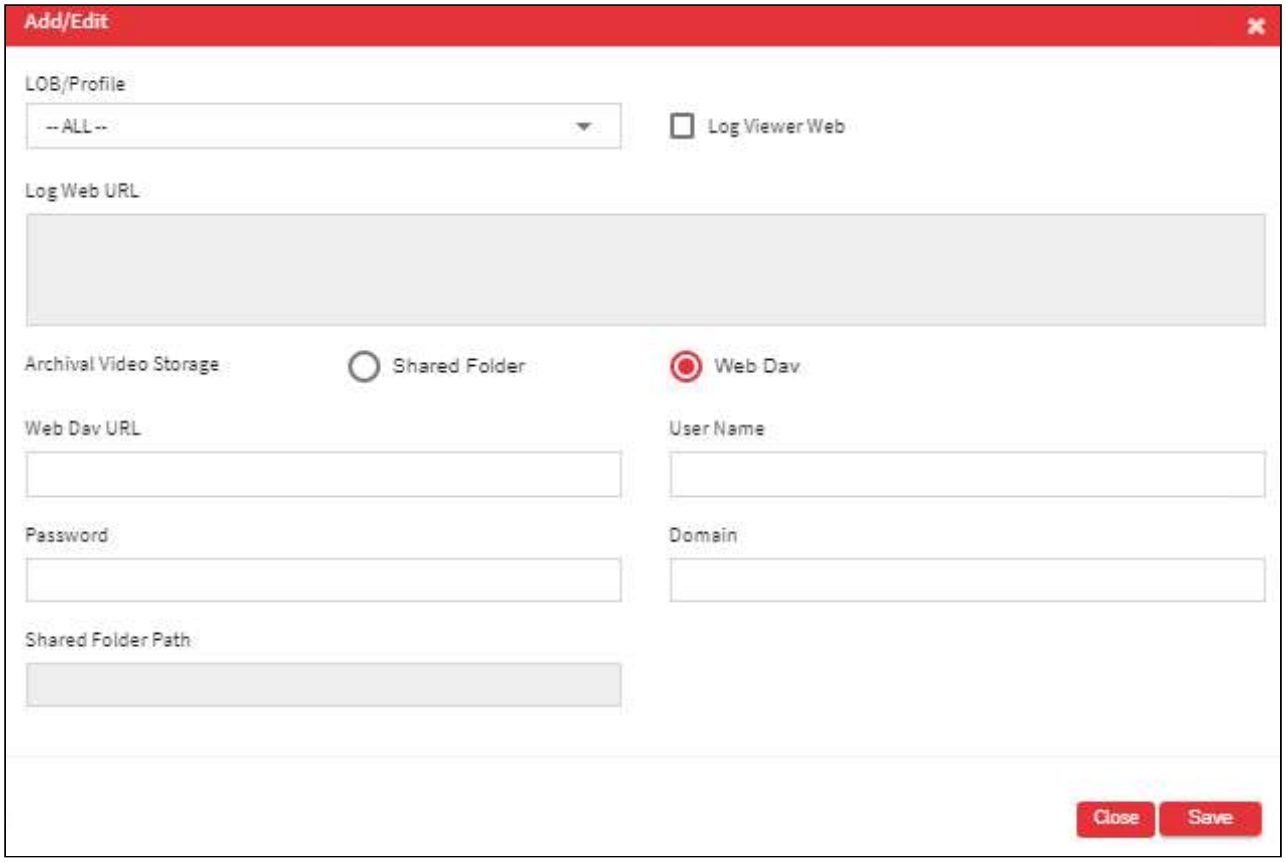
To navigate, use the following path:

Settings → Log

1. Select LOB Wise Log Archival Settings.



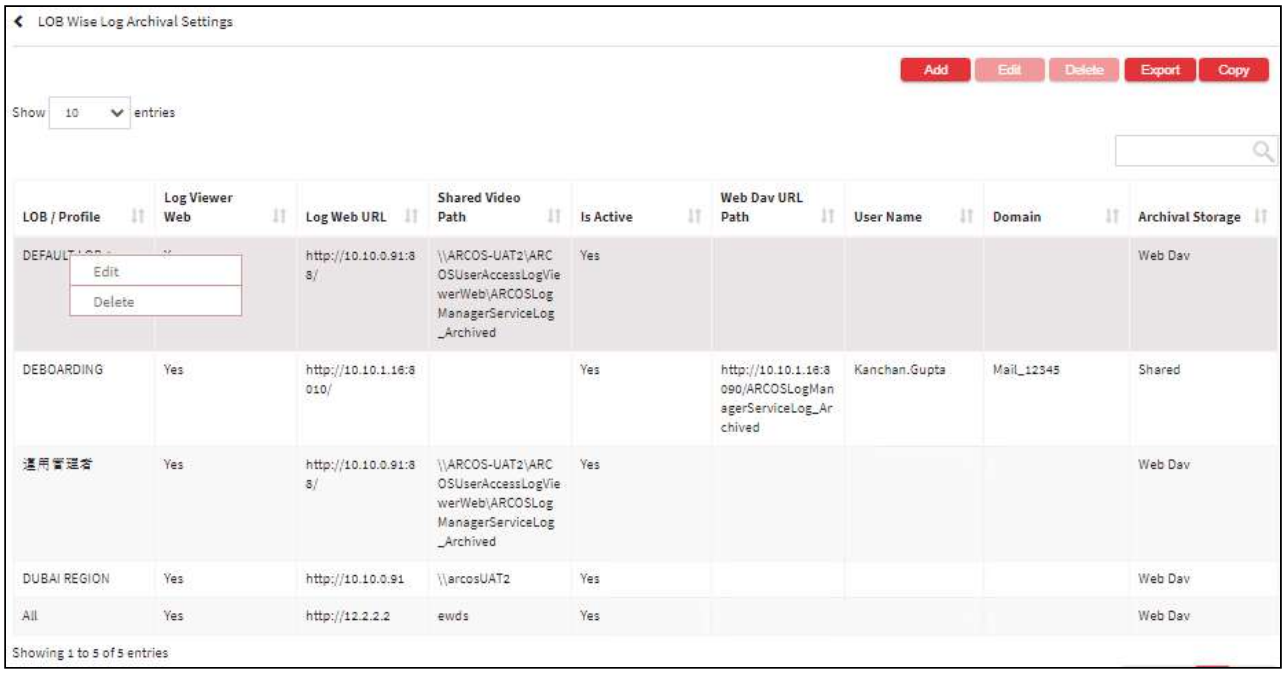
2. Select the Add button to add a new LOB Wise Log Archival Setting.



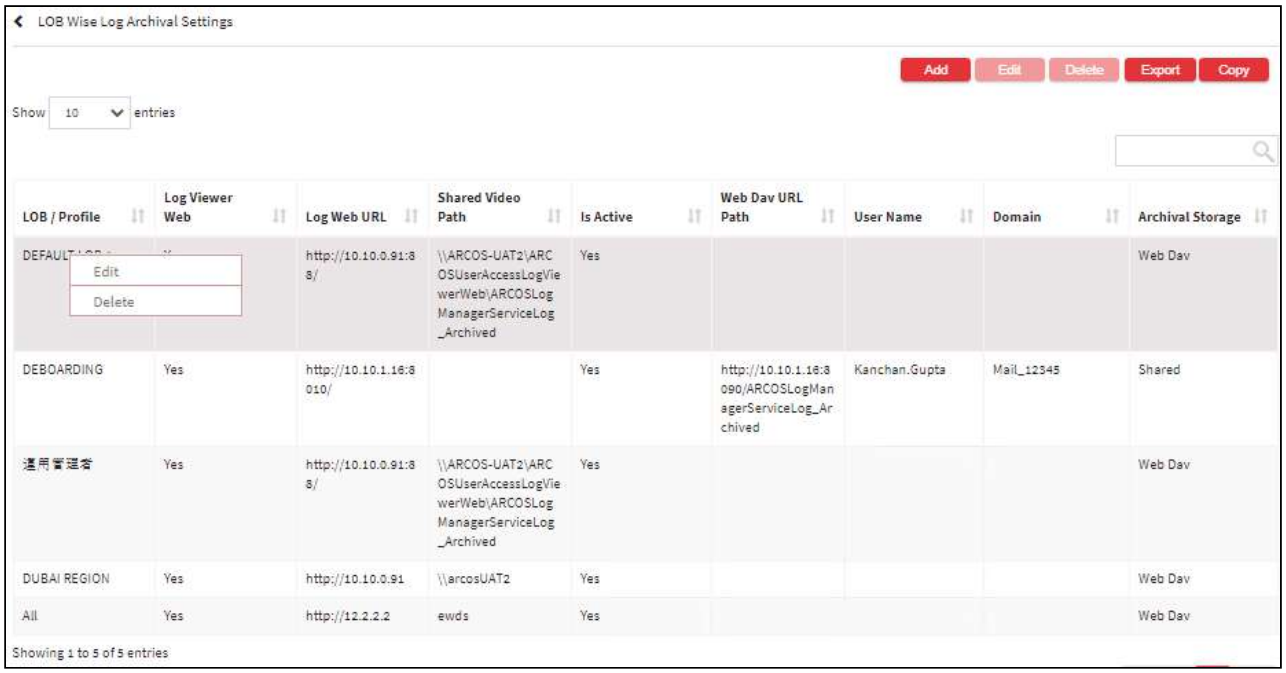
The **LOB Wise Log Archival Settings** screen contains the following fields:

Field Name	Description
LOB Profile	Select the LOB for which the Log staging settings are to be set.
Log Viewer Web	Enable Log Viewer Web to enter the Log Web URL.
Log Web URL	This is the URL of the log web viewer play website hosted on IIS. This URL will allow you to play videos.
Archival Video Storage	Select the storage ▪ Shared Folder ▪ Web Dav
Web Dav URL	This is the URL of **ARCOS UserAccessLogViewer** Website hosted on IIS. This URL is used to store video. The URL should be in the following format: IP Address:Port/ARCOSLogManagerServiceLog_Archived
User Name	Enter a user name of the server where user access log viewer is hosted
Password	Enter the password of the above user name
Domain	Enter the Domain.
Shared Folder Path	Enter the path of the Shared folder.

3. Enter the details and click Save button to create a new LOB Wise Log Archival Setting.
4. For Editing, the details of the existing LOB Wise Log Archival Setting click on the existing row and select the Edit button at the top and make the required changes. Also, you can right-click on the row and select Edit.



5. For Deleting the existing LOB Wise Log Archival Setting click on the existing row and select the Delete button at the top and make the required changes. Also, you can right-click on the row and select Delete.



6. The Export button will export all the LOB Wise Log Archival Setting details in the form .xlsx format. The Copy button will copy all the details of the table.

⚠ If StagingLogServer is **True**, then images are picked from the path configured in **URL** field of Staging Log Server in Server Manager and archived videos are stored in the path configured for **Web Dav URL** of **LOB Wise Log Archival Settings** in Server Manager.

13.12.2 Image Quality

This section helps you to with Image Quality configurations in logs.
To navigate, use the following path:

Settings → Logs → Image Quality

Field Name	Description
ARCOS Video Log Image Config - Is Enabled	**This configuration enables/disables ARCON PAM Video Log Image Configuration.**
Disable	If Toggle value is 'Disabled', then this feature is disabled.
Enable	If Toggle value is 'Enabled', then this feature is enabled.
ARCOS Video Log Image Width	**This configuration sets Width of Image in Video Log.**
Valid Values	The valid range is 0-1920.

Field Name	Description
ARCOS Video Log Image Height	**This configuration sets the Height of Image in Video Log.**
Valid Values	The valid range is 0-1080.
ARCOS Video Log Image Compression - Is Enabled	**This configuration enables/disables ARCON PAM Video Log Image Compression**
Disable	If Toggle value is 'Disabled', then it disables ARCON PAM Video Log Image Compression.
Enable	If Toggle value is 'Enabled', then it enables ARCON PAM Video Log Image Compression.
ARCOS Video Log Image Quality	**This configuration sets the Quality of Image in ARCON PAM Video Log in percentage. e.g. 50% compression**
Valid Values	The valid range is 0-100.
ARCOSSIEMConnectorService - ARCOS Event ID From SIEM	**This configuration sets the ARCON PAM Event ID that is defined in ARCON PAM SIEM Connector Service.**
Valid Values	Failed Login Attempts: This Event ID represents the invalid logon attempts in ARCON PAM. Service Access: This Event ID represents the individual servers accessed by any ARCON PAM user. Service Command This Event ID represents the command and informs you about the particular command that is fired in the session. Password View: This Event ID contains the information about the level of user who has requested and approved the password, time of the password request, device for which the password request is sent, and so on. Password Change: This Event ID is a password change service. It consists of information about the password that is printed on the server. Service Password Envelope Print: This Event ID consists of the information about the envelope printing and password printing. There are 10 levels of printing status. ARCOS Log: This Event ID represents the all generic ARCON PAM logs (They are Object type and Operation Type).
Video Download File Name format	**This configuration is used to change the Video Download Video Filename format.**

Field Name	Description
Valid Values	If the value of the last element of the configuration is 0 i.e USER ID,HOSTNAME,IP ADDRESS,0 then this configuration is not active. The file name will be downloaded by the name of the SessionID. If the value of the last element of the configuration is 1 i.e USER ID,HOSTNAME,IP ADDRESS,1 then this configuration is active. The file name will be downloaded by the name of the USER ID_ HOSTNAME_ IPADDRESS_ddmmyyyy_SessionID.

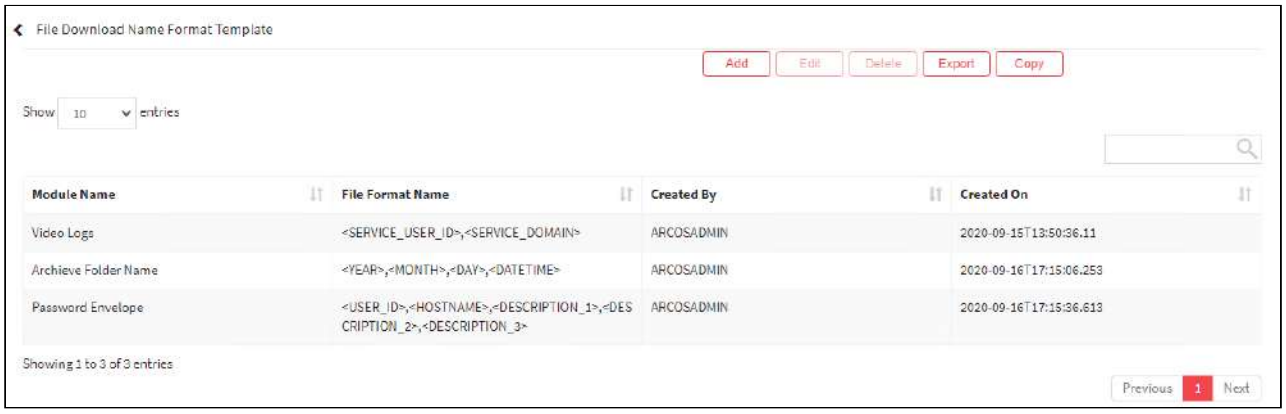
13.12.2.1 File Download Name Format Template

Organizations usually have tons of files, and if the filenames are not consistent then searching and retrieving the file becomes an uphill task. Thus we have a File Download Name Format Template which sets the standardized format for the files once they are downloaded. This naming convention ensures that the team and collaborators can discover, manage, and access the file easily as and when needed. The order of selection of these configurations forms a template. The configurations under this template include User Id, User Name, Machine details, Service Type, Service IP, Service hostname, Service User Name, Service DB Instance, Service Port Number, Connection type, Description 1, Description 2, Description 3, Service Group, User Group, LOB, Task/Incident number, Task/Incident Description, and Log fileName.

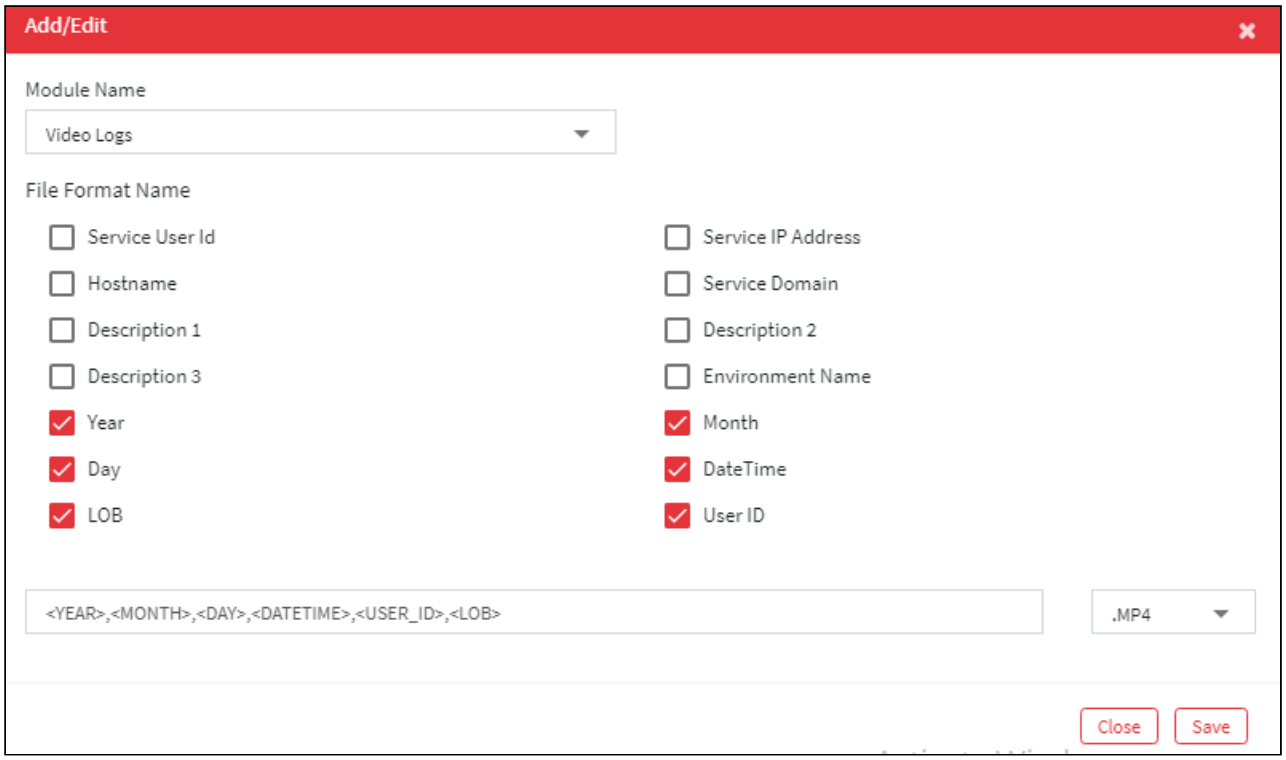
To navigate, use the following path:

Settings → Log → Image Quality

1. Select File Download Name Format Template under Image Quality.



2. Select the Add button to create a new template.

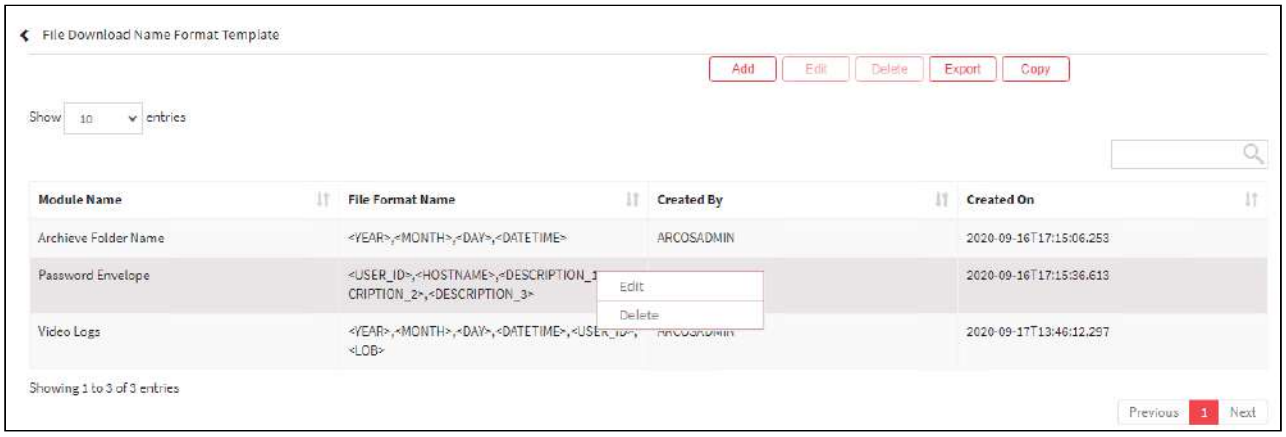


The **File Download Name Format Template** contains the following fields:

Field Name	Description
Module Name	Select the module for which the template should be set ▪ Video Logs ▪ Archive Folder Name ▪ Password Envelope
File Format Name	Select the configurations one by one, the naming template is formed. Example- If the admin wants the filename of the logs to be in accordance with the date format (yyyy-mm-dd) followed the UserId and LOB. The checkboxes are selected in this way- Year, followed by Month, Day, DateTime, UserID, LOB.

3. Click on Save to save all the changes and the File Download Name Format Template has been set.
4. For Editing, the details of the existing template click on the existing row and select the Edit button at the top and make the required changes. Also, you can right-click on the row and select Edit.

5. For Deleting the existing template click on the existing row and select the Delete button at the top and make the required changes. Also, you can right-click on the row and select Delete.



6. The Export button will export the File Download Name Format Template details in the form .xlsx format. The Copy button will copy all the details of the table.

13.12.3 Capture

13.12.3.1 Log Manager Service

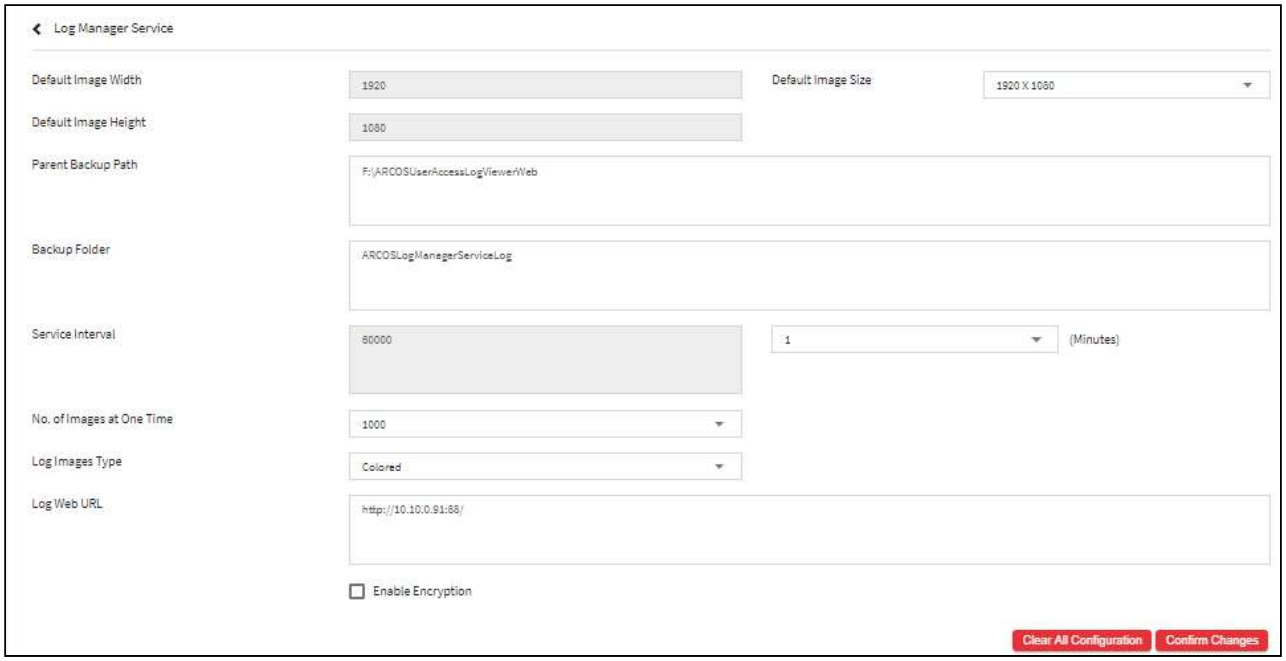
Log Manager Service configuration allows ARCON PAM to capture images during session recording for any GUI based access taken by User. The images are transferred to Database Server on a real-time basis. This is a one-time configuration wherein the width and height of the image, path of storage server to retain logs are configured as per the company's policy.

⚠ The Administrator having **Default Configuration** and **Log Manager Service** privileges in Server's Privileges will only be able to configure Log Manager Service.

To navigate, use the following path:

Settings → Logs → Capture

1. Select the Log manager service under Capture.



The **Log Manager Service** screen contains the following fields:

Field Name	Description
Default Image Size	Select the resolution to maintain the quality of images.
Parent Backup Path	Enter the path of the backup folder, to store the recorded session images.
Backup Folder	Specify the name of the backup folder in which the logs of recorded session images are stored.
Service Interval	Once the interval is set to 1 or 2 or more minute(s) the 'ARCOS Log Manager Service' will connect the DB after that interval and empty the database and save the images in the 'Backup Folder'.
No of Images At One Time	Select the number of images you want ARCON PAM to process at one time by Log Manager Service.
Log Images Type	Select the type for log images. The valid values are: ▪ Colored ▪ Black and White ▪ Gray Scaled
Log web URL field	Specify the IP Address and Port of User Access Log Viewer hosted on the Server.
Enable Encryption checkbox	If you enable the Enable Encryption checkbox, the images are stored in an encrypted format.

2. Click **Confirm Changes** button to configure the details.

13.12.3.2 Video Log Information Configuration

Video Log Information Configuration is a form of template which is displayed at the start of the video logs. This template also appears when at the start when Images are played through Server Manager and Access Logs or when Images are downloaded from the Server Manager, or when archived videos are played or downloaded from Server

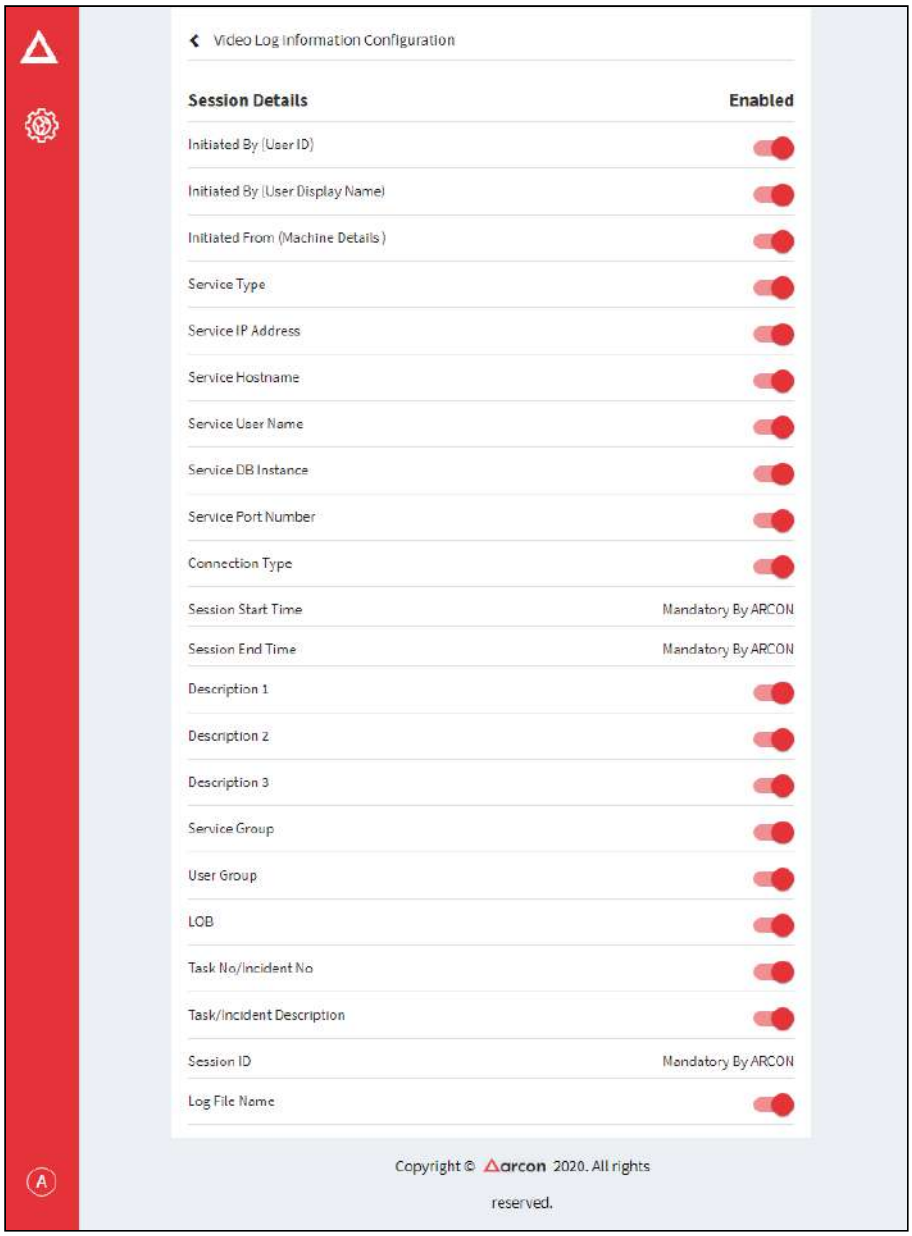
manager. Apart from that, this template is also used when we export the videos in word format from the server manager.

The configurations in this template include details such as User Id, User Name, Machine details, Service Type, Service IP, Service hostname, Service User Name, Service DB Instance, Service Port Number, Connection type, Description 1, Description 2, Description 3, Service Group, User Group, LOB, Task/Incident number, Task/Incident Description, and Log fileName. On enabling these toggle configuration, this information can be seen in the first screen of the video logs.

To navigate, use the following path:

Settings → Log → Capture

1. Select Video log Information Configuration under Capture.



2. Enabled configurations will be seen in the first screen of video logs.

13.12.3.3 Staging Log Server

Staging Log Server is used to store logs before they are transferred to Database Server. Logs are compressed and stored on this Server.

In a few organizations, the size of logs generated per day is higher and users accessing ARCON PAM are of greater volume. The bandwidth falls short for transferring logs to Database Server. In such a scenario, Log Staging Server is

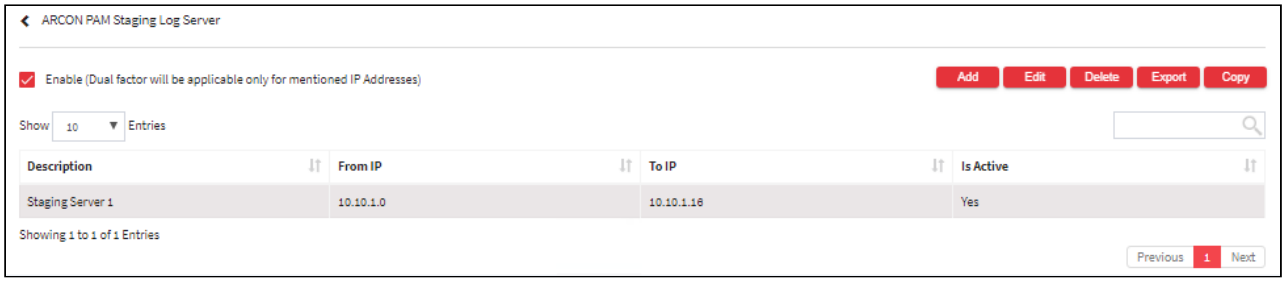
used to store logs. These logs are then transferred to Database Server in the configured time interval. The status of the logs can be monitored by hosting on URL.

⚠ The Administrator having **ARCOS Staging Log Server** privileges in Server's Privileges will only be able to configure values for Staging Log Server.

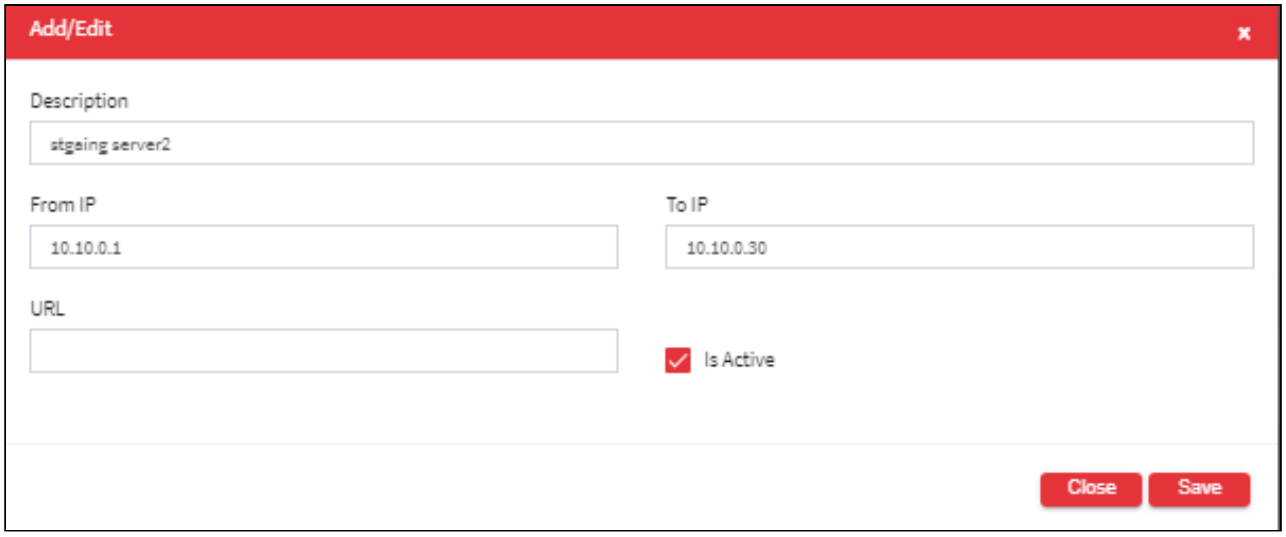
To navigate, use the following path:

Settings → Logs → Capture

1. Select the ARCON PAM Staging Log server under Capture.
2. Select **Enable (ARCON PAM Staging Log Server only for mentioned IP addresses)** checkbox to enable the configuration.



3. Select the add button to add a new Staging Log Server.

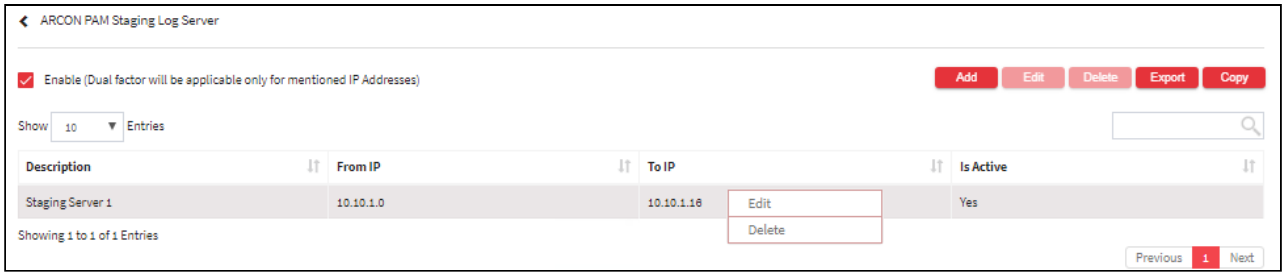


The **Staging Log Server** screen contains the following fields:

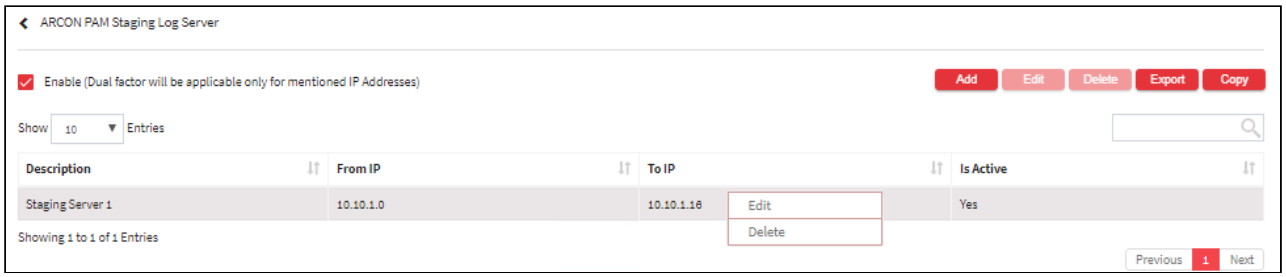
Field Name	Description
Description	Enter the description.
From IP	Enter the start IP address of the server from where log staging will start.

Field Name	Description
To IP	Enter the end IP address of the server, where the log staging will end.
URL	Enter the URL of the hosted Log Staging Server.
Is Active	To enable the configuration.

4. Enter the details and click **Save** to create a new Staging Log Server.
5. For Editing, the details of the existing ARCON PAM Staging Log Server click on the existing row and select the Edit button at the top and make the required changes. Also, you can right-click on the row and select Edit.



6. For Deleting the existing ARCON PAM Staging Log Server click on the existing row and select the Delete button at the top and make the required changes. Also, you can right-click on the row and select Delete.



7. The Export button will export all the ARCON PAM Staging Log Server details in the form .xlsx format. The Copy button will copy all the details of the table.

⚠

- It is the basic configuration for the Staging Server. When logging in from the IP range, 0.0.0.0 to 192.168.0.237, ARCON PAM captures the local IP address, MAC address, processor ID, and BIOS cell number. So, on that particular IP address, ARCON PAM will decide which server to use as a Local Staging Server or Local Log Collector.
- The From IP field refers to the local IP that is a laptop IP or desktop IP. If there is an IP range, as in “From IP and To IP”, it will use the gateway server specified in the URL field. To configure another gateway server, one can configure same server in another range or configure multiple range on the multiple gateway servers. Every gateway server will need to have the sync service installed.

13.12.3.4 Modify Service Type- Settings

Modify Service type allows the administrator to enable and disable the service types in ARCON PAM, Client Manager The disabled services will not be visible in ARCON PAM or CM. Administrators can also customize the list of service types to be listed under Command Profiler.

⚠ The Administrator having **Modify Service Type** privilege shall only be able to select service types to be displayed in ARCON PAM or CM.

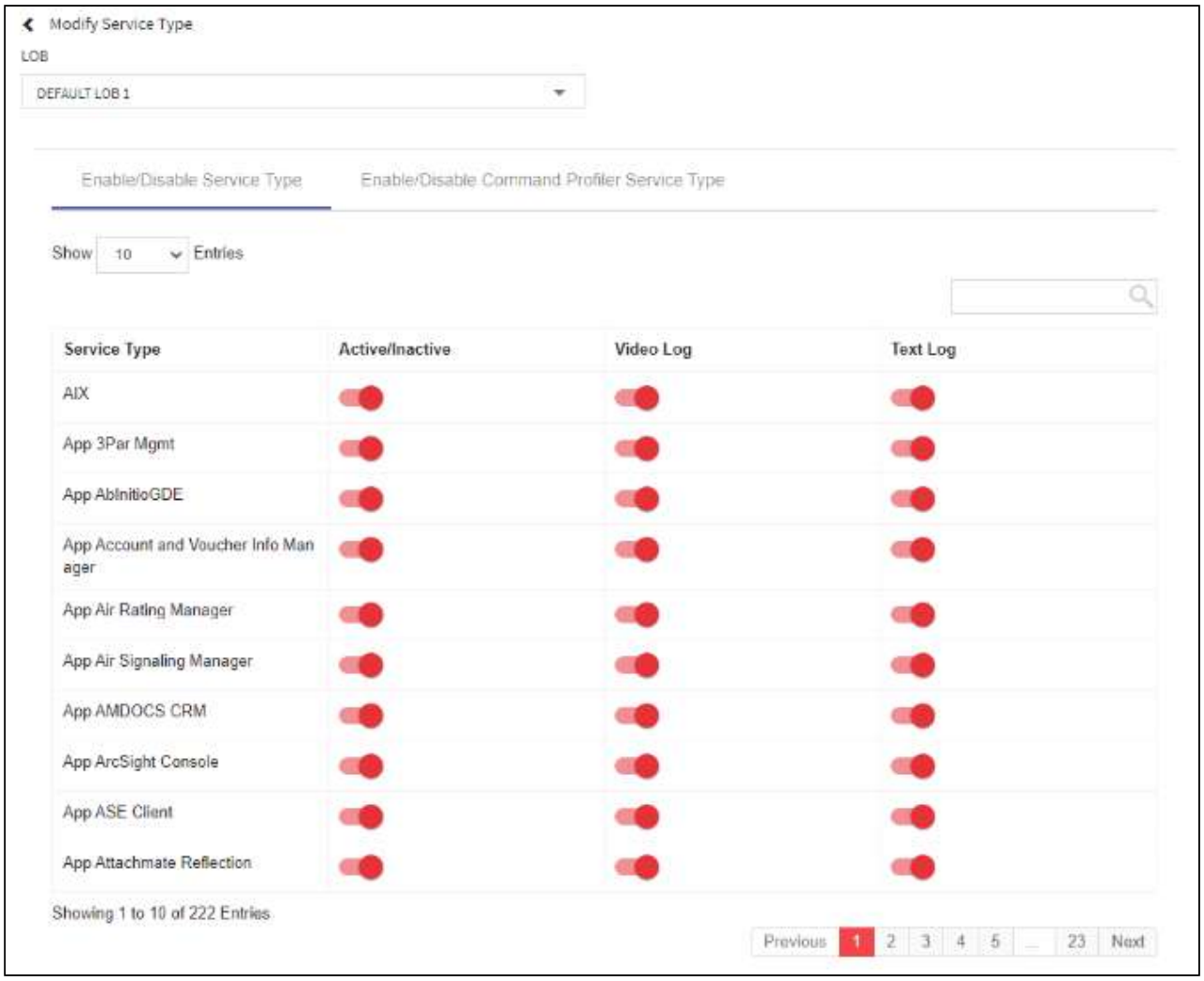
To navigate, use the following path:

Settings → Log → Capture

1. Select Modify Service Type under Capture.
2. Select the LOB.
3. Now, we have the following two tabs under this screen
    a. Enable/Disable Service Type
    b. Enable/Disable Command Profiler Service Type

Process to Enable/Disable Service Type in ARCON PAM and Client Manager:

1. Click the **Enable/Disable Service Type** tab to view the list of services.



2. The toggle configurations can be set to
    a. Activate/Inactivate a particular service
    b. Enable/Disable Video logs for services

    > ⚠ The **Enable Video Log** configuration should be enabled to enable video logs for all the service types.

    c. Enable/Disable Text logs for services

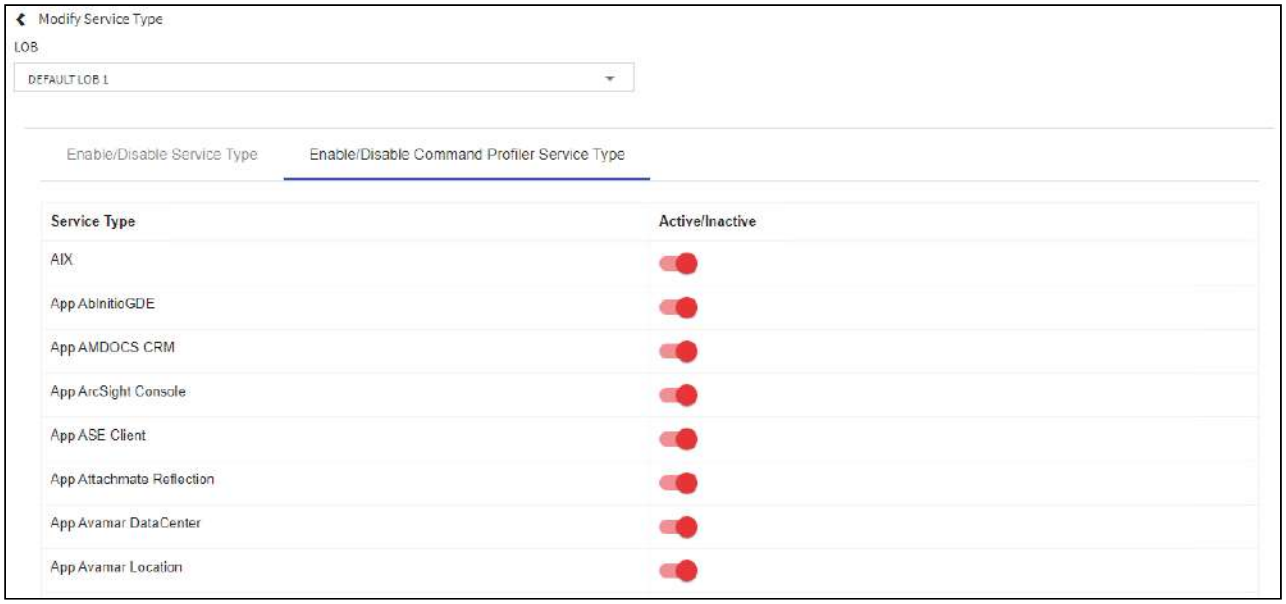
    > ⚠ The **Enable Text Log** configuration should be enabled to enable text logs for all the service types.

3. Only the enabled services will be visible in ARCON PAM and CM.

> ⓘ All the service types that are not checked in this list will not be visible in ARCON PAM and CM.

Process to Enable/Disable Command Profiler Service Type in ARCON PAM and Client Manager:

1. Click the **Enable/Disable Command Profiler Service Type** tab to view the list of services.



2. Enable the Toggle button to activate the command profiler for service types.
3. Only the selected services will be visible under the Server Manager → Manage→ Command Profiler.

13.12.3.5 Capture Configurations

To navigate, use the following path:

Settings → Logs → Capture

Field Name	Description
SSH Video Log - Is Enabled For All	**This configuration enables/disables Video Logs for SSH/Telnet based service.**
Disable	If Toggle value is 'Disabled', then it disables Video logs.
Enable	If Toggle value is 'Enabled', then it enables Video logs.
ARCON Desk Insight Video Log - Is Enabled For All	**This configuration enables/disables ARCON Desk Insight Video Log globally for all the services of Workstation being integrated into ARCON PAM.**
Disable	If Toggle value is 'Disabled', then it disables Video logs.
Enable	If Toggle value is 'Enabled', it generates Video logs.
Oracle QA (Client App) Only Video Logs - Is Enabled	**This configuration enables/disables Video Logs for Oracle QA (Client App).**

Field Name	Description
Disable	If Toggle value is 'Disabled', then it disables the feature.
Enable	If Toggle value is 'Enabled', then it enables the feature.
ARCOSRDPDB SQL Connect Timeout	**This configuration sets the time in seconds for setting up the 'timeout' threshold when connecting ARCOSRDPDB for sending logs.**
Valid Values	The valid range is 1-20.
Video Log Threading For RDP - Is Enabled	**This configuration enables/disables multithreading of Video Logs for RDP. This can be useful if connectivity is weak with ARCON PAM Server.**
Disable	If Toggle value is 'Disabled', then it disables the feature.
Enable	If Toggle value is 'Enabled', then it enables the feature.
Capture Window Activated/ Inactivated State - Is Enabled	**This configuration enables/disables Capturing of logs when Window in Active / Inactive State once the session of target Server/device is taken through ARCON PAM.** **Note: The selected window is active. If you click somewhere else, the window is inactive i.e. grayed**
Disable	If Toggle value is 'Disabled', then it disables the feature.
Enable	If Toggle value is 'Enabled', then it enables the feature.
Capture Window Minimized / Maximized State - Is Enabled	**This configuration enables/disables capturing of Window in Minimized / Maximized State.**
Disable	If Toggle value is 'Disabled', then it disables the feature.
Enable	If Toggle value is 'Enabled', then it enables the feature.
Max Duration(in days) For Log Generation	**This configuration sets the value for viewing logs. Users can view logs as per the configured days. This configured value is applicable to all logs except Service Password Status logs.**
Valid Values	The valid range is 1-180. By default, the value is 90 days.

Field Name	Description
Disable Video Logs by Server Group	**This configuration will allow to disable video logs for Server Groups.**
Disable	If Toggle value is 'Disabled', the checkbox for Disable video logs will not be displayed under the Section of Manage Groups.
Enable	If Toggle value is 'Enabled', the checkbox for Disable video logs will be displayed under the Section of Manage Groups.
ARCON QA Video Log Enable	**This configuration enables/disables video logs for all QA connectors.**
Disable	If Toggle value is 'Disabled', then this feature is disabled.
Enable	If Toggle value is 'Enabled', then this feature is enabled.
Use RDPDB For Image Log	**This configuration enables/disables the saving of pictures in the RDP database.**
Disable	If Toggle value is 'Disabled', then images will be saved directly into a folder.
Enable	If Toggle value is 'Enabled', then images will be saved in the RDP Database.
Enable SSM	**Used to enable Smart Session Monitoring for Connectors.**
Disable	If Toggle value is 'Disabled', then this feature is disabled.
Enable	If Toggle value is 'Enabled', then this feature is enabled.
Command capture format for clipboard data in Command logs.	
Disable	
Enable	
Use WebDT for Web API Image Capture	
Disable	
Enable	

Field Name	Description
New Image encryption (Applicable incase of NO RDPDB Database)	
Valid Value	The valid values are below Old encryption- Image Encoding New encryption- AES 256 Encryption New Encryption with Tamperproof

13.12.4 Archival Service

This section helps you to with configurations in Archival Services of logs.
To navigate, use the following path:

Settings → Logs → Archival Service

Field Name	Description
ARCOS Log Archiver Service - Is Enabled	**This configuration enables/disables the Log Archiving Operation (start/stop).**
Disable	If Toggle value is 'Disabled', then this feature is disabled.
Enable	If Toggle value is 'Enabled', then this feature is enabled.
ARCOS Log Archiver Service - Is Delete Service Log (If Archive Success)	**This configuration enables/disables the deletion of Archived Logs from the Server.**
Disable	If Toggle value is 'Disabled', then it disables the deletion of logs.
Enable	If Toggle value is 'Enabled', then it enables the deletion of logs.
ARCOS Log Archiver Service - Archive Older Than Hours	**Configuration sets the number of hours for which the logs will be retained. Logs prior to set hours will be archived into video logs (with higher compression).**
Valid Values	It ranges from 0-99999. Recommended Value: 3 hours.
Rule Based Video Archival	**Enables or Disables Rule Based Video Archival.** **Once the Rule based configuration is enabled, you cannot revert back the configuration.**

Field Name	Description
Disable	If Toggle value is 'Disabled', then this feature is disabled.
Enable	If Toggle value is 'Enabled', then this feature is enabled.

13.12.5 Scheduler

A scheduler is a program that schedules or arranges operations into an appropriate sequence. It carries out the planned scheduled activity for a proposed objective, especially with reference to the sequence of and time allotted for each operation necessary to its completion. Schedulers are often implemented to allow multiple users to share system resources effectively, or to achieve the quality of service. Therefore, it helps in monitoring the performance and necessary reports are generated based on the scheduled activity.

This section includes the following topics:

- Scheduler Master
- Schedule Password Envelope
- Schedule Reports

13.12.5.1 Schedule Master

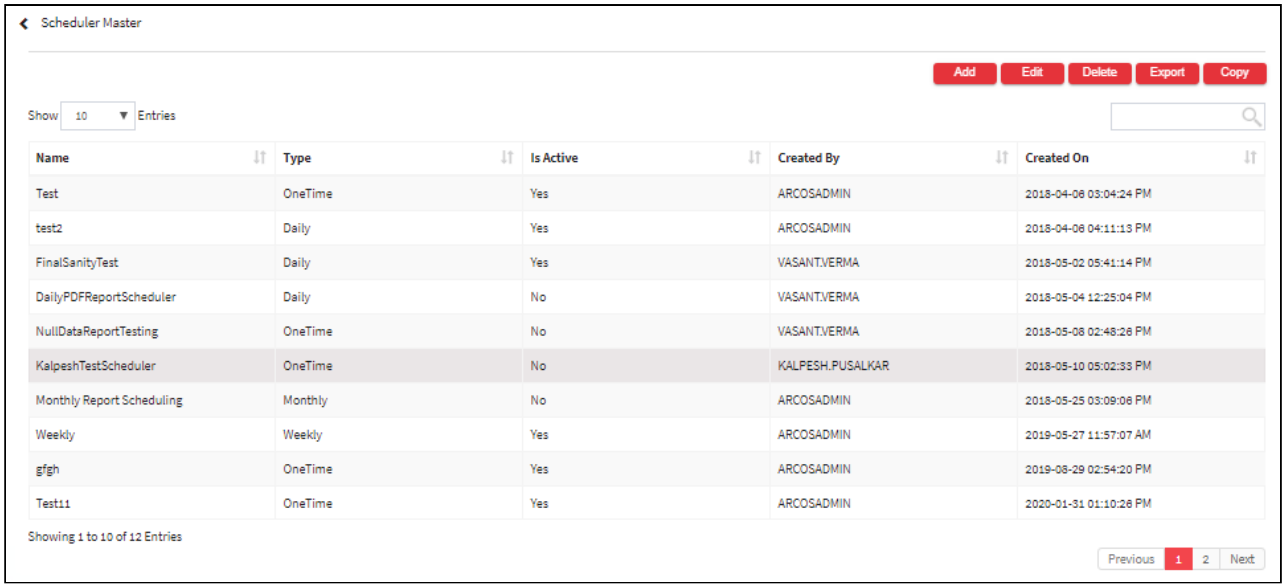
This section helps you to configure a scheduler master. The Administrator can define multiple schedulers as per the requirement. The appropriate name for the scheduler, duration, and span details are provided while defining a scheduler. In addition, you can modify the details of a configured scheduler.

⚠ The Administrator having **Scheduler Master** privilege will only be able to configure a scheduler.

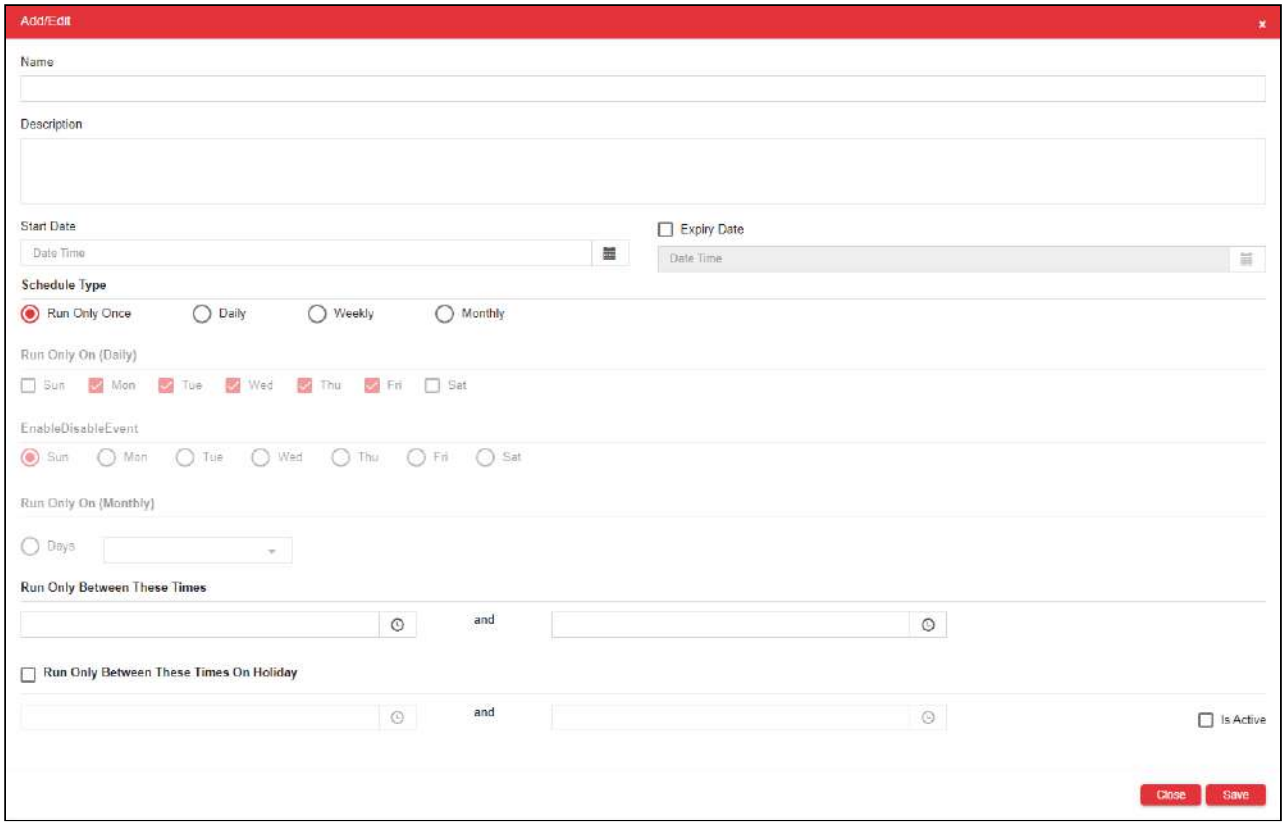
To navigate, use the following path:

Settings → Logs → Scheduler

1. Select Scheduler Master under Scheduler.



2. Select the Add button to add a new Scheduler Master

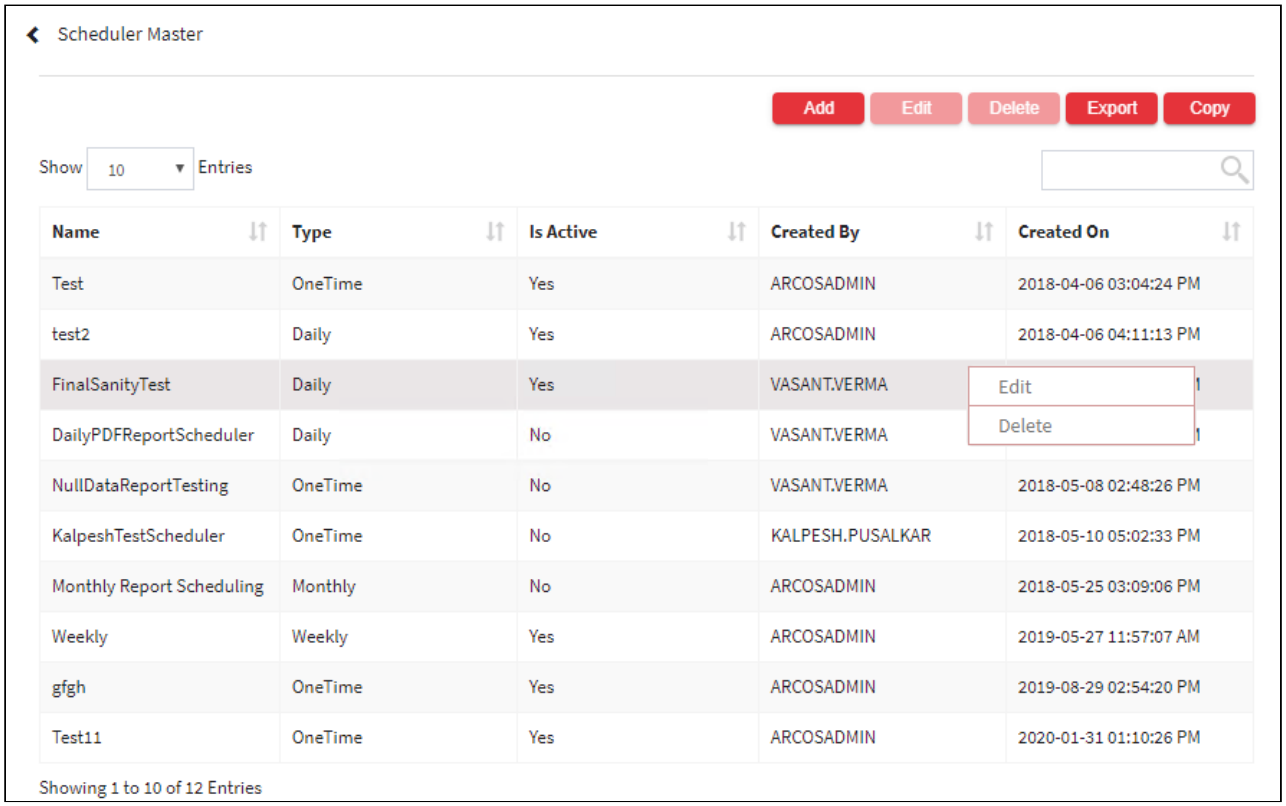


3. The **Scheduler Master Configure** screen contains the following fields:

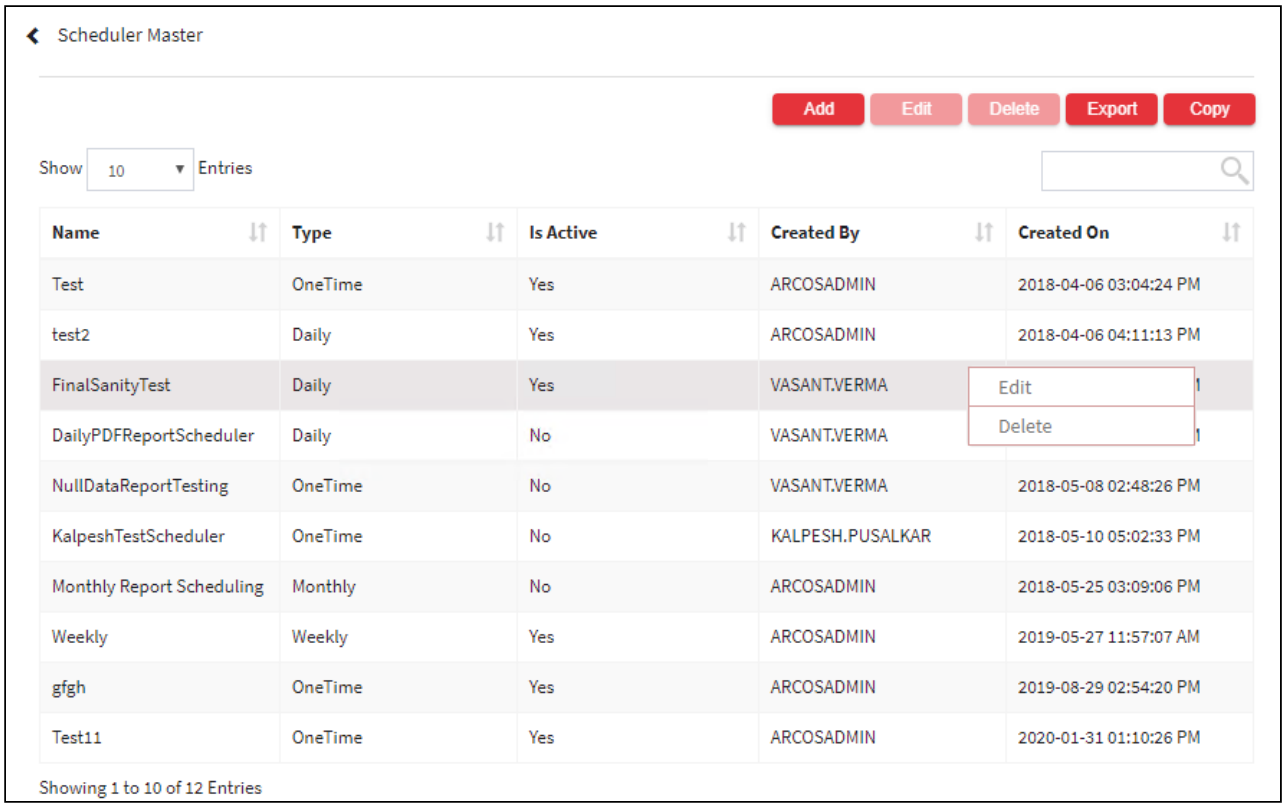
Field Name	Description
Name	Enter name for the scheduler.
Description	Enter short description for the scheduler.
Start Time	Select the date and time for the scheduler to start processing.
Expire	Select the end time for the scheduler to stop processing. ⚠ Expire Time field when set will stop sending emails of Scheduled Password Envelope and Scheduled Reports to the user/admin after the set period.
Schedule Type	Used to select the schedule type for the scheduler. The valid values are: ▪ **Run only once:** Enables the scheduler to run only once. ▪ **Daily:** Enables the scheduler to run on a daily basis. ▪ **Weekly:** Enables the scheduler to run on a weekly basis. ▪ **Monthly:** Enables the scheduler to run on a monthly basis.

Field Name	Description
Run Only On (Daily)	Select the number of days in a Week required for a scheduler to run, to fetch reports or password envelope ⚠ This field is enabled if you select the **Schedule Type** as **Daily.**
Run Only On (Weekly)	Select a day in a Week required for a scheduler to run, to fetch reports or password envelope. ⚠ This field is enabled if you select the **Schedule Type** as **Weekly.**
Run Only On (Monthly)	Select the number of days in months required for a scheduler to run, to fetch reports or password envelope. ⚠ This field is enabled if you select the **Schedule Type** as **Monthly.**
Run Only Between These Times	Select time to enable the scheduler to run on a timely basis.
Is Active	Enable the scheduler to start processing.

4. Enter the details and click **Save** button to create a new scheduler master.
5. For Editing, the details of the existing scheduler master click on the existing row and select the Edit button at the top and make the required changes. Also, you can right-click on the domain and select Edit.



6. For Deleting the existing scheduler master click on the existing row and select the Delete button at the top and make the required changes. Also, you can right-click on the domain and select Delete.



Name	Type	Is Active	Created By	Created On
Test	OneTime	Yes	ARCOSADMIN	2018-04-06 03:04:24 PM
test2	Daily	Yes	ARCOSADMIN	2018-04-06 04:11:13 PM
FinalSanityTest	Daily	Yes	VASANT.VERMA	
DailyPDFReportScheduler	Daily	No	VASANT.VERMA	
NullDataReportTesting	OneTime	No	VASANT.VERMA	2018-05-08 02:48:26 PM
KalpeshTestScheduler	OneTime	No	KALPESH.PUSALKAR	2018-05-10 05:02:33 PM
Monthly Report Scheduling	Monthly	No	ARCOSADMIN	2018-05-25 03:09:06 PM
Weekly	Weekly	Yes	ARCOSADMIN	2019-05-27 11:57:07 AM
gfgh	OneTime	Yes	ARCOSADMIN	2019-08-29 02:54:20 PM
Test11	OneTime	Yes	ARCOSADMIN	2020-01-31 01:10:26 PM

7. The Export button will export all the scheduler master details in the form .xlsx format. The Copy button will copy all the details of the table.

- You can filter details displayed in the grid view by entering the required value in the respective column filter displayed above the header.
- To generate a Unique Password Envelope for similar Domain ID's, the **Envelope By Domain IDs** configuration should be **enabled**. This configuration is used to generate and send a unique password envelope for similar Domain IDs based on the scheduled time in **Schedule Master**.

13.12.5.2 Schedule Password Envelopes

A password Envelope is an envelope that stores the password of service in an encrypted format which will help the password to be secure. This section helps you to configure the scheduler for a password envelope. The password envelope scheduler once configured, will help the User to receive passwords in encrypted format as envelope emails to their configured email IDs.

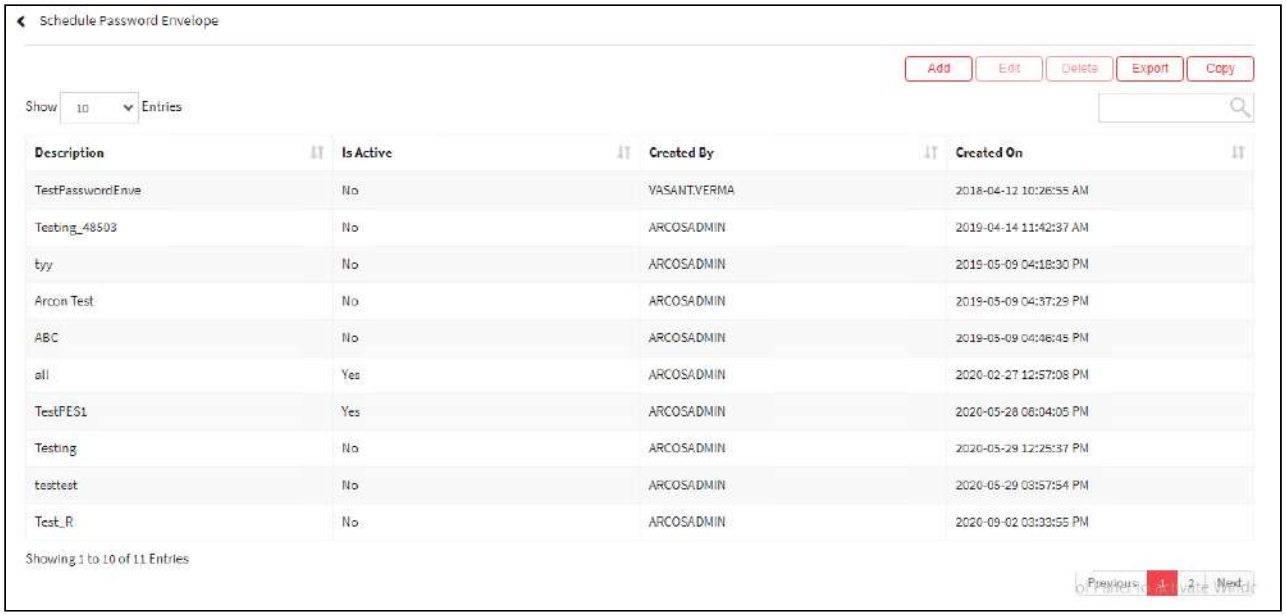
- The Administrator having **Scheduler Master** and **Schedule Password Envelope** privileges in Server's Privileges will only be able to configure the scheduler for password envelope.

- Once the scheduler is configured in **Scheduler Master**, you need to then schedule a password envelope.
- To generate a Unique Password Envelope for similar Domain ID's, the **Envelope By Domain IDs** configuration should be enabled. This configuration is used to generate and send a unique password envelope for similar Domain IDs based on the scheduled time in **Schedule Master**.

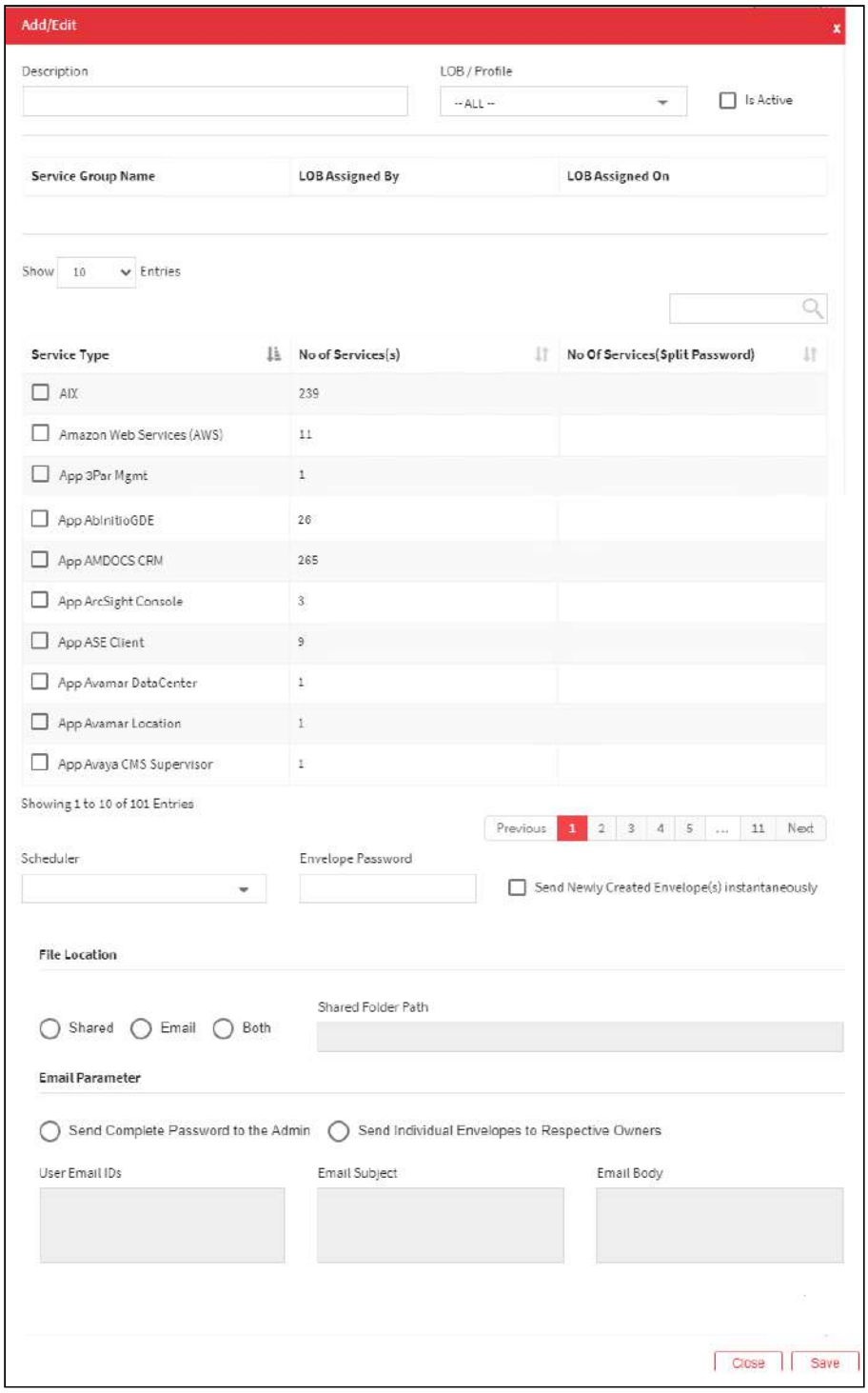
To navigate, use the following path:

Settings → Logs → Scheduler

1. Select Schedule Password Envelope under Scheduler.



2. Select the Add button to add a new Password Envelope.

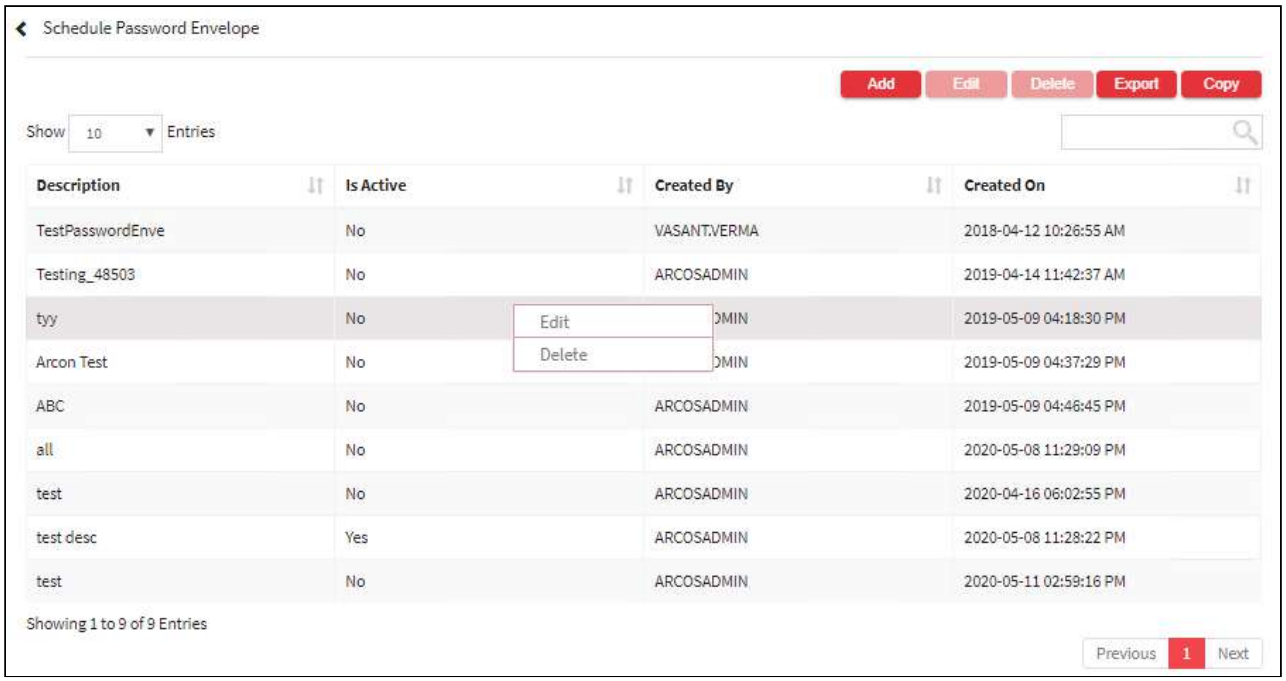


The **Schedule Password Envelope** screen contains the following fields:

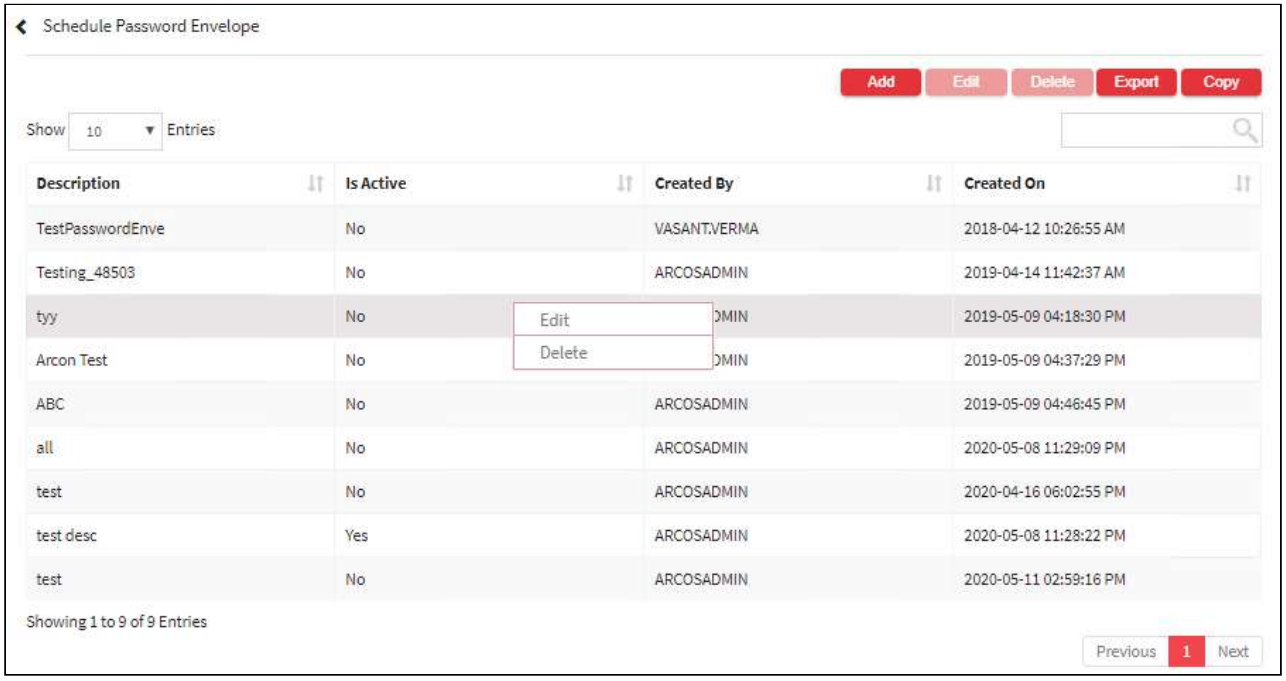
Field Name	Description
Description	Specify a short description for the specific scheduler.
LOB/Profile	Select the LOB. On selecting LOB, the Service Group Details are displayed in the grid. On selecting Service Group, the Service Types are displayed.

Is Active	Enable the scheduler to start processing.
Scheduler	Select the scheduler. ⚠ The schedulers configured under **Scheduler Master** will be available for selection.
Envelope Password	Specify the envelope password. ⚠ You can enter a minimum of 12 character password.
Send Newly Created Envelope(s) Instantaneously	Indicates that when a new connection password is changed, the password envelope of that connection will be mailed to their configured email IDs. ⚠ For Instantaneous Password Envelope, the email Subject in Schedule Password Envelope should contain IP Address and Username of Service. Any alert notification sent via email for Instantaneous Password Envelope will have<IP, Username>which will help the Administrator to identify the envelope is for which service based on the subject Line i.e, <IP, Username>.
File Location	
File Location (Select)	Select the radio button and accordingly enter the details of the path to the folder. ▪ Shared ▪ Email ▪ Both
Shared Folder Path	Enter the path of the shared folder to save the file.
Email Parameters	
Email Parameters	Select the radio button: ▪ Send Complete Password to the Admin: The password envelope is sent to the owner whose email Id is configured below. ▪ Send Individual Envelopes to Respective Owners: For services with split passwords, envelopes are sent to individual owners.
User Email IDs	Specify the email id of the user to whom the email has to be sent. ⚠ Multiple Email IDs can be added separated by semi-colon or comma.
Email Subject	Specify the subject for the email.
Email Body	Specify the description for the mail

3. Enter the details and click **Save** button to create a new Schedule Password Envelope.
4. For Editing the details of the existing Schedule Password Envelope click on the existing row and select the Edit button at the top and make the required changes. Also, you can right-click on the domain and select Edit.



5. For Deleting the existing Schedule Password Envelope click on the existing row and select the Delete button at the top and make the required changes. Also, you can right-click on the domain and select Delete.



6. The Export button will export all the Schedule Password Envelope details in the form .xlsx format. The Copy button will copy all the details of the table.

- You can save the password envelope in a shared drive.
- You can filter details displayed in the grid view by entering the required value in the respective column filter displayed above the header.
- If the Password Envelope Protected File configuration is enabled, then the password envelope will be sent in .zip format whereas if it is disabled then it will be sent in .txt format.

13.12.5.3 Schedule Reports

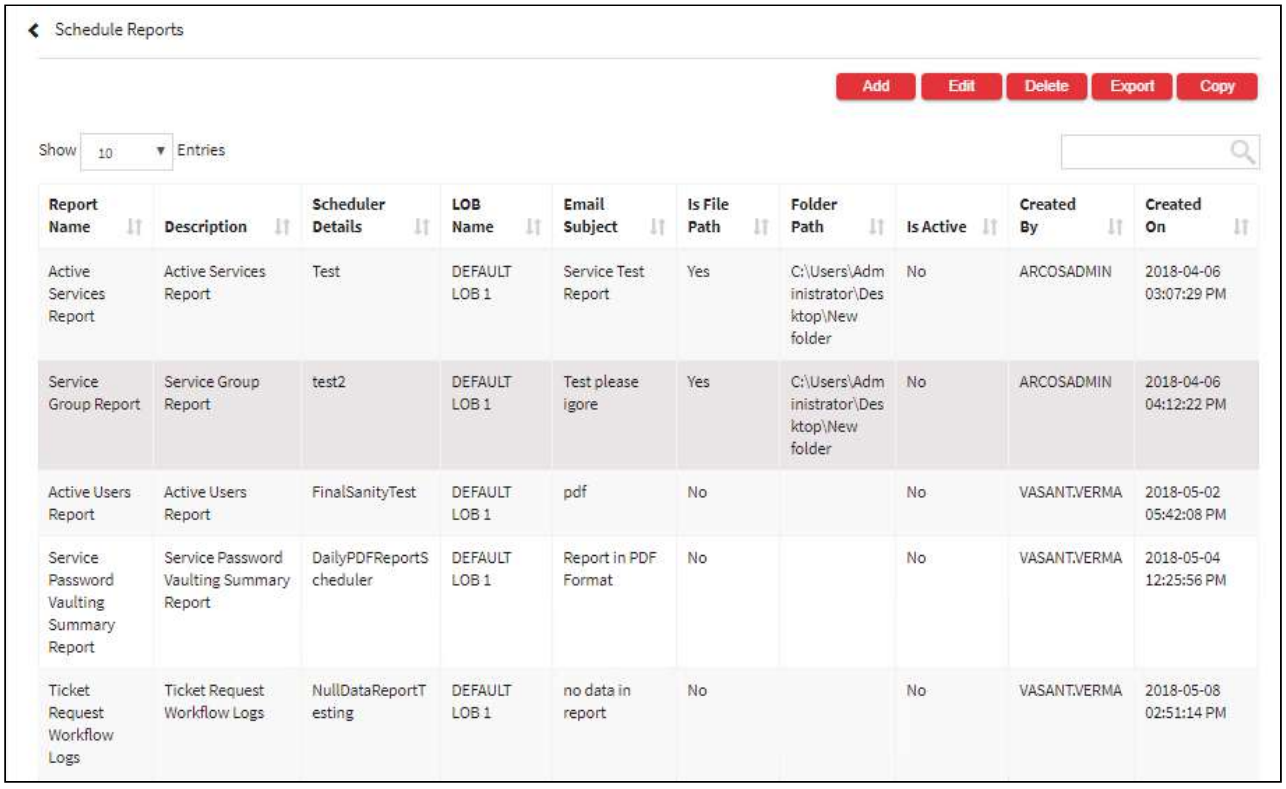
This section helps you to schedule various types of reports. It will help the User to receive generated reports through email on scheduled date/time intervals. A Schedule Report is based on the configured Scheduler master. So prior to scheduling reports it is mandatory to configure Scheduler Master.

- The Administrator having **Scheduler Master** and **Schedule Reports** privileges in Server's Privileges will only be able to configure scheduler for reports.
- Once the scheduler is configured in **Scheduler Master**, you need to then schedule reports.

To navigate, use the following path:

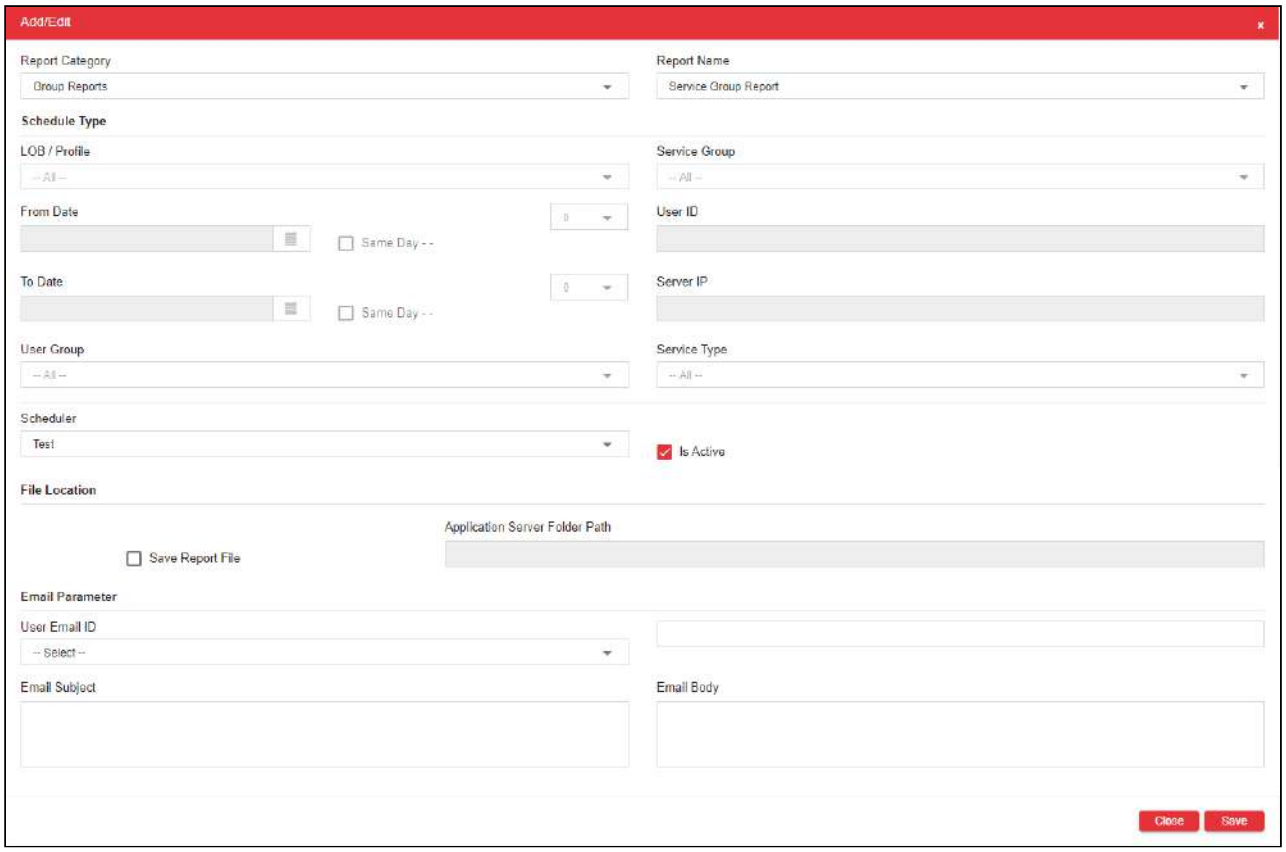
Settings → Logs → Scheduler

1. Select Schedule Reports under Scheduler.



Report Name	Description	Scheduler Details	LOB Name	Email Subject	Is File Path	Folder Path	Is Active	Created By	Created On
Active Services Report	Active Services Report	Test	DEFAULT LOB 1	Service Test Report	Yes	C:\Users\Administrator\Desktop\New folder	No	ARCOSADMIN	2018-04-06 03:07:29 PM
Service Group Report	Service Group Report	test2	DEFAULT LOB 1	Test please igore	Yes	C:\Users\Administrator\Desktop\New folder	No	ARCOSADMIN	2018-04-06 04:12:22 PM
Active Users Report	Active Users Report	FinalSanityTest	DEFAULT LOB 1	pdf	No		No	VASANT.VERMA	2018-05-02 05:42:08 PM
Service Password Vaulting Summary Report	Service Password Vaulting Summary Report	DailyPDFReportScheduler	DEFAULT LOB 1	Report in PDF Format	No		No	VASANT.VERMA	2018-05-04 12:25:56 PM
Ticket Request Workflow Logs	Ticket Request Workflow Logs	NullDataReportTesting	DEFAULT LOB 1	no data in report	No		No	VASANT.VERMA	2018-05-08 02:51:14 PM

2. Select the Add button to add a new Schedule Report

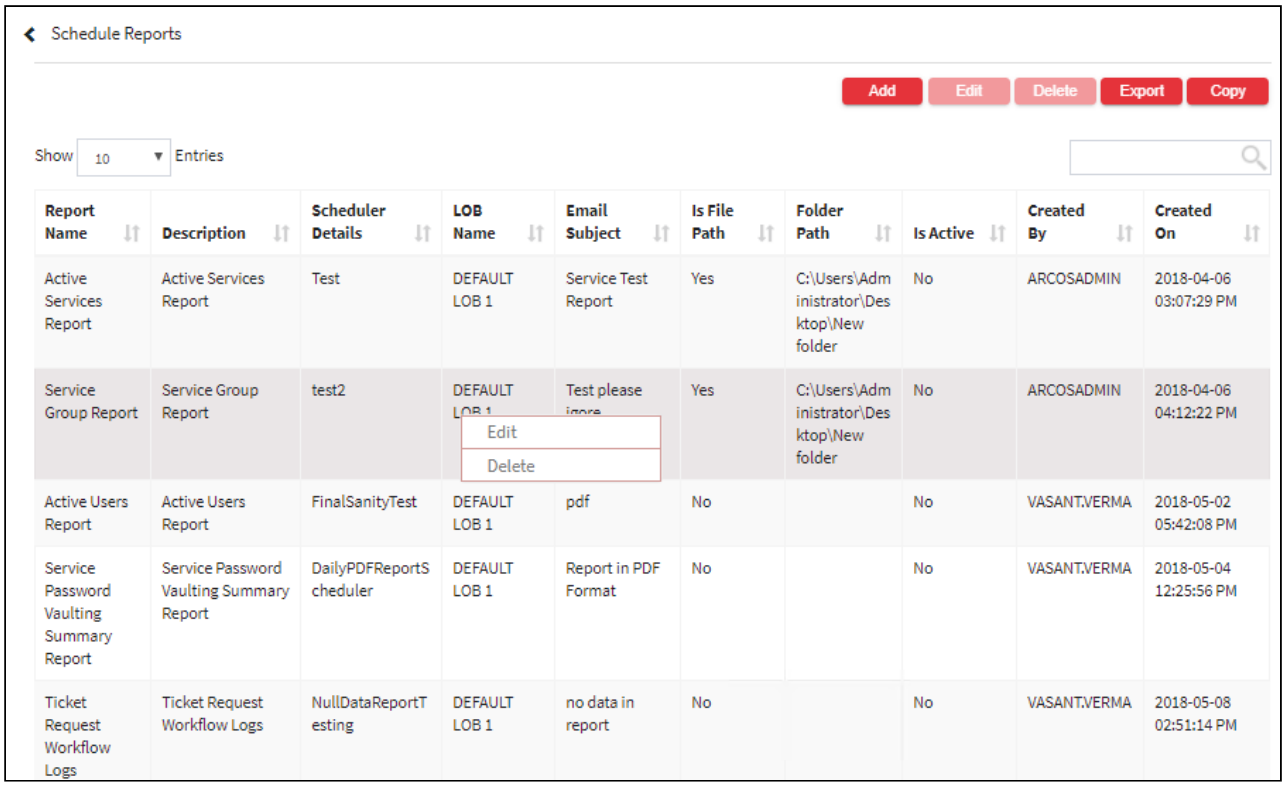


The **Schedule Reports** screen contains the following fields:

Field Name	Description
Report Category	Select the category of the report.
Report Name	Displays the list of reports. ⚠ The data in this field is auto-populated based on the Report Category selected.
Report Parameters	
LOB/Profile	Select the LOB. ⚠ This field is enabled or disabled on the **Master Report** selected.
From Date	Select the start date to fetch reports. ⚠ This field is enabled or disabled on the **Master Report** selected.
To Date	Select the end date for the reports to be fetched. ⚠ This field is enabled or disabled on the **Master Report** selected.

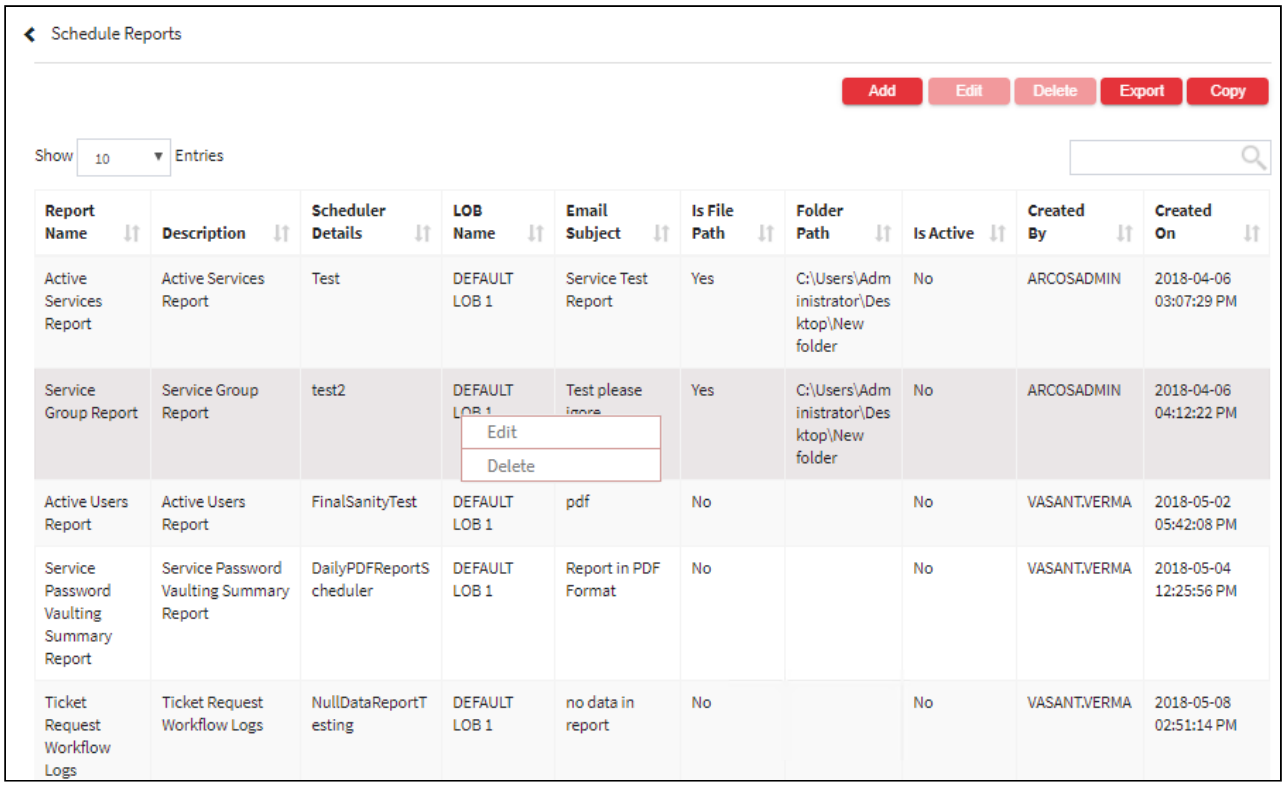
User Group	Select the user group. ⚠ This field is enabled or disabled on the **Master Report** selected.
Service Group	Select the service group. ⚠ This field is enabled or disabled on the **Master Report** selected.
User ID	Enter the user ID. ⚠ This field is enabled or disabled on the **Master Report** selected.
Server IP	Enter the server IP. ⚠ This field is enabled or disabled on the **Master Report** selected.
Service Type	Select the type of service. ⚠ This field is enabled or disabled on the **Master Report** selected.
Scheduler	Select the corresponding scheduler master.
Is Active	Enable the scheduler.
File Location	
Save Report File	Select to save the scheduled report.
Application Server Folder Path	Enter the path of the application server to save the file.
Email Parameters	
User Email ID	Specify the email id of the user to whom the email is to be sent.
Email Subject	Specify the subject for the email.
Email Body	Specify the description for the mail.

3. Enter the details and click **Save** button. A window pops up with the following message: **New Report Scheduled**
4. For Editing the details of the existing scheduled report click on the existing row and select the Edit button at the top and make the required changes. Also, you can right-click on the domain and select Edit.



Report Name	Description	Scheduler Details	LOB Name	Email Subject	Is File Path	Folder Path	Is Active	Created By	Created On
Active Services Report	Active Services Report	Test	DEFAULT LOB 1	Service Test Report	Yes	C:\Users\Administrator\Desktop\New folder	No	ARCOSADMIN	2018-04-06 03:07:29 PM
Service Group Report	Service Group Report	test2	DEFAULT LOB 1	Test please ignore	Yes	C:\Users\Administrator\Desktop\New folder	No	ARCOSADMIN	2018-04-06 04:12:22 PM
Active Users Report	Active Users Report	FinalSanityTest	DEFAULT LOB 1	pdf	No		No	VASANT.VERMA	2018-05-02 05:42:08 PM
Service Password Vaulting Summary Report	Service Password Vaulting Summary Report	DailyPDFReportScheduler	DEFAULT LOB 1	Report in PDF Format	No		No	VASANT.VERMA	2018-05-04 12:25:56 PM
Ticket Request Workflow Logs	Ticket Request Workflow Logs	NullDataReportTesting	DEFAULT LOB 1	no data in report	No		No	VASANT.VERMA	2018-05-08 02:51:14 PM

5. For Deleting the existing scheduled report click on the existing row and select the Delete button at the top and make the required changes. Also, you can right-click on the domain and select Delete.



Report Name	Description	Scheduler Details	LOB Name	Email Subject	Is File Path	Folder Path	Is Active	Created By	Created On
Active Services Report	Active Services Report	Test	DEFAULT LOB 1	Service Test Report	Yes	C:\Users\Administrator\Desktop\New folder	No	ARCOSADMIN	2018-04-06 03:07:29 PM
Service Group Report	Service Group Report	test2	DEFAULT LOB 1	Test please ignore	Yes	C:\Users\Administrator\Desktop\New folder	No	ARCOSADMIN	2018-04-06 04:12:22 PM
Active Users Report	Active Users Report	FinalSanityTest	DEFAULT LOB 1	pdf	No		No	VASANT.VERMA	2018-05-02 05:42:08 PM
Service Password Vaulting Summary Report	Service Password Vaulting Summary Report	DailyPDFReportScheduler	DEFAULT LOB 1	Report in PDF Format	No		No	VASANT.VERMA	2018-05-04 12:25:56 PM
Ticket Request Workflow Logs	Ticket Request Workflow Logs	NullDataReportTesting	DEFAULT LOB 1	no data in report	No		No	VASANT.VERMA	2018-05-08 02:51:14 PM

6. The Export button will export all the scheduled report details in the form .xlsx format. The Copy button will copy all the details of the table.

- You can filter details displayed in the grid view by entering the required value in respective column filter displayed above header.
- The file naming convention for reports where the **LOB** filter is enabled will be Report name_LOB name_Timestamp.
- The reports configured using **Weekly** Schedule Type will be received on configured day containing the last seven days data.

13.12.5.4 Scheduler Configurations

To navigate, use the following path:

Settings → Logs → Scheduler

Field Name	Description
Show ServiceType, Service Group & UserID Filters In ACMO.ViewAccessLogs	**This configuration enables/disables availability of Service Type, Service Group, and UserID filters for selection in CM > View Access Logs tab.**
Disable	If Toggle value is 'Disabled', then it disables the availability of these options.
Enable	If Toggle value is 'Enabled', then it enables the availability of these options.

Field Name	Description
Exclude Inactive Or Disabled Users From Reports - Is Enabled	**This configuration sets whether Inactive and Disabled Users are to be excluded from Idle Users and User Last Logon reports.**
Disable	If Toggle value is 'Disabled', then it includes Users.
Enable	If Toggle value is 'Enabled', then it excludes Users.
Service ID for Dashboard Widget	**Based on this configuration, a list of Service details accessed by User are displayed in Services Currently Being Accessed widget (Client Manager > Dashboard > Services Currently Being Accessed > More Info):** **The list will be displayed based on the following two scenarios:** • **If you configure value as service username in this configuration then details of services accessed from Client Manager with configured username will be displayed.** • **If you do not configure any value in this configuration then details of all services accessed from the Client Manager will be displayed.**
Valid Values	Service Username
Generate Envelope By Domain IDs	**This configuration is used to generate and send a unique password envelope for similar Domain IDs based on the scheduled time in Schedule Master.**
Disable	If Toggle value is 'Disabled', then this feature is disabled.
Enable	If Toggle value is 'Enabled', then this feature is enabled.

13.13 Network/Connection

13.13.1 Gateway

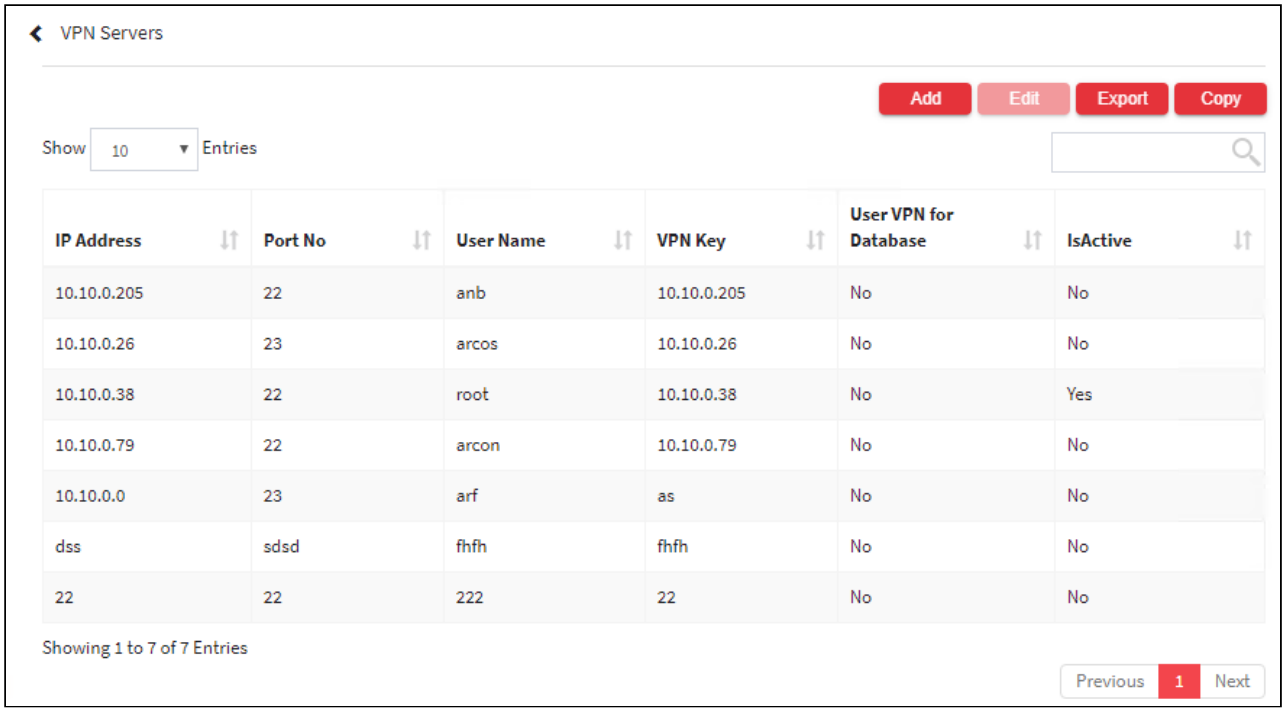
13.13.1.1 VPN Servers

VPN Servers are Secure Gateway Server (SGS) for ARCON PAM. If VPN Server is configured in ARCON PAM, connection is invoked from User's workstation to SGS and then from SGS to the target server/devices for SSO or password change on the target device. If the VPN server is not configured, then the connection is established directly from the User's machine to the Target Device. The connection from the User workstation to the secured gateway server is established through an AES 256 bit with an encrypted tunnel on a secured port, making the connection more secure. In case of an organization, when there is a Firewall in use, a port needs to be open from a particular local machine to a remote machine (it may be any server) which is on the other side of the Firewall for communication. In this case, there should be a VPN Server whose credentials are stored in an ARCON PAM Server.

⚠ The Administrator having **VPN Server** privileges in Server's Privileges will only be able to configure the VPN server.

To navigate, use the following path:
Settings → Network/Connection → Gateway

1. Select VPN Server service under Gateway.



2. For adding a new VPN server select the Add button. Click Save after adding the details.

The **VPN Server** screen contains the following fields:

Field Name	Description
IP Address	Enter the IP address of the VPN Server.

Field Name	Description
Port No	Enter the port number.
User Name	Enter the user name of the VPN Server.
Password	Enter the password of VPN Server
VPN Key	Enter key for identification of service. The default value is **ARCOS**.
Use VPN For Database	In ARCON PAM the session recording is sent from user's workstation to database in the following three ways: ▪ Directly to Database (PVSL - Password Vault Session Logging) on a set port ▪ Via Application Server (EPAM - Enterprise Privileged Account Management) to PVSL using port 443 ▪ Via Secure Gateway Server (SGS) to PVSL using port 22 – for enabling this 'Use VPN for Database' is checked. ⚠ It is enabled when the database is on the other side of the Firewall and is accessed from a local machine that is inside the boundary of the firewall.
Is Active	Enable the configuration. ⚠ The status is active for VPN Server once enabled. If disabled the server will not be used in LOB to which it is mapped.

3. The Export button will export all the VPN server details in the form .xlsx format. The Copy button will copy all the details of the table.

13.13.1.2 Gateway Configurations

To navigate, use the following path:
Settings → Network/Connection → Gateway

Field Name	Description
ARCON VPN Client Version	**This configuration sets the Version of internal VPN.** **There are multiple versions of internal VPN's, one of which can be used to connect to destination servers. Depending on the architecture, User selects the appropriate VPN type.**
Valid Values	It ranges from 1-4.
VPN For ARCON Desk Insight (RDP) - Is Enabled	**This configuration enables/disables VPN for ARCON Desk Insight (RDP).**
Disable	If Toggle value is 'Disabled', then it disables VPN for ARCON Desk Insight (RDP).
Enable	If Toggle value is 'Enabled', then it enables VPN for ARCON Desk Insight (RDP).

Field Name	Description
ARCON VPN Client Version (For SSH, Telnet)	**This configuration sets the Version of internal VPN for SSH and Telnet based services.** **Multiple versions of internal VPN's can be used to connect to SSH destination servers. Depending on the architecture, user selects the appropriate VPN type.**
Valid Values	It ranges from 1-4.
ARCON VPN Client Version (For SFTP, FTP)	This configuration sets the Version of internal VPN for SFTP and FTP only. There are multiple versions of internal VPN's, one of which can be used to connect to destination servers for SFTP and FTP for Linux. Depending on the architecture user selects the appropriate VPN type.
Valid Values	It ranges from 1-4.
ARCOS Compro Secure Gateway Is Enable	This configuration helps you to enable/disable SHA-2 enabled gateways. Secure Gateway supports following Ciphers: • Key Exchange Method ▪ diffie-hellman-group-exchange-sha256 ▪ diffie-hellman-group-exchange-sha1 ▪ diffie-hellman-group14-sha1 ▪ diffie-hellman-group1-sha1 • Message Authentication Code (MAC) algorithms: ▪ hmac-md5 ▪ hmac-md5-96 ▪ hmac-sha1 ▪ hmac-sha1-96 ▪ hmac-sha2-256 ▪ hmac-sha2-256-96 ▪ hmac-sha2-512 ▪ hmac-sha2-512-96 ▪ hmac-ripemd160 ▪ hmac-ripemd160@openssh.com
Disable	If Toggle value is 'Disabled', then it disables SHA-2 enabled gateways.
Enabled	If Toggle value is 'Enabled', then it enables SHA-2 enabled gateways.

13.13.2 AGW

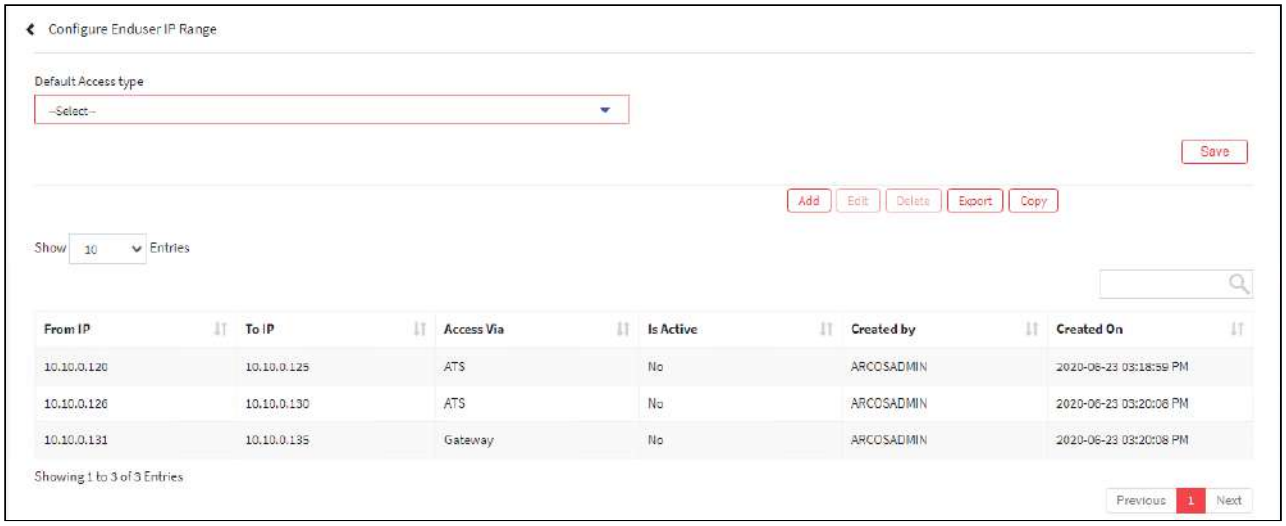
13.13.2.1 Configure Enduser IP Range

This Enduser IP Range configuration allows the selected endusers to connect to the target server at User level. Since the connection is set at User level, any services mapped with that particular User ID will know how the connection will take place i.e via AGW, Gateway, or Direct.

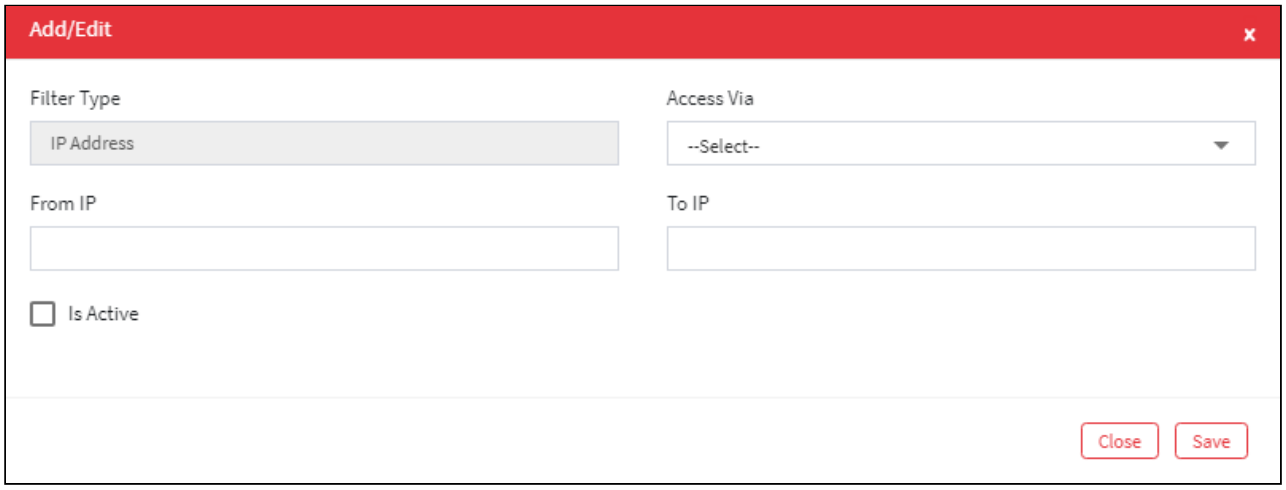
To navigate, use the following path:

Settings → Network/Connection → AGW

1. Select Configure Enduser IP Range under AGW.



2. Select the add button to configure a new **Enduser IP range**.

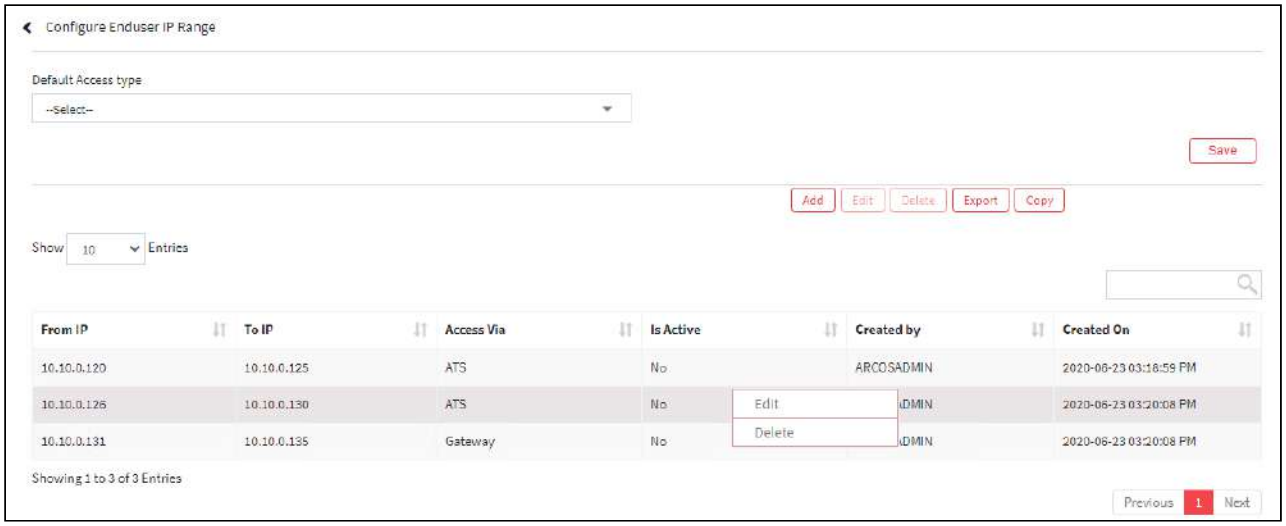


The **Configure Enduser IP range** screen contains the following fields:

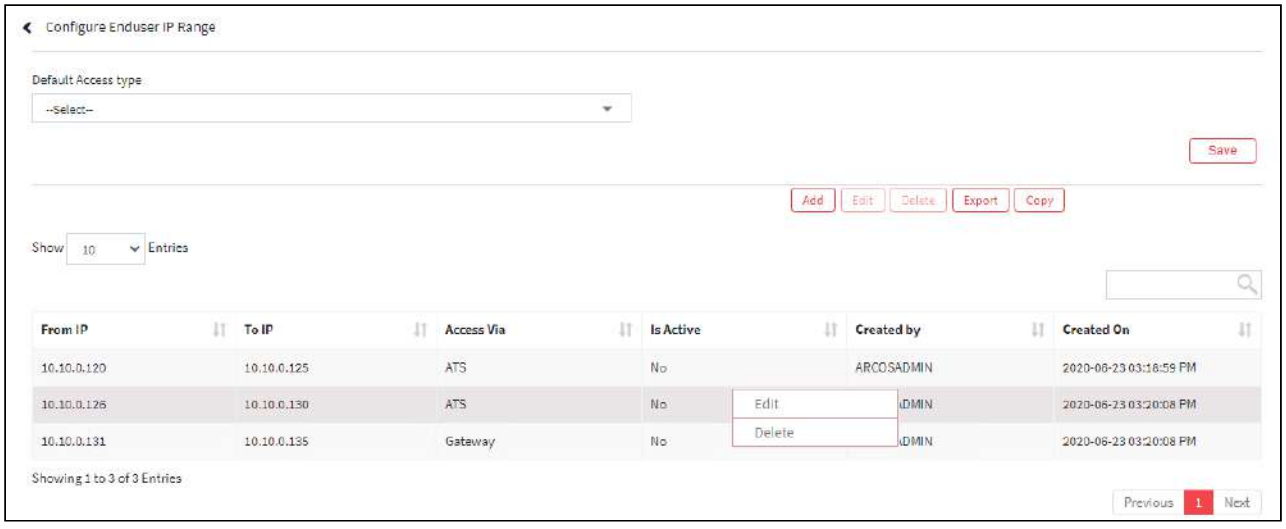
Field Name	Description
Access Via	The User is routed via ▪ Gateway ▪ AGW
From IP	Enter starting IP address to configure Enduser IP range.

Field Name	Description
To IP	Enter ending IP address to configure Enduser IP range.
Is Active	Click to enable the configuration.

3. Enter the details and click **Save** to Configure Enduser IP range.
4. For Editing, the details of the existing Configure Enduser IP range, Click on the existing row and select the Edit button at the top and make the required changes. Also, you can right-click on the row and select Edit.



5. For Deleting the existing Configure Enduser IP range, Click on the existing row and select the Delete button at the top and make the required changes. Also, you can right-click on the row and select Delete.



6. The Export button will export all the Configure Enduser IP range details in the form .xlsx format. The Copy button will copy all the details of the table.

13.13.2.2 AGW Configuration

To navigate, use the following path:
Settings → Network/Connection → AGW

Field Name	Description
Use AGW for Open Connection	**This configuration enables/disables the option of AGW.**
Disable	If Toggle value is 'Disabled', then the AGW icon will not be displayed in ACMO (under My Services) and users won't be able to access service sessions in ACMO through AGW.
Enable	If Toggle value is 'Enabled', then the AGW icon will be displayed next to the open connection icon in ACMO (under My Services) and users can take service sessions via AGW.
Use AGW to open Server manager	**This configuration enables/disables the configuration to open ARCON PAM Server Manager on a specific AGW Server where only PAM Admin activities can be performed.**
Disable	If Toggle value is 'Disabled', then Server Manager cannot be launched on AGW.
Enable	If Toggle value is 'Enabled', then it will map the AGW servers to ARCON PAM Server Manager.
Use User's AGW pin to connect to AGW	**This configuration enables/ disables connection to the AGW server through PAM Username**
Disable	If Toggle value is 'Disabled', hen it will connect by username which is configured in AGW configuration
Enable	If Toggle value is 'Enabled', then it will connect to the AGW server using the PAM user name.

13.14 API

In ARCON PAM, there is a Web API collection. Instead of creating the same configuration again and again, a repository of configurations is created. In the repository of configuration, one can configure a number of configuration types such as URL, description, method, API ID, user name, and password.

This section includes the following topics:

- API Configure
- 3rd Party API Notifier
- Service Creation Validator
- Registered Machine

13.14.1 API Configure

13.14.1.1 Web API Configuration

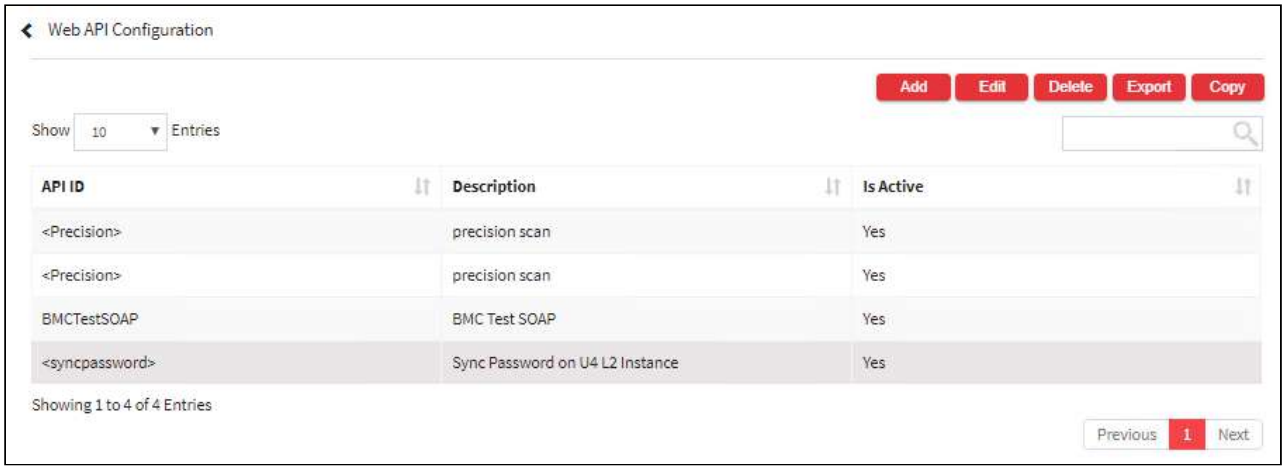
SNA API and ID1 are the identification (ID) of API. In ARCON PAM, there is standardization. Standardization describes how ARCON PAM will communicate with the target device or target system, in what format it will

communicate, and the number of parameters. These factors are already defined. When performing the implementation, it becomes a challenge because the alternate system may not have the same parameter configuration. The alternate system may also not have the flexibility to configure the parameters as per the ARCON PAM requirements. However, they will have a standardization of the parameters. To overcome this challenge, we have created the API configuration.

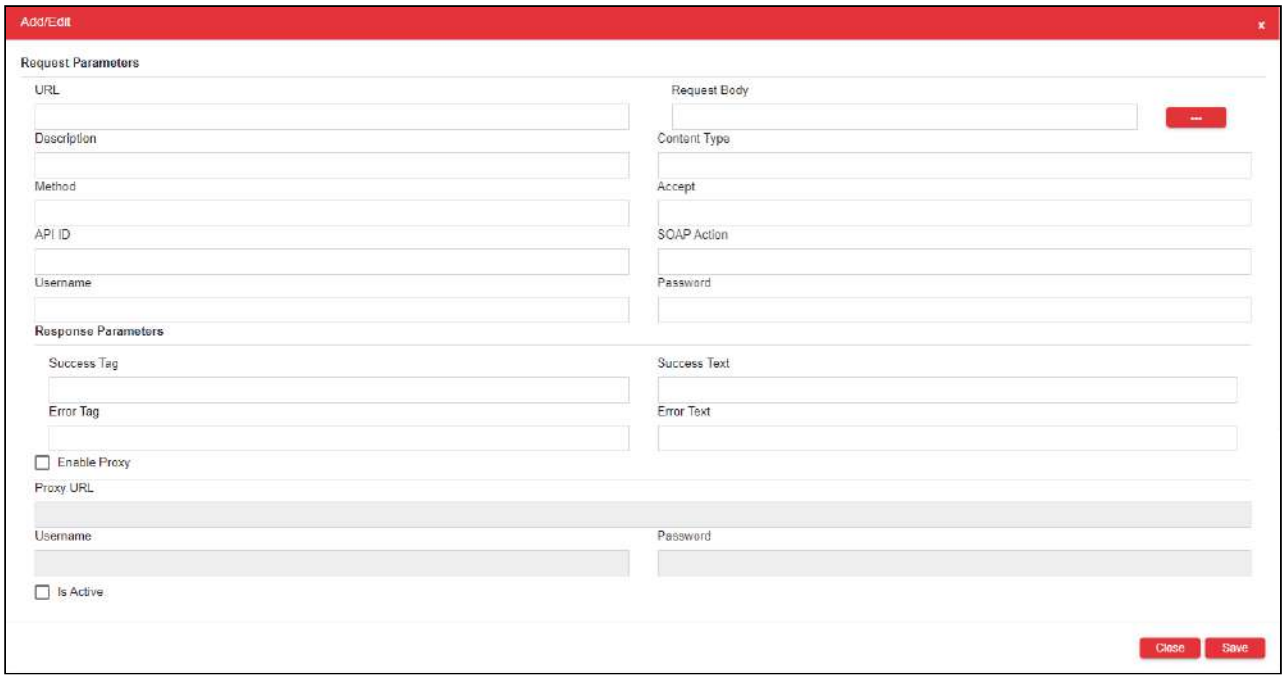
⚠ The Administrator having **Web API Configuration** privileges in Server's Privileges will only be able to configure details in Web API Configuration.

To navigate, use the following path:
Settings → API → Configure

1. Select Web API Configuration under Configure.



2. Select the Add button to add a new Web API.

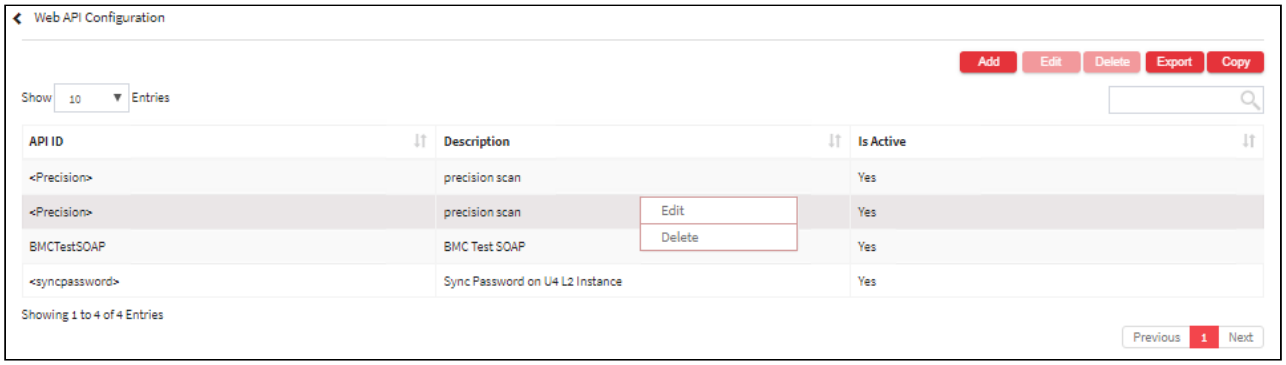


The **Web API Configuration** screen contains the following fields:

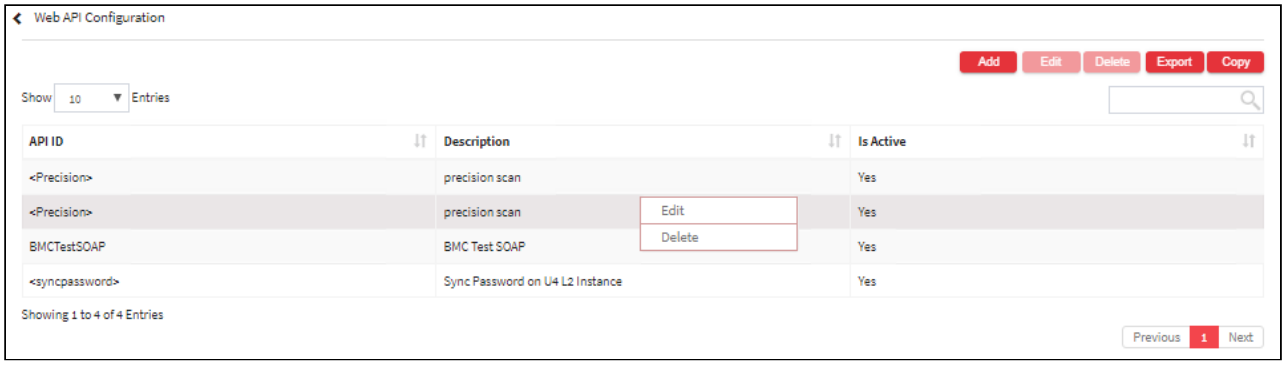
Field Name	Description
URL	Enter the URL of Web IP.
Request Body	Enter XML Data. The XML data can be imported by clicking on button.
Description	Enter the description of Web API.
Content Type	Displays the predefined content type of Web API.
Method	Enter the method of Web API.
Accept	Displays the predefined response value of Web API.
API ID	Enter the application programming interface ID.
SOAP Action	
User Name	Enter the username of web IP page.
Password	Enter the password of web API page.
Is Active	To enable the configuration.
Response Parameters	
Success Tag	Define a tag for successful API calling.
Success Text	This text will be displayed on a successful API call
Error Tag	Define a tag for API call failure.
Error Text	This text will be displayed on an API call failure
Enable Proxy	
Proxy URL	Enter the proxy server URL.
User Name	Enter the username of proxy server.

Password	Enter the password of proxy server.
Is Active	To enable the configuration.

3. Enter the details and click Save button to create a new Web API.
4. For Editing, the details of the existing Web API Configuration click on the existing row and select the Edit button at the top and make the required changes. Also, you can right-click on the row and select Edit.



5. For Deleting the existing Web API Configuration click on the existing row and select the Delete button at the top and make the required changes. Also, you can right-click on the row and select Delete.



6. The Export button will export all the Web API Configuration details in the form .xlsx format. The Copy button will copy all the details of the table.

⚠

- You need to enable Precision Biometric for fingerprint authentication over API from the back end.
- The Precision Authentication API URL will be provided by the Client. Enter this URL in the **URL** text field and configure details in **Web API Configuration** window.

To navigate, use the following path:

Settings → API → API Configure

Field Name	Description
ARCON API URL	**This configuration is used to configure the ARCON API URL. This API will notify Third Party API when the password of a service is changed in ARCON PAM.**

Field Name	Description
Valid Values	Configure ARCON API URL
TLS Configuration for SMS Web API	
Valid Values	

13.14.2 3rd Party API Notifier

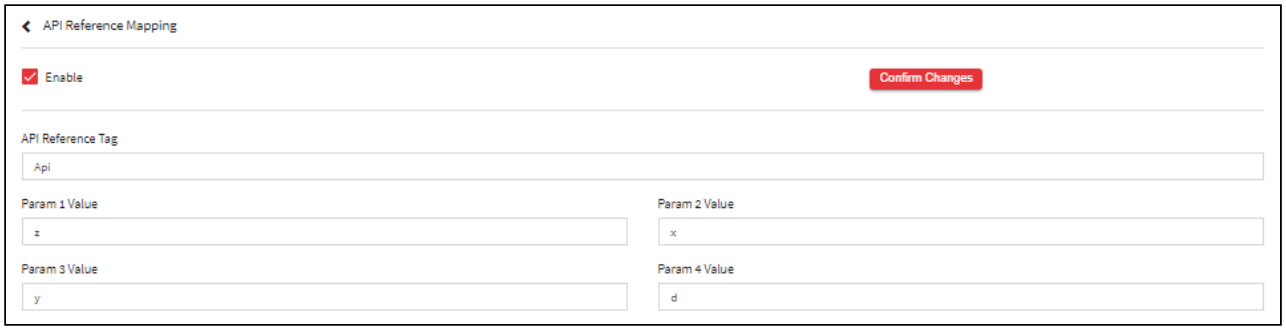
13.14.2.1 API Reference Mapping

This section explains how ARCON PAM notifies Third Party API when password of a service is changed in application. Administrator having access to **API Reference Mapping** configuration can enable ARCON API to notify Third Party API about service password change. You need to configure Third Party API details in **Web API** configuration and give its reference in **API Reference Mapping**. The URL of ARCON API should be configured in **ARCON API URL** under **Global Configuration**.

⚠ The Administrator having **API Reference Mapping** privileges in Server's Privileges will only be able to configure API Reference Mapping.

To navigate, use the following path:
Settings → API → 3rd Party API Notifier

1. Select API Reference Mapping under 3rd Party API Notifier.



The **API Reference Mapping** screen contains the following fields:

Field Name	Description
Enable	Select to Enable API Reference Mapping
API Reference Tag	Enter same value followed by **<WAPI>** tag which you have entered in **API ID** field under **Web API** screen.
Param 1 Value	Not Applicable
Param 2 Value	Not Applicable
Param 3 Value	Not Applicable
Param 4 Value	Not Applicable

4. Enter the details and click **Confirm Changes** button to configure the detail.

> ⚠ Configure the URL of ARCON API in **ARCON API URL** in **Global Configuration**. This API will notify Third Party API when the password of a service is changed in ARCON PAM.

13.14.3 Service Creation Validator

13.14.3.1 Server Monitoring System

The server monitoring system is configured to validate whether the service or the server is already monitored by some monitoring system. If it is not, ARCON PAM will not allow the server to get integrated for the user to access it. Further to explain this, the user can perform checks to make sure that any Server when goes online in the network it has been passed through all the necessary hygiene checks, security checks, etc. The status of the same may be available with various systems such as:

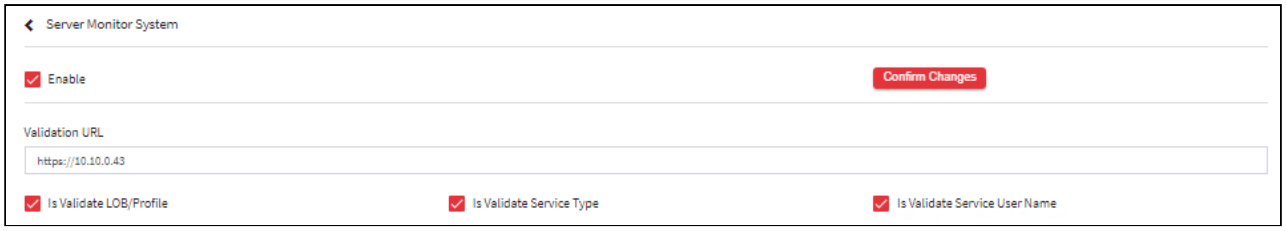
- **Monitoring System:** It is responsible to monitor the server health status.
- **SIEM System:** It is responsible to check for any vulnerabilities left open which may attack the system or any hardening checks, configuration missed, or real-time analysis.
- **Anti-Virus System:** It is responsible to check if the server is updated with the latest signature of Anti-virus and is fully protected from viruses or similar attacks.

To all of these systems, ARCON PAM has a framework available to get integrated with these systems, to check for the respective status of a server and then allow a server or system to be integrated in the application for any User to access it.

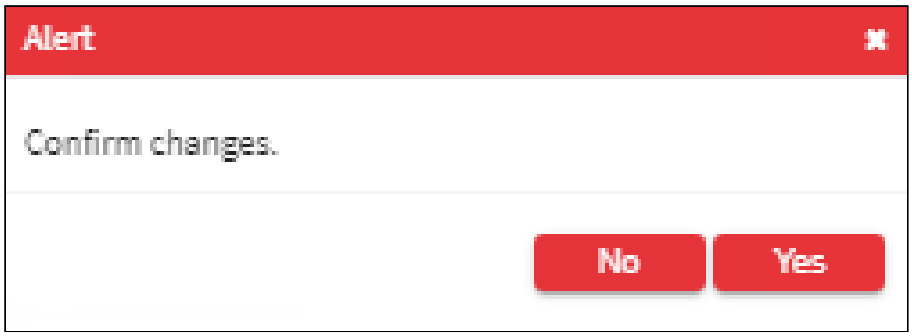
> ⚠ The Administrator having **Server Monitoring System** privileges in **Server's Privileges** will only be able to configure values for Server Monitoning System.

To navigate, use the following path:
Settings → API → Service Creation Validator

1. Select the Server Monitoring system under Service Creation Validator. Select the **Enable** checkbox.



2. A window pops up with the following message:
Confirm Changes?



3. Click **Yes**. The **Server Monitoring System** fields are enabled.

The **Server Monitoring System** screen displays the following fields:

Field Name	Description
Validation URL	Enter the URL of web service (Web API). This URL has the web service parameters required to validate the service which is created in ARCON PAM. It sends the details to web service and based on the response, it will allow or deny the creation of a new service post validation with the monitoring system. In the Validation URL, enter the URL of the API with the corresponding tags. There are URL's based on Java, some of the web services are .Net based web services. They can be configured as if the format is same. But if web service is Java or JSP based, they need certain parameters to be enabled in .Net. If it is Java based, certain parameters need to be enabled, else the communication fails. <Java> is the tag to be configured in the web service configuration.
Is Validate LOB/Profile	Indicates if the user wants to validate using LOB/Profile.
Is Validate Service Type	Indicates if the user wants to validate service type.
Is Validate Service User Name	Indicates if the user wants to validate service user name.

4. Select the details and click **Confirm Changes** button to configure the details.

13.14.4 Registered Machines

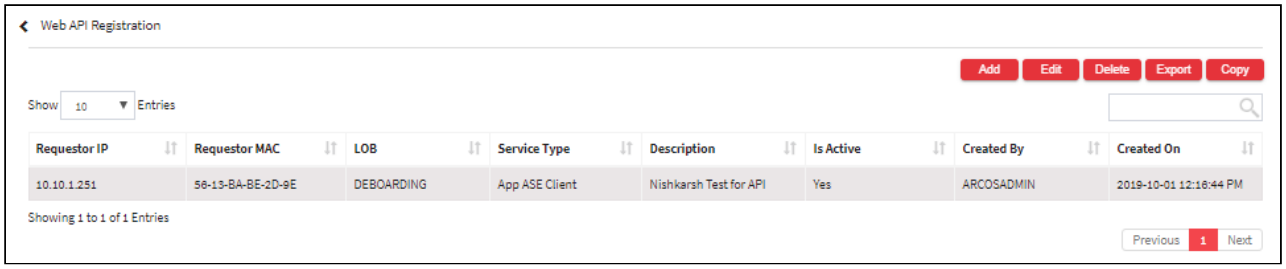
13.14.4.1 Web API Registration

Web API Registration helps you to register the user's machine IP address, where the user can view the password from the registered machine or laptop.

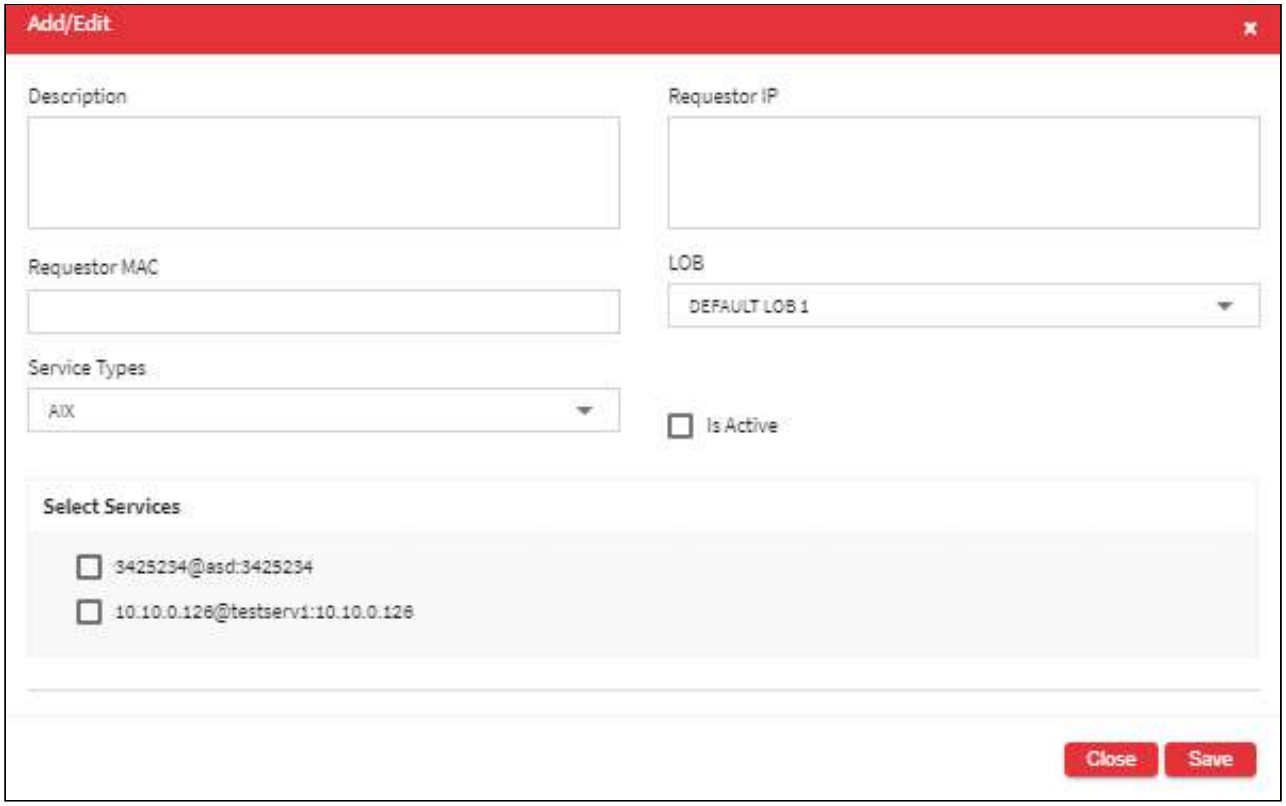
⚠ The Administrator having **ARCON PAM Web API Registration** privileges in Server's Privileges will only be able to configure the Web API registration details.

To navigate, use the following path:
Settings → API → Registered Machines

1. Select Web API Registration under Registered Machines.



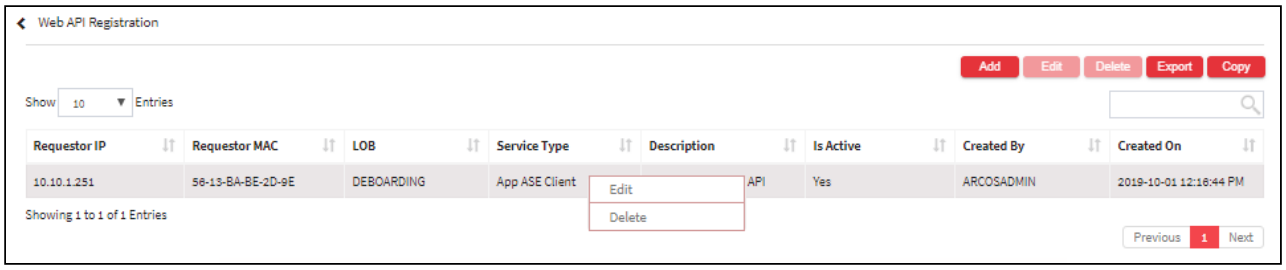
2. Select the Add button to register a new Web API.



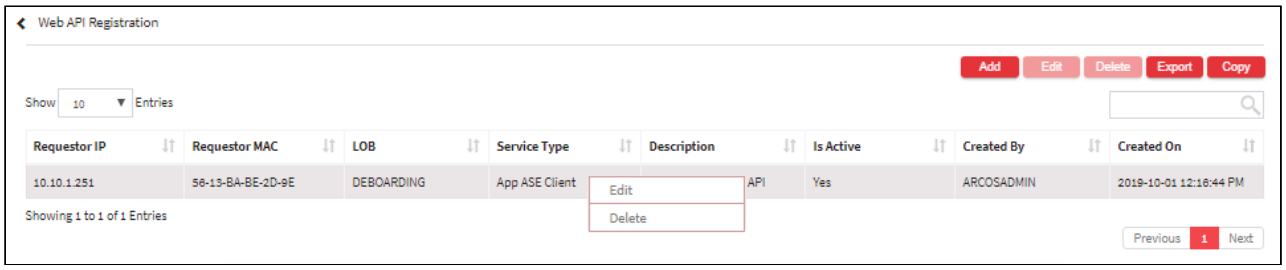
The **Web API Registration** screen contains the following fields:

Field Name	Description
Description	Specify the description for registration.
Requestor IP	Specify the IP address of the requestor.
Requestor MAC	Specify the MAC address of the requestor.
LOB	Select LOB.
Service Type	Select the type of service.
Is Active	Enable the configuration.
Select Services	The list of services are displayed in the **Select Services** grid, once you select the service type from the **Service Type** dropdown list.

3. Enter the details and click Save button to create a new Web API.
4. For Editing, the details of the existing Web API Registration click on the existing row and select the Edit button at the top and make the required changes. Also, you can right-click on the row and select Edit.



5. For Deleting the existing Web API Registration click on the existing row and select the Delete button at the top and make the required changes. Also, you can right-click on the row and select Delete.



6. The Export button will export all the Web API Registration details in the form .xlsx format. The Copy button will copy all the details of the table.

⚠

- If ARCOSAPI(Password Retrieval)RequestorValidator – Is Enabled configuration is disabled, then the user can view the password of the service from any machine.
- If ARCOSAPI(Password Retrieval)RequestorValidator – Is Enabled configuration is enabled, then the user can view the password of the service from only the registered machine.

⚠

- For API Restriction to work the configuration **ARCOSAPI(Password Retrieval)RequestorValidator** should be **enabled**. It works only if both the Requestor Machine and API Server are in the same Vlan/ Subnet.
- On enabling this configuration it will restrict all API Access and will allow only those API Request for which IP address and MAC address is registered in API registration.

13.15 General

To navigate, use the following path:

Settings → General

Field Name	Description
ARCOS Server Manager Login Mode	**This configuration sets whether User ID and Password are required to be entered when an Admin User logs in to Server Manager.**

Field Name	Description
Valid Values	The valid range is 0-2. • If '0' value is set then the system will prompt for both User ID and Password. • If '1' value is set then the system will prompt only for Password. • If '2' value is set then the system considers this as Single Sign-On, that is, Admin can log into Server Manager directly, as here the Portal Authentication will be used to validate the User.
Force Java Applet In IE	**This configuration sets whether Java Applet is forced in Internet Explorer. By default ARCON PAM is loads ActiveX for the Internet Explorer browser. If enabled, it uses Java instead of ActiveX on both the Internet Explorer and non-Internet Explorer browsers.**
Disable	If Toggle value is 'Disabled', then it does not force Java Applet.
Enable	If Toggle value is 'Enabled', then it forces Java Applet.
ARCOS PerfMonIT - Is Enabled	**ARCON PAM PerfMonIT is a service that helps to monitor the Servers - CPU, Memory, and Disk space utilization.** **This configuration enables/disables ARCON PAM PerfMonIT.**
Disable	If Toggle value is 'Disabled', then it disables the dashboard.
Enable	If Toggle value is 'Enabled', then it enables the dashboard.
ARCOS Server Master - Is Enabled	**This configuration sets the availability of Server Master under Server Manager > Settings > Logs > Scheduler**
Disable	If Toggle value is 'Disabled', then the option is not available.
Enable	If Toggle value is 'Enabled', then the option is available.
Show List Of Newly Discovered Devices In Server Manager - Is Enabled	**This configuration will enable or disable the Discovered Devices option in Server Manager.**
Disable	If Toggle value is 'Disabled', then this feature is disabled.
Enable	If Toggle value is 'Enabled', then this feature is enabled.
Cisco ISE Http Protocol for Certificated validation	**This configuration sets protocols for Cisco ISE configuration.**

Field Name	Description
Valid Values	SSL3, TLS, TLS1.1, TLS1.2
Environment Information	**This configuration enables users to display environment information (Eg.: Production/UAT) in Server Manager and Client Manager.**
Valid Values	Production/UAT.
Disable Domain Dropdown for Login page	**This configuration will enable or disable the Domain dropdown option asked on the login page in ACMO/Server Manager/settings.**
Disable	If the Toggle value is 'Disabled', then this feature is disabled.
Enable	If the Toggle value is 'Enabled', then this feature is enabled.
Enable SSH File Encryption	**This configuration will enable or disable the encryption of the SSH text file whhich is genearted in SSH output to file.**
Disable	If the Toggle value is 'Disabled', then this feature is disabled.
Enable	If the Toggle value is 'Enabled', then this feature is enabled.
SSH Output to File	**This configuration will enable/disable the SSH output in file.**
Disable	If the Toggle value is 'Disabled', then this feature is disabled.
Enable	If the Toggle value is 'Enabled', then the file is saved based on config value in ./api/Command/WriteCommandDataToDatabase.
SSH Output to Log	**This configuration will enable/disable the SSH output to log.**
Disable	If the Toggle value is 'Disabled', then this feature is disabled.
Enable	If the Toggle value is 'Enabled', then CLI output for the executed commands over putty will be captured in the Server manager → Manage Menu → Logs → Service Logs.

13.15.1 ARCON PAM Server Configuration

ARCON PAM Server Configuration helps you to configure Server details like UAT, Production, Application,etc. These details will be displayed in **About** (Client Manager).

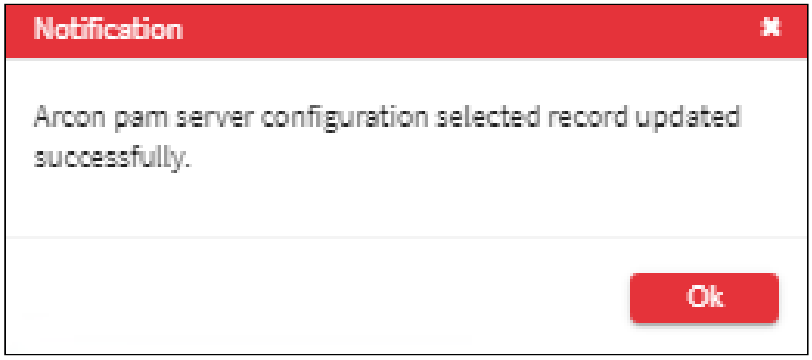
⚠ The Administrator having **ARCOS Server Configuration** privileges in Server's Privileges will only be able to configure server details.

To navigate, use the following path:

Settings → General

1. Select the ARCON PAM Server Configuration.

2. Enter server details in **Server Description** text field.
3. Click **Confirm Changes** to save the configuration. The following message will be displayed: **ARCON PAM Server Configuration Value Updated Successfully.**



13.15.2 Server Master

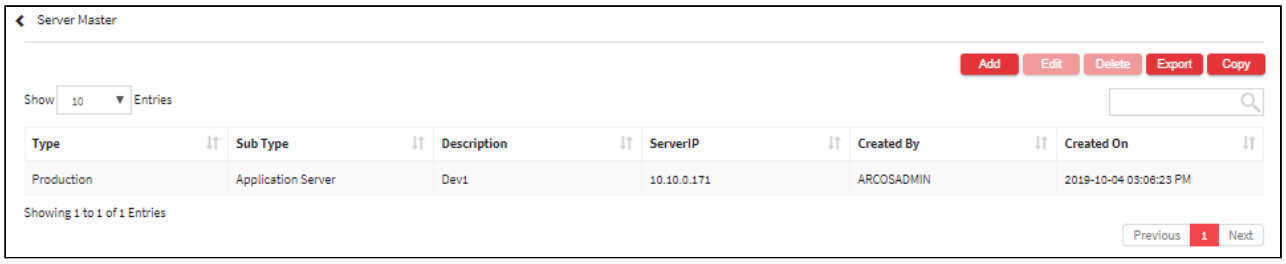
This section monitors the performance of ARCON PAM servers. In addition, it allows adding or modifying servers such as application server, database server, gateway server, and DR servers.

⚠ The Administrator having **ARCOS Server Master** privilege in Server's Privileges will only be able to configure details in Server Master.

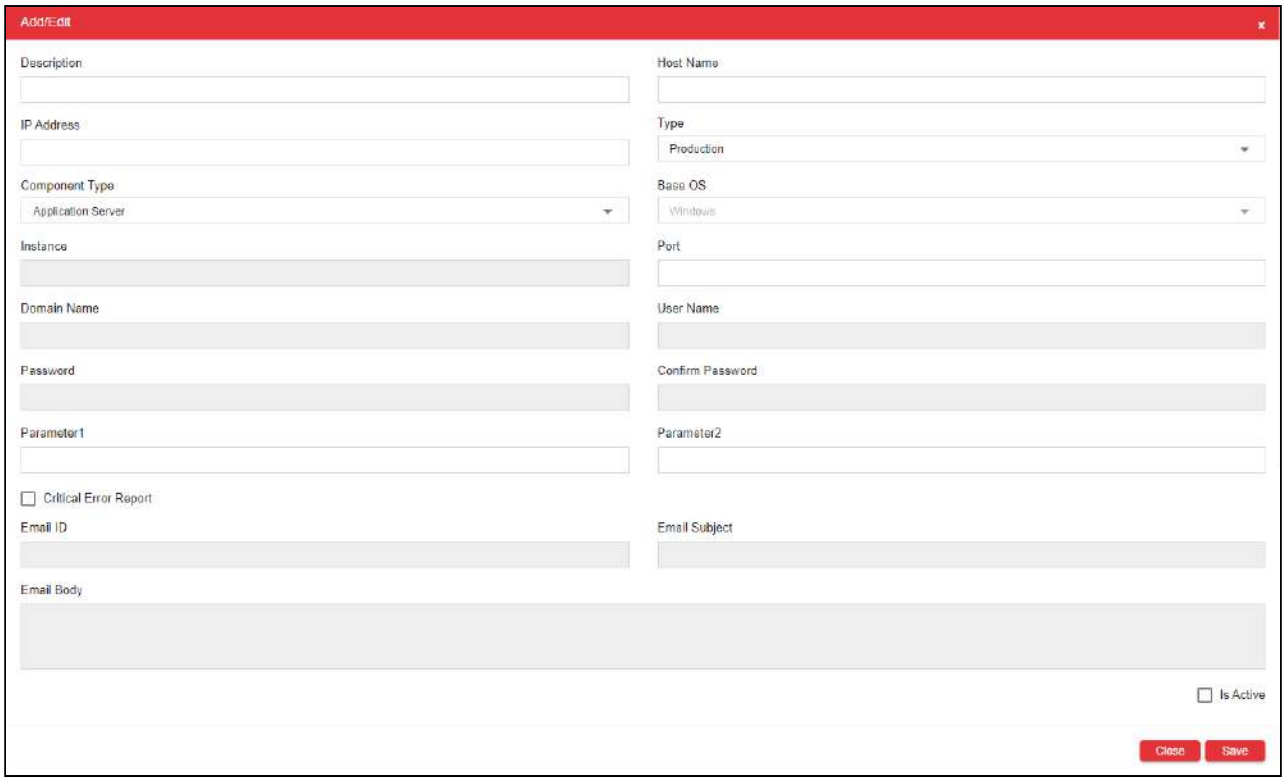
To navigate, use the following path:

Settings → General

1. Select Server Master.



2. Select the add button to add a new Server Master.

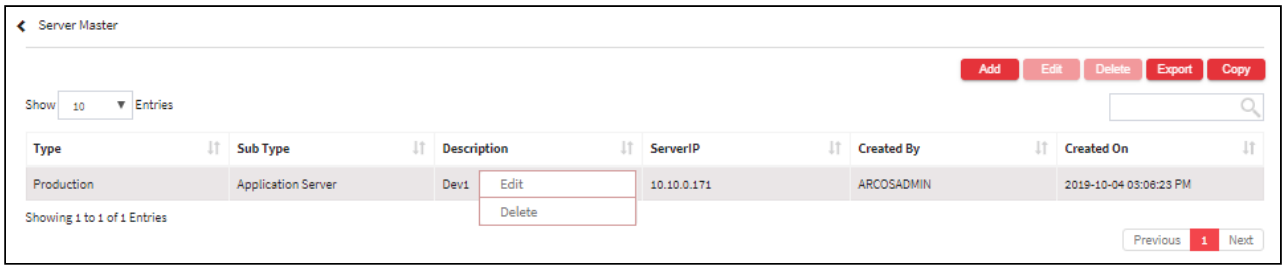


The **Server Master** screen contains the following fields:

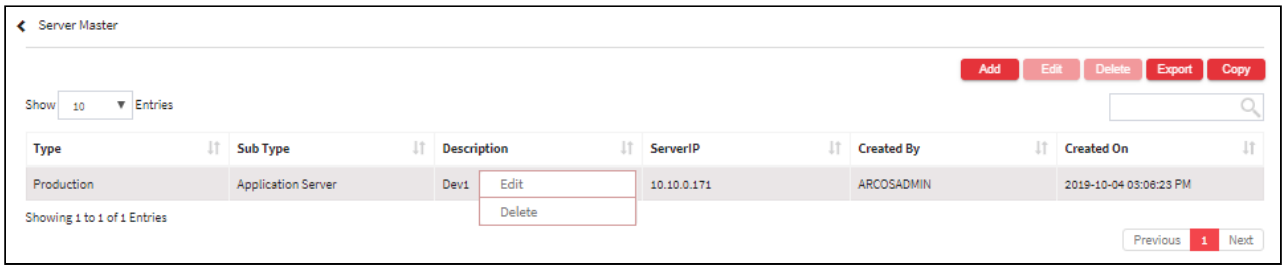
Field Name	Description
Description	Specify the type of server such as application server, or database server.
Host Name	Specify the hostname of the server.
IP Address	Specify the IP address of the server.
Type	Select the type of server. The valid values are: ▪ Production ▪ Production – HA ▪ Disaster Recovery ▪ Disaster Recovery - HA

Field Name	Description
Component Type	Select the type of component (sub type server). The valid values are: ▪ Application Server ▪ Vault Server ▪ Gateway (VPN) Server
Base OS	Displays the base OS used.
Instance	Specify the instance.(if applicable)
Port	Specify the standard port number.
Domain Name	Specify the domain name.
User Name	Specify the username. ⚠ The data in this field is auto populated, if you select the **Component Type** as **Vault Server**.
Password	Specify the password.
Confirm Password	Re-enter the password and confirm.
Parameter 1	Specify the parameter. (if applicable) ⚠ The data in this field is auto populated, if you select the **Component Type** as **Vault Server**.
Parameter 2	Specify the parameter. (if applicable) ⚠ The data in this field is auto populated, if you select the **Component Type** as **Vault Server**.
Critical Error Alert (checkbox)	Enable the Email ID, Email Subject, and Email Body text field.
Email ID	Specify the email ID of the user.
Email Subject	Specify the subject title for the email.
Email Body	Specify the description for the email.
Is Active (checkbox)	Enable the configuration in ARCON PAM.

3. Enter the details and click **Save** to create a new Server Master. A window pops up with the following message: **New ARCOS Server Created**
4. For Editing, the details of the existing Server Master click on the existing row and select the Edit button at the top and make the required changes. Also, you can right-click on the row and select Edit.



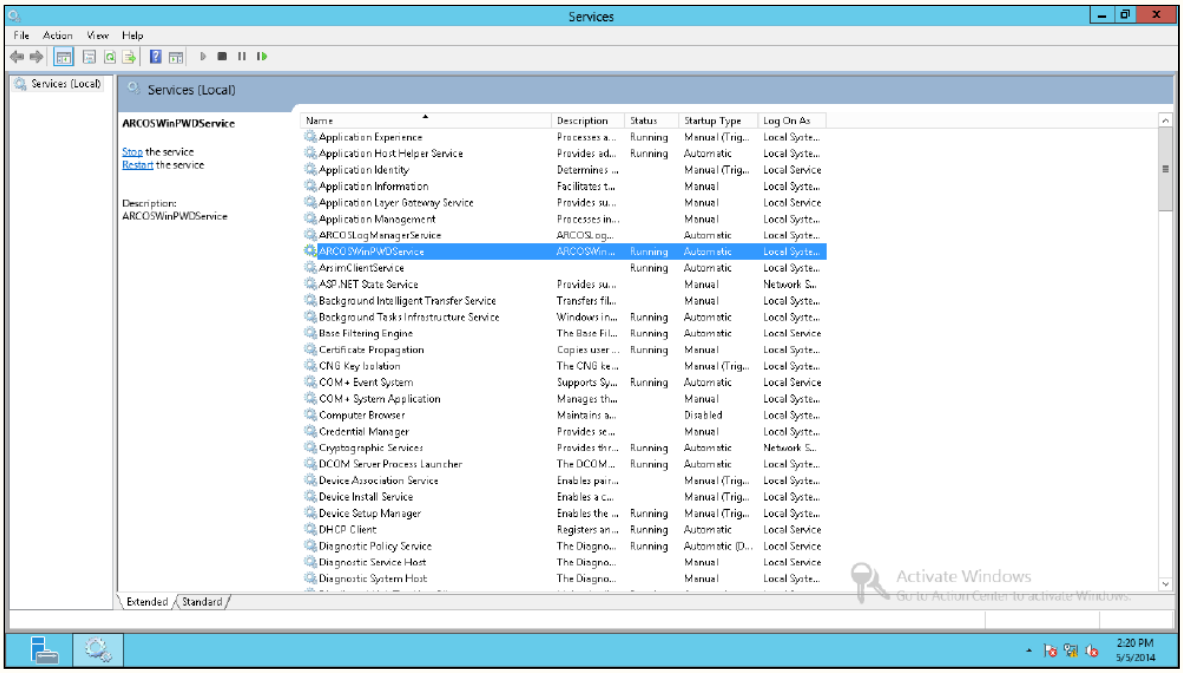
5. For Deleting the existing Server Master click on the existing row and select the Delete button at the top and make the required changes. Also, you can right-click on the row and select Delete.



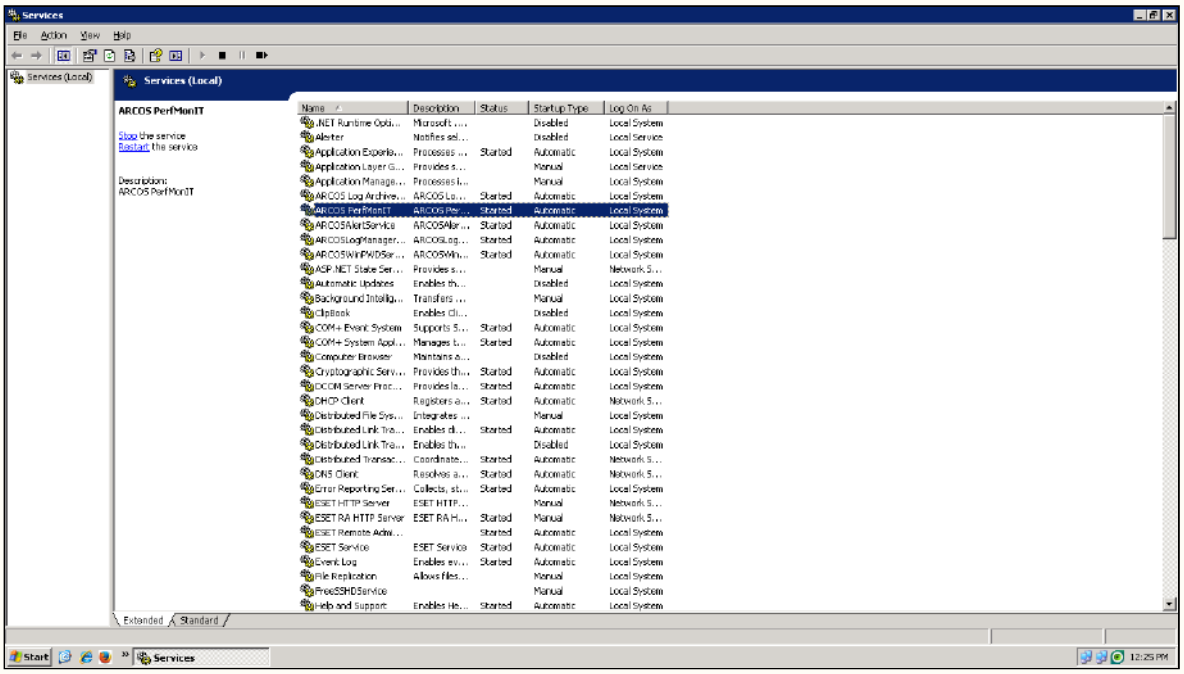
6. The Export button will export all the Server Master details in the form .xlsx format. The Copy button will copy all the details of the table.

⚠

- The win PWD service.exe should be installed on ARCON PAM Servers which is Windows-based.
- Port 45045 should be opened from Database Server to all windows based servers (i.e. App and DB servers).
- Port 22 (SSH) should be opened from Database Server to all UNIX based servers (i.e. Secured servers).



- PerformIT service should be installed and running on the Application or Database server of ARCON PAM.



13.15.3 Server Type Configuration

In Server Type Configuration users can define the separation of the production and non-production server in different colors. Production servers will be visible in a different color in ACMO and non-production server in other colors. User can identify that which is the production server and which all are non-production servers before performing any activity.

⚠ The Administrator having **Configure Server Tag type** privilege in Server's Privileges will only be able to configure details in Server Type Configuration.

ACMO Screen

1. Admin can access **Global Configuration** to add values such as IP Address, Hostname, etc. all values which we currently display in ACMO → My Access → My Services.
2. Based on admin selection, only those will be displayed in the User's Client Manager.
3. The user will have the option to set his preference which will be saved for his login.

To navigate, use the following path:

Settings → General

1. Select **Server Type Configuration**.

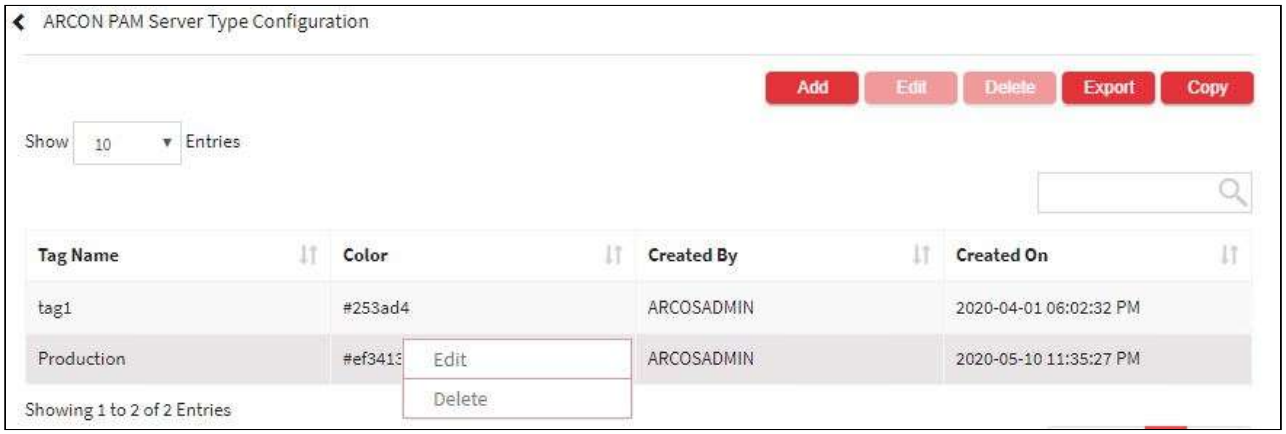
2. Select the add button to add a new **Server Type Configuration**.

The **Server Type Configuration** screen contains the following fields:

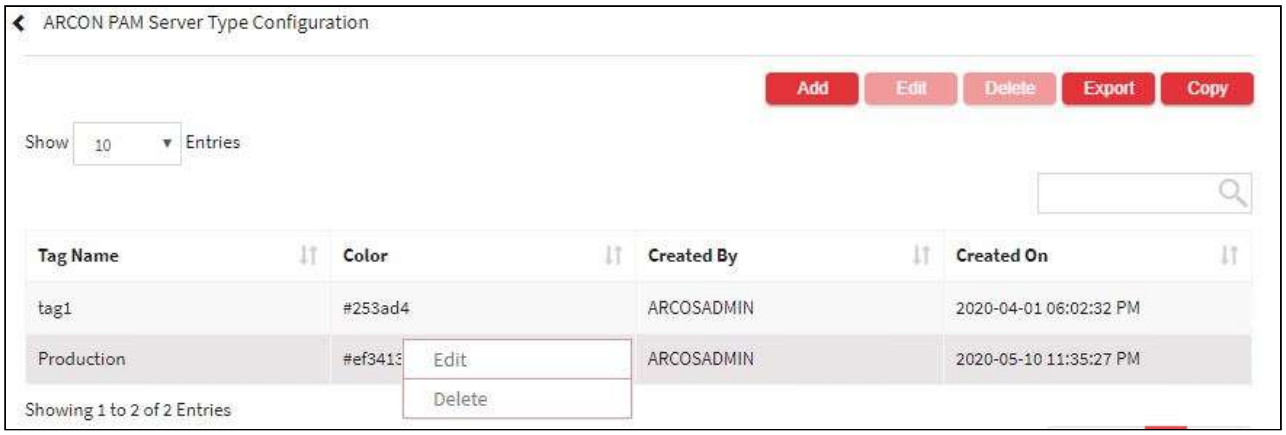
Field Name	Description
Tag Name	Enter the server type name as the tag value to identify production/ nonproduction servers when attached to the service.

Field Name	Description
Color	Choose colors for the respective tag value (server type). Click on the three dots button, a palette is opened and which will show a list of basic colors with a name to select. Basic colors to be shown are as follows: None - In case of admin wishes to disable this tag. Similar message to display while deleting the tag as mentioned below. BLACK #000000 RGB(0, 0, 0) RED #FF0000 RGB(255, 0, 0) MAROON #800000 RGB(128, 0, 0) YELLOW #FFFF00 RGB(255, 255, 0) OLIVE #808000 RGB(128, 128, 0) LIME #00FF00 RGB(0, 255, 0) GREEN #008000 RGB(0, 128, 0) AQUA #00FFFF RGB(0, 255, 255) TEAL #008080 RGB(0, 128, 128) BLUE #0000FF RGB(0, 0, 255) NAVY #000080 RGB(0, 0, 128) PURPLE #800080 RGB(128, 0, 128)) ⚠ Make sure that no two tag values have the same colors.

3. Enter the details and click **Save** to create a new tag in **Server Type Configuration**.
4. For Editing, the details of the existing **Server Type Configuration,** click on the existing row and select the Edit button at the top and make the required changes. Also, you can right-click on the row and select Edit.



5. For Deleting the existing **Server Type Configuration,** click on the existing row and select the Delete button at the top and make the required changes. Also, you can right-click on the row and select Delete.



6. The Export button will export all the **Server Type Configuration** details in the form .xlsx format. The Copy button will copy all the details of the table.

13.15.4 User Access Review

This section helps the Administrator to review the service access provided to users at regular intervals. You can define a new user access review process, wherein the review process is initialized or re-initialized and email notification is sent to the approver for approval. In addition, you can modify the details of configured user access review and delete user access review which has not been initialized.

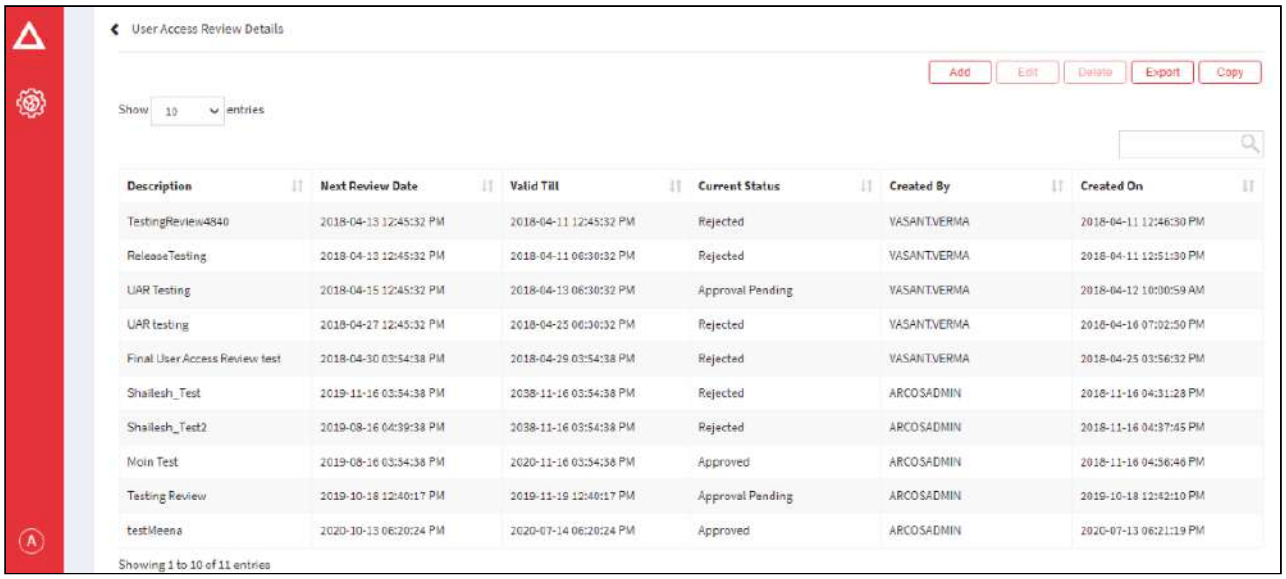
⚠

- The Administrator should have **User Access Review Manager** privilege in **Server Privileges**, to create a user access review.
- The Administrator having **User Access Reviewer** privilege in **Group Admin Privileges** , shall be able to review the services mapped to User in **Client Manager**. In this process, the Administrator can also preserve or revoke the services mapped to a User.

To navigate to user access review, use the following path:

General → User Access Review

1. Select User Access Review

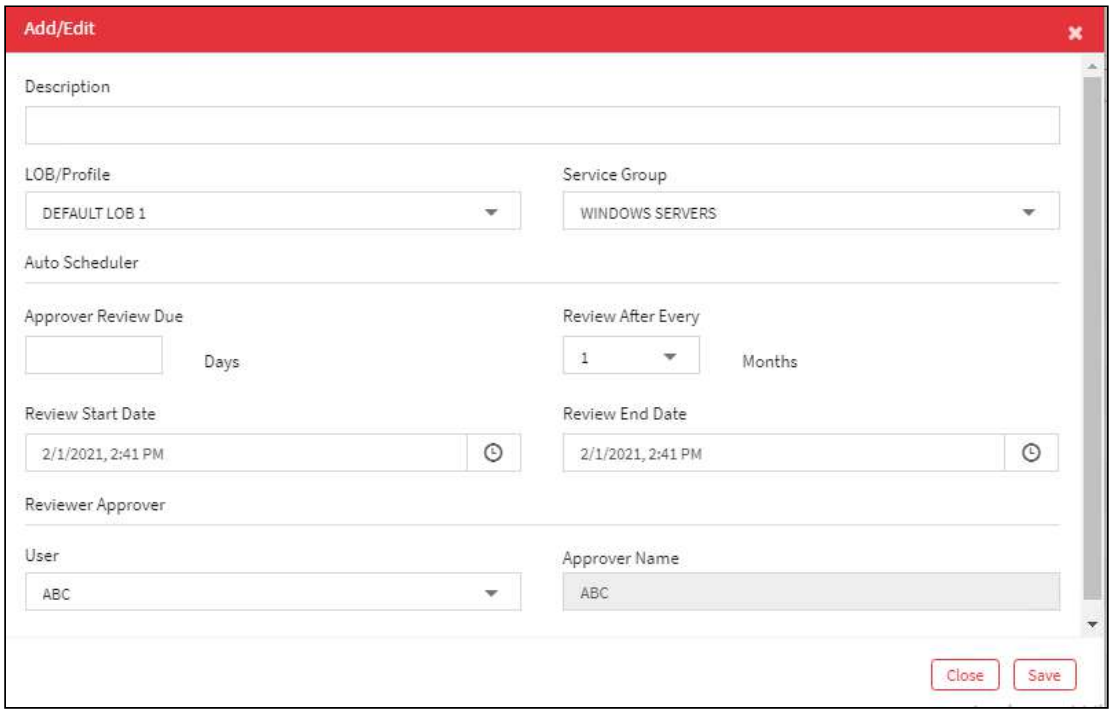


The **User Access Review Details** screen contains the following fields:

Field Name	Description
Description	Specify a short description.
LOB/Profile	Select the LOB.
Service Group	Select the service group.
Auto Scheduler	
Approver Review Due	Select number of Days. ▪ The review will be available to Approver for approval for selected number of days from the initialized/re-initialized date. ▪ If the Approver fails to submit review within the selected number of days, then the review process will be be auto closed and the **Current Status** will be updated to **Rejected**. Administrator can re-initialize such review process.
Review After Every	Select number of Months. ▪ Review process will be auto initialized after the selected number of months from the **Review Start Date**. ▪ Review process will not be auto initialized after date selected in **Scheduler Expiry Date** field. The **Current Status** of such review process will be updated to **Rejected**. Administrator can re-initialize such review process.
Review Start Date	Select the start date of the review process.
Scheduler Expiry Date	Select the end date of the review process.
Reviewer/Approver	

User	Search and select the name of the user. The selected User is displayed as Approver in the Approver Name field.
Approver Name	Displays the name of the Approver.
Buttons	
Modify	Click **Modify** button, to modify details of User Access Review. To modify details of User Access Review, select the required record from the grid on the left pane. The selected User Access Review details are displayed on the right side. Modify the required details and click **Modify** button, to update the details.
Delete	Click **Delete**, to delete a particular User Access Review. To delete a User Access Review, select the required User Access Review from the grid on the left pane. The details are displayed on the right side. View the details and click **Delete** button, to delete a particular User Access Review.

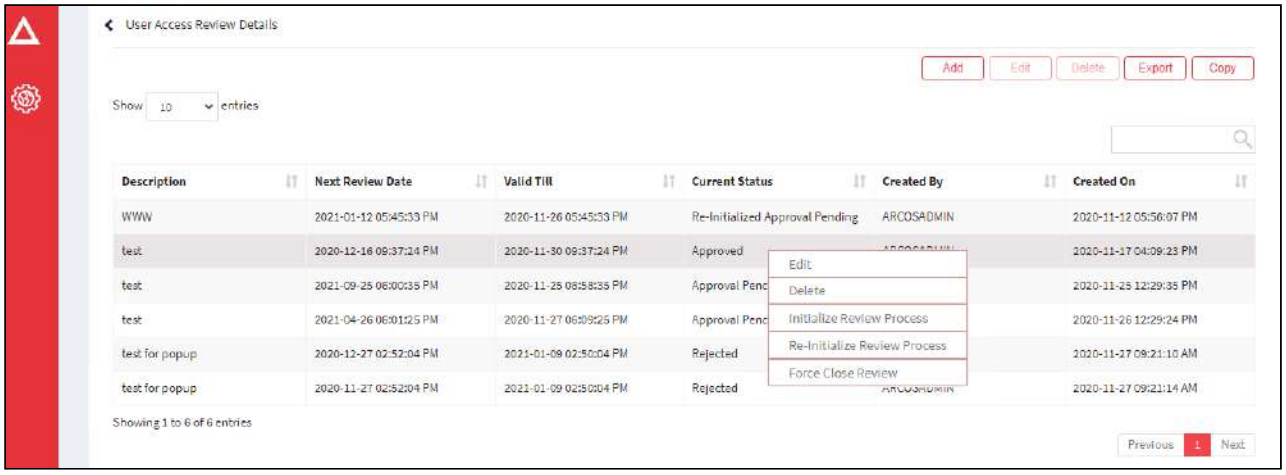
2. Select the Add button to add a new User access review.



3. Enter/ Select the details and click **Create**. A window pops up with the following message: **New User Access Review Workflow Successfully Created.**
4. Click **OK**. The new user access review workflow is added to the grid on the left pane.

> ⚠ The **Current Status** of created User Access Review is **Added To Workflow**.

5. Right-click on the user access review detail and choose **Initialize Review Process** option.



6. Choose **Initialize Review Process** option. A window pops up with the following message:
   Are You Sure You Want To Initialize Review Process?
7. Click **Yes**. Another window pops up with the following message:
   Selected Review Process Initialized And Email Notification Has Been Sent To Reviewer/ Approver.
8. Click **OK**. The review process is initialized and email notification is sent to the approver for approval.

> ⚠ The **Current Status** of initialized user access review is **Approval Pending**.

9. When Approver submits review from Client Manager or through link sent in email, the **Current Status** of user access review is updated to **Approved**.
10. You can re-initialize user access review with **Current Status** as **Approved** or **Rejected**.
11. Right-click on the user access review detail and choose **Re-Initialize Review Process** option. A window pops up with the following message:
    Are You Sure You Want To Re-Initialize Review Process?
12. Click **Yes**. Another window pops up with the following message:
    Selected Review Process Re-Initialized And Email Notification Has Been Sent To Reviewer/ Approver.
13. Click **OK**. The review process is re-initialized and email notification is sent to the approver for approval.

> ⚠
> - Once the review process is initiated or re-initialized from Server Manager, an email notification is sent to the Approver for approving the request. The Administrator shall review the services mapped to user in Client Manager or on the link sent through email. On reviewing, the services shall then be preserved or revoked for access. (For more information, refer **User Access Review** in **Client Manager**)
> - If the initiated or re-initiated review process is still pending for approval or the approver fails to approve the request within the specified time, or due to some reasons then the Administrator can forcefully close the initiated review process using the **Force Close Review** option wherein you need to specify the reason to force close a review process. The status is updated to **Rejected**, once the review is forcefully closed.

13.15.5 Object Counter

This section helps you to view or monitor different entities. It helps to view the count of the objects integrated in ARCON PAM such as count of services, server group, user group, profile, details of password change, command log,

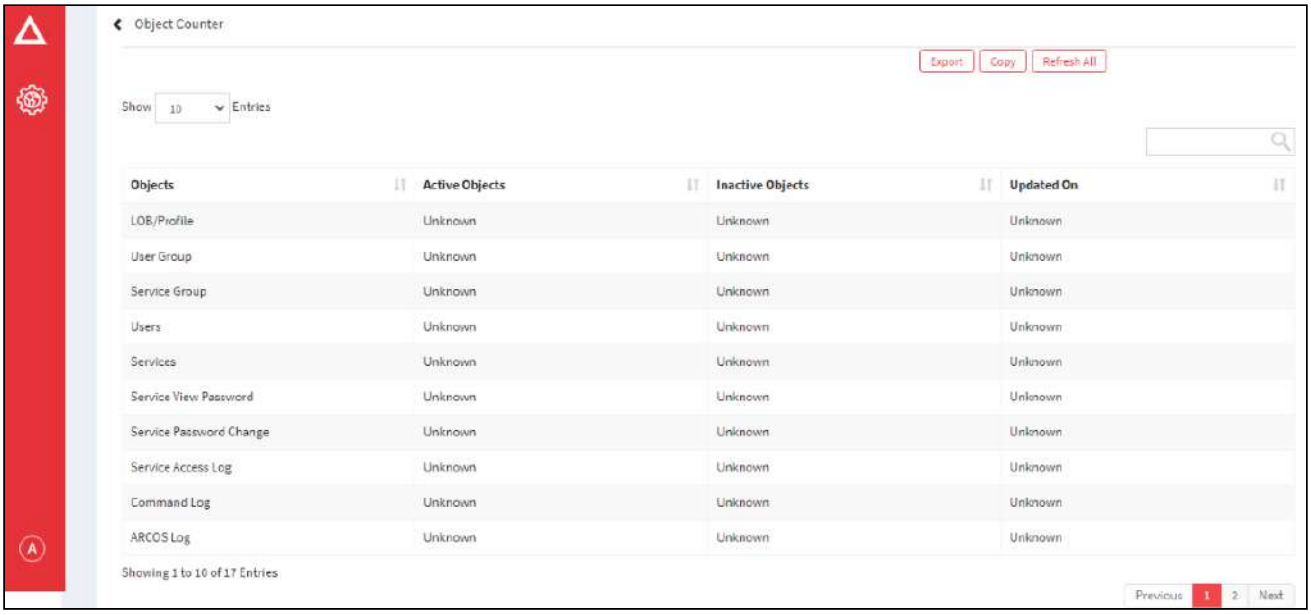
and captured images in ARCOSRDPDB database. In addition, it displays the count of all the active and inactive objects integrated with ARCON PAM.

> ⚠ The Administrator having **ARCON PAM Object Counter** privilege in Server's Privilege will only be able to view and monitor different entities in ARCON PAM.

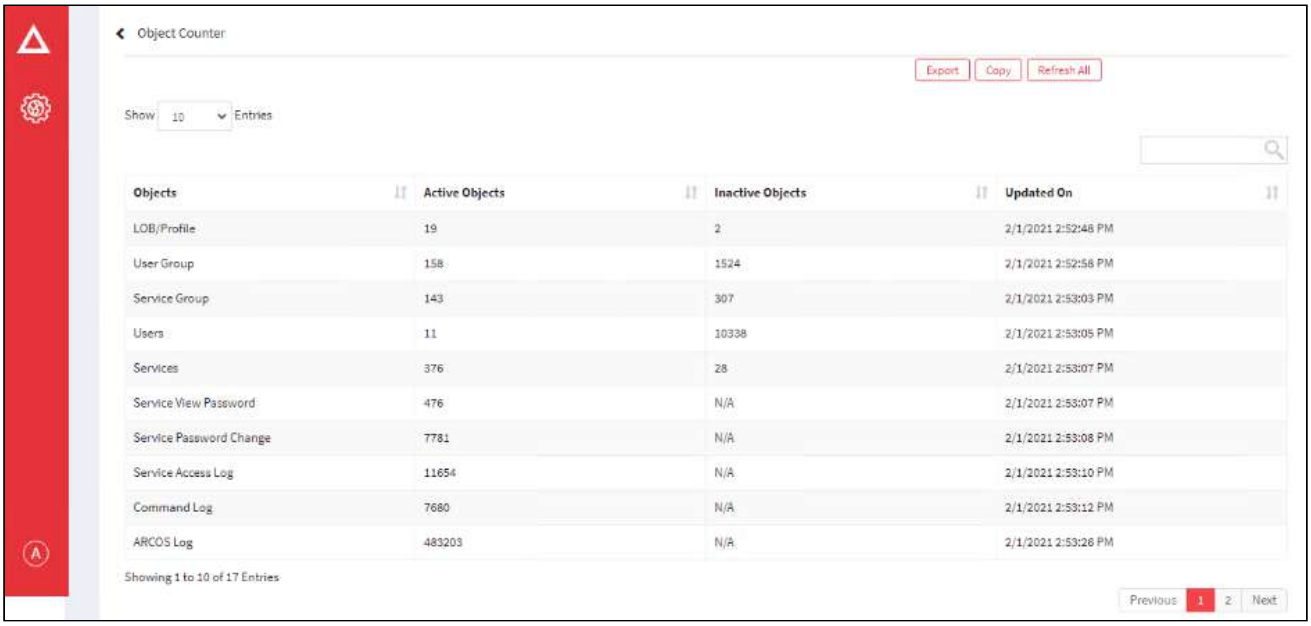
To view Object Counter:

To view object counter use the following path:

General → ARCOS Object Counter



On refreshing, you can see the detailed screen.



13.15.6 Performance Monitoring

Performance Monitoring feature provides users the status of the server being accessed. The functionality will show whether the server is up and running or not. The Performance Monitoring page will display the IP Address, the current status, and the last updated Date and Time.

> ⚠ The Administrator having **Performance Monitoring Utility** privileges in Server's Privileges will only be able to do configurations under Performance Monitoring.

To navigate, use the following path:

Settings → General

1. Select **Performance Monitoring**.

2. The Performace Monitoring Report will display the IP Address, The Current status of the User IP, and the last updated status.
3. The Export button will export all the **Performance Monitoring** details in the form .xlsx format. The Copy button will copy all the details of the table.

13.15.7 LOB Wise

To navigate, use the following path:

Settings → General → LOB Wise

Field Name	Description
LOB Wise User Management - Is Enabled	**This configuration enables/disables LOB Wise User Management.**
Disable	If Toggle value is 'Disabled', then all users will be displayed under Server Manager > Manage Users and Server Manager > Manage > Maker's Checker irrespective of the selected LOB.

Field Name	Description
Enable	If Toggle value is 'Enabled', then users assigned to selected LOB will be displayed under Server Manager > Manage Users and Server Manager > Manage > Maker's Checker.
LOB Wise Workflow Configuration - Is Enabled	**This configuration sets whether Workflow should be configured LOB wise or for all.**
Disable	If Toggle value is 'Disabled', then the "All" option will be available in LOB/Profile drop-down.
Enable	If Toggle value is 'Enabled', then only LOB names will be available for selection in LOB/Profile drop-down in Server Manager > Settings >Workflow >Raise Request > User Request Approval Workflow. Also configured workflows will be displayed LOB wise.
LOB Wise Master And Manager - Is Enabled	**This configuration sets whether all or only LOBs assigned to logged in user will be displayed under LOB Wise Master and Manager > Map LOB tabs.**
Disable	then all LOBs will be available in the drop-down for selection.
Enable	If Toggle value is 'Enabled' (and "Add New LOB" privilege is not assigned) then only those LOBs will be available in the drop-down which is assigned to the user.
LOB Wise Real Time Session Monitoring - Is Enabled	**This configuration sets whether live sessions under Server Manager > Tools > Real Time Session Monitoring should be displayed for all LOBs or LOB Wise.**
Disable	If Toggle value is 'Disabled', live sessions of all LOBs will be displayed.
Enable	If Toggle value is 'Enabled', then live sessions of single LOB will be displayed.
LOB Wise Service Management - Is Enabled	**This configuration enables/disables LOB Wise Service Management.**
Disable	If Toggle value is 'Disabled', then Admin ID should assign newly created service to required LOB under Server Manager > Manage > LOB/Profile Master & Manager.
Enable	If Toggle value is 'Enabled', then newly created service will be directly assigned to the selected LOB in Server Manager > Select LOB/Profile.

Field Name	Description
LOB Wise Authorize Users	**This configuration sets whether Users will be displayed LOB wise in Authorising User 1 and Authorising User 2 drop-down under Print Password Envelope (SM > Manage > Password Manager) while authorizing the password printing process for APEM Tool.** **Note:** **The LOB selected in Select LOB/Profile dropdown on the Server Manager home screen will be considered while listing Users.**
Disable	If Toggle value is 'Disabled', then User from all LOBs will be listed.
Enable	If Toggle value is 'Enabled', then Users will be listed LOB wise.

13.15.7.1 Ticket

To navigate, use the following path:

Settings → General → Ticket

Field Name	Description
Access Duration For Ticket Access Request(in days)	**The users can raise a service access request for the ticket with specified number of days.**
Valid Values	It ranges from 1-45 days. The minimum value is 1 (default value), the users shall be able to raise a service access request only for a day. The maximum value is 45, the users shall be able to raise a service access request for 45 days.
Max Hours For Ticket Session Duration(in hours)	**This configuration sets the maximum number of hours to be displayed in Expected Duration dropdown under Ticket Request (Client Manager > My Access > Raise Request > Ticket Request).**
Valid Values	It ranges from 0-999. If value '0' is selected then, the Expected Duration dropdown will be displayed as blank.

13.15.7.2 Real Time Session Monitoring

To navigate, use the following path:

Settings → General → Real Time Session Monitoring

Field Name	Description
Real Time Session Monitoring - Is Enabled	**This configuration sets availability of Real Time Session Monitoring under Server Manager > Tools.**
Disable	If Toggle value is 'Disabled', then this option is not available.

Field Name	Description
Enable	If Toggle value is 'Enabled', then the option is available to view live sessions accessed through ARCON PAM.
Real Time Session Monitoring With Freeze / Unfreeze Session - Is Enabled	**This configuration sets the availability of Freeze and Unfreeze Session options on Real Time Session Monitoring window when the live session is accessed.**
Disable	If Toggle value is 'Disabled', then these options are not available.
Enable	If Toggle value is 'Enabled', then options are available.

13.15.7.3 Privileged User Discovery and Reconciliation

To navigate, use the following path:

Settings → General → Privileged User Discovery and Reconciliation

Field Name	Description
Privileged User Discovery & Reconciliation - Is Enabled	**This configuration sets the availability of Privileged User Discovery & Reconciliation under Server Manager > Tools.**
Disable	If Toggle value is 'Disabled', then this option is not available.
Enable	If Toggle value is 'Enabled', then the option is available to discover users on servers.

13.15.7.4 Maker Checker

To navigate, use the following path:

Settings → General → Maker Checker

Field Name	Description
User Maker Checker - Is Enabled	**This configuration enables the approval process of User creation using Maker's Checker option.**
Disable	If Toggle value is 'Disabled', then a new User will be created without the approval process.
Enable	If Toggle value is 'Enabled', then a new User creation process will be approved using **Maker's Checker** option.

13.15.7.5 Log Staging Server

To navigate, use the following path:

Settings → General → Log Staging Server

Field Name	Description
ARCOS Staging Log Server - Is Enabled	**It enables or disables the ARCOS Staging Server.**
Disable	If Toggle value is 'Disabled', then it disables ARCOS Staging Server.
Enable	If Toggle value is 'Enabled', then it enables ARCOS Staging Server.

13.15.8 Ticket.

To navigate, use the following path:

Settings → General → Ticket

Field Name	Description
Access Duration For Ticket Access Request(in days)	**The users can raise a service access request for the ticket with specified number of days.**
Valid Values	It ranges from 1-45 days. The minimum value is 1 (default value), the users shall be able to raise a service access request only for a day. The maximum value is 45, the users shall be able to raise a service access request for 45 days.
Max Hours For Ticket Session Duration(in hours)	**This configuration sets the maximum number of hours to be displayed in Expected Duration dropdown under Ticket Request (Client Manager > My Access > Raise Request > Ticket Request).**
Valid Values	It ranges from 0-999. If value '0' is selected then, the Expected Duration dropdown will be displayed as blank.

13.15.8.1 Real Time Session Monitoring

To navigate, use the following path:

Settings → General → Real Time Session Monitoring

Field Name	Description
Real Time Session Monitoring - Is Enabled	**This configuration sets availability of Real Time Session Monitoring under Server Manager > Tools.**
Disable	If Toggle value is 'Disabled', then this option is not available.
Enable	If Toggle value is 'Enabled', then the option is available to view live sessions accessed through ARCON PAM.

Field Name	Description
Real Time Session Monitoring With Freeze / Unfreeze Session - Is Enabled	**This configuration sets the availability of Freeze and Unfreeze Session options on Real Time Session Monitoring window when the live session is accessed.**
Disable	If Toggle value is 'Disabled', then these options are not available.
Enable	If Toggle value is 'Enabled', then options are available.

13.15.8.2 Privileged User Discovery and Reconciliation

To navigate, use the following path:

Settings → General → Privileged User Discovery and Reconciliation

Field Name	Description
Privileged User Discovery & Reconciliation - Is Enabled	**This configuration sets the availability of Privileged User Discovery & Reconciliation under Server Manager > Tools.**
Disable	If Toggle value is 'Disabled', then this option is not available.
Enable	If Toggle value is 'Enabled', then the option is available to discover users on servers.

13.15.8.3 Maker Checker

To navigate, use the following path:

Settings → General → Maker Checker

Field Name	Description
User Maker Checker - Is Enabled	**This configuration enables the approval process of User creation using Maker's Checker option.**
Disable	If Toggle value is 'Disabled', then a new User will be created without the approval process.
Enable	If Toggle value is 'Enabled', then a new User creation process will be approved using **Maker's Checker** option.

13.15.8.4 Log Staging Server

To navigate, use the following path:

Settings → General → Log Staging Server

Field Name	Description
ARCOS Staging Log Server - Is Enabled	**It enables or disables the ARCOS Staging Server.**
Disable	If Toggle value is 'Disabled', then it disables ARCOS Staging Server.
Enable	If Toggle value is 'Enabled', then it enables ARCOS Staging Server.

13.15.9 Real Time Session Monitoring

To navigate, use the following path:

Settings → General → Real Time Session Monitoring

Field Name	Description
Real Time Session Monitoring - Is Enabled	**This configuration sets availability of Real Time Session Monitoring under Server Manager > Tools.**
Disable	If Toggle value is 'Disabled', then this option is not available.
Enable	If Toggle value is 'Enabled', then the option is available to view live sessions accessed through ARCON PAM.
Real Time Session Monitoring With Freeze / Unfreeze Session - Is Enabled	**This configuration sets the availability of Freeze and Unfreeze Session options on Real Time Session Monitoring window when the live session is accessed.**
Disable	If Toggle value is 'Disabled', then these options are not available.
Enable	If Toggle value is 'Enabled', then options are available.

13.15.9.1 Privileged User Discovery and Reconciliation

To navigate, use the following path:

Settings → General → Privileged User Discovery and Reconciliation

Field Name	Description
Privileged User Discovery & Reconciliation - Is Enabled	**This configuration sets the availability of Privileged User Discovery & Reconciliation under Server Manager > Tools.**
Disable	If Toggle value is 'Disabled', then this option is not available.
Enable	If Toggle value is 'Enabled', then the option is available to discover users on servers.

13.15.9.2 Maker Checker

To navigate, use the following path:

Settings → General → Maker Checker

Field Name	Description
User Maker Checker - Is Enabled	**This configuration enables the approval process of User creation using Maker's Checker option.**
Disable	If Toggle value is 'Disabled', then a new User will be created without the approval process.
Enable	If Toggle value is 'Enabled', then a new User creation process will be approved using **Maker's Checker** option.

13.15.9.3 Log Staging Server

To navigate, use the following path:

Settings → General → Log Staging Server

Field Name	Description
ARCOS Staging Log Server - Is Enabled	**It enables or disables the ARCOS Staging Server.**
Disable	If Toggle value is 'Disabled', then it disables ARCOS Staging Server.
Enable	If Toggle value is 'Enabled', then it enables ARCOS Staging Server.

13.15.10 Privileged User Discovery and Reconciliation

To navigate, use the following path:

Settings → General → Privileged User Discovery and Reconciliation

Field Name	Description
Privileged User Discovery & Reconciliation - Is Enabled	**This configuration sets the availability of Privileged User Discovery & Reconciliation under Server Manager > Tools.**
Disable	If Toggle value is 'Disabled', then this option is not available.
Enable	If Toggle value is 'Enabled', then the option is available to discover users on servers.

13.15.10.1 Maker Checker

To navigate, use the following path:

Settings → General → Maker Checker

Field Name	Description
User Maker Checker - Is Enabled	**This configuration enables the approval process of User creation using Maker's Checker option.**
Disable	If Toggle value is 'Disabled', then a new User will be created without the approval process.
Enable	If Toggle value is 'Enabled', then a new User creation process will be approved using **Maker's Checker** option.

13.15.10.2 Log Staging Server

To navigate, use the following path:

Settings → General → Log Staging Server

Field Name	Description
ARCOS Staging Log Server - Is Enabled	**It enables or disables the ARCOS Staging Server.**

Field Name	Description
Disable	If Toggle value is 'Disabled', then it disables ARCOS Staging Server.
Enable	If Toggle value is 'Enabled', then it enables ARCOS Staging Server.

13.15.11 Maker Checker

To navigate, use the following path:

Settings → General → Maker Checker

Field Name	Description
User Maker Checker - Is Enabled	**This configuration enables the approval process of User creation using Maker's Checker option.**
Disable	If Toggle value is 'Disabled', then a new User will be created without the approval process.
Enable	If Toggle value is 'Enabled', then a new User creation process will be approved using **Maker's Checker** option.

13.15.11.1 Log Staging Server

To navigate, use the following path:

Settings → General → Log Staging Server

Field Name	Description
ARCOS Staging Log Server - Is Enabled	**It enables or disables the ARCOS Staging Server.**
Disable	If Toggle value is 'Disabled', then it disables ARCOS Staging Server.
Enable	If Toggle value is 'Enabled', then it enables ARCOS Staging Server.

13.15.12 Log Staging Server

To navigate, use the following path:

Settings → General → Log Staging Server

Field Name	Description
ARCOS Staging Log Server - Is Enabled	**It enables or disables the ARCOS Staging Server.**
Disable	If Toggle value is 'Disabled', then it disables ARCOS Staging Server.
Enable	If Toggle value is 'Enabled', then it enables ARCOS Staging Server.

13.15.13 Database

To navigate, use the following path:

Settings → General → Database

Field Name	Description
Use ARCOS Web Service DT For Database (Script Manager) - Is Enabled	**This configuration enables/disables routing of Script Manager connecting to Database server for sending audit logs from Application Server.**
Disable	If Toggle value is 'Disabled', then this feature disables routing.
Enable	If Toggle value is 'Enabled', then this feature enables routing. If this value is enabled, no Direct port for Database is required from Local system.
Use ARCOS Web Service DT For Database (ARCOS Clients) - Is Enabled	**This configuration enables/disables routing of Video Logs to ARCON PAM Database server from Application Server.**
Disable	If Toggle value is 'Disabled', then this feature disables routing.
Enable	If Toggle value is 'Enabled', then this feature enables routing. If this value is enabled, no Direct port for Database is required from Local system.

13.15.14 Assigned IAM User

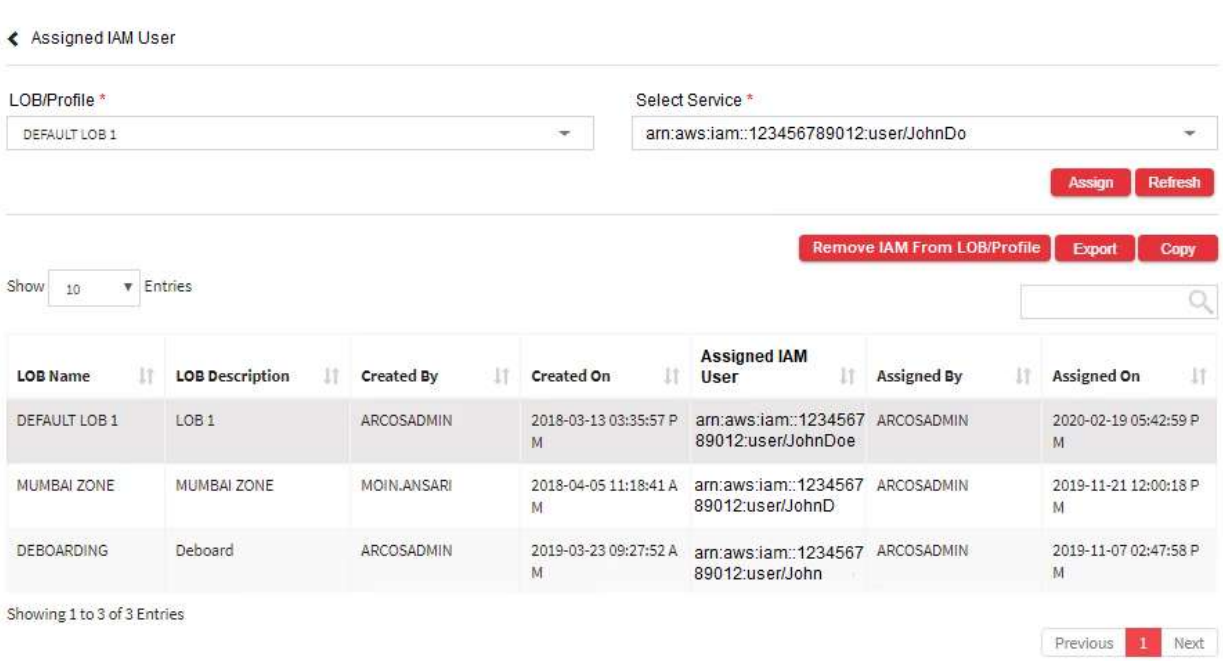
The assigned IAM User feature is used to configure the AWS Credentials for LOB Under the AWS Service Type. The PAM Admin can assign this service to a PAM User in Manage User/Service page in Server Manager. The Admin needs to then set a role for PAM User plus the Service combo in Manage Commands.

> The Administrator having the Assigned IAM User Privileges in server privileges will be able to do the configurations under the Assigned IAM User.

To navigate, use the following path:

Settings → General

1. Select Assigned IAM User



2. Select the service of the Assigned IAM User to the Selected LOB/Profile and click the Assign button
3. The LOB is therefore mapped to the selected service for the assigned IAM User.
4. To remove the IAM from LOB Profile select the row and click Remove IAM from LOB Profile. Also, you can right-click on the row and select Remove IAM from LOB Profile.
5. The Export button will export all the Assigned IAM User details in the form .xlsx format. The Copy button will copy all the details of the table.

13.16 My Vault

13.16.1 File(s)

This section helps you to with configurations to view passwords.
To navigate, use the following path:

Settings → My Vault → Files(s)

Field Name	Description
Allowed File types for upload	**This configuration, if blank will allow you to upload all file formats to My Vault; if file formats are added only these added file formats will be allowed to upload to My Vault.**
Valid Values	jpg, gif, png, txt, pdf are supported.
Upload all files to file vault	**This configuration sets the location for uploaded files in the file vault.**
Disable	If the toggle value is 'Disabled', then it uploads small files(file size less than 10MB) to the database and large files(file size greater than 10 MB) to file server.

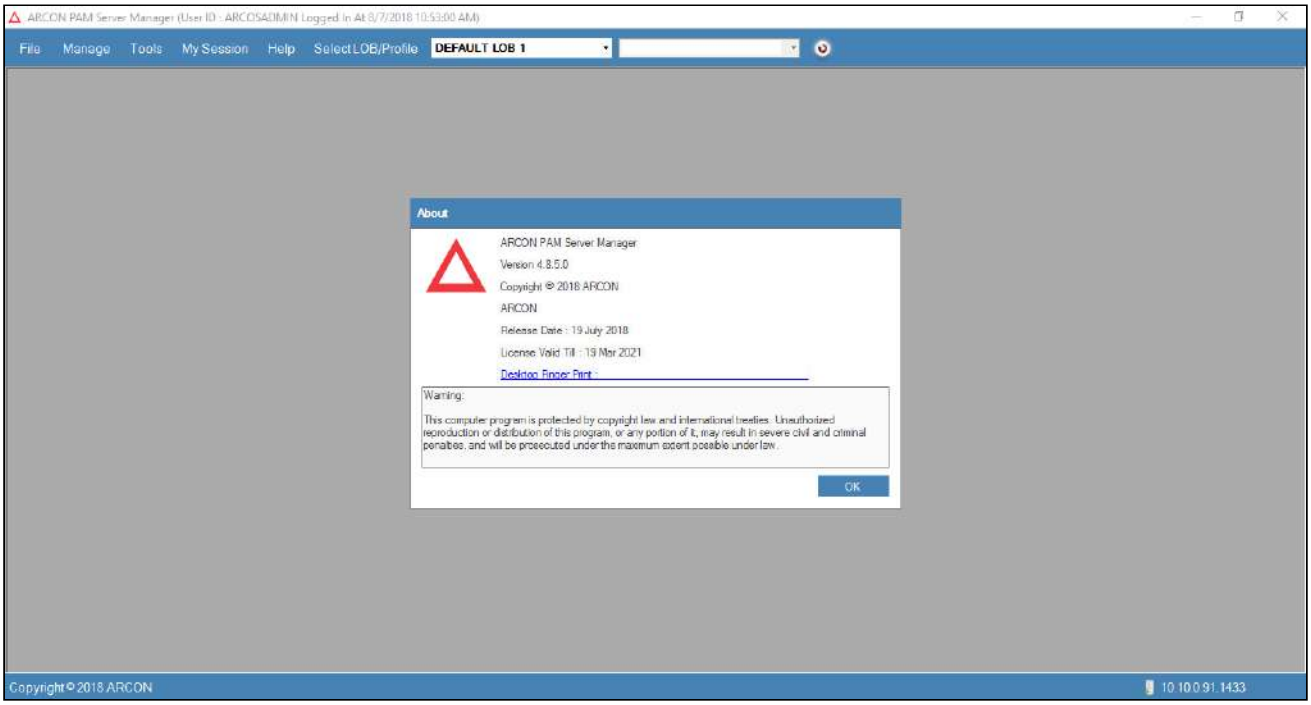
Field Name	Description
Enable	If the toggle value is 'Enabled', then it uploads all the files to the file server.

14 About

About section provides details about **ARCON PAM Server Manager,** which includes Version, its Release Date, License valid till date and Desktop Finger Print.

To navigate to About, use the following path:

Server Manager → Help → About



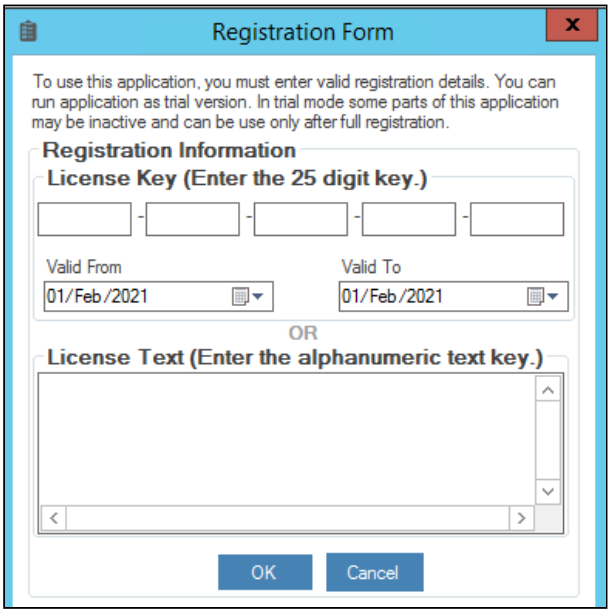
15 License Registration

Registration Form helps you to register in ARCON PAM by entering license key or license text. You will be able to use ARCON PAM only till the valid date displayed in **About** screen. If your license is about to expire, you need to enter the new license key or license text to continue using ARCON PAM.

> ⚠ The License Key or License Text will be provided by ARCON Team.

To navigate to Registration Form, use the following path:

Server Manager → Help → ARCON PAM Registration



Register Using License Key:

1. Enter the 25 digit key in the **License Key (Enter the 25 digit key.)** text boxes.
2. Select the validity dates in **Valid From** and **Valid To** fields.
3. Click **OK** to save settings.

Register Using License Text:

1. Enter the alphanumeric text key in the **License Text (Enter the alphanumeric text key.)** text box.
2. Click **OK** to save settings.

> ⚠ When you register using License Text, the license validity is auto updated in backend.

Privileged Access Management Suite