

Predict | Protect | Prevent

ARCON|PAM

Reports

Table of Contents

- 1 Report Builder Functionalities..... 7
- 2 How to Generate a Report 9
- 3 Exported Reports 10
 - 3.1 Deleting Reports 10
- 4 Dashboard Reports 11
 - 4.1 ARCON PAM Live 11
 - 4.2 Enterprise Password..... 12
 - 4.3 Live Server Sessions..... 13
 - 4.4 User Access & Usage..... 14
- 5 Group Reports 17
 - 5.1 Servers in Server Group 17
 - 5.2 Service Group Report..... 19
 - 5.3 Services in Server Group..... 20
 - 5.4 User Group Report 21
 - 5.5 Users in User Group..... 22
- 6 LOB Reports..... 25
 - 6.1 Active Services Group Wise Report 25
 - 6.2 Active Services Report..... 27
 - 6.3 Active Users Report 29
 - 6.4 Dormant Users Report..... 30
 - 6.5 Inactive Services Report..... 31
 - 6.6 LOB Details Report 33
 - 6.7 Object Status Report 34
 - 6.8 Service Count Report 35
- 7 Logs Reports..... 38
 - 7.1 APEM Logs Report..... 38
 - 7.2 Approval Delegation Report..... 40
 - 7.3 Day Wise Summary Report..... 42
 - 7.4 Day Wise User Access Summary Report 43
 - 7.5 Incident Management Logs..... 43
 - 7.6 Log Review Report..... 45
 - 7.7 My Vault Logs 47
 - 7.8 Outside ARCON PAM Access Log 48

7.9	Service Access Log.....	49
7.10	Service Access Log Day Wise Report.....	51
7.11	Service Password Request Workflow Logs.....	52
7.12	Service Password Status Logs.....	56
7.13	Service Request Workflow Logs.....	57
7.14	Session Activity Log.....	61
7.15	Session Wise Summary Report.....	62
7.16	SIEM Command Logs Report.....	64
7.17	SMS and Email Logs.....	65
7.18	Ticket Request Workflow Logs.....	66
7.19	User Access Log Report.....	70
8	Performance Reports.....	73
8.1	MS SQL Connection Report.....	73
8.2	New Arcon DeskInsight Devices.....	74
8.2.1	New ARCON PAM DeskInsight Devices report in ACMO.....	74
9	Privilege Reports.....	76
9.1	Client Manager Privilege Report.....	76
9.2	Group Admin Privilege Report.....	77
9.3	Server Manager Privilege Report.....	79
9.4	User & Services Privileges.....	80
9.5	User & Services Privileges - Windows RDP.....	82
10	Security Reports.....	84
10.1	Commands Executed on Service Session Detail Report.....	84
10.2	Critical Commands Executed Report.....	86
10.3	High Usage (in hrs) Services Report.....	88
10.4	Invalid Login Attempts Report.....	89
10.5	Low Usage (in days) Services Report.....	91
10.6	Multiple Desktop Logon Report.....	92
10.7	Multiple User Logon Report.....	93
10.8	Network Segment Wise Logon Report.....	94
10.9	Restricted Commands Executed Report.....	95
10.10	Service Access Off Production Hrs Report.....	97
10.11	Service Accessed – Multiple Times Report.....	98
10.12	User Service Accessed - Multiple Times Report.....	99
11	Service Reports.....	101
11.1	Active Services Report.....	101

11.2 Active Session Report 103

11.3 AGW Service Access Report..... 104

11.4 Device Detailed Report 105

11.5 Multiple Service Reference No. Report 107

11.6 Password Envelope Never Generated Report 108

11.7 Password Envelope Print Report..... 109

11.8 Scheduled Password Change Services 110

11.9 Server Last Accessed On..... 112

11.10 Servers in Domain..... 113

11.11 Service Accessed Summary Day Wise Report..... 115

11.12 Service Accessed Summary Report 115

11.13 Service Application Report 116

11.14 Services Creation Deletion Details Report 118

11.15 Services Creation Deletion Summary Report..... 119

11.16 Service Dependency Report 120

11.17 Service Group Wise Service Type Report 121

11.18 Service Timeline Report 122

11.19 Services in Domain Report 123

11.20 Unique Services IP Address Report..... 124

12 User Reports 126

12.1 Active Users Report..... 126

12.2 Consolidated User & Service Mapping Report..... 128

12.3 Dormant User Report..... 130

12.4 Dual Factor Auth Configuration Report 131

12.5 Dual Factor Auth Configuration Report - All LOB..... 133

12.6 Idle Users Report..... 135

12.7 Inactive Users Report..... 137

12.8 Last Service Accessed Report 138

12.9 Locked Out User Report..... 139

12.10 User & Service Mapping Report 140

12.11 User Biometric Auth Report 142

12.12 User Biometric Auth Report - All LOB..... 144

12.13 User Compliance Report 145

12.14 User Creation Deletion Summary Report..... 146

12.15 User Dormant in next 5 day Report..... 147

12.16 User Hardware Auth Report 148

12.17 User Last Logon Report 150

12.18 User Mobile OTP Auth Report 151

12.19 User SMS OTP Auth Report..... 153

12.20 User Status Report 154

13 Vault Reports 156

13.1 Allow Password Change Report..... 156

13.2 Current Password Status Report..... 158

13.3 Maximum Password Failed Attempts Report..... 159

13.4 Restore Service Password Option Used 160

13.5 Service Last Password Failed Reason 161

13.6 Service Password Age Report 162

13.7 Service Password Change Consolidated Report 164

13.8 Service Password Change Failed (Server Unavailable) Report 166

13.9 Service Password Changed Status Report..... 168

13.10 Service Password Changed Status Report - All LOB 170

13.11 Service Password Changed Success/Failed Report 171

13.12 Service Password Check Out Report 172

13.13 Service Password Envelope Print Status Report..... 174

13.14 Service Password Expires in 5 Days Report 175

13.15 Service Password Manually Changed Report..... 177

13.16 Service Password Never Changed Report 178

13.17 Service Password Never Changed Report - All LOB..... 180

13.18 Service Password Security Status Report 181

13.19 Service Password Vaulting Status 182

13.20 Service Password Vaulting Summary Report 185

13.21 Service Password Viewed By Administrator 185

13.22 Service Reached Maximum Failed Attempts 187

13.23 Service Reconcile Status Report 188

13.24 Services Details for SPC - Maximum Failed Attempts 189

13.25 Services Scheduled for SPC 190

13.26 SPC Not Configured Report 192

13.27 SPC Success and Failed Report..... 193

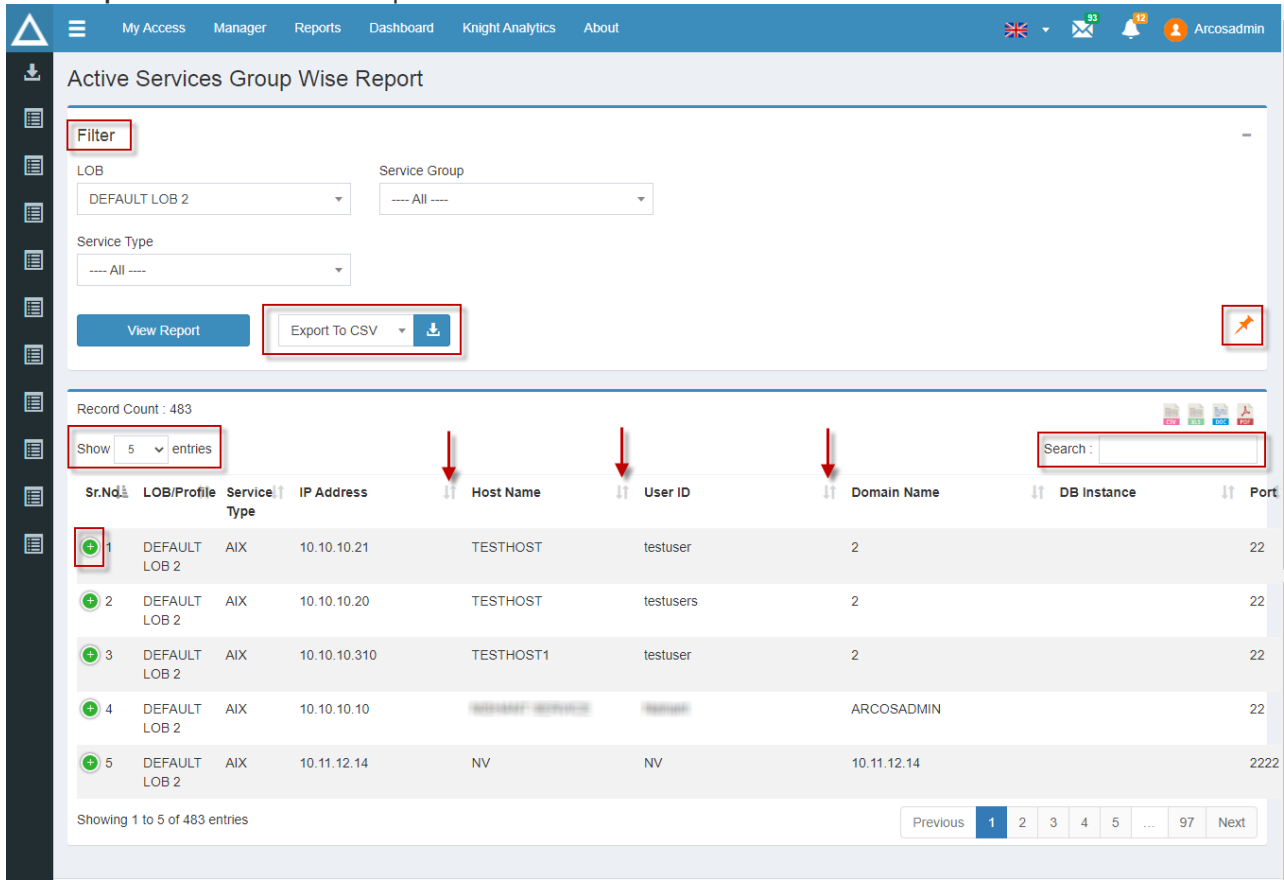
13.28 Users Extracting Password Envelope Report 194

ARCON | PAM provides **reports** of all transactions performed under its systems to help users discover and prioritize important fixes. Reports can be obtained easily from the Client Manager and exported in .xls, .doc, .csv, and .pdf file formats. Reports can be generated automatically, daily, weekly, or monthly, based on the scheduler configured in Server Manager (Refer to Scheduler Master and Schedule Reports for detailed information).

The screenshot shows the ARCON Reports interface. The top navigation bar includes 'My Access', 'Manager', 'Reports' (highlighted with a red box), 'Dashboard', 'Knight Analytics', and 'About'. On the right, there are icons for a flag, a mail icon with '96', a notification bell with '11', and a user profile 'Arcosadmin'. The main content area is titled 'My Services' and features a search bar with a magnifying glass icon. Below the search bar are filters for 'LOB' (set to '9318T2'), 'Service Type' (set to '--Select--'), and 'IP Address / Host Name'. There are also 'All Services' and 'My Favourite' toggle buttons. A 'My Tags' section shows a '--Select--' dropdown with minus and plus buttons. Below this is a 'Filter' button and a 'Show 10 entries' dropdown. A search input field is labeled 'Search:'. The main data area is a table with columns: 'Service Type', 'Host Name', 'Host IP', 'Username', 'Domain', 'Server Type', 'Description 1', 'Description 2', and 'Description 3'. The table contains one row: 'Windows RDP', '10.10.0.126', '10.10.0.126', 'moin.ansari', '10.10.0.126', 'abc', and 'D2'. Action icons (share, lock, star, refresh) are visible at the bottom right of the table row.

1 Report Builder Functionalities

The following report builder functionalities are applicable to all reports on ACMO. The **Active Services Group Wise Report** is shown as an example below:



Refer to the following table to understand the Report Builder Functionalities:

UI Components	Description
Filter	Filtering provides a more advanced and versatile way of controlling which records should be displayed. The filters can be selected from the attributes at the top.
Pin Filter	Filters can be pinned to access the report directly and eliminate the need for selection over and over again.
Show Entries	Display the number of rows selected from the drop-down in the reporting grid.
Searching	The searching filter at the top provides a quick and easy way to reduce the records in the report grid and display only those records that contain the data that you want to see.

UI Components	Description
Sorting	Sort data alphabetically or numerically in ascending/ descending order. This functionality is available at the top of every column.
Pagination	The Report grid at the bottom is paginated. It prints all the data in a table, no matter how long. You can scroll down through all the rows with the stroll bar on the right.
Export to CSV, Excel, Word, and PDF	Export and download any report downloaded in .CSV, .XLS, .DOC or .PDF format.
Expand	Click on the :Plus_icon: icon to view columns that are not displayed because of limited screen size.

2 How to Generate a Report

Reports are generated based on activities performed in PAM. Not all reports are accessible/visible to everyone. Users can view reports only those reports for which they have permission. These permissions have to be assigned by Administrators.

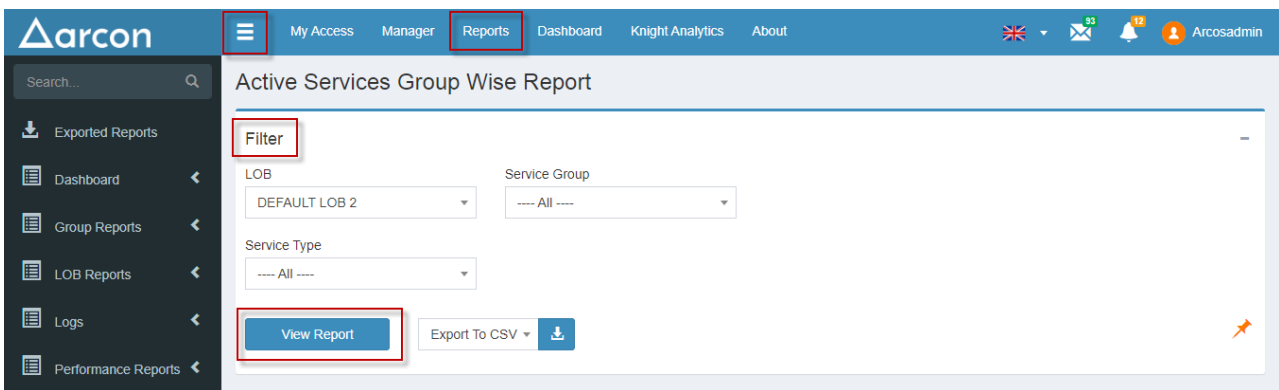
Perform the following steps to generate a report:

1. From the Menu Bar, select the **Reports** menu.
2. Click on the three-line `:3_line_icon:` icon to expand the left pane.
3. Choose the type of report.
4. Apply the required filters in the **Filter** section.
5. Click on the **View Report** button.



Users can see reports across all LOBs only if they have the following privilege(s):

- **Client Manager Privileges - View All LOB**



3 Exported Reports

This section explains how to export the reports requested for download in various formats as shown in the table below. The **Exported Reports** page (also titled **My Report Downloads**) will help you download or delete exported reports record-wise from the list.

Reports can be exported in the following formats:

Format	Procedure
CSV	<ol style="list-style-type: none"> In the Generated Reports list, click on the .csv :c: icon. Select the Email Notification checkbox and enter the email address to receive the report via email. Reports received on emails are usually longer. For example, reports generated for 3 months or more. Smaller reports (generated for less than 90 days) can be downloaded directly from the Exported Report section. The name of the downloaded report will be LOBName_ReportName.csv
XLS	<ol style="list-style-type: none"> In the Generated Reports list, click on the .xls :XLS: icon. Select the Email Notification checkbox and enter the email address to receive the report via email. Reports received on emails are usually longer. For example, reports generated for 3 months or more. Smaller reports (generated for less than 90 days) can be downloaded directly from the Exported Report section. The name of the downloaded report will be LOBName_ReportName.xls
DOC	<ol style="list-style-type: none"> In the Generated Reports list, click on the .doc X icon. Select the Email Notification checkbox and enter the email address to receive the report via email. Reports received on emails are usually longer. For example, reports generated for 3 months or more. Smaller reports (generated for less than 90 days) can be downloaded directly from the Exported Report section. The name of the downloaded report will be LOBName_ReportName.doc
PDF	<ol style="list-style-type: none"> In the Generated Reports list, click on the .pdf :pdf_icon: icon. Select the Email Notification checkbox and enter the email address to receive the report via email. Reports received on emails are usually longer. For example, reports generated for 3 months or more. Smaller reports (generated for less than 90 days) can be downloaded directly from the Exported Report section. The name of the downloaded report will be LOBName_ReportName.pdf

3.1 Deleting Reports

To delete reports in bulk from the **Exported Reports** section, click on the **Check/ Uncheck All** button to select all reports and then click the **Delete Selected Mails** button.

4 Dashboard Reports


The Dashboard displays a graphical view of real-time user interfaces of different activities being performed in ARCON | PAM. It is a graphical view of the user’s access to services in terms of commands fired, password rotation, and status of password security. The Dashboard palette further provides links to view and filter the various reports running in the ARCON | PAM application.

The following reports are available in Dashboard Reports:

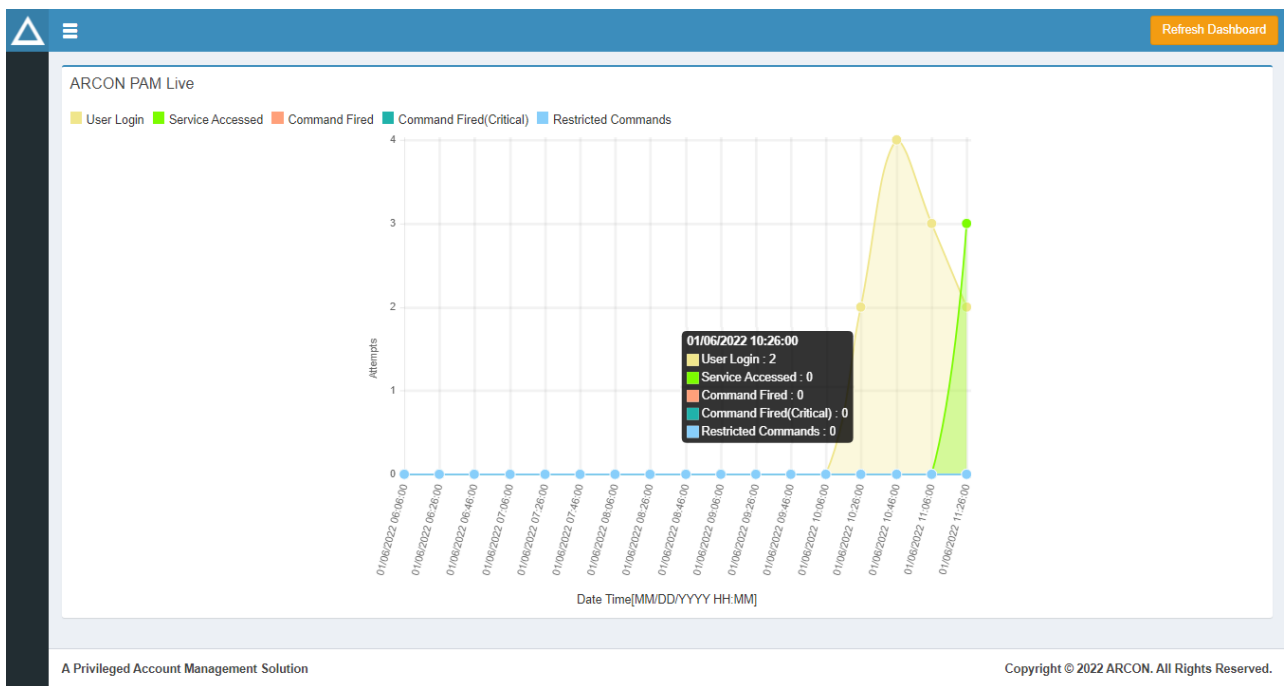
- ARCOS PAM Live
- Enterprise Password
- Live Server Sessions
- User Access & Usage

4.1 ARCON PAM Live

The **ARCON PAM Live** report displays user activity over the last 5 hours as a line graph. It displays the number of users who have logged in, the number of services that have been accessed, the total number of commands that have been fired, and the number of critical and restricted commands that have been fired.

 In order to view this report, users must have the following permission(s):

- **ARCON PAM Live**



Drag and navigate the cursor anywhere on the graph to view the exact count details.

For instance, In the above figure, you can see that at **10:26:00 AM** on **01/06/2022** there were only two users logged in, zero Services Accessed, zero Commands Fired (both Critical and Non-Critical), and zero Restricted Commands.

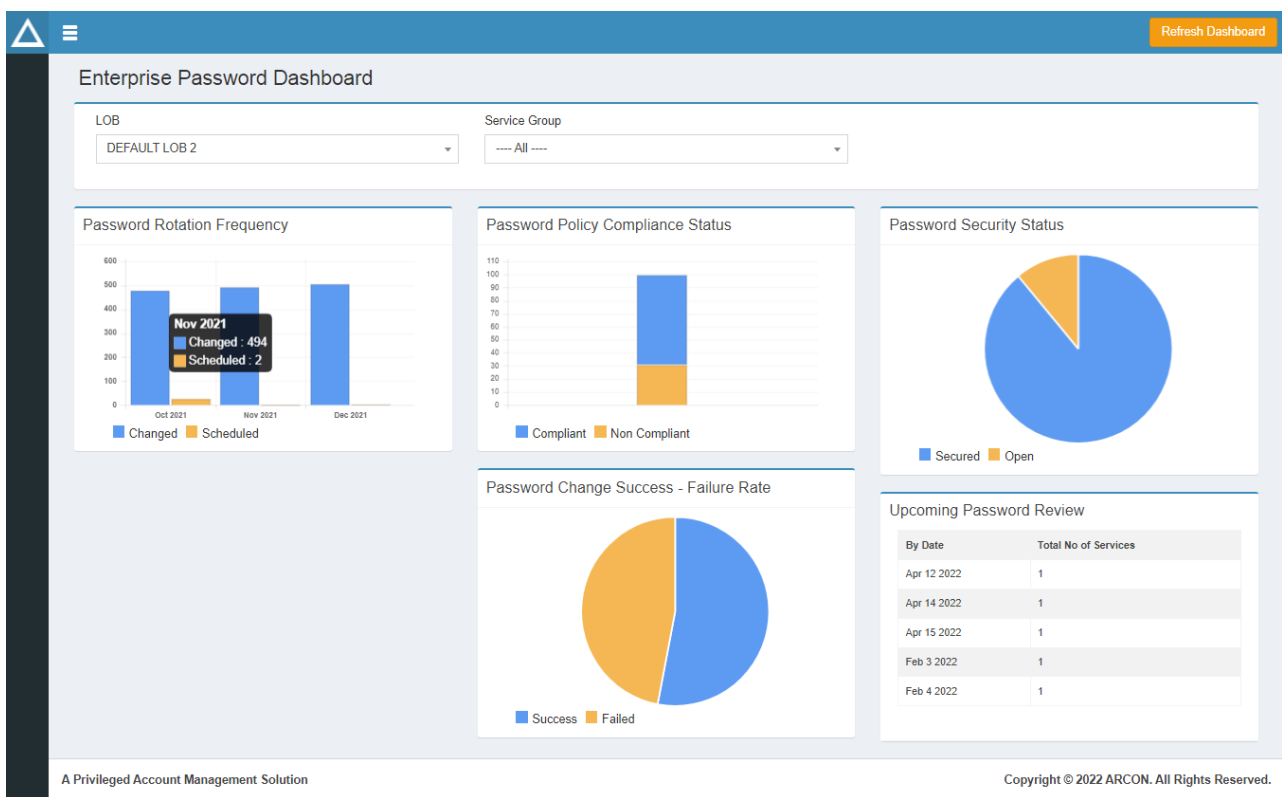
i Click on the **Refresh Dashboard** button on the extreme right-hand side of the report window to refresh the report.

4.2 Enterprise Password

The **Enterprise Password** report displays a dashboard that gives information about the rotation frequency of passwords changed and scheduled, the compliant status of the password, security status of the password (open or closed), the success/failure rate of the password change, and provides a table containing information about upcoming password reviews.

! In order to view this report, users must have the following permission(s):

- **Enterprise Password**




Drag and navigate the cursor anywhere on the graph to view the exact count details.

For example, the **Password Rotation Frequency** graph above shows the **Changed** password and the **Scheduled** password for **November 2021**.



i Click on the **Refresh Dashboard** button on the extreme right-hand side of the report window to refresh the report.

4.3 Live Server Sessions

The **Live Server Sessions** report displays a list of ongoing sessions, services that users have accessed. Information about access to critical servers is shown in a table and through pie graphs. The most-used servers are displayed as a bar graph.

 In order to view this report, users must have the following permission(s):

- **Live Server Sessions**

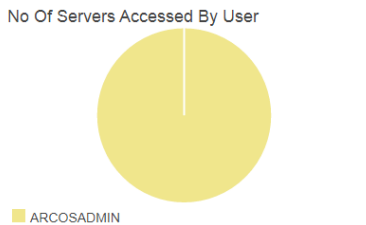
 
Refresh Dashboard

Live Server Sessions

LOB: DEFAULT LOB 2

Service Group: ---- All ----

No Of Servers Accessed By User

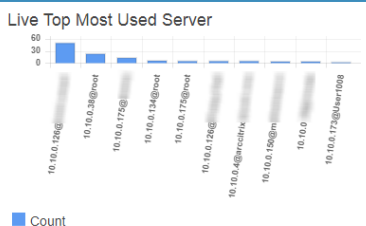


ARCOSADMIN

List Of Servers Accessed By User

User ID	Service Type	Service IP Address	Service User Name	Accessed At
ARCOSADMIN	App SQL Developer - Oracle	10.10.0.154	super	01/12/2022 12:43:01
ARCOSADMIN	App SQL Developer - Oracle	10.10.0.154	super	01/12/2022 12:42:44
ARCOSADMIN	App SAPHana	10.10.1.0	abc	01/12/2022 12:41:11
ARCOSADMIN	SSH LINUX	10.10.0.89	ARCOSADMIN	01/11/2022 16:22:03
ARCOSADMIN	SSH LINUX	10.10.0.89	ARCOSADMIN	01/11/2022 16:08:51
ARCOSADMIN	Windows RDP	10.10.0.58	ARCOSADMIN	01/11/2022 15:57:41
ARCOSADMIN	Windows RDP	10.10.0.64	LAMTest1	01/11/2022 15:47:17
ARCOSADMIN	SSH LINUX	13.232.49.179	ARCOSADMIN	01/11/2022 15:46:41
ARCOSADMIN	SSH LINUX	10.10.0.89	ARCOSADMIN	01/11/2022 15:46:21

Live Top Most Used Server




Count

No Of Servers Accessed With Privileged ID (High Critical Server)

undefined

List Of Servers Accessed By User (High Critical Server)

User ID	Service Type	Service IP Address	Service User Name	Accessed At
ARCOSADMIN	Windows RDP	99.99.99.98	RDP998	06/04/2021 11:25:22
ARCOSADMIN	Windows RDP	99.99.99.98	RDP998	06/04/2021 11:12:41

 Click on the **Refresh Dashboard** button on the extreme right-hand side of the report window to refresh the report.

4.4 User Access & Usage

The **User Access & Usage** report gives information about criticality-based user activity, time-based user activity, service access, high usage service accounts, and provides a table containing information about critical commands and their count.



In order to view this report, users must have the following permission(s):

- **User Access & Usage**

User Access And Usage Dashboard

Refresh Dashboard

LOB: DEFAULT LOB 1 | Service Group: --- All --- | User Group: --- All --- | User ID:

View Report

Criticality Based User Activity (No. of time servers accessed)

Criticality	Nov 2021	Dec 2021	Jan 2022
None	20	68	0
Low	36	38	0
Medium	0	0	0
High	0	28	0

Critical Command Usage

Critical Command	Count
cal	36
at	21
sudo	9
clear	6
date	6

Time Based User Activity (No. of time servers accessed)

Time Interval	Nov 2021	Dec 2021	Jan 2022
12:00 AM - 07:59 AM	2	12	0
08:00 AM - 02:59 PM	18	32	0
03:00 PM - 08:59 PM	30	85	0
09:00 PM - 11:59 PM	2	0	0

Services Access Report

High Usage Service Accounts

Date	Usage Count
Dec 12 2021	14
Nov 15 2021	5
Nov 22 2021	6
Dec 20 2021	5
Dec 2 2021	7
Dec 2 2021	5
Dec 2 2021	20
Dec 6 2021	6

A Privileged Account Management Solution | Copyright © 2022 ARCON. All Rights Reserved.

Drag and navigate the cursor anywhere on the graph to view the exact count details.

For example, the **Criticality Based User Activity** graph shows the exact count of the servers accessed in the month of November, December, and January of **Low Critical Status**.



Click on the **Refresh Dashboard** button on the extreme right-hand side of the report window to refresh the report.

5 Group Reports

Group Reports generate details for all ARCON | PAM groups such as service groups and user groups.

The following reports are available in Group Reports:

- Servers In Server Group
- Service Group Report
- Services in Server Group
- User Group Report
- Users in User Group

5.1 Servers in Server Group

The **Servers in Server Group** report displays details of all the servers created in a Server Group, regardless of the LOB. The information is represented in a graphical and grid view format, based on the server's IP address.



In order to view this report, users must have the following permission(s):

- **Servers In Server Group**


The following columns can be seen in this report:

Column Name	Description
Sr. No.	To identify and distinguish rows
IP Address	Displays IP address of the target servers
Host Name	Displays hostname of the target servers
Instance	Displays instance of the target servers
Port	Displays port number of the target server (if configured)
Domain Name	Displays the domain name to which the target server belongs

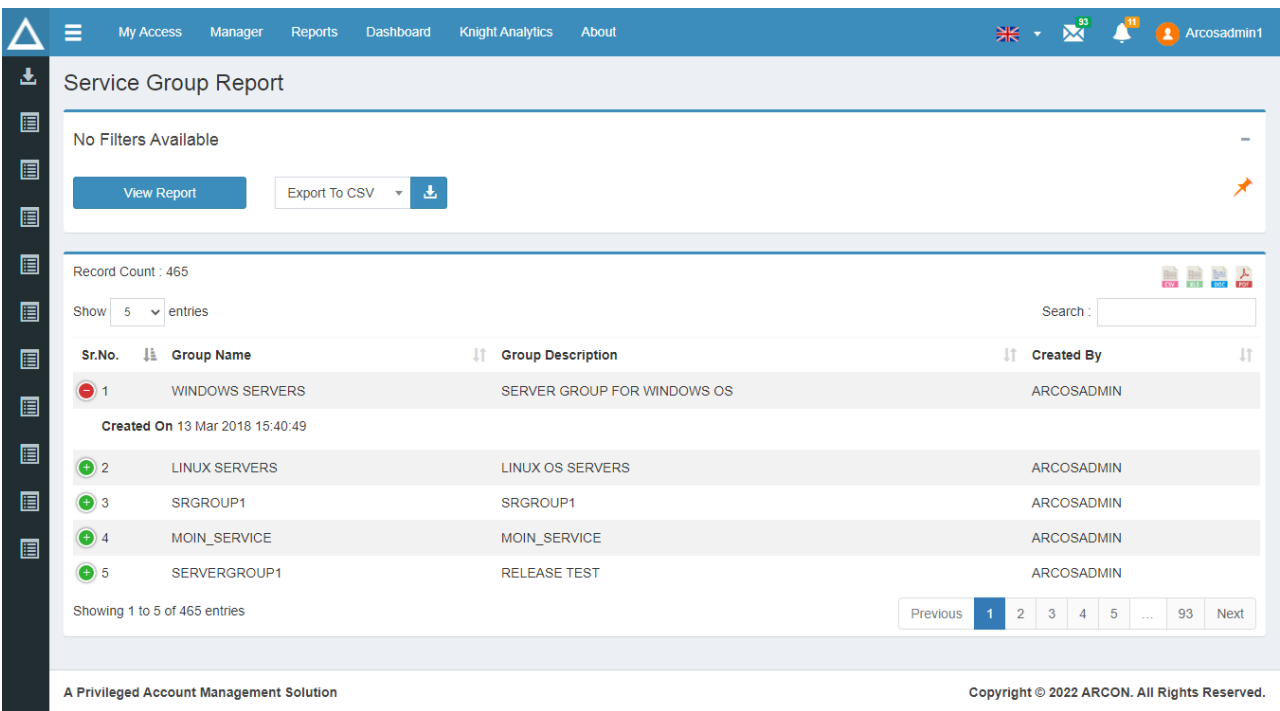
Column Name	Description
Service Group	Displays the service group name to which that particular server belongs
LOB/Profile	Displays name of the LOB for which the server is configured

5.2 Service Group Report

Service Group Report provides information about all of the service groups created in ARCON | PAM, regardless of the LOB.

 In order to view this report, users must have the following permission(s):

- **Service Group Report**




The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Group Name	The name of service group
Group Description	Text entered during the creation of the service group
Created By	The name of the user who created the service group

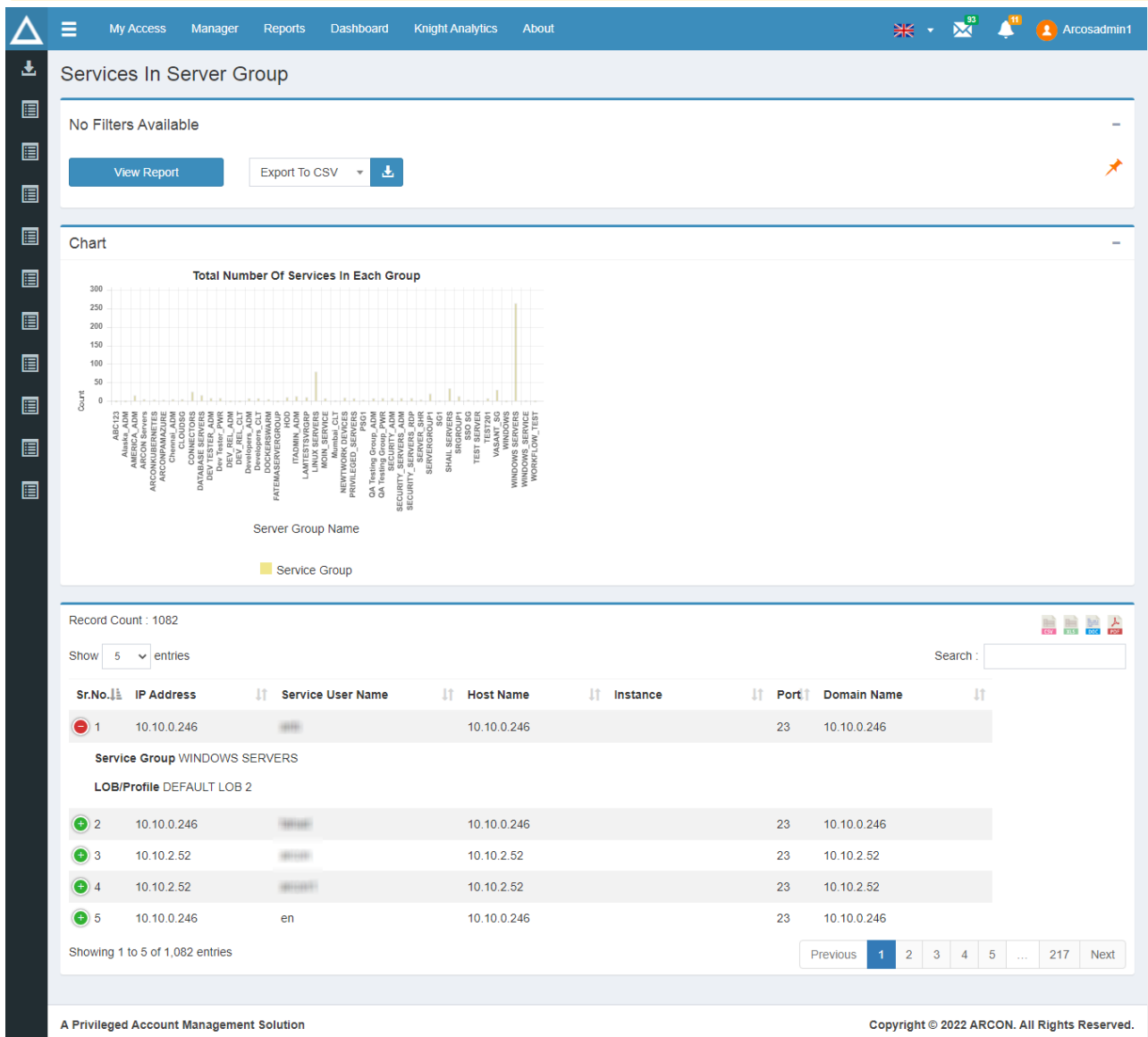
Column Names	Description
Created On	Date/time of the creation of the service group

5.3 Services in Server Group

The **Services in Server Group** report displays information about all of the services created in a Server Group, regardless of the LOB. The information is represented in a graphical and grid view format, based on the Service username of the server.

 In order to view this report, users must have the following permission(s):

- **Services in Server Group**




The screenshot shows the 'Services In Server Group' report interface. At the top, there is a navigation bar with 'My Access', 'Manager', 'Reports', 'Dashboard', 'Knight Analytics', and 'About'. The main content area is titled 'Services In Server Group' and includes a 'No Filters Available' section with 'View Report' and 'Export To CSV' buttons. Below this is a bar chart titled 'Total Number Of Services In Each Group' showing the count of services for various server group names. The chart shows a significant peak for 'WINDOWS_SERVERS'. Below the chart is a table with columns: Sr.No., IP Address, Service User Name, Host Name, Instance, Port, and Domain Name. The table displays 5 entries, with the first entry having a red minus icon and the others having green plus icons. The footer contains 'A Privileged Account Management Solution' and 'Copyright © 2022 ARCON. All Rights Reserved.'

The following columns can be seen in this report:

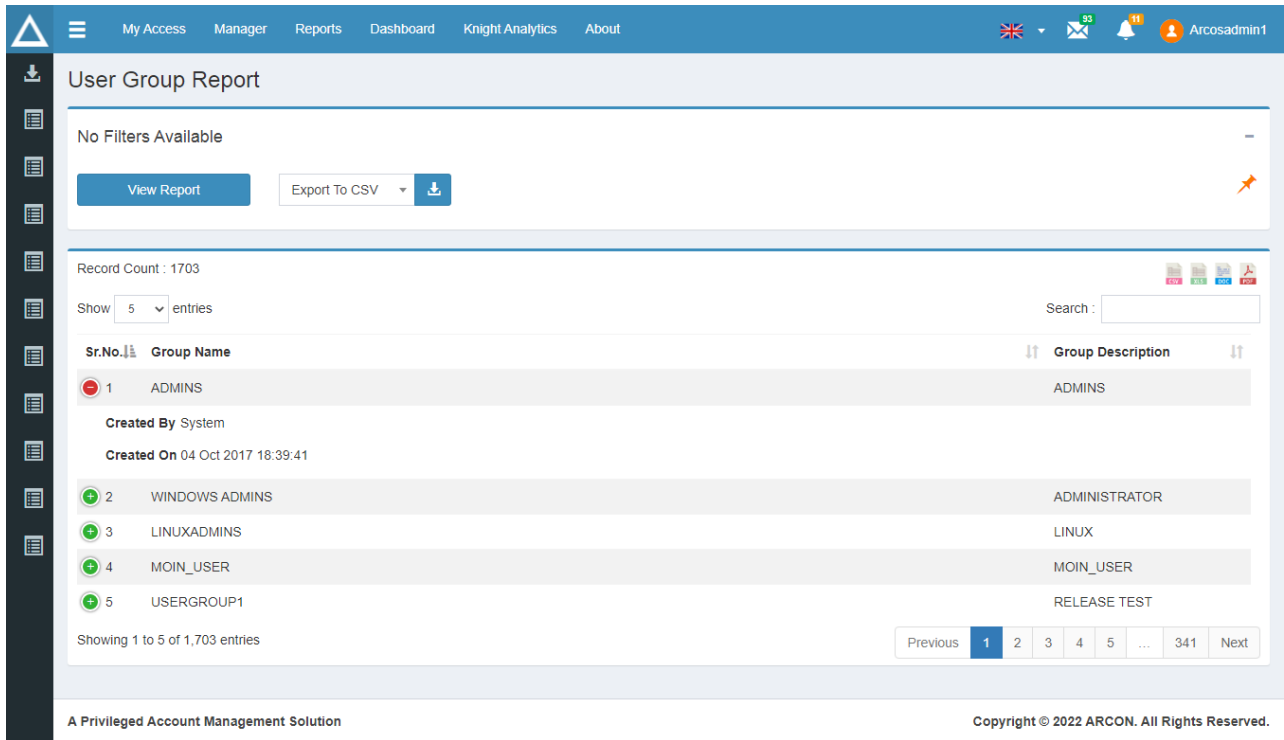
Column Names	Description
Sr. No.	To identify and distinguish rows
IP Address	The IP address of the target servers
Service User Name	The username of the service
Host Name	The hostname of the target servers
Instance	The instance of the target servers
Port	The port number of the target server (if configured)
Domain Name	The domain name to which the target server belongs
Service Group	The service group name to which that particular server belongs
LOB/Profile	The name of the LOB for which the server is configured

5.4 User Group Report

The **User Group Report** provides information about all of the user groups created in ARCON | PAM, regardless of the LOB.

 In order to view this report, users must have the following permission(s):

- **User Group Report**




The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Group Name	The name of the user group
Group Description	Text entered during the creation of the user group
Created By	The name of the Administrator who created the user group
Created On	Date/time of the creation of the user group by the Administrator

5.5 Users in User Group

The **Users in User Group** report displays information about all of the users created in a User Group, regardless of the LOB. The information is represented in a graphical and grid view format, based on the Service username of the server.

 In order to view this report, users must have the following permission(s):

- **Users in User Group**

Record Count : 20436

Show 5 entries

Search :

Sr.No.	Username	Display Name	User Group
1	ADMINISTRATOR	ADMINISTRATOR	USERGROUP1
Domain ADMINSTRATOR			
User Type Admin			
2	\$872000-F8NPG221BGHB		Bulk_User
3	\$A72000-CKRI01K4QFJ4		Bulk_User
4	\$H72000-2CE6KP8UHKF1		Bulk_User
5	\$J72000-53VAV0VTB1M3		Bulk_User

Showing 1 to 5 of 20,436 entries

Previous 1 2 3 4 5 ... 4088 Next

A Privileged Account Management Solution Copyright © 2022 ARCON. All Rights Reserved.

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
User name	The name of the user
Display Name	The display name of the user
User Group	User group name to which that particular user belongs
Domain	The domain name to which that user belongs

Column Names	Description
User Type	Type of user <ul style="list-style-type: none">• Client• Admin

6 LOB Reports

LOB Reports generate details for all ARCON | PAM LOBs and their relationships with PAM entities such as users, services, groups, etc. It helps generate a graphical view and exact count of group-wise details of users and services that are active and inactive in ARCON | PAM. In addition, it also displays detailed descriptions of all the LOBs created in ARCON | PAM, descriptions of the objects mapped to LOBs, and LOB-wise status of unique IP addresses and services.

The following reports are available in LOB Reports:

- Active Services Group Wise Report
- Active Services Report
- Active Users Report
- Dormant Users Report
- Inactive Services Report
- LOB Details Report
- Object Status Report
- Service Count Report

6.1 Active Services Group Wise Report

Active Services Group Wise Report gives information about all active services in ARCON | PAM service groups.



In order to view this report, users must have the following permission(s):

- **Active Services Group Wise Report**

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
LOB/Profile	The name of the LOB in which there are active services
Service Type	The active service type for the selected server group
IP Address	The IP address of the target server
Host Name	The hostname of the target server
User ID	The User ID associated with the user
Domain Name	The domain name to which the target server belongs

Column Names	Description
DB Instance	The instance of the target servers
Port	The port number of the target server (if configured)
Description 1	Text entered during the creation of the service
Description 2	Text entered during the creation of the service
Description 3	Text entered during the creation of the service
Active Till	The date until which the service will work

6.2 Active Services Report

Active Services Report gives information about all active services in ARCON | PAM. Active services are ones whose validity has not expired yet.



In order to view this report, users must have the following permission(s):

- **Active Services Report**


The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Username	Username given to the service by the Administrator
Server IP	The IP address of the target server
Service Type	The active service type
Service Group	The server group to which the service belongs
Description 1	Text entered during the creation of the service by the Administrator
Service Valid Till	Date/time until which the service will work
Assign By	The Administrator who allocated the service to the LOB

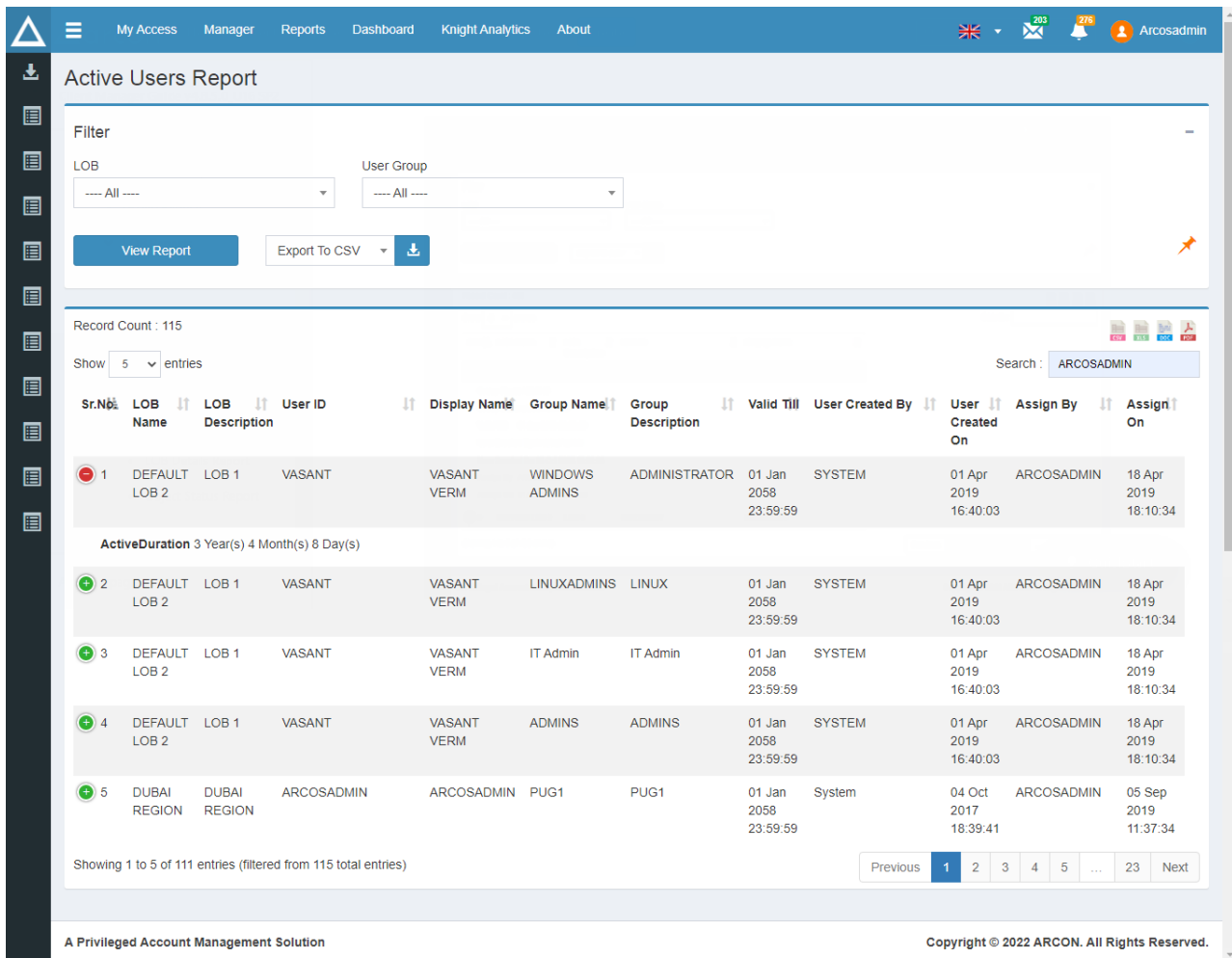
Column Names	Description
Assign On	Date/time of allocation of service to LOB by the Administrator
Vault Status	The status of the vault <ul style="list-style-type: none"> Manually Vaulted Vaulted Not Vaulted
Last Accessed Time	Date/time on which the service was last used

6.3 Active Users Report

The Active Users Report gives information about all active users and their related LOBs in ARCON | PAM. An active user is defined as one who has interacted with the PAM application within a certain time period.

 In order to view this report, users must have the following permission(s):

- Active Users Report**



Active Users Report

Filter

LOB: User Group:

Record Count : 115

Show entries

Search :

Sr.No	LOB Name	LOB Description	User ID	Display Name	Group Name	Group Description	Valid Till	User Created By	User Created On	Assign By	Assign On
1	DEFAULT LOB 2	LOB 1	VASANT	VASANT VERM	WINDOWS ADMINS	ADMINISTRATOR	01 Jan 2058 23:59:59	SYSTEM	01 Apr 2019 16:40:03	ARCOSADMIN	18 Apr 2019 18:10:34
ActiveDuration 3 Year(s) 4 Month(s) 8 Day(s)											
2	DEFAULT LOB 2	LOB 1	VASANT	VASANT VERM	LINUXADMINS	LINUX	01 Jan 2058 23:59:59	SYSTEM	01 Apr 2019 16:40:03	ARCOSADMIN	18 Apr 2019 18:10:34
3	DEFAULT LOB 2	LOB 1	VASANT	VASANT VERM	IT Admin	IT Admin	01 Jan 2058 23:59:59	SYSTEM	01 Apr 2019 16:40:03	ARCOSADMIN	18 Apr 2019 18:10:34
4	DEFAULT LOB 2	LOB 1	VASANT	VASANT VERM	ADMINS	ADMINS	01 Jan 2058 23:59:59	SYSTEM	01 Apr 2019 16:40:03	ARCOSADMIN	18 Apr 2019 18:10:34
5	DUBAI REGION	DUBAI REGION	ARCOSADMIN	ARCOSADMIN	PUG1	PUG1	01 Jan 2058 23:59:59	System	04 Oct 2017 18:39:41	ARCOSADMIN	05 Sep 2019 11:37:34

Showing 1 to 5 of 111 entries (filtered from 115 total entries)

Previous ... Next


A Privileged Account Management Solution Copyright © 2022 ARCON. All Rights Reserved.

The following columns can be seen in this report:

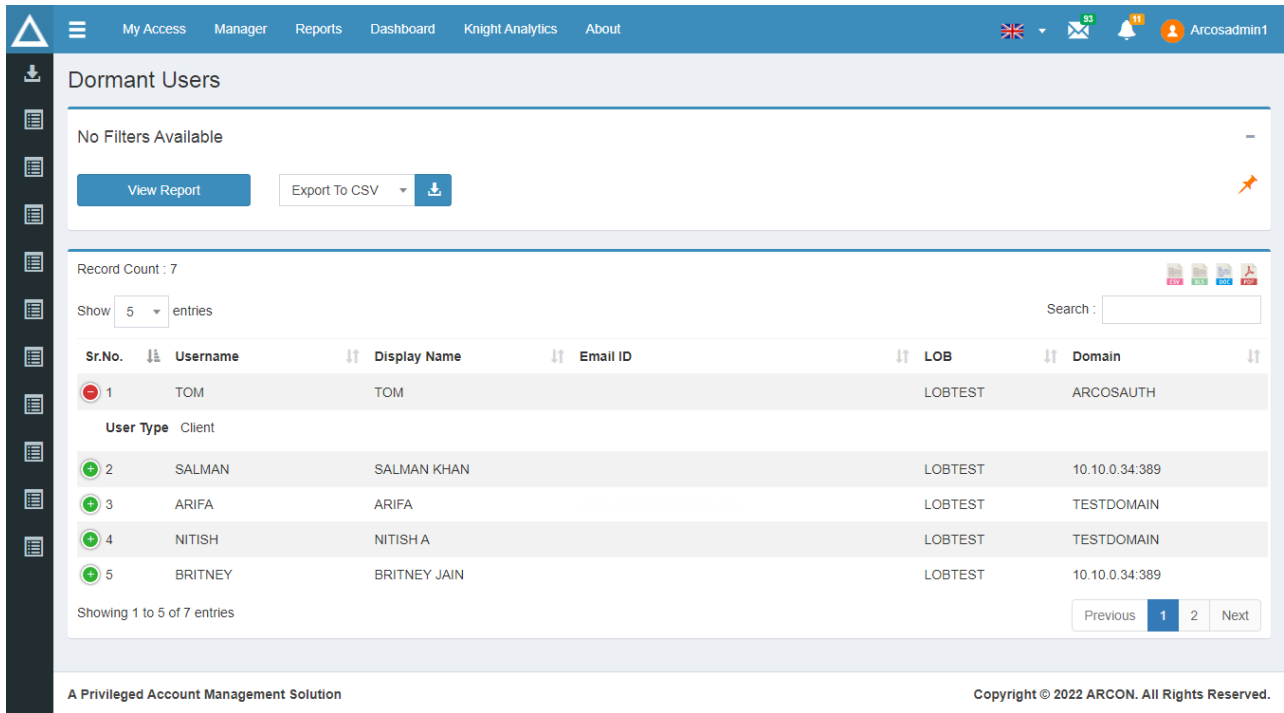
Column Names	Description
Sr. No.	To identify and distinguish rows
LOB Name	Name of the LOB that has active users
LOB Description	Description of the LOB that has active users
User ID	The User ID associated with the user
Display Name	The display name of the user
Group Name	User group name to which that particular user belongs
Group Description	Text entered during the creation of the user group
Valid Till	Date until which the user will be active
User Created By	The name of the Administrator who created the user
User Created On	Date-time of the creation of the user by Administrator
Assign By	The Administrator who allocated the user to the LOB
Assign On	Date/time of allocation of the user to LOB by the Administrator
Active Duration	Total time duration since the user is active.

6.4 Dormant Users Report

The Dormant Users Report gives information about all dormant users and their related LOBs in ARCON PAM. A dormant user is one who hasn't interacted with the PAM application in a certain period of time.

 In order to view this report, users must have the following permission(s):

- **Dormant Users Report**



Dormant Users

No Filters Available

View Report Export To CSV

Record Count : 7

Show 5 entries Search :

Sr.No.	Username	Display Name	Email ID	LOB	Domain
1	TOM	TOM		LOBTEST	ARCOSAUTH
User Type Client					
2	SALMAN	SALMAN KHAN		LOBTEST	10.10.0.34:389
3	ARIFA	ARIFA		LOBTEST	TESTDOMAIN
4	NITISH	NITISH A		LOBTEST	TESTDOMAIN
5	BRITNEY	BRITNEY JAIN		LOBTEST	10.10.0.34:389

Showing 1 to 5 of 7 entries Previous 1 2 Next


A Privileged Account Management Solution Copyright © 2022 ARCON. All Rights Reserved.

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Username	The name of the user
Display Name	The display name of the user
Email ID	Email ID of the user
LOB	The name of the LOB in which the user is present
Domain	The domain name to which the user belongs
User Type	Type of user <ul style="list-style-type: none"> • Client • Admin

6.5 Inactive Services Report

The Inactive Services Report gives information about all inactive services and their related LOBs in ARCON | PAM.

 In order to view this report, users must have the following permission(s):


- **Inactive Services Report**

The following columns can be seen in this report:

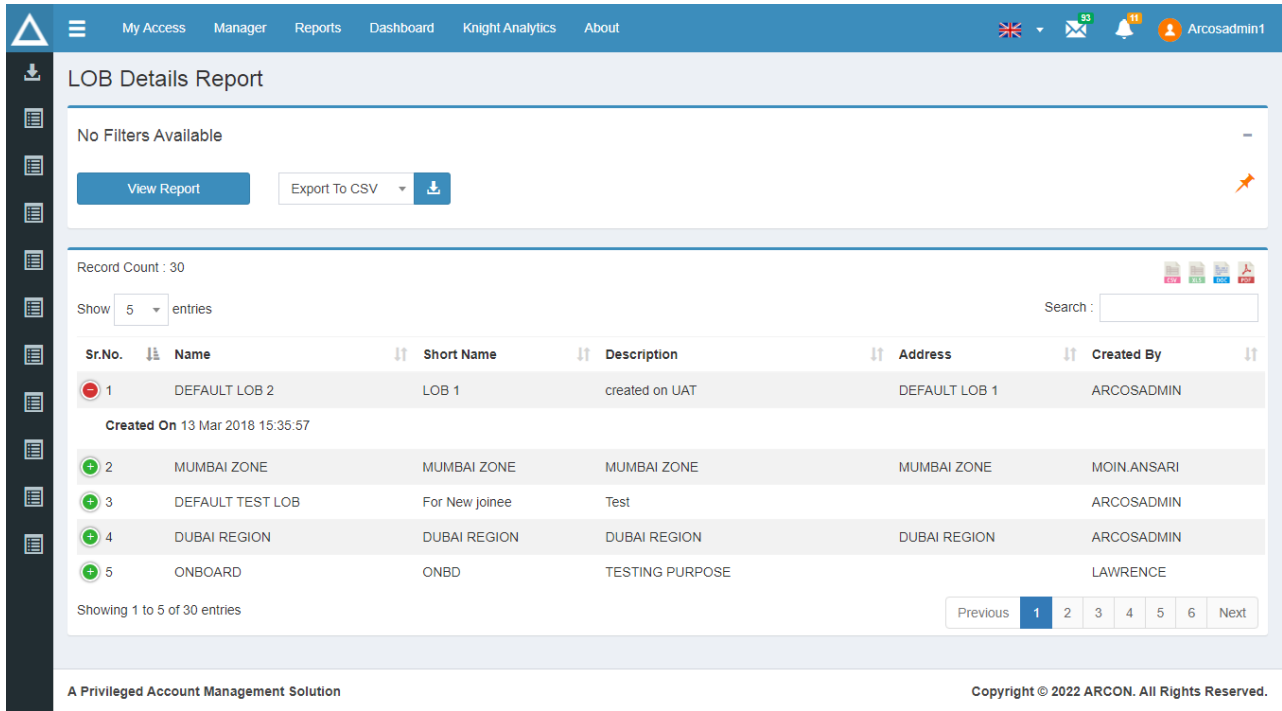
Column Names	Description
Sr. No.	To identify and distinguish rows
LOB Name	Name of the LOB that has active users
LOB Description	Description of the LOB that has active users
Username	The name of the user
Server IP	The IP address of the target server
Service Type	The inactive service type
Service Valid Till	Date/time until which the service will work
Assign By	The Administrator who allocated the user to the LOB
Assign On	Date/time of allocation of the user to LOB by the Administrator
Last Accessed Time	Date/time at which the service was last used

6.6 LOB Details Report

The LOB Details Report gives information about all the LOBs created in ARCON | PAM.

 In order to view this report, users must have the following permission(s):

- **LOB Details Report**



The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Name	Name of the LOB that was created
Short Name	Short name assigned to that LOB
Description	Description of the LOB entered by the Administrator at the time of creation
Address	LOB Address
Created By	The name of the Administrator who created the LOB
Created On	Date/time of the creation of the user by the Administrator

6.7 Object Status Report

The Object Status Report gives information about the relationship between PAM entities (objects) and LOBs. The information is represented in a graphical and grid view format and gives the exact count of the total number of objects that are mapped to LOB.



In order to view this report, users must have the following permission(s):

- Object Status Report

My Access Manager Reports Dashboard Knight Analytics About

Arcosadmin1

Object Status Report

No Filters Available

View Report
Export To CSV
↓

Chart

ABC
 9318TESTING
 9318T2
 MUMBAI ZONE
 DUBAI REGION

LOBTTEST
 TESTLOB
 HIRENTEST
 TESTSSOLOB2
 DEFAULT LOB 2

DEFAULT TEST LOB
 LOADTEST_LOB
 通用管理者
 9318T3

TEST_KARISHMA
 AUTOMATION_LOB
 ONBOARD
 DEBOARDING

YASHTEST
 MUMBAI
 TEJAL LOB
 TEST_LOB1
 TESTSSOLOB

Record Count : 23

Show 5 entries Search :

Sr.No	LOB Profile Name	LOB Profile Description	Active Users	Inactive Users	Active Services	Inactive Services	Active Unique IP	Inactive Unique IP	User Groups
1	ABC	abc	0	0	2	0	1	0	0
2	9318TESTING	9318T	0	0	0	0	0	0	0
3	9318T2	9318T2	2	0	3	1	3	1	0
4	MUMBAI ZONE	MUMBAI ZONE	3	2	9	5	7	3	8
Service Groups 47									
5	DUBAI REGION	DUBAI REGION	3	1	7	2	2	1	1

Showing 1 to 5 of 23 entries
Previous
1
2
3
4
5
Next

A Privileged Account Management Solution
Copyright © 2022 ARCON. All Rights Reserved.

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
LOB Profile Name	Name of the LOB
LOB Profile Description	Description of the LOB entered by the Administrator at the time of the creation
Active Users	Count of active users LOB-wise
Inactive Users	Count of inactive users LOB-wise
Active Services	Count of active services LOB-wise
Inactive Services	Count of inactive services LOB-wise
Active Unique IP	Count of active unique IPs LOB-wise
Inactive Unique IP	Count of inactive unique IPs LOB-wise
User Groups	Count of user groups LOB-wise
Service Groups	Count of service groups LOB-wise

6.8 Service Count Report

The Service Count Report gives information about the relationship between PAM services and LOBs. The information is represented in a graphical and grid view format and gives the exact count of:

- Unique (Active & Inactive) IP status LOB-wise
- Service (Active & Inactive) status LOB-wise



In order to view this report, users must have the following permission(s):

- **Service Count Report**

My Access | Manager | Reports | Dashboard | Knight Analytics | About

 |
 |
 |
 Arcosadmin1

Service Count Report

No Filters Available

View Report
Export To CSV
↓

Chart

LOB Wise Unique IP Status

DEFAULT LOB 2

- Unique Active IPAddress : 304
- Unique Inactive IPAddress : 25

LOB Wise Services Status

DEFAULT LOB 2

- Active Services : 521
- Inactive Services : 30

Record Count : 6394

Show 5 entries

📄 📄 📄 📄 📄

Sr.No.	LOB Profile Name	LOB Profile Description	Service Type	Active Services	Inactive Services	Unique Active IPAddress
1	TEST_KARISHIMA	test	AIX	0	0	0
Unique Inactive IPAddress 0						
2	TEST_KARISHIMA	test	Amazon Web Services (AWS)	0	0	0
3	TEST_KARISHIMA	test	App 3Par Mgmt	0	0	0
4	TEST_KARISHIMA	test	App AblInitioGDE	0	0	0
5	TEST_KARISHIMA	test	App Account and Voucher Info Manager	0	0	0

Showing 1 to 5 of 6,394 entries

Previous
1
2
3
4
5
...
1279
Next

A Privileged Account Management Solution
Copyright © 2022 ARCON. All Rights Reserved.

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
LOB Profile Name	Name of the LOB
LOB Profile Description	Description of the LOB entered by the Administrator at the time of the creation
Service Type	Name of the service type
Active Services	Count of active services LOB-wise
Inactive Services	Count of inactive services LOB-wise
Unique Active IPAddress	Count of active unique IPs LOB-wise

Column Names	Description
Unique Inactive IPAddress	Count of inactive unique IPs LOB-wise

7 Logs Reports

Logs Reports capture details of all the available logs in a report format.

The following reports are available in Logs Reports:

- APEM Logs
- Approval Delegation Report
- Day Wise Summary Report
- Day Wise User Access Summary Report
- Log Review Report
- My Vault Logs
- Outside ARCON PAM Access Log
- Service Access Log
- Service Access Log Day Wise Report
- Service Password Request Workflow Logs
- Service Password Status Logs
- Service Request Workflow Logs
- Session Activity Log
- Session Wise Summary Report
- SIEM command logs Report
- SMS and Email Logs
- Ticket Request Workflow Logs
- User Access Log report

7.1 APEM Logs Report

The APEM Logs Report captures print password activities performed via the APEM tool.



In order to view this report, users must have the following permission(s):

- **APEM Logs Report**

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
File Name	Name of the file
Activity Performed	Captures all the print password actions taken through the APEM tool <ul style="list-style-type: none"> • APEM tool opened • Password Viewed • Read File • Read File process completed • SSH key file successfully downloaded
Envelope No.	The unique number associated with each generated envelope
Envelope Generated On	Date/time of generation of the envelope by the Administrator
Envelope Generated By	The Administrator who generated the envelope

Column Names	Description
Service Type	Name of the service type
Service IP Address	The IP address of the target server for which the password is opened through the APEM tool
Server name	Name of the server
Server user name	Username assigned to the server
Domain Name	The domain name to which the target server belongs
Description 1	Text entered during the creation of the service
Description 2	Text entered during the creation of the service
Description 3	Text entered during the creation of the service
Desktop Details	Details of desktop
Log Date	Date of log

7.2 Approval Delegation Report

The Approval Delegation Report keeps track of operations performed in the ARCON | PAM delegation module. Delegation is the process of transferring ownership to a higher-level employee in order to complete transactions such as approving raised requests.



In order to view this report, users must have the following permission(s):

- **Approval Delegation Report**


The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Operation	Actions that are taken on delegation <ul style="list-style-type: none"> • Create • Modify • Delete
Delegated By	User who sets the delegation module
Delegated To	User who becomes the approver in the absence of actual approver set in the workflow
Approval Type	Type of approvals users
Start Date	Date/time from which the delegation is active
End Date	Date/time until which the delegation will be active
Is Active	If the module is ON
Created By	The name of the user who created the delegation
Created On	Date/time of the creation of the delegation by the user
Modified By	The user who changed an existing delegation module
Last Modified On	Date/time of change in delegation module

Column Names	Description
Date	Date/time of appointment of the module

7.3 Day Wise Summary Report

The Day Wise Summary Report displays the date- and time-wise count of activities performed on the Server.

 In order to view this report, users must have the following permission(s):

- **Day-wise Summary Report**

Sr.No.	Day	Time	Session Count	User Count	Critical Command	Restricted Command	Open Password
1	2019-10-20	02:00 PM - 03:00 PM	31	31	0	0	0
Restricted Process 0							
2	2019-10-20	03:00 PM - 04:00 PM	8	8	0	0	0
3	2019-10-20	04:00 PM - 05:00 PM	4	4	0	0	0
4	2019-10-20	12:00 PM - 01:00 PM	2	2	0	0	0
5	2019-10-21	01:00 PM - 02:00 PM	1	1	0	0	0

 The interface also includes a search bar, pagination controls (Showing 1 to 5 of 2,138 entries), and footer text: 'A Privileged Account Management Solution' and 'Copyright © 2022 ARCON. All Rights Reserved.'


The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Day	Date for which the summary is given
Time	The time range for which the summary of that day is given
Session Count	Number of sessions accessed on that day
User Count	Number of users using PAM on that day

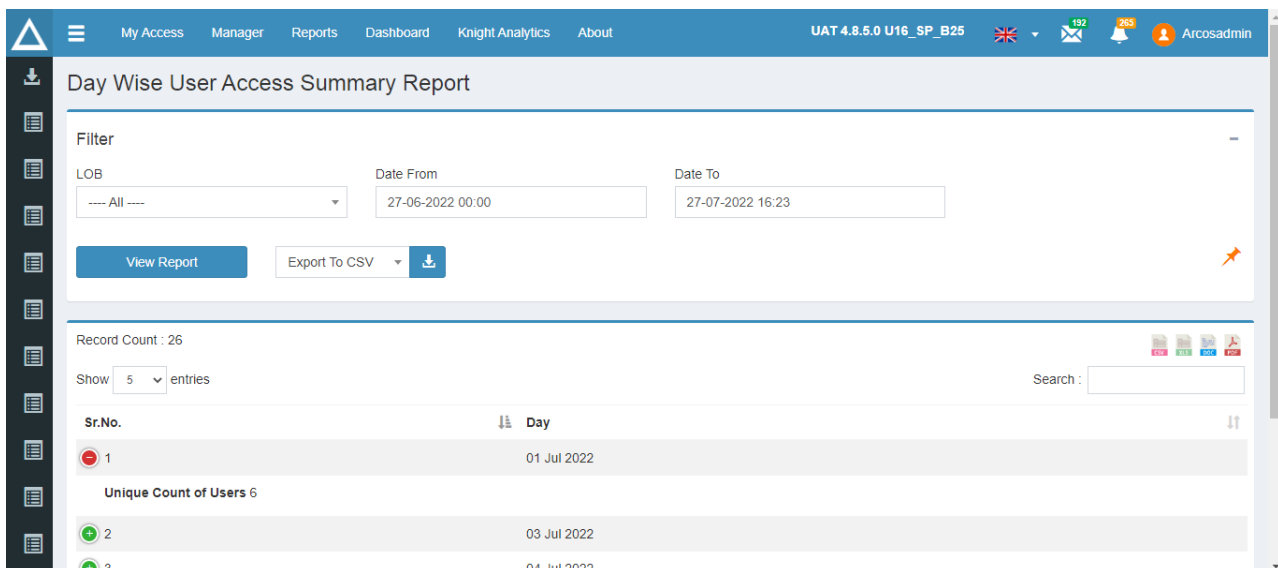
Column Names	Description
Critical Command	The total number of critical commands fired on that day
Restricted Command	The total number of restricted commands fired on that day
Open Password	Number of passwords viewed on that day
Restricted Process	Number of restricted processes

7.4 Day Wise User Access Summary Report

The Day Wise User Access Summary Report displays the information for the day-wise unique count of users.

 In order to view this report, users must have the following permission(s):

- **Day Wise User Access Summary Report**



The following columns can be seen in this report:


Column Names	Description
Sr. No.	To identify and distinguish rows
Day	The date

After clicking on the (+) action, the unique count of users can be displayed.

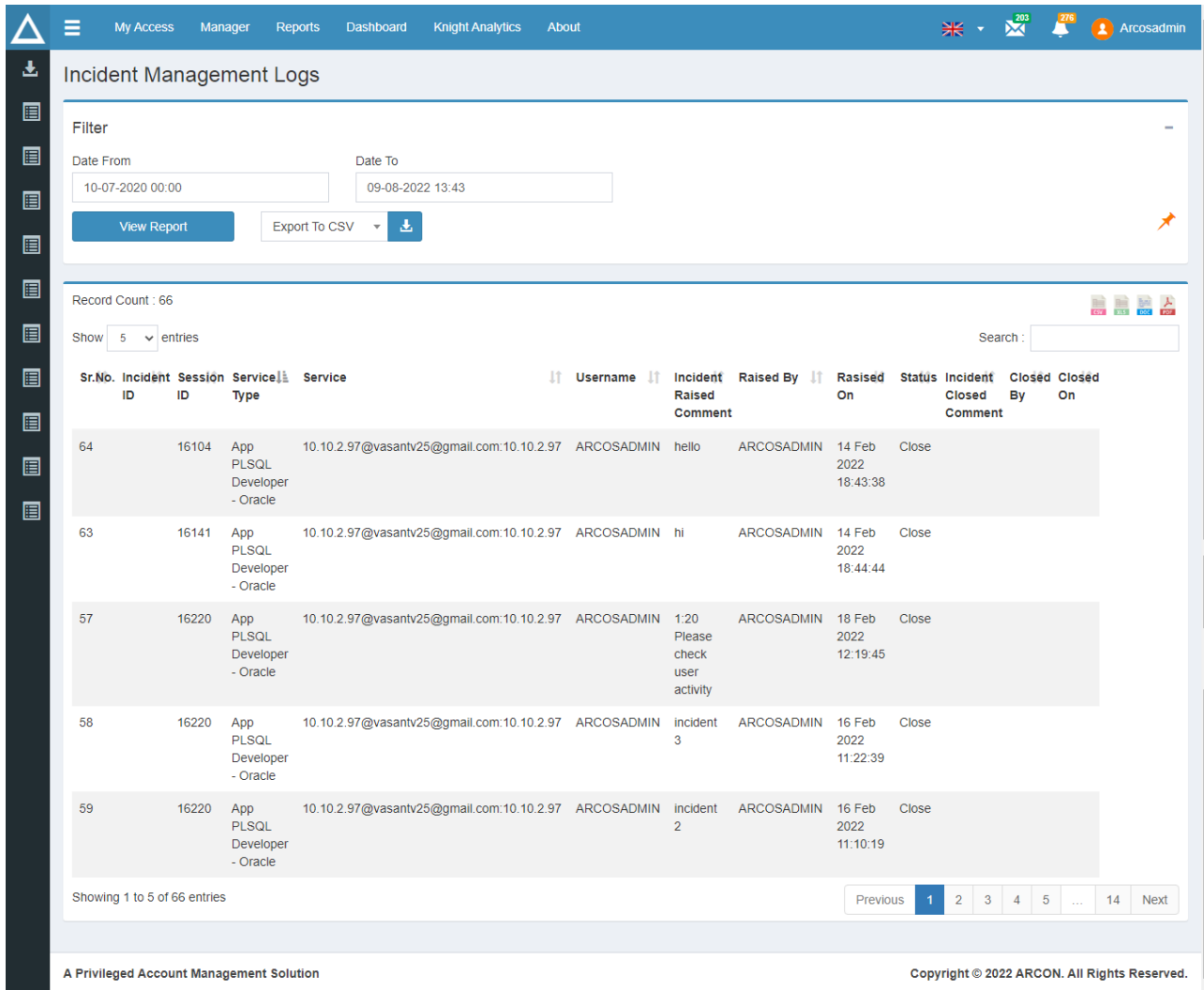
7.5 Incident Management Logs

The Incident Management Logs report captures the logs of the incident which is raised or closed performed by Incident Management.

When the admin user watches video logs and checks the text logs, the user should be able to raise incidents for the session. In case if they find any suspicious activity and notify the group admin of the server group to which the service belongs. The group admin should review that incident to take necessary actions and close the incident.

 In order to view this report, users must have the following permission(s):

- **Incident Management Logs**



Incident Management Logs

Filter

Date From: 10-07-2020 00:00 | Date To: 09-08-2022 13:43

View Report | Export To CSV

Record Count : 66

Show 5 entries | Search :

Sr.No.	Incident ID	Sesión ID	Service Type	Service	Username	Incident Raised Comment	Raised By	Raised On	Status	Incident Closed Comment	Closed By	Closed On
64		16104	App PLSQL Developer - Oracle	10.10.2.97@vasantv25@gmail.com:10.10.2.97	ARCOSADMIN	hello	ARCOSADMIN	14 Feb 2022 18:43:38	Close			
63		16141	App PLSQL Developer - Oracle	10.10.2.97@vasantv25@gmail.com:10.10.2.97	ARCOSADMIN	hi	ARCOSADMIN	14 Feb 2022 18:44:44	Close			
57		16220	App PLSQL Developer - Oracle	10.10.2.97@vasantv25@gmail.com:10.10.2.97	ARCOSADMIN	1:20 Please check user activity	ARCOSADMIN	18 Feb 2022 12:19:45	Close			
58		16220	App PLSQL Developer - Oracle	10.10.2.97@vasantv25@gmail.com:10.10.2.97	ARCOSADMIN	incident 3	ARCOSADMIN	16 Feb 2022 11:22:39	Close			
59		16220	App PLSQL Developer - Oracle	10.10.2.97@vasantv25@gmail.com:10.10.2.97	ARCOSADMIN	incident 2	ARCOSADMIN	16 Feb 2022 11:10:19	Close			

Showing 1 to 5 of 66 entries

Previous 1 2 3 4 5 ... 14 Next

A Privileged Account Management Solution | Copyright © 2022 ARCON. All Rights Reserved.

The following columns can be seen in this report:

Column Name	Description
Sr. No.	To identify and distinguish rows
Incident ID	This is a ID number which is given to identify the incident.

Column Name	Description
Session ID	This is a ID number which is given to identify the session.
Service Type	This column shows the type of service
Service	This column shows the name of the service and it contains the service IP address and server user name of the user etc.
User Name	This column shows the name of the user.
Incident Raised Comment	This column shows the comment putted by used while raising the incident.
Incident Raised By	This column shows the name of the user who raised the incident.
Raised On	This column shows the date and time when the incident was raised.
Status	This column shows the status of this incident as closed or open.
Incident Closed Comment	This column shows the comment putted by used while closing the incident.
Closed By	This column shows the name of the user who closed the incident.
Closed On	This column shows the date and time when the incident was closed.

7.6 Log Review Report

The Log Review Report displays details of all the logs accessed or viewed by Administrators in ARCON | PAM. Additionally, it also records information from real-time session monitoring, such as video viewing, session freeze, unfreeze, and logout activities.



In order to view this report, users must have the following permission(s):

- **Log Review Report**


The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Log Name	Name of logs accessed
Log Type	Action on logs
Log Viewed Downloaded By	The name of the Administrator who downloaded the logs
Log Viewed Downloaded On	Date-time of download by the Administrator
Session Accessed By	The name of the Administrator who was using the session
Session ID	ID associated with that session
Connection	Connection details of the target server
User Machine IP	Machine IP details of the target server
Logged In	Date/time of login

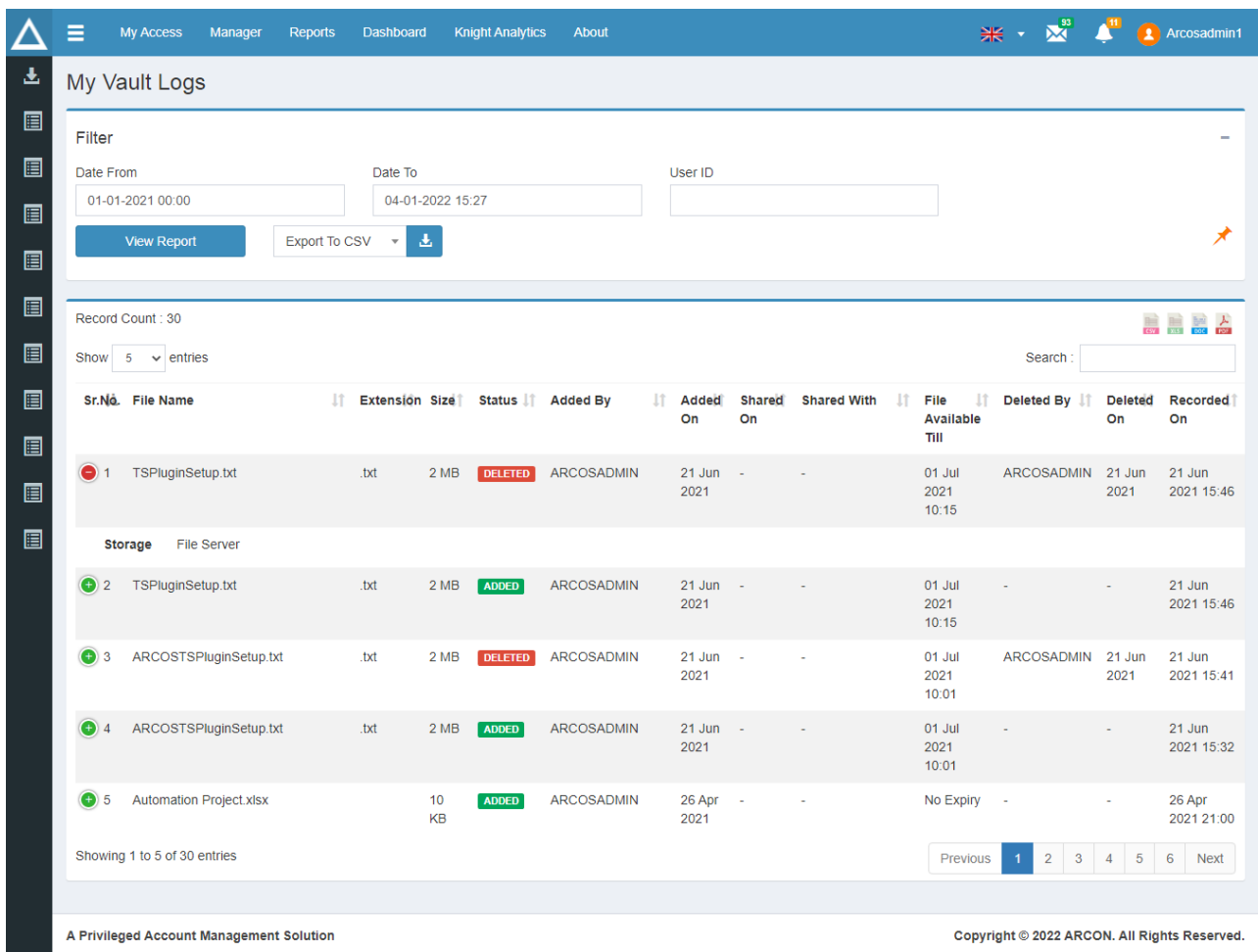
Column Names	Description
Logged Out	Date/time of logout

7.7 My Vault Logs

The My Vault Logs report captures all the activities that are carried out in My Vault of ARCON | PAM.

 In order to view this report, users must have the following permission(s):

- My Vault Logs



My Vault Logs

Filter

Date From: 01-01-2021 00:00 | Date To: 04-01-2022 15:27 | User ID: []

View Report | Export To CSV

Record Count : 30

Show 5 entries | Search: []

Sr.No.	File Name	Extension	Size	Status	Added By	Added On	Shared On	Shared With	File Available Till	Deleted By	Deleted On	Recorded On
1	TSPluginSetup.txt	.txt	2 MB	DELETED	ARCOSADMIN	21 Jun 2021	-	-	01 Jul 2021 10:15	ARCOSADMIN	21 Jun 2021	21 Jun 2021 15:46
Storage File Server												
2	TSPluginSetup.txt	.txt	2 MB	ADDED	ARCOSADMIN	21 Jun 2021	-	-	01 Jul 2021 10:15	-	-	21 Jun 2021 15:46
3	ARCOSTSPluginSetup.txt	.txt	2 MB	DELETED	ARCOSADMIN	21 Jun 2021	-	-	01 Jul 2021 10:01	ARCOSADMIN	21 Jun 2021	21 Jun 2021 15:41
4	ARCOSTSPluginSetup.txt	.txt	2 MB	ADDED	ARCOSADMIN	21 Jun 2021	-	-	01 Jul 2021 10:01	-	-	21 Jun 2021 15:32
5	Automation Project.xlsx		10 KB	ADDED	ARCOSADMIN	26 Apr 2021	-	-	No Expiry	-	-	26 Apr 2021 21:00

Showing 1 to 5 of 30 entries | Previous 1 2 3 4 5 6 Next

A Privileged Account Management Solution | Copyright © 2022 ARCON. All Rights Reserved.


The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
File Name	Name of the file used in My Vault

Column Names	Description
Extension	Type of file <ul style="list-style-type: none"> • Text • PDF • JPG • GIF • PNG
Size	Weight of file
Status	Activity performed on my vault <ul style="list-style-type: none"> • Upload • Download • Shared • Deleted
Added By	The Administrator who added the file
Added On	Date/time at which the file was added in my vault
Shared On	Date/time at which the file was shared (value will come only if it was shared) with some user
Shared With	The Administrator who shared the file
File Available Till	Date/time until which the file will be accessible on my vault
Deleted By	The Administrator who deleted the file
Deleted On	Date/time at which the file was deleted (value will come only if it was deleted)
Recorded On	Date/time at which the file was uploaded
Storage	The repository where the file is stored <ul style="list-style-type: none"> • DataBase • File Server

7.8 Outside ARCON PAM Access Log

The Outside ARCON PAM Access Log report displays information about unauthorized users (outsiders) attempting to access ARCON | PAM services.

 In order to view this report, users must have the following permission(s):

- **Outside ARCON PAM Access Logs**

Sr.No.	Service Type	ServerIPAddress	Domain Name	ClientHostName	ClientIPAdress	ClientUserName	Action Performed
1	WINDOWS RDP	10.10.0.173	ARCON.COM	ARCOSDESVSR4	10.10.0.179	suhas.dingankar	Email Notification
2	WINDOWS RDP	10.10.0.173	ARCON.COM	ARCOSDESVSR4	10.10.0.179	suhas.dingankar	Email Notification
3	WINDOWS RDP	10.10.0.173	ARCON.COM	ARCOSDESVSR4	10.10.0.179	suhas.dingankar	Email Notification
4	SSH LINUX	10.10.0.176	SERVER	EXH8LRUJV1DGLY	10.10.1.175	Lawrence	No Action

The following columns can be seen in this report:

Column Names	Description
Sr.No.	To identify and distinguish rows
Service Type	Name of the service type
ServerIPAddress	The IP address of the target server
Domain Name	The domain name of the target server
ClientHostName	The hostname of the end user’s machine
ClientIPAdress	The IP address of the end user’s machine
ClientUserName	The name of the end user
Action Performed	Activity performed on that service <ul style="list-style-type: none"> Block Email Email-Block
ServerAccessDateTime	Date/time when the server was accessed

7.9 Service Access Log

The Service Access Log report displays information about all of the services that users have accessed based on the filters they have chosen.

In order to view this report, users must have the following permission(s):

• Service Access Log


The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
WorkflowID	Unique ID generated for the workflow request
User ID	Unique ID associated with the user
User Machine IP	Machine IP Details of the target server

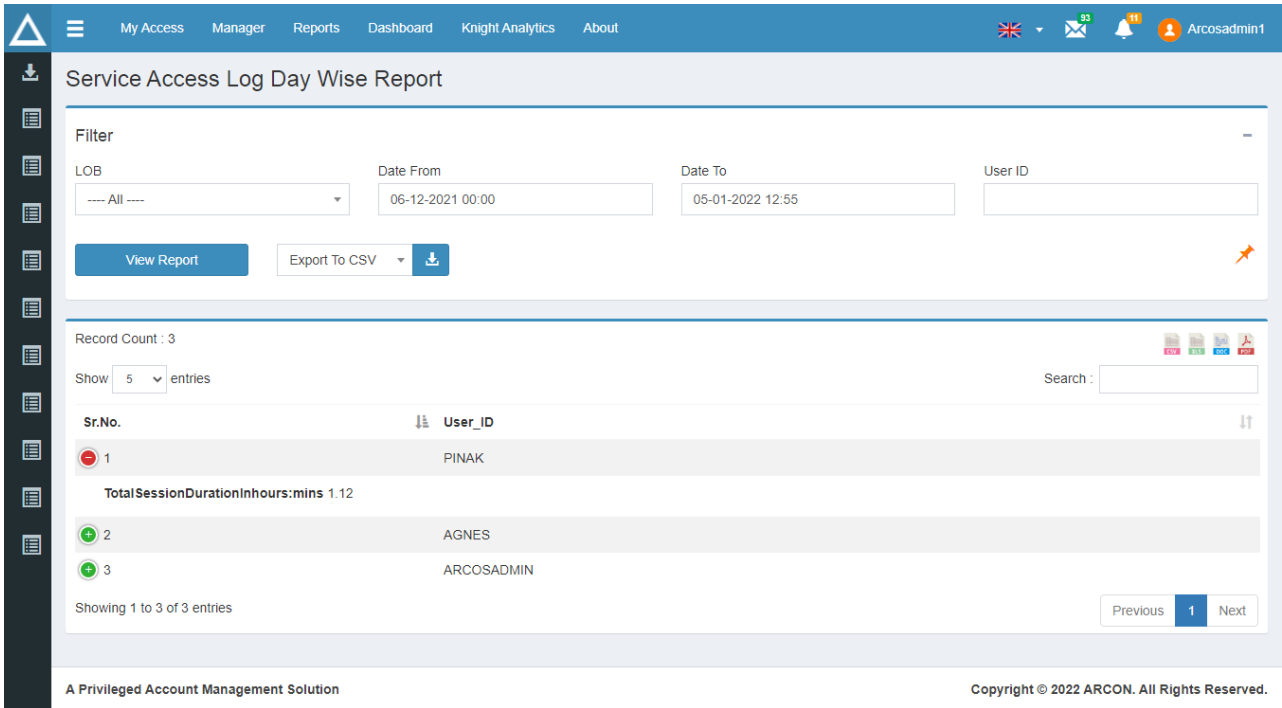
Column Names	Description
Service Type	Name of the service type
Connection	Connection details of the target server
Username	The username associated with the target server
Prompt_UserAccessedUsingUser	Name of the prompt user
ServiceRefNo	Reference Number associated with each SSO while accessing the service
ServiceReferencetype	Reference Type associated with each SSO while accessing the service
ServiceReferenceDetail	Reference Details associated with each SSO while accessing the service
Domain Name	The domain name to which the service belongs
Host Name	The hostname of the service
Description 1	Text entered during the creation of the service by the Administrator
Description 2	Text entered during the creation of the service by the Administrator
Other Details	Text entered during the creation of the service by the Administrator
Service Logged In	Date/time of logging in of that service
Service Logged Out	Date/time of logging out of that service
Total Session Duration Minutes	Timespan while accessing the service
connection_type	Type of connection to that server
Application SessionId	Unique ID associated with all sessions
SessionExtended	Information about whether the session was extended or not
SessionExtendedCount	Number of times the session was extended

7.10 Service Access Log Day Wise Report

Service Access Log Day Wise Report displays information about the user's total session duration in the hour-minute format.

 In order to view this report, users must have the following permission(s):

• Service Access Log Day Wise Report




The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
User_ID	Unique ID associated with the user
TotalSessionDurationInhours:mins	Total time spanned in hours : minutes while accessing the service

7.11 Service Password Request Workflow Logs

The Service Password Request Workflow Logs report displays information about all the service password requests raised by users and actions taken by the approver for that request.

 In order to view this report, users must have the following permission(s):

- Service Password Request Workflow Logs

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Request Number	The unique number associated with every raised request
WorkflowId	Unique ID generated for the workflow request


Column Names	Description
LOB/Profile	The name of the LOB from which the request was raised
Requested By	The username of the user who raised the request
Requested On	Date/time at which the request was raised
Requester EmailId	Email ID associated with the user who raised the request
LOB Workflow	LOB name for which the workflow is working
User Group Workflow	User group for which the workflow is working
Server Group Workflow	Server group for which the workflow is working
Priority	Priority of the workflow as defined by the Administrator at the time of the creation
Description	Text entered during the creation of that workflow by the Administrator
Service type	Name of the service type
Service IP address	IP Address of the target server
Domain Name	The domain name in which the service belongs
Service Username	The username associated with the target server
DB Instance	Displays instance of the target servers
View On date	Date/time on which the request was opened
Open for Hours	Time in hours until which the request will remain valid
Open till Date	Last date till which the request will remain valid
Current Approver Level	The latest level of approval
Approver Levels	Total number of approval levels in the workflow
Approver 1 User Name	Username of the first approver
Approver 1 Status	Status of the request by the first approver <ul style="list-style-type: none"> • Approved • Rejected
Approver 1 Status On	Date/time at which the request was approved/ rejected by the first approver
Approver 1 Comment	Remarks entered by approver 1

Column Names	Description
Approver 1 Email ID	Email ID associated with the approver 1
Approver 2 User Name	Username of the second approver
Approver 2 Status	Status of the request by the second approver <ul style="list-style-type: none"> • Approved • Rejected
Approver 2 Status On	Date/time at which the request was approved/ rejected by the second approver
Approver 2 Comment	Remarks entered by approver 2
Approver 2 Email ID	Email ID associated with the approver 2
Approver 3 User Name	Username of the third approver
Approver 3 Status	Status of the request by the third approver <ul style="list-style-type: none"> • Approved • Rejected
Approver 3 Status On	Date/time at which the request was approved/ rejected by the third approver
Approver 3 Comment	Remarks entered by approver 3
Approver 3 Email ID	Email ID associated with the approver 3
Approver 4 User Name	Username of the fourth approver
Approver 4 Status	Status of the request by the fourth approver <ul style="list-style-type: none"> • Approved • Rejected
Approver 4 Status On	Date/time at which the request was approved/ rejected by the fourth approver
Approver 4 Comment	Remarks entered by approver 4
Approver 4 Email ID	Email ID associated with the approver 4
Approver 5 User Name	Username of the fifth approver
Approver 5 Status	Status of the request by the fifth approver <ul style="list-style-type: none"> • Approved • Rejected

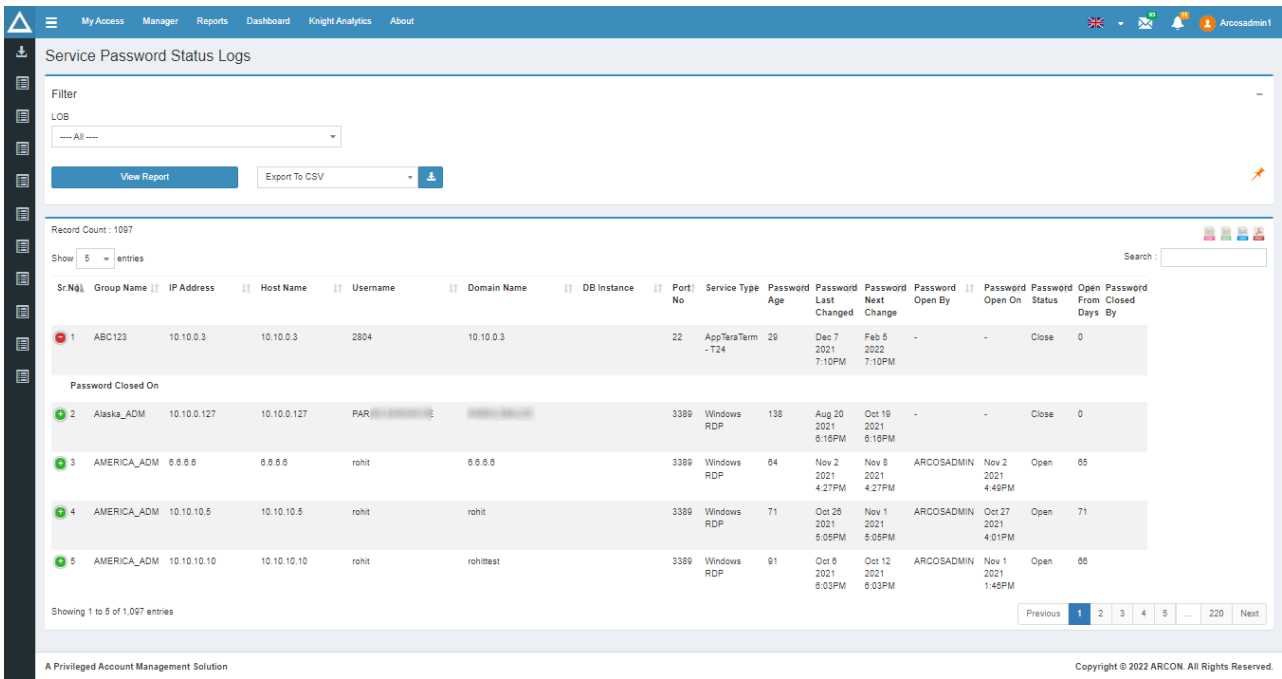
Column Names	Description
Approver 5 Status On	Date/time at which the request was approved/rejected by the fifth approver
Approver 5 Comment	Remarks entered by approver 5
Approver 5 Email ID	Email ID associated with the approver 5
Final status	The final degree of the request <ul style="list-style-type: none"> • Approved • Rejected

7.12 Service Password Status Logs

The Service Password Status Logs report displays information about the password status of all services.

 In order to view this report, users must have the following permission(s):

- **Service Password Status Logs**




The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows

Column Names	Description
Group Name	Name of the Service Group to which the target server belongs
IP Address	The IP address of the target server
Host Name	The hostname of the service
User Name	The username associated with the target server
Domain Name	The domain name in which the service belongs
DB Instance	The instance of that target server
Port No	Port number to connect the target server
Service Type	Name of the service type
Password Age	Number of days passed until which password was the same of the target server
Password Last Changed	Date/time of last password change
Password Next Change	Date/time of next password change
Password Opened By	Name of the user who viewed the password
Password Opened On	Date/time at which the password was viewed
Password Status	Status of the password <ul style="list-style-type: none"> • Open • Close
Opened from Days	Number of days passed after the password was viewed and was open
Password Closed By	Name of the Administrator who changed the password of the target server which was open
Password Closed On	Date/time at which the password was closed

7.13 Service Request Workflow Logs

The Service Request Workflow Logs report displays information about all the service access requests raised by users and actions taken by the approver on that request.

 In order to view this report, users must have the following permission(s):

- **Service Request Workflow Logs**

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows


Column Names	Description
WorkflowID	Unique ID generated for the workflow request
LOB/Profile	The name of the LOB from which the request was raised
Requested By	Username who raised the request
Requester Email Id	Email ID associated with the user who raised the request
LOB Workflow	LOB name for which the workflow is working
UserGroup_Workflow	User group for which the workflow is working
ServerGroup_Workflow	Server group for which the workflow is working
Priority	Priority of the workflow as defined by the Administrator at the time of the creation
Requested On	Date/time at which the request was raised
Requested Description	Text entered at the time of raising the request by the Administrator
Service Access Requested type	Type of service access requested <ul style="list-style-type: none"> • New • Existing
Requested Access Type	Type of request access to that service by the user <ul style="list-style-type: none"> • Permanent • Time-based • One-time
Service Type	Name of the service type
Service IP Address	IP Address of the target server
Domain Name	The domain name to which the service belongs
Service User Name	The user name associated with the target server
DB Instance	Displays instance of the target servers
Access Required From Date	Date/time from which access is required
Access Required To Date	Date/time until which service access is valid
Access Duration Time	The total duration of access
Access Period	Time at which the user accessed the service

Column Names	Description
Current Approver Level	The latest level of approval
Approver Levels	Total number of approval levels in the workflow
Approver 1 User Name	Username of the first approver
Approver 1 Status	Status of the request by the first approver <ul style="list-style-type: none"> • Approved • Rejected
Approver 1 Status On	Date/time at which the request was approved/ rejected by the first approver
Approver 1 Comment	Remarks entered by approver 1
Approver 1 Email ID	Email ID associated with the approver 1
Approver 2 User Name	User name of the second approver
Approver 2 Status	Status of the request by the second approver <ul style="list-style-type: none"> • Approved • Rejected
Approver 2 Status On	Date/time at which the request was approved/ rejected by the second approver
Approver 2 Comment	Remarks entered by approver 2
Approver 2 Email ID	Email ID associated with the approver 2
Approver 3 User Name	Username of the third approver
Approver 3 Status	Status of the request by the third approver <ul style="list-style-type: none"> • Approved • Rejected
Approver 3 Status On	Date/time at which the request was approved/ rejected by the third approver
Approver 3 Comment	Remarks entered by approver 3
Approver 3 Email ID	Email ID associated with the approver 3
Approver 4 User Name	Username of the fourth approver
Approver 4 Status	Status of the request by the fourth approver <ul style="list-style-type: none"> • Approved • Rejected

Column Names	Description
Approver 4 Status On	Date/time at which the request was approved/ rejected by the fourth approver
Approver 4 Comment	Remarks entered by approver 4
Approver 4 Email ID	Email ID associated with the approver 4
Approver 5 User Name	Username of the fifth approver
Approver 5 Status	Status of the request by the fifth approver <ul style="list-style-type: none"> • Approved • Rejected
Approver 5 Status On	Date/time at which the request was approved/ rejected by the fifth approver
Approver 5 Comment	Remarks entered by approver 5
Approver 5 Email ID	Email ID associated with the approver 5
Forwarded to	If the request has been forwarded
AdHoc username	Name of ad hoc users to whom the request has been forwarded
AdHoc status	Status of the request by ad hoc approver <ul style="list-style-type: none"> • Approved • Rejected
AdHoc status on	Date/time at which the request was approved/ rejected by ad hoc approver
AdHoc comment	Remarks entered by ad hoc approver
Final status	The final degree of the request <ul style="list-style-type: none"> • Approved • Rejected

7.14 Session Activity Log

The Session Activity Log report displays the logs containing the reasons for switching users in SSH Linux, Telnet, and SQL Plus.

 In order to view this report, users must have the following permission(s):


- **Session Activity Log**

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Username	The name of the user
Domain Name	The domain name to which the user belongs
Host Name	The hostname of the target server
Port	Displays port of the target servers
User Input	This is the information about switching user
Date	Date and time at which the user started the session activity
Activity Type	Type of activity (For example, Switch User Logs)

7.15 Session Wise Summary Report

Session Wise Summary Report displays a session-by-session count of activities performed on the server and service details.

 In order to view this report, users must have the following permission(s):

• Session-wise Summary Report

Session Wise Summary Report

No Filters Available

View Report Export To CSV

Record Count : 10704

Show 5 entries Search:

Sr.No.	Session ID	Image Log Count	Critical Command	Restricted Command	Restricted Process	Start Time	End Time	User Log Id	User ID
1	816	0	0	0	0	2018-11-15	2018-11-15	1877	ARCOSADMIN
Service User Name sshlinux									
2	817	0	0	0	0	2018-11-15	2018-11-15	1877	ARCOSADMIN
3	818	0	0	0	0	2018-11-15	2018-11-15	1877	ARCOSADMIN
4	819	0	0	0	0	2018-11-15	2018-11-15	1877	ARCOSADMIN
5	821	0	0	0	0	2018-11-15	2018-11-15	1877	ARCOSADMIN

Showing 1 to 5 of 10,704 entries

Previous 1 2 3 4 5 ... 2141 Next

A Privileged Account Management Solution Copyright © 2022 ARCON. All Rights Reserved.


The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Session ID	Unique ID associated with each session
Image Log count	Total number of images captured in the session
Critical Command	The total number of critical commands fired on the day
Restricted command	The total number of restricted commands fired on the day
Restricted Process	Number of restricted processes
Start Time	Time at which the session starts
End Time	Time at which the session ends
User Log Id	Log ID associated with the session
User Id	User ID associated with the user

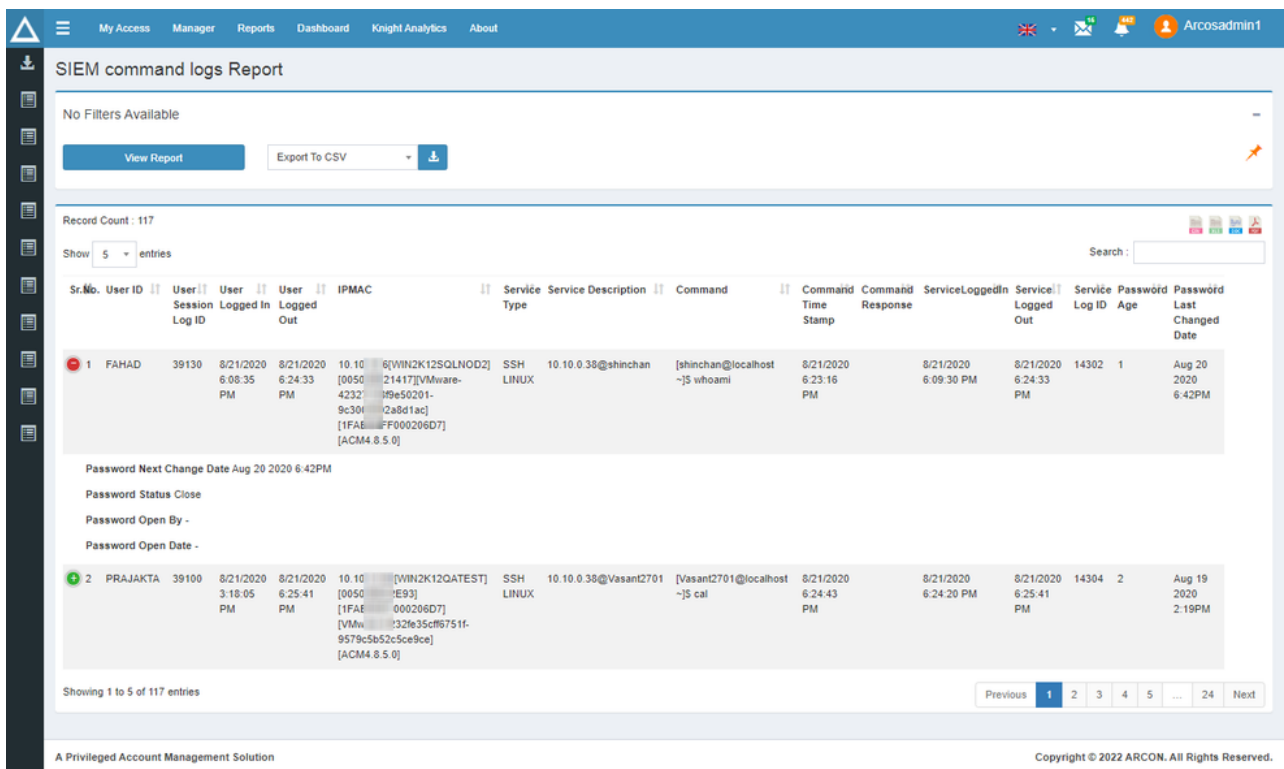
Column Names	Description
Service Username	Username of the service

7.16 SIEM Command Logs Report

The SIEM Command Logs Report displays logs of commands run on Linux services that are obtained from the SIEM service.

 In order to view this report, users must have the following permission(s)

- SIEM Command Logs




The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
User ID	ID associated with the user
User Session LogID	Log ID associated with each session
User Logged In	Date/time of login by user
User Logged Out	Date/time of logout by user

Column Names	Description
IPMAC	IPMAC Address of the target server
Service Type	Name of the service type
Service Description	A combination of IP Address, service username, domain name, hostname and description (For example, 10.10.0.142@administrator:ANBGLOBALDC:10.10.0.142administrator)
Command	Lists the commands fired
Command Time Stamp	Date/time when the command was fired
Command Response	Captures the response after the command was fired
Service Logged In	Date/time of the user when they logged in to the service
Service Logged Out	Date/time of the user when they logged out from the service
Service Log ID	Log ID associated with the service
Password Age	Number of days passed until which the password of the target server was the same
Password Last Changed	Date/time of last password change
Password Next Changed	Date/time of next password change
Password Status	Status of the password <ul style="list-style-type: none"> • Open • Close
Password Opened By	Name of the user who viewed the password
Password Opened Date	Date/time at which the password was viewed

7.17 SMS and Email Logs

The SMS and Email Logs report keeps track of failed login attempts on ACMO and records the reasons for authentication failures where SMS and Mobile are configured as 2FA.

 In order to view this report, users must have the following permission(s):

- **SMS and Email Logs**

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Source	The start point of login failure
Error Type	Type of error
Error Message	The reason why the authentication failed
Timestamp	Date/time at which authentication failed

7.18 Ticket Request Workflow Logs

The Ticket Request Workflow Logs report displays information about all the ticket requests raised by users and actions taken by the approver on that request.

In order to view this report, users must have the following permission(s):

- **Ticket Request Workflow Logs**

The screenshot displays the 'Ticket Request Workflow Logs' report. At the top, there are filter options for LOB (set to 'All'), Date From (05-12-2021 00:00), and Date To (05-01-2022 17:27). Below the filters, there are buttons for 'View Report' and 'Export To CSV'. The main area shows a table with 4 records. The first record (Sr. No. 1) is highlighted in red, indicating it is 'Initiated'. The table columns include Sr. No., Ticket ID, LOB/Profile, Ticket Number, Ticket Status, Ticket Type, Requester Email ID, LOB, User Group, Server Group, Priority, Activity Type, Service Group, Server Domain, Server Instance, Server Port, Server Originator, Executor, Start Time, End Time, and Request Date. Below the table, there are sections for 'Description Xz', 'Impact', 'Requested By User', 'Current Status', 'Approval Levels', and 'Final Approval Status'.

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Ticket ID	The unique number associated with every raised ticket request
LOB/Profile	The name of the LOB from which the request was raised
Ticket Number	The unique number associated with the ticket
Ticket Status	Status of the ticket <ul style="list-style-type: none"> Initiated Approved Rejected


Column Names	Description
Ticket Type	Name of ticket type <ul style="list-style-type: none"> Planned Event (PE) Changed Request (CR)
Requester Email Id	Email ID associated with the user who raised the request
LOB Workflow	Name of the LOB used for creating workflow
User Group Workflow	User group for which the workflow is working
Server Group Workflow	Server group for which the workflow is working
Priority	Priority of the workflow as defined by the Administrator at the time of the creation
Activity Type	Name of Activity type <ul style="list-style-type: none"> Service Affecting (SA) Non Service Affecting (NSA)
Service Group	Server group for which the ticket is raised
Server Domain Name	Domain Name of the target server
Server Instance	Displays Instance of the target servers
Server Port	Displays Port required to connect to the target servers
Originator	Name of the requestor who raised the ticket
Executor	Name of the executor who is accessing the ticket
Start Time	Date/time from which access is given
End time	Date/time until which access is working
Request Date	Date/time at which the request was raised
Description	Text entered during the creation of that workflow by the Administrator
Impact	Impact on ticket
Impact Location	Location of impact
Requested By User	Username who raised the request
Current Status	Status of the current request
Current Approver Level	The latest level of approval

Column Names	Description
Approver Levels	Total number of approval levels in the workflow
Approver 1 Username	Username of the first approver
Approver 1 Status	Status of the request by the first approver <ul style="list-style-type: none"> • Approved • Rejected
Approver 1 Status On	Date/time at which the request was approved/ rejected by the first approver
Approver 1 Comment	Remarks entered by approver 1
Approver 1 Email ID	Email ID associated with approver 1
Approver 2 Username	Username of the second approver
Approver 2 Status	Status of the request by the second approver <ul style="list-style-type: none"> • Approved • Rejected
Approver 2 Status On	Date/time at which the request was approved/ rejected by the second approver
Approver 2 Comment	Remarks entered by approver 2
Approver 2 Email ID	Email ID associated with approver 2
Approver 3 Username	Username of the third approver
Approver 3 Status	Status of the request by the third approver <ul style="list-style-type: none"> • Approved • Rejected
Approver 3 Status On	Date/time at which the request was approved/ rejected by the third approver
Approver 3 Comment	Remarks entered by approver 3
Approver 3 Email ID	Email ID associated with approver 3
Approver 4 Username	Username of the fourth approver
Approver 4 Status	Status of the request by the fourth approver <ul style="list-style-type: none"> • Approved • Rejected

Column Names	Description
Approver 4 Status On	Date/time at which the request was approved/ rejected by the fourth approver
Approver 4 Comment	Remarks entered by approver 4
Approver 4 Email ID	Email ID associated with approver 4
Approver 5 Username	Username of the fifth approver
Approver 5 Status	Status of the request by the fifth approver <ul style="list-style-type: none"> • Approved • Rejected
Approver 5 Status On	Date/time at which the request was approved/ rejected by the fifth approver
Approver 5 Comment	Remarks entered by approver 5
Approver 5 Email ID	Email ID associated with approver 5
Final status	The final degree of the request <ul style="list-style-type: none"> • Approved • Rejected

7.19 User Access Log Report

User Access Log Report displays the users logged into the PAM application in graphical format. The table below displays additional information, such as the user's login and log-out times.

 In order to view this report, users must have the following permission(s):

- **User Access Log Report**

My Access
Manager
Reports
Dashboard
Knight Analytics
About

93

11

Arcosadmin1

User Access Log Report

Filter

LOB

--- All ---

Date From

06-12-2021 00:00

Date To

05-01-2022 17:29

View Report

Export To CSV ▼

Chart

Total User Login Day Wise

Record Count : 7884

Show 5 entries

Search :

Sr.No.	LOB/Profile	Username	Display Name
1	MUMBAI ZONE	ARCOSADMIN	ARCOSADMIN
<p>IP Address 10.10.10.5[WIN2K12STDEV6][000C2939EF3E][1FABFBFF000306F2][VMware-564dc6826f8c9f8f-b5ae02cd4839ef3e] [ACM4.8.5.0]</p> <p>Logged In 2021-12-06 10:40:37.450</p> <p>Logged Out 2021-12-06 10:41:10.320</p> <p>User Type Admin</p> <p>Connection Type ACMO</p>			
2	DEFAULT LOB 2	ARCOSADMIN	ARCOSADMIN
3	DEBOARDING	ARCOSADMIN	ARCOSADMIN
4	DEVEN	ARCOSADMIN	ARCOSADMIN
5	DUBAI REGION	ARCOSADMIN	ARCOSADMIN

Showing 1 to 5 of 7,884 entries

Previous 1 2 3 4 5 ... 1577 Next

A Privileged Account Management Solution
Copyright © 2022 ARCON. All Rights Reserved.

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
LOB/Profile	Name of the LOB

Column Names	Description
User name	Name of the user
Display name	The display name of the user
IP Address	IP Address of the target server
Logged In	Date/time of login into PAM application by the user
Logged Out	Date/time of logout from PAM application by the user
User Type	Type of user <ul style="list-style-type: none">• Client• Admin
Connection Type	Type of connection <ul style="list-style-type: none">• Direct• Gateway• AGW

8 Performance Reports


Performance Reports provide information about the performance of the application.

The following reports are available in Performance Reports:

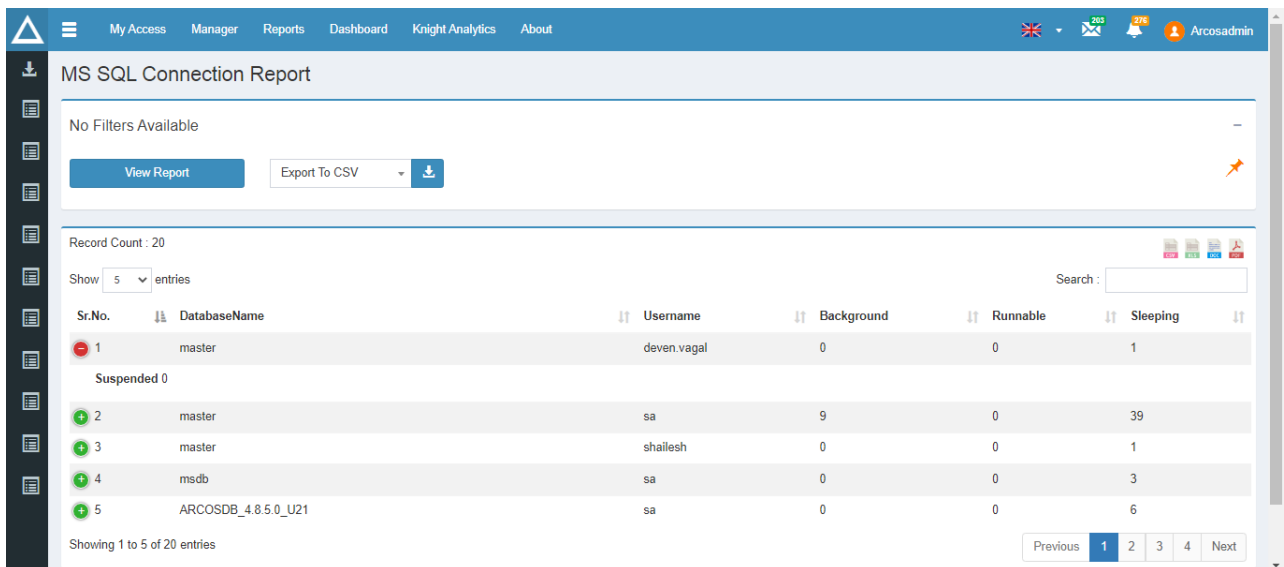
- MS SQL Connection Report
- New ARCON DeskInsight Devices

8.1 MS SQL Connection Report

The MS SQL Connection Report displays information about all users who have access to the MS SQL (Microsoft Sequel) instance on the ARCON | PAM database server.

 In order to view this report, users must have the following permission(s):

- **MS SQL Connection Report**




The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Database Name	Name of the database with which the target server is integrated
User Name	Username of the target server
Background	Count of background instances
Runnable	Count of runnable instances
Sleeping	Count of sleeping instances

Column Names	Description
Suspended	Count of suspended instances

8.2 New Arcon DeskInsight Devices

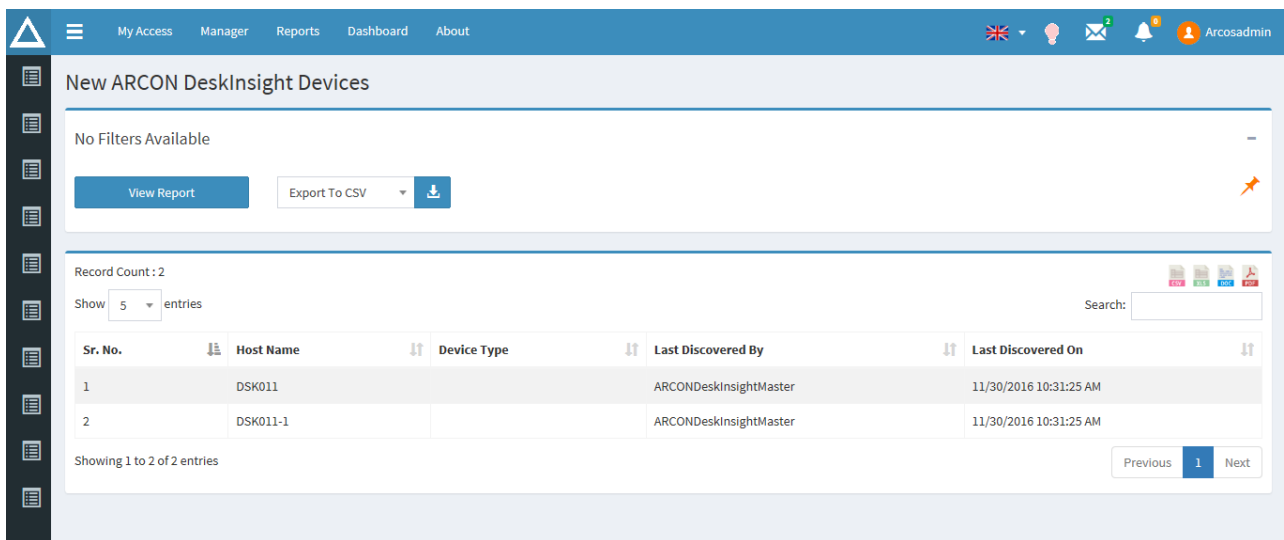
The New Arcon DeskInsight Devices report displays newly added desktops in Windows Active Directory Organizational Units (OUs). It retrieves information about ARCON | PAM-integrated desktops.

 In order to view this report, users must have the following permission(s):

- **New Arcon DeskInsight Devices**

The above-mentioned details can be accessed in one of these two ways:

- Discovered Devices in Server Manager → Manage
- New ARCON DeskInsight Devices report in ACMO



8.2.1 New ARCON PAM DeskInsight Devices report in ACMO

Upon installing the service, update the configurations shown in the screen below in the configuration file. Then, wait for an hour to fetch the report.

```

ARCONDIMasterConfig.ini - Notepad
File Edit Format View Help
60000
true
45046
1
true
true
true
true
true
LDAP://IPADDRESS/DC=DOMAINNAME,DC=com~LDAP://IPADDRESS/CN=Servers,DC=DOMAINNAME,DC=com
computer
true
LDAP://IPADDRESS/DC=DOMAINNAME,DC=com~LDAP://IPADDRESS/CN=Servers,DC=DOMAINNAME,DC=com
computer
-----Till This Line Only-----
Service Interval = 60000 (milliseconds)
Enable Trace Log = true or false
Default ARCON Desk Insight Port = 45046
Run Process Every Hours = 1
Enable IP Range Based Scanning = true or false
Enable Advanced Multithreaded Method = true or false
Enable ARCON DeskInsight Master = true or false
ADM Enable LDAP Based Scanning = true or false
ADM LDAP String = LDAP://IPADDRESS/CN=Computers,DC=DOMAINNAME,DC=com~LDAP://IPADDRESS/CN=Servers,DC=DOMAINNAME,DC=com
ADM LDAP String Filter ObjectClass = computer
WRDP Enable LDAP Based Scanning = true or false
WRDP LDAP String = LDAP://IPADDRESS/CN=Computers,DC=DOMAINNAME,DC=com~LDAP://IPADDRESS/CN=Servers,DC=DOMAINNAME,DC=com
WRDP LDAP String Filter ObjectClass = computer
    
```

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Host Name	Hostname of the target server
Device Type	Type of device
Last Discovered By	Name of last discovery
Last Discovered On	Date/time of last discovery

9 Privilege Reports

Privilege reports provide information about the permissions that give users the ability to conduct activities in ARCON | PAM.

The following reports are available in Privilege Reports:

- Client Manager Privilege Report
- Group Admin Privilege Report
- Server Manager Privilege Report
- User & Service Privileges
- User & Service Privileges – Windows RD

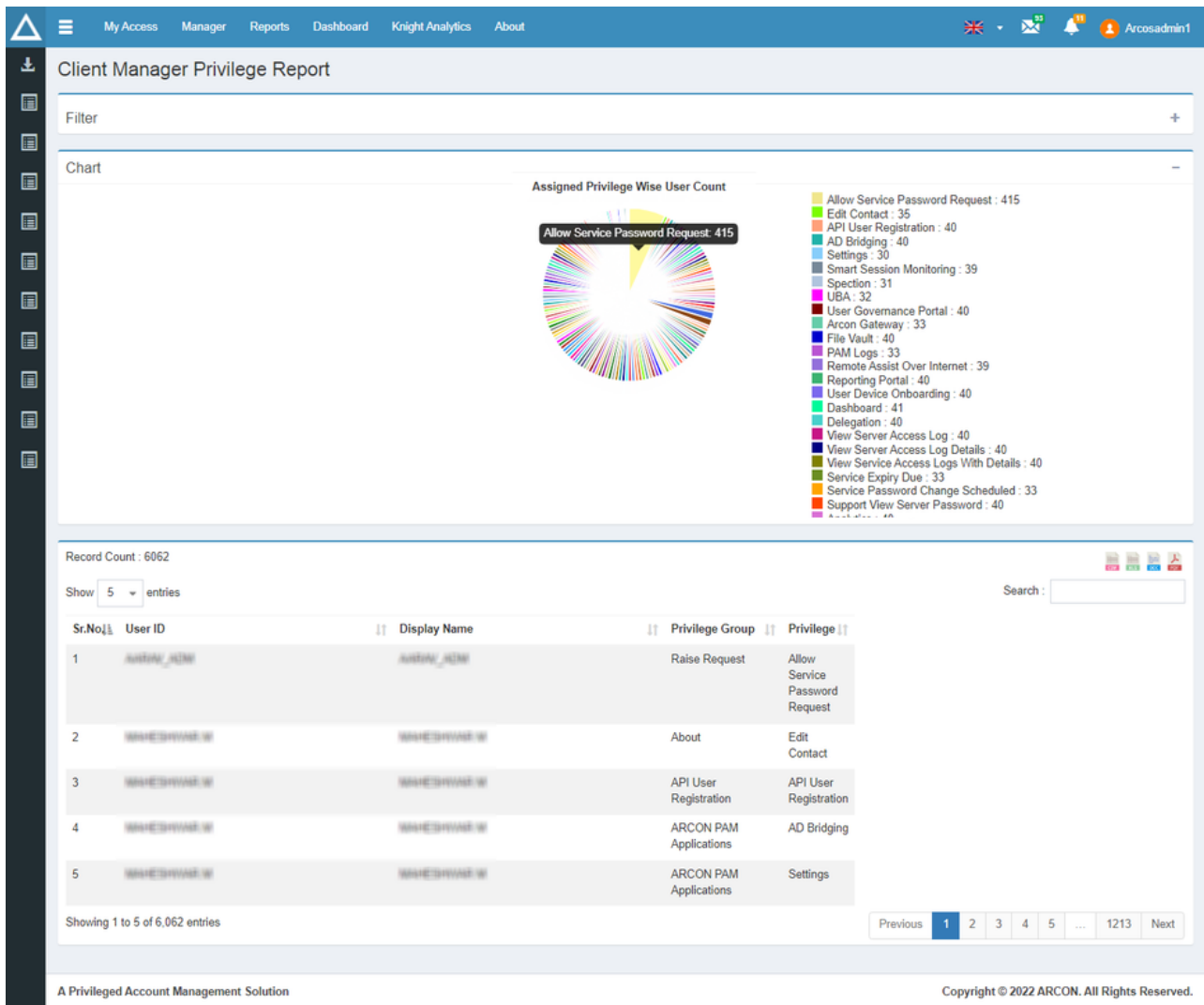
9.1 Client Manager Privilege Report

The Client Manager Privilege Report lists and describes all ACMO privileges that have been assigned to users in graphical and grid view format.



In order to view this report, users must have the following permission(s):

- **Client Manager Privilege Report**



The following columns can be seen in this report:

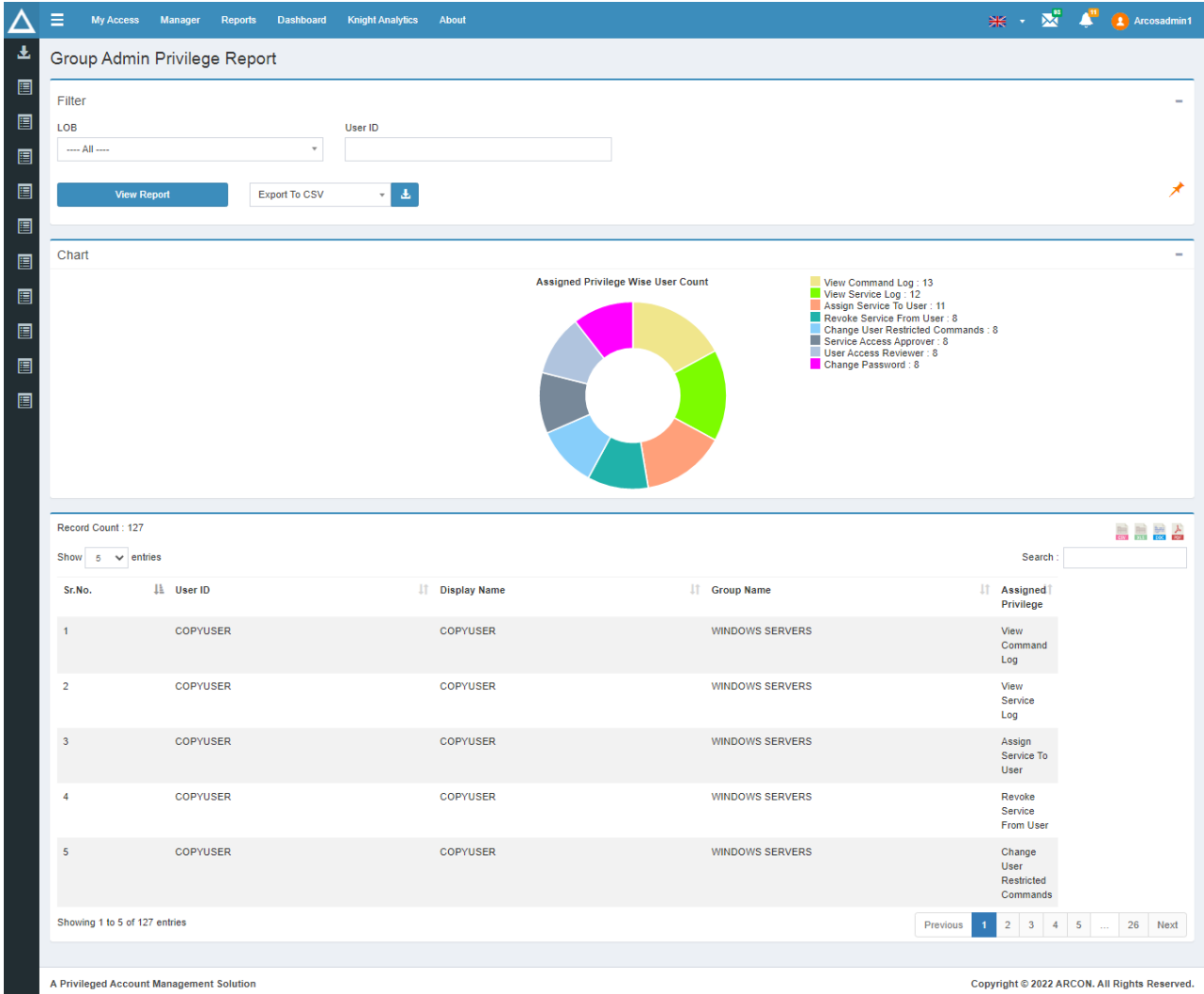
Column Names	Description
Sr. No.	To identify and distinguish rows
User ID	The User ID associated with the user
Display Name	The display name of the user
Privilege Group	The name of the privilege group to which the privilege belongs
Privilege	The name of the assigned privilege

9.2 Group Admin Privilege Report

Group Admin Privilege Report lists and describes all of the ARCON | PAM group admin privileges that have been assigned to Administrators in graphical and grid view format.

! In order to view this report, users must have the following permission(s):

- **Group Admin Privilege Report**



Assigned Privilege Wise User Count

- View Command Log : 13
- View Service Log : 12
- Assign Service To User : 11
- Revoke Service From User : 8
- Change User Restricted Commands : 8
- Service Access Approver : 8
- User Access Reviewer : 8
- Change Password : 8

Sr.No.	User ID	Display Name	Group Name	Assigned Privilege
1	COPYUSER	COPYUSER	WINDOWS SERVERS	View Command Log
2	COPYUSER	COPYUSER	WINDOWS SERVERS	View Service Log
3	COPYUSER	COPYUSER	WINDOWS SERVERS	Assign Service To User
4	COPYUSER	COPYUSER	WINDOWS SERVERS	Revoke Service From User
5	COPYUSER	COPYUSER	WINDOWS SERVERS	Change User Restricted Commands


The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
User ID	The User ID associated with the user
Display Name	The display name of the user
Group Name	The name of the group to which the privilege belongs

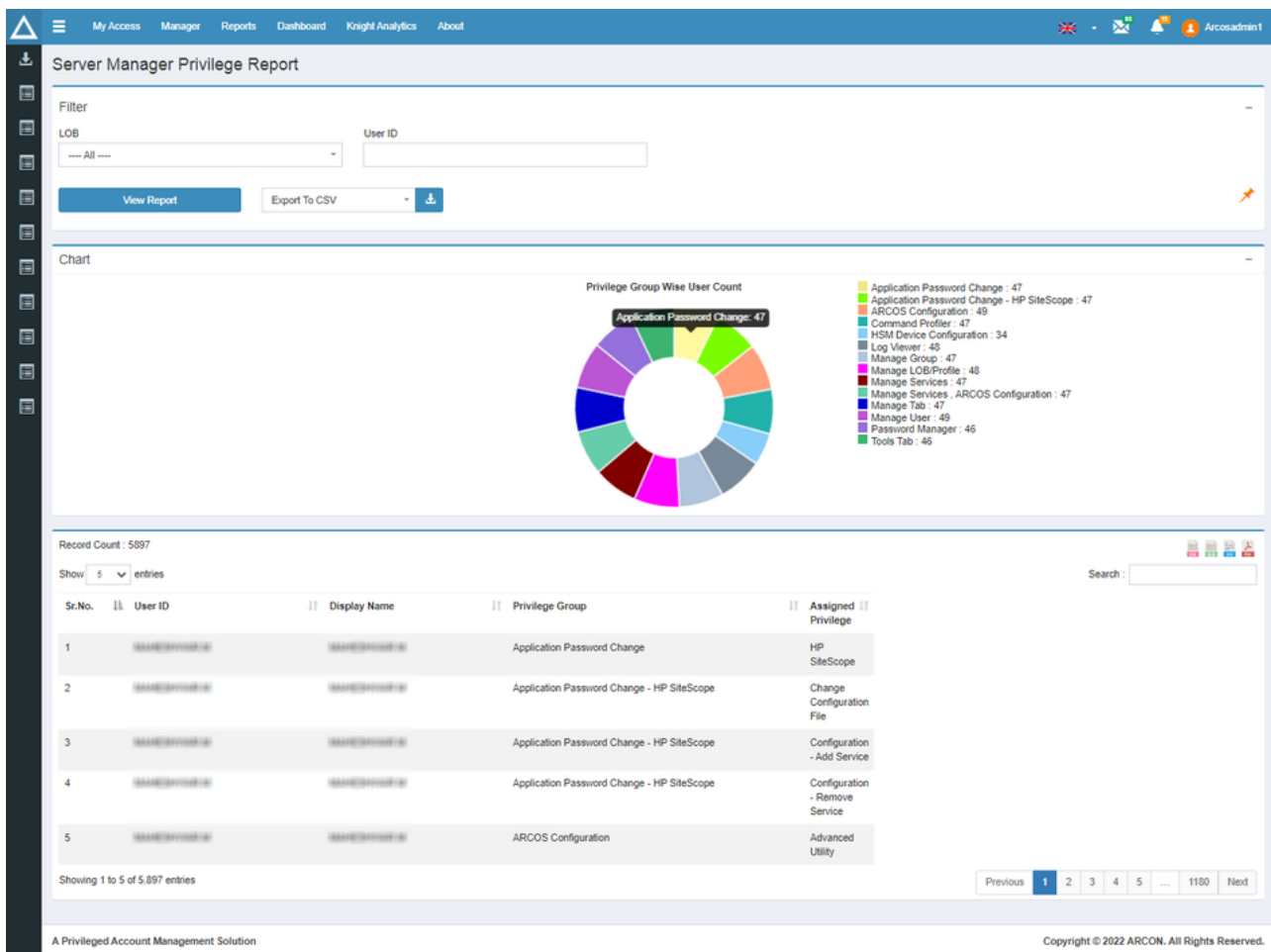
Column Names	Description
Assigned Privilege	The name of the assigned privilege

9.3 Server Manager Privilege Report

Server Manager Privilege Report lists and describes all of the ARCON server manager privileges that have been assigned to Administrators in graphical and grid view format.

 In order to view this report, users must have the following permission(s):

- **Server Manager Privilege Report**




The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
User ID	The User ID associated with the user

Column Names	Description
Display Name	The display name of the user
Privilege Group	The name of the privilege group to which the privilege belongs
Assigned Privilege	The name of the assigned privilege

9.4 User & Services Privileges

The User and Services Privileges report lists and describe all of the configuration command privileges that have been assigned to users and are mapped to the SSH Linux service type in graphical and grid view format.

 In order to view this report, users must have the following permission(s):

- **User and Services Privileges - SSH Linux**

My Access
Manager
Reports
Dashboard
Knight Analytics
About

93
11
Arcosadmin1

User & Service Privileges

Filter

LOB

---- All ----

Service Group

---- All ----

Service / Server IP

Service Type

---- All ----

View Report
Export To CSV
↓

Chart

Command Wise User Count

- RedirectClipboard, : 2078
- EnableRDPConsole, RedirectClipboard, RedirectDrives, : 1
- ARCOS-TS-Monitor, RedirectClipboard, : 2
- ARCOS-TS-Monitor, : 2
- ARCOS-HW-SystemScreen, DisableLog, EnableRDPConsole, : 1
- RedirectClipboard, RedirectSmartCards, : 1
- ARCOS-Command-White-Listing, ARCOS-SFTP-Delete, ARCOS-SFTP-Transfer, ARCOS-SFTP-Upload, : 1

Record Count : 2086

Show 5 entries Search :

Sr.No.	User ID	Display Name	IP Address	Host Name	HostUserName	Domain Name	Port
1	19.162.27.100	19.162.27.100	split7878	domain	3389
Command RedirectClipboard,							
2	19.162.27.100	19.162.27.100	...	19.162.27.100	3389
3	19.162.27.100	TESTDOMAIN	3389
4	19.162.27.100	3389
5	19.162.27.100	3389

Showing 1 to 5 of 2,086 entries

Previous
1
2
3
4
5
...
418
Next

A Privileged Account Management Solution
Copyright © 2022 ARCON. All Rights Reserved.


The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
User ID	The User ID associated with the user
Display Name	The display name of the user
IP Address	The IP address of the target server
Host Name	The Hostname of the target server

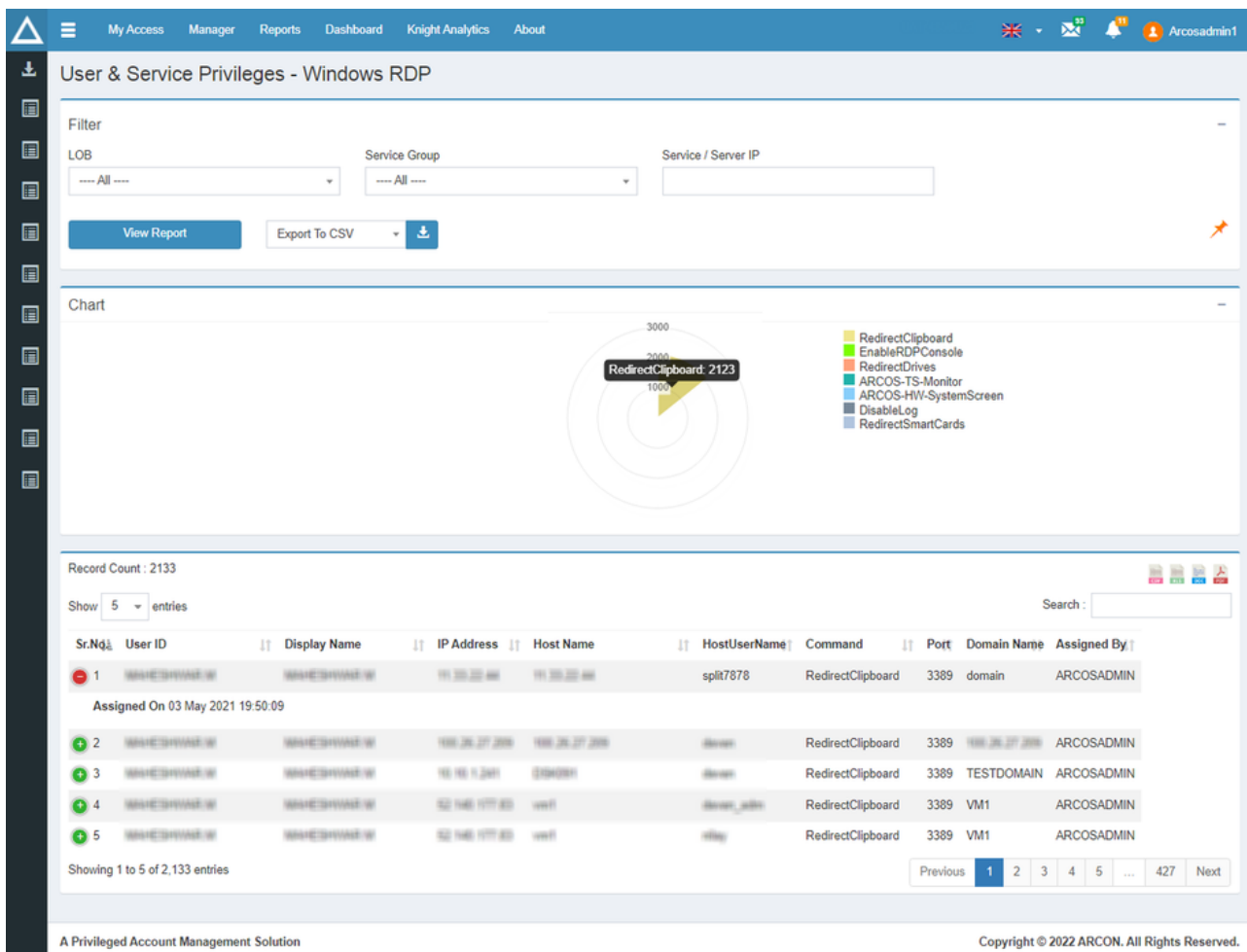
Column Names	Description
Host username	The Host username of the target server
Domain Name	The domain name to which that user belongs
Port	The port number of the target server
Command	List of all the commands mapped to that user

9.5 User & Services Privileges - Windows RDP

The User and Services Privileges - Windows RDP report lists and describes all of the command privileges that have been assigned to users and are mapped to the Windows RDP service type in graphical and grid view format.

 In order to view this report, users must have the following permission(s):

- User and Services Privileges - Windows RDP**



User & Service Privileges - Windows RDP

Filter

LOB: Service Group: Service / Server IP:

Chart

Record Count : 2133

Show entries Search:

Sr.No	User ID	Display Name	IP Address	Host Name	HostUserName	Command	Port	Domain Name	Assigned By
1	WVESHYAR-W	WVESHYAR-W	191.20.22.86	191.20.22.86	split7878	RedirectClipboard	3389	domain	ARCOSADMIN
Assigned On 03 May 2021 19:50:09									
2	WVESHYAR-W	WVESHYAR-W	199.26.27.209	199.26.27.209	devan	RedirectClipboard	3389	199.26.27.209	ARCOSADMIN
3	WVESHYAR-W	WVESHYAR-W	191.16.1.241	191.16.1.241	devan	RedirectClipboard	3389	TESTDOMAIN	ARCOSADMIN
4	WVESHYAR-W	WVESHYAR-W	52.142.177.83	vst1	devan_admin	RedirectClipboard	3389	VM1	ARCOSADMIN
5	WVESHYAR-W	WVESHYAR-W	52.142.177.83	vst1	vllay	RedirectClipboard	3389	VM1	ARCOSADMIN

Showing 1 to 5 of 2,133 entries

Previous ... Next

A Privileged Account Management Solution Copyright © 2022 ARCON. All Rights Reserved.

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
User ID	The User ID associated with the user
Display Name	The display name of the user
IP Address	The IP address of the target server
Host Name	The Hostname of the target server
Host UserName	The Host username of the target server
Command	List of all the commands mapped to that user
Port	The port number of the target server
Domain Name	The domain name to which the user belongs
Assigned By	The Administrator who allocated the commands to the user
Assigned On	Date/time of allocation of command to the user by the Administrator

10 Security Reports

Security Reports give information about the security of ARCON | PAM. They display details of command execution, usage of services, and login attempts made by the user.

The following reports are available in Security Reports:

- Commands executed on service session detail report
- Critical Commands Executed Report
- High Usage (in hrs) Services Report
- Invalid Login Attempts Report
- Low Usage (in days) Services Report
- Multiple Desktop Logon Report
- Multiple User Logon Report
- Network Segment Wise Logon Report
- Restricted Commands Executed Report
- Service Access Off Production Hrs Report
- Service Accessed – Multiple Times Report
- User Service Accessed – Multiple Times Report

10.1 Commands Executed on Service Session Detail Report

Commands Executed on Service Session Detail Report displays commands executed in a session by the user while accessing that service.



In order to view this report, users must have the following permission(s):

- **Commands Executed on Service Session Detail Report**

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
LOB/Profile	The name of the LOB in which there are active services
Service Type	The name of the service type whose session is taken
IP Address	The IP address of the target server
User ID	The User ID associated with the user
User Machine IP	The IP address assigned to the user machine

Column Names	Description
Service User name	The username of the service
Domain	The domain name of the target server
Hostname	The hostname of the target server
Command Details	List of commands executed in that session

10.2 Critical Commands Executed Report

The Critical Commands Executed Report displays all the critical commands executed by users on the servers in grid view format. Critical commands are defined by Administrators in the server manager. In addition the bar graphs displays:

- Top ten users who fired critical commands.
- Top ten IP Addresses from where the critical commands were fired.



In order to view this report, users must have the following permission(s):

- **Critical Commands Executed Report**

My Access Manager Reports Dashboard Knight Analytics About

Arcosadmin1

Critical Commands Executed Report

Filter

LOB: ---- All ---- Date From: 06-12-2021 00:00 Date To: 05-01-2022 13:35 User Group: ---- All ----

Service Type: ---- All ----

View Report
Export To CSV ▼

Chart

Top 10 Users

User ID	Count
ARCOSADMIN	31

Top 10 IP Address

IP Address	Count
54.236.233.214	1
10.10.0.67	5
10.10.0.38	22
10.10.0.175	3

Record Count : 31

Show 5 entries Search:

Sr.No.	User ID	IP Address	Service Type	IP Address	Service User Name	DB Instance	Command	Command Response	Timestamp
1	ARCOSADMIN	10.10.0.175	SSH LINUX	10.10.0.175	manj		# ls	Restricted Command	04 Jan 2022 17:53:17
Group Name SHAIL SERVERS,									
2	ARCOSADMIN	10.10.0.38	SSH LINUX	10.10.0.38	root		root@hello # bc<-->cal<-->ls<-->whoami<-->bc	Restricted Command	20 Dec 2021 18:02:39
3	ARCOSADMIN	10.10.0.38	SSH LINUX	10.10.0.38	root		root@hello # cd /var/log/httpd/		20 Dec 2021 17:38:09
4	ARCOSADMIN	10.10.0.38	SSH LINUX	10.10.0.38	root		root@hello # ls	Critical Command Execution Is Confirmed	20 Dec 2021 11:40:49
5	ARCOSADMIN	10.10.0.38	SSH LINUX	10.10.0.38	root		root@hello # ls	Critical Command Execution Is Confirmed	20 Dec 2021 11:42:14

Showing 1 to 5 of 31 entries Previous 1 2 3 4 5 6 7 Next

A Privileged Account Management Solution
Copyright © 2022 ARCON. All Rights Reserved.

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows

Column Names	Description
User ID	The User ID associated with the user
IP Address Desktop	The IP address of the desktop from where the command was fired
Service Type	The name of the service type where critical commands were executed
IP Address	The IP address of the target server
Service Username	The username of the service
DB Instance	Instance of the target servers
Command	List of commands fired
Command Response	Captures the response after the command was fired
Timestamp	Date/time when the command was fired
Group name	Name of the server group to which the target server belongs

10.3 High Usage (in hrs) Services Report

The High Usage (in hrs) Services Report displays services which are used a maximum number of times depending on the time range:

- Between 30 - 60 mins
- Greater than 1 hour but less than 2 hours
- Greater than 2 hours.



In order to view this report, users must have the following permission(s):


- **High Usage (in hrs) Services Report**

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Service Type	The name of the service type whose usage is displayed in hours
Service IP	The IP address of the target server
Service Username	The username of the service
No of times accessed >30 <60 mins	Number of times the service was used for a duration of greater than 30 mins but less than 1 hour
No of times accessed >=1 <2 hours	Number of times the service was used for a duration of greater than or equal to 1 hour but less than 2 hours
No of times accessed >=2 hours	Number of times the service was used for a duration of greater than or equal to 2 hours

10.4 Invalid Login Attempts Report


The Invalid Login Attempts Report displays the number of invalid login attempts faced while logging into ACMO as well as the reason for the invalid login.

 In order to view this report, users must have the following permission(s):

Column Names	Description
No of times accessed >=1 <2 hours	Number of times the service was used for a duration of duration greater than or equal to 1 hour but less than 2 hours
No of times accessed >=2 hours	Number of times the service was used for a duration of duration greater than or equal to 2 hours

10.5 Low Usage (in days) Services Report

The Low Usage (in days) Services Report displays the services which were used the least, along with the number of days they were not used for, in graphical and grid format.

 In order to view this report, users must have the following permission(s):

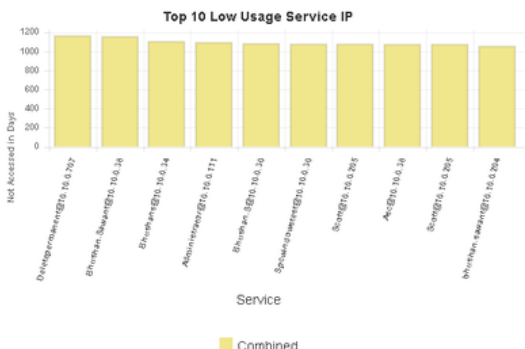
- **Low Usage (in days) Services Report**

My Access Manager Reports Dashboard Knight Analytics About
Lawrence Rodrigues

Low Usage(in days) Services Report

Filter +

Chart -



Record Count : 281

Show 5 entries Search:

Sr.No.	Service Type	Service IP	Service User Name	Last Accessed on
1	SSH LINUX	10.10.0.11	Qa1	30 Dec 2020 16:59:10
No. of Days Not Accessed 341				
2	Oracle QA	10.10.0.156	sys	30 Dec 2020 12:58:41
3	Oracle QA	10.10.0.156	neel9	29 Dec 2020 15:32:50
4	Oracle QA	10.10.0.156	NEEL	29 Dec 2020 15:31:23
5	App WinSCP	10.10.0.200	Shuchan Stewart	28 Sep 2018 15:32:30

Showing 1 to 5 of 281 entries

Previous 1 2 3 4 5 ... 57 Next

A Privileged Account Management Solution
Copyright © 2022 ARCON. All Rights Reserved.

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Service Type	The name of the service type not used for many days
Service IP	The IP address of the target server
Service User Name	The username of the service
Last Accessed On	Date/time on which the service was last used
No. of Days Not Accessed	Number of days passed since service was not used

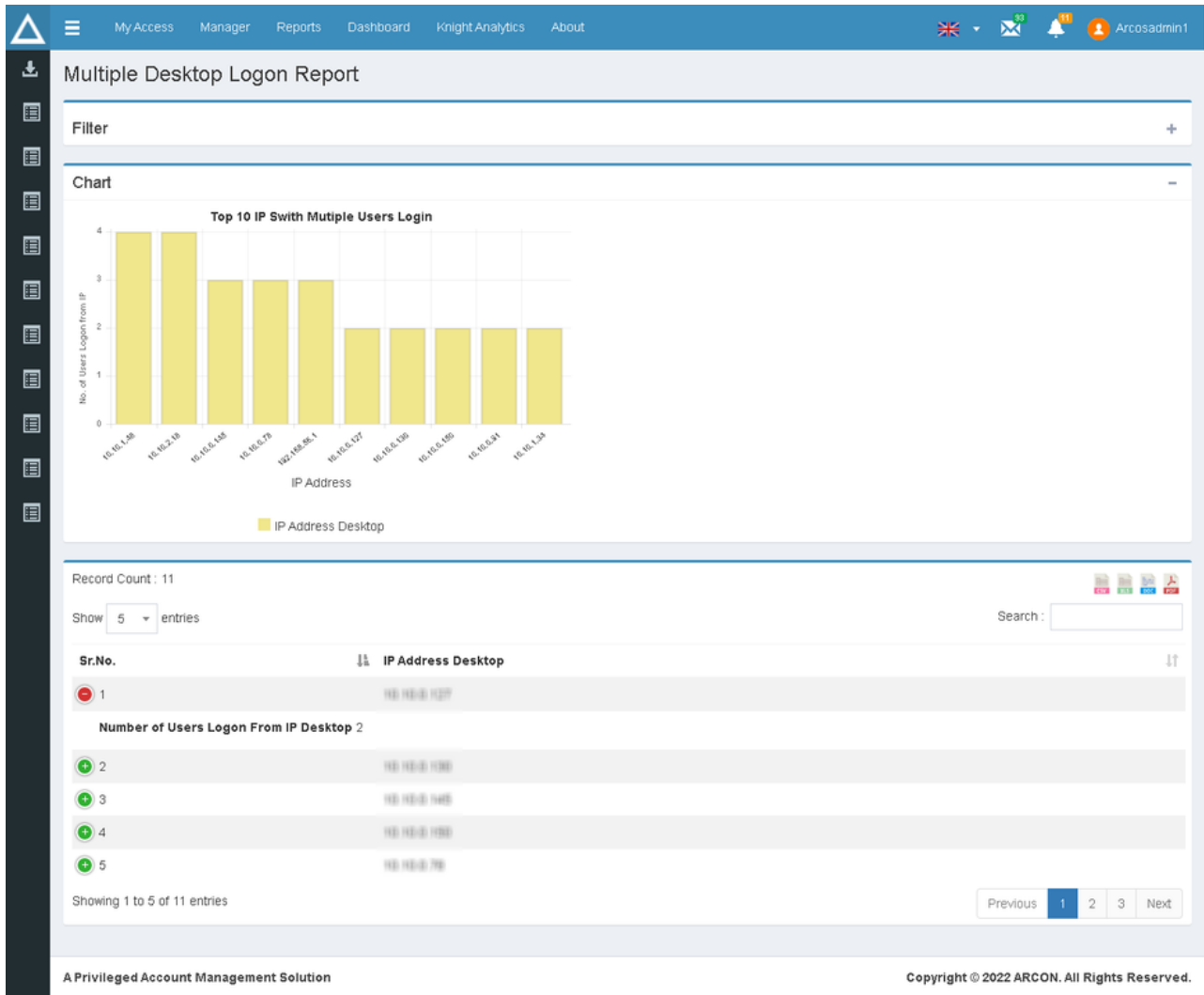
10.6 Multiple Desktop Logon Report

Multiple Desktop Logon Report displays information about the desktop IP address used by multiple users to log in to ARCON | PAM in grid view format. Additionally, a bar graph displays the top ten IP user logins.



In order to view this report, users must have the following permission(s):

- **Multiple Desktop Logon Report**




The following columns can be seen in this report:

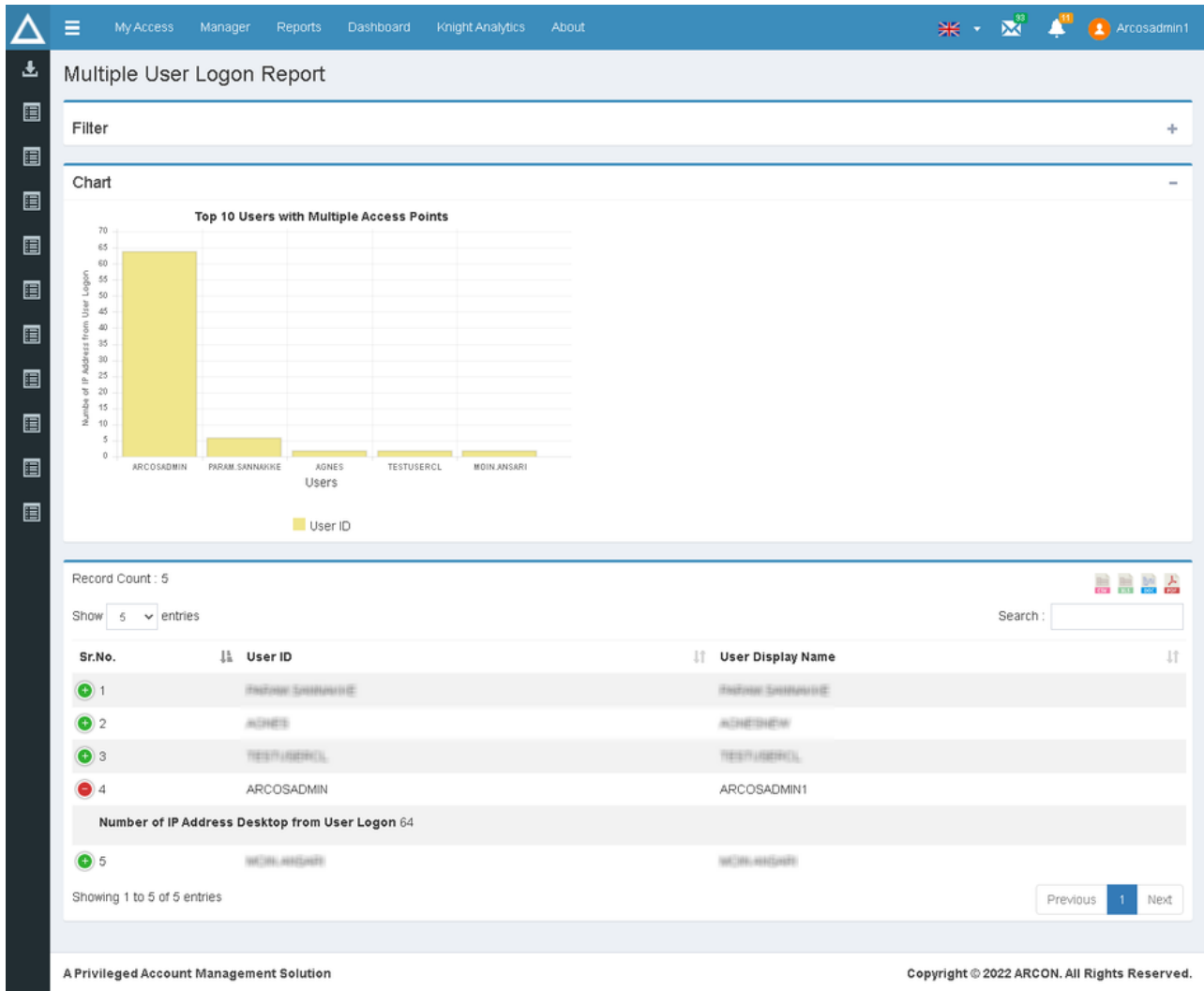
Column Names	Description
Sr. No.	To identify and distinguish rows
IP Address (Desktop)	The IP address of the target server
No. of Users Logon from IP (Desktop)	Number of users logged on from that IP

10.7 Multiple User Logon Report

Multiple User Logon Report displays information about users who logged into ARCON | PAM from various IP addresses/desktops. Additionally, a bar graph displays the top ten IP user logins.

 In order to view this report, users must have the following permission(s):

- **Multiple User Logon Report**



The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
User ID	The User ID associated with the user
Display Name	The display name of the user
No of IP Address (Desktop) from User Logon	Number of desktops used by users to log in

10.8 Network Segment Wise Logon Report

The Network Segment Wise Logon Report displays information about all users who have logged into ARCON | PAM via any network device configured in the Network Segments module of Settings.

In order to view this report, users must have the following permission(s):

• Network Segment-wise Logon Report

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
User ID	The User ID associated with the user
User Display Name	The display name of the user
Desktop Finger Print	Captures the fingerprint
User IP Address	The IP Address of the user logged in
Network Segment	Name of the network segment

10.9 Restricted Commands Executed Report

Restricted Commands Executed Report displays all the restricted commands entered by users on the servers in grid view format. Restricted commands are defined by Administrators in the server manager. In addition the bar graphs displays:

- Top ten users who entered restricted commands.
- Top ten IP Addresses from where the restricted commands were entered.

! In order to view this report, users must have the following permission(s):

- **Restricted Commands Executed Report**

My Access Manager Reports Dashboard Knight Analytics About

 Arcosadmin1

Restricted Commands Executed Report

Filter +

Top 10 Users

User ID	Count
ARCOSADMIN	54

Top 10 IP Address

IP Address	Count
10.10.0.38	40
10.10.0.175	14

Record Count : 54

Show 5 entries Search :

Sr.No.	User ID	IP Address	Desktop	Service Type	IP Address	Service User Name	DB Instance	Command	Command Response
1	ARCOSADMIN	10.10.0.38	10.10.0.38	SSH LINUX	10.10.0.38	root		root@hello # cal	Restricted Command
2	ARCOSADMIN	10.10.0.38	10.10.0.38	SSH LINUX	10.10.0.38	root		root@hello # cal	Restricted Command
3	ARCOSADMIN	10.10.0.38	10.10.0.38	SSH LINUX	10.10.0.38	root		root@hello # cal	Restricted Command
4	ARCOSADMIN	10.10.0.38	10.10.0.38	SSH LINUX	10.10.0.38	root		root@hello # cal	Restricted Command
5	ARCOSADMIN	10.10.0.38	10.10.0.38	SSH LINUX	10.10.0.38	root		root@hello # cal	Restricted Command

Showing 1 to 5 of 54 entries
 Previous 1 2 3 4 5 ... 11 Next

A Privileged Account Management Solution
Copyright © 2022 ARCON. All Rights Reserved.

The following columns are available in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
User ID	The User ID associated with the user

Column Names	Description
IP Address (Desktop)	The IP Address of the User logged in
Service Type	Name of the service type
IP Address	IP Address of the target server
Service Username	The username associated with the target server
DB Instance	Instance of the target servers
Command	Lists the commands fired
Command Response	Captures the response after the command was fired
Timestamp	Date/time when the command was fired

10.10 Service Access Off Production Hrs Report

The Service Access Off Production Hrs Report displays records of users accessing the services during non-working hours. Working hours are set in **start shift time** and **end shift time** by Administrators in Settings.

In order to view this report, users must have the following permission(s):

- Service Access Off Production Hrs Report**

Service Access Off Production Hrs Report

Filter

LOB: All | Date From: 11-12-2021 00:00 | Date To: 10-01-2022 11:23

Service Type: All

View Report | Export To CSV

Record Count : 8

Show 5 entries

Sr.No.	User ID	Username	Service Type	Service IP Address	Service User Name	Domain	DB Instance	Host Name	Logged In Time
1	SSH LINUX	...	root	2022-01-06 12:41:16
2	SSH LINUX	...	root	2022-01-05 11:14:25
3	SSH LINUX	...	rhel	2021-12-16 15:39:29
4	SSH LINUX	...	rhel	2021-12-16 13:18:33
5	LAWRENCE REEDHOLMES	LAWRENCE REEDHOLMES	SSH LINUX	...	rhel	2021-12-13 19:19:20

Showing 1 to 5 of 8 entries

Previous 1 2 Next

A Privileged Account Management Solution | Copyright © 2022 ARCON. All Rights Reserved.

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
User ID	The User ID associated with the user
Username	Name of the user accessing the service
Service Type	Name of the service type
Service IP Address	IP Address of the target server
Service Username	The username associated with the target server
Domain	The domain name to which the server belongs
DB Instance	Instance of the target servers
Host Name	The hostname of the target server
Logged In Time	Date/time when the service access started

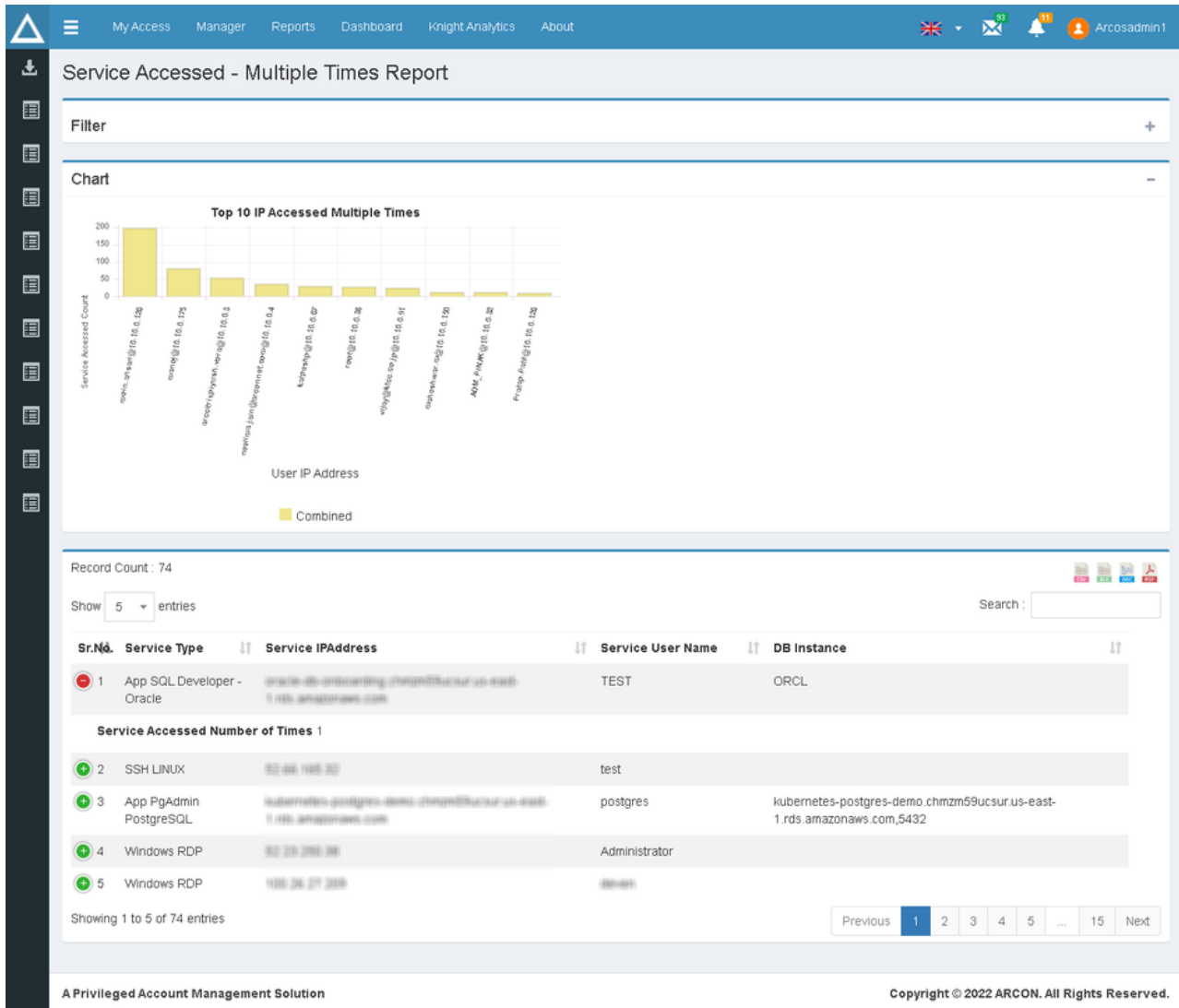
10.11 Service Accessed – Multiple Times Report

The Service Accessed – Multiple Times Report displays details of all the services accessed multiple times by users in grid view format. Additionally, a bar graph displays the top ten IP users who accessed the service numerous times.



In order to view this report, users must have the following permission(s):

- **Service Accessed - Multiple Times Report**




The following columns can be seen in this report:

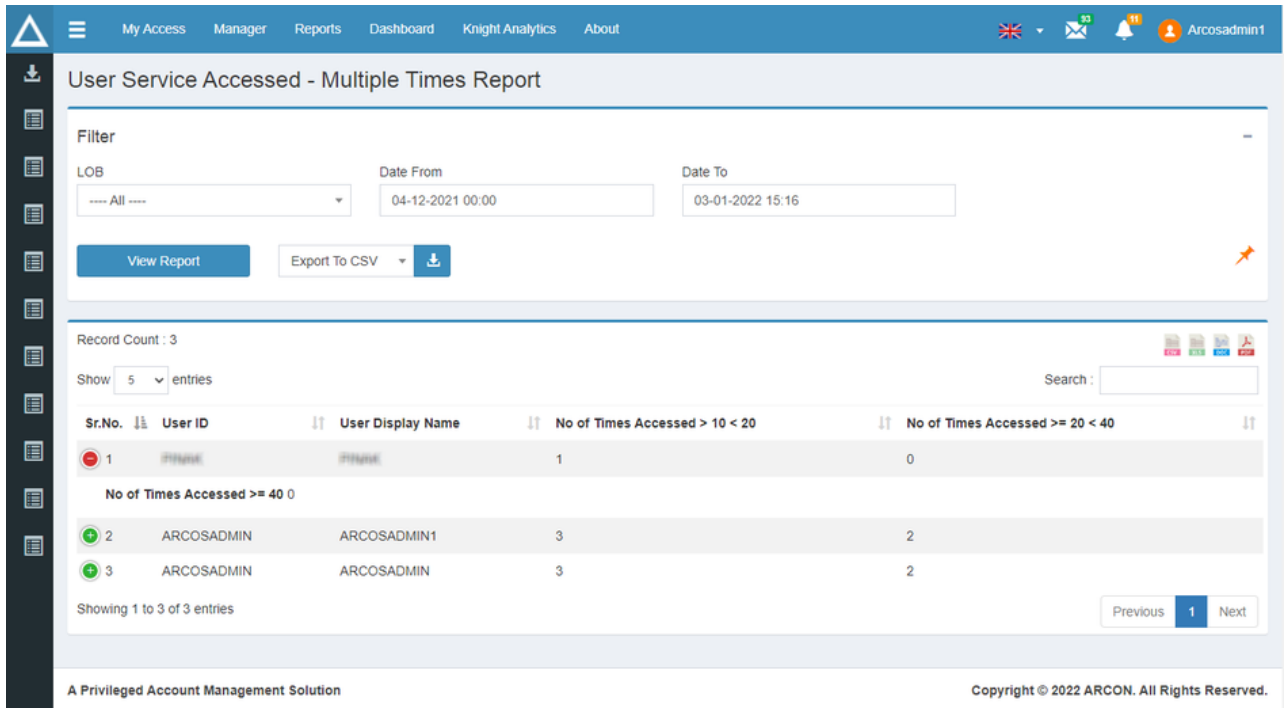
Column Names	Description
Sr. No.	To identify and distinguish rows
Service Type	Name of the service type
Service IP Address	IP Address of the target server
Service Username	The username associated with the target server
DB Instance	Displays Instance of the target servers
Service Accessed Number of Times	Number of times the service was accessed

10.12 User Service Accessed - Multiple Times Report

The User Service Accessed - Multiple Times Report displays the number of times the user has accessed services between the defined range.

 In order to view this report, users must have the following permission(s):

- **User Service Accessed - Multiple Times Report**



The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
User ID	The User ID associated with the user
User Display Name	The display name of the user
No of Times Accessed > 10 < 20	Number of services accessed by the user - greater than 10 and less than 20 times
No of Times Accessed >= 20 < 40	Number of services accessed by the user - greater than or equal to 20 and less than 40 times
No of Times Accessed >= 40	Number of services accessed by the user - greater than or equal to 40 times

11 Service Reports

A Service Report is used to generate details of the services that are active in ARCON | PAM. In addition, it generates details of the reference number provided by the user before accessing any service and unique IP addresses of services.

The following reports are available in Service Reports:

- Active Services Report
- Active Sessions Report
- AGW Service Access report
- Device Detailed Report
- Multiple Service Reference No. Report
- Password Envelope never generated
- Password Envelope Print Report
- Scheduled Password Change Services
- Server last accessed on
- Servers in Domain
- Service Accessed Summary Days Wise Report
- Service Accessed Summary Report
- Service Application Report
- Service Creation Deletion Details Report
- Service Creation Deletion Summary Report
- Service Dependency Report
- Service Group wise Service Type Report
- Service Timeline Report
- Services in Domain
- Unique Services IP Address Report

11.1 Active Services Report.

Active Services Report displays information about all ARCON | PAM active services. Active service is one that has not expired or has a valid till date that is greater than today's date.



In order to view this report, users must have the following permission(s):

- **Active Services Report**

My Access
Manager
Reports
Dashboard
Knight Analytics
About

53

7

Arcosadmin

Active Services Report

Filter +

Chart

Total Number of Connections Imported for Each Service Type

Record Count : 1190

Show 5 entries Search :

Sr.No.	LOB/Profile	Service Type	Service Group	IP Address	Host Name	User ID	Domain Name
1	ABC	AIX		10.10.0.200	TEST	test37	ARCOSADMIN
<p>DB Instance</p> <p>Port 22</p> <p>Description 1 test1</p> <p>Description 2 test2</p> <p>Description 3 test3</p> <p>Vault Status Not Vaulted</p> <p>Last Accessed Time</p> <p>Active Till 01 Jan 2058 00:00:00</p> <p>LOB Status ACTIVE</p> <p>Created By ARCOSADMIN</p> <p>Created On 17 Jul 2020 15:09:21</p>							
2	ABC	AIX		10.10.0.200	TEST	test15	ARCOSADMIN
3	MUMBAI ZONE	AIX		10.10.0.142	10.10.0.142	satyatest	10.10.0.142
4	DEFAULT LOB 2	AIX	CONNECTORS	10.10.0.699	10.10.0.127	testserv1h	10.10.0.128
5	DEFAULT LOB 2	AIX	DATABASE SERVERS	10.10.0.699	10.10.0.127	testserv1h	10.10.0.128

Showing 1 to 5 of 1,190 entries
Previous
1
2
3
4
5
...
238
Next

A Privileged Account Management Solution

Copyright © 2022 ARCON. All Rights Reserved.

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows

Column Names	Description
Username	The name of the user
Server IP	The IP address of the target server
Service Type	The name of the service type whose session is taken
Service Group	The name of the service group to which the service belongs
Description 1	Text entered during the creation of that service by the Administrator
Service Valid Till	Date/time till which the service remains active
Assign By	The name of the Administrator who assigned the service
Assign On	Date/time of the assignment of service to that user by the Administrator
Vault status	Status of the vault <ul style="list-style-type: none"> Manually Vaulted
Last Accessed On	Date/time the service was last used

11.2 Active Session Report

Active Session Report displays a list of ongoing sessions in ARCON | PAM.



In order to view this report, users must have the following permission(s):

- Active Session Report

Active Sessions Report

No Filters Available

View Report | Export To CSV

Record Count : 4

Show 5 entries

Sr.No.	Server IP	User ID	Display Name	Service Type	Service User Name
1	10.10.0.150	ARCOSADMIN	ARCOSADMIN	Windows RDP	maheshwar.m
Session Source 10.10.0.195[WIN2K12R2-ORA6][005056B25B12][1FABFBFF000206C2][VMware-4232c72ce00e5632-369541cf5890144a][ACM4.8.5.0]					
2	10.10.0.150	ARCOSADMIN	ARCOSADMIN1	Windows RDP	maheshwar.m
3	10.10.0.150	ARCOSADMIN	ARCOSADMIN1	Windows RDP	maheshwar.m
4	10.10.0.150	ARCOSADMIN	ARCOSADMIN1	Windows RDP	maheshwar.m

Showing 1 to 4 of 4 entries

A Privileged Account Management Solution | Copyright © 2022 ARCON. All Rights Reserved.

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Server IP	The IP address of the target server
User ID	The User ID associated with the user
Display Name	The display name of the user
Service Type	The name of the service type whose session is taken
Service Username	The username assigned to the service
Session Source	Source of session

11.3 AGW Service Access Report

The AGW (Arcon Gateway) Service Access Report lists all of the users who have connected to the services using ARCON AGW.

In order to view this report, users must have the following permission(s):


- AGW Service Access Report

The following columns can be seen in this report:

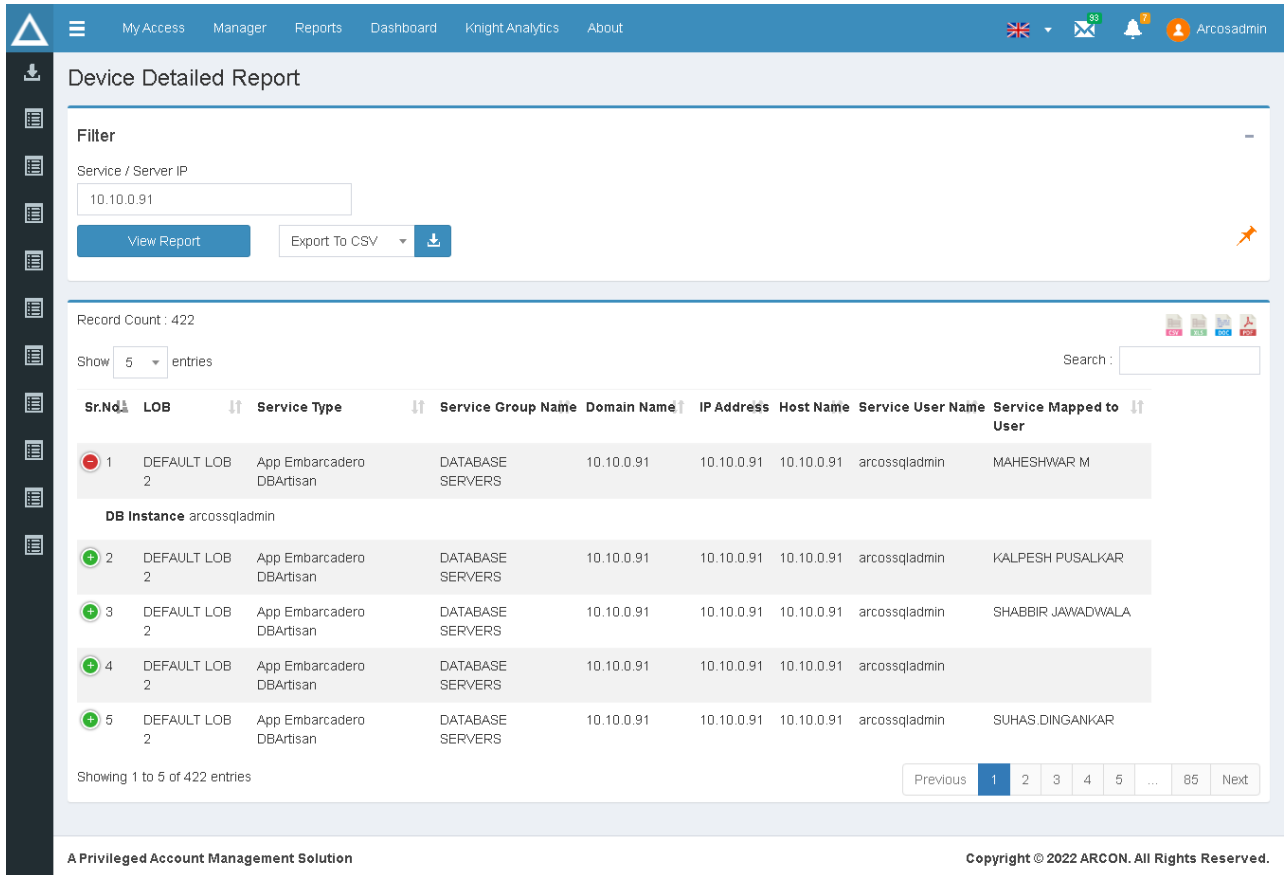
Column Names	Description
Sr. No.	To identify and distinguish rows
AGW Name	Name of the AGW (Arcon Gateway) server
AGW Description	Text entered during the creation of that AGW server
Username	The name of the user
IP Address	The IP address of the target server
Service User Name	The username of the service
Host Name	The hostname of the target server
Domain Name	The domain name of the target server
Logged In Time	Date/time of login
Logout Time	Date/time of logout

11.4 Device Detailed Report

The Device Detailed Report assists in locating and viewing a specific service across all LOBs. The user can search details for multiple IP addresses in the service/server IP filter with comma-separated search queries.

 In order to view this report, users must have the following permission(s):

- **Device Detailed Report**



Device Detailed Report

Filter

Service / Server IP
10.10.0.91

View Report Export To CSV

Record Count : 422

Show 5 entries Search :

Sr.No.	LOB	Service Type	Service Group Name	Domain Name	IP Address	Host Name	Service User Name	Service Mapped to User
1	DEFAULT LOB 2	App Embarcadero DBArtisan	DATABASE SERVERS	10.10.0.91	10.10.0.91	10.10.0.91	arcossqladmin	MAHESHWAR M
DB Instance arcossqladmin								
2	DEFAULT LOB 2	App Embarcadero DBArtisan	DATABASE SERVERS	10.10.0.91	10.10.0.91	10.10.0.91	arcossqladmin	KALPESH PUSALKAR
3	DEFAULT LOB 2	App Embarcadero DBArtisan	DATABASE SERVERS	10.10.0.91	10.10.0.91	10.10.0.91	arcossqladmin	SHABBIR JAWADWALA
4	DEFAULT LOB 2	App Embarcadero DBArtisan	DATABASE SERVERS	10.10.0.91	10.10.0.91	10.10.0.91	arcossqladmin	
5	DEFAULT LOB 2	App Embarcadero DBArtisan	DATABASE SERVERS	10.10.0.91	10.10.0.91	10.10.0.91	arcossqladmin	SUHAS.DINGANKAR

Showing 1 to 5 of 422 entries

Previous 1 2 3 4 5 ... 85 Next

A Privileged Account Management Solution Copyright © 2022 ARCON. All Rights Reserved.


The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
LOB	Name of the LOB
Service Type	The name of the service type
Service Group	The server group in which the service belongs
Domain Name	The domain name of the target server
IP Address	The IP address of the target server
Host name	The hostname of the target server

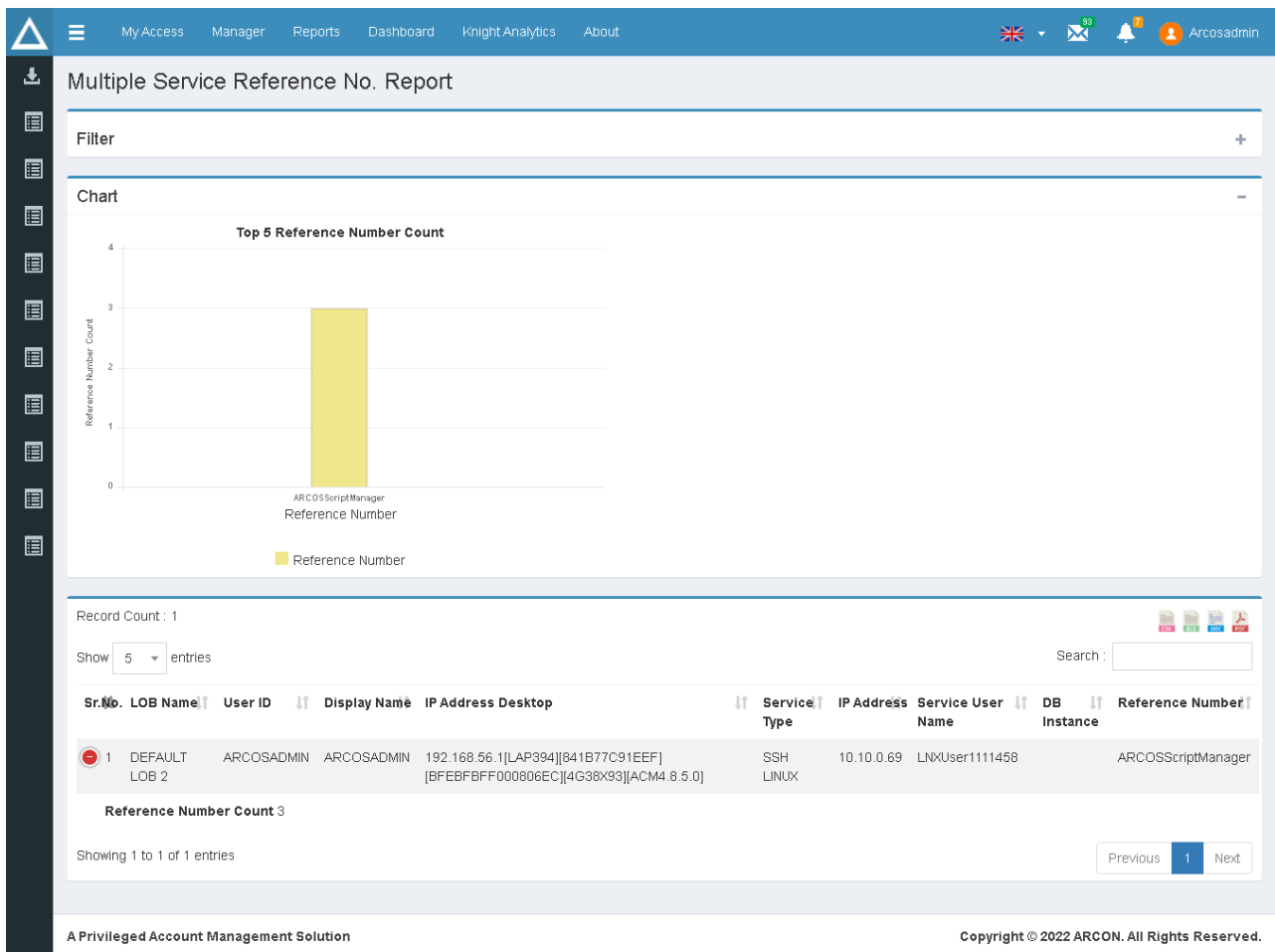
Column Names	Description
Service Username	The user name of the service
Service Mapped to User	The user name to which the service is mapped
DB Instance	Instance of the target servers

11.5 Multiple Service Reference No. Report

The Multiple Service Reference No. Report displays the reference number provided to the user before accessing any service in graphical and grid view format.

 In order to view this report, users must have the following permission(s):

- **Multiple Service Reference Number Report**



Multiple Service Reference No. Report

Filter +

Chart -

Top 5 Reference Number Count

Reference Number	Count
ARCOScriptManager	3

Record Count : 1

Show entries Search:

Sr.No.	LOB Name	User ID	Display Name	IP Address Desktop	Service Type	IP Address	Service User Name	DB Instance	Reference Number
1	DEFAULT LOB 2	ARCOSADMIN	ARCOSADMIN	192.168.56.1[LAP394][841B77C91EEF] [BFEBFBFF000806EC][4G38X93][ACM4.8.5.0]	SSH LINUX	10.10.0.69	LNxUser1111458		ARCOScriptManager

Reference Number Count 3

Showing 1 to 1 of 1 entries Previous Next


A Privileged Account Management Solution Copyright © 2022 ARCON. All Rights Reserved.

The following columns can be seen in this report:

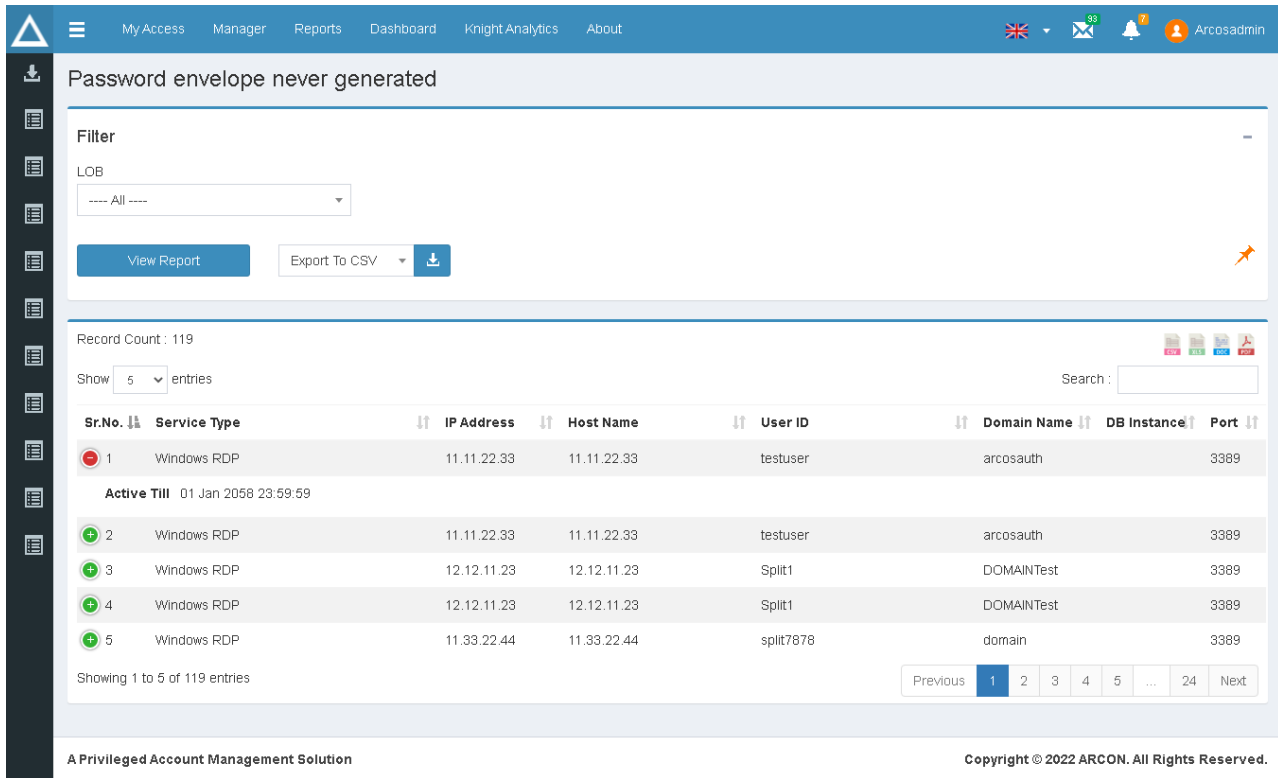
Column Names	Description
Sr. No.	To identify and distinguish rows
LOB Name	Name of the LOB
User ID	The User ID associated with the user
Display Name	The display name of the user
IP Address(Desktop)	The IP address of the desktop
Service Type	The name of the service type whose session is taken
IP Address	The IP address of the target server
Service username	The username of the service
DB Instance	The instance of the target server
Reference Number	The reference number of that service
Refernce Number Count	Number of times the reference is used

11.6 Password Envelope Never Generated Report

The Password Envelope Never Generated Report displays details of those services for which password envelopes have never been produced.

 In order to view this report, users must have the following permission(s):

- **Password Envelope Never Generated Report**



Password envelope never generated

Filter

LOB: ---- All ----

View Report | Export To CSV

Record Count : 119

Show 5 entries | Search:

Sr.No.	Service Type	IP Address	Host Name	User ID	Domain Name	DB Instance	Port	Active Till
1	Windows RDP	11.11.22.33	11.11.22.33	testuser	arcosauth		3389	01 Jan 2058 23:59:59
2	Windows RDP	11.11.22.33	11.11.22.33	testuser	arcosauth		3389	
3	Windows RDP	12.12.11.23	12.12.11.23	Split1	DOMAINTest		3389	
4	Windows RDP	12.12.11.23	12.12.11.23	Split1	DOMAINTest		3389	
5	Windows RDP	11.33.22.44	11.33.22.44	split7878	domain		3389	

Showing 1 to 5 of 119 entries

Previous | 1 | 2 | 3 | 4 | 5 | ... | 24 | Next


A Privileged Account Management Solution | Copyright © 2022 ARCON. All Rights Reserved.

The following columns can be seen in this report:

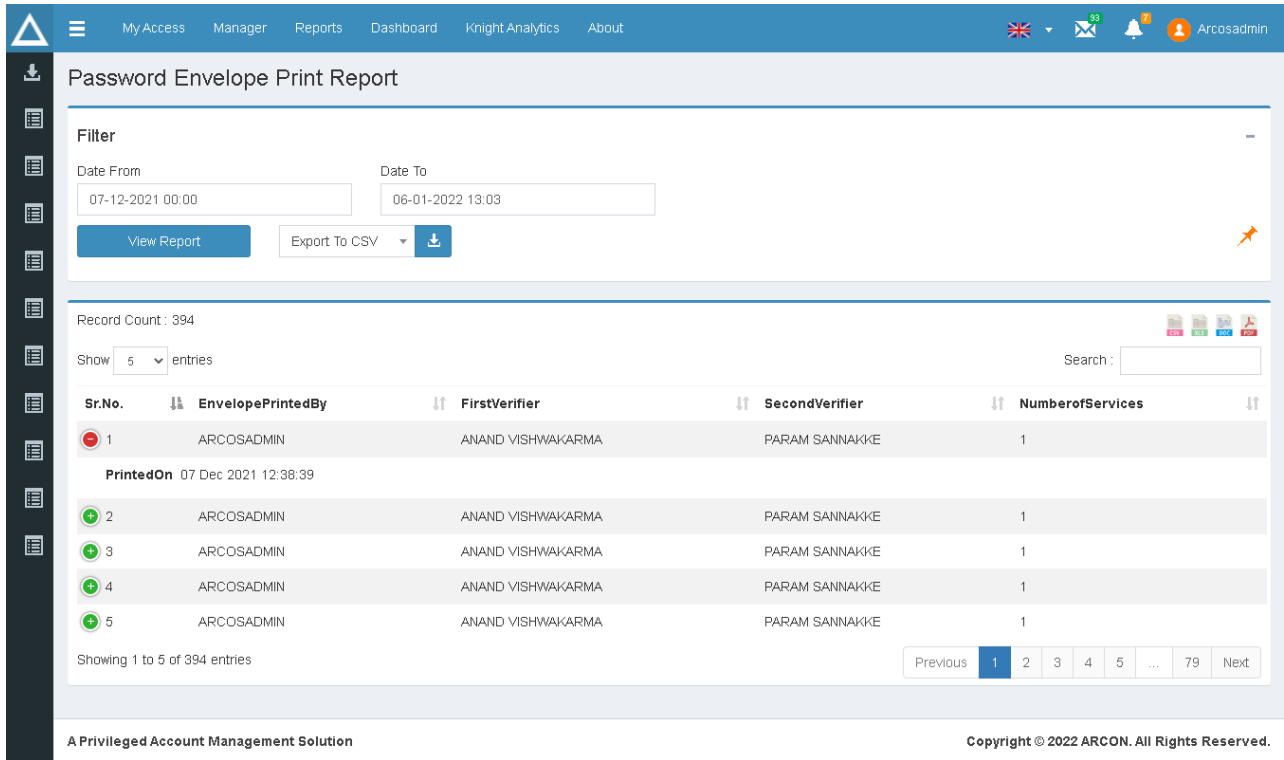
Column Names	Description
Sr. No.	To identify and distinguish rows
Service Type	The name of the service type for which a password was never generated
IP Address	The IP address of the target server
Host name	The Hostname of the target servers
User ID	The User ID associated with the user
Domain Name	The domain name to which the target server belongs for which a password was never generated
DB Instance	The instance of the target servers
Port	The port number of the target server
Active Till	Date until which the service will work

11.7 Password Envelope Print Report

The Password Envelope Print Report displays information about users who have printed password envelopes and confirmed the process.

 In order to view this report, users must have the following permission(s):

- Password Envelope Print Report



Filter

Date From: 07-12-2021 00:00 | Date To: 06-01-2022 13:03

View Report | Export To CSV

Record Count : 394

Show 5 entries | Search:

Sr.No.	EnvelopePrintedBy	FirstVerifier	SecondVerifier	NumberofServices
1	ARCOSADMIN	ANAND VISHWAKARMA	PARAM SANNAKKE	1
PrintedOn 07 Dec 2021 12:38:39				
2	ARCOSADMIN	ANAND VISHWAKARMA	PARAM SANNAKKE	1
3	ARCOSADMIN	ANAND VISHWAKARMA	PARAM SANNAKKE	1
4	ARCOSADMIN	ANAND VISHWAKARMA	PARAM SANNAKKE	1
5	ARCOSADMIN	ANAND VISHWAKARMA	PARAM SANNAKKE	1

Showing 1 to 5 of 394 entries | Previous 1 2 3 4 5 ... 79 Next


A Privileged Account Management Solution | Copyright © 2022 ARCON. All Rights Reserved.

The following columns can be seen in this report:

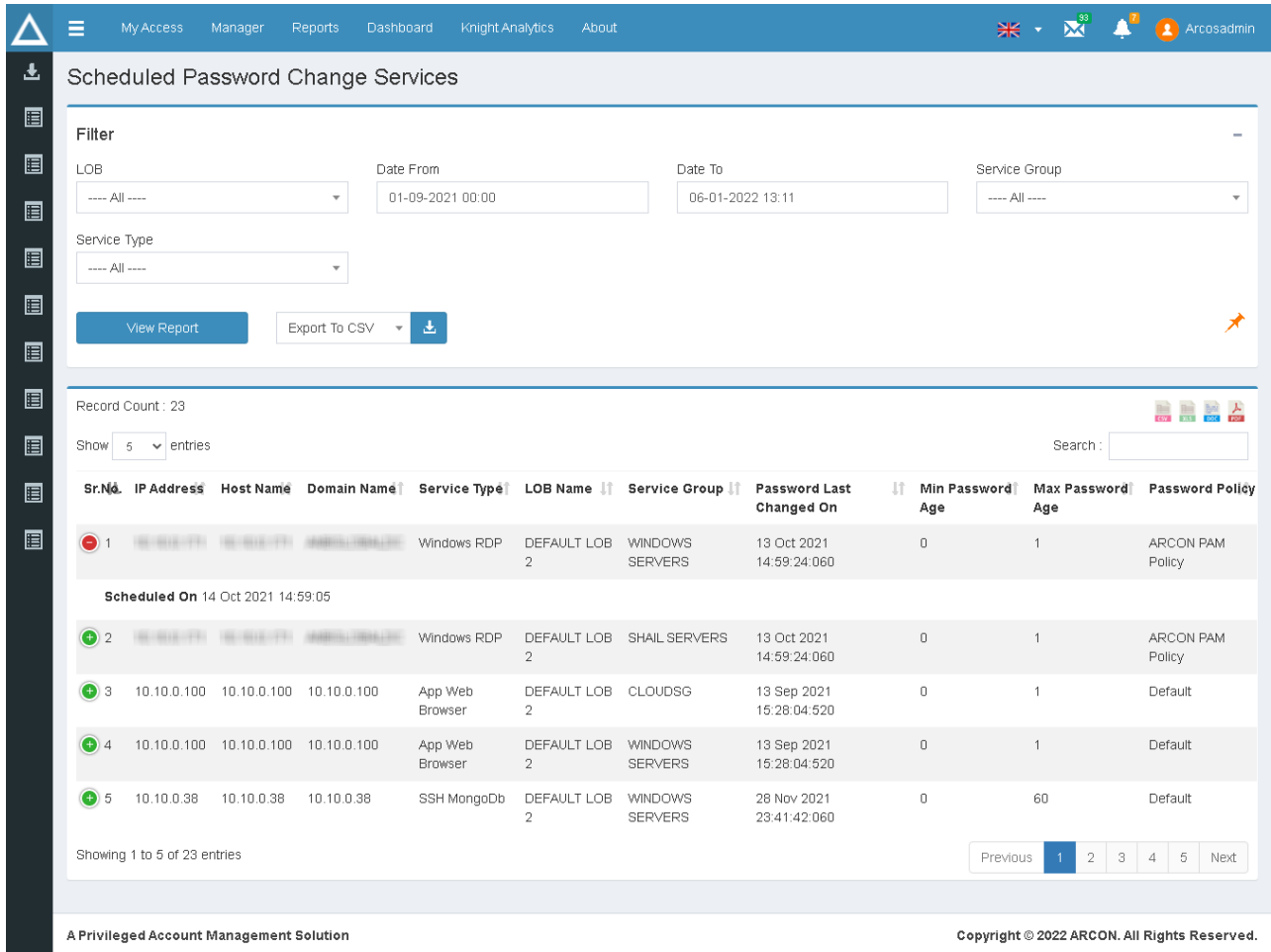
Column Names	Description
Sr. No.	To identify and distinguish rows
Envelope Printed By	Name of the user who printed the envelope
First Verifier	Name of the first Administrator who verified the print command before printing the envelope
Second Verifier	Name of the second Administrator who verified the print command before printing the envelope
Number of Services	Number of services set for print by the user
Printed On	Date/time at which the envelope was printed

11.8 Scheduled Password Change Services

The Scheduled Password Change Services report displays details of all the services that are scheduled for the password change process.

 In order to view this report, users must have the following permission(s):

- **Scheduled Password Change Services**



Scheduled Password Change Services

Record Count : 23

Show 5 entries

Sr.No.	IP Address	Host Name	Domain Name	Service Type	LOB Name	Service Group	Password Last Changed On	Min Password Age	Max Password Age	Password Policy
1				Windows RDP	DEFAULT LOB 2	WINDOWS SERVERS	13 Oct 2021 14:59:24.060	0	1	ARCON PAM Policy
Scheduled On 14 Oct 2021 14:59:05										
2				Windows RDP	DEFAULT LOB 2	SHAIL SERVERS	13 Oct 2021 14:59:24.060	0	1	ARCON PAM Policy
3	10.10.0.100	10.10.0.100	10.10.0.100	App Web Browser	DEFAULT LOB 2	CLOUDSG	13 Sep 2021 15:28:04.520	0	1	Default
4	10.10.0.100	10.10.0.100	10.10.0.100	App Web Browser	DEFAULT LOB 2	WINDOWS SERVERS	13 Sep 2021 15:28:04.520	0	1	Default
5	10.10.0.38	10.10.0.38	10.10.0.38	SSH MongoDB	DEFAULT LOB 2	WINDOWS SERVERS	28 Nov 2021 23:41:42.060	0	60	Default

Showing 1 to 5 of 23 entries

A Privileged Account Management Solution Copyright © 2022 ARCON. All Rights Reserved.


The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
IP Address	The IP address of the target server
Host Name	The hostname of the target server
Domain Name	The domain name of the target server
Service type	Name of the service type
LOB Name	The name of the LOB in which passwords are scheduled for change

Column Names	Description
Service Group	The name of the service group to which the service belongs
Password Last Changed On	Date/time of last password change
Min Password Age	Lowest age of the password
Max Password Age	Maximum age of the password after which the password changes
Password Policy	Name of the assigned password policy
Scheduled On	Date/time when the password was scheduled

11.9 Server Last Accessed On

The Server Last Accessed On report displays records of servers that are not accessed for a number of days. The number of days is set in **Days of server last accessed on** configuration by the Administrator in Settings.

 In order to view this report, users must have the following permission(s)

- **Server Last Accessed On**

Sr.No	Server IP	Host Name	Domain Name	Last Accessed On
1	3.6.49.70	I-09B0215568CECB707		Sep 23 2021 4:43PM
Days Since Last Accessed 105				
2	3.6.49.70	I-004C0C0F311C9B23F		Oct 28 2021 1:14PM
3	6.6.6.6	6.6.6.6	6.6.6.6	NEVER
4	10.10.5.401	10.10.5.401	10.10.5.401	Oct 19 2021 11:32AM
5	10.10.5.40	10.10.5.40	10.10.5.40	Oct 18 2021 11:43AM

 The interface also shows 'Showing 1 to 5 of 284 entries' and a pagination control with 'Previous', '1', '2', '3', '4', '5', '...', '57', and 'Next'. At the bottom, it says 'A Privileged Account Management Solution' and 'Copyright © 2022 ARCON. All Rights Reserved.'

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Server IP	The IP address of the target server
Host Name	The hostname of the target server
Domain Name	The domain name of the target server
Last Accessed On	Date/time when the server was last used
Days Since Last Accessed	The number of days passed since the server was accessed

11.10 Servers in Domain

The Servers in Domain report provides information about all the servers in a domain regardless of the LOB in graphical and grid view format.



In order to view this report, users must have the following permission(s):

- Servers in Domain

Record Count : 347

Show 5 entries

Sr.No.	Domain Name	IP Address	Host Name	Instance	Port
1	1.1.1.3	1.1.1.3	1.1.1.3		3389
LOB/Profile DEFAULT LOB 2					
2	testservices	10.10.0.201	TESTSERVICES		34
3	testservice	44.44.44.44	TESTSERVICE		34
4	http://10.10.0.53/svn	10.10.0.53	HTTP://10.10.0.53/SVN		22
5	arcosauth	10.10.0.87	10.10.0.87	As	22

Showing 1 to 5 of 347 entries

Previous 1 2 3 4 5 ... 70 Next


A Privileged Account Management Solution Copyright © 2022 ARCON. All Rights Reserved.

The following columns can be seen in this report:

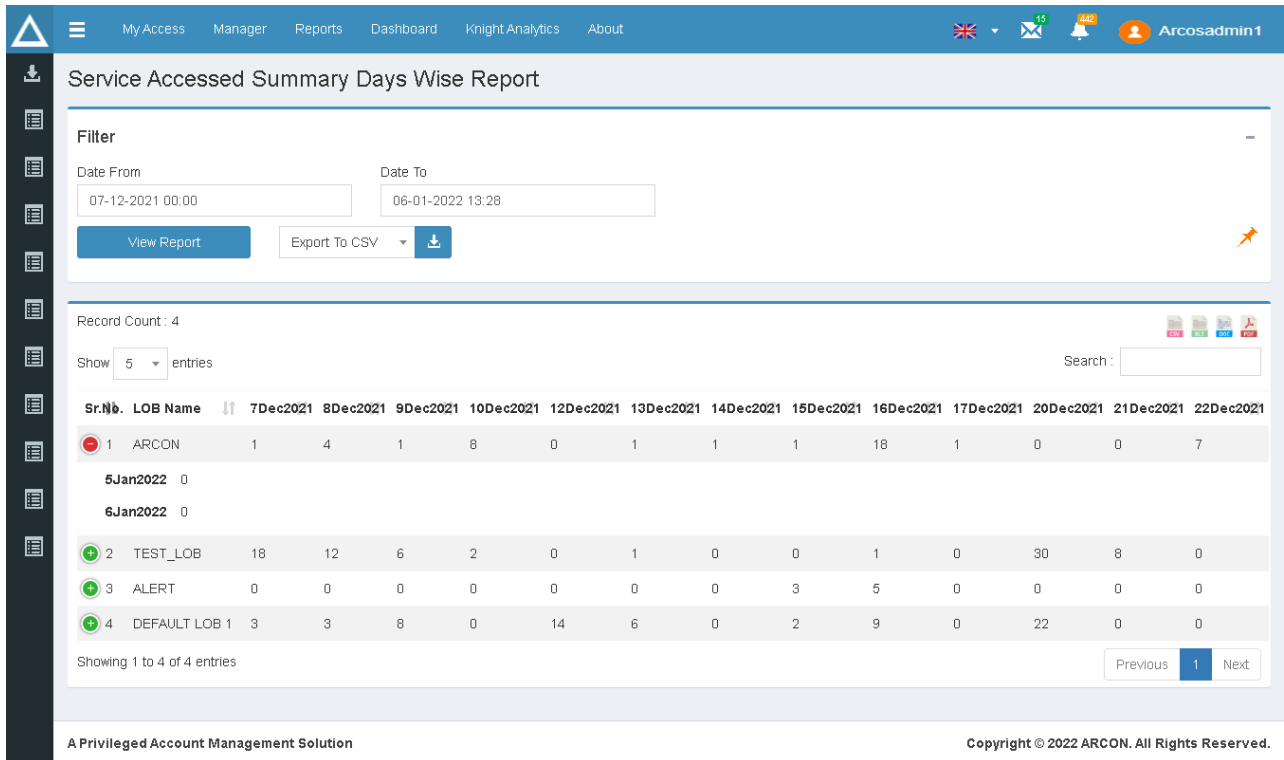
Column Names	Description
Sr. No.	To identify and distinguish rows
Domain Name	The domain name of the target server
IP Address	The IP address of the target server
Host Name	The hostname of the target server
Instance	The instance of the target server
Port	The port number of the target server
LOB/Profile	The name of the LOB in which the servers are present

11.11 Service Accessed Summary Day Wise Report

The Service Accessed Summary Day Wise Report provides information about the total count of the services accessed on a daily basis.

 In order to view this report, users must have the following permission(s):

- **Service Accessed Summary Day-wise Report**




The following columns can be seen in this report:

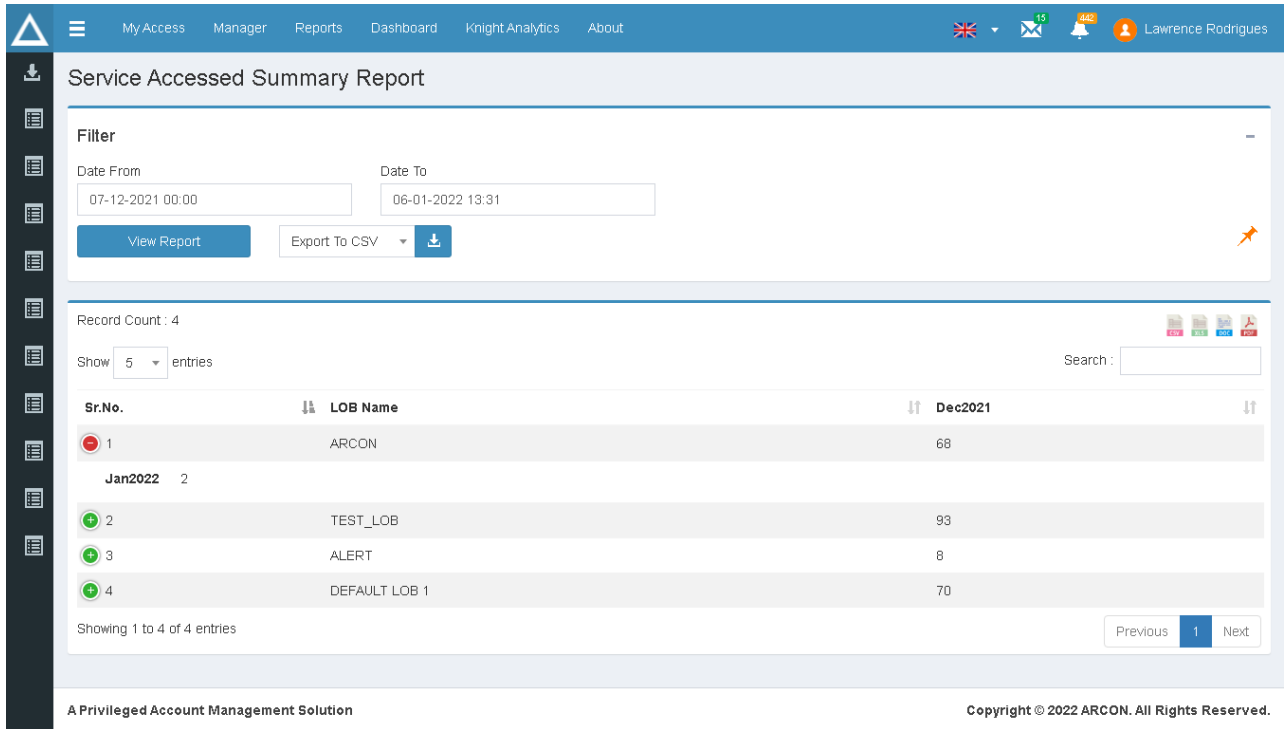
Column Names	Description
Sr. No.	To identify and distinguish rows
LOB/Profile	The name of the LOB through which the services are accessed
Date wise - first date as selected in the filter (Example- 3rd May 2021)	Total number of services accessed on that day

11.12 Service Accessed Summary Report

The Service Accessed Summary Report displays the total number of services accessed by users on a monthly basis, LOB-wise.

 In order to view this report, users must have the following permission(s):

- **Service Accessed Summary Report**



Service Accessed Summary Report

Filter

Date From: 07-12-2021 00:00 Date To: 06-01-2022 13:31

View Report Export To CSV

Record Count : 4

Show 5 entries Search :

Sr.No.	LOB Name	Dec2021
1	ARCON	68
Jan2022 2		
2	TEST_LOB	93
3	ALERT	8
4	DEFAULT LOB 1	70

Showing 1 to 4 of 4 entries Previous 1 Next


A Privileged Account Management Solution Copyright © 2022 ARCON. All Rights Reserved.

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
LOB/Profile	The name of the LOB through which the services are accessed
Date wise - first date as selected in the filter (Example- Dec 2021)	Total number of services accessed in that month

11.13 Service Application Report

The Service Application Report displays the mapping of all the applications to their service type while configuring the service.

 In order to view this report, users must have the following permission(s):

- **Service Application Report**


The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
LOB Name	The name of the LOB in which the services are accessed
Service Group	The name of the service group to which the service belongs
IP Address	The IP address of the target server
Instance Name	The instance of the target servers
Host name	The Hostname of the target server
Domain name	The domain name to which the target server belongs
Service type	The name of the service type
Application Name	Names of applications that are mapped to the main service
Description 1	Text entered during the creation of the service
Description 2	Text entered during the creation of the service

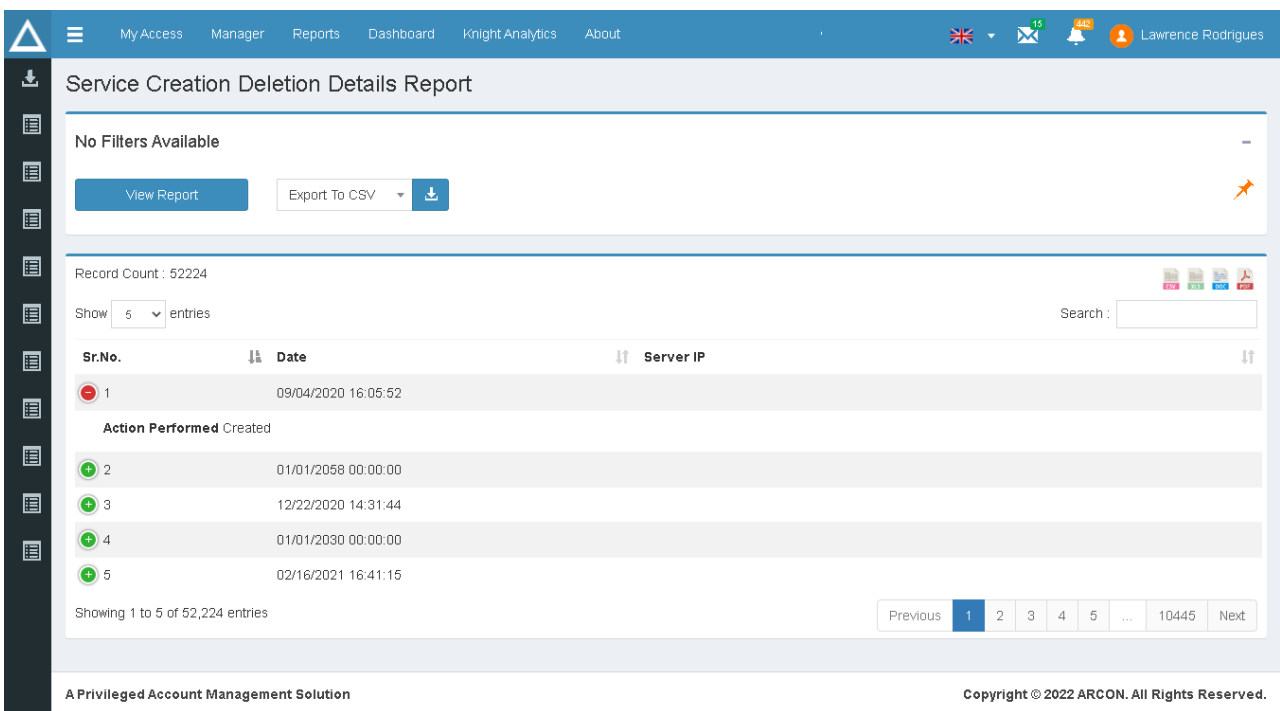
Column Names	Description
Description 3	Text entered during the creation of the service
Description 4	Text entered during the creation of the service

11.14 Services Creation Deletion Details Report

The Services Creation Deletion Details Report informs the user about the creation or deletion of service groups in ARCON | PAM.

 In order to view this report, users must have the following permission(s):

- **Services Creation Deletion Details Report**




The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Date	Date/time of service creation
Server IP	The IP address of the target server

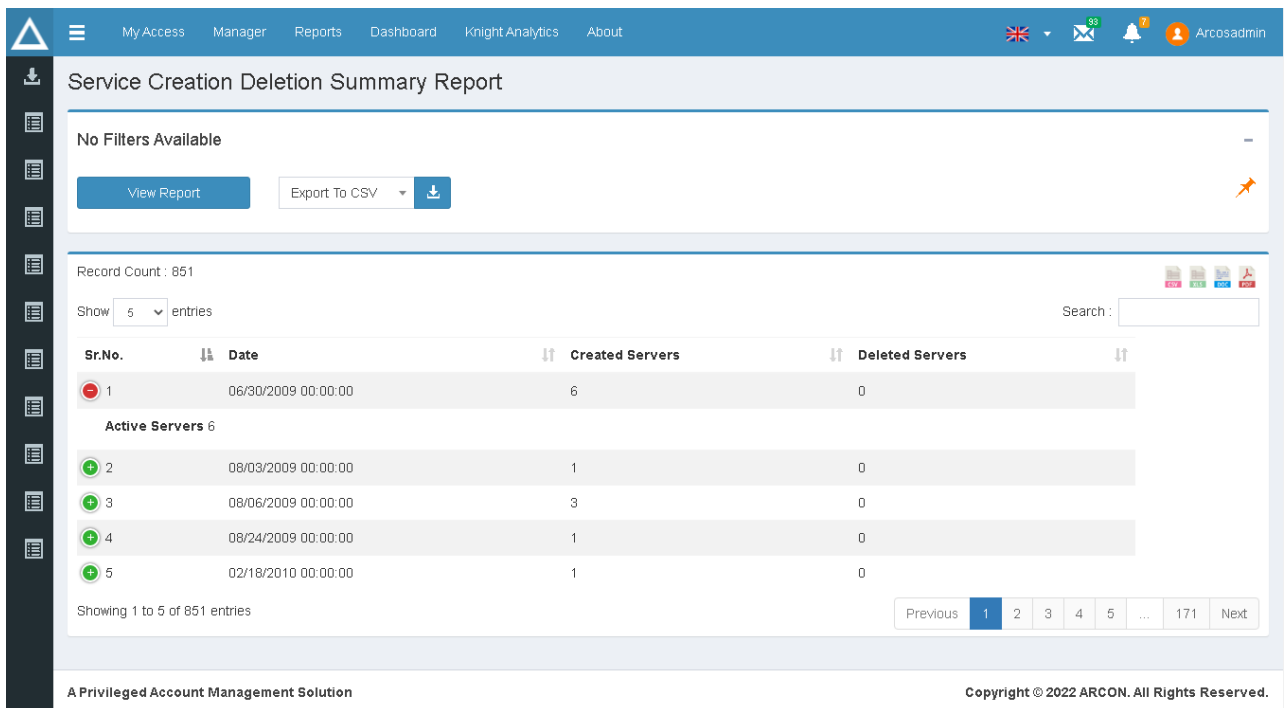
Column Names	Description
Action Performed	Activity performed on the service <ul style="list-style-type: none"> • Creation • Deletion

11.15 Services Creation Deletion Summary Report

The Services Creation Deletion Summary Report displays the total number of services created and deleted on a date-by-date basis.

 In order to view this report, users must have the following permission(s):

- **Services Creation Deletion Summary Report**




The following columns are available in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Date	Date/time of service creation
Created servers	The total number of servers created on that day
Deleted Servers	The total number of servers deleted on that day

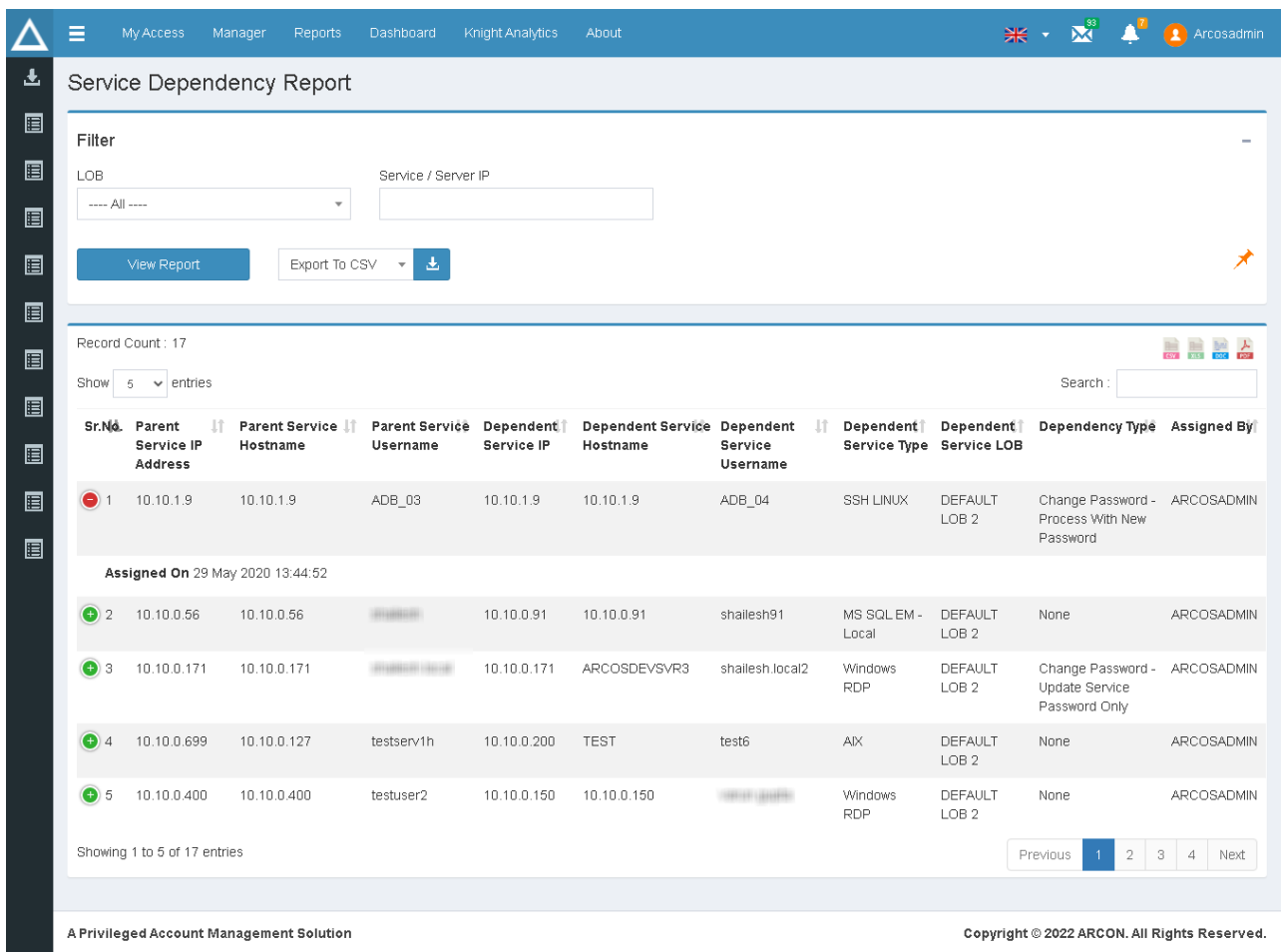
Column Names	Description
Active Servers	The total number of active servers on that day

11.16 Service Dependency Report

The Service Dependency Report displays the details of dependency between mapped applications and their services.

 In order to view this report, users must have the following permission(s):

- **Service Dependency Report**



Service Dependency Report

Filter

LOB: Service / Server IP:

Record Count : 17

Show entries Search :

Sr.No.	Parent Service IP Address	Parent Service Hostname	Parent Service Username	Dependent Service IP	Dependent Service Hostname	Dependent Service Username	Dependent Service Type	Dependent Service LOB	Dependency Type	Assigned By
1	10.10.1.9	10.10.1.9	ADB_03	10.10.1.9	10.10.1.9	ADB_04	SSH LINUX	DEFAULT LOB 2	Change Password - Process With New Password	ARCOSADMIN
Assigned On 29 May 2020 13:44:52										
2	10.10.0.56	10.10.0.56	...	10.10.0.91	10.10.0.91	shailesh91	MS SQLEM - Local	DEFAULT LOB 2	None	ARCOSADMIN
3	10.10.0.171	10.10.0.171	...	10.10.0.171	ARCOSDEVSVR3	shailesh.local2	Windows RDP	DEFAULT LOB 2	Change Password - Update Service Password Only	ARCOSADMIN
4	10.10.0.699	10.10.0.127	testserv1h	10.10.0.200	TEST	test6	AIX	DEFAULT LOB 2	None	ARCOSADMIN
5	10.10.0.400	10.10.0.400	testuser2	10.10.0.150	10.10.0.150	...	Windows RDP	DEFAULT LOB 2	None	ARCOSADMIN

Showing 1 to 5 of 17 entries

Previous Next

A Privileged Account Management Solution Copyright © 2022 ARCON. All Rights Reserved.


The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Parent Service IP address	The IP address of the parent server

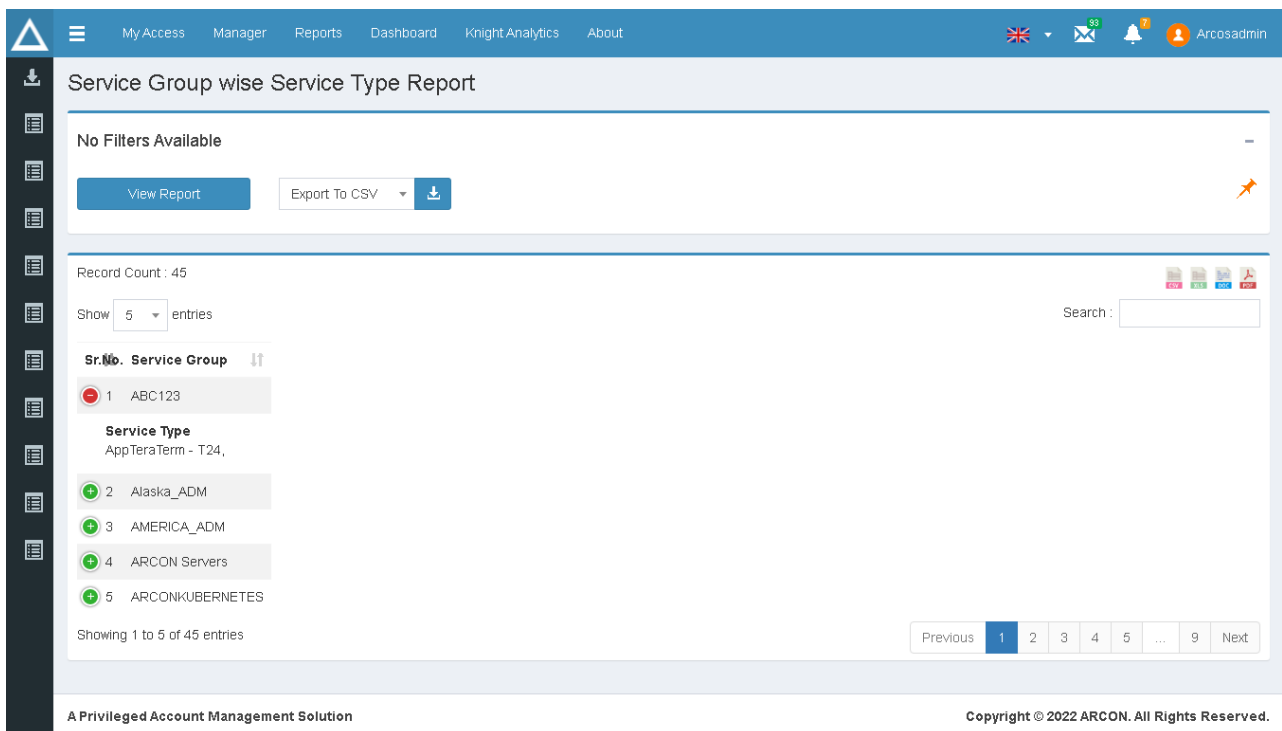
Column Names	Description
Parent Service Hostname	The Hostname of the parent server
Parent Service Username	The username of the parent server
Dependent Service IP	The IP address of the dependent server
Dependent Service Hostname	The Hostname of the dependent server
Dependent Service Username	The username of the dependent server

11.17 Service Group Wise Service Type Report

The Service Group Wise Service Type Report informs the user about all the service groups in ARCON | PAM and the services that belong to them.

 In order to view this report, users must have the following permission(s):

- **Service Group-wise Service Type Report**




The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows

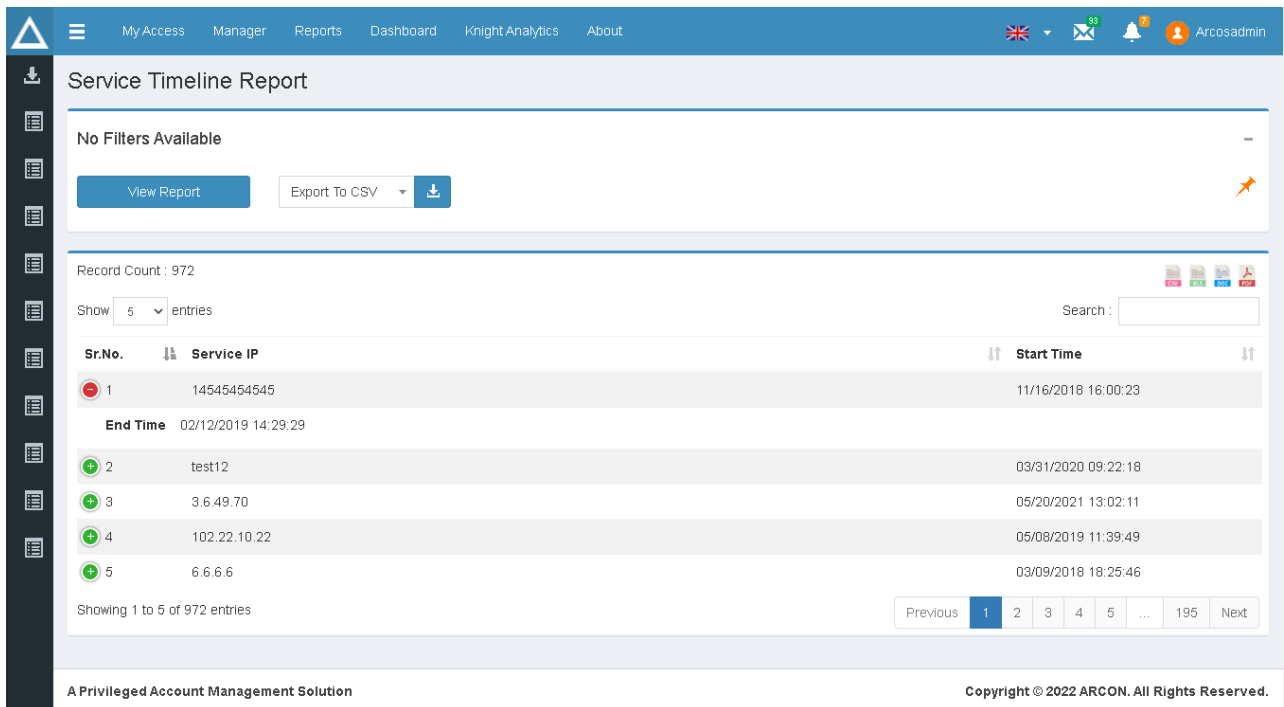
Column Names	Description
Service Group	The name of the service group to which the services belong
Service Type	List of all the service types belonging to that service group

11.18 Service Timeline Report

The Service Timeline Report informs the user about start and termination times of the service.

 In order to view this report, users must have the following permission(s):

- **Service Timeline Report**



The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Service IP	The IP Address of the target server
Start time	Date/time captured at the start when accessing the target server
End time	Date/time captured at end of the session

11.19 Services in Domain Report

The Services in Domain Report informs the user about all the services in a domain in graphical and grid view format, regardless of the LOB.



In order to view this report, users must have the following permission(s)

- **Services in Domain Report**

The screenshot shows the 'Services In Domain' report interface. At the top, there is a navigation bar with options like 'My Access', 'Manager', 'Reports', 'Dashboard', 'Knight Analytics', and 'About'. The main content area is divided into sections: 'No Filters Available' with 'View Report' and 'Export To CSV' buttons; a 'Chart' section titled 'Total Number of Services in Each Domain' showing a bar chart with domain names on the x-axis and 'Count' on the y-axis; and a table section with a 'Record Count : 617' and 'Show 5 entries' dropdown. The table has columns for 'Sr.No.', 'Domain Name', 'Service User Name', 'IP Address', 'Host Name', 'Instance', and 'Port'. The first five rows of data are as follows:

Sr.No.	Domain Name	Service User Name	IP Address	Host Name	Instance	Port
1	192.168.0.242	Mssqladmin	192.168.0.242	192.168.0.242		3389
2	178.249.3.21	arcos007	178.249.3.21	178.249.3.21		992
3	96.47.200.189	SINGHS	96.47.200.189	96.47.200.189	96.47.200.189	1433
4	10.10.0.205	sys	10.10.0.205	10.10.0.205	oracle	1521
5	LNXRH4_ARCONSRV	root	192.168.0.240	LNXRH4_ARCONSRV		5902

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Domain Name	The domain name of the target server

Column Names	Description
Service username	The username of the service
IP Address	The IP address of the target server
Hostname	The hostname of the target server
Instance	Instance of the target servers
Port	Port number of the target server
LOB/Profile	The name of the LOB

11.20 Unique Services IP Address Report

The Unique Services IP Address Report displays information on all services with unique IP addresses in a graphical and grid view format.



In order to view this report, users must have the following permission(s):

- **Unique Services IP Address Report**

Service Type Wise Percentage

- App ASE Client : 1
- App duck : 1
- App LMT Client : 1
- App Toad for SQLserver : 1
- App Web Browser : 1
- MS SQL EM - Local : 1
- SSH LINUX : 2
- Windows RDP : 5

Sr.No.	Service Type	LOB Name	Host Name	IP Address	Total Services	Active Services	Inactive Services
1	App ASE Client	DEBOARDING	10.10.0.382	10.10.0.38	3	3	0
2	App duck	DEBOARDING	10.10.0.10	10.10.0.10	2	2	0
3	App LMT Client	DEBOARDING	10.10.0.2	10.10.0.2	1	1	0
4	App Toad for SQLserver	DEBOARDING	10.10.0.56	10.10.0.56	1	1	0
5	App Web Browser	DEBOARDING	10.10.0.11	10.10.0.11	1	1	0

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Service type	The name of the service type
LOB/Profile	The name of the LOB
Host Name	The hostname of the target server
IP address	The IP address of the target server
Total services	The total number of services
Active services	The total number of active services
Inactive services	The total number of inactive services

12 User Reports

User reports generate details of all types of users, whether they are active, inactive, dormant, logged out, etc., and the activities performed by them.

The following reports are available in User Reports:

- Active Users Report
- Consolidated User & Service Mapping Report
- Dormant User Report
- Dual Factor Auth Configuration Report
- Dual Factor Auth Configuration Report - All LOB
- Idle Users Report
- Inactive Users Report
- Last Service Accessed Report
- Locked Out User Report
- User & Service Mapping Report
- User Biometric Auth Report
- User Biometric Auth Report - All LOB
- User Compliance Report
- User Creation Deletion Summary Report
- User Dormant in next 5 day Report
- User Hardware Auth Report
- User Last Logon Report
- User Mobile OTP Auth Report
- User SMS OTP Auth Report
- User Status Report

12.1 Active Users Report.

The Active Users Report displays information about all active users and their type in graphical and grid view format. An active user is one who has interacted with the PAM application within a certain time period.



In order to view this report, users must have the following permission(s)

- **Active Users Report**

My Access
 Manager
Reports
Dashboard
Knight Analytics
About

 Arcosadmin1

Active Users Report

No Filters Available

View Report

Export To CSV
↓
↓

Chart

Total Number of Admins and Clients

User Type	Count
Client	~10000
Admin	~0

Record Count : 10452

Show 5 entries Search :

Sr.No.	User ID	Display Name	Domain	User Valid Till	User Type	Created By
1	USER6008		ATSTESTDC	01 Jan 2058 00:00:00	Client	SYSTEM
<div style="font-size: 0.8em; margin-left: 10px;"> <p>Email ID</p> <p>Mobile No</p> <p>AltLOB</p> <p>AltGroups</p> <p>Country</p> <p>Created On 28 Mar 2019 13:11:24</p> </div>						
2	USER3737		ATSTESTDC	01 Jan 2058 00:00:00	Client	SYSTEM
3	USER2861		ATSTESTDC	01 Jan 2058 00:00:00	Client	SYSTEM
4	USER9722		ATSTESTDC	01 Jan 2058 00:00:00	Client	SYSTEM
5	USER2772		ATSTESTDC	01 Jan 2058 00:00:00	Client	SYSTEM




Showing 1 to 5 of 10,452 entries

Previous 1 2 3 4 5 ... 2091 Next

A Privileged Account Management Solution
Copyright © 2022 ARCON. All Rights Reserved.


The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
User ID	The User ID associated with the user

Column Names	Description
Display Name	The display name of the user
Domain	The domain name to which the user belongs
User Valid till	Date until which the user will be active
User Type	Type of user <ul style="list-style-type: none"> • Client • Admin
Created By	The name of the Administrator who created the user
Email Id	Email address of the user as configured by the Administrator
Mobile Number	Mobile number of the user as configured by the Administrator
Description 1 - Example - Country (Customized Field)	Specifies country name to which the user belongs <div style="border: 1px solid #ccc; background-color: #e6e6fa; padding: 5px; margin-top: 5px;"> <p> This field name is bespoke and can be set according to the organization's requirements by the Administrator</p> </div>
Description 2 - Example - State (Customized Field)	Specifies state name to which the user belongs <div style="border: 1px solid #ccc; background-color: #e6e6fa; padding: 5px; margin-top: 5px;"> <p> This field name is bespoke and can be set according to the organization's requirements by the Administrator</p> </div>
Description 3 - Example - District (Customized Field)	Specifies district name to which the user belongs <div style="border: 1px solid #ccc; background-color: #e6e6fa; padding: 5px; margin-top: 5px;"> <p> This field name is bespoke and can be set according to the organization's requirements by the Administrator</p> </div>
Created On	Date/time of the creation of the user by the Administrator

12.2 Consolidated User & Service Mapping Report

The Consolidated User & Service Mapping Report displays the total count of each service type linked to the user.

 In order to view this report, users must have the following permission(s):


• **Consolidated User & Service Mapping Report**

The following columns can be seen in this report:

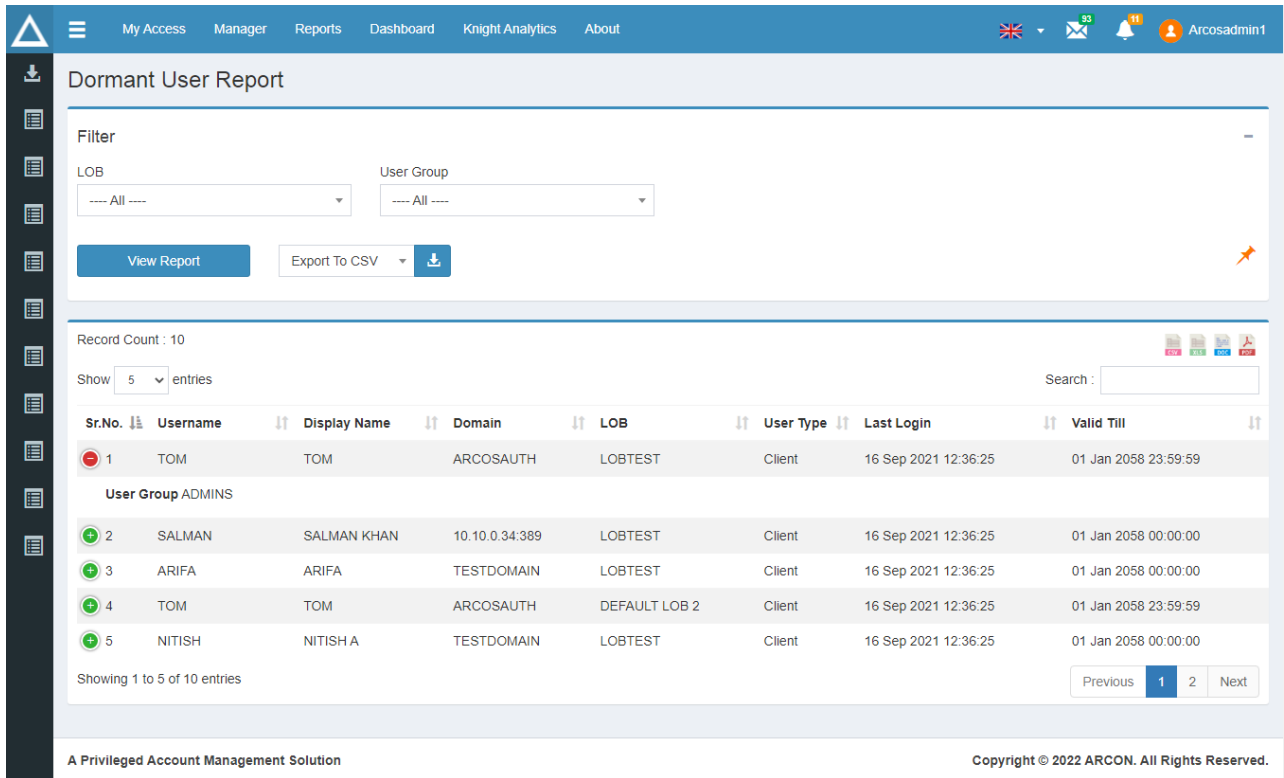
Column Names	Description
Sr. No.	To identify and distinguish rows
User ID	The User ID associated with the user
Display Name	The display name of the user
Service Type	The name of the service type
User Group	The name of the user group to which the user belongs
Total Services Count	The total of all the services of a particular service type mapped to the user

12.3 Dormant User Report

The Dormant User Report displays information about all the dormant users in ARCON | PAM. A dormant user is one who hasn't interacted with the PAM application in a certain period of time (specified in the **User Dormancy Alert - Schedule Days** configuration in Settings).

 In order to view this report, users must have the following permission(s):

- **Dormant User Report**



The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Username	The name of the user
Display Name	The display name of the user
Domain	The domain name to which the user belongs
LOB	The name of the LOB in which the user is present

Column Names	Description
User Type	Type of user <ul style="list-style-type: none"> • Client • Admin
Last Login	Date/time when the user last logged in
Valid Till	Date until which the user will be active
User Group	The name of the user group to which the user belongs

12.4 Dual Factor Auth Configuration Report

Dual Factor Auth Configuration Report displays information of all the users and the status (enabled, configured, not configured, etc.) of each dual-factor authentication configuration to make the ACMO login process more secure.



In order to view this report, users must have the following permission(s):

- **Dual Factor Auth Configuration Report**

Dual Factor Auth Configuration Report

Filter

LOB: User ID:

[View Report](#) [Export To CSV](#)

Record Count : 10319

Show entries

Sr.No.	User ID	Display Name	Email ID	Email OTP	Email OTP Configured on	Mobile No	Mobile OTP	Mobile OTP Configured on
1	USER6008			Not Configured Yet			Not Configured Yet	
2	USER3737			Not Configured Yet			Not Configured Yet	
3	USER2861			Not Configured Yet			Not Configured Yet	
4	USER9722			Not Configured Yet			Not Configured Yet	
5	USER2772			Not Configured Yet			Not Configured Yet	

Showing 1 to 5 of 10,319 entries

Previous 1 2 3 4 5 ... 2064 Ne

A Privileged Account Management Solution Copyright © 2022 ARCON. All Rights Reserved


The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
User ID	The user ID associated with the user
Display Name	The display name of the user
Email OTP	Status of configuration <ul style="list-style-type: none"> Not configured yet Configured but not enabled Configured and enabled
Email OTP Configured on	Date/time when email 2FA was configured
Mobile No	Mobile number of the user configured by the Administrator

Column Names	Description
Mobile OTP	Status of configuration <ul style="list-style-type: none"> • Not configured yet • Configured but not enabled • Configured and enabled
Mobile OTP Configured On	Date/time when mobile OTP was configured
RSA secure ID	Status of configuration <ul style="list-style-type: none"> • Not configured yet • Configured but not enabled • Configured and enabled
RSA secure ID Configured On	Date/time when RSA secure ID 2FA was configured
Biometric	Status of configuration <ul style="list-style-type: none"> • Not configured yet • Configured but not enabled • Configured and enabled
Biometric Configured On	Date/time when biometric 2FA was configured
SMS OTP	Status of configuration <ul style="list-style-type: none"> • Not configured yet • Configured but not enabled • Configured and enabled
SMS OTP Configured On	Date/time when SMS OTP was configured

12.5 Dual Factor Auth Configuration Report - All LOB

The Dual Factor Auth Configuration Report - All LOB displays reports for the users who have configured the dual-factor authorization across all LOBs to make the login process more secure.

 In order to view this report, users must have the following permission(s):

- **Dual Factor Auth Configuration Report - All LOB**

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
User ID	The User ID associated with the user
Display Name	The display name of the user
Email ID	Email ID of the user
Mobile No.	Mobile number of the user configured by the Administrator

Column Names	Description
Mobile OTP	Status of configuration <ul style="list-style-type: none"> • Not configured yet • Configured but not enabled • Configured and enabled
Mobile OTP Configured on	Date/time when mobile OTP was configured
RSA Secure ID	Status of configuration <ul style="list-style-type: none"> • Not configured yet • Configured but not enabled • Configured and enabled
RSA Secure ID Configured on	Date/time when RSA secure ID 2FA was configured
Biometric	Status of configuration <ul style="list-style-type: none"> • Not configured yet • Configured but not enabled • Configured and enabled
Biometric Configured on	Date/time when biometric 2FA was configured
SMS OTP	Status of configuration <ul style="list-style-type: none"> • Not configured yet • Configured but not enabled • Configured and enabled
SMS OTP Configured on	Date/time when SMS OTP was configured

12.6 Idle Users Report

The Idle Users Report displays information on all idle users in ARCON | PAM.



In order to view this report, users must have the following permission(s):

- **Idle Users Report**


The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
LOB Name	The name of the LOB to which the idle user belongs
Username	The name of the user
Display name	The display name of the user
Domain name	The domain name to which that user belongs
Last Logon	Date/time when the user last logged in
Not Logon Since Days	Number of days since passed since the last login

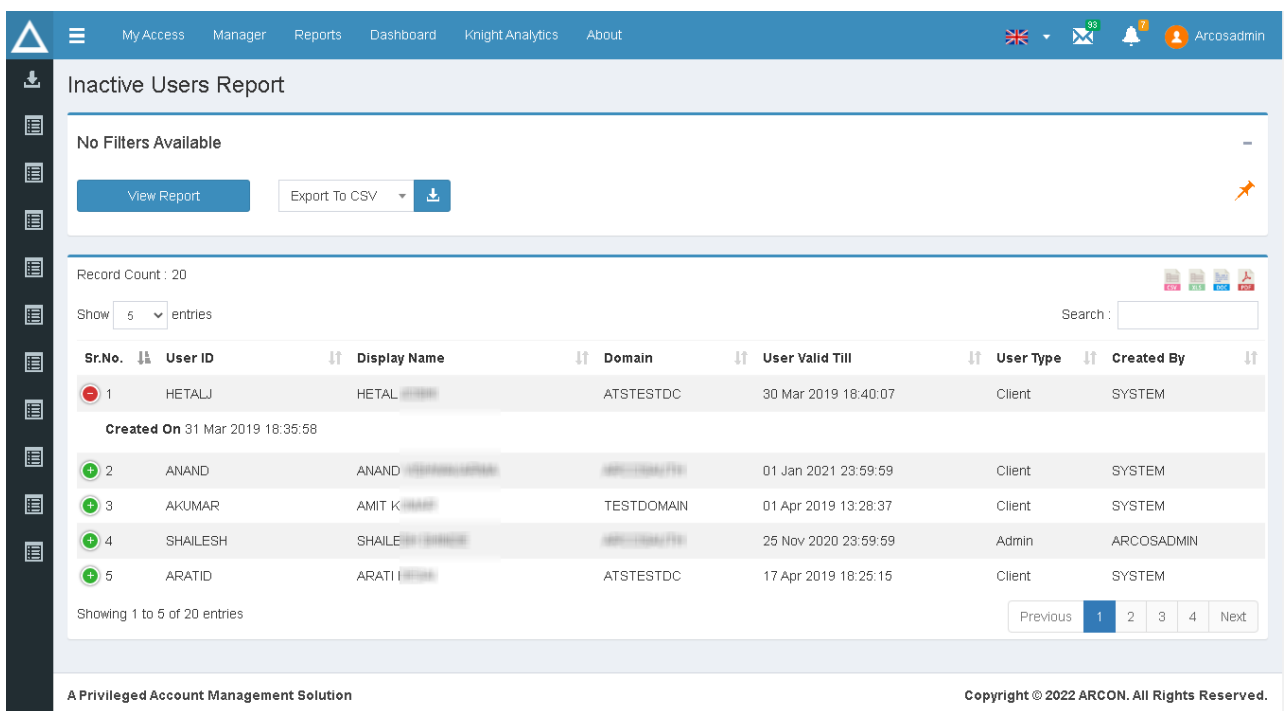
Column Names	Description
User status	Status of the user <ul style="list-style-type: none"> Active Inactive

12.7 Inactive Users Report.

Inactive Users Report informs the user about all inactive users in ARCON | PAM.

 In order to view this report, users must have the following permission(s):

- Inactive Users Report**




The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
User ID	The User ID associated with the user
Display Name	The display name of the user
Domain	The domain name to which the user belongs
User Valid Till	Date until which the user will be active

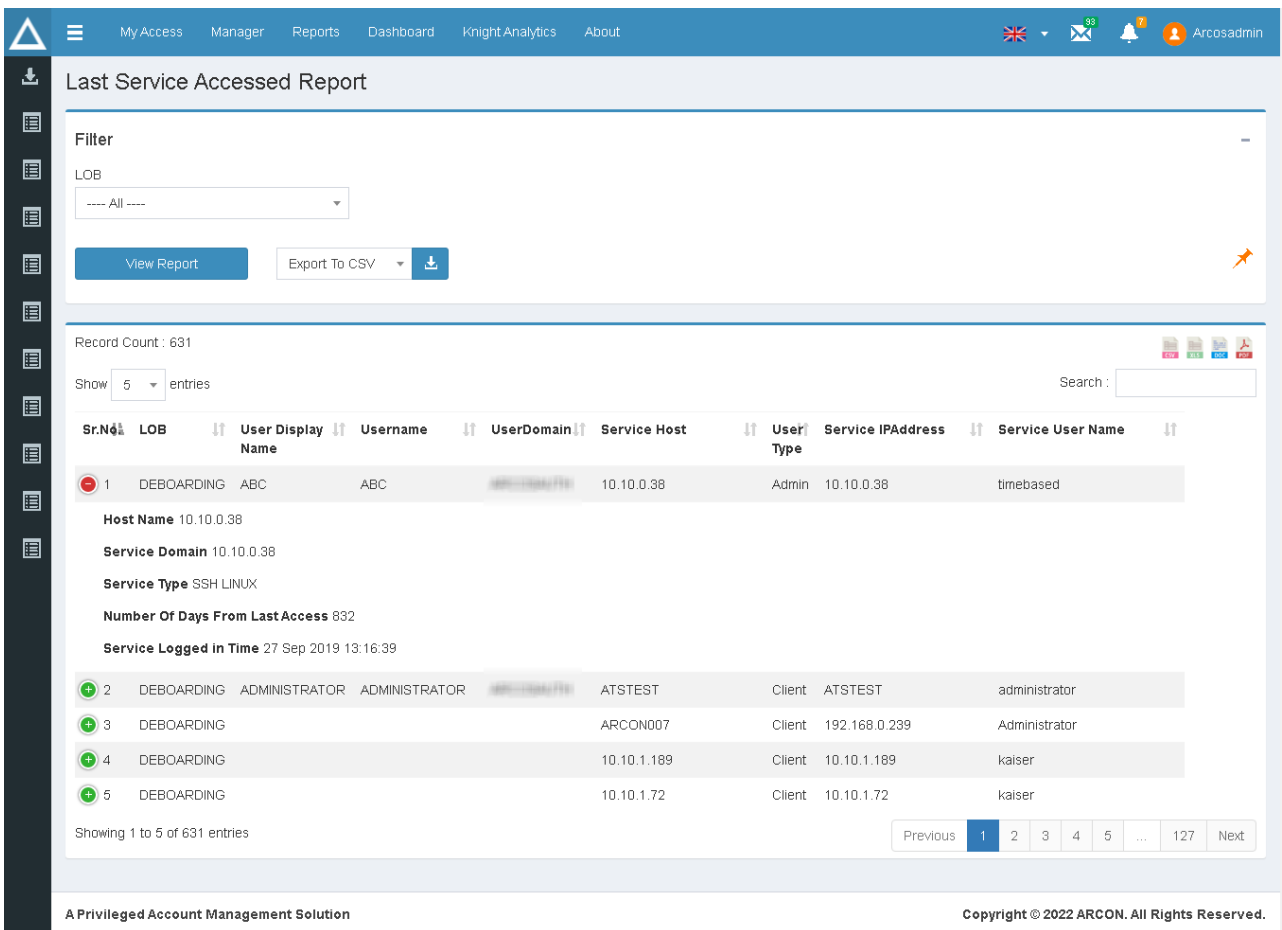
Column Names	Description
User Type	Type of user <ul style="list-style-type: none"> • Client • Admin
Created By	The name of Administrator who created the user
Created On	Date/time of the creation of the user by the Administrator

12.8 Last Service Accessed Report

The Last Service Accessed Report displays information about users and the last time they accessed that service.

 In order to view this report, users must have the following permission(s):

- **Last Service Accessed Report**



Record Count : 631

Show **5** entries

Sr.No.	LOB	User Display Name	Username	UserDomain	Service Host	User Type	Service IPAddress	Service User Name
1	DEBOARDING	ABC	ABC	ARCON\ABC	10.10.0.38	Admin	10.10.0.38	timebased
Host Name 10.10.0.38 Service Domain 10.10.0.38 Service Type SSH LINUX Number Of Days From Last Access 832 Service Logged in Time 27 Sep 2019 13:16:39								
2	DEBOARDING	ADMINISTRATOR	ADMINISTRATOR	ARCON\ADMINISTRATOR	ATSTEST	Client	ATSTEST	administrator
3	DEBOARDING				ARCON007	Client	192.168.0.239	Administrator
4	DEBOARDING				10.10.1.189	Client	10.10.1.189	kaiser
5	DEBOARDING				10.10.1.72	Client	10.10.1.72	kaiser

Showing 1 to 5 of 631 entries

Previous **1** 2 3 4 5 ... 127 Next


A Privileged Account Management Solution Copyright © 2022 ARCON. All Rights Reserved.

The following columns can be seen in this report:

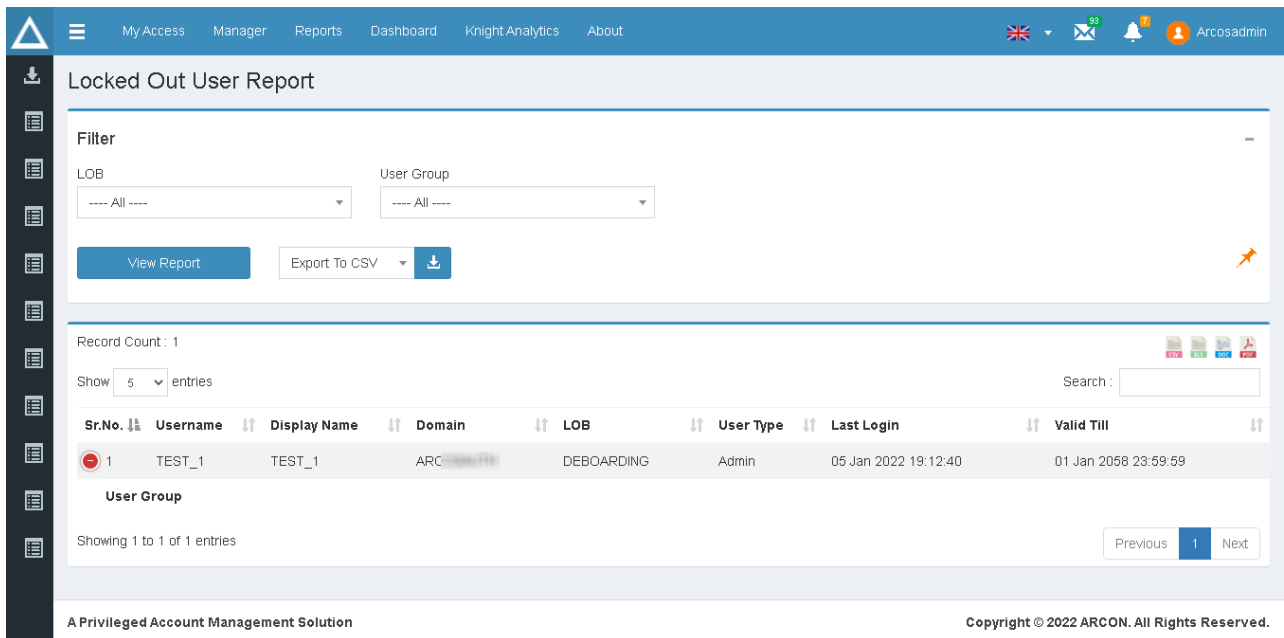
Column Names	Description
Sr. No.	To identify and distinguish rows
User Display Name	The display name of the user
Username	The name of the user
Domain	The domain name in which the user belongs
User Type	Type of user <ul style="list-style-type: none"> • Client • Admin
Service Logged In Time	Date/time of the last login to the service
Service Username	The username of the service
Service IP Address	The IP Address of the target server used last

12.9 Locked Out User Report

The Locked Out User Report displays users that attempted to log in with an invalid password and exceeded the lockout attempts value defined in Settings. Such users get their ID gets locked and added to the Lockout Users List under Manage Users. They are not able to log into ARCON | PAM even with the correct password.

 In order to view this report, users must have the following permission(s):

- **Locked Out User Report**



Locked Out User Report

Filter

LOB: User Group:

[View Report](#) [Export To CSV](#)

Record Count : 1

Show entries Search:

Sr.No.	Username	Display Name	Domain	LOB	User Type	Last Login	Valid Till
1	TEST_1	TEST_1	ARC.../...	DEBOARDING	Admin	05 Jan 2022 19:12:40	01 Jan 2058 23:59:59

User Group

Showing 1 to 1 of 1 entries [Previous](#) [1](#) [Next](#)

A Privileged Account Management Solution Copyright © 2022 ARCON. All Rights Reserved.

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Username	The name of the user
Display Name	The display name of the user
Domain	The name of the domain
LOB	The name of the LOB
User Type	Type of user <ul style="list-style-type: none"> • Admin • Client
Last Login	Date/time when the user last logged in
Valid Till	Date until which the user will be active

12.10 User & Service Mapping Report

The User & Service Mapping Report displays information about users and services that are mapped to the user and service groups, LOB-wise.



In order to view this report, users must have the following permission(s):

- **User & Service Mapping Report**

My Access Manager Reports Dashboard Knight Analytics About

 Arcosadmin

User & Service Mapping Report

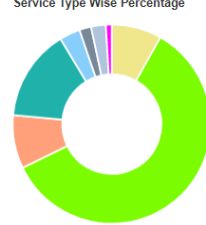
Filter

LOB: User Group: User ID: Service / Server IP:

[View Report](#) [Export To CSV](#)

Chart

Service Type Wise Percentage



Record Count : 208

Show entries Search:

Sr.No.	User ID	Display Name	User Group	Service Type	IP Address	Host Name	Service User Name	DB Instance	Service Assigned By	Service Assigned on
1	USER9999		Application Server	SSH LINUX	10.10.0.38	10.10.0.38	timebased		ARCOSADMIN	18 Sep 2019 19:03:34
Request Type Permanent										
Config. Command Restriction Type										
Service Group ARCON Servers										
2	USER9999		Application Server	SSH LINUX	10.10.0.38	10.10.0.38	timebased		ARCOSADMIN	18 Sep 2019 19:03:34
3	USER9999		ARCON Servers	App ASE Client	10.10.0.38	10.10.0.382	SSHU41	ssd	ARCOSADMIN	09 May 2020 16:09:57
4	USER9999		ARCON Servers	App ASE Client	10.10.0.38	10.10.0.382	SSHU41	ssd	ARCOSADMIN	09 May 2020 16:09:57
5	USER9999		ARCON Servers	App ASE Client	10.10.0.38	10.10.0.382	SSHU41	ssd	ARCOSADMIN	09 May 2020 16:09:57

Showing 1 to 5 of 208 entries
[Previous](#)
[1](#)
[2](#)
[3](#)
[4](#)
[5](#)
[...](#)
[42](#)
[Next](#)

A Privileged Account Management Solution
Copyright © 2022 ARCON. All Rights Reserved.


The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
User ID	The User ID associated with the user
Display Name	The display name of the user
User Group	The name of the user group to which the user belongs

Column Names	Description
Service Type	The name of service type
IP Address	The IP address of the target server
Host Name	The hostname of the target server
Service Username	The username of the service
DB Instance	Instance of the target server
Service Assigned on	Date/time of assignment of the service to the user
Request Type	Type of access <ul style="list-style-type: none"> • Permanent • Time-based • One-time
Config Command Restriction Type	The restricted command for that target server
Service Group	The name of the service group to which the server belongs

12.11 User Biometric Auth Report

User Biometric Auth Report displays information of all the users and the status (enabled, configured, not configured, etc) of biometric dual-factor authentication to make the ACMO login process more secure.

 In order to view this report, users must have the following permission(s):

- **User Biometric Auth Report**

User Biometric Auth Report

Filter

LOB: All, User ID: []

View Report | Export To CSV

Chart

Configuration Status Wise Percentage

- Not Configured Yet : 10291
- Enabled but Mob. No. is blank : 34
- Not Enabled and Mob. No. is blank : 19

Record Count : 10344

Show 5 entries | Search: []

Sr.No.	User ID	Display Name	Email ID	Mobile No	Is Configured	Configured By
1	USER6008				Not Configured Yet	
Configured On						
2	USER3737				Not Configured Yet	
3	USER2861				Not Configured Yet	
4	USER9722				Not Configured Yet	
5	USER2772				Not Configured Yet	

Showing 1 to 5 of 10,344 entries | Previous 1 2 3 4 5 ... 2069 Next

A Privileged Account Management Solution | Copyright © 2022 ARCON. All Rights Reserved.


The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
User ID	The User ID associated with the user
Display Name	The display name of the user
Email ID	The email ID of the user as configured by the Administrator
Mobile No	The mobile number of the user as configured by the Administrator

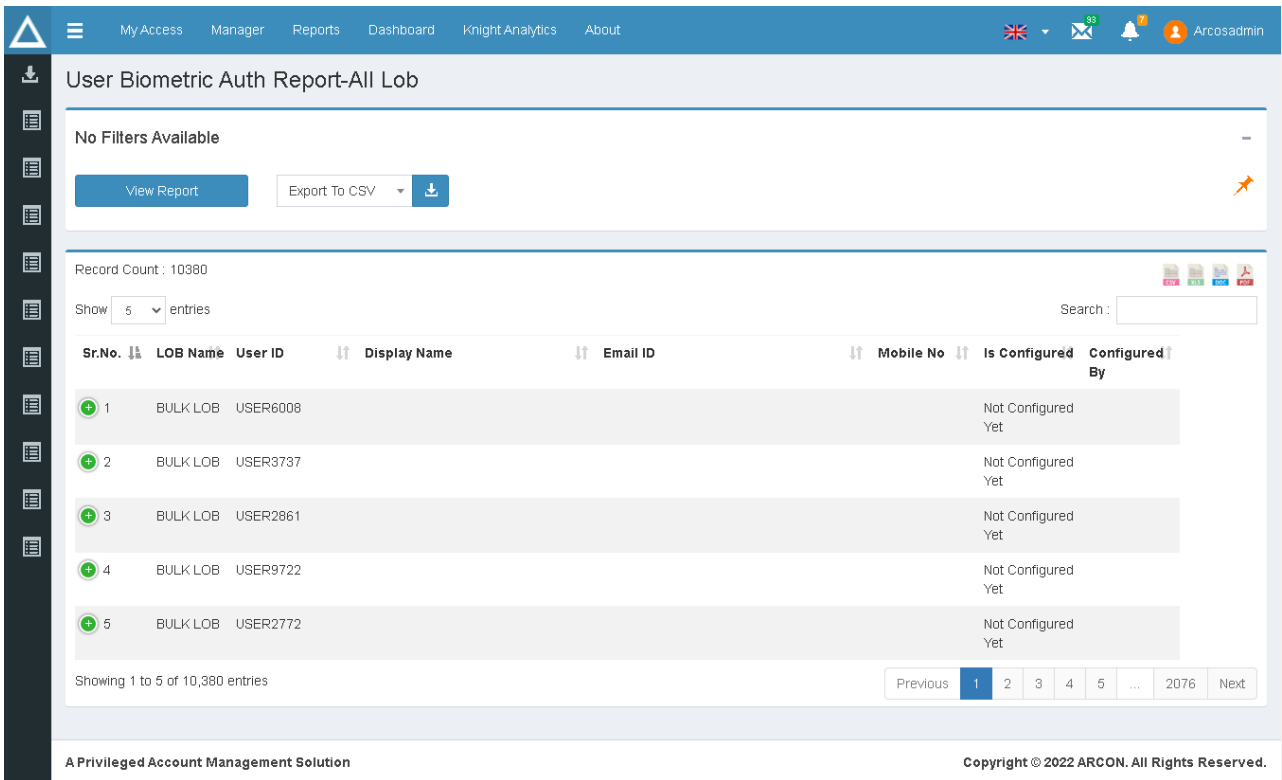
Column Names	Description
Is Configured	Status of configuration <ul style="list-style-type: none"> • Not configured yet • Configured but not enabled • Configured and enabled
Configured By	Name of the user who configured the 2FA biometric
Configured On	Date/time when biometric 2FA was configured

12.12 User Biometric Auth Report - All LOB

User Biometric Auth Report - ALL LOB displays reports for the users who have configured the biometric authorization to make the login process more secure across all LOBs.

 In order to view this report, users must have the following permission(s):

- **User Biometric Auth Report - All LOB**




The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows

Column Names	Description
LOB Name	Name of the LOB
User ID	The User ID associated with the user
Display Name	The display name of the user
Email ID	The email ID of the user as configured by the Administrator
Mobile No	The mobile number of the user as configured by Administrator
Is Configured	Status of configuration <ul style="list-style-type: none"> • Not configured yet • Configured but not enabled • Configured and enabled
Configured By	Name of the user who configured the 2FA biometric
Configured On	Date/time when biometric 2FA was configured

12.13 User Compliance Report

The User Compliance Report shows the user's status (Active/Inactive) and whether or not multi-factor authentication has been activated.

 In order to view this report, users must have the following permission(s):

- **User Compliance Report**

The screenshot displays the 'User Compliance Report' page. At the top, there are navigation tabs: My Access, Manager, Reports, Dashboard, Knight Analytics, and About. The user is logged in as 'Arcosadmin'. The report title is 'User Compliance Report'. Below the title, it states 'No Filters Available'. There are buttons for 'View Report' and 'Export To CSV'. The record count is 10354. The table shows 5 entries with the following data:

Sr.No.	User ID	Display Name	User Status	MFA Status	Last Logon
1	USER6008		Active	Disabled	16 Sep 2021 12:36:25
Duplicate Access to Multiple User Group Yes					
2	USER3737		Active	Disabled	16 Sep 2021 12:36:25
3	USER2861		Active	Disabled	16 Sep 2021 12:36:25
4	USER9722		Active	Disabled	16 Sep 2021 12:36:25
5	USER2772		Active	Disabled	16 Sep 2021 12:36:25


Showing 1 to 5 of 10,354 entries. The footer includes 'A Privileged Account Management Solution' and 'Copyright © 2022 ARCON. All Rights Reserved.'

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
User ID	The User ID associated with the user
Display Name	The display name of the user
User Status	Status of the user <ul style="list-style-type: none"> Active Inactive
MFA Status	Status of multi-factor authentication <ul style="list-style-type: none"> Enabled Disabled
Last Logon	Date/time when the user last logged in
Duplicate access to multiple user group	Whether the user has duplicate access to multiple user groups or not

12.14 User Creation Deletion Summary Report

The User Creation Deletion Summary Report gives the total cumulative count of users created and deleted date-wise until a particular date.

 In order to view this report, users must have the following permission(s):

• **User Creation Deletion Summary Report**

The screenshot displays the 'User Creation Deletion Summary Report' interface. At the top, there are navigation tabs: My Access, Manager, Reports, Dashboard, Knight Analytics, and About. The user is logged in as 'Arcosadmin'. The report title is 'User Creation Deletion Summary Report'. Below the title, there is a section for filters, currently showing 'No Filters Available'. There are buttons for 'View Report' and 'Export To CSV'. The record count is 44083. The table shows the following data:

Sr.No.	Date	Created	Deleted	Total
1	10/04/2017 18:39:41	1	0	1
2	01/01/2018 23:59:59	1	1	
3	04/03/2018 12:51:00	2	1	
4	04/03/2018 14:40:25	3	1	
5	04/03/2018 14:40:25	4	1	


The interface also includes a search bar, pagination controls (Previous, 1, 2, 3, 4, 5, ..., 8817, Next), and a footer with the text 'A Privileged Account Management Solution' and 'Copyright © 2022 ARCON. All Rights Reserved.'

The following columns can be seen in this report:

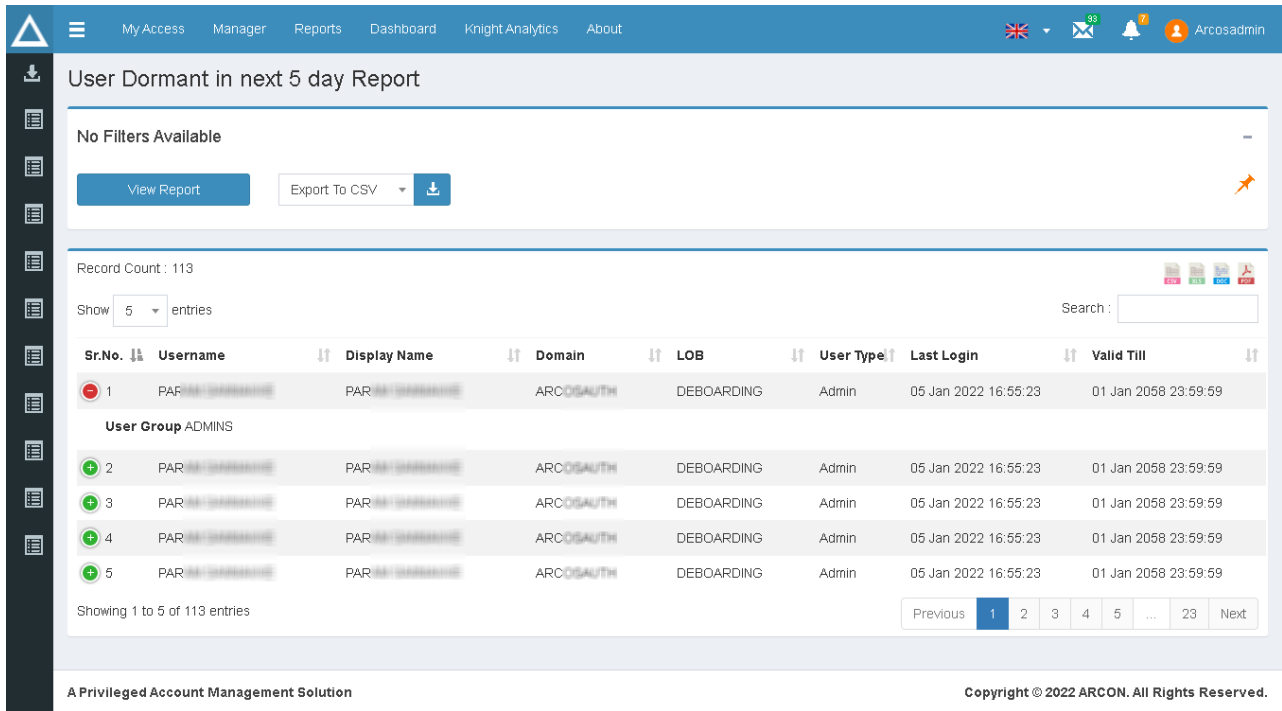
Column Names	Description
Sr. No.	To identify and distinguish rows
Date	Date/time of user creation
Created servers	The total number of users created on that day
Deleted Servers	The total number of users deleted on that day
Total	The total number of users created and deleted till that particular date

12.15 User Dormant in next 5 day Report

The User Dormant in next 5 day Report displays users whose accounts are about to go dormant in the next five days. Dormancy days are configured in Application Configuration under Settings.

 In order to view this report, users must have the following permission(s):

- **User Dormant in next 5 day Report**



User Dormant in next 5 day Report

No Filters Available

View Report Export To CSV

Record Count : 113

Show 5 entries Search :

Sr.No.	Username	Display Name	Domain	LOB	User Type	Last Login	Valid Till
1	PAR...	PAR...	ARCOSAUTH	DEBOARDING	Admin	05 Jan 2022 16:55:23	01 Jan 2058 23:59:59
User Group ADMINS							
2	PAR...	PAR...	ARCOSAUTH	DEBOARDING	Admin	05 Jan 2022 16:55:23	01 Jan 2058 23:59:59
3	PAR...	PAR...	ARCOSAUTH	DEBOARDING	Admin	05 Jan 2022 16:55:23	01 Jan 2058 23:59:59
4	PAR...	PAR...	ARCOSAUTH	DEBOARDING	Admin	05 Jan 2022 16:55:23	01 Jan 2058 23:59:59
5	PAR...	PAR...	ARCOSAUTH	DEBOARDING	Admin	05 Jan 2022 16:55:23	01 Jan 2058 23:59:59

Showing 1 to 5 of 113 entries

Previous 1 2 3 4 5 ... 23 Next


A Privileged Account Management Solution Copyright © 2022 ARCON. All Rights Reserved.

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Username	The name of the user
Display Name	The display name of the user
Domain	The domain name to which the user belongs
LOB	The name of the LOB in which the user is present
User Type	Type of user <ul style="list-style-type: none"> • Client • Admin
Last Login	Date/time when the user last logged in
Valid Till	Date until which the user will be active





12.16 User Hardware Auth Report

User Hardware Auth Report displays information of all the users and the status (enabled, configured, not configured, etc.) of the user hardware tool as dual-factor authentication to make the ACMO login process more secure.

 In order to view this report, users must have the following permission(s):

- **User Hardware Auth Report**


My Access Manager Reports Dashboard Knight Analytics About




 Arcosadmin

User Hardware Auth Report

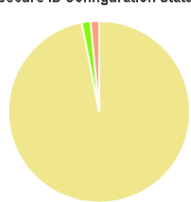
Filter

LOB: User ID:

View Report Export To CSV 

Chart

Secure ID Configuration Status



■ Not Configured Yet : 315
■ Enabled but Mob. No. is blank : 5
■ Not Enabled and Mob. No. is blank : 5

Record Count : 325

Show entries Search:

Sr.No.	User ID	Display Name	Email ID	Mobile No	Is Configured	Configured By
1	AARAV_ADM	AARAV_ADM			Not Configured Yet	
Configured On						
2	MAHESHWAR_M	MAHESHWAR M			Not Configured Yet	
3	TEJAL	TEJAL			Not Configured Yet	
4	USER9999				Not Configured Yet	
5	25JAN2020	25JAN2020			Not Configured Yet	

Showing 1 to 5 of 325 entries

Previous 1 2 3 4 5 ... 65 Next

A Privileged Account Management Solution
Copyright © 2022 ARCON. All Rights Reserved.


The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
User ID	The user ID associated with the user
Display Name	The display name of the user
Email ID	The email ID of the user as configured by the Administrator

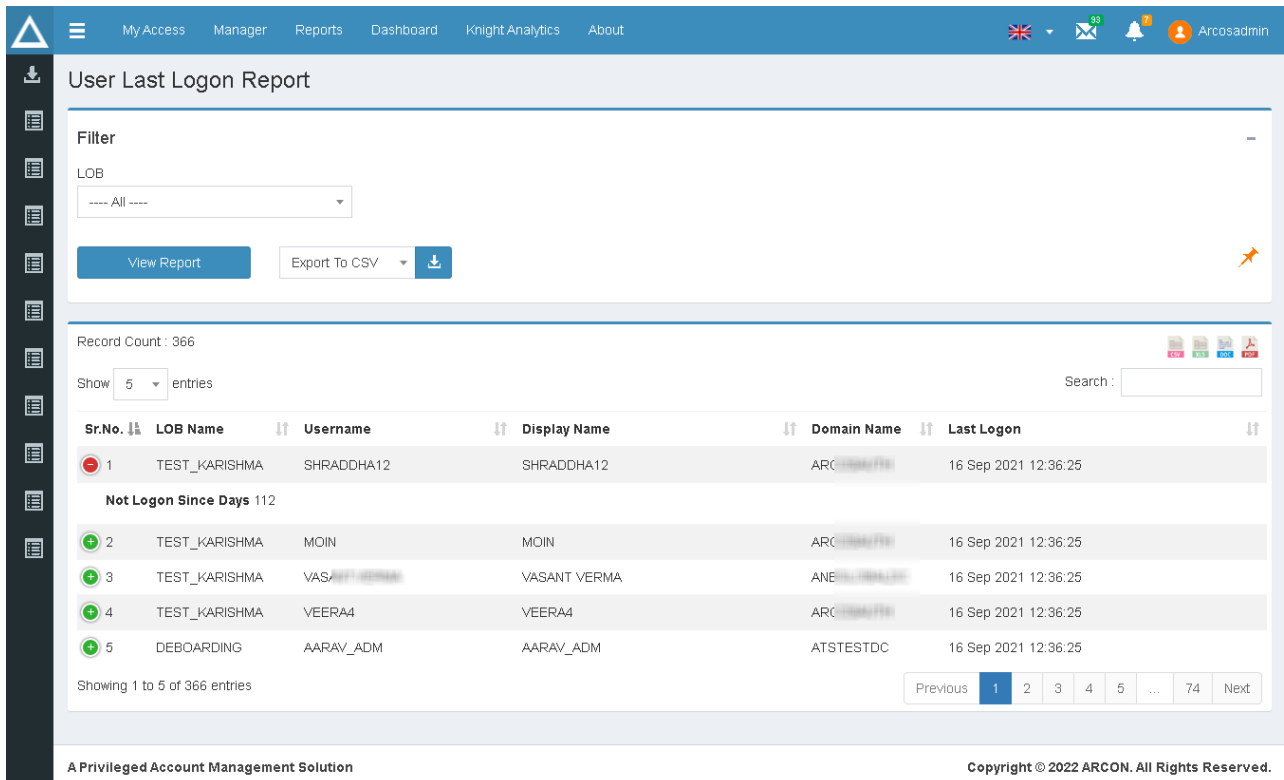
Column Names	Description
Is configured	Status of configuration <ul style="list-style-type: none"> • Not configured yet • Configured but not enabled • Configured
Mobile No	Mobile number of the user as configured by the Administrator
Configured By	The name of the Administrator who configured this authentication
Configured On	Date/time when the user hardware authentication was configured

12.17 User Last Logon Report

The User Last Logon Report displays when a user last logged into the ARCON | PAM application.

 In order to view this report, users must have the following permission(s):

- **User Last Logon Report**



Record Count : 366

Show 5 entries

Sr.No.	LOB Name	Username	Display Name	Domain Name	Last Logon
1	TEST_KARISHMA	SHRADDHA12	SHRADDHA12	ARCOSMART	16 Sep 2021 12:36:25
Not Logon Since Days 112					
2	TEST_KARISHMA	MOIN	MOIN	ARCOSMART	16 Sep 2021 12:36:25
3	TEST_KARISHMA	VASANT VERMA	VASANT VERMA	ARCOSMART	16 Sep 2021 12:36:25
4	TEST_KARISHMA	VEERA4	VEERA4	ARCOSMART	16 Sep 2021 12:36:25
5	DEBOARDING	AARAV_ADM	AARAV_ADM	ATSTESTDC	16 Sep 2021 12:36:25

Showing 1 to 5 of 366 entries

Previous 1 2 3 4 5 ... 74 Next

administrative user

Column Names	Description
Sr. No.	To identify and distinguish rows
LOB Name	The name of the LOB
Username	The name of the user
Display Name	The display name of the user
Domain	The domain name to which the user belongs
Last Logon	Date/time of the last login by that user into the application
Not logon Since Days	Number of days passed since the last login

12.18 User Mobile OTP Auth Report

The User Mobile OTP Auth Report displays information of all the users and the status (enabled, configured, not configured, etc.) of Mobile OTP as dual-factor authentication to make the ACMO login process more secure.

📄 In order to view this report, users must have the following permission(s)

- **User Mobile OTP Auth Report**


The following columns are available in this report:

Column Names	Description
Sr No.	To identify and distinguish rows
User ID	The user ID associated with the user
Display Name	The display name of the user
Email ID	The email ID of the user as configured by the Administrator
Is Configured	Status of configuration <ul style="list-style-type: none"> • Not configured yet • Configured but not enabled • Configured and enabled

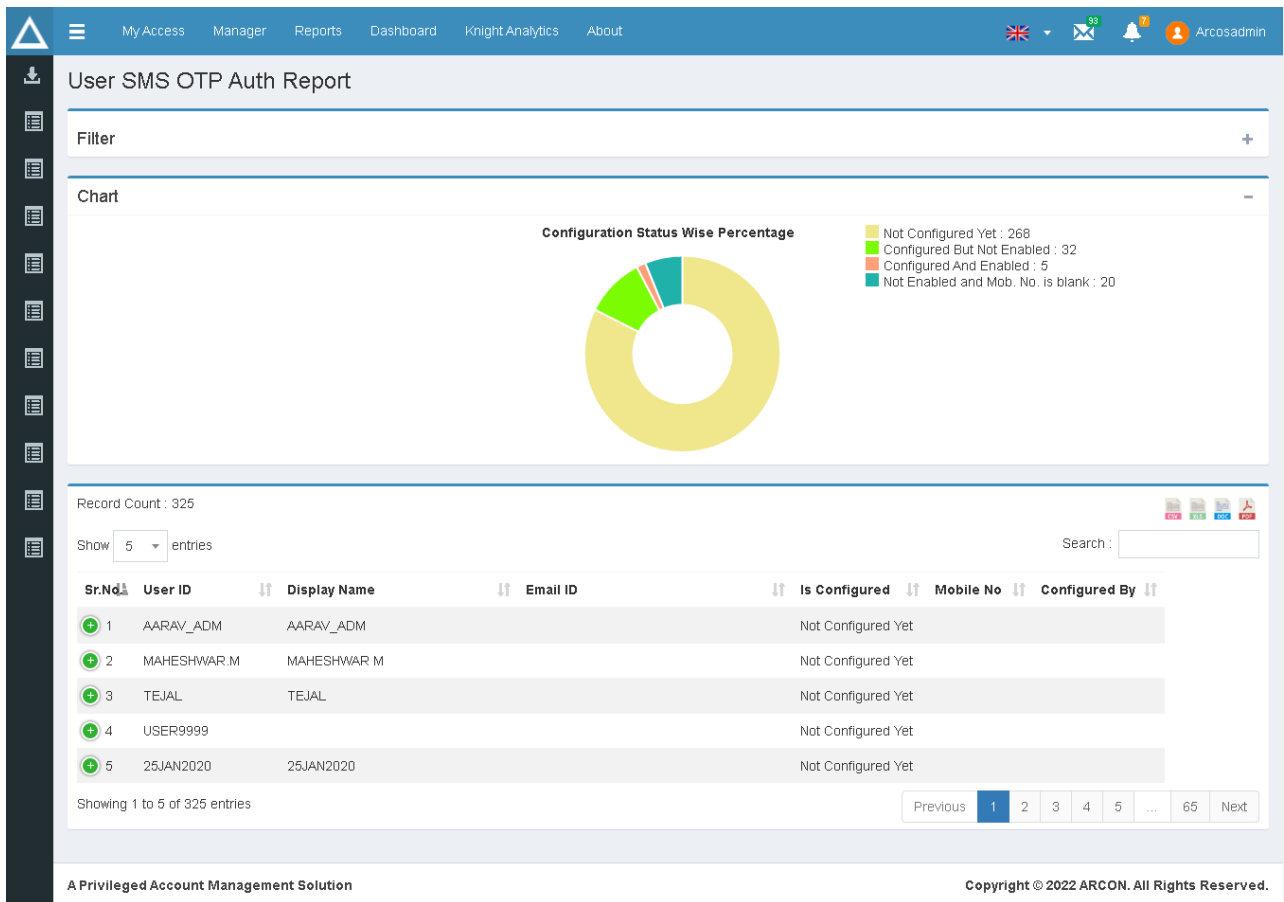
Column Names	Description
Mobile No	Mobile number of the user as configured by the Administrator
Configured By	Name of the user who configured the Mobile OTP 2FA
Configured On	Date/time when mobile OTP was configured

12.19 User SMS OTP Auth Report

User SMS OTP Auth Report displays information of all the users and the status (enabled, configured, not configured, etc) of SMS OTP as dual-factor authentication to make the ACMO login process more secure.

 In order to view this report, users must have the following permission(s):

- User SMS OTP Auth Report**



Configuration Status Wise Percentage

- Not Configured Yet : 268
- Configured But Not Enabled : 32
- Configured And Enabled : 5
- Not Enabled and Mob. No. is blank : 20

Sr.No.	User ID	Display Name	Email ID	Is Configured	Mobile No	Configured By
1	AARAV_ADM	AARAV_ADM		Not Configured Yet		
2	MAHESHWAR.M	MAHESHWAR.M		Not Configured Yet		
3	TEJAL	TEJAL		Not Configured Yet		
4	USER9999			Not Configured Yet		
5	25JAN2020	25JAN2020		Not Configured Yet		


The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows

Column Names	Description
User ID	The user ID associated with the user
Display Name	The display name of the user
Email ID	The email ID of the user as configured by the administrative user
Is Configured	Status of configuration <ul style="list-style-type: none"> • Not configured yet • Configured but not enabled • Configured and enabled
Mobile No	Mobile number of the user as configured by the Administrator
Configured By	Name of the user who configured the SMS OTP 2FA
Configured On	Date/time when SMS OTP was configured

12.20 User Status Report

The User Status Report displays a history of a user's status, such as when they were dormant, locked out, or disabled, and when they became active again.

 In order to view this report, users must have the following permission(s):

- **User Status Report**

User Status Report

Filter

LOB: All | Date From: 07-12-2021 00:00 | Date To: 06-01-2022 15:11 | User Group: All

User ID:

[View Report](#) | [Export To CSV](#)

Record Count : 54

Show 5 entries | Search:

Sr.No.	Username	User ID	Date	From Status	To Status	No of Times to	LOB Name
1	SHABBIR JAWADWALA	SHABBIRSCIM_TEST2	05 Jan 2022 22:20:32	Active	Active	Active : 1	DEFAULT LOB 2
User Group LINUXADMINS							
2	DFG	DFG	05 Jan 2022 23:32:00	Disabled	Active	Active : 2	DEFAULT LOB 2
3	TEST_1	TEST_1	05 Jan 2022 21:53:14	Active	Lock	Lock : 1	DEBOARDING
4	VEER1DEMO3431234156111212341	VEER1DEMO34312341561	06 Jan 2022 15:12:19	Active	Active	Active : 1	DEFAULT LOB 2
5	VEER1DEMO3431234156	VEER1DEMO3431234156	06 Jan 2022 15:12:19	Active	Active	Active : 1	DEFAULT LOB 2

Showing 1 to 5 of 54 entries | [Previous](#) | 1 | 2 | 3 | 4 | 5 | ... | 11 | [Next](#)

A Privileged Account Management Solution | Copyright © 2022 ARCON. All Rights Reserved.

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
User Name	The name of the user
Date	Date/time of user status
From Status	Previous status of the user
To Status	The final status of the user
Number of Times to	Number of times the status of the user changed
LOB	The name of the LOB
User Group	The name of the user group to which the user belongs

13 Vault Reports

The vault is the secure storage space for all the passwords in ARCON | PAM, where the users' and services passwords are saved. Vault reports generate details of all the password activities performed in ARCON | PAM.

The following reports are available in Vault Reports:

- Allow Password Change Report
- Current Password Status Report
- Maximum Password Failed Attempts
- Restore Service Password Option Used
- Service Last Password Failed Reason
- Service Password Age Report
- Service password Change Consolidated Report
- Service Password Change Failed (Server Unavailable) Report
- Service Password Changed Status Report
- Service Password Changed Status Report - All LOB
- Service Password Changed Success/Failed Report
- Service Password Check Out Report
- Service Password Envelope Print Status Report
- Service Password Expires in 5 Days Report
- Service Password Manually Changed Report
- Service Password Never Changed Report
- Service Password Never Changed Report - All LOB
- Service Password Security Status
- Service Password Vaulting Status
- Service Password Vaulting Summary Report
- Service Password Viewed By Administrator
- Service Reached Maximum Failed Attempts
- Service Reconcile Status Report
- Services Details for SPC - Maximum Failed Attempts
- Services Scheduled for SPC
- SPC Not Configured Report
- SPC Success and Failed Report
- Users Extracting Password Envelope

13.1 Allow Password Change Report

The Allow Password Change Report displays information of the services for which password change is allowed.



In order to view this report, users must have the following permission(s):

- **Allow Password Change Report**

Record Count : 489

Show 5 entries

Sr.No.	IP Address	Host Name	Username	DB Instance	Service Type	Group Name	Min Password Age	Max Password Age	Current Password Age	Last Password Changed On	PasswordExpiredOn
1	3.6.49.70	I-09B0215568CECB707			EC2 access using AWS SSM	WINDOWS SERVERS	0	60	236	May 20 2021 1:02:11	Jul 19 2021 1:02:11
2	3.6.49.70	I-004C0C0F311C9B23F			EC2 access using AWS SSM	WINDOWS SERVERS	0	60	236	May 20 2021 1:04:37	Jul 19 2021 1:04:37
3	6.6.6.6	6.6.6.6	rohit		Windows RDP	WINDOWS SERVERS	0	6	70	Nov 2 2021 4:27:23	Nov 8 2021 4:27:23
4	3.83.211.28	3.83.211.28	Deven		Windows RDP	WINDOWS SERVERS	0	100	1	Jan 10 2022 6:12:18	Apr 20 2022 6:12:18
5	10.10.5.401	10.10.5.401	preeti		SSH LINUX	WINDOWS SERVERS	0	1	868	Aug 27 2019 3:16:46	Aug 28 2019 3:16:46

Showing 1 to 5 of 489 entries

Previous 1 2 3 4 5 ... 98 Next

A Privileged Account Management Solution Copyright © 2022 ARCON. All Rights Reserved.


The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
IP Address	The IP Address of the target server
Host Name	The hostname of the target server
Username	The name of the user
DB Instances	The instance of the target server
Service Type	Name of the service type
Group Name	Name of the server group to which the server belongs
Min. Password Age	Minimum age set for the password to be valid
Max. Password Age	Maximum age set for the password to be valid
Current Password Age	The current age of the password set
Last Password Changed On	The last date when the password was changed

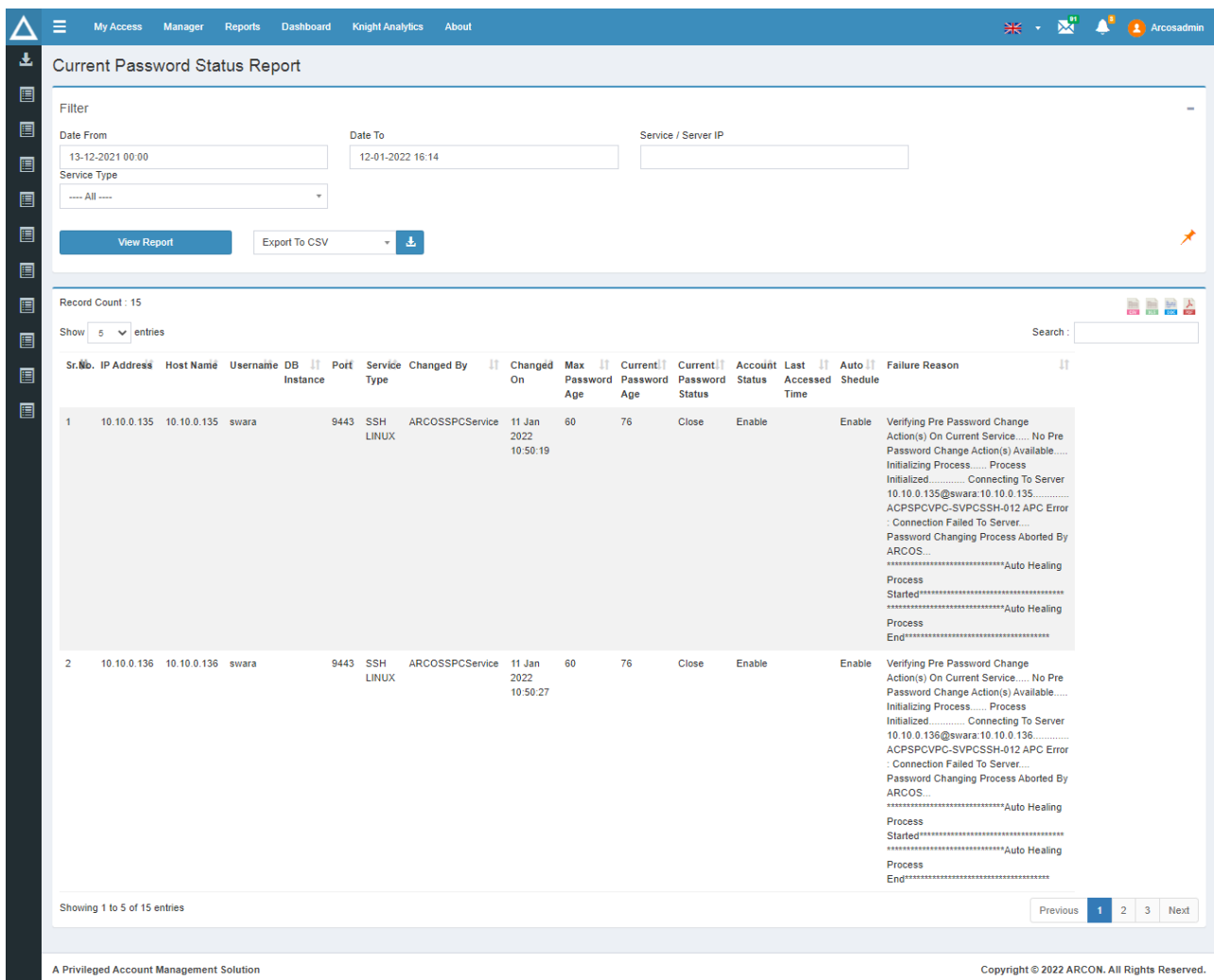
Column Names	Description
Password Expired On	The date for when the password expires

13.2 Current Password Status Report

The Current Password Status Report displays the current password status (open/closed) of all services.

 In order to view this report, users must have the following permission(s):

- **Current Password Status Report**




The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
IP Address	The IP address of the target server

Column Names	Description
Host Name	The hostname of the target server
User Name	The name of the user
DB Instance	Displays instance of the target servers
Port	Displays port connecting to the target server
Service type	Name of the service type
Changed By	Name of the Administrator who changed the password
Changed On	Date/time of password change
Max Password Age	Maximum age of password after which the password changes
Current Password age	The present age of the password
Current Password Status	Status of password <ul style="list-style-type: none"> • Open • Closed
Account Status	Status of the service account <ul style="list-style-type: none"> • Enabled • Disabled
Last Accessed Time	Date/time when the service was last used
Auto Schedule	If password change will happen automatically <ul style="list-style-type: none"> • Enabled • Disabled
Failure Reason	Steps captured during the password change

13.3 Maximum Password Failed Attempts Report

The Maximum Password Failed Attempts Report displays all the services for which the scheduled password change has been terminated due to exceeding the maximum number of failed attempts. The maximum number of failed attempts is specified in the **Scheduled Password Change - Maximum Failed Attempt** in Settings.

 In order to view this report, users must have the following permission(s):


- **Maximum Password Failed Attempts Report**

The following columns can be seen in this report:

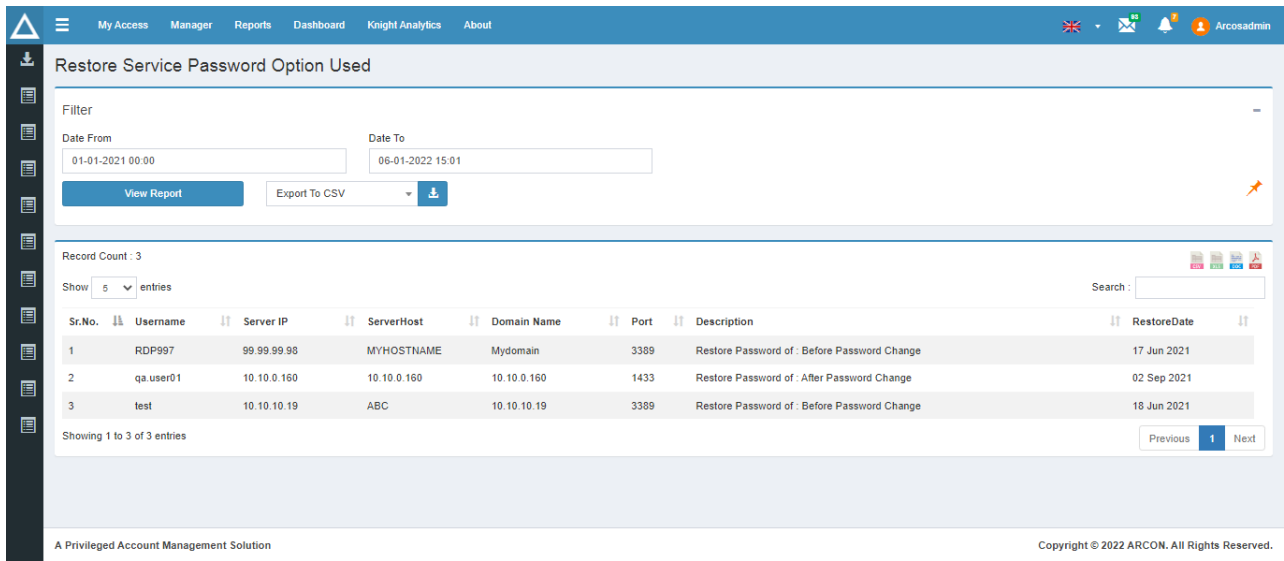
Column Names	Description
Sr. No.	To identify and distinguish rows
Count	Number of times the password change failed
Service ID	The ID associated with the target server
IP Address	The IP address of the target server
Host Name	The hostname of the target server
Domain name	The domain name of the target server
User Name	The name of the user
DB Instance	Instance of the target server
Service type	Name of the service type
Service Group	Name of the service group to which the server belongs
Last Password Changed By	Name of the user who changed the password last

13.4 Restore Service Password Option Used

The Restore Service Password Option Used report displays the list of users who used the Restore Service Password option.

 In order to view this report, users must have the following permission(s):

- **Restore Service Password Option Used**




The following columns can be seen in this report:

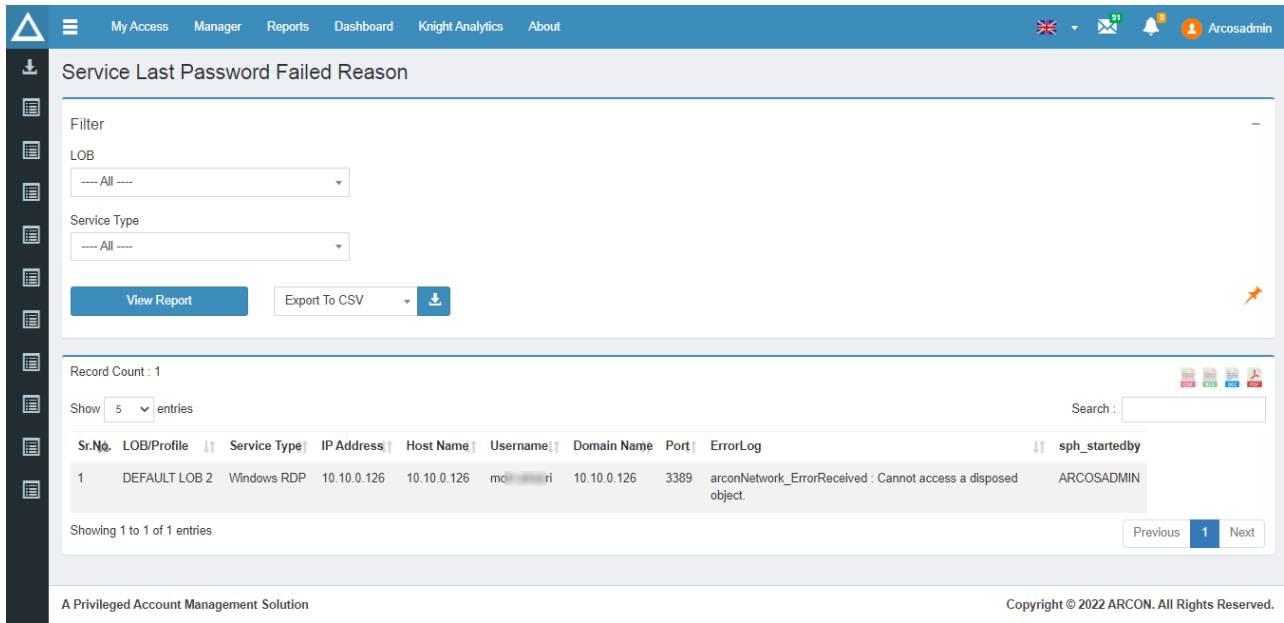
Column Names	Description
Sr. No.	To identify and distinguish rows
User Name	The name of the user
Server IP	The IP address of the target server
Server Host	The hostname of the target server
Domain name	The domain name of the target server
Port	Port of the target server
Description	Step at which restore service password was used
Restore Date	Date/time at which the service was restored

13.5 Service Last Password Failed Reason

The Service Last Password Failed Reason report displays the reason for the failure of the password change for each service type.

 In order to view this report, users must have the following permission(s):

- **Service Last Password Failed Reason Report**




The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
LOB/Profile	The name of the LOB to which the service belongs
Service Type	Name of the service type
IP Address	The IP address of the target server
Host Name	The hostname of the target server
User Name	The name of the user
Domain Name	The domain name of the target server
Port	Port of the target server
Error Log	Steps captured of why the password change failed
SPH Started By	Name of the Administrator who started SPH

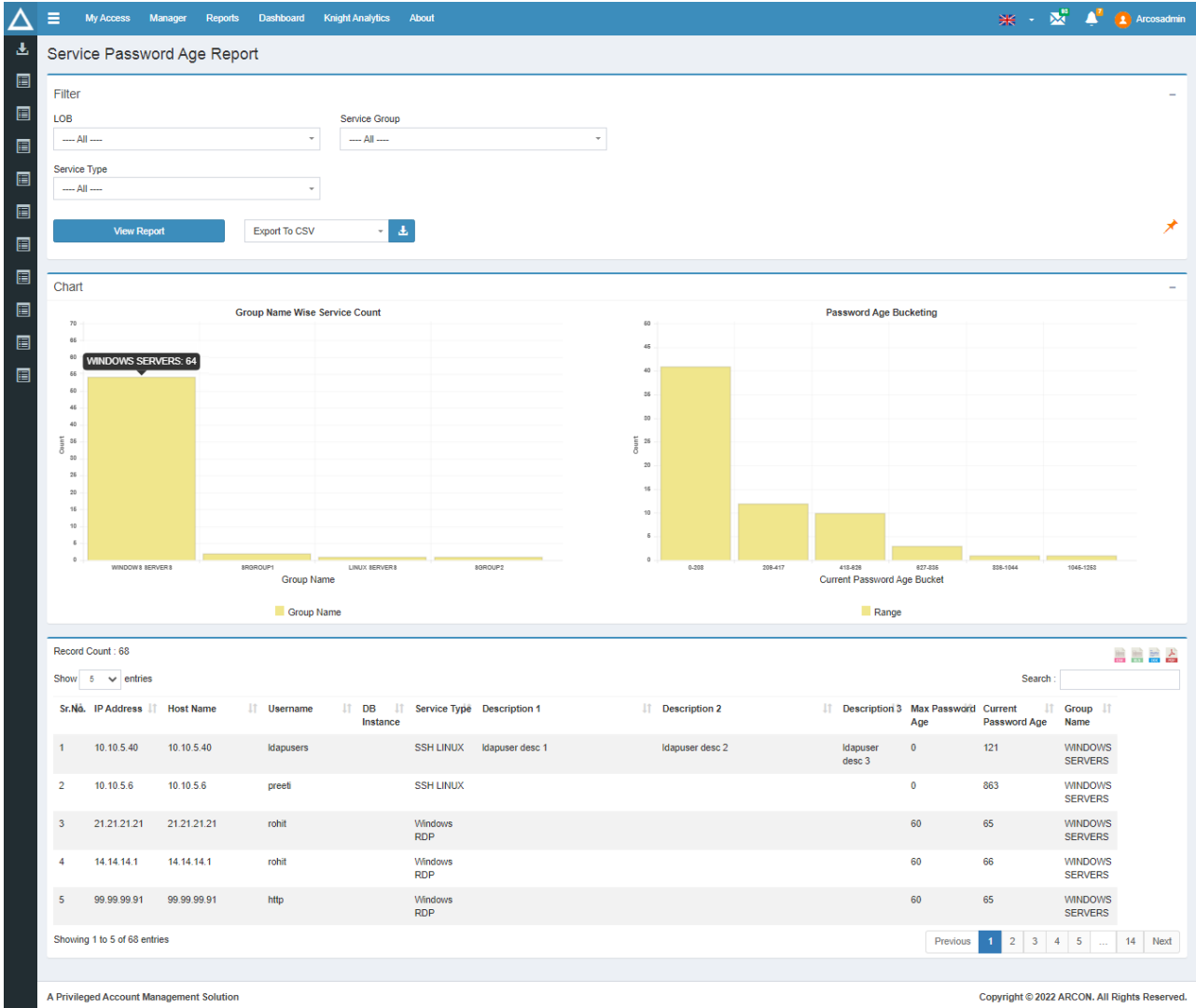
13.6 Service Password Age Report

The Service Password Age Report displays the password's age for each service, which is the number of days the password has been active in ARCON | PAM, in graphical and grid view format. In addition, the bar graphs displays:

- Group name-wise service count
- Password age bucketing

 In order to view this report, users must have the following permission(s):

- **Service Password Age Report**



The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
IP Address	The IP address of the target server
Host Name	The hostname of the target server
User Name	The name of the user
DB Instance	The instance of the target server

Column Names	Description
Service Type	Name of the service type
Description 1	Text entered during the creation of the service
Description 2	Text entered during the creation of the service
Description 3	Text entered during the creation of the service
Max Password Age	Maximum age of password - after this the password changes
Current Password Age	Age of the current password
Group Name	Name of the group to which the server belongs

13.7 Service Password Change Consolidated Report

Service Password Change Consolidated Report displays the consolidated information of the password changed for the different services.

📄 In order to view this report, users must have the following permission

- **Service Password Change Consolidated Report**

Service Password Change Consolidated Report

No Filters Available

View Report | Export To CSV

Record Count : 233

Show 5 entries

Sr.No	IP Address	Host Name	Password Changed By	Status	Failure Reason	Password Change Attempt	Last Successful Password Change
1	3.83.211.28	3.83.211.28	ARCOSADMIN	Success		10 Jan 2022 18:12:13	10 Jan 2022 18:12:18
2	10.10.5.401	10.10.5.401	ARCONAHService	Failed		21 Mar 2021 00:33:35	27 Aug 2019 15:16:46
3	10.10.5.40	10.10.5.40	ARCOSADMIN	Success		07 Sep 2021 22:15:35	07 Sep 2021 22:15:35
4	10.10.5.6	10.10.5.6	ARCONAHService	Failed		21 Mar 2021 00:33:22	27 Aug 2019 14:55:14
5	oracle-db-onboarding.chmzm59ucsur.us-east-1.rds.amazonaws.com	oracle-db-onboarding.chmzm59ucsur.us-east-1.rds.amazonaws.com	ARCOSADMIN	Failed	Verifying Pre Password Change Action(s) On Current Service..... No Pre Password Change Action(s) Available..... Initializing Process..... Process Initialized..... Connecting To Server oracle-db-onboarding.chmzm59ucsur.us-east-1.rds.amazonaws.com@TEST:ORACLE-DB-ONBOARDING.CHMZM59UCSUR.US-EAST-1.RDS.AMAZONAWS.COM (ORCL)..... DBA Privilege cannot be set to an invalid value of <basic><default><sid> Connection Failed To Server... SMCP-CORACLEP-054 Password Changing Process Aborted By ARCON PAM...	11 Jan 2022 00:27:03	03 Jan 2022 10:18:20

Showing 1 to 5 of 233 entries

Previous 1 2 3 4 5 ... 47 Next

A Privileged Account Management Solution | Copyright © 2022 ARCON. All Rights Reserved.


The following columns are available in the report:

Column Names	Description
Sr. No	To identify and distinguish rows
IP Address	The IP Address of the target server
Host Name	The hostname of the target servers
Password Changed By	The username of the user that changed the password
Status	The status of the password change, if it was a success or a failure
Failure Reason	The reason for which the password change failed for
Password Change Attempt	The date on which the password changed was attempted

Column Names	Description
Last Successful Password Change	The last date on which the password change was successful

13.8 Service Password Change Failed (Server Unavailable) Report

The Service Password Change Failed (Server Unavailable) Report displays all the services that have had their password changes fail due to server downtime.

 In order to view this report, users must have the following permission(s):

- **Service Password Change Failed (Server Unavailable) Report**

My Access
Manager
Reports
Dashboard
Knight Analytics
About

 33
 7
 Arcosadmin

Service Password Change Failed(Server Unavailable) Report

Filter

LOB

Date From

Date To

Service Group

Service Type

View Report
Export To CSV
↓

Chart

Service Type Count

Record Count : 12

Show entries

Search :

Sr.No.	IP Address	Host Name	Username	DB Instance	Description 1	Description 2	Description 3	Service Type	Changed By	Changed On
1	10.10.2.52	10.10.2.52	arcon					SSH Telnet	ARCOSADMIN	10 Nov 2021 14:50:32
<p>Current Status Close</p> <p>Error Description Verifying Pre Password Change Action(s) On Current Service..... No Pre Password Change Action(s) Available..... Initializing Process..... Process Initialized..... Connecting To Server 10.10.2.52@arcon:10.10.2.52..... Object reference not set to an instance of an object. Connection Failed To Server.... SMCP-CTNPCPCP-090 Password Changing Process Aborted By ARCON PAM...</p> <p>ErrorReason Connection Failed To Server. Object reference not set to an instance of an object.</p>										
2	127.0.0.1	127.0.0.1	vidhvattamah		MUMEINOKIAOSSNETACTOSS1110.10.0.69SSH			SSH LINUX	ARCOSADMIN	04 Jan 2022 15:54:21
3	127.0.0.1	127.0.0.1	vidhvattamah		MUMEINOKIAOSSNETACTOSS1110.10.0.69SSH			SSH LINUX	ARCOSADMIN	28 Nov 2021 23:38:35
4	10.10.0.101	10.10.0.101	ANBUser	o365		DA		App Web Browser	ARCOSADMIN	01 Oct 2021 16:19:00
5	10.10.0.300	10.10.0.300	shabbir_sshk					SSH LINUX	ARCOSADMIN	06 Jan 2022 13:48:11

Showing 1 to 5 of 12 entries

Previous 1 2 3 Next


A Privileged Account Management Solution
Copyright © 2022 ARCON. All Rights Reserved.

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
IP Address	The IP address of the target server
Host Name	The hostname of the target server
User Name	The name of the user
DB Instance	The instance of the target server
Description 1	Text entered during the creation of the service
Description 2	Text entered during the creation of the service
Description 3	Text entered during the creation of the service
Service Type	Name of the service type
Changed By	Name of the Administrator who changed the password
Changed On	Date/time at which the password was changed
Current Status	Present status of the password <ul style="list-style-type: none"> • Open • Closed
Error Description	Reason for password failure

13.9 Service Password Changed Status Report

The Service Password Changed Status Report displays services that have had their passwords successfully changed since they were created.

 In order to view this report, users must have the following permission(s):

- **Service Password Changed Status Report**

Service Password Changed Status Report

Filter

LOB: All | Service Group: All | Service Type: All

View Report | Export To CSV

Record Count : 65

Show 5 entries | Search :

Sr.No.	IP Address	Host Name	Domain Name	Username	DB Instance	Service Type	Last Successful Password Changed By	Last Successful Password Changed On	Last Successful Password Changed Through	No. of Successful Password Change	Current Status
1	1	HTTP://GMAIL.COM	HTTP://GMAIL.COM	test		App Web Browser	ARCOSADMIN	06 Oct 2021 15:55:37	Manually By User	3	Close
2	10.10.10.19	10.10.10.19	10.10.10.19	test123		Windows RDP	ARCOSADMIN	12 Apr 2021 07:54:54	Manually By User	2	Close
3	103.13.112.44	SPINE	HTTPS://HR.IN	jane		App Web Browser	ARCOSADMIN	08 Sep 2021 13:18:59	Manually By User	6	Close
4	10.10.1.27	DSK015		anbread		Windows RDP	ARCOSADMIN	21 Jun 2021 15:14:12	Manually By User	4	Open
5	10.10.1.244	10.10.1.244	10.10.1.244	root		SSH LINUX	ARCOSADMIN	09 Mar 2021 15:41:37	Manually By User	1	Close

Showing 1 to 5 of 65 entries | Previous 1 2 3 4 5 ... 13 Next

A Privileged Account Management Solution | Copyright © 2022 ARCON. All Rights Reserved.


The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
IP Address	The IP address of the target server
Host Name	The hostname of the target server
Domain Name	The domain name of the target server
User Name	The name of the user
DB Instance	The instance of the target server
Service Type	Name of the service type
Last Successful Password Changed By	Name of the Administrator who changed the last password successfully
Last Password Changed On	Date/time at which the last password was changed
Last Successful Password Changed Through	The method by which the last password was changed

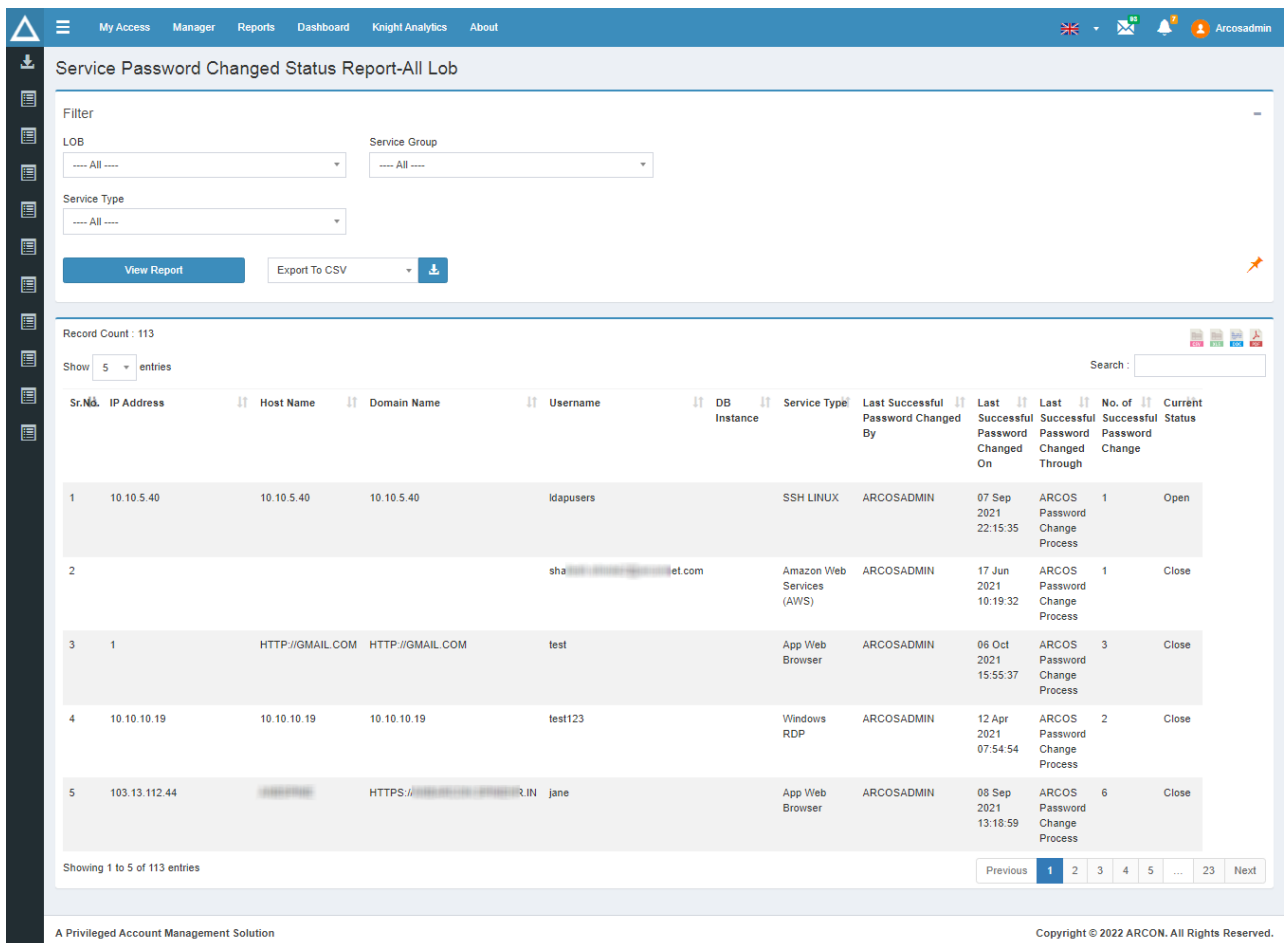
Column Names	Description
No. of Successful Password Changes	Total number of successful password changes
Current status	Present status of the password <ul style="list-style-type: none"> • Open • Closed

13.10 Service Password Changed Status Report - All LOB

The Service Password Changed Status Report - All LOB displays details of all the services whose passwords have been successfully changed since the service was created across all LOBs.

 In order to view this report, users must have the following permission(s):

- **Service Password Changed Status Report-All LOB**



Service Password Changed Status Report-All Lob

Filter

LOB: All | Service Group: All | Service Type: All

View Report | Export To CSV

Record Count : 113

Show 5 entries

Sr.No.	IP Address	Host Name	Domain Name	Username	DB Instance	Service Type	Last Successful Password Changed By	Last Successful Password Changed On	Last Successful Password Changed Through	No. of Successful Password Change	Current Status
1	10.10.5.40	10.10.5.40	10.10.5.40	ldapusers		SSH LINUX	ARCOSADMIN	07 Sep 2021 22:15:35	ARCOS Password Change Process	1	Open
2				sha...		Amazon Web Services (AWS)	ARCOSADMIN	17 Jun 2021 10:19:32	ARCOS Password Change Process	1	Close
3	1	HTTP://GMAIL.COM	HTTP://GMAIL.COM	test		App Web Browser	ARCOSADMIN	06 Oct 2021 15:55:37	ARCOS Password Change Process	3	Close
4	10.10.10.19	10.10.10.19	10.10.10.19	test123		Windows RDP	ARCOSADMIN	12 Apr 2021 07:54:54	ARCOS Password Change Process	2	Close
5	103.13.112.44		HTTPS://...	jane		App Web Browser	ARCOSADMIN	08 Sep 2021 13:18:59	ARCOS Password Change Process	6	Close

Showing 1 to 5 of 113 entries

Previous 1 2 3 4 5 ... 23 Next


A Privileged Account Management Solution | Copyright © 2022 ARCON. All Rights Reserved.

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
IP Address	The IP address of the target server
Host Name	The hostname of the target server
Domain Name	The domain name of the target server
Username	The name of the user
Last Successful Password Changed By	Name of the Administrator who changed the last password successfully
Last Successful Password Changed On	Date/time at which the last password was changed
Last Successful Password Changed Through	The method by which the last password was changed
No. of Successful Password Changes	Total number of successful password changes
Current Status	Present status of the password <ul style="list-style-type: none"> • Open • Closed

13.11 Service Password Changed Success/Failed Report

The Service Password Changed Success/Failed Report displays if the password change is successful or failed for all services.

 In order to view this report, users must have the following permission(s):

- **Service Password Changed Success Failed Report**


The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Service	Name of the service type
Host Name	The hostname of the target server
Service IP	The IP address of the target server
User Name	The name of the user
Domain Name	The domain name of the target server
Start Date	Date/time at which the password was changed
Status	Status of the password change <ul style="list-style-type: none"> • Success • Failed

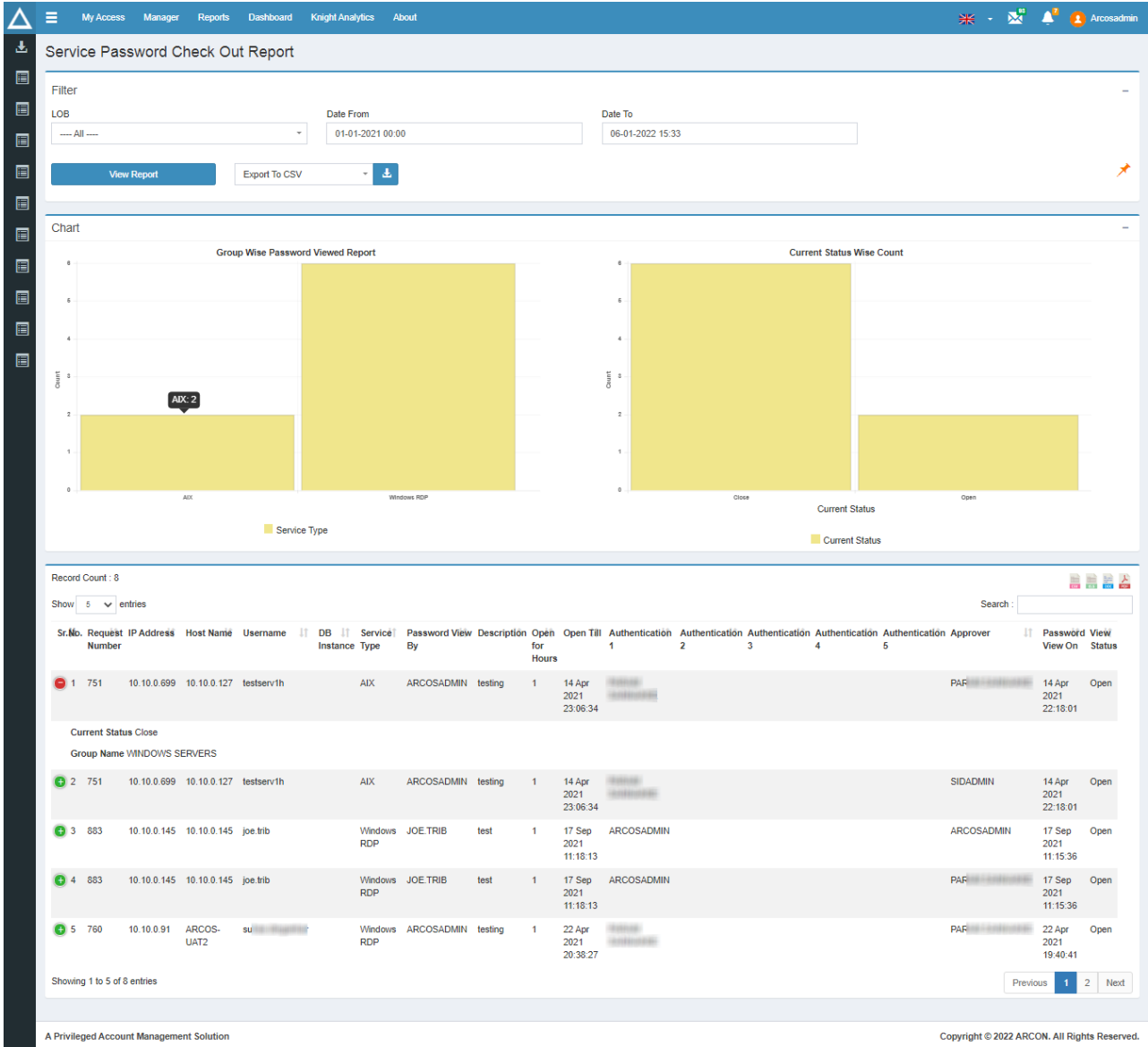
13.12 Service Password Check Out Report

The Service Password Check Out Report displays details of users who have requested to view the service password for a specified amount of time in graphical and grid view format. In addition, the bar graph displays:

- Group-wise Password Viewed Report
- Current Status-wise Count

 In order to view this report, users must have the following permission(s):

- **Service Password Check Out Report**



Service Password Check Out Report

Filter
 LOB: All | Date From: 01-01-2021 00:00 | Date To: 06-01-2022 15:33
 View Report | Export To CSV

Chart

Group Wise Password Viewed Report

Service Type	Count
AIX	2
Windows RDP	6

Current Status Wise Count

Current Status	Count
Close	6
Open	2

Record Count : 8
 Show 5 entries | Search: []

Sr.No.	Request Number	IP Address	Host Name	Username	DB Instance	Service Type	Password View By	Description	Open for Hours	Authentication 1	Authentication 2	Authentication 3	Authentication 4	Authentication 5	Approver	Password View On	View Status
1	751	10.10.0.699	10.10.0.127	testserv1h		AIX	ARCOSADMIN	testing	1	14 Apr 2021 23:06:34					PAR	14 Apr 2021 22:18:01	Open
Current Status Close																	
Group Name WINDOWS SERVERS																	
2	751	10.10.0.699	10.10.0.127	testserv1h		AIX	ARCOSADMIN	testing	1	14 Apr 2021 23:06:34					SIDADMIN	14 Apr 2021 22:18:01	Open
3	883	10.10.0.145	10.10.0.145	joe.trib		Windows RDP	JOE.TRIB	test	1	17 Sep 2021 11:18:13	ARCOSADMIN				ARCOSADMIN	17 Sep 2021 11:15:36	Open
4	883	10.10.0.145	10.10.0.145	joe.trib		Windows RDP	JOE.TRIB	test	1	17 Sep 2021 11:18:13	ARCOSADMIN				PAR	17 Sep 2021 11:15:36	Open
5	760	10.10.0.91	ARCOS-UAT2	su		Windows RDP	ARCOSADMIN	testing	1	22 Apr 2021 20:38:27					PAR	22 Apr 2021 19:40:41	Open

Showing 1 to 5 of 8 entries | Previous 1 2 Next

A Privileged Account Management Solution | Copyright © 2022 ARCON. All Rights Reserved.

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Request Number	The unique number associated with each service password raised request
IP Address	The IP address of the target server

Column Names	Description
Host Name	The hostname of the target server
User Name	The name of the user
DB Instance	The instance of the target server
Service Type	Name of the service type
Password viewed by	Name of the user who viewed the password
Description	Text entered while viewing the password
Open for Hours	Number of hours the password remains open
Open Till	Date/time till which the password remains open
Authentication 1	Name of approver 1
Authentication 2	Name of approver 2
Authentication 3	Name of approver 3
Authentication 4	Name of approver 4
Authentication 5	Name of approver 5
Approver	Name of final approver who approved the request
Password Viewed On	Date/time at which the password was viewed
View Status	If the password is viewed <ul style="list-style-type: none"> • Open • Closed
Current Status	Present status of the password <ul style="list-style-type: none"> • Open • Closed
Group Name	Name of the server group to which the server belongs

13.13 Service Password Envelope Print Status Report

The Service Password Envelope Print Status Report displays the print status of all the services for which the password envelope was created.



In order to view this report, users must have the following permission(s):

- **Service Password Envelope Print Status Report**

Service Password Envelope Print Status Report

Filter

LOB: All | Date From: 01-10-2021 00:00

View Report | Export To CSV

Record Count : 11

Show 5 entries

Sr.No.	LOB	Service IP	Service Host	Service User Name	Domain	Instance	Service Port	Service Type	Start Date	Started By User	Printing Status
1	DEFAULT LOB 2	1	HTTP://GMAIL.COM	test	HTTP://GMAIL.COM		22	App Web Browser	06 Oct 2021 15:55:37	ARCOSADMIN	Generated
2	DEFAULT LOB 2	192.168.0.240	LNXRH4_ARCONSRV	tuser1	LNXRH4_ARCONSRV			SSH LINUX	11 Oct 2021 19:50:09	ARCOSADMIN	Generated
3	DEFAULT LOB 2	10.10.0.154	10.10.0.154	sys	10.10.0.154	arcon	1521	App Toad - Oracle	08 Oct 2021 21:31:16	ARCOSADMIN	Generated
4	DEFAULT LOB 2	10.10.0.38	10.10.0.38	shalleesh	10.10.0.38	arcon	22	SSH MongoDB	28 Nov 2021 23:39:41	ARCOSADMIN	Generated
5	DEFAULT LOB 2	10.10.0.3	10.10.0.3	arccitrix/piyush.vora	10.10.0.3		80	App Web Browser	06 Dec 2021 13:24:20	ARCOSADMIN	Generated

Showing 1 to 5 of 11 entries

A Privileged Account Management Solution | Copyright © 2022 ARCON. All Rights Reserved.

The following columns can be seen in this report:

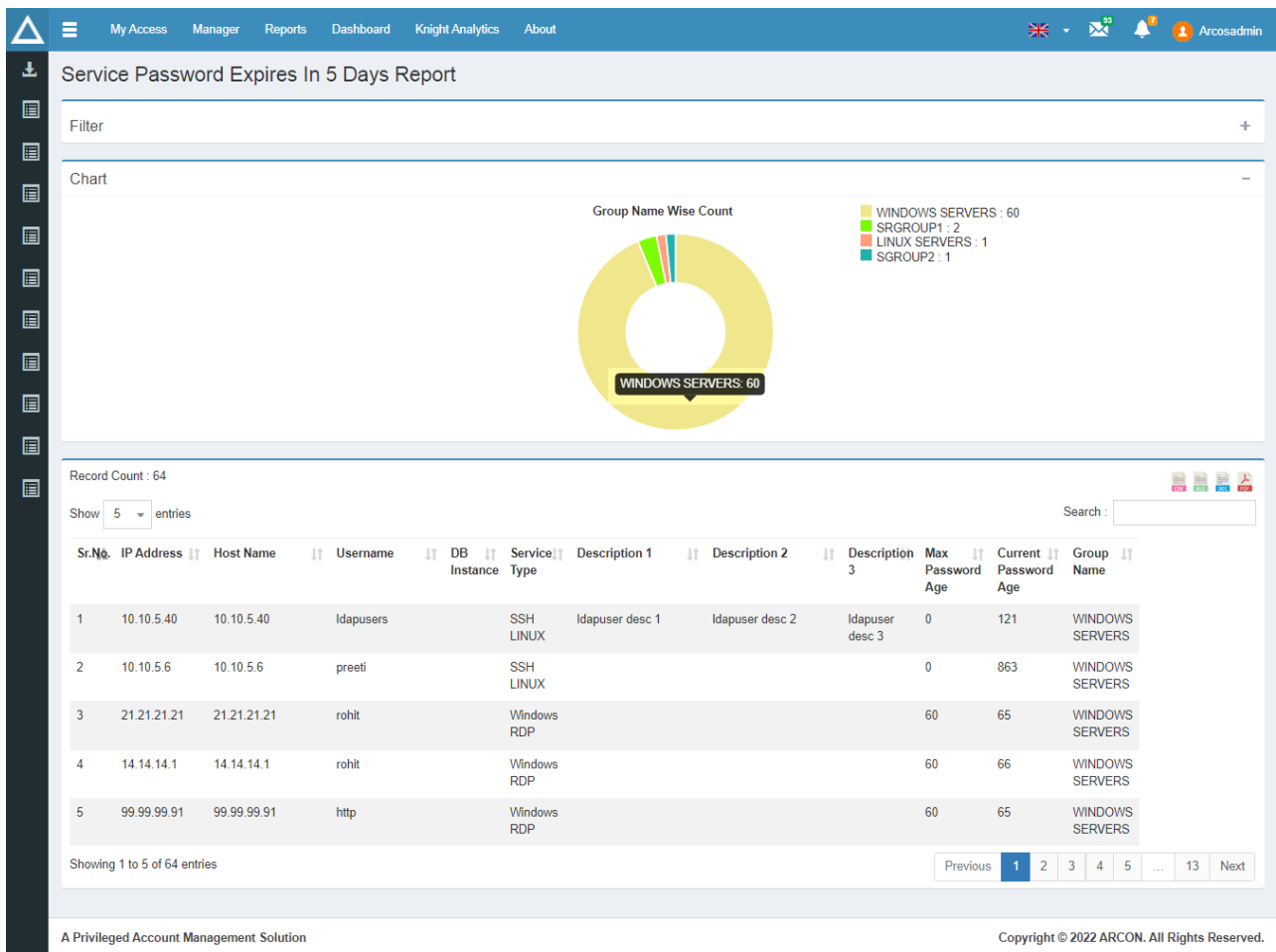
Column Names	Description
Sr. No.	To identify and distinguish rows
LOB/Profile	The name of the LOB to which the service belongs
Service IP	The IP address of the target server
Service Host	The hostname of the target server
Service User Name	The name of the user
Domain	The domain name of the target server
Service Port	Pport of the target servers
Service Type	Name of the service type
Start Date	Date on which the password envelope will generate
Started By User	Name of the user who printed the envelope
Printing status	Status of print <ul style="list-style-type: none"> Generated

13.14 Service Password Expires in 5 Days Report

The Service Password Expires in 5 Days Report displays the services whose passwords will expire in the next 5 days.

In order to view this report, users must have the following permission(s):

- Service Password Expires in 5 days Report




The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
IP Address	The IP address of the target server
Host Name	The hostname of the target server
User Name	The name of the user
DB Instance	The instance of the target servers
Service Type	Name of the service type
Description 1	Text entered during the creation of the service
Description 2	Text entered during the creation of the service
Description 3	Text entered during the creation of the service

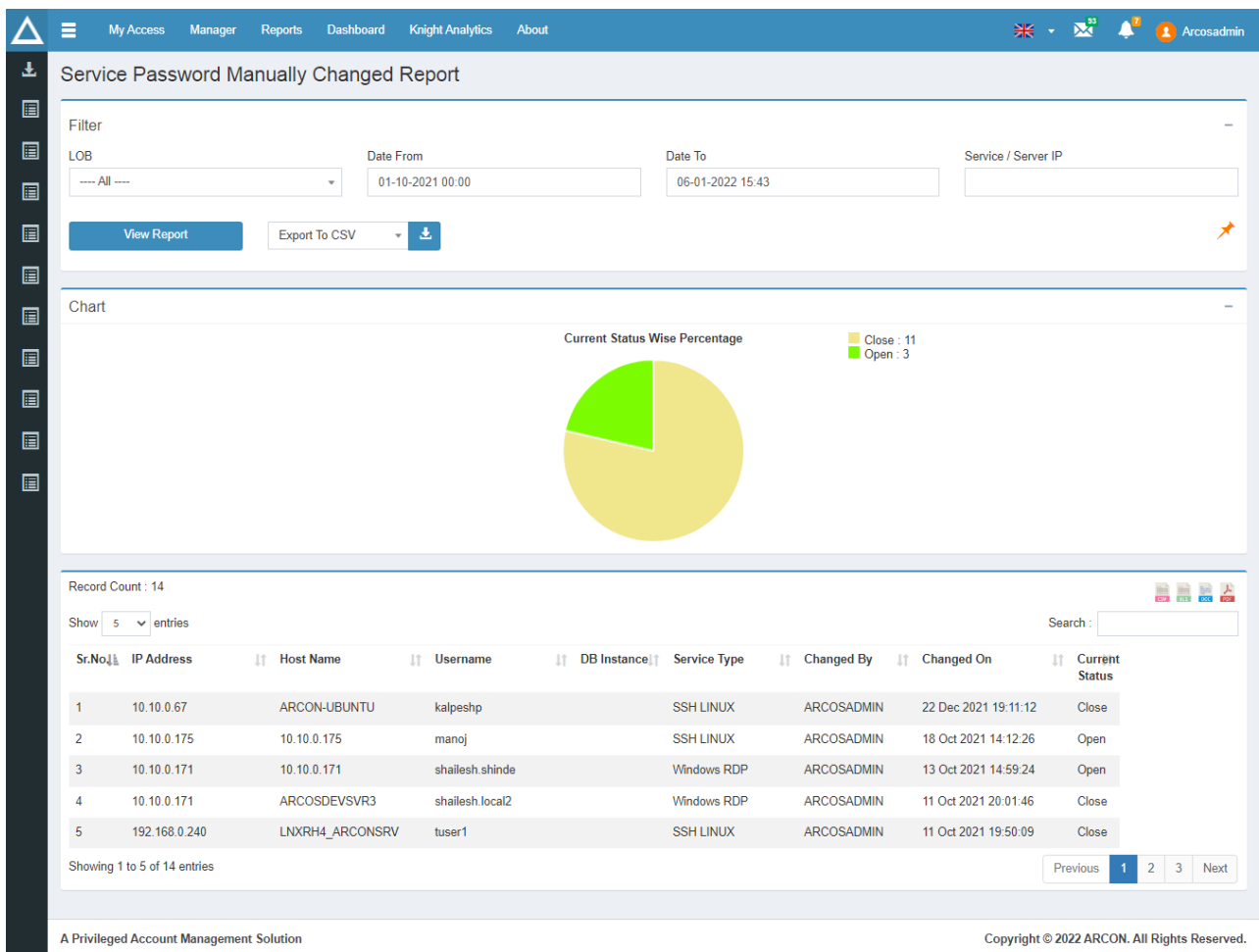
Column Names	Description
Max Password Age	Maximum age of password after which the password changes
Current Password Age	The current age of password in days
Group Name	Name of the server group to which the server belongs

13.15 Service Password Manually Changed Report

The Service Password Manually Changed Report displays all of the services whose passwords have been manually changed.

 In order to view this report, users must have the following permissions(s):

- **Service Password Manually Changed Report**



Service Password Manually Changed Report

Filter

LOB: --- All --- | Date From: 01-10-2021 00:00 | Date To: 06-01-2022 15:43 | Service / Server IP: []

View Report | Export To CSV | [Download]

Chart

Current Status Wise Percentage

- Close : 11
- Open : 3

Record Count : 14

Show 5 entries | Search: []

Sr.No	IP Address	Host Name	Username	DB Instance	Service Type	Changed By	Changed On	Current Status
1	10.10.0.67	ARCON-UBUNTU	kalpeshp		SSH LINUX	ARCOSADMIN	22 Dec 2021 19:11:12	Close
2	10.10.0.175	10.10.0.175	manoj		SSH LINUX	ARCOSADMIN	18 Oct 2021 14:12:26	Open
3	10.10.0.171	10.10.0.171	shailesh.shinde		Windows RDP	ARCOSADMIN	13 Oct 2021 14:59:24	Open
4	10.10.0.171	ARCOSDEVSVR3	shailesh.local2		Windows RDP	ARCOSADMIN	11 Oct 2021 20:01:46	Close
5	192.168.0.240	LNXRH4_ARCONSRV	tuser1		SSH LINUX	ARCOSADMIN	11 Oct 2021 19:50:09	Close

Showing 1 to 5 of 14 entries | Previous 1 2 3 Next


A Privileged Account Management Solution | Copyright © 2022 ARCON. All Rights Reserved.

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
IP Address	The IP address of the target server
Host Name	The hostname of the target server
User Name	The name of the user
DB Instance	The instance of the target servers
Service Type	Name of the service type
Changed By	Name of the Administrator who changed the password manually
Changed On	Date/time at which the password was changed
Current Status	Present status of the password <ul style="list-style-type: none"> • Open • Closed

13.16 Service Password Never Changed Report

The Service Password Never Changed Report displays all of the services that have never had their passwords changed, either manually or through a password change process.

 In order to view this report, users must have the following permission(s):

- **Service Password Never Changed Report**

My Access Manager Reports Dashboard Knight Analytics About

Service Password Never Changed Report

Filter

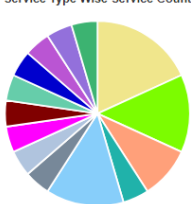
LOB: DEFAULT LOB 2 Service Group: CONNECTORS

Service Type: All

View Report
Export To CSV

Chart

Service Type Wise Service Count



Record Count : 22

Show 5 entries Search:

Sr.No.	IP Address	Host Name	Username	DB Instance	Service Type	Group Name
1	6.6.6.6	6.6.6.6	rohit		Windows RDP	WINDOWS SERVERS
2	13.107.21.200	AWS	test		App Web Browser	WINDOWS SERVERS
3	10.10.10.5	10.10.10.5	rohit		Windows RDP	WINDOWS SERVERS
4	10.10.10.10	10.10.10.10	rohit		Windows RDP	WINDOWS SERVERS
5	172.217.27.196	WWW.GOOGLE.COM	hello		App Web Browser	WINDOWS SERVERS

Showing 1 to 5 of 22 entries
Previous 1 2 3 4 5 Next


A Privileged Account Management Solution Copyright © 2022 ARCON. All Rights Reserved.

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
IP Address	The IP address of the target server
Host Name	The hostname of the target server
User Name	The name of the user
DB Instance	The instance of the target server
Service Type	Name of the service type
Group Name	Name of the service group to which the server belongs


www.arconnet.com | Copyright © 2022

179

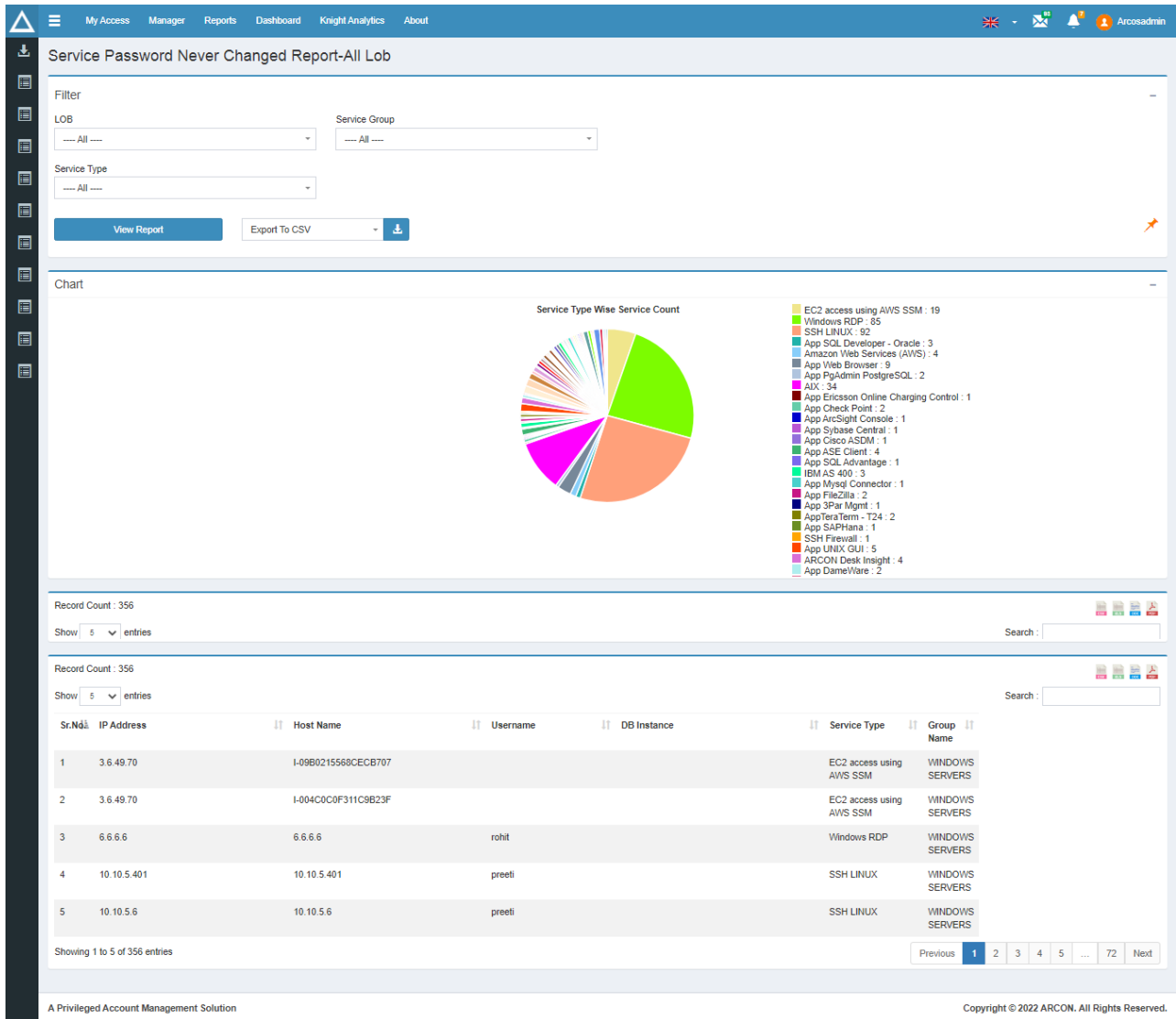


13.17 Service Password Never Changed Report - All LOB

The Service Password Never Changed Report - All LOB displays details of all the services whose passwords have never been changed, either manually or through the password change process, across all LOBs.

 In order to view this report, users must have the following permission(s):

- **Service Password Never Changed Report-All LOB**




The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
IP Address	The IP address of the target server





Column Names	Description
Host Name	The hostname of the target server
User Name	The name of the user
DB Instance	The instance of the target server
Service Type	Name of the service type
Group Name	Name of the service group to which the server belongs

13.18 Service Password Security Status Report

The Service Password Security Status Report displays the security password status (open/closed) of all services in graphical and grid view format.

 In order to view this report, users must have the following permission(s):

- **Service Password Security Status Report**


 91
  3
  Arcosadmin

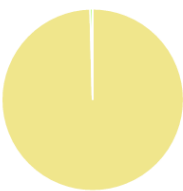
Service Password Security Status

Filter

LOB: Service Group:

Chart

Service Password Security Status



■ CLOSED : 475
■ OPEN : 2

Record Count : 2

Show entries

Sr.No.	Service User Name	Service IPAddress	Service Hostname	Service Instance	Service Domain
1	arcossqladmin	10.10.0.91	10.10.0.91	10.10.0.91,1433	10.10.0.91
Service Type MS SQL EM - Local					
2	administrator	10.10.0.162	WIN2K12QATEST		WIN2K12QATEST

Showing 1 to 2 of 2 entries

A Privileged Account Management Solution
Copyright © 2022 ARCON. All Rights Reserved.

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Service User Name	The user name of the service
Service IP Address	The IP address of the target server
Service Host Name	The hostname of the target server
Service Instance	The instance of the target server
Service Domain	The domain name of the target server
Service Type	Name of the service type

13.19 Service Password Vaulting Status

The Service Password Vaulting Status Report displays the vaulting password status (open/closed) of all services in grid view format.



To view this report, users must have the following permission(s):

- **Service Password Vaulting Status Report**

Zoom out to the screen to view all the columns or click on the + button to expand the hidden columns.


The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Service ID	The ID associated with the target server
LOB	Line of Business
Group	Name of the Server Group
Service Type	The name of the service type
System IP Instance hostname	The hostname of the IP instance
Host Name	The hostname of the target server
Instance Name	The instance of the target server
URL Parameter	Displays the URL parameter

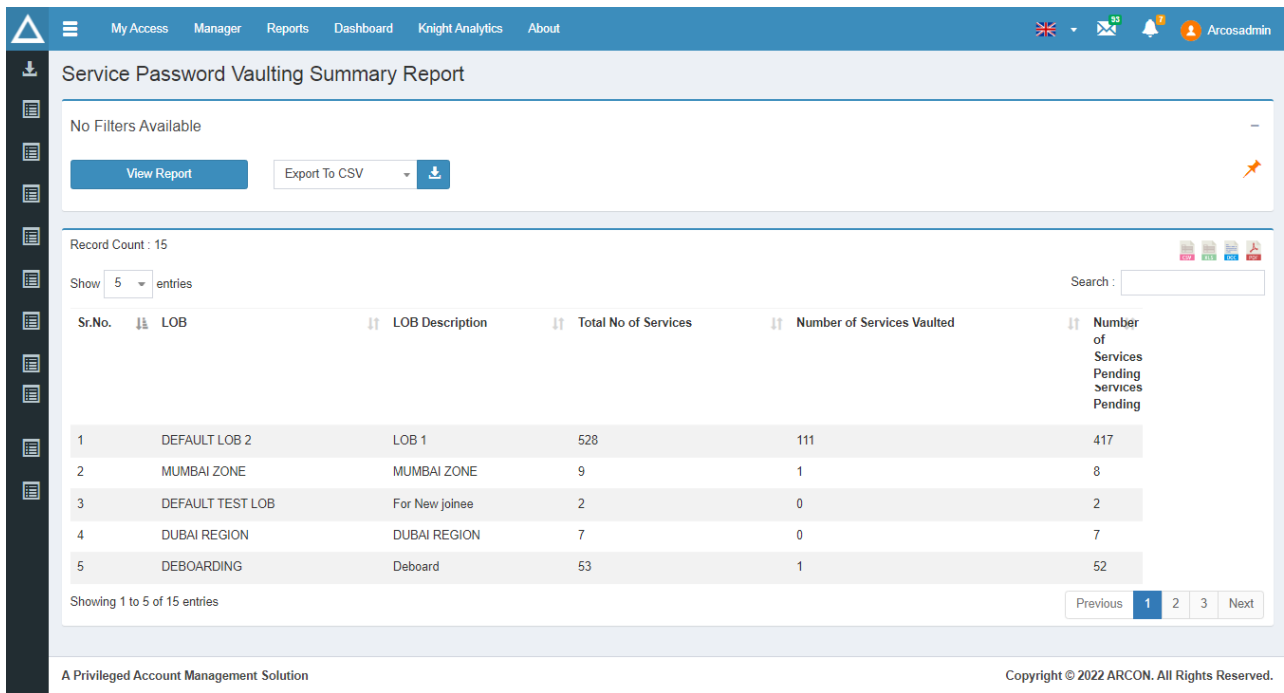
Column Names	Description
Privilege Id Service User Name	The username of the privilege Id service
Port	Displays the port number of the target server
Domain	The domain name of the target server
Current Password Age	Age of the current password
Min Password Age	The lowest age of the password
Max Password Age	Maximum age of the password after which the password changes
Allow Password Change	Is the password change feature enabled
Allow SPC	Is the SPC feature enabled
Sealed Status	Status of Seal
Vault Status As On Report Date	Status of the Vault on till date
Password Open By	Name of the User who opens the password
Password Open For Hours	Select the time for which you want the password to remain open
Password Open On	Displays the date when the password was open
Password Open Till	Displays the date and time until when the password is open for use
Password Rotate Status	Status of the password rotation
APC Errors	Display if APC error found
Allow Auto Heal	Is the Auto Heal feature enabled
LTC Service Ip and Username	IP and Username of the LTC Service
Last Password Change On	Displays the date when the password was changed last time
Last Password Change By	Displays the name who has changed the password last time
Next Password Change	Displays the date of the next password change
Dependency On Primary Service	Displays if has a dependency on primary service
Service Status	Status of the Service

13.20 Service Password Vaulting Summary Report

The Service Password Vaulting Summary Report displays the total number of services, the number of services vaulted, and the number of services pending for vaulting, LOB-wise.

 In order to view this report, users must have the following permission(s):

- **Service Password Vaulting Summary Report**



The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
LOB	The name of the LOB
LOB Description	Description of the LOB entered by the Administrator at the time of creation
Total No of services	Total number of services in that LOB
Number of services vaulted	Total number of services vaulted
Number of services pending for vaulting	Total number of services pending for vaulting

13.21 Service Password Viewed By Administrator

The Service Password Viewed By Administrator Report displays details of all the service passwords viewed by the Administrators in grid view format.

i To view this report, users must have the following permission(s):

- **Service Password Viewed By Administrator**

i Zoom out to the screen to view all the columns or click on the + button to expand the hidden columns.

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
ID	The ID of the service
Requested By	The name of the user who raised the request
Requested On	Date/time at which the request was raised
Service IP	The IP address of the target servers
Service Host Name	The hostname of the target server
Service Domain Name	The domain name to which the service belongs

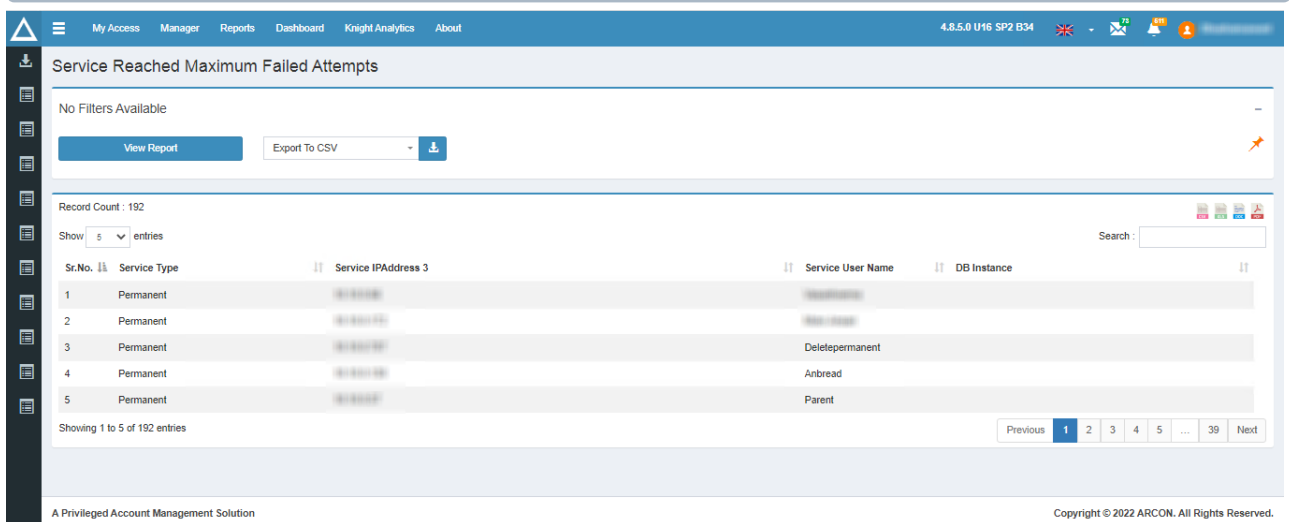
Column Names	Description
Service Type	The server type for which the request has been raised
Approver 1 User ID	The User ID associated with the Approver 1
Approved On Date and Time	Date/time at which the service password was approved by Approver 1
Approver 2 User ID	The User ID associated with the Approver 2
Approved On Date and Time	Date/time at which the service password was approved by Approver 2
Description	Description of the service password
Open For Hours	Time in hours until which the request will remain valid
Current Status	The current status of the request

13.22 Service Reached Maximum Failed Attempts

The Service Reached Maximum Failed Attempts Report displays all the services for which the scheduled password change has been terminated due to exceeding the maximum number of failed attempts. The maximum number of failed attempts is specified in the **Scheduled Password Change - Service Reached Maximum Failed Attempts** in Settings.

i In order to view this report, users must have the following permission(s):

- **Service Reached Maximum Failed Attempts**



i Zoom out to the screen to view all the columns or click on the + button to expand the hidden columns.

The following columns are available in this report:

Column Names	Description
Sr No.	To identify and distinguish rows
Service type	Name of the service type
Service IP Address	The IP address of the target server
Service User Name	Username of the service
DB Instance	Displays DB Instance of service

13.23 Service Reconcile Status Report

The Service Reconcile Status Report displays the status of all reconciliations as well as the details of each reconciliation.

In order to view this report, users must have the following permission(s):

- Service Reconcile Status Report**

Service Reconcile Status Report

Filter

LOB:

Service Type:

[View Report](#) [Export To CSV](#)

Record Count : 1098

Show entries

Sr.No.	LOB/Profile	Service Type	IP Address	Host Name	Username	Domain Name	Port	Reconcile Status	Reconciled On	Error!
1	DEFAULT LOB 2	SSH Telnet	10.10.0.246	10.10.0.246	en	10.10.0.246	23	Never Reconciled.		Never Reconciled.
Server Group Name WINDOWS SERVERS										
2	DEFAULT LOB 2	SSH Telnet	10.10.0.246	10.10.0.246	en	10.10.0.246	23	Never Reconciled.		Never Reconciled.
3	DEFAULT LOB 2	SSH Telnet	10.10.2.52	10.10.2.52	arcon	10.10.2.52	23	Never Reconciled.		Never Reconciled.
4	DEFAULT LOB 2	SSH Telnet	10.10.2.52	10.10.2.52	arcon1	10.10.2.52	23	Reconciled Success.	22 Mar 2021 21:09:22	Success.
5	DEFAULT LOB 2	SSH Telnet	10.10.0.246	10.10.0.246	anb	10.10.0.246	23	Never Reconciled.		Never Reconciled.

Showing 1 to 5 of 1,098 entries

Previous **1** 2 3 4 5 ... 220 Next

A Privileged Account Management Solution Copyright © 2022 ARCON. All Rights Reserved.

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
LOB/Profile	The name of the LOB
Service Type	Name of the service type
IP Address	The IP address of the target server
Host Name	The hostname of the target server
User Name	The name of the user
Domain Name	The domain name of the target server
Port	The port opened to connect to the target server
Reconciled Status	Status of the password reconciliation <ul style="list-style-type: none"> • Reconciled success • Never reconciled
Reconciled On	Date/time at which the reconciliation happened
Error	Errors captured in case of failure of reconciliation
Server Group Name	Name of the server group to which the target server belongs

13.24 Services Details for SPC - Maximum Failed Attempts

The Service Details for SPC - Maximum Failed Attempts report displays the information of the services for SPC for which there were maximum failed attempts.



In order to view this report, users must have the following permission(s):

- **Service Details for SPC - Maximum Failed Attempts**

Services details for SPC-Maximum Failed Attempts

No Filters Available

View Report Export To CSV

Record Count : 7

Show 5 entries Search :

Sr.No.	IP Address	Host Name	Domain Name	Username	DB Instance	Service Type	Group Name
1	10.10.5.6	10.10.5.6	10.10.5.6	preeti		SSH LINUX	SGROUP2
1	10.10.5.6	10.10.5.6	10.10.5.6	preeti		SSH LINUX	SGROUP2
2	10.10.5.6	10.10.5.6	10.10.5.6	preeti		SSH LINUX	WINDOWS SERVERS
3	10.10.1.183	LOCALHOST	localdomain	kaiser		SSH LINUX	LINUX SERVERS
4	10.10.1.183	LOCALHOST	localdomain	kaiser		SSH LINUX	WINDOWS SERVERS
5	10.10.1.9	10.10.1.9	ATSTESTDC	ADB_03		SSH LINUX	LINUX SERVERS

Showing 1 to 5 of 7 entries Previous 1 2 Next

A Privileged Account Management Solution Copyright © 2022 ARCON. All Rights Reserved.

The following columns can be seen in this report:

Columns	Description
Sr. No.	To identify and distinguish rows
IP Address	The IP Address of the target server
Host Name	The host name of the target server
Domain Name	The domain name of the target server
User Name	The name of the user
DB Instance	The instance of the target server
Service Type	Name of the service type
Group Name	Name of the server group for which the services were scheduled for SPC.

13.25 Services Scheduled for SPC

The Services Scheduled for SPC Report displays services that are scheduled or queued for password change.

In order to view this report, users must have the following permission(s):

- **Services Scheduled for SPC Report**

Record Count : 76

Show 5 entries

Sr.No.	IP Address	Host Name	Username	DB Instance	Service Type	Description 1	Description 2	Description 3
1	10.10.5.401	10.10.5.401	preeti		SSH LINUX			
Description 3								
Group Name WINDOWS SERVERS								
2	99.99.99.98	MYHOSTNAME	RDP999		SSH LINUX			
3	10.11.10.190	10.11.10.190	preeti		SSH LINUX			
4	10.10.170.36	10.10.170.36	preeti		SSH LINUX			
5	10.10.170.100	10.10.170.100	preeti		SSH LINUX			

Showing 1 to 5 of 76 entries

A Privileged Account Management Solution Copyright © 2022 ARCON. All Rights Reserved.


The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
IP Address	The IP address of the target server
Host Name	The host name of the target server
User Name	The name of the user
DB Instance	The instance of the target server
Service Type	Name of the service type
Description 1	Text entered during the creation of the service
Description 2	Text entered during the creation of the service
Description 3	Text entered during the creation of the service

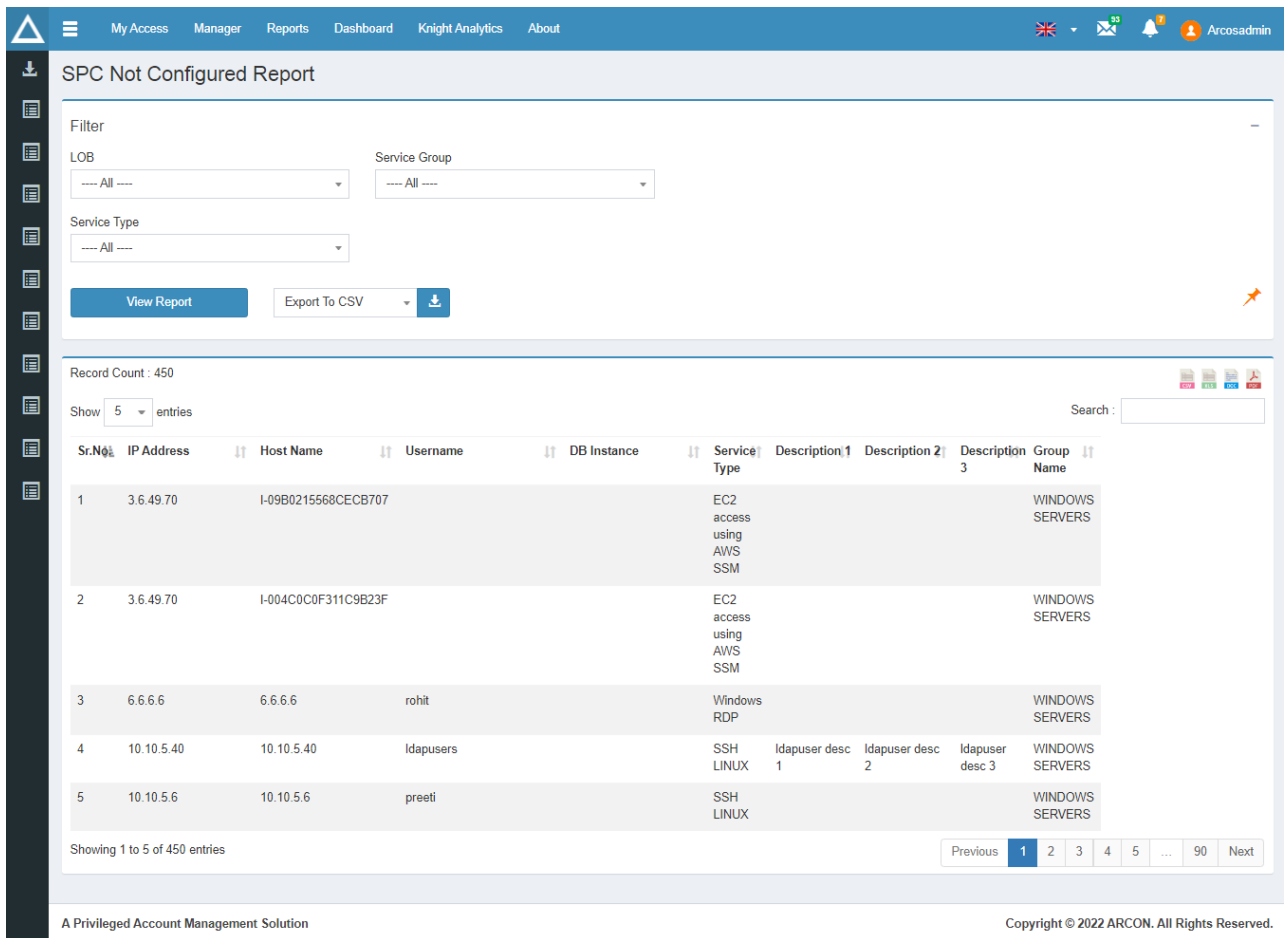
Column Names	Description
Group Name	Name of the server group in which the services are scheduled for SPC

13.26 SPC Not Configured Report

SPC Not Configured Report displays services for which SPC has not been configured.

 In order to view this report, users must have the following permission(s):

- **SPC Not Configured Report**



Record Count : 450

Show 5 entries

Sr.No.	IP Address	Host Name	Username	DB Instance	Service Type	Description 1	Description 2	Description 3	Group Name
1	3.6.49.70	I-09B0215568CECB707			EC2 access using AWS SSM				WINDOWS SERVERS
2	3.6.49.70	I-004C0C0F311C9B23F			EC2 access using AWS SSM				WINDOWS SERVERS
3	6.6.6.6	6.6.6.6	rohit		Windows RDP				WINDOWS SERVERS
4	10.10.5.40	10.10.5.40	Idapusers		SSH LINUX	Idapuser desc 1	Idapuser desc 2	Idapuser desc 3	WINDOWS SERVERS
5	10.10.5.6	10.10.5.6	preeti		SSH LINUX				WINDOWS SERVERS

Showing 1 to 5 of 450 entries

Previous 1 2 3 4 5 ... 90 Next

A Privileged Account Management Solution Copyright © 2022 ARCON. All Rights Reserved.


The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
IP Address	The IP address of the target server
Host Name	The hostname of the target server

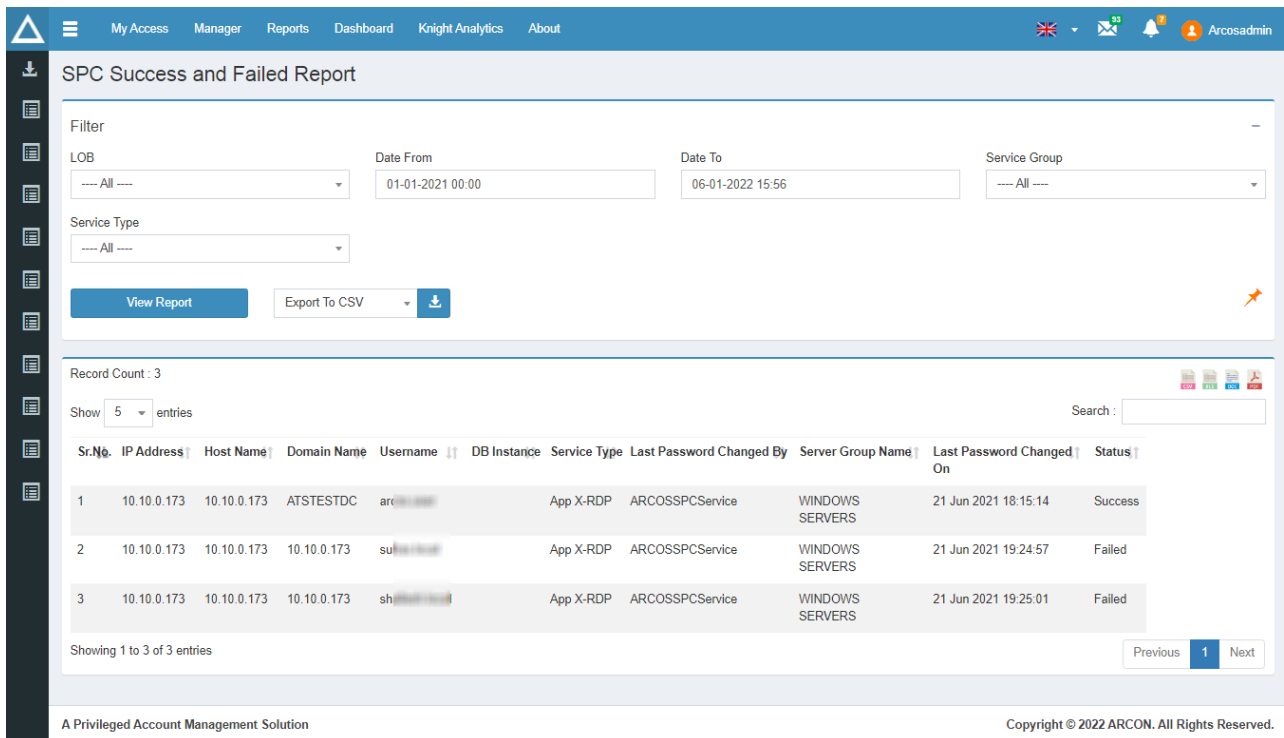
Column Names	Description
User Name	The name of the user
DB Instance	The instance of the target server
Service Type	Name of the service type
Description 1	Text entered during the creation of the service
Description 2	Text entered during the creation of the service
Description 3	Text entered during the creation of the service
Group Name	Name of the server group in which the service is present

13.27 SPC Success and Failed Report

SPC Success and Failed Report displays details of service password changes through the SPC service.

 In order to view this report, users must have the following permission(s):

- **SPC Success and Failed Report**



The screenshot shows the 'SPC Success and Failed Report' interface. It features a navigation bar at the top with options like 'My Access', 'Manager', 'Reports', 'Dashboard', 'Knight Analytics', and 'About'. Below the navigation bar, there's a filter section with dropdown menus for 'LOB' (set to 'All'), 'Date From' (01-01-2021 00:00), 'Date To' (06-01-2022 15:56), and 'Service Group' (set to 'All'). A 'View Report' button and an 'Export To CSV' button are also present. Below the filter section, the 'Record Count' is 3, and the 'Show' dropdown is set to 5 entries. A search bar is available on the right. The main table displays the following data:

Sr.No	IP Address	Host Name	Domain Name	Username	DB Instance	Service Type	Last Password Changed By	Server Group Name	Last Password Changed On	Status
1	10.10.0.173	10.10.0.173	ATSTESTDC	arcosadmin		App X-RDP	ARCOSSPCService	WINDOWS SERVERS	21 Jun 2021 18:15:14	Success
2	10.10.0.173	10.10.0.173	10.10.0.173	subadmin		App X-RDP	ARCOSSPCService	WINDOWS SERVERS	21 Jun 2021 19:24:57	Failed
3	10.10.0.173	10.10.0.173	10.10.0.173	shadmin		App X-RDP	ARCOSSPCService	WINDOWS SERVERS	21 Jun 2021 19:25:01	Failed

Showing 1 to 3 of 3 entries. Navigation buttons for 'Previous', '1', and 'Next' are visible at the bottom right of the table.

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
IP Address	The IP address of the target server
Host Name	The hostname of the target server
Domain Name	The domain name of the target server
User Name	The name of the user
DB Instance	The instance of the target server
Service Type	Name of the service type
Last successful Password Changed By	Name of the Administrator who changed the last password successfully
Server Group name	Name of the server group to which the server belongs
Last Password Changed On	Date/time at which the last password was changed
Last successful Password Changed Through	The method by which the last password was changed
Current Status	Present status of the password <ul style="list-style-type: none"> • Success • Failed

13.28 Users Extracting Password Envelope Report

The Users Extracting Password Envelope Report displays details of users who have opened the printed password envelopes.



In order to view this report, users must have the following permission(s):

- **Users Extracting Password Envelope Report**

The following columns can be seen in this report:

Column Names	Description
Sr. No.	To identify and distinguish rows
Login User	Name of the user opening the password envelope
LOB	Name of the LOB
Authenticator 1	Name of the first authorizer who allowed the envelope to be opened
Authenticator 2	Name of the second authorizer who allowed the envelope to be opened
Domain of Authenticator 1	Domain to which the Authorizer 1 belongs

Column Names	Description
Domain of Authenticator 2	Domain to which the Authorizer 2 belongs
Envelope Category	Type of password envelope
Service IP	The IP address of the target server
Host Name	The hostname of the target server
Domain Name	The domain name of the target server
User Name	The name of the user
Service Type	Name of the service type
Envelope Status	Status of envelope
Date of Generation	Date/time at which the envelope was created

Privileged Access Management Suite



No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means such as electronic, mechanical, photocopying, recording, or otherwise without permission.