Predict | Protect | Prevent

ARCON|PAM

Offline Vault

Table of Contents

Disclaimer

The handbook of ARCON PAM solution is being published to guide stakeholders and users. If any of the statements in this document are at variance or inconsistent it shall be brought to the notice of ARCON through the support team. Wherever appropriate, references have been made to facilitate a better understanding of the PAM solution. ARCON team has made every effort to ensure that the information contained in it was correct at the time of publishing.
Nothing in this document constitutes a guarantee, warranty, or license, expressed or implied. ARCON disclaims all liability for all such guarantees, warranties, and licenses, including but not limited to: Fitness for a particular purpose; merchantability; non-infringement of intellectual property or other rights of any third party or of ARCON; indemnity; and all others. The reader is advised that third parties can have intellectual property rights that can be relevant to this document and the technologies discussed herein, and is advised to seek the advice of competent legal counsel, without obligation of ARCON.

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

1 Introduction

It is important to be able to provide service access to network engineers who work onsite, or other users who cannot connect to PAM because of PAM server unavailability and also it is important to audit each and every activity performed by the users. To meet with this requirement we have introduced the Offline Vault feature.

Offline Vault is a local database that is hosted on end user's machine .The Offline sync service will sync all the required information like services information that is approved for offline access, offline users information, etc from ARCON PAM Database and store it in the end user's local database. The logs stored in end user's machine are tamper - proof.

Offline Vault allows the users who work onsite and are not connected to PAM to take offline sessions. The services request has to be approved for offline access for performing their required activities. The activities performed by these users are audited. These offline activities are then synced back to the ARCON PAM Application with the help of Offline sync service , once the PAM server is available.

1.1 Key Features

Offline Storage:
Tamper Proof Video Logs will be stored on the end-user device. The security features are applied to ensure that the end-user will not be able to view/edit/delete storage location to maintain the integrity of the video logs captured.

Offline Access Request:

When connected to the network, the end-user should be able to raise a request for offline access to the required service which shall be approved by the Approver. When the request is approved, the required information for offline access will be synced from the PAM database to the local/offline database by the offline agent.

Offline Application + Agent

Only the local accounts will be authenticated and not domain accounts during application access.

The offline agent will sync all the logs captured on the end-user device to ARCON PAM and free the local storage on the device after a successful sync.

Offline Connector

Multitab will launch the Connector by passing the required parameters from Offline Vault. The service access session login/logout time is punched and recorded in the local database (Offline Vault). Once a user takes offline access to the service, the screen recording takes place and the recording is stored in the local database.

Logs And Reports

All the session logs, user logs, service logs , command logs etc. which are usually captured and maintained for normal PAM service access will also be maintained for offline access.

1.2 Pre-requisites

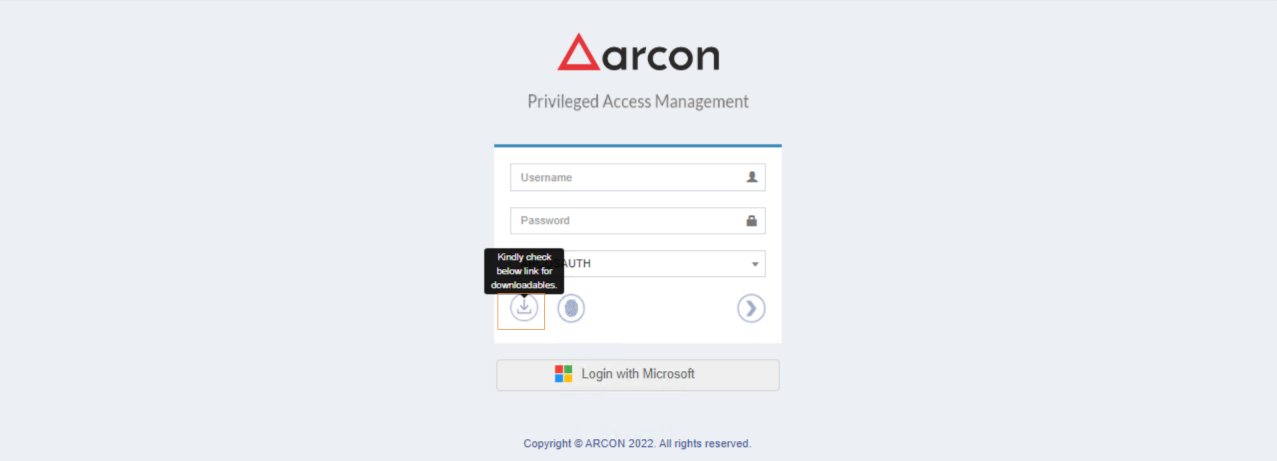
Following are the pre - requisites for Offline Access :

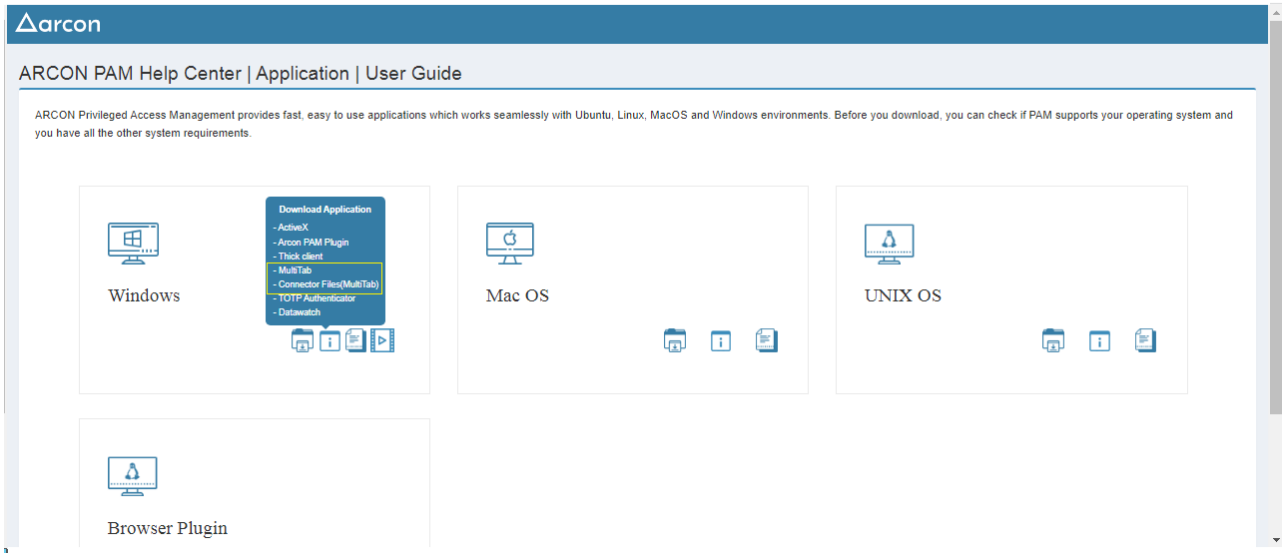
- Configuration file needs to be generated from Multitab configuration tool which includes offline API URL.
- Multitab application - Through this application end user can take offline access to the services. Need to be downloaded from ACMO → Downloads → Multitab zip.
- Connector zip - This zip file will consist of connector files of all the service types. Need to be downloaded from ACMO → Downloads → Connector Files zip.
- Offline sync service - Offline Sync service is responsible for syncing the required information for offline access from the ARCOS DB to the local database. In addition to that, it is syncing the generated logs from the local database to the ARCOS DB. (Included in the Multitab zip)
- Offline API service - This service communicates with local DB and fetches required data from the local DB for successful connection to the offline services. (Included in Multitab zip)

Offline Sync and Offline API service to be installed from the msi file that is available in Multitab zip file.

Connector files are available in Connectors zip file.

Navigate to **ARCON PAM Help Center** from the PAM login page to download the Multitab zip file and Connectors zip file.





Offline Multitab Configuration

Offline multitab depends on two windows services which can be installed through msi, that is available under multitab zip file

1. OfflineSyncService
2. OfflineAPI

– Offline multitab is configured to use windows authentication. Windows logged in user (domain user) will be directly authenticated to Offline Multitab.

1. Configuration in OfflineSyncService (appsettings.json)

a. Add PAM API url in "PAMAPIURL": "",

b. Add service execution intervals in hours encrypted

1. Sync from main db to local db "ExecutionIntervalsDataSync": "",
2. Sync from local db to main db "ExecutionIntervalsLogSync": ""

c. Add api encrypted user name and password

1. Configuration in OfflineAPI (appsettings.json)

a. Add offline api url (local host with port number),

Note: this url should be the same while adding offline url in multitab configuration tool.

b. AllowedStorageMB – allowed disk size in MB for video logs, this will restrict further SSO once defined limit reached

c. AllowedDays – number of days allowed to take SSO, restrict service access once limit reached

1. Configuration in multitab configuration tool

Add offline api url in multitab configuration tool, so that the generated config file will contains offline api url.

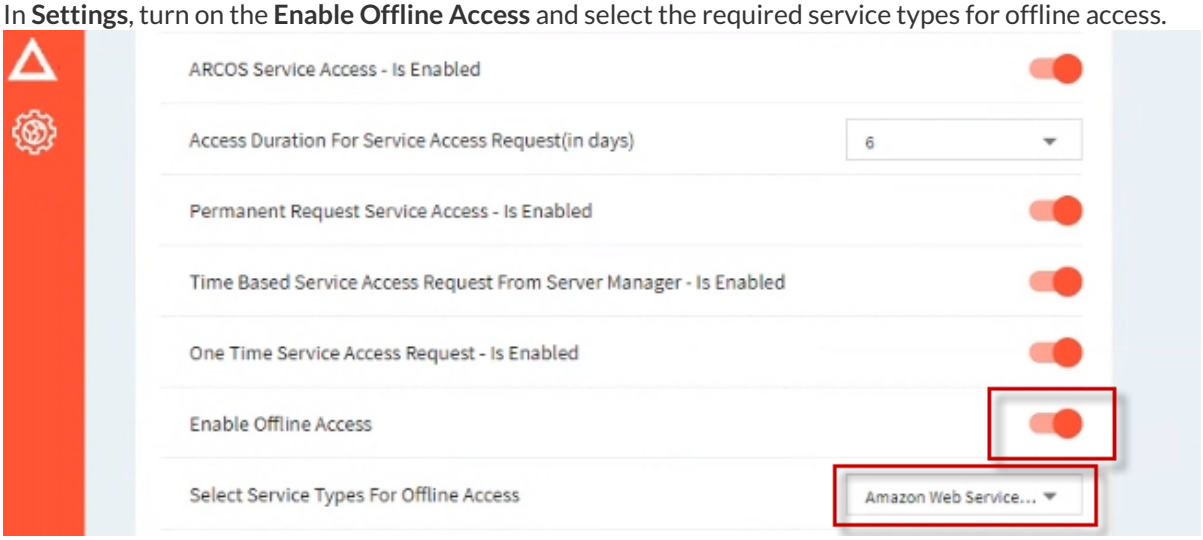
1.3 Flow Of Offline logs (Steps) :

1. **Enable Offline Access from Settings**

The administrator needs to enable offline access configuration in **NG - Settings** in order to enable Offline Vault functionality globally in PAM.

To enable Offline Access, perform these steps below:

1. Log in to the **Settings** application.
2. In **Settings**, turn on the **Enable Offline Access** and select the required service types for offline access.

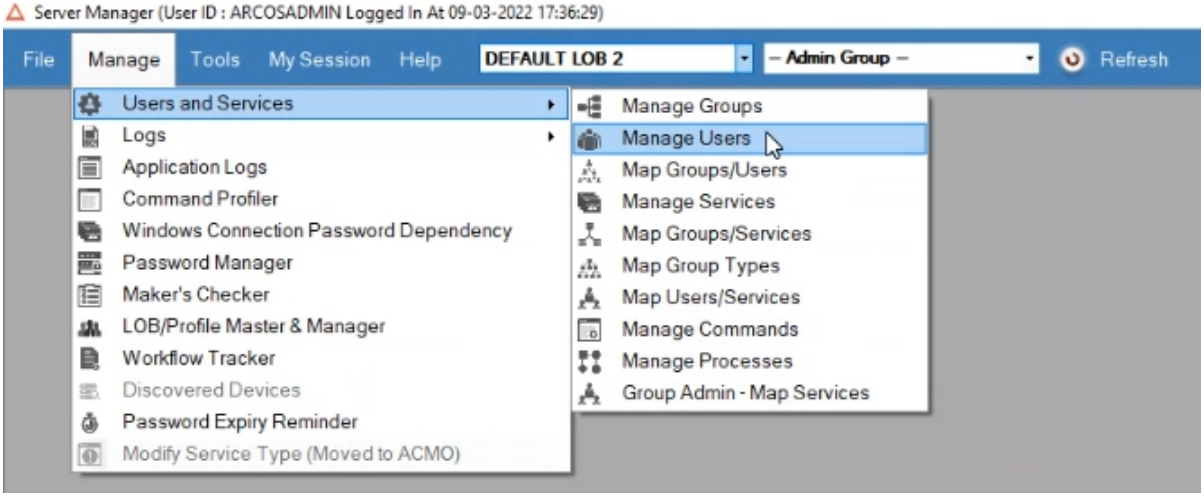


2. Allow Offline Access Privilege

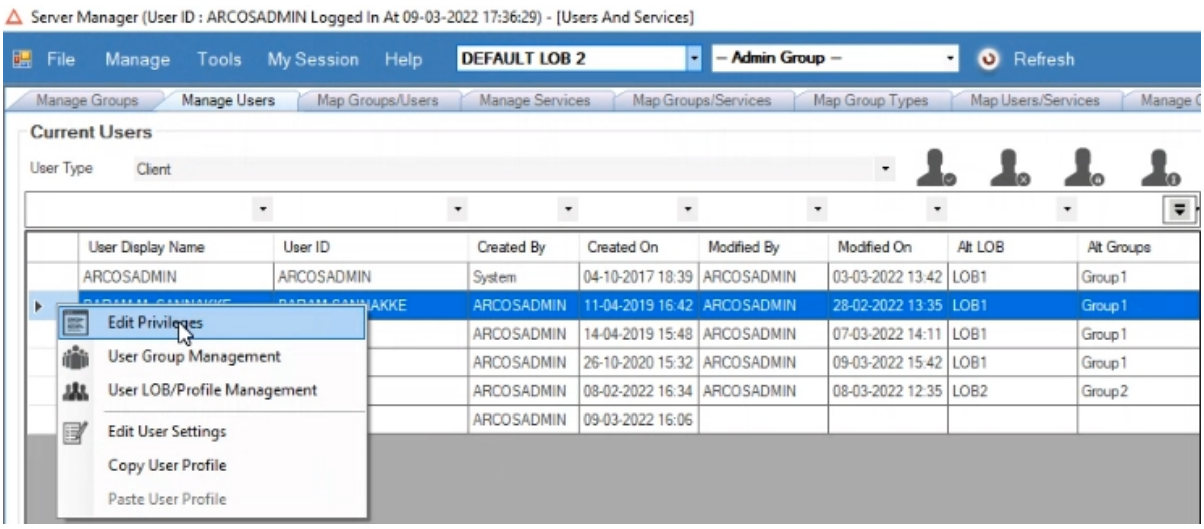
The administrator has to provide the **Allow Offline Access Request** privilege to the end-user who requires offline service access.

Perform the steps below, to provide the Allow Offline Access Request privilege:

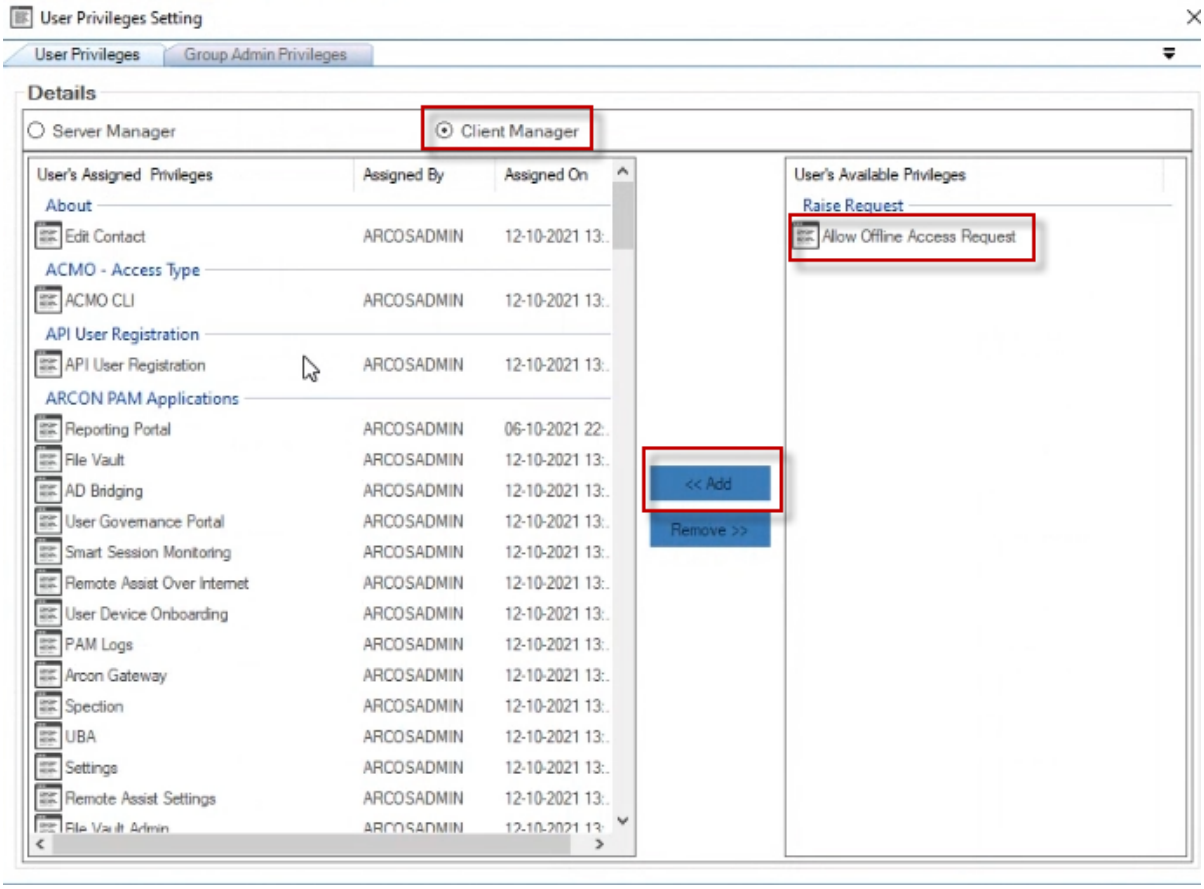
1. Login to the Server Manager and navigate to Manage → Users and Services → Manage Users



2. Select the user who required offline access, right-click and click on the **Edit Privileges** option.



3. Select the **Client Manager** radio button, click on the **Allow Offline Access Request,** and then click on the **Add** button to provide the privilege to the user.

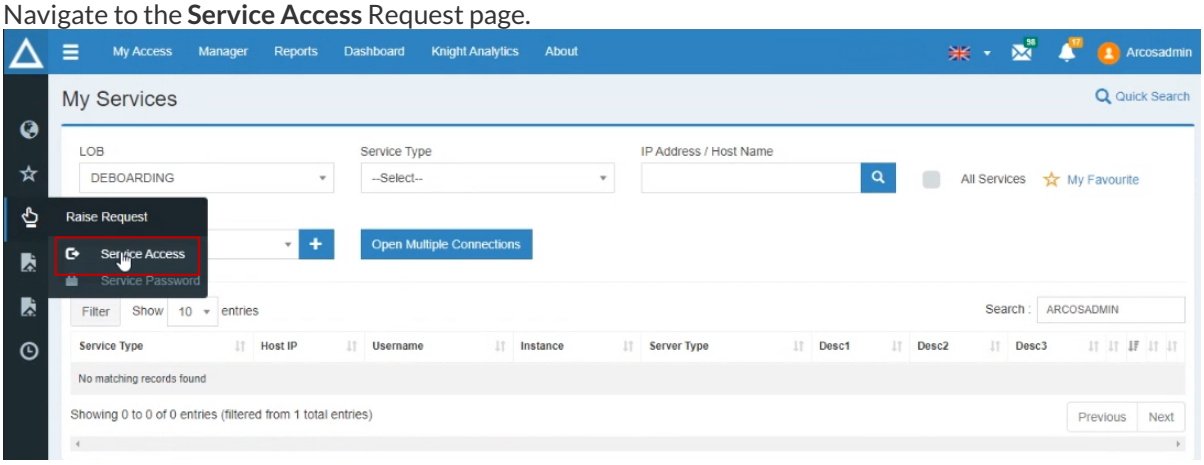


3. Request for an Offline Service

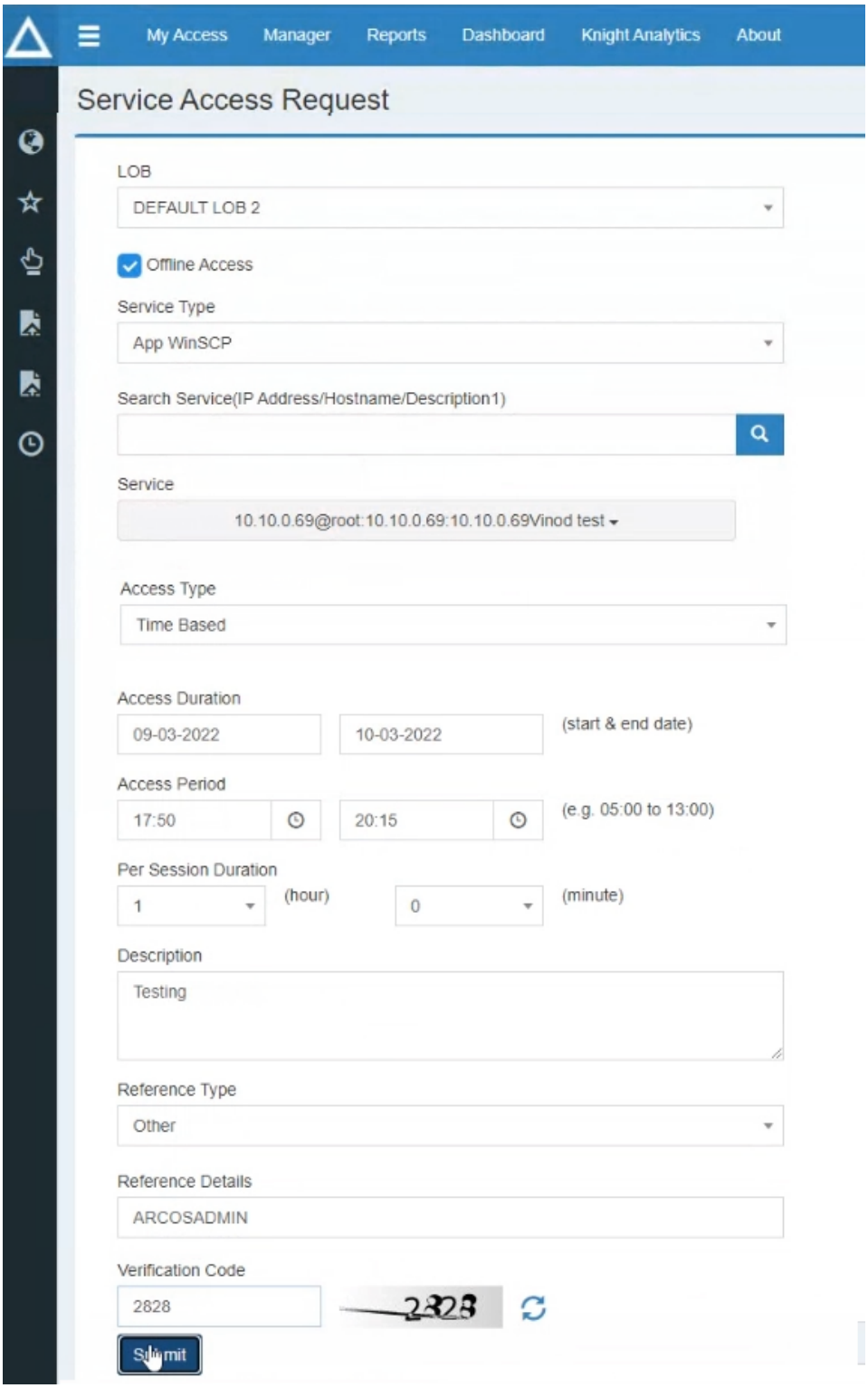
This section explains the steps involved in raising an offline request for a service.

To request an offline service, the user shall perform these steps below:

1. Log in to the PAM application.
2. Navigate to the **Service Access** Request page.



3. Enter the required details as shown in the table below and **submit** the request:



Refer to the table below to understand the fields in the above screen:

Field	Description		
LOB	The name of the LOB		
Offline Access	Select this checkbox to send the offline access request for the selected service ⓘ This configuration is visible only if Offline Access is enabled in NG - Settings and the user raising the request has Offline Access privilege.		
Service Type	The name of the service type for which the offline access request is raised		
Search service(IP Address/ Hostname)	The target server can be searched directly by entering its IP Address/ Hostname/ Description1 labels.		
All Services	This will list all the services in the service box which are not assigned to that user but belong to that LOB and Service type		
Service	Select the target server for which the request is raised		
Configuration Command	Specify the configuration commands you need access to for that server ✓ The configuration command box is visible only if the following configuration is disabled from settings: • **Hide Configuration Command for Service Request**		
Access Type	Time Based Access	The request is raised to access the target server for a certain duration	
		Access Duration	The dates between which the user requires server access.
		Access Period	The period of time during which the user requires access to the server between the dates provided in the access duration.
		Per Session duration	In a session, the amount of time in hours and minutes a user can access the service.
	One Time Access	The request is raised to access the target server for only one time	
		Access Duration	The dates between which the user requires server access.
		Per Session duration	In a session, the number of hours and minutes a user can access the service.

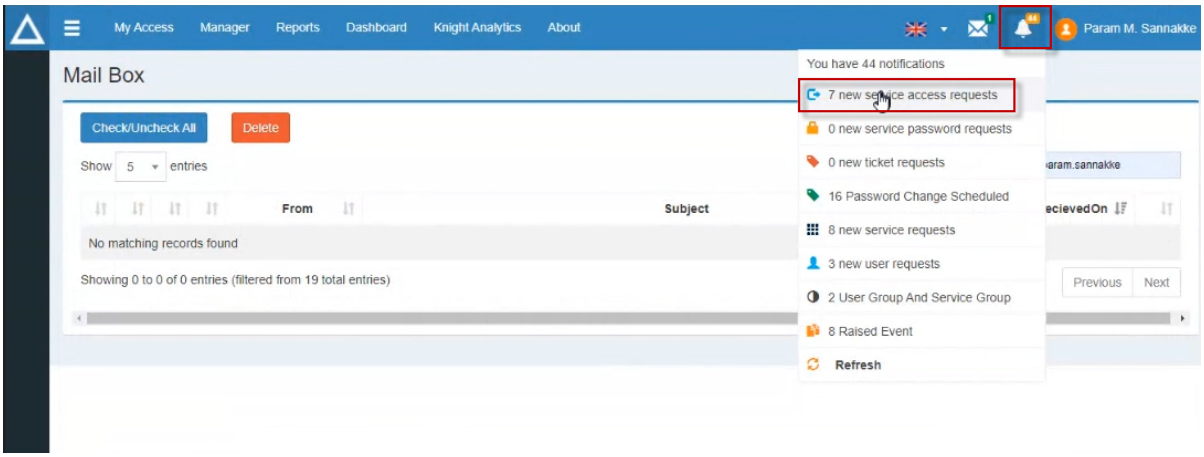
Field	Description
Description	Brief summary explaining the purpose of the request to the approver
Reference Type ** Customized field	This field name is bespoke and can be set according to an organization's needs in **Settings**. This is a mandatory field only if the following configuration is enabled from settings: • **Reference Details Mandate while raising Service Access Request- Is Enable**
Reference Details ** Customized field	This field name is bespoke and can be set according to an organization's needs in **Settings**. This is a mandatory field only if the following configuration is enabled from settings. • **Reference Details Mandate while raising Service Access Request- Is Enable**
Verification Code	This captcha code is entered only for validating the human identity The verification code appears only if the following configuration is enabled from settings. • **CAPTCHA Validation In ACMO Service Access And Password Request - Is Enabled**

4. Approval Process by the Approver

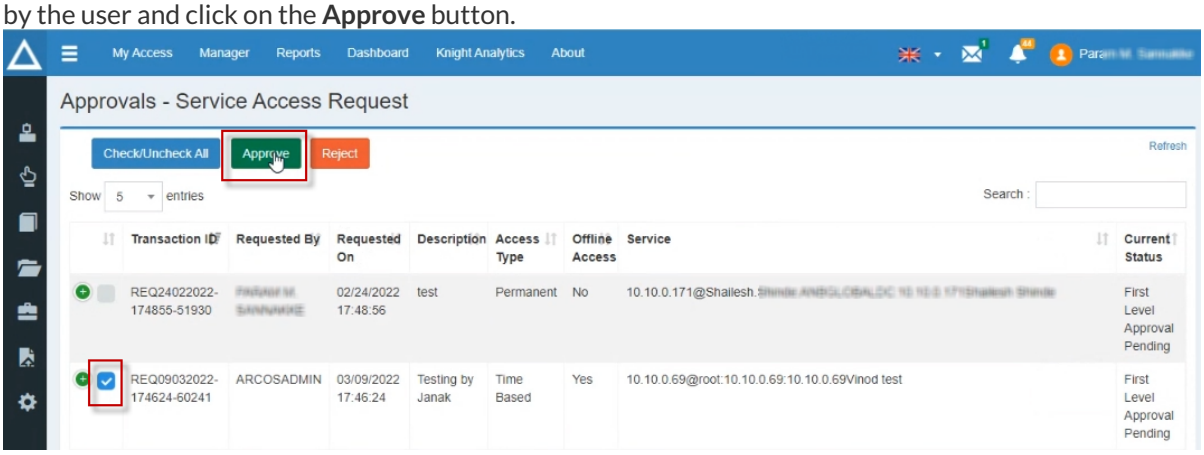
This section explains the steps involved in approving an offline request for a service.

To provide access to the offline vault, the Approver shall perform these steps below:

1. Log in to the PAM application. Click on the notification icon and then select the **new service access requests** notification.



2. You will get redirected to the **Approvals - Service Access Request** page. Select the offline request raised by the user and click on the **Approve** button.



You can find the Offline Access requests under the **Offline Access** column. If it says **Yes**, then the user requested Offline Access.

3. After the offline access for the service has been approved by the approver , Offline Sync Service will sync all the data required for connection to service , from the ARCOS DB to Local Database .

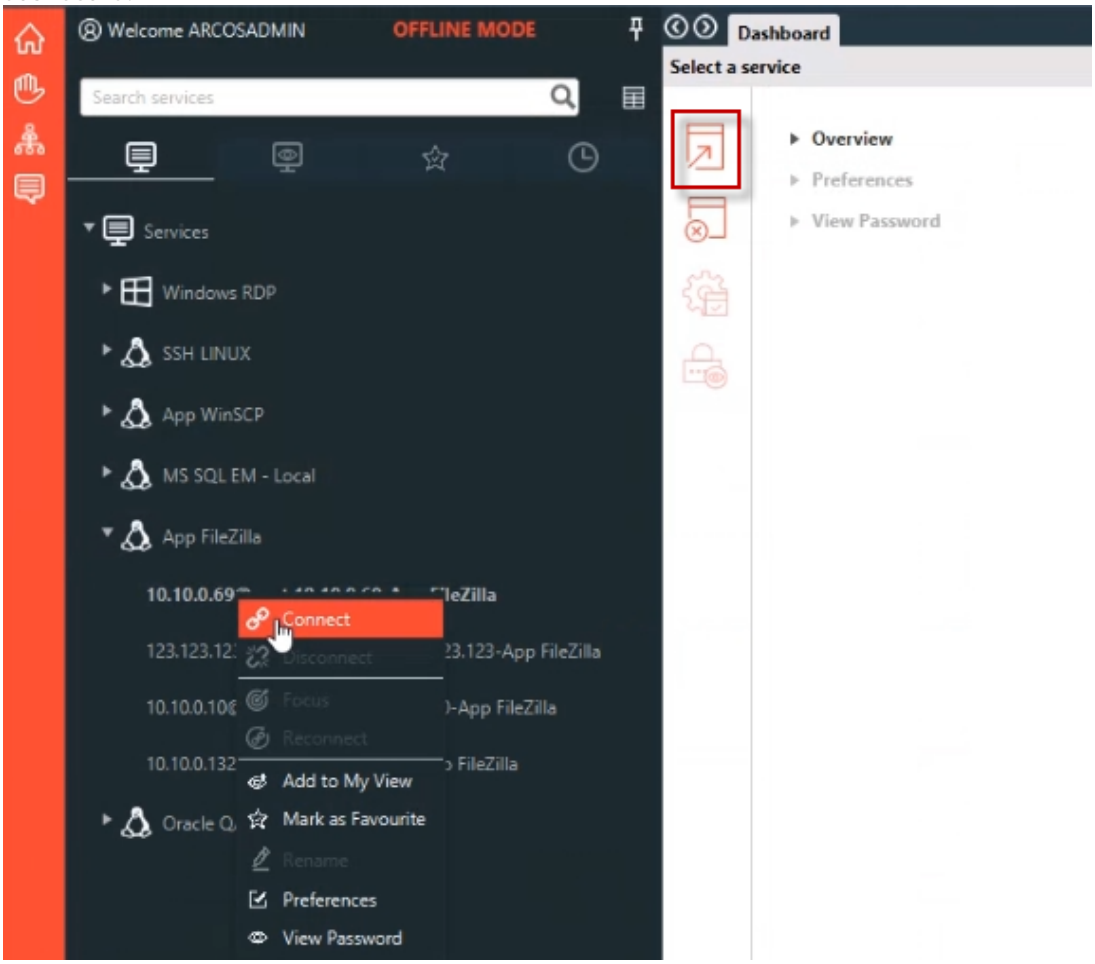
5. Connect to Offline Multitab

The Offline sync service is responsible for syncing the required information for offline access from the ARCOS DB to the local database. In addition to that, it is syncing the generated logs from the local database to the ARCOS DB. Sync will happen as per the execution interval set by the administrator for data sync and log sync. During the offline sync service phase, allow some time as specified in the configuration of the Offline sync service for syncing. Offline API service will check whether the user is able to connect online to PAM API for ARCOS DB. If user is not able to connect to online PAM API for ARCOSDB , then only the user will be able to access the Multitab application in offline mode.

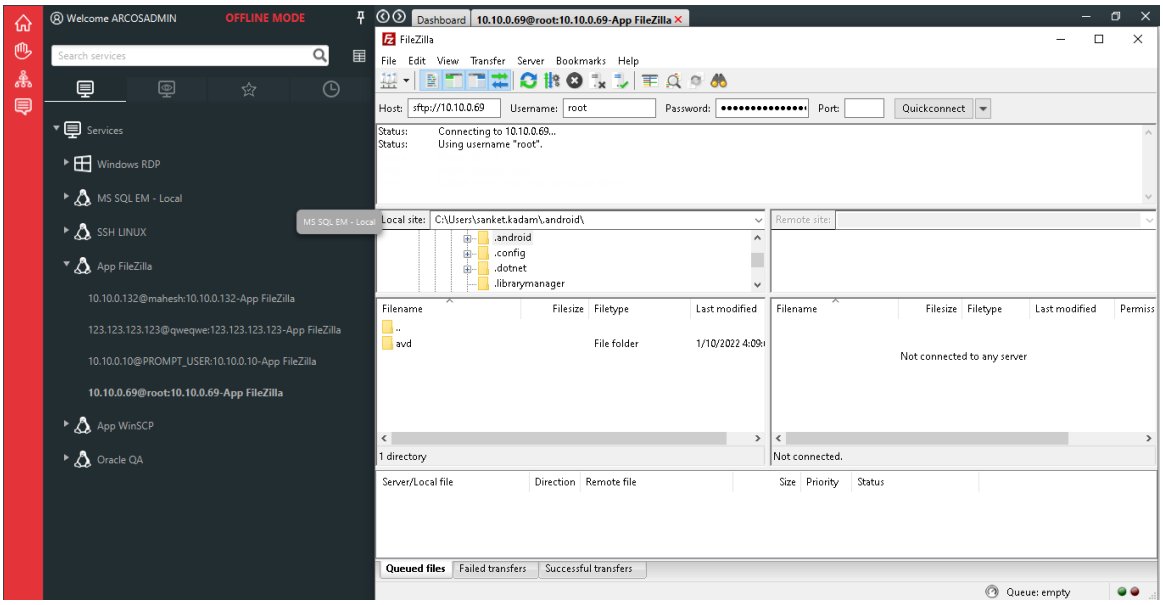
When the Multitab application is launched in offline mode, it validates the credentials of the windows authenticated user with local DB and fetches the offline services approved for the user. All the logs are captured and stored in the user's device and when you connect to the PAM server all the logs are moved from the local database to the PAM database with the help of the Offline sync service.

To access offline services, the user shall perform these steps below:

1. Open the multitab application and navigate to the available service.
2. Right-click on any service and click on the **Connect** button or click on the Open session icon in the dashboard.



3. The user will be able to take offline access for the service as shown below:



4. During the session access, all the logs captured will be captured and stored in local DB. All the log files are stored in encrypted format and cannot be tampered.
5. Depending upon the sync interval time set, all logs will be synced back to Arcos DB and after successful sync the local storage will be cleared.
6. There will be manual sync option in Online Multitab mode in case automatic sync is not operational for some reason.
7. If the Local DB has reached the maximum limit configured then, end user will not be able to take further offline sessions. He/she will have to necessarily sync back to PAM DB first in order to take further sessions.

6. View Logs And Reports

1. In the User Access Logs and Service Access Logs in ACMO Reports, we will be able to identify and check the offline access logs on basis of Connection Type column which will have value equal to Offline.
2. From the Client Manager Privileges Report, we can identify the users who have the privilege of Offline Access.
3. And all the session logs, command logs , service logs, Smart Session Monitoring Logs etc which are usually captured and maintained for normal access will also be maintained for offline access.

Privileged Access Management Suite