12Port for Privileged Access Management

QUICK START GUIDE

Table of Contents

Introduction

Welcome to the 12Port for PAM Quick Start Guide. This guide is designed to help you understand and use the core features of Privileged Access Management with minimal friction. Whether you're new to PAM or just getting started with our platform, this guide will help you navigate the essentials including credential storage, secure access workflows, and password rotation. By the end, you will be ready to manage privileged accounts with confidence and enforce consistent access controls across your environment.

Setup Guidance

To get the most out of your first experience, we recommend approaching this guide as a hands-on companion while working through the product. Use it to explore each feature with a specific goal in mind, such as securing a shared credential or launching a remote session. Focus on real use cases relevant to your environment so you can evaluate how well the platform aligns with your access control needs.

> For more advanced features and deeper walk-through guides, please visit our documentation portal: https://docs.12port.com/

- One physical or virtual server to act as the 12Port host server.
- One physical or virtual server for Remote Access Sessions and Credential Rotation.
    - Optionally, two; one Windows server for RDP and one Linux server for SSH connectivity.
- Open RDP or SSH connectivity between the 12Port host server and the Remote Access Server(s).
- WinRM or SSH service running on all Remote Access servers.
- Valid local test credentials (username and password) to authenticate Remote Sessions and with Administrator rights for remote access and password reset.

Key Concepts

This section introduces core terms used throughout the 12Port for PAM platform. Understanding this vocabulary will help you follow configuration steps, interpret interface labels, and make informed decisions as you begin managing access and credentials.

Assets

An asset is an electronic record describing a network device, an account, or any other physical or logical entity to hold data in a secure way. It could also be a container to logically group other assets for navigation and configuration purposes.

An asset must belong to one of the pre-configured asset types to categorize the asset, to define its metadata requirements and to define the asset behavior. Many other objects like tags, permissions, tasks, and policies are applied to assets to create network micro-segments.

Credential Vault

Credential Vault refers to the secure storage layer responsible for protecting sensitive information such as credentials, private keys, and other authentication data used in remote access and credential management operations. Within the PAM system, the Vault serves as the centralized repository for secrets, ensuring they are encrypted, access-controlled, and auditable.

Remote Access Sessions

Remote Access refers to the authorization framework that governs how users interact with remote endpoints through privileged remote access sessions. Within the PAM module, Access defines the permissions, controls, and methods by which an authorized user may initiate, monitor, or terminate remote sessions to managed assets.

Credential Rotation

Credential Rotation refers to the controlled process of resetting and updating privileged credentials associated with managed assets. As a core function of the PAM system, Rotation helps enforce strong credential hygiene by automating the periodic change of passwords, SSH keys, or other secret material used to authenticate remote systems.

Jobs

Jobs are scheduled or on-demand execution tasks that run predefined actions against managed endpoints. In the context of credential rotation, jobs automate the process of resetting, verifying, or validating privileged account credentials using secure protocols and customizable scripts.

Workflows

A workflow represents a structured sequence of automated or user-driven steps designed to accomplish a specific operational or administrative task. In the context of system orchestration or service management, workflows define how actions are executed, in what order, and under what conditions, ensuring consistency and repeatability across environments.

Auditing and Reporting

Auditing and reports provide visibility into system activity by capturing detailed records of user actions, system events, and policy enforcement across the platform. This functionality supports both operational oversight and compliance requirements by delivering traceable, time-stamped data that can be reviewed, filtered, and analyzed.

Installing the Application

12Port for PAM supports deployment in both Windows and Linux environments. For simplicity, this guide will briefly focus on installation in a Windows or Linux environment. Refer to our online Installation guide for more information about offline installation and software updates.

For trial or test deployments, you can install the software on a laptop or workstation with minimal resources. For Production deployments, use a dedicated server that meets the required specifications. Refer to our System Requirements for details.

Designate one Windows server to host the 12Port for PAM application. Download the Windows installer script **setup.ps1** from (https://bin.12port.com/product/setup.ps1) and save it to a non-temp directory such as **C:\Program Files\12port**. Do not use a temporary directory. Run the script from an elevated PowerShell session and follow the prompts to complete installation and start the 12Port application service.

Designate one Linux server to host the 12Port for PAM application. Download the Linux installer script **setup.sh** from (https://bin.12port.com/product/setup.sh) and save it to a non-temp directory such as **/opt/12port**. Do not use a temporary directory. Run the script using a non-root user and follow the prompts to complete installation and start the 12Port application service.

Initial Setup

After installation, access the 12Port for PAM web interface using a browser on the application server. Navigate to **https://<ztnahost>:6443/ztna**, where <ztnahost> refers to the address of the system running the application. This may be *https://localhost:6443/ztna* or if accessed remotely, a custom domain such as *https://access.contoso.com:6443/ztna*.

On first access, you will be directed to the **Administrator Registration** page. Enter a username and password to create the master Administrator account. This first account will be the first Administrator of the base deployment, have full control over the deployment, and should be secured appropriately.

12Port for PAM supports multitenancy, and all credential and session management take place within an asset tenant. The installation starts with only the base tenant, which is used to create and manage other tenants. You cannot manage credentials or assets directly from the base tenant. After registering this administrator account, you will be prompted to create the first asset tenant so that you can begin managing assets and implementing PAM policies.

Depending on your planned usage, there are several choices to consider on this screen:

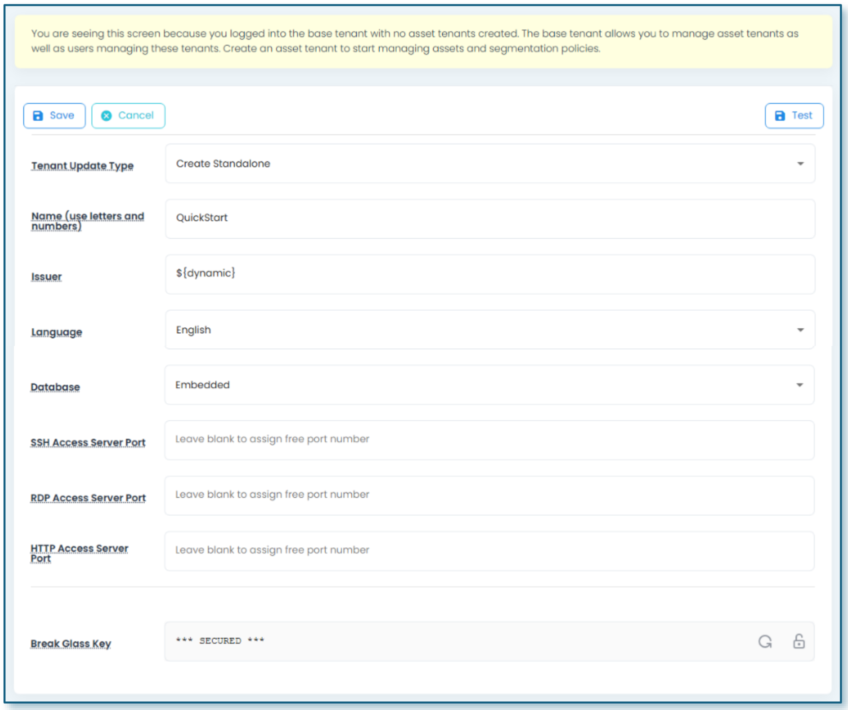
- **Tenant Update Type**: If you are using a single server deployment, choose "Create Standalone."
- **Name**: Enter a descriptive name for the asset tenant. This name will become part of the URL used to access the tenant. Alphanumeric characters only.
- **Issuer**: Issuer, which is usually a tenant URL, identifies a tenant for external parties such as SSO identity providers, browsers, scripts, or applications integrating with this tenant using REST API calls. Tokens and exchange documents that the tenant signs are generated with this unique identifier.
  When using the default *${dynamic}* value, the tenant generates the issuer value based on the URL a client accesses the tenant during the request to use the issuer. The downside of using dynamic issuer generation is that all tokens and exchange

documents generated with a different issuer will be invalid when the tenant is accessed using a different URL.

- **Language**: Select the tenant's default language.
- **Database**: If you would like to use the embedded database included with the application, choose "Embedded." The embedded database is suitable for trials and small-scale test or production deployments. If you would instead like to use an existing standalone database, choose the DBMS variant, and enter your URL and credentials for access.
- **SSH Access Server Port**: Will be used in conjunction with the SSH Proxy service.
- **RDP Access Server Port**: Will be used in conjunction with the RDP Proxy service.
- **HTTP Access Server Port**: Will be used in conjunction with the HTTP Proxy service.

For this Quick Start Guide, we will select the following:

- **Tenant Update Type**: Create Standalone
- **Name**: QuickStart *or another alphanumeric name of your choosing*
- **Issuer**: ${dynamic}
- **Language**: English
- **Database**: Embedded
- **SSH Access Server Port**: leave blank
- **RDP Access Server Port**: leave blank
- **HTTP Access Server Port**: leave blank



You are seeing this screen because you logged into the base tenant with no asset tenants created. The base tenant allows you to manage asset tenants as well as users managing these tenants. Create an asset tenant to start managing assets and segmentation policies.

Tenant Update Type	Create Standalone
Name (use letters and numbers)	QuickStart
Issuer	${dynamic}
Language	English
Database	Embedded
SSH Access Server Port	Leave blank to assign free port number
RDP Access Server Port	Leave blank to assign free port number
HTTP Access Server Port	Leave blank to assign free port number
Break Glass Key	*** SECURED ***

Click **Save** to complete tenant creation. The process may take a few seconds. Once created, you will be redirected into the new tenant and can begin adding assets and managing privileged access.

Guide Overview

In this Quick Start guide, you will work with several foundational components of the 12Port for PAM platform. These include Assets, Users, Permissions, Workflows, Remote Access Sessions, Credential Rotation, and Auditing. Each topic is introduced in a practical context to help you understand the platform's capabilities without requiring deep prior knowledge.

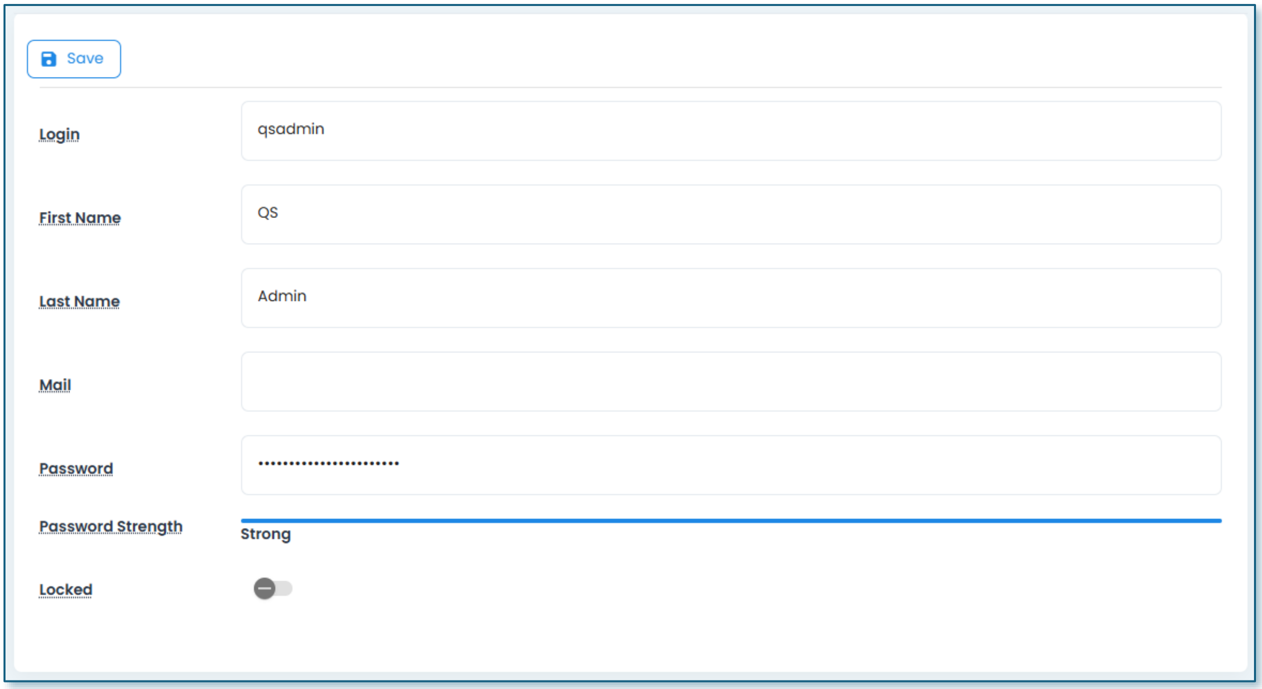
User Account Setup

Once you are redirected into your new *QuickStart* tenant, begin by creating two local tenant user accounts. These local users exist only within the current tenant and cannot be shared across other tenants. One will be assigned the Site Administrator role and used for configuration tasks. The other will represent a standard, non-Admin user experience.

> Local tenant users are created and managed entirely in this tenant and cannot be added, granted, or shared with any other tenant.

To create these local user accounts:

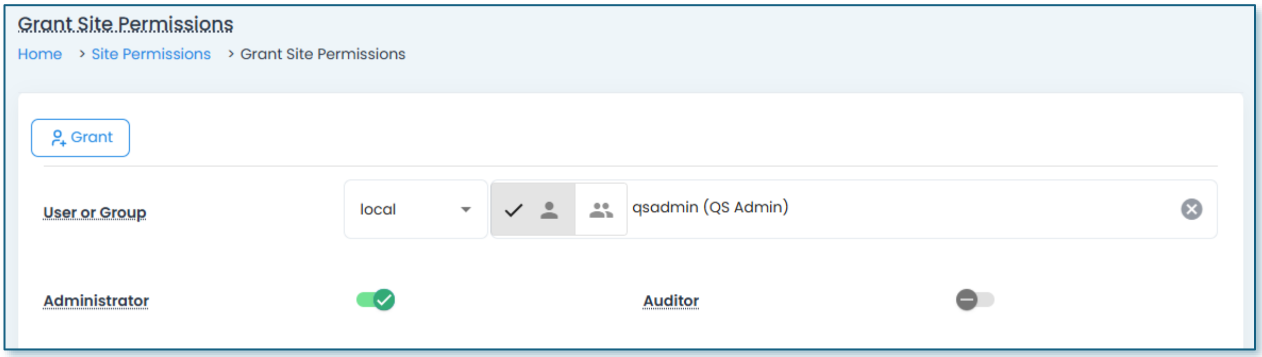
1. Go to **Management > Users** and click **Add**.
2. Fill in the required fields to create the first user account (e.g., qsadmin). This first account will be assigned the Site Administrator role.
3. Repeat the process to create a second account (e.g., qsuser). This account will become our non-Admin user.



Login	qsadmin
First Name	QS
Last Name	Admin
Mail	
Password	•••••••••••••••••••••••••
Password Strength	Strong
Locked	○

After both local user accounts have been created, we will now assign the first user account the Administrator role.

1. Navigate to **Management > Site Roles** and click **Grant**.
2. In the **User or Group** parameter, enter the login name of the first user account.
3. Toggle the **Administrator** option and click **Grant**.


Grant Site Permissions

Home > Site Permissions > Grant Site Permissions

User or Group	local	qsadmin (QS Admin)	
Administrator	✓	Auditor	○

With the Administrator role assigned, the user now has full configuration access within the tenant.

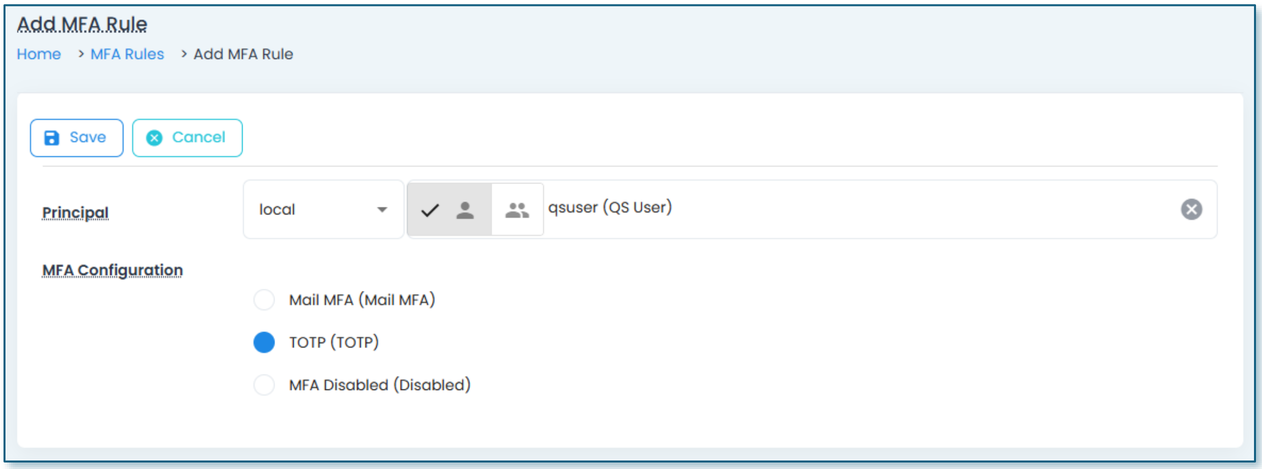
Log out of the tenant using the Master Admin account, then sign in again with the newly created local Admin account to verify the credentials and confirm that the Administrator role is active. The Master Admin account will not be needed for the rest of this guide.

Enabling MFA for User Accounts

Optionally, you can assign an MFA provider to the user to provide extra login. While this is not required, it is recommended to secure access to the 12Port tenant.

To assign MFA:

1. Navigate to **Management > MFA Rules** and click **Add**.
2. In the **Principal** field, enter the login name of your non-Admin account. We will only be assigning MFA to this account, not the Admin account, for this guide. MFA can be assigned to the Admin account later.
3. Select the **TOTP** radio button in the **MFA configuration** section.
4. Click **Save**.



Add MFA Rule

Principal: local | qsuser (QS User)

MFA Configuration

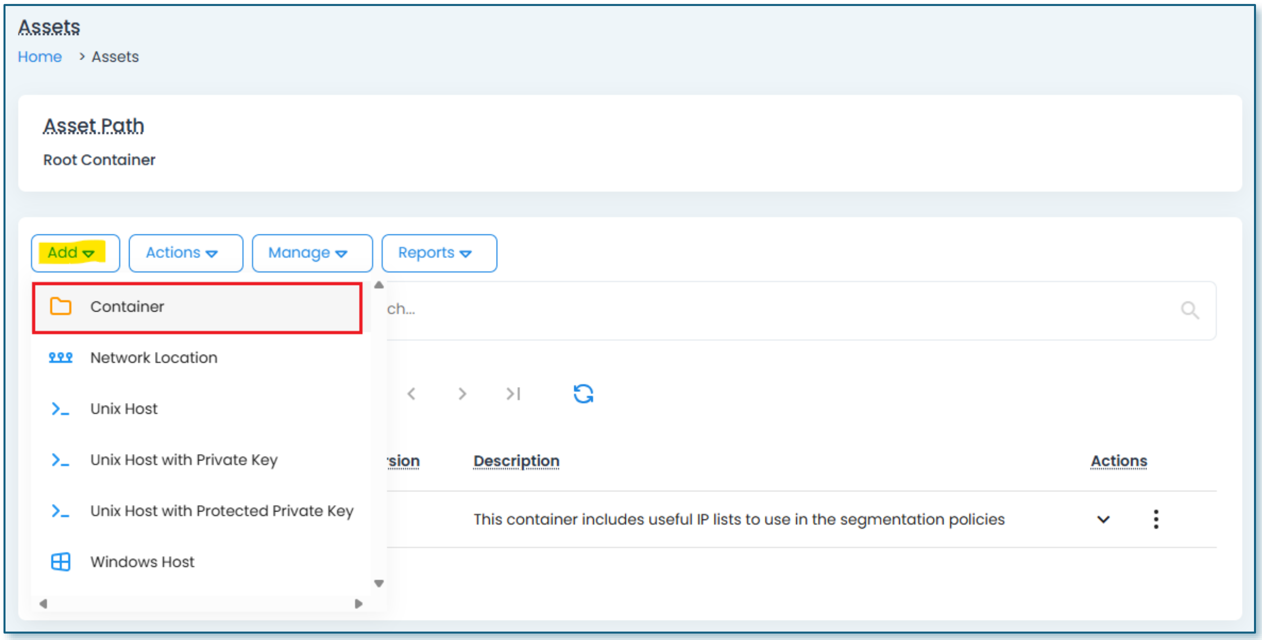
○ Mail MFA (Mail MFA)
● TOTP (TOTP)
○ MFA Disabled (Disabled)

We will register with the MFA provider for this user later in this guide.

Asset Configuration

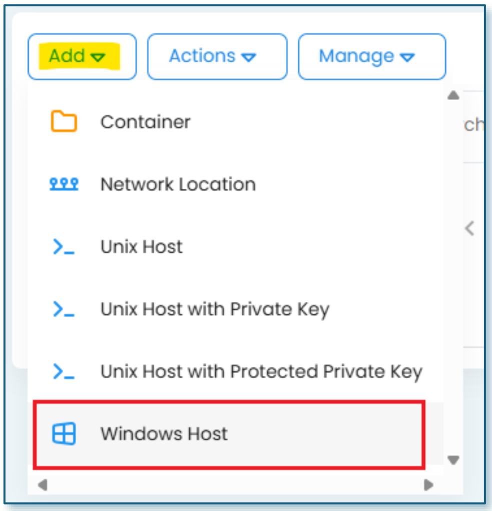
Now that user roles are in place, the next step is to create the Assets. Assets represent servers or endpoints where privileged credentials and access will be controlled.

1. In the left navigation, go to **Database > Assets**.
2. Click **Add > Container** to create a new folder for organizing your assets (e.g., QS Assets).



This container includes useful IP lists to use in the segmentation policies

3. Open the newly created folder.
4. Inside the folder, select **Add > Windows Host** (for a Windows server) or **Add > Unix Host** (for a Linux server) depending on the type of server you are adding.


Add
Actions
Manage
Container
Network Location
Unix Host
Unix Host with Private Key
Unix Host with Protected Private Key
Windows Host

5. Consider the following guidance for this first Asset:
   a. **Name**: Windows Remote Access Server *or* Linux Remote Access Server
   b. **Description**: *optional*

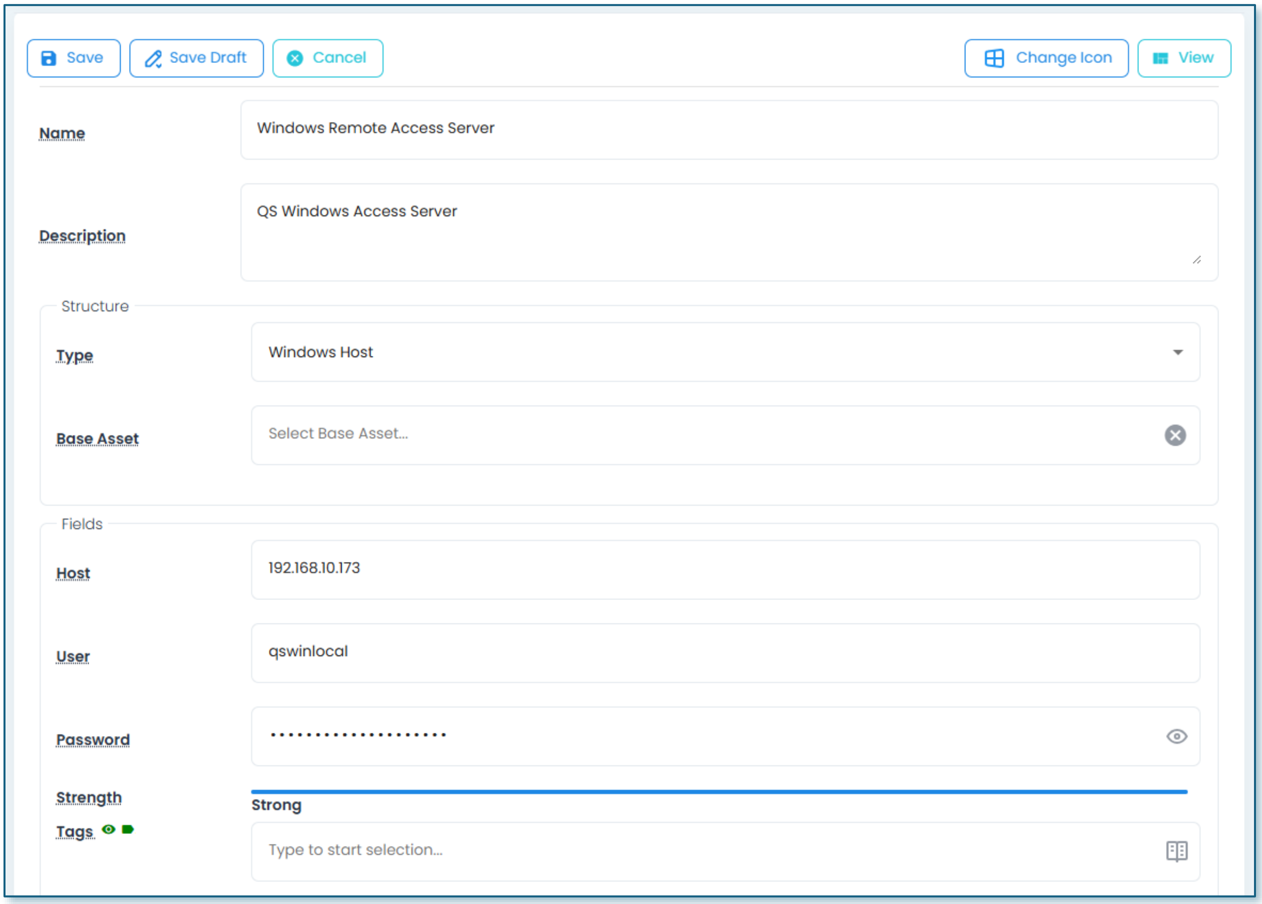
c. **Host**: Enter the IP address or network accessible computer name of your first server. Must be accessible from the 12Port host server.

d. **User**: Enter the username of an account that has Administrator access to the server

e. **Password**: Enter the password of this account

f. **Tags**: *optional*

6. Click **Save** to create the asset.



Name: Windows Remote Access Server

Description: QS Windows Access Server

Structure

Type: Windows Host

Base Asset: Select Base Asset...

Fields

Host: 192.168.10.173

User: qswinlocal

Password: ••••••••••••••••••••

Strength: Strong

Tags: Type to start selection...

If you have a second endpoint to include, repeat the process selecting the proper Asset Type (Windows Host or Unix Host) to create the asset.

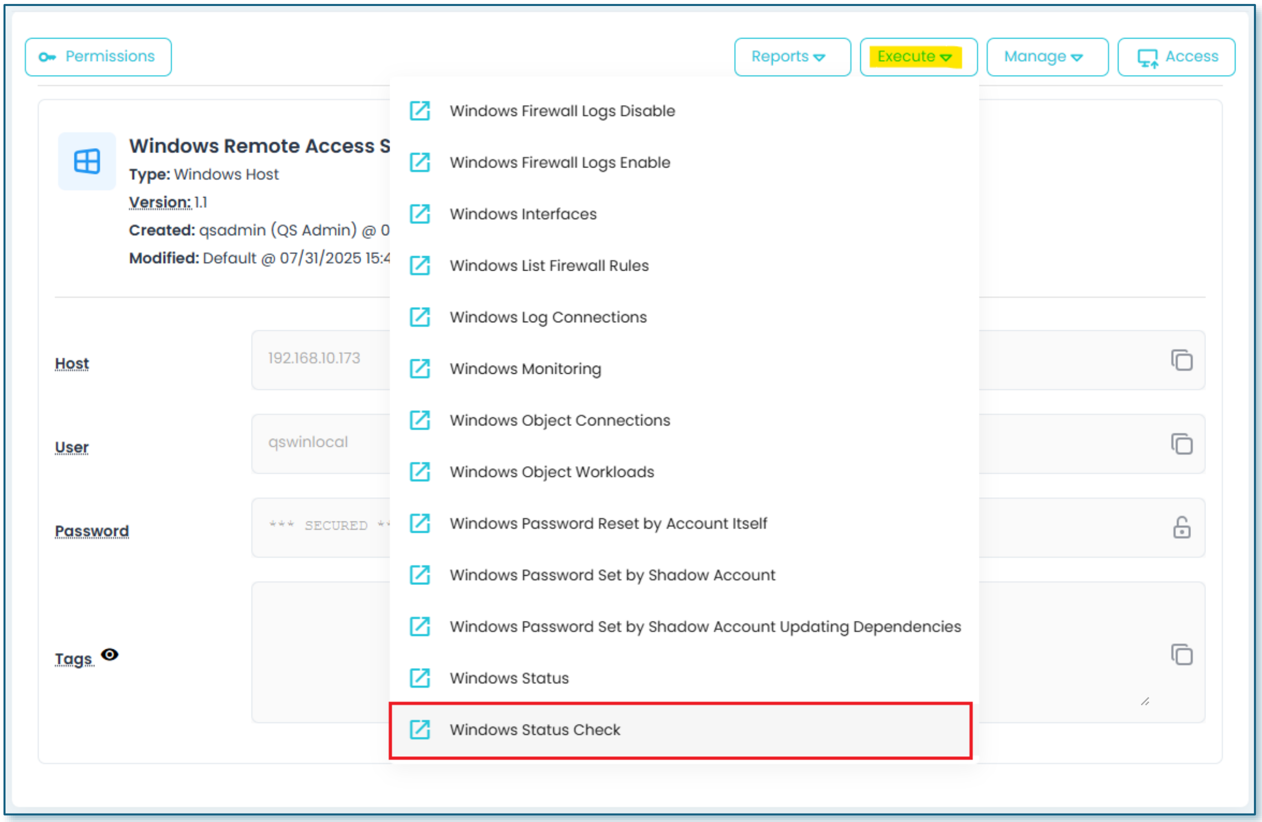
Verifying Asset Connectivity

Before continuing, verify that 12Port can connect to each server asset and authenticate using the provided credentials.

Windows-based remote job execution requires the **WinRM service to be enabled and running** on the target endpoint. Before executing a task, make sure that WinRM is active and that the account defined in the asset is a member of either the local **Administrators** group or the **Remote Management Users** group on the remote machine, as these permissions are necessary for successful WinRM execution.

You can use the PowerShell command ***winrm quickconfig*** to enable the service or contact your IT administrator for assistance.

1. In the folder, click the name of the server asset (Windows or Linux) to open its view page.
2. Open the **Execute** dropdown and select **Windows Status Check** or **Unix Status Check**, depending on the asset type.



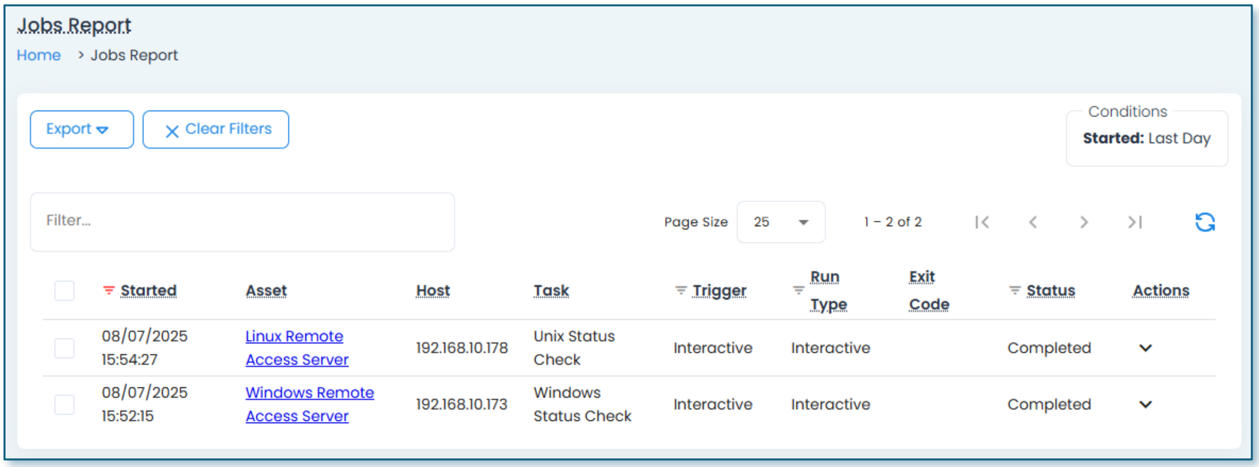
Permissions
Reports
Execute
Manage
Access
Windows Firewall Logs Disable
Windows Firewall Logs Enable
Windows Interfaces
Windows List Firewall Rules
Windows Log Connections
Windows Monitoring
Windows Object Connections
Windows Object Workloads
Windows Password Reset by Account Itself
Windows Password Set by Shadow Account
Windows Password Set by Shadow Account Updating Dependencies
Windows Status
Windows Status Check

Windows Remote Access S
Type: Windows Host
Version: 1.1
Created: qsadmin (QS Admin) @ 0
Modified: Default @ 07/31/2025 15:4

Host 192.168.10.173
User qswinlocal
Password *** SECURED **
Tags

3. Confirm the action when prompted.
4. Repeat this for any other server assets that were created.
5. After a brief period, use the left side menu to navigate to **Reports > Jobs**. From this report, each asset should have a corresponding entry confirming a *Completed* status. The presence of these report entries, and the information contained in the

details, confirms the connectivity from 12Port was successful to each of these assets.



Conditions
Started: Last Day

Page Size 25

	Started	Asset	Host	Task	Trigger	Run Type	Exit Code	Status	Actions
□	08/07/2025 15:54:27	Linux Remote Access Server	192.168.10.178	Unix Status Check	Interactive	Interactive		Completed	⌄
□	08/07/2025 15:52:15	Windows Remote Access Server	192.168.10.173	Windows Status Check	Interactive	Interactive		Completed	⌄

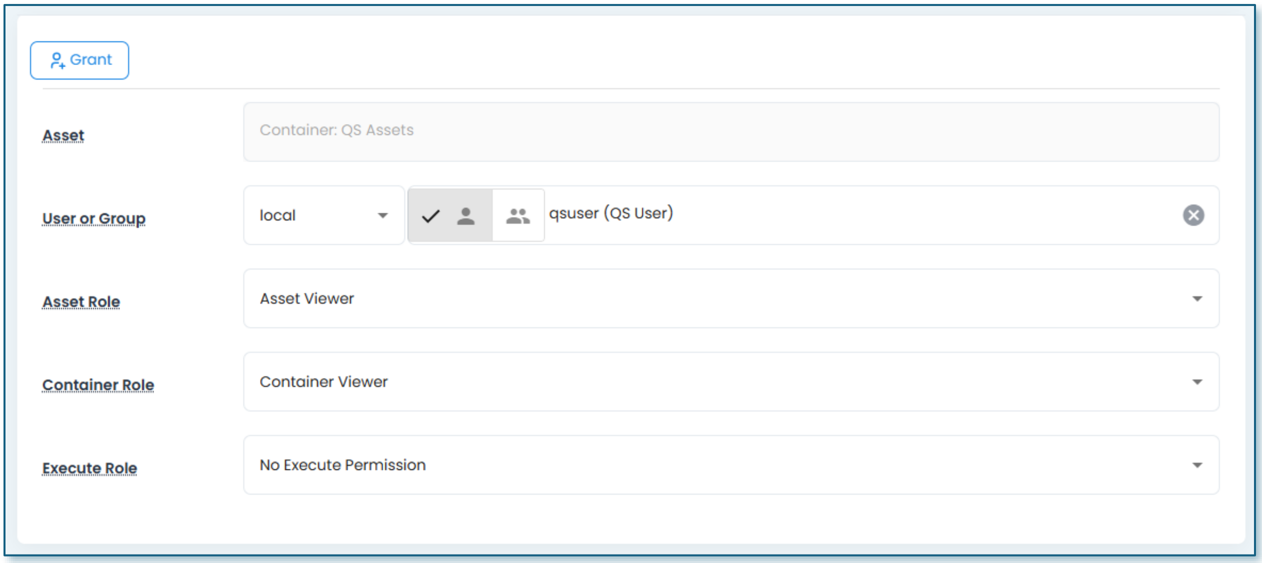
If an entry in the Jobs report has a status other than Completed, review the Troubleshooting section of the Documentation Portal for further assistance with Job failures.

Configuring Asset Permissions

Next, we grant the non-Admin local user access to the assets via its parent container. This user will not receive a Site Role. Instead, permissions will be limited to only what is necessary for working with the assets in a typical PAM scenario.

To assign permissions:

1. In the Assets library, open the folder we created earlier.
2. Select **Manage > Permissions** and click **Make Unique**. This will break the permission inherited from the folder parent and allow us to customize them on this container (and its child assets through inheritance) only.
3. Click **Grant**.
4. In **User or Group**, enter the login name of our non-Admin local user account.
5. Assign the following permissions:
    a. **Asset Role**: Asset Viewer
    b. **Container Role**: Container Viewer
    c. **Execute Role**: No Execute Permission
6. Click **Grant** to apply.



Asset: Container: QS Assets

User or Group: local ✓ qsuser (QS User)

Asset Role: Asset Viewer

Container Role: Container Viewer

Execute Role: No Execute Permission

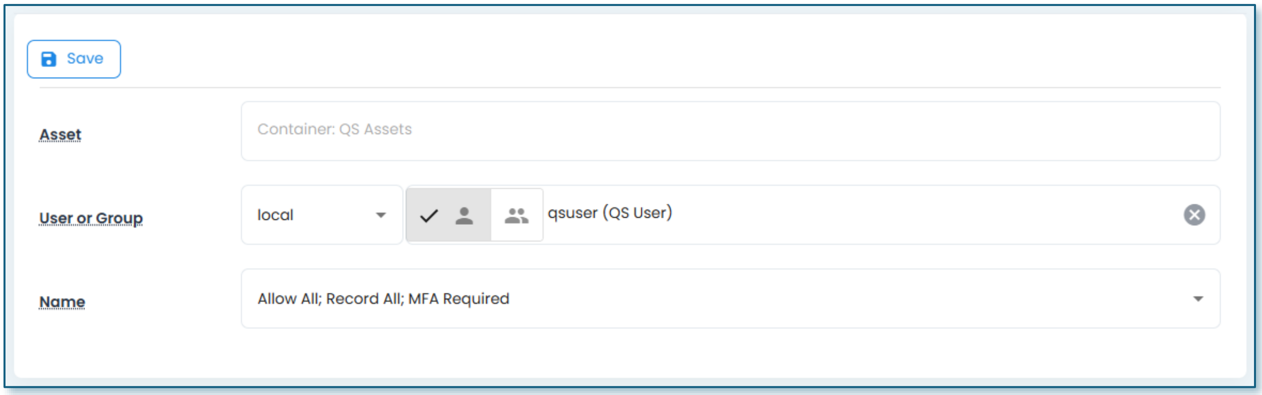
This configuration provides the least required access for the non-Admin user to interact with the asset structure without allowing overly elevated actions.

Enabling Session Access

Access Profiles are required for non-Admin users to start remote sessions with managed assets. These profiles define the session type and restrictions, including whether recording is enabled and if file transfer is allowed. Without an assigned Access Profile, a non-Admin user cannot start a session.

To assign an Access Profile:

1. In the Assets library, open the folder we created earlier.
2. Go to **Manage > Access Profiles** and click **Add**.
3. For **User or Group**, enter the login name of the non-Admin local user created earlier.
4. In **Name**, select the default profile **Allow All, Record All, MFA Required**.
5. Click **Save**.



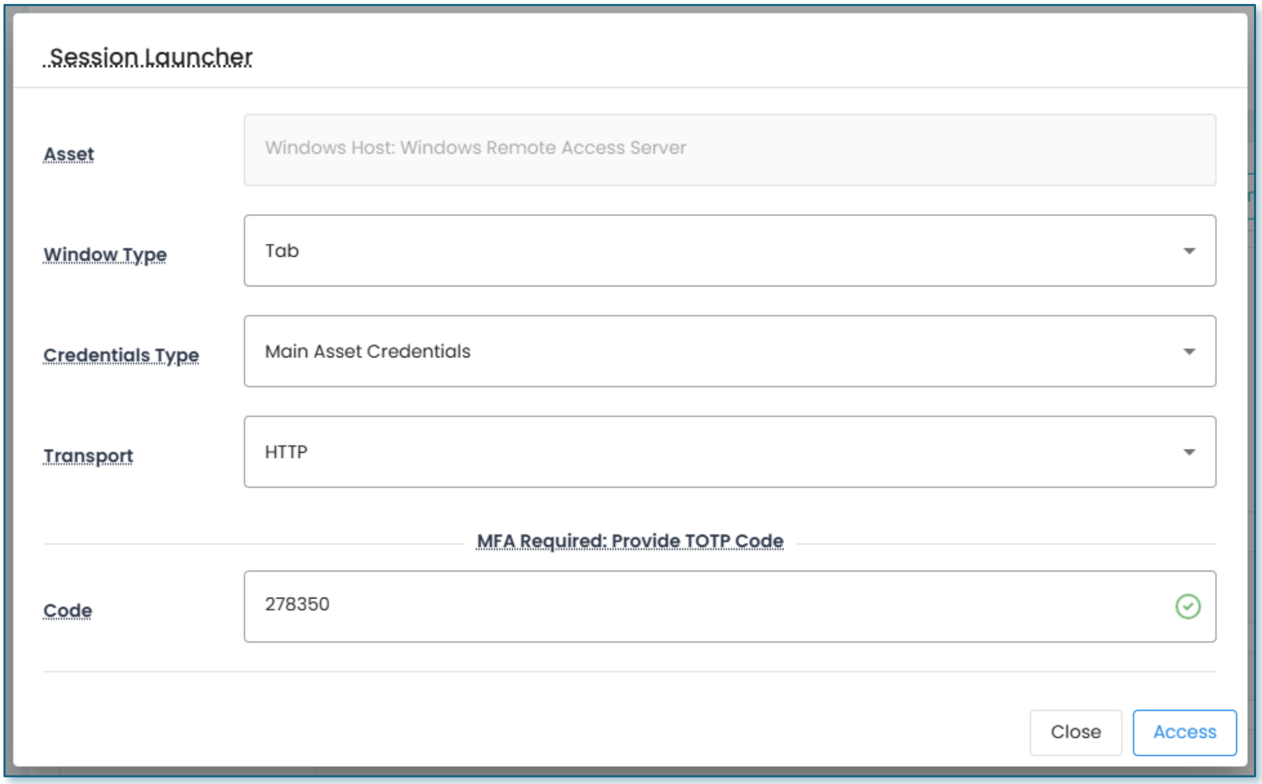
Asset	Container: QS Assets
User or Group	local ✓ qsuser (QS User)
Name	Allow All; Record All; MFA Required

This grants the user full remote access features (*Allow All*), with session recording (*Record All*), and MFA enforcement (*MFA Required*), ensuring both full functionality and security during access.

Launching Remote Access Sessions

With configuration complete, you can now test a Remote Access Session using the non-Admin account.

1. Open a private browser window and login to the 12Port web portal using the non-Admin account.
2. If prompted, enroll your mobile device app for TOTP MFA. Skip this step if MFA is not required.
3. Navigate to **Database > Assets** and open the folder.
4. The user should see all the assets created earlier.
5. Open one of the assets by clicking on its name.
6. Note that only the **Access** button is available. All other options are hidden or disabled, compared to the Admin user, due to the limited permissions we configured earlier.
7. Click **Access** to launch the Session Launcher prompt.
8. In the Session Launcher, adjust settings if needed, or continue with the default values.
9. If MFA is required, enter the TOTP token in the **Code** field and click the green **Checkmark** to confirm.
10. Click **Access** to begin the session.



Session Launcher

Asset: Windows Host: Windows Remote Access Server

Window Type: Tab

Credentials Type: Main Asset Credentials

Transport: HTTP

MFA Required: Provide TOTP Code

Code: 278350

Once connected, interact with the host using the asset defined credentials. Perform typical actions such as typing, clipboard use, or file transfers to generate session activity. When done, disconnect or sign off using the endpoint's native controls.

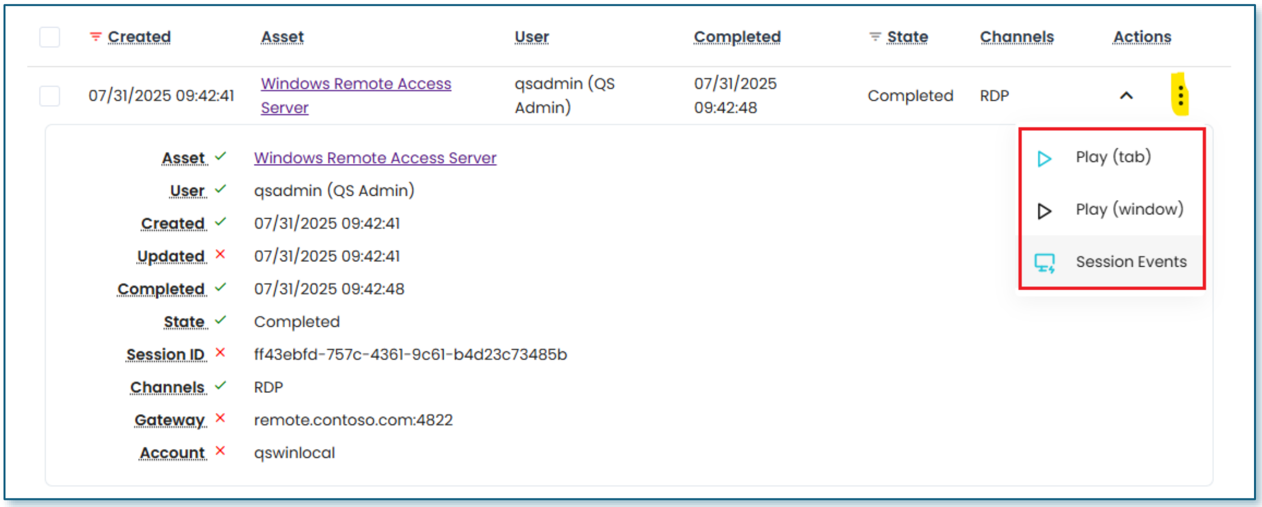
If there are other created assets in the folder, repeat this process to start the session for each.

Auditing: Review Session Activity

After completing a session with the non-Admin user, you can audit the session activity from the Administrator account.

1. Return to the browser where the Administrator user is logged in.
2. Navigate to **Reports > Sessions**.
3. Locate the recently completed session in the list.
4. Click the expansion arrow to view the session details.
5. Use **Actions > Play (tab)** or **Actions > Play (window)** to launch the recorded session video playback in a new tab or browser window.
6. Close the playback tab or window after reviewing.

7. Select **Actions > Sessions Events** to view recorded session events such as Keyboard input, Clipboard copy, or File Transfer. For any file transfer events (File Upload or File Download), click the file name to download a copy.



	Created	Asset	User	Completed	State	Channels	Actions
□	07/31/2025 09:42:41	Windows Remote Access Server	qsadmin (QS Admin)	07/31/2025 09:42:48	Completed	RDP	

Asset	✓	Windows Remote Access Server
User	✓	qsadmin (QS Admin)
Created	✓	07/31/2025 09:42:41
Updated	×	07/31/2025 09:42:41
Completed	✓	07/31/2025 09:42:48
State	✓	Completed
Session ID	×	ff43ebfd-757c-4361-9c61-b4d23c73485b
Channels	✓	RDP
Gateway	×	remote.contoso.com:4822
Account	×	qswinlocal

If multiple sessions were performed, each can be reviewed from this report.

Alternatively, you can view an Asset's own Session report by navigating to this Asset and opening its **Reports > Sessions** report.

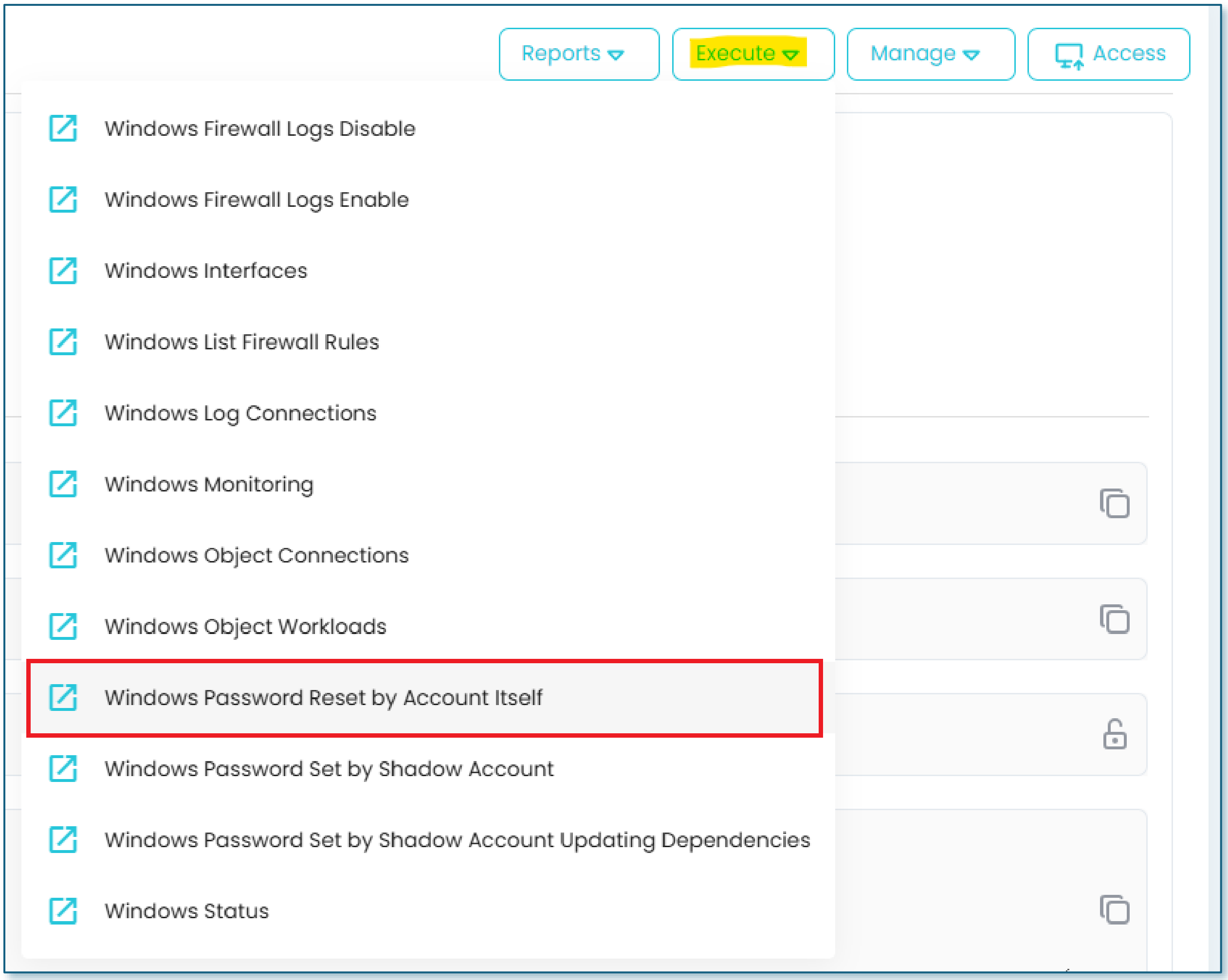
Rotating Credentials

Credential rotation is a core function of PAM that helps reduce risk by regularly updating passwords on managed endpoints. For this guide, we will use the out of the box, default configuration. Advanced option configurations such as scheduled or policy-based automated rotations are available in the Documentation Portal.

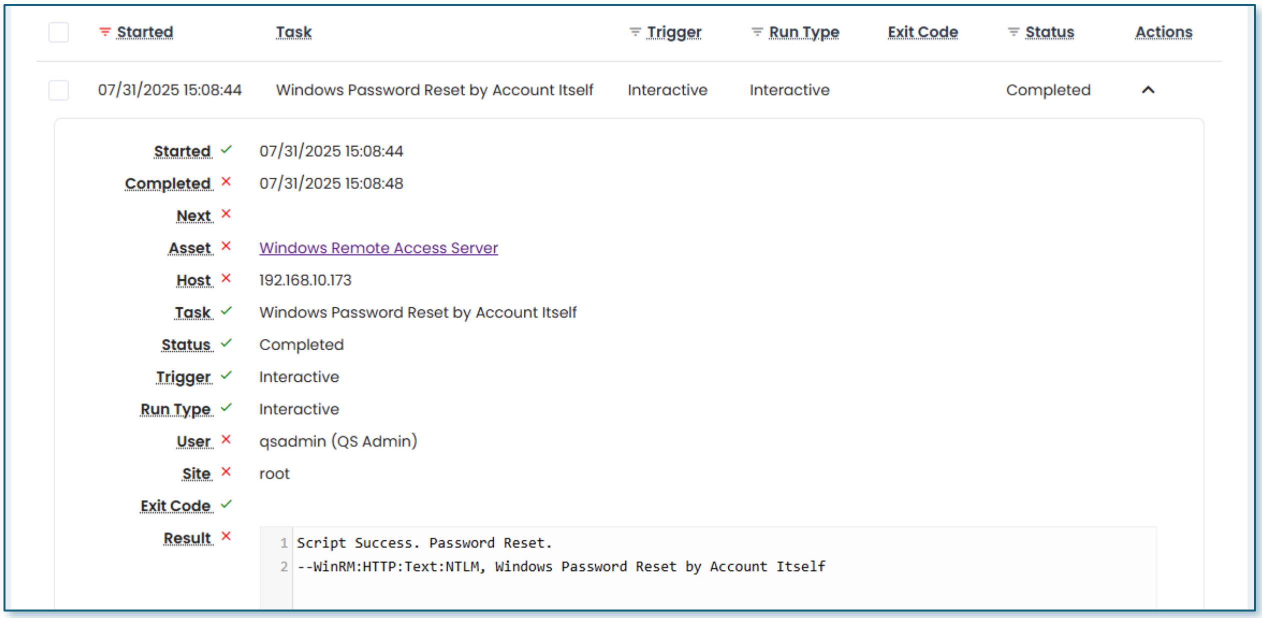
Since credential rotation requires elevated permissions, we will use the Administrator account for this task.

To perform a rotation:

1. Return to the browser where the Administrator user is logged in.
2. Navigate to **Database > Assets** and open the folder.
3. Open one of the earlier created assets by clicking on its name.
4. From the **Execute** menu, select:
   a. **Windows Password Reset by Account Itself** (for a Windows asset)
   b. **Unix Password Reset by Account Itself** (for a Linux asset)


Reports
Execute
Manage
Access
Windows Firewall Logs Disable
Windows Firewall Logs Enable
Windows Interfaces
Windows List Firewall Rules
Windows Log Connections
Windows Monitoring
Windows Object Connections
Windows Object Workloads
Windows Password Reset by Account Itself
Windows Password Set by Shadow Account
Windows Password Set by Shadow Account Updating Dependencies
Windows Status

5. Click **Ok** on the confirmation dialog to continue with the Password reset operation.
6. Navigate to **Reports > Jobs** to monitor the rotation task.
7. Once the job status is *Completed*, use the **Show Details** arrow under the **Actions** menu to view more details.



□	Started	Task	Trigger	Run Type	Exit Code	Status	Actions
□	07/31/2025 15:08:44	Windows Password Reset by Account Itself	Interactive	Interactive		Completed	^

Started	✓	07/31/2025 15:08:44
Completed	✗	07/31/2025 15:08:48
Next	✗	
Asset	✗	Windows Remote Access Server
Host	✗	192.168.10.173
Task	✓	Windows Password Reset by Account Itself
Status	✓	Completed
Trigger	✓	Interactive
Run Type	✓	Interactive
User	✗	qsadmin (QS Admin)
Site	✗	root
Exit Code	✓	
Result	✗	

```
Script Success. Password Reset.
--WinRM:HTTP:Text:NTLM, Windows Password Reset by Account Itself
```

8. Return to the Asset **View** page, unlock the **Password** field, and verify that the password value has changed.
9. Click **Access** to start a session using the updated password and confirm the connection is successful.

Repeat the process for other assets as needed.

To see all executed jobs across the site, visit **Reports > Jobs** for a full history.

If an entry in the Jobs report has a status *Failed*, review the Troubleshooting section of the Documentation Portal for further assistance with Job failures.

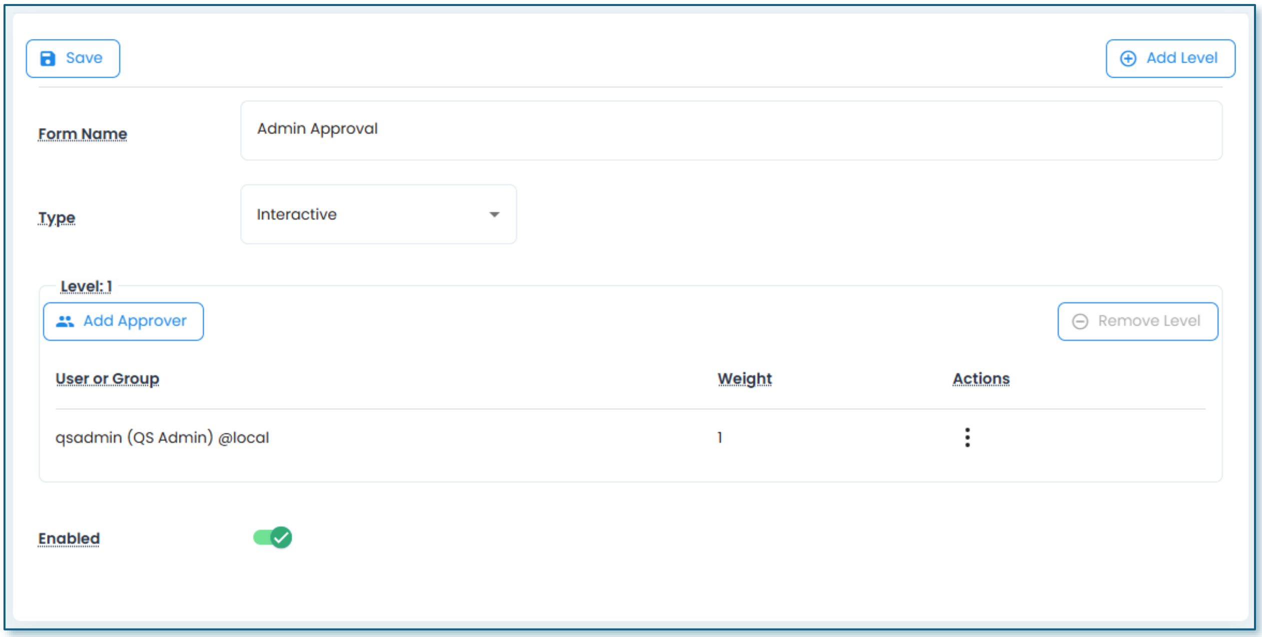
Configuring Access Approvals (Workflows)

Optionally, workflows allow you to require approval before certain actions, such as remote access or password unlocks, are performed. In this guide, we'll configure a workflow where the non-Admin user must submit a request for remote access, which the Administrator must approve.

To begin, we must first create a Workflow Form, which dictates who the submitted requests are sent to for Approval.

Step 1: Create a Workflow Form:

1. Return to the browser where the Administrator user is logged in.
2. Navigate to **Management > Workflow Forms** and click **Add**.
3. Configure the form as follows:
    a. **Form Name**: Enter a unique, but recognizable name.
    b. **Type**: select **Interactive**
    c. Click **Add Approver,** enter the Administrator user account in the **User or Group** field and Click **Select.**
    d. Enable the form by toggling the **Enabled** switch.
4. Click **Save.**



Form Name: Admin Approval

Type: Interactive

Level: 1

User or Group	Weight	Actions
qsadmin (QS Admin) @local	1	⋮

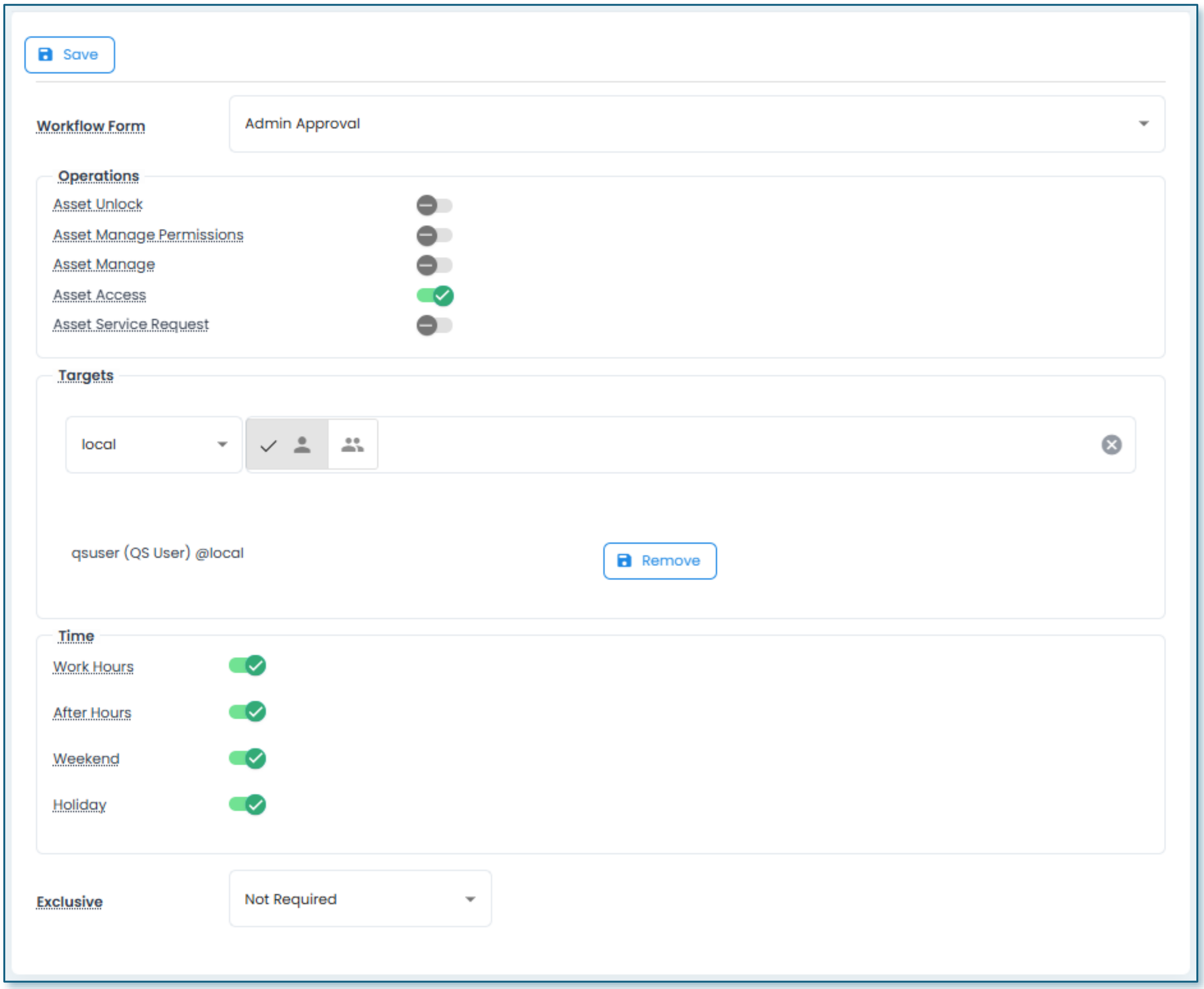
Enabled: ✓

Next, we must apply the Workflow Selector to the required assets and conditions.

Step 2: Apply Workflow Selector to the Assets

1. Navigate to **Database > Assets** and open the folder.
2. Select **Manage > Workflow Selectors** and click **Add**.
3. Create the Selector:
    a. **Workflow Form**: Choose the **Form Name** created above.
    b. **Operations**: *Toggle* **Asset Access**
    c. **Targets**: Enter the non-Admin user account
    d. **Time**: *Toggle* all options
    e. **Exclusive**: Select **Not Required**

4. Click **Save**.



Workflow Form: Admin Approval

Operations

- Asset Unlock ☐
- Asset Manage Permissions ☐
- Asset Manage ☐
- Asset Access ☑
- Asset Service Request ☐

Targets

local

qsuser (QS User) @local

Time

- Work Hours ☑
- After Hours ☑
- Weekend ☑
- Holiday ☑

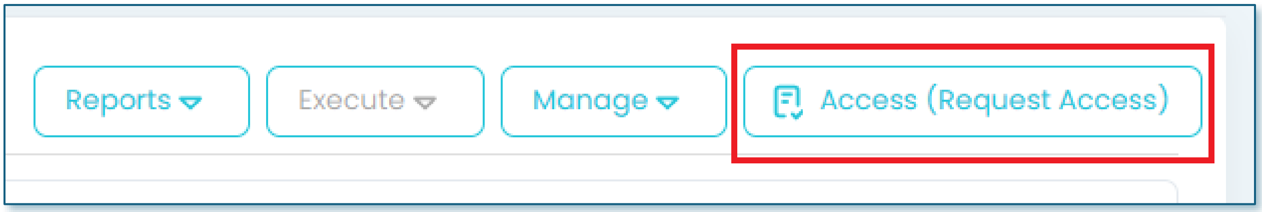
Exclusive: Not Required

Step 3: Executing the Workflow

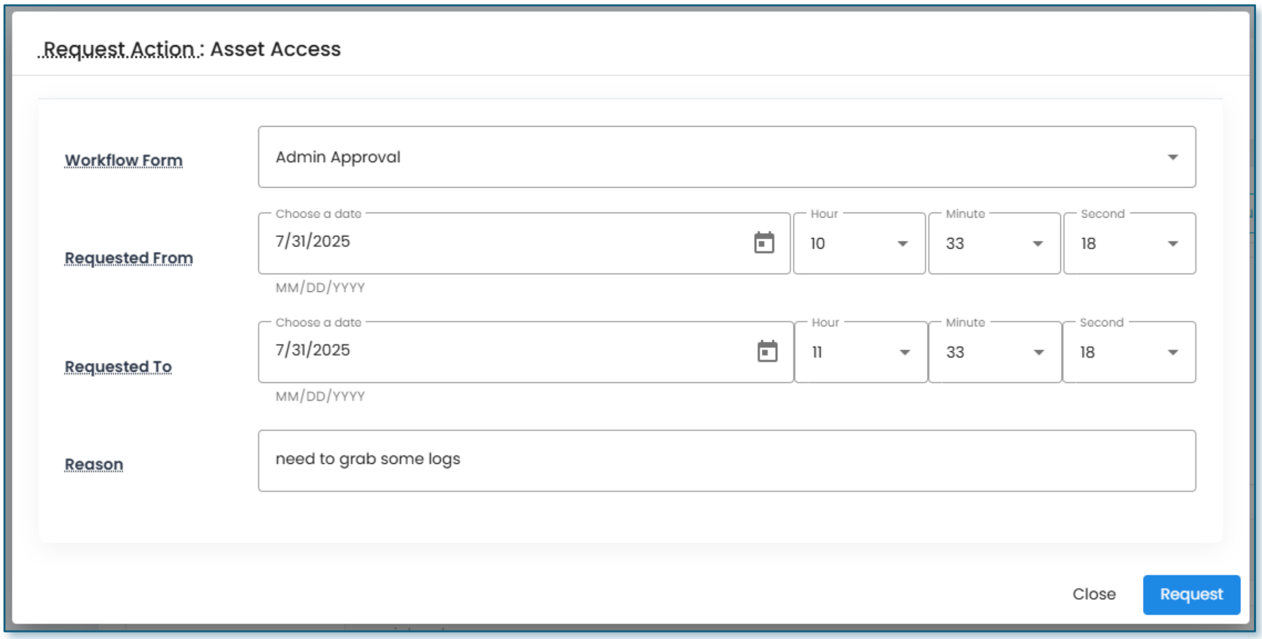
With the configuration now complete, we will use our non-Admin user to submit the request for Access. Be sure that you have both users logged into the 12Port web portal using a normal and a private session. We will be switching between both during this procedure.

Non-Admin User:

1. From the *non-Admin user*, navigate to **Database > Assets** and open the folder.
2. Click an asset name to open it and confirm the earlier **Access** button now reads **Access (Request Access)**, indicating the presence of a workflow requirement.



3. Click **Access (Request Access)**.
4. In the *Request Action: Asset Access* form:
    a. **Workflow Form**: Select the **Workflow Name** created earlier.
    b. **Requested From**: leave default, which is current time.
    c. **Requested To**: leave default (+1 hour) or adjust to the length of time access is requested. Be sure it is later than the *Request From* time.
    d. **Reason**: Enter the reason you are requesting access.
    e. Click **Request**.



Request Action : Asset Access

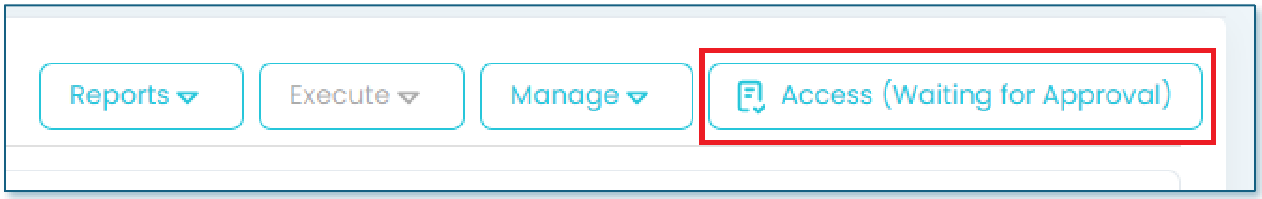
Workflow Form: Admin Approval

Requested From: Choose a date 7/31/2025 (MM/DD/YYYY) Hour 10 Minute 33 Second 18

Requested To: Choose a date 7/31/2025 (MM/DD/YYYY) Hour 11 Minute 33 Second 18

Reason: need to grab some logs

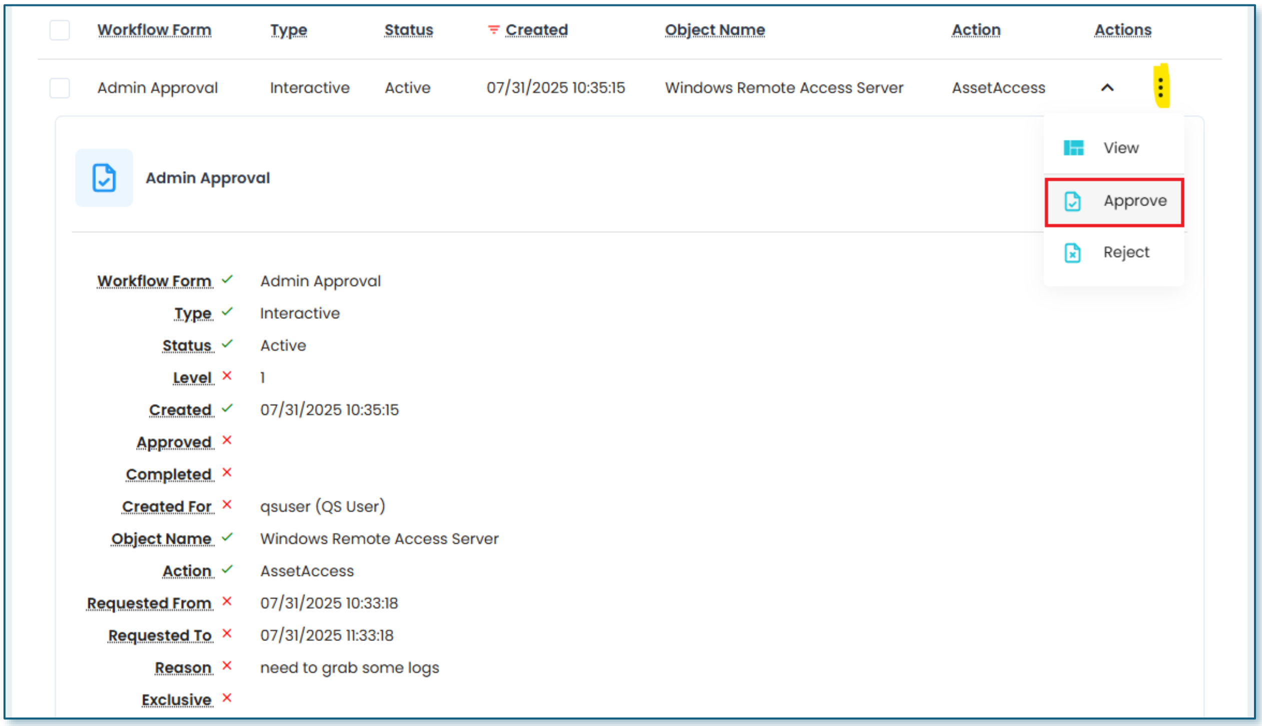
5. The **Access (Request Access)** button is now updated to read **Access (Waiting for Approval)** while the workflow approval is pending.



With the non-Admin user request submitted, we turn our attention to the Administrator user that will review and approve (or reject) this request.

Administrator User:

1. Return to the browser where the Administrator user is logged in.
2. Navigate to **My Profile > Approver List**.
3. Locate the submitted request in the list and review the requested details using the expansion arrow to *Show Details*.
4. Select **Actions > Approve** to approve this request or **Actions > Reject** to reject the request. If the request is rejected, then the non-Admin user must submit a new request for Access approval.
5. Approved or Rejected requests are removed from the *Approver List* queue.



□	Workflow Form	Type	Status	Created	Object Name	Action	Actions
□	Admin Approval	Interactive	Active	07/31/2025 10:35:15	Windows Remote Access Server	AssetAccess	^ ⋮

Admin Approval

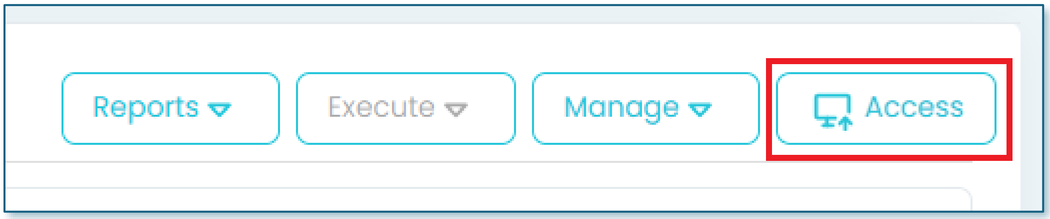
Workflow Form	✓	Admin Approval
Type	✓	Interactive
Status	✓	Active
Level	×	1
Created	✓	07/31/2025 10:35:15
Approved	×	
Completed	×	
Created For	×	qsuser (QS User)
Object Name	✓	Windows Remote Access Server
Action	✓	AssetAccess
Requested From	×	07/31/2025 10:33:18
Requested To	×	07/31/2025 11:33:18
Reason	×	need to grab some logs
Exclusive	×	

With the request now *Approved*, we can return to our non-Admin user.

Non-Admin User:

1. Return to the browser where the non-Administrator user is logged in.
2. Navigate back to the asset where the request was submitted or refresh the page if you are still there.
3. The **Access (Waiting for Approval)** button now reads **Access**.
4. Click **Access** to open the Session Launcher and begin the session.

5. **Disconnect** to end the session.



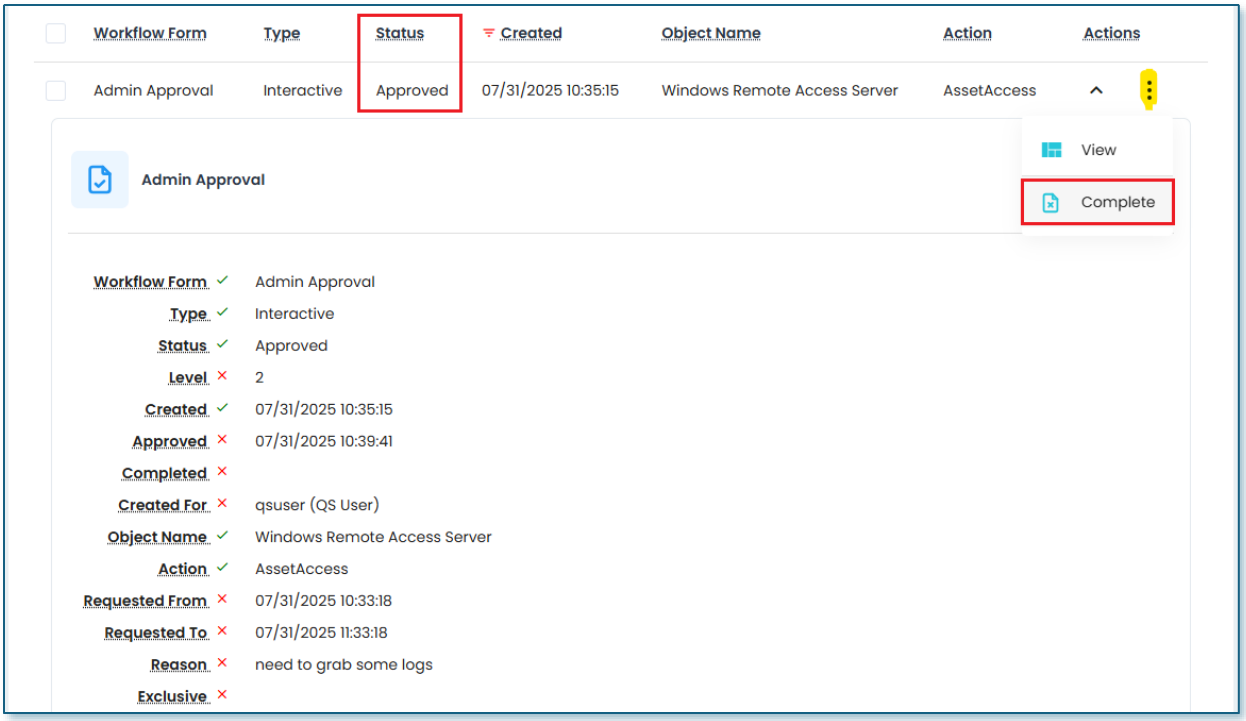
Alternatively, this user can monitor the status of all their submitted requests from their **My Profile** > **My Requests** page.

- For *Active* workflow requests, the user may use the **Actions** > **Delete** option to cancel and remove this pending request.
- For *Approved* workflow requests, the user may use the **Actions** > **Complete** option to conclude the approved workflow where time remains.

This completes the workflow process from request submission to request approval to the remote access session start.

Auditing Workflow Requests

The Administrator can go to **Reports** > **Action Requests** to view all submitted workflows. Each entry shows the workflow's current state, Active, Approved, Rejected, or Completed. Use the **Actions** > **Complete** option to end an approved workflow immediately, if needed.



□	Workflow Form	Type	Status	Created	Object Name	Action	Actions
□	Admin Approval	Interactive	Approved	07/31/2025 10:35:15	Windows Remote Access Server	AssetAccess	⋮

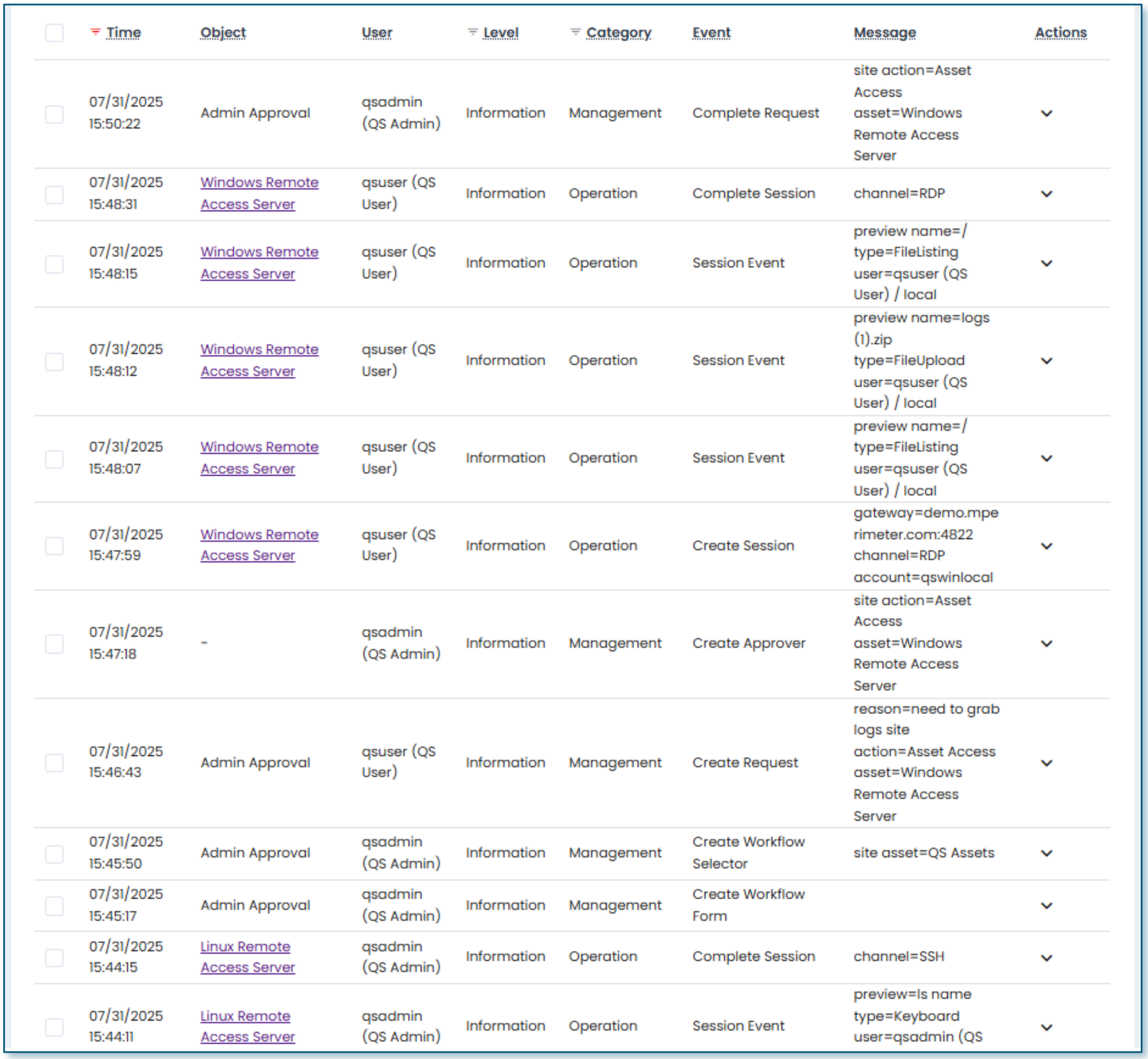
Admin Approval

Workflow Form	✓	Admin Approval
Type	✓	Interactive
Status	✓	Approved
Level	✗	2
Created	✓	07/31/2025 10:35:15
Approved	✗	07/31/2025 10:39:41
Completed	✗	
Created For	✗	qsuser (QS User)
Object Name	✓	Windows Remote Access Server
Action	✓	AssetAccess
Requested From	✗	07/31/2025 10:33:18
Requested To	✗	07/31/2025 11:33:18
Reason	✗	need to grab some logs
Exclusive	✗	

1. Click the **Actions > Complete** option to end the non-Admins approved workflow.
2. Return to the browser session of the non-Admin user and observe the **Access** button has once again returned to **Access (Request Access)** because their approved workflow is now complete.

Event Audit Logging

To review audit activity, the Administrator can navigate to **Reports > Events**. This report captures all site actions performed throughout the use of 12Port. Spend time exploring this view and its available actions, as the Event report is central to monitoring, compliance, and ongoing audit visibility across the platform.



☐	Time	Object	User	Level	Category	Event	Message	Actions
☐	07/31/2025 15:50:22	Admin Approval	qsadmin (QS Admin)	Information	Management	Complete Request	site action=Asset Access asset=Windows Remote Access Server	⌄
☐	07/31/2025 15:48:31	Windows Remote Access Server	qsuser (QS User)	Information	Operation	Complete Session	channel=RDP	⌄
☐	07/31/2025 15:48:15	Windows Remote Access Server	qsuser (QS User)	Information	Operation	Session Event	preview name=/ type=FileListing user=qsuser (QS User) / local	⌄
☐	07/31/2025 15:48:12	Windows Remote Access Server	qsuser (QS User)	Information	Operation	Session Event	preview name=logs (1).zip type=FileUpload user=qsuser (QS User) / local	⌄
☐	07/31/2025 15:48:07	Windows Remote Access Server	qsuser (QS User)	Information	Operation	Session Event	preview name=/ type=FileListing user=qsuser (QS User) / local	⌄
☐	07/31/2025 15:47:59	Windows Remote Access Server	qsuser (QS User)	Information	Operation	Create Session	gateway=demo.mperimeter.com:4822 channel=RDP account=qswinlocal	⌄
☐	07/31/2025 15:47:18	-	qsadmin (QS Admin)	Information	Management	Create Approver	site action=Asset Access asset=Windows Remote Access Server	⌄
☐	07/31/2025 15:46:43	Admin Approval	qsuser (QS User)	Information	Management	Create Request	reason=need to grab logs site action=Asset Access asset=Windows Remote Access Server	⌄
☐	07/31/2025 15:45:50	Admin Approval	qsadmin (QS Admin)	Information	Management	Create Workflow Selector	site asset=QS Assets	⌄
☐	07/31/2025 15:45:17	Admin Approval	qsadmin (QS Admin)	Information	Management	Create Workflow Form		⌄
☐	07/31/2025 15:44:15	Linux Remote Access Server	qsadmin (QS Admin)	Information	Operation	Complete Session	channel=SSH	⌄
☐	07/31/2025 15:44:11	Linux Remote Access Server	qsadmin (QS Admin)	Information	Operation	Session Event	preview=ls name type=Keyboard user=qsadmin (QS	⌄

Quick Start Completion Overview

You've reached the end of the Quick Start Guide and completed the essential steps to begin managing privileged access with 12Port for PAM. Here's a quick summary of what you accomplished:

1. Installed the application and initialized your first tenant.
2. Created local user accounts and assigned proper roles, permissions, and MFA rules.
3. Added managed server assets and confirmed connectivity.

4. Configured asset-level access permissions and assigned an Access Profile to a non-Admin user.
5. Started and completed a secure, recorded remote access session.
6. Audited session activity through video playback and event logs.
7. Performed a credential rotation to update and confirm password changes.
8. Optionally implemented and tested a workflow approval process for session requests.

You now have a working foundation of 12Port for PAM and have seen its key features in action. For more advanced topics, configuration options, integrations, or troubleshooting guidance, visit our Documentation Portal.

Next Steps and Support

This guide introduced the essential features of 12Port for PAM and walked you through a functional setup from installation to access control and auditing. If you have any questions, encounter issues, or need further guidance beyond what’s covered here, reach out to our support team at **support@12port.com**. We're here to help.