



Examples

FortiPAM 1.9.0



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



May 4, 2026

FortiPAM 1.9.0 Examples

74-190-1245222-20260504

TABLE OF CONTENTS

Change Log	9
Introduction	10
FortiToken and FortiToken Mobile	11
2FA with FortiToken Mobile	11
Adding a FortiToken to FortiPAM	11
Configuring a local user with FortiToken as the authentication type	12
Enabling FortiToken Mobile push notification	14
Results	14
Setting up FortiToken Mobile	14
RADIUS authentication	17
2FA on FortiPAM for RADIUS users using FortiAuthenticator	17
Configuring a RADIUS server on FortiPAM	17
Creating remote user group on FortiPAM	19
Enabling 2FA on FortiAuthenticator	19
Creating a RADIUS user on FortiPAM	20
Results	21
SAML authentication	23
2FA on FortiPAM for SAML users using FortiAuthenticator	23
Importing FortiAuthenticator certificate to FortiPAM	23
Configuring FortiAuthenticator as a SAML IdP	24
Configuring FortiPAM as an SP	26
Creating a remote user group on FortiPAM	27
Creating a SAML user on FortiPAM	28
Results	29
JWT	30
JWT (JSON Web Token) integration with DevOps	30
Integrating FortiPAM and GitLab- GUI	31
Integrating FortiPAM and GitLab- CLI	32
Integrating FortiPAM and Jenkins- CLI	35
ZTNA	39
ZTNA endpoint control on FortiPAM	39
Configuring EMS on FortiPAM	39
Registering the endpoint PC to EMS server	41
Configuring a ZTNA server on FortiPAM	44
Configuring proxy rule on FortiPAM	45
Adding a ZTNA tag to a secret for launching control	46
Secret configurations	47
Accessing a Linux server using PuTTY	47
Creating a secret with Unix template	47
Launching a secret for the Linux server	48
Accessing a Cisco router using PuTTY	48
Creating an associated secret	48
Creating a secret with Cisco User (SSH Secret) template	49
Launching a secret for the Cisco router	51

Accessing a FortiGate using PuTTY, Web SSH, or the Web launcher	52
Creating a secret with Unix template	52
Launching a secret for the FortiGate	53
Accessing a Windows server using the Remote Desktop- Windows launcher	54
Creating a secret with Windows Machine template	54
Launching a secret for the Windows server	55
Visiting a web application/platform using web launchers	55
Installing Fortinet Privileged Access Agent web extension on Chrome/Edge	56
Creating a secret for general web application/platform	57
Creating a secret for AWS root/IAM account	57
Visiting web application/platform using web launcher	59
Reviewing video recording for the web launching session	59
Reviewing secret log for the web launching session	60
Accessing a generic machine using Web VNC, VNC Viewer, or the TightVNC launcher	61
Creating a secret with Machine template	61
Launching a secret for the machine	62
Accessing a target server using locally installed WinSCP client	62
Installing WinSCP on a local machine	63
Creating a secret with Unix Account (SSH Password) template	63
Launching a secret for the target server using the WinSCP launcher	64
Accessing an SFTP server using the Web SFTP secret launcher	64
Creating a secret with Unix Account (SSH Password) template	65
Launching a secret for the SFTP server using the Web SFTP launcher	66
Accessing an SMB server using Web SMB launcher	66
Creating a secret with Windows Domain Account (Samba) template	67
Verifying the password	68
Launching a secret for the SMB server using the Web SMB launcher	69
Checking out and checking in a secret	69
Creating a secret with check out enabled	70
Checking out a secret	71
Checking in a secret	72
Using a secret requiring approval	72
Creating an approval profile	72
Creating a secret with mandatory approval requirement	73
Sending a request to access a secret	74
Approving a secret request	75
Launching a secret that requires approval	76
Running a script on a target server using jobs	77
Creating a job approval profile	77
Creating a secret with mandatory approval requirement for launching a job	78
Creating an ssh script type job	79
Sending a request to access the job	80
Approving a job request	81
Results	82
Configuring a secret that supports TOTP	83
Configuring a secret template with TOTP	83
Creating a secret with TOTP enabled	85
Accessing a MySQL server using MySQL CLI launcher	86

Creating a secret using the database server template	86
Launching a secret for the MySQL server	87
Configuring integrity check for the PuTTY launcher	88
Creating an entry for the PuTTY launcher	88
Enabling integrity check in the launcher and secret template	89
Creating a secret with integrity check	90
Launching the secret	91
Block uploading a JavaScript file via the Web SFTP launcher	92
Configuring the DLP file pattern	92
Configuring a DLP sensor profile	93
Creating a secret with a DLP sensor profile	94
Results	95
Block transferring .exe files and log file downloads of size larger than 500KB	95
Configuring the DLP file pattern	96
Configuring a DLP sensor profile	96
Creating a secret with a DLP sensor profile	98
Results	99
Updating a service account credential	99
Updating a service account credential	99
Creating a secret with the Certificate Vault template	101
Creating a certificate secret	102
Setting up email alert for certificate expiry	102
Configuring a secret using the Target Only secret template	103
Example 1: Creating a secret using the Target Only template	103
Example 1: Launching the secret	104
Example 2: Creating a secret using the Target Only template	105
Example 2: Launching the secret	106
Smart association for Windows AD server as the target	106
Creating a secret with Windows Domain Account as the secret template	107
Creating a remote user	108
Results	109
Access multiple Windows servers on the same domain	110
Creating targets	110
Creating a secret for the domain user	112
Creating a secret for the Windows PC- 10.59.112.201 and Windows PC- 10.59.112.208	112
Sharing secrets to a contractor	113
Result	115
Azure AD password changer	115
Requirements	115
Configuring the Azure portal	115
Configuring FortiPAM	117
Results	118
Troubleshooting	119
Audit	120
Sponsored administrator audits secret activities	120
Creating a sponsored group	120
Creating a sponsor admin	121

Creating a secret with view permission for the sponsored group	122
Creating sponsored group members	123
Auditing	125
Web proxy	126
Configuring the web proxy feature to prevent web credentials from leaking	126
Enabling the web proxy feature	126
Creating a secret target with web proxy	127
Creating a secret with web proxy	128
FortiPAM behind a FortiGate device	129
RDP log retrieval	131
RDP log retrieving on FortiPAM	131
Creating an event filter profile	131
Creating a secret policy	132
Creating a secret target	132
Creating secret with an RDP event filter profile	133
Launching the secret	134
Checking the RDP logs	135
Gateway	136
FortiPAM connects to a target through a FortiProxy acting as the gateway	136
Creating the FortiProxy gateway	136
Creating the secret target on FortiPAM	137
FortiProxy related configurations	137
Configuring FortiPAM/FortiGate as the reverse gateway	138
Configuring the reverse service on FortiPAM (control plane)	140
Configuring reverse service on the gateway (control plane)	140
Configuring traffic proxy on the gateway for forwarding secret launch (traffic plane)	141
Configuring a gateway entry on FortiPAM server for secret launch (traffic plane)	144
Configuring a target using reverse gateway on the FortiPAM server	146
Creating a secret for the target that uses the FortiPAM reverse gateway	147
Launching the FortiPAM secret	148
Creating a secret for the target that uses the FortiGate reverse gateway	149
Launching the FortiGate secret	150
Troubleshooting	150
Configuring FortiGate forwarding access request from FortiPAM to the private target	152
Configuring forward gateway on FortiGate	152
Configuring a gateway on the FortiPAM server	155
Configuring a target using the forward gateway on FortiPAM server	156
Creating a secret for the target	156
Launching the secret from the FortiPAM server	157
Monitoring the secret	158
Troubleshooting	158
Accessing a private target using secret gateway chaining	159
Prerequisites	159
Topology	159
Configure Reverse Service on the root FortiPAM (Upstream Device)	160
Configuring the downstream connection on Service Gateway/Reverse Gateway	161
Verifying the dynamic gateway discovery	162
Configuring a target using the Reverse Gateway (fortipam_gw2)	162

Creating and launching a secret	163
Results	163
Troubleshooting	163
SSH filter profiles	166
Configuring an SSH filter profile on FortiPAM to restrict SSH access to secret servers ...	166
Configuring SSH filter profiles in the CLI	166
Configuring SSH filter profiles using the GUI	167
Automation	174
Using default automation stitch- Secret Credential View	174
Using the Secret Credential View automation stitch	174
Results	175
Customizing an automation stitch	175
Creating an automation trigger	175
Create an action	177
Creating a stitch	178
Results	179
Windows application filter	180
Creating a Windows application filter to prevent running executables	180
Setting up WinRM on the remote server	180
Creating a target with server information as Windows	180
Creating a Windows application filter profile	181
Creating a privileged account secret	183
Creating a non-privileged account	184
Launching the secret	186
Creating a non-Windows application filter to prevent running executables	188
Creating a target with server information as non-Windows	188
Creating a non-priviledged secret	189
Web launcher	192
Using web launcher to auto fill credentials on a website	192
Creating a secret template	192
Creating a secret to connect to FortiAuthenticator	196
Launching the secret	196
Log and video disks	198
Back up and restore your log and video files	198
Enabling maintenance mode on FortiPAM	198
Backing up videos to the FTP server	199
Backing up logs to the FTP server	199
Shutting down the FortiPAM-VM and change log and video disks	200
Restoring videos from the FTP server	200
Restoring logs from the FTP server	201
Certificate management	203
Configuring certificate using the ACME protocol to access a FortiPAM instance	203
Creating a certificate	203
Configuring the FortiPAM SSL certificate	207
How to deploy FortiPAM CA to Windows host using EMS and FortiClient	207
Deploying FortiPAM CA using EMS	208

Avoiding the web browser warning on the FortiPAM GUI	209
Downloading FortiPAM CA from the FortiPAM GUI	211
Logging servers	212
FortiAnalyzer Cloud as a logging server	212
Registering FortiAnalyzer Cloud	212
Deploying a FortiAnalyzer Cloud instance	213
Add FortiPAM to FortiAnalyzer Cloud instance	215
Enabling FortiAnalyzer Cloud in FortiPAM	215
Launching a secret	217
FortiGate	218
FortiPAM behind FortiGate	218
Configuring a VIP on FortiGate for FortiPAM access	218
Configuring ZTNA on FortiGate for FortiPAM access	220
Results	225

Change Log

Date	Change Description
2026-05-04	Initial release.

Introduction

This document serves as a reference guide to common FortiPAM 1.9 configuration and deployment scenarios. The scope of this document is to explain specific examples and include information required for those examples to work. The examples rely on the other documents to provide full product information.



For further FortiPAM related information, refer to the *FortiPAM Administration Guide* available on the Fortinet Docs Library.

This section includes configuration examples for FortiPAM 1.9:

- [FortiToken and FortiToken Mobile on page 11](#)
- [RADIUS authentication on page 17](#)
- [SAML authentication on page 23](#)
- [JWT on page 30](#)
- [ZTNA on page 39](#)
- [Secret configurations on page 47](#)
- [Audit on page 120](#)
- [Web proxy on page 126](#)
- [RDP log retrieval on page 131](#)
- [Gateway on page 136](#)
- [SSH filter profiles on page 166](#)
- [Automation on page 174](#)
- [Windows application filter on page 180](#)
- [Web launcher on page 192](#)
- [Log and video disks on page 198](#)
- [Certificate management on page 203](#)
- [Logging servers on page 212](#)
- [FortiGate on page 218](#)

FortiToken and FortiToken Mobile

This section describes various authentication scenarios involving FortiToken and FortiToken Mobile.

2FA with FortiToken Mobile

In this example, you set up a local FortiPAM user to use 2FA with FortiToken Mobile to log in to FortiPAM.

To set up 2FA with FortiToken Mobile:

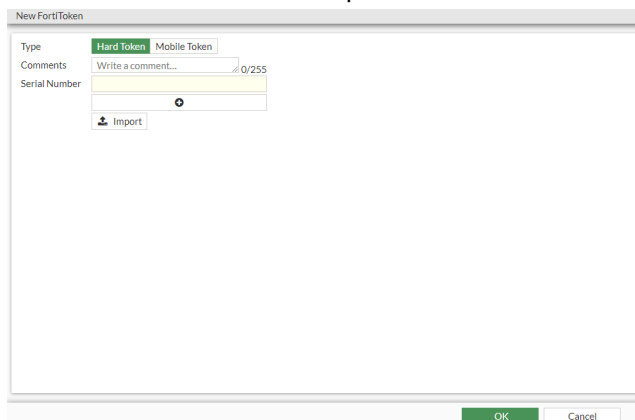
1. [Adding a FortiToken to FortiPAM on page 11](#)
2. [Configuring a local user with FortiToken as the authentication type on page 12](#)
3. [Enabling FortiToken Mobile push notification on page 14](#)
4. [Results on page 14](#)

Additionally, see [Setting up FortiToken Mobile on page 14](#).

Adding a FortiToken to FortiPAM

To add a FortiToken Mobile token:

1. Go to *User Management > FortiTokens*, and select *Create New*.
The *New FortiToken* window opens.



The screenshot shows a 'New FortiToken' dialog box. At the top, there are two tabs: 'Hard Token' and 'Mobile Token', with 'Mobile Token' selected. Below the tabs, there is a 'Comments' field with the placeholder text 'Write a comment...' and a character count '0/255'. Underneath is a 'Serial Number' field, which is currently empty. Below the 'Serial Number' field, there is an 'Import' button with a download icon. At the bottom of the dialog, there are 'OK' and 'Cancel' buttons.

2. Select the *Type* as *Mobile Token*.
3. In *Activation Code*, enter the FortiToken activation code.
4. Click *OK*.

Configuring a local user with FortiToken as the authentication type

To configure a local user:

1. Go to *User Management > User Definition*, and select *Create*.
The *New User Definition* wizard is launched.
2. In *Choose a User Role type*, select *Administrator*, and from the *Choose an Administrator Role* dropdown, select *Super Administrator*.

New User Definition

1 2 3 4 5 6
Configure Role Configure Type Configure User Details Two Factor Authentication Configure Trusted Hosts and Schedule Review

Choose a User Role type

Guest User
Guest users are created for demonstration purposes. It can only view secrets and has very restricted access to different features.

Standard User
Standard users are created for any users who has basic access to secrets. It has the ability to make request, claiming ownership for secrets that requires checkout etc.

Power User
Power users are created for managing general settings of secrets. For example, they can change who could approval secrets, the commands that are blocked on the target server etc.

Administrator
Staff Administrators used for configuring the FortiPAM, and managing access to privileged resources. An example is an IT staff member, who manages the access of Standard Users, or approves requests.

Choose an Administrator Role:

Previous Next Cancel

3. Click *Next*.
4. In *Choose a User type*, select *Local User*.

New User Definition

1 2 3 4 5 6
Configure Role Configure Type Configure User Details Two Factor Authentication Configure Trusted Hosts and Schedule Review

Choose a User type

Local User
A user which has their information configured and stored on the FortiPAM.

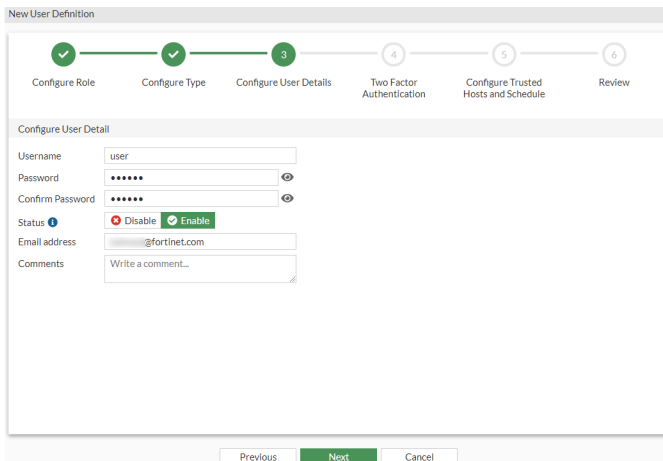
API User
API User can only access FortiPAM by using a token via the REST API instead of GUI.

Remote User
A user which has their information configured and stored on a remote server. Check this option if you want to enable login for one remote user in a remote group, and assign them this role for their FortiPAM session.

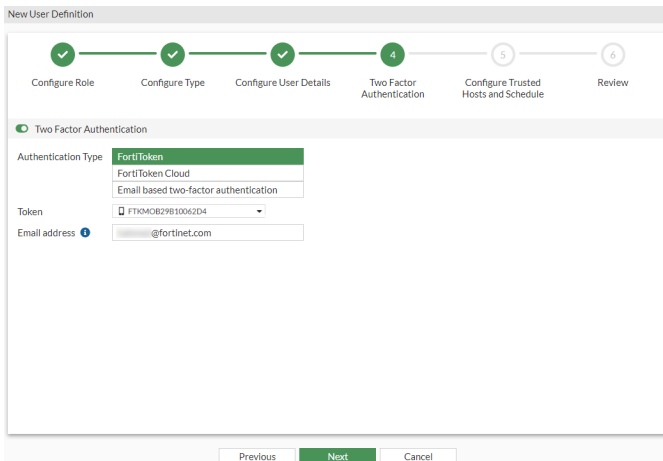
Previous Next Cancel

5. Click *Next*.
6. In *Configure User Detail*:
 - a. In *Username*, enter a name.
 - b. In *Password*, enter a password.
 - c. In *Confirm Password*, reenter password to confirm.
 - d. In *Status*, enable logging in to FortiPAM.

- e. In *Email address*, enter the email address for the user.



- 7. Click *Next*.
- 8. Enable *Two Factor Authentication*, and:
 - a. In *Authentication Type*, select *FortiToken*.
 - b. From the *Token* dropdown, select a FortiToken Mobile that you earlier added in [Adding a FortiToken to FortiPAM on page 11](#).
 - c. Ensure that the email address is the same email address of the user you entered in step 6.



- d. Click *Next*.
- 9. Click *Next*.
- 10. In the *Review* tab, verify the information you entered and click *Submit* to create the user.
- 11. Go *User Management > FortiTokens*, select the token used in step 8 from the list and then click *Provision*. An email notification is sent to the user. This is the email address configured in step 8.

CLI configuration to set up a user with FortiToken as the authentication type:

- 1. In the CLI console, enter the following commands:


```
config system admin
edit "token"
    set accprofile "super_admin" #administrator role
    set two-factor fortitoken
    set fortitoken "FTKMOB29B10062D4"
    set email-to "username@example.com"
```

```
set password "myPassword"  
next  
end
```

Enabling FortiToken Mobile push notification

To enable FortiToken Mobile push notification:

1. Go to *Network > Interfaces* and double-click port1.
2. In the *Service Access Setting* pane, enable *FortiToken Mobile Push*.
3. Click *Save*.
4. In the CLI console, enter the following commands:

```
config system ftm-push  
set server-cert "Fortinet_Factory"  
set server x.x.x.x #IP address of the FortiPAM interface  
set status enable  
end
```

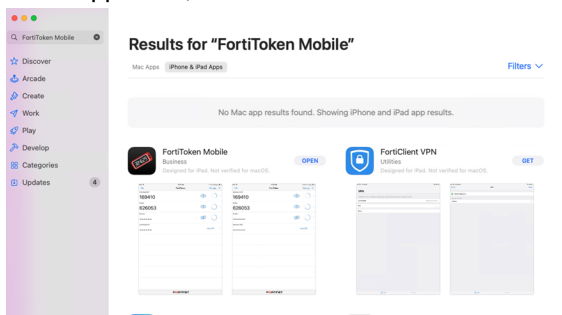
Results

1. From the user dropdown on the top-right, select *Logout*.
2. On the login screen, enter the username and password for the user you just created, and select *Continue*.
3. On the token screen, enter the token from your FortiToken Mobile application and select *Continue* to log in to FortiPAM, or approve the push login request that appears on your mobile phone to log in to FortiPAM. For more information, see [Setting up FortiToken Mobile on page 14](#).

Setting up FortiToken Mobile

To set up FortiToken Mobile:

1. In the App Store, look for FortiToken Mobile and install the application.



2. After your system administrator assigns a token to you, you will receive a notification with an activation code and an activation expiration date by which you must activate your token. For more information on *Token Activation*, see [FortiToken Mobile User Guide](#).

Subject: **FTM Activation on FortiPAM**

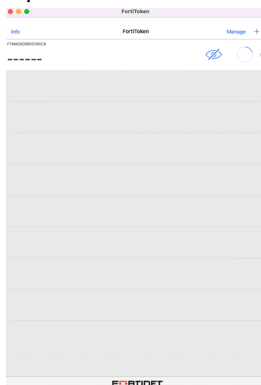
Welcome to FortiToken Mobile - One-Time-Password software token.
 Please visit <http://docs.fortinet.com/ftoken.html> for instructions on how to install your FortiToken Mobile application on your device and activate your token.
 You must use FortiToken Mobile version 2 or above to activate this token.
 Your Activation Code, which you will need to enter on your device later, is
 "EEILCAJLEF3ETZQU"

Alternatively, use the attached QR code image to activate your token with the "Scan Barcode" feature of the app.
 You must activate your token by:
 Fri Feb 24 14:01:36 2023 (GMT-8:00) Pacific Time (US & Canada),
 after which you will need to contact your system administrator to re-enable your activation.

FortiPAM

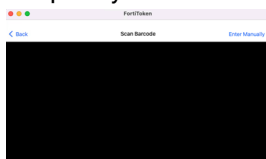
> 1 attachment: ftm_qr_FTKM082981D195C8.png 254 bytes

3. Open the FortiToken Mobile application and click + icon on the top-right to add a token.




4. There are two ways to add a token to the FortiToken Mobile application:

a. **Scan QR code:** If your device supports QR code recognition, select + in the FortiToken Mobile home screen and point your device camera at the QR code attached to the activation email.



b. **Enter Manually:**

- i. Select + and then select *Enter Manually* from the bottom.
- ii. Select *Fortinet* and enter *Name* and *Key*.

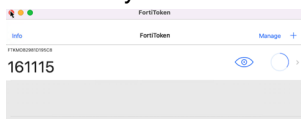
 **Key is the activation key from your activation email notification and must be entered exactly as it appears in the activation message, either by typing or copying and pasting.**

iii. Click *Done*.

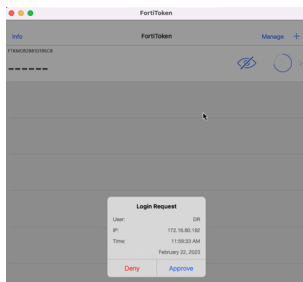
FortiToken Mobile communicates with the secure provisioning server to activate your token. The token is now displayed in the token list view.



5. Click the eye icon to retrieve the token to be used in step 3 in [Results on page 14](#).



Alternatively, if approving the push login request in step 3 in [Results on page 14](#), click *Approve* in *Login Request*.



RADIUS authentication

This section describes configuring RADIUS authentication.

2FA on FortiPAM for RADIUS users using FortiAuthenticator

FortiPAM can be integrated with your installed authentication system through the standard protocol, e.g., RADIUS, LDAP, and SAML.

This example demonstrates how to connect FortiPAM to FortiAuthenticator through RADIUS protocol and how to enable 2FA to improve security.

Requirements:

This example uses FortiPAM 1.0.0 and FortiAuthenticator 6.5.0.

To configure 2FA on FortiPAM for RADIUS users using FortiAuthenticator:

1. [Configuring a RADIUS server on FortiPAM on page 17](#)
2. [Creating remote user group on FortiPAM on page 19](#)
3. [Enabling 2FA on FortiAuthenticator on page 19](#)
4. [Creating a RADIUS user on FortiPAM on page 20](#)
5. [Results on page 21](#)

Configuring a RADIUS server on FortiPAM

Configure the details of the remote FortiAuthenticator RADIUS server on FortiPAM.

To configure a RADIUS server on FortiPAM:

1. Log in to FortiPAM with as an administrator.
2. Go to *User Management > Radius Servers*, and select *Create*.
The *New RADIUS Server* wizard opens.
3. In *Name*, enter a name for the RADIUS server.
4. In *Authentication Type*, ensure that *Default* is selected.
5. Click *Next*.
6. In the *Primary Server* pane:
 - a. In *IP/Name*, enter an IP address or FQDN. This is the IP address/FQDN of the remote FortiAuthenticator RADIUS server.

- b. In *Secret*, enter the pre-shared passphrase used to access this RADIUS server.

New RADIUS Server

Configure Settings **2** Configure Servers Test Connection Review

Primary Server

IP/Name

Secret

Secondary Server

IP/Name

Secret

Back **Test Connection** Cancel

- 7. Click *Test Connection* to test the connection to the RADIUS server. If the configuration is correct, *Connection Status: Successful* is displayed.

New RADIUS Server

Configure Settings Configure Servers **3** Test Connection Review

Primary Server

IP/Name

Connection Status ✔ Successful

Back **Next** Cancel

- 8. Click *Next*.
- 9. In the *Review* tab, verify the information you entered and click *Submit* to create the RADIUS server.

New RADIUS Server

Configure Settings Configure Servers Test Connection **4** Review

Settings

Name test_RADIUS

Authentication Type Default

Primary Server

IP/Name

Connection Status ✔ Successful

Back **Submit** Cancel

Creating remote user group on FortiPAM

To create a remote user group on FortiPAM:

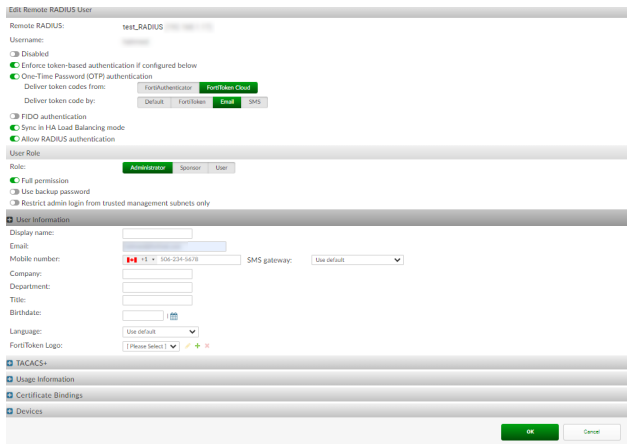
1. Go to *User Management > User Groups*.
2. Select *Create* to create a new user group.
The *Create New User Group* window opens.
3. In *Name*, enter a name for the user group.
4. In *Type*, select *Remote*.
5. In the *Remote Groups* pane:
 - a. Select *Create*.
The *Add Group Match* window opens.
 - b. In the *Remote Server* dropdown, select the remote RADIUS server created in [Configuring a RADIUS server on FortiPAM on page 17](#).
 - c. Click *OK*.
6. Click *OK*.

The screenshot shows the 'Edit User Group' configuration window. The 'Name' field is filled with 'test_group' and the 'Type' dropdown is set to 'Remote'. Below this, there is a section titled 'Remote Groups' which contains a table with two columns: 'Remote Server' and 'Group Name'. The table has one row with 'test_RADIUS' in the 'Remote Server' column and an empty 'Group Name' column. Above the table are buttons for '+ Create', 'Edit', and 'Delete'. At the bottom of the window, there are 'OK' and 'Cancel' buttons.

Enabling 2FA on FortiAuthenticator

To enable 2FA on the FortiAuthenticator RADIUS server:

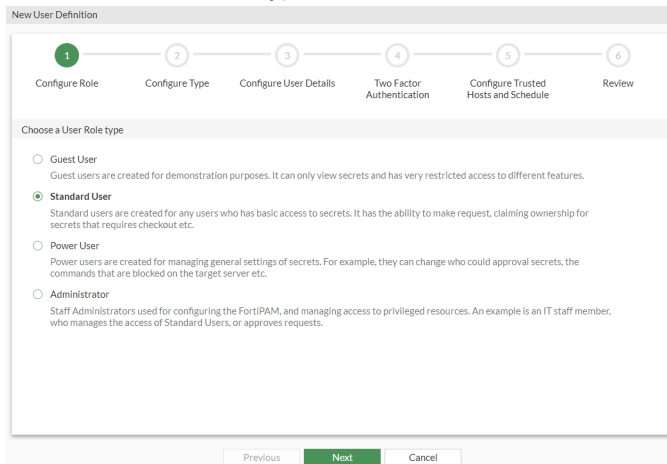
1. Log in to FortiAuthenticator as an administrator.
2. Go to *Authentication > User Management > Remote Users*.
3. Select *RADIUS* and then double-click a remote RADIUS user to edit it.
4. Enable *One-Time Password (OTP) authentication*, and:
 - a. In *Deliver token codes from*, select *FortiToken Cloud*.
 - b. In *Deliver token code by*, select *Email*.
5. In the *User Information* pane, ensure that the email address of the user is entered in the *Email* field.
6. Click *OK*.
7. In the dialog that appears, enter the password to your FortiAuthenticator and then click *Validate* to validate the changes.



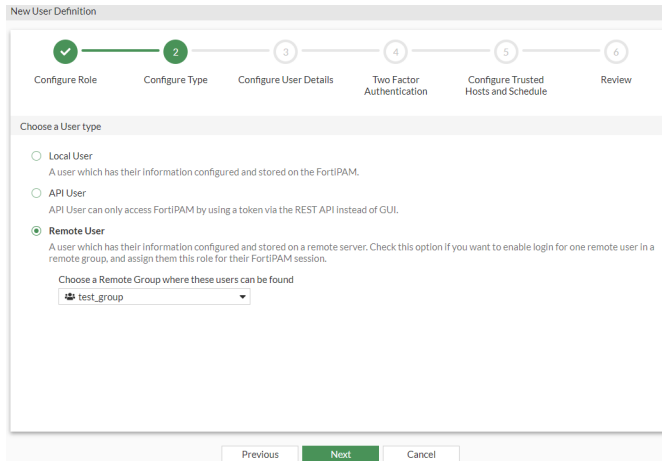
Creating a RADIUS user on FortiPAM

To create a RADIUS user on FortiPAM:

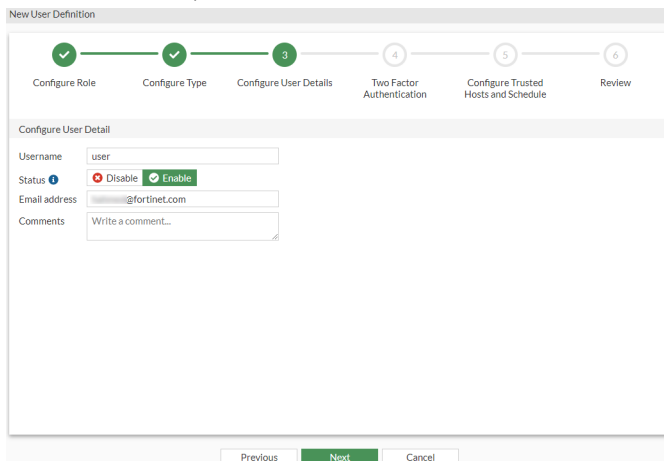
1. Go to *User Management > User Definition*, and select *Create*. The *New User Definition* wizard is launched.
2. In *Choose a User Role type*, select *Standard User*.



3. Click *Next*.
4. In *Choose a User type*, select *Remote User*, and from *Choose a Remote Group where these users can be found*, select the remote user group created in [Creating remote user group on FortiPAM on page 19](#).



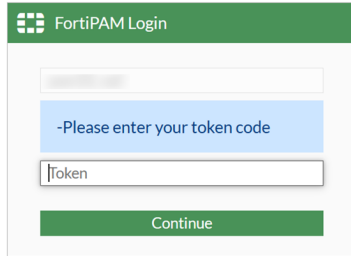
5. Click *Next*.
6. In *Configure User Detail*:
 - a. In *Username*, enter a username.
 - b. In *Status*, enable logging in to FortiPAM.
 - c. In *Email address*, enter the email address for the user.



7. Click *Next*.
8. Disable *Two Factor Authentication*.
9. Click *Next*.
10. Click *Next*.
11. In the *Review* tab, verify the information you entered and click *Submit* to create the user.

Results

1. From the user dropdown on the top-right, select *Logout*.
2. On the login screen, enter the username and password for the user you created in [Creating a RADIUS user on FortiPAM on page 20](#), and click *Continue*.
A new token input dialog appears.



The image shows a 'FortiPAM Login' dialog box. It has a green header with the FortiPAM logo and the text 'FortiPAM Login'. Below the header is a blurred input field. A blue box contains the text '-Please enter your token code'. Below that is a text input field with the placeholder text 'Token'. At the bottom is a green button labeled 'Continue'.

3. In the token input dialog, enter the token received on the email address you gave while [Enabling 2FA on FortiAuthenticator on page 19](#) and click *Continue*.
You have successfully logged in to FortiPAM using FortiAuthenticator as a remote RADIUS server.

SAML authentication

This section describes configuring SAML authentication.

2FA on FortiPAM for SAML users using FortiAuthenticator

FortiPAM can be integrated with your installed authentication system through the standard protocol, e.g., RADIUS, LDAP, and SAML.

This example demonstrates how FortiPAM works with FortiAuthenticator as a SAML IdP.

Requirements:

This example uses FortiPAM 1.0.0 and FortiAuthenticator 6.5.1.

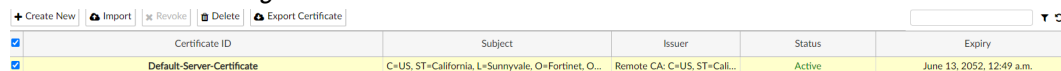
To set up 2FA on FortiPAM for SAML users with FortiAuthenticator as a SAML IdP:

1. [Importing FortiAuthenticator certificate to FortiPAM on page 23](#)
2. [Configuring FortiAuthenticator as a SAML IdP on page 24](#)
3. [Configuring FortiPAM as an SP on page 26](#)
4. [Creating a remote user group on FortiPAM on page 27](#)
5. [Creating a SAML user on FortiPAM on page 28](#)
6. [Results on page 29](#)

Importing FortiAuthenticator certificate to FortiPAM

To import FortiAuthenticator certificate to FortiPAM:

1. Log in to FortiAuthenticator.
2. Go to *Certificate Management > End Entities > Local Services*.

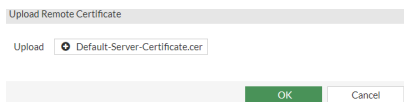


The screenshot shows the 'Local Services' view in FortiAuthenticator's Certificate Management section. At the top, there are buttons for '+ Create New', 'Import', 'Revoke', 'Delete', and 'Export Certificate'. Below these is a search bar and a refresh icon. A table lists certificates with columns for Certificate ID, Subject, Issuer, Status, and Expiry. One certificate is selected, highlighted in yellow.

Certificate ID	Subject	Issuer	Status	Expiry
Default-Server-Certificate	C=US, ST=California, L=Sunnyvale, O=Fortinet, O...	Remote CA: C=US, ST=Call...	Active	June 13, 2052, 12:49 a.m.

3. Select the *Default-Server-Certificate* and then select *Export Certificate* to download the default certificate to your management computer.
4. Log in to FortiPAM.
5. Go to *System > Certificates* and from the *+Create/Import* dropdown, select *Remote Certificate*. The *Upload Remote Certificate* window opens.
6. Select *+Upload* and locate the certificate file on your management computer that you earlier imported from FortiAuthenticator in step 3.

7. Click OK.



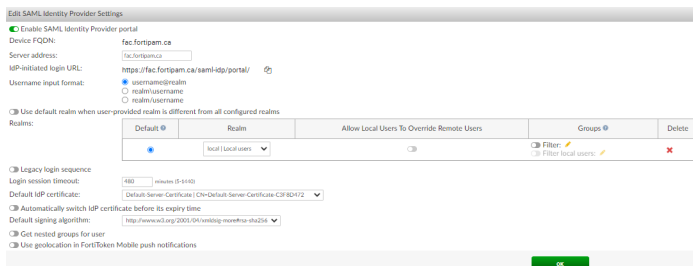
The imported certificate shows up under *Remote Certificate*.

Name	Subject	Comments	Issuer	Expires	Status	Source
Fortinet_CA_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Aut...	This is the default CA certificate the SSL Inspection will use when genera...	Fortinet	2033/01/18 07:39:20	Valid	Factory
Fortinet_CA_Untrusted	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Aut...	This is the default CA certificate the SSL Inspection will use when genera...	Fortinet	2033/01/05 06:23:22	Valid	Factory
Local Certificate						
Fortinet_Factory	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2056/11/20 11:58:17	Valid	Factory
Fortinet_Factory_Backup	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2038/01/18 19:14:07	Valid	Factory
Fortinet_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2025/04/22 08:39:20	Valid	Factory
Fortinet_SSL_DSA1024	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2025/04/22 08:39:21	Valid	Factory
Fortinet_SSL_DSA2048	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2025/04/22 08:39:21	Valid	Factory
Fortinet_SSL_ECDSA256	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2025/04/22 08:39:21	Valid	Factory
Fortinet_SSL_ECDSA384	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2025/04/22 08:39:21	Valid	Factory
Fortinet_SSL_ECDSA521	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2025/04/22 08:39:21	Valid	Factory
Fortinet_SSL_ED448	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2025/04/22 08:39:21	Valid	Factory
Fortinet_SSL_ED25519	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2025/04/22 08:39:21	Valid	Factory
Fortinet_SSL_RSA1024	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2025/04/22 08:39:20	Valid	Factory
Fortinet_SSL_RSA2048	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2025/04/22 08:39:20	Valid	Factory
Fortinet_SSL_RSA4096	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN...	This certificate is embedded in the hardware at the factory and is unique...	Fortinet	2025/04/22 08:39:21	Valid	Factory
Fortinet_WiFi	C = US, ST = California, L = Sunnyvale, O = "Fortinet, Inc.", CN = auth-cert...	This certificate is embedded in the firmware and is the same on every unli...	DigiCert Inc	2023/09/05 16:59:59	Valid	Factory
Remote CA Certificate						
Fortinet_CA	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Aut...		Fortinet	2056/05/27 13:27:39	Valid	Factory
Fortinet_CA_Backup	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Aut...		Fortinet	2038/01/19 14:34:39	Valid	Factory
Fortinet_Sub_CA	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Aut...		Fortinet	2056/05/27 13:48:33	Valid	Factory
Fortinet_WiFi_CA	C = US, O = DigiCert Inc, CN = DigiCert TLS RSA SHA256 2020 CA 1		DigiCert Inc	2030/09/23 16:59:59	Valid	Factory
Remote Certificate						
REMOTE_Cert_1	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Fortiauthentic...		Fortinet	2052/06/13 01:49:25	Valid	User

Configuring FortiAuthenticator as a SAML IdP

To configure FortiAuthenticator as a SAML IdP:

1. Log in to FortiAuthenticator.
2. Go to *Authentication > SAML IdP > General*.
The *Edit SAML Identity Provider Settings* window opens.
3. Toggle on *Enable SAML Identity Provider portal*.
4. In *Server address*, enter the FQDN of the FortiAuthenticator device.
5. In the *Default IdP certificate* dropdown, select the *Default-Server-Certificate* exported in [Importing FortiAuthenticator certificate to FortiPAM on page 23](#).
6. Click *OK*.



To configure SP settings on FortiAuthenticator:

1. In FortiAuthenticator, go to *Authentication > SAML IdP > Service Providers* and select *Create New* to create a new SAML SP.

2. In *SP name*, enter a name for the FortiPAM SP.
3. In *IdP prefix*, select *+* and enter an IdP prefix. Alternatively, you can select *Generate prefix* in the *Create Alternate IdP Prefix* dialog to generate a random 16 digit alphanumeric string.
IdP entity id, *IdP single sign-on URL*, and *IdP single logout URL* are automatically filled in.
4. In *Server certificate*, select the *Default-Server-Certificate* exported in [Importing FortiAuthenticator certificate to FortiPAM on page 23](#).
5. In the *IdP signing algorithm* dropdown, select SHA-256 signing algorithm.
6. Enable participation in single logout for the SAML IdP service.
7. In *Authentication method*, select *Password-only*.
8. Click *Save*.
9. In the *SP Metadata* pane:
 - a. In *SP entity ID*, enter the FortiPAM SP entity ID.
 - b. In *SP ACS (login) URL*, enter the FortiPAM SP Assertion Consumer Service (ACS) login URL.
 - c. In *SP SLS (logout) URL*, enter the FortiPAM SP Single Logout Service (SLS) logout URL.



SP entity ID, *SP ACS (login) URL*, and *SP SLS (logout) URL* values are same as those in the *Configure Service Provider* tab when *Configuring FortiPAM as an SP on page 26*.

For example:

SP entity ID- `http://[PAM_IP]/saml/metadata`

SP ACS (login) URL- `https://[PAM_IP]/XX/YY/ZZ/saml/login/`

SP SLS (logout) URL- `https://[PAM_IP]/remote/saml/logout/`

10. In the *Assertion Attributes* pane:
 - a. Select *Add Assertion Attribute*.
 - b. In *SAML attribute*, enter username.
 - c. In the *User attribute* dropdown, select *Username*.
 - d. Similarly, add another attribute with *SAML attribute* as group and *User attribute* as *Group*.
11. Click *OK*.

The screenshot shows the 'Edit SAML Service Provider' configuration page. The 'SP Metadata' section is expanded, showing the following fields:

- SP entity ID: `http://[PAM_IP]/saml/metadata`
- SP ACS (login) URL: `https://[PAM_IP]/XX/YY/ZZ/saml/login/`
- SP SLS (logout) URL: `https://[PAM_IP]/remote/saml/logout/`

The 'Authentication' section shows the 'Password-only' method selected. The 'Assertion Attributes' section shows two attributes:

- SAML attribute: `username`, User attribute: `Username`
- SAML attribute: `group`, User attribute: `Group`

At the bottom, there are 'OK' and 'Cancel' buttons.

Configuring FortiPAM as an SP

To configure FortiPAM as an SP:

1. Go to *User Management > Saml Single Sign-On*.
2. In the *Configure Service Provider* tab, keep the default values.



Ensure that the FortiAuthenticator IdP uses the same configuration as in *Configure Service Provider* tab in *SP Metadata* when Configuring FortiAuthenticator as a SAML IdP on page 24:

FortiPAM	FortiAuthenticator
Entity ID	SP entity ID
Single Logout Service (SLS) URL	SP SLS (logout) URL
Portal (Sign On) URL	SP ACS (login) URL

3. Click *Next*.
4. In the *Configure Identity Provider* tab:
 - a. In *Type*, select *Custom*.
 - b. In *IdP entity ID*, enter the FortiAuthenticator IdP entity ID.
 - c. In *IdP single sign-on URL*, enter the FortiAuthenticator IdP login URL.
 - d. In *IdP single logout URL*, enter the FortiAuthenticator IdP logout URL.



IdP entity ID, *IdP single sign-on URL*, and *IdP single logout URL* were initially configured in *Configuring FortiAuthenticator as a SAML IdP* on page 24.

- e. In the *IdP Certificate* dropdown, select the remote certificate imported in *Importing FortiAuthenticator certificate to FortiPAM* on page 23.
 - f. Click *Next*.
5. In the *Additional Saml Attributes* tab:
 - a. In *Attribute used to identify users*, enter *username*.
 - b. In *Attribute used to identify groups*, enter *group*.



These attributes are the same as those configured in the *Assertion Attributes* pane when *Configuring FortiAuthenticator as a SAML IdP* on page 24.

6. Click *Next*.

7. In the *Review* tab, verify the information you entered and click *Submit*.

New SAML SSO Server

Configure Service Provider Configure Identity Provider Additional SAML Attributes **Review**

Service Provider Configuration

Base URL:

Entity ID:

Single Logout Service (SLS) URL:

Portal (Sign On) URL:

Sp Certificate:

Identity Provider Configuration

IdP Entity ID:

IdP Single Sign-On URL:

IdP Single Log-Out URL:

IdP Certificate:

Additional Attributes

User Attribute:

Group Attribute:

ADFS Claim:

Back Submit

Creating a remote user group on FortiPAM

To create a remote user group on FortiPAM:

1. Go to *User Management > User Groups*.
2. Select *Create* to create a new user group.
The *Create New User Group* window opens.
3. In *Name*, enter a name for the user group.
4. In *Type*, select *Remote*.
5. In the *Remote Groups* pane:
 - a. Select *Create*.
The *Add Group Match* window opens.
 - b. In the *Remote Server* dropdown, select the SAML server created in [Configuring FortiPAM as an SP on page 26](#).
 - c. Click *OK*.
6. Click *OK*.

Create New User Group

Name:

Type:

Remote Groups

+ Create Edit Delete

Remote Server	Group Name
fortipam-saml-ssp-server	

OK Cancel

Creating a SAML user on FortiPAM

To create a SAML user on FortiPAM:

1. Go to *User Management > User Definition*, and select *Create*. The *New User Definition wizard* is launched.
2. In *Choose a User Role type*, select *Standard User*.

The screenshot shows the 'New User Definition' wizard with six steps: 1. Configure Role, 2. Configure Type, 3. Configure User Details, 4. Two Factor Authentication, 5. Configure Trusted Hosts and Schedule, and 6. Review. Step 1 is completed. The 'Choose a User Role type' section has four radio button options: 'Guest User', 'Standard User' (selected), 'Power User', and 'Administrator'. Each option has a brief description of its capabilities. At the bottom, there are 'Previous', 'Next', and 'Cancel' buttons.

3. Click *Next*.
4. In *Choose a User type*, select *Remote User*, and from *Choose a Remote Group where these users can be found*, select the remote user group created in [Creating a remote user group on FortiPAM on page 27](#).
5. Enable *Force SAML login*.

The screenshot shows the 'New User Definition' wizard at step 2, 'Choose a User type'. The progress bar shows step 1 is complete and step 2 is active. There are three radio button options: 'Local User', 'API User', and 'Remote User' (selected). The 'Remote User' option has a description and a dropdown menu for 'Choose a Remote Group where these users can be found', which is set to 'SAML_Group'. Below this, there is a 'Force SAML login' section with 'Disable' and 'Enable' buttons, where 'Enable' is selected. At the bottom, there are 'Previous', 'Next', and 'Cancel' buttons.

6. In *Configure User Detail*:
 - a. In *Username*, enter a username.
 - b. In *Status*, enable logging in to FortiPAM.
 - c. In *Email address*, enter the email address for the user.

The screenshot shows the 'New User Definition' wizard with six steps: 1. Configure Role, 2. Configure Type, 3. Configure User Details (current step), 4. Two Factor Authentication, 5. Configure Trusted Hosts and Schedule, and 6. Review. The 'Configure User Detail' section contains the following fields: Username (user_SAML), Status (Disable/Enable), Email address (@fortinet.com), and Comments (Write a comment...). The 'Next' button is highlighted in green.

7. Click *Next*.
8. Disable *Two Factor Authentication*.
9. Click *Next*.
10. Click *Next*.
11. In the *Review* tab, verify the information you entered and click *Submit* to create the user.

Results

1. From the user dropdown on the top-right, select *Logout*.
2. On the login screen, select *SAML* from the dropdown, and click *Continue*.

The screenshot shows the 'FortiPAM Login' page with fields for Username, Password, and Authentication mode. The Authentication mode dropdown is set to 'SAML' and is highlighted in blue. The 'Continue' button is visible at the bottom.

A new SAML login page opens.

The screenshot shows the 'SAML Test: Redirect Authentication' page with fields for Username and Password. The 'Login' button is visible at the bottom.

3. In the SAML login page, enter username and password for the SAML account created on the FortiAuthenticator and click *Login*.
You have successfully logged in to FortiPAM using FortiAuthenticator as a SAML IdP.

JWT

This section describes configuring JWT (JSON Web Token) integration.

JWT (JSON Web Token) integration with DevOps

For improved security when integrating FortiPAM with DevOps platform (such as, GitLab, Jenkins), JWT is introduced into FortiPAM 1.6.0.

It provides the following advantages:

- FortiPAM creates a dynamic token to GitLab or Jenkins. This ensures you are not required to save a permanent token for GitLab or Jenkins.
- After some time, the dynamic token expires for improved security.

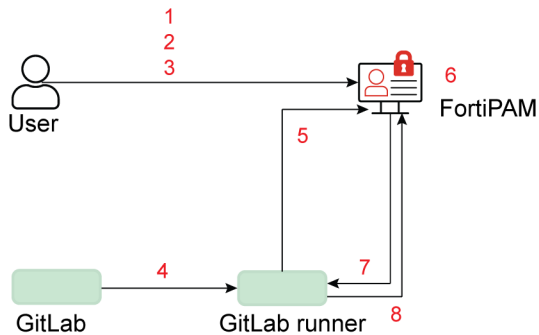


Starting FortiPAM 1.7.0, the feature is supported in GUI and the CLI console.



In FortiPAM 1.6.0, the feature is only supported via the CLI console.

The following shows how JWT works to integrate FortiPAM and DevOps:



1. Configure JWKS to retrieve JWT public key from GitLab
2. Configure JWT user with claims
3. Grant secret permission to users created in 2
4. Provide JWT to the CI job
5. Authentication with JWT
6. Verify JWT and match user claims to generate an access token
7. Return the access token
8. Retrieve secrets from FortiPAM with the access token

To configure JWT authentication in the GUI:

1. [Integrating FortiPAM and GitLab- GUI on page 31](#)

To configure JWT authentication via the CLI:

1. [Integrating FortiPAM and GitLab- CLI on page 32](#)
2. [Integrating FortiPAM and Jenkins- CLI on page 35](#)

Integrating FortiPAM and GitLab- GUI

In the GitLab design, there are 3 methods to connect FortiPAM to JWT.

- ID Token Mode (GitLab recommended)
- Legacy \$CI_JOB_JWT
- Terraform Mode

Integrating FortiPAM and GitLab

To create a JWT key:

1. In the FortiPAM GUI, go to *User Management > JWT Key Management*, and select *Create*.
The *New JWT Key* window opens.
2. Enter a name for the JWT key.
3. In *Type*, select *JWKS*.
4. In *Key*, enter the public key used to verify JWTs received from the remote server.
Select *+* to add additional keys.
Note: The key ensures the tokens are valid and issued by a trusted source.
5. In *JWKS URL*, enter the JWKS URL.
6. In *Check Interval*, keep the default value 24.
The *Check Interval* is the frequency at which the authorization server retrieves the key, in hours.
7. Click *Save*.

The screenshot shows the 'Edit JWT Key' configuration window in the FortiPAM GUI. The 'Name' field contains 'JWT_KEY_1'. The 'Type' is set to 'JWKS'. The 'Key' field contains a multi-line public key. The 'JWKS URL' is 'https://gitlab214.fortipam.ca/authorities/'. The 'Check Interval' is set to '24' hours. The 'CA Certificate' is set to 'None'. On the right side, there is a sidebar with 'Last Update Time' (2025-07-31 15:52:15) and 'Last Check Time' (2025-07-31 15:52:14). At the bottom, there are 'Save', 'Cancel', and 'Discard' buttons.

To create a JWT user:

1. Go to *User Management > User List*, and select *Create*.
The *New User List* wizard is launched.
2. In *User Privilege*, select *Standard User*, and click *Next*.
3. In *User Type*, select *JWT User*, and click *Next*.

4. In *User Details*:
 - a. In *Username*, enter a username.
 - b. In *JWT key*, select the JWT key earlier created.
 - c. In *JWT Claims*, select *Add custom claims* to add JWT claims *Field* and *Value*.
 - d. Ensure that the *Lease Duration* is set to 10 minutes.
The *Lease Duration* is the validity period of the token obtained through JWT authentication, in minutes.
 - e. Select the language for the user.
 - f. Click *Next*.
5. Review the changes and click *Submit*.

To grant secret permission to the JWT user:

1. In *Secrets*, go to the secret folder.
2. Double-click the folder to open it.
3. Select *Edit Current Folder*.
4. Go to the *Permission* tab, add users, and adjust the level of access they get into the folder.
5. Click *Save*.

User / Group	Folder Permission	Secret Permission	Allowed Service
admin	Owner	Owner	All Services
robert	Owner	Owner	All Services
JWT_Key_User	Edit	Edit	All Services

Integrating FortiPAM and GitLab- CLI

In the GitLab design, there are 3 methods to connect FortiPAM to JWT.

- ID Token Mode (GitLab recommended)
- Legacy \$CI_JOB_JWT
- Terraform Mode

To integrate FortiPAM and GitLab:

1. In the CLI console, enter the following commands to configure JWKS:

```
config secret jwt-key
  edit [xxx]
    set type jwks
    set jwks-url <gitlab jwks-url>
  next
end
```



The default jwks-url of GitLab is `https://[GITlab-FQDN]/oauth/discovery/keys`.

After finishing the above configuration, use `show secret jwt` command to check if the public key was retrieved from GitLab.

You should see the following message:

```
set key "-----BEGIN PUBLIC KEY-----"
```

If the public key does not appear, use `diagnose wad jwt-key refresh [key-name]` command to manually retrieve the public key.

2. In the CLI console, enter the following commands to configure the JWT user:

```
config system api-user
  edit "git214_project_01_id_token"
    set type jwt
    set accprofile "pam_standard_user"
    set vdom "root"
  config claims
    edit "project_id"
      set value "2"
    next
  edit "iss"
    set value "gitlab214.fortipam.ca"
  next
  edit "project_path"
    set value "gitlab-instance-ff0dfc9a/robert_pj_001"
  next
end
next
end
```



The entry names in the CLI configuration must match with those on the GitLab side.

3. Grant secret permission to the JWT user created in step 2 on the GUI.

Note: This step is identical to how you would normally assign secret permissions to a regular user.

`.gitlab-ci.yml` example with ID token mode

```
build-job:
  stage: build
```

```

variables:
  VAULT_ADDR: https://[PAM_Addr]:443
id_tokens:
  VAULT_ID_TOKEN:
    aud:https://[GitLab_Addr]

```

```

script
-echo $VAULT_ID_TOKEN
-export TOKEN_INFO="$(curl -k https://10.59.112.15:443/auth/jwt/login -H "Content-Type:\
\application/json"
-d {"jwt\":"\$VAULT_ID_TOKEN"})"
-echo $TOKEN_INFO
-export Token=$(echo "$TOKEN_INFO" | jq -r '["access-token"]')
-echo $Token
-export password="$(curl -k https://[PAM_
Addr]/api/v2/cmdb/secret/database/1?fieldname=Password -H "Authorization:Bearer $Token)"
-echo $password
-username="$(curl -k https://10.59.112.15/api/v2/cmdb/secret/database/1?fieldname=Username -H
X-Authorization-Cred-Token:$Token)"
-echo $username

```

gitlab-ci.yml example with legacy \$CI_JOB_JWT mode

```

build-job:
  stage: build
  script:
    -echo $CI_JOB_JWT
    -export TOKEN_INFO="$(curl -k https://[PAM_Addr]:443/auth/jwt/login -H "Content-
Type:application/json" -d {"jwt\":"$CI_JOB_JWT"})"
    -export Token=$(echo "$TOKEN_INFO" | jq -r '["access-token"]')
    -echo $TOKEN_INFO
    -export Token=$(echo "$TOKEN_INFO" | jq -r '["access-token"]')
    -echo $Token
    -export password="$(curl -k https://[PAM_Addr]
/api/v2/cmdb/secret/database/1?fieldname=Password -H "Authorization:Bearer $Token)"
    -echo $password
    -export username=$(curl -k https://[PAM_Addr]/api/v2/cmdb/secret/database/1?fieldname=Username
-H X-Authorization-Cred-Token:$Token)
    -echo $username

```

gitlab-ci.yml with Terraform mode

```

build-job:
  stage: build
  script:
    -ls -l
    -echo $CI_JOB_JWT
    -export TOKEN_INFO="$(curl -k https://[PAM_Addr]:443/auth/jwt/login -H "Content-
Type:application/json" -d {"jwt\":"$CI_JOB_JWT"})"
    -echo $TOKEN_INFO
    -export TF_VAR_Access_Token=$(echo "$TOKEN_INFO" | jq -r '["access-token"]')

```

```
- echo $TF_VAR_Access_Token
- export TF_VAR_Access_Token=$(echo "$TOKEN_INFO" | jq -r '["access-token"]')
- echo $TF_VAR_Access_Token
- terraform init
- terraform apply
- cat terraform.tfstate
```

Notes: The terraform configuration file (main.tf) is set as below:

```
variables "Access_Token" {
  description = "access_token which is dynamic generated by JWT auth"
}
terraform {
  required_providers {
    fortipam = {
      source = "fortinetdev/fortipam"
      version = "1.0.0"
    }
  }
}
provider "fortipam" {
  base_url = "https://10.59.112.19"
  access_token = var.Access_Token
  verify_ssl = false
}
data "fortipam_secret" "usr_test" {
  path = "Linux"
  name = "Ubuntu_100"
  field = "Username"
}
data "fortipam_secret" "pwd" {
  path = "Linux"
  name = "Ubuntu_100"
  field = "Password"
}
```

Integrating FortiPAM and Jenkins- CLI

Before you begin

1. Install the [Jenkins OIDC provider plugin](#).
 - a. Manage *Jenkins* > *System configuration* > *Plugins*.
 - b. Search OpenID Connect Provider in *Available Plugins*.
OR
 - c. Download the hpi file in <https://plugins.jenkins.io/oidc-provider/releases/>.
 - d. Go to *Advanced setting* > *Deploy Plugin* > *Choose file*.

2. jq
 - a. On the Jenkins host Unix machine , use:

```
sudo apt install jq
```

3. curl
 - a. On the Jenkins host Unix machine, use:

```
sudo apt install curl
```

Setting up Jenkins URL

1. Go to *Manage Jenkins -> System configuration -> System -> Jenkins URL*, and enter the URL.

Setting up Jenkins OIDC provider

1. Go to *Manage Jenkins > Security > Credentials*.
2. To open the *System* page, go to the *Stores scoped to Jenkins* field and click *System*.
3. To open the *Global Credentials*, click *Global credentials*.
4. Click *Add credentials* and choose *OpenID Connect id token*.
5. Optionally, edit *Issuer*, *Audience*, and *ID*.
6. Click *Create*.
7. Click *Update* to update the new credential.

If the issuer is changed, you need to manually host the OIDC files. Otherwise, the OIDC link is `https://<Jenkins_URL>/oidc/.well-known/openid-configuration`.

Issuer ?

Serve `https://jenkin228.fortipam.ca/oidc/.well-known/openid-configuration` with [this content](#) and `https://jenkin228.fortipam.ca/oidc/jwks` with [this content](#) (both as application/json).

Note that the JWKS document will need to be updated if you resave these credentials.

8. If the ID is not set, the credential ID is generated.

ID ?

Setting up FortiPAM JWT authentication

1. In the FortiPAM CLI console, enter the following commands:

```
config secret jwt-key
edit "jenkins"
set type jwks
set url <url> #The JWT URL
next
end
```

2. Check that the key has been retrieved.

3. Set up the JWT api user.

```

config system api-user
edit "jenkins_jwt_test"
set type jwt
set accprofile "pam_standard_user"
set vdom "root"
config claims
edit "iss"
set value <value> #This is same as the Jenkins settings, e.g.,
https://jenkin220.fortipam.ca/oidc
next
edit "sub"
set value "<by default the URL of a Jenkins job>" #e.g.,
https://jenkin220.fortipam.ca/job/jwt-test/
next
end
next
end

```

4. In the FortiPAM GUI, grant API user secret and folder permission.

Jenkins job example script

```

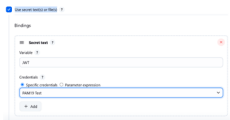
pipeline {
agent any
stages {
stage ('JWT-TEST') {
steps {
withCredentials([string(credentialsId: '<This will be the Jenkins credential id>', variable:
'JWT')])
script{
def PAM_ADDR = https://[PAM_Addr]:443
sh 'echo $JWT | base64'
def TOKEN_INFO = sh (
script: "curl -k $PAM_ADDR/auth/jwt/login -H 'Content-Type:application/json' -d '{\"jwt\": \"\$JWT\"}'",
returnStdout: true
).trim()
sh "echo $TOKEN_INFO"
def TOKEN = sh (
script: "echo '$TOKEN_INFO' | jq -r '.[\"access-token\"]'",
returnStdout: true
).trim()
sh "echo $TOKEN"
def FIELD_NAME = "<FPAM secret field name>"
def SEC_CRED = sh (
script "curl -k $PAM_ADDR/api/v2/cmdb/secret/database/<secret_id>?fieldname=$FIELD_NAME
-H \"Authorization:Bearer $TOKEN\"",
returnStdout: true
).trim()

```

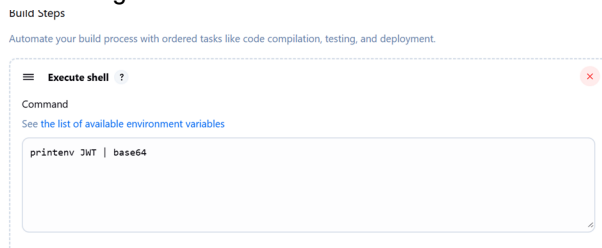
```
    sh"echo $SEC_CRED"
    pwd = sh (
script: "echo '$SEC_CRED' | jq -r '.results[0].$FIELD_NAME'",
returnStdout: true
    ).trim()
    println pwd
  }
}
}
}
}
}
```

Jenkins freestyle setup

1. Go to *Job > Configure*.
2. In *Environment*, select *Use secret text(s) or file(s)*.



3. Enter the environment variable name and select the OIDC provider credential.
4. In the build setup, proceed with the script used in [Jenkins job example script on page 37](#), e.g., environment variable referencing.



ZTNA

This section describes configuring ZTNA using FortiPAM.

ZTNA endpoint control on FortiPAM

This example demonstrates how to enable ZTNA endpoint control for FortiPAM user login and target server launching control.

Requirements:

This example uses FortiPAM 1.1.0, FortiClient 7.2.0, and FortiClient EMS 7.2.0.

To set up ZTNA endpoint control on FortiPAM:

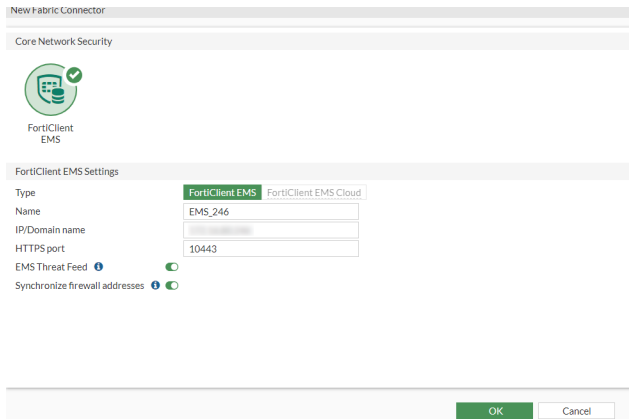
1. [Configuring EMS on FortiPAM on page 39](#)
2. [Registering the endpoint PC to EMS server on page 41](#)
3. [Configuring a ZTNA server on FortiPAM on page 44](#)
4. [Configuring proxy rule on FortiPAM on page 45](#)
5. [Adding a ZTNA tag to a secret for launching control on page 46](#)

Configuring EMS on FortiPAM

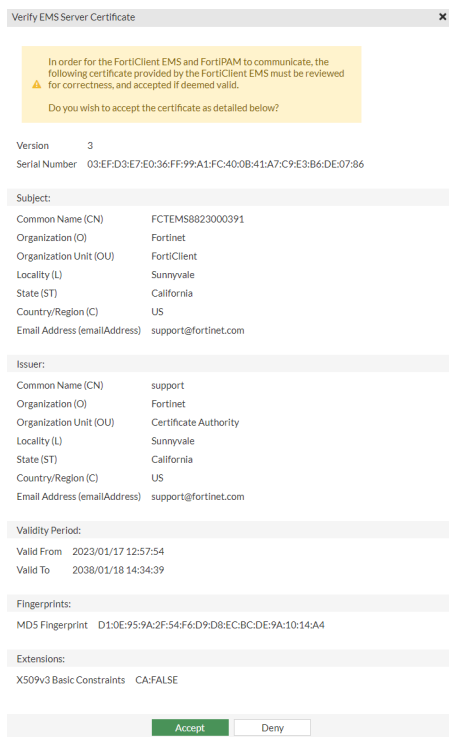
To configure EMS on FortiPAM:

1. Go to *Network > Fabric Connectors*.
2. In the *Core Network Security* pane, select *FortiClient EMS* and then select *Edit*. The *New Fabric Connector* window opens.
3. In *Name*, enter a name of the FortiClient EMS connector.
4. In *IP/Domain name*, enter the IP address of the FortiClient EMS.
5. In *HTTPS port*, enter the HTTPS port number for the FortiClient EMS. In this example, 10443 is used.
6. Ensure that *EMS Threat Feed* and *Synchronize firewall addresses* options are enabled.

7. Click **OK**.

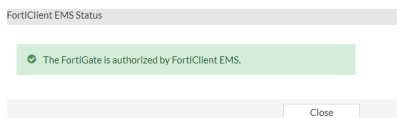


The *Verify EMS Server Certificate* window is displayed.



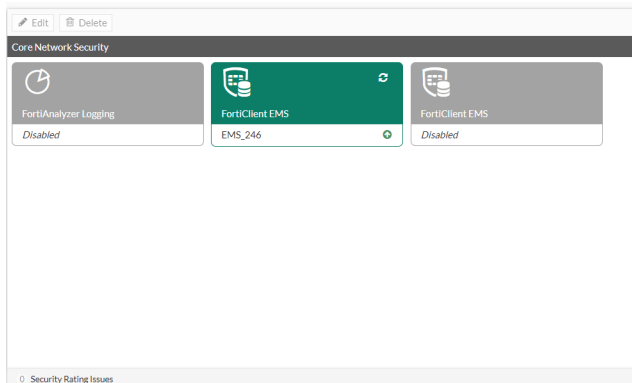
8. Click **Accept**.

The *FortiClient EMS Status* pane is displayed.



9. Click **Close**.

The FortiClient EMS is up.



Error connecting to the EMS server

If there is an error connecting to the EMS server in step 7 when [Configuring EMS on FortiPAM](#):

1. Log in to the EMS server and click *Authorize* in the *Fabric Device Authorization Requests* dialog to add FortiPAM.
2. If no *Fabric Device Authorization Requests* dialog appears when you log in to the EMS server:
 - a. Go to *Administration > Fabric Devices* and locate FortiPAM.
 - b. Click *Authorize*.
3. Log in to FortiPAM and go to *Network > Fabric Connectors*.
4. Select the previously created FortiClient EMS and then select *Edit*.
5. In *FortiClient EMS Status*, select *Authorize*.
6. In the *Verify EMS Server Certificate* window that appears, click *Accept*.
FortiPAM is now connected to the EMS successfully.

To view the ZTNA tags from the EMS server:

1. Go to *System > ZTNA* and select the *ZTNA Tags* tab to see available tags from the EMS server.

ZTNA Rules ZTNA Servers ZTNA Tags						
+ Create New Group Edit Delete Search						
Name	Provided By	Details	Type	Comments	Ref.	
FCTEMS8823000391L	EMS_246		ZTNA IP Tag		0	
FCTEMS8823000391	EMS_246		ZTNA IP Tag		0	
FCTEMS8823000391_Cubical_Subnet_80	EMS_246		ZTNA IP Tag		0	
FCTEMS8823000391_Lab_Subnet	EMS_246		ZTNA IP Tag		0	
FCTEMS8823000391_all_registered_clients	EMS_246		ZTNA IP Tag		0	
FCTEMS_ALL_FORTICLOUD_SERVERS			ZTNA IP Tag		0	
MAC_FCTEMS8823000391	MAC_FCTEMS8823000391		ZTNA MAC Tag		0	
MAC_FCTEMS8823000391	MAC_FCTEMS8823000391		ZTNA MAC Tag		0	
MAC_FCTEMS8823000391_Cubical_Subnet_80	MAC_FCTEMS8823000391		ZTNA MAC Tag		0	
MAC_FCTEMS8823000391_Lab_Subnet	MAC_FCTEMS8823000391		ZTNA MAC Tag		0	
MAC_FCTEMS8823000391_all_registered_clients	MAC_FCTEMS8823000391		ZTNA MAC Tag		0	

Registering the endpoint PC to EMS server

The endpoint PC is registered to the EMS server configured in [Configuring EMS on FortiPAM on page 39](#).

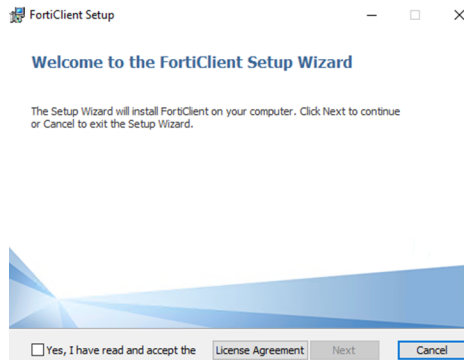
To register the endpoint PC to EMS server:

1. On the endpoint PC, install the standard FortiClient by unzipping the FortiClient setup file and executing the installer.

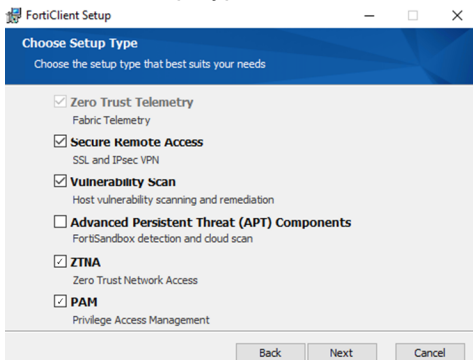


File name: FortiClientSetup_7.2.0.0xxx_x64.zip.

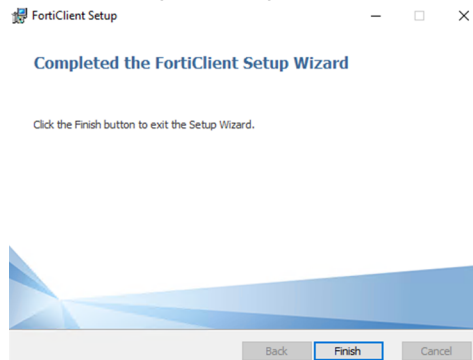
The *FortiClient Setup* wizard opens.



2. Read the license agreement and then select *Yes, I have read and*
3. In *Choose Setup Type*, in addition to other options, select *ZTNA* and *PAM*.

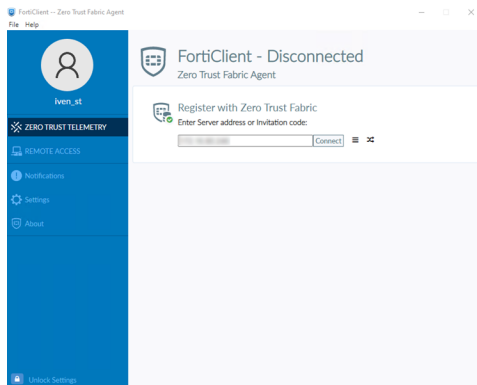


4. Follow the steps to complete the FortiClient installation and click *Finish*.

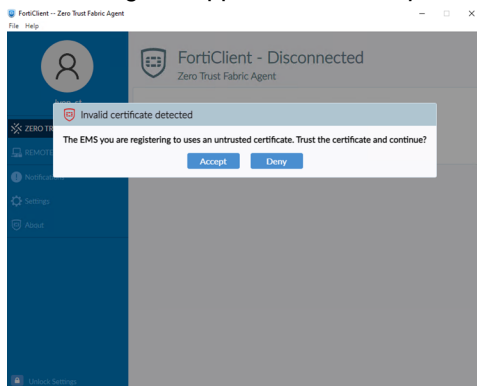


5. Open the FortiClient console and go to *ZERO TRUST TELEMETRY*.

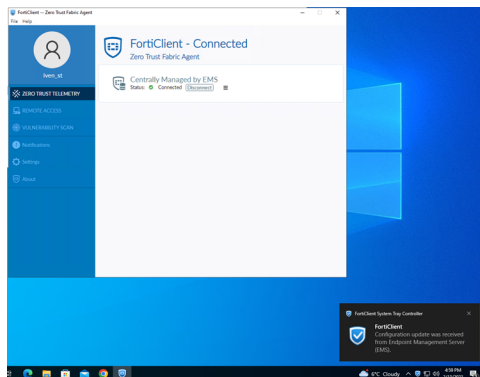
- Enter the EMS server IP address and click *Connect*.



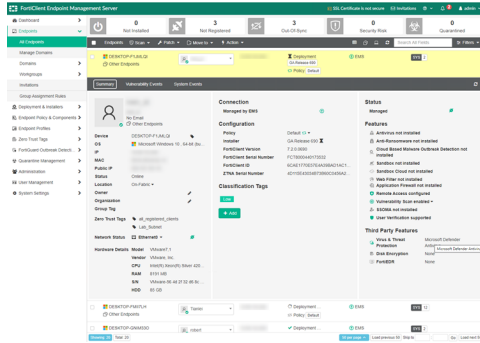
- In the dialog that appears, click *Accept* to accept the certificate from the EMS server.



FortiClient is now connected to the EMS successfully.



- In the EMS server, go to *Endpoints > All Endpoints*. The endpoint PC is tagged with zero trust tags.



Configuring a ZTNA server on FortiPAM

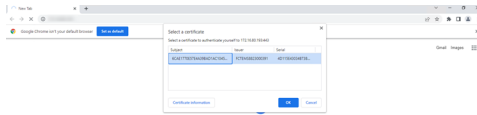
To configure a ZTNA server on FortiPAM:

 ZTNA servers can only be configured via the CLI (`config firewall access-proxy`).

1. In the CLI console enter the following commands to configure a ZTNA server:

```
config firewall access-proxy
edit "fortipam_access_proxy"
set vip "fortipam_vip"
set client-cert enable #Must be enabled
config api-gateway
edit 1
set url-map "/pam"
set service pam-service
next
edit 2
set url-map "/tcp"
set service tcp-forwarding
config realservers
edit 1
set address "all"
next
end
next
edit 3
set service gui
config realservers
edit 1
set ip 127.0.0.1
set port 80
next
end
next
end
next
end
```

From now on, you must select the browser certificate to access FortiPAM GUI. In this example, you must click *OK* to select the certificate issued by the EMS server.



Configuring proxy rule on FortiPAM

There is already a default proxy rule named *FortiPAM_Default*, so you only need to add a ZTNA tag to this rule. When no ZTNA tag is configured, endpoints registered to the EMS server match to the rule to successfully log in to FortiPAM.

To configure a proxy rule on FortiPAM:

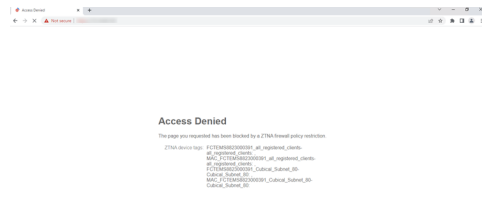


On the FortiPAM GUI, you can only edit an existing proxy rule. Use the CLI to create new proxy rules (`config firewall policy`).

1. In the CLI console enter the following commands to configure a proxy rule:

```
config firewall policy
edit 1
set type access-proxy
set name "FortiPAM_Default"
set srcintf "any"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set access-proxy "fortipam_access_proxy"
set ztna-ems-tag "FCTEMS8823000391_Lab_Subnet" #Only endpoints with this tag can
access FortiPAM
set utm-status enable
set groups "SSO_Guest_Users"
set ssl-ssh-profile "deep-inspection"
next
end
```

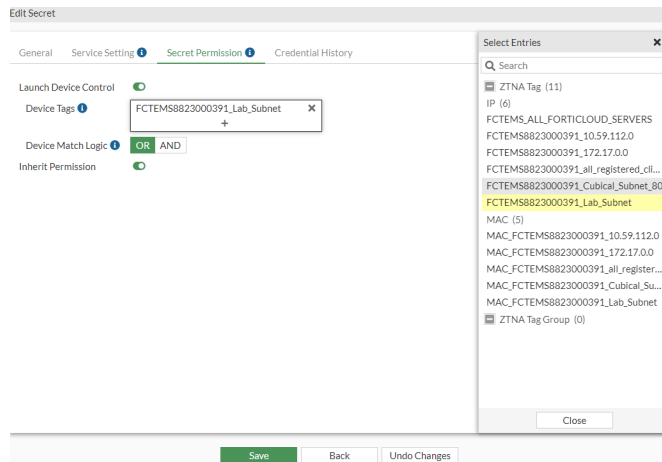
Endpoints that do not have the FCTEMS8823000391_Lab_Subnet ZTNA tag are denied access to FortiPAM.



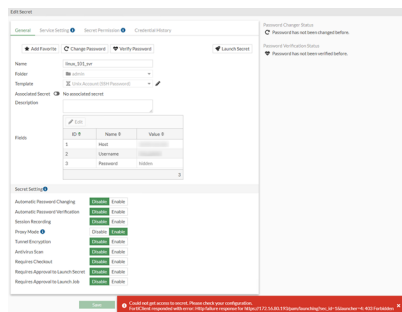
Adding a ZTNA tag to a secret for launching control

To add a ZTNA tag to a secret:

1. Go to *Secrets > Secret List*.
2. In the *Secrets List*, double-click a secret to open.
3. Go to the *Secret Permission* tab.
4. Enable *ZTNA Control* to limit the permission of launching by `ztna-ems-tag`:
 - a. In *Device Tags*, select `*`; from *Select Entries*, select `FCTEMS8823000391_Lab_Subnet`.
Only permitted devices with the selected `FCTEMS8823000391_Lab_Subnet` tag are allowed to launch the secret.
5. Click *Save*.



Launching a secret from an endpoint without the `FCTEMS8823000391_Lab_Subnet` tag leads to an error.



Secret configurations

This section describes various secret configurations for FortiPAM.

Accessing a Linux server using PuTTY

This example demonstrates how to access a Linux server by setting up a Unix template based secret on FortiPAM and then using PuTTY as a secret launcher to remotely gain access to the Linux server.

To access a Linux server using PuTTY:

1. [Creating a secret with Unix template on page 47](#)
2. [Launching a secret for the Linux server on page 48](#)

Creating a secret with Unix template

To create a secret with Unix template:

1. Go to *Secrets > Secret List*.
2. In *Secret List*, select *Create*.
The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.
4. Select *Create Secret*.
The *New Secret* window opens.
5. Enter a name for the secret.
6. In the *Template* dropdown, select *Unix Account (SSH Password)* default template.
7. In the *Fields* pane:
 - a. In the *Host* field, enter the IP address or the FQDN of the Linux server.
 - b. In the *Username* field, enter the username for the Linux server.
 - c. In the *Password* field, enter the password for the Linux server.
 - d. In the *Confirm Password* field that appears after the password is filled in, enter the password again.

8. Click *Submit*.

Launching a secret for the Linux server

To launch a secret for the Linux server:

1. In *Secrets > Secret List*, select the newly created secret, and select *Launch Secret*.
2. In *Launch Progress*, select *PuTTY* to gain access to the Linux server.
PuTTY is launched. You can now access the Linux server.



For instructions on how to install PuTTY, visit <https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>.

Accessing a Cisco router using PuTTY

This example demonstrates how to create an associated secret, access a Cisco router by setting up a Cisco User template based secret on FortiPAM, and then use PuTTY as a secret launcher to remotely gain access to the Cisco router.

To access a Cisco server using PuTTY:

1. [Creating an associated secret on page 48](#)
2. [Creating a secret with Cisco User \(SSH Secret\) template on page 49](#)
3. [Launching a secret for the Cisco router on page 51](#)

Creating an associated secret

To create an associated secret:

1. Go to *Secrets > Secrets*.
Alternatively, go to *Secrets > Personal/Public Folder*, and select a folder where you intend to add a secret.
From the *Create* dropdown, select *Secret*, and skip to step 5.

2. In *Secret List*, select *Create*.
The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.
The folder is already selected if you are creating secret from inside a folder.
4. Select *Create*.
The *New Secret* window opens.
5. Enter a name for the secret.
6. Ensure that you are in the *To connect to a remote server pane*.
7. In the *Target* dropdown, select the target server.
8. In the *Templates* dropdown, select *Cisco Enable Secret* default template.
9. Disable *Associated Secret*.
10. In the *Fields* pane:
 - a. In the *Password* field, enter the password for the Cisco machine.
 - b. In the *Confirm Password* field that appears after the password is filled in, enter the password again.
11. Click *Submit*.

Creating a secret with Cisco User (SSH Secret) template

To create a secret with Cisco User (SSH Secret) template:

1. Go to *Secrets > Secrets*.
Alternatively, go to *Secrets > Personal/Public Folder*, and select a folder where you intend to add a secret.
From the *Create* dropdown, select *Secret*, and skip to step 5.
2. In *Secret List*, select *Create*.
The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.
The folder is already selected if you are creating secret from inside a folder.
4. Select *Create*.
The *New Secret* window opens.
5. Enter a name for the secret.
6. Ensure that you are in the *To connect to a remote server pane*.
7. In the *Template* dropdown, select *Cisco User (SSH Secret)* default template.

8. Enable *Associated Secret*, and select a secret from the *Associated Secret* dropdown. In this example, a *Cisco Enable Secret* template based secret is selected as the associated secret. This allows auto-password delivery and password change feature for the *Cisco User (SSH Secret)* template based secret being created.
9. In the *Fields* pane:
 - a. In the *Username* field, enter the username for the Cisco router.
 - b. In the *Password* field, enter the password for the Cisco router.
 - c. In the *Confirm Password* field that appears after the password is filled in, enter the password again.

The screenshot shows the 'New Secret' configuration interface. The 'Associated Secret' dropdown is set to 'cisco_enable'. The 'Fields' section is expanded, showing the following fields:

- Host: (empty)
- Username*: admin
- Password*: (masked with dots)
- Confirm Password: (masked with dots)

10. Go to the *Secret Setting* tab, enable *Session Recording*.

The screenshot shows the 'New Secret' configuration interface, 'Secret Setting' tab. The 'Session Recording' option is set to 'Enable'. Other settings include:

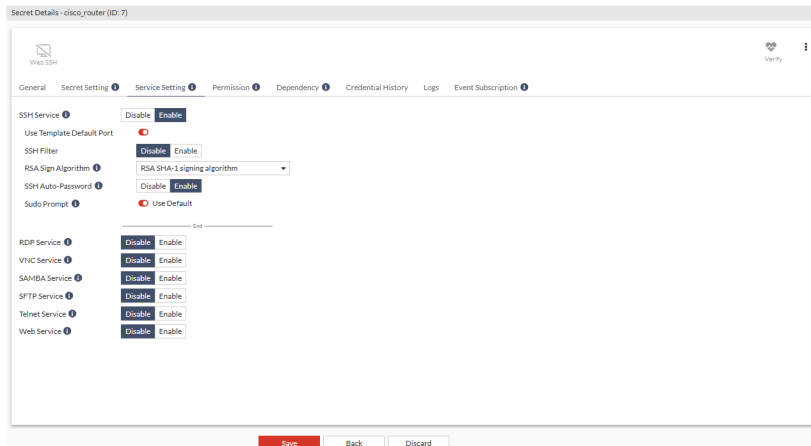
- Automatic Password Changing: Disable/Enable
- Automatic Password Verification: Disable/Enable
- Proxy Mode: Disable/Enable
- Tunnel Encryption: Disable/Enable
- Antivirus Scan: Not Available
- DLP Status: Not Available
- Requires Checkout: Disable/Enable
- Requires Approval to Launch Secret: Disable/Enable
- Requires Approval to Launch Job: Disable/Enable
- Block Clipboard: Disable/Enable
- Windows Application Filter: Not Available
- TOTP Setting: TOTP Status: Disable/Enable

Enabling *Session Recording* ensures that the user action performed on the secret is recorded.



The video file is available in the log for users with appropriate permission.

- Go to the *Service Setting* tab, in *SSH Service*, enable *SSH Auto-Password*.



- Click *Submit*.

Verifying the password

To verify the password manually:

- Go to *Secrets > Secrets*.
- In *Secret List*, select the recently created secret, and select *Edit*.
Alternatively, go to the folder where the secret is located, and double-click the secret.
The *Secret Details* window opens.
- From the top, select *Verify*.
Once the password has been verified, *Password Verification Status* shows the date and time when the password was verified and its status.

Password Verification Status

- 🔒 Password was last verified at 2023-02-08 13:03:52.
- ✅ Password was verified successfully



If there is an error in password verification, check your entries for fields and the server status.

Launching a secret for the Cisco router

To launch a secret for the Cisco router:

- In *Secrets > Secrets*, select the newly created secret, and select *Launch Secret*.
Alternatively, right-click the secret and then select *Launch Secret*.
- In *Launch Progress*, select *PuTTY* to gain access to Cisco router.
Alternatively, you can also select the *Web SSH* launcher.
PuTTY is launched. You are now successfully connected to the Cisco terminal via SSH.



Accessing a FortiGate using PuTTY, Web SSH, or the Web launcher

This example demonstrates how to access a FortiGate by setting up a Unix template based secret on FortiPAM and then using PuTTY/Web SSH/Web launcher as a secret launcher to remotely gain access to the FortiGate.

To access a FortiGate using PuTTY, Web SSH, or the Web launcher:

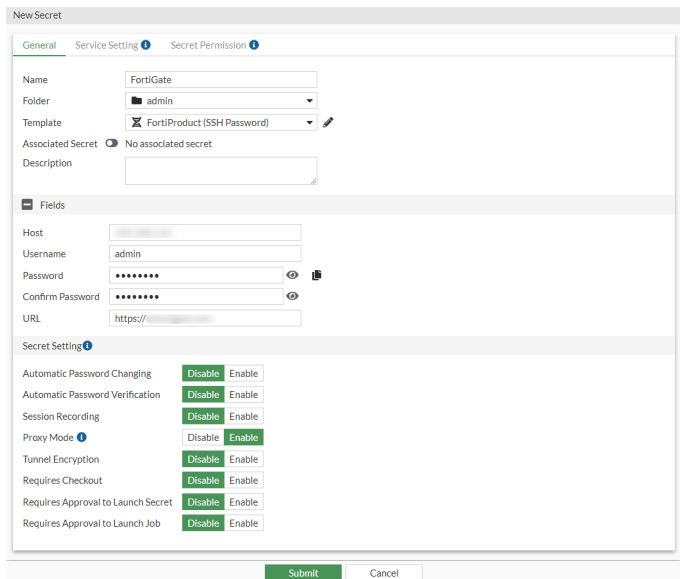
1. [Creating a secret with Unix template on page 52](#)
2. [Launching a secret for the FortiGate on page 53](#)

Creating a secret with Unix template

To create a secret with Unix template:

1. Go to *Secrets > Secret List*.
2. In *Secret List*, select *Create*.
The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.
4. Select *Create Secret*.
The *New Secret* window opens.
5. Enter a name for the secret.
6. In the *Template* dropdown, select *FortiProduct (SSH Password)* default template.
7. In the *Fields* pane:
 - a. In the *Host* field, enter the IP address or the FQDN of the FortiGate.
 - b. In the *Username* field, enter the username for the FortiGate.
 - c. In the *Password* field, enter the password for the FortiGate.
 - d. In the *Confirm Password* field that appears after the password is filled in, enter the password again.
 - e. In the *URL* field, enter the URL of the FortiGate.
The URL is the landing page of the FortiGate GUI, e.g., `https://<Host>` for the FortiGate.

8. Click *Submit*.




Launching a secret for the FortiGate

To launch a secret for the FortiGate:

1. In *Secrets > Secret List*, select the newly created secret, and select *Launch Secret*.
2. In *Launch Progress*, select *PuTTY* to gain access to the FortiGate. PuTTY is launched. You can now access FortiGate using SSH.



Alternatively, in *Launch Progress*, select *Web SSH* to gain access to the FortiGate. Web SSH allows you to access the FortiGate using the browser SSH client.

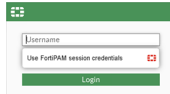
 To use the *Web SSH* launcher, ensure that you have already installed the FortiPAM extension for your browser.

A new browser tab opens. You can now access FortiGate using Web SSH. You can also access the FortiGate web GUI using FortiPAM. In *Launch Progress*, select *Web Launcher* to gain access to the FortiGate web GUI.



To use the *Web Launcher*, ensure that you have already installed the FortiPAM extension for your browser.

In the login page, click the *Username/Password* fields, click *Use FortiPAM session credentials* to fill in the credentials, and click *Login*.



Accessing a Windows server using the Remote Desktop- Windows launcher

This example demonstrates how to access a Windows server by setting up a Windows Machine template based secret on FortiPAM and then using the default Remote Desktop- Windows launcher to remotely gain access to the server.

Alternatively, depending on your requirements, you can also use Windows Domain Account or Windows Domain Account(Samba) secret templates.

To access a Windows server using the Remote Desktop- Windows launcher:

1. [Creating a secret with Windows Machine template on page 54](#)
2. [Launching a secret for the Windows server on page 55](#)

Creating a secret with Windows Machine template

To create a secret Windows Machine template:

1. Go to *Secrets > Secret List*.
2. In *Secret List*, select *Create*.
The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.
4. Select *Create Secret*.
The *New Secret* window opens.
5. Enter a name for the secret.
6. In the *Template* dropdown, select *Windows Machine* default template.
7. In the *Fields* pane:
 - a. In the *Host* field, enter the IP address or the FQDN of the Windows server.
 - b. In the *Username* field, enter the username for the Windows server.
 - c. In the *Password* field, enter the password for the Windows server.
 - d. In the *Confirm Password* field that appears after the password is filled in, enter the password again.

8. Click *Submit*.

Launching a secret for the Windows server

1. In *Secrets > Secret List*, select the newly created secret, and select *Launch Secret*.
2. In *Launch Progress*, select *Remote Desktop-Windows* to gain access to the Windows server. The remote desktop connection starts, and you can now access the Windows server.

Visiting a web application/platform using web launchers

This example demonstrates how to access a web application/platform by using web launchers in FortiPAM.

Password auto-filling and session video recording are enabled.

To visit a web application/platform using web launchers:

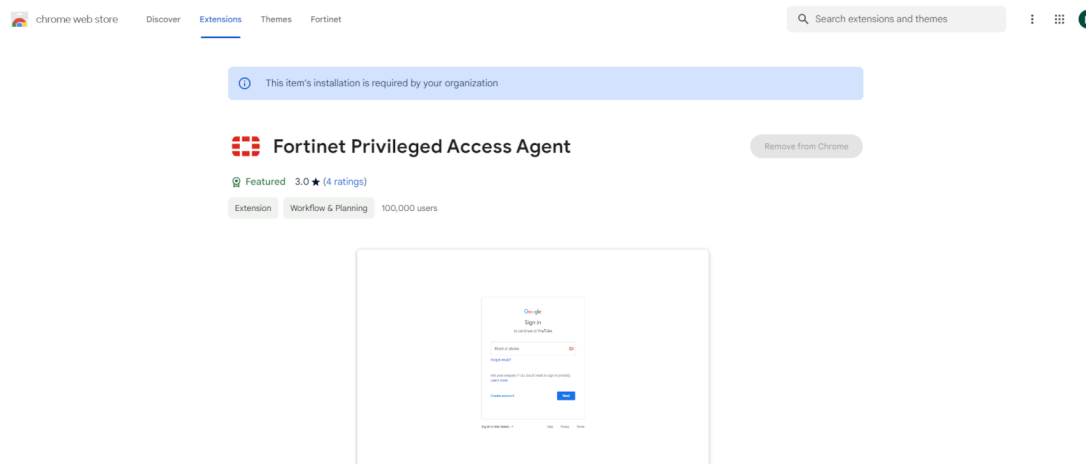
1. [Installing Fortinet Privileged Access Agent web extension on Chrome/Edge on page 56](#)
2. [Creating a secret for general web application/platform on page 57](#)
3. [Creating a secret for AWS root/IAM account on page 57](#)
4. [Visiting web application/platform using web launcher on page 59](#)
5. [Reviewing video recording for the web launching session on page 59](#)
6. [Reviewing secret log for the web launching session on page 60](#)

Installing Fortinet Privileged Access Agent web extension on Chrome/Edge

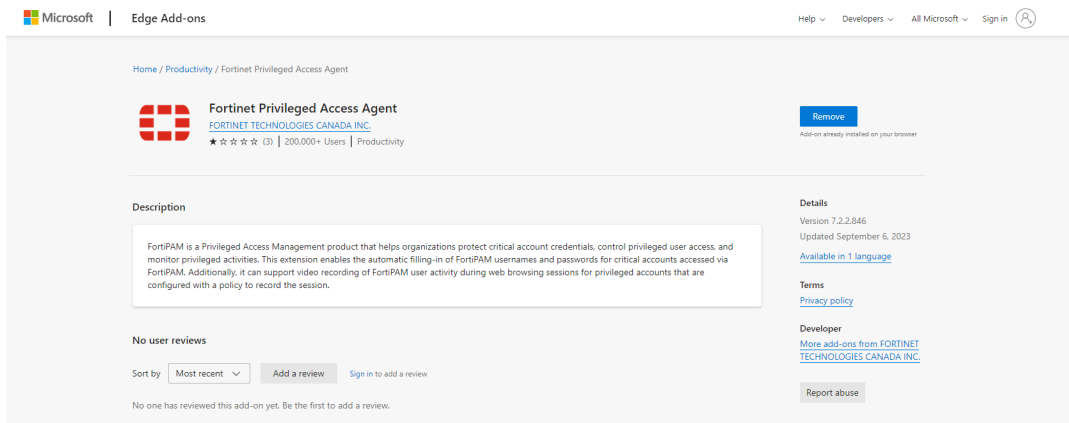
With the *Fortinet Privileged Access Agent* web extension installed, you can use FortiPAM web launchers to visit target servers.

To install Fortinet Privileged Access Agent web extension on Chrome/Edge:

1. For the Chrome browser:
 - a. Look for FortiPAM on the [Chrome Web Store](#).
 - b. Click *Add to Chrome* on the *Fortinet Privileged Access Agent* page to install the FortiPAM extension.



2. For the Edge browser:
 - a. Look for FortiPAM on [Microsoft Edge Add-ons](#).
 - b. Click *Get* on the *Fortinet Privileged Access Agent* page to install the FortiPAM extension.



Creating a secret for general web application/platform

To create a secret for general web application/platform:

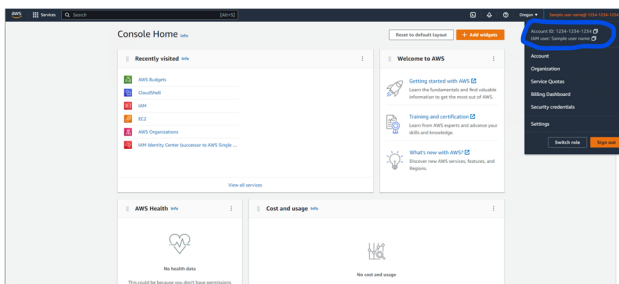
1. Go to *Secrets > Secret List*.
2. In *Secret List*, select *Create*.
The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.
4. Select *Create Secret*.
The *New Secret* window opens.
5. Enter a name for the secret.
6. In the *Template* dropdown, select *Web Account* default template.
7. In the *Fields* pane:
 - a. In the *URL* field, enter the login URL for the target web application/platform.
Note: The URL must start with either `http://` or `https://`.
 - b. In the *Username* field, enter the username for the web application/platform.
 - c. In the *Password* field, enter the password for the web application/platform.
 - d. In the *Confirm Password* field that appears after the password is filled in, enter the password again.
8. In the *Secret Setting* pane, enable *Session Recording*.
When enabled, user action performed on the secret is recorded.
9. Click *Submit*

Creating a secret for AWS root/IAM account

FortiPAM provides a basic template for an AWS account.

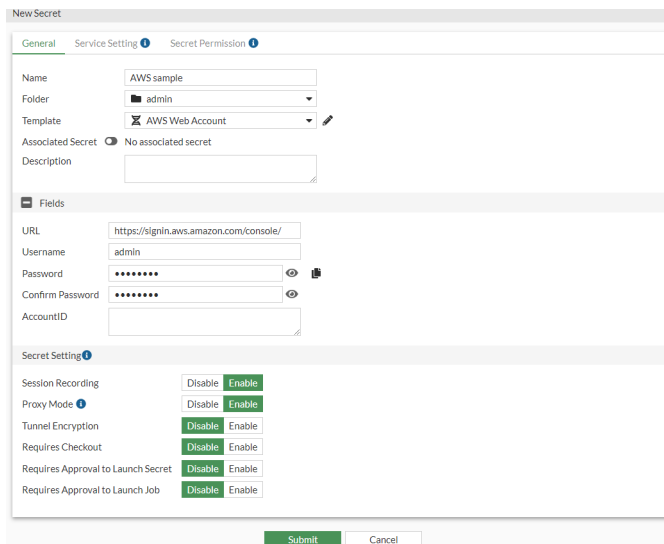
To create a secret for AWS root/IAM account:

1. Go to *Secrets > Secret List*.
2. In *Secret List*, select *Create*.
The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.
4. Select *Create Secret*.
The *New Secret* window opens.
5. Enter a name for the secret.
6. In the *Template* dropdown, select *AWS Web Account* default template.
7. In the *Fields* pane:
 - a. In the *URL* field, enter the login URL for AWS.
Use <https://signin.aws.amazon.com/console/> for an AWS root account.
Use <https://123456789012.signin.aws.amazon.com/console/> for an AWS IAM account.
Note: 123456789012 in the URL should be replaced with your AWS IAM AccountID.
 - b. In the *Username* field, enter the username for AWS.
 - c. In the *Password* field, enter the password for AWS.
 - d. In the *Confirm Password* field that appears after the password is filled in, enter the password again.
 - e. Keep the *Account ID* field empty when attempting to access an AWS root account.
For an AWS IAM account, the *Account ID* can be found on the AWS console page. Enter the *Account ID* without -.



8. In the *Secret Setting* pane, enable *Session Recording*.
When enabled, user action performed on the secret is recorded.

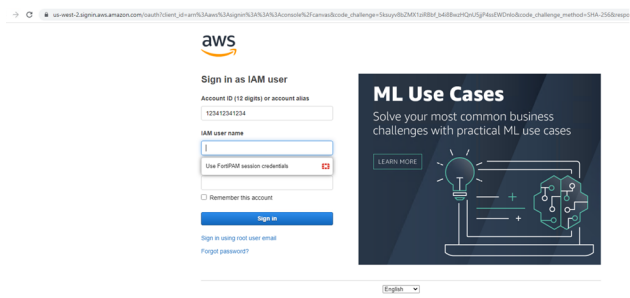
9. Click *Submit*.



Visiting web application/platform using web launcher

To visit web application/platform using web launcher:

1. In *Secrets > Secret List*, select the newly created secret, and select *Launch Secret*.
A new tab opens. You are now on the web application login page that you entered as a URL in [Creating a secret for general web application/platform on page 57](#) and [Creating a secret for AWS root/IAM account on page 57](#).



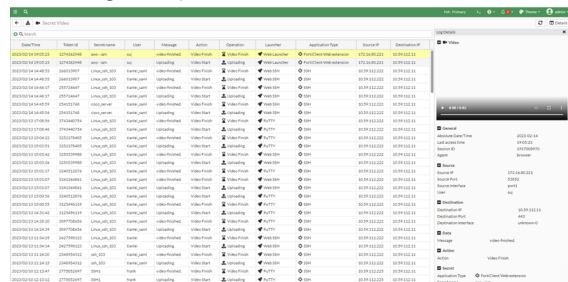
2. In the login page, click the *IAM user name/Password* fields, click *Use FortiPAM session credentials* to fill in the credentials, and click *Sign in*.

Reviewing video recording for the web launching session

Since secret session recording was enabled in [Creating a secret for general web application/platform on page 57](#) and [Creating a secret for AWS root/IAM account on page 57](#), all user activities are recorded while the session is active or till the secret session tab is closed.

To review video recording for the web launching session:

1. Go to *Log & Report > Secret > Secret Video* and double-click the secret video entry in the list.



The video player provides the following features:

- **Download:** Select to download the secret session video recording to your computer.

The file is downloaded as a WEBM file.

- **Playback speed:** From the dropdown, change the playback speed to:

- 0.25
- 0.5
- 0.75
- Normal (default)
- 1.25
- 1.5
- 1.75
- 2

- **picture in picture:** Select to shrink the video into a small player.

2. Select the play option on the video to start watching the recorded secret session.

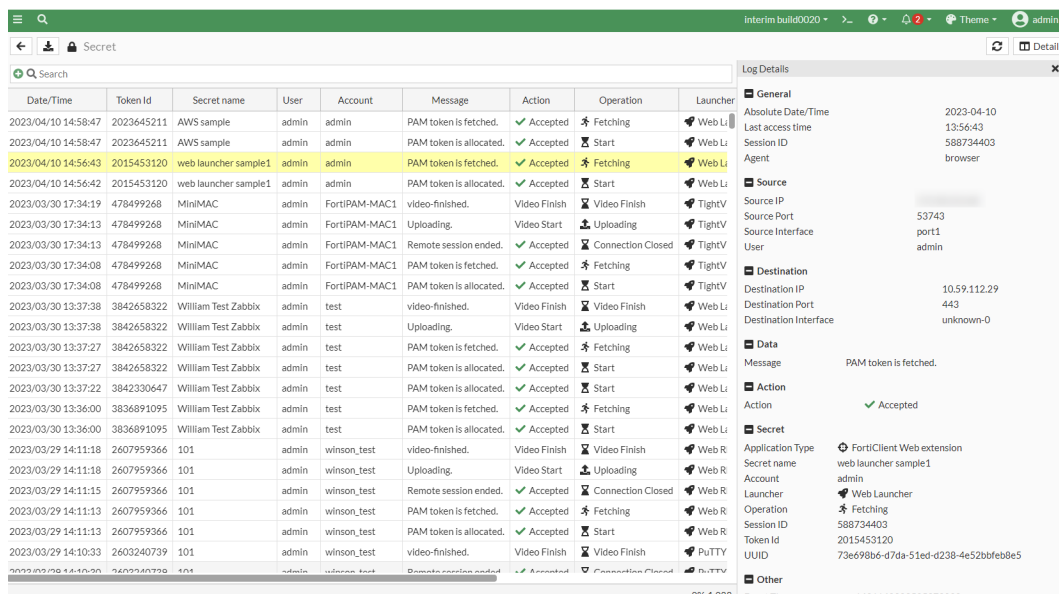
Reviewing secret log for the web launching session

As an administrator, you can review the logs for the launched secret session.

To review secret log for the web launching session:

1. Go to *Log & Report > Secret > Secret* and double-click the secret log entry in the list.

The *Log Details* pane opens on the right.



Accessing a generic machine using Web VNC, VNC Viewer, or the TightVNC launcher

This example demonstrates how to access a generic machine by setting up a Machine template based secret on FortiPAM and then using Web VNC/VNC Viewer/TightVNC as a secret launcher to remotely gain access to the machine.

To access a generic machine using Web VNC, VNC Viewer, or the TightVNC launcher:

1. Creating a secret with Machine template on page 61
2. Launching a secret for the machine on page 62

Creating a secret with Machine template

To create a secret with Machine template:

1. Go to *Secrets > Secret List*.
2. In *Secret List*, select *Create*.
The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.
4. Select *Create Secret*.
The *New Secret* window opens.
5. Enter a name for the secret.
6. In the *Template* dropdown, select *Machine* default template.

7. In the *Fields* pane:
 - a. In the *Host* field, enter the IP address or the FQDN of the machine.
 - b. In the *Username* field, enter the username for the machine.
 - c. In the *Password* field, enter the password for the machine.
 - d. In the *Confirm Password* field that appears after the password is filled in, enter the password again.
8. Click *Submit*.

Launching a secret for the machine

To launch a secret for the machine:

1. In *Secrets > Secret List*, select the newly created secret, and select *Launch Secret*.
2. In *Launch Progress*, select *Web VNC*, *VNC Viewer*, or the *TightVNC* launcher to gain access to the generic machine.

Accessing a target server using locally installed WinSCP client

This example demonstrates how to access a target server by setting up a Unix Account (SSH Password) template based secret on FortiPAM and then using the WinSCP as a secret launcher to remotely gain access to the target server.

To access a target server using locally installed WinSCP client:

1. [Installing WinSCP on a local machine on page 63](#)
2. [Creating a secret with Unix Account \(SSH Password\) template on page 63](#)
3. [Launching a secret for the target server using the WinSCP launcher on page 64](#)


Installing WinSCP on a local machine

To install WinSCP:

1. Download WinSCP from <https://winscp.net/> and install it on your local machine.
During the installation, the path of the WinSCP executable is added to the environment variables. Alternatively, you can add the path of executables manually.

Creating a secret with Unix Account (SSH Password) template

To create a secret with Unix Account (SSH Password) template

1. Go to *Secrets > Secret List*.
 2. In *Secret List*, select *Create*.
The *Create New Secret in:* dialog appears.
 3. Select the folder where you intend to add the secret.
 4. Select *Create Secret*.
The *New Secret* window opens.
 5. Enter a name for the secret.
 6. In the *Template* dropdown, select *Unix Account (SSH Password)* default template.
Alternatively, in the *Template* dropdown, select *Unix Account (SSH Key)* default template.
 7. In the *Fields* pane, when *Unix Account (SSH Password)* is selected as the template:
 - a. In the *Host* field, enter the IP address or the FQDN of the target server.
 - b. In the *Username* field, enter the username for the target server.
 - c. In the *Password* field, enter the password for the target server.
 - d. In the *Confirm Password* field that appears after the password is filled in, enter the password again.In the *Fields* pane, when *Unix Account (SSH Key)* is selected as the template:
 - a. In the *Host* field, enter the IP address or the FQDN of the target server.
 - b. In the *Username* field, enter the username for the target server.
 - c. In *Public-key*, select from *File Upload*, *Text*, or *Generate*.
 - i. When *File Upload* is selected, select *Upload*, locate the key file on your management computer, and select *Open*.
 - ii. When *Text* is selected, enter the public key in the text area.
 - iii. When *Generate* is selected, you can automatically generate a public key by choosing a type of encryption algorithm and the number of bits.
 - d. In *Private-key*, select either *File Upload* or *Text* and follow the corresponding instructions from the previous step.
-  *Private-key* is automatically generated when the *Public-key* is set to be automatically generated.
- e. Optionally, in *Passphrase*, enter a passphrase used to decrypt the private key set during the key pair generation.
 - f. In the *Confirm Passphrase* field that appears after the passphrase is filled in, enter the passphrase again.

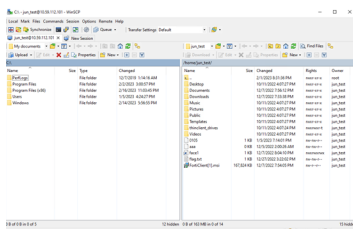
 The WinSCP launcher does not support secrets with key authentication in non-proxy mode.

8. Click *Submit*.

Launching a secret for the target server using the WinSCP launcher

To launch a secret for the target sever:

1. In *Secrets > Secret List*, select the newly created secret, and select *Launch Secret*.
2. In *Launch Progress*, select *WinSCP* launcher to gain access to the target server.
The WinSCP client automatically starts, and you are logged into the target server.



Accessing an SFTP server using the Web SFTP secret launcher

This example demonstrates how to access an SFTP server by setting up a Unix Account (SSH Password) template based secret on FortiPAM and then using the Web SFTP as a secret launcher to remotely gain access to the SFTP

server.

To access an SFTP server using the Web SFTP secret launcher:

1. [Creating a secret with Unix Account \(SSH Password\) template on page 65](#)
2. [Launching a secret for the SFTP server using the Web SFTP launcher on page 66](#)

Creating a secret with Unix Account (SSH Password) template

To create a secret with Unix Account (SSH Password) template

1. Go to *Secrets > Secret List*.
2. In *Secret List*, select *Create*.
The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.
4. Select *Create Secret*.
The *New Secret* window opens.
5. Enter a name for the secret.
6. In the *Template* dropdown, select *Unix Account (SSH Password)* default template.
Alternatively, in the *Template* dropdown, select *Unix Account (SSH Key)* default template.
7. In the *Fields* pane, when *Unix Account (SSH Password)* is selected as the template:

- a. In the *Host* field, enter the IP address or the FQDN of the SFTP server.
- b. In the *Username* field, enter the username for the SFTP server.
- c. In the *Password* field, enter the password for the SFTP server.

In the *Fields* pane, when *Unix Account (SSH Key)* is selected as the template:

- a. In the *Host* field, enter the IP address or the FQDN of the SFTP server.
- b. In the *Username* field, enter the username for the SFTP server.
- c. In *Public-key*, select from *File Upload*, *Text*, or *Generate*.
 - i. When *File Upload* is selected, select *Upload*, locate the key file on your management computer, and select *Open*.
 - ii. When *Text* is selected, enter the public key in the text area.
 - iii. When *Generate* is selected, you can automatically generate a public key by choosing a type of encryption algorithm and the number of bits.
- d. In *Private-key*, select *File Upload* or *Text* and follow the corresponding instructions from the previous step.



Private-key is automatically generated when the *Public-key* is set to be automatically generated.

- e. Optionally, in *Passphrase*, enter a passphrase used to decrypt the private key set during the key pair generation.
- f. In the *Confirm Passphrase* field that appears after the passphrase is filled in, enter the passphrase again.

3. [Launching a secret for the SMB server using the Web SMB launcher on page 69](#)

Creating a secret with Windows Domain Account (Samba) template

To create a secret with Windows Domain Account (Samba) template:

1. Go to *Secrets > Secret List*.
2. In *Secret List*, select *Create*.
The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.
4. Select *Create Secret*.
The *New Secret* window opens.
5. Enter a name for the secret.
6. In the *Template* dropdown, select *Windows Domain Account (Samba)* default template.



You must have the corresponding domain server configuration on hand before filling in the fields of the secret.

7. In the *Fields* pane:
 - a. In the *Domain-Controller* field, enter the IP address of the domain controller.
 - b. In the *Domain* field, enter the domain name of the SMB server.
 - c. In the *Username* field, enter the username for the SMB server.
 - d. In the *Password* field, enter the password for the SMB server.
 - e. In the *Confirm Password* field that appears after the password is filled in, enter the password again.
8. In the *Secret Setting* pane, enable *Session Recording*.
Enabling *Session Recording* ensures that the user action performed on the secret is recorded.



The video file is available in the log for users with appropriate permission.

9. Click *Submit*.

Verifying the password

To verify the password manually:

1. Go *Secrets > Secret List*.
2. In *Secret List*, select the recently created secret, and select *Edit*.
Alternatively, go to *Personal/Public Folder*, and select the folder where the secret is located, and double-click the secret.
The *Secret Details* window opens.
3. From the top, select *Verify Password*.
Once the password has been verified, *Password Verification Status* shows the date and time when the password was verified and its status.

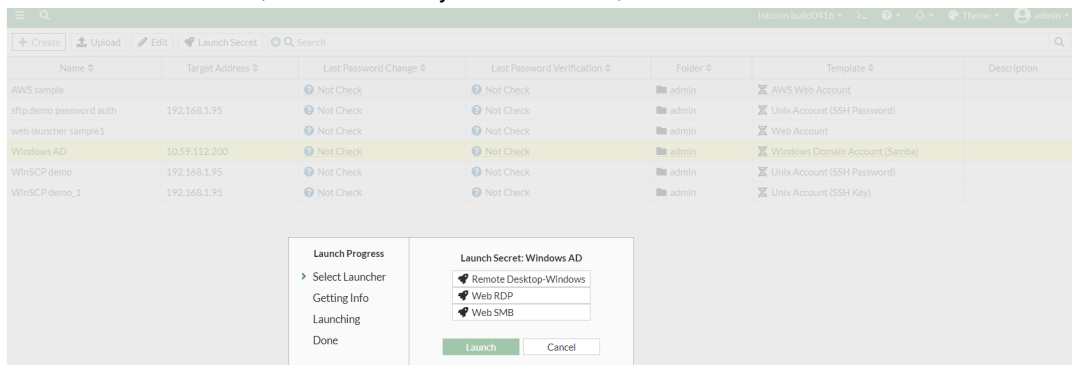
Password Verification Status

- 🔒 Password was last verified at 2023-02-08 13:03:52.
- ✅ Password was verified successfully

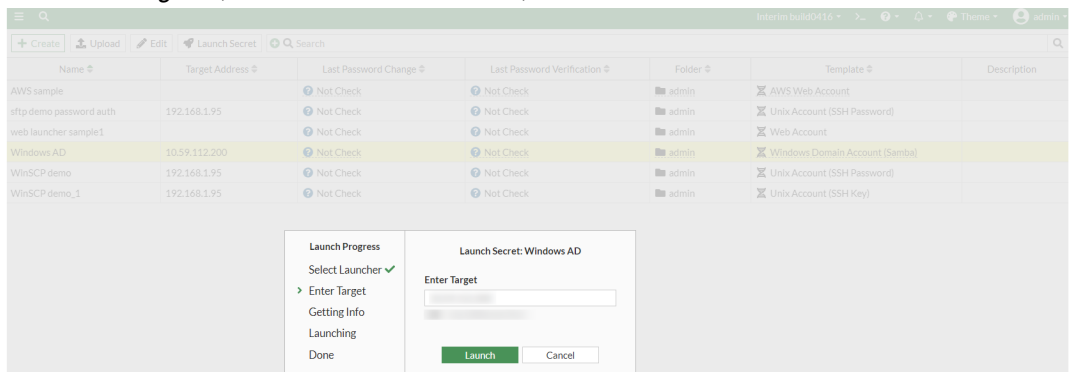
Launching a secret for the SMB server using the Web SMB launcher

To launch a secret for the SMB sever:

1. In *Secrets > Secret List*, select the newly created secret, and select *Launch Secret*.

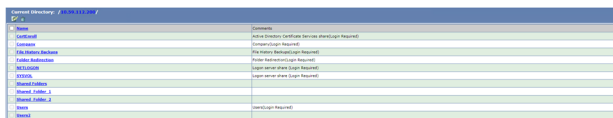


2. In *Launch Progress*, select *Web SMB* launcher, and then select *Launch*.



3. Click *Launch* to gain access to the SMB server.

A new browser tab opens with Web SMB interactive UI. You can now modify files or folders from the SMB server according to your Windows account privileges.



Checking out and checking in a secret

Checking out a secret gives you exclusive access to the secret for a limited time.

Checking in a secret allows other approved users to access the secret.

This example demonstrates how to check out and check in a secret on FortiPAM.

To check out and check in a secret:

1. [Creating a secret with check out enabled on page 70](#)
2. [Checking out a secret on page 71](#)
3. [Checking in a secret on page 72](#)

Creating a secret with check out enabled

To create a secret with check out enabled:

1. Go to *Secrets > Secret List*.
2. In *Secret List*, select *Create*.
The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.
4. Select *Create Secret*.
The *New Secret* window opens.
5. Enter a name for the secret.
6. In the *Template* dropdown, select *Unix Account (SSH Password)* default template.
7. In the *Fields* pane:
 - a. In the *Host* field, enter the IP address or the FQDN of the Linux server.
 - b. In the *Username* field, enter the username for the Linux server.
 - c. In the *Password* field, enter the password for the Linux server.
 - d. In the *Confirm Password* field that appears after the password is filled in, enter the password again.
8. In the *Secret Setting* pane:
 - a. Ensure that *Requires Checkout* is enabled.




Requires Checkout depends on the secret policy applied to the folder where the secret resides.

- b. In *Checkout Duration*, enter the duration for which the secret is checked out. In this example, *Checkout Duration* is set to 30 minutes (default).
- c. For added security, enable *Checkin Password Change*. This allows automatically changing the password when you check in.
- d. If needed, you can enable *Renew Checkout* and enter the maximum number of renewals allowed in *Max Renew Count*. This gives you additional exclusive access to the secret. In this example, the *Renew Checkout* option is disabled.

9. Click *Submit*.


Checking out a secret


 Since the secret has *Requires Checkout* enabled, you cannot directly launch the secret without first checking it out. The *Launch Secret* option is unavailable till you first check out the secret.



1. In *Secrets > Secret List*, select the newly created secret, and select *Check-out Secret*. If the check out is successful, the following message appears on the bottom-right:



2. Double-click the secret to open it and select *Launch Secret* from the top-right to launch the secret.

 In *Secret Details*, *Check-out Secret* option on the top-right is replaced with *Check-in Secret* once the secret has been checked out.

 In *Secret Details*, the *Checkout Status* pane on the right displays the current owner of the secret and the duration until they have access to it.

Checkout Status
 User **admin** has checked out this secret at 2023-04-27 12:21:21.
 Checkout time remaining: 00:27:39

3. In *Launch Progress*, select *PuTTY* to gain access to the Linux server. PuTTY is launched. You can now access the Linux server.



For other users who attempt to use the secret while it is checked out, they see a message indicating that someone else has checked out the secret, and the secret will only be available once it is checked in.

A Editing of the secret is disabled because
• The secret is being checked out.

Checking in a secret

To check in a secret:

1. In *Secrets > Secret List*, select the newly created secret, and select *Check-in Secret*.



Once you check in the secret, the *Launch Secret* button becomes unavailable.

If the check in is successful, the following message appears on the bottom-right:

✔ Successfully checked in secret ✕

Other approved users can now access the secret.

Using a secret requiring approval

This example demonstrates how to create an approval profile, create a secret that requires approval to access it, send a request for approval, approve the request (if you are an approver), and then access the secret once the approval is granted.

To use a secret requiring approval:

1. [Creating an approval profile on page 72](#)
2. [Creating a secret with mandatory approval requirement on page 73](#)
3. [Sending a request to access a secret on page 74](#)
4. [Approving a secret request on page 75](#)
5. [Launching a secret that requires approval on page 76](#)

Creating an approval profile

If there is no approval profile available on FortiPAM, you must create an approval profile.

To create an approval profile:

1. Go to *Secret Settings > Approval Profile*.
2. Select *Create* to create a new approval profile.
The *New Approval Profile* window opens.
3. Enter a name for the approval profile.

4. In *Number of Approval Tiers*, select the number of approval tiers the secret request is processed through. In this example, *Number of Approval Tiers* is *Two*.
5. Optionally, enter a description for the approval profile.
6. In the *Tier-1 Settings* pane:
 - a. In *Required number of Approvals*, enter the minimum number of approvals required from this tier so that the request is successfully forwarded to the next tier. In this example, *Required number of Approvals* is 1.
 - b. From *Approvers*, select + and from the list, select users in the *Select Entries* window. The selected users review the secret request. In this example, two users and a user group are selected.
7. Similar to step 6, set up the *Tier-2 Settings*. In this example, *Tier-2 Settings* require at least 1 approval from the tier consisting of two users.
8. Click *OK*.

Creating a secret with mandatory approval requirement

To create a secret with mandatory approval requirement:

1. Go to *Secrets > Secret List*.
2. In *Secret List*, select *Create*. The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.
4. Select *Create Secret*. The *New Secret* window opens.
5. Enter a name for the secret.
6. In the *Template* dropdown, select *Unix Account (SSH Password)* default template.
7. In the *Fields* pane:
 - a. In the *Host* field, enter the IP address or the FQDN of the Linux server.
 - b. In the *Username* field, enter the username for the Linux server.
 - c. In the *Password* field, enter the password for the Linux server.
 - d. In the *Confirm Password* field that appears after the password is filled in, enter the password again.

8. In the *Secret Setting* pane:
 - a. Enable *Requires Approval to Launch Secret*.
 - b. From the *Approval Profile* dropdown, select the approval profile created in [Creating an approval profile on page 72](#).
9. Click *Submit*.

The screenshot shows the 'New Secret' configuration window with the following details:

- General:** Name: approval_example, Folder: admin, Template: Unix Account (SSH Password), Associated Secret: No associated secret, Description: (empty).
- Fields:** Host: (empty), Username: admin, Password: (masked), Confirm Password: (masked).
- Secret Setting:**
 - Automatic Password Changing: Disable/Enable
 - Automatic Password Verification: Disable/Enable
 - Session Recording: Disable/Enable
 - Proxy Mode: Disable/Enable
 - Tunnel Encryption: Disable/Enable
 - Antivirus Scan: Disable/Enable
 - DLP Status: Disable/Enable
 - Requires Checkout: Disable/Enable
 - Requires Approval to Launch Secret: **Disable/Enable** (highlighted)
 - Requires Approval to Launch Job: Disable/Enable
 - Approval Profile: approval_profile_1

Sending a request to access a secret

To send a request to access a secret:

1. Go to *Secrets > Secret List*.
2. In the *Secrets List*, double-click the secret created in [Creating a secret with mandatory approval requirement on page 73](#) to open it.
3. On the top-right, click *Make Request* to send out a request to launch the secret. Alternatively, go to *Secrets > My Request List*, select *Create*. The *New secret request* window opens.
4. In *Request Type*, ensure that *Launcher* is selected.
5. In *Secret*, if you are making a request from the *Secrets List*, the secret is already selected. If you are creating an approval request in *Secrets > My Request List*, select a secret from the dropdown. These are secrets with *Requires Approval to Launch Secret* set as enabled.
6. In *Request Duration*, select a duration of time or select *Custom* and then enter a date (MM/DD/YYYY) and time range. Alternatively, select the calendar icon and select a start/end date and time. In this example, *1 hour* is selected.
7. Optionally, enter comments for the request in *Requester Comments*.

8. Click *Submit*.

New secret request

Requester: admin

Request Type: Launcher

Secret: approval_example

Request Duration: 1 hour

Start time: 05/04/2023 11:39 AM

End time: 05/04/2023 12:39 PM

Requester Comments:

Status

Tier 1 → Tier 2 → Final

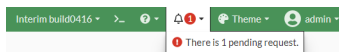
Submit Cancel

Once the request is submitted, it appears in *My Request List* tab in *Pending*.

The screenshot shows a dashboard with two donut charts: 'Request Type' (1 Launcher) and 'Availability' (1 Pending). Below the charts is a table with columns: Secret, Request Type, Tier Approval Progress, Start Time, Expiration Time, Duration, and Creation Time. A single row is visible for 'approval_example#1' with a 'Pending' status.

Approving a secret request

When an approver from the approval profile set in [Creating an approval profile on page 72](#) logs in to FortiPAM, the approver sees a notification that requires action.



The request that was made in [Sending a request to access a secret on page 74](#) appears in the *Approval List* tab in *Action is required*.

The screenshot shows a dashboard with two donut charts: 'Request Type' (1 Launcher) and 'Action Status' (1 Action is required). Below the charts is a table with columns: Secret, Request Type, Requestor, Requestor Comments, Creation Time, Start Time, Expiration Time, and Duration. A single row is visible for 'approval_example#2 - tier1' with a status of 'Action is required' and requestor 'admin'.

To approve a secret request:

1. From the notifications icon, select the pending approval request message to open the *Approval List* tab. Alternatively, go to *Secrets > Approval List*.
2. Select the secret request, and then select *Edit*. The *Approving secret request* window opens.



To override the requested duration:

In *Start time* and *End time*, select the *Calendar* icon and select a new date and time range to override the requested duration. Alternatively, enter a new date and time range.

- In the *Approval Status* pane, select *Approve* to approve the request.
- Optionally, enter comments related to the secret approval request.



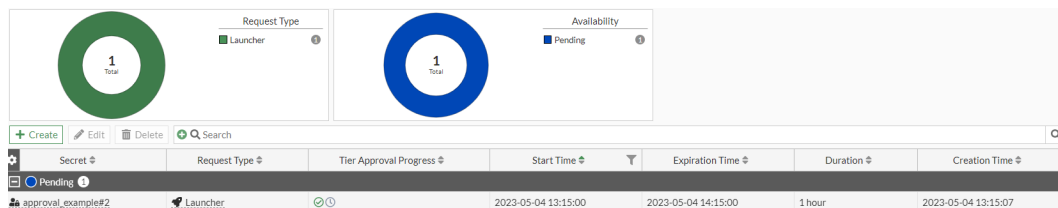
Approver comments are visible to the requester.

- Click *Save*.
Once approved, the *Approval Status* is updated. In this example, the request now moves to the next tier as configured in [Creating an approval profile on page 72](#).

Approval Status
Permission The request has moved onto next stage of approval



The requester can see the status of the secret approval request in the *Tier Approval Progress* column in *Secrets > My Request List*.



Once the request successfully passes through all the approval tiers (in this example the two approval tiers), the requester can now launch the secret.

Launching a secret that requires approval



Since the secret has *Requires Approval to Launch Secret* enabled, you cannot directly launch the secret without first sending an approval request which is then approved.
The *Launch Secret* option is unavailable until you get approval to access the secret.

To launch a secret that requires approval:

- Send a secret approval request as shown in [Sending a request to access a secret on page 74](#).
- Once the secret approval request is approved, in *Secrets > Secret List*, select the newly created secret, and select *Launch Secret*.
- In *Launch Progress*, select *PuTTY* to gain access to the Linux server.
PuTTY is launched. You can now access the Linux server.

Running a script on a target server using jobs

This example demonstrates how to create an approval profile, create a secret that requires approval to launch a job, create an ssh script type job, send a request to gain approval to execute a job, and approve the request (if you are an approver) to execute the job.

To run a script on a target server using jobs:

1. [Creating a job approval profile on page 77](#)
2. [Creating a secret with mandatory approval requirement for launching a job on page 78](#)
3. [Creating an ssh script type job on page 79](#)
4. [Sending a request to access the job on page 80](#)
5. [Approving a job request on page 81](#)
6. [Results on page 82](#)

Creating a job approval profile

If there is no approval profile available on FortiPAM, you must create an approval profile for jobs.

To create a job approval profile:

1. Go to *Secret Settings > Approval Profile*.
2. Select *Create* to create a new approval profile.
The *New Approval Profile* window opens.
3. Enter a name for the approval profile.
4. In *Number of Approval Tiers*, select the number of approval tiers the secret request is processed through.
In this example, *Number of Approval Tiers* is *Two*.
5. Optionally, enter a description for the approval profile.
6. In the *Tier-1 Settings* pane:
 - a. In *Required number of Approvals*, enter the minimum number of approvals required from this tier so that the request is successfully forwarded to the next tier.
In this example, *Required number of Approvals* is 1.
 - b. From *Approvers*, select *+* and from the list, select users in the *Select Entries* window.
The selected users review the secret request.
In this example, two users and a user group are selected.
7. Similar to step 6, set up the *Tier-2 Settings*.
In this example, *Tier-2 Settings* require at least 1 approval from the tier consisting of two users.

8. Click *OK*.

Creating a secret with mandatory approval requirement for launching a job

To create a secret with mandatory approval requirement for launching a job:

1. Go to *Secrets > Secret List*.
2. In *Secret List*, select *Create*.
The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.
4. Select *Create Secret*.
The *New Secret* window opens.
5. Enter a name for the secret.
6. In the *Template* dropdown, select *Unix Account (SSH Password)* default template.
7. In the *Fields* pane:
 - a. In the *Host* field, enter the IP address or the FQDN of the Linux server.
 - b. In the *Username* field, enter the username for the Linux server.
 - c. In the *Password* field, enter the password for the Linux server.
 - d. In the *Confirm Password* field that appears after the password is filled in, enter the password again.
8. In the *Secret Setting* pane:
 - a. Enable *Requires Approval to Launch Job*.
 - b. From the *Approval Profile* dropdown, select the approval profile created in [Creating a job approval profile on page 77](#).

9. Click *Submit*.

The screenshot shows the 'New Secret' configuration interface. The 'General' tab is selected, displaying the following fields and settings:

- Name:** job_example
- Folder:** admin
- Template:** Unix Account (SSH Password)
- Associated Secret:** No associated secret
- Description:** (empty text area)
- Fields:**
 - Host:** (empty text field)
 - Username:** admin
 - Password:** (masked with dots)
 - Confirm Password:** (masked with dots)
- Secret Setting:**
 - Automatic Password Changing: Disable
 - Automatic Password Verification: Disable
 - Session Recording: Disable
 - Proxy Mode: Disable
 - Tunnel Encryption: Disable
 - Antivirus Scan: Disable
 - DLP Status: Disable
 - Requires Checkout: Disable
 - Requires Approval to Launch Secret: Disable
 - Requires Approval to Launch Job: Disable
 - Approval Profile: approval_profile_job

At the bottom of the window, there are 'Submit' and 'Cancel' buttons.

Creating an ssh script type job

To create an ssh script type job:

1. Go to *Secrets > Job List*.
2. Select *+Create*.
The *New Job* window opens.
3. Enter a name for the job.
4. In the *Type* dropdown, select *SSH Script* to target secrets that work on linux-like machines.
5. Enable *Status* to allow the execution of the job.
6. From the *Secret* dropdown, select the secret created in [Creating a secret with mandatory approval requirement for launching a job on page 78](#).
7. In *Start Time*, enter date (MM/DD/YYYY) and time or select the *Calendar* icon and then select a date and time.
This is time when the script is first executed.
8. In *Script*, enter the script to be executed on the target server.
9. Click *Submit*.
In this example, the script is executed one-time only at the *Start Time* set in step 7.

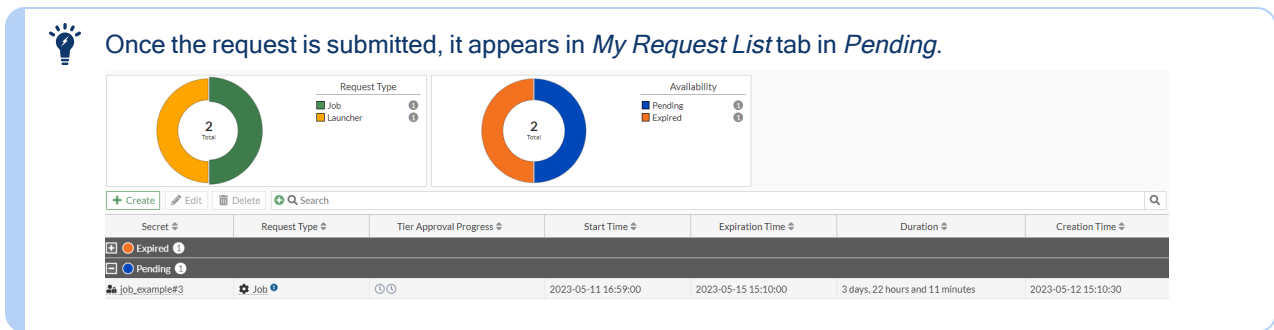
Sending a request to access the job

To send a request to access the job:

1. Go to *Secrets > Job List*.
2. In the *Job List*, double-click the job created in [Creating an ssh script type job on page 79](#) to open in.
3. On the top, click *Make Request* to send out a request to access the job.
Alternatively, go to *Secrets > My Request List*, select *Create*.
The *New secret request* window opens.
4. In *Request Type*, ensure that *Job* is selected.
5. In *Job*, if you are making a request from the *Job List*, the job is already selected.
If you are creating an approval request in *Secrets > My Request List*, select the job created in [Creating an ssh script type job on page 79](#) from the dropdown.
The secret associated with the job is already selected and cannot be changed. This is the secret set up in [Creating a secret with mandatory approval requirement for launching a job on page 78](#) with *Requires Approval to Launch Job* option enabled.
6. In *End time*, enter an end date (MM/DD/YYYY) and time by when the job request must be approved.

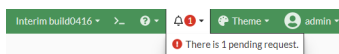
 The job request cannot be approved past the time set in *End time*.

7. Optionally, enter comments for the request in *Requester Comments*.
8. Click *Submit*.

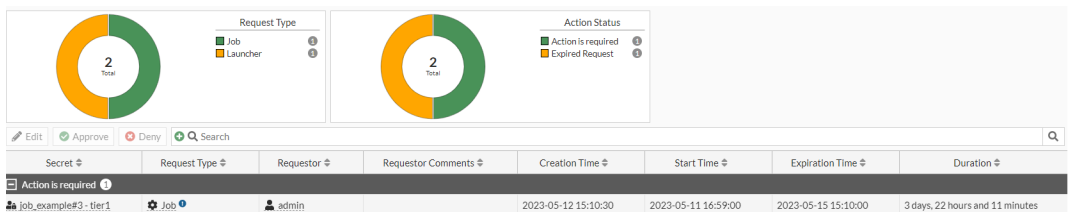


Approving a job request

When an approver from the approval profile set in [Creating a job approval profile on page 77](#) logs in to FortiPAM, the approver sees a notification that requires action.




The request that was made in [Sending a request to access the job on page 80](#) appears in the *Approval List* tab in *Action is required*.




To approve a job request:

1. From the notifications icon, select the pending approval request message to open the *Approval List* tab. Alternatively, go to *Secrets > Approval List*.
2. Select the secret request, and then select *Edit*. The *Approving secret request* window opens.

 **To override the requested duration:**
 In *Start time* and *End time*, select the *Calendar* icon and select a new date and time range to override the requested duration. Alternatively, enter a new date and time range.

3. In the *Approval Status* pane, select *Approve* to approve the request.
4. Optionally, enter comments related to the secret approval request.

 Approver comments are visible to the requester.

5. Click *Save*.
 Once approved, the *Approval Status* is updated. In this example, the request now moves to the next tier as configured in [Creating a job approval profile on page 77](#).



 The requester can see the status of the job approval request in the *Tier Approval Progress* column in *Secrets > My Request List*.

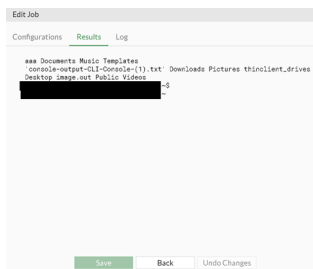


When the request has successfully passed through all the approval tiers (in this example the two approval tiers):

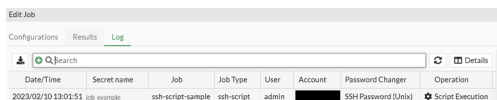
- Only the *Status* option when [Creating an ssh script type job on page 79](#) can be edited. The other options become noneditable.
- The script related job now runs.

Results

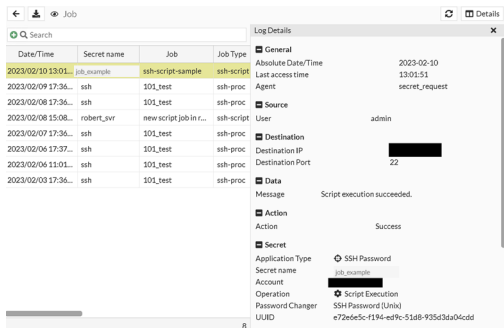
After a job is executed, you can check the results by double-clicking the job in *Secrets > Job List* and going to the *Results* tab. This is the job set up in [Creating an ssh script type job on page 79](#).



If you have permission to view logs, you can also see when the job was executed before by switching to the *Log* tab.



Alternatively, you can go to *Log & Report > Secret > Job* to view additional details related to the job.



Configuring a secret that supports TOTP

This example demonstrates how FortiPAM can be configured to support TOTP.

SSH secrets support TOTP auto-delivery when launched.

To configure a secret that supports TOTP:

1. [Configuring a secret template with TOTP on page 83](#)
2. [Creating a secret with TOTP enabled on page 85](#)

Limitations

1. TOTP auto delivery only supports SSH target and RDP authentication.
2. TOTP auto delivery for RDP needs the FortiAuthenticator agent running in the target machine and security level set to TLS.
3. Password changer does not support public key + TOTP authentication.
4. With TOTP, WebSSH only supports keyboard-interactive authentication method.
5. With the non-proxy launcher or web launcher, TOTP code must be copied and entered manually.
6. Do not enable the password changer for the SSH server with password + FortiToken authentication if the username, password, and FortiToken are from another LDAP server.

Configuring a secret template with TOTP

To configure a secret template with TOTP:

1. Go to *Secret Settings > Templates*.
2. In the secret template list, select *Create*.
The *General* tab in the *New Secret Template* window opens.
3. In the *General* tab:
 - a. In *Name*, enter a name for the secret template.
 - b. Optionally, enter a description for the secret template.
 - c. In *Sever Information*, select *Unix-Like*.
4. In the *Fields* pane, select *Create* to add a new field.
The *New Field* window opens.
 - a. In *Field Name*, enter *Username*.
 - b. In the *Type* dropdown, select *Username*.
 - c. In the *Mandatory* dropdown, ensure that it is enabled.
 - d. Click *OK*.
5. Use steps in 4 to create the following fields:
 - a. *Public-Key* (disabled)
 - b. *Private-Key* (disabled)
 - c. *Passphrase* (disabled)
 - d. *URL* (enabled)

6. In the *Launcher* pane, select *Create* to add a new launcher. The *New Launcher Selection* window opens.
 - a. In *Launcher Name* dropdown, select *PuTTY*.
 - b. In the *Launcher Port*, ensure that port *22* is selected.
 - c. Click *OK*.
7. Use steps in 6 to select *Web SSH* launcher.
8. In the *Password Changer* pane:
 - a. In *Password Changer*, select *SSH Key (FortiProduct)*.
 - b. Ensure that remaining settings in the *Password Changer* pane are on default.
9. In the *TOTP Setting* pane:
 - a. In *Length*, *Duration*, and *Hash Algorithm*, ensure that the default values are used.

Notes:

- *Length*: Number of digits in the TOTP code.
- *Duration*: Period of time for which the TOTP code is valid.
- *Hash Algorithm*: HMAC algorithm used to generate the TOTP code.

10. Click *Submit*.

General | Permission

Name: test_TOTP
Description:

Server Information: **Unix-Like** | Cisco | FortiOS | Other

Fields

Field Name	Type	Mandatory
Username	Text	Enable
Public-Key	Public-Key	Disable
Private-Key	Text	Disable
Passphrase	Passphrase	Disable
URL	URL	Enable

Launcher

ID	Launcher	Port	Integrity Check
1	PuTTY	22	disable
2	Web SSH	22	disable

Password Changer

Password Changer: SSH Key (FortiProduct)
Port: 22
Max Number of Verification Retries: 10
Verify After Password Change: Enable

TOTP Setting

Length: 6
Duration: 30 Seconds
Hash Algorithm: HMAC-SHA-1

Submit | Cancel

 Generally, you should avoid changing secret template TOTP settings, if a target server requires special TOTP setting, you can configure this from the *TOTP Setting* pane when creating or editing the secret.

Creating a secret with TOTP enabled

Here, we create a secret with TOTP enabled using the secret template configured in [Configuring a secret template with TOTP on page 83](#).



In case, you require special TOTP setting for the secret, you can:

- Ask the administrator to change the secret TOTP setting using the CLI or change it yourself if you have the CLI permission.
- Clone a new secret template and configure the TOTP setting according to your requirement.

To create a secret with TOTP enabled:

1. Go to *Secrets > Secret List*.
2. In *Secret List*, select *Create*.
The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.
4. Select *Create Secret*.
The *New Secret* window opens.
5. Enter a name of the secret.
6. In the *Template* dropdown, select the template created in [Configuring a secret template with TOTP on page 83](#).
7. In the *Fields* pane:
 - a. In *Username*, enter a username.
 - b. In *URL*, enter the URL for the target server.
8. In the *TOTP Setting* pane:
 - a. Enable *TOTP Status*.
 - b. In *Verification Code with*, select *FortiToken*.
If the target server uses a 3rd party TOTP solution such as Google Authenticator, select *3rd Party*.
 - c. When using FortiToken Mobile as the TOTP mobile application, an activation code from the FortiToken Mobile token issuer is required to activate the token. In that case, you must provide the activation token, and FortiPAM then acts as a surrogate for the FortiToken Mobile application.
In *Activation Code*, enter the FortiToken Mobile activation code.
When *3rd Party* is selected in *Verification Code with*, enter the shared key instead.
One of the ways you receive a shared key from a 3rd party provider is by scanning QR code. Usually, when you enable TOTP service, the 3rd party provider should send you a message that includes the shared key.
For example, in case of Google Authenticator, you receive a QR code once you enable the TOTP service. By scanning the QR code, you receive a string of random numbers and characters. This string is the shared key.
9. Click *Submit*.

SSH authentication challenge setting

If the SSH target server requires a keyboard-interactive authentication, it requests one or more challenge responses during the authentication process.

In most cases, when a challenge/response occurs, the server asks for a password or code. The client must respond with the corresponding password or code.

In FortiPAM, password and code, i.e., TOTP or any other code, are the two built-in case tolerant challenge patterns.

If a more specific challenge is required, you can add a new challenge pattern to FortiPAM via the CLI:

```
config ssh-challenge pattern
  edit a-new-pattern
    set type password
  next
end
```

Accessing a MySQL server using MySQL CLI launcher

This example demonstrates how to access an MySQL server by setting up a database server based secret on FortiPAM and then using the MySQL CLI launcher to remotely gain access to the MySQL server.

The database server secret template is a basic default secret template for MySQL servers. In the database server secret template, username and password are used for authentication.

To access an MySQL server using MySQL CLI:

1. [Creating a secret using the database server template on page 86](#)
2. [Launching a secret for the MySQL server on page 87](#)

Creating a secret using the database server template

To create a secret using the database server template:

1. Go to *Secrets > Secret List*.
2. In *Secret List*, select *Create*.
The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.
4. Select *Create Secret*.
The *New Secret* window opens.
5. Enter a name of the secret.
6. In the *Template* dropdown, select *Database Server* default template.
7. In the *Fields* pane:
 - a. In *Host*, enter the IP address of the MySQL server.
 - b. In *Username*, enter the username for the MySQL server.
 - c. In *Password*, enter the password for the MySQL server.
 - d. In the *Confirm Password* field that appears after the password is filled in, enter the password again.

Configuring integrity check for the PuTTY launcher

In this example, we configure integrity check for the PuTTY launcher.

Using the integrity check feature of FortiPAM, you can prevent launching of corrupt executables.

For every client software, we can configure multiple packages to compare. An integrity check is considered passed when at least one version of the client software package is matched. Therefore, this allows us to support the integrity check with different software versions.

When the integrity check fails, secret launching stops and a prompt appears showing where to download a version of the client software based on your FortiPAM configurations.

For more information on the integrity check feature, see [Integrity Check](#) in the latest *FortiPAM Administration Guide*.


To configure integrity check for the PuTTY launcher:

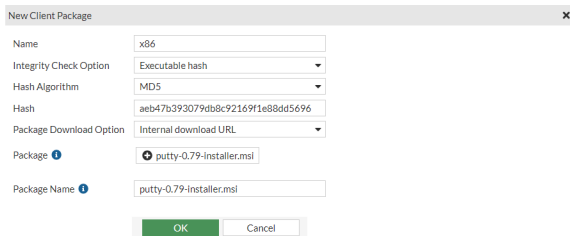
1. [Creating an entry for the PuTTY launcher on page 88](#)
2. [Enabling integrity check in the launcher and secret template on page 89](#)
3. [Creating a secret with integrity check on page 90](#)
4. [Launching the secret on page 91](#)

Creating an entry for the PuTTY launcher

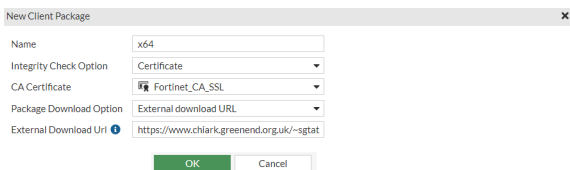
To create an entry for the PuTTY launcher:

1. Go to *Secret Settings > Integrity Check* and select *Create*.
The *New Client Software* window opens.
2. In *Name*, enter *putty*.
3. In the *Package* pane, select *Create*.
The *New Client Package* window opens.
4. In the first client package, we check if the software is a 32-bit version by checking the executable hash with MD5. We also intend to store a copy of the software on the FortiPAM disk for the user to download.
 - a. In *Name*, enter *x86*.
 - b. In *Integrity Check Option*, select *Executable hash*.
 - c. In the *Hash Algorithm* dropdown, select *MD5*.
 - d. In the *Hash field*, enter the client package hexadecimal hash value.

 We use the `Certutil -hashfile filename MD5` command and replace the filename with the path to the uncorrupted software (`putty.exe`) to generate the hash field.
 - e. In the *Package Download Option* dropdown, select *Internal download URL*.
 - f. In *Package*, select *+Upload File*, locate the PuTTY MSI file from your management computer, and click *Open*.
The PuTTY MSI file is provided when the integrity check fails.
 - g. Click *OK*.



5. In the second client package, we check the certificate of the software to see if it is the latest 64-bit version. In this case, we do not store a local copy of the software. Instead, we provide an official link to the 64-bit version of PuTTY (MSI file) in the *External Download Url* field.
 - a. In *Name*, enter *x64*.
 - b. In *Integrity Check Option*, select *Certificate*.
 - c. In *CA Certificate*, select the *Fortinet_CA_SSL* certificate.
 - d. In *Package Download Option*, select *External download URL*.
 - e. In *External Download Url*, enter the official download URL for the 64-bit version of PuTTY (MSI file).
 - f. Click *OK*.



6. Click *Submit*.

Enabling integrity check in the launcher and secret template

An integrity check entry was created for the default PuTTY launcher in [Creating an entry for the PuTTY launcher on page 88](#).

To enable integrity check in the launcher:

1. Go to *Secret Settings > Launchers*.
2. In the secret launchers list, select *PuTTY* and then select *Edit*.
The *Edit Secret Launcher* window opens.
3. Enable *Client Software*, and from the dropdown select the client software entry created in [Creating an entry for the PuTTY launcher on page 88](#).

4. Click **Save**.

Only client software is editable in default launcher.

Name: PuTTY
 Type: SSH client
 File Launcher: True False
 Executable:
 Parameter:
 Client Software: putty

Initial Commands

ID	Command
No results	


Clean Commands

ID	Command
No results	

Save Back Discard Changes

To enable integrity check in the secret template that uses the PuTTY launcher:

1. Go to *Secret Settings > Templates*.
2. In the secret templates list, select *FortiProduct (SSH Key)* and then select *View*.

 *FortiProduct (SSH Key)* template uses PuTTY as one of its launchers.

3. In the *Launcher* pane, select *PuTTY* and then select *Edit*.
The *Edit Launcher Selection* window opens.
4. Enable *Integrity Check*.
5. Click *OK*.
6. Click *Save*.

Edit Launcher Selection

Launcher Name: PuTTY
 Launcher Port: 22
 Integrity Check: Disable Enable

OK Cancel

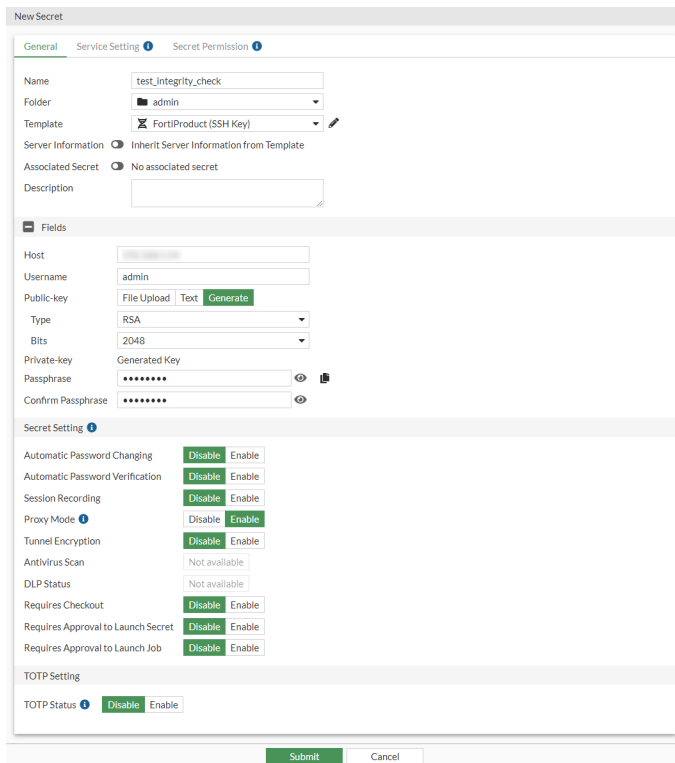
Creating a secret with integrity check

We now create a secret that uses the *FortiProduct (SSH Key)* secret template and PuTTY as the launcher. This ensures that every time the secret is launched, it includes integrity check.

To create a secret with integrity check:

1. Go to *Secrets > Secret List*.
2. In *Secret List*, select *Create*.
The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.

4. Select *Create Secret*.
The *New Secret* window opens.
5. Enter a name for the secret.
6. In the *Template* dropdown, select *FortiProduct (SSH Key)*.
FortiProduct (SSH Key) is the template where we enabled integrity check for the PuTTY launcher in [Enabling integrity check in the launcher and secret template on page 89](#).
7. In the *Fields* pane:
 - a. In *Host*, enter the IP address of the target server.
 - b. In *Username*, enter the username for the target server.
 - c. In *Public-key*, select *Generate*:
 - i. In *Type*, select *RSA* encryption algorithm.
 - ii. In *Bits*, select *2048*.
 - d. In *Passphrase*, enter a passphrase.
 - e. In the *Confirm Passphrase* field that appears after the passphrase is filled in, enter the passphrase again.
8. Click *Submit*.



Launching the secret

Here, we launch the secret created in [Creating a secret with integrity check on page 90](#).

To launch the secret:

1. In *Secrets > Secret List*, select the newly created secret, and select *Launch Secret*.
2. In *Launch Progress*, select *PuTTY*.
In [Enabling integrity check in the launcher and secret template on page 89](#), we enabled integrity check for the PuTTY launcher.
PuTTY is launched and an integrity check is performed. If the integrity check is successful, you can then access the target server.

Block uploading a JavaScript file via the Web SFTP launcher

This example demonstrates how you can block uploading of a JavaScript file from the client side to the target using the FortiPAM Web SFTP launcher.

To block uploading a JavaScript file:

1. [Configuring the DLP file pattern on page 92](#)
2. [Configuring a DLP sensor profile on page 93](#)
3. [Creating a secret with a DLP sensor profile on page 94](#)
4. [Results on page 95](#)

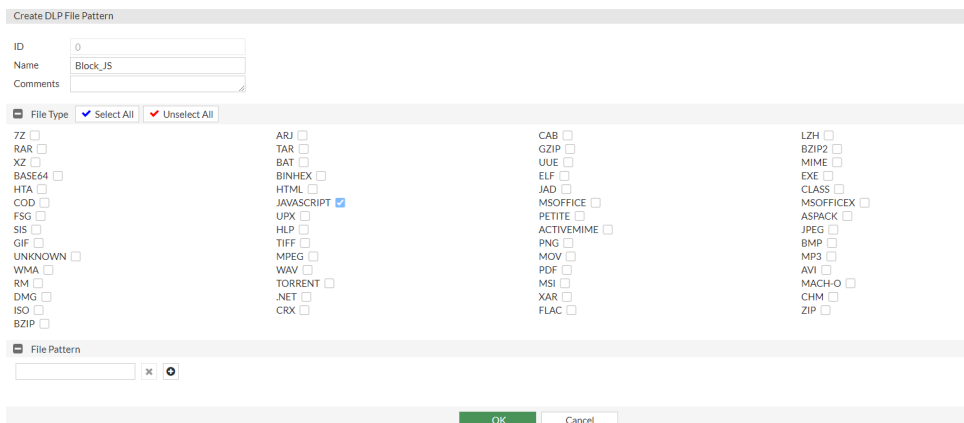
Configuring the DLP file pattern

Here, we configure a DLP file pattern for JavaScript file type.

To configure the DLP file pattern:

1. Go to *Secret Settings > DLP File Pattern*.
2. From the DLP file pattern list, select *Create New*.
The *Create DLP File Pattern* window opens.
3. In *Name*, enter a name for the DLP file pattern.
4. In the *File Type* pane, select *JAVASCRIPT*.

5. Click *OK*.

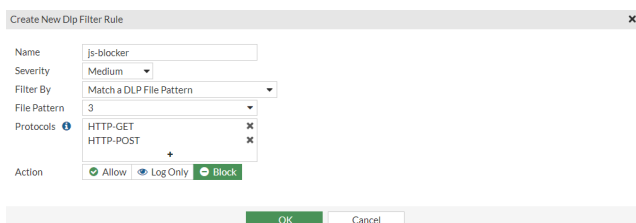


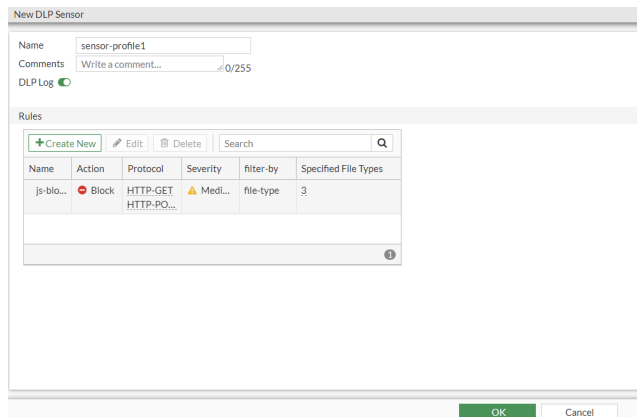
Configuring a DLP sensor profile

Here, we configure a DLP sensor profile with a DLP filter rule that blocks JavaScript files. The DLP file pattern for JavaScript files was configured in [Configuring the DLP file pattern on page 92](#).

To configure a DLP sensor profile:

1. Go to *Secret Settings > Data Leak Prevention*.
2. From the DLP sensors list, select *Create New*.
The *New DLP Sensor* window opens.
3. In *Name*, enter the name for the DLP sensor.
4. In the *Rules* pane, select *Create New* to create a new DLP filter rule.
The *Create New Dlp Filter Rule* window opens.
5. In *Name*, enter a name for the DLP filter rule.
6. In the *Severity* dropdown, select *Medium*.
7. In the *Filter By* dropdown, select *Match a DLP File Pattern*.
8. In the *File Pattern* dropdown, select the DLP file pattern (by ID) created in [Configuring the DLP file pattern on page 92](#).
9. In the *Protocols* dropdown:
 - a. Select *+*.
 - b. In the *Select Entries* window, select *HTTP-GET* and *HTTP-POST*.
 - c. Click *Close*.
10. In *Action*, select *Block*.
11. Click *OK*.
12. Click *OK*.





Creating a secret with a DLP sensor profile

Now, we create a Unix account secret that uses the DLP sensor profile configured in [Configuring a DLP sensor profile on page 93](#).

To create a secret with DLP sensor profile:

1. Go to *Secrets > Secret List*.
2. In *Secret List*, select *Create*.
The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.
4. Select *Create Secret*.
The *New Secret* window opens.
5. Enter a name for the secret.
6. In the *Template* dropdown, select *Unix Account (SSH Password)*.
7. In the *Fields* pane:
 - a. In *Host*, enter the IP address of the target SFTP server.
 - b. In *Username*, enter the username for the target SFTP server.
 - c. In *Password*, enter a password.
 - d. In the *Confirm Password* field that appears after the password is filled in, enter the password again.
8. Ensure that *Proxy Mode* is enabled.
Enabling proxy mode ensures that FortiPAM proxies the connection between the user and the target.
9. Enable *DLP Status*.
10. In the *DLP Profile* dropdown, select the DLP sensor profile created in [Configuring a DLP sensor profile on page 93](#).

11. Click *Submit*.

Results

Once the secret created in [Creating a secret with a DLP sensor profile on page 94](#) is launched via the Web SFTP launcher and the user attempts to upload a JavaScript file, FortiPAM blocks this operation, and a log entry is created in *Log & Report > Data Leak Prevention*.

Date/Time	User	Source IP	Service	URL	Action	File Name	Filter Index	DLP Extra	Filter Type	Filter Co
13:28:23:89	admin	admin	SFTP		block	sample1.js	1	block.js	file-type	file

Block transferring .exe files and log file downloads of size larger than 500KB

This example demonstrates how you can block transfer of .exe files and log file downloads/uploads of size larger than 500KB from the client side to the target using the FortiPAM WinSCP launcher.

To block transferring .exe files larger than 500KB in size:

1. [Configuring the DLP file pattern on page 96](#)
2. [Configuring a DLP sensor profile on page 96](#)
3. [Creating a secret with a DLP sensor profile on page 98](#)
4. [Results on page 99](#)

Configuring the DLP file pattern

Here, we configure a DLP file pattern for .exe file type.

To configure the DLP file pattern:

1. Go to *Secret Settings > DLP File Pattern*.
2. From the DLP file pattern list, select *Create New*.
The *Create DLP File Pattern* window opens.
3. In *Name*, enter a name for the DLP file pattern.
4. In the *File Type* pane, select *EXE*.
5. Click *OK*.

The screenshot shows the 'Edit DLP File Pattern' dialog box. At the top, there are fields for 'ID' (value: 3), 'Name' (value: Block_exe), and 'Comments'. Below these is a 'File Type' section with two buttons: 'Select All' (checked) and 'Unselect All'. A grid of file types follows, each with a checkbox. The 'EXE' checkbox is checked, while others are unchecked. At the bottom, there is a 'File Pattern' field and 'OK' and 'Cancel' buttons.

Configuring a DLP sensor profile

Here, we configure a DLP sensor profile with the following two DLP filter rules:

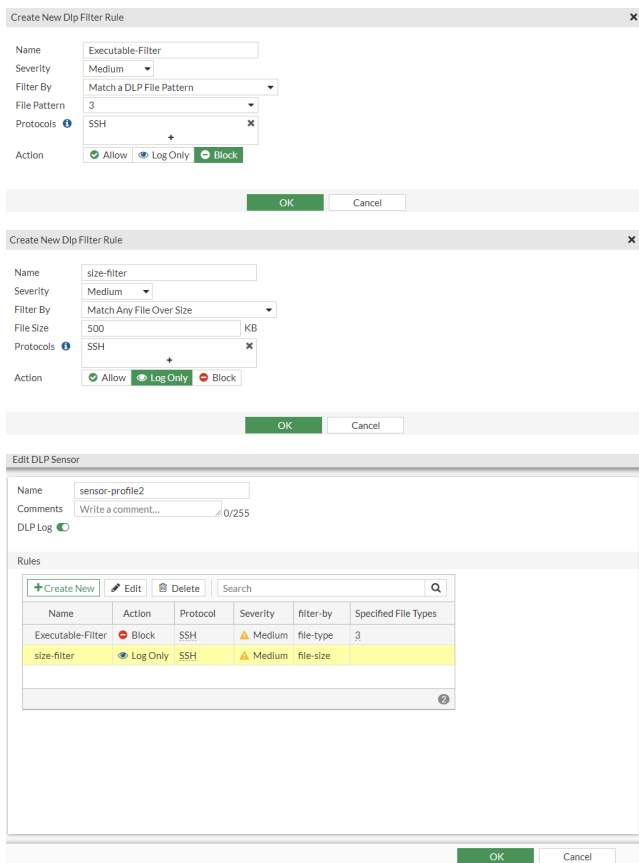
- A DLP filter rule that blocks transfer of .exe files.
- A DLP filter rule that logs download/upload of files larger than 500KB in size.

The DLP file pattern for .exe files was configured in [Configuring the DLP file pattern on page 96](#).

To configure a DLP sensor profile:

1. Go to *Secret Settings > Data Leak Prevention*.
2. From the DLP sensors list, select *Create New*.
The *New DLP Sensor* window opens.
3. In *Name*, enter the name for the DLP sensor.
4. In the *Rules* pane, select *Create New* to create a new DLP filter rule:
The *Create New Dlp Filter Rule* window opens.
 - a. In *Name*, enter a name for the DLP filter rule.
 - b. In the *Severity* dropdown, select *Medium*.
 - c. In the *Filter By* dropdown, select *Match a DLP File Pattern*.

- d. In the *File Pattern* dropdown, select the DLP file pattern (by ID) created in [Configuring the DLP file pattern on page 96](#).
 - e. In the *Protocols* dropdown:
 - i. Select *+*.
 - ii. In the *Select Entries* window, select *SSH*.
 - iii. Click *Close*.
 - f. In *Action*, select *Block*.
 - g. Click *OK*.
5. In the *Rules* pane, select *Create New* to create another DLP filter rule:
The *Create New Dlp Filter Rule* window opens.
- a. In *Name*, enter a name for the DLP filter rule.
 - b. In the *Severity* dropdown, select *Medium*.
 - c. In the *Filter By* dropdown, select *Match Any File Over Size*.
 - d. In the *File Size* field, enter 500 (KB).
 - e. In *Action*, select *Log Only*.
 - f. Click *OK*.
6. Click *OK*.



Creating a secret with a DLP sensor profile

Now, we create a Unix account secret that uses the DLP sensor profile configured in [Configuring a DLP sensor profile on page 96](#).

To create a secret with DLP sensor profile:

1. Go to *Secrets > Secret List*.
2. In *Secret List*, select *Create*.
The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.
4. Select *Create Secret*.
The *New Secret* window opens.
5. Enter a name for the secret.
6. In the *Template* dropdown, select *Unix Account (SSH Password)*.
7. In the *Fields* pane:
 - a. In *Host*, enter the IP address of the target server.
 - b. In *Username*, enter the username for the target server.
 - c. In *Password*, enter a password.
 - d. In the *Confirm Password* field that appears after the password is filled in, enter the password again.
8. Ensure that *Proxy Mode* is enabled.
Enabling proxy mode ensures that FortiPAM proxies the connection between the user and the target.
9. Enable *DLP Status*.
10. In the *DLP Profile* dropdown, select the DLP sensor profile created in [Configuring a DLP sensor profile on page 96](#).
11. Click *Submit*.

The screenshot shows the 'Secret Details' configuration page for a secret named 'test_DLP_profile_2'. The page is divided into several sections:

- General:** Name (test_DLP_profile_2), Folder (admin), Template (Unix Account (SSH Password)), and Description.
- Server Information:** Inherit Server Information from Template (checked), Associated Secret (No associated secret), and a Description field.
- Fields:** Host (IP address), Username (admin), and Password (masked).
- Secret Setting:** A list of settings with 'Disable' and 'Enable' buttons:
 - Automatic Password Changing: Disable (selected), Enable
 - Automatic Password Verification: Disable (selected), Enable
 - Session Recording: Disable (selected), Enable
 - Proxy Mode: Disable (selected), Enable
 - Tunnel Encryption: Disable (selected), Enable
 - Antivirus Scan: Disable (selected), Enable
 - DLP Status: Disable (selected), Enable
 - DLP Profile: sensor-profile2 (selected)
 - Requires Checkout: Disable (selected), Enable
 - Requires Approval to Launch Secret: Disable (selected), Enable
 - Requires Approval to Launch Job: Disable (selected), Enable
- TOTP Setting:** TOTP Status: Disable (selected), Enable

At the bottom, there are buttons for 'Save', 'Back', and 'Discard Changes'.

Results

Once the secret created in [Creating a secret with a DLP sensor profile on page 98](#) is launched via the WinSCP launcher and the user attempts to download/upload a .exe file via the WinSCP launcher, FortiPAM blocks the operation.

When the user downloads/uploads a file larger than 500KB via the WinSCP launcher, FortiPAM generates a log entry in *Log & Report > Data Leak Prevention*.

Date/Time	%	User	Source IP	Service	URL	Action	File Name	Filter Index	DLP Extra
25 seconds ago		admin	admin	SSH		log-only	[MS-RDPBCGR]220429.pdf	2	500 kB
3 minutes ago		admin	admin	SSH		block	OBS-Studio-29.0-Full-Installer-x64.exe	1	block_exe

Updating a service account credential

In this example, we use the FortiPAM dependency updater feature to update the credential for a service running on a machine that relies on credential management by FortiPAM.

For detailed information on dependency updaters and service accounts, see [Dependency updater](#) in the latest *FortiPAM Administration Guide*.

To update a service account credential:


1. [Updating a service account credential on page 99](#)

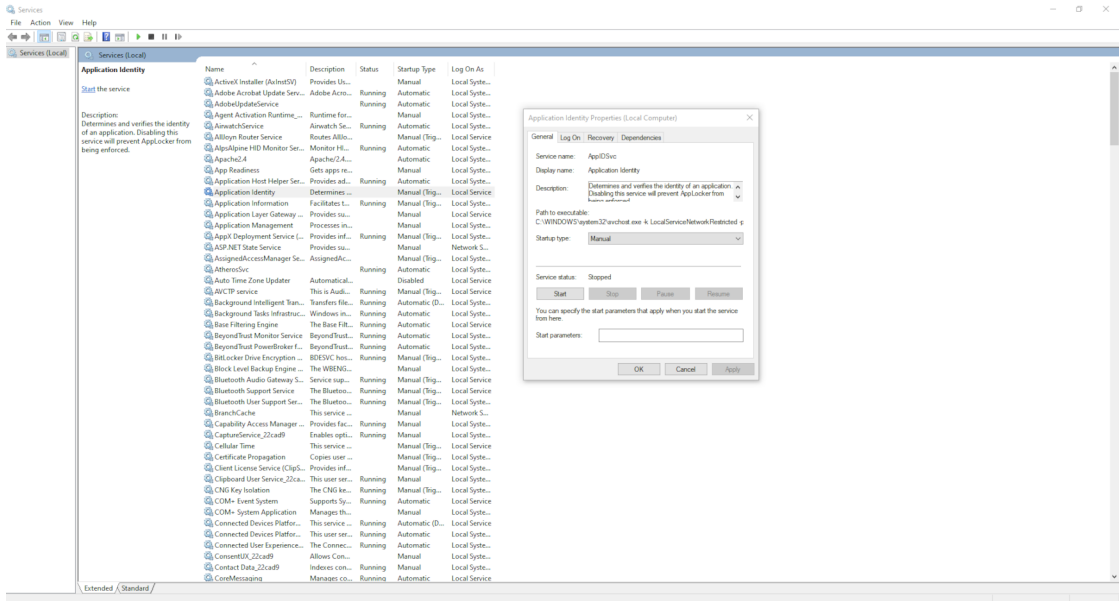
Updating a service account credential

To update a service account credential:

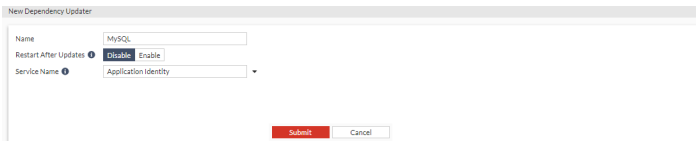
1. Go to *Secret Settings > Dependency Updater*.
2. Select *Create*.
The *New Dependency Updater* window opens.
3. In *Name*, enter a name for the dependency updater.
4. Set *Restart After Updates* to *Disable*.
If you intend to restart the service each time after updating the service credential, set *Restart After Updates* to *Enable*.

5. In the *Service Name* dropdown, select *Application Identity*.

 On Windows, the Service *Display name* is different from the *Service name*. For example, in *Services* on Windows, when you double-click *Application Identity*, you see that the *Service name* is *AppIDSvc*.



6. Click *Submit*.



7. Go to *Secrets > Secret List*.

8. Double-click the secret that you intend to use as the credential for a target where the service defined in the dependency updater runs.

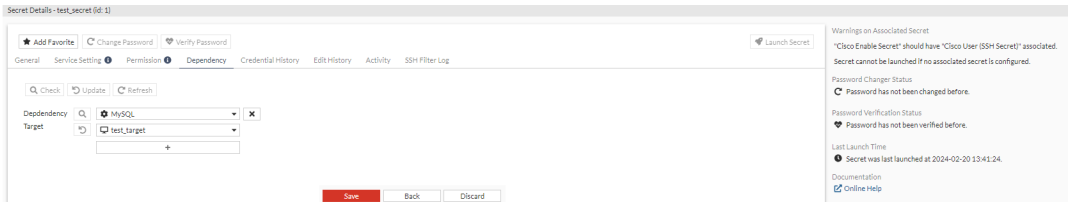
9. Select the *Dependency* tab.

10. Select \pm .

11. From the *Dependency* dropdown, select the dependency updater created earlier.


12. From the *Target* dropdown, select a target.

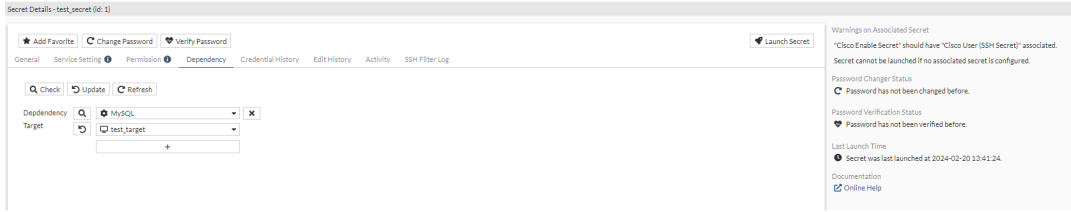
13. Click *Save*.




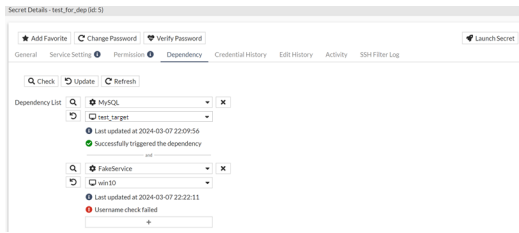

Once the secret password changer successfully rotates the secret password, all the dependencies in the secret are automatically updated.

 To update an individual dependency, click the *Update Dependency* (↻) icon on the left of each dependency when editing a secret.

 If needed, you can update all the dependencies by selecting *Update* from the top when editing the secret.



 Click the *Check Dependency* (🔍) icon on the left of each dependency to check if the service is running or not, and whether the service is running with the particular secret user name.



 To check all the dependencies in a secret, select *Check* from the top when editing a secret.

 To sync the current status of the dependencies, select *Refresh* from the top when editing a secret.

Creating a secret with the *Certificate Vault* template

Besides supporting launching secrets, FortiPAM supports the secret vault feature.

With the new default template *Certificate Vault*, you can store certificate with or without corresponding private key and passphrase in FortiPAM. The validity of this certificate will be monitored by FortiPAM.

Using the new *Certificate Vault* template, you can create secrets to store certificates in *Secrets > Secrets*.

To create a secret with the *Certificate Vault* template:

1. [Creating a certificate secret on page 102](#)
2. [Setting up email alert for certificate expiry on page 102](#)

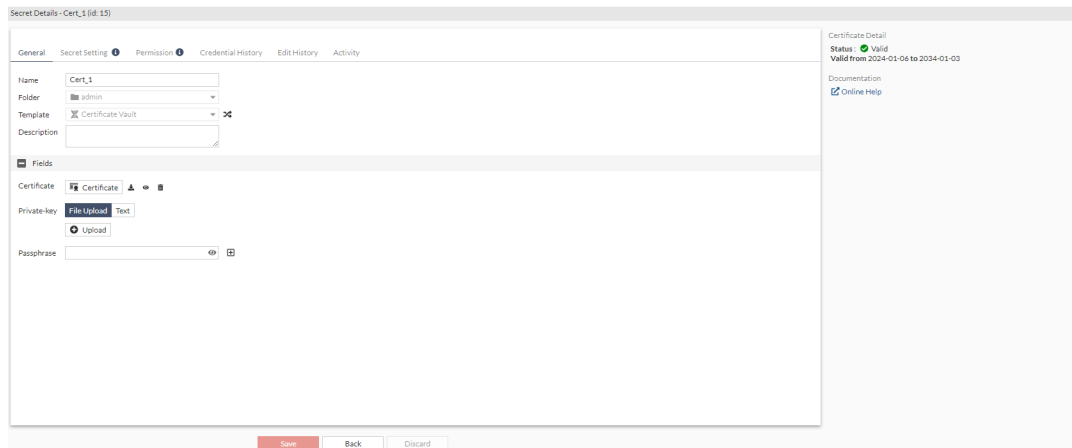
Limitation

PKCS type certificates are not supported.

Creating a certificate secret

To create a secret:

1. Go to *Secrets > Secrets*.
2. In Secrets List, select *Create*.
The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.
4. Select *Create*.
The *New Secret* window opens.
5. Enter the secret name.
6. Disable *Target*.
7. From *Template* dropdown, select the *Certificate Vault* template.
8. Optionally, enter a description.
9. In the *Fields* pane:
 - a. In *Certificate*, select *Upload*, from your management computer upload a certificate, and select *Open*.
 - b. Optionally, upload or enter a private key.
 - c. Optionally, enter a passphrase.
10. Click *Submit*.
The certificate is created.



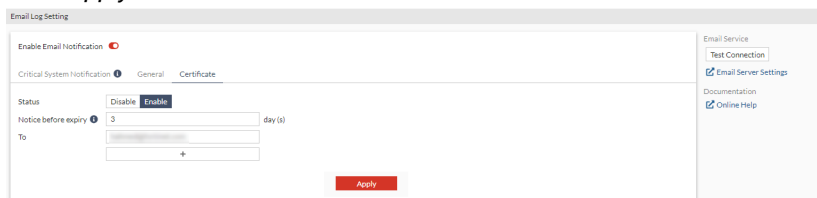
When the certificate secret is opened, the certificate status is displayed on the top-right under *Certificate Detail*.

Setting up email alert for certificate expiry

To set up email alert for certificate expiry:

1. Go to *Log & Report > Email Alert Settings*.
2. Ensure that *Enable Email Notification* is enabled.
3. Switch to the *Certificate* tab.

4. Keep the default value in *Notice before expiry*.
This is the number of days before the certificate expiry, alerts are sent, in days.
5. In *To*, enter the email address of the receiver.
6. Click *Apply*.



Configuring a secret using the *Target Only* secret template

The *Target Only* secret template requires preconfigured target address. You can enter the user name/password manually or use the current FortiPAM login automatically (SSO) when you launch the secret to access the target.

For more information on the *Target Only* secret template, see [Templates](#) in the latest *FortiPAM Administration Guide*.

The following examples demonstrate:

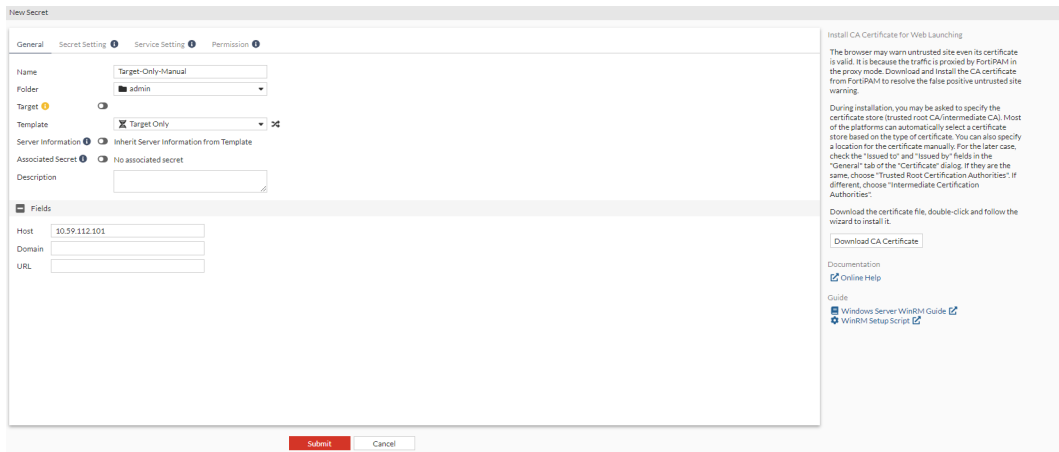
- Manually enter the user name/password to access the target.
One secret is used by many different logins to the same target.
See:
 - [Example 1: Creating a secret using the Target Only template on page 103](#)
 - [Example 1: Launching the secret on page 104](#)
- Automatically use the current FortiPAM login (SSO) to access the target.
User name/password are not required to be configured statically in a secret.
See:
 - [Example 2: Creating a secret using the Target Only template on page 105](#)
 - [Example 2: Launching the secret on page 106](#)

Example 1: Creating a secret using the *Target Only* template

To create a secret using the *Target Only* template:

1. Go to *Secrets > Secrets*.
2. In *Secrets List*, select *Create*.
The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.
4. Select *Create*.
The *New Secret* window opens.
5. Enter the secret name.
6. Disable *Target*.

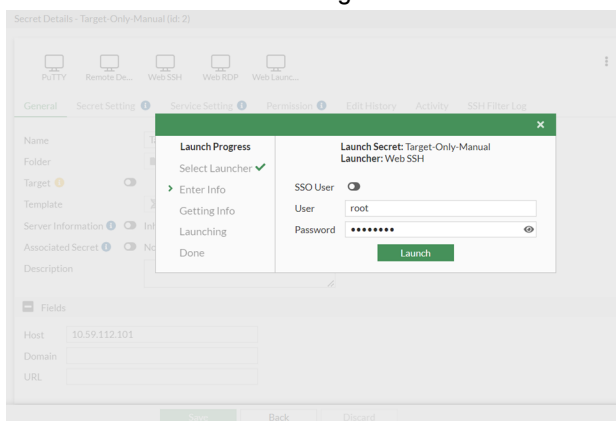
7. From the *Template* dropdown, select *Target Only*.
8. In the *Fields* pane:
 - a. In *Host*, enter the host IP address.
9. Click *Submit*.



Example 1: Launching the secret

To launch the secret:

1. Go to *Secrets > Secrets*.
2. From the *Secrets List*, double-click to open the secret created in [Example 1: Creating a secret using the Target Only template on page 103](#).
3. From the top, select *Web SSH*.
The *Launch Progress* dialog opens.
4. Enter the user name.
5. Enter the password.
6. Click *Launch* to access the target.



Example 2: Creating a secret using the *Target Only* template

Prerequisites

- FortiPAM user name/password: test-user/123.
Note: The user is not a SAML user.
- The target FortiGate has the same user name/password: test-user/123.

Both FortiPAM and the target FortiGate have the same credentials.

When using the credentials to log in to FortiPAM, the FortiPAM uses the same credentials to log in to the target FortiGate. This is SSO.

To create the secret using the *Target Only* template:

1. Go to *Secrets > Secrets*.
2. In Secrets List, select *Create*.
The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.
4. Select *Create*.
The *New Secret* window opens.
5. Enter the secret name.
6. Disable *Target*.
7. From the *Template* dropdown, select *Target Only*.
8. In the *Fields* pane:
 - a. In *URL*, enter the target URL.
9. Click *Submit*.

The screenshot shows the 'New Secret' configuration window in FortiPAM. The 'General' tab is active, showing the following configuration:

- Name:** Target-Only-SSO
- Folder:** admin
- Target:** (disabled)
- Template:** Target Only
- Server Information:** Inherit Server Information from Template
- Associated Secret:** No associated secret
- Description:** (empty)
- Fields:**
 - Host:** (empty)
 - Domain:** (empty)
 - URL:** http://10.99.112.121

On the right side, there is a section titled 'Install CA Certificate for Web Launching' with the following text:

The browser may warn untrusted site even its certificate is valid. It is because the traffic is proxied by FortiPAM in the proxy mode. Download and install the CA certificate from FortiPAM to resolve the false positive untrusted site warning.

During installation, you may be asked to specify the certificate store (Trusted root CA/Intermediate CA). Most of the platforms can automatically select a certificate store based on the type of certificate. You can also specify a location for the certificate manually. For the later case, check the "Issued for" and "Issued by" fields in the "General" tab of the "Certificate" dialog. If they are the same, choose "Trusted Root Certification Authorities". If different, choose "Intermediate Certification Authorities".

Download the certificate file, double-click and follow the wizard to install it.

[Download CA Certificate](#)

Documentation

[Online Help](#)

Guide

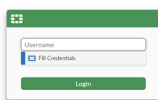
- [Windows Server WinRM Guide](#)
- [WinRM Setup Script](#)

At the bottom of the window, there are 'Submit' and 'Cancel' buttons.

Example 2: Launching the secret

To launch the secret:

1. Go to *Secrets > Secrets*.
2. From the Secrets List, double-click to open the secret created in [Example 2: Creating a secret using the Target Only template on page 105](#).
3. From the top, select *Web Launcher*.
The *Launch Progress* dialog opens.
4. Enable *SSO User*.
5. Click *Launch* to access the target.
6. On the target login page, select *Fill Credentials* to fill in the login credentials.



7. Click *Login* to log in to the target.

Smart association for Windows AD server as the target

This example demonstrates how smart association works for the Windows AD server as the target.

When using *Smart Association*, FortiPAM:

- Combines the account prefix and the currently logged-in username to generate a new username.
- Looks into the secret database to search for any secret username that matches the generated username.
- When a matching secret is found, its credentials are used to launch the secret.

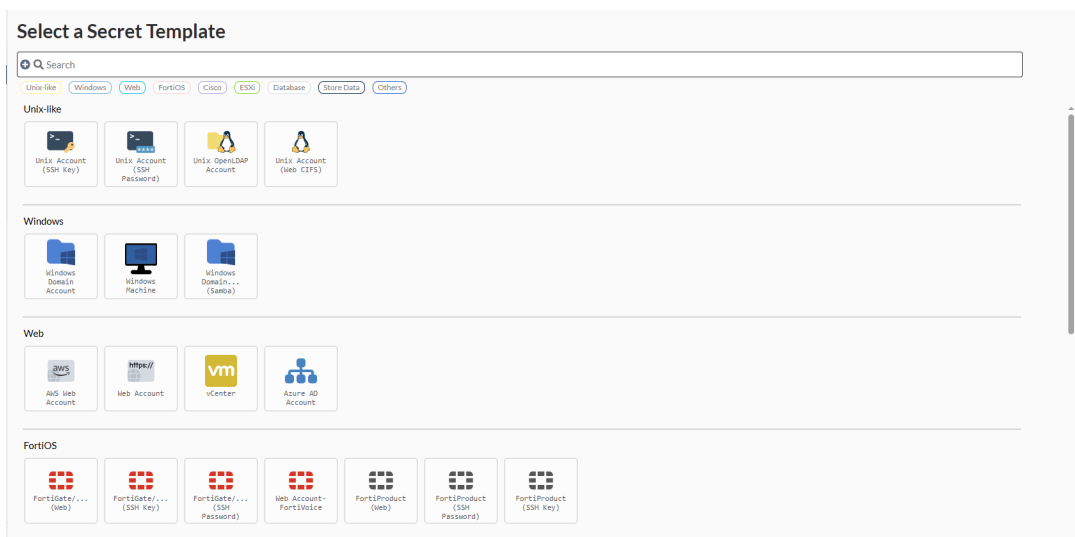
To set up smart association for Windows AD server as the target:

1. [Creating a secret with Windows Domain Account as the secret template on page 107](#)
2. [Creating a remote user on page 108](#)
3. [Results on page 109](#)

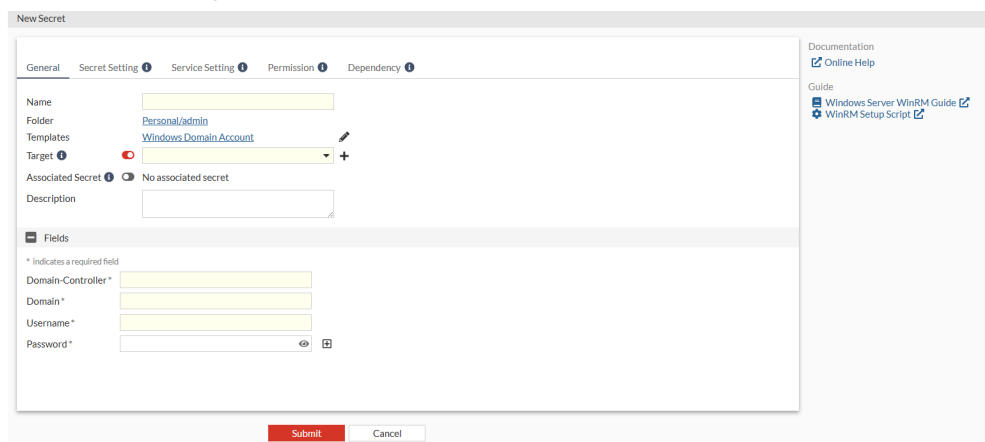
Creating a secret with Windows Domain Account as the secret template

To create the secret:

1. Go to *Secrets > Secrets*.
2. In *Secret List*, select *Create*.
The *Select a Secret Template* window opens.



3. In the *Windows* pane, select *Windows Domain Account*.
The *General* tab opens.



4. In *Name*, enter a name for the secret.
5. In *Target*, select the Windows AD server.
6. Enable *Associated Secret* and select *Smart Association* from the dropdown.
7. In *Account Prefix*, enter "fortipam."
8. In *Fields*:
 - a. In *Username*, enter a username.
 - b. In *Password*, enter the password.
 - c. Reenter the password to confirm.

9. Click *Submit*.

The screenshot shows the 'New Secret' configuration page in FortiPAM. The 'General' tab is selected, and the following fields are visible:

- Name: smart_218_base
- Folder: Personal/admin
- Templates: Windows.Domain Account
- Target: win_ad_218
- Privileged Account: Yes/No
- Associated Secret: Smart Association
- Account Prefix: fortipam.
- Description: (empty)

Below the 'General' tab is the 'Fields' section, which includes:

- Host: www.dco1.example.com
- Domain: dc01
- Username: (empty)
- Password: (masked with dots)
- Confirm Password: (masked with dots)

At the bottom right of the form, there are 'Submit' and 'Cancel' buttons.

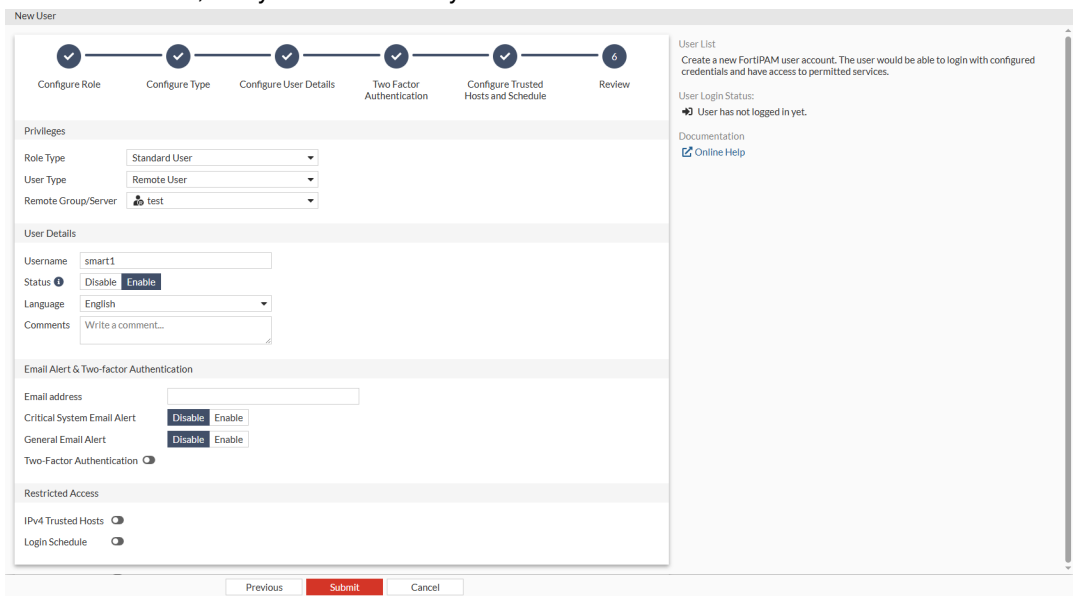
Creating a remote user

We create a new remote user located on a remote server smart1.

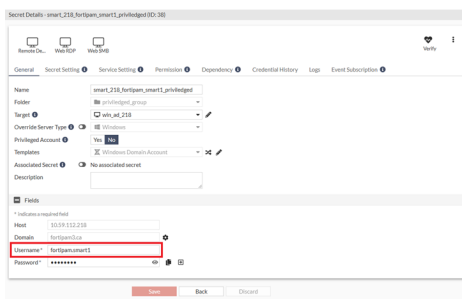
To create a remote user:

1. Go to *User Management > User List*, and select *Create*.
The *New User* wizard is launched.
2. In *User Privilege*, select *Standard User*, and click *Next*.
3. In *User Type*, select *Remote User*, and from *Choose a Remote Group where these users can be found*, select the remote user group, and click *Next*.
4. In *Username*, enter a username.
5. Ensure that *Status* is *Enable*.
6. Optionally, enter a description in *Comments*, and Click *Next*.
7. Click *Next*.
8. Click *Next*.

9. In the *Review* tab, verify the information you entered and click *Submit* to create the user.

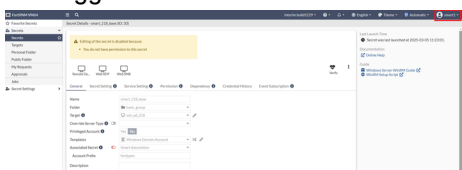


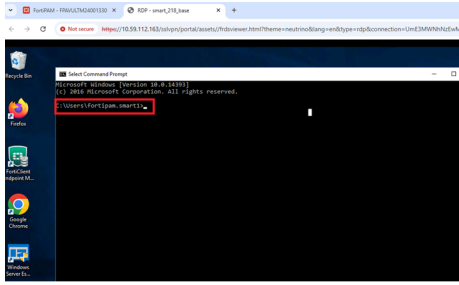
In the secret database, a secret with username containing the *Account Prefix* set in [Creating a secret with Windows Domain Account as the secret template on page 107](#) and the currently logged in user's username is expected, e.g., `fortipam.smart1`.



Results

1. When the user `smart1` logs in to FortiPAM, FortiPAM combines the account prefix and the currently logged-in username to generate a new secret username, i.e., `fortipam.smart1`.
2. FortiPAM then looks into the secret database to search for any secret username that matches the generated `fortipam.smart1` username.
3. The logged in `smart1` user can now launch the smart associated secret.





Access multiple Windows servers on the same domain

This example demonstrates how to access multiple Windows servers on the same domain.

The example uses:

- **Windows Domain server (AD server):** 10.59.112.200
- **Windows PCs in the domain:** 10.59.112.201 and 10.59.112.208
- A domain user

To access multiple Windows servers on the same domain:

1. [Creating targets on page 110](#)
2. [Creating a secret for the domain user on page 112](#)
3. [Creating a secret for the Windows PC- 10.59.112.201 and Windows PC- 10.59.112.208 on page 112](#)
4. [Sharing secrets to a contractor on page 113](#)
5. [Result on page 115](#)

Creating targets

We create three targets: one for the AD server and another two for PCs in the domain control.

To create a *Windows Domain Account* target:

1. Go to *Secrets > Targets*.
2. Select *+Create*.
The *New Secret Target* window opens to the *General* tab.
3. In *Classification Tag*, select a classification tag.
4. In *Default Template*, select *Windows Domain Account*.
5. In *Domain-Controller*, enter the DC IP address.

6. In *Domain*, enter the domain.
 - a. Click *Submit*.

The screenshot shows the 'New Secret Target' configuration page. The 'Classification Tag' is set to 'Windows'. Under 'Target Server Information', the 'Default Template' is 'Windows Domain Account', 'Domain-Controller' is '10.59.112.200', 'Domain' is 'fortipam.ca', and 'Gateway' is 'None'. Under 'Advanced Domain Setting', there is a plus icon. Under 'Additional Information', the 'Alias' is '10.59.112.200 - fortipam.ca' and the 'Description' field is empty. At the bottom, there are 'Submit' and 'Cancel' buttons.

Similarly, create two more targets for the Windows PCs in the 10.59.112.200 domain: 10.59.112.201 and 10.59.112.208 using the *Windows Machine* default secret template.

- **Windows PC- 10.59.112.201**

The screenshot shows the 'New Secret Target' configuration page. The 'Classification Tag' is 'Windows'. Under 'Target Server Information', the 'Default Template' is 'Windows Machine', 'Host' is '10.59.112.201', and 'Gateway' is 'None'. Under 'Additional Information', the 'Alias' is '10.59.112.201' and the 'Description' field is empty. At the bottom, there are 'Submit' and 'Cancel' buttons.

- **Windows PC- 10.59.112.208**

The screenshot shows the 'New Secret Target' configuration page. The 'Classification Tag' is 'Windows'. Under 'Target Server Information', the 'Default Template' is 'Windows Machine', 'Host' is '10.59.112.208', and 'Gateway' is 'None'. Under 'Additional Information', the 'Alias' is '10.59.112.208' and the 'Description' field is empty. At the bottom, there are 'Submit' and 'Cancel' buttons.

Creating a secret for the domain user

To create a secret for the domain user:

1. Go to *Secrets > Secrets*.
2. Select *+Create*.
The *Select a Secret Template* page opens.
3. Look for *Windows Domain Account* and click its icon.
The *New Secret* window opens.
4. Enter a name for the secret.
5. In *Target*, select the first target created in [Creating targets on page 110](#).
6. Enter the username.
7. Enter the password.
8. Reenter the password to confirm.
9. Click *Submit*.

Creating a secret for the Windows PC- 10.59.112.201 and Windows PC- 10.59.112.208

To create a secret:

1. Go to *Secrets > Secrets*.
2. Select *+Create*.
The *Select a Secret Template* page opens.
3. Look for *Target Only* and click its icon.
The *New Secret* window opens.
4. Enter a name for the secret.
5. In *Target*, select the target that you earlier created for **Windows PC- 10.59.112.201** in [Creating targets on page 110](#).
6. The selected template changes to *Windows Machine*.
Click the template and from *Select a Secret Template*, change the template to *Target Only*.

7. Enable *Associated Secret*, and from the dropdown, select the secret created in [Creating a secret for the domain user on page 112](#).
8. Enable *Launch with Associated Secret Credentials*.
Note: The associated secret credential is used for launching the secret.
9. Optionally, enter a description.
10. Click *Submit*.

Similarly, create a secret for **Windows PC- 10.59.112.208**.

Sharing secrets to a contractor

To share secrets to a contractor:

1. For the secrets created in [Creating a secret for the domain user on page 112](#) and [Creating a secret for the Windows PC- 10.59.112.201 and Windows PC- 10.59.112.208 on page 112](#), double-click secret in *Secrets > Secrets* to open.
2. Go to the *Permission* tab.
3. In the *Permission* pane, disable *Inherit Permission*.
4. Select *+*:
 - a. In *User/Group*, from the dropdown, select the contractor user, e.g., test.
 - b. In *Permission*, ensure that it is set to *View*.
 - c. In *Allowed Services*, select *RDP* and *Web*.

5. Click Save.

The screenshot shows the 'Secret Details' page for 'lab_domain_200 (ID: 5)'. The 'Permission' tab is active, displaying a table of permissions. The table has three columns: 'User / Group', 'Permission', and 'Allowed Service'. There are two rows: one for 'admin' with 'Owner' permission for 'All Services', and one for 'test' with 'View' permission for 'RDP' and 'Web'. The 'Save' button is highlighted in red.

User / Group	Permission	Allowed Service
admin	Owner	All Services
test	View	RDP, Web

Similarly, share the other two secrets created in [Creating a secret for the Windows PC- 10.59.112.201](#) and [Windows PC- 10.59.112.208](#) on page 112.

This screenshot is identical to the one above, showing the 'Secret Details' page for 'Win_PC_201 (ID: 6)'. The 'Permission' tab is active, and the table shows 'admin' as the owner for 'All Services' and 'test' as a viewer for 'RDP' and 'Web'. The 'Save' button is highlighted in red.

User / Group	Permission	Allowed Service
admin	Owner	All Services
test	View	RDP, Web

This screenshot is also identical to the previous ones, showing the 'Secret Details' page for 'Win_PC_208 (ID: 7)'. The 'Permission' tab is active, and the table shows 'admin' as the owner for 'All Services' and 'test' as a viewer for 'RDP' and 'Web'. The 'Save' button is highlighted in red.

User / Group	Permission	Allowed Service
admin	Owner	All Services
test	View	RDP, Web

Result

The test user can RDP/web access the target server 10.59.112.201 and 10.59.112.208.

Azure AD password changer

FortiPAM supports changing and verifying user credentials stored in Azure AD by integrating with a Microsoft Entra (Azure AD) Enterprise application and an application client secret.

This example walks you through the required configuration on Azure and on FortiPAM so that password verification and rotation work end-to-end.

Requirements

- An Azure tenant where you can register an application, configure Certificates & secrets, and grant API permissions (admin consent).
- FortiAuthenticator with access to create secrets using the *Azure Credential* and *Azure AD Account* templates.

To configure an Azure AD password changer:

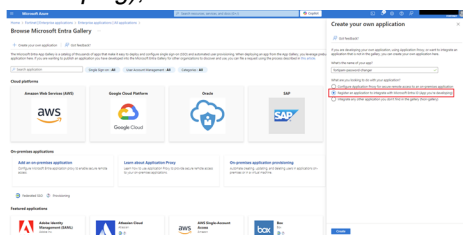
1. [Configuring the Azure portal on page 115](#)
2. [Configuring FortiPAM on page 117](#)
3. [Results on page 118](#)
4. [Troubleshooting on page 119](#)

Configuring the Azure portal


Register an Enterprise Application

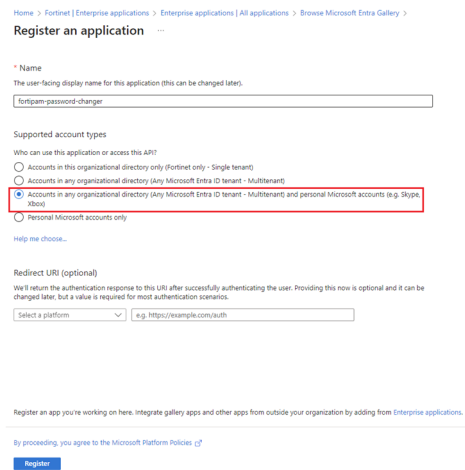
To register an Enterprise Application:

1. In the Microsoft Entra (Azure AD) portal, go to *Enterprise applications* and register a new application for the password changer.
2. In *Create your own application*, select *Register an application to integrate with Microsoft Entra ID (App you're developing)*, and select *Create*.

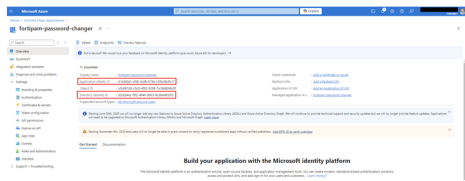


3. In the *Register an application* page that opens, select the application scope based on your organization request, and select *Register*.

 It is recommended that you select *Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)* and *personal Microsoft accounts (e.g. Skype, Xbox)*.



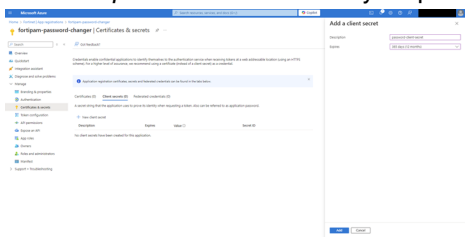
4. After registration, record *Application (client) ID* and *Directory (tenant) ID*. You need these on the FortiPAM side.




Creating a client secret

To create a client secret:

1. In the application, open *Certificates & secrets > New client secret*.
2. Set an *Expires* value that meets your policy and save the secret value displayed after creation.

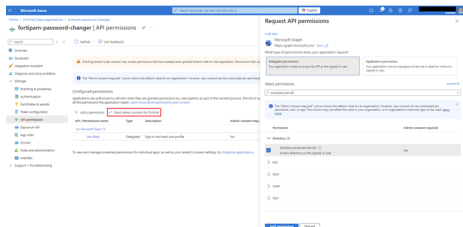


 Record the secret value as this is displayed only once after its creation.

Granting API permission

To grant API permission:

1. In *API permissions*, add `Directory.AccessAsUser.All` to the newly created application.
2. Click *Grant admin consent* to make the permission effective across your organization.

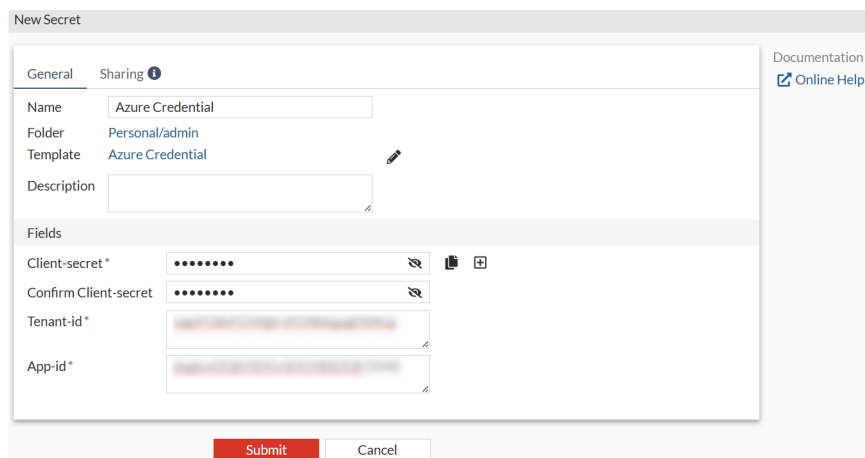


Configuring FortiPAM

Creating *Azure Credential* secret

To create an *Azure Credential* secret:

1. Go to *Secrets > Secrets*, and select *Create*.
2. In *Select a Secret Template*, select *Azure Credential*.
3. Enter a name for the secret.
4. In *Fields*:
 - a. Enter the *Client-secret*.
The *Client-secret* value is from [Creating a client secret on page 116](#).
 - b. Enter the *Tenant-id*.
The *Tenant-id* is the *Directory (tenant) ID* from step 4 in [Register an Enterprise Application on page 115](#).
 - c. Enter the *App-id*.
The *App-id* is the *Application (client) ID* from step 4 in [Register an Enterprise Application on page 115](#).
5. Click *Submit* to save the secret.



Creating Azure AD Account secret

Create another secret using the *Azure AD Account* template. Associate it with the *Azure Credential* secret created before.

To create Azure AD Account secret:

1. Go to *Secrets > Secrets*, and select *Create*.
 2. In *Select a Secret Template*, select *Azure AD Account*.
 3. Enter a name for the secret.
 4. Select *Associated Secret*, from the dropdown select *Select from Secret List*, and select the secret created in [Creating Azure Credential secret on page 117](#).
 5. In *Launch with*, select *Associated Secret Credentials*.
 6. In *Fields*:
 - a. Enter the URL.
 - b. Enter the *Username*.
 - c. Enter the password.
 - d. Reenter the password to confirm.
 7. Select *Submit* to save the secret.
- With the association in place, password verification and change operations for the Azure AD account will succeed.

The screenshot shows the 'Secret Details - Azure (ID: 4)' page in FortiPAM. The interface includes a top navigation bar with 'Verify' and 'Invite' buttons. Below the navigation bar are tabs for 'General', 'Settings', 'Sharing', 'Audit', 'Dependency', 'Event Subscription', and 'Requests & Jobs'. The 'General' tab is active, displaying the following fields:

- Name:** Azure
- Folder:** Personal/admin
- Template:** Azure AD Account
- Override Server Type:** Other
- Target:** Auto Match / Create
- Privileged Account:**
- Associated Secret:** Select from Secret List
 - Secret:** Azure Credential
- Launch with:** Associated Secret Credentials
- Description:** (empty)

The 'Fields' section contains:

- URL *:** https://azure.microsoft.com
- Username *:** (empty)
- Password *:** (masked with dots)

On the right side of the page, there are status indicators and instructions:

- Last Launch Time:** Secret has not been launched before.
- Password Changer Status:** Password has not been changed before.
- Password Verification Status:** Password has not been verified before.
- Install CA Certificate for Web Launching:** The browser may warn untrusted site even its certificate is valid. It is because the traffic is proxied by FortiPAM in the proxy mode. Download and Install the CA certificate from FortiPAM to resolve the false positive untrusted site warning. During installation, you may be asked to specify the certificate store (trusted root CA/intermediate CA). Most of the platforms can automatically select a certificate store based on the type of certificate. You can also specify a location for the certificate manually. For the later case, check the "Issued to" and "Issued by" fields in the "General" tab of the "Certificate" dialog. If they are the same, choose "Trusted Root Certification Authorities". If different, choose "Intermediate Certification Authorities".
- Download the certificate file, double-click and follow the wizard to install it.**
- Download Local CA Certificate** button.

Results

You can now verify the Azure AD account password and change/rotate it through FortiPAM using the associated *Azure Credential + Azure AD Account* secrets.

Troubleshooting

- If password verification or change fails, re-check:
 - The `Directory.AccessAsUser.All` permission and Admin consent status on the Azure application.
 - The Client secret validity (expiry) and that the Tenant ID and the Application ID match the application you registered.
- Password rotations will fail if the client secret has expired; renew the secret in *Certificates & secrets* and update the *FortiPAM Azure Credential* secret.

Audit

This section describes auditing and monitoring features available on FortiPAM.

Sponsored administrator audits secret activities

In this example, we create a sponsored group, a sponsor admin for the sponsored group, and members for the sponsored group.

The sponsor admin is able to audit and monitor secret activities of the sponsored group members.

For information on sponsored groups, see [Sponsored groups](#) in the latest *FortiPAM Administration Guide*.

To create sponsored administrator that audits secret activities:

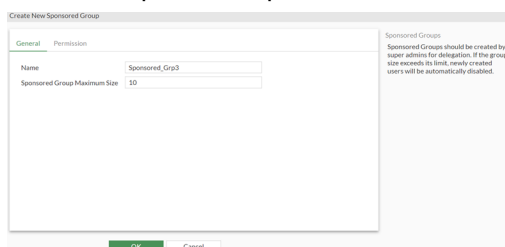
1. [Creating a sponsored group on page 120](#)
2. [Creating a sponsor admin on page 121](#)
3. [Creating a secret with view permission for the sponsored group on page 122](#)
4. [Creating sponsored group members on page 123](#)
5. [Auditing on page 125](#)

Creating a sponsored group

To create a sponsored group:

1. Go to *User Management > Sponsored Groups*.
2. Select *Create* to create a new user group.
The *General* tab in the *Create New Sponsored Group* window opens.
3. In the *General* tab:
 - a. In *Name*, enter a name for the sponsored group.
 - b. In *Sponsored Group Maximum Size*, if needed, change the maximum number of users that can be assigned to the sponsored group.

In this example, we keep the default value, i.e., 10.



4. Click *OK*.

Creating a sponsor admin

We now create a sponsor admin assigned to the sponsored group created in [Creating a sponsored group on page 120](#).

To create a sponsor admin:

1. Go to *User Management > User List*, and select *Create*.
The *New User List* wizard is launched.
2. In *Configure Role*, select *Sponsor Admin*, and from the *Choose a Sponsor Administrator Role* dropdown, select the sponsored group created in [Creating a sponsored group on page 120](#).



Sponsor admins can only manage users within their assigned sponsored group.

New User List

1 Configure Role 2 Configure Type 3 Configure User Details 4 Two Factor Authentication 5 Configure Trusted Hosts and Schedule 6 Review

User Privilege

- Guest User
Guest users are created for demonstration purposes. It can only view secrets and has very restricted access to different features.
- Standard User
Standard users are created for any users who has basic access to secrets. It has the ability to make request, claiming ownership for secrets that requires checkout etc.
- Sponsor Admin**
Sponsor admins are delegated the responsibility of managing users within a sponsored group, including the ability to create, edit, or delete those users.
 - Choose a Sponsor Administrator Role:
 - Sponsored Group:
- Power User
Power users are created for managing general settings of secrets. For example, they can change who could approve secrets, the commands that are blocked on the target server etc.
- Administrator
Staff Administrators used for configuring the FortiPAM, and managing secret access. An example is an IT staff member, who manages the access of Standard Users, or approves requests.
- Customized User
Customized users have tailored permissions and restrictions to match their needs and responsibilities, allowing to control access to features or pages based on assigned roles. Users can create a customized role in the Role page.

Previous **Next** Cancel

User List
Create a new FortiPAM user account. The user would be able to login with configured credentials and have access to permitted services.
User Login Status:
 User has not logged in yet.

3. Click *Next*.
4. In *Configure Type*, select *Local User* and click *Next*.
5. In *Configure User Details*:
 - a. In *Username*, enter a username.
 - b. In *Password*, enter a password.
 - c. In *Confirm Password*, enter the password again.
 - d. In *Status*, select *Enable*.
 - e. Optionally, you can enter a description about the user.

New User List

1 Configure Role 2 Configure Type 3 Configure User Details 4 Two Factor Authentication 5 Configure Trusted Hosts and Schedule 6 Review

User Details

Username:

Password:

Confirm Password:

Status: Enable Disable

Comment:

Previous **Next** Cancel

User List
Create a new FortiPAM user account. The user would be able to login with configured credentials and have access to permitted services.
User Login Status:
 User has not logged in yet.

- f. Click *Next*.
6. In *Two Factor Authentication*, click *Next*.
 7. In *Configure Trusted Hosts and Schedule*, click *Next*.

8. Review the configuration and click *Submit*.

Creating a secret with view permission for the sponsored group

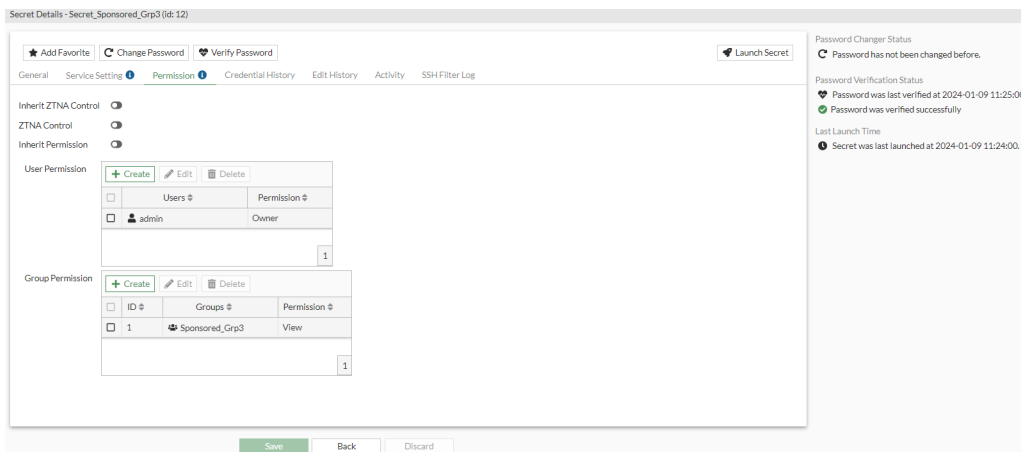
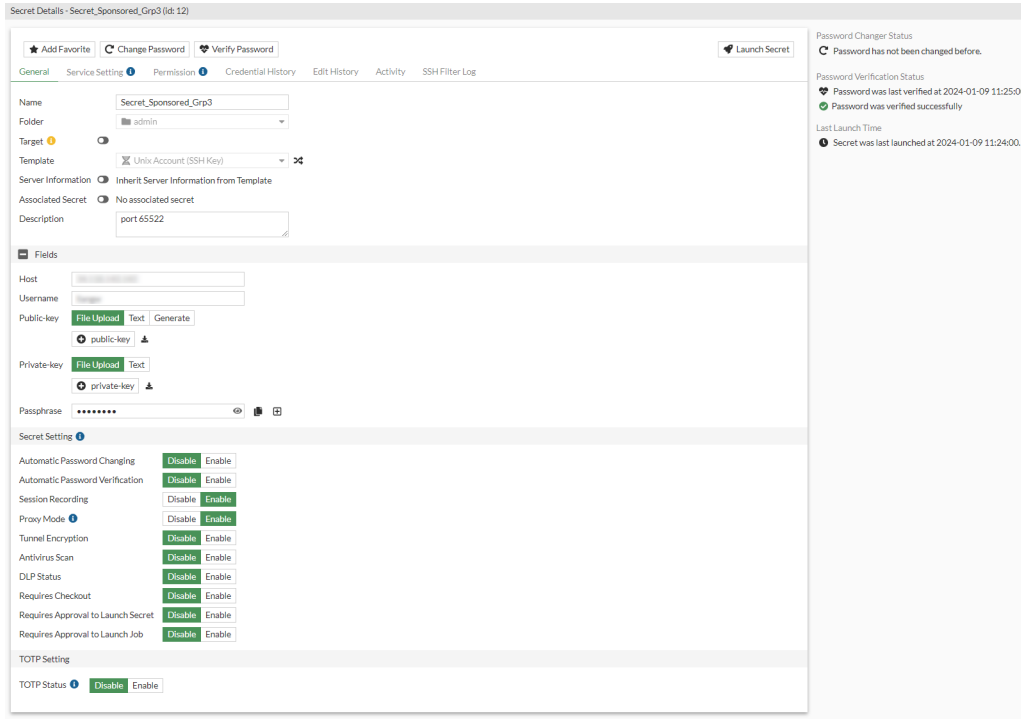
We create a secret with view permission for the sponsored group created in [Creating a sponsored group on page 120](#).

To create a secret with view permission:

1. Go to *Secrets > Secret List*.
2. In *Secret List*, select *Create*.
The *Create New Secret in:* dialog appears
3. Select the folder where you intend to add the secret.
4. Select *Create*.
The *General* tab opens.
5. In the *General* tab:
 - a. In *Name*, enter a name for the secret.
 - b. Disable *Target*.
 - c. In *Template*, select *Unix Account (SSH Key)*.
 - d. In *Host*, enter the IP address of the server.
 - e. In *Username*, enter a username.
 - f. In *Public-key*, select *File Upload* and then select *Upload* to locate and upload public key file from the management computer.
 - g. In *Private-key*, select *File Upload*, and then select *Upload* to locate and upload private key file from the management computer.
 - h. In *Passphrase*, enter a passphrase.
 - i. In *Confirm Passphrase*, reenter the passphrase.
 - j. Enable *Session Recording*.
6. In the *Permission* tab:
 - a. Disable *Inherit Permission*.
 - b. In *Group Permission*:
 - i. Select *Create*.
The *New Group Permission* window opens.

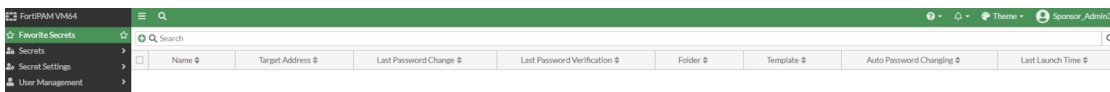
- ii. In *Groups*, select the sponsored group created in [Creating a sponsored group on page 120](#).
- iii. In *Permission*, select *View*.
- iv. Click *OK*.

7. Click *Submit*.



Creating sponsored group members

The sponsor admin created in [Creating a sponsor admin on page 121](#) logs in to the FortiPAM.



To create sponsored group members as a sponsor admin:

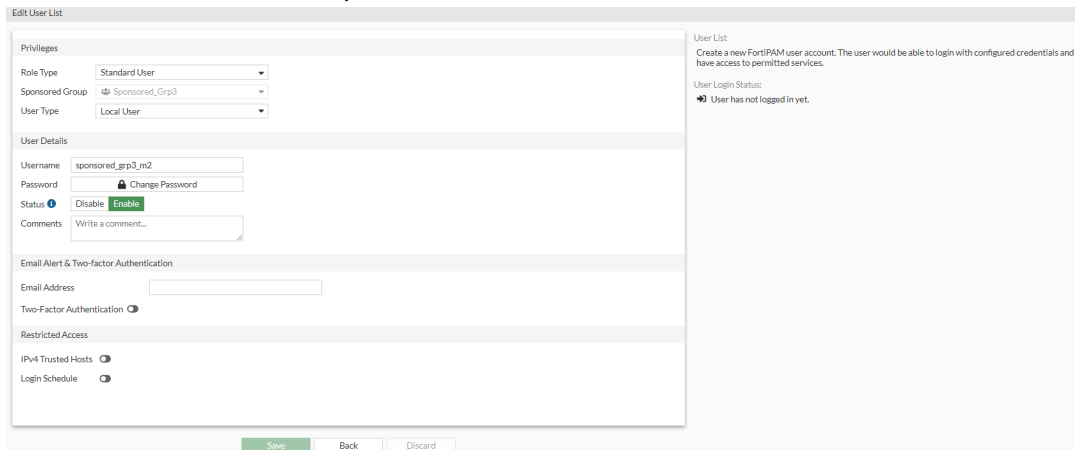
1. Log in to FortiPAM as the sponsor admin.
2. Go to *User Management > User List*, and select *Create*.
The *New User List* wizard is launched.
3. In *Configure Role*, select *Standard User* and click *Next*.



The user is automatically assigned to the sponsored group created in *Creating a sponsored group* on page 120.

4. In *Configure Type*, select *Local User*.
5. In *Configure User Details*:
 - a. In *Username*, enter a username.
 - b. In *Password*, enter the password.
 - c. In *Confirm Password*, reenter the password.
 - d. Enable *Status*.
 - e. Optionally, you can enter a description about the user.
 - f. Click *Next*.
6. In *Two Factor Authentication*, click *Next*.
7. In *Configure Trusted Hosts and Schedule*, click *Next*.
8. Review the configuration and click *Submit*.

9. For additional users, follow steps 1 - 8.



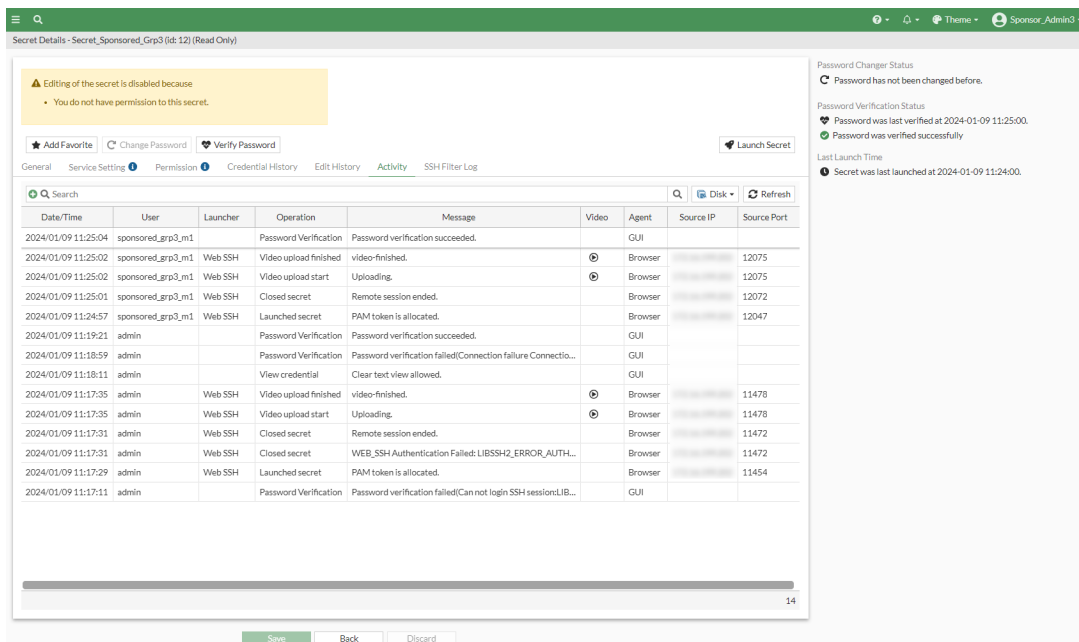
Note: The maximum number of users that can be created will depend on the number that you have set up in [Creating a sponsored group on page 120](#).

For a sponsor admin with two users in the sponsored group, the *User List* in *User Management* is shown below:

Name #	Sponsored Group #	Role #	Type #	Lastest Login #	Status #	References #
Sponsor_Admin	Sponsored_Grp3	Sponsor_Admin	Local	2024-01-11 16:37:04	Enable	1
sponsored_grp3_m1	Sponsored_Grp3	Standard User	Local	2024-01-09 11:24:48	Enable	1
sponsored_grp3_m2	Sponsored_Grp3	Standard User	Local		Enable	1

Auditing

When a sponsored group member launches the secret configured in [Creating a secret with view permission for the sponsored group on page 122](#), the sponsor admin configured in [Creating a sponsor admin on page 121](#) can check secret activities by double-clicking the secret in *Secrets > Secret List* and going to the *Activity* tab.



Web proxy

This section describes configuring web proxy on FortiPAM.

Configuring the web proxy feature to prevent web credentials from leaking

To improve FortiPAM security and flexibility when accessing a web account secret, FortiPAM offers a new web proxy feature to dynamically operate on the web browser tab's PAC rule (on Google Chrome and Microsoft Edge) to successfully proxy the traffic to FortiPAM based on the configured domain. On Mozilla Firefox, FortiPAM sends the request to the web proxy instead.

This example shows how to configure the web proxy feature to prevent your web credentials from leaking.

We assume that the FortiPAM WAN interface is reachable from the web browser directly.



For information on how the web proxy feature works, see [Web proxy](#) in the latest *FortiPAM Administration Guide*.

To configure the web proxy feature:

1. [Enabling the web proxy feature on page 126](#)
2. [Creating a secret target with web proxy on page 127](#)
3. [Creating a secret with web proxy on page 128](#)

If FortiPAM is behind a FortiGate device, see [FortiPAM behind a FortiGate device on page 129](#).

Enabling the web proxy feature

To enable the web proxy feature:

1. Log in to FortiPAM.
2. Go to *Network > Interfaces*.

3. According to your network topology, double-click a WAN interface and enable *Explicit web proxy*.

The screenshot shows the 'Edit Interface' configuration page for 'port1'. The interface is a physical interface with an undefined role. The address is manually set to 192.168.255.255/255.255.255.0. Administrative access is configured with IPv4, PING, and SSH enabled. In the 'Miscellaneous' section, the 'Explicit web proxy' checkbox is checked and labeled 'Enabled'.

Alternatively, use the following CLI commands to enable the web proxy feature for the interface that handles incoming and outgoing traffic.

```
config system interface
edit "port1"
set explicit-web-proxy enable #must be enabled
next
end
```

After the web proxy has been enabled, FortiPAM starts the web proxy service on the WAN interface where web proxy was enabled with port 8080.

If you want to change the port from 8080 to any other port, use the following CLI commands.

```
config web-proxy explicit-proxy
edit "web-proxy"
set http-incoming-port 65530 #between 0 - 65535, default = 8080
next
end
```

4. Click *OK*.

Creating a secret target with web proxy

To create a secret target:

1. Go to *Secrets > Target List*.
2. Select *Create* to create a new target.
3. In the *General* tab, enter the following information:
 - a. In *Name*, enter a name for the secret target.
 - b. In *Classification Tag*, from the dropdown, select a tag.
A classification tag is used to classify targets. Here, we select a custom *Web_Account* tag. The *Web_Account* tag helps identify web account targets.
 - c. In *Default Template*, we select *Web_Account*.
Web_Account is a custom template with *URL* field.
 - d. In *URL*, enter the URL for the service to be accessed.

4. In the *Advanced Web Setting* pane:
 - a. Enable *Web Proxy*.
 - b. Enable *Replace Web Credential* to replace the web authentication credential. This prevents your web credential from leaking.
 - c. Disable *Authentication URL*.
 - d. Enable *Domain List*.
 - e. Ensure that *Access Mode* is *Proxy*.
 - f. In *FQDN List*, click *+* and enter an FQDN to add to the domain list based on the login page of the HTTP server.
 - g. To add additional FQDNs, click *+* and enter an FQDN.
5. Click *Submit*.

The screenshot shows the 'Edit Secret Target' interface. The 'Advanced Web Setting' section is expanded, showing the following configuration:

- Web Proxy:** Enable (checked)
- Replace Web Credential:** Checked
- Authentication URL:** Unchecked
- Domain List:** Checked
- Access Mode:** Proxy (selected)
- FQDN List:** login.microsoftonline.com, login.live.com

Creating a secret with web proxy

To create a secret with web proxy:

1. Go to *Secrets > Secret List*.
2. In *Secret List*, select *Create*.
The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.
4. Select *Create*.
The *General* tab opens.
5. In the *General* tab:
 - a. In *Name*, enter a name for the secret.
 - b. Ensure *Target* is enabled and select the target created in [Creating a secret target with web proxy on page 127](#).
Some fields and the template are automatically imported from the target. The imported fields can only be edited when editing the target.
In this example, the *URL* field is imported from the target.
The template is the custom template used in [Creating a secret target with web proxy on page 127](#).
 - c. Fill in the remaining fields.

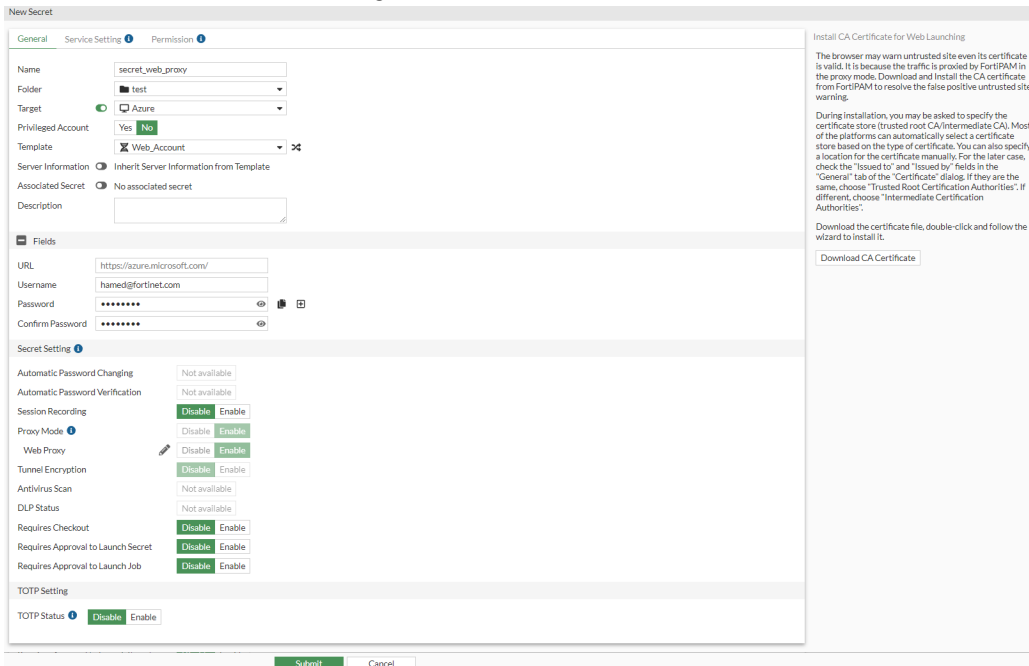
- d. Ensure that the *Web Proxy* option in *Secret Setting* is enabled.

 The *Web Proxy* option is only available when *Proxy Mode* is enabled.

The *Web Proxy* setting is inherited from the target.

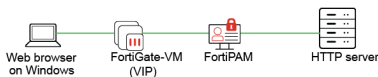
When you edit the *Web Proxy* setting, you are editing the *Web Proxy* setting available from within the associated secret target.

- e. Configure other secret related settings as required.
- f. Before launching the secret for the first time, you must download the FortiPAM CA certificate by selecting *Download CA Certificate* on the right to download the CA certificate.



- g. Double-click the certificate file and install it by following the installation wizard. You can now launch the web account secret.

FortiPAM behind a FortiGate device



If the FortiPAM interface cannot be reached from a web browser on Windows as the FortiPAM interface is behind FortiOS, configure a VIP on the FortiOS side to forward to the FortiPAM interface IP and VIP. You must add the VIP to your DNS server and give it an FQDN.

On the FortiPAM side, add the FQDN to your web proxy configuration:

```

config web-proxy global
  set proxy-fqdn [FQDN]
end
  
```

The remaining configuration is the same as shown for the topology diagram in [Configuring the web proxy feature to prevent web credentials from leaking on page 126](#).

You can now launch the web account secret with the web proxy feature.

RDP log retrieval

This section describes retrieving specific logs for events that occurred during an RDP session from a target.

RDP log retrieving on FortiPAM

Using event filter profiles, FortiPAM can retrieve specific logs for events that occurred during an RDP session from a target.

For information on WinRM configuration of the target machine, see [Appendix L: WinRM configuration for Windows server](#) in the latest *FortiPAM Administration Guide*.

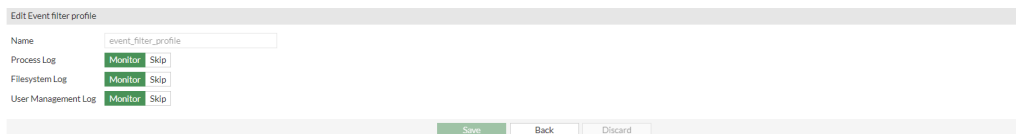
To configure RDP log retrieval on FortiPAM:

1. [Creating an event filter profile on page 131](#)
2. [Creating a secret target on page 132](#)
3. [Creating a secret policy on page 132](#)
4. [Creating secret with an RDP event filter profile on page 133](#)
5. [Launching the secret on page 134](#)
6. [Checking the RDP logs on page 135](#)

Creating an event filter profile

To create an event filter profile:

1. Go to *Secret Settings > Event Filter Profile*.
2. In *Event Filter Profile*, select *Create*.
The *New Event filter profile* window opens.
3. In *Name*, enter a name for the event filter profile.
4. Select *Monitor* for the logs you intend to monitor.
5. Click *Submit*.



Event filter profile configuration interface showing the following options:

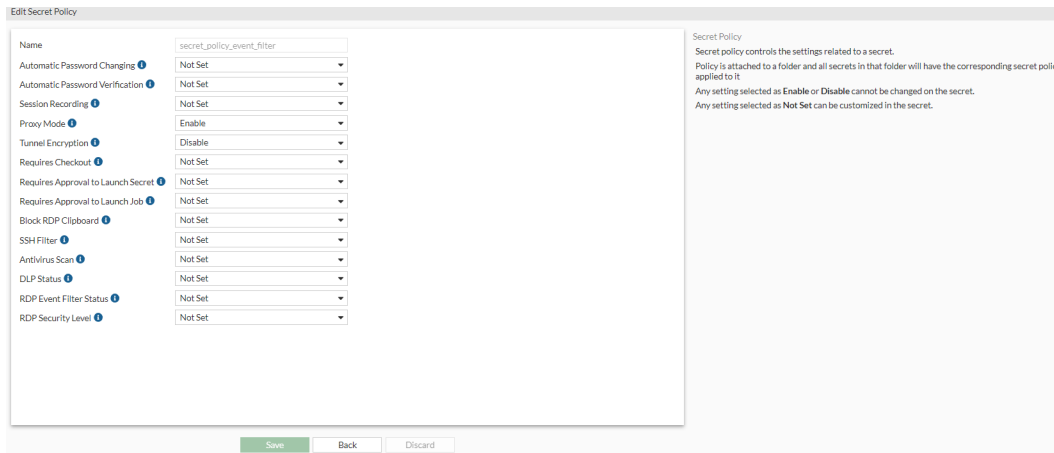
Log Category	Monitor	Skip
Process Log	Monitor	Skip
Filesystem Log	Monitor	Skip
User Management Log	Monitor	Skip

Buttons: Save, Back, Discard

Creating a secret policy

To create a secret policy:

1. Go to *Secret Settings > Policies*.
2. In *Policies*, select *Create*.
The *New Secret Policy* window opens.
3. Ensure that *RDP Event Filter Status* is *Not Set*.
Since *RDP Event Filter Status* is *Not Set*, it can be customized in the secret.
4. Click *Submit*.



Creating a secret target


To create a secret target:

1. Go to *Secrets > Target List*.
2. Select *Create* to create a new target.
3. In the *General* tab, enter the following information:
 - a. In *Name*, enter a name for the secret target.
 - b. In *Classification Tag*, from the dropdown, select a tag.
A classification tag is used to classify targets.
 - c. In *Default Template*, we select *Windows_Domain_Account*.
Windows_Domain_Account is a custom template with *Domain-Controller* and *Domain* fields.
 - d. In *Domain-Controller*, enter the IP address of the target machine.
 - e. In *Domain*, enter the domain name for the target machine.

4. Click *Submit*.

Creating secret with an RDP event filter profile

To create a secret:

1. Go to *Secrets > Secret List*.
 2. In *Secret List*, select *Create*.
The *Create New Secret in:* dialog appears.
 3. Select the folder where you intend to add the secret.
Note: The folder must use the policy created in [Creating a secret policy on page 132](#).
 4. Select *Create*.
The *General* tab opens.
 - a. In *Name*, enter a name for the secret.
 - b. Ensure *Target* is enabled and select the target created in [Creating a secret target on page 132](#).
Some fields and the template are automatically imported from the target. The imported fields can only be edited when editing the target.
In this example, the *Host* and the *Domain* fields are imported from the target.
The template is the custom template used in [Creating a secret target on page 132](#).
 - c. In *Privileged Account*, select *Yes*.
-  Each target can have only one privileged account.
- d. Fill in the remaining fields.
 - e. Enable *Session Recording*.
5. In the *Service Setting* tab:
 - a. Enable *RDP Event Filter*.
 - b. From the *RDP Event Filter Profile* dropdown, select event filter profile created in [Creating an event filter profile on page 131](#).

6. Click *Submit*.

The image displays two screenshots of the FortiPAM web interface for configuring a secret profile named 'secret_event_filter_profile'.

Top Screenshot (General Tab):

- Name:** secret_event_filter_profile
- Folder:** admin
- Target:** target_event_filter_profile
- Privileged Account:** Yes (selected), No
- Template:** Windows_Domain_Account
- Server Information:** Inherit Server Information from Template
- Associated Secret:** No associated secret
- Description:** (empty text area)
- Fields:**
 - Host:** 192.168.1.43
 - Domain:** company.org
 - Username:** admin
 - Password:** (masked with dots)
- Secret Setting:**
 - Automatic Password Changing: Disable/Enable
 - Automatic Password Verification: Disable/Enable
 - Session Recording: Disable/Enable
 - Proxy Mode: Disable/Enable
 - Tunnel Encryption: Disable/Enable
 - Antivirus Scan: Disable/Enable
 - DLP Status: Disable/Enable
 - Requires Checkout: Disable/Enable
 - Requires Approval to Launch Secret: Disable/Enable
 - Requires Approval to Launch Job: Disable/Enable
 - TOTP Setting:
 - TOTP Status: Disable/Enable

Bottom Screenshot (Service Setting Tab):

- SSH Service:** Disable/Enable
- RDP Service:** Disable/Enable
- Use Template Default Port:** (toggle)
- Block RDP Clipboard:** Disable/Enable
- RDP Security Level:** Best Effort | NLA | RDP | TLS
- RDP Restricted Admin Mode:** Disable/Enable
- Keyboard Layout:** English, United States
- RDP Event Filter:** Disable/Enable
- RDP Event Filter Profile:** event_filter_profile
- VNC Service:** Disable/Enable
- SAMBA Service:** Disable/Enable
- Use Template Default Port:** (toggle)
- SFTP Service:** Disable/Enable

Both screenshots include a right-hand sidebar with status indicators for Password Changer, Password Verification, Last Launch Time, and Documentation.

Launching the secret

To launch the secret:

1. Go to *Secret > Secret List*.
2. In *Secret List*, select the secret created in [Creating secret with an RDP event filter profile on page 133](#), and select *Launch Secret*.
3. In *Launch Progress*, select *Web RDP*.
Alternatively, you can also select native RDP.
4. Confirm the target IP address and select *Launch*.
You can now access the target server.

Gateway

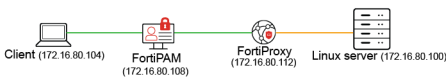
This section describes examples related to the FortiPAM network gateway and reverse gateway feature for distributed target deployment.

FortiPAM connects to a target through a FortiProxy acting as the gateway

In this example, FortiPAM connects to a target server using a FortiProxy device as the gateway.

For detailed information on FortiPAM gateways, see [Gateway](#) in the latest *FortiPAM Administration Guide*.

Topology



To connect FortiPAM to a target through a FortiProxy as the gateway:

1. [Creating the FortiProxy gateway on page 136](#)
2. [Creating the secret target on FortiPAM on page 137](#)
3. [FortiProxy related configurations on page 137](#)

Creating the FortiProxy gateway

To create the FortiProxy gateway:

1. In the GUI, go to *Network > Secret Gateway*, and select *Create*.
Alternatively, enter the following commands in the CLI console to create the FortiProxy gateway:

```
config secret gateway
edit test_gateway
set address "172.16.80.112"
set port 443
set url-map "tcp"
set ssl-max-version tls-1.3
next
end
```

Creating the secret target on FortiPAM

To create the secret target:

1. In the GUI, go to *Secrets > Targets*, and select *Create*.
Alternatively, enter the following commands in the CLI console to create the secret target (Linux server)

```
config secret target
edit "172.16.80.100"
  set class "Other"
  set template "Unix Account (SSH Password)"
  set address "172.16.80.100"
  set gateway "test_gateway" #from Creating the FortiProxy gateway on page 136
  set creation-time 2023-11-10 09:34:23
  set web-proxy-status disable
next
end
```

FortiProxy related configurations

Configuring a VIP on FortiProxy

To configure a VIP on FortiProxy:

1. In the FortiProxy CLI console, enter the following commands to configure a VIP:

```
config firewall vip
edit "test_vip"
  set type access-proxy
  set server-type https
  set extip 172.16.80.112
  set extintf "any"
  set h2-support disable
  set extport 443
  set ssl-certificate "Fortinet_GUI_Server"
  set ssl-min-version tls-1.3
next
end
```

Configuring an IPv4 access proxy on FortiProxy

To configure an IPv4 access proxy:

1. In the FortiProxy CLI console, enter the following commands to configure an IPv4 access proxy:

```
config firewall access-proxy
edit "test_access_proxy"
  set vip "test_vip" #from Configuring a VIP on FortiProxy on page 137
```

```
set client-cert disable
set auth-portal enable
config api-gateway
edit 1
  set url-map "/tcp"
  set service tcp-forwarding
  config realservers
  edit 1
    set address "all"
  next
end
next
end
next
end
```

Configuring a firewall proxy

To configure a firewall proxy:

1. In the FortiProxy CLI console, enter the following commands to configure a firewall proxy:

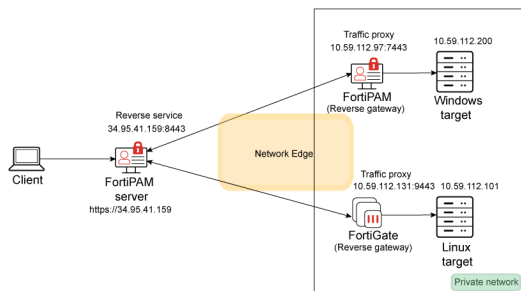
```
config firewall policy
edit 1
  set type access-proxy
  set srcintf "any"
  set srcaddr "all"
  set dstaddr "all"
  set action accept
  set schedule "always"
  set access-proxy "test_access_proxy" #from Configuring an IPv4 access proxy on FortiProxy on page 137
  next
end
```

Configuring FortiPAM/FortiGate as the reverse gateway

For information on the reverse gateway feature, see [Gateway](#) in the latest *FortiPAM Administration Guide*.

In this example, we demonstrate how to configure FortiPAM/FortiGate as a reverse gateway to provide access from a public network to a private resource.

Topology



Prerequisites

- FortiPAM 1.4.0 or above.
- FortiGate 7.6.3 or above.



To enable the Service mode for a reverse gateway, ensure that the FortiPAM server and the gateway are on the same FortiPAM version (at least 1.5.0).

- Certificates required for reverse control connection mTLS.

In this example the following certificates are used:

- **On the FortiPAM server:** FortiPAM server certificate for reverse control plane connection: `fortipam_cert5.pem`.
- **On the FortiPAM server:** Reverse gateway certificate CA: `CA_Cert_1`. Both gateways- FortiPAM and FortiGate use the same CA in the example.
- **On the reverse gateway (FortiPAM or FortiGate):** FortiPAM server certificate CA: `CA_Cert_1`.
- **On the reverse gateway (FortiPAM):** Reverse gateway FortiPAM certificate: `fortipam_gw4.pem` and its common name used for gateway ID in the FortiPAM server: `fortipam_gw4`.
- **On the reverse gateway (FortiGate):** Reverse gateway FortiGate certificate: `fortipam_gw5` and its common name used for gateway ID on the FortiPAM server: `fortipam_gw5`.



To import a CA, on FortiPAM/FortiGate, go to *System > Certificates* and from the *+Create/Import* dropdown select *Import CA Certificate*.



To import a certificate, on FortiPAM/FortiGate, go to *System > Certificates* and from the dropdown select *Import Certificate*.

To configure FortiPAM/FortiGate as the reverse gateway (including FortiPAM in the Service mode):

1. [Configuring the reverse service on FortiPAM \(control plane\) on page 140](#)
2. [Configuring reverse service on the gateway \(control plane\) on page 140](#)
3. [Configuring traffic proxy on the gateway for forwarding secret launch \(traffic plane\) on page 141](#)
4. [Configuring a gateway entry on FortiPAM server for secret launch \(traffic plane\) on page 144](#)

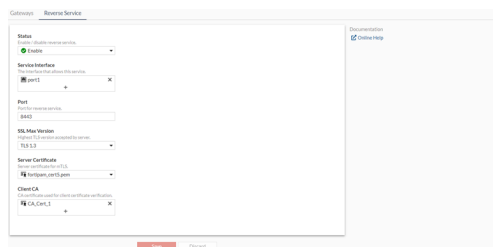
5. [Configuring a target using reverse gateway on the FortiPAM server on page 146](#)
6. [Creating a secret for the target that uses the FortiPAM reverse gateway on page 147](#)
7. [Launching the FortiPAM secret on page 148](#)
8. [Creating a secret for the target that uses the FortiGate reverse gateway on page 149](#)
9. [Launching the FortiGate secret on page 150](#)
10. [Troubleshooting on page 150](#)

Configuring the reverse service on FortiPAM (control plane)

We configure the reverse service on FortiPAM for the reverse connection (control plane).

To configure the reverse service:

1. Go to *Network > Secret Gateway*.
2. Select the *Reverse Service* tab.
The *Reverse Service* tab opens.
3. From the *Status* dropdown, select *Enable*.
4. From the *Service Interface*, select *+*, from *Select Entries*, select *port1*, and click *Close*.
This is the IP address on the selected interface and the port the FortiPAM server listens on to receive the reverse connection from a gateway for the control plane connection. In this example, it is `34.95.41.159:8443`.
5. Ensure that the *Port* is `8443` and the *SSL Max Version* is *TLS 1.3*.
6. In the *Server Certificate* dropdown, select *fortipam_cert5.pem*.
This is the correct FortiPAM server certificate for control plane mTLS connection.
7. In the *Client CA* dropdown, select *CA_Cert_1*.
This is the gateway certificate CA.
8. Click *Save*.



Configuring reverse service on the gateway (control plane)

We configure the reverse service on the gateway for a reverse connection to the FortiPAM server (control plane).

To configure a reverse service on a FortiPAM gateway:

1. In the GUI, go to *Network > FortiPAM Server*, and select *Create*.
Alternatively, in the CLI console, enter the following commands:

```
config secret server
edit "pam_gcp159"
set status enable
set address "34.95.41.159" #same as the one on the interface in Service Interface in
Configuring the reverse service on FortiPAM \(control plane\) on page 140
set port 8443 #same as the one on Port configured in Configuring the reverse service on
FortiPAM \(control plane\) on page 140
set service-gateway-launch enable #enables the service feature
set health-check-interval 60
set set ssl-max-version tls-1.3
set client-cert "fortipam_gw4.pem"
set ca "CA_Cert_1"
next
end
```

To configure reverse service on a FortiGate gateway:

1. In the CLI console, enter the following commands:

```
config ztna reverse-connector
edit "gcp159"
set address "34.95.41.159" #same as the one on the interface in Service Interface in
Configuring the reverse service on FortiPAM \(control plane\) on page 140
set port 8443 #same as the one on Port configured in Configuring the reverse service on
FortiPAM \(control plane\) on page 140
set certificate "fortipam_gw5"
set trusted-server-ca "CA_Cert_1"
next
end
```

Configuring traffic proxy on the gateway for forwarding secret launch (traffic plane)

We configure the traffic proxy on the gateway for forwarding secret launch.



Traffic proxy can only be configured via the CLI console.

To configure traffic proxy on the FortiPAM gateway:

Starting 1.5.0, the default vip/access-proxy/policy is used for traffic proxy for reverse/service mode. There is no need to manually create traffic proxy in the gateway.

There is always a default firewall address and policy for the reverse mode.

```
config firewall address
edit "fortipam_vip_gwy_addr"
```

```
set uuid 71be08b0-9635-51ef-15dd-cc38fbd02e05
set subnet 172.17.219.98 255.255.255.255
next
end
```

The IP address in the default `firewall.address` is the same as the default VIP.

```
config firewall policy
edit 2001
set type access-proxy
set name "fortipam_vip_gwy_pol"
set uuid 71be3eca-9635-51ef-ee0f-1fd59c381492
set srcintf "any"
set srcaddr
set dstaddr "all"
set action accept
set schedule "always"
set access-proxy "fortipam_access_proxy"
set ssl-ssh-profile "deep-inspection"
next
end
```

Both the reverse and the service mode work on the default `fortipam_vip`, so when you switch the mode on the Gateway device, there is no need to change the corresponding `secret.gateway` entry on the FortiPAM device.

If the gateway device is required to function as both the forward and the reverse gateway, you must add a new `firewall.address` representing the source device IP address and add that address next to `fortipam_vip_gwy_addr` in the policy.

Notes:

- If the secret server and the gateway are different products, i.e., one is FortiPAM and the other is FortiSRA, the gateway always works on the reverse mode.

If you require a customized VIP for traffic forwarding, follow the below configuration:

1. In the CLI console, enter the following commands:

```
config firewall vip
edit "fortipam_vip_gw"
set uuid d39c1138-032a-51ef-8508-24d8bb973e7a
set type access-proxy
set extip 10.59.112.97
set extintf "port1"
set server-type https
set extport 7443
set ssl-certificate "Fortinet_SSL"
next
end
config firewall access-proxy
edit "gw_access_proxy"
set vip "fortipam_vip_gw"
config api-gateway
edit 2
set url-map "/tcp"
```

```
set service tcp-forwarding
config realservers
  edit 1
    set address "all"
  next
end
next
end
next
end
config firewall policy
  edit 2
    set type access-proxy
    set uuid 380dc436-032b-51ef-0ef6-a260ec98f34b
    set srcintf "any"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set access-proxy "gw_access_proxy"
    set ssl-ssh-profile "deep-inspection"
  next
end
```



extip and extport in vip are configured in the gateway entry on the FortiPAM server to proxy the traffic.

To configure traffic proxy on the FortiGate gateway:

1. In the CLI console, enter the following commands:

```
config firewall vip
  edit "rvs_gw_vip"
    set uuid 070aabf8-1c88-51ef-7522-ee10d057882a
    set type access-proxy
    set server-type https
    set extip 10.59.112.131
    set extintf "port1"
    set client-cert disable
    set extport 9443
    set ssl-certificate "fortipam_gw5"
  next
end
config ztna traffic-forward-proxy
  edit "ztfp_fpam"
    set vip "rvs_gw_vip"
  next
end
config firewall proxy-policy
  edit 3
    set uud 4d3ad48c-1d45-51ef-24ad-e8ec50ae317d
```

```
set proxy ztna-proxy
set ztna-proxy "ztfp_fpm"
set srcintf "any"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set logtraffic all
set utm-status enable
set ssl-ssh-profile "deep-inspection"
next
end
```



The `extip` and the `extport` are configured in the gateway entry on the FortiPAM server to proxy the traffic. By default, the `client-cert` is enabled. If `client-cert` is set to enable, add the FortiPAM certificate CA to the FortiGate:

```
config authentication setting
  set user-cert-ca "CA_Cert_1"
end
```

Configuring a gateway entry on FortiPAM server for secret launch (traffic plane)

To configure a FortiPAM gateway entry on FortiPAM:

1. Go to *Network > Secret Gateway*.
2. From the Gateways List, select *Create*.
The *New Gateway* window opens.
3. Enter a name for the gateway.
4. Ensure that the status is set to enable.
5. In *Type*, select *Reverse*.
6. In *Address*, enter the gateway IPv4 address.
7. In *Port*, enter 7443.
The *Address* and *Port* were configured in `vip` in [Configuring traffic proxy on the gateway for forwarding secret launch \(traffic plane\) on page 141](#).
8. Ensure that *Health Check* is enabled and set to 60 seconds.
The gateway status is displayed on the right.
9. Optionally, enter a description.
10. In *Gateway ID*, enter the gateway client certificate common name to create mapping between FortiPAM and the gateway.
11. In *Mode*, select *Reverse Gateway*.
12. In *SSL Max Version*, select *TLS 1.3*.
13. In the *Client Certificate* dropdown, select the client certificate for mTLS.
The *Client Certificate* is the current server certificate for secret launch.

It is required only when `client-cert` is set to enable in `access-proxy` in [Configuring traffic proxy on the gateway for forwarding secret launch \(traffic plane\) on page 141](#).

The certificate CA is configured on the gateway using the CLI commands as shown below or from *Network > FortiPAM Server > Server CA*:

```
config authentication setting
set user-cert-ca "CA_Cert_1"
end
```

14. Click *Submit*.

To configure a FortiGate gateway entry on FortiPAM:

1. Go to *Network > Secret Gateway*.
2. From the Gateway List, select *Create*.
The *New Gateway* window opens.
3. Enter a name for the gateway.
4. Ensure that the status is set to *Enable*.
5. From the *Type* dropdown, select *Reverse*.
6. In *Address*, enter the gateway IPv4 address.
7. In *Port*, enter 9443.
The *Gateway Address* and *Port* were configured in `ztna traffic-forward-proxy` in [Configuring traffic proxy on the gateway for forwarding secret launch \(traffic plane\) on page 141](#).
8. Ensure that *Health Check* is enabled and set to 60 seconds.
9. Optionally, enter a description.
10. In *Gateway ID*, enter the FortiGate reverse gateway common name.
11. In *Mode*, select *Reverse Gateway*.
12. In *SSL Max Version*, select *TLS 1.3*.
13. In the *Client Certificate* dropdown, select the client certificate for mTLS.
The *Client Certificate* is the current server certificate for secret launch.
It is required only when `client-cert` is set to enable in `traffic-forward-proxy` in [Configuring traffic proxy on the gateway for forwarding secret launch \(traffic plane\) on page 141](#).

The certificate CA is configured on the gateway using the CLI commands as shown below or from *Network > FortiPAM Server > Server CA*:

```
config authentication setting
set user-cert-ca "CA_Cert_1"
end
```

14. Click *Submit*.

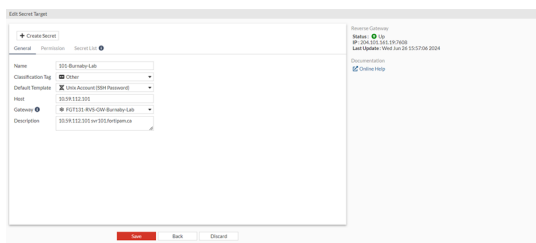
Configuring a target using reverse gateway on the FortiPAM server

To configure a target using the FortiPAM reverse gateway:

1. Go to *Secrets > Targets*.
2. Select *+Create*.
The *New Secret Target* window opens to the *General* tab.
3. Enter a name for the target.
4. From the *Classification Tag*, select a classification tag.
5. From the *Default Template* dropdown, select *Windows Domain Account*.
6. In *Domain-Controller*, enter the IP address of the server.
7. In *Domain*, enter the domain of the server.
8. In the *Gateway* dropdown, select the FortiPAM gateway entry created in [Configuring a gateway entry on FortiPAM server for secret launch \(traffic plane\)](#) on page 144.
9. Optionally, enter a description.
10. Click *Submit*.

To configure a target using the FortiGate reverse gateway:

1. Go to *Secrets > Targets*.
2. Select *+Create*.
The *New Secret Target* window opens to the *General* tab.
3. Enter a name for the target.
4. From the *Classification Tag*, select a classification tag.
5. From the *Default Template* dropdown, select *Unix Account (SSH Password)*.
6. In *Host*, enter the host IP address.
7. In the *Gateway* dropdown, select the FortiGate gateway created in [Configuring a gateway entry on FortiPAM server for secret launch \(traffic plane\) on page 144](#).
8. Optionally, enter a description.
9. Click *Submit*.



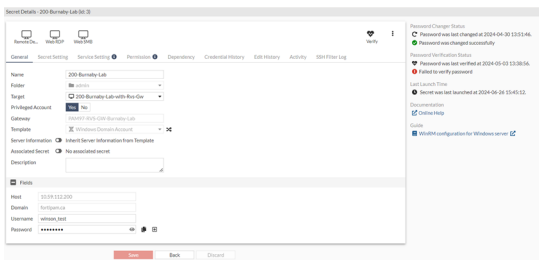
Creating a secret for the target that uses the FortiPAM reverse gateway

We create a secret for the target that uses FortiPAM reverse gateway and launch the secret from the FortiPAM server.

To create a secret for target:

1. Go to *Secrets > Secrets*.
2. In the *Secrets List*, select *Create*.
The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.
4. Select *Create*.
The *New Secret* window opens.
5. Enter a name for the secret.
6. From the *Target* dropdown, select the target that uses FortiPAM gateway created in [Configuring a target using reverse gateway on the FortiPAM server on page 146](#).
7. Enable *Privileged Account*.
8. In *Fields*:
 - a. In *Host*, enter the host IP address.
 - b. In *Domain*, enter the server domain.
 - c. Enter the user name.
 - d. Enter the password.
 - e. Reenter the password to confirm.

f. Click **Submit**.



Launching the FortiPAM secret

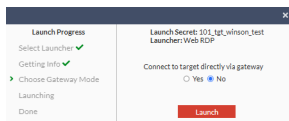
To launch the FortiPAM secret:

1. Go to *Secrets > Secrets*.
2. From the list, double-click to open the secret created in [Creating a secret for the target that uses the FortiPAM reverse gateway on page 147](#).
3. From the top, select *Remote Desktop - Windows*.

The *Launch Progress* dialog open:

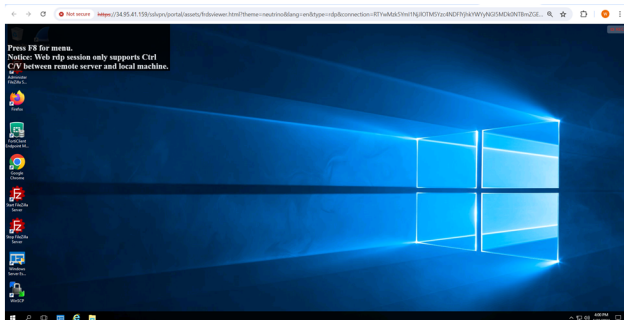
Select *No* to launch the secret using the gateway in the Reverse mode.

Select *Yes* to launch the secret using the gateway in the Service mode.



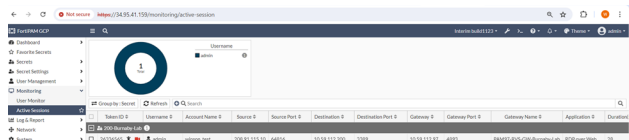
4. Select *Launch*.

You can now access the target Windows server.



To oversee activities of the launched secret:

1. From the secret server, go to *Monitoring > Active Sessions*.
The gateway information is displayed for the launched secret.



- For secret launch using the Service mode, you can monitor the ongoing secret sessions from the secret server. Also, you can monitor the secret sessions from the service gateway.

 In the service gateway, the username contains @<secret server SN> suffix.



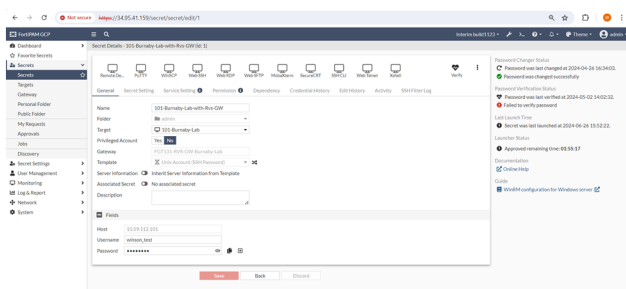
Token ID #	Username #	Account Name #	Source #	Source Port #	Destination #	Destination Port #	Gateway #	Gateway Port #	Gateway Name #	Application #	Duration(sec) #	Expires(sec) #
12549636	admin_winson@FF6VULTM4000212	winson_test	172.16.199.44	8695	10.59.112.101	443	N/A	N/A	N/A	SSH over Web	27	59969

Creating a secret for the target that uses the FortiGate reverse gateway

We create a secret for the target that uses FortiGate reverse gateway and launch the secret from the FortiPAM server.

To create a secret for target:

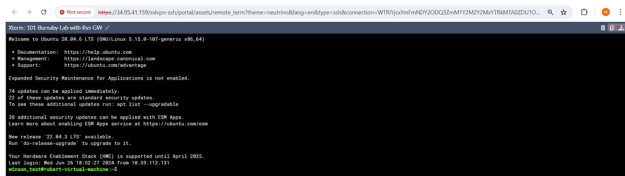
- Go to *Secrets > Secrets*.
- In the Secrets List, select *Create*.
The *Create New Secret in:* dialog appears.
- Select the folder where you intend to add the secret.
- Select *Create*.
The *New Secret* window opens.
- Enter a name for the secret.
- From the *Target* dropdown, select the target that uses FortiGate gateway created in [Configuring a target using reverse gateway on the FortiPAM server on page 146](#).
- Disable *Privileged Account*.
- In *Fields*:
 - In *Host*, enter the host IP address.
 - Enter the user name.
 - Enter the password.
 - Reenter the password to confirm.
 - Click *Submit*.



Launching the FortiGate secret

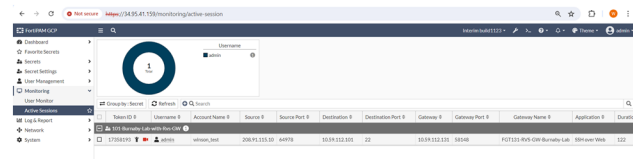
To launch the FortiGate secret:

1. Go to *Secrets > Secrets*.
2. From the list, double-click to open the secret created in [Creating a secret for the target that uses the FortiGate reverse gateway on page 149](#).
3. Launch the secret.
You can now access the target Linux server.



To oversee activities of the launched secret:

1. Go to *Monitoring > Active Sessions*.
The gateway information is displayed for the launched secret.



Troubleshooting

Use the following FortiPAM CLI commands to check the connection status.

1. In the CLI console on the FortiPAM server, use the following commands to show the reverse connections:

```
diagnose debug enable
diagnose test application wad 21600
Set diagnosis process: type=rev-connector index=0 pid=1237
diagnose test application wad 622
cert CAS
wss=0x7f2315b33930 cert->name=fortipam_cert5.pem
SSL CA store: Opened
[1] C = CA, ST = BC, L = Burnaby, O = Fortinet, OU = FortiPAM, CN = QA
remote client connections
1, src_addr=207.102.138.19:53900, dst_addr=10.0.1.15:8443, ctrl/sslled=1/1, gwy=PAM94-RVS-GW-Burnaby-Lab, cn=fortipam_gw3, ka_tm=1, ka/req/rsp/pending/ka_left=1/121/121/0/6
2, src_addr=204.101.161.19:7608, dst_addr=10.0.1.15:8443, ctrl/sslled=1/1, gwy=FGT131-RVS-GW-Burnaby-Lab, cn=fortipam_gw5, ka_tm=1, ka/req/rsp/pending/ka_left=1/120/120/0/6
3, src_addr=204.101.161.19:58632, dst_addr=10.0.1.15:8443, ctrl/sslled=1/1, gwy=PAM97-RVS-GW-Burnaby-Lab, cn=fortipam_gw4, ka_tm=1, ka/req/rsp/pending/ka_left=1/100/100/0/6
```

```
rmt stats: err_max_len=14, err_type=14, err_internal=0, data-act=18, ctrl_failure=0, dev_id_err=0
```

2. On the reverse gateway (FortiPAM), use the following commands:

```
diagnose de enable
diagnose test application wad 21600
Set diagnosis process: type=rev-connector index=0 pid=1664
diagnose test application wad 623
1 port=0x7f76b9c56600, state=3, act=1, reconn_tm=0 server=pam_gcp159, n_fails=0, reconn_tm_cnt=0, ka_tm=1, ka/req/resp/pending/tm_left(1/103/103/0/6)src=10.59.112.97:58632, dst=34.95.41.159:8443
2 port=0x7f76b9c56258, state=3, act=1, reconn_tm=0 server=pam_gcp, n_fails=0, reconn_tm_cnt=0, ka_tm=1, ka/req/resp/pending/tm_left(1/103/103/0/6)src=10.59.112.97:35460, dst=34.118.146.233:8443
Total reconnects=0
```

3. On the reverse gateway (FortiGate), use the following commands:

```
diagnose de enable
diagnose test application wad 21300
Set diagnosis process: type=reverse-connector index=0 pid=2685
diagnose test application wad 622
1 port=0x7ffbe18dc4c8, state=3, act=1, reconn_tm=0 server=pam78, n_fails=0, reconn_tm_cnt=0, ka_tm=1, ka/req/resp/pending/tm_left(1/22622/22598/0/2)src=10.59.112.131:2672, dst=10.59.112.133:8443
2 port=0x7ffbe18dc890, state=3, act=1, reconn_tm=0 server=gcp159, n_fails=0, reconn_tm_cnt=0, ka_tm=1, ka/req/resp/pending/tm_left(1/8709/8707/0/4)src=10.59.112.131:7608, dst=34.95.41.159:8443
Total reconnects=29
```

Debug trace for FortiPAM and FortiGate

For FortiPAM debug trace, use the following commands:

```
diagnose wad debug enable category gateway
diagnose wad debug enable category svc-conn
diagnose wad debug enable level verbose
diagnose debug enable
```

For FortiGate debug trace, use the following commands:

```
diagnose wad debug enable category ztna_rev_conn
diagnose wad debug enable category vs
diagnose debug enable
```

Configuring FortiGate forwarding access request from FortiPAM to the private target

Setting up a forward gateway on FortiPAM gives you access to private resources from anywhere.

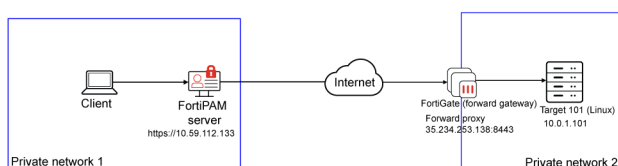
For more information about the forward gateway feature, see [Gateway](#) in the latest *FortiPAM Administration Guide*.

The example demonstrates FortiGate forwarding the access request from FortiPAM to a private target.

There are two methods to configure a FortiGate forward gateway:

1. **Legacy access proxy:** `firewall.access-proxy` is involved.
2. **New ZTNA forward proxy:** `ztna.traffic-forward-proxy` is involved (applicable to FortiGate 7.6.3 or above).

Topology



Prerequisites

- FortiPAM 1.4.0 or above

To configure FortiGate forwarding access request from FortiPAM to the private target:

1. [Configuring forward gateway on FortiGate on page 152](#)
2. [Configuring a gateway on the FortiPAM server on page 155](#)
3. [Configuring a target using the forward gateway on FortiPAM server on page 156](#)
4. [Creating a secret for the target on page 156](#)
5. [Launching the secret from the FortiPAM server on page 157](#)
6. [Monitoring the secret on page 158](#)
7. [Troubleshooting on page 158](#)

Configuring forward gateway on FortiGate

To configure on FortiGate:

1. In the CLI console, enter the following commands:
When using the legacy access proxy:

```
config firewall vip
edit "fwd_gw_vip"
set uuid 9b3ca40a-665d-51f0-95ee-b8ea5be9b17c
set type access-proxy
set server-type https
set extip 35.234.253.138
set extintf "port1"
set extport 8443
set client-cert disable
set ssl-certificate "Fortinet_SSL"
next
end
config firewall access-proxy
set "gw_access_proxy"
set vip "fwd_gw_vip"
set svr-pool-multiplex disable
config api-gateway
edit 2
set url-map "/tcp"
set service tcp-forwarding
config realservers
edit 1
set address "all"
next
end
next
end
next
end
config firewall proxy-policy
edit 4
set uuid 2a3e37a4-665e-51f0-8883-4c71a6572530
set proxy access-proxy
set access-proxy "gw_access_proxy"
set srcintf "any"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set logtraffic all
set utm-status enable
set ssl-ssh-profile "deep-inspection"
next
end
```

When using new ZTNA forward proxy:

```
config firewall vip
edit "fwd_gw_vip"
set uuid 9b3ca40a-665d-51f0-95ee-b8ea5be9b17c
set type access-proxy
set server-type https
```

```
set extip 35.234.253.138
set extintf "port1"
set extport 8443
set client-cert disable
set ssl-certificate "Fortinet_SSL"
next
end
config ztna traffic-forward-proxy
edit "ztna_fpam"
set vip "fwd_gw_vip"
next
end
config firewall proxy-policy
edit 3
set uuid 4d3ad48c-1d45-51ef-24ad-e8ec50ae317d
set proxy ztna-proxy
set ztna-proxy "ztna_fpam"
set srcintf "any"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set logtraffic all
set utm-status enable
set ssl-ssh-profile "deep-inspection"
next
end
```



`client-cert` is enabled by default.

When disabled, the forward gateway FortiGate does not check the FortiPAM server certificate during TLS handshake.

If enabled, you must configure the *Client Certificate* on the FortiPAM server in *Configuring a gateway on the FortiPAM server* on page 155.

The corresponding CA is configured on the FortiGate:

```
config authentication setting
set user-cert-ca "CA_Cert_1"
end
```



To import a CA on FortiPAM, go to *System > Certificates > Import CA Certificate*.

To import a certificate on FortiPAM or FortiGate, go to *System > Certificates > Import Certificate > Import Certificate*.

Configuring a gateway on the FortiPAM server

To configuring a gateway on the FortiPAM server:

1. Go to *Secrets > Gateway*.
2. In the Gateways list, select *+Create*.
The *New Gateway* window opens.
3. In *Name*, enter a name for the gateway.
4. Ensure that the *Status* is enabled.
5. Ensure that *Type* is *Forward*.
6. In *Address*, enter the IP address of the forward proxy.
This was set up on port1 in [Configuring forward gateway on FortiGate on page 152](#).
7. In *Port*, enter the gateway port number.
In this example, it is 8443.
This was set up in [Configuring a gateway on the FortiPAM server on page 155](#).
8. Ensure that the *SSL Max Version* is *TLS 1.3* (default).
9. Ensure that the *TCP Forwarding Path* is *tcp* (default). This tells the gateway how to internally process the request from FortiPAM.
10. Optionally, enter a description.
11. Click *Submit*.

The screenshot shows the 'New Gateway' configuration window with the following settings:

Field	Value
Name	fvrd_gcp_fg760
Status	Enable
Type	Forward
Address	33.234.253.138
Port	8443
SSL Max Version	TLS 1.3
Client Certificate	None
CA Certificate	None
TCP Forwarding Path	tcp
Description	



Client Certificate is required only when `client-cert` is enabled in [Configuring forward gateway on FortiGate on page 152](#).



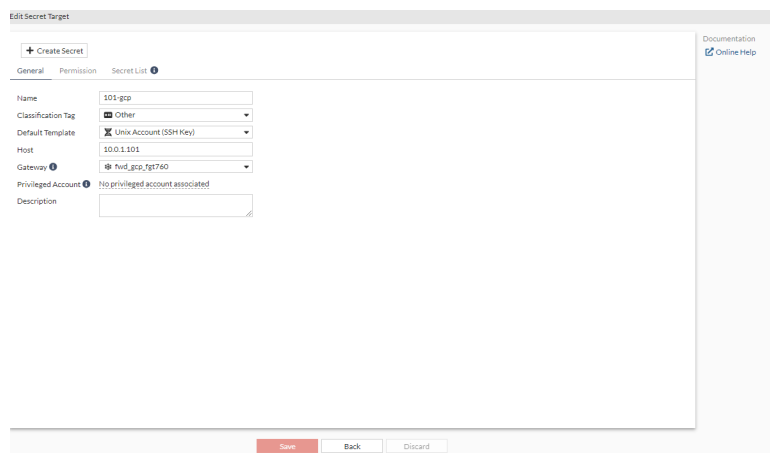
CA Certificate is the CA for the FortiGate certificate configured in [Configuring forward gateway on FortiGate on page 152 \(ssl-certificate\)](#).

If it is not configured, FortiPAM server does not check the FortiGate certificate during the TLS handshake.

Configuring a target using the forward gateway on FortiPAM server

To configure a target using the forward gateway on the FortiPAM server:

1. Go to *Secrets > Targets*.
2. Select *+Create*.
The *New Secret Target* window opens.
3. In *Name*, enter a name for the target.
4. In the *Classification Tag* dropdown, select *Other*.
5. In the *Default Template* dropdown, select *Unix Account (SSH Key)*.
6. In *Host*, enter `10.0.1.101`.
7. In the *Gateway* dropdown, select the gateway created in [Configuring a gateway on the FortiPAM server on page 155](#).
8. Optionally, enter a description.
9. Click *Submit*.



The screenshot shows the 'Edit Secret Target' configuration window. The 'General' tab is active, displaying the following fields:

- Name:** 101.gwp
- Classification Tag:** Other
- Default Template:** Unix Account (SSH Key)
- Host:** 10.0.1.101
- Gateway:** fwd_gwp_791740
- Privileged Account:** No privileged account associated
- Description:** (empty text area)

At the bottom of the window, there are three buttons: 'Save' (highlighted in red), 'Back', and 'Discard'. In the top right corner, there are links for 'Documentation' and 'Online Help'.

Creating a secret for the target

To create a secret for the target:

1. Go to *Secrets > Secrets*.
2. In *Secrets List*, select *Create*.
The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.
4. Select *Create*.
The *New Secret* window opens.
5. Enter the secret name.
6. Enable *Target*, from the dropdown, select the target created in [Configuring a target using the forward gateway on FortiPAM server on page 156](#).
7. From *Template* dropdown, select the *Unix Account (SSH Key)* template.
8. Optionally, enter a description.

9. In the *Fields* pane:
 - a. In *Host*, enter the target IP address.
 - b. In *Username*, enter the user name.
 - c. In *Passphrase*, enter the password.
 - d. Reenter the password to confirm.
10. Click *Submit*.

Launching the secret from the FortiPAM server

To launch the secret:

1. Go to *Secrets > Secrets*.
2. In *Secrets List*, double-click to open the secret created in [Creating a secret for the target on page 156](#).
3. From the top select *Web SSH* to launch the secret to access Target 101 (Linux server).
Web SSH allows you to access the target using the browser SSH client.



To use the *Web SSH* launcher, ensure that you have already installed the FortiPAM extension for your browser.

A new browser tab opens. You can now access the target using Web SSH.

```

cat /etc/os-release
NAME="Ubuntu"
VERSION="22.04 LTS (Jammy Jellyfish)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 22.04 LTS"
VERSION_ID="22.04"
HOME_URL="https://www.ubuntu.com/"
SUPPORT="https://ubuntu.com/support"

```

Monitoring the secret

To monitor the secret:

1. Go to *Monitoring > Active Sessions*.

The gateway information is displayed for the launched secret.



Troubleshooting

Use the following FortiPAM CLI command to check the connection status:

```
diagnose wad session list
172.16.199.154:58507->10.0.1.101:65522
id=212935453 worker=0 vd=0:0 fw-policy=1 type=proxy
duration=600 expire=6599 session-ttl=7200
state=0 app=http sub_type=0 wan_opt_mode=0 dd_method=0
username=admin account name=liangw secret=1042 sec_name=101-gcp-via-fwd-gw token-id=13968146
gateway name=fwd_gcp_fgt760 port=35.234.253.138:8443
TCP Port:
state=2 r_blocks=1 w_blocks=0 read_blocked=0
bytes_in=3577 bytes_out=3255 shutdown=0x0
Sessions total=1
```

Use the following FortiGate CLI command on the FortiGate forward gateway:

```
diagnose wad session list
Session: access proxy 207.102.138.19:46302(10.0.1.2:2890)->10.0.1.101:65522
id=255592312 worker=0 vd=0:0 fw-policy=1
duration=681 expire=3575 session-ttl=3600
state=3 app=http sub_type=0 wan_opt_mode=0 dd_method=0
SSL enabled
to-client
SSL Port:
state=3
TCP Port:
state=2 r_blocks=1 w_blocks=0 read_blocked=0
bytes_in=4909 bytes_out=7311 shutdown=0x0
To-server
TCP Port:
state=2 r_blocks=0 w_blocks=0 read_blocked=0
bytes_in=4986 bytes_out=3828 shutdown=0x0
Sessions total=1
```

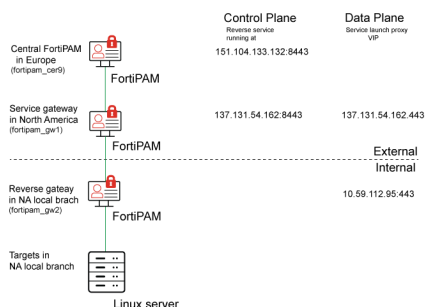
Accessing a private target using secret gateway chaining

This example demonstrates how to use Secret Gateway Chaining to access a target located in a private network that is not directly reachable from the root FortiPAM.

Prerequisites

- All FortiPAM devices and Service Gateways run the same FortiPAM version.
- Reverse Service connectivity from downstream gateways to upstream gateways is allowed.
- Certificates are installed on all devices and signed by the same trusted CA.
- Each gateway certificate uses a unique CN.
- The target server is reachable from the reverse gateway (`fortipam_gw2`).

Topology



- Central FortiPAM in Europe (`fortipam_cert9`)
 - Control plane (Reverse Service): 151.104.133.132:8443
- Service Gateway in North America (`fortipam_gw1`)
 - Control plane (Reverse Service): 137.131.54.162:8443
 - Data plane (Secret launch proxy VIP): 137.131.54.162:443
- Reverse Gateway in North America local branch (`fortipam_gw2`)
 - Data plane (Secret launch proxy): 10.59.112.95:443
- Targets in North America local branch
 - Accessible only through `fortipam_gw2`

Traffic flows as follows:

- Control plane reverse connections are established from downstream gateways to upstream gateways on port 8443.
- Data plane secret launch traffic flows through the gateway chain on port 443 to reach the target.

Note:

- Only the reverse gateway (fortipam_gw2) has direct network access to the target systems.
- All other connectivity follows the chained reverse connections illustrated in the diagram.
- The Central FortiPAM is also known as Root FortiPAM.
- The gateway ID is the CN of the certificate used by a gateway for TLS connection. In a gateway chain, this ID identifies a gateway.

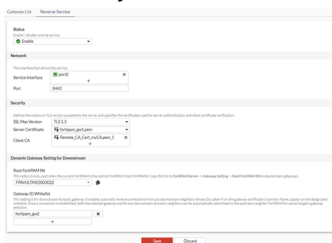
Accessing a private target using secret gateway chaining

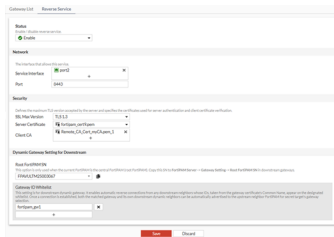
1. [Configure Reverse Service on the root FortiPAM \(Upstream Device\) on page 160](#)
2. [Configuring the downstream connection on Service Gateway/Reverse Gateway on page 161](#)
3. [Configuring a target using the Reverse Gateway \(fortipam_gw2\) on page 162](#)
4. [Creating and launching a secret on page 163](#)
5. [Results on page 163](#)
6. [Troubleshooting on page 163](#)

Configure Reverse Service on the root FortiPAM (Upstream Device)

To configure Reverse Service on the root FortiPAM (Upstream Device):

1. Go to *Network > Secret Gateway* and select the *Reverse Gateway* tab.
2. From the *Status* dropdown, select *Enable*.
3. In *Service Interface*, select the interface where the reverse service is enabled.
In this example, port2 with public IP address (151.104.133.132) is selected.
Note: port2 is the external port for public access on the central FortiPAM.
4. Ensure that the *Port* is 8443 (the reverse service port number).
5. Ensure that *SSL Max version* is *TLS 1.3*.
6. In *Server Certificate*, select the current FortiPAM certificate for the reverse plane mTLS.
7. In *Client CA*, select the CA issuing the certificate used by the downstream neighbor.
8. *Root FortiPAM SN* indicates the central FortiPAM for downstream gateways when establishing the dynamic chain.
Note: If the current FortiPAM is not the central FortiPAM ignore *Root FortiPAM SN* the field.
Save the *Root FortiPAM SN* value for downstream configuration.
9. In *Gateway ID Whitelist*, enter the certificate CN of the service gateway.
Note: The setting enables automatic reverse connections from any downstream gateways, provided that the gateway certificate CN appears on the allowlist.
 - a. In the service gateway, go to *Network > Secret Gateway*, and select the *Reverse Gateway* tab.
 - b. In *Gateway ID Whitelist*, enter the downstream reverse gateway ID.



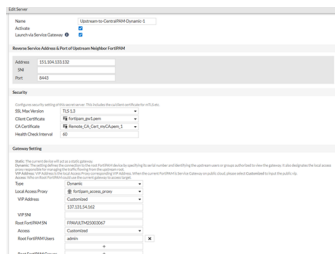
10. Select *Save*.

Configuring the downstream connection on Service Gateway/Reverse Gateway

To configure the downstream connection on Service Gateway:

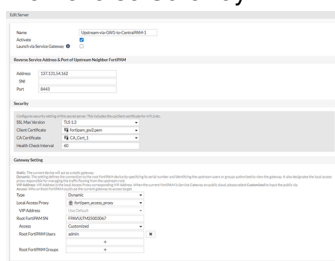
1. In the Service Gateway, go to *Network > FortiPAM Server*, and select *Create*.
2. Enter a name for the server.
3. Enable *Launch via Service Gateway*.
When enabled, the current FortiPAM acts as the service gateway.
4. In *Reverse Service Address & Port of Upstream Neighbor FortiPAM*:
 - a. In *Address*, enter the central FortiPAM reverse service listening IP address.
 - b. In *Port*, enter the central FortiPAM reverse service port number.
5. In *Security*:
 - a. In *SSL Max Version*, ensure that *TLS 1.3* is selected.
 - b. In *Client Certificate*, select the same certificate as in the service gateway.
 - c. In *CA Certificate*, select the same CA as in [Configure Reverse Service on the root FortiPAM \(Upstream Device\) on page 160](#).
 - d. In *Health Check Interval*, ensure that 60 (seconds) is entered.
6. In *Gateway Setting*:
 - a. In *Type*, select *Dynamic*.
 - b. In *Local Access Proxy*, select the current device access proxy for secret launch traffic.
Note: If the current FortiPAM is deployed on public cloud, you must select *Customized* in *VIP Address*, and enter the corresponding public VIP.
 - c. In *Root FortiPAM SN*, enter the serial number copied from the root (central) FortiPAM as in step 8 in [Configure Reverse Service on the root FortiPAM \(Upstream Device\) on page 160](#).
Note: *Root FortiPAM SN* is the destination of the current gateway information.
 - d. In *Access*, select *Customized*:
 - i. In *Root FortiPAM Users*, select the users from the central FortiPAM allowed to use the current gateway.
 - ii. In *Root FortiPAM Groups*, select the user groups from the central FortiPAM allowed to use the current gateway.

7. Click *Submit*.



To configure the downstream connection on Reverse Gateway:

1. On the *Reverse Gateway*, go to *Network > FortiPAM Server*, and select *Create*.
2. Similar to [Configuring the downstream connection on Service Gateway](#), configure the downstream connection on the *Reverse Gateway*.



Verifying the dynamic gateway discovery

To verify the dynamic gateway discovery:

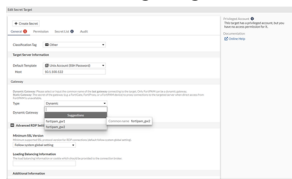
1. On the central FortiPAM, go to *Network > Secret Gateway* to check the dynamic gateway status.



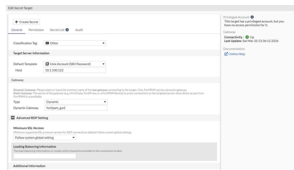
Configuring a target using the Reverse Gateway (fortipam_gw2)

To configure a target using the Reverse Gateway (fortipam_gw2):

1. Create or edit an existing target in *Secrets > Targets*.
2. In an existing target, change the *Type* to *Dynamic*.



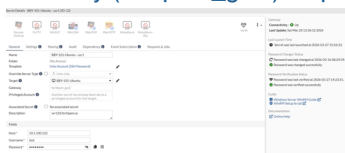
- In *Dynamic Gateway*, select the gateway.
 - Click *Save*.
- Note:** The gateway status is displayed on the right.



Creating and launching a secret

To create a secret:

- Go to *Secrets > Secrets*, and create a secret associated with the target in [Configuring a target using the Reverse Gateway \(fortipam_gw2\)](#) on page 162.



- Launch the secret.
Traffic is automatically routed through:
Root FortiPAM → Service Gateway A → Reverse Gateway B → Target Server

Results

- The private target is accessed without direct connectivity to the root FortiPAM.
- No static gateway configuration is required.
- Gateway participation is enforced through *Gateway ID Whitelist*.
- Gateway chaining and session routing are handled automatically.

Troubleshooting

Status check

- Check the control pane status using the following CLI commands:
Central-PAM

```
diagnose de en
diagnose test application wad 21600
Set diagnosis process: type=rev-connector index=0 pid=6258
```

```
diagnose test application wad {622 | 623} #For check downstream use 622, for check upstream use 623
```

```

=====cert CAS=====
wss=0x7f309a9f6768 cert->name=fortipam_cert9.pem
SSL CA store: Opened
[1] C = CA, ST = BC, L = Burnaby, O = Fortinet, OU = FortiPAM, CN = QA
=====remote client connections=====
1, src_addr=137.131.54.162:59544, dst_addr=10.0.0.2:8443, ctrl/ssled/svc_gwy=1/1/1, gwy=[auto]
fortipam_gw1, cn=fortipam_gw1, ka_tm=1, ka/req/rsp/pending/ka_left=1/13/13/0/4
rmt stats: err_max_len=2, err_type=2, err_internal=0, data-act=0, ctrl_failure=0, dev_id_err=8

```

```

diagnose test application wad 623 #for checking chanining
chain #0, root=FPAVULTM25003067, terminal(1)
downstream:
  neighbor gwy=[auto] fortipam_gw1, id=fortipam_gw1, setup=1
  other gwy=[auto] fortipam_gw2_16, id=fortipam_gw2, distance=2

```

2. Check the data plane status using the following CLI commands:

Central-PAM

```

diagnose de en
diagnose test application wad 2200
Set diagnosis process: type=worker index=0 pid=6263

```

```

diagnose test application wad 426
1 reverse gateway(Service-Gateway-Phoenix-gw1), enabled=0, pam() ref_cnt=9, addr
(sni)/port=137.131.54.162():443, api_path=tcp,
ssl_max_ver=4, ca=, cert=, addr=137.131.54.162:47873, id=fortipam_gw1x, distance=1, ka_
interval=60, svc_mode=2, wp_addr=, wp_port=0 ssl_min_ver=770
2 reverse gateway(Service-Gateway-Montreal-GCP), enabled=0, pam() ref_cnt=2, addr
(sni)/port=35.203.50.31():443, api_path=tcp,
ssl_max_ver=4, ca=Remote_CA_Cert_myCA.pem_1, cert=, addr=35.203.50.31:47873, id=fortipam_
cert8, distance=1, ka_interval=60, svc_mode=2, wp_addr=, wp_port=0 ssl_min_ver=770
1 auto rev gateway([auto] fortipam_gw2_16), pam(FPAVULTM25003067) ref_cnt=1, id=fortipam_gw2,
source=fortipam_gw1, distance=2, conf_addr=:0, sni= addr= wp=(:0)
[groups]: [users]:admin
2 auto rev gateway([auto] fortipam_gw1), pam(FPAVULTM25003067) ref_cnt=1, id=fortipam_gw1,
source=, distance=1, conf_addr=137.131.54.162:443, sni= addr=137.131.54.162:59544 wp=(:0)
[groups]: [users]:admin
2 auto rev gateway([auto] fortipam_gw1), pam(FPAVULTM25003067) ref_cnt=1, id=fortipam_gw1,
source=, distance=1, conf_addr=137.131.54.162:443, sni= addr=137.131.54.162:59544 wp=(:0)
[groups]: [users]:admin

```

There are total two gateways and two auto gateways

```

diagnose test application wad 437
local shm /tmp/wad/persistent/revs_gwy_info(updater=0) sz=248332, max_cnt=0, stats is:
sz=248332, elem_sz=3880, elem_used=2
n_attach_failure:0, n_create_failure:0, n_inc_try:0, n_inc_failure:0, n_shrink:0, n_shrink_
failure:0;
n_insert_failure:0, n_inc_max_reached:0
1 gwy:[auto] fortipam_gw1, dyn:1 distance=1, id:fortipam_gw1 src=, up=1, ver=16778956, svc_
gwy=1(enable), addr:137.131.54.162:59544, last-act:Sat Mar 28 13:55:49 2026
,msg:

```

```
[groups]: [users]: admin
2 gwy:[auto] fortipam_gw2_16, dyn:1 distance=2, id:fortipam_gw2 src=fortipam_gw1, up=1, ver=0,
svc_gwy=0(disable), addr:, last-act:Sat Mar 28 13:36:12 2026
,msg:
[groups]: [users]: admin
```

Use the following CLI commands to generate debug trace:

```
diagnose wad debug enable category svc-conn
diagnose wad debug enable category gateway
diagnose wad debug enable level verbose
diagnose de en
```

SSH filter profiles

This section describes examples related to FortiPAM SSH filter profiles.

For information on *SSH filter profiles*, see SSH filter profiles in the latest *FortiPAM Administration Guide*.

Configuring an SSH filter profile on FortiPAM to restrict SSH access to secret servers

The FortiPAM SSH filter allows you to control SSH access to a secret server so that only specific commands execute.

Starting FortiPAM 1.4.0, SSH filter profiles can operate in two modes:

- *Deny*: You can configure a list of SSH command patterns that cannot be used by the FortiPAM user.
- *Allow*: You can configure a list of SSH command patterns that can be executed by the user. Other commands entered by the user are blocked by FortiPAM.

To configure an SSH filter profile on FortiPAM to restrict SSH access to secret servers:

1. [Configuring SSH filter profiles in the CLI on page 166](#)
2. [Configuring SSH filter profiles using the GUI on page 167](#)

Configuring SSH filter profiles in the CLI

To configure SSH filter profiles in the CLI:

1. In the CLI console, enter the following commands to create SSH filter profiles with restricted mode disabled and another with restricted mode enabled:

```
config ssh-filter profile
edit "test_profile" #SSH filter profile with restricted mode disabled
set restricted-mode disable
config shell-commands
edit 1
set pattern "ping 8.8.8.8"
set exact-match enable
set severity low
next
edit 2
set pattern "ifconfig"
set log enable
set severity low
next
```

```
edit 3
  set pattern "ls"
  next
end
next
edit "test_profile2" #SSH filter profile with restricted mode enabled
set restricted-mode enable
set shortcut-input enable
config shell-commands
edit 1
  set pattern "ping"
  set severity low
  next
edit 2
  set pattern "ifconfig virbr0"
  set exact-match enable
  next
edit 3
  set pattern "ls"
  set log enable
  next
end
next
end
```

Configuring SSH filter profiles using the GUI

Deny mode

The *Deny mode* is the legacy mode where you can configure the SSH shell command patterns that users are not allowed to execute when using the SSH launchers to connect to the server.

Command with parameters

Start with single word

When *Exact Match* is not enabled in the configuration, i.e., type *Start with single word* is selected, FortiPAM parses a user entered shell input into two parts: "command" and "parameters".

For example, when a user enters `ifconfig eth0 up`, `ifconfig` is interpreted as a command, and `eth0 up` is interpreted as the parameter of `ifconfig`. Therefore, `ifconfig` is configured as one of the patterns in the SSH filter profile, any shell inputs starting with `ifconfig` are blocked. However, you may only want to block commands with certain parameters sometimes. For example, if we only want to block the execution of `ifconfig eth0 down` but allow the execution of `ifconfig virbr0 up/down`, then *Exact Match* should be used.

Exact Match

When you configure a shell command pattern in an SSH filter profile with *Exact Match*, FortiPAM performs exact match for commands. In the example below with *test_profile* SSH filter profile, when the user enters `ping 8.8.8.8`, FortiPAM blocks it. The command `ping 8.8.8.7` or any other destination is allowed to execute.

Examples

- `date; ls -l; rm /home/folder/sensitive/docs`

If “;” separates multiple commands in a sentence, all the commands are checked against all the shell patterns with the type “simple”. In the above case, `date`, `ls`, and `rm` are checked. Simple mode inspection is performed first. In this example, `date` is checked first against all the simple mode patterns defined in the SSH filter profile. If there is any pattern match, the sentence is blocked. Otherwise, `ls` then `rm` is checked.

If all the commands pass the simple mode inspection but no pattern is found, we go to the regular expression pattern check. The sentence will also be blocked if any predefined regex patterns match `date; ls -l; rm /home/folder/sensitive/doc`.

- `(ls /home/user1)\&(pwd)`

When the character `&` is used to separate two commands, both command `ls` and `pwd` are checked against the SSH filter profile. See the example with *test_profile* below. The input is blocked as it matches the predefined shell command pattern entry 3 `ls`.

Restricted mode

Restricted mode refers to the *Allow* mode in GUI, where you can configure the SSH shell command patterns that users can execute. Other than the configured command patterns, all other inputs that do not match the predefined patterns are blocked. FortiPAM in this mode interprets the user inputs in the same way as the blocklist mode, i.e., parses the input as command and parameters, exact match, etc.

Menu command

In restricted mode, a banner message contains the list of commands allowed to execute. This appears before the user logs in to the SSH secret server. After that, users can also use the “menu” (customizable) to list the commands anytime as needed.

```

:~$ menu
List of commands that're allowed to execute in this system(CMD index shortcut is enabled):
No.      Type      Exact-match  CMD
1.       simple    yes          "ifconfig virbr0"
2.       simple    no           "ls"
3.       simple    no           "ping"
4.       regex     n/a          "exec ping.*"
^C

```

Shortcut input

Under restricted mode, for ease of input, users can directly enter the command number in the menu list for execution. For example, in the below case, the user can enter 1 to execute command `ifconfig virbr0` as shown below.

```

:~$ menu
List of commands that're allowed to execute in this system(CMD index shortcut is enabled):
No.      Type      Exact-match  CMD
1.       simple    yes          "ifconfig virbr0"
2.       simple    no           "ls"
3.       simple    no           "ping"
4.       regex     n/a         "exec ping.*"
^C
:~$ 1 -> ifconfig virbr0
virbr0: error fetching interface information: Device not found
:~$ █

```

Examples

- (ls /);(ping 8.8.8.8)

As “,” separates two commands in a sentence, command `ls` and `ping` must match against all the patterns (type simple) defined in the SSH filter profile.

The sentence can execute, if both `ls` and `ping` can be matched to a pattern. Otherwise, it goes to the regular expression matching. The sentence can execute if any predefined regex patterns match (ls /);(ping 8.8.8.8). If no regular expression pattern can still be matched, FortiPAM blocks the input.

Use the configuration from *Shortcut input* as an example. The input (ls /);(ping 8.8.8.8) is allowed, while input (ls /);(pwd) is blocked as `pwd` cannot match any pattern in the profile.

```

:~$ menu
List of commands that're allowed to execute in this system(CMD index shortcut is enabled):
No.      Type      Exact-match  CMD
1.       simple    yes          "ifconfig virbr0"
2.       simple    no           "ls"
3.       simple    no           "ping"
4.       regex     n/a         "exec ping.*"
^C
:~$ 1 -> ifconfig virbr0
virbr0: error fetching interface information: Device not found
:~$ ifconfig virbr0
virbr0: error fetching interface information: Device not found
:~$ ifconfig virbr1
This command is not allowed to execute. Use "menu" command to show the list of commands that are
allowed to execute.
^C
:~$ (ls /);(ping 8.8.8.8)
bin  cdrom  etc  lib  lib64  lost+found  mnt  proc  run  snap  swapfile  tmp  usr
boot  dev  home  lib32  libx32  media  opt  root  sbin  srv  sys  time  var
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=117 time=4.33 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=5.03 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=117 time=4.17 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 4.168/4.509/5.030/0.374 ms
:~$ (ls /);(pwd)
This command is not allowed to execute. Use "menu" command to show the list of commands that are
allowed to execute.
^C
:~$ 4
Please type your command directly for regex type CMD!
^C
:~$ █

```

To configure SSH filter profiles on the GUI with *Deny* mode:

1. Go to *Secret Settings > SSH Filter Profiles* and select *Create*.
The *New SSH Filter Profile* window opens.
2. In *Name*, enter a name for the SSH filter profile.
3. Set *Mode* as *Deny*.

4. In *Pattern*, add the following patterns:
 - a. Select *Exact Match*, enter `ping 8.8.8.8`, and select *Add Pattern*.
 - b. Select *Start with single word*, enter `ifconfig`, and select *Add Pattern*.
 - c. Select the pen icon to edit the last added pattern, enable *Log*, and select the checkmark.
 - d. Select *Start with single word*, enter `ls`, and select *Add Pattern*.
 - e. Select the pen icon to edit the last added pattern, set *Severity to Medium*, and select the checkmark.
5. Click *Submit*.

The screenshot shows the 'New SSH Filter Profile' configuration window. The 'Name' field is set to 'test_profile'. The 'Shell Channel' is set to 'Other Channels'. The 'Mode' is set to 'Deny', and 'Log All Unlisted Commands' is set to 'Enable'. The 'Pattern' section contains a table with the following data:

Pattern	Type	Log	Email Alert	Severity	Operation
ping 8.8.8.8	Exact Match	Disable	Disable	Low	[Edit] [Delete]
ifconfig	Start with	Enable	Disable	Low	[Edit] [Delete]
ls	Start with	Disable	Disable	Medium	[Edit] [Delete]

At the bottom of the window, there are 'Submit' and 'Cancel' buttons.

To configure SSH filter profiles on the GUI with *Allow* mode:

1. Go to *Secret Settings > SSH Filter Profiles* and select *Create*.
The *New SSH Filter Profile* window opens.
2. In *Name*, enter a name for the SSH filter profile.
3. Set *Mode* as *Allow*.
4. Enable *Shortcut To Run Listed Commands*.
5. In *Pattern*, add the following patterns:
 - a. Select *Start with single word*, enter `ping`, and select *Add Pattern*.
 - b. Select *Exact Match*, enter `ifconfig virb0`, and select *Add Pattern*.
 - c. Select the pen icon to edit the last added pattern, set *Severity to Medium*, and select the checkmark.
 - d. Select *Start with single word*, enter `ls`, and select *Add Pattern*.
 - e. Select the pen icon to edit the last added pattern, set *Log to Enable*, set *Severity to Medium*, and select the checkmark.

6. Click *Submit*.

New SSH Filter Profile

Name: test_profile2

Shell Channel: Other Channels: 1

Mode: Deny Allow

Show Allowed List Command: menu

Shortcut To Run Listed Commands: Disable Enable

Log All Unlisted Commands: Disable Enable

Pattern	Type	Log	Email Alert	Severity	Operation
<input type="checkbox"/> ping	Start with	Disable	Disable	Low	
<input type="checkbox"/> ifconfigvibr0	Exact Match	Disable	Disable	Medium	
<input type="checkbox"/> ls	Start with	Enable	Disable	Medium	

Submit Cancel

Configuring log only command pattern

The SSH filter profile configured in the example below does not block any command but logs only some command patterns.

To configure log only command pattern:

1. Go to *Secret Settings > SSH Filter Profiles* and select *Create*.
The *New SSH Filter Profile* window opens.
2. In *Name*, enter a name for the SSH filter profile.
3. Set *Mode* as *Deny*.
4. Disable *Log All Unlisted Commands*.
5. In *Pattern*, add the following patterns:
 - a. Select *Exact Match*, enter ping 8.8.8.8, and select *Add Pattern*.
 - b. Select the pen icon to edit the last added pattern, enable *Log*, and select the checkmark.
6. Click *Submit*.

Edit SSH Filter Profile

Name: log_only

Shell Channel: Other Channels: 1

Mode: Deny Allow

Log All Unlisted Commands: Disable Enable

Pattern	Type	Log	Email Alert	Severity	Operation
<input type="checkbox"/> ping.8.8.8	Exact Match	Enable	Disable	Low	

Save Back Discard

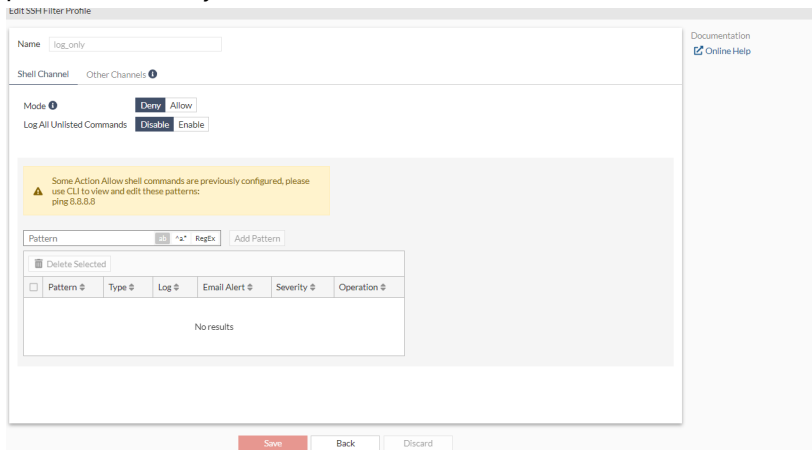
7. In the CLI console, enter the following commands:

```

config ssh-filter profile
edit "log_only"
set block x11 exec port-forward tun-forward sftp unknown
unset log
set restricted-mode disable
set default-command-log disable
config shell-commands
edit 1
set type simple
set pattern "ping 8.8.8.8"
set exact-match enable
set action allow #enable this option
set log enable
set alert disable
set severity low
next
end
next
end

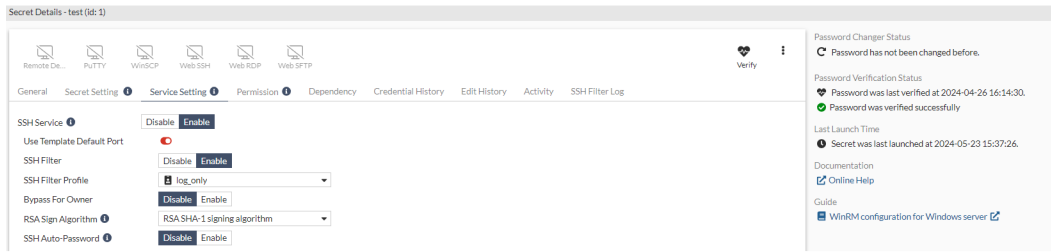
```

In the SSH filter profile, no pattern is shown. Instead, a warning indicates that you configured Action = Allow pattern in the *Deny* mode.

**To apply the SSH filter profile to a secret:**

1. Go to *Secrets > Secrets*.
2. From the list, double-click to open a secret and go to the *Service Setting* tab.
3. Enable *SSH Service*:
 - a. Enable *SSH Filter*.
 - b. From the *SSH Filter Profile* dropdown, select the SSH filter profile created in [Configuring an SSH filter profile with log only command pattern](#).

4. Click Save.



Results

When you launch the secret, you see that no commands are blocked; they are only logged.

```

:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=54 time=4.95 ms
^C
--- 8.8.8.8 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 4.951/4.951/4.951/0.000 ms
:~$ ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.027 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.039 ms
^C
--- 127.0.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1013ms
rtt min/avg/max/mdev = 0.027/0.033/0.039/0.006 ms
:~$ ls
Desktop Documents Downloads Music Pictures Public Templates thinclient_drives tmp_test Videos
:~$
    
```

When you open the secret from *Secrets > Secrets*, in the *SSH Filter Log* tab, you see that command is allowed:

Date/Time	User	Severity	Action	Command	Message
2024/06/28 10:44:...	admin	■■■■■	Passthrough	ping 8.8.8.8	

Automation

This section describes examples related to FortiPAM automations.

Using default automation stitch- Secret Credential View

In this example, we demonstrate how to use the *Secret Credential View* default automation stitch.

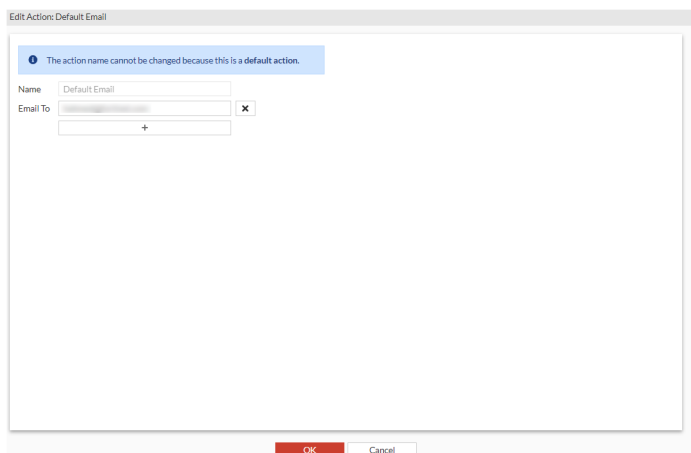
To use the default **Secret Credential View** automation stitch:

1. [Using the Secret Credential View automation stitch on page 174](#)
2. [Results on page 175](#)

Using the Secret Credential View automation stitch

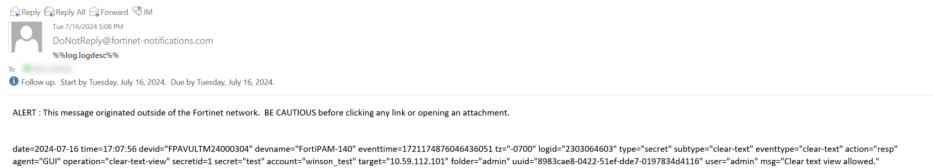
To use the **Secret Credential View** automation stitch:

1. Go to *Log & Report > Automation*.
2. From the list, select *Secret Credential View*, and select *Enable*.
3. Go to the *Action* tab.
4. Since the *Secret Credential View* stitch uses *Default Email* action, double-click *Default Email* to edit it. The *Edit Action: Default Email* window opens.
5. In *Email To*, enter the recipient email address.
6. Click *OK*.



Results

1. Go to *Secrets > Secrets*.
2. In *Secrets*, double-click to open a secret.
3. In the *Fields* pane, click the eye icon to view the secret password.
You will receive an alert email on the email address that you set up in step 5 in [Using the Secret Credential View automation stitch on page 174](#).



The alert email contains information about secret password being viewed by the user.

Customizing an automation stitch

In this example, we create a new automation stitch to monitor when a secret is launched:

- The automation trigger is the secret launch event.
We specify the secret to be monitored.
- An alert email is sent to the recipient.

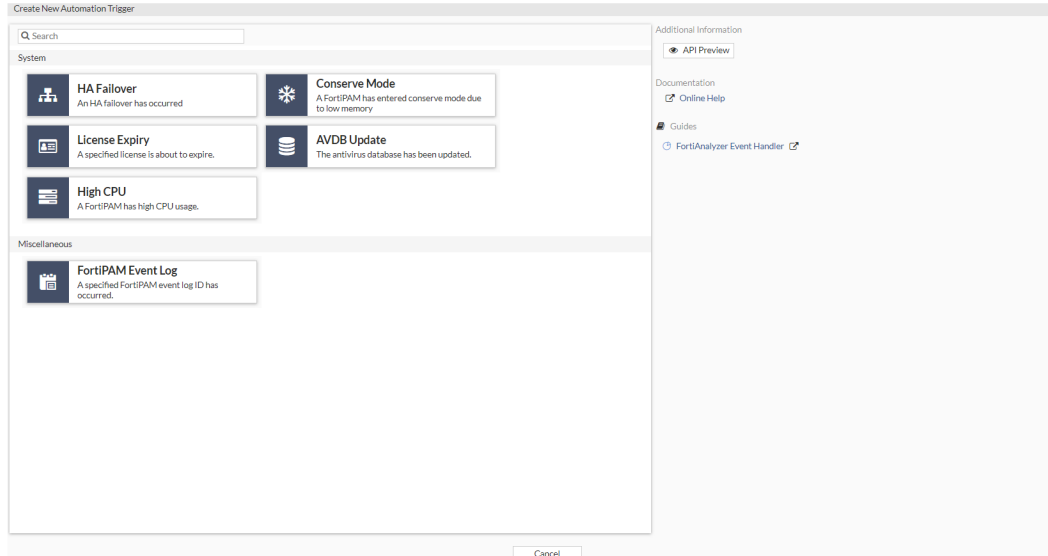
To customize an automation stitch:

1. [Creating an automation trigger on page 175](#)
2. [Create an action on page 177](#)
3. [Creating a stitch on page 178](#)
4. [Results on page 179](#)

Creating an automation trigger

To create an automation trigger:

1. Go to *Log & Report > Automation* and select the *Trigger* tab.
2. In the *Trigger* tab, select *Create*.
A *Create New Automation Trigger* window opens.



3. From the *Miscellaneous* pane, select *FortiPAM Event Log*.
This category is used when a specified FortiPAM event log ID has occurred.
An updated *Create New Automation Trigger* window opens.
4. In *Name*, enter a name.
5. In the *FortiPAM Event Log* pane:
 - a. In *Event*, select *+*, from *Select Entries*, select *Secret launch*.
 - b. Click *Close*.
 - c. Optionally, for *Field filter(s)*, we will monitor field name *secret* and a field value:
The field value is the name of the secret to be monitored.
 - i. In the CLI console, enter the following:

```
execute log filter category 23 #23 is for secrets
execute log display #If no log found,launch a secret and run the CLI command again
```

- ii. From the list displayed in the CLI console, copy the value for *secret* to your management computer:

```
date=2024-07-16 time=17:07:55 eventtime=1721174876046436051 tz="-0700"
logid="2303064603" type="secret" subtype="clear-text" eventtype="clear-text"
action="resp" agent="GUI" operation="clear-text-view" secretid=1 secret="test"
account="winson_test" target="10.59.112.101" folder="admin" uuid="8983cae8-0422-51ef-
d4116" user="admin" msg="Clear text view allowed.
```

- d. In *Field name*, enter *secret*.
- e. In *Value*, enter the secret name that you copied and saved to your management computer in step 5-c-ii, i.e., *test*.

f. Click *OK*.

The screenshot shows a 'Create New Automation Trigger' window. The main title is 'FortiPAM Event Log' with a subtitle 'A specified FortiPAM event log ID has occurred.' and a 'CHANGE TYPE' link. The 'Name' field contains 'secret-launch' and the 'Description' field contains 'A specified FortiPAM event log ID has occurred.' with a '0/255' character count. Under the 'FortiPAM Event Log' section, the 'Event' field is set to 'Secret launch' and the 'Field filter(s)' are 'secret' and 'test'. On the right side, there is an 'Additional Information' panel with links for 'API Preview', 'Documentation', 'Online Help', 'Guides', and 'FortiAnalyzer Event Handler'. At the bottom, there are 'OK' and 'Cancel' buttons.

Create an action

To create an action:

1. Go to *Log & Report > Automation* and select the *Action* tab.
2. In the *Action* tab, select *Create*.
A *Create New Automation Action* window opens.
3. From *Notifications*, select *Email*.
An updated *Create New Automation Action* window opens.
4. In *Name*, enter a name for the action.
5. In the *Email* pane:
 - a. In *To*, enter the name of the recipient email address.
 - b. In *Subject*, enter a subject name.

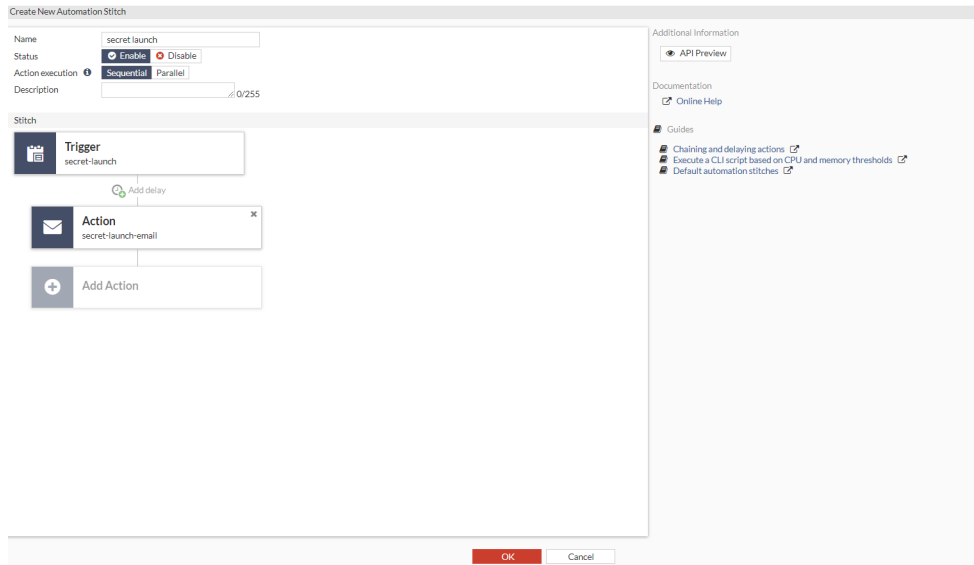
c. Click *OK*.

The screenshot shows the 'Create New Automation Action' dialog box for an Email action. The dialog has a title bar 'Create New Automation Action' and a close button. The main content area is titled 'Email' and includes the instruction 'Send a custom email to the specified recipients.' and a 'CHANGE TYPE' link. The form fields are: Name (secret-launch-email), Minimum Interval (0 seconds), Description (empty), Email To (empty), Subject (Secret Launch), and Body (%log%). There is a 'Replacement message' checkbox. At the bottom are 'OK' and 'Cancel' buttons. On the right side, there is an 'Additional Information' panel with 'API Preview' and 'Documentation' sections, and a 'Guides' section listing various integration options like FortiNAC, VMware NSX, Stack Notification, AWS Lambda, Azure Function, Google Cloud Function, AllCloud Function, CLI Script, and Webhook.

Creating a stitch

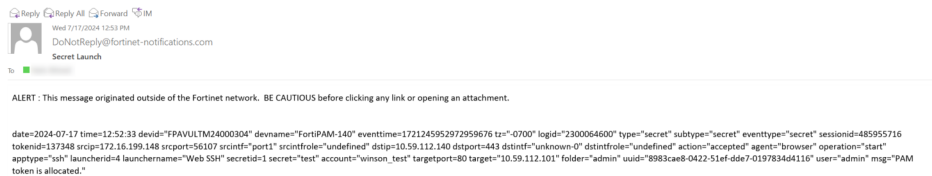
To create a stitch:

1. Go to *Log & Report > Automation*.
2. In the *Stitch* tab, select *Create*.
The *Create New Automation Stitch* window opens.
3. In *Name*, enter the name for the automation stitch.
4. In the *Stitch* pane:
 - a. Select *Trigger*, from *Select Entries*, select the trigger created in [Creating an automation trigger on page 175](#).
 - b. Click *Apply*.
 - c. Select *Add Action*, from *Select Entries*, select the action created in [Create an action on page 177](#).
 - d. Click *Apply*.

5. Click **OK**.

Results

1. Go to *Secrets > Secrets*.
2. In *Secrets*, double-click to open the secret used in step 5-e in [Creating an automation trigger on page 175](#).
3. From the top, select a launcher to launch the secret.
You will receive an alert email on the email address set in step 5-a in [Create an action on page 177](#).



The alert email contains information on the secret being launched.

Windows application filter

The section describes examples related to Windows application filter.

For information on the Windows application filter feature, see *Window app filter* in the latest *FortiPAM Administration Guide*.

Creating a Windows application filter to prevent running executables

In this example, we create a Windows application filter profile that prevents users from running Powershell, MS Paint, and other executables except in the %PROGRAMFILES%*, %WINDIR%* directories.

We then apply this Windows application filter to a non-privileged secret.

To create the Windows application filter:

1. [Setting up WinRM on the remote server on page 180](#)
2. [Creating a target with server information as Windows on page 180](#)
3. [Creating a Windows application filter profile on page 181](#)
4. [Creating a privileged account secret on page 183](#)
5. [Creating a non-privileged account on page 184](#)
6. [Launching the secret on page 186](#)

Setting up WinRM on the remote server

To set up WinRM on the remote server, see *Appendix L: WinRM configuration for Windows server* in the latest *FortiPAM Administration Guide*.

Creating a target with server information as Windows

To create the target:

1. Go to *Secrets > Targets* and select *+Create*.
2. In *Name*, enter a name for the target.
3. In *Classification Tag*, select *Other*.
4. In *Default Template*, select a secret template with server information set to Windows, e.g., *Windows Domain Account*.

5. In *Domain-Controller*, enter the IP address of the server.
6. In *Domain*, enter the domain of the server.
7. In *Advanced Setting*, enable *WinRM HTTPS* for advanced security.
8. Click *Submit*.

The above target can be created in the CLI using the following commands [CLI](#):

```
config secret target
edit "Demo - Windows Server"
set class "Other"
set template "Windows Domain Account"
set address "10.59.112.231"
set domain "demofpam.ca"
set user-naming-attribute "sAMAccountName"
set user-base ''
set description ''
set ldaps-min-ssl-version default
set ldaps-port 636
set winrm-https enable
set access everyone
set web-proxy-status disable
next
end
```

Creating a Windows application filter profile

We create a Windows application filter profile that prevents the user from running Powershell, MS Paint, and other executables except in the directories %PROGRAMFILES%*, %WINDIR*.

To create the Windows application filter:

1. Go to *Secret Settings > Windows App Filter Profiles* and select *+Create*.
2. Enter the name for the Windows application filter.
3. In *Executable*:
 - a. Select *+*.
 - b. In *Deny*, enter *C:\Windows\System32\WindowsPowerShell.exe*.

- c. Select **+**.
- d. In *Deny*, enter `%WINDIR%\system32\mspaint.exe`.

4. Go to the *Script* tab:

- a. Select **+**.
- b. In *Deny*, enter `C:\Users%\USER%\Desktop*` to block any script located on the desktop.

5. Go to the *Installer* tab:

- a. In *Deny (Recommend)*, all installers are blocked except those in the directories `%PROGRAMFILES%*`, `%WINDIR%*`.

6. Go to the *Advanced Setting* tab.

- a. In *Refresh Period*, keep the default value, 30 minutes.

7. Click *Submit*.

The above target can be created in the CLI using the following commands [CLI](#):

```
config secret winappfilter-profile
edit "Block Paint"
config rules
edit 1
set deny "*"
set exception
"%PROGRAMFILES%\* %WINDIR%\*"
next
edit 3
set type script
set deny "C:\\Users\\%USER%\\Desktop\\*"
next
edit 4
set type msi
set "*"
set exception
"%PROGRAMFILES%\* %WINDIR%\*"
next
edit 5
set deny "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe"
next
edit 6
set deny
"%WINDIR%\\system32\\mspaint.exe"
next
end
next
end
```

Creating a privileged account secret

To create a secret:

1. Go to *Secrets > Secrets*.
2. In the Secrets List, select *Create*.
The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.
4. Select *Create*.
The *New Secret* window opens.
5. Enter a name for the secret.
6. From the *Target* dropdown, select the target that you created in [Creating a target with server information as Windows on page 180](#).
7. Enable *Privileged Account* and ensure that this account has administrator privileges on the remote server. This is needed to modify policy settings.
8. In *Fields*:
 - a. Enter the user name.
 - b. Enter the password.
 - c. Reenter the password to confirm.

9. Click *Submit*.

The above secret can be created in the CLI using the following commands [CLI](#)

```
config secret database
edit 4
  set name "Demo - Priv Account"
  set target "Demo - Windows Server"
  set target-privilege-account enable
  set folder 1
  set template "Windows Domain Account"
  set proxy enable
  set rdp-service-status up
  set ldaps-service-status up
  set samba-service-status up
  config credentials-history
end
edit 1
  set name "Username"
  set value "demo-priv-acc"
next
edit 2
  set name "Password"
  set value "ENC jdiQCYRCdK9Hcxb1oyHpwaWGgltZZji2N3ZFQA=="
next
end
next
end
```

Creating a non-privileged account

To create the secret:

1. Go to *Secrets > Secrets*.
2. In the Secrets List, select *Create*.
The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.

4. Select *Create*.
The *New Secret* window opens.
5. Enter a name for the secret.
6. From the *Target* dropdown, select the target that you created in [Creating a target with server information as Windows on page 180](#).
7. In *Fields*:
 - a. Enter the user name.
 - b. Enter the password.
 - c. Reenter the password to confirm.
8. Go to the *Secret Setting* tab.
9. Enable *Session Recording*.
10. Ensure that *Proxy Mode* is enabled.
11. Enable *Windows Application Filter* and from the dropdown select the Windows application filter created in [Creating a Windows application filter profile on page 181](#).
12. Click *Submit*.

The screenshot shows the 'New Secret' window with the following configuration:

- Name:** Demo - Non - Priv - Acc
- Folder:** admin
- Target:** Demo - Windows Server
- Privileged Account:** Demo - Windows Server
- Template:** Windows Domain Account
- Server Information:** Inherit Server Information from Template
- Associated Secret:** No associated secret
- Description:** [Empty]
- Fields:**
 - Host: 10.59.112.231
 - Domain: demofam.ca
 - Username: demo-non-priv-acc
 - Password: [Masked]
 - Confirm Password: [Masked]

The screenshot shows the 'New Secret' window with the following configuration in the 'Secret Setting' tab:

- Automatic Password Changing:** Disable
- Automatic Password Verification:** Disable
- Session Recording:** Enable
- Proxy Mode:** Enable
- Tunnel Encryption:** Disable
- Antivirus Scan:** Disable
- DLP Status:** Disable
- Requires Checkout:** Disable
- Requires Approval to Launch Secret:** Disable
- Requires Approval to Launch Job:** Disable
- Block Clipboard:** Disable
- Windows Application Filter:** Enable
 - Profile: Block Paint
- TOTP Setting:**
 - TOTP Status:** Disable

The above secret can be created in the CLI using the following commands

```

config secret database
edit 5
  set name "Demo - Non - Priv - Account"
  set target "Demo - Windows Server"
  set target-privilege-account enable
  set folder 1
  set template "Windows Domain Account"
  set recording enable
  set proxy enable
  set winappfilter enable
  set winappfilter-profile "Block Paint"
  set rdp-service-status up
  set ldaps-service-status up
  set samba-service-status up
  config credentials-history
end
config field
edit 1
  set name "Username"
  set value "demo-non-priv-acc"
next
edit 2
  set name "Password"
  set value "ENC jdiQCYRCdK9Hcxb1oyHpwaWGglTZZjI2N3ZFQA=="
next
end
next
end

```

Launching the secret

Launching the secret:

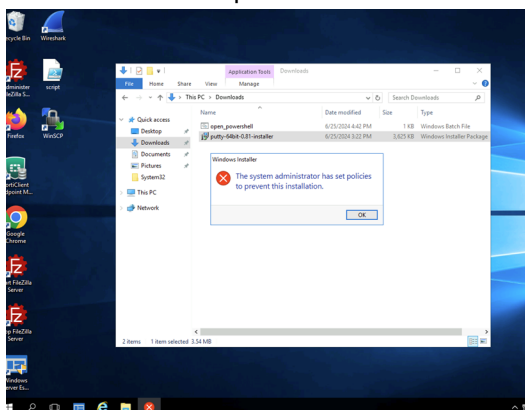
1. Go to *Secrets > Secrets*.
2. From the list, double-click to open the secret created in [Creating a non-privileged account on page 184](#).

The screenshot shows the 'Secret Details' page for a secret named 'Demo - Non - Priv - Acc'. The page is divided into several sections:

- General:** Name: Demo - Non - Priv - Acc; Folder: admin; Target: Demo - Windows Server; Privileged Account: Another secret has already been set as a privileged account for this target; Template: Windows Domain Account; Server Information: Inherit Server Information from Template; Associated Secret: No associated secret; Description: (empty).
- Fields:** Host: 10.59.112.231; Domain: demofpam.ca; Username: demo-non-priv-acc; Password: (masked with dots).
- Right Panel:** Password Changer Status: Password has not been changed before; Password Verification Status: Password has not been verified before; Last Launch Time: Secret has not been launched before; Documentation: Online Help; Guide: Windows Server WinRM Guide, WinRM Setup Script.

At the bottom of the page, there are buttons for 'Save', 'Back', and 'Discard'.

- d. Run the installer not permitted in the directories.



Creating a non-Windows application filter to prevent running executables

You may encounter scenarios where the template server information is not for Windows, e.g., the *Machine* template.

Nonetheless, you may continue to set *Machine* as the remote server template to access the Windows server.

For this case, you can still use the Windows application filter.

The overall procedures are similar to those in [Creating a Windows application filter to prevent running executables on page 180](#) except the ones below.

To create the Windows application filter:

1. Creating a target with server information as non-Windows on page 188
2. Creating a non-privileged secret on page 189

Creating a target with server information as non-Windows

To create the target:

1. Go to *Secrets > Targets* and select *+Create*.
2. In *Name*, enter a name for the target.
3. In *Classification Tag*, select *Other*.
4. In *Default Template*, select a secret template that does not have Windows as the server information, e.g., *Machine*.
Note: For the *Machine* template, *WinRM HTTPS* option can be set in the CLI.
5. In *Host*, enter the IP address of the server.

6. Click *Submit*.

The screenshot shows the 'New Secret Target' configuration window. The 'General' tab is selected, and the following fields are visible:

- Name: Demo - Windows Server
- Classification Tag: Other
- Default Template: Machine
- Host: 10.59.112.231
- Gateway: None
- Description: (empty text area)

At the bottom of the window, there are two buttons: 'Submit' (highlighted in red) and 'Cancel'.

The above target can be created in the CLI using the following commands [CLI](#):

```
config secret target
edit "Demo - Windows Server"
set class "Other"
set template "Machine"
set address "10.59.112.231"
set winrm-https disable
set sql-server-log-status disable
next
end
```

Creating a non-privileged secret

To create the secret:

1. Go to *Secrets > Secrets*.
2. In the *Secrets List*, select *Create*.
The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.
4. Select *Create*.
The *New Secret* window opens.
5. Enter a name for the secret.
6. From the *Target* dropdown, select the target that you created in [Creating a target with server information as non-Windows on page 188](#).
7. Enable *Server Information* and from the dropdown select *Windows*.
8. In *Fields*:
 - a. Enter the user name.
 - b. Enter the password.
 - c. Reenter the password to confirm.
9. Go to the *Secret Setting* tab.
10. Enable *Session Recording*.

11. Ensure that *Proxy Mode* is enabled.
12. Enable *Windows Application Filter* and from the dropdown select the Windows application filter created in [Creating a Windows application filter profile on page 181](#).
13. Click *Submit*.

The above secret can be created in the CLI using the following commands [\(CLI\)](#)

```
config secret database
edit 5
set name "Demo - Non - Priv - Account"
set target "Demo - Windows Server"
set folder 1
set template "Machine"
set server-info Windows
set recording enable
set proxy enable
set winappfilter enable
```

```
set winappfilter-profile "Block Paint"
set ssh-service-status up
set telnet-service-status up
set rdp-service-status up
set vnc-service-status up
set samba-service-status up
config credentials-history
end
config field
edit 1
  set name "Username"
  set value "demo-non-priv-acc"
next
edit 2
  set name "Password"
  set value "ENC jdiQCYRCdK9Hcxb1oyHpwaWGglTZZjI2N3ZFQA=="
next
end
next
end
```

You can now launch the secret to check the Windows application filter profile functionalities.

Web launcher

The section describes examples related to Web launcher.

Using web launcher to auto fill credentials on a website

In the previous FortiPAM versions, the web launching feature had the following three limitations:

- When launching to some special website, the extension cannot find the user name or the password field correctly using its predefined key.
- After logging in to a website, the extension tries to fill in user name or password into an unrelated field.
- The extension can only fill in user name, password, but 2FA Token is not supported.

In this example, we demonstrate the improved web launcher auto fill feature that fixes the above mentioned issues. We set up a secret for FortiAuthenticator that uses a clone of the *Web Account* secret template. Once you log in to FortiAuthenticator using FortiPAM and create a user, the FortiPAM extension does not attempt to fill in user name or password into unrelated fields.

To use web launcher to auto fill credentials on a website:

1. [Creating a secret template on page 192](#)
2. [Creating a secret to connect to FortiAuthenticator on page 196](#)
3. [Launching the secret on page 196](#)

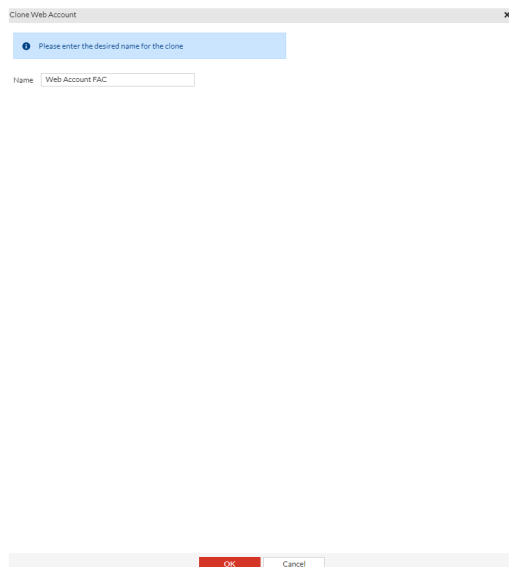
Creating a secret template

We create a new customizable secret template *Web Account FAC* by cloning the default *Web Account* secret template.

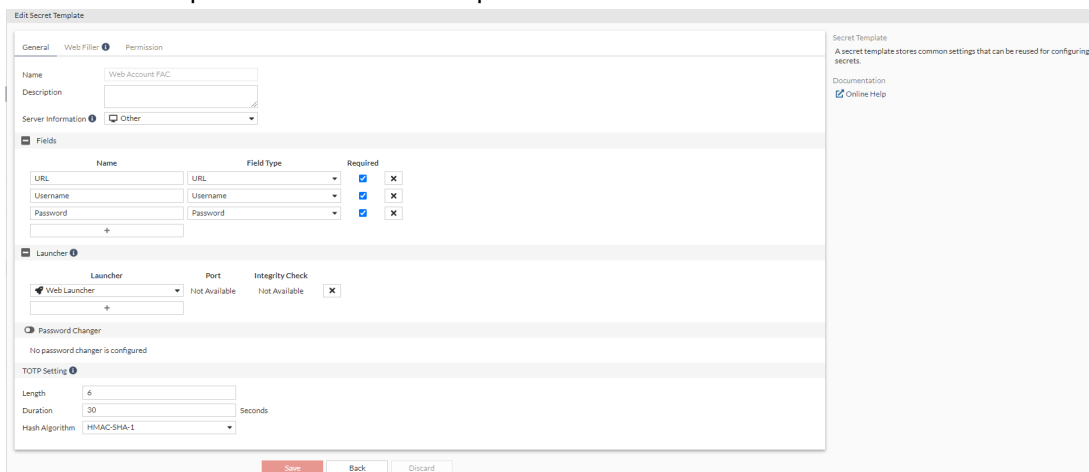
To create the secret template:

1. Go to *Secret Settings > Templates*.
2. From the list, select *Web Account* and click *Clone*.
3. Rename the template as *Web Account FAC*.

4. Click *OK*.



5. Double-click to open the cloned secret template.



6. Go to the *Web Filler* tab:

a. In *Authentication path*, enter `/login/`.

For example:

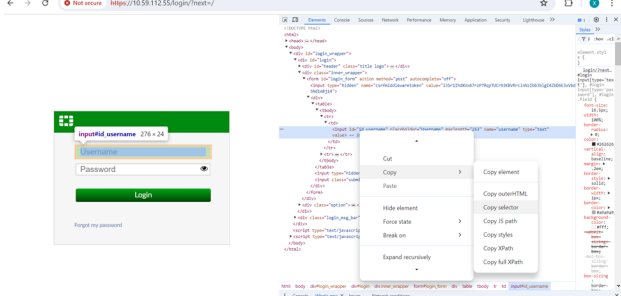
- If the FortiAuthenticator login page is `https://x.x.x.x/login/`, the authentication path is `/login/`.
- If the ESXi login page is `https://x.x.x.x/ui/`, the authentication path is `/ui/`.
- If the vCenter login page is `https://vcenter.fortipam.ca/websso/SAML2/SSO/fortipam.ca?SAMLRequest=xxxxxxx`, the authentication path is `/websso/SAML2/SSO/fortipam.ca`.

Note: FortiPAM GUI helps you trim the authentication path when you input the login path.

- b. In the *Field* pane, select **+**.

To locate the input fields:

1. Open the FortiAuthenticator login page.
2. Right-click the *Username/ Password* field and select *Inspect*.
The HTML code for the *Username* field is highlighted in the Chrome developer tool.
3. Right-click the highlighted area and select *Copy > Copy selector*.



The copied selector can be used as the *Web Element Selector*.

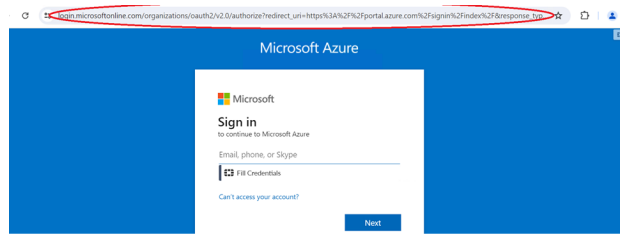
- c. For the *Username* field, enter `#id_username` as the *Web Element Selector*.
- d. Select **+**.
- e. For the *Password* field, enter `#id_password` as the *Web Element Selector*.
- f. As both the user name and password are on the login page, the override path can be kept empty. The FortiPAM extension searches the user name and password selectors on the login page.



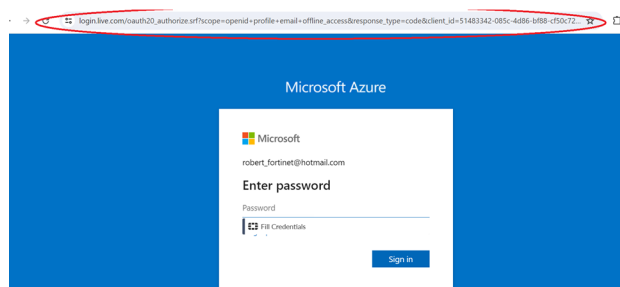
For some websites, the input fields for user name and password are on different pages, for such cases, you can define the override path to inform the FortiPAM extension where to search for the corresponding selectors.

For example, on the Azure portal login pages:

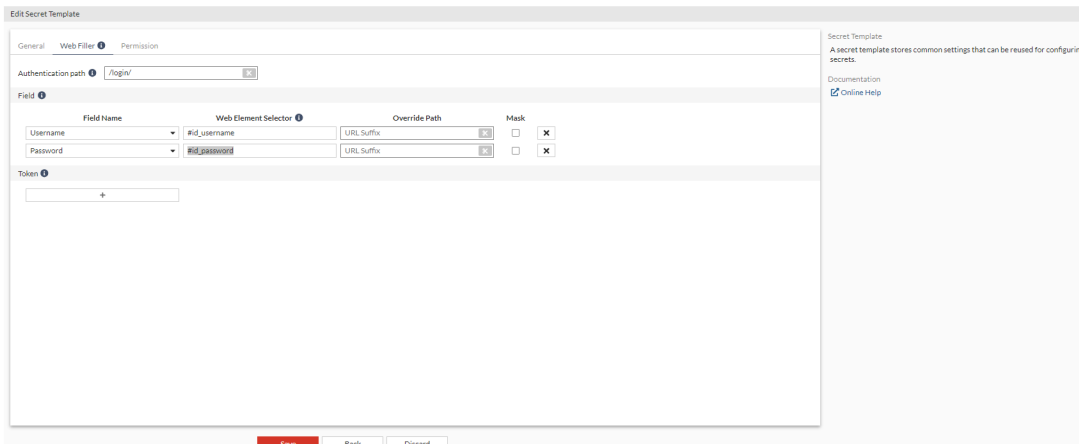
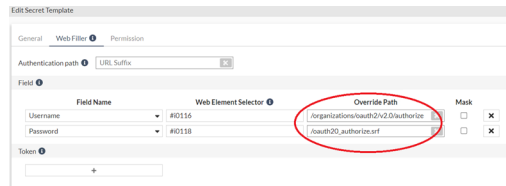
Username



Password



In the secret template *Web Filler* tab, the *Override Path* is set as below:



7. Click **Save**.

Creating a secret to connect to FortiAuthenticator

We create a secret based on the secret template in [Creating a secret template on page 192](#) to connect to FortiAuthenticator.

To create the secret:

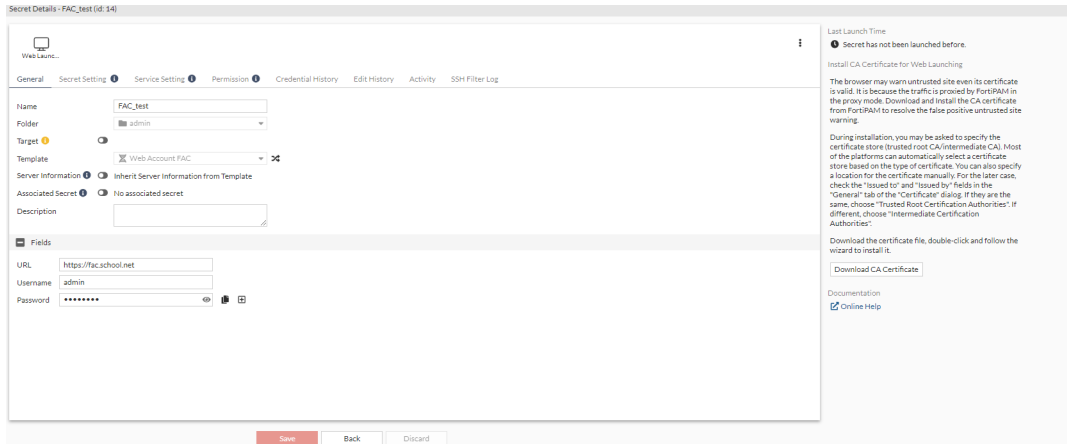
1. Go to *Secrets > Secrets*.
2. In the Secrets List, select *Create*.
The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.
4. Select *Create*.
The *New Secret* window opens.
5. Enter a name for the secret.
6. Disable *Target*.
7. From the *Template* dropdown, select *Web Account FAC*.
This is the secret template created in [Creating a secret template on page 192](#).
8. In the *Fields* pane:
 - a. In *URL*, enter the URL of FortiAuthenticator.
 - b. Enter user name.
 - c. Enter password.
 - d. Reenter the password to confirm.
9. Click *Submit*.

Launching the secret

We launch the secret created in [Creating a secret to connect to FortiAuthenticator on page 196](#).

To launch the secret:

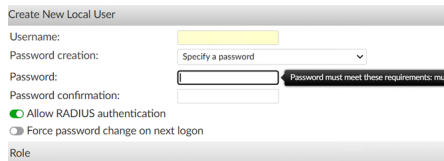
1. Go to *Secrets > Secrets*.
2. From the list double-click to open the secret created in [Creating a secret to connect to FortiAuthenticator on page 196](#).



3. From the top, select *Web Launcher* to launch the secret.
A new browser tab opens.
4. In the FortiAuthenticator login page, click *Username/Password* fields, click *Use FortiPAM session credentials* to fill in the credentials, and click *Login*.
You are now logged in to FortiAuthenticator.



On FortiAuthenticator, when you create a user and try to enter user name/password, the FortiPAM extension does not auto fill in the user name/password.



Log and video disks

The section describes examples related to FortiPAM log and video disks.

Back up and restore your log and video files

When you plan to replace your current log and video disk with a larger disk, *FTP support for video/log backup* feature helps you back up and restore your log and video files into/from the new disk.

You will first need to set up an FTP server reachable from FortiPAM.



Ensure that the FTP user has *Read/Write* permission to the folder.

To back up and restore your log and video files:

1. [Enabling maintenance mode on FortiPAM on page 198](#)
2. [Backing up videos to the FTP server on page 199](#)
3. [Backing up logs to the FTP server on page 199](#)
4. [Shutting down the FortiPAM-VM and change log and video disks on page 200](#)
5. [Restoring videos from the FTP server on page 200](#)
6. [Restoring logs from the FTP server on page 201](#)

Enabling maintenance mode on FortiPAM

To enable maintenance mode on FortiPAM:

1. From the user dropdown, in *System*, select *Activate Maintenance Mode*.
2. In the *Warning* dialog:
 - a. Enter the maximum duration, in minutes.
 - b. Enter a reason for activating the maintenance mode.
 - c. Click *OK*.

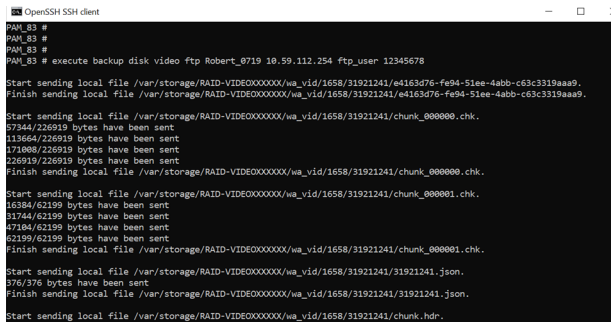
Backing up videos to the FTP server

To back up videos to the FTP server:

1. In the FortiPAM CLI console, enter the following command to backup the video:

```
execute backup disk video ftp <remote folder path> <ftp server>[:ftp port] <user> <passwd>
```

FortiPAM starts to backup the video.

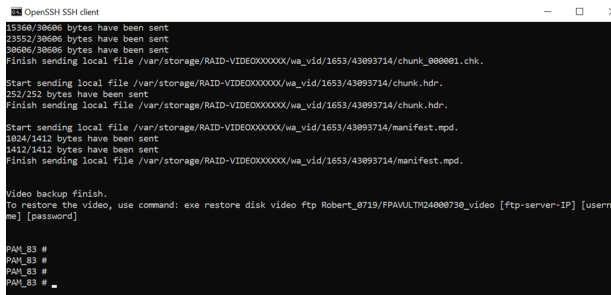


```
OpenSSH SSH client
PAM_83 #
PAM_83 #
PAM_83 # execute backup disk video ftp Robert_0719 10.59.112.254 ftp_user 12345678
Start sending local file /var/storage/RAID-VIDEOXXXXXX/wa_vid/1658/31921241/e4163d76-fe94-51ee-4abb-c63c3319aaa9.
Finish sending local file /var/storage/RAID-VIDEOXXXXXX/wa_vid/1658/31921241/e4163d76-fe94-51ee-4abb-c63c3319aaa9.
Start sending local file /var/storage/RAID-VIDEOXXXXXX/wa_vid/1658/31921241/chunk_000000.chk.
57344/226919 bytes have been sent
113664/226919 bytes have been sent
173808/226919 bytes have been sent
226919/226919 bytes have been sent
Finish sending local file /var/storage/RAID-VIDEOXXXXXX/wa_vid/1658/31921241/chunk_000000.chk.
Start sending local file /var/storage/RAID-VIDEOXXXXXX/wa_vid/1658/31921241/chunk_000001.chk.
16384/62199 bytes have been sent
31744/62199 bytes have been sent
47184/62199 bytes have been sent
62199/62199 bytes have been sent
Finish sending local file /var/storage/RAID-VIDEOXXXXXX/wa_vid/1658/31921241/chunk_000001.chk.
Start sending local file /var/storage/RAID-VIDEOXXXXXX/wa_vid/1658/31921241/31921241.json.
376/376 bytes have been sent
Finish sending local file /var/storage/RAID-VIDEOXXXXXX/wa_vid/1658/31921241/31921241.json.
Start sending local file /var/storage/RAID-VIDEOXXXXXX/wa_vid/1658/31921241/chunk_hdr.
```

After the video backup is completed, *Video backup finish* is displayed on the console.

FortiPAM creates a folder named *FortiPAM-license-number_video* in the path provided in the backup command and places all the video files in it.

FortiPAM displays how to restore the backed up video files.



```
OpenSSH SSH client
13569/30606 bytes have been sent
13552/30606 bytes have been sent
30606/30606 bytes have been sent
Finish sending local file /var/storage/RAID-VIDEOXXXXXX/wa_vid/1653/43093714/chunk_000001.chk.
Start sending local file /var/storage/RAID-VIDEOXXXXXX/wa_vid/1653/43093714/chunk_hdr.
252/252 bytes have been sent
Finish sending local file /var/storage/RAID-VIDEOXXXXXX/wa_vid/1653/43093714/chunk_hdr.
Start sending local file /var/storage/RAID-VIDEOXXXXXX/wa_vid/1653/43093714/manifest.mpd.
1024/1412 bytes have been sent
1412/1412 bytes have been sent
Finish sending local file /var/storage/RAID-VIDEOXXXXXX/wa_vid/1653/43093714/manifest.mpd.
Video backup finish.
To restore the video, use command: exe restore disk video ftp Robert_0719/PPAVULTM24000730_video [ftp-server-IP] [userna
me] [password]
PAM_83 #
PAM_83 #
PAM_83 #
PAM_83 #
```

Backing up logs to the FTP server

To backup logs to the FTP server:

1. In the FortiPAM CLI console, enter the following command to backup logs to the FTP server:

```
execute backup disk alllogs ftp <remote folder path> <ftp server>[:ftp port] <user> <passwd>
```

FortiPAM starts to backup logs.

```

OpenSSH SSH client
PAM_83 #
PAM_83 #
PAM_83 #
PAM_83 #
PAM_83 #
PAM_83 #
PAM_83 # execute backup disk alllogs ftp Robert_0719 10.59.112.254 ftp_user 12345678
You will kill the process for log and report.
Whether new log nor report will be generated during the log backup.
No videos should be recorded during the process.
Do you want to continue? (y or n)y
log backup start:
killed log process
killed report process
Start sending local file /var/log/log/root/offset/elog.65532.ofs.12
Finish sending local file /var/log/log/root/offset/elog.65532.ofs.12
Start sending local file /var/log/log/root/offset/secretlog.65538.ofs.8
    
```

After the logs backup is completed, *All logs backup finish* is displayed on the console.

FortiPAM creates a folder named *FortiPAM-license-number_all_logs* in the path provided in the backup command and places all the log files in it.

FortiPAM displays how to restore the backed up log files.

```

OpenSSH SSH client
_30240714_115404_65532 Ok.
connect to ftp server 10.59.112.254 ...
Please wait...
sent log file secretlog.65533 to ftp server as Robert_0719/PPAVULTM24000730_all_logs/disk-secretlog_FPAVULTM24000730_roo
_30240713_115404_65533 Ok.
connect to ftp server 10.59.112.254 ...
Please wait...
sent log file secretlog.65534 to ftp server as Robert_0719/PPAVULTM24000730_all_logs/disk-secretlog_FPAVULTM24000730_roo
_30240712_155404_65534 Ok.
connect to ftp server 10.59.112.254 ...
Please wait...
sent log file secretlog.65535 to ftp server as Robert_0719/PPAVULTM24000730_all_logs/disk-secretlog_FPAVULTM24000730_roo
_30240711_120404_65535 Ok.
connect to ftp server 10.59.112.254 ...
Please wait...
sent log file secretlog.0 to ftp server as Robert_0719/PPAVULTM24000730_all_logs/disk-secretlog_FPAVULTM24000730_roo_20
40710_180957_0 Ok.
all logs backup finish.
to restore the logs, use command:
exe restore disk alllogs ftp Robert_0719/PPAVULTM24000730_all_logs [ftp-server-IP] [username] [password]
    
```

Shutting down the FortiPAM-VM and change log and video disks

To shutdown FortiPAM VM and change log and video disks:

1. From the user dropdown, in *System*, select *Shutdown* to shutdown the FortiPAM-VM.
2. In this example, FortiPAM was deployed on a VMware ESXi server.
In the VMware vSphere Client, right-click the name of the FortiPAM virtual machine, and select *Edit Settings*.
3. Ensure that you are in the *Virtual Hardware* tab.
4. Remove the log and video disks.



Do not remove the FortiPAM system disk. The system disk is always the first disk on your VM client.

5. Add the new log and video disks.
6. Reboot the FortiPAM-VM.

Restoring videos from the FTP server

To restore videos from the FTP server:

1. In the FortiPAM CLI console, enter the following command to restore from the FTP server with your FTP server IP address, user name, and password:

```
execute restore disk video ftp <string> <ftp server>[:ftp port] <user> <passwd>
```

```

OpenSSH SSH client
PAM_83 #
PAM_83 #
PAM_83 #
PAM_83 #
PAM_83 # exe restore disk video ftp Robert_0719/FPAVULTM24000730_all_logs 10.59.112.254 ftp_user 12345678
FTP folder Robert_0719/FPAVULTM24000730_all_logs has name different from the backed up folder's default name, are you
sure to use it for restore(y or n)y
Video restoration start.
Start receiving /Robert_0719/FPAVULTM24000730_all_logs/disk-a-log_FPAVULTM24000730_root_20240719_000000_65529
Received empty file /Robert_0719/FPAVULTM24000730_all_logs/disk-a-log_FPAVULTM24000730_root_20240719_000000_65529
Start receiving /Robert_0719/FPAVULTM24000730_all_logs/disk-d-log_FPAVULTM24000730_root_20240719_000000_65529
Received empty file /Robert_0719/FPAVULTM24000730_all_logs/disk-d-log_FPAVULTM24000730_root_20240719_000000_65529
Start receiving /Robert_0719/FPAVULTM24000730_all_logs/disk-e-log_FPAVULTM24000730_root_20240711_000000_0
7240 of 18435 bytes have been received.
11336 of 18435 bytes have been received.
14480 of 18435 bytes have been received.
18435 of 18435 bytes have been received.
Finished receiving /Robert_0719/FPAVULTM24000730_all_logs/disk-e-log_FPAVULTM24000730_root_20240711_000000_0
Start receiving /Robert_0719/FPAVULTM24000730_all_logs/disk-f-log_FPAVULTM24000730_root_20240712_000000_65535
22572 of 74313 bytes have been received.

```

After the logs are restored, *Video restoration finish* is displayed in the FortiPAM CLI console.

```

OpenSSH SSH client
109552 of 141142 bytes have been received.
141142 of 141142 bytes have been received.
Finished receiving /Robert_0719/FPAVULTM24000730_all_logs/report/generated/Schedule-default-2024-07-18-000100/default.pdf
Start receiving /Robert_0719/FPAVULTM24000730_all_logs/report/generated/Schedule-default-2024-07-19-000100/default.pdf
36200 of 141308 bytes have been received.
72400 of 141308 bytes have been received.
108604 of 141308 bytes have been received.
141308 of 141308 bytes have been received.
Finished receiving /Robert_0719/FPAVULTM24000730_all_logs/report/generated/Schedule-default-2024-07-19-000100/default.pdf
Start receiving /Robert_0719/FPAVULTM24000730_all_logs/report/generated/reportlist.txt
1107 of 1107 bytes have been received.
Finished receiving /Robert_0719/FPAVULTM24000730_all_logs/report/generated/reportlist.txt
Start receiving /Robert_0719/FPAVULTM24000730_all_logs/rpt-vir.db
12288 of 36864 bytes have been received.
24576 of 36864 bytes have been received.
36864 of 36864 bytes have been received.
Finished receiving /Robert_0719/FPAVULTM24000730_all_logs/rpt-vir.db
Video restoration finish.
PAM_83 #
PAM_83 #

```

Restoring logs from the FTP server

To restore logs from the FTP server:

1. In the FortiPAM CLI console, enter the following command to restore logs from the FTP server with your FTP server IP address, user name, and password:

```
execute restore disk alllogs ftp <remote folder path> <ftp server>[:ftp port] <user> <passwd>
```

```

OpenSSH SSH client
PAM_83 #
PAM_83 #
PAM_83 # exe restore disk alllogs ftp Robert_0719/FPAVULTM24000730_all_logs 10.59.112.254 ftp_user 12345678
You will kill the process for log and report.
Neither new log nor report will be generated during the log restoration.
No videos should be recorded during the process.
Do you want to continue? (y or n)y
Log restoration start.
killed log process
killed report process
Start receiving /Robert_0719/FPAVULTM24000730_all_logs/disk-a-log_FPAVULTM24000730_root_20240719_000000_65529 to local fi
le /var/log/log/root/alog.65529
Received empty file /Robert_0719/FPAVULTM24000730_all_logs/disk-e-log_FPAVULTM24000730_root_20240719_000000_65529
to local file /var/log/log/root/elog.65529
Start receiving /Robert_0719/FPAVULTM24000730_all_logs/disk-d-log_FPAVULTM24000730_root_20240719_000000_65529 to local fi
le /var/log/log/root/dlog.65529
Received empty file /Robert_0719/FPAVULTM24000730_all_logs/disk-f-log_FPAVULTM24000730_root_20240719_000000_65529
to local file /var/log/log/root/flog.65529
Start receiving /Robert_0719/FPAVULTM24000730_all_logs/disk-g-log_FPAVULTM24000730_root_20240711_000000_0 to local file /
var/log/log/root/glog.0
7240 of 18435 bytes have been received.
11336 of 18435 bytes have been received.
14480 of 18435 bytes have been received.
18435 of 18435 bytes have been received.
Finish receiving /Robert_0719/FPAVULTM24000730_all_logs/disk-g-log_FPAVULTM24000730_root_20240711_000000_0 to local file
/var/log/log/root/glog.0
Start receiving /Robert_0719/FPAVULTM24000730_all_logs/disk-h-log_FPAVULTM24000730_root_20240712_000000_65535 to local fi
le /var/log/log/root/hlog.65535
22572 of 74313 bytes have been received.

```

After the logs are restored, *Log restoration finish* is displayed in the FortiPAM CLI console.

```
OpenSSH SSH client
73184 of 141445 bytes have been received.
107850 of 141445 bytes have been received.
141445 of 141445 bytes have been received.
Start receiving /Robert_0719/PPAVULTM24000730_all_logs/report/generated/Schedule-default-2024-07-18-000100/default.pdf
36200 of 141142 bytes have been received.
70794 of 141142 bytes have been received.
106994 of 141142 bytes have been received.
141142 of 141142 bytes have been received.
Start receiving /Robert_0719/PPAVULTM24000730_all_logs/report/generated/Schedule-default-2024-07-19-000100/default.pdf
36200 of 141388 bytes have been received.
74552 of 141388 bytes have been received.
108104 of 141388 bytes have been received.
141388 of 141388 bytes have been received.
Start receiving /Robert_0719/PPAVULTM24000730_all_logs/report/generated/reportlist.txt
1187 of 1807 bytes have been received.
Start receiving /Robert_0719/PPAVULTM24000730_all_logs/rpt-vir.db to local file /var/log/log/root/rpt-vir.db
12288 of 36864 bytes have been received.
18576 of 36864 bytes have been received.
36864 of 36864 bytes have been received.
Finish receiving /Robert_0719/PPAVULTM24000730_all_logs/rpt-vir.db to local file /var/log/log/root/rpt-vir.db

Log restoration finish.

RM #
RM #
```

Certificate management

This section describes managing certificates with the FortiPAM device.

Configuring certificate using the ACME protocol to access a FortiPAM instance

FortiPAM implements the ACME protocol to help you apply and generate a certificate issued by [Let's Encrypt](#) automatically.

The default certificate validity is three months and it is automatically renewed within one month before the expiry.

Requirements

- FortiPAM 1.9 or above with a public IP address. Usually, an AWS or Azure FortiPAM instance.
- Enable Dynamic DNS (DDNS) service or purchase a domain for the FortiPAM public IP address.

Bind the FortiPAM instance to the domain.

Before using ACME to create a certificate, you should be able to reach the FortiPAM through the domain without any issue.

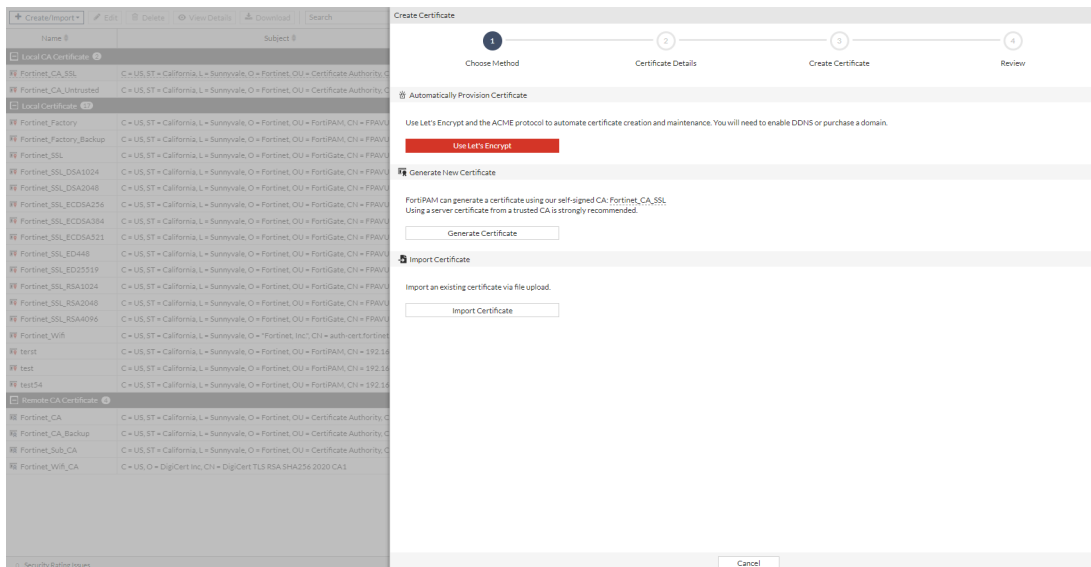
To configure certificate using the ACME protocol:

1. [Creating a certificate on page 203](#)
2. [Configuring the FortiPAM SSL certificate on page 207](#)

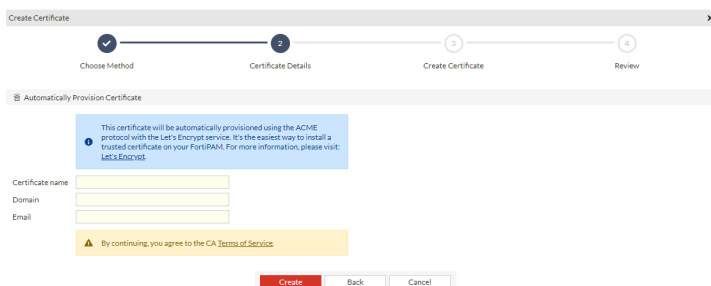
Creating a certificate

To create a certificate:

1. Go to *System > Certificates*.
2. From *+Create/Import*, select *Certificate*.
The *Create Certificate* window opens.

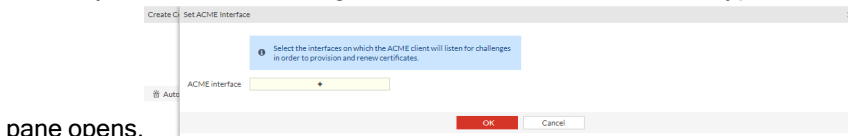


- From the *Automatically Provision Certificate* pane, select *Use Let's Encrypt* to automatically create a certificate using the ACME protocol with the Let's Encrypt service. The *Certificate Details* tab opens.



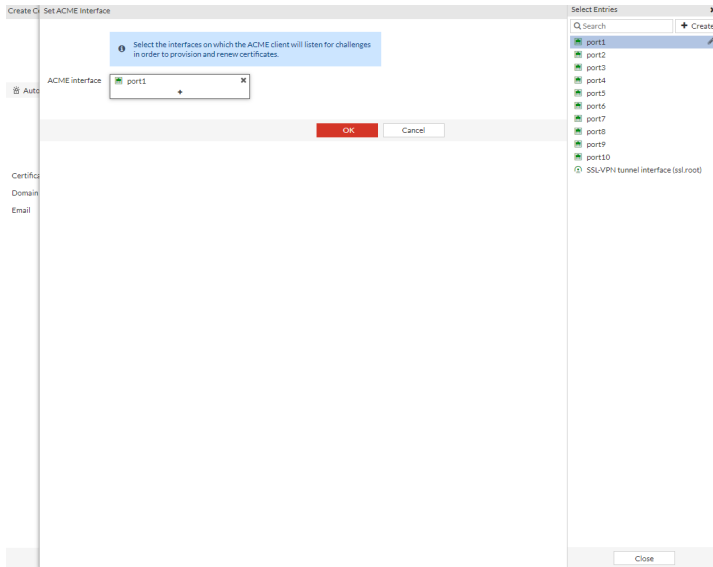
- In *Certificate name*, enter the name for the certificate.
- In *Domain*, enter the public FQDN of FortiPAM.
- In *Email*, enter the email address.
- Click *Create*.

If this is your first time enrolling a server certificate with Let's Encrypt on the FortiPAM unit, the *Set ACME Interface*

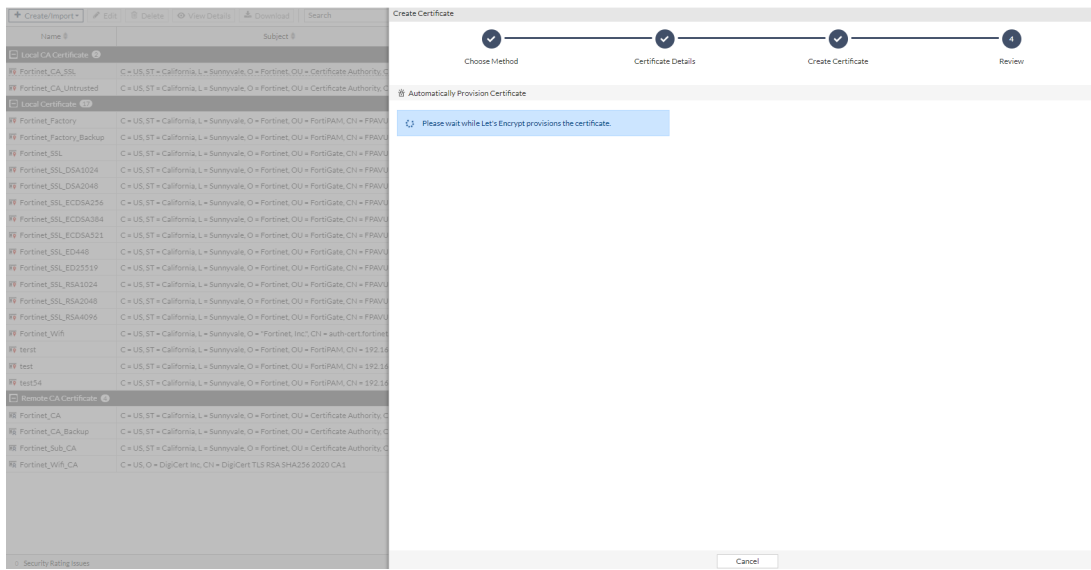


pane opens.

- Select *+* and from *Select Entries*, select a port, or create new interfaces on which the ACME client will listen for challenges to provision and renew certificates. It is suggested that you select one of the existing entries and use the port interface for FortiPAM access which is port1 in most cases.

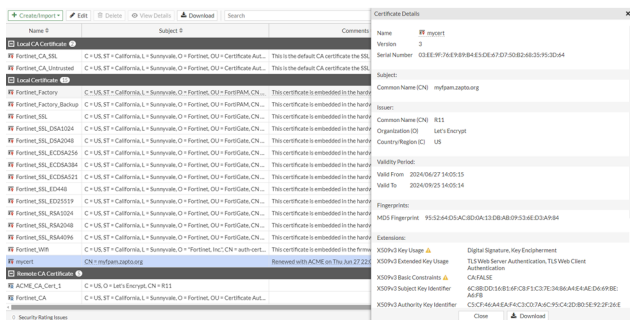
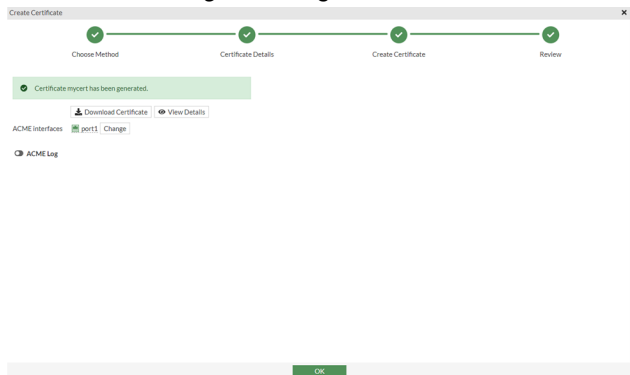


9. Click *Close*.
 10. Click *OK*.
- Wait for Let's Encrypt to provision the certificate.

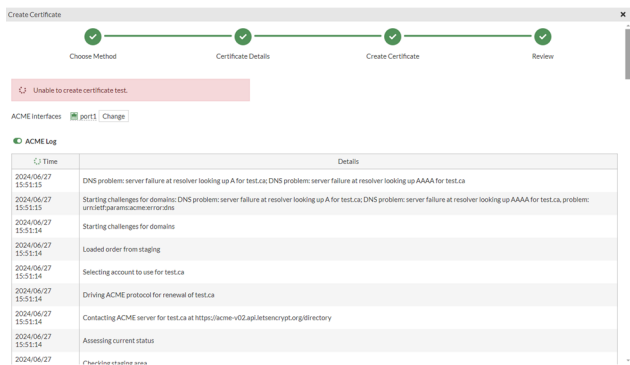



After successfully creating the certificate, the newly created certificate can be viewed or downloaded.


11. Enable ACME Log to see logs related to the certificate created using the ACME protocol.



If the certificate cannot be created, the ACME log is displayed for troubleshooting.



 Delete the certificate that could not be provisioned from the certificates list.

 Use the following CLI command to check the ACME status:

```
diagnose system acme status-full <domain> #displays the latest ACME trace log for <domain>
```

Configuring the FortiPAM SSL certificate

To configure the FortiPAM SSL certificate:

1. In the CLI console, enter the following commands:

```
config firewall vip
  edit "fortipam_vip"
    set uuid b9aebf22-2f4f-51ef-b35c-79e3f23c5adc
    set type access-proxy
    set extip 172.31.2.85
    set extintf "port1"
    set server-type https
    set extport 443
    set ssl-certificate "mycert" #set to the certificate created in Creating a certificate on page 203.
  next
end
```

You can now access FortiPAM using `https://fqdn` where FQDN is the FortiPAM FQDN used in [Creating a certificate on page 203](#).

How to deploy FortiPAM CA to Windows host using EMS and FortiClient

After FortiPAM installation, 2 certificates are available by default:

- `Fortinet_CA_SSL`:
A CA certificate used to resign https server certificate when launching a secret with *Web Proxy* enabled. Before launching a web proxy secret, the CA certificate must be installed on Windows.
- `Fortinet_SSL`:
FortiPAM GUI certificate used for FortiPAM HTTPS GUI and ZTNA tunnel with FortiClient. By default, the web browser displays Not secure warning when you log in to the FortiPAM GUI.

This example introduces how to deploy `Fortinet_CA_SSL` to Windows by EMS and FortiClient automatically and how to avoid the web browser warning.

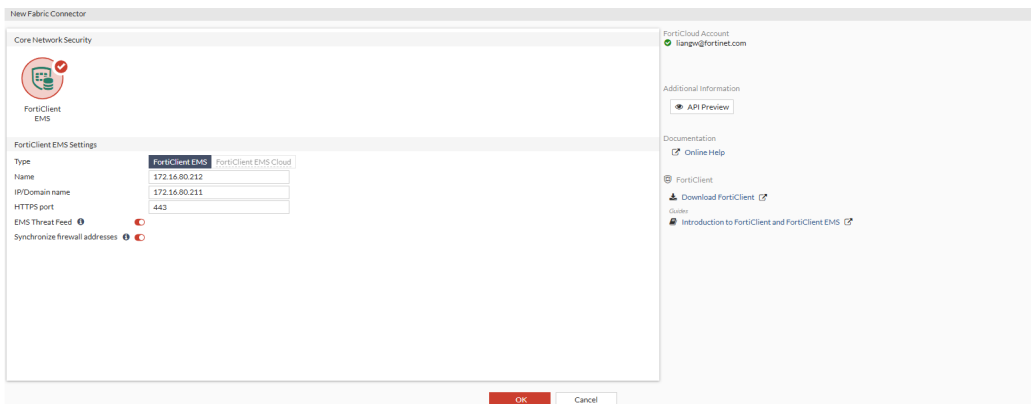
To deploy FortiPAM CA to Windows using EMS and FortiClient:

1. [Deploying FortiPAM CA using EMS on page 208](#)
2. [Avoiding the web browser warning on the FortiPAM GUI on page 209](#)
3. [Downloading FortiPAM CA from the FortiPAM GUI on page 211](#)

Deploying FortiPAM CA using EMS

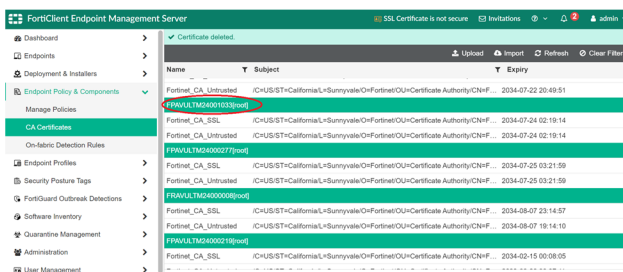
To deploy FortiPAM CA using EMS:

1. Connect FortiPAM to the EMS:
 - a. Log in to FortiPAM.
 - b. Go to *Network > Fabric Connectors*.
 - c. In the *Core Network Security* pane, select *FortiClient EMS* and then select *Edit*. The *New Fabric Connector* pane opens.
 - d. In *Name*, enter the name of the FortiClient EMS connector.
 - e. In *IP/Domain name*, the IP address of the FortiClient EMS.
 - f. In *HTTPS port*, enter the HTTPS port number for the FortiClient EMS.
 - g. Ensure that *EMS Threat Feed* and *Synchronize firewall addresses* are enabled.
 - h. Click *OK*.



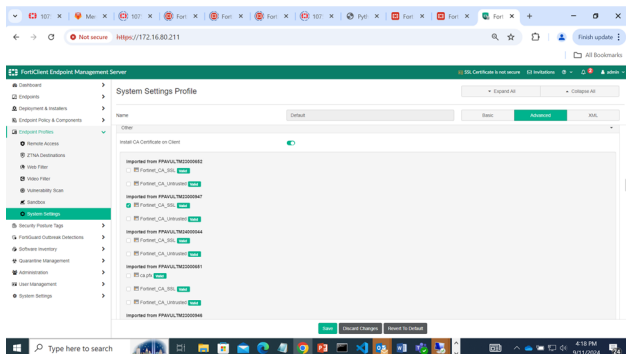
FortiPAM verifies the EMS server certificate.

2. On the EMS GUI, deploy the FortiPAM default CA to FortiClient.
 - a. Log in to the EMS GUI.
 - b. Go *Endpoint Policy & Components > CA Certificates*.
 - c. In the list, locate FortiPAM from step 1 using the serial number, e.g., FortiPAM serial number: FPAVULTM24001033.



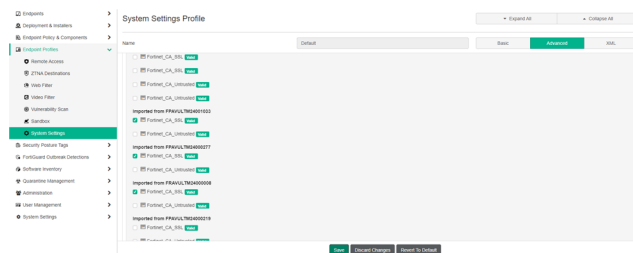
- d. Go to *Endpoint Profiles > System Setting*.
- e. Select the corresponding profile and edit it.

f. Go to the *Others* pane.

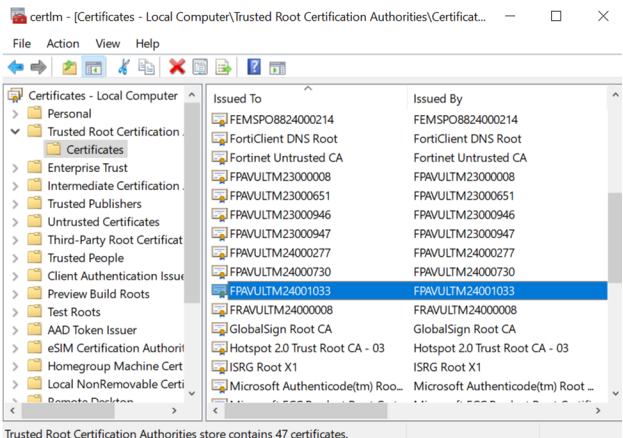


g. Look for your FortiPAM serial number and enable *Fortinet_CA_SSL*.

h. Click *Save*.



3. Wait for a few minutes. All the Windows host with FortiClient belonging to *Endpoint Profiles* in step 2 are pushed and installed above the default FortiPAM CA certificate. If needed, run *manage user certificate* on Windows to check whether the CA certificate has been installed.



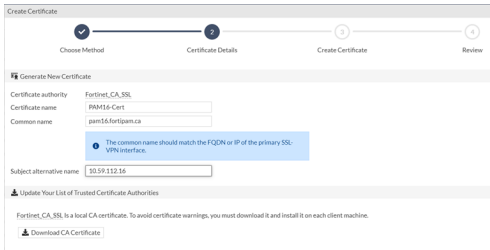
4. After the FortiPAM CA certificate has been installed, you can launch the *Web Account* secret with *Web Proxy* enabled.

Avoiding the web browser warning on the FortiPAM GUI

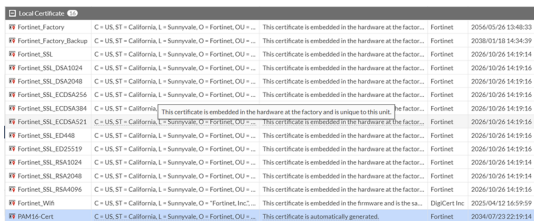
Besides avoiding the Not secure web browser warning when you log in to the FortiPAM GUI, the newly created GUI certificate is a requirement if the EMS uses *Enforce Valid Server Certificate* in *Endpoint Profile > ZTNA destinations > Advanced*.

To avoid the web browser warning on the FortiPAM GUI:

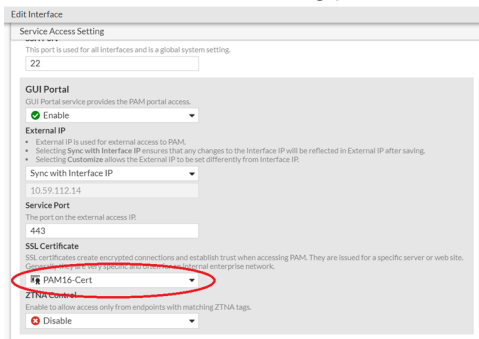
1. Create a FortiPAM GUI certificate signed by the FortiPAM CA certificate.
 - a. In the FortiPAM GUI, go to *System > Certificates*, click *Create/Import*, and select *Certificate* from the dropdown.
 - b. In *Generate Certificate using Local CA*, select *Generate Certificate*. The *Certificate Details* tab opens.
 - c. In *Certificate name*, enter the certificate name.
 - d. In *Common name*, enter the common name for the certificate, i.e., an FQDN.
 - e. In *Subject alternative name*, enter the IP address.



- f. Click *Create*. The new certificate is created and listed under *Local Certificate*.



2. Enable the newly created certificate on the FortiPAM GUI.
 - a. Go to *Network > Interfaces*.
 - b. Double-click to edit the network interface.
 - c. In the *Service Access Setting* pane, from the *SSL Certificate* dropdown, select the certificate created in step 1.

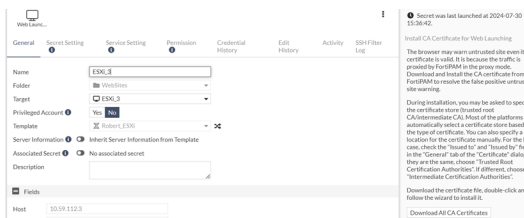


- d. Click *Save*.

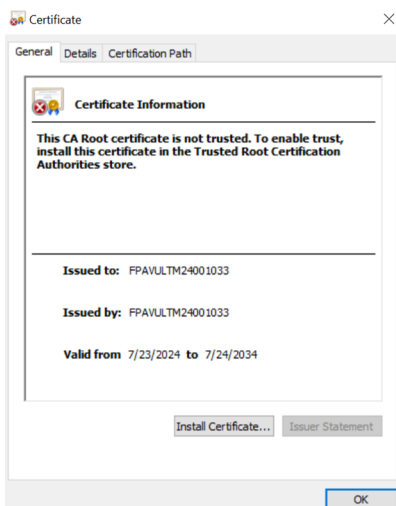
Downloading FortiPAM CA from the FortiPAM GUI

To download the FortiPAM CA from the FortiPAM GUI and manually install it:

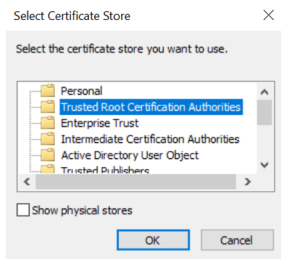
1. Download FortiPAM default CA on the FortiPAM GUI.
2. Go to *Secrets > Secrets*, select a *Web Account* secret, and select *Edit* to edit the secret.
3. Click *Download All CA Certificates*.



4. Double-click the downloaded file to unzip it.
5. Double-click the CA certificate.



6. Click *Install Certificate* and follow the installation prompts to install the certificate to the trust root.



7. Click *OK*.

Logging servers

This section describes various logging servers available to FortiPAM.

FortiAnalyzer Cloud as a logging server

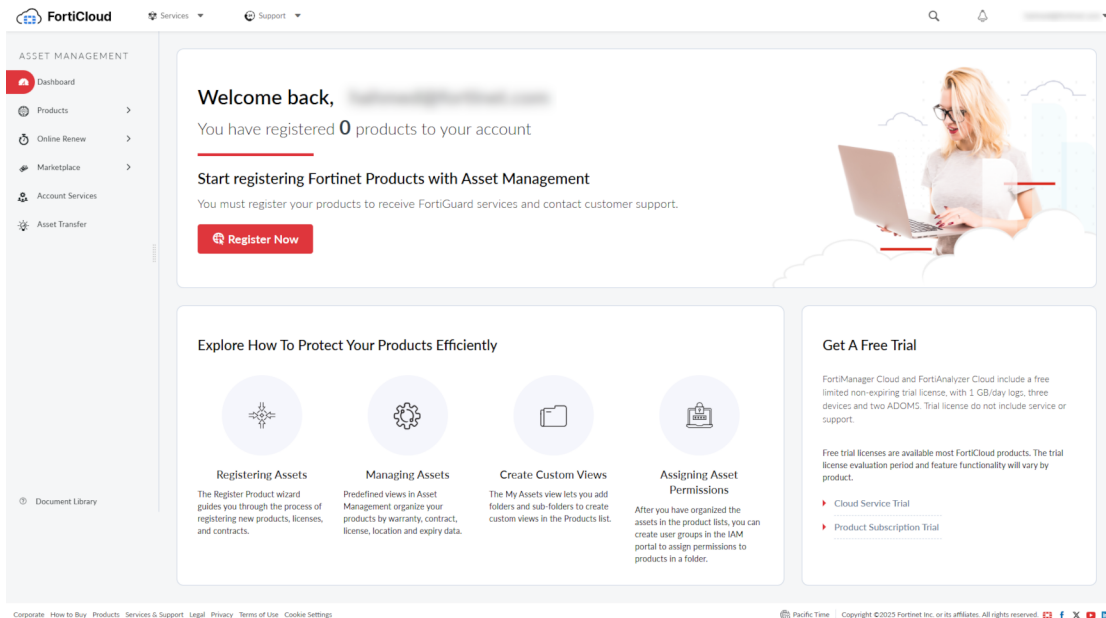
FortiAnalyzer Cloud is a remote logging server that keeps an additional copy of logs from FortiPAM.

Configuring FortiAnalyzer Cloud as a logging server:

1. [Registering FortiAnalyzer Cloud on page 212](#)
2. [Deploying a FortiAnalyzer Cloud instance on page 213](#)
3. [Add FortiPAM to FortiAnalyzer Cloud instance on page 215](#)
4. [Enabling FortiAnalyzer Cloud in FortiPAM on page 215](#)
5. [Launching a secret on page 217](#)

Registering FortiAnalyzer Cloud

1. Go to the [FortiCare portal](#) and create a new account or log in with an existing account. The *Asset Management* portal opens.



2. On the *Asset Management* portal, click *Register Now* to register FortiAnalyzer Cloud.

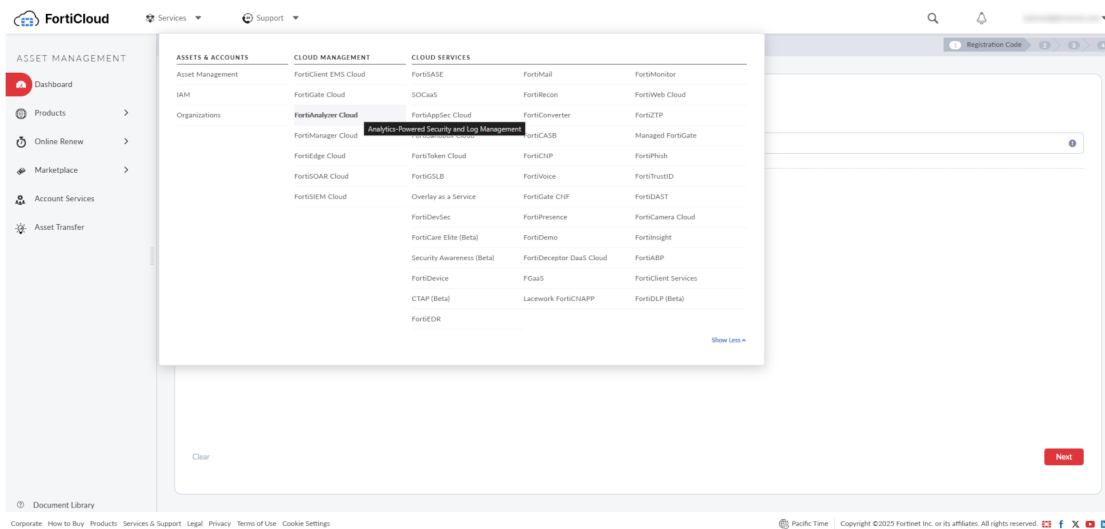
3. Provide the registration code:
 - a. Enter the FortiAnalyzer Cloud registration code.
 - b. Choose your end user type as either a government or non-government user.
 - c. Click *Next*.
4. The *Fortinet Product Registration Agreement* page displays.
Select the check box to indicate that you have read, understood, and accepted the service contract. Click *Next*.
5. The *Verification page* displays.
Select the checkbox to indicate that you accept the terms.
Click *Confirm*.
Registration is now complete and your registration summary is displayed.
See [Registering assets](#) in the latest *Asset Management Administration Guide*.

Deploying a FortiAnalyzer Cloud instance

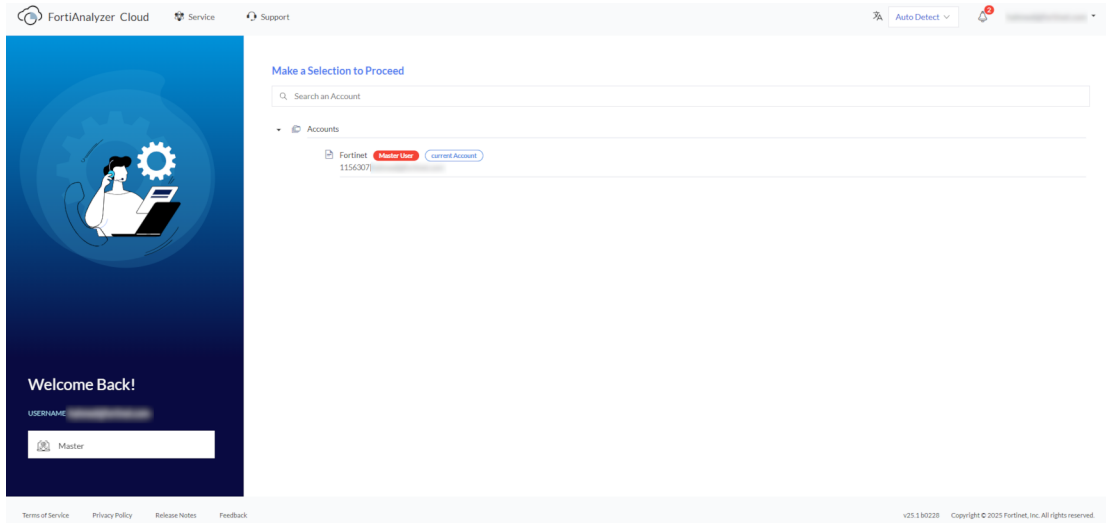
After registering a FortiAnalyzer Cloud instance, deploy the FortiAnalyzer Cloud instance.

To deploy a FortiAnalyzer Cloud instance:

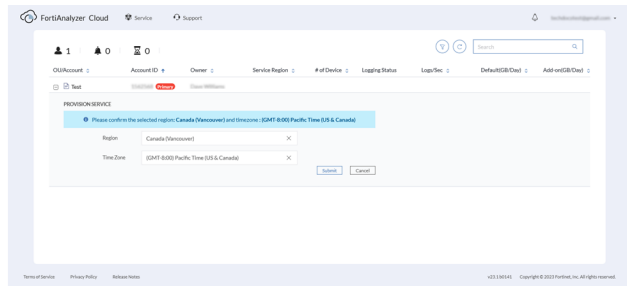
1. From the *Services* menu, in *CLOUD MANAGEMENT*, select *FortiAnalyzer Cloud*.



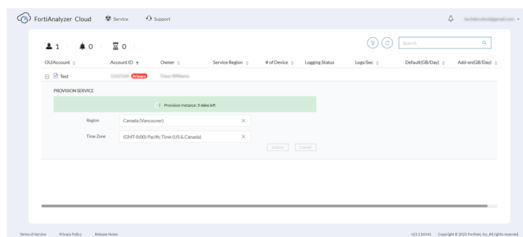
- In FortiAnalyzer Cloud, select a FortiCloud account to proceed.



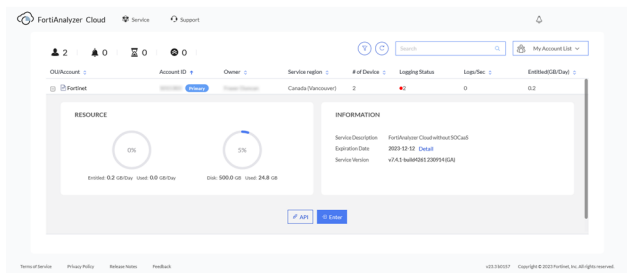
- In the new window, select a *Region*.
In this example, the region is *Canada (Vancouver)*.
- Select a *Time Zone* for the FortiAnalyzer Cloud instance.



- Click *Submit*.
- Confirm the selected region and the timezone.
- Review and accept the *Terms of Service* and *Privacy Policy*.
FortiAnalyzer Cloud instance is provisioned in a few minutes.



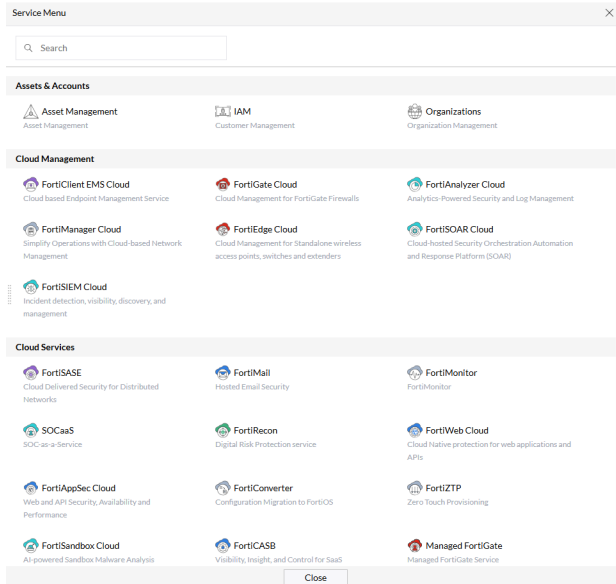
- Once provisioned, expand the account, and click *Enter* to access the FortiAnalyzer Cloud instance.



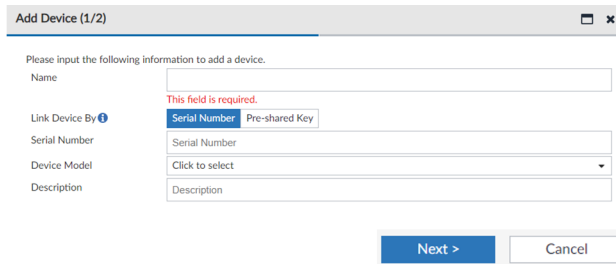
Add FortiPAM to FortiAnalyzer Cloud instance

To add FortiPAM to FortiAnalyzer Cloud instance:

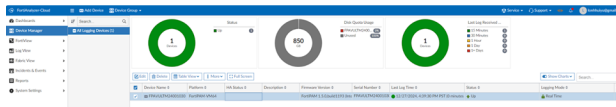
1. Beside the FortiAnalyzer Cloud title, click *Service*.
The *Service Menu* opens.



2. Select *FortiAnalyzer Cloud*.
This redirects you to the *FortiAnalyzer Cloud* portal.
3. Click *Add Device*, and enter FortiPAM related information.
In this example, FortiPAM device is linked to FortiAnalyzer Cloud by serial number.



4. Once the *Add Device* dialog is filled in, click *Next*.
5. Verify that the newly linked FortiPAM device is in *Device Manager > All Logging Devices*.

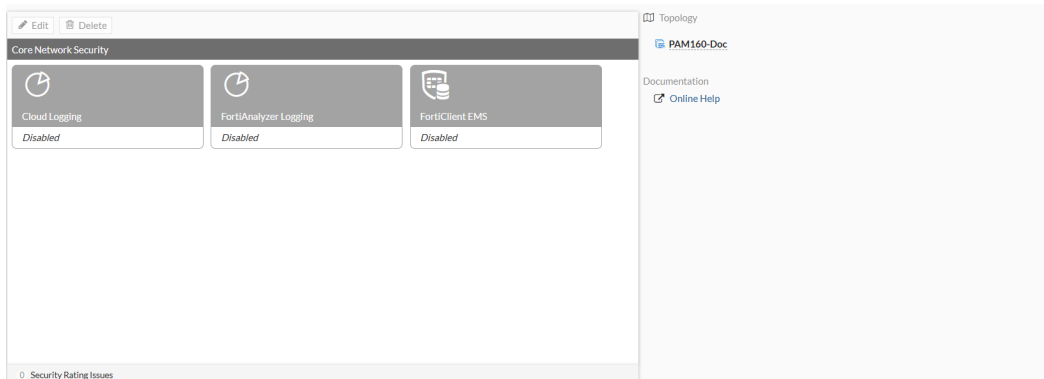


Enabling FortiAnalyzer Cloud in FortiPAM

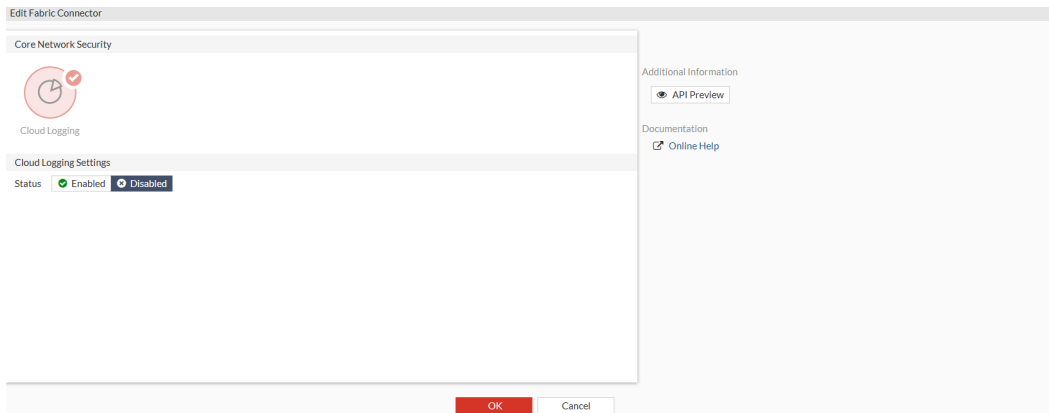
You can now use FortiAnalyzer Cloud on FortiPAM.

To enable FortiAnalyzer Cloud in FortiPAM:

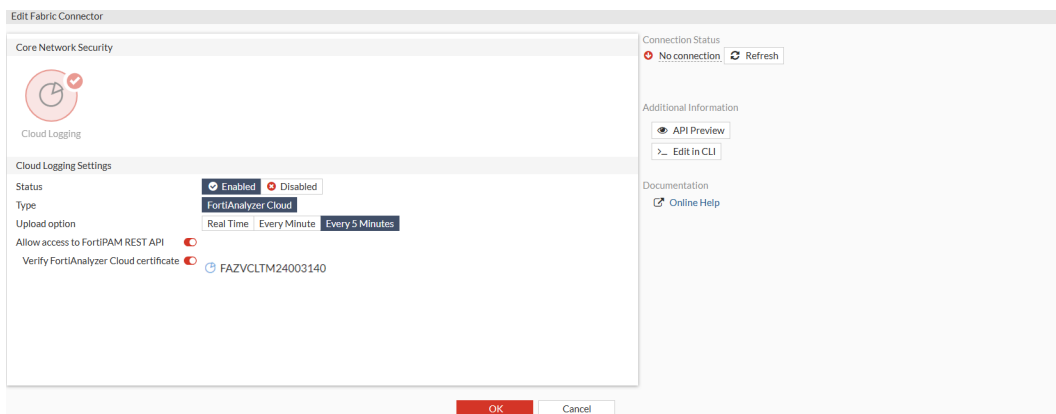
1. Go to *Network > Fabric Connectors*.
Core Network Security opens.



2. Select *Cloud Logging* and select *Edit*.
The *Edit Fabric Connector* window opens.



3. In the *Cloud Logging Settings* pane, set Status as *Enabled*.
You now see new options in the *Edit Fabric Connector* window.



4. In *Upload option*, select the frequency of log uploads to the remote FortiAnalyzer Cloud:
 - a. *Real Time*: Logs are sent to the remote device in real time.
 - b. *Every Minute*: Logs are sent to the remote device once every minute.
 - c. *Every 5 Minutes*: Logs are sent to the remote device once every 5 minutes (default).

5. In *Allow access to FortiPAM REST API*, you can define access to the FortiPAM API:
 - a. *Enable*: The REST API accesses the FortiPAM topology and shares data and results.
 - b. *Disable*: The REST API does not share data and results.
6. In *Verify FortiAnalyzer Cloud certificate*, you can define the FortiAnalyzer Cloud certificate verification process:
 - a. *Enable*: FortiPAM verifies FortiAnalyzer Cloud serial number against the FortiAnalyzer certificate. When verified, the serial number is stored in the FortiPAM configuration.
 - b. *Disable*: FortiPAM does not verify the FortiAnalyzer Cloud certificate against the serial number.
7. Click *OK*.
8. In the window that opens, verify the FortiAnalyzer Cloud serial number and click *Accept*.
The verified FortiAnalyzer Cloud certificate appears in the settings, and the *Connection Status* is *Connected*.

Launching a secret

To launch a secret and check its logs:

1. In *Secrets > Secrets*, select a secret, and click *Launch Secret*.
2. In *Launch Progress*, select a launcher to launch the secret.
3. Go to *Log & Report > Secret Event & Video*.
4. From the *Log location* dropdown, select *FortiAnalyzer Cloud* to see the logs available on FortiAnalyzer Cloud.

Date/Time	User	Secret name	Account	Operation	Message
2024/12/27 16:23:12	admin	101_webftpt		Video upload finished	Secret video uploading completed.
2024/12/27 16:23:12	admin	101_webftpt		Closed secret	Secret session ended.
2024/12/27 16:23:05	admin	101_webftpt		Video upload start	Start recording secret session.

FortiGate

FortiPAM behind FortiGate

In some network topologies, FortiPAM is protected by a FortiGate device.

In this example, the following two scenarios are discussed:

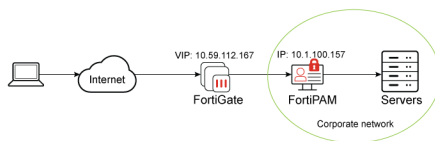
1. [Configuring a VIP on FortiGate for FortiPAM access on page 218](#)
2. [Configuring ZTNA on FortiGate for FortiPAM access on page 220](#)

Configuring a VIP on FortiGate for FortiPAM access

Prerequisites

1. An IP address as the VIP for the FortiPAM GUI, e.g., 10.59.112.167.
The actual FortiGate GUI IP address is 10.59.112.58.
2. The actual FortiPAM IP address is 10.1.100.157.
Note: This IP address is within the corporate network and is not exposed publicly.

VIP mode topology



Configuring a VIP for FortiPAM access

To configure a VIP for FortiPAM access:

1. In the FortiGate CLI console, enter the following commands:

```
config firewall vip
edit "VIP_PAM_167"
set uuid bb4bf8ac-789d-51f0-4976-2cc09088e220
set extip 10.59.112.167
set mappedip "10.1.100.157"
set extintf "any"
set portforward enable
set extport 443-2000 #Port 443: PAM GUI; Port 1444: PAM web-proxy
set mappedport 443-2000
next
end
```



For a port supporting the web proxy feature, FortiPAM port can use any port, e.g., 1444 in this example.

```
config firewall policy
edit 7
set name "VIP167_Policy"
set uuid ee86b2a2-789d-51f0-f736-4483abb85ec9
set srcintf "port1"
set dstintf "port2" #port2 connects to the 10.1.100.x subnet
set action accept
set srcaddr "all"
set dstaddr "VIP_PAM_167"
set schedule "always"
set service "ALL"
set nat enable
next
end
```

2. In the FortiPAM CLI console, enter the following commands to enable web proxy:

```
config system interface
edit "port2"
set ip 10.1.100.157 255.255.255.0
set allowaccess ping ssh
set type physical
set explicit-web-proxy enable #enable web proxy
set snmp-index 2
next
end
config web-proxy explicit-proxy
edit "web-proxy"
set status enable
set interface "any"
set http-incoming-port 1444
```

```

next
end
config web-proxy global
  set proxy-fqdn "10.59.112.167"
end

```

You can now access FortiPAM using the VIP 10.59.112.167 set up on the FortiGate.

Configuring ZTNA on FortiGate for FortiPAM access

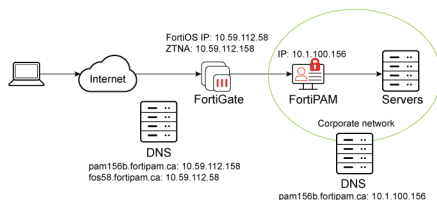
For information ZTNA and web proxy forwarding, see:

1. [Basic ZTNA configuration](#)
2. [Technical Tip: How to configure web proxy forwarding server \(proxy chaining\)](#)

Prerequisites

1. FortiGate ZTNA external IP address, e.g., 10.59.112.158.
2. FQDN for FortiPAM, e.g., pam156b.fortipam.ca.
3. **Public DNS server:**
 - a. FQDN (pam156b.fortipam.ca) is resolved to the FortiGate ZTNA external IP address: 10.59.112.158.
 - b. FQDN (fos58.fortipam.ca) is resolved to the FortiGate GUI IP address: 10.59.112.58.
4. **Private DNS server:** FQDN (pam156b.fortipam.ca) is resolved to the FortiPAM GUI IP address: 10.1.100.156.
5. The PC connects to the public DNS server.
6. The FortiGate connects to the private DNS server.

Topology



Configuring ZTNA for FortiPAM access

To configure the FortiPAM FQDN:

1. In the FortiGate GUI, go to *Policy & Objects > Addresses*, and select *Create new* to configure address for the FortiPAM FQDN.

The *New Address* window opens.

2. In *Name*, enter a name for the address.
3. Ensure that *Interface* is *any*.
4. In *Type*, select *FQDN*.
5. In *FQDN*, enter the FortiPAM FQDN.

pam156b.fortipam.ca

6. Click *OK*.

Alternatively, in the CLI console, enter the following commands:

```
config firewall address
edit "pam_156b_fqdn"
set uuid b0997e8a-7888-51f0-54aa-9b97280518cd
set type fqdn
set "pam156b.fortipam.ca"
next
end
```

To configure the ZTNA server:

1. In the FortiGate GUI, go to *Policy & Objects > ZTNA*, and select *Create new* in the *ZTNA Server* tab.
The *New ZTNA Server* window opens.
2. In *Name*, enter a name for the ZTNA server.
3. In *Interface*, select *port1*.
4. In *IP address*, enter the IP address for the FortiGate, e.g., *10.59.112.158*.
5. Ensure that the *Port* is *443*.
6. In *Default certificate*, select *Fortinet_SSL*.
7. In *Service/server mapping*, select *Create new*.
The *New Service/Server Mapping* window opens.
 - a. Ensure that the *Service* is set to *HTTPS*.
 - b. In *Virtual Host*, select *Specify*.

- c. In *Host*, enter the FortiPAM FQDN.
See [Configuring the FortiPAM FQDN](#).
- d. In *Use certificate*, select *Fortinet_SSL*.
- e. Ensure that *Match path by* is *Substring*.
- f. In *Address type*, select *FQDN*.
- g. In the *Address* dropdown, select the FortiPAM FQDN created in [Configuring the FortiPAM FQDN](#).
- h. Ensure that *Port* is 443.
- i. Click *OK*.

8. Click *OK*.

Service	URL	Server	Type
HTTPS	pam156b.fortipam.ca/	pam_156b_fqdn:443	IPv4

Alternatively, in the CLI console, enter the following commands:

```
config firewall vip
edit "ZTNA_PAM156b"
set uuid f1ecb802-7888-51f0-222d-713912cbeb51
set type access-proxy
set server-type https
set extip 10.59.112.158
set extintf "port1"
set extport 443
set ssl-certificate "Fortinet_SSL"
next
end
config firewall access-proxy
edit "ZTNA_PAM156b"
set vip "ZTNA_PAM156b"
set client-cert disable #Disable if FortiGate is not connected with the EMS
set svr-pool-multiplex disable
config api-gateway
edit 1
set virtual-host "auto-ZTNA_PAM156b-0"
config realservers
edit 1
set addr-type fqdn
set address "pam_156b_fqdn"
next
end
next
end
next
end
config firewall access-proxy-virtual-host
edit "auto-ZTNA-PAM156-0"
set ssl-certificate "Fortinet_SSL"
set host "pam156b.FORTIPAM.CA"
next
end
```

To configure the firewall policy:

1. In the FortiGate console, enter the following commands:

```
config firewall policy
edit 6
set name "ZTNA_PAM156b_Policy"
set uuid 5c0cf6de-7889-51f0-24ae-e45e7e6a4f12
set srcintf "port1"
set dstintf "any"
set action accept
set srcaddr "all"
set dstaddr "ZTNA_PAM156b"
set schedule "always"
set nat enable
```

```
next
end
```

To configure web proxy forwarding on FortiGate:

1. In the CLI console, enter the following commands:

```
config system interface
edit "port1"
set vdom "root"
set ip 10.49.112.58 255.255.255.0
set allowaccess ping https ssh http
set type physical
set explicit-web-proxy enable #enable web proxy
set snmp-index 1
next
end
config web-proxy explicit
set status enable
set https-incoming-port 8080
end
config web-proxy forward-server
edit "pam156b_web_proxy"
set addr-type fqdn
set fqdn "pam156b.fortipam.ca"
set port 8080
next
end
config firewall proxy-policy
edit 2
set uuid 024adcf4-7967-51f0-01cd-00e184cc0c25
set name "pam156b_proxy_policy"
set proxy explicit-web
set dstintf "any"
set srcaddr "all"
set dstaddr "all"
set service "webproxy"
set action accept
set schedule "always"
set logtraffic all
set webproxy-forward-server "pam156b_web_proxy"
next
end
```

To configure FortiPAM:

1. In the CLI console, enter the following commands to enable web proxy on the port interface:

```
config system interface
edit "port2"
set ip 10.1.100.156 255.255.255.0
```

```

set allowaccess ping ssh
set type physical
set explicit-web-proxy enable
set snmp-index 2
next
end

```

- In the CLI console, enter the following commands to change the proxy-fqdn to the FortiGate GUI FQDN:

```

config web -proxy global
set proxy-fqdn "fos58.fortipam.ca"
end

```

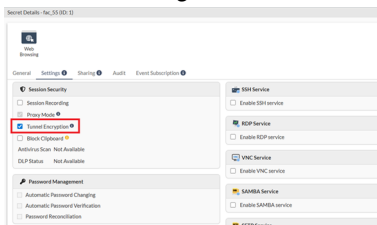
- In the CLI console, enter the following commands to verify the web proxy listening port number:

```

config web-proxy explicit-proxy
edit "web-proxy"
set status enable
set interface "any"
set http-incoming-port 8080 #Sync with the web proxy forward port configured on the
FortiGate
next
end

```

- In the FortiPAM GUI, go to *Secrets > Secrets*, from the list, open a secret:
 - Go to the *Settings* tab, enable *Tunnel Encryption*, and click *Save*.



Results

- You can access FortiPAM by going to `https://pam156b.fortipam.ca`.
- You can launch secrets with native launcher (*PuTTY*, *RDP*) or web launcher (*Web SSH*, *Web RDP*), or Web Account with/without web proxy.



www.fortinet.com

Copyright© 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.