Examples

FortiPAM 1.8.0

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

February 13, 2026
FortiPAM 1.8.0 Examples
74-180-1202990-20260213

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-12-01	Initial release.
2025-12-23	Added Azure AD password changer on page 115.
2026-02-13	Updated Configuring traffic proxy on the gateway for forwarding secret launch (traffic plane) on page 142.

Introduction

This document serves as a reference guide to common FortiPAM 1.8 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 1.8:

- 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 121
- Web proxy on page 127
- RDP log retrieval on page 132
- Gateway on page 137
- SSH filter profiles on page 160
- Automation on page 168
- Windows application filter on page 174
- Web launcher on page 186
- Log and video disks on page 192
- Certificate management on page 197
- Logging servers on page 206
- FortiGate on page 212

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.

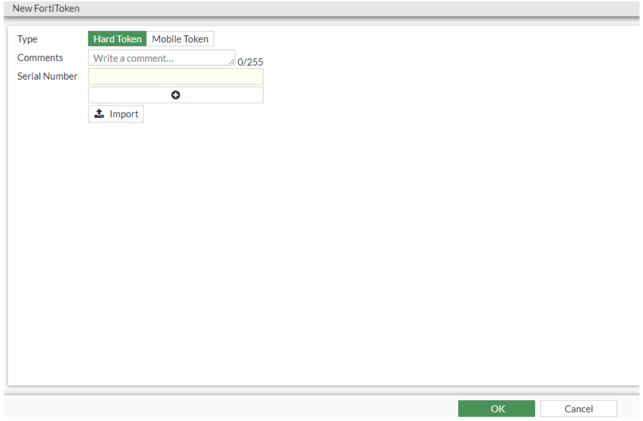
To set up 2FA with FortiToken Mobile:

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.

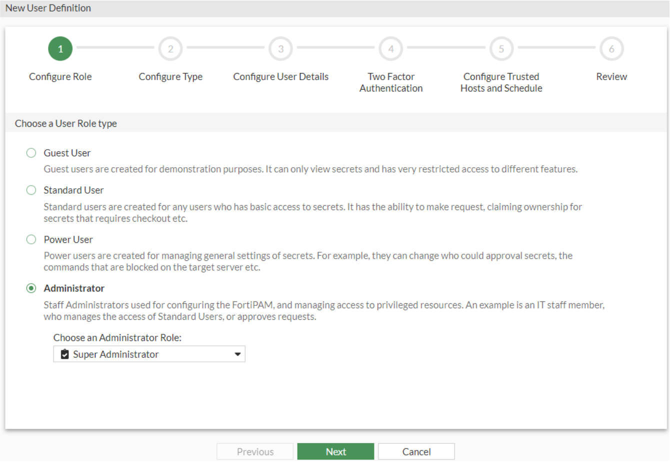


2. Select the *Type* as *Mobile Token*.
3. In *Activation Code*, enter the FortiToken activation code.
4. Click *OK*.

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*.



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.

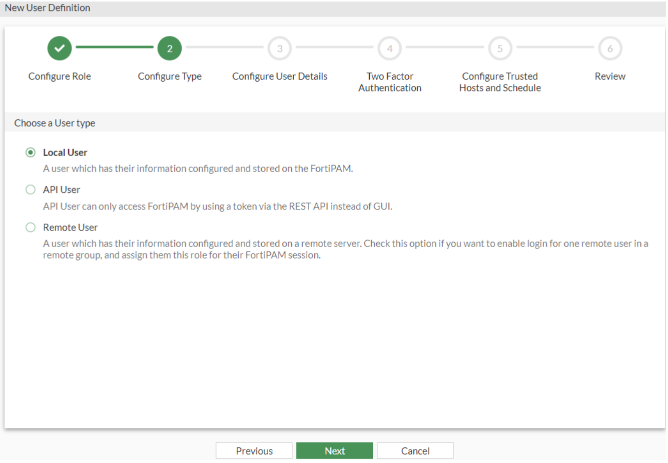
○ Standard User
Standard users are created for any users who has basic access to secrets. It has the ability to make request, claiming ownership for secrets that requires checkout etc.

○ 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: Super Administrator

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



Choose a User type

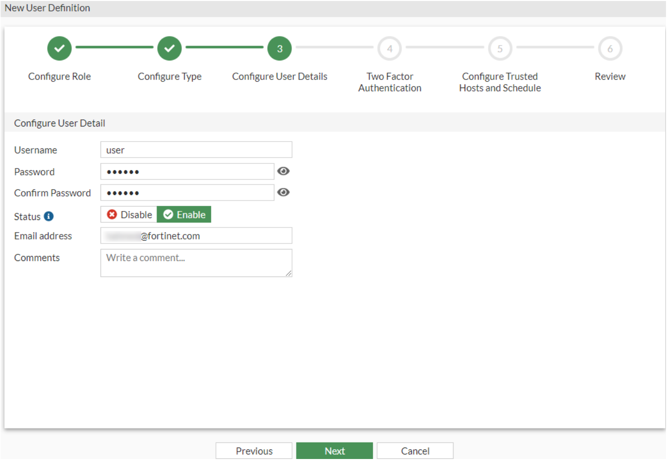
● Local User
A user which has their information configured and stored on the FortiPAM.

○ 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.

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.



Configure User Detail

Username: user

Password: ••••••

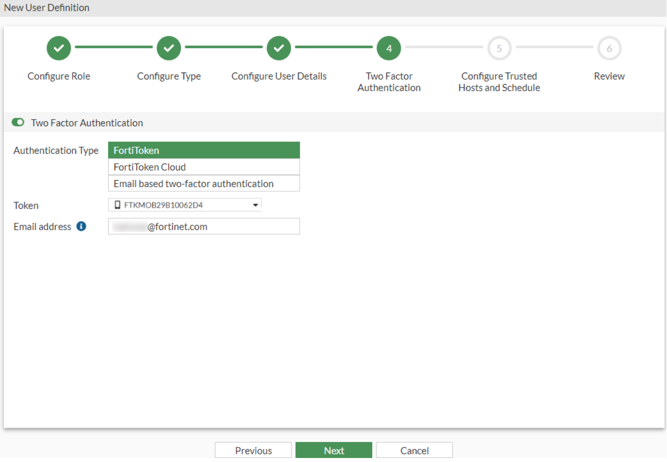
Confirm Password: ••••••

Status: Disable | Enable

Email address: [redacted]@fortinet.com

Comments: Write a comment...

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.



Two Factor Authentication

Authentication Type: FortiToken | FortiToken Cloud | Email based two-factor authentication

Token: FTKMOB29B10062D4

Email address: [redacted]@fortinet.com

   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
```

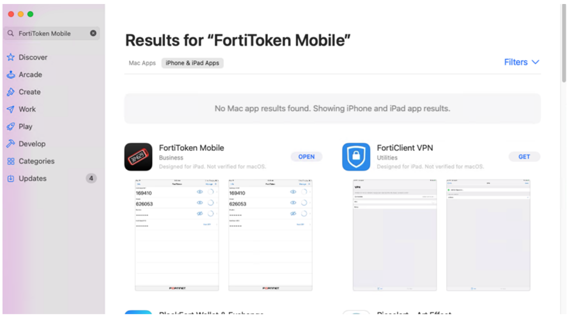
Results

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:

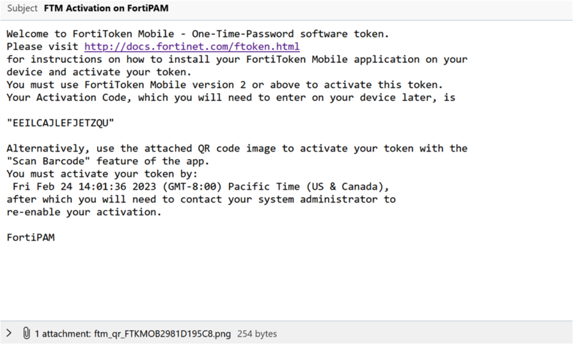
1. In the App Store, look for FortiToken Mobile and install the application.



Results for “FortiToken Mobile”

No Mac app results found. Showing iPhone and iPad app results.

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*, *FortiToken Mobile User Guide*.

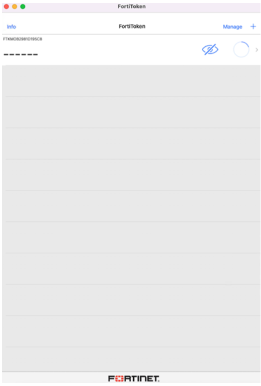


Subject **FTM Activation on FortiPAM**

```
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

"EEILCAJLEFJETZQU"

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_FTKMOB2981D195C8.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**:

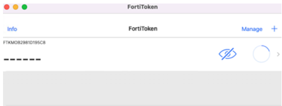
      i. Select *+* and then select *Enter Manually* from the bottom.

      ii. Select *Fortinet* and enter *Name* and *Key*.

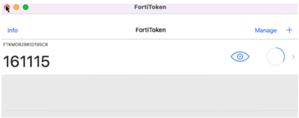
      > *Key* is the activation key from your activation email notification and must be entered exactly as it appears in the activation message, either by typing or copying and pasting.

      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.

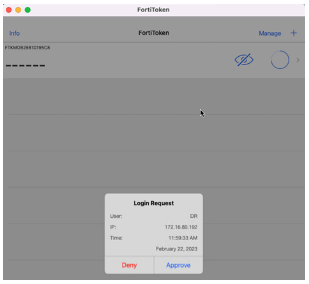
5. Click the eye icon to retrieve the token to be used in step 3 in Results on page 14.



FTKMOB2981D195C8

161115

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



FTKMOB2981D195C8

Login Request

User: DR

IP: 172.16.80.192

Time: 11:59:33 AM February 22, 2023

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

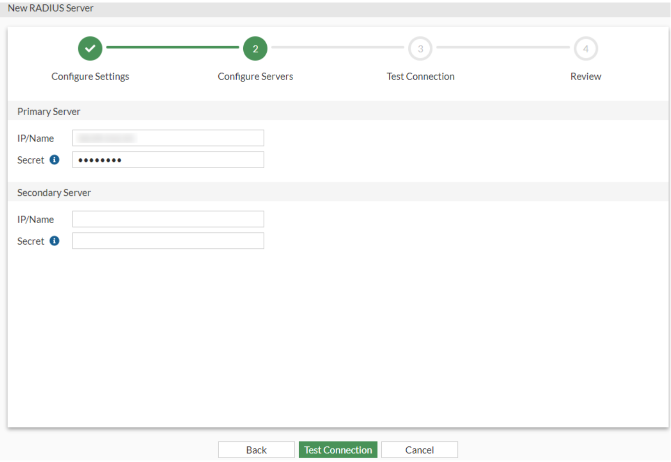
Configuring a RADIUS server on FortiPAM

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.



Primary Server

IP/Name [redacted]

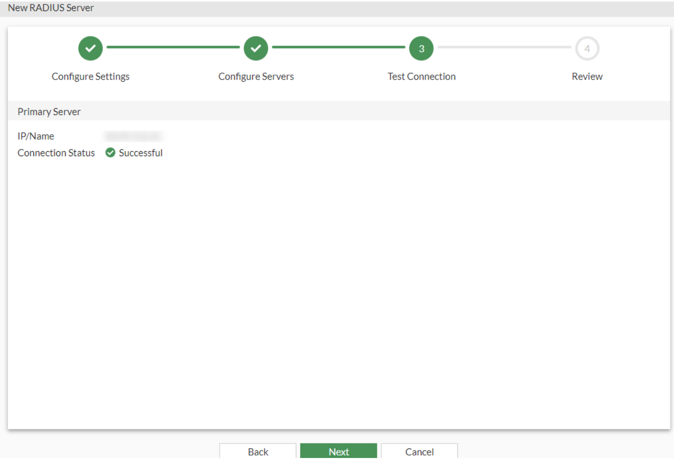
Secret ••••••••

Secondary Server

IP/Name

Secret

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



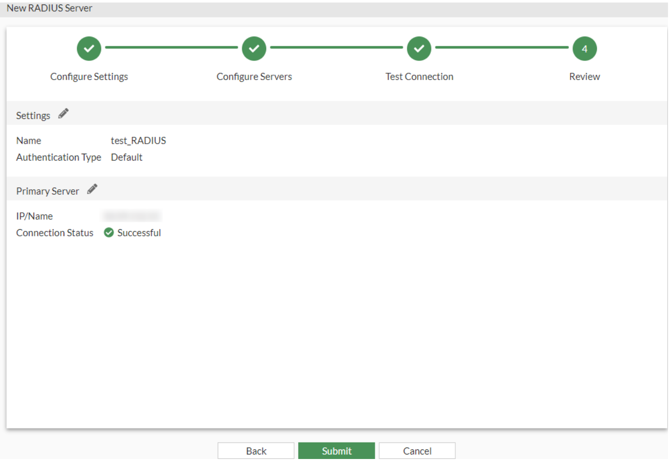
Primary Server

IP/Name [redacted]

Connection Status ✓ Successful

8. Click *Next*.

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



Settings

Name test_RADIUS

Authentication Type Default

Primary Server

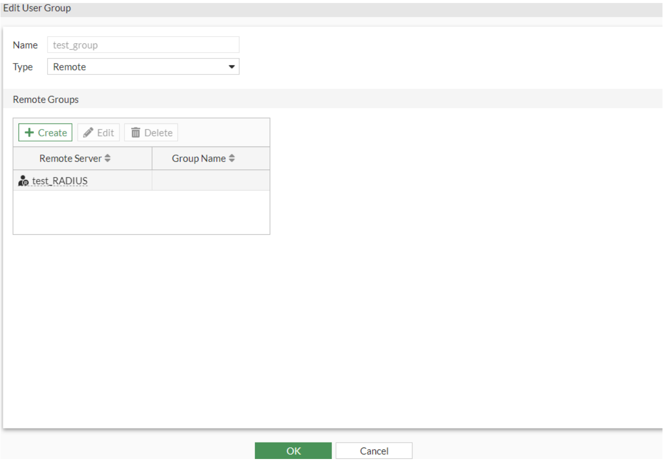
IP/Name [redacted]

Connection Status ✓ Successful

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*.



Edit User Group

Name: test_group
Type: Remote

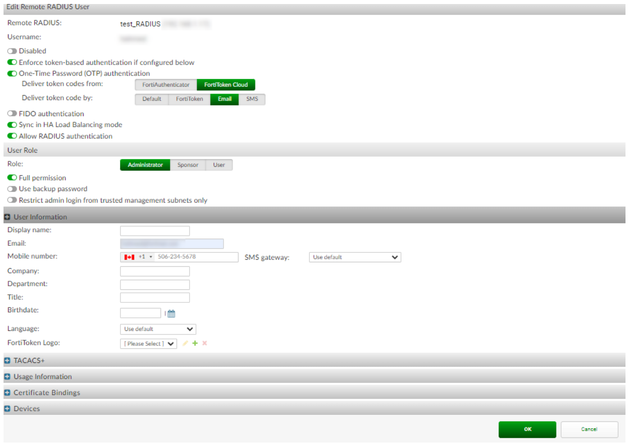
Remote Groups

Remote Server	Group Name
test_RADIUS	

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.



Edit Remote RADIUS User

Remote RADIUS: test_RADIUS [redacted]

Username: [redacted]

Disabled

Enforce token-based authentication if configured below

One-Time Password (OTP) authentication

Deliver token codes from: FortiAuthenticator | FortiToken Cloud

Deliver token code by: Default | FortiToken | Email | SMS

FIDO authentication

Sync in HA Load Balancing mode

Allow RADIUS authentication

User Role

Role: Administrator | Sponsor | User

Full permission

Use backup password

Restrict admin login from trusted management subnets only

User Information

Display name:

Email: [redacted]

Mobile number: +1 506-234-5678 SMS gateway: Use default

Company:

Department:

Title:

Birthdate:

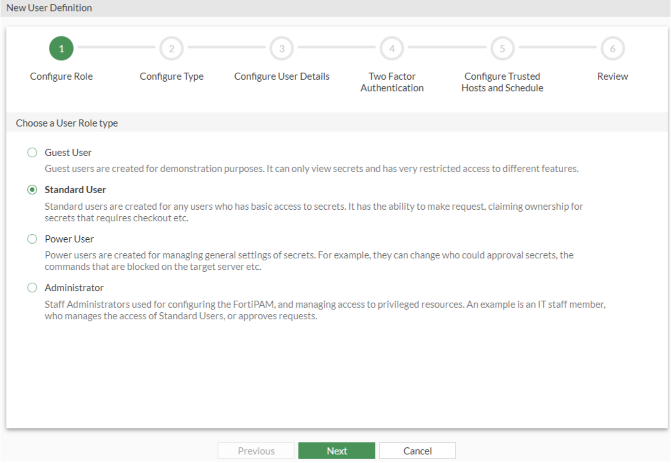
Language: Use default

FortiToken Logo: [Please Select]

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*.



New User Definition

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

Choose a User Role type

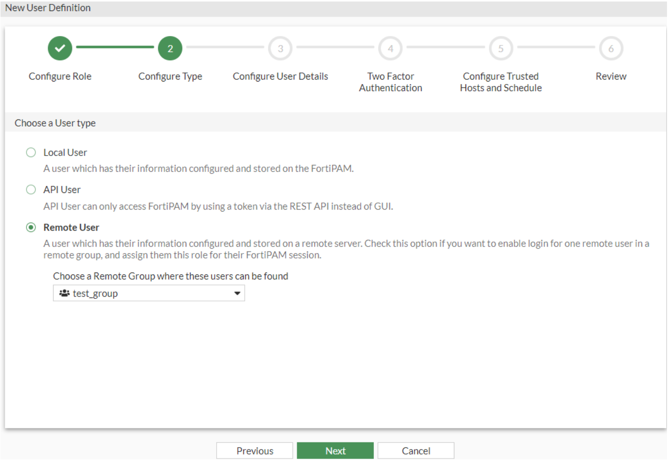
○ Guest User
Guest users are created for demonstration purposes. It can only view secrets and has very restricted access to different features.

● 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.

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.



New User Definition

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

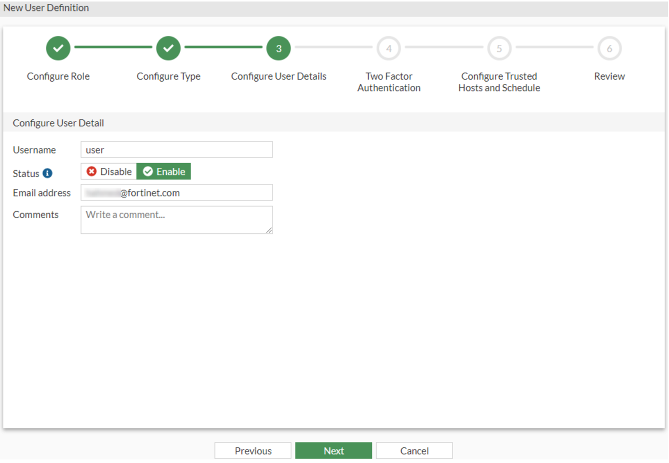
● Remote User

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.

Choose a Remote Group where these users can be found

test_group

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.



New User Definition

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

Configure User Detail

Username: user

Status: Disable [✓ Enable]

Email address: [redacted]@fortinet.com

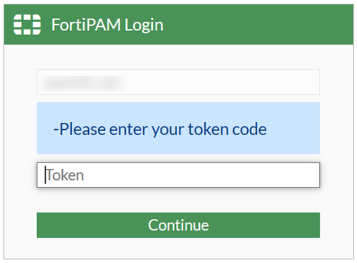
Comments: Write a comment...

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.



FortiPAM Login

[redacted]

-Please enter your token code

Token

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.

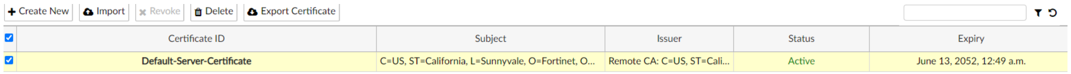
To set up 2FA on FortiPAM for SAML users with FortiAuthenticator as a SAML IdP:

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:

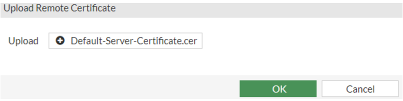
1. Log in to FortiAuthenticator.
2. Go to *Certificate Management > End Entities > Local Services*.



☑	Certificate ID	Subject	Issuer	Status	Expiry
☑	Default-Server-Certificate	C=US, ST=California, L=Sunnyvale, O=Fortinet, O...	Remote CA: C=US, ST=Cali...	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.

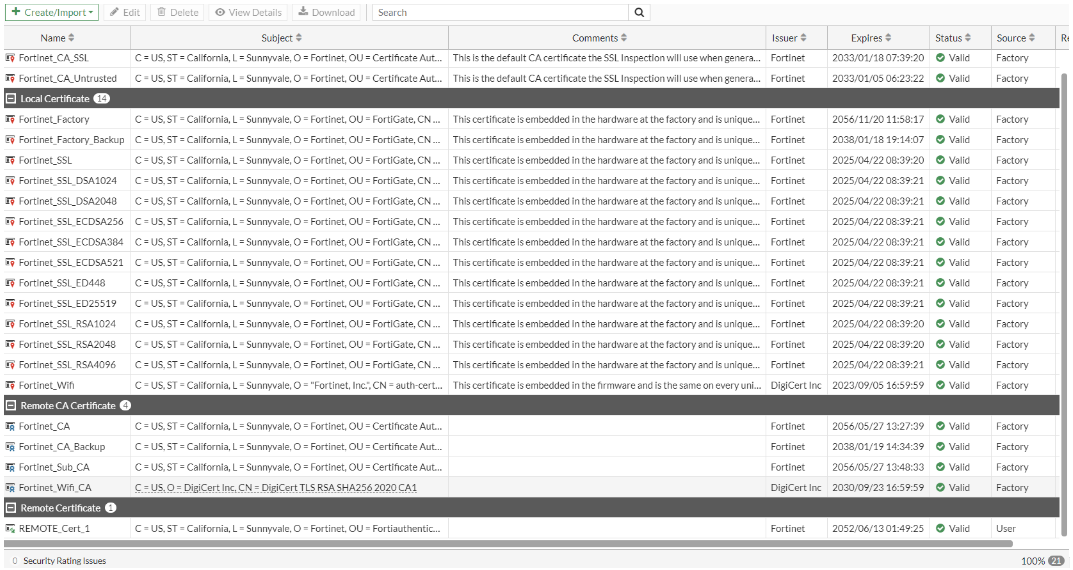
7. Click *OK*.



Upload Remote Certificate

Upload: Default-Server-Certificate.cer

The imported certificate shows up under *Remote Certificate*.



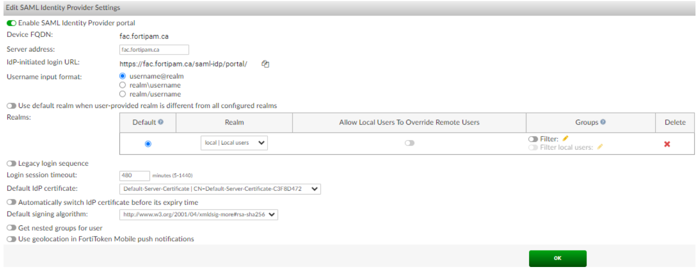
Name	Subject	Comments	Issuer	Expires	Status	Source	Re
Fortinet_CA_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Aut...	This is the default CA certificate the SSL Inspection will use when genera...	Fortinet	2033/01/18 07:39:20	✓ Valid	Factory	
Fortinet_CA_Untrusted	C = US, 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 14							
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 uni...	DigiCert Inc	2023/09/05 16:59:59	✓ Valid	Factory	
Remote CA Certificate 4							
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 CA1		DigiCert Inc	2030/09/23 16:59:59	✓ Valid	Factory	
Remote Certificate 1							
REMOTE_Cert_1	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Fortiauthentic...		Fortinet	2052/06/13 01:49:25	✓ Valid	User	

0 Security Rating Issues   100% 21

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*.



Edit SAML Identity Provider Settings

Enable SAML Identity Provider portal: on

Device FQDN: fac.fortipam.ca

Server address: fac.fortipam.ca

IdP-initiated login URL: https://fac.fortipam.ca/saml-idp/portal/

Username input format:
● username@realm
○ realm\username
○ realm/username

Use default realm when user-provided realm is different from all configured realms: off

Realms:

Default	Realm	Allow Local Users To Override Remote Users	Groups	Delete
●	local | Local users	off	Filter: Filter local users:	✖

Legacy login sequence: off

Login session timeout: 480 minutes (5-1440)

Default IdP certificate: Default-Server-Certificate | CN=Default-Server-Certificate-C3F8D472

Automatically switch IdP certificate before its expiry time: off

Default signing algorithm: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256

Get nested groups for user: off

Use geolocation in FortiToken Mobile push notifications: off

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.

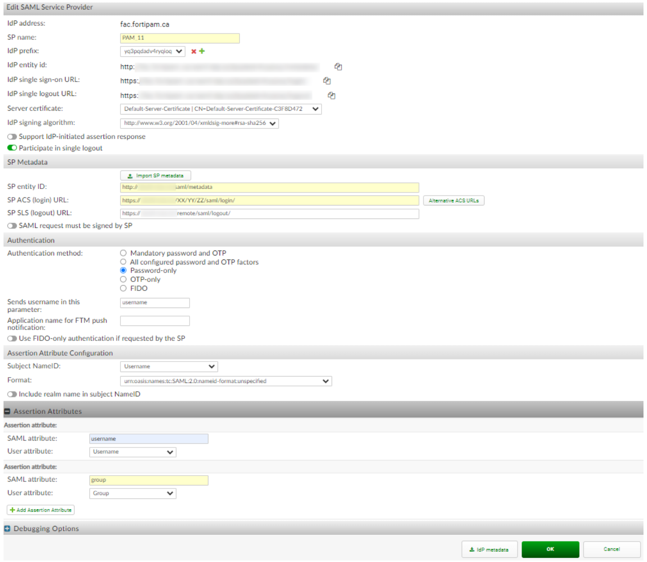
   SP entity ID, *SP ACS (login) URL*, and *SP SLS (logout) URL* values are same as those in the *Configure Service Provider* tab when Configuring FortiPAM as an SP on page 26.

   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*.



Edit SAML Service Provider

IdP address: fac.fortipam.ca

SP name: PAM_11

IdP prefix: yq3pqdadv4ryqioq

IdP entity id: http:[redacted]

IdP single sign-on URL: https:[redacted]

IdP single logout URL: https:[redacted]

Server certificate: Default-Server-Certificate | CN=Default-Server-Certificate-C3F8D472

IdP signing algorithm: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256

Support IdP-initiated assertion response

Participate in single logout

SP Metadata

SP entity ID: http://[redacted]saml/metadata

SP ACS (login) URL: https://[redacted]/XX/YY/ZZ/saml/login/

SP SLS (logout) URL: https://[redacted]remote/saml/logout/

SAML request must be signed by SP

Authentication

Authentication method:
○ Mandatory password and OTP
○ All configured password and OTP factors
● Password-only
○ OTP-only
○ FIDO

Sends username in this parameter: username

Application name for FTM push notification:

Use FIDO-only authentication if requested by the SP

Assertion Attribute Configuration

Subject NameID: Username

Format: urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified

Include realm name in subject NameID

Assertion Attributes

Assertion attribute:

SAML attribute: username

User attribute: Username

Assertion attribute:

SAML attribute: group

User attribute: Group

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:
   1. In *Type*, select *Custom*.
   2. In *IdP entity ID*, enter the FortiAuthenticator IdP entity ID.
   3. In *IdP single sign-on URL*, enter the FortiAuthenticator IdP login URL.
   4. In *IdP single logout URL*, enter the FortiAuthenticator IdP logout URL.

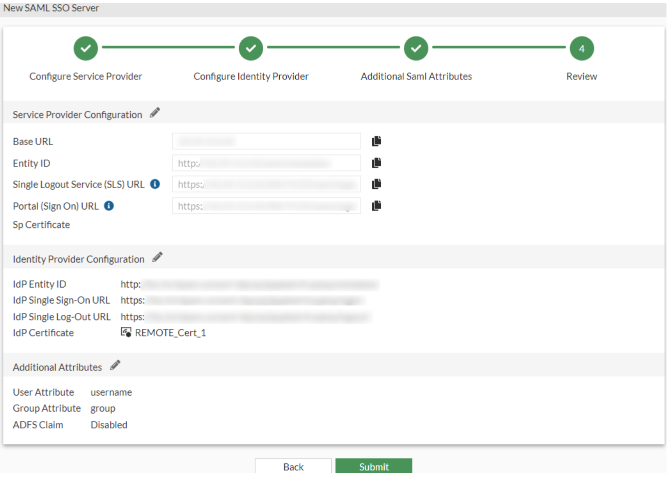
      IdP entity ID, *IdP single sign-on URL*, and *IdP single logout URL* were initially configured in Configuring FortiAuthenticator as a SAML IdP on page 24.

   5. In the *IdP Certificate* dropdown, select the remote certificate imported in Importing FortiAuthenticator certificate to FortiPAM on page 23.
   6. Click *Next*.
5. In the *Additional Saml Attributes* tab:
   1. In *Attribute used to identify users*, enter *username*.
   2. 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
4
Review

Service Provider Configuration

Base URL [redacted]
Entity ID http:[redacted]
Single Logout Service (SLS) URL https:[redacted]
Portal (Sign On) URL https:[redacted]
Sp Certificate

Identity Provider Configuration

IdP Entity ID http:[redacted]
IdP Single Sign-On URL https:[redacted]
IdP Single Log-Out URL https:[redacted]
IdP Certificate REMOTE_Cert_1

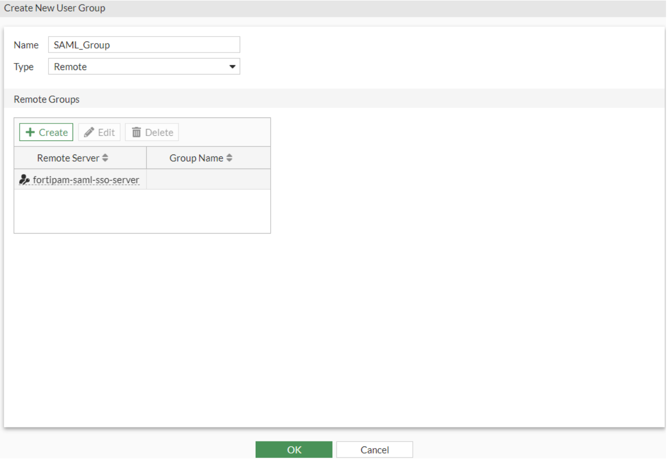
Additional Attributes

User Attribute username
Group Attribute group
ADFS Claim Disabled

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 SAML_Group
Type Remote

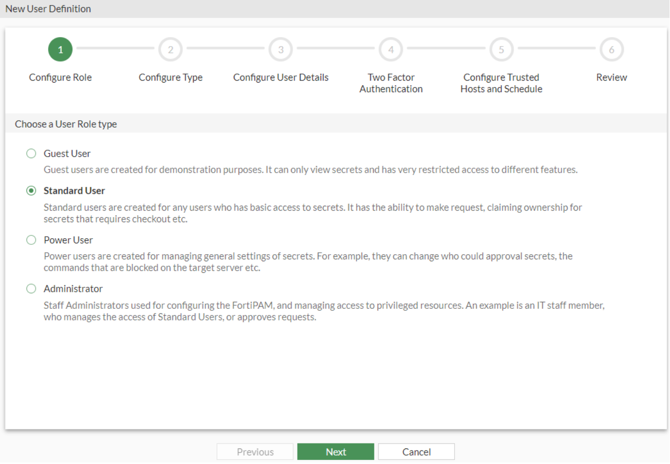
Remote Groups

Remote Server	Group Name
fortipam-saml-sso-server	

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*.



Choose a User Role type

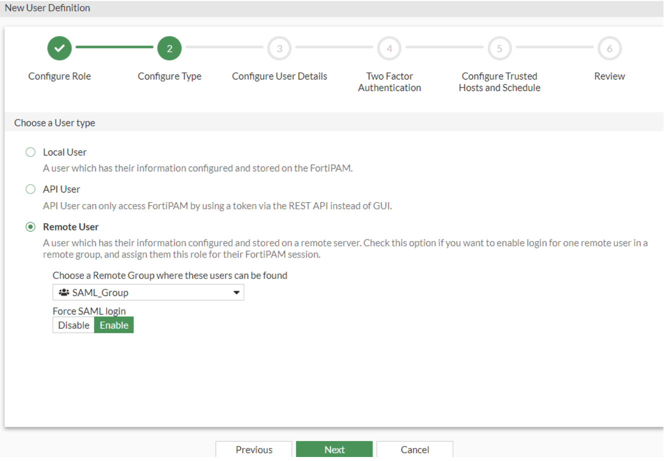
○ Guest User
Guest users are created for demonstration purposes. It can only view secrets and has very restricted access to different features.

● 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.

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*.



Choose a User type

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

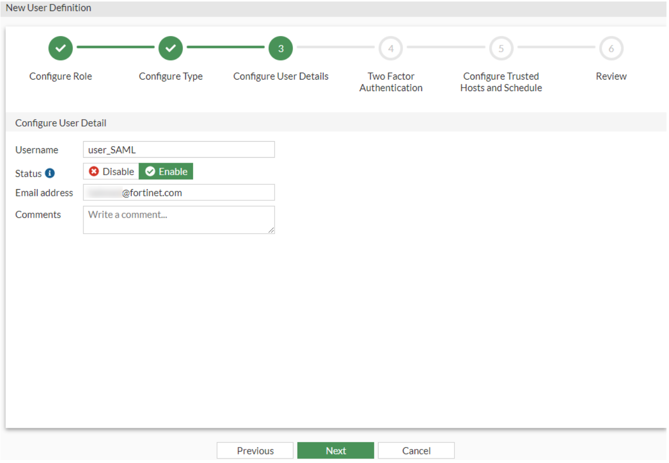
○ API User
API User can only access FortiPAM by using a token via the REST API instead of GUI.

● 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.

Choose a Remote Group where these users can be found: SAML_Group

Force SAML login: Disable [✓ Enable]

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.



New User Definition

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

Configure User Detail

Username: user_SAML

Status: Disable | ✓ Enable

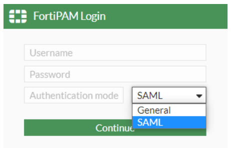
Email address: [redacted]@fortinet.com

Comments: Write a comment...

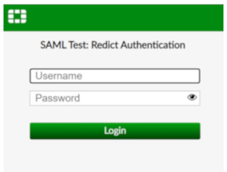
7. Click *Next*.
8. Disable *Two Factor Authentication*.
9. Click *Next*.
10. Click *Next*.
11. In the *Review* tab, verify the information you entered and click *Submit* to create the user.

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*.



A new SAML login page opens.



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.

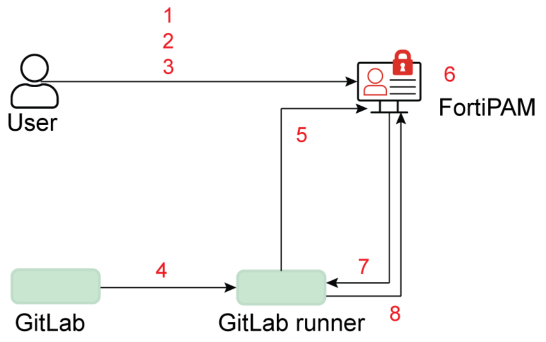
It provides the following advantages:

- 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 33
2. Integrating FortiPAM and Jenkins- CLI on page 36

Integrating FortiPAM and GitLab- GUI

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

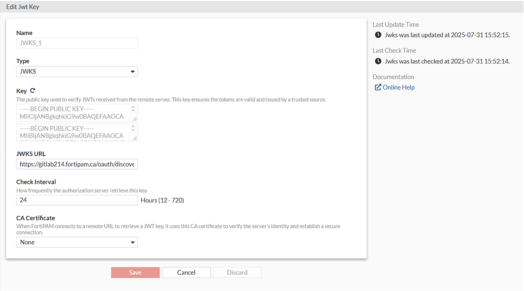
- ID Token Mode (GitLab recommended)
- Legacy `$CI_JOB_JWT`
- Terraform Mode

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*.



Edit Jwt Key

Name: JWKS_1

Type: JWKS

Key

The public key used to verify JWTs received from the remote server. This key ensures the tokens are valid and issued by a trusted source.

-----BEGIN PUBLIC KEY-----
MIICIjANBgkqhkiG9w0BAQEFAAOCA

-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCA

JWKS URL: https://gitlab214.fortipam.ca/oauth/discove

Check Interval

How frequently the authorization server retrieve this key.

24 Hours (12 - 720)

CA Certificate

When FortiPAM connects to a remote URL to retrieve a JWT key, it uses this CA certificate to verify the server's identity and establish a secure connection.

None

Last Update Time

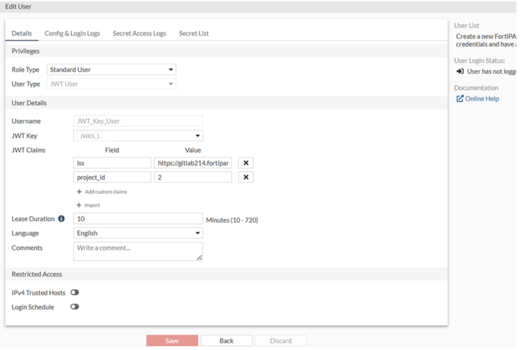
Jwks was last updated at 2025-07-31 15:52:15.

Last Check Time

Jwks was last checked at 2025-07-31 15:52:14.

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*.



Privileges

Role Type: Standard User

User Type: JWT User

User Details

Username: JWT_Key_User

JWT Key: JWKS_1

JWT Claims

Field	Value
iss	https://gitlab214.fortipar
project_id	2

Lease Duration: 10 Minutes (10 - 720)

Language: English

Comments: Write a comment...

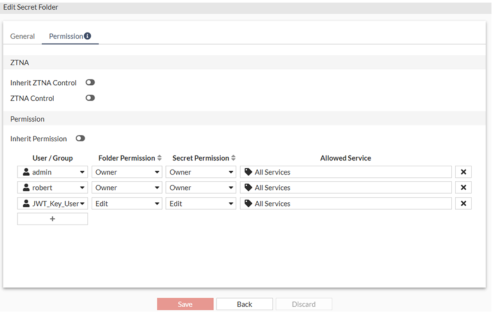
Restricted Access

IPv4 Trusted Hosts ○

Login Schedule ○

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*.



ZTNA

Inherit ZTNA Control ○

ZTNA Control ○

Permission

Inherit Permission ○

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_provides {
   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:

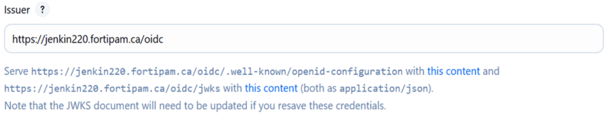
      ```
      sudo apt install curl
      ```

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`.

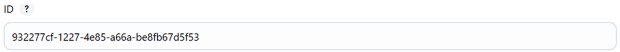
   

   Issuer ?

   https://jenkin220.fortipam.ca/oidc

   Serve `https://jenkin220.fortipam.ca/oidc/.well-known/openid-configuration` with this content and `https://jenkin220.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 ?

   932277cf-1227-4e85-a66a-be8fb67d5f53

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
```

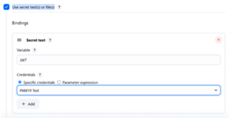
4. In the FortiPAM GUI, grant API user secret and folder permission.

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)*.



☑ Use secret text(s) or file(s)

Bindings

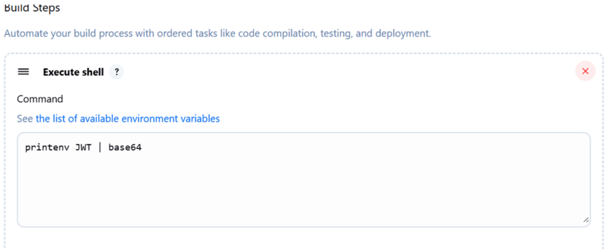
Secret text

Variable: JWT

Credentials: ● Specific credentials ○ Parameter expression

PAM19 Test

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.



Build Steps

Automate your build process with ordered tasks like code compilation, testing, and deployment.

Execute shell

Command

See the list of available environment variables

```
printenv JWT | base64
```

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:

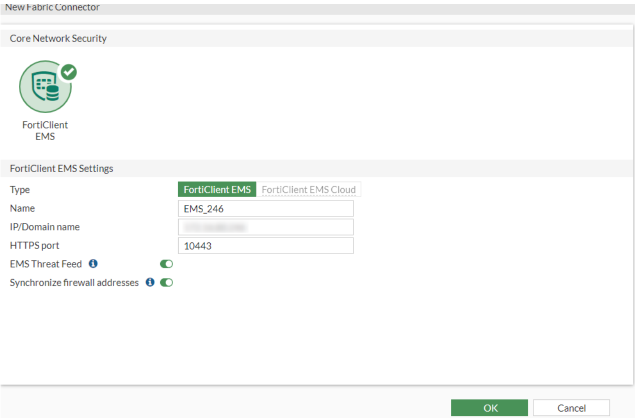
1. Configuring EMS on FortiPAM on page 39
2. Registering the endpoint PC to EMS server on page 41
3. Configuring a ZTNA server on FortiPAM on page 44
4. Configuring proxy rule on FortiPAM on page 45
5. Adding a ZTNA tag to a secret for launching control on page 46

Configuring EMS on FortiPAM

To configure EMS on FortiPAM:

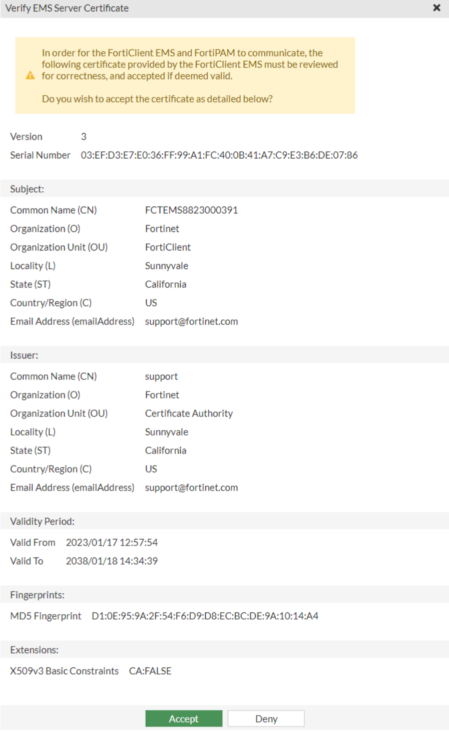
1. Go to *Network* > *Fabric Connectors*.
2. In the *Core Network Security pane*, select *FortiClient EMS* and then select *Edit*.
   The *New Fabric Connector* window opens.
3. In *Name*, enter a name of the FortiClient EMS connector.
4. In *IP/Domain name*, enter the IP address of the FortiClient EMS.
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*.



Type	FortiClient EMS / FortiClient EMS Cloud
Name	EMS_246
IP/Domain name	[redacted]
HTTPS port	10443
EMS Threat Feed	●
Synchronize firewall addresses	●

The *Verify EMS Server Certificate* window is displayed.



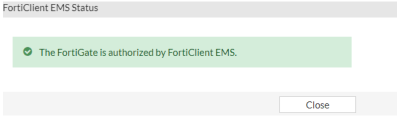
In order for the FortiClient EMS and FortiPAM to communicate, the following certificate provided by the FortiClient EMS must be reviewed for correctness, and accepted if deemed valid.

Do you wish to accept the certificate as detailed below?

Version	3
Serial Number	03:EF:D3:E7:E0:36:FF:99:A1:FC:40:0B:41:A7:C9:E3:B6:DE:07:86
Subject:	
Common Name (CN)	FCTEMS8823000391
Organization (O)	Fortinet
Organization Unit (OU)	FortiClient
Locality (L)	Sunnyvale
State (ST)	California
Country/Region (C)	US
Email Address (emailAddress)	support@fortinet.com
Issuer:	
Common Name (CN)	support
Organization (O)	Fortinet
Organization Unit (OU)	Certificate Authority
Locality (L)	Sunnyvale
State (ST)	California
Country/Region (C)	US
Email Address (emailAddress)	support@fortinet.com
Validity Period:	
Valid From	2023/01/17 12:57:54
Valid To	2038/01/18 14:34:39
Fingerprints:	
MD5 Fingerprint	D1:0E:95:9A:2F:54:F6:D9:D8:EC:BC:DE:9A:10:14:A4
Extensions:	
X509v3 Basic Constraints	CA:FALSE

8. Click *Accept*.

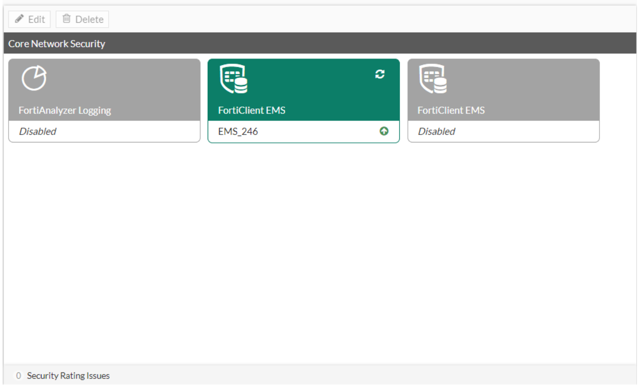
The *FortiClient EMS Status* pane is displayed.



The FortiGate is authorized by FortiClient EMS.

9. Click *Close*.

The FortiClient EMS is up.



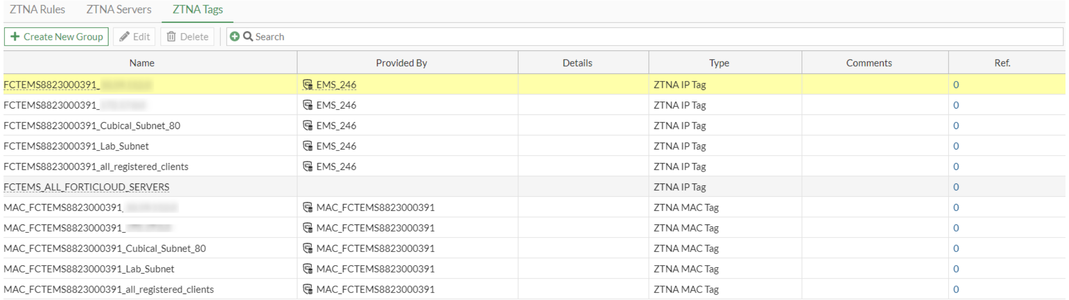
Error connecting to the EMS server

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.



Name	Provided By	Details	Type	Comments	Ref.
FCTEMS8823000391_[redacted]	EMS_246		ZTNA IP Tag		0
FCTEMS8823000391_[redacted]	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_[redacted]	MAC_FCTEMS8823000391		ZTNA MAC Tag		0
MAC_FCTEMS8823000391_[redacted]	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

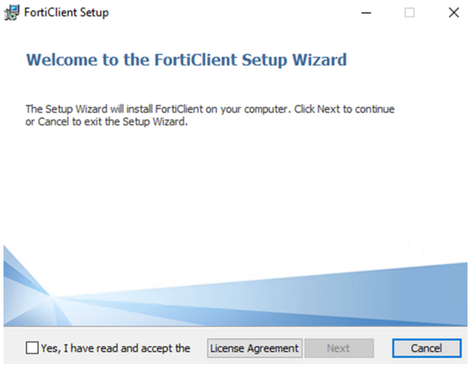
The endpoint PC is registered to the EMS server configured in Configuring EMS on FortiPAM on page 39.

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.

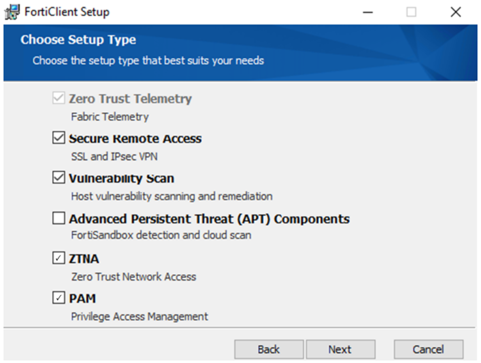


FortiClient Setup

Welcome to the FortiClient Setup Wizard

The Setup Wizard will install FortiClient on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

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*.



FortiClient Setup

Choose Setup Type

Choose the setup type that best suits your needs

☑ Zero Trust Telemetry
Fabric Telemetry

☑ **Secure Remote Access**
SSL and IPsec VPN

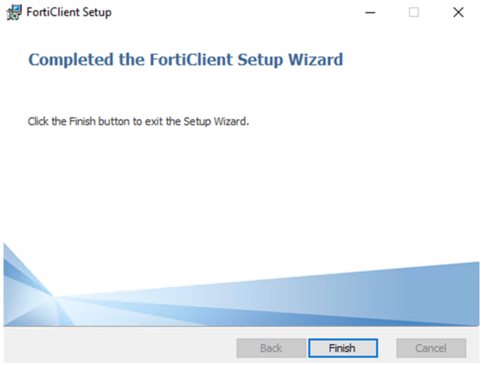
☑ **Vulnerability Scan**
Host vulnerability scanning and remediation

□ **Advanced Persistent Threat (APT) Components**
FortiSandbox detection and cloud scan

☑ **ZTNA**
Zero Trust Network Access

☑ **PAM**
Privilege Access Management

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



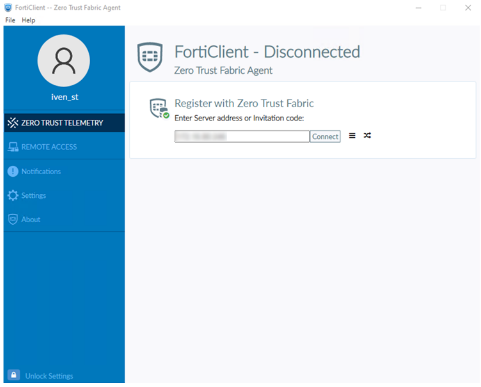
FortiClient Setup

Completed the FortiClient Setup Wizard

Click the Finish button to exit the Setup Wizard.

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

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



FortiClient -- Zero Trust Fabric Agent

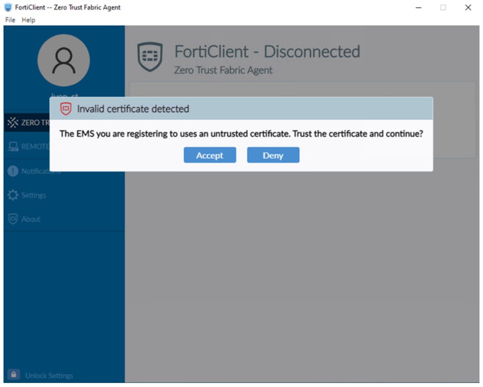
FortiClient - Disconnected

Zero Trust Fabric Agent

Register with Zero Trust Fabric

Enter Server address or Invitation code: [redacted]

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



FortiClient -- Zero Trust Fabric Agent

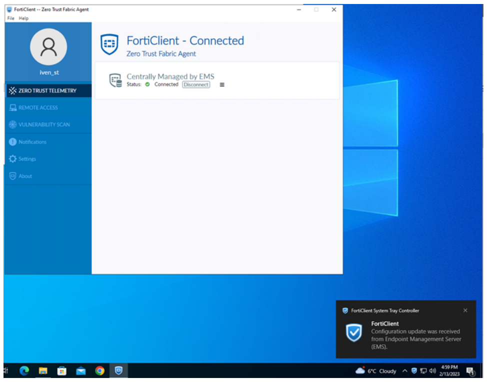
FortiClient - Disconnected

Zero Trust Fabric Agent

Invalid certificate detected

The EMS you are registering to uses an untrusted certificate. Trust the certificate and continue?

FortiClient is now connected to the EMS successfully.



FortiClient -- Zero Trust Fabric Agent

FortiClient - Connected

Zero Trust Fabric Agent

Centrally Managed by EMS

Status: Connected

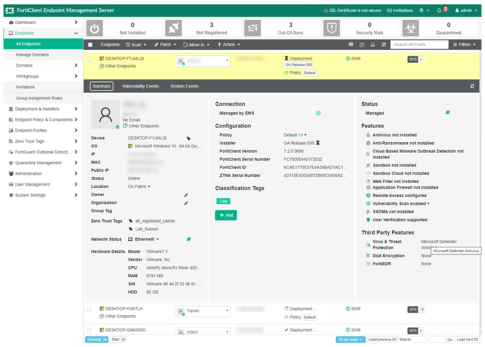
FortiClient System Tray Controller

FortiClient

Configuration update was received from Endpoint Management Server (EMS).

8. In the EMS server, go to *Endpoints > All Endpoints*.

The endpoint PC is tagged with zero trust tags.



0 Not Installed | 3 Not Registered | 3 Out-Of-Sync | 0 Security Risk | 0 Quarantined

DESKTOP-F1JMLQI — Other Endpoints — Deployment GA Release 690 — Policy Default — EMS — SYS 2

No Email
Other Endpoints

Device	DESKTOP-F1JMLQI
OS	Microsoft Windows 10 , 64-bit (bu...
IP	
MAC	
Public IP	
Status	Online
Location	On-Fabric
Owner	
Organization	
Group Tag	
Zero Trust Tags	all_registered_clients Lab_Subnet
Network Status	Ethernet0

Hardware Details		
	Model	VMware7,1
	Vendor	VMware, Inc.
	CPU	Intel(R) Xeon(R) Silver 420...
	RAM	8191 MB
	S/N	VMware-56 4d 2f 32 d6 8c ...
	HDD	85 GB

Connection
Managed by EMS

Configuration

Policy	Default
Installer	GA Release 690
FortiClient Version	7.2.0.0690
FortiClient Serial Number	FCT8000440173532
FortiClient ID	6CAE1770E57E4A39BAD1AC1...
ZTNA Serial Number	4D115E43034B73B60C0456A2...

Classification Tags
Low

Status
Managed

Features
Antivirus not installed
Anti-Ransomware not installed
Cloud Based Malware Outbreak Detection not installed
Sandbox not installed
Sandbox Cloud not installed
Web Filter not installed
Application Firewall not installed
Remote Access configured
Vulnerability Scan enabled
SSOMA not installed
User Verification supported

Third Party Features

Virus & Threat Protection	Microsoft Defender Antivirus
Disk Encryption	None
FortiEDR	None

DESKTOP-FMII7LH — Other Endpoints — Tianlei — Deployment ... — Policy Default — EMS — SYS 12

DESKTOP-GNIM33O — robert — Deployment ... — EMS — SYS 2

Configuring a ZTNA server on FortiPAM

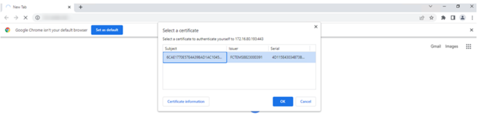
To configure a ZTNA server on FortiPAM:

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.



Select a certificate

Select a certificate to authenticate yourself to 172.16.80.193:443

Subject	Issuer	Serial
6CAE1770E57E4A39BAD1AC1045...	FCTEMS8823000391	4D115E43034B738...

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.

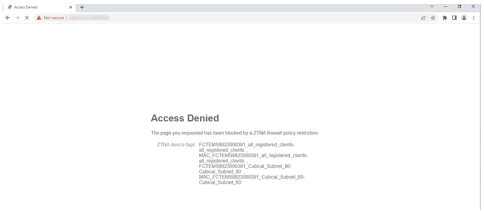
To configure a proxy rule on FortiPAM:

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.



Access Denied

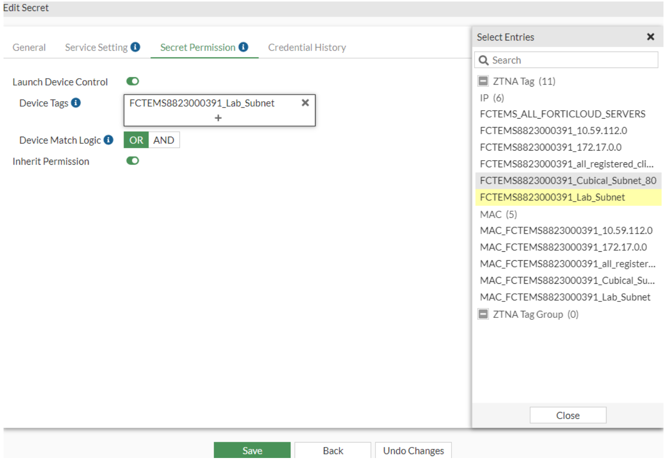
The page you requested has been blocked by a ZTNA firewall policy restriction.

ZTNA device tags: FCTEMS8823000391_all_registered_clients-all_registered_clients: , MAC_FCTEMS8823000391_all_registered_clients-all_registered_clients: , FCTEMS8823000391_Cubical_Subnet_80-Cubical_Subnet_80: , MAC_FCTEMS8823000391_Cubical_Subnet_80-Cubical_Subnet_80:

Adding a ZTNA tag to a secret for launching control

To add a ZTNA tag to a secret:

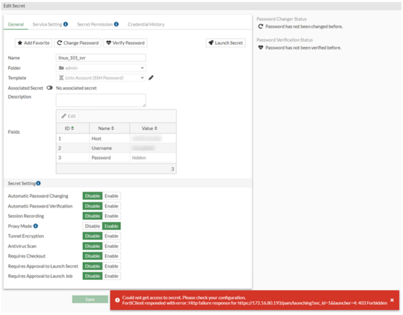
1. Go to *Secrets > Secret List*.
2. In the *Secrets List*, double-click a secret to open.
3. Go to the *Secret Permission* tab.
4. Enable *ZTNA Control* to limit the permission of launching by `ztna-ems-tag`:
    a. In *Device Tags*, select *+*; from *Select Entries*, select *FCTEMS8823000391_Lab_Subnet*.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



Launch Device Control: ●
Device Tags: FCTEMS8823000391_Lab_Subnet ✕ +
Device Match Logic: [✓ OR] AND
Inherit Permission: ●

ZTNA Tag (11)
IP (6)
FCTEMS_ALL_FORTICLOUD_SERVERS
FCTEMS8823000391_10.59.112.0
FCTEMS8823000391_172.17.0.0
FCTEMS8823000391_all_registered_cli...
FCTEMS8823000391_Cubical_Subnet_80
FCTEMS8823000391_Lab_Subnet
MAC (5)
MAC_FCTEMS8823000391_10.59.112.0
MAC_FCTEMS8823000391_172.17.0.0
MAC_FCTEMS8823000391_all_register...
MAC_FCTEMS8823000391_Cubical_Su...
MAC_FCTEMS8823000391_Lab_Subnet
ZTNA Tag Group (0)

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



Password Changer Status
Password has not been changed before.
Password Verification Status
Password has not been verified before.

Name: linux_101_svr
Folder: admin
Template: Unix Account (SSH Password)
Associated Secret: No associated secret
Description:

Fields:

ID	Name	Value
1	Host	[redacted]
2	Username	[redacted]
3	Password	hidden

3

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
Requires Checkout	[✓ Disable]	Enable
Requires Approval to Launch Secret	[✓ Disable]	Enable
Requires Approval to Launch Job	[✓ Disable]	Enable

```
Could not get access to secret. Please check your configuration.
FortiClient responded with error: Http failure response for https://172.16.80.193/pam/launching?sec_id=1&launcher=4: 403 Forbidden
```

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:

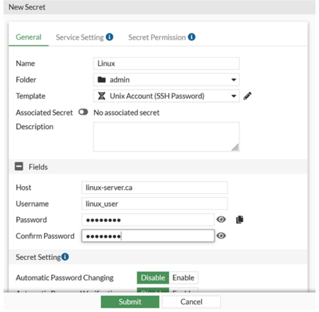
1. Creating a secret with Unix template on page 47
2. Launching a secret for the Linux server on page 48

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*.



Name: Linux
Folder: admin
Template: Unix Account (SSH Password)
Associated Secret: No associated secret
Description:
Host: linux-server.ca
Username: linux_user
Password: ••••••••
Confirm Password: ••••••••
Automatic Password Changing: Disable | Enable

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:

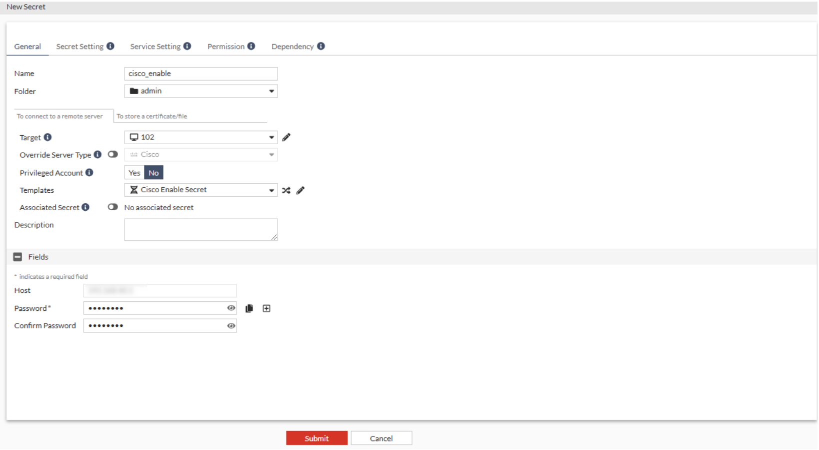
1. Creating an associated secret on page 48
2. Creating a secret with Cisco User (SSH Secret) template on page 49
3. Launching a secret for the Cisco router on page 51

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*.



Name: cisco_enable
Folder: admin

Target: 102
Override Server Type: Cisco
Privileged Account: Yes [✓ No]
Templates: Cisco Enable Secret
Associated Secret: No associated secret
Description:

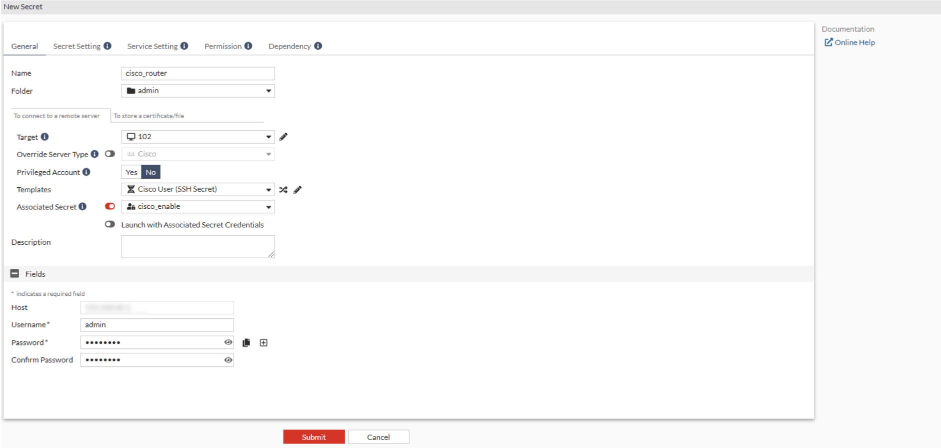
* indicates a required field
Host: [redacted]
Password*: ••••••••
Confirm Password: ••••••••

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.



New Secret

General | Secret Setting | Service Setting | Permission | Dependency

Name: cisco_router
Folder: admin

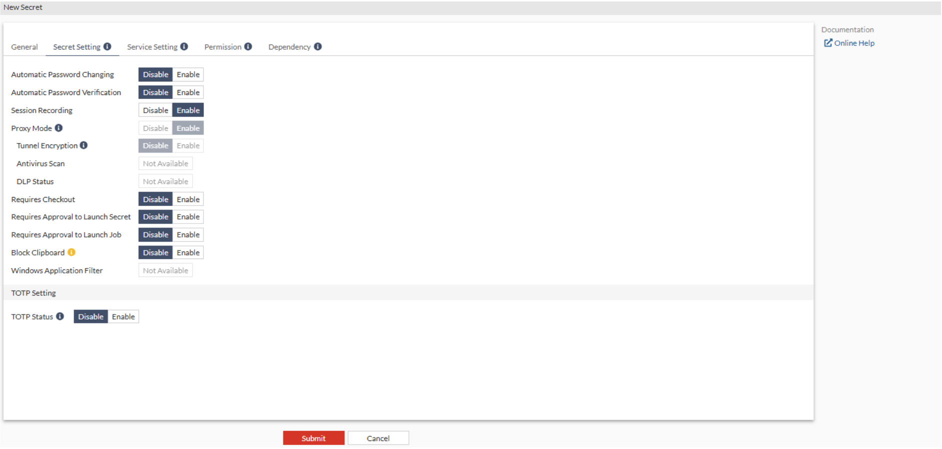
To connect to a remote server | To store a certificate/file

Target: 102
Override Server Type: Cisco
Privileged Account: Yes [✓ No]
Templates: Cisco User (SSH Secret)
Associated Secret: cisco_enable
Launch with Associated Secret Credentials
Description:

Fields

* indicates a required field
Host: [redacted]
Username*: admin
Password*: ••••••••
Confirm Password: ••••••••

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



New Secret

General | Secret Setting | Service Setting | Permission | Dependency

Automatic Password Changing: [✓ Disable] Enable
Automatic Password Verification: [✓ Disable] Enable
Session Recording: 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

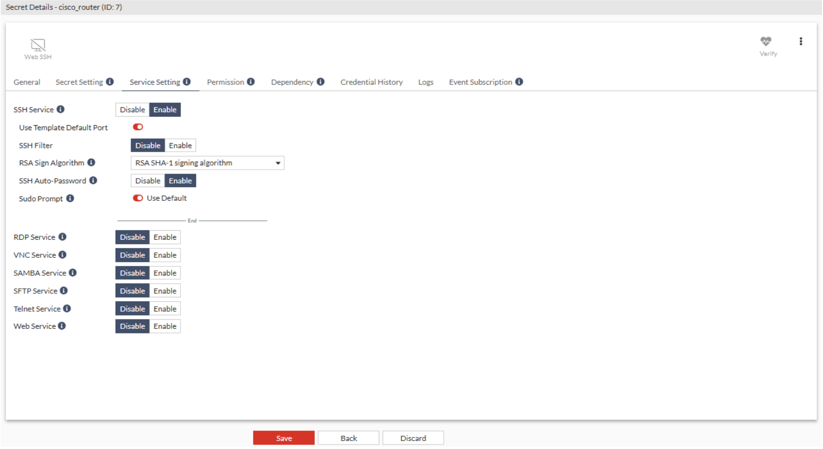
TOTP Setting

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.

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



Secret Details - cisco_router (ID: 7)

SSH Service: Enable
Use Template Default Port: ●
SSH Filter: Disable
RSA Sign Algorithm: RSA SHA-1 signing algorithm
SSH Auto-Password: Enable
Sudo Prompt: ● Use Default

RDP Service: Disable
VNC Service: Disable
SAMBA Service: Disable
SFTP Service: Disable
Telnet Service: Disable
Web Service: Disable

12. Click *Submit*.

Verifying the password

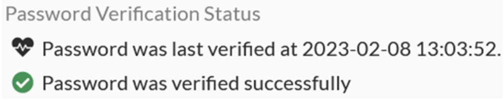
To verify the password manually:

1. Go to *Secrets* > *Secrets*.
2. 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.
3. 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

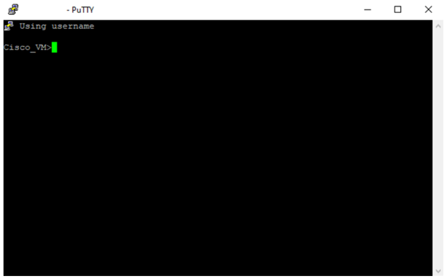
To launch a secret for the Cisco router:

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

   Alternatively, right-click the secret and then select *Launch Secret*.
2. 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.



```
Using username

Cisco_VM>
```

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:

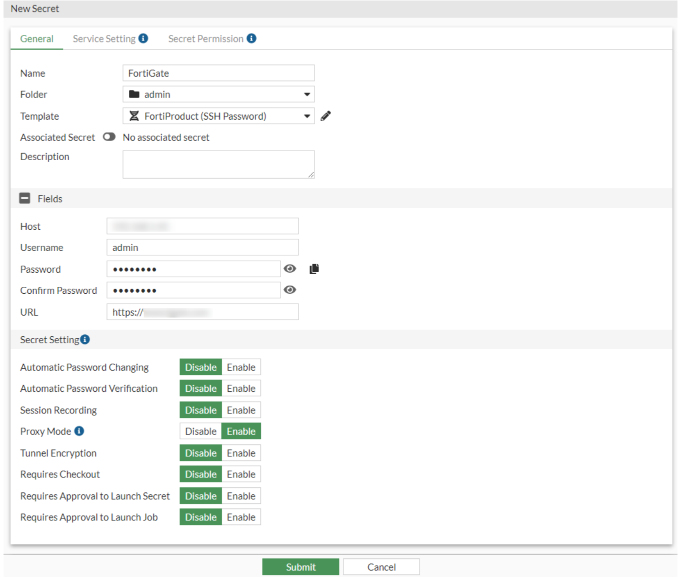
1. Creating a secret with Unix template on page 52
2. Launching a secret for the FortiGate on page 53

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*.



New Secret

Name	FortiGate
Folder	admin
Template	FortiProduct (SSH Password)
Associated Secret	No associated secret
Description	

Fields

Host	[redacted]
Username	admin
Password	••••••••
Confirm Password	••••••••
URL	https://[redacted]

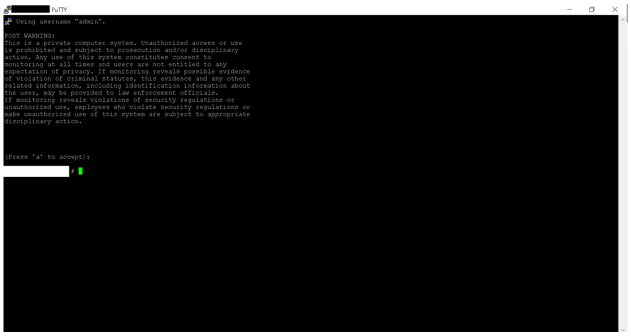
Secret Setting

Automatic Password Changing	Disable
Automatic Password Verification	Disable
Session Recording	Disable
Proxy Mode	Enable
Tunnel Encryption	Disable
Requires Checkout	Disable
Requires Approval to Launch Secret	Disable
Requires Approval to Launch Job	Disable

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.



[redacted] PuTTY

```
Using username "admin".

POST WARNING:
This is a private computer system. Unauthorized access or use
is prohibited and subject to prosecution and/or disciplinary
action. Any use of this system constitutes consent to
monitoring at all times and users are not entitled to any
expectation of privacy. If monitoring reveals possible evidence
of violation of criminal statutes, this evidence and any other
related information, including identification information about
the user, may be provided to law enforcement officials.
If monitoring reveals violations of security regulations or
unauthorized use, employees who violate security regulations or
make unauthorized use of this system are subject to appropriate
disciplinary action.



(Press 'a' to accept):
[redacted] #
```

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.

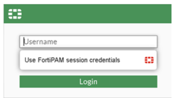
A new browser tab opens. You can now access FortiGate using Web SSH.

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:

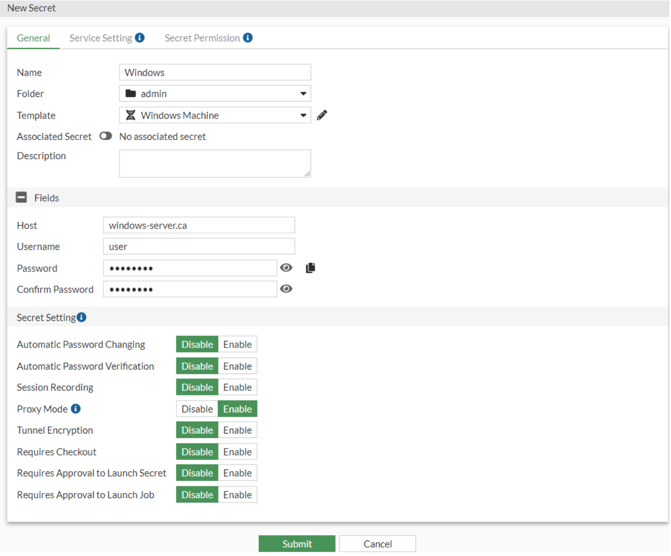
1. Creating a secret with Windows Machine template on page 54
2. Launching a secret for the Windows server on page 55

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*.



New Secret

General | Service Setting | Secret Permission

Name: Windows
Folder: admin
Template: Windows Machine
Associated Secret: No associated secret
Description:

Fields

Host: windows-server.ca
Username: user
Password: ••••••••
Confirm Password: ••••••••

Secret Setting

Automatic Password Changing: [✓ Disable] Enable
Automatic Password Verification: [✓ Disable] Enable
Session Recording: [✓ Disable] Enable
Proxy Mode: Disable [✓ Enable]
Tunnel Encryption: [✓ Disable] Enable
Requires Checkout: [✓ Disable] Enable
Requires Approval to Launch Secret: [✓ Disable] Enable
Requires Approval to Launch Job: [✓ Disable] Enable

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:

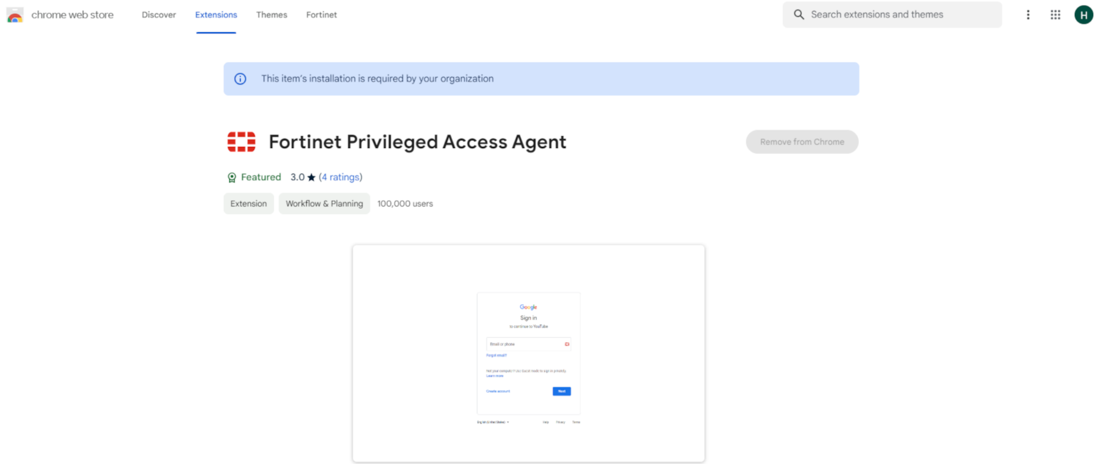
1. Installing Fortinet Privileged Access Agent web extension on Chrome/Edge on page 56
2. Creating a secret for general web application/platform on page 57
3. Creating a secret for AWS root/IAM account on page 57
4. Visiting web application/platform using web launcher on page 59
5. Reviewing video recording 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.

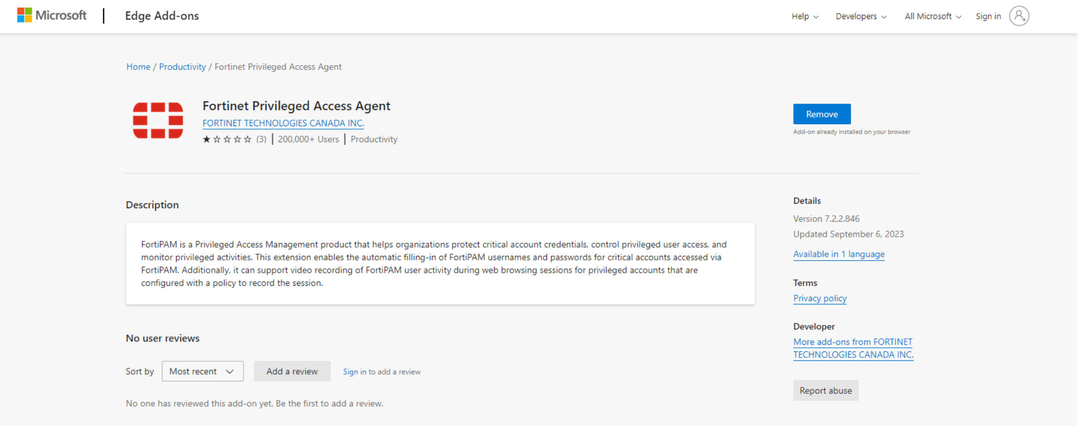
To install Fortinet Privileged Access Agent web extension on Chrome/Edge:

1. For the Chrome browser:
   1. Look for FortiPAM on the Chrome Web Store.
   2. Click *Add to Chrome* on the *Fortinet Privileged Access Agent* page to install the FortiPAM extension.



This item's installation is required by your organization

2. For the Edge browser:
   1. Look for FortiPAM on Microsoft Edge Add-ons.
   2. Click *Get* on the *Fortinet Privileged Access Agent* page to install the FortiPAM extension.


Microsoft | Edge Add-ons
Help
Developers
All Microsoft
Sign in
Home / Productivity / Fortinet Privileged Access Agent
Fortinet Privileged Access Agent
FORTINET TECHNOLOGIES CANADA INC.
★ ☆ ☆ ☆ ☆ (3) | 200,000+ Users | Productivity
Remove
Description
Details
Terms
Privacy policy
Developer
More add-ons from FORTINET TECHNOLOGIES CANADA INC.
Report abuse
No user reviews
Sort by
Most recent
Add a review
Sign in to add a review

Add-on already installed on your browser

FortiPAM is a Privileged Access Management product that helps organizations protect critical account credentials, control privileged user access, and monitor privileged activities. This extension enables the automatic filling-in of FortiPAM usernames and passwords for critical accounts accessed via FortiPAM. Additionally, it can support video recording of FortiPAM user activity during web browsing sessions for privileged accounts that are configured with a policy to record the session.

Version 7.2.2.846

Updated September 6, 2023

Available in 1 language

No one has reviewed this add-on yet. Be the first to add a review.

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.

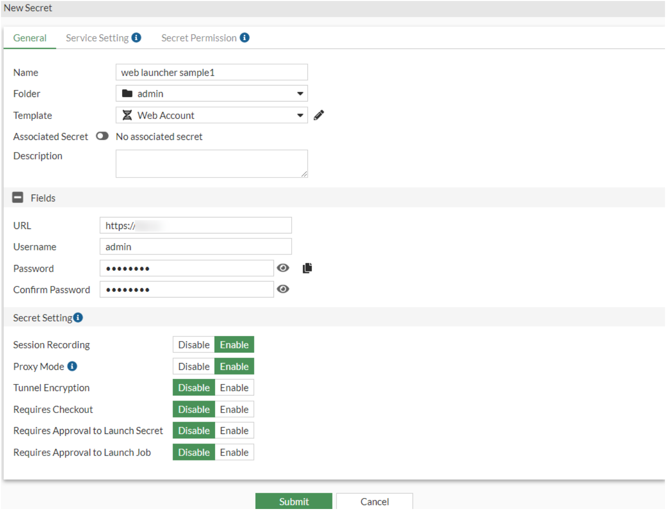
      Note: The URL must start with either `http://` or `https://`.

   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*



Name: web launcher sample1

Folder: admin

Template: Web Account

Associated Secret: No associated secret

Description:

URL: https://

Username: admin

Password: ••••••••

Confirm Password: ••••••••

Secret Setting

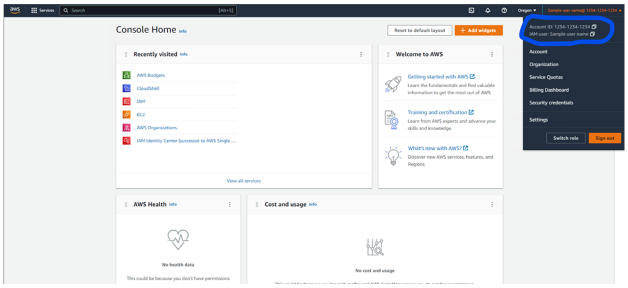
Session Recording	Disable [✓ Enable]
Proxy Mode	Disable [✓ Enable]
Tunnel Encryption	[✓ Disable] Enable
Requires Checkout	[✓ Disable] Enable
Requires Approval to Launch Secret	[✓ Disable] Enable
Requires Approval to Launch Job	[✓ Disable] Enable

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:
   1. 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.
   2. In the *Username* field, enter the username for AWS.
   3. In the *Password* field, enter the password for AWS.
   4. In the *Confirm Password* field that appears after the password is filled in, enter the password again.
   5. 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 `-`.



Learn the fundamentals and find valuable information to get the most out of AWS.

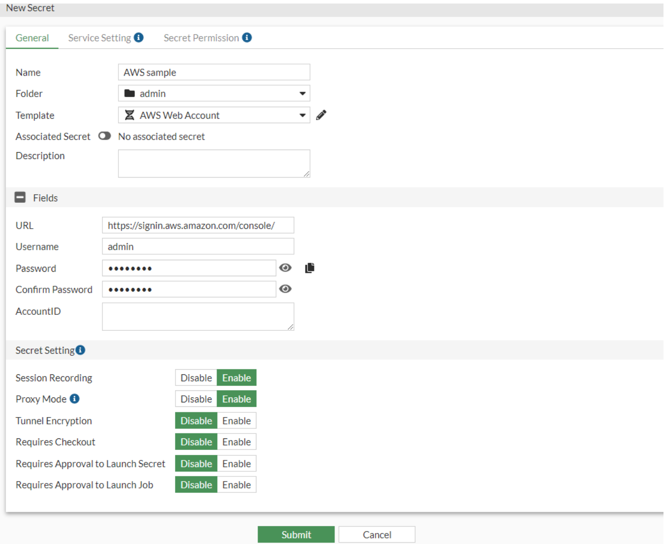
Learn from AWS experts and advance your skills and knowledge.

Discover new AWS services, features, and Regions.

This could be because you don't have permissions

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

9. Click *Submit*.



New Secret

Name: AWS sample
Folder: admin
Template: AWS Web Account
Associated Secret: No associated secret
Description:

Fields

URL: https://signin.aws.amazon.com/console/
Username: admin
Password: ••••••••
Confirm Password: ••••••••
AccountID:

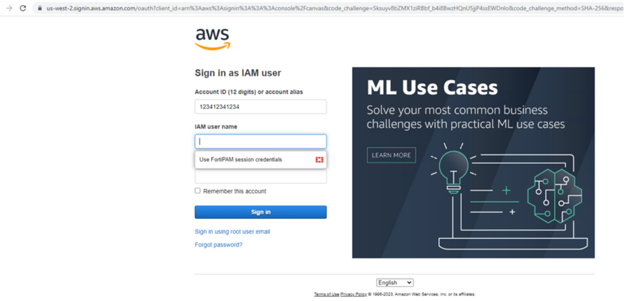
Secret Setting

Session Recording	Disable [✓ Enable]
Proxy Mode	Disable [✓ Enable]
Tunnel Encryption	[✓ Disable] Enable
Requires Checkout	[✓ Disable] Enable
Requires Approval to Launch Secret	[✓ Disable] Enable
Requires Approval to Launch Job	[✓ Disable] Enable

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.



us-west-2.signin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code_challenge=5ksuyv8bZMX1ziRBbf_b4i8BwzHQnU5jjP4ssEWDnlo&code_challenge_method=SHA-256&respo

Sign in as IAM user

Account ID (12 digits) or account alias: 123412341234

IAM user name:

aws
Use FortiPAM session credentials
□ Remember this account
Sign in
Sign in using root user email
Forgot password?
ML Use Cases
Solve your most common business challenges with practical ML use cases
LEARN MORE
English

Terms of Use Privacy Policy © 1996-2023, Amazon Web Services, Inc. or its affiliates.

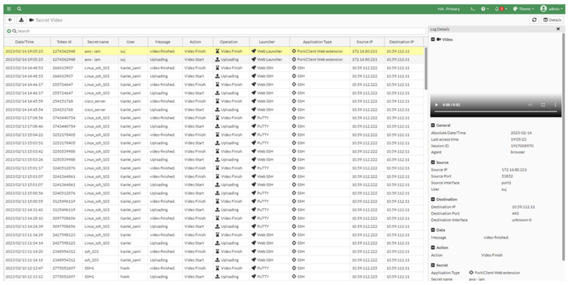
2. In the login page, click the *IAM user name/Password* fields, click *Use FortiPAM session credentials* to fill in the credentials, and click *Sign in*.

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.



Date/Time	Token Id	Secret name	User	Message	Action	Operation	Launcher	Application Type	Source IP	Destination IP
2023/02/14 19:05:23	1274362948	aws - iam	suj	video-finished.	Video Finish	Video Finish	Web Launcher	FortiClient Web extension	172.16.80.221	10.59.112.11
2023/02/14 19:05:23	1274362948	aws - iam	suj	Uploading.	Video Start	Uploading	Web Launcher	FortiClient Web extension	172.16.80.221	10.59.112.11
2023/02/14 14:48:53	266013907	Linux_ssh_103	tianlei_saml	video-finished.	Video Finish	Video Finish	Web SSH	SSH	10.59.112.222	10.59.112.11
2023/02/14 14:48:53	266013907	Linux_ssh_103	tianlei_saml	Uploading.	Video Start	Uploading	Web SSH	SSH	10.59.112.222	10.59.112.11
2023/02/14 14:46:17	255724647	Linux_ssh_103	tianlei_saml	video-finished.	Video Finish	Video Finish	Web SSH	SSH	10.59.112.222	10.59.112.11
2023/02/14 14:46:17	255724647	Linux_ssh_103	tianlei_saml	Uploading.	Video Start	Uploading	Web SSH	SSH	10.59.112.222	10.59.112.11
2023/02/14 14:45:59	254151768	cisco_server	tianlei_saml	video-finished.	Video Finish	Video Finish	Web SSH	SSH	10.59.112.222	10.59.112.11
2023/02/14 14:45:54	254151768	cisco_server	tianlei_saml	Uploading.	Video Start	Uploading	Web SSH	SSH	10.59.112.222	10.59.112.11
2023/02/13 17:08:56	3743440754	Linux_ssh_103	tianlei_saml	video-finished.	Video Finish	Video Finish	PuTTY	SSH	10.59.112.222	10.59.112.11
2023/02/13 17:08:46	3743440754	Linux_ssh_103	tianlei_saml	Uploading.	Video Start	Uploading	PuTTY	SSH	10.59.112.222	10.59.112.11
2023/02/13 15:04:22	3252178405	Linux_ssh_103	tianlei_saml	video-finished.	Video Finish	Video Finish	PuTTY	SSH	10.59.112.222	10.59.112.11
2023/02/13 15:03:51	3252178405	Linux_ssh_103	tianlei_saml	Uploading.	Video Start	Uploading	PuTTY	SSH	10.59.112.222	10.59.112.11
2023/02/13 15:03:42	3250539988	Linux_ssh_103	tianlei_saml	video-finished.	Video Finish	Video Finish	Web SSH	SSH	10.59.112.222	10.59.112.11
2023/02/13 15:03:26	3250539988	Linux_ssh_103	tianlei_saml	Uploading.	Video Start	Uploading	Web SSH	SSH	10.59.112.222	10.59.112.11
2023/02/13 15:01:17	3240512876	Linux_ssh_103	tianlei_saml	video-finished.	Video Finish	Video Finish	PuTTY	SSH	10.59.112.222	10.59.112.11
2023/02/13 15:01:07	3241364861	Linux_ssh_103	tianlei_saml	video-finished.	Video Finish	Video Finish	Web SSH	SSH	10.59.112.222	10.59.112.11
2023/02/13 15:01:07	3241364861	Linux_ssh_103	tianlei_saml	Uploading.	Video Start	Uploading	Web SSH	SSH	10.59.112.222	10.59.112.11
2023/02/13 15:00:56	3240512876	Linux_ssh_103	tianlei_saml	Uploading.	Video Start	Uploading	PuTTY	SSH	10.59.112.222	10.59.112.11
2023/02/13 15:00:55	3125496119	Linux_ssh_103	tianlei_saml	video-finished.	Video Finish	Video Finish	PuTTY	SSH	10.59.112.222	10.59.112.11
2023/02/13 14:31:42	3125496119	Linux_ssh_103	tianlei_saml	Uploading.	Video Start	Uploading	PuTTY	SSH	10.59.112.222	10.59.112.11
2023/02/13 14:28:10	3097708656	Linux_ssh_103	tianlei_saml	video-finished.	Video Finish	Video Finish	PuTTY	SSH	10.59.112.222	10.59.112.11
2023/02/13 14:24:39	3097708656	Linux_ssh_103	tianlei_saml	Uploading.	Video Start	Uploading	PuTTY	SSH	10.59.112.222	10.59.112.11
2023/02/13 11:34:29	2427598123	Linux_ssh_103	tianlei	video-finished.	Video Finish	Video Finish	Web SSH	SSH	10.59.112.222	10.59.112.11
2023/02/13 11:34:14	2427598123	Linux_ssh_103	tianlei	Uploading.	Video Start	Uploading	Web SSH	SSH	10.59.112.222	10.59.112.11
2023/02/13 11:14:20	2348954312	ssh_103	tianlei_saml	video-finished.	Video Finish	Video Finish	Web SSH	SSH	10.59.112.222	10.59.112.11
2023/02/13 11:14:15	2348954312	ssh_103	tianlei_saml	Uploading.	Video Start	Uploading	Web SSH	SSH	10.59.112.222	10.59.112.11
2023/02/10 12:13:47	2775052697	SSH1	frank	video-finished.	Video Finish	Video Finish	PuTTY	SSH	10.59.112.225	10.59.112.11
2023/02/10 12:13:12	2775052697	SSH1	frank	Uploading.	Video Start	Uploading	PuTTY	SSH	10.59.112.225	10.59.112.11

General

Absolute Date/Time	2023-02-14
Last access time	19:05:23
Session ID	1917008970
Agent	browser

Source

Source IP	172.16.80.221
Source Port	53852
Source Interface	port1
User	suj

Destination

Destination IP	10.59.112.11
Destination Port	443
Destination Interface	unknown-0

Data

Message	video-finished.

Action

Action	Video Finish

Secret

Application Type	FortiClient Web extension
Secret name	aws - iam

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.

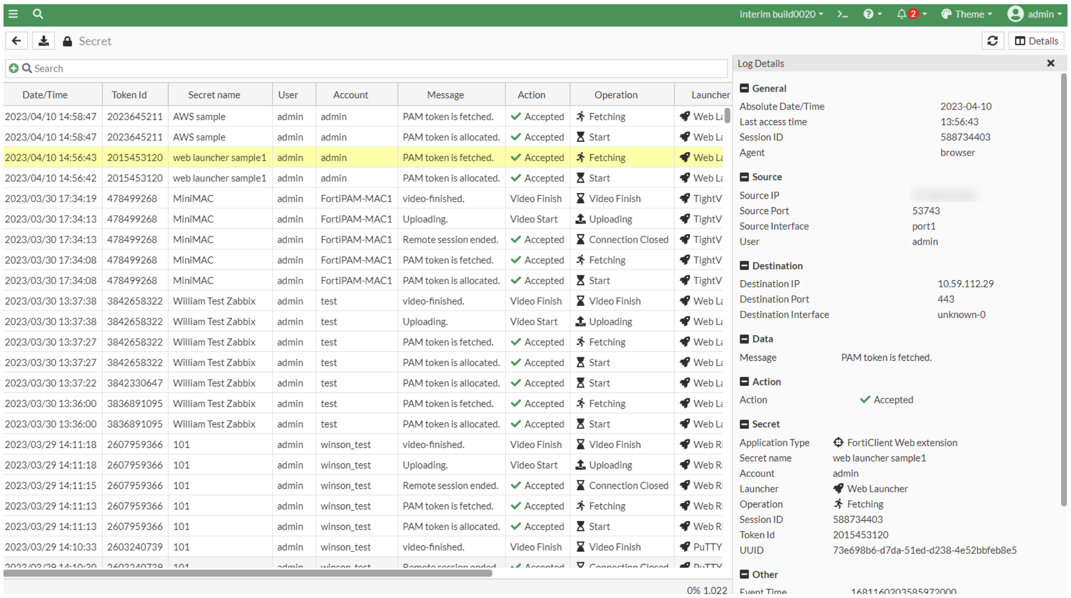
Reviewing secret log for the web launching session

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.



Date/Time	Token Id	Secret name	User	Account	Message	Action	Operation	Launcher
2023/04/10 14:58:47	2023645211	AWS sample	admin	admin	PAM token is fetched.	✓ Accepted	Fetching	Web La
2023/04/10 14:58:47	2023645211	AWS sample	admin	admin	PAM token is allocated.	✓ Accepted	Start	Web La
2023/04/10 14:56:43	2015453120	web launcher sample1	admin	admin	PAM token is fetched.	✓ Accepted	Fetching	Web La
2023/04/10 14:56:42	2015453120	web launcher sample1	admin	admin	PAM token is allocated.	✓ Accepted	Start	Web La
2023/03/30 17:34:19	478499268	MiniMAC	admin	FortiPAM-MAC1	video-finished.	Video Finish	Video Finish	TightV
2023/03/30 17:34:13	478499268	MiniMAC	admin	FortiPAM-MAC1	Uploading.	Video Start	Uploading	TightV
2023/03/30 17:34:13	478499268	MiniMAC	admin	FortiPAM-MAC1	Remote session ended.	✓ Accepted	Connection Closed	TightV
2023/03/30 17:34:08	478499268	MiniMAC	admin	FortiPAM-MAC1	PAM token is fetched.	✓ Accepted	Fetching	TightV
2023/03/30 17:34:08	478499268	MiniMAC	admin	FortiPAM-MAC1	PAM token is allocated.	✓ Accepted	Start	TightV
2023/03/30 13:37:38	3842658322	William Test Zabbix	admin	test	video-finished.	Video Finish	Video Finish	Web La
2023/03/30 13:37:38	3842658322	William Test Zabbix	admin	test	Uploading.	Video Start	Uploading	Web La
2023/03/30 13:37:27	3842658322	William Test Zabbix	admin	test	PAM token is fetched.	✓ Accepted	Fetching	Web La
2023/03/30 13:37:27	3842658322	William Test Zabbix	admin	test	PAM token is allocated.	✓ Accepted	Start	Web La
2023/03/30 13:37:22	3842330647	William Test Zabbix	admin	test	PAM token is allocated.	✓ Accepted	Start	Web La
2023/03/30 13:36:00	3836891095	William Test Zabbix	admin	test	PAM token is fetched.	✓ Accepted	Fetching	Web La
2023/03/30 13:36:00	3836891095	William Test Zabbix	admin	test	PAM token is allocated.	✓ Accepted	Start	Web La
2023/03/29 14:11:18	2607959366	101	admin	winson_test	video-finished.	Video Finish	Video Finish	Web R
2023/03/29 14:11:18	2607959366	101	admin	winson_test	Uploading.	Video Start	Uploading	Web R
2023/03/29 14:11:15	2607959366	101	admin	winson_test	Remote session ended.	✓ Accepted	Connection Closed	Web R
2023/03/29 14:11:13	2607959366	101	admin	winson_test	PAM token is fetched.	✓ Accepted	Fetching	Web R
2023/03/29 14:11:13	2607959366	101	admin	winson_test	PAM token is allocated.	✓ Accepted	Start	Web R
2023/03/29 14:10:33	2603240739	101	admin	winson_test	video-finished.	Video Finish	Video Finish	PuTTY
2023/03/29 14:10:30	2603240739	101	admin	winson_test	Remote session ended.	✓ Accepted	Connection Closed	PuTTY

0% 1,022

Log Details

General

Absolute Date/Time	2023-04-10
Last access time	13:56:43
Session ID	588734403
Agent	browser

Source

Source IP	[redacted]
Source Port	53743
Source Interface	port1
User	admin

Destination

Destination IP	10.59.112.29
Destination Port	443
Destination Interface	unknown-0

Data

Message	PAM token is fetched.

Action

Action	✓ Accepted

Secret

Application Type	FortiClient Web extension
Secret name	web launcher sample1
Account	admin
Launcher	Web Launcher
Operation	Fetching
Session ID	588734403
Token Id	2015453120
UUID	73e698b6-d7da-51ed-d238-4e52bbfeb8e5

Other

Event Time	1681160203585972000

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:

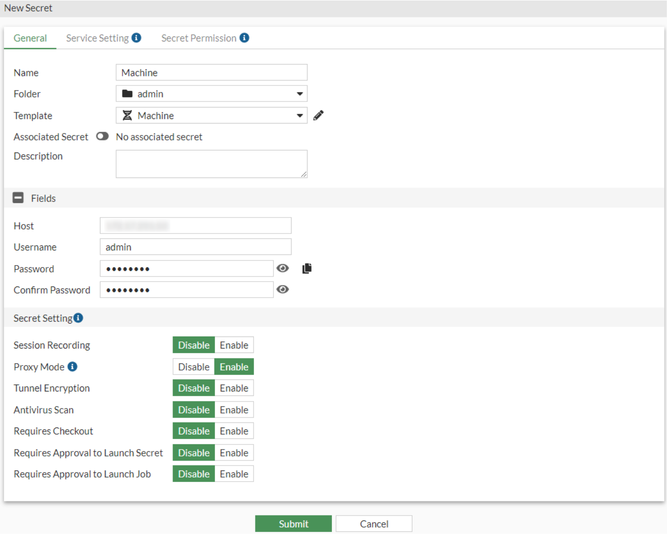
1. Creating a secret with Machine template on page 61
2. Launching a secret for the machine on page 62

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*.



Name	Machine
Folder	admin
Template	Machine
Associated Secret	No associated secret
Description	

Host	[redacted]
Username	admin
Password	••••••••
Confirm Password	••••••••

Session Recording	[✓ Disable] Enable
Proxy Mode ℹ	Disable [✓ Enable]
Tunnel Encryption	[✓ Disable] Enable
Antivirus Scan	[✓ Disable] Enable
Requires Checkout	[✓ Disable] Enable
Requires Approval to Launch Secret	[✓ Disable] Enable
Requires Approval to Launch Job	[✓ Disable] Enable

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.

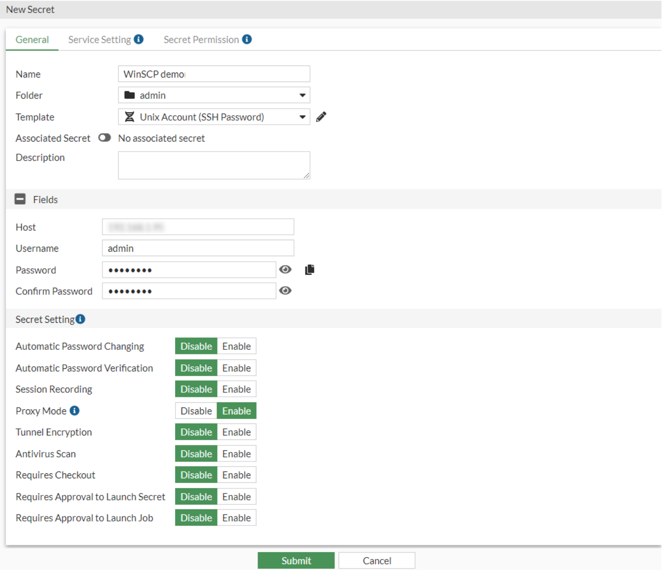
   In the *Fields* pane, when *Unix Account (SSH Key)* is selected as the template:
   a. In the *Host* field, enter the IP address or the FQDN of the target server.
   b. In the *Username* field, enter the username for the target server.
   c. In *Public-key*, select from *File Upload*, *Text*, or *Generate*.
      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*.



New Secret

General | Service Setting | Secret Permission

Name	WinSCP demo
Folder	admin
Template	Unix Account (SSH Password)
Associated Secret	No associated secret
Description	

Fields

Host	[redacted]
Username	admin
Password	••••••••
Confirm Password	••••••••

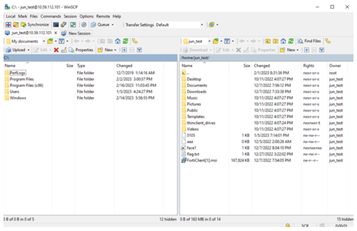
Secret Setting

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
Requires Checkout	[✓ Disable] Enable
Requires Approval to Launch Secret	[✓ Disable] Enable
Requires Approval to Launch Job	[✓ Disable] Enable

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:
   1. In the *Host* field, enter the IP address or the FQDN of the SFTP server.
   2. In the *Username* field, enter the username for the SFTP server.
   3. In the *Password* field, enter the password for the SFTP server.

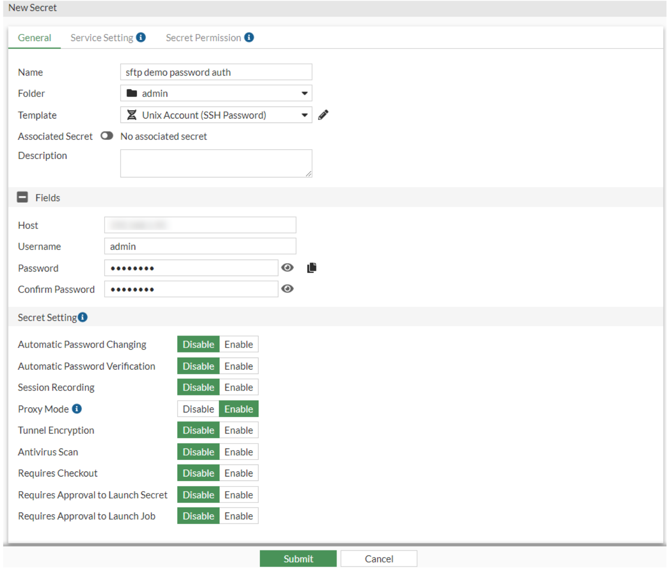
   In the *Fields* pane, when *Unix Account (SSH Key)* is selected as the template:
   1. In the *Host* field, enter the IP address or the FQDN of the SFTP server.
   2. In the *Username* field, enter the username for the SFTP server.
   3. In *Public-key*, select from *File Upload*, *Text*, or *Generate*.
      1. When *File Upload* is selected, select *Upload*, locate the key file on your management computer, and select *Open*.
      2. When *Text* is selected, enter the public key in the text area.
      3. When *Generate* is selected, you can automatically generate a public key by choosing a type of encryption algorithm and the number of bits.
   4. 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.

8. Click *Submit*.



New Secret

Name	sftp demo password auth
Folder	admin
Template	Unix Account (SSH Password)
Associated Secret	No associated secret
Description	

Fields

Host	[redacted]
Username	admin
Password	••••••••
Confirm Password	••••••••

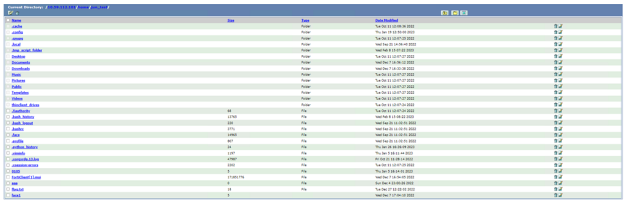
Secret Setting

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
Requires Checkout	[✓ Disable] Enable
Requires Approval to Launch Secret	[✓ Disable] Enable
Requires Approval to Launch Job	[✓ Disable] Enable

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

To launch a secret for the SFTP sever:

1. In *Secrets > Secret List*, select the newly created secret, and select *Launch Secret*.
2. In *Launch Progress*, select *Web SFTP* launcher to gain access to the SFTP server.
   A new browser tab opens with the Web SFTP interactive UI. You can now modify files or folders from the SFTP server.



Current Directory: /10.59.112.101/home/jun_test/

Name	Size	Type	Date Modified
.cache		Folder	Tue Oct 11 12:08:36 2022
.config		Folder	Thu Jan 19 12:50:00 2023
.gnupg		Folder	Tue Oct 11 12:07:25 2022
.local		Folder	Wed Sep 21 14:56:40 2022
.tmp_script_folder		Folder	Wed Feb 8 15:07:22 2023
Desktop		Folder	Tue Oct 11 12:07:27 2022
Documents		Folder	Wed Dec 7 16:56:12 2022
Downloads		Folder	Wed Dec 7 16:33:38 2022
Music		Folder	Tue Oct 11 12:07:27 2022
Pictures		Folder	Tue Oct 11 12:07:27 2022
Public		Folder	Tue Oct 11 12:07:27 2022
Templates		Folder	Tue Oct 11 12:07:27 2022
Videos		Folder	Tue Oct 11 12:07:27 2022
thinclient_drives		Folder	Tue Oct 11 12:07:24 2022
.Xauthority	68	File	Tue Oct 11 12:07:24 2022
.bash_history	13765	File	Wed Feb 8 15:08:22 2023
.bash_logout	220	File	Wed Sep 21 11:32:51 2022
.bashrc	3771	File	Wed Sep 21 11:32:51 2022
.face	14965	File	Wed Sep 21 11:32:51 2022
.profile	807	File	Wed Sep 21 11:32:51 2022
.python_history	24	File	Thu Jan 26 16:26:09 2023
.viminfo	1197	File	Thu Jan 5 16:11:44 2023
.xorgxrdp.13.log	47987	File	Fri Oct 21 11:28:14 2022
.xsession-errors	2202	File	Tue Oct 11 12:07:25 2022
0105	5	File	Thu Jan 5 16:14:01 2023
FortiClient(1).msi	171851776	File	Wed Dec 7 16:54:05 2022
aaa	0	File	Sun Dec 4 23:00:26 2022
flag.txt	18	File	Tue Dec 27 12:22:02 2022
face1	5		Wed Dec 7 17:04:10 2022

Accessing an SMB server using Web SMB launcher

This example demonstrates how to access an SMB server by setting up a Windows Domain Account (Samba) template based secret on FortiPAM and then using the Web SMB as a secret launcher to remotely gain access to the SMB server.

To access an SMB server using the Web SMB launcher:

1. Creating a secret with Windows Domain Account (Samba) template on page 67
2. Verifying the password on page 68
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:

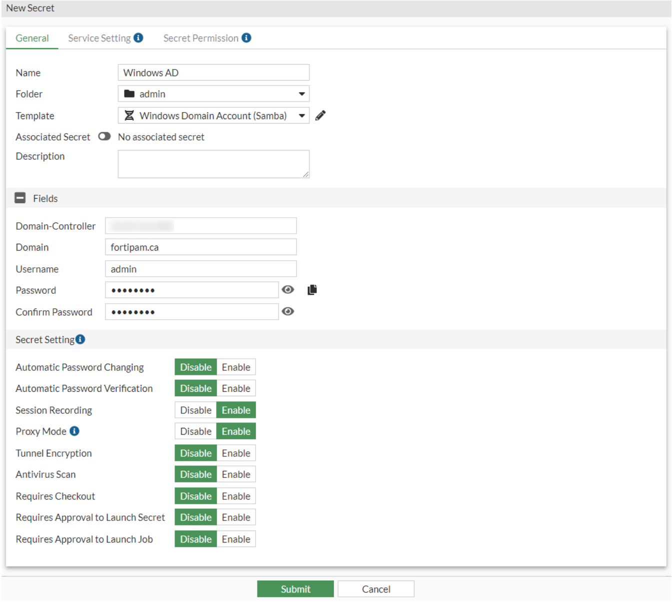
1. Go to *Secrets* > *Secret List*.
2. In *Secret List*, select *Create*.
   The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.
4. Select *Create Secret*.
   The *New Secret* window opens.
5. Enter a name for the secret.
6. In the *Template* dropdown,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



New Secret

Name	Windows AD
Folder	admin
Template	Windows Domain Account (Samba)
Associated Secret	No associated secret
Description	

Fields

Domain-Controller	[redacted]
Domain	fortipam.ca
Username	admin
Password	••••••••
Confirm Password	••••••••

Secret Setting

Automatic Password Changing	Disable
Automatic Password Verification	Disable
Session Recording	Enable
Proxy Mode	Enable
Tunnel Encryption	Disable
Antivirus Scan	Disable
Requires Checkout	Disable
Requires Approval to Launch Secret	Disable
Requires Approval to Launch Job	Disable

Verifying the password

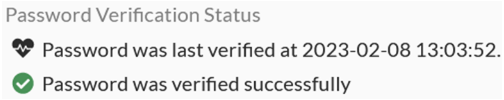
To verify the password manually:

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

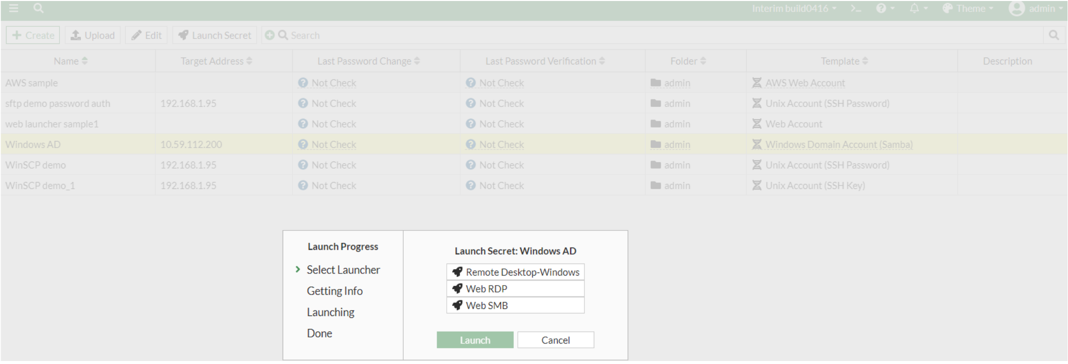
Password was last verified at 2023-02-08 13:03:52.

✓ 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*.

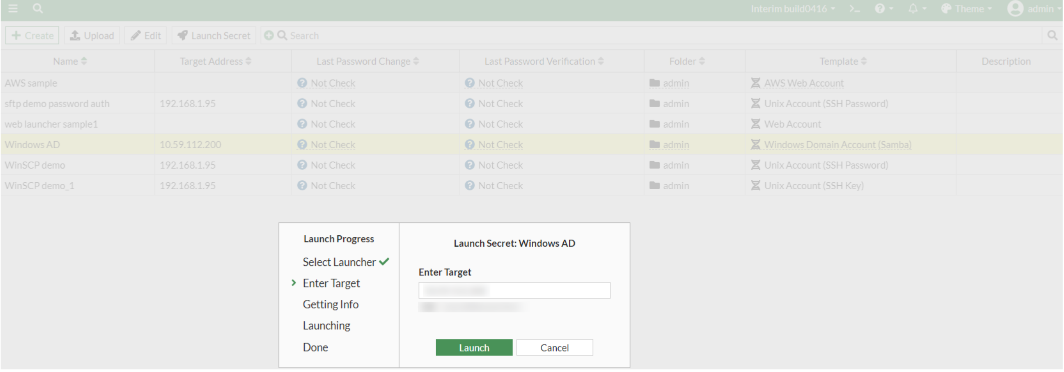


Name	Target Address	Last Password Change	Last Password Verification	Folder	Template	Description
AWS sample		Not Check	Not Check	admin	AWS Web Account	
sftp demo password auth	192.168.1.95	Not Check	Not Check	admin	Unix Account (SSH Password)	
web launcher sample1		Not Check	Not Check	admin	Web Account	
Windows AD	10.59.112.200	Not Check	Not Check	admin	Windows Domain Account (Samba)	
WinSCP demo	192.168.1.95	Not Check	Not Check	admin	Unix Account (SSH Password)	
WinSCP demo_1	192.168.1.95	Not Check	Not Check	admin	Unix Account (SSH Key)	

Launch Progress
- Select Launcher
- Getting Info
- Launching
- Done

Launch Secret: Windows AD
- Remote Desktop-Windows
- Web RDP
- Web SMB

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



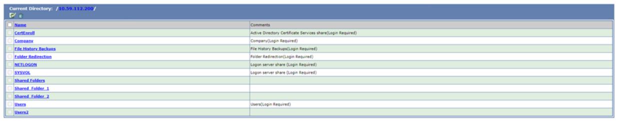
Name	Target Address	Last Password Change	Last Password Verification	Folder	Template	Description
AWS sample		Not Check	Not Check	admin	AWS Web Account	
sftp demo password auth	192.168.1.95	Not Check	Not Check	admin	Unix Account (SSH Password)	
web launcher sample1		Not Check	Not Check	admin	Web Account	
Windows AD	10.59.112.200	Not Check	Not Check	admin	Windows Domain Account (Samba)	
WinSCP demo	192.168.1.95	Not Check	Not Check	admin	Unix Account (SSH Password)	
WinSCP demo_1	192.168.1.95	Not Check	Not Check	admin	Unix Account (SSH Key)	

Launch Progress
- Select Launcher ✓
- Enter Target
- Getting Info
- Launching
- Done

Launch Secret: Windows AD

Enter Target

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 priviliges.



Current Directory: /10.59.112.200/

Name	Comments
CertEnroll	Active Directory Certificate Services share(Login Required)
Company	Company(Login Required)
File History Backups	File History Backups(Login Required)
Folder Redirection	Folder Redirection(Login Required)
NETLOGON	Logon server share (Login Required)
SYSVOL	Logon server share (Login Required)
Shared Folders	
Shared_Folder_1	
Shared_Folder_2	
Users	Users(Login Required)
Users2	

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

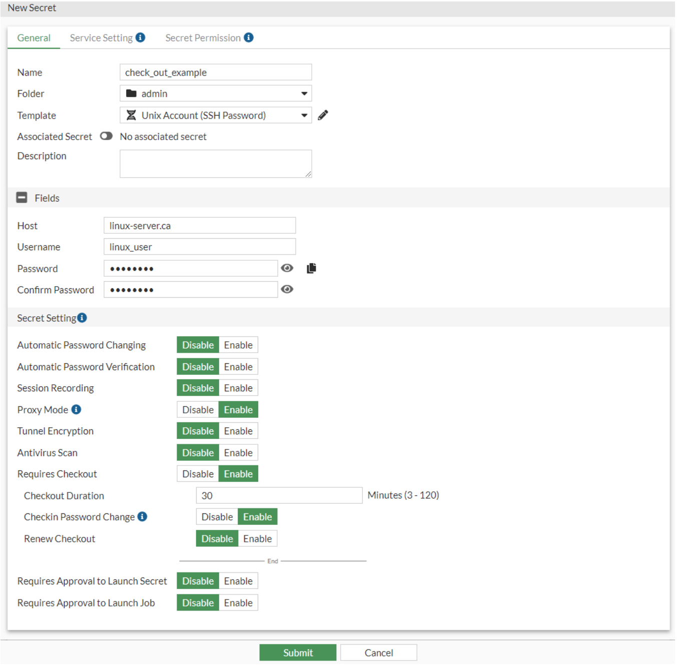
To create a secret with check out enabled:

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*.



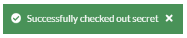
Name	check_out_example
Folder	admin
Template	Unix Account (SSH Password)
Associated Secret	No associated secret
Description	
Host	linux-server.ca
Username	linux_user
Password	••••••••
Confirm Password	••••••••
Automatic Password Changing	Disable
Automatic Password Verification	Disable
Session Recording	Disable
Proxy Mode	Enable
Tunnel Encryption	Disable
Antivirus Scan	Disable
Requires Checkout	Enable
Checkout Duration	30 Minutes (3 - 120)
Checkin Password Change	Enable
Renew Checkout	Disable
Requires Approval to Launch Secret	Disable
Requires Approval to Launch Job	Disable

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:

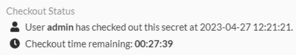


Successfully checked out secret ✕

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.



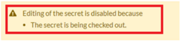
Checkout Status

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.



Editing of the secret is disabled because

- The secret is being checked out.

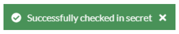
Checking in a secret

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:

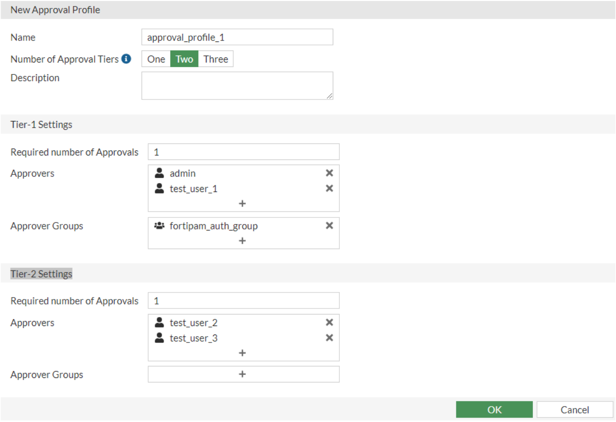
1. Creating an approval profile on page 72
2. Creating a secret with mandatory approval requirement on page 73
3. Sending a request to access a secret on page 74
4. Approving a secret request on page 75
5. Launching a secret that requires approval on page 76

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*.



New Approval Profile

Name: approval_profile_1

Number of Approval Tiers: One [✓ Two] Three

Description:

Tier-1 Settings

Required number of Approvals: 1

Approvers: admin, test_user_1

Approver Groups: fortipam_auth_group

Tier-2 Settings

Required number of Approvals: 1

Approvers: test_user_2, test_user_3

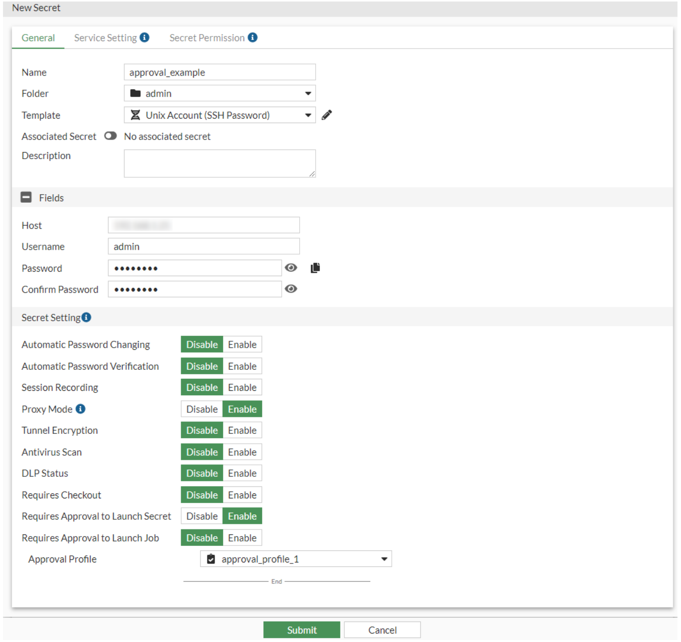
Approver Groups:

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*.



New Secret

General | Service Setting | Secret Permission

Name	approval_example
Folder	admin
Template	Unix Account (SSH Password)
Associated Secret	No associated secret
Description	

Fields

Host	[redacted]
Username	admin
Password	••••••••
Confirm Password	••••••••

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
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.

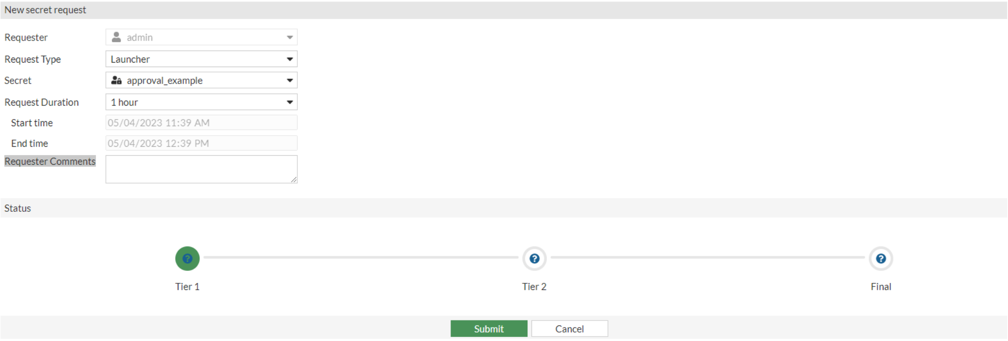
   Alternatively, go to *Secrets > My Request List*, select *Create*.

   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*.

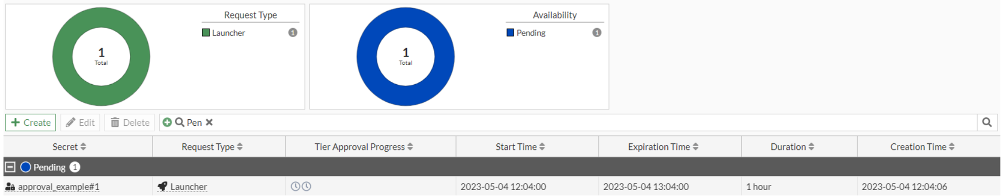


New secret request

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

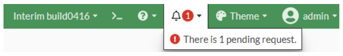
Once the request is submitted, it appears in *My Request List* tab in *Pending*.



Secret	Request Type	Tier Approval Progress	Start Time	Expiration Time	Duration	Creation Time
Pending						
approval_example#1	Launcher		2023-05-04 12:04:00	2023-05-04 13:04:00	1 hour	2023-05-04 12:04:06

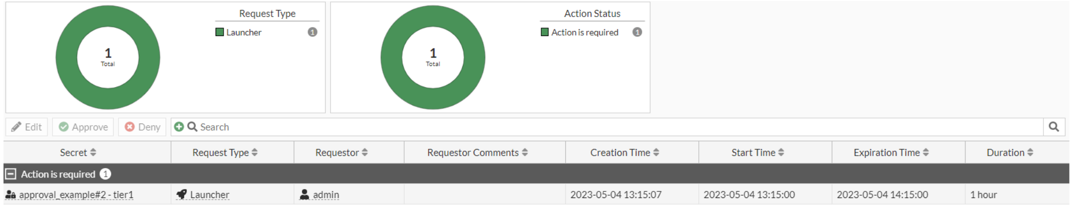
Approving a secret request

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.



There is 1 pending request.

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*.



Secret	Request Type	Requestor	Requestor Comments	Creation Time	Start Time	Expiration Time	Duration
Action is required							
approval_example#2 - tier1	Launcher	admin		2023-05-04 13:15:07	2023-05-04 13:15:00	2023-05-04 14:15:00	1 hour

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.

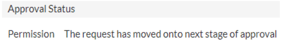
To override the requested duration:

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.

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.

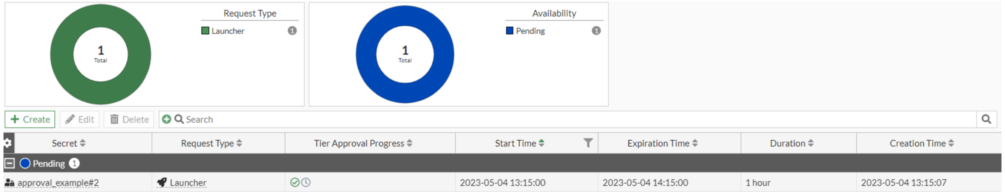
5. Click *Save*.
 Once approved, the *Approval Status* is updated. In this example, the request now moves to the next tier as configured in Creating an approval profile on page 72.



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*.



Secret	Request Type	Tier Approval Progress	Start Time	Expiration Time	Duration	Creation Time
Pending 1						
approval_example#2	Launcher	✓ 🕓	2023-05-04 13:15:00	2023-05-04 14:15:00	1 hour	2023-05-04 13:15:07

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:

1. Send a secret approval request as shown in Sending a request to access a secret on page 74.
2. Once the secret approval request is approved, in *Secrets > Secret List*, select the newly created secret, and select *Launch Secret*.
3. 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

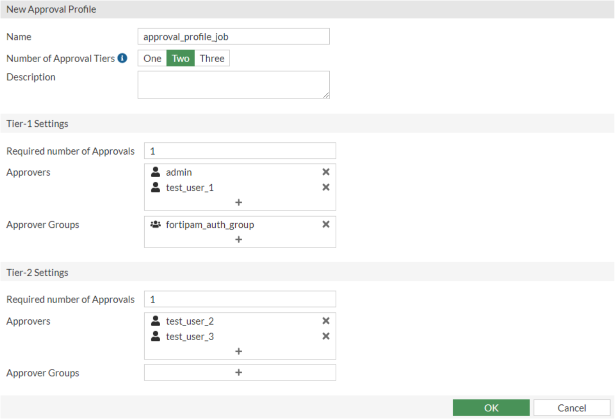
Creating a job approval profile

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*.



New Approval Profile

Name: approval_profile_job

Number of Approval Tiers: One [✓ Two] Three

Description:

Tier-1 Settings

Required number of Approvals: 1

Approvers: admin, test_user_1

Approver Groups: fortipam_auth_group

Tier-2 Settings

Required number of Approvals: 1

Approvers: test_user_2, test_user_3

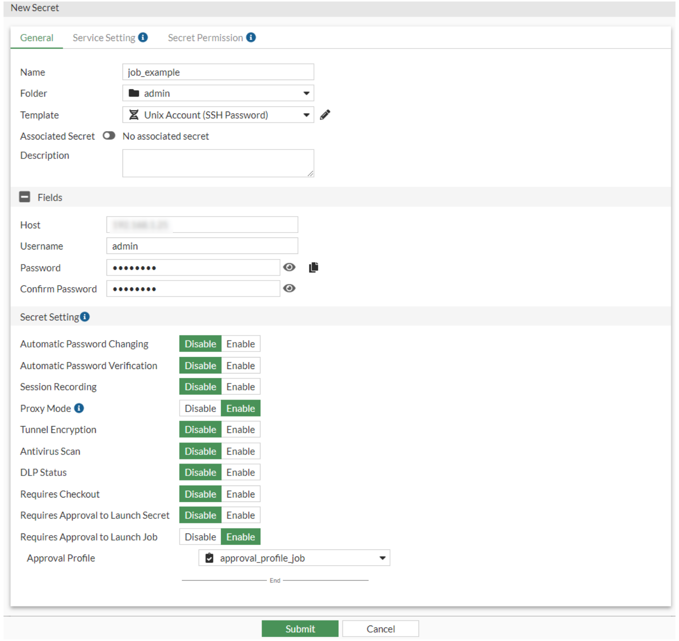
Approver Groups:

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*.



Name: job_example
Folder: admin
Template: Unix Account (SSH Password)
Associated Secret: No associated secret
Description:

Host: [redacted]
Username: admin
Password: ••••••••
Confirm Password: ••••••••

Automatic Password Changing	Disable
Automatic Password Verification	Disable
Session Recording	Disable
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	Enable
Approval Profile	approval_profile_job

Creating an ssh script type job

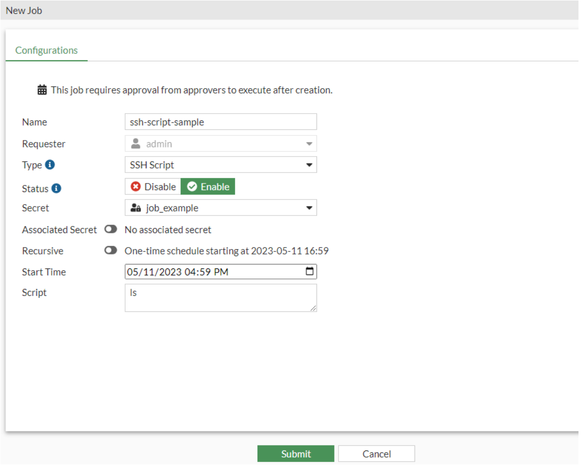
To create an ssh script type job:

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.



New Job

This job requires approval from approvers to execute after creation.

Name	ssh-script-sample
Requester	admin
Type	SSH Script
Status	Disable [✓ Enable]
Secret	job_example
Associated Secret	No associated secret
Recursive	One-time schedule starting at 2023-05-11 16:59
Start Time	05/11/2023 04:59 PM
Script	ls

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*.

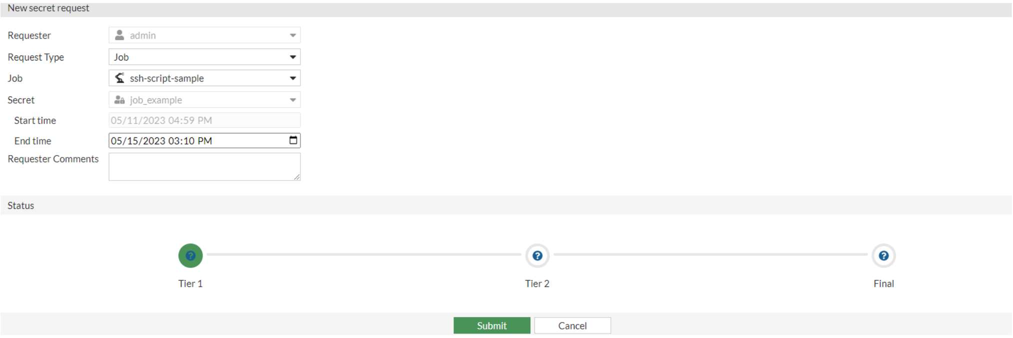
   The *New secret request* window opens.
4. In *Request Type*, ensure that *Job* is selected.
5. In *Job*, if you are making a request from the *Job List*, the job is already selected.
   If you are creating an approval request in *Secrets > My Request List*, select the job created in Creating an ssh script 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*.

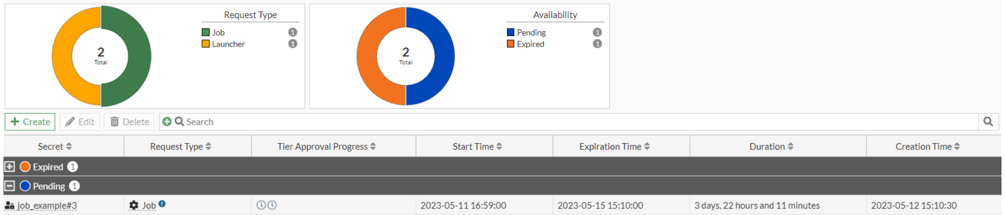


New secret request

Requester	admin
Request Type	Job
Job	ssh-script-sample
Secret	job_example
Start time	05/11/2023 04:59 PM
End time	05/15/2023 03:10 PM
Requester Comments	

Status

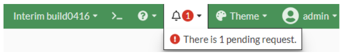
Once the request is submitted, it appears in *My Request List* tab in *Pending*.



Secret	Request Type	Tier Approval Progress	Start Time	Expiration Time	Duration	Creation Time
Expired 1						
Pending 1						
job_example#3	Job		2023-05-11 16:59:00	2023-05-15 15:10:00	3 days, 22 hours and 11 minutes	2023-05-12 15:10:30

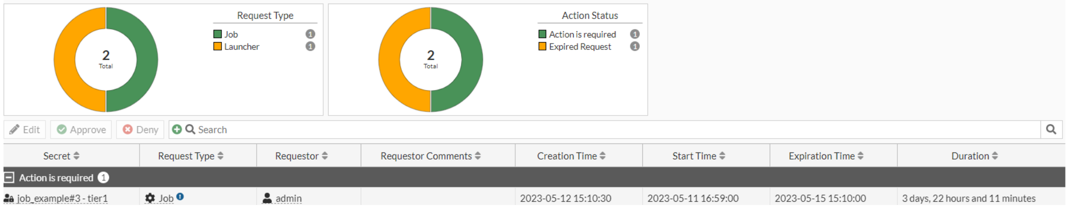
Approving a job request

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.



There is 1 pending request.

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*.



Secret	Request Type	Requestor	Requestor Comments	Creation Time	Start Time	Expiration Time	Duration
Action is required 1							
job_example#3 - tier1	Job	admin		2023-05-12 15:10:30	2023-05-11 16:59:00	2023-05-15 15:10:00	3 days, 22 hours and 11 minutes

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.

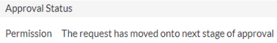
To override the requested duration:

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.

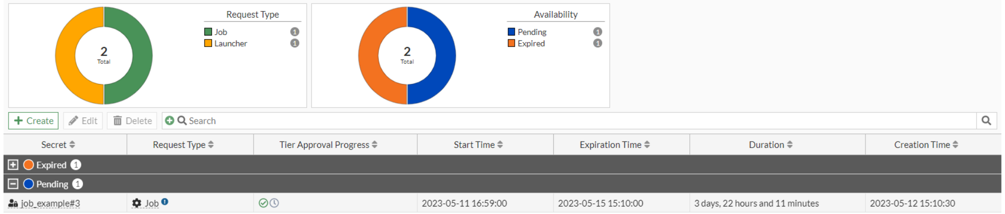
5. Click *Save*.
   Once approved, the *Approval Status* is updated. In this example, the request now moves to the next tier as configured in Creating a job approval profile on page 77.



Approval Status

Permission The request has moved onto next stage of approval

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



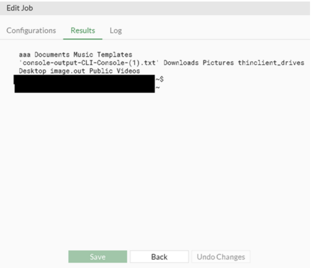
Secret ⇕	Request Type ⇕	Tier Approval Progress ⇕	Start Time ⇕	Expiration Time ⇕	Duration ⇕	Creation Time ⇕
⊞ ● Expired 1						
⊟ ● Pending 1						
job_example#3	Job	✓ 🕓	2023-05-11 16:59:00	2023-05-15 15:10:00	3 days, 22 hours and 11 minutes	2023-05-12 15:10:30

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.

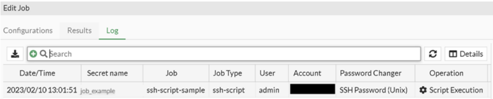
Results

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.



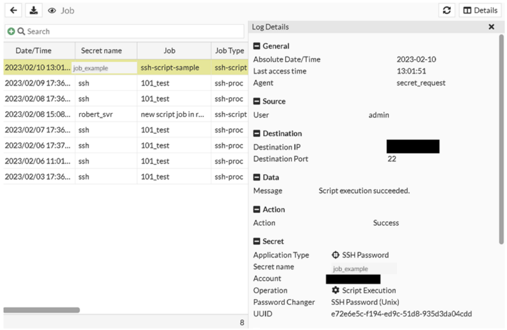
```
aaa Documents Music Templates
'console-output-CLI-Console-(1).txt' Downloads Pictures thinclient_drives
Desktop image.out Public Videos
[redacted]~$
~
```

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



Date/Time	Secret name	Job	Job Type	User	Account	Password Changer	Operation
2023/02/10 13:01:51	job_example	ssh-script-sample	ssh-script	admin	[redacted]	SSH Password (Unix)	Script Execution

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



Date/Time	Secret name	Job	Job Type
2023/02/10 13:01...	job_example	ssh-script-sample	ssh-script
2023/02/09 17:36...	ssh	101_test	ssh-proc
2023/02/08 17:36...	ssh	101_test	ssh-proc
2023/02/08 15:08...	robert_svr	new script job in r...	ssh-script
2023/02/07 17:36...	ssh	101_test	ssh-proc
2023/02/06 17:37...	ssh	101_test	ssh-proc
2023/02/06 11:01...	ssh	101_test	ssh-proc
2023/02/03 17:36...	ssh	101_test	ssh-proc

8

General
Absolute Date/Time 2023-02-10
Last access time 13:01:51
Agent secret_request

Source
User admin

Destination
Destination IP [redacted]
Destination Port 22

Data
Message Script execution succeeded.

Action
Action Success

Secret
Application Type SSH Password
Secret name job_example
Account [redacted]
Operation Script Execution
Password Changer SSH Password (Unix)
UUID e72e6e5c-f194-ed9c-51d8-935d3da04cdd

Configuring a secret that supports TOTP

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

SSH secrets support TOTP auto-deliviery 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.

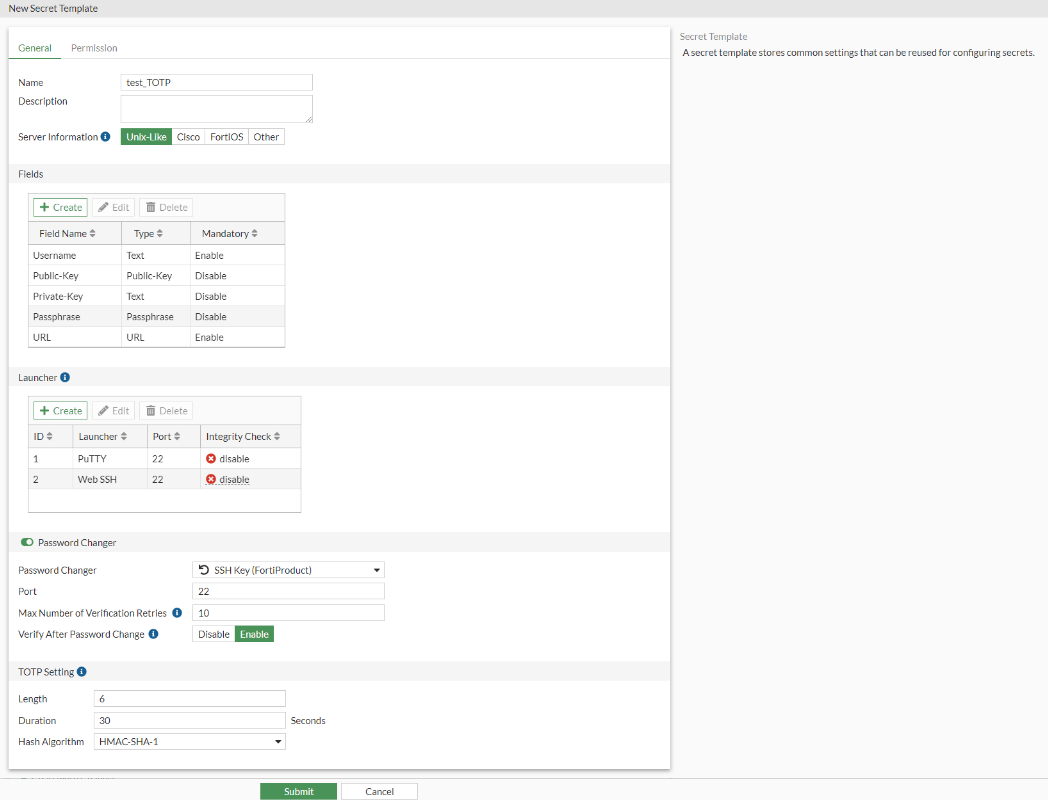
Configuring a secret template with TOTP

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*.



New Secret Template

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: Disable [✓ Enable]

TOTP Setting

Length: 6

Duration: 30 Seconds

Hash Algorithm: HMAC-SHA-1

Secret Template

A secret template stores common settings that can be reused for configuring secrets.

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.

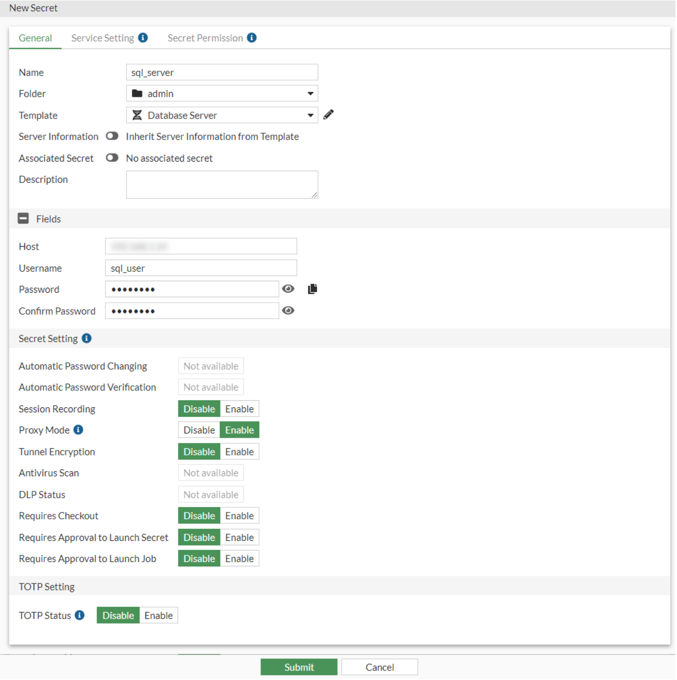
To access an MySQL server using MySQL CLI:

1. Creating a secret using the database server template on page 87
2. Launching a secret for the MySQL server on page 88

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.
8. Click *Submit*.



Name	sql_server
Folder	admin
Template	Database Server
Server Information	Inherit Server Information from Template
Associated Secret	No associated secret
Description	

Fields

Host	[redacted]
Username	sql_user
Password	••••••••
Confirm Password	••••••••

Secret Setting

Automatic Password Changing	Not available
Automatic Password Verification	Not available
Session Recording	[✓ 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

TOTP Setting

TOTP Status	[✓ Disable] Enable

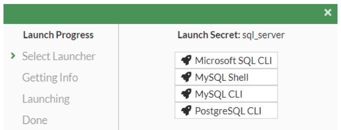
The following secret settings are not available when using the default database server secret template:

- *Automatic Password Changing*
- *Automatic Password Verification*
- *Antivirus Scan*
- *DLP Status*

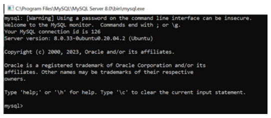
Launching a secret for the MySQL server

To launch a secret for the MySQL server:

1. In *Secrets > Secret List*, select the newly created secret, and select *Launch Secret*.
2. In *Launch Progress*, select the *MySQL CLI* launcher.



The MySQL CLI is launched. You can now access the MySQL server.



```
C:\Program Files\MySQL\MySQL Server 8.0\bin\mysql.exe
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 126
Server version: 8.0.33-0ubuntu0.20.04.2 (Ubuntu)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

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 89
2. Enabling integrity check in the launcher and secret template on page 90
3. Creating a secret with integrity check on page 91
4. Launching the secret on page 92

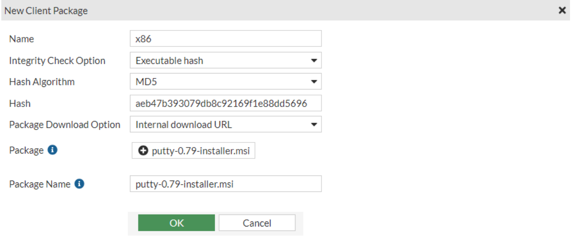
Creating an entry for the PuTTY launcher

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.

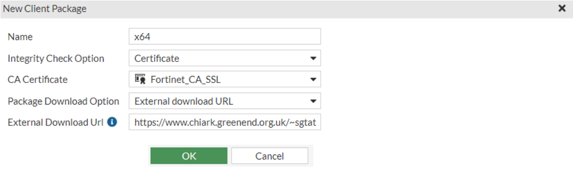
   > We use the `Certutil -hashfile filename MD5` command and replace the filename with the path to the uncorrupted software (`putty.exe`) to generate the hash field.

   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*.



Name	x86
Integrity Check Option	Executable hash
Hash Algorithm	MD5
Hash	aeb47b393079db8c92169f1e88dd5696
Package Download Option	Internal download URL
Package	putty-0.79-installer.msi
Package Name	putty-0.79-installer.msi

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*.



Name	x64
Integrity Check Option	Certificate
CA Certificate	Fortinet_CA_SSL
Package Download Option	External download URL
External Download Url	https://www.chiark.greenend.org.uk/~sgtat

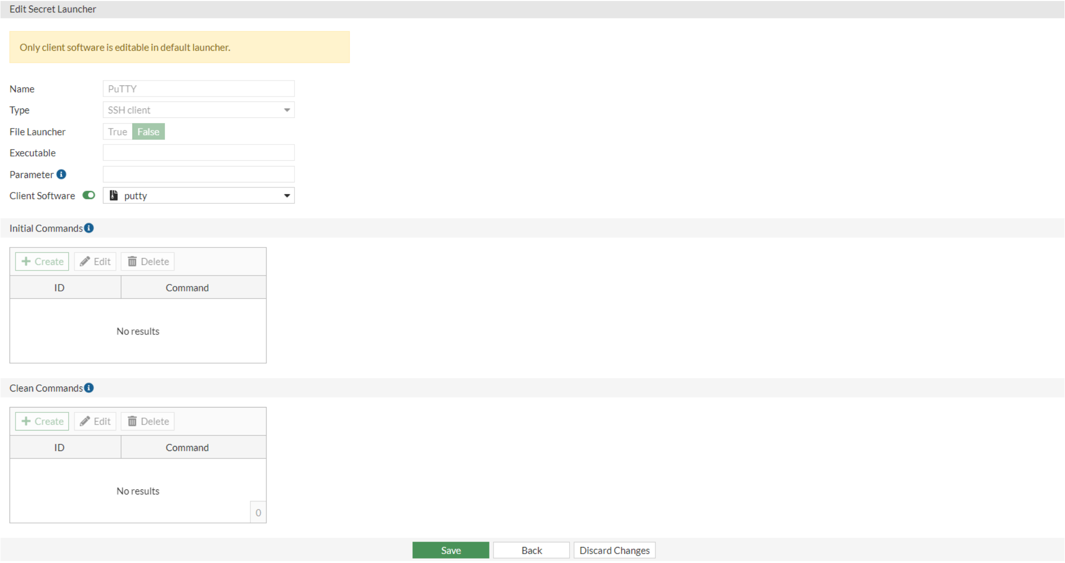
6. Click *Submit*.

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 89.

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 89.
4. Click *Save*.



Edit Secret Launcher

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	

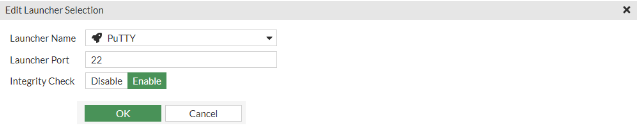
To enable integrity check in the secret template that uses the PuTTY launcher:

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*.



Launcher Name: PuTTY
Launcher Port: 22
Integrity Check: Disable [✓ Enable]

Creating a secret with integrity check

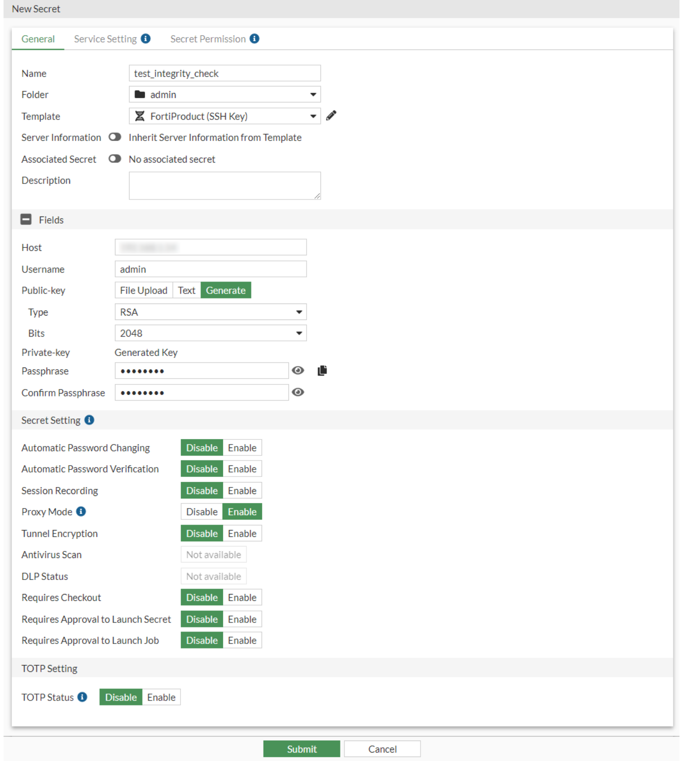
We now create a secret that uses the *FortiProduct (SSH Key)* secret template and PuTTY as the launcher.

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 90.
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*.



New Secret

General | Service Setting | Secret Permission

Name: test_integrity_check

Folder: admin

Template: FortiProduct (SSH Key)

Server Information: Inherit Server Information from Template

Associated Secret: No associated secret

Description:

Fields

Host: [redacted]

Username: admin

Public-key: File Upload | Text | [✓ Generate]

Type: RSA

Bits: 2048

Private-key: Generated Key

Passphrase: ••••••••

Confirm Passphrase: ••••••••

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: Not available

DLP Status: Not available

Requires Checkout: [✓ Disable] Enable

Requires Approval to Launch Secret: [✓ Disable] Enable

Requires Approval to Launch Job: [✓ Disable] Enable

TOTP Setting

TOTP Status: [✓ Disable] Enable

Launching the secret

Here, we launch the secret created in Creating a secret with integrity check on page 91.

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 90, 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:

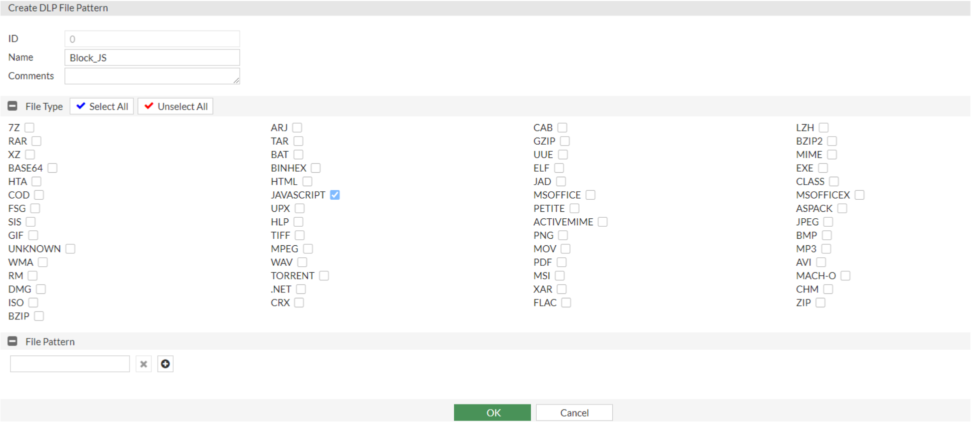
1. Configuring the DLP file pattern on page 93
2. Configuring a DLP sensor profile on page 93
3. Creating a secret with a DLP sensor profile on page 94
4. Results on page 95

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*.



Create DLP File Pattern

ID: 0
Name: Block_JS
Comments:

File Type ✓ Select All ✓ Unselect All

7Z □
RAR □
XZ □
BASE64 □
HTA □
COD □
FSG □
SIS □
GIF □
UNKNOWN □
WMA □
RM □
DMG □
ISO □
BZIP □

ARJ □
TAR □
BAT □
BINHEX □
HTML □
JAVASCRIPT ☑
UPX □
HLP □
TIFF □
MPEG □
WAV □
TORRENT □
.NET □
CRX □

CAB □
GZIP □
UUE □
ELF □
JAD □
MSOFFICE □
PETITE □
ACTIVEMIME □
PNG □
MOV □
PDF □
MSI □
XAR □
FLAC □

LZH □
BZIP2 □
MIME □
EXE □
CLASS □
MSOFFICEX □
ASPACK □
JPEG □
BMP □
MP3 □
AVI □
MACH-O □
CHM □
ZIP □

File Pattern

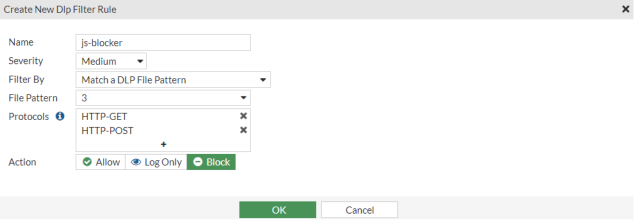
Configuring a DLP sensor profile

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 93.

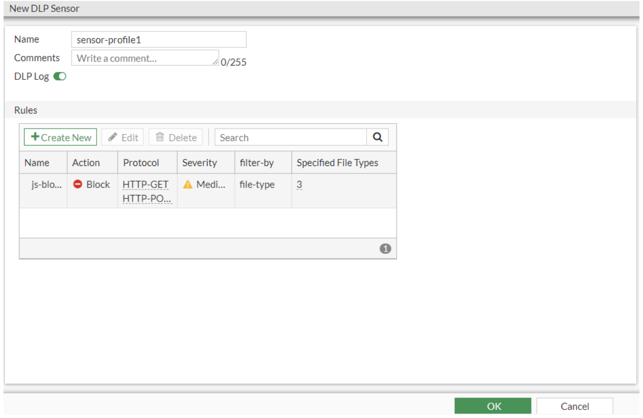
To configure a DLP sensor profile:

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* drodown, 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 93.
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*.


Create New Dlp Filter Rule

Name: js-blocker
Severity: Medium
Filter By: Match a DLP File Pattern
File Pattern: 3
Protocols: HTTP-GET, HTTP-POST
Action: ○ Allow ○ Log Only ● Block


New DLP Sensor

Name: sensor-profile1
Comments: Write a comment... 0/255
DLP Log ●

Rules

Name	Action	Protocol	Severity	filter-by	Specified File Types
js-blo...	Block	HTTP-GET HTTP-PO...	Medi...	file-type	3

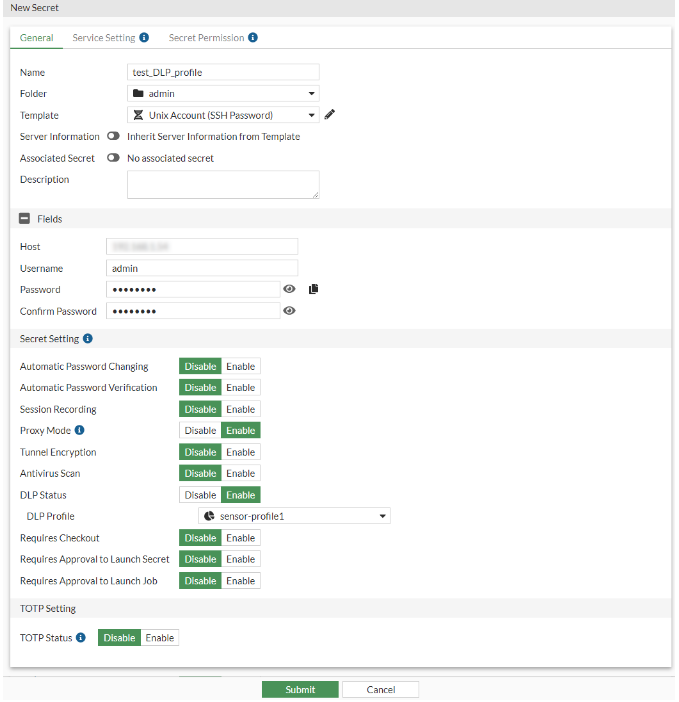
Creating a secret with a DLP sensor profile

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*.



New Secret

General | Service Setting | Secret Permission

Name	test_DLP_profile
Folder	admin
Template	Unix Account (SSH Password)
Server Information	Inherit Server Information from Template
Associated Secret	No associated secret
Description	

Fields

Host	[redacted]
Username	admin
Password	••••••••
Confirm Password	••••••••

Secret Setting

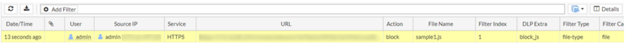
Automatic Password Changing	Disable
Automatic Password Verification	Disable
Session Recording	Disable
Proxy Mode	Enable
Tunnel Encryption	Disable
Antivirus Scan	Disable
DLP Status	Enable
DLP Profile	sensor-profile1
Requires Checkout	Disable
Requires Approval to Launch Secret	Disable
Requires Approval to Launch Job	Disable

TOTP Setting

TOTP Status	Disable

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 Ca
13 seconds ago		admin	admin [redacted]	HTTPS	[redacted]	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:

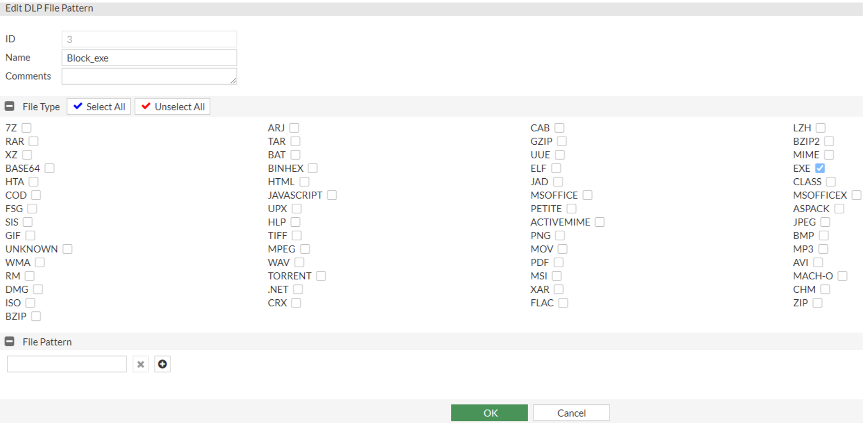
1. Configuring the DLP file pattern on page 96
2. Configuring a DLP sensor profile on page 96
3. Creating a secret with a DLP sensor profile on page 98
4. Results on page 99

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*.



Edit DLP File Pattern

ID: 3
Name: Block_exe
Comments:

File Type ✓ Select All ✓ Unselect All

7Z □	ARJ □	CAB □	LZH □
RAR □	TAR □	GZIP □	BZIP2 □
XZ □	BAT □	UUE □	MIME □
BASE64 □	BINHEX □	ELF □	EXE ☑
HTA □	HTML □	JAD □	CLASS □
COD □	JAVASCRIPT □	MSOFFICE □	MSOFFICEX □
FSG □	UPX □	PETITE □	ASPACK □
SIS □	HLP □	ACTIVEMIME □	JPEG □
GIF □	TIFF □	PNG □	BMP □
UNKNOWN □	MPEG □	MOV □	MP3 □
WMA □	WAV □	PDF □	AVI □
RM □	TORRENT □	MSI □	MACH-O □
DMG □	.NET □	XAR □	CHM □
ISO □	CRX □	FLAC □	ZIP □
BZIP □			

File Pattern

OK Cancel

Configuring a DLP sensor profile

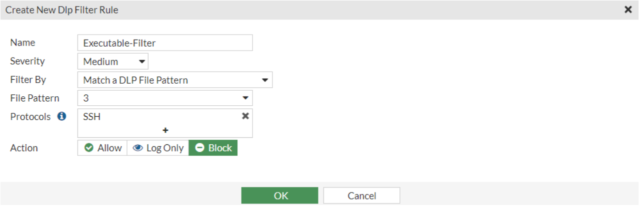
Here, we configure a DLP sensor profile with the following two DLP filter rules:

- 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.

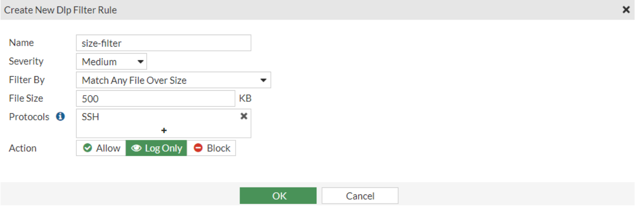
To configure a DLP sensor profile:

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* drodown, 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* drodown, 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*.



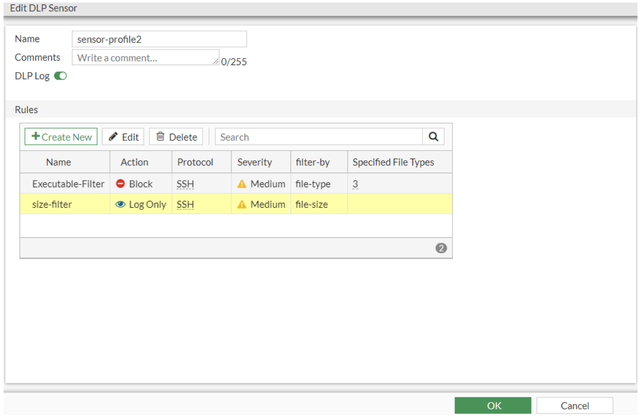
Create New Dlp Filter Rule

Name	Executable-Filter
Severity	Medium
Filter By	Match a DLP File Pattern
File Pattern	3
Protocols	SSH
Action	Allow / Log Only / [✓ Block]



Create New Dlp Filter Rule

Name	size-filter
Severity	Medium
Filter By	Match Any File Over Size
File Size	500 KB
Protocols	SSH
Action	Allow / [✓ Log Only] / Block



Name: sensor-profile2
Comments: Write a comment... 0/255
DLP Log

Name	Action	Protocol	Severity	filter-by	Specified File Types
Executable-Filter	Block	SSH	Medium	file-type	3
size-filter	Log Only	SSH	Medium	file-size	

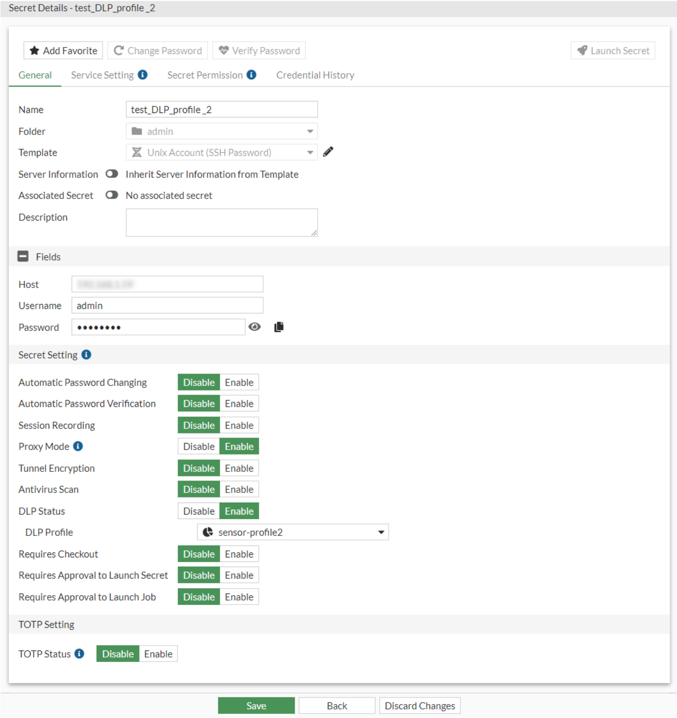
Creating a secret with a DLP sensor profile

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*.



Secret Details - test_DLP_profile_2

Name	test_DLP_profile_2
Folder	admin
Template	Unix Account (SSH Password)
Server Information	Inherit Server Information from Template
Associated Secret	No associated secret
Description	

Fields

Host	[redacted]
Username	admin
Password	••••••••

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]
DLP Profile	sensor-profile2
Requires Checkout	[✓ Disable] Enable
Requires Approval to Launch Secret	[✓ Disable] Enable
Requires Approval to Launch Job	[✓ Disable] Enable

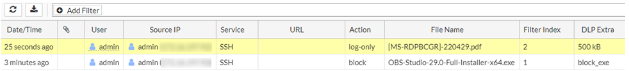
TOTP Setting

TOTP Status	[✓ Disable] Enable

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 [redacted]	SSH		log-only	[MS-RDPBCGR]-220429.pdf	2	500 kB
3 minutes ago		admin	admin [redacted]	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 100

Updating a service account credential

To update a service account credential:

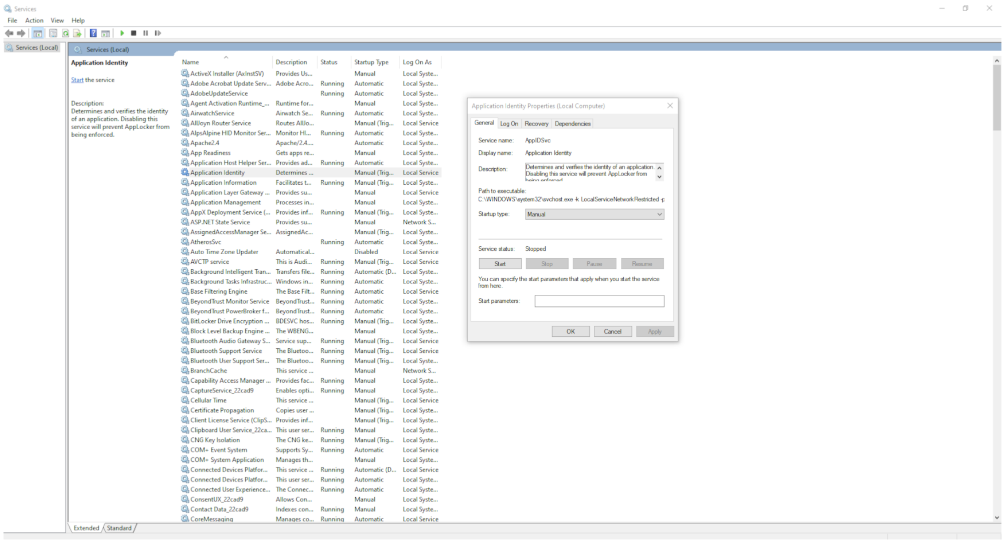
1. Go to *Secret Settings > Dependency Updater*.
2. Select *Create*.

   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*.



Application Identity

Start the service

Description:
Determines and verifies the identity of an application. Disabling this service will prevent AppLocker from being enforced.

Name	Description	Status	Startup Type	Log On As
ActiveX Installer (AxInstSV)	Provides Us...		Manual	Local Syste...
Adobe Acrobat Update Serv...	Adobe Acro...	Running	Automatic	Local Syste...
AdobeUpdateService		Running	Automatic	Local Syste...
Agent Activation Runtime_...	Runtime for...		Manual	Local Syste...
AirwatchService	Airwatch Se...	Running	Automatic	Local Syste...
AllJoyn Router Service	Routes AllJo...		Manual (Trig...	Local Service
AlpsAlpine HID Monitor Ser...	Monitor HI...	Running	Automatic	Local Syste...
Apache2.4	Apache/2.4....		Automatic	Local Syste...
App Readiness	Gets apps re...		Manual	Local Syste...
Application Host Helper Ser...	Provides ad...	Running	Automatic	Local Syste...
Application Identity	Determines ...		Manual (Trig...	Local Service
Application Information	Facilitates t...	Running	Manual (Trig...	Local Syste...
Application Layer Gateway ...	Provides su...		Manual	Local Service
Application Management	Processes in...		Manual	Local Syste...
AppX Deployment Service (...	Provides inf...	Running	Manual (Trig...	Local Syste...
ASP.NET State Service	Provides su...		Manual	Network S...
AssignedAccessManager Se...	AssignedAc...		Manual (Trig...	Local Syste...
AtherosSvc		Running	Automatic	Local Syste...
Auto Time Zone Updater	Automatical...		Disabled	Local Service
AVCTP service	This is Audi...	Running	Manual (Trig...	Local Service
Background Intelligent Tran...	Transfers file...	Running	Automatic (D...	Local Syste...
Background Tasks Infrastruc...	Windows in...	Running	Automatic	Local Syste...
Base Filtering Engine	The Base Filt...	Running	Automatic	Local Service
BeyondTrust Monitor Service	BeyondTrust...	Running	Automatic	Local Syste...
BeyondTrust PowerBroker f...	BeyondTrust...	Running	Automatic	Local Syste...
BitLocker Drive Encryption ...	BDESVC hos...	Running	Manual (Trig...	Local Syste...
Block Level Backup Engine ...	The WBENG...		Manual	Local Syste...
Bluetooth Audio Gateway S...	Service sup...	Running	Manual (Trig...	Local Service
Bluetooth Support Service	The Bluetoo...	Running	Manual (Trig...	Local Service
Bluetooth User Support Ser...	The Bluetoo...	Running	Manual (Trig...	Local Syste...
BranchCache	This service ...		Manual	Network S...
Capability Access Manager ...	Provides fac...	Running	Manual	Local Syste...
CaptureService_22cad9	Enables opti...	Running	Manual	Local Syste...
Cellular Time	This service ...		Manual (Trig...	Local Service
Certificate Propagation	Copies user ...		Manual (Trig...	Local Syste...
Client License Service (ClipS...	Provides inf...		Manual (Trig...	Local Syste...
Clipboard User Service_22ca...	This user ser...	Running	Manual	Local Syste...
CNG Key Isolation	The CNG ke...	Running	Manual (Trig...	Local Syste...
COM+ Event System	Supports Sy...	Running	Automatic	Local Service
COM+ System Application	Manages th...		Manual	Local Syste...
Connected Devices Platfor...	This service ...	Running	Automatic (D...	Local Service
Connected Devices Platfor...	This user ser...	Running	Automatic	Local Syste...
Connected User Experience...	The Connec...	Running	Automatic	Local Syste...
ConsentUX_22cad9	Allows Con...		Manual	Local Syste...
Contact Data_22cad9	Indexes con...	Running	Manual	Local Syste...
CoreMessaging	Manages co...	Running	Automatic	Local Service

Application Identity Properties (Local Computer)

Service name: AppIDSvc

Display name: Application Identity

Description: Determines and verifies the identity of an application. Disabling this service will prevent AppLocker from being enforced.

Path to executable:
C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p

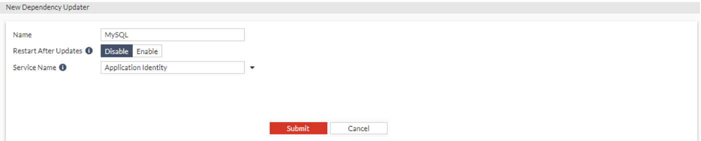
Startup type: Manual

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

6. Click *Submit*.



New Dependency Updater

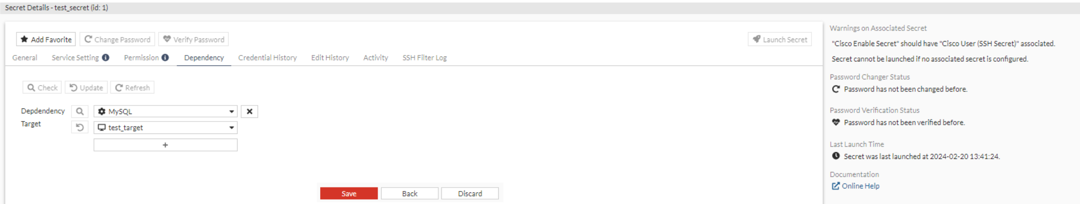
Name: MySQL

Restart After Updates: [✓ Disable] Enable

Service Name: Application Identity

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 *+*.
11. From the *Dependency* dropdown, select the dependency updater created earlier.
12. From the *Target* dropdown, select a target.

13. Click *Save*.



Warnings on Associated Secret

"Cisco Enable Secret" should have "Cisco User (SSH Secret)" associated.

Secret cannot be launched if no associated secret is configured.

Password Changer Status

Password has not been changed before.

Password Verification Status

Password has not been verified before.

Last Launch Time

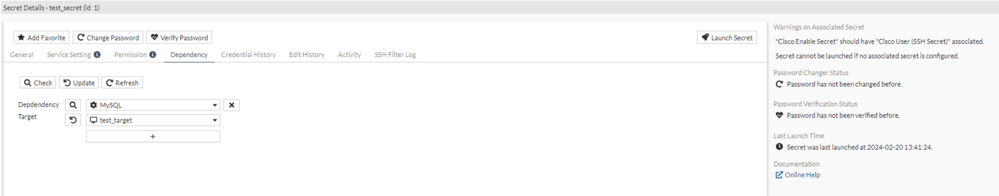
Secret was last launched at 2024-02-20 13:41:24.

Documentation

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.



Warnings on Associated Secret

"Cisco Enable Secret" should have "Cisco User (SSH Secret)" associated.

Secret cannot be launched if no associated secret is configured.

Password Changer Status

Password has not been changed before.

Password Verification Status

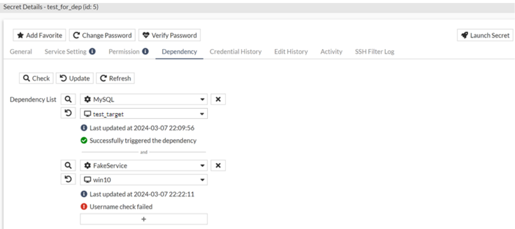
Password has not been verified before.

Last Launch Time

Secret was last launched at 2024-02-20 13:41:24.

Documentation

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.



Last updated at 2024-03-07 22:09:56

Successfully triggered the dependency

Last updated at 2024-03-07 22:22:11

Username check failed

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 103

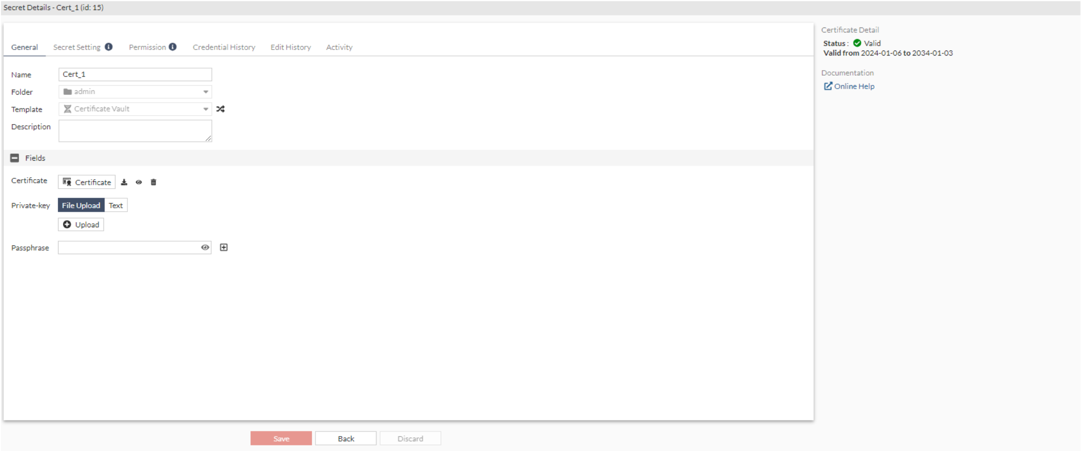
Limitation

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.



Secret Details - Cert_1 (id: 15)

Name: Cert_1
Folder: admin
Template: Certificate Vault
Description:
Certificate: Certificate
Private-key: File Upload | Text
Passphrase:

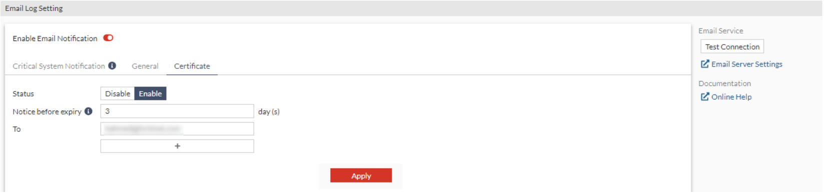
Certificate Detail
Status : Valid
Valid from 2024-01-06 to 2034-01-03

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*.



Email Log Setting

Enable Email Notification: enabled
Status: Disable | Enable
Notice before expiry: 3 day (s)
To: [redacted]

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 104
  - Example 1: Launching the secret on page 105
- 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

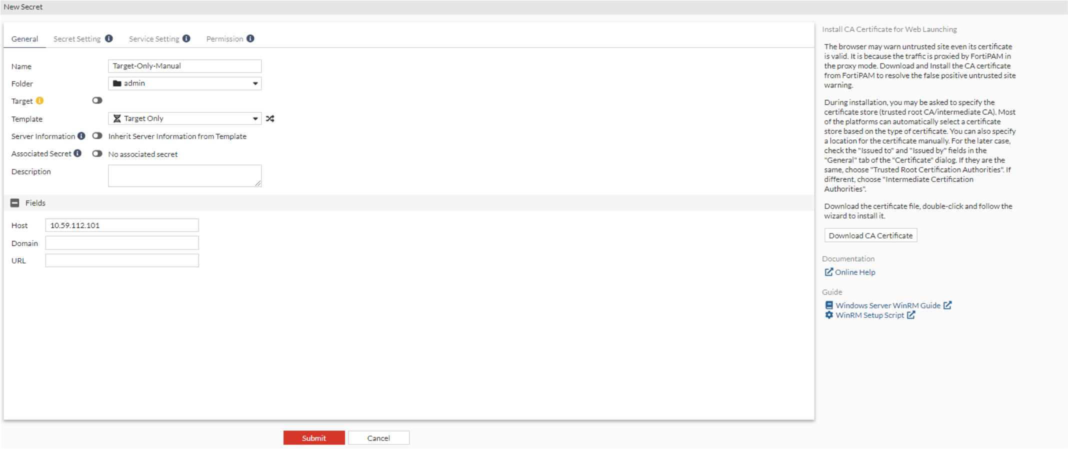
Example 1: Creating a secret using the *Target Only* template

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*.



Name: Target-Only-Manual
Folder: admin
Target: ○
Template: Target Only
Server Information: ○ Inherit Server Information from Template
Associated Secret: ○ No associated secret
Description:

Host: 10.59.112.101
Domain:
URL:

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 CA Certificate

Documentation

Online Help

Guide

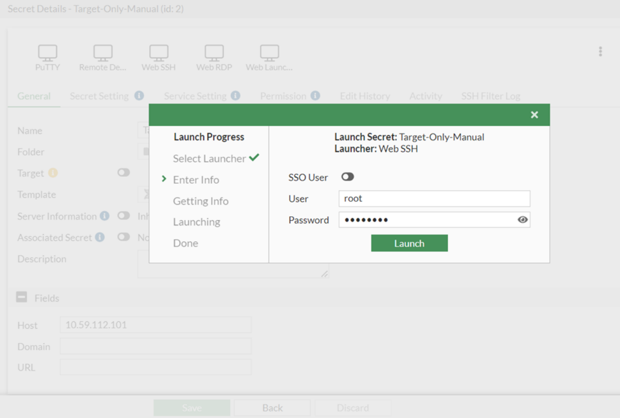
Windows Server WinRM Guide

WinRM Setup Script

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 104.
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.



Secret Details - Target-Only-Manual (id: 2)

Launch Progress: Select Launcher ✓, Enter Info, Getting Info, Launching, Done

Launch Secret: Target-Only-Manual
Launcher: Web SSH

SSO User: ○
User: root
Password: ••••••••

Host: 10.59.112.101

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`.

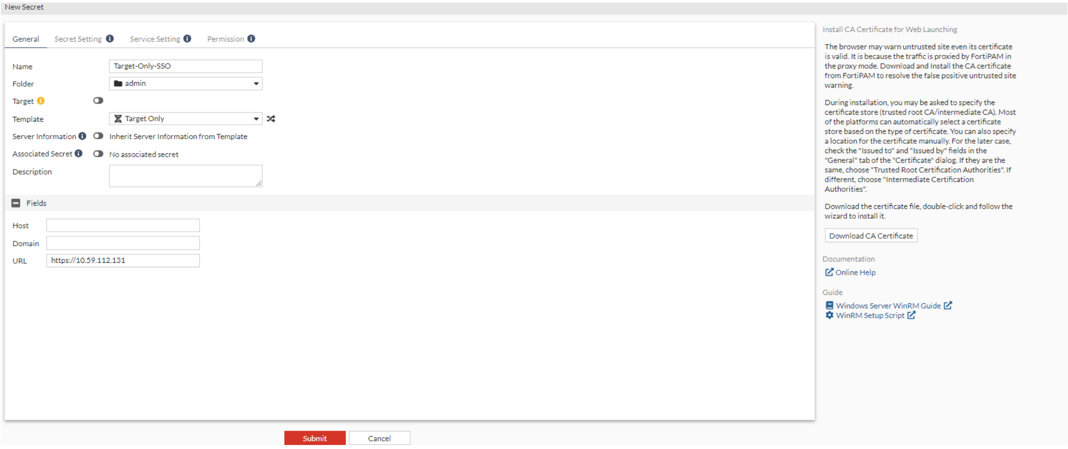
Both FortiPAM and the target FortiGate have the same credentials.

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*.



Name: Target-Only-SSO
Folder: admin
Target
Template: Target Only
Server Information: Inherit Server Information from Template
Associated Secret: No associated secret
Description

Fields

Host
Domain
URL: https://10.59.112.131

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.

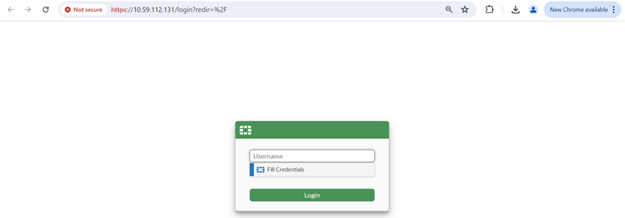
During installation, you may be asked to specify the certificate store (trusted root CA/intermediate CA). Most of the platforms can automatically select a certificate store based on the type of certificate. You can also specify a location for the certificate manually. For the later case, check the "Issued 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.

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.

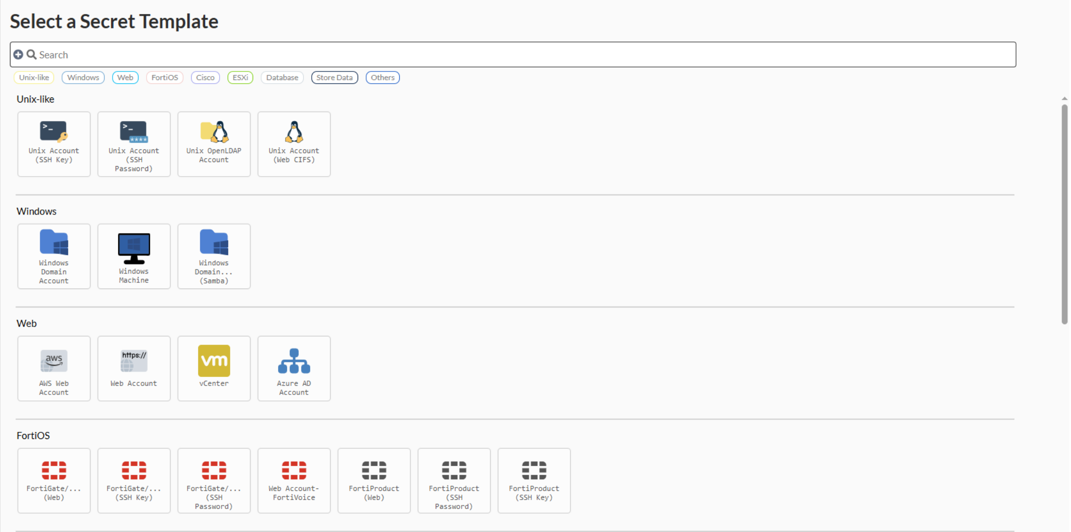
To set up smart association for Windows AD server as the target:

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

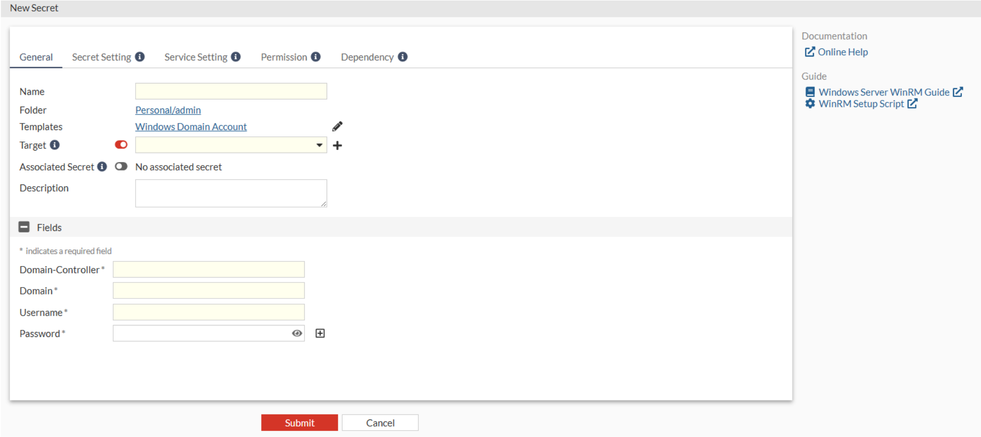
Creating a secret with Windows Domain Account as the secret template

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.



New Secret

General | Secret Setting | Service Setting | Permission | Dependency

Name	
Folder	Personal/admin
Templates	Windows Domain Account
Target	
Associated Secret	No associated secret
Description	

Fields

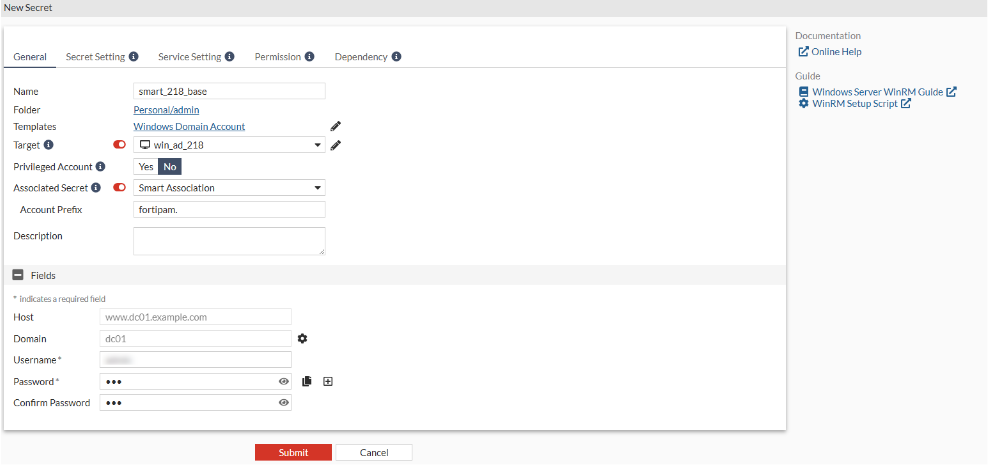
* indicates a required field

Domain-Controller *	
Domain *	
Username *	
Password *	

Documentation
Online Help
Guide
Windows Server WinRM Guide
WinRM Setup Script

Submit | Cancel

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*.



New Secret

General | Secret Setting | Service Setting | Permission | Dependency

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	

Fields

* indicates a required field

Host	www.dc01.example.com
Domain	dc01
Username *	[redacted]
Password *	•••
Confirm Password	•••

Documentation
Online Help
Guide
Windows Server WinRM Guide
WinRM Setup Script

Submit | Cancel

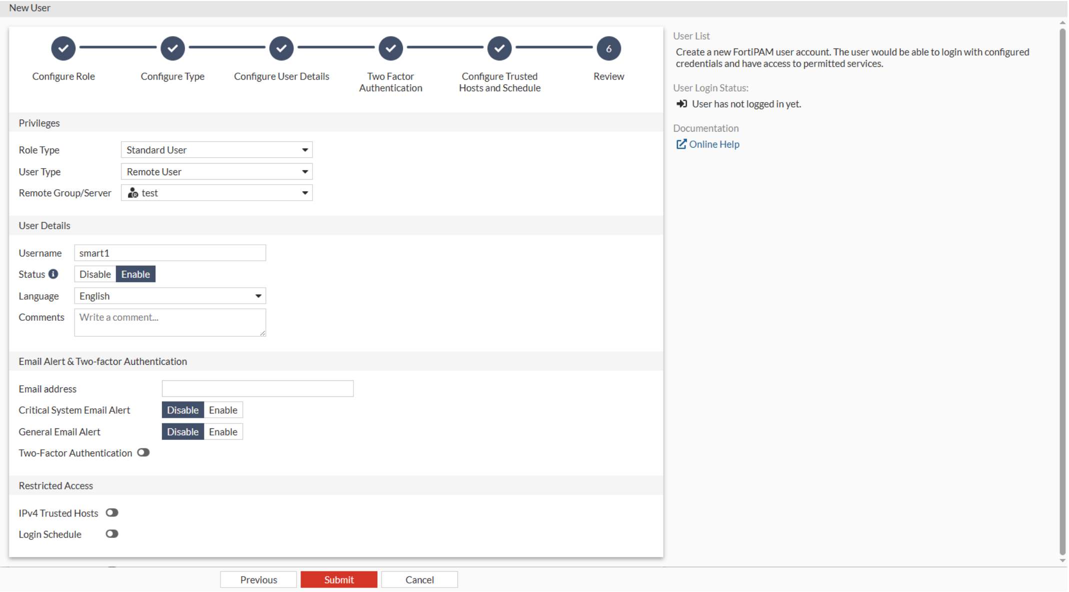
Creating a remote user

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.



New User

Configure Role
Configure Type
Configure User Details
Two Factor Authentication
Configure Trusted Hosts and Schedule
6
Review

Privileges

Role Type: Standard User
User Type: Remote User
Remote Group/Server: test

User Details

Username: smart1
Status: Disable [✓ Enable]
Language: English
Comments: Write a comment...

Email Alert & Two-factor Authentication

Email address:
Critical System Email Alert: [✓ Disable] Enable
General Email Alert: [✓ Disable] Enable
Two-Factor Authentication

Restricted Access

IPv4 Trusted Hosts
Login Schedule

User List

Create a new FortiPAM user account. The user would be able to login with configured credentials and have access to permitted services.

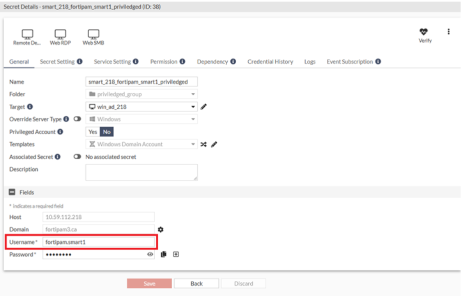
User Login Status:

User has not logged in yet.

Documentation

Online Help

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`.



Secret Details - smart_218_fortipam_smart1_priviledged (ID: 38)

Name: smart_218_fortipam_smart1_priviledged
Folder: priviledged_group
Target: win_ad_218
Override Server Type: Windows
Privileged Account: Yes [✓ No]
Templates: Windows Domain Account
Associated Secret: No associated secret
Description:

Fields

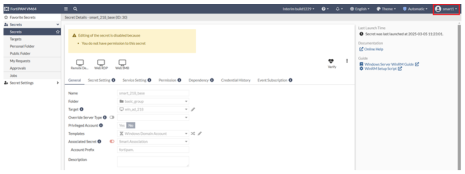
* indicates a required field

Host: 10.59.112.218
Domain: fortipam3.ca
Username *: fortipam.smart1
Password *: ••••••••

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.



Secret Details - smart_218_base (ID: 30)

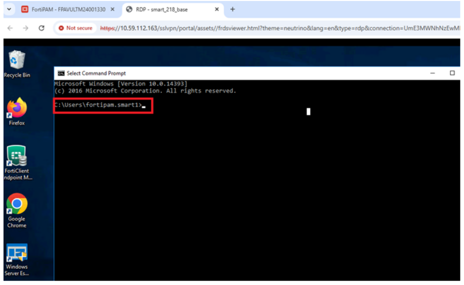
Editing of the secret is disabled because

- You do not have permission to this secret

Last Launch Time

Secret was last launched at 2025-03-05 11:23:01.

Name	smart_218_base
Folder	basic_group
Target	win_ad_218
Override Server Type	
Privileged Account	Yes [✓ No]
Templates	Windows Domain Account
Associated Secret	Smart Association
Account Prefix	fortipam.
Description	



https://10.59.112.163/sslvpn/portal/assets//frdsviewer.html?theme=neutrino&lang=en&type=rdp&connection=UmE3MWNhNzEwMI

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\fortipam.smart1>_
```

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 113
4. Sharing secrets to a contractor on page 114
5. Result on page 115

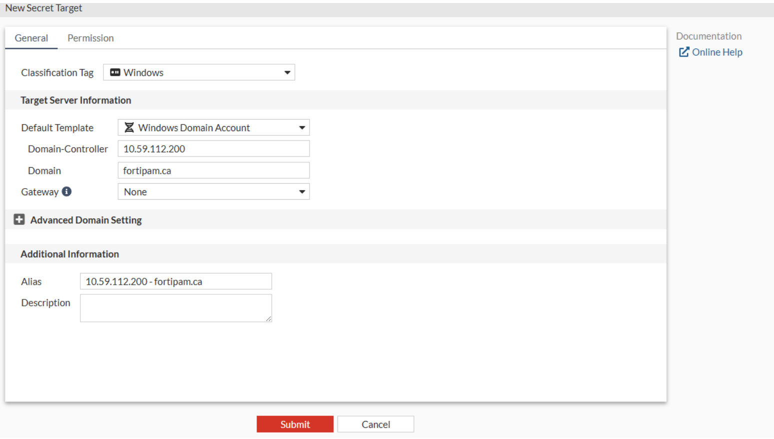
Creating targets

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 Accoun*t.
5. In *Domain-Controller*, enter the DC IP address.
6. In *Domain*, enter the domain.
    a. Click *Submit*.



Classification Tag: Windows

Target Server Information

Default Template: Windows Domain Account

Domain-Controller: 10.59.112.200

Domain: fortipam.ca

Gateway: None

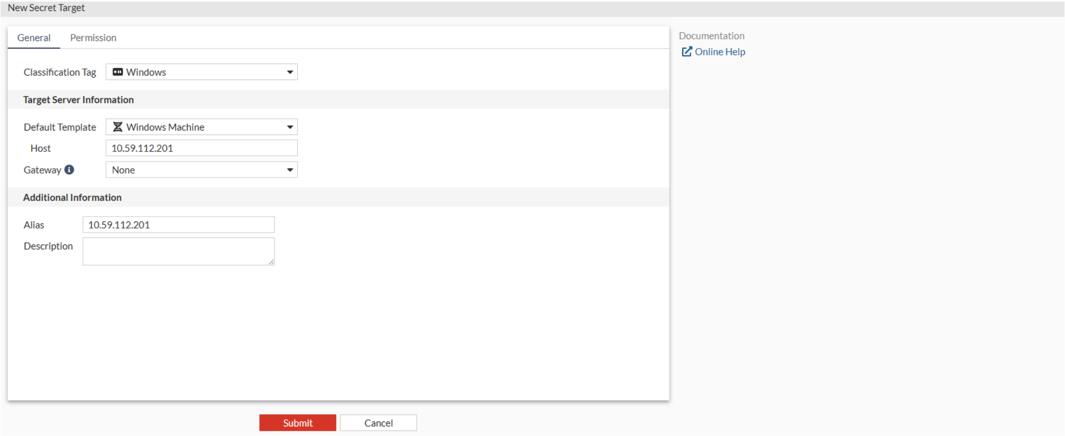
Additional Information

Alias: 10.59.112.200 - fortipam.ca

Description:

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`



Classification Tag: Windows

Target Server Information

Default Template: Windows Machine

Host: 10.59.112.201

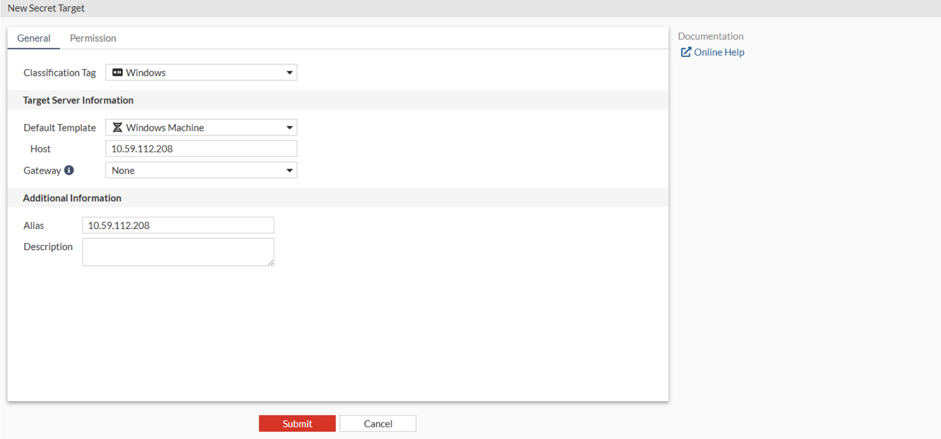
Gateway: None

Additional Information

Alias: 10.59.112.201

Description:

- **Windows PC-** `10.59.112.208`



New Secret Target

Classification Tag: Windows

Target Server Information

Default Template: Windows Machine

Host: 10.59.112.208

Gateway: None

Additional Information

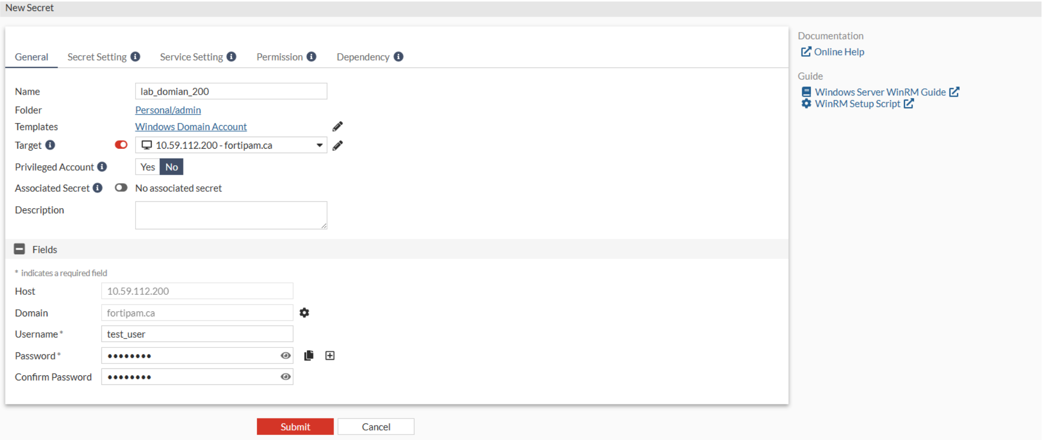
Alias: 10.59.112.208

Description:

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*.



New Secret

Name: lab_domian_200

Folder: Personal/admin

Templates: Windows Domain Account

Target: 10.59.112.200 - fortipam.ca

Privileged Account: Yes [✓ No]

Associated Secret: No associated secret

Description:

Fields

* indicates a required field

Host: 10.59.112.200

Domain: fortipam.ca

Username *: test_user

Password *: ••••••••

Confirm Password: ••••••••

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

To create a secret:

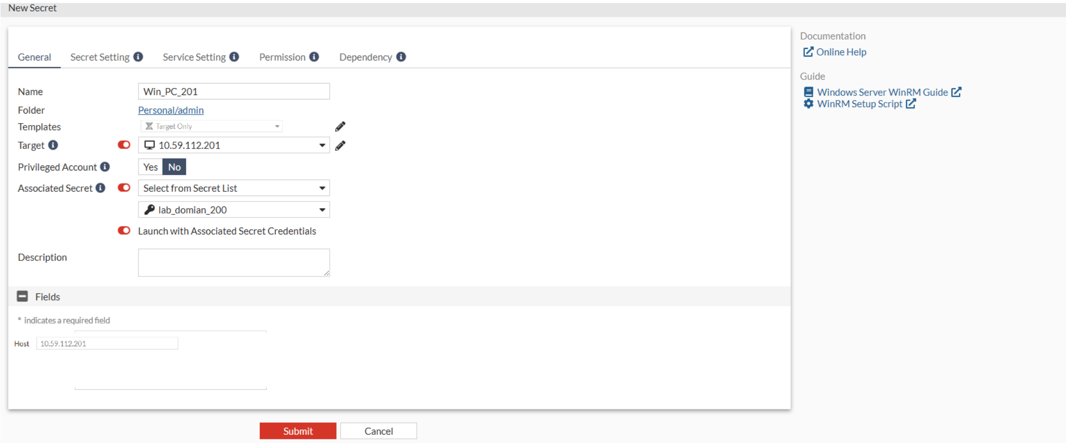
1. Go to *Secrets* > *Secrets*.
2. Select *+Create*.

   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*.



New Secret

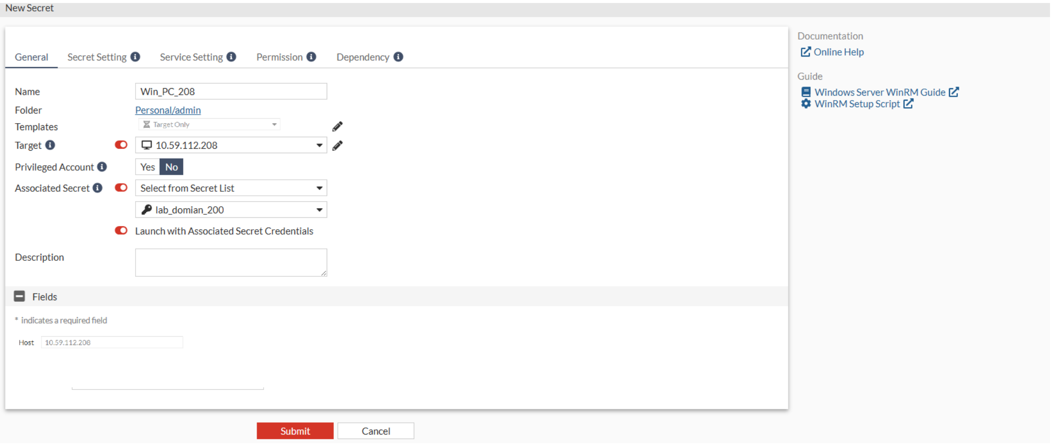
Name	Win_PC_201
Folder	Personal/admin
Templates	Target Only
Target	● 10.59.112.201
Privileged Account	Yes [✓ No]
Associated Secret	● Select from Secret List
	lab_domian_200
	● Launch with Associated Secret Credentials
Description	

Fields

* indicates a required field

Host	10.59.112.201

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



Name: Win_PC_208
Folder: Personal/admin
Templates: Target Only
Target: 10.59.112.208
Privileged Account: Yes [✓ No]
Associated Secret: Select from Secret List
lab_domian_200
Launch with Associated Secret Credentials
Description:

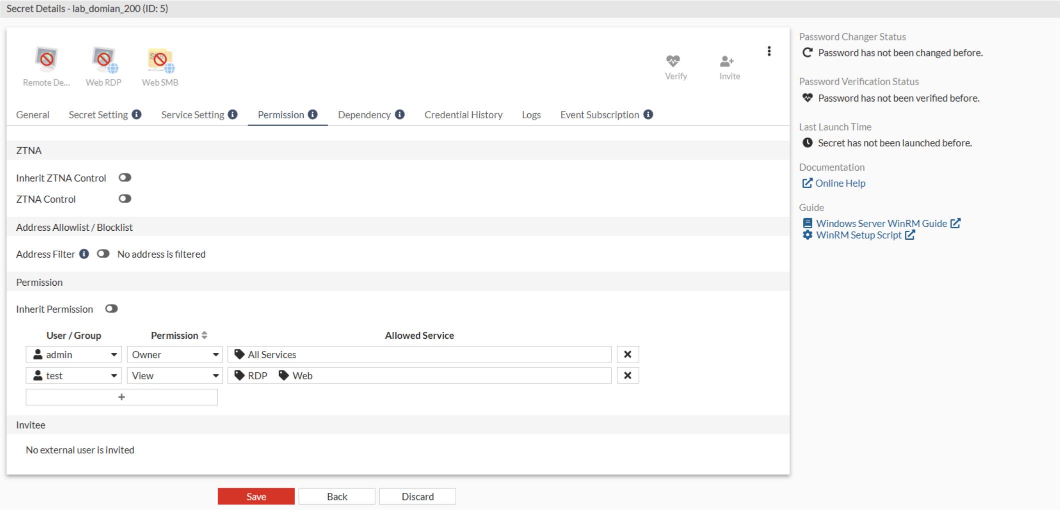
Fields
* indicates a required field
Host: 10.59.112.208

Documentation
Online Help
Guide
Windows Server WinRM Guide
WinRM Setup Script

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 113, 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*.



ZTNA
Inherit ZTNA Control
ZTNA Control

Address Allowlist / Blocklist
Address Filter: No address is filtered

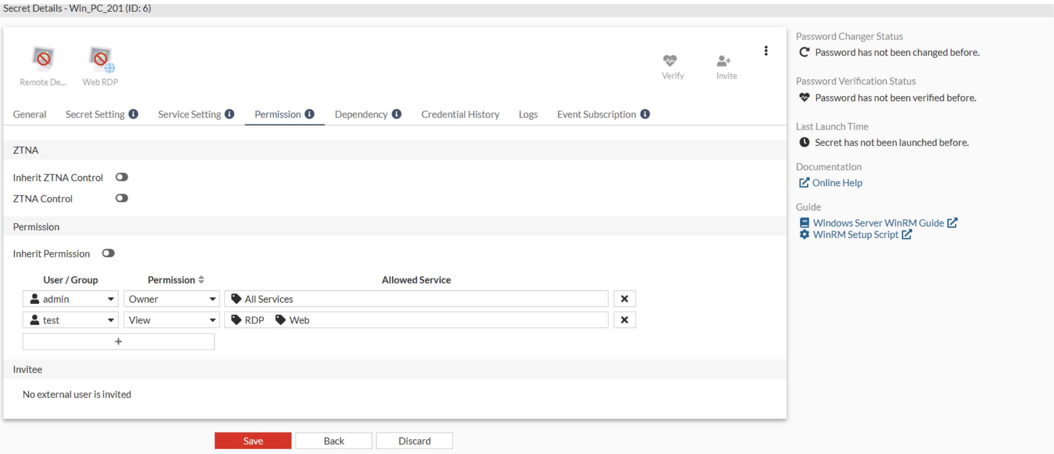
Permission
Inherit Permission

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

Invitee
No external user is invited

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

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 113.



Secret Details - Win_PC_201 (ID: 6)

ZTNA

Inherit ZTNA Control ○

ZTNA Control ○

Permission

Inherit Permission ○

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

Invitee

No external user is invited

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.

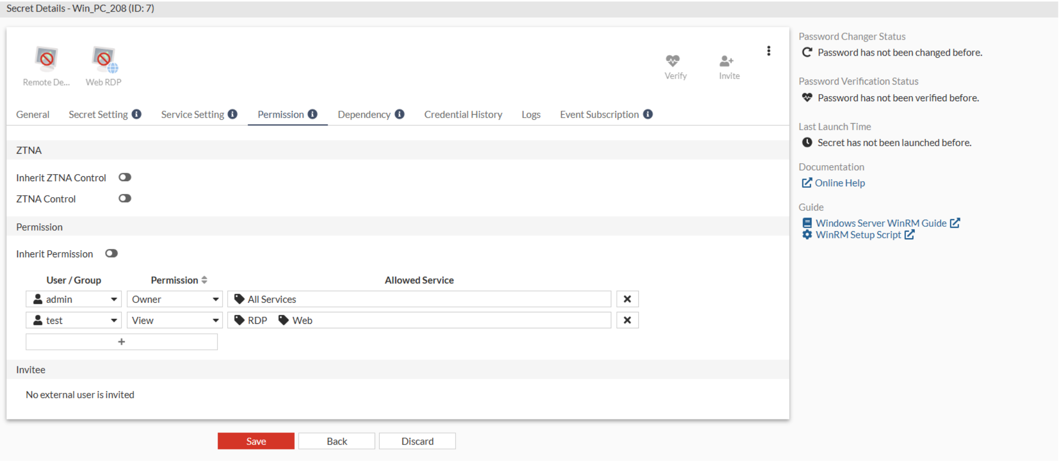
Documentation

Online Help

Guide

Windows Server WinRM Guide

WinRM Setup Script



Secret Details - Win_PC_208 (ID: 7)

ZTNA

Inherit ZTNA Control ○

ZTNA Control ○

Permission

Inherit Permission ○

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

Invitee

No external user is invited

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

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:

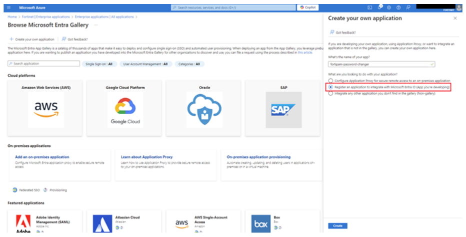
1. Configuring the Azure portal on page 116
2. Configuring FortiPAM on page 118
3. Results on page 119
4. Troubleshooting on page 120

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*.



[redacted]

Create your own application

Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

fortipam-password-changer

What are you looking to do with your application?

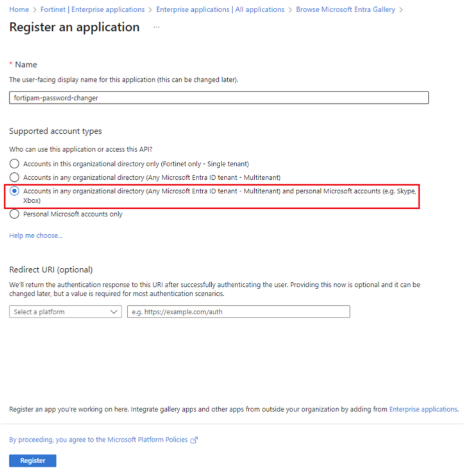
○ Configure Application Proxy for secure remote access to an on-premises application

● Register an application to integrate with Microsoft Entra ID (App you're developing)

○ Integrate any other application you don't find in the gallery (Non-gallery)

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)*.



Home > Fortinet | Enterprise applications > Enterprise applications | All applications > Browse Microsoft Entra Gallery >

Register an application ···

* Name

The user-facing display name for this application (this can be changed later).

fortipam-password-changer

Supported account types

Who can use this application or access this API?

○ Accounts in this organizational directory only (Fortinet only - Single tenant)

○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

● Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

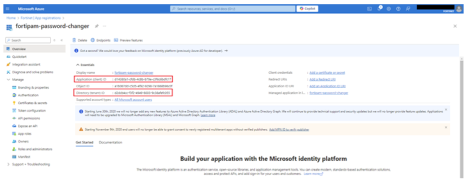
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform | e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

By proceeding, you agree to the Microsoft Platform Policies

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



[redacted]

Home > Fortinet | App registrations >

fortipam-password-changer

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name : fortipam-password-changer

Application (client) ID : d14380a1-cfdb-4c8b-b79e-c3f6c6bdfc17

Object ID : a1b067dd-c5d5-4f92-9298-7a1868b96c0f

Directory (tenant) ID : d2dcb4cc-f3f2-4949-8003-9c38afefc055

Supported account types : All Microsoft account users

Client credentials : Add a certificate or secret

Redirect URIs : Add a Redirect URI

Application ID URI : Add an Application ID URI

Managed application in l... : fortipam-password-changer

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Starting November 9th, 2020 end users will no longer be able to grant consent to newly registered multitenant apps without verified publishers. Add MPN ID to verify publisher

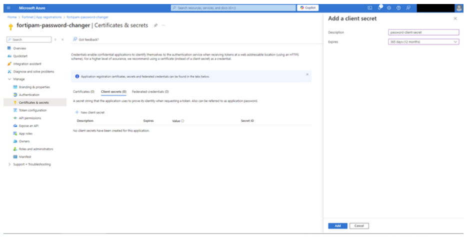
Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. Learn more

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.



[redacted]

Home > Fortinet | App registrations > fortipam-password-changer

fortipam-password-changer | Certificates & secrets

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID

No client secrets have been created for this application.

Add a client secret

Description: password-client-secret

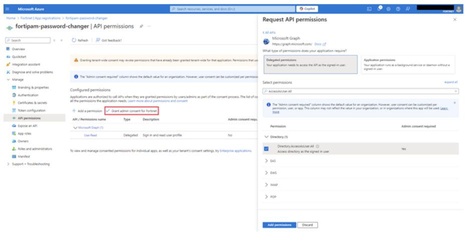
Expires: 365 days (12 months)

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.



Granting tenant-wide consent may revoke permissions that have already been granted tenant-wide for that application. Permissions that us

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permissio

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of co all the permissions the application needs. Learn more about permissions and consent

+ Add a permission ✓ Grant admin consent for Fortinet

API / Permissions name	Type	Description	Admin consent requ...
Microsoft Graph (1)			
User.Read	Delegated	Sign in and read user profile	No

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try Enterprise applications.

Request API permissions

< All APIs

Microsoft Graph
https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions Your application needs to access the API as the signed-in user.

Application permissions Your application runs as a background service or daemon without a signed-in user.

Select permissions — expand all

AccessAsUser.All

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. Learn more

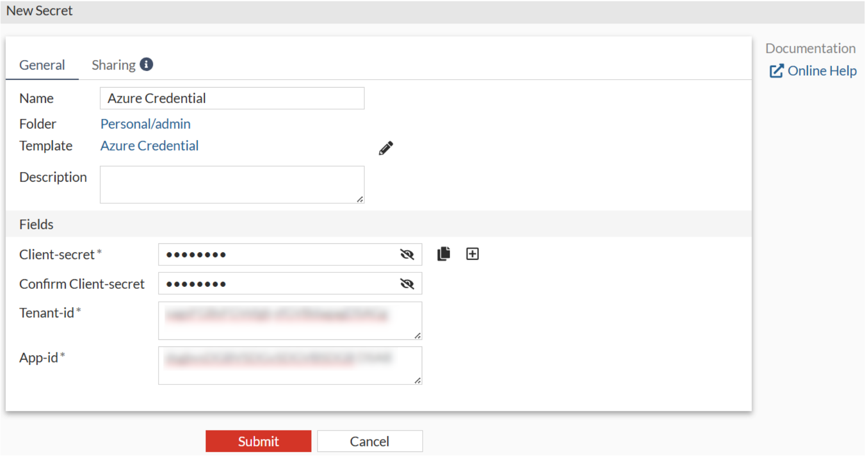
Permission	Admin consent required
Directory (1)	
☑ Directory.AccessAsUser.All Access directory as the signed in user	Yes
EAS	
EWS	
IMAP	
POP	

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 117.
    b. Enter the *Tenant-id*.
    The *Tenant-id* is the *Directory (tenant) ID* from step 4 in Register an Enterprise Application on page 116.
    c. Enter the *App-id*.
    The *App-id* is the *Application (client) ID* from step 4 in Register an Enterprise Application on page 116.
5. Click *Submit* to save the secret.



Name	Azure Credential
Folder	Personal/admin
Template	Azure Credential
Description	

Fields

Client-secret *	••••••••
Confirm Client-secret	••••••••
Tenant-id *	[redacted]
App-id *	[redacted]

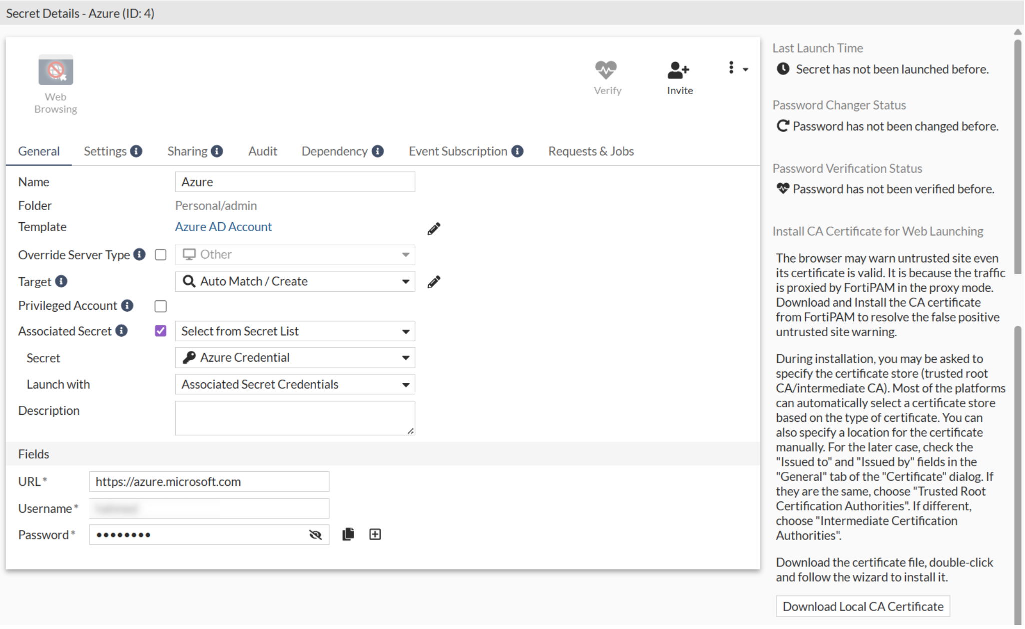
Creating *Azure AD Account* secret

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 118.
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.



Secret Details - Azure (ID: 4)

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	

Fields

URL *	https://azure.microsoft.com
Username *	[redacted]
Password *	••••••••

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.

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*.

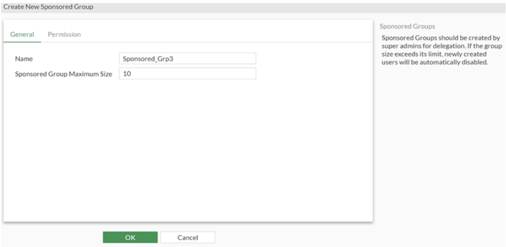
To create sponsored administrator that audits secret activities:

1. Creating a sponsored group on page 121
2. Creating a sponsor admin on page 122
3. Creating a secret with view permission for the sponsored group on page 123
4. Creating sponsored group members on page 124
5. Auditing on page 126

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`.



Create New Sponsored Group

Name: Sponsored_Grp3

Sponsored Group Maximum Size: 10

Sponsored Groups

Sponsored Groups should be created by super admins for delegation. If the group size exceeds its limit, newly created users will be automatically disabled.

4. Click *OK*.

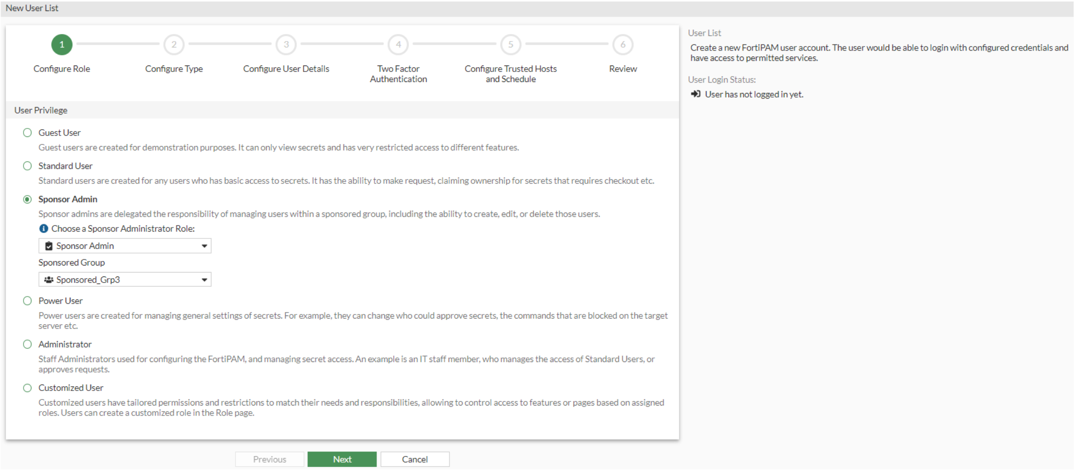
Creating a sponsor admin

We now create a sponsor admin assigned to the sponsored group created in Creating a sponsored group on page 121.

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 121.

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



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: Sponsor Admin
Sponsored Group: Sponsored_Grp3

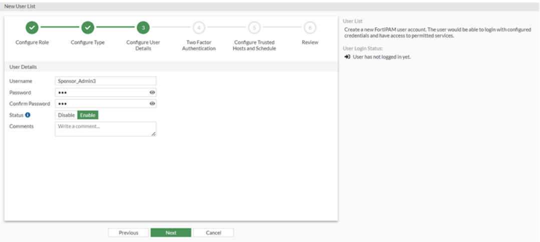
○ Power User
Power users are created for managing general settings of secrets. For example, they can change who could approve secrets, the commands that are blocked on the target server etc.

○ 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.

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.

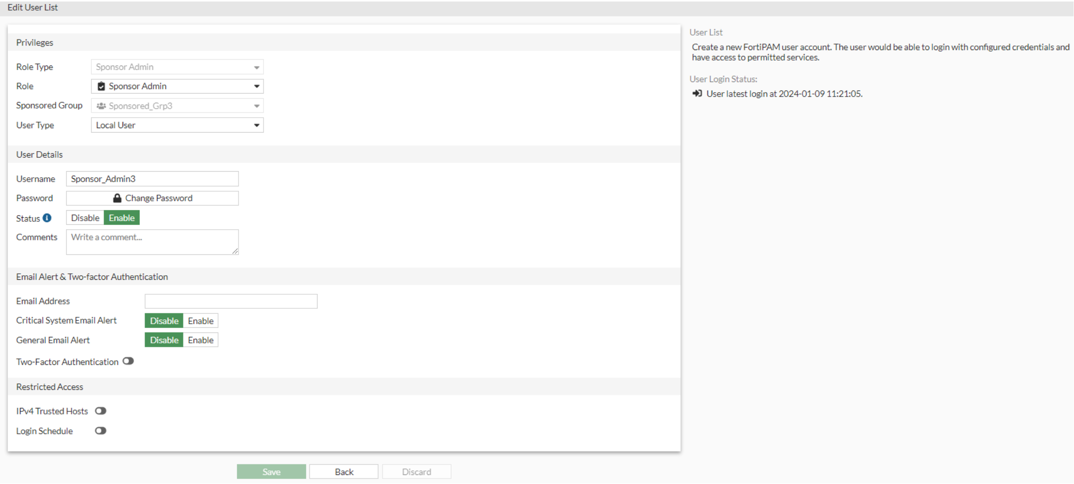


User Details
Username: Sponsor_Admin3
Password: •••
Confirm Password: •••
Status: Disable **Enable**
Comments: Write a comment...

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*.



Edit User List

Privileges

Role Type: Sponsor Admin
Role: Sponsor Admin
Sponsored Group: Sponsored_Grp3
User Type: Local User

User Details

Username: Sponsor_Admin3
Password: Change Password
Status: Disable [✓ Enable]
Comments: Write a comment...

Email Alert & Two-factor Authentication

Email Address:
Critical System Email Alert: [✓ Disable] Enable
General Email Alert: [✓ Disable] Enable
Two-Factor Authentication ○

Restricted Access

IPv4 Trusted Hosts ○
Login Schedule ○

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 latest login at 2024-01-09 11:21:05.

Creating a secret with view permission for the sponsored group

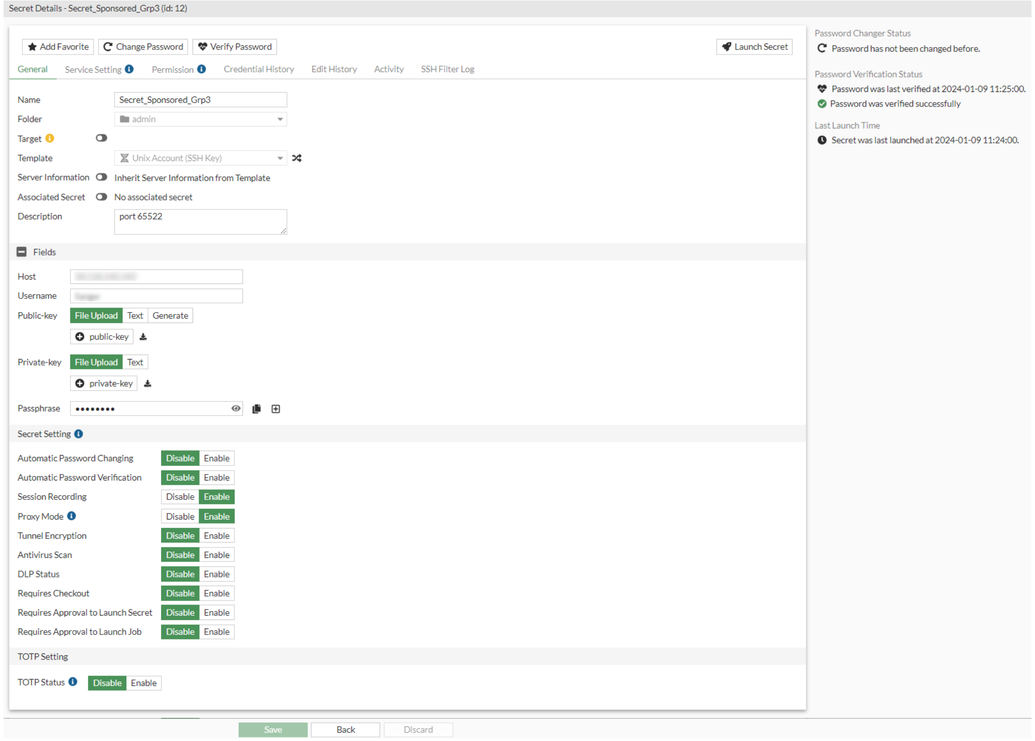
We create a secret with view permission for the sponsored group created in Creating a sponsored group on page 121.

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 121.
   iii. In *Permission*, select *View*.
   iv. Click *OK*.

7. Click *Submit*.



Secret Details - Secret_Sponsored_Grp3 (id: 12)

Add Favorite | Change Password | Verify Password | Launch Secret

General | Service Setting | Permission | Credential History | Edit History | Activity | SSH Filter Log

Name	Secret_Sponsored_Grp3
Folder	admin
Target	
Template	Unix Account (SSH Key)
Server Information	Inherit Server Information from Template
Associated Secret	No associated secret
Description	port 65522

Fields

Host	[redacted]
Username	[redacted]
Public-key	File Upload | Text | Generate public-key
Private-key	File Upload | Text private-key
Passphrase	••••••••

Secret Setting

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

TOTP Setting

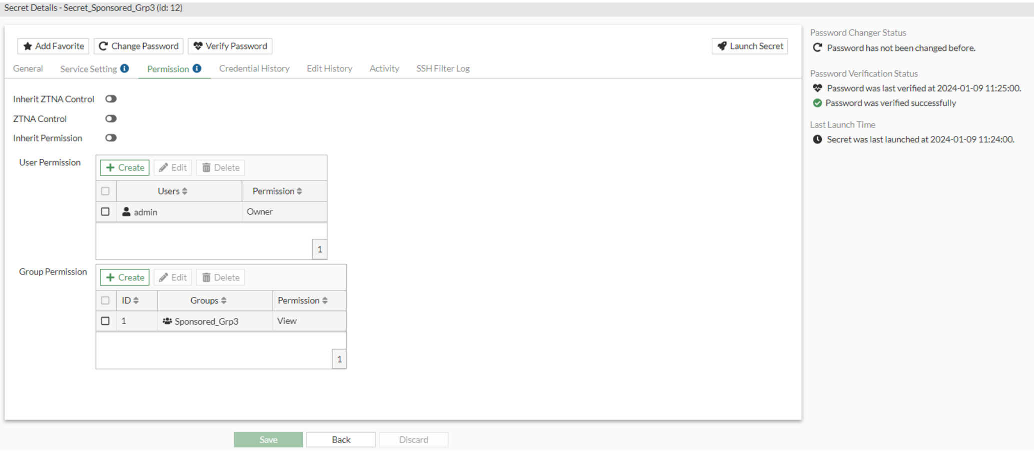
TOTP Status	Disable

Save | Back | Discard

Password Changer Status
Password has not been changed before.

Password Verification Status
Password was last verified at 2024-01-09 11:25:00.
Password was verified successfully

Last Launch Time
Secret was last launched at 2024-01-09 11:24:00.



Secret Details - Secret_Sponsored_Grp3 (id: 12)

Add Favorite | Change Password | Verify Password | Launch Secret

General | Service Setting | Permission | Credential History | Edit History | Activity | SSH Filter Log

Inherit ZTNA Control
ZTNA Control
Inherit Permission

User Permission

Create | Edit | Delete

☐	Users	Permission
☐	admin	Owner

Group Permission

Create | Edit | Delete

☐	ID	Groups	Permission
☐	1	Sponsored_Grp3	View

Save | Back | Discard

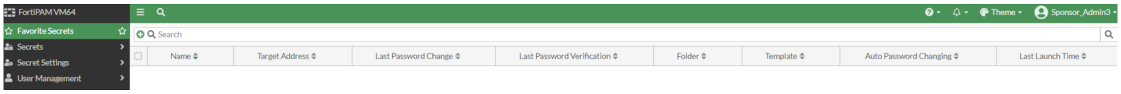
Password Changer Status
Password has not been changed before.

Password Verification Status
Password was last verified at 2024-01-09 11:25:00.
Password was verified successfully

Last Launch Time
Secret was last launched at 2024-01-09 11:24:00.

Creating sponsored group members

The sponsor admin created in Creating a sponsor admin on page 122 logs in to the FortiPAM.



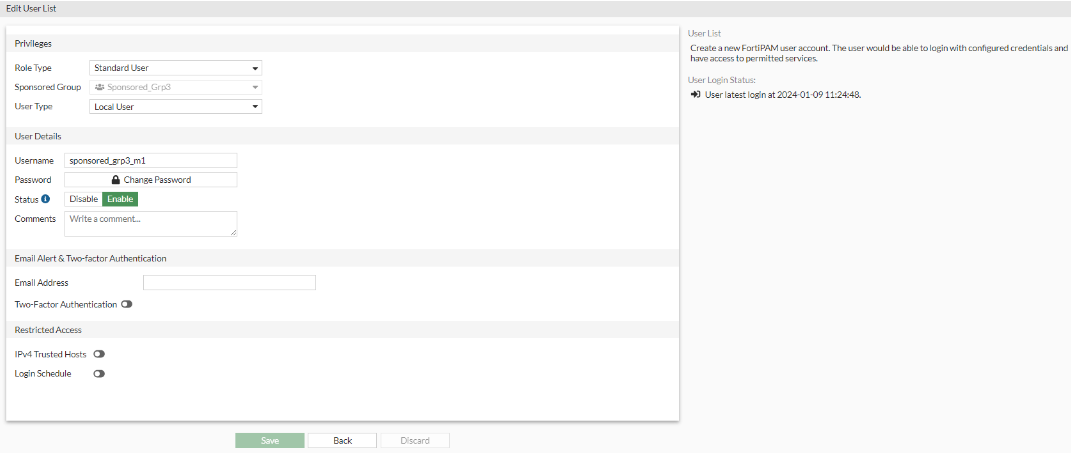
☐	Name	Target Address	Last Password Change	Last Password Verification	Folder	Template	Auto Password Changing	Last Launch Time

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 121.

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*.



Edit User List

Privileges

Role Type: Standard User

Sponsored Group: Sponsored_Grp3

User Type: Local User

User Details

Username: sponsored_grp3_m1

Password: Change Password

Status: Disable **Enable**

Comments: Write a comment...

Email Alert & Two-factor Authentication

Email Address:

Two-Factor Authentication ○

Restricted Access

IPv4 Trusted Hosts ○

Login Schedule ○

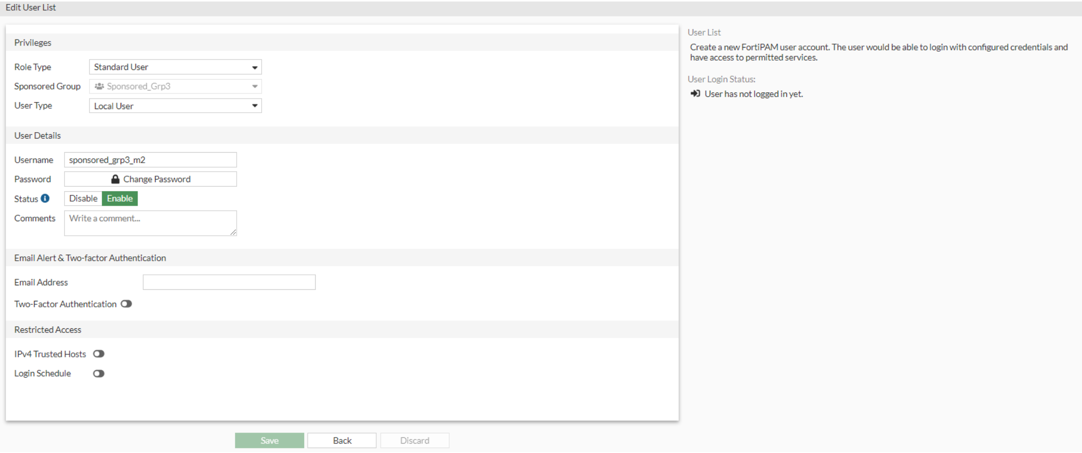
User List

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 latest login at 2024-01-09 11:24:48.

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



Edit User List

Privileges

Role Type: Standard User

Sponsored Group: Sponsored_Grp3

User Type: Local User

User Details

Username: sponsored_grp3_m2

Password: Change Password

Status: Disable [✓ Enable]

Comments: Write a comment...

Email Alert & Two-factor Authentication

Email Address:

Two-Factor Authentication

Restricted Access

IPv4 Trusted Hosts

Login Schedule

User List

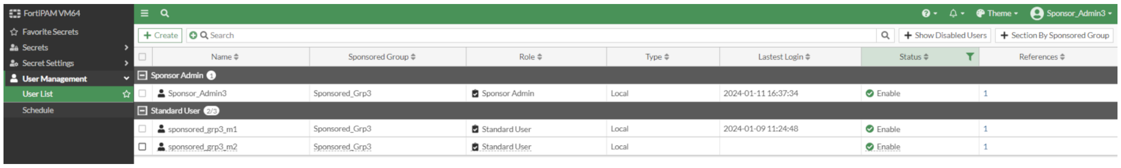
Create a new FortiPAM user account. The user would be able to login with configured credentials and have access to permitted services.

User Login Status:

User has not logged in yet.

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 121.

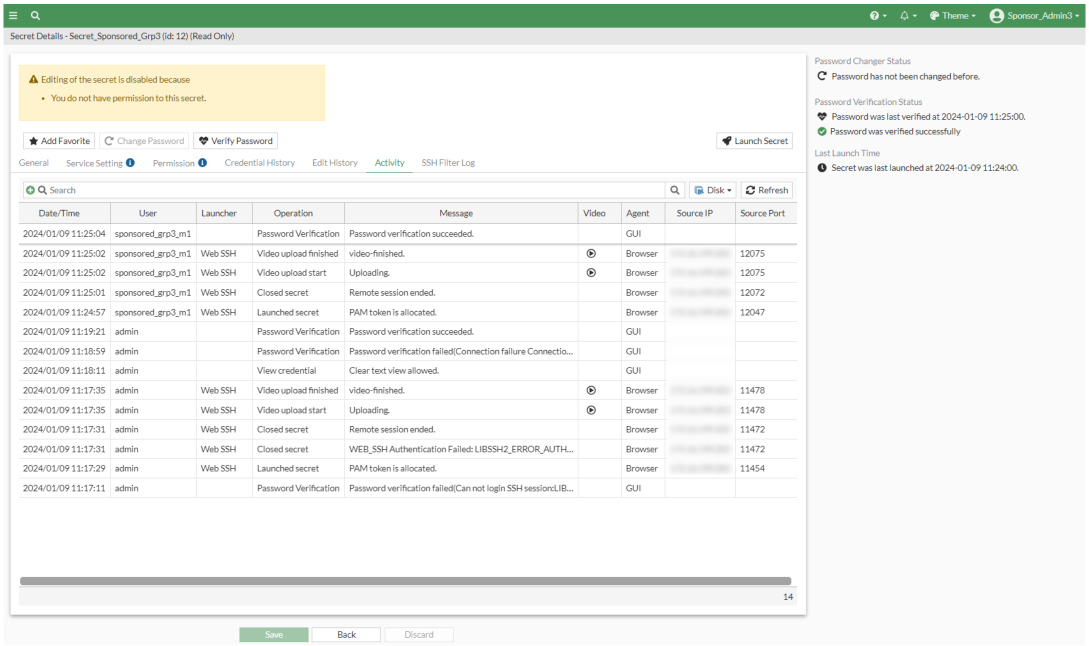
For a sponsor admin with two users in the sponsored group, the *User List* in *User Management* is shown below:



Name	Sponsored Group	Role	Type	Lastest Login	Status	References
Sponsor Admin 1						
Sponsor_Admin3	Sponsored_Grp3	Sponsor Admin	Local	2024-01-11 16:37:34	Enable	1
Standard User 2/3						
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 123, the sponsor admin configured in Creating a sponsor admin on page 122 can check secret activities by double-clicking the secret in *Secrets > Secret List* and going to the *Activity* tab.



Secret Details - Secret_Sponsored_Grp3 (id: 12) (Read Only)

Editing of the secret is disabled because

- You do not have permission to this secret.

Date/Time	User	Launcher	Operation	Message	Video	Agent	Source IP	Source Port
2024/01/09 11:25:04	sponsored_grp3_m1		Password Verification	Password verification succeeded.		GUI		
2024/01/09 11:25:02	sponsored_grp3_m1	Web SSH	Video upload finished	video-finished.	▶	Browser	[redacted]	12075
2024/01/09 11:25:02	sponsored_grp3_m1	Web SSH	Video upload start	Uploading.	▶	Browser	[redacted]	12075
2024/01/09 11:25:01	sponsored_grp3_m1	Web SSH	Closed secret	Remote session ended.		Browser	[redacted]	12072
2024/01/09 11:24:57	sponsored_grp3_m1	Web SSH	Launched secret	PAM token is allocated.		Browser	[redacted]	12047
2024/01/09 11:19:21	admin		Password Verification	Password verification succeeded.		GUI		
2024/01/09 11:18:59	admin		Password Verification	Password verification failed(Connection failure Connectio...		GUI		
2024/01/09 11:18:11	admin		View credential	Clear text view allowed.		GUI		
2024/01/09 11:17:35	admin	Web SSH	Video upload finished	video-finished.	▶	Browser	[redacted]	11478
2024/01/09 11:17:35	admin	Web SSH	Video upload start	Uploading.	▶	Browser	[redacted]	11478
2024/01/09 11:17:31	admin	Web SSH	Closed secret	Remote session ended.		Browser	[redacted]	11472
2024/01/09 11:17:31	admin	Web SSH	Closed secret	WEB_SSH Authentication Failed: LIBSSH2_ERROR_AUTH...		Browser	[redacted]	11472
2024/01/09 11:17:29	admin	Web SSH	Launched secret	PAM token is allocated.		Browser	[redacted]	11454
2024/01/09 11:17:11	admin		Password Verification	Password verification failed(Can not login SSH session:LIB...		GUI		

14

Password Changer Status

Password has not been changed before.

Password Verification Status

Password was last verified at 2024-01-09 11:25:00.

Password was verified successfully

Last Launch Time

Secret was last launched at 2024-01-09 11:24:00.

Web proxy

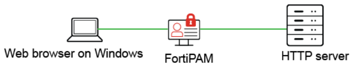
This section describes configuring web proxy on FortiPAM.

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 127
2. Creating a secret target with web proxy on page 128
3. Creating a secret with web proxy on page 129

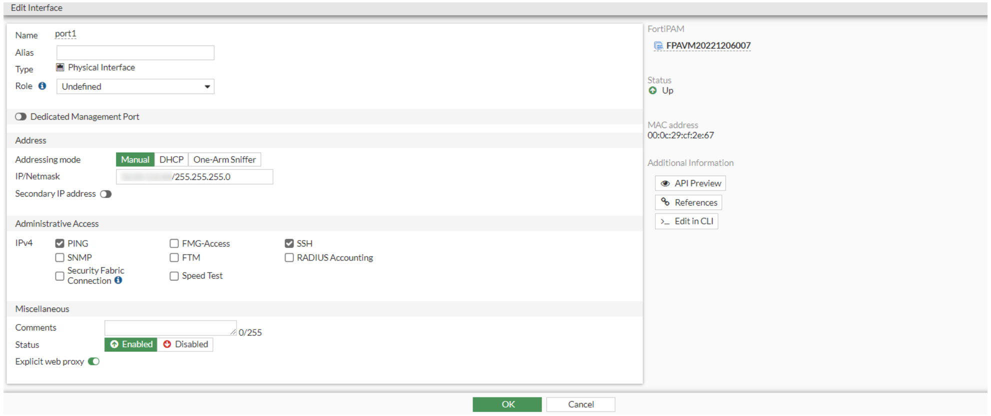
If FortiPAM is behind a FortiGate device, see FortiPAM behind a FortiGate device on page 130.

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*.



Edit Interface

Name port1
Alias
Type Physical Interface
Role Undefined

Dedicated Management Port

Address
Addressing mode [✓ Manual] DHCP One-Arm Sniffer
IP/Netmask [redacted]/255.255.255.0
Secondary IP address

Administrative Access
IPv4 ☑ PING ☐ FMG-Access ☑ SSH
☐ SNMP ☐ FTM ☐ RADIUS Accounting
☐ Security Fabric Connection ☐ Speed Test

Miscellaneous
Comments 0/255
Status [✓ Enabled] Disabled
Explicit web proxy

FortiPAM
FPAVM20221206007
Status
Up
MAC address
00:0c:29:cf:2e:67
Additional Information

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
```

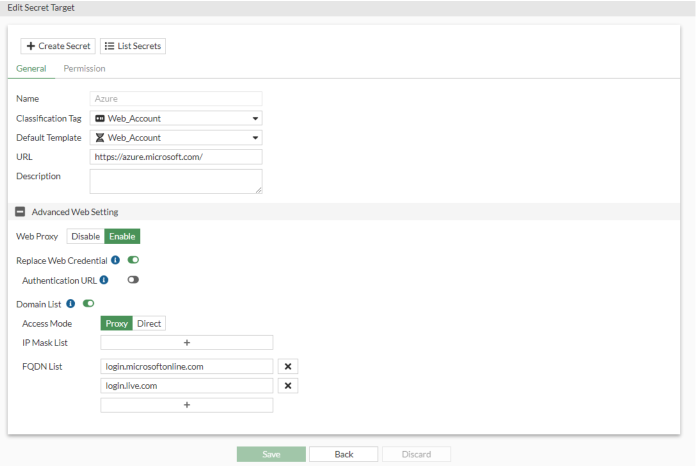
4. Click *OK*.

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*.



Name: Azure
Classification Tag: Web_Account
Default Template: Web_Account
URL: https://azure.microsoft.com/
Description:
Web Proxy: Disable [✓ Enable]
Replace Web Credential: ●
Authentication URL: ○
Domain List: ●
Access Mode: [✓ Proxy] Direct
IP Mask List: +
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 128.
      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 128.
   c. Fill in the remaining fields.

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

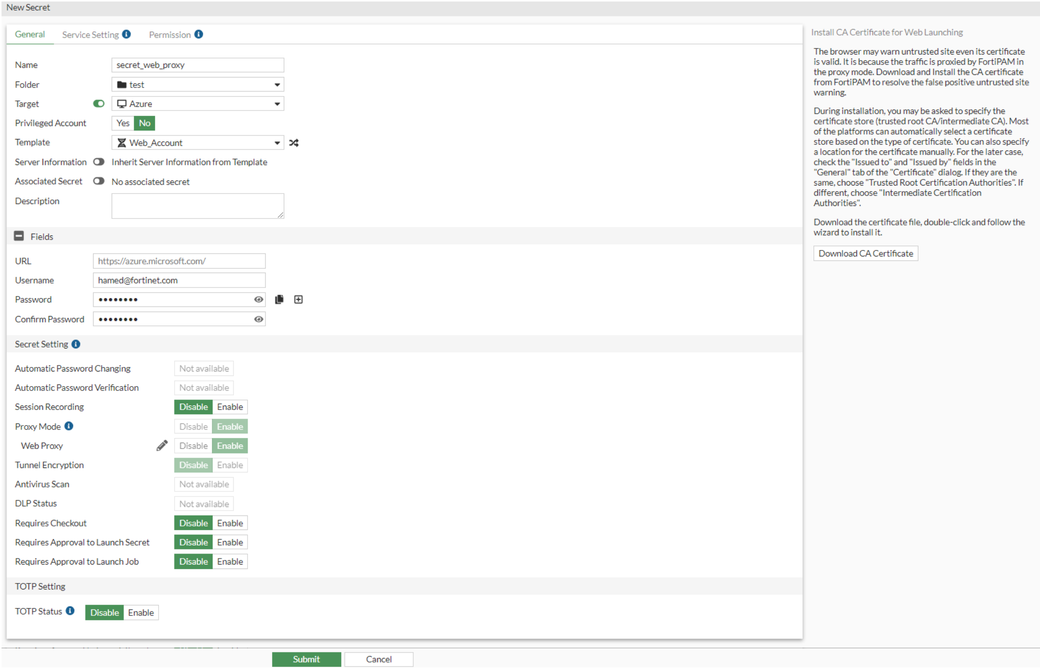
> The *Web Proxy* option is only available when *Proxy Mode* is enabled.

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.



New Secret

General | Service Setting | Permission

Name	secret_web_proxy
Folder	test
Target	Azure
Privileged Account	Yes [✓ No]
Template	Web_Account
Server Information	Inherit Server Information from Template
Associated Secret	No associated secret
Description	

Fields

URL	https://azure.microsoft.com/
Username	hamed@fortinet.com
Password	••••••••
Confirm Password	••••••••

Secret Setting

Automatic Password Changing	Not available
Automatic Password Verification	Not available
Session Recording	[✓ Disable] Enable
Proxy Mode	Disable [✓ Enable]
Web Proxy	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

TOTP Setting

TOTP Status	[✓ Disable] Enable

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.

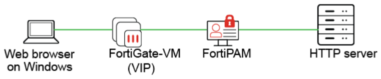
During installation, you may be asked to specify the certificate store (trusted root CA/intermediate CA). Most of the platforms can automatically select a certificate store based on the type of certificate. You can also specify a location for the certificate manually. For the later case, check the "Issued 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.

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 127.

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*.

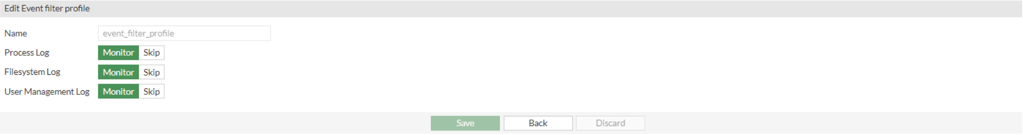
To configure RDP log retrieval on FortiPAM:

1. Creating an event filter profile on page 132
2. Creating a secret target on page 133
3. Creating a secret policy on page 133
4. Creating secret with an RDP event filter profile on page 134
5. Launching the secret on page 135
6. Checking the RDP logs on page 136

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*.



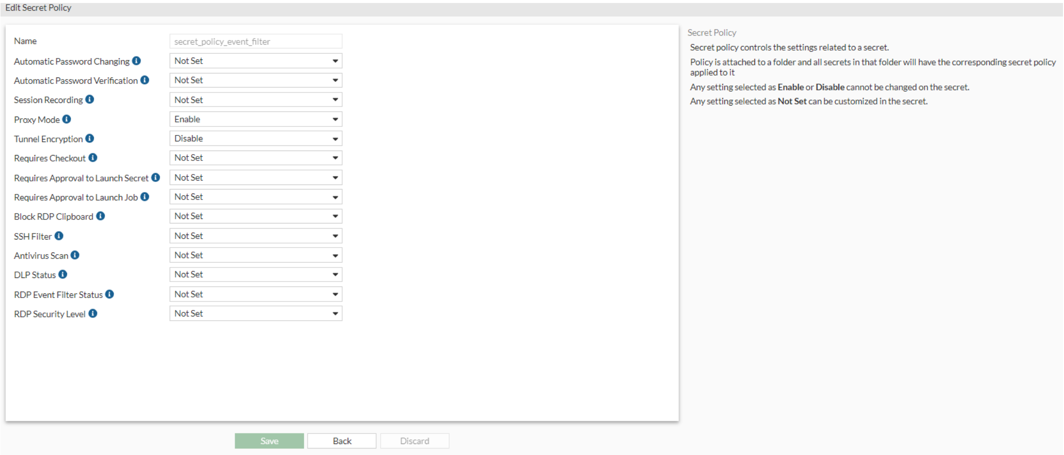
Edit Event filter profile

Name	event_filter_profile
Process Log	Monitor Skip
Filesystem Log	Monitor Skip
User Management Log	Monitor Skip

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*.



Edit Secret Policy

Name	secret_policy_event_filter
Automatic Password Changing	Not Set
Automatic Password Verification	Not Set
Session Recording	Not Set
Proxy Mode	Enable
Tunnel Encryption	Disable
Requires Checkout	Not Set
Requires Approval to Launch Secret	Not Set
Requires Approval to Launch Job	Not Set
Block RDP Clipboard	Not Set
SSH Filter	Not Set
Antivirus Scan	Not Set
DLP Status	Not Set
RDP Event Filter Status	Not Set
RDP Security Level	Not Set

Secret Policy

Secret policy controls the settings related to a secret.

Policy is attached to a folder and all secrets in that folder will have the corresponding secret policy applied to it

Any setting selected as **Enable** or **Disable** cannot be changed on the secret.

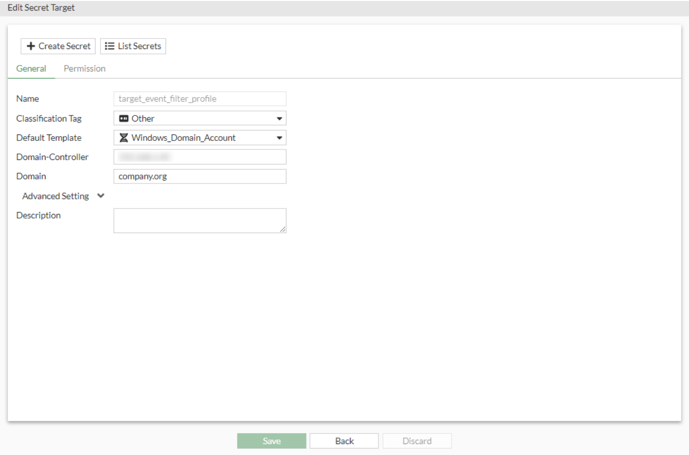
Any setting selected as **Not Set** can be customized in the secret.

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*.



Name	target_event_filter_profile
Classification Tag	Other
Default Template	Windows_Domain_Account
Domain-Controller	[redacted]
Domain	company.org
Description	

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 133.
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 133.
   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.

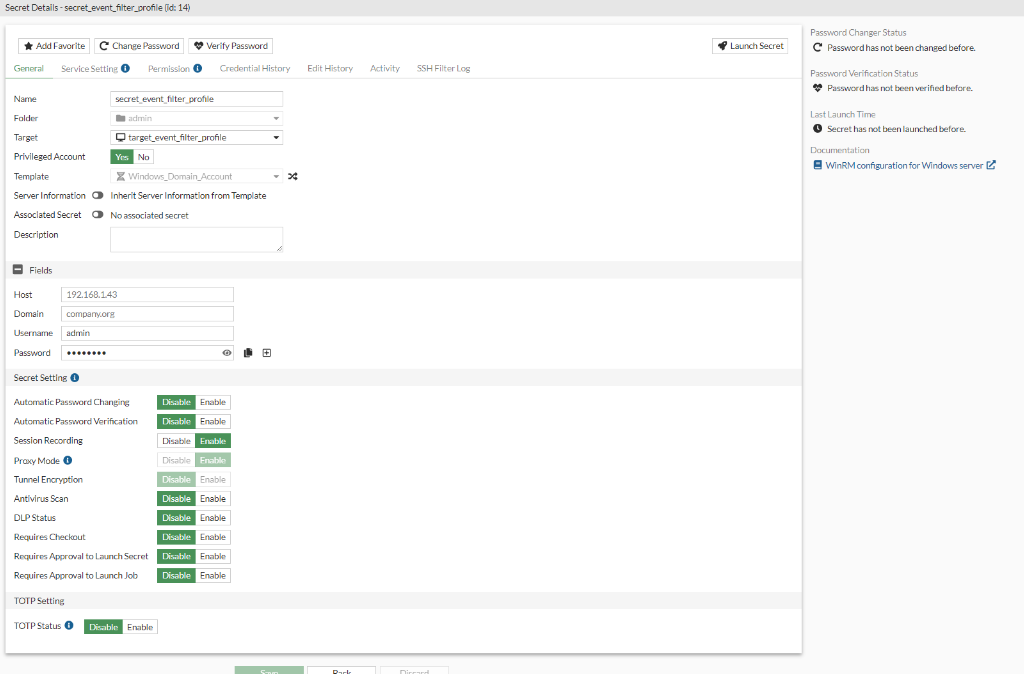
   The template is the custom template used in Creating a secret target on page 133.

   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 132.

6. Click *Submit*.



Secret Details - secret_event_filter_profile (id: 14)

Name: secret_event_filter_profile
Folder: admin
Target: target_event_filter_profile
Privileged Account: [✓ Yes] No
Template: Windows_Domain_Account
Server Information: Inherit Server Information from Template
Associated Secret: No associated secret
Description:

Fields

Host: 192.168.1.43
Domain: company.org
Username: admin
Password: ••••••••

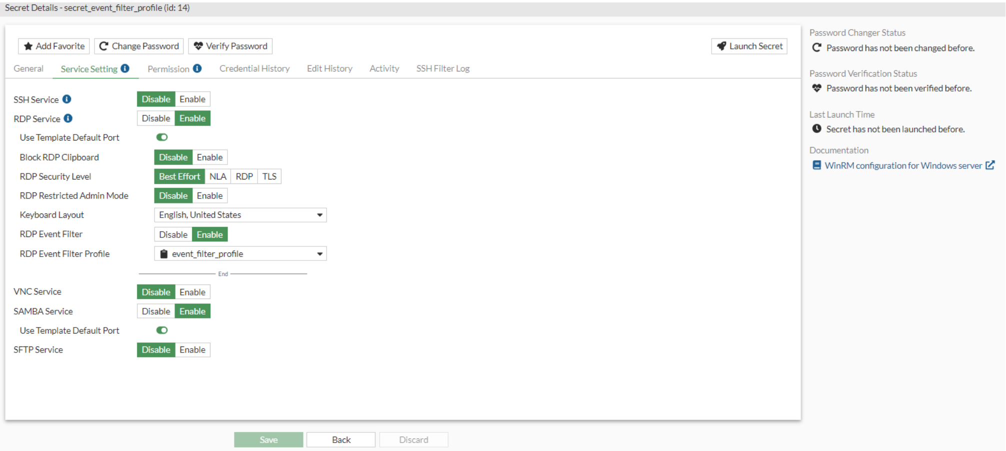
Secret Setting

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

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: WinRM configuration for Windows server



Secret Details - secret_event_filter_profile (id: 14)

SSH Service: [✓ Disable] Enable
RDP Service: Disable [✓ Enable]
Use Template Default Port: ●
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
End
VNC Service: [✓ Disable] Enable
SAMBA Service: Disable [✓ Enable]
Use Template Default Port: ●
SFTP Service: [✓ Disable] Enable

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: WinRM configuration for Windows server

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 134, 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.

5. On the target server, perform some operations:
   a. *Process log*: Open Chrome/Firefox, open close Control Panel, etc.
   b. *Filesystem log*: Create/delete text files, etc.
   c. *User Management log*: create/delete users, etc.
6. Close the launcher.

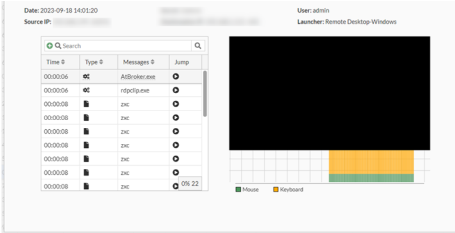
Checking the RDP logs

To check the RDP logs:

1. Go to *Log & Report > Secret*.
2. Select *Secret Video*.
3. Select the log with the operation labelled as *Video Finish*, then click the *Details* button located at the right of the menu. Alternatively, double-click the log labelled as *Video Finish*.

   The video player opens.

   You can now check the secret video.



Date: 2023-09-18 14:01:20 [redacted] **User:** admin

Source IP: [redacted] [redacted] **Launcher:** Remote Desktop-Windows

Time	Type	Messages	Jump
00:00:06	⚙	AtBroker.exe	▶
00:00:06	⚙	rdpclip.exe	▶
00:00:08	🗎	zxc	▶
00:00:08	🗎	zxc	▶
00:00:08	🗎	zxc	▶
00:00:08	🗎	zxc	▶
00:00:08	🗎	zxc	▶
00:00:08	🗎	zxc	▶
00:00:08	🗎	zxc	▶

Gateway

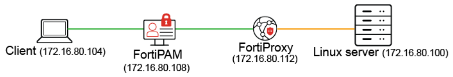
This section describes examples related to the FortiPAM network gateway and reverse gateway feature for distributed target deployment.

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 137
2. Creating the secret target on FortiPAM on page 138
3. FortiProxy related configurations on page 138

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 137
  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 138
  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:

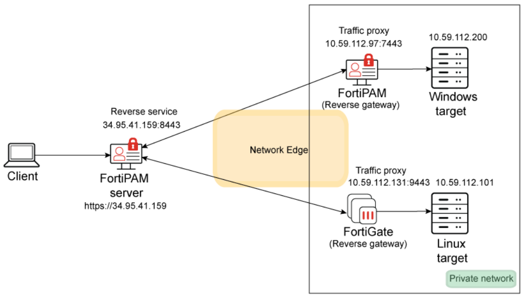
```
 config firewall policy
  edit 1
   set type access-proxy
   set srcintf "any"
   set srcaddr "all"
   set dstaddr "all"
   set action accept
   set schedule "always"
   set access-proxy "test_access_proxy" #from  Configuring an IPv4 access proxy on
FortiProxy on page 138
  next
 end
```

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: `foritpam_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):

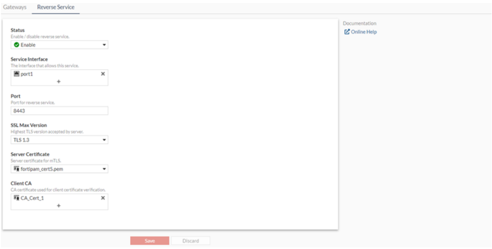
1. Configuring the reverse service on FortiPAM (control plane) on page 141
2. Configuring reverse service on the gateway (control plane) on page 141

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 currect 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*.



Status
Enable / disable reverse service.
Enable

Service Interface
The interface that allows this service.
port1

Port
Port for reverse service.
8443

SSL Max Version
Highest TLS version accepted by server.
TLS 1.3

Server Certificate
Server certificate for mTLS.
fortipam_cert5.pem

Client CA
CA certificate used for client certificate verification.
CA_Cert_1

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 141
   set port 8443 #same as the one on Port configured in Configuring the reverse service on
FortiPAM (control plane) on page 141
   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 141
    set port 8443 #same as the one on Port configured in Configuring the reverse service on
FortiPAM (control plane) on page 141
    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 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_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
```

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

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 142.
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.

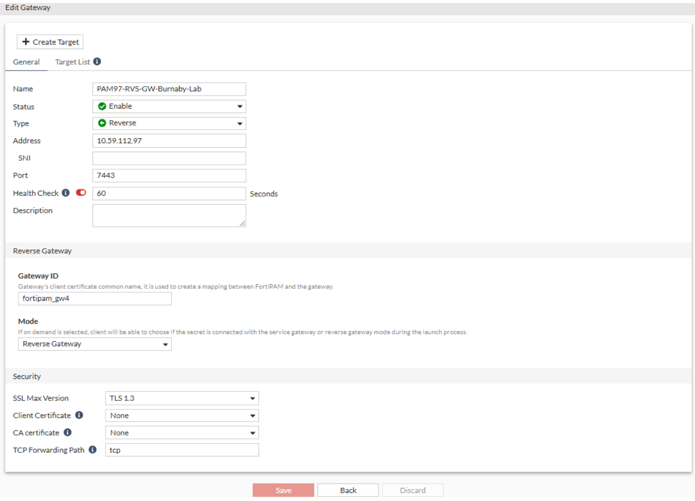
    The *Client Certificate* is the current server certificate for secret launch.

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 142.

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*.



Name: PAM97-RVS-GW-Burnaby-Lab
Status: Enable
Type: Reverse
Address: 10.59.112.97
SNI:
Port: 7443
Health Check: 60 Seconds
Description:

Reverse Gateway

Gateway ID
Gateway's client certificate common name, it is used to create a mapping between FortiPAM and the gateway.
fortipam_gw4

Mode
If on demand is selected, client will be able to choose if the secret is connected with the service gateway or reverse gateway mode during the launch process.
Reverse Gateway

Security

SSL Max Version: TLS 1.3
Client Certificate: None
CA certificate: None
TCP Forwarding Path: tcp

To configure a FortiGate gateway entry on FortiPAM:

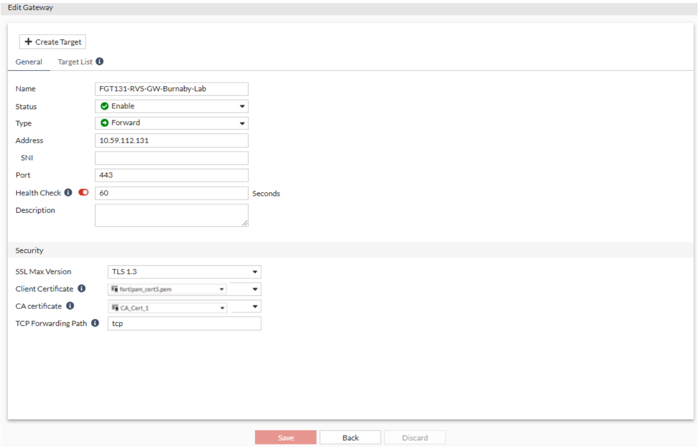
1. Go to *Network > Secret Gateway*.
2. From the Gateway List, select *Create*.
   The *New Gateway* window opens.
3. Enter a name for the gateway.
4. Ensure that the status is set to *Enable*.
5. From the *Type* dropdown, select *Reverse*.
6. In *Address*, enter the gateway IPv4 address.
7. In *Port*, 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 142.
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 142.

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*.



Name: FGT131-RVS-GW-Burnaby-Lab
Status: Enable
Type: Forward
Address: 10.59.112.131
SNI:
Port: 443
Health Check: 60 Seconds
Description:

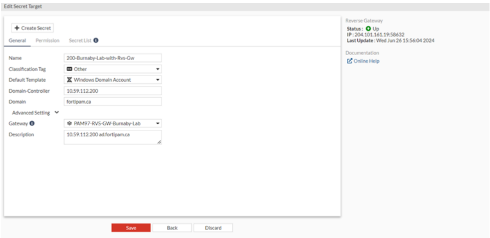
Security

SSL Max Version: TLS 1.3
Client Certificate: fortipam_cert5.pem
CA certificate: CA_Cert_1
TCP Forwarding Path: tcp

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 145.
9. Optionally, enter a description.
10. Click *Submit*.

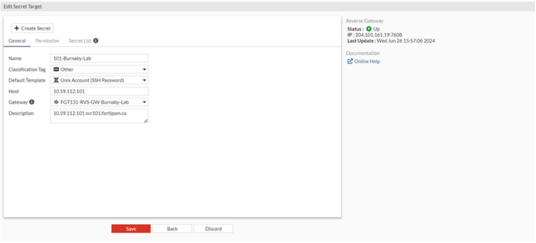


Name: 200-Burnaby-Lab-with-Rvs-Gw
Classification Tag: Other
Default Template: Windows Domain Account
Domain-Controller: 10.59.112.200
Domain: fortipam.ca
Gateway: PAM97-RVS-GW-Burnaby-Lab
Description: 10.59.112.200 ad.fortipam.ca

Reverse Gateway
Status : Up
IP : 204.101.161.19:58632
Last Update : Wed Jun 26 15:56:04 2024

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 ForitGate gateway created in Configuring a gateway entry on FortiPAM server for secret launch (traffic plane) on page 145.
8. Optionally, enter a description.
9. Click *Submit*.



Edit Secret Target

Name: 101-Burnaby-Lab
Classification Tag: Other
Default Template: Unix Account (SSH Password)
Host: 10.59.112.101
Gateway: FGT131-RVS-GW-Burnaby-Lab
Description: 10.59.112.101 svr101.fortipam.ca

Reverse Gateway
Status : Up
IP : 204.101.161.19:7608
Last Update : Wed Jun 26 15:57:06 2024

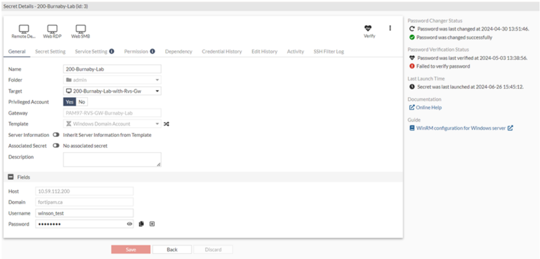
Creating a secret for the target that uses the FortiPAM reverse gateway

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 147.
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*.



Secret Details - 200-Burnaby-Lab (id: 3)

Name	200-Burnaby-Lab
Folder	admin
Target	200-Burnaby-Lab-with-Rvs-Gw
Privileged Account	Yes No
Gateway	PAM97-RVS-GW-Burnaby-Lab
Template	Windows Domain Account
Server Information	Inherit Server Information from Template
Associated Secret	No associated secret
Description	

Fields

Host	10.59.112.200
Domain	fortipam.ca
Username	winson_test
Password	••••••••

Password Changer Status
Password was last changed at 2024-04-30 13:51:46.
Password was changed successfully

Password Verification Status
Password was last verified at 2024-05-03 13:38:56.
Failed to verify password

Last Launch Time
Secret was last launched at 2024-06-26 15:45:12.

Documentation
Online Help

Guide
WinRM configuration for Windows server

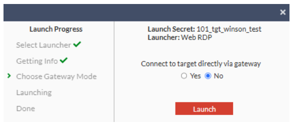
Launching the FortiPAM secret

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 148.
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.

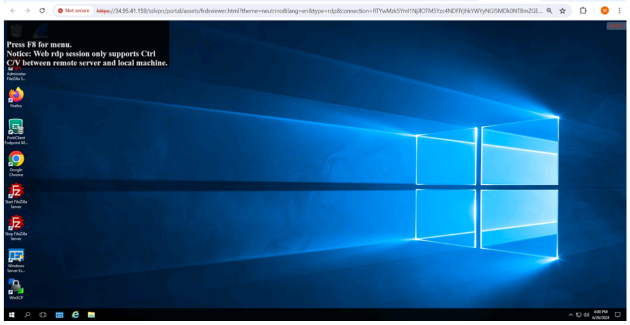
   Select *Yes* to launch the secret using the gateway in the Service mode.



Launch Secret: 101_tgt_winson_test
Launcher: Web RDP

Connect to target directly via gateway
○ Yes ● No

4. Select *Launch*.
   You can now access the target Windows server.

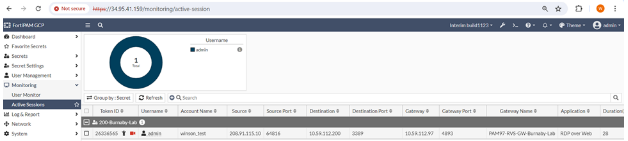


Not secure https://34.95.41.159/sslvpn/portal/assets/frdsviewer.html?theme=neutrino&lang=en&type=rdp&connection=RTYwMzk5Yml1NjJlOTM5Yzc4NDFlYjhkYWYyNGI5MDk0NTBmZGE...

Press F8 for menu.
Notice: Web rdp session only supports Ctrl C/V between remote server and local machine.

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.

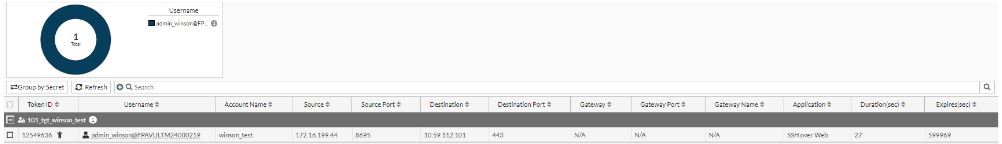


Not secure https://34.95.41.159/monitoring/active-session

Token ID	Username	Account Name	Source	Source Port	Destination	Destination Port	Gateway	Gateway Port	Gateway Name	Application	Duration(
200-Burnaby-Lab											
26336565	admin	winson_test	208.91.115.10	64816	10.59.112.200	3389	10.59.112.97	4893	PAM97-RVS-GW-Burnaby-Lab	RDP over Web	28

2. 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.



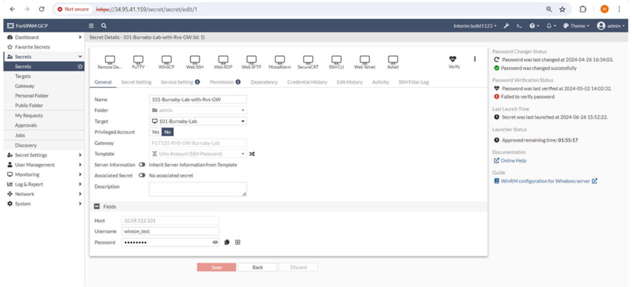
	Token ID	Username	Account Name	Source	Source Port	Destination	Destination Port	Gateway	Gateway Port	Gateway Name	Application	Duration(sec)	Expires(sec)
⊟ 101_tgt_winson_test 1													
□	12549636	admin_winson@FPAVULTM24000219	winson_test	172.16.199.44	8695	10.59.112.101	443	N/A	N/A	N/A	SSH over Web	27	599969

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:

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 FortiGate gateway created in Configuring a target using reverse gateway on the FortiPAM server on page 147.
7. Disable *Privileged Account*.
8. In *Fields*:
   a. In *Host*, enter the host IP address.
   b. Enter the user name.
   c. Enter the password.
   d. Reenter the password to confirm.
   e. Click *Submit*.



Secret Details - 101-Burnaby-Lab-with-Rvs-GW (id: 1)

Name: 101-Burnaby-Lab-with-Rvs-GW
Folder: admin
Target: 101-Burnaby-Lab
Privileged Account: Yes [✓ No]
Gateway: FGT131-RVS-GW-Burnaby-Lab
Template: Unix Account (SSH Password)
Server Information: Inherit Server Information from Template
Associated Secret: No associated secret
Description:

Fields

Host: 10.59.112.101
Username: winson_test
Password: ••••••••

Password Changer Status
Password was last changed at 2024-04-26 16:34:03.
Password was changed successfully

Password Verification Status
Password was last verified at 2024-05-02 14:02:32.
Failed to verify password

Last Launch Time
Secret was last launched at 2024-06-26 15:52:22.

Launcher Status
Approved remaining time: 01:55:17

Documentation
Online Help

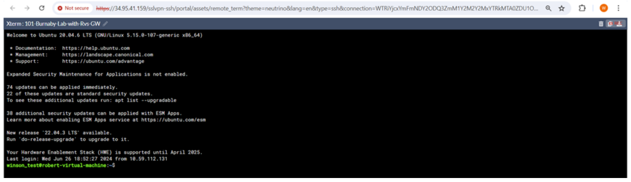
Guide
WinRM configuration for Windows server

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 150.
3. Launch the secret.

   You can now access the target Linux server.



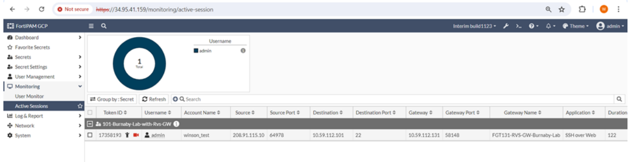
Not secure
https://34.95.41.159/sslvpn-ssh/portal/assets/remote_term?theme=neutrino&lang=en&type=ssh&connection=WTRiYjcxYmFmNDY2ODQ3ZmM1Y2M2Y2MxYTRkMTA0ZDU1O...
Xterm: 101-Burnaby-Lab-with-Rvs-GW

```
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-107-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

Expanded Security Maintenance for Applications is not enabled.

74 updates can be applied immediately.
22 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

38 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Wed Jun 26 18:52:27 2024 from 10.59.112.131
winson_test@robert-virtual-machine:~$
```

To oversee activities of the launched secret:

1. Go to *Monitoring > Active Sessions*.

   The gateway information is displayed for the launched secret.



Token ID	Username	Account Name	Source	Source Port	Destination	Destination Port	Gateway	Gateway Port	Gateway Name	Application	Duration
101-Burnaby-Lab-with-Rvs-GW											
17358193	admin	winson_test	208.91.115.10	64978	10.59.112.101	22	10.59.112.131	58148	FGT131-RVS-GW-Burnaby-Lab	SSH over Web	122

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
 dignose 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/ssled=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/ssled=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/ssled=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
```

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.

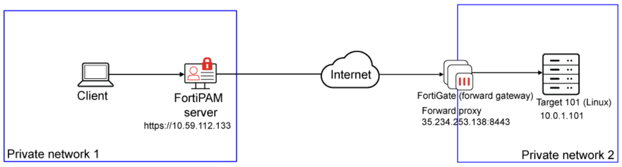
For more information about the forward gateway feature, see *Gateway* in the latest *FortiPAM Administration Guide*.

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 153
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 157
5. Launching the secret from the FortiPAM server on page 158
6. Monitoring the secret on page 158
7. Troubleshooting on page 159

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 uuid 9b3ca40a-665d-51f0-95ee-b8ea5be9b17c
   set type access-porxy
   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 "ztfp_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*.

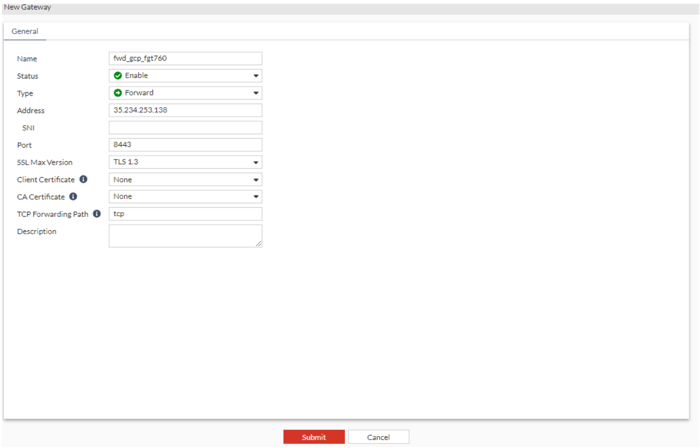
Configuring a gateway on the FortiPAM server

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 153.
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*.



Name	fwd_gcp_fgt760
Status	Enable
Type	Forward
Address	35.234.253.138
SNI	
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 153.

CA Certificate is the CA for the FortiGate certificate configured in Configuring forward gateway on FortiGate on page 153 (`ssl-certificate`).

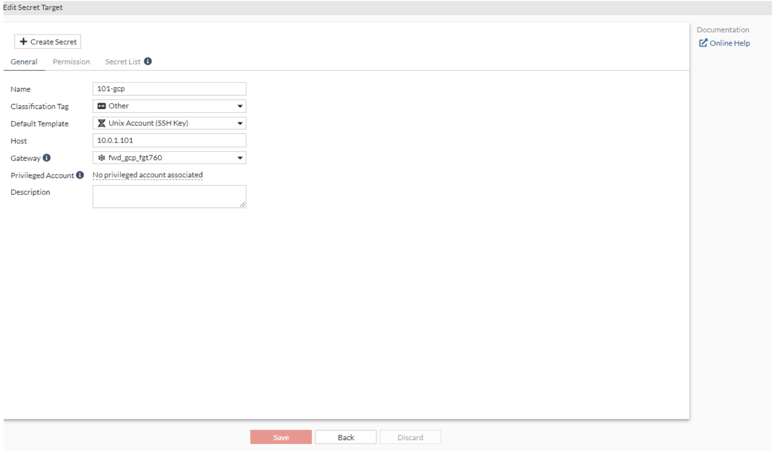
If it is not configured, FortiPAM server does not check the FortiGate certificate during the TLS handshake.

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*.



Edit Secret Target

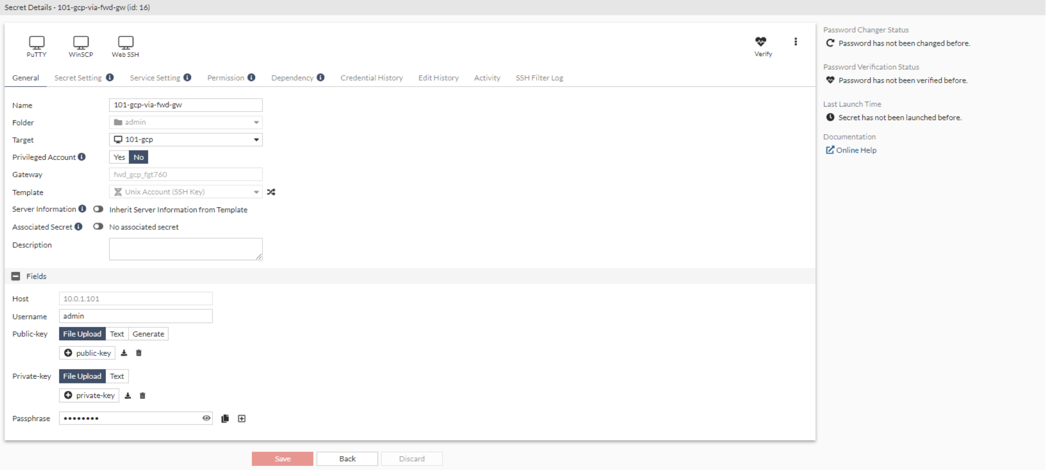
Name	101-gcp
Classification Tag	Other
Default Template	Unix Account (SSH Key)
Host	10.0.1.101
Gateway	fwd_gcp_fgt760
Privileged Account	No privileged account associated
Description	

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*.



Secret Details - 101-gcp-via-fwd-gw (id: 16)

Name: 101-gcp-via-fwd-gw
Folder: admin
Target: 101-gcp
Privileged Account: Yes [✓ No]
Gateway: fwd_gcp_fgt760
Template: Unix Account (SSH Key)
Server Information: Inherit Server Information from Template
Associated Secret: No associated secret
Description:

Fields

Host: 10.0.1.101
Username: admin
Public-key: [✓ File Upload] Text Generate
public-key
Private-key: [✓ File Upload] Text
private-key
Passphrase: ••••••••

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

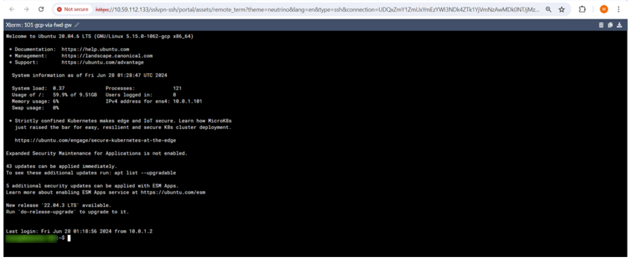
Launching the secret from the FortiPAM server

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 157.
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.



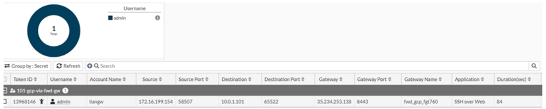
Not secure
~~https~~://10.59.112.133/sslvpn-ssh/portal/assets/remote_term?theme=neutrino&lang=en&type=ssh&connection=UDQxZmY1ZmUxYmEzYWI3NDk4ZTk1YjVmNzAwMDk0NTJjMz...
Xterm: 101-gcp-via-fwd-gw

```
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-1062-gcp x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Jun 28 01:28:47 UTC 2024

  System load:  0.37              Processes:             121
  Usage of /:   59.9% of 9.51GB   Users logged in:       0
  Memory usage: 6%                IPv4 address for ens4: 10.0.1.101
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

43 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

5 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Fri Jun 28 01:18:56 2024 from 10.0.1.2
[redacted]:~$ 
```

Monitoring the secret

To monitor the secret:

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



Token ID	Username	Account Name	Source	Source Port	Destination	Destination Port	Gateway	Gateway Port	Gateway Name	Application	Duration(sec)
101-gcp-via-fwd-gw											
13968146	admin	liangw	172.16.199.154	58507	10.0.1.101	65522	35.234.253.138	8443	fwd_gcp_fgt760	SSH over Web	84

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
```

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 160
2. Configuring SSH filter profiles using the GUI on page 161

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)`

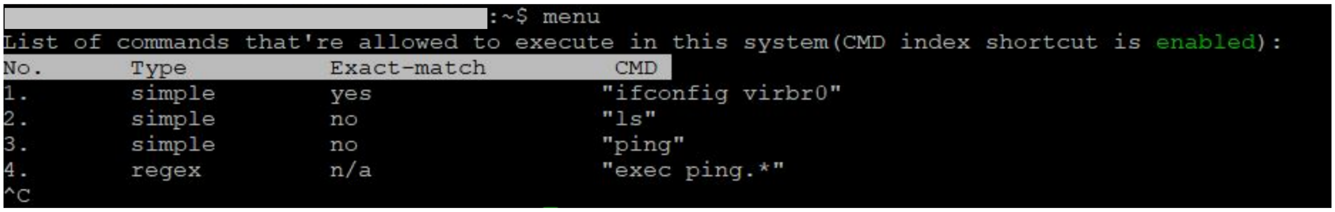
  When the character `&` is used to separate two commands, both command `ls` and `pwd` are checked against the SSH filter profile. See the example with *test_profile* below. The input is blocked as it matches the predefined shell command pattern entry 3 `ls`.

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

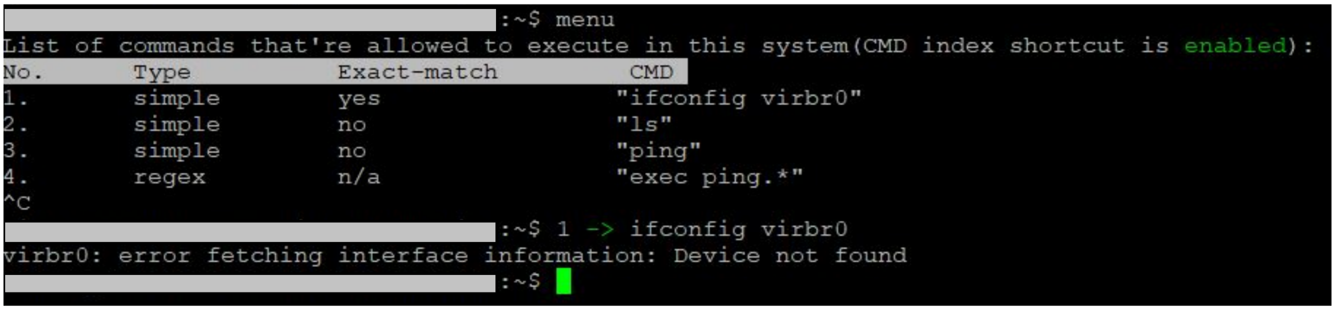
In restricted mode, a banner message contains the list of commands allowed to execute. This appears before the user logs in to the SSH secret server. After that, users can also use the "menu" (customizable) to list the commands anytime as needed.



```
[redacted]:~$ 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.



```
[redacted]:~$ 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
[redacted]:~$ 1 -> ifconfig virbr0
virbr0: error fetching interface information: Device not found
[redacted]:~$
```

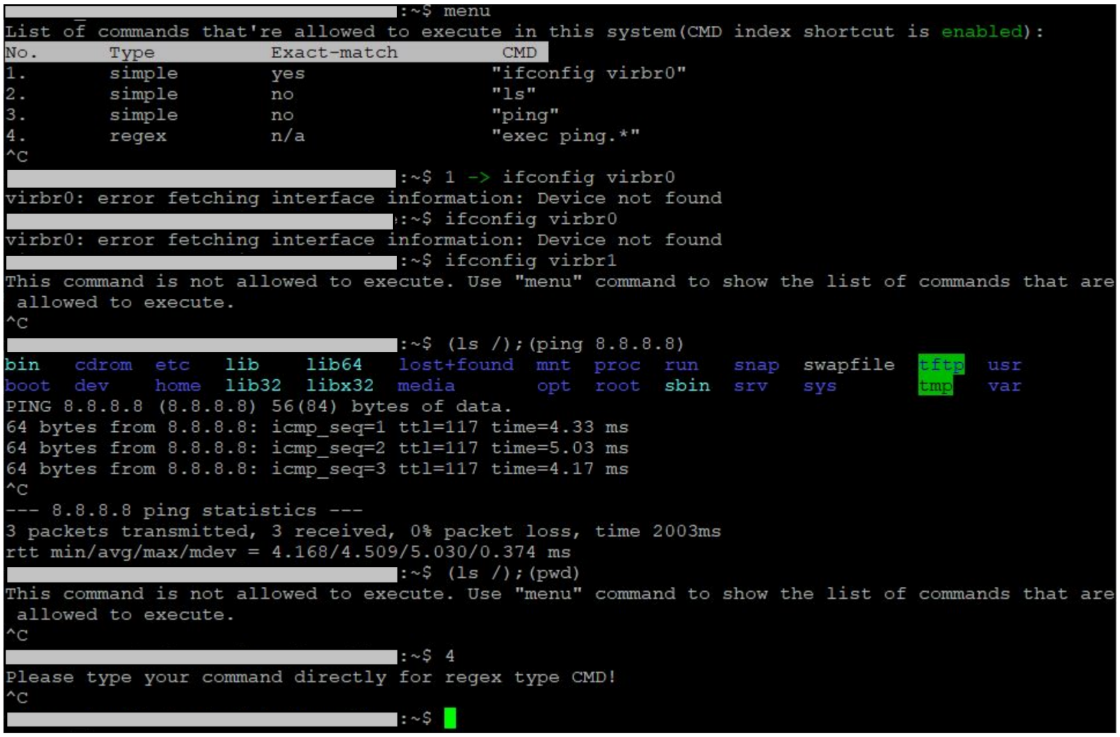
Examples

- `(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.

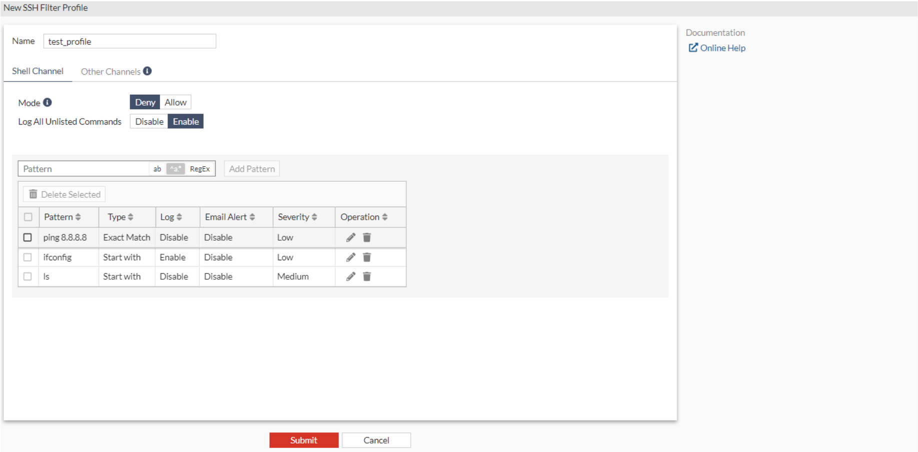


```
[redacted]:~$ menu
List of commands that're allowed to execute in this system(CMD index shortcut is enabled):
No.       Type          Exact-match          CMD
1.        simple        yes                  "ifconfig virbr0"
2.        simple        no                   "ls"
3.        simple        no                   "ping"
4.        regex         n/a                  "exec ping.*"
^C
[redacted]:~$ 1 -> ifconfig virbr0
virbr0: error fetching interface information: Device not found
[redacted]:~$ ifconfig virbr0
virbr0: error fetching interface information: Device not found
[redacted]:~$ ifconfig virbr1
This command is not allowed to execute. Use "menu" command to show the list of commands that are
 allowed to execute.
^C
[redacted]:~$ (ls /);(ping 8.8.8.8)
bin   cdrom  etc   lib    lib64   lost+found  mnt  proc  run   snap  swapfile  tftp  usr
boot  dev    home  lib32  libx32  media       opt  root  sbin  srv   sys       tmp   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
[redacted]:~$ (ls /);(pwd)
This command is not allowed to execute. Use "menu" command to show the list of commands that are
 allowed to execute.
^C
[redacted]:~$ 4
Please type your command directly for regex type CMD!
^C
[redacted]:~$
```

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*.



New SSH Filter Profile

Name: test_profile

Mode: Deny | Allow (Deny selected)

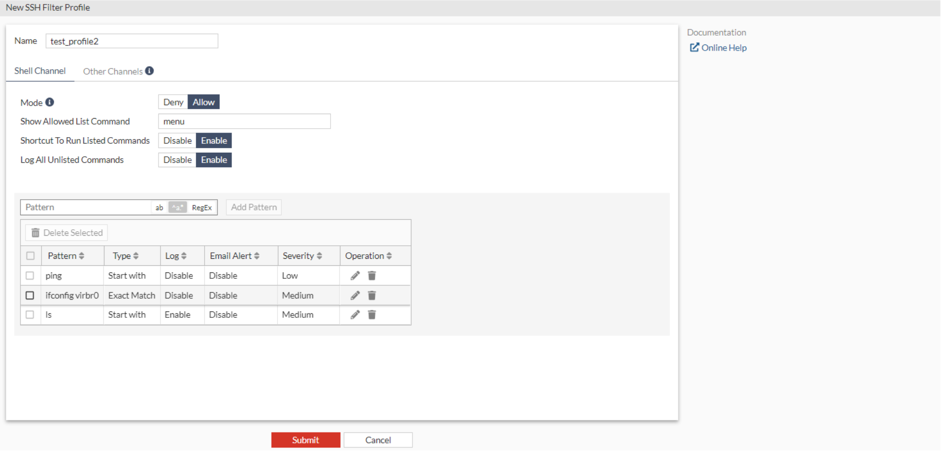
Log All Unlisted Commands: Disable | Enable (Enable selected)

□	Pattern	Type	Log	Email Alert	Severity	Operation
□	ping 8.8.8.8	Exact Match	Disable	Disable	Low	
□	ifconfig	Start with	Enable	Disable	Low	
□	ls	Start with	Disable	Disable	Medium	

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

Mode: Deny [✓ Allow]

Show Allowed List Command: menu

Shortcut To Run Listed Commands: Disable [✓ Enable]

Log All Unlisted Commands: Disable [✓ Enable]

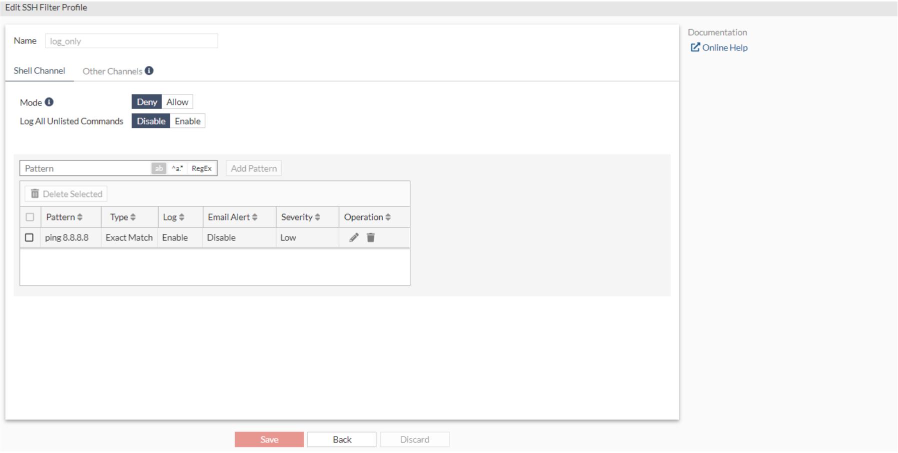
	Pattern	Type	Log	Email Alert	Severity	Operation
□	ping	Start with	Disable	Disable	Low	
□	ifconfig virbr0	Exact Match	Disable	Disable	Medium	
□	ls	Start with	Enable	Disable	Medium	

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

Mode: [✓ Deny] Allow

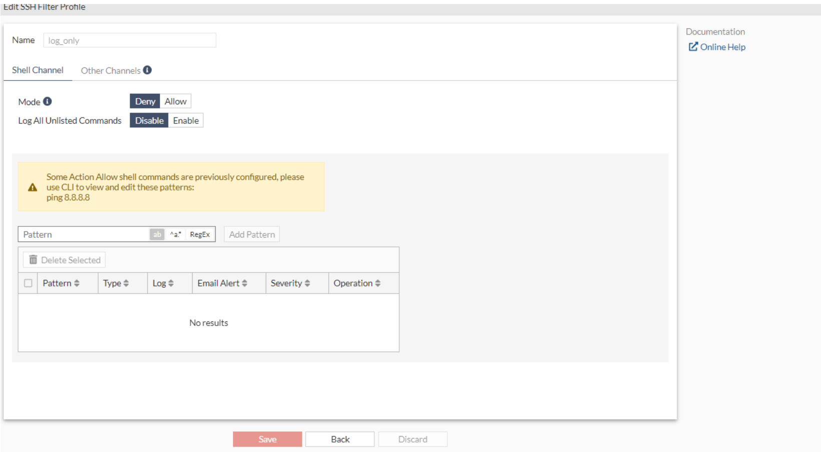
Log All Unlisted Commands: [✓ Disable] Enable

	Pattern	Type	Log	Email Alert	Severity	Operation
□	ping 8.8.8.8	Exact Match	Enable	Disable	Low	

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.


Edit SSH Filter Profile

Name: log_only

Mode: [✓ Deny] Allow

Log All Unlisted Commands: [✓ Disable] Enable

Some Action Allow shell commands are previously configured, please use CLI to view and edit these patterns:
ping 8.8.8.8

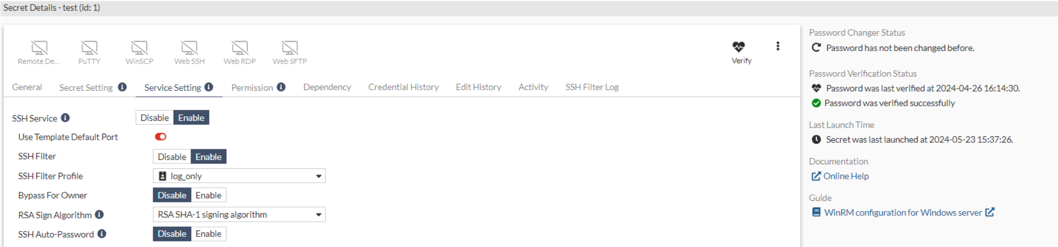
□	Pattern	Type	Log	Email Alert	Severity	Operation

No results

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*.



SSH Service: Disable [✓ Enable]
Use Template Default Port
SSH Filter: Disable [✓ Enable]
SSH Filter Profile: log_only
Bypass For Owner: [✓ Disable] Enable
RSA Sign Algorithm: RSA SHA-1 signing algorithm
SSH Auto-Password: [✓ Disable] Enable

Password Changer Status
Password has not been changed before.

Password Verification Status
Password was last verified at 2024-04-26 16:14:30.
Password was verified successfully

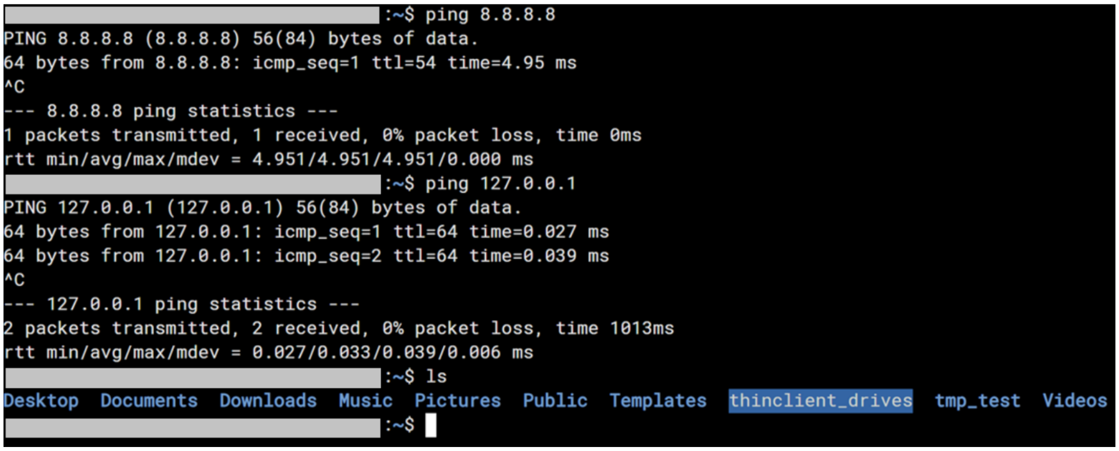
Last Launch Time
Secret was last launched at 2024-05-23 15:37:26.

Documentation
Online Help

Guide
WinRM configuration for Windows server

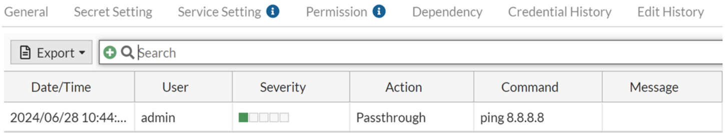
Results

When you launch the secret, you see that no commands are blocked; they are only logged.



```
[redacted]:~$ 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
[redacted]:~$ 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
[redacted]:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  thinclient_drives  tmp_test  Videos
[redacted]:~$
```

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.

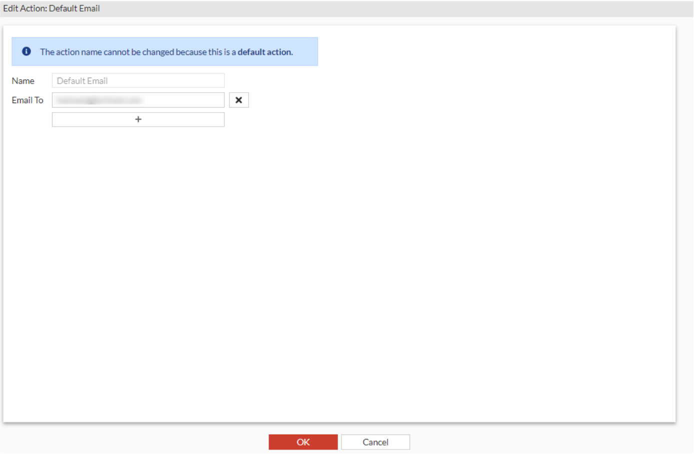
To use the default Secret Credential View automation stitch:

1. Using the Secret Credential View automation stitch on page 168
2. Results on page 169

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*.



Edit Action: Default Email

The action name cannot be changed because this is a **default action**.

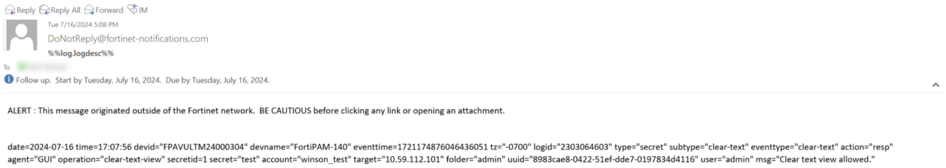
Name: Default Email

Email To: [redacted]

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 168.

   Tue 7/16/2024 5:08 PM

   DoNotReply@fortinet-notifications.com

   %%log.logdesc%%

   To [redacted]

   Follow up. Start by Tuesday, July 16, 2024. Due by Tuesday, July 16, 2024.

   ALERT : This message originated outside of the Fortinet network. BE CAUTIOUS before clicking any link or opening an attachment.

   ```
   date=2024-07-16 time=17:07:56 devid="FPAVULTM24000304" devname="FortiPAM-140" 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-dde7-0197834d4116" user="admin" msg="Clear text view allowed."
   ```

   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:

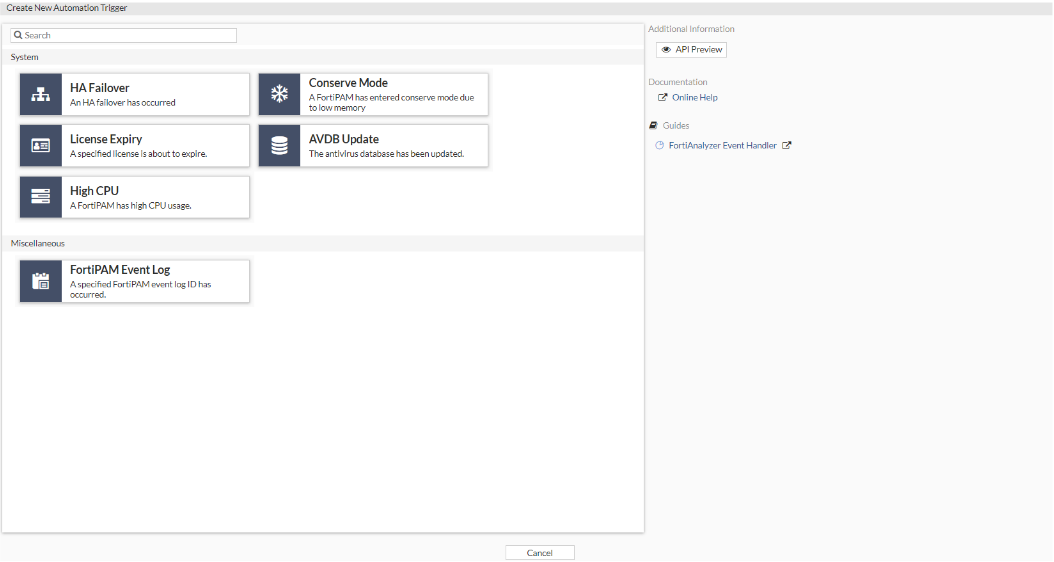
1. Creating an automation trigger on page 169
2. Create an action on page 171
3. Creating a stitch on page 172
4. Results on page 173

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.



Create New Automation Trigger

System

HA Failover
An HA failover has occurred

Conserve Mode
A FortiPAM has entered conserve mode due to low memory

License Expiry
A specified license is about to expire.

AVDB Update
The antivirus database has been updated.

High CPU
A FortiPAM has high CPU usage.

Miscellaneous

FortiPAM Event Log
A specified FortiPAM event log ID has occurred.

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:

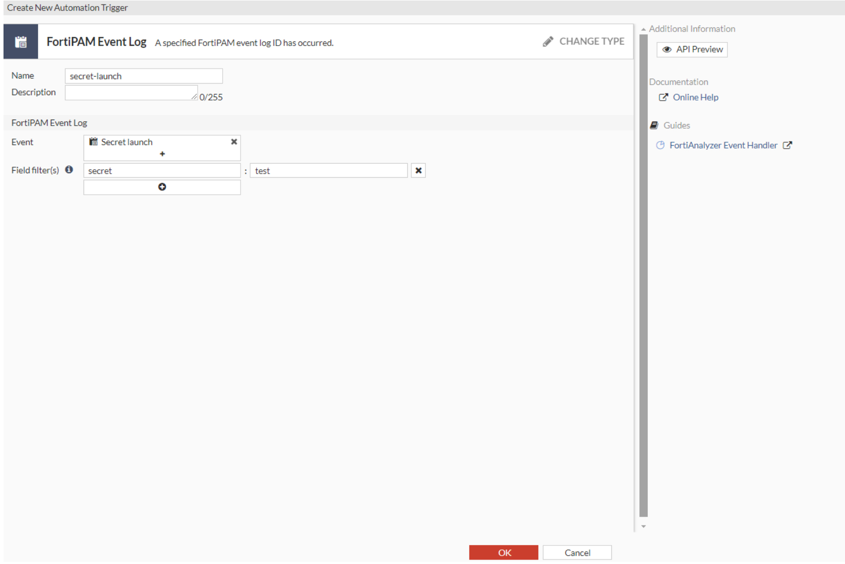
```
execute log filter category 23 #23 is for secrets
execute log display #If no log found,launch a secret and run the CLI command  again
```

      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-
dde7-0197834d4116" 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*.



Create New Automation Trigger

FortiPAM Event Log A specified FortiPAM event log ID has occurred.

Name: secret-launch

Description: 0/255

FortiPAM Event Log

Event: Secret launch

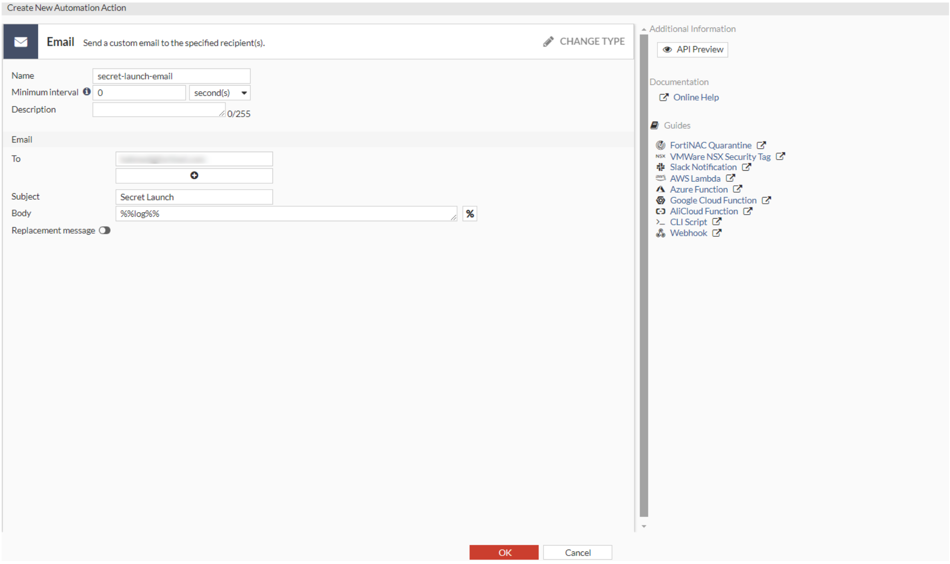
Field filter(s): secret : test

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*.



Create New Automation Action

Email Send a custom email to the specified recipient(s).

Name: secret-launch-email

Minimum interval: 0 second(s)

Description: 0/255

Email

To: [redacted]

Subject: Secret Launch

Body: %%log%%

Replacement message

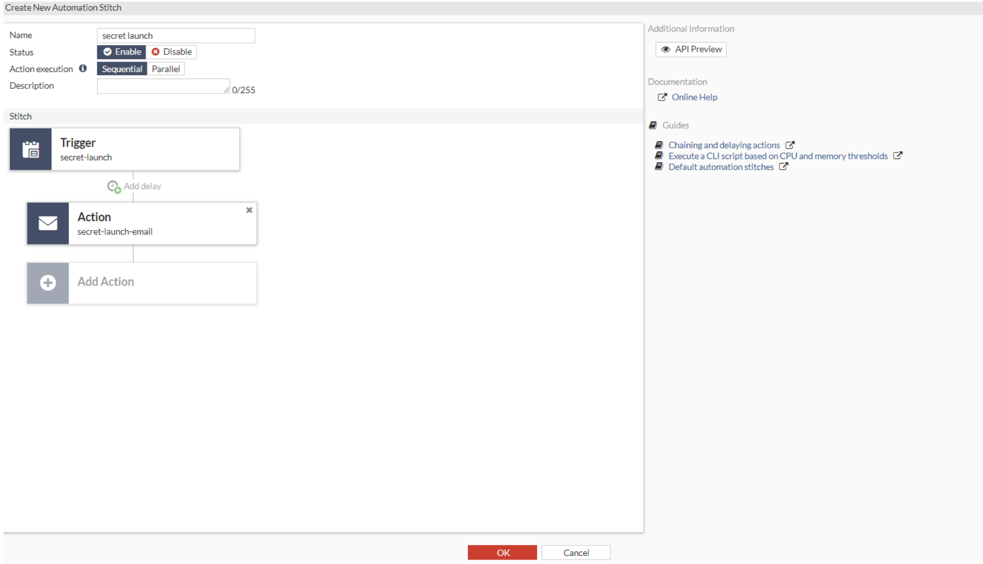
Creating a stitch

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 169.
   b. Click *Apply*.
   c. Select *Add Action*, from *Select Entries*, select the action created in Create an action on page 171.
   d. Click *Apply*.

5. Click *OK*.



Create New Automation Stitch

Name: secret launch

Status: Enable (selected) | Disable

Action execution: Sequential (selected) | Parallel

Description: 0/255

Stitch

Trigger: secret-launch

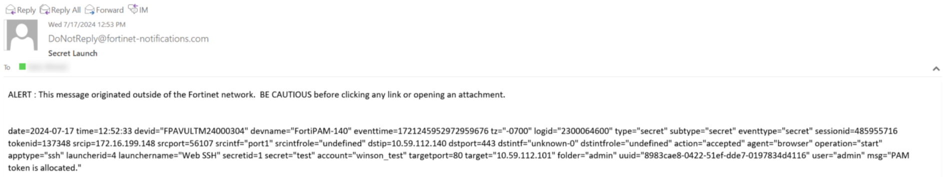
Action: secret-launch-email

Add delay
Add Action
Additional Information
API Preview
Documentation
Online Help
Guides
Chaining and delaying actions
Execute a CLI script based on CPU and memory thresholds
Default automation stitches
OK
Cancel

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 169.
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 171.

   Wed 7/17/2024 12:53 PM

   DoNotReply@fortinet-notifications.com

   Secret Launch

   To [redacted]

   ALERT : This message originated outside of the Fortinet network. BE CAUTIOUS before clicking any link or opening an attachment.

   ```
   date=2024-07-17 time=12:52:33 devid="FPAVULTM24000304" devname="FortiPAM-140" eventtime=1721245952972959676 tz="-0700" logid="2300064600" type="secret" subtype="secret" eventtype="secret" sessionid=485955716
   tokenid=137348 srcip=172.16.199.148 srcport=56107 srcintf="port1" srcintfrole="undefined" dstip=10.59.112.140 dstport=443 dstintf="unknown-0" dstintfrole="undefined" action="accepted" agent="browser" operation="start"
   apptype="ssh" launcherid=4 launchername="Web SSH" secretid=1 secret="test" account="winson_test" targetport=80 target="10.59.112.101" folder="admin" uuid="8983cae8-0422-51ef-dde7-0197834d4116" user="admin" msg="PAM
   token is allocated."
   ```

   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 174
2. Creating a target with server information as Windows on page 174
3. Creating a Windows application filter profile on page 175
4. Creating a privileged account secret on page 177
5. Creating a non-privileged account on page 178
6. Launching the secret on page 180

Setting up WinRM on the remote server

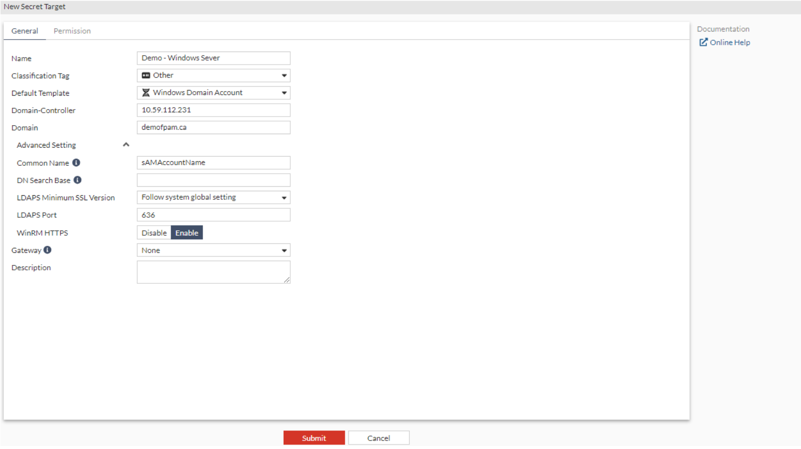
To set up WinRM on the remote server, see *Appendix L: WinRM configuration for Windows server* in the latest *FortiPAM Administration Guide*.

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*.



New Secret Target

Name	Demo - Windows Sever
Classification Tag	Other
Default Template	Windows Domain Account
Domain-Controller	10.59.112.231
Domain	demofpam.ca
Advanced Setting	
Common Name	sAMAccountName
DN Search Base	
LDAPS Minimum SSL Version	Follow system global setting
LDAPS Port	636
WinRM HTTPS	Disable [✓ Enable]
Gateway	None
Description	

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
```

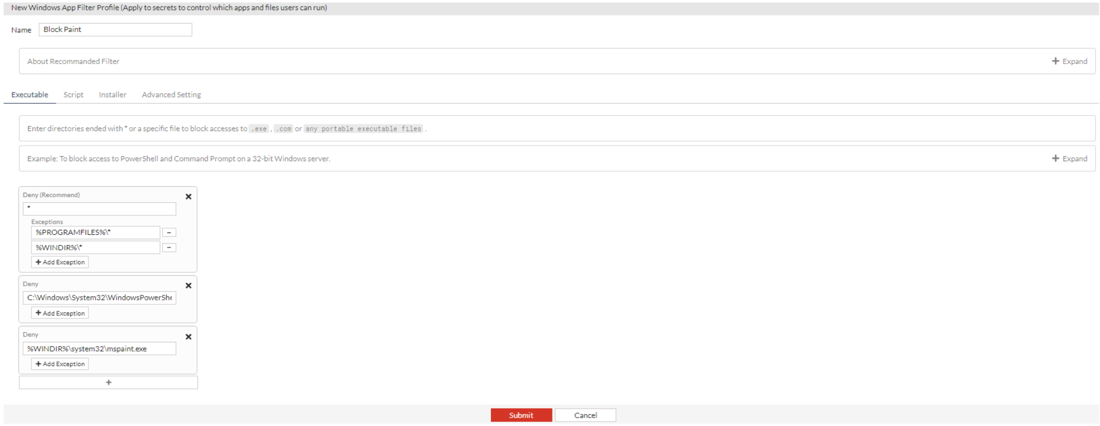
Creating a Windows application filter profile

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`.



New Windows App Filter Profile (Apply to secrets to control which apps and files users can run)

Name: Block Paint

About Recommanded Filter

Executable | Script | Installer | Advanced Setting

Enter directories ended with * or a specific file to block accesses to `.exe`, `.com` or `any portable executable files`.

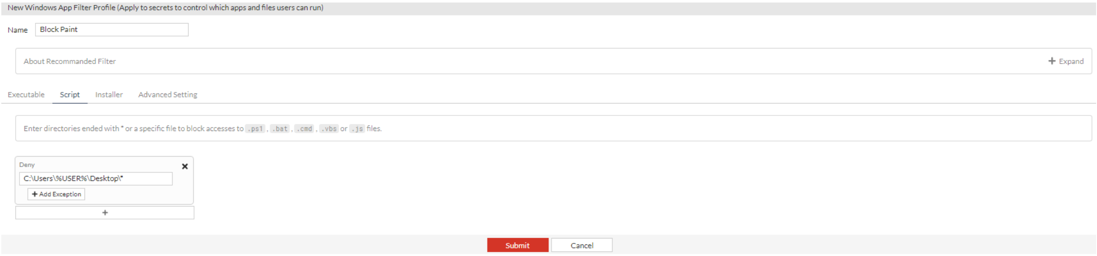
Example: To block access to PowerShell and Command Prompt on a 32-bit Windows server.

Deny (Recommend): *
Exceptions: %PROGRAMFILES%* ; %WINDIR%*

Deny: C:\Windows\System32\WindowsPowerShe

Deny: %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.



New Windows App Filter Profile (Apply to secrets to control which apps and files users can run)

Name: Block Paint

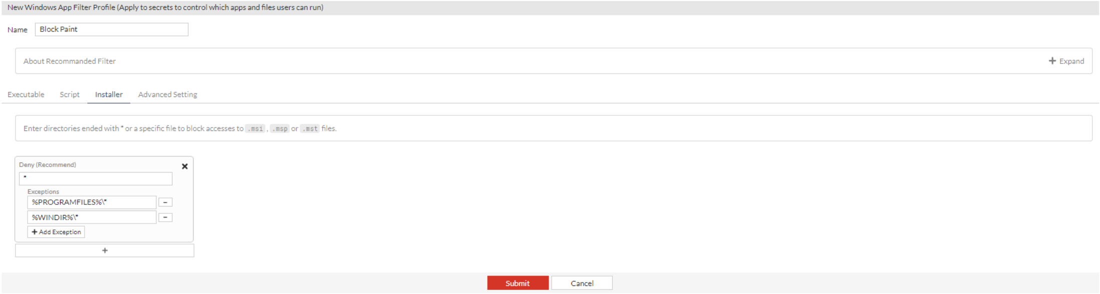
About Recommanded Filter

Executable | Script | Installer | Advanced Setting

Enter directories ended with * or a specific file to block accesses to `.ps1`, `.bat`, `.cmd`, `.vbs` or `.js` files.

Deny: C:\Users\%USER%\Desktop\*

5. Go to the *Installer* tab:
   a. In *Deny (Recommend)*, all installers are blocked except those in the directories `%PROGRAMFILES%\*`, `%WINDIR%\*`.



New Windows App Filter Profile (Apply to secrets to control which apps and files users can run)

Name: Block Paint

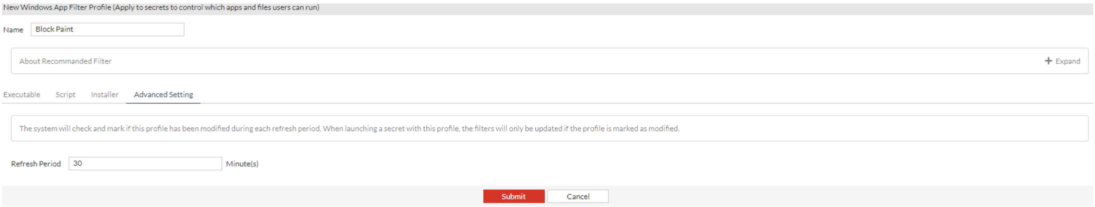
About Recommanded Filter

Executable | Script | Installer | Advanced Setting

Enter directories ended with * or a specific file to block accesses to `.msi`, `.msp` or `.mst` files.

Deny (Recommend): *
Exceptions: %PROGRAMFILES%* ; %WINDIR%*

6. Go to the *Advanced Setting* tab.
   a. In *Refresh Period*, keep the default value, 30 minutes.



New Windows App Filter Profile (Apply to secrets to control which apps and files users can run)

Name: Block Paint

About Recommanded Filter

Executable | Script | Installer | Advanced Setting

The system will check and mark if this profile has been modified during each refresh period. When launching a secret with this profile, the filters will only be updated if the profile is marked as modified.

Refresh Period: 30 Minute(s)

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

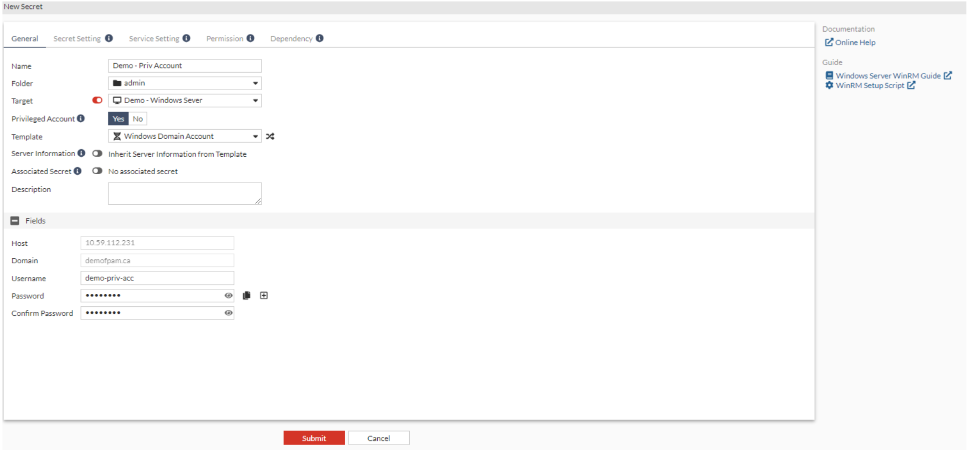
To create a secret:

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 174.
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*.



Name: Demo - Priv Account
Folder: admin
Target: Demo - Windows Sever
Privileged Account: Yes No
Template: Windows Domain Account
Server Information: Inherit Server Information from Template
Associated Secret: No associated secret
Description:

Fields

Host: 10.59.112.231
Domain: demofpam.ca
Username: demo-priv-acc
Password: ••••••••
Confirm Password: ••••••••

The above secret can be created in the CLI using the following commands CLI:

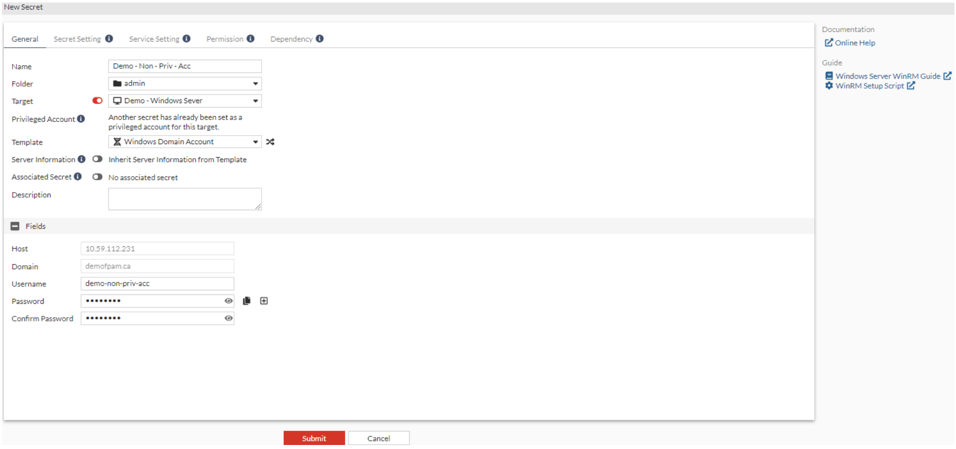
```
  config secret database
   edit 4
    set name "Demo - Priv Account"
    set target "Demo - Windows Server"
    set target-privilege-account enable
    set folder 1
    set template "Windows Domain Account"
    set proxy enable
    set rdp-service-status up
    set ldaps-service-status up
    set 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 174.
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 175.
12. Click *Submit*.



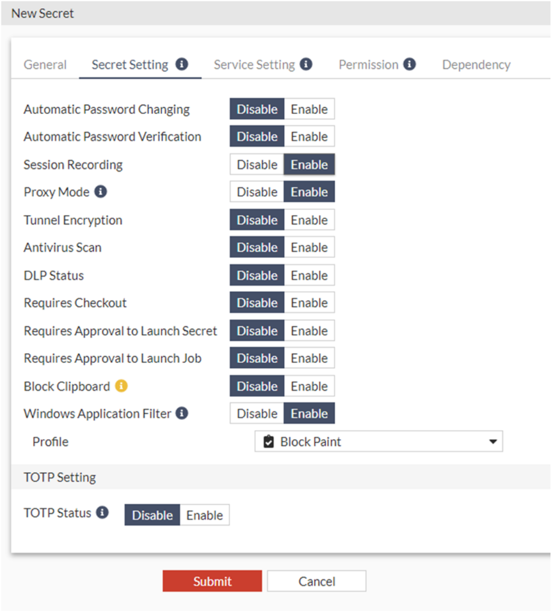
New Secret

General | Secret Setting | Service Setting | Permission | Dependency

Name	Demo - Non - Priv - Acc
Folder	admin
Target	Demo - Windows Sever
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	

Fields

Host	10.59.112.231
Domain	demofpam.ca
Username	demo-non-priv-acc
Password	••••••••
Confirm Password	••••••••



New Secret

General | Secret Setting | Service Setting | Permission | Dependency

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
Block Clipboard	[✓ Disable] Enable
Windows Application Filter	Disable [✓ Enable]
Profile	Block Paint

TOTP Setting

TOTP Status	[✓ Disable] Enable

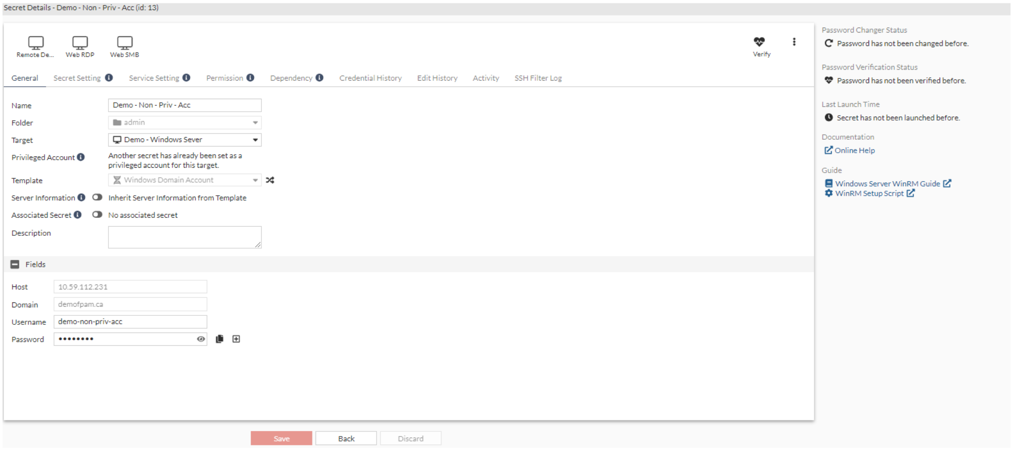
The above secret can be created in the CLI using the following commands CLI:

```
 config secret database
  edit 5
   set name "Demo - Non - Priv - Account"
   set target "Demo - Windows Server"
   set 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 178.



Secret Details - Demo - Non - Priv - Acc (id: 13)

Name: Demo - Non - Priv - Acc

Folder: admin

Target: Demo - Windows Sever

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:

Host: 10.59.112.231

Domain: demofpam.ca

Username: demo-non-priv-acc

Password: ••••••••

Password Changer Status: Password has not been changed before.

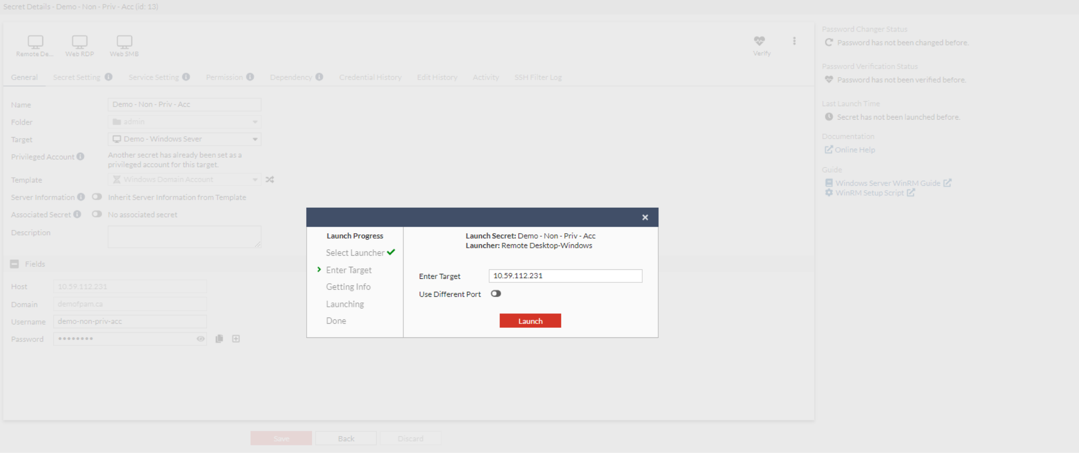
Password Verification Status: Password has not been verified before.

Last Launch Time: Secret has not been launched before.

Documentation: Online Help

Guide: Windows Server WinRM Guide, WinRM Setup Script

3. From the top, select either *Web RDP* or *Remote Desktop - Windows*.
   The *Launch Progress* dialog opens.

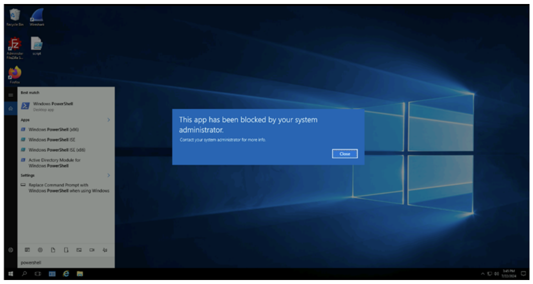


Launch Progress
Select Launcher ✓
Enter Target
Getting Info
Launching
Done

Launch Secret: Demo - Non - Priv - Acc
Launcher: Remote Desktop-Windows

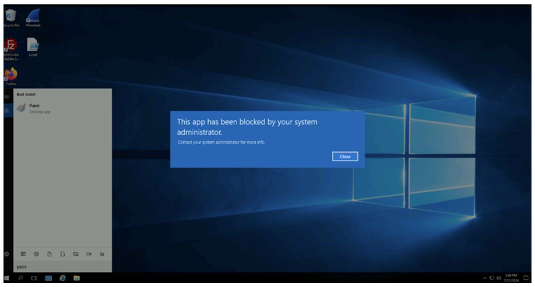
Enter Target: 10.59.112.231
Use Different Port ○

4. Select *Launch*.
5. Verify the Windows application filter functionality by executing the blocked executables and scripts:
   a. Open Powershell.



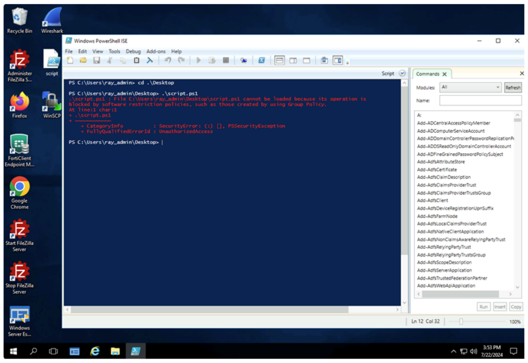
This app has been blocked by your system administrator.
Contact your system administrator for more info.

   b. Open MS Paint.



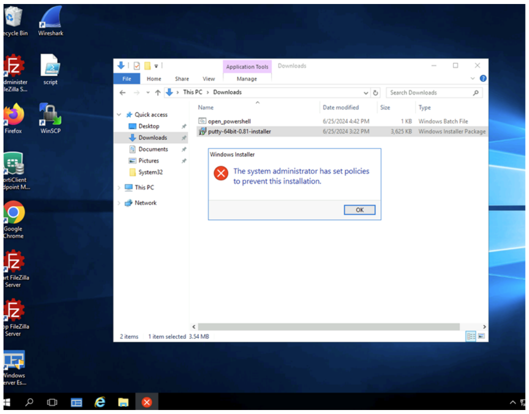
This app has been blocked by your system administrator.
Contact your system administrator for more info.

   c. Run scripts on the desktop.



```
PS C:\Users\ray_admin> cd .\Desktop

PS C:\Users\ray_admin\Desktop> .\script.ps1
.\script.ps1 : File C:\Users\ray_admin\Desktop\script.ps1 cannot be loaded because its operation is
blocked by software restriction policies, such as those created by using Group Policy.
At line:1 char:1
+ .\script.ps1
+ ~~~~~~~~~~~~
    + CategoryInfo          : SecurityError: (:) [], PSSecurityException
    + FullyQualifiedErrorId : UnauthorizedAccess

PS C:\Users\ray_admin\Desktop> |
```

d. Run the installer not permitted in the directories.



Name	Date modified	Size	Type
open_powershell	6/25/2024 4:42 PM	1 KB	Windows Batch File
putty-64bit-0.81-installer	6/25/2024 3:22 PM	3,625 KB	Windows Installer Package

Windows Installer

The system administrator has set policies to prevent this installation.

OK

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 174 except the ones below.

To create the Windows application filter:

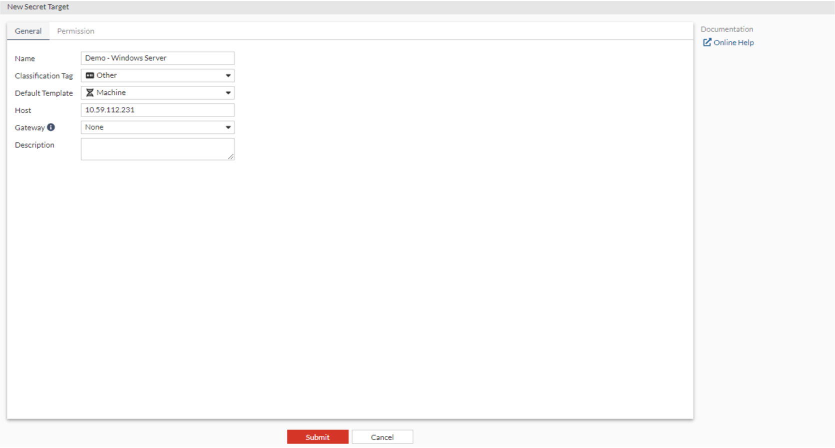
1. Creating a target with server information as non-Windows on page 182
2. Creating a non-privilged secret on page 183

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*.



New Secret Target

General | Permission

Name: Demo - Windows Server

Classification Tag: Other

Default Template: Machine

Host: 10.59.112.231

Gateway: None

Description:

The above target can be created in the CLI using the following commands (CLI):

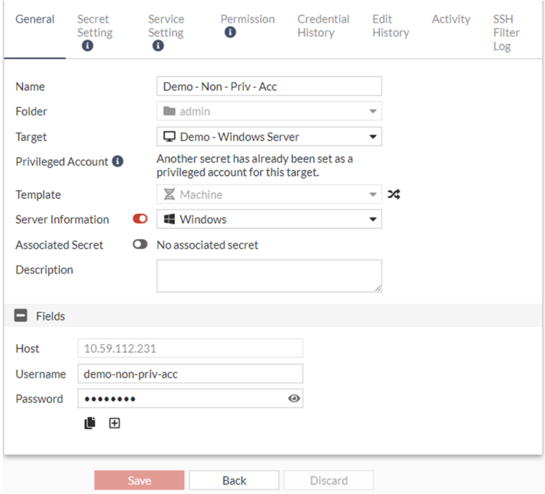
```
config secret target
 edit "Demo - Windows Server"
  set class "Other"
  set template "Machine"
  set address "10.59.112.231"
  set winrm-https disable
  set sql-server-log-status disable
 next
end
```

Creating a non-privilged 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 182.
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*.

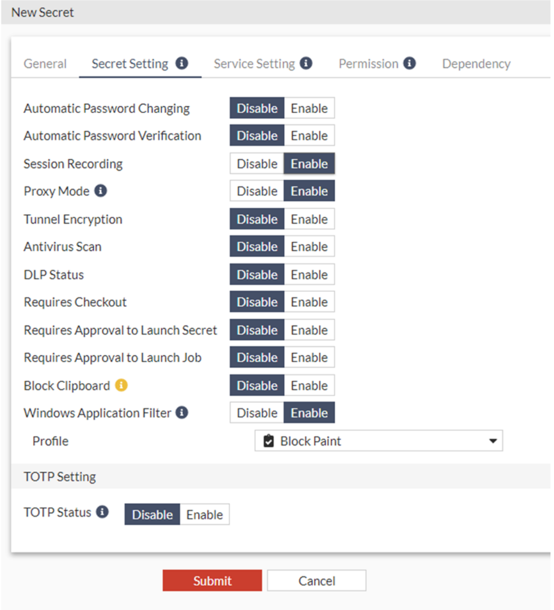
11. Ensure that *Proxy Mode* is enabled.
12. Enable *Windows Application Filter* and from the dropdown select the Windows application filter created in Creating a Windows application filter profile on page 175.
13. Click *Submit*.



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	Machine
Server Information	Windows
Associated Secret	No associated secret
Description	

Fields

Host	10.59.112.231
Username	demo-non-priv-acc
Password	••••••••



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 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 186
2. Creating a secret to connect to FortiAuthenticator on page 190
3. Launching the secret on page 190

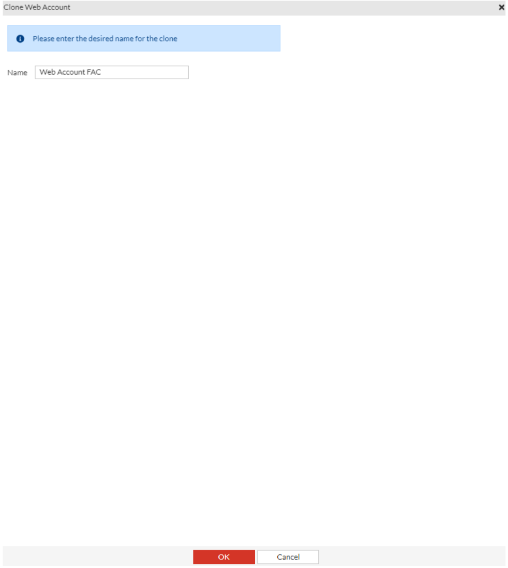
Creating a secret template

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*.

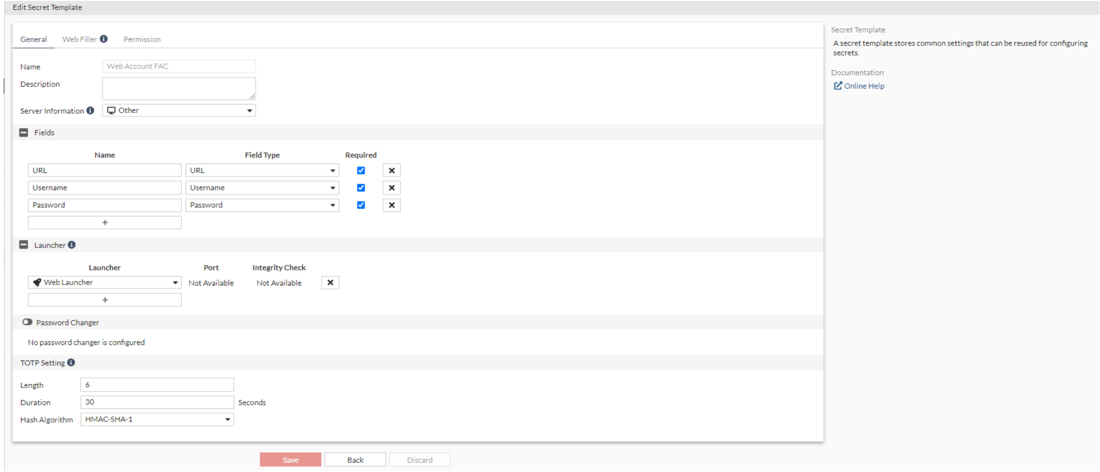
4. Click *OK*.



Please enter the desired name for the clone

Name: Web Account FAC

5. Double-click to open the cloned secret template.



Name: Web Account FAC

Description:

Server Information: Other

Fields

Name	Field Type	Required
URL	URL	☑
Username	Username	☑
Password	Password	☑

Launcher

Launcher	Port	Integrity Check
Web Launcher	Not Available	Not Available

Password Changer

No password changer is configured

TOTP Setting

Length: 6

Duration: 30 Seconds

Hash Algorithm: HMAC-SHA-1

Secret Template

A secret template stores common settings that can be reused for configuring secrets.

Documentation

Online Help

6. Go to the *Web Filler* tab:

   a. In *Authentication path*, enter `/login/`.

      For example:

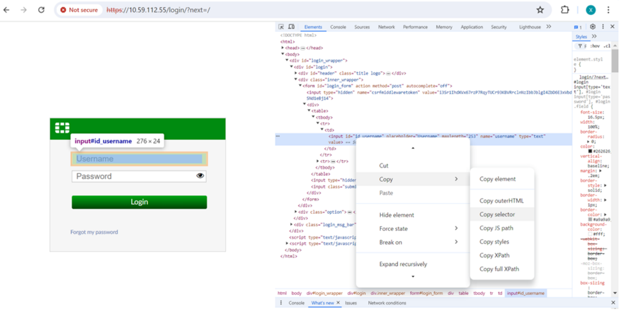
      - If the FortiAuthenticator login page is `https://x.x.x.x/login/`, the authentication path is `/login/`.
      - If the ESXi login page is `https://x.x.x.x/ui/`, the authentication path is `/ui/`.
      - If the vCenter login page is `https://vcenter.fortipam.ca/websso/SAML2/SSO/fortipam.ca?SAMLRequest=xxxxxxx`, 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*.



```
<!DOCTYPE html>
<html>
▸<head>…</head>
▾<body>
  ▾<div id="login_wrapper">
    ▾<div id="login">
      ▸<div id="header" class="title logo">…</div>
      ▾<div class="inner_wrapper">
        ▾<form id="login_form" action method="post" autocomplete="off">
           <input type="hidden" name="csrfmiddlewaretoken" value="i3Sr1IhdXvx67rzP7RqyTUCr93KBVRrclnNzIbbJblgI4ZbD6E3xVbdSNd1eBj14">
          ▾<div>
            ▾<table>
              ▾<tbody>
                ▾<tr>
                  ▾<td>
                     <input id="id_username" placeholder="Username" maxlength="253" name="username" type="text" value>
```

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 *+*.

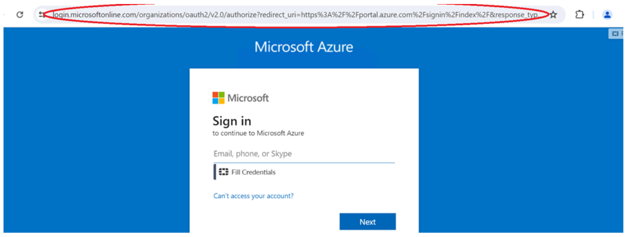
e. For the *Password* field, enter `#id_password` as the *Web Element Selector*.

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.

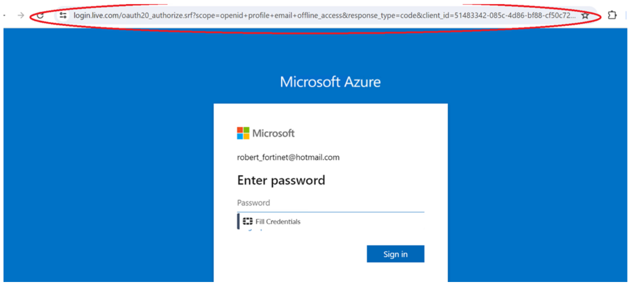
For example, on the Azure portal login pages:

Username



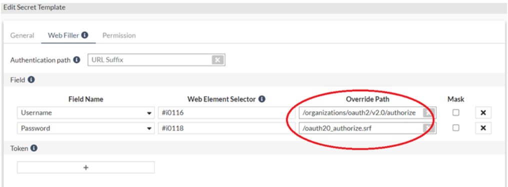
login.microsoftonline.com/organizations/oauth2/v2.0/authorize?redirect_uri=https%3A%2F%2Fportal.azure.com%2Fsignin%2Findex%2F&response_typ

Password



login.live.com/oauth20_authorize.srf?scope=openid+profile+email+offline_access&response_type=code&client_id=51483342-085c-4d86-bf88-cf50c72...

In the secret template *Web Filler* tab, the *Override Path* is set as below:

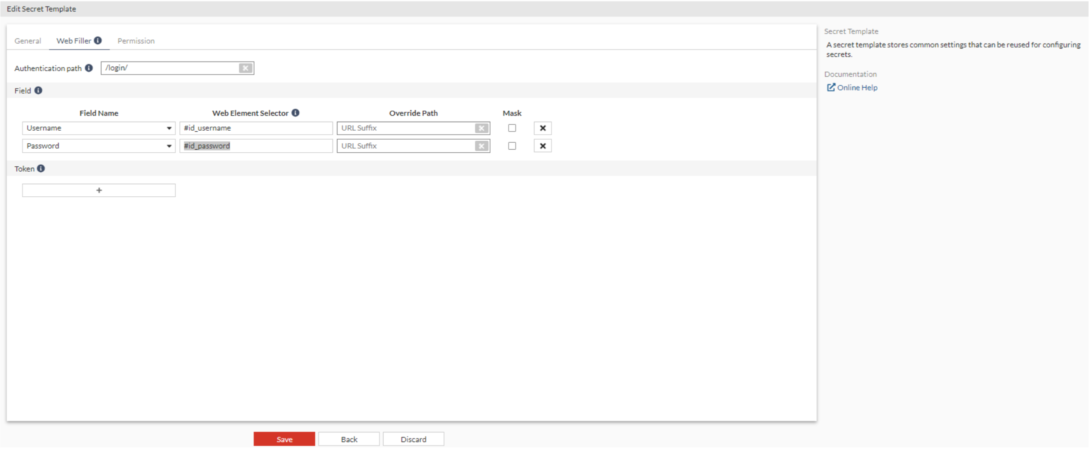


Authentication path: URL Suffix

Field

Field Name	Web Element Selector	Override Path	Mask
Username	#i0116	/organizations/oauth2/v2.0/authorize	□
Password	#i0118	/oauth20_authorize.srf	□

Token



Authentication path: /login/

Field

Field Name	Web Element Selector	Override Path	Mask
Username	#id_username	URL Suffix	□
Password	#id_password	URL Suffix	□

Token

Secret Template

A secret template stores common settings that can be reused for configuring secrets.

Documentation

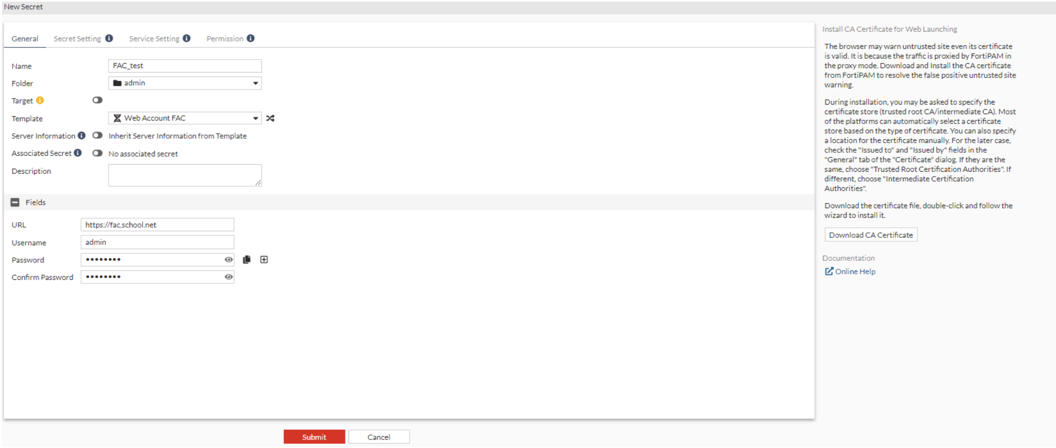
7. Click *Save*.

Creating a secret to connect to FortiAuthenticator

We create a secret based on the secret template in Creating a secret template on page 186 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 186.
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*.



Name: FAC_test
Folder: admin
Target: ○
Template: Web Account FAC
Server Information: ○ Inherit Server Information from Template
Associated Secret: ○ No associated secret
Description:

Fields
URL: https://fac.school.net
Username: admin
Password: ••••••••
Confirm Password: ••••••••

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.

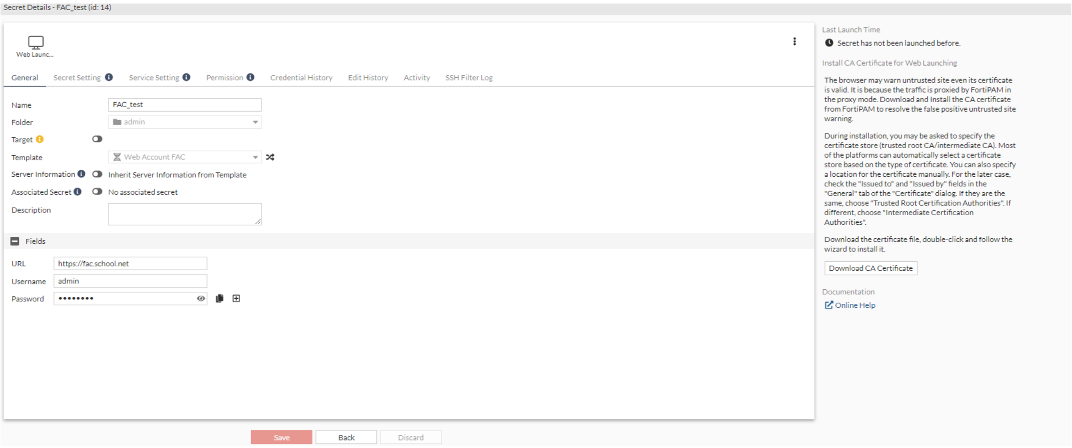
Documentation

Launching the secret

We launch the secret created in Creating a secret to connect to FortiAuthenticator on page 190.

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 190.



Secret Details - FAC_test (id: 14)

Name: FAC_test
Folder: admin
Target
Template: Web Account FAC
Server Information: Inherit Server Information from Template
Associated Secret: No associated secret
Description

Fields

URL: https://fac.school.net
Username: admin
Password: ••••••••

Last Launch Time

Secret has not been launched before.

Install CA Certificate for Web Launching

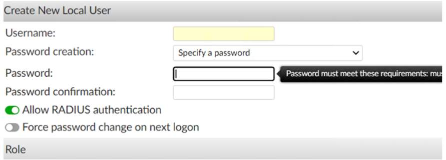
The browser may warn untrusted site even its certificate is valid. It is because the traffic is proxied by FortiPAM in the proxy mode. Download and Install the CA certificate from FortiPAM to resolve the false positive untrusted site warning.

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.

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.



Create New Local User

Username:
Password creation: Specify a password
Password: Password must meet these requirements: mu
Password confirmation:
● Allow RADIUS authentication
○ Force password change on next logon

Role

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 192
2. Backing up videos to the FTP server on page 193
3. Backing up logs to the FTP server on page 193
4. Shutting down the FortiPAM-VM and change log and video disks on page 194
5. Restoring videos from the FTP server on page 194
6. Restoring logs from the FTP server on page 195

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*.

.

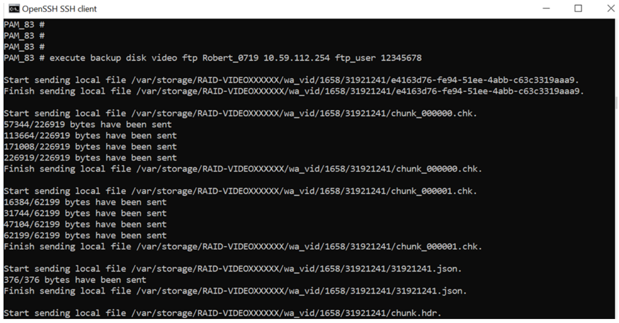
Backing up videos to the FTP server

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.

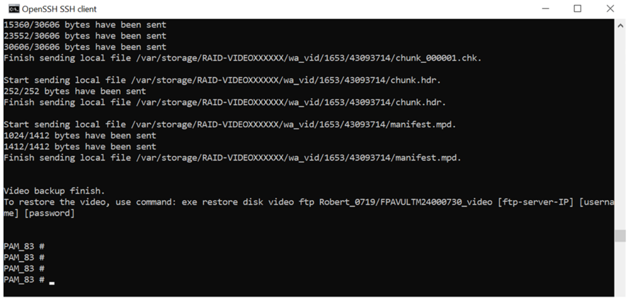


```
PAM_83 #
PAM_83 #
PAM_83 #
PAM_83 # execute backup disk video ftp Robert_0719 10.59.112.254 ftp_user 12345678

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
171008/226919 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
47104/62199 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.



```
15360/30606 bytes have been sent
23552/30606 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/FPAVULTM24000730_video [ftp-server-IP] [userna
me] [password]


PAM_83 #
PAM_83 #
PAM_83 #
PAM_83 #
```

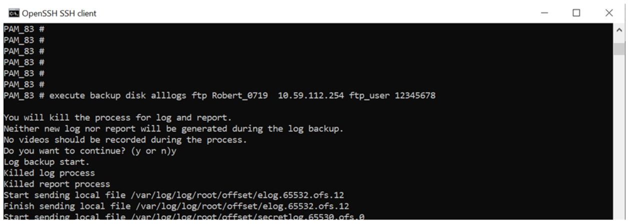
Backing up logs to the FTP server

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.

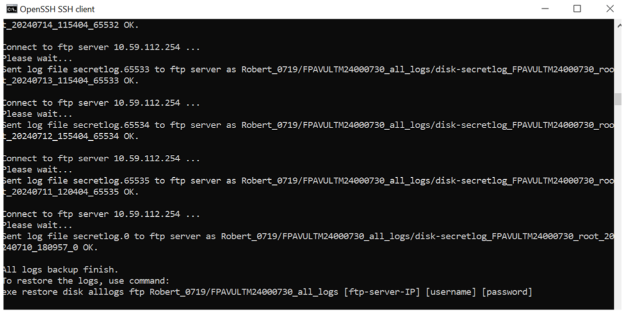


```
PAM_83 #
PAM_83 #
PAM_83 #
PAM_83 #
PAM_83 #
PAM_83 #
PAM_83 # execute backup disk alllogs ftp Robert_0719  10.59.112.254 ftp_user 12345678

You will kill the process for log and report.
Neither 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.65530.ofs.0
```

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.



```
t_20240714_115404_65532 OK.

Connect to ftp server 10.59.112.254 ...
Please wait...
Sent log file secretlog.65533 to ftp server as Robert_0719/FPAVULTM24000730_all_logs/disk-secretlog_FPAVULTM24000730_roo
t_20240713_115404_65533 OK.

Connect to ftp server 10.59.112.254 ...
Please wait...
Sent log file secretlog.65534 to ftp server as Robert_0719/FPAVULTM24000730_all_logs/disk-secretlog_FPAVULTM24000730_roo
t_20240712_155404_65534 OK.

Connect to ftp server 10.59.112.254 ...
Please wait...
Sent log file secretlog.65535 to ftp server as Robert_0719/FPAVULTM24000730_all_logs/disk-secretlog_FPAVULTM24000730_roo
t_20240711_120404_65535 OK.

Connect to ftp server 10.59.112.254 ...
Please wait...
Sent log file secretlog.0 to ftp server as Robert_0719/FPAVULTM24000730_all_logs/disk-secretlog_FPAVULTM24000730_root_20
240710_180957_0 OK.

All logs backup finish.
To restore the logs, use command:
exe restore disk alllogs ftp Robert_0719/FPAVULTM24000730_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.

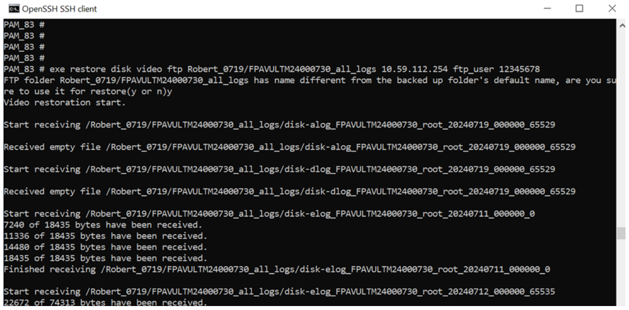
5. Add the new log and video disks.
6. Reboot the FortiPAM-VM.

Restoring videos from the FTP server

To restore videos from the FTP server:

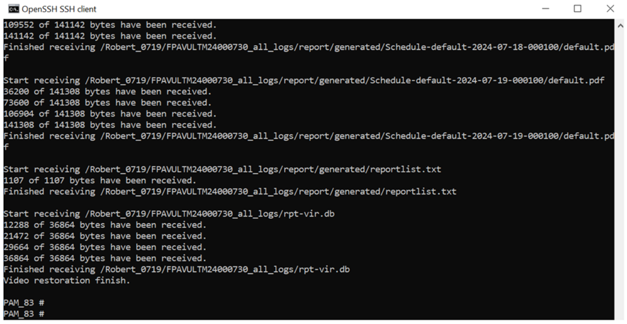
1. In the FortiPAM CLI console, enter the following command to restore from the FTP server with your FTP server IP address, user name, and password:

```
execute restore disk video ftp <string> <ftp server>[:ftp port] <user> <passwd>
```



```
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 su
re to use it for restore(y or n)y
Video restoration start.

Start receiving /Robert_0719/FPAVULTM24000730_all_logs/disk-alog_FPAVULTM24000730_root_20240719_000000_65529

Received empty file /Robert_0719/FPAVULTM24000730_all_logs/disk-alog_FPAVULTM24000730_root_20240719_000000_65529

Start receiving /Robert_0719/FPAVULTM24000730_all_logs/disk-dlog_FPAVULTM24000730_root_20240719_000000_65529

Received empty file /Robert_0719/FPAVULTM24000730_all_logs/disk-dlog_FPAVULTM24000730_root_20240719_000000_65529

Start receiving /Robert_0719/FPAVULTM24000730_all_logs/disk-elog_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-elog_FPAVULTM24000730_root_20240711_000000_0

Start receiving /Robert_0719/FPAVULTM24000730_all_logs/disk-elog_FPAVULTM24000730_root_20240712_000000_65535
22672 of 74313 bytes have been received.
```

After the logs are restored, *Video restoration finish* is displayed in the FortiPAM CLI console.



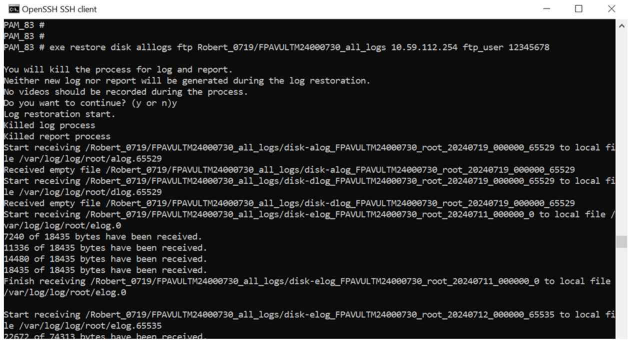
```
109552 of 141142 bytes have been received.
141142 of 141142 bytes have been received.
Finished receiving /Robert_0719/FPAVULTM24000730_all_logs/report/generated/Schedule-default-2024-07-18-000100/default.pd
f

Start receiving /Robert_0719/FPAVULTM24000730_all_logs/report/generated/Schedule-default-2024-07-19-000100/default.pdf
36200 of 141308 bytes have been received.
73600 of 141308 bytes have been received.
106904 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.pd
f

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.
21472 of 36864 bytes have been received.
29664 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:

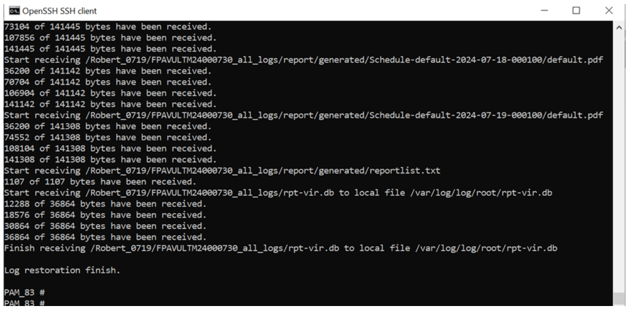
1. In the FortiPAM CLI console, enter the following command to restore logs from the FTP server with your FTP server IP address, user name, and password:

```
execute restore disk alllogs ftp <remote folder path> <ftp server>[:ftp port] <user> <passwd>
```



```
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-alog_FPAVULTM24000730_root_20240719_000000_65529 to local fi
le /var/log/log/root/alog.65529
Received empty file /Robert_0719/FPAVULTM24000730_all_logs/disk-alog_FPAVULTM24000730_root_20240719_000000_65529
Start receiving /Robert_0719/FPAVULTM24000730_all_logs/disk-dlog_FPAVULTM24000730_root_20240719_000000_65529 to local fi
le /var/log/log/root/dlog.65529
Received empty file /Robert_0719/FPAVULTM24000730_all_logs/disk-dlog_FPAVULTM24000730_root_20240719_000000_65529
Start receiving /Robert_0719/FPAVULTM24000730_all_logs/disk-elog_FPAVULTM24000730_root_20240711_000000_0 to local file /
var/log/log/root/elog.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-elog_FPAVULTM24000730_root_20240711_000000_0 to local file
/var/log/log/root/elog.0

Start receiving /Robert_0719/FPAVULTM24000730_all_logs/disk-elog_FPAVULTM24000730_root_20240712_000000_65535 to local fi
le /var/log/log/root/elog.65535
22672 of 74313 bytes have been received.
```

After the logs are restored, *Log restoration finish* is displayed in the FortiPAM CLI console.



```
73104 of 141445 bytes have been received.
107856 of 141445 bytes have been received.
141445 of 141445 bytes have been received.
Start receiving /Robert_0719/FPAVULTM24000730_all_logs/report/generated/Schedule-default-2024-07-18-000100/default.pdf
36200 of 141142 bytes have been received.
70704 of 141142 bytes have been received.
106904 of 141142 bytes have been received.
141142 of 141142 bytes have been received.
Start receiving /Robert_0719/FPAVULTM24000730_all_logs/report/generated/Schedule-default-2024-07-19-000100/default.pdf
36200 of 141308 bytes have been received.
74552 of 141308 bytes have been received.
108104 of 141308 bytes have been received.
141308 of 141308 bytes have been received.
Start receiving /Robert_0719/FPAVULTM24000730_all_logs/report/generated/reportlist.txt
1107 of 1107 bytes have been received.
Start receiving /Robert_0719/FPAVULTM24000730_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.
30864 of 36864 bytes have been received.
36864 of 36864 bytes have been received.
Finish receiving /Robert_0719/FPAVULTM24000730_all_logs/rpt-vir.db to local file /var/log/log/root/rpt-vir.db

Log restoration finish.

PAM_83 #
PAM_83 #
```

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 1.8 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:

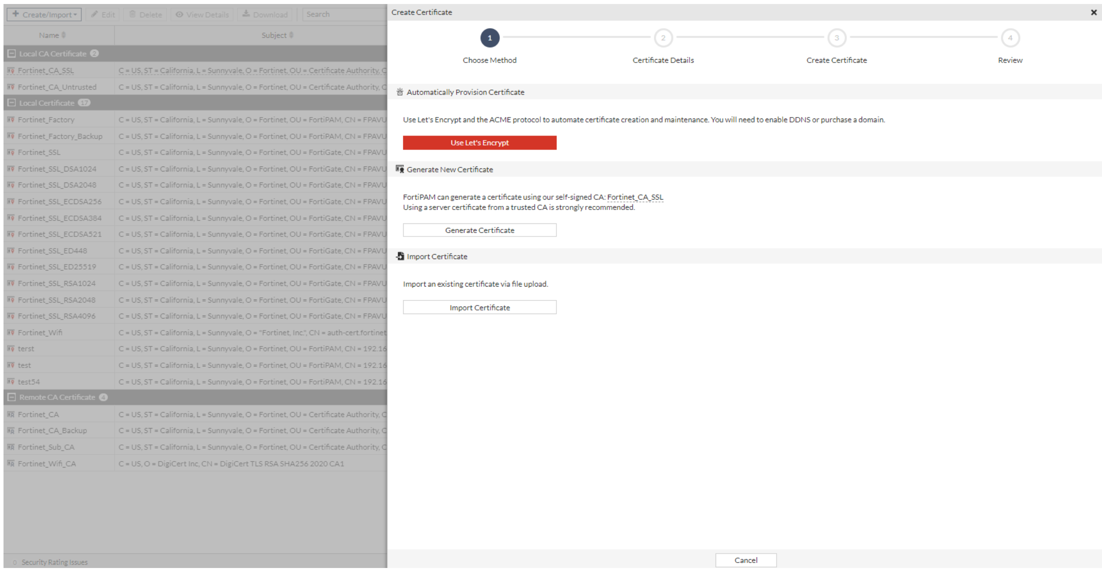
1. Creating a certificate on page 197
2. Configuring the FortiPAM SSL certificate on page 201

Creating a certificate

To create a certificate:

1. Go to *System > Certificates*.
2. From *+Create/Import*, select *Certificate*.

   The *Create Certificate* window opens.



Create Certificate

1 Choose Method — 2 Certificate Details — 3 Create Certificate — 4 Review

Automatically Provision Certificate

Use Let's Encrypt and the ACME protocol to automate certificate creation and maintenance. You will need to enable DDNS or purchase a domain.

Generate New Certificate

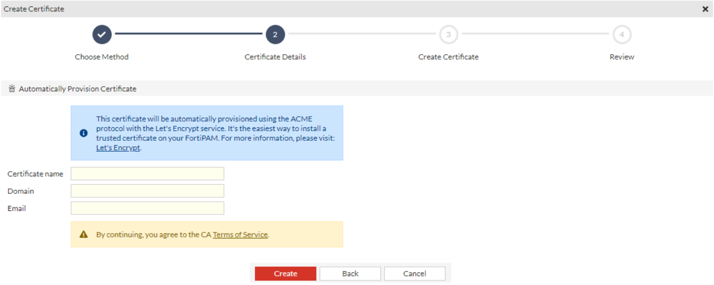
FortiPAM can generate a certificate using our self-signed CA: Fortinet_CA_SSL
Using a server certificate from a trusted CA is strongly recommended.

Import Certificate

Import an existing certificate via file upload.

3. 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.



Create Certificate

Choose Method — 2 Certificate Details — 3 Create Certificate — 4 Review

Automatically Provision Certificate

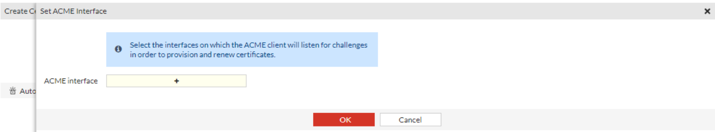
This certificate will be automatically provisioned using the ACME protocol with the Let's Encrypt service. It's the easiest way to install a trusted certificate on your FortiPAM. For more information, please visit: Let's Encrypt.

Certificate name
Domain
Email

By continuing, you agree to the CA Terms of Service.

4. In *Certificate name*, enter the name for the certificate.
5. In *Domain*, enter the public FQDN of FortiPAM.
6. In *Email*, enter the email address.
7. 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.



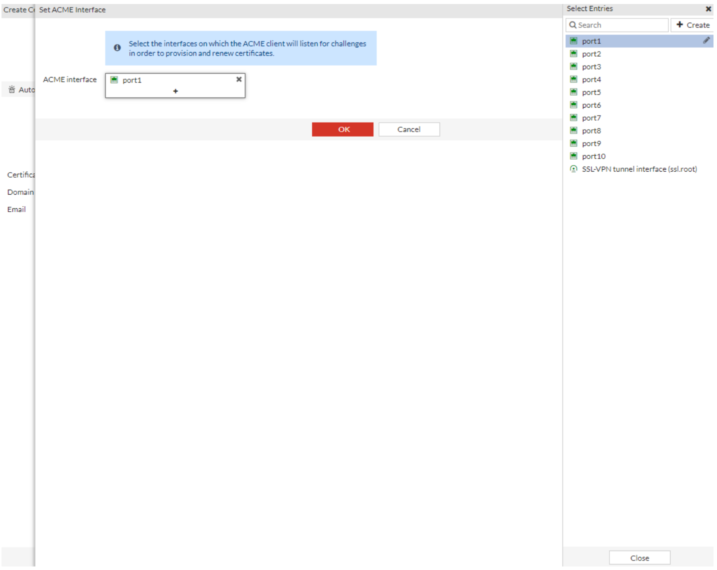
Set ACME Interface

Select the interfaces on which the ACME client will listen for challenges in order to provision and renew certificates.

ACME interface +

8. 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.

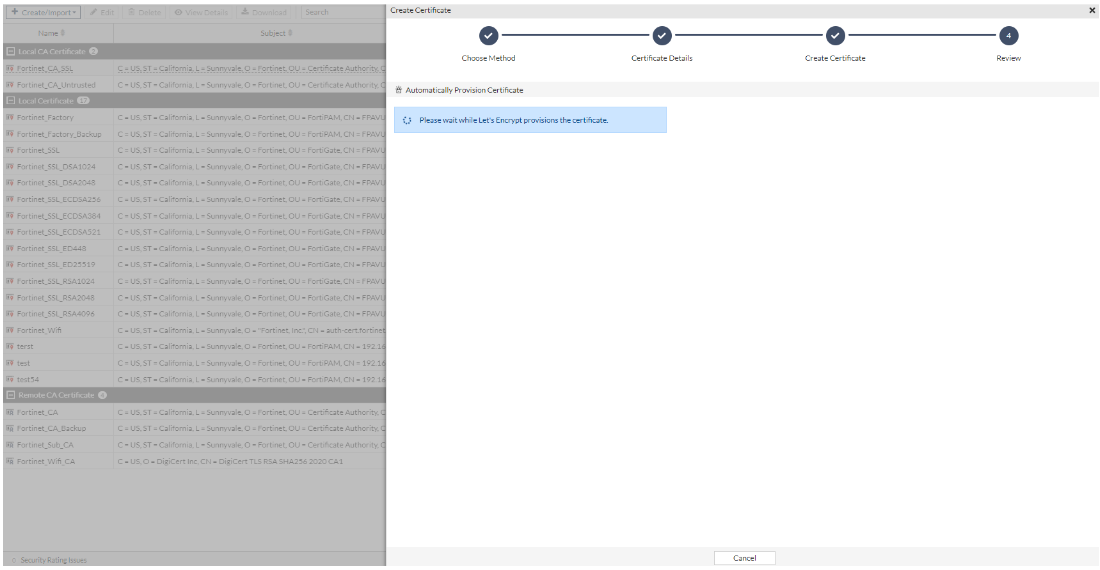


Select the interfaces on which the ACME client will listen for challenges in order to provision and renew certificates.

ACME interface: port1

9. Click *Close*.
10. Click *OK*.

 Wait for Let's Encrypt to provision the certificate.

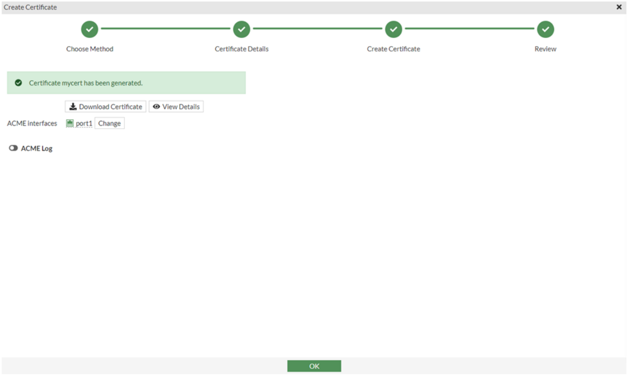


Please wait while Let's Encrypt provisions the certificate.

Name	Subject
Local CA Certificate 2	
Fortinet_CA_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, C
Fortinet_CA_Untrusted	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, C
Local Certificate 17	
Fortinet_Factory	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiPAM, CN = FPAVU
Fortinet_Factory_Backup	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiPAM, CN = FPAVU
Fortinet_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FPAVU
Fortinet_SSL_DSA1024	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FPAVU
Fortinet_SSL_DSA2048	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FPAVU
Fortinet_SSL_ECDSA256	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FPAVU
Fortinet_SSL_ECDSA384	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FPAVU
Fortinet_SSL_ECDSA521	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FPAVU
Fortinet_SSL_ED448	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FPAVU
Fortinet_SSL_ED25519	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FPAVU
Fortinet_SSL_RSA1024	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FPAVU
Fortinet_SSL_RSA2048	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FPAVU
Fortinet_SSL_RSA4096	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FPAVU
Fortinet_Wifi	C = US, ST = California, L = Sunnyvale, O = "Fortinet, Inc.", CN = auth-cert.fortinet
terst	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiPAM, CN = 192.16
test	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiPAM, CN = 192.16
test54	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiPAM, CN = 192.16
Remote CA Certificate 4	
Fortinet_CA	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, C
Fortinet_CA_Backup	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, C
Fortinet_Sub_CA	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, C
Fortinet_Wifi_CA	C = US, O = DigiCert Inc, CN = DigiCert TLS RSA SHA256 2020 CA1

After successfully creating the certificate, the newly created certificate can be viewed or downloaded.

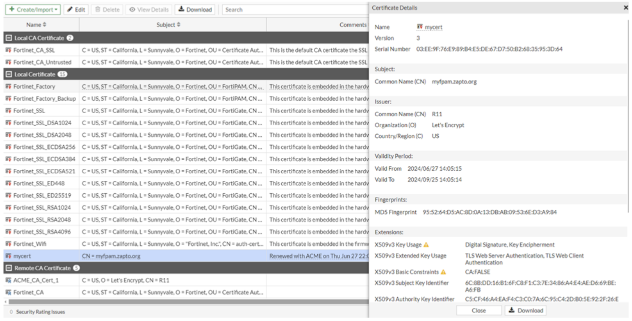
11. Enable *ACME Log* to see logs related to the certificate created using the ACME protocol.



Certificate mycert has been generated.

ACME interfaces port1 Change

ACME Log



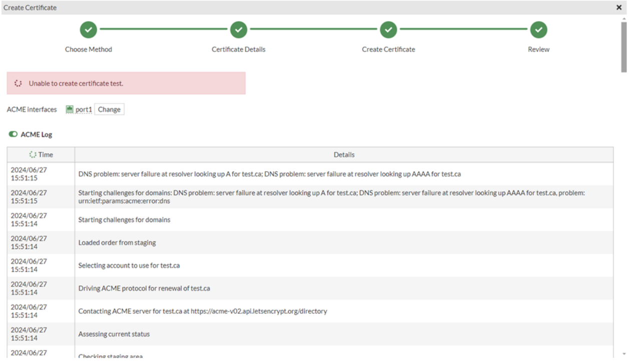
Name	Subject	Comments
Local CA Certificate 2		
Fortinet_CA_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Aut...	This is the default CA certificate the SSL
Fortinet_CA_Untrusted	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Aut...	This is the default CA certificate the SSL
Local Certificate 15		
Fortinet_Factory	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiPAM, CN ...	This certificate is embedded in the hardw
Fortinet_Factory_Backup	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiPAM, CN ...	This certificate is embedded in the hardw
Fortinet_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardw
Fortinet_SSL_DSA1024	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardw
Fortinet_SSL_DSA2048	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardw
Fortinet_SSL_ECDSA256	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardw
Fortinet_SSL_ECDSA384	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardw
Fortinet_SSL_ECDSA521	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardw
Fortinet_SSL_ED448	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardw
Fortinet_SSL_ED25519	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardw
Fortinet_SSL_RSA1024	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardw
Fortinet_SSL_RSA2048	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardw
Fortinet_SSL_RSA4096	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...	This certificate is embedded in the hardw
Fortinet_Wifi	C = US, ST = California, L = Sunnyvale, O = "Fortinet, Inc.", CN = auth-cert...	This certificate is embedded in the firmw
mycert	CN = myfpam.zapto.org	Renewed with ACME on Thu Jun 27 22:(
Remote CA Certificate 5		
ACME_CA_Cert_1	C = US, O = Let's Encrypt, CN = R11	
Fortinet_CA	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Aut...	

0 Security Rating Issues

Certificate Details

Name	mycert
Version	3
Serial Number	03:EE:9F:76:E9:89:B4:E5:DE:67:D7:50:B2:68:35:95:3D:64
Subject:	
Common Name (CN)	myfpam.zapto.org
Issuer:	
Common Name (CN)	R11
Organization (O)	Let's Encrypt
Country/Region (C)	US
Validity Period:	
Valid From	2024/06/27 14:05:15
Valid To	2024/09/25 14:05:14
Fingerprints:	
MD5 Fingerprint	95:52:64:D5:AC:8D:0A:13:DB:AB:09:53:6E:D3:A9:84
Extensions:	
X509v3 Key Usage ⚠	Digital Signature, Key Encipherment
X509v3 Extended Key Usage	TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Basic Constraints ⚠	CA:FALSE
X509v3 Subject Key Identifier	6C:8B:DD:16:B1:6F:C8:F1:C3:7E:34:86:A4:E4:AE:D6:69:BE:A6:FB
X509v3 Authority Key Identifier	C5:CF:46:A4:EA:F4:C3:C0:7A:6C:95:C4:2D:B0:5E:92:2F:26:E

If the certificate cannot be created, the ACME log is displayed for troubleshooting.



Unable to create certificate test.

ACME interfaces port1 Change

ACME Log

Time	Details
2024/06/27 15:51:15	DNS problem: server failure at resolver looking up A for test.ca; DNS problem: server failure at resolver looking up AAAA for test.ca
2024/06/27 15:51:15	Starting challenges for domains: DNS problem: server failure at resolver looking up A for test.ca; DNS problem: server failure at resolver looking up AAAA for test.ca, problem: urn:ietf:params:acme:error:dns
2024/06/27 15:51:14	Starting challenges for domains
2024/06/27 15:51:14	Loaded order from staging
2024/06/27 15:51:14	Selecting account to use for test.ca
2024/06/27 15:51:14	Driving ACME protocol for renewal of test.ca
2024/06/27 15:51:14	Contacting ACME server for test.ca at https://acme-v02.api.letsencrypt.org/directory
2024/06/27 15:51:14	Assessing current status
2024/06/27	Checking staging area

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 197.
  next
 end
```

 You can now access FortiPAM using *https://fqdn* where FQDN is the FortiPAM FQDN used in Creating a certificate on page 197.

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 certifiate 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.

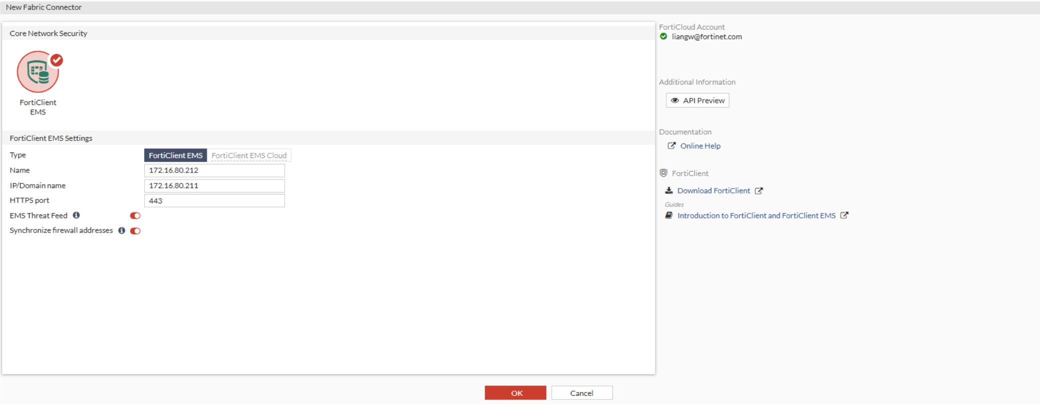
To deploy FortiPAM CA to Windows using EMS and FortiClient:

1. Deploying FortiPAM CA using EMS on page 202
2. Avoiding the web browser warning on the FortiPAM GUI on page 203
3. Downloading FortiPAM CA from the FortiPAM GUI on page 205

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*.

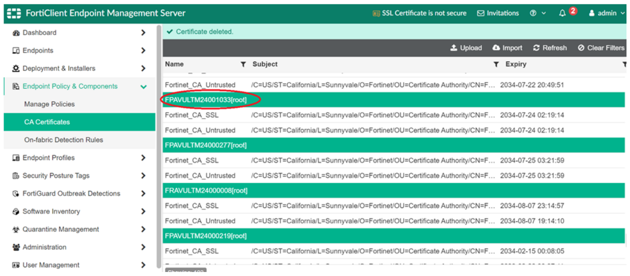


FortiClient EMS Settings

Type: FortiClient EMS | FortiClient EMS Cloud
Name: 172.16.80.212
IP/Domain name: 172.16.80.211
HTTPS port: 443
EMS Threat Feed: ●
Synchronize firewall addresses: ●

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`.

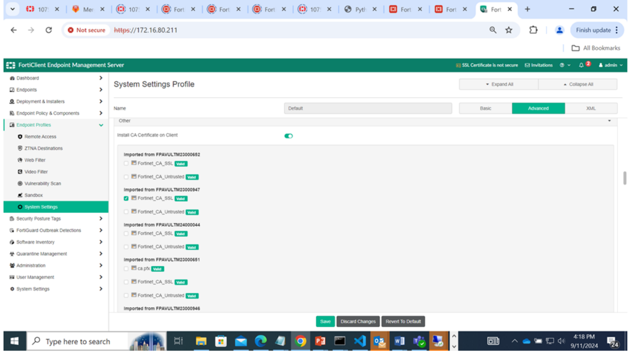


✓ Certificate deleted.

Name	Subject	Expiry
Fortinet_CA_Untrusted	/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=F...	2034-07-22 20:49:51
FPAVULTM24001033[root]		
Fortinet_CA_SSL	/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=F...	2034-07-24 02:19:14
Fortinet_CA_Untrusted	/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=F...	2034-07-24 02:19:14
FPAVULTM24000277[root]		
Fortinet_CA_SSL	/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=F...	2034-07-25 03:21:59
Fortinet_CA_Untrusted	/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=F...	2034-07-25 03:21:59
FRAVULTM24000008[root]		
Fortinet_CA_SSL	/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=F...	2034-08-07 23:14:57
Fortinet_CA_Untrusted	/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=F...	2034-08-07 19:14:10
FPAVULTM24000219[root]		
Fortinet_CA_SSL	/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=F...	2034-02-15 00:08:05

    d. Go to *Endpoint Profiles > System Setting*.
    e. Select the corresponding profile and edit it.

f. Go to the *Others* pane.



System Settings Profile

Name: Default

Other

Install CA Certificate on Client: ●

Imported from FPAVULTM23000652
□ Fortinet_CA_SSL Valid
□ Fortinet_CA_Untrusted Valid

Imported from FPAVULTM23000947
☑ Fortinet_CA_SSL Valid
□ Fortinet_CA_Untrusted Valid

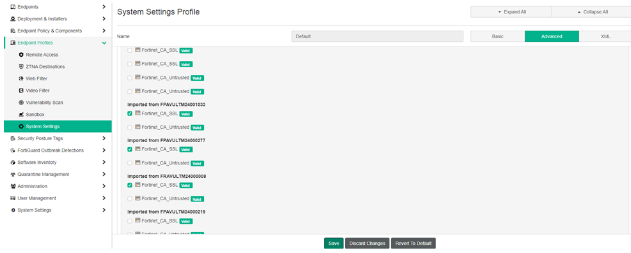
Imported from FPAVULTM24000044
□ Fortinet_CA_SSL Valid
□ Fortinet_CA_Untrusted Valid

Imported from FPAVULTM23000651
□ ca.pfx Valid
□ Fortinet_CA_SSL Valid
□ Fortinet_CA_Untrusted Valid

Imported from FPAVULTM23000946

g. Look for your FortiPAM serial number and enable *Fortinet_CA_SSL*.

h. Click *Save*.



System Settings Profile

Name: Default

□ Fortinet_CA_SSL Valid
□ Fortinet_CA_SSL Valid
□ Fortinet_CA_Untrusted Valid
□ Fortinet_CA_Untrusted Valid

Imported from FPAVULTM24001033
☑ Fortinet_CA_SSL Valid
□ Fortinet_CA_Untrusted Valid

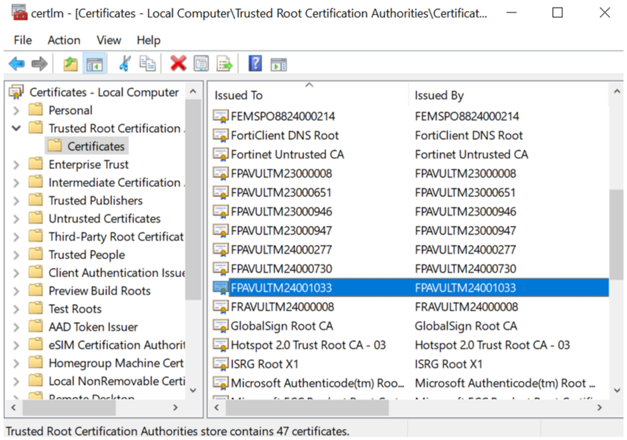
Imported from FPAVULTM24000277
☑ Fortinet_CA_SSL Valid
□ Fortinet_CA_Untrusted Valid

Imported from FRAVULTM24000008
☑ Fortinet_CA_SSL Valid
□ Fortinet_CA_Untrusted Valid

Imported from FPAVULTM24000219
□ Fortinet_CA_SSL Valid

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.


certlm - [Certificates - Local Computer\Trusted Root Certification Authorities\Certificat...
File
Action
View
Help
Certificates - Local Computer
Personal
Trusted Root Certification
Certificates
Enterprise Trust
Intermediate Certification
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificat
Trusted People
Client Authentication Issue
Preview Build Roots
Test Roots
AAD Token Issuer
eSIM Certification Authorit
Homegroup Machine Cert
Local NonRemovable Certi
Remote Desktop

Issued To	Issued By
FEMSPO8824000214	FEMSPO8824000214
FortiClient DNS Root	FortiClient DNS Root
Fortinet Untrusted CA	Fortinet Untrusted CA
FPAVULTM23000008	FPAVULTM23000008
FPAVULTM23000651	FPAVULTM23000651
FPAVULTM23000946	FPAVULTM23000946
FPAVULTM23000947	FPAVULTM23000947
FPAVULTM24000277	FPAVULTM24000277
FPAVULTM24000730	FPAVULTM24000730
FPAVULTM24001033	FPAVULTM24001033
FRAVULTM24000008	FRAVULTM24000008
GlobalSign Root CA	GlobalSign Root CA
Hotspot 2.0 Trust Root CA - 03	Hotspot 2.0 Trust Root CA - 03
ISRG Root X1	ISRG Root X1
Microsoft Authenticode(tm) Roo...	Microsoft Authenticode(tm) Root ...

Trusted Root Certification Authorities store contains 47 certificates.

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.

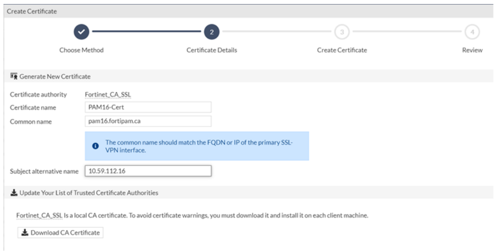
   a. In the FortiPAM GUI, go to *System > Certificates*, click *Create/Import*, and select *Certificate* from the dropdown.

   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.



Create Certificate

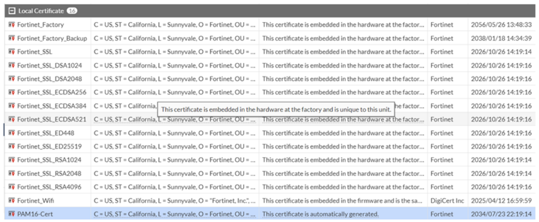
Generate New Certificate

Certificate authority	Fortinet_CA_SSL
Certificate name	PAM16-Cert
Common name	pam16.fortipam.ca
	The common name should match the FQDN or IP of the primary SSL-VPN interface.
Subject alternative name	10.59.112.16

Update Your List of Trusted Certificate Authorities

Fortinet_CA_SSL Is a local CA certificate. To avoid certificate warnings, you must download it and install it on each client machine.

   f. Click *Create*.
   The new certificate is created and listed under *Local Certificate*.



Local Certificate 16

Fortinet_Factory	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = ...	This certificate is embedded in the hardware at the factor...	Fortinet	2056/05/26 13:48:33
Fortinet_Factory_Backup	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = ...	This certificate is embedded in the hardware at the factor...	Fortinet	2038/01/18 14:34:39
Fortinet_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = ...	This certificate is embedded in the hardware at the factor...	Fortinet	2026/10/26 14:19:14
Fortinet_SSL_DSA1024	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = ...	This certificate is embedded in the hardware at the factor...	Fortinet	2026/10/26 14:19:16
Fortinet_SSL_DSA2048	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = ...	This certificate is embedded in the hardware at the factor...	Fortinet	2026/10/26 14:19:16
Fortinet_SSL_ECDSA256	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = ...	This certificate is embedded in the hardware at the factor...	Fortinet	2026/10/26 14:19:16
Fortinet_SSL_ECDSA384	C = US, ST = California,	he factor...	Fortinet	2026/10/26 14:19:16
Fortinet_SSL_ECDSA521	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = ...	This certificate is embedded in the hardware at the factor...	Fortinet	2026/10/26 14:19:16
Fortinet_SSL_ED448	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = ...	This certificate is embedded in the hardware at the factor...	Fortinet	2026/10/26 14:19:16
Fortinet_SSL_ED25519	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = ...	This certificate is embedded in the hardware at the factor...	Fortinet	2026/10/26 14:19:16
Fortinet_SSL_RSA1024	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = ...	This certificate is embedded in the hardware at the factor...	Fortinet	2026/10/26 14:19:14
Fortinet_SSL_RSA2048	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = ...	This certificate is embedded in the hardware at the factor...	Fortinet	2026/10/26 14:19:14
Fortinet_SSL_RSA4096	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = ...	This certificate is embedded in the hardware at the factor...	Fortinet	2026/10/26 14:19:16
Fortinet_Wifi	C = US, ST = California, L = Sunnyvale, O = "Fortinet, Inc.", ...	This certificate is embedded in the firmware and is the sa...	DigiCert Inc	2025/04/12 16:59:59
PAM16-Cert	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = ...	This certificate is automatically generated.	Fortinet	2034/07/23 22:19:14

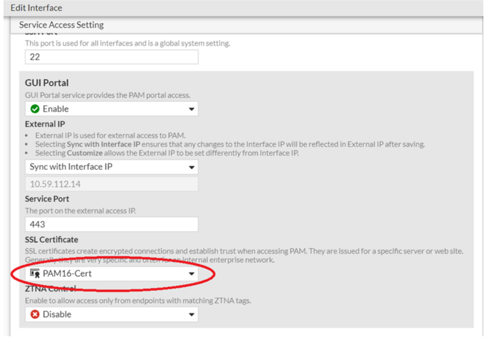
This certificate is embedded in the hardware at the factory and is unique to this unit.

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.



Edit Interface

Service Access Setting

This port is used for all interfaces and is a global system setting.

22

GUI Portal

GUI Portal service provides the PAM portal access.

Enable

External IP

- External IP is used for external access to PAM.
- Selecting **Sync with Interface IP** ensures that any changes to the Interface IP will be reflected in External IP after saving.
- Selecting **Customize** allows the External IP to be set differently from Interface IP.

Sync with Interface IP

10.59.112.14

Service Port

The port on the external access IP.

443

SSL Certificate

SSL certificates create encrypted connections and establish trust when accessing PAM. They are issued for a specific server or web site. Generally they are very specific and often for an internal enterprise network.

PAM16-Cert

ZTNA Control

Enable to allow access only from endpoints with matching ZTNA tags.

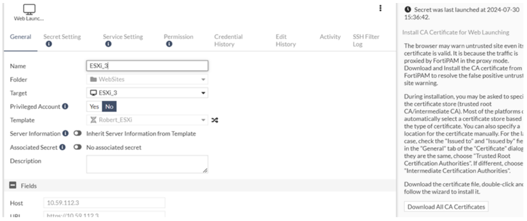
Disable

   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*.



Name: ESXi_3
Folder: WebSites
Target: ESXi_3
Privileged Account: Yes [✓ No]
Template: Robert_ESXi
Server Information: Inherit Server Information from Template
Associated Secret: No associated secret
Description:
Host: 10.59.112.3
URL: https://10.59.112.3

Secret was last launched at 2024-07-30 15:36:42.

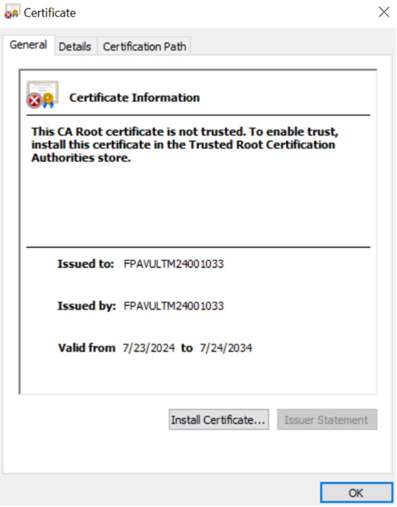
Install CA Certificate for Web Launching

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 untrust site warning.

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

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

4. Double-click the downloaded file to unzip it.
5. Double-click the CA certificate.



Certificate Information

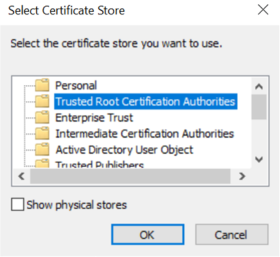
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: FPAVULTM24001033

Issued by: FPAVULTM24001033

Valid from 7/23/2024 to 7/24/2034

6. Click *Install Certificate* and follow the installation prompts to install the certificate to the trust root.


Select Certificate Store
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
OK
Cancel

Select the certificate store you want to use.

□ Show physical stores

7. Click *OK*.

Logging servers

This section describes various logging servers available to FortiPAM.

FortiAnalyzer Cloud as a logging server

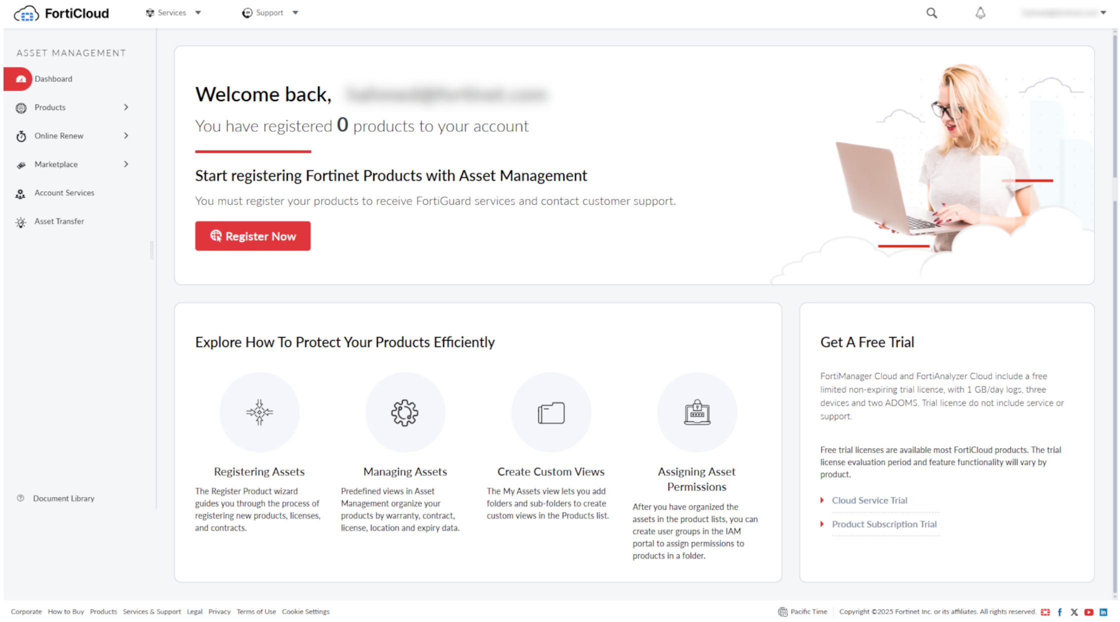
FortiAnalyzer Cloud is a remote logging server that keeps an additional copy of logs from FortiPAM.

Configuring FortiAnalyzer Cloud as a logging server:

1. Registering FortiAnalyzer Cloud on page 206
2. Deploying a FortiAnalyzer Cloud instance on page 207
3. Add FortiPAM to FortiAnalyzer Cloud instance on page 209
4. Enabling FortiAnalyzer Cloud in FortiPAM on page 209
5. Launching a secret on page 211

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.



Welcome back, [redacted]

You have registered 0 products to your account

Start registering Fortinet Products with Asset Management

You must register your products to receive FortiGuard services and contact customer support.

Explore How To Protect Your Products Efficiently

Registering Assets

The Register Product wizard guides you through the process of registering new products, licenses, and contracts.

Managing Assets

Predefined views in Asset Management organize your products by warranty, contract, license, location and expiry data.

Create Custom Views

The My Assets view lets you add folders and sub-folders to create custom views in the Products list.

Assigning Asset Permissions

After you have organized the assets in the product lists, you can create user groups in the IAM portal to assign permissions to products in a folder.

Get A Free Trial

FortiManager Cloud and FortiAnalyzer Cloud include a free limited non-expiring trial license, with 1 GB/day logs, three devices and two ADOMS. Trial license do not include service or support.

Free trial licenses are available most FortiCloud products. The trial license evaluation period and feature functionality will vary by product.

Copyright ©2025 Fortinet Inc. or its affiliates. All rights reserved.

2. On the *Asset Management* portal, click *Register Now* to register FortiAnalyzer Cloud.

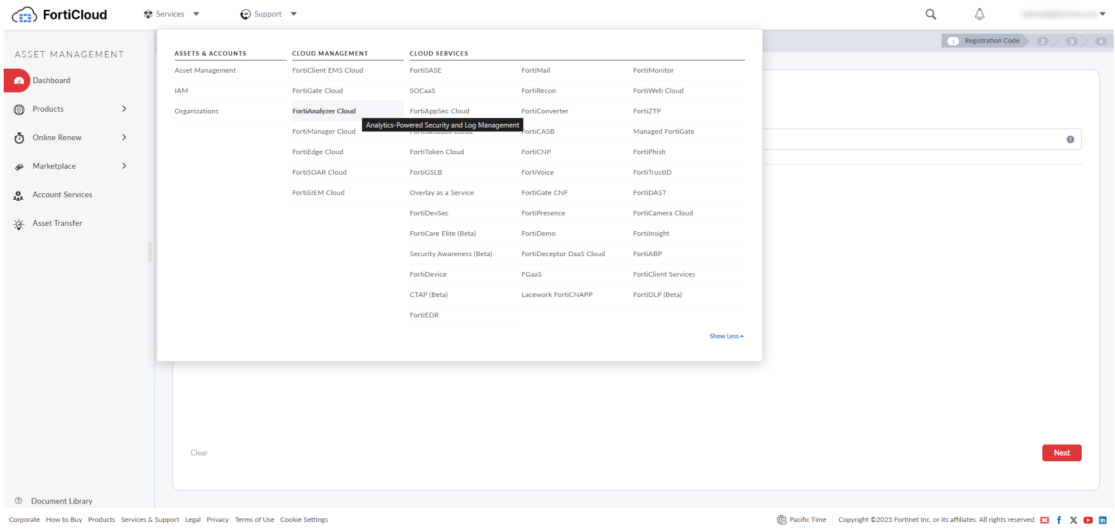
3. Provide the registration code:
   a. Enter the FortiAnalyzer Cloud registration code.
   b. Choose your end user type as either a government or non-government user.
   c. Click *Next*.
4. The *Fortinet Product Registration Agreement* page displays.
   Select the check box to indicate that you have 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

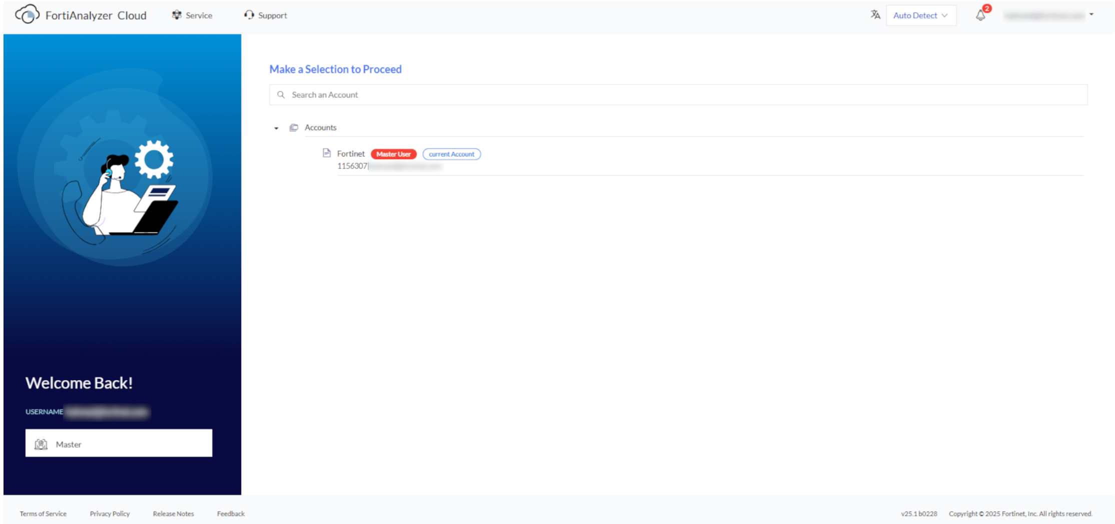
After registering a FortiAnalyzer Cloud instance, deploy the FortiAnalyzer Cloud instance.

To deploy a FortiAnalyzer Cloud instance:

1. From the *Services* menu, in *CLOUD MANAGEMENT*, select *FortiAnalyzer Cloud*.



2. In FortiAnalyzer Cloud, select a FortiCloud account to proceed.



[redacted]

Make a Selection to Proceed

Search an Account

Accounts

Fortinet Master User current Account
1156307[redacted]

Welcome Back!

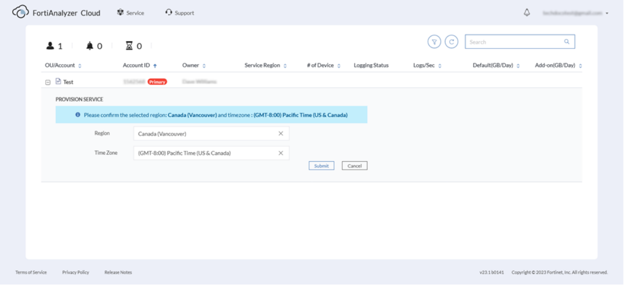
USERNAME [redacted]

Master

Terms of Service Privacy Policy Release Notes Feedback

v25.1 b0228 Copyright © 2025 Fortinet, Inc. All rights reserved.

3. In the new window, select a *Region*.
   In this example, the region is *Canada (Vancouver)*.
4. Select a *Time Zone* for the FortiAnalyzer Cloud instance.



[redacted]

OU/Account	Account ID	Owner	Service Region	# of Device	Logging Status	Logs/Sec	Default(GB/Day)	Add-on(GB/Day)
Test	[redacted] Primary	[redacted]						

PROVISION SERVICE

Please confirm the selected region: **Canada (Vancouver)** and timezone : **(GMT-8:00) Pacific Time (US & Canada)**

Region: Canada (Vancouver)

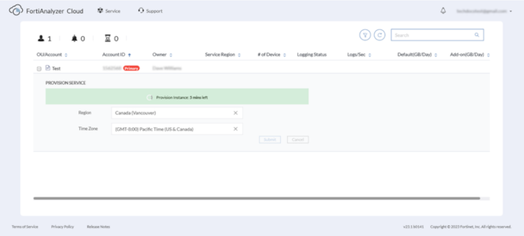
Time Zone: (GMT-8:00) Pacific Time (US & Canada)

Submit Cancel

Terms of Service Privacy Policy Release Notes

v23.1 b0141 Copyright © 2023 Fortinet, Inc. All rights reserved.

5. Click *Submit*.
6. Confirm the selected region and the timezone.
7. Review and accept the *Terms of Service* and *Privacy Policy*.
   FortiAnalyzer Cloud instance is provisioned in a few minutes.



[redacted]

OU/Account	Account ID	Owner	Service Region	# of Device	Logging Status	Logs/Sec	Default(GB/Day)	Add-on(GB/Day)
Test	[redacted] Primary	[redacted]						

PROVISION SERVICE

Provision Instance: 5 mins left

Region: Canada (Vancouver)

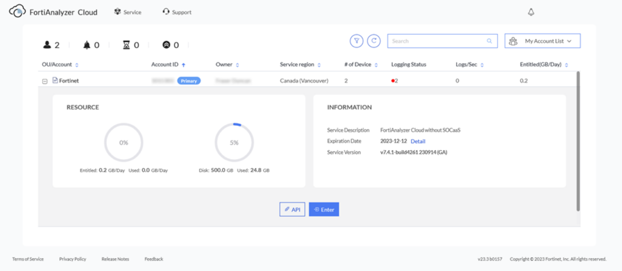
Time Zone: (GMT-8:00) Pacific Time (US & Canada)

Submit Cancel

Terms of Service Privacy Policy Release Notes

v23.1 b0141 Copyright © 2023 Fortinet, Inc. All rights reserved.

8. Once provisioned, expand the account, and click *Enter* to access the FortiAnalyzer Cloud instance.



OU/Account	Account ID	Owner	Service region	# of Device	Logging Status	Logs/Sec	Entitled(GB/Day)
Fortinet	[redacted] Primary	[redacted]	Canada (Vancouver)	2	●2	0	0.2

RESOURCE

0% Entitled: 0.2 GB/Day Used: 0.0 GB/Day

5% Disk: 500.0 GB Used: 24.8 GB

INFORMATION

Service Description: FortiAnalyzer Cloud without SOCaaS

Expiration Date: 2023-12-12 Detail

Service Version: v7.4.1-build4261 230914 (GA)

API Enter

Terms of Service Privacy Policy Release Notes Feedback

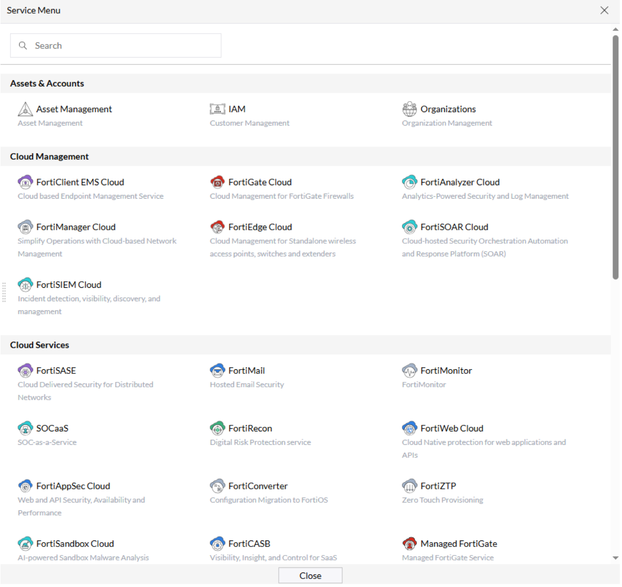
v23.3 b0157 Copyright © 2023 Fortinet, Inc. All rights reserved.

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.

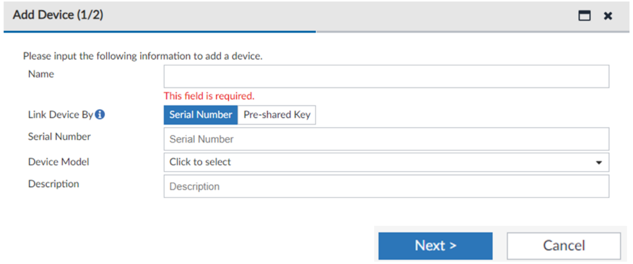

Service Menu
Search
Assets & Accounts
Asset Management
Asset Management
IAM
Customer Management
Organizations
Organization Management
Cloud Management
FortiClient EMS Cloud
Cloud based Endpoint Management Service
FortiGate Cloud
Cloud Management for FortiGate Firewalls
FortiAnalyzer Cloud
Analytics-Powered Security and Log Management
FortiManager Cloud
Simplify Operations with Cloud-based Network Management
FortiEdge Cloud
Cloud Management for Standalone wireless access points, switches and extenders
FortiSOAR Cloud
Cloud-hosted Security Orchestration Automation and Response Platform (SOAR)
FortiSIEM Cloud
Incident detection, visibility, discovery, and management
Cloud Services
FortiSASE
Cloud Delivered Security for Distributed Networks
FortiMail
Hosted Email Security
FortiMonitor
FortiMonitor
SOCaaS
SOC-as-a-Service
FortiRecon
Digital Risk Protection service
FortiWeb Cloud
Cloud Native protection for web applications and APIs
FortiAppSec Cloud
Web and API Security, Availability and Performance
FortiConverter
Configuration Migration to FortiOS
FortiZTP
Zero Touch Provisioning
FortiSandbox Cloud
AI-powered Sandbox Malware Analysis
FortiCASB
Visibility, Insight, and Control for SaaS
Managed FortiGate
Managed FortiGate Service
Close

2. Select *FortiAnalyzer Cloud*.

   This redirects you to the *FortiAnalyzer Cloud* portal.

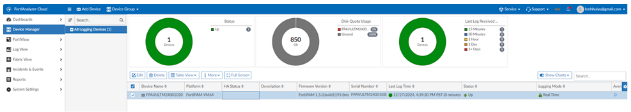
3. Click *Add Device*, and enter FortiPAM related information.

   In this example, FortiPAM device is linked to FortiAnalyzer Cloud by serial number.



Please input the following information to add a device.

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*.



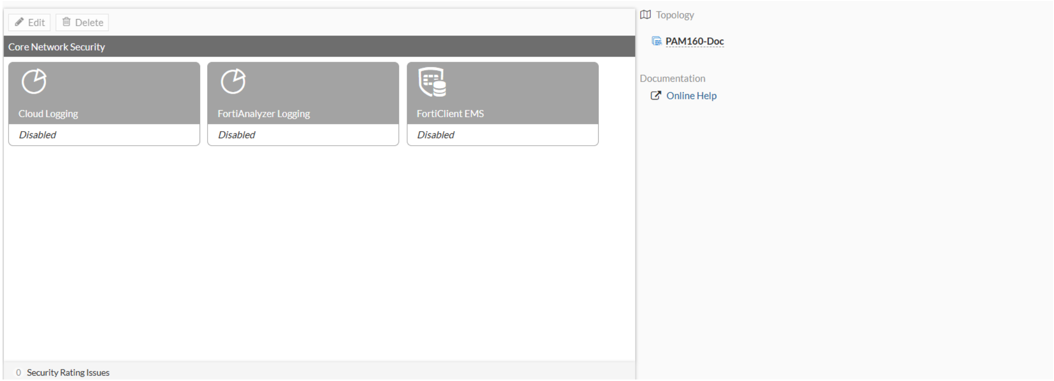
Enabling FortiAnalyzer Cloud in FortiPAM

You can now use FortiAnalyzer Cloud on FortiPAM.

To enable FortiAnalyzer Cloud in FortiPAM:

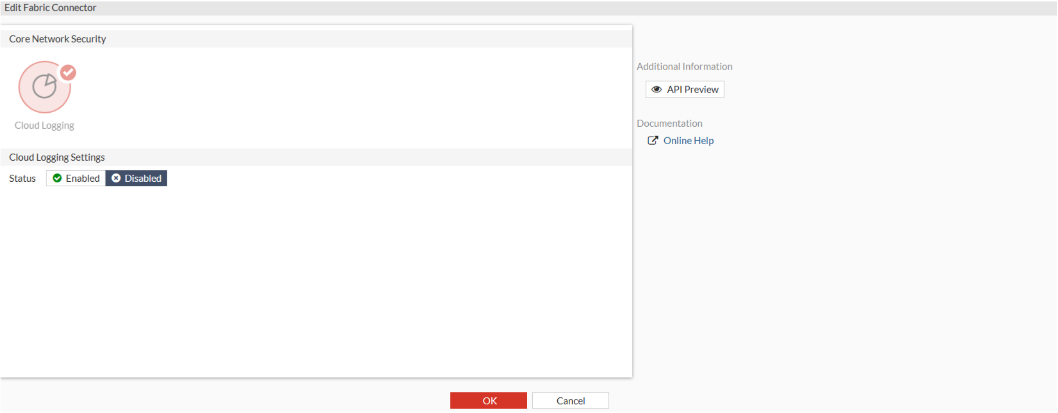
1. Go to *Network > Fabric Connectors*.

   Core Network Security opens.



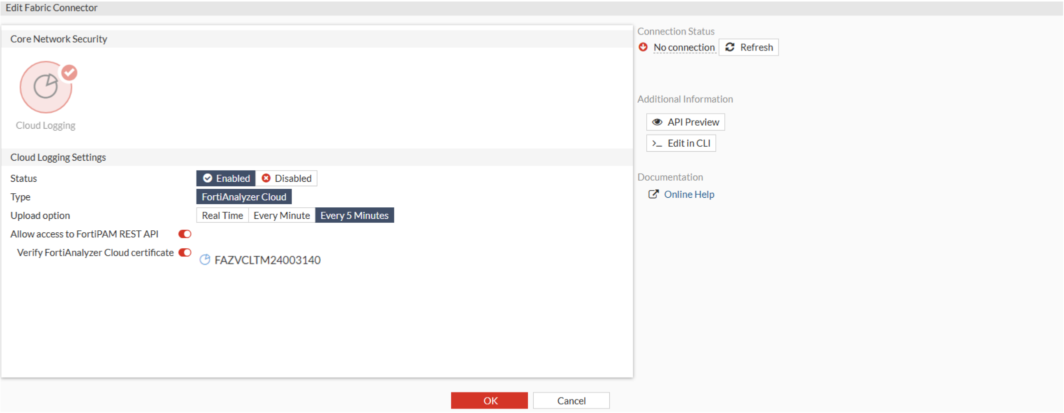
2. Select *Cloud Logging* and select *Edit*.

   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.



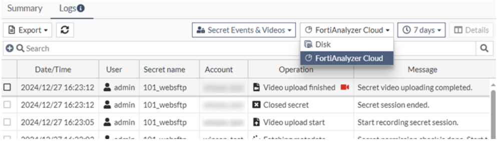
4. In *Upload option*, select the frequency of log uploads to the remote FortiAnalyzer Cloud:
   a. *Real Time*: Logs are sent to the remote device in real time.
   b. *Every Minute*: Logs are sent to the remote device once every minute.
   c. *Every 5 Minutes*: Logs are sent to the remote device once 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_websftp	[redacted]	Video upload finished	Secret video uploading completed.
□	2024/12/27 16:23:12	admin	101_websftp	[redacted]	Closed secret	Secret session ended.
□	2024/12/27 16:23:05	admin	101_websftp	[redacted]	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:

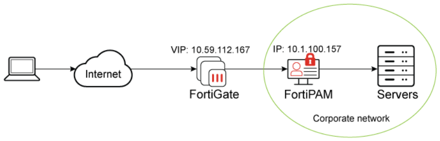
1. Configuring a VIP on FortiGate for FortiPAM access on page 212
2. Configuring ZTNA on FortiGate for FortiPAM access on page 214

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 stattus 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

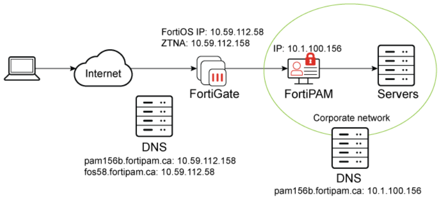
For information ZTNA and web proxy forwarding, see:

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



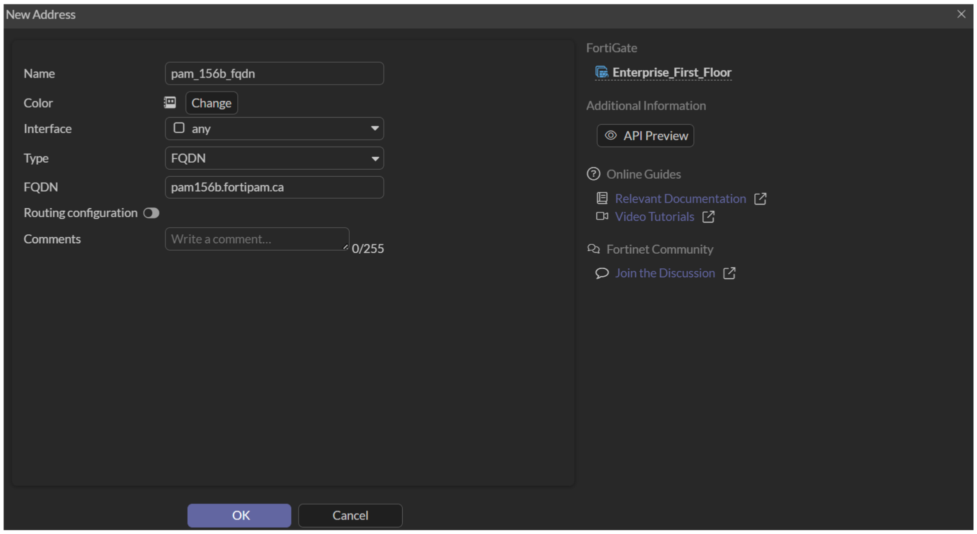
Configuring ZTNA for FortiPAM access

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*.



New Address

Name: pam_156b_fqdn

Color: Change

Interface: any

Type: FQDN

FQDN: pam156b.fortipam.ca

Routing configuration

Comments: Write a comment... 0/255

FortiGate: Enterprise_First_Floor

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:

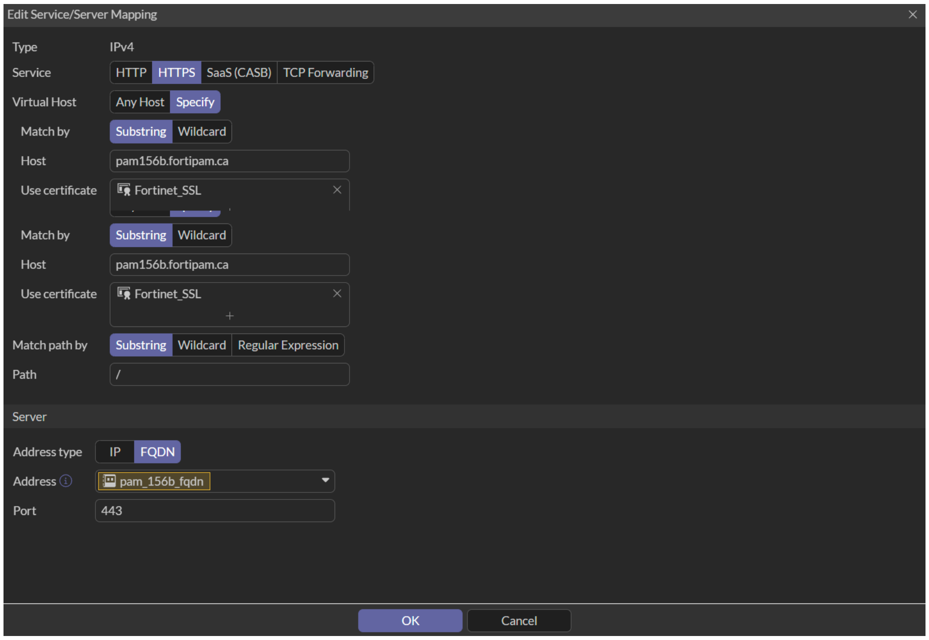
1. In the FortiGate GUI, go to *Policy & Objects > ZTNA*, and select *Create new* in the *ZTNA Server* tab.
   The *New ZTNA Server* window opens.
2. In *Name*, enter a name for the ZTNA server.
3. In *Interface*, select *port1*.
4. In *IP address*, enter the IP address for the FortiGate, e.g., `10.59.112.158`.
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*.



Edit Service/Server Mapping

Type IPv4

Service: HTTPS

Virtual Host: Specify

Match by: Substring

Host: pam156b.fortipam.ca

Use certificate: Fortinet_SSL

Match by: Substring

Host: pam156b.fortipam.ca

Use certificate: Fortinet_SSL

Match path by: Substring

Path: /

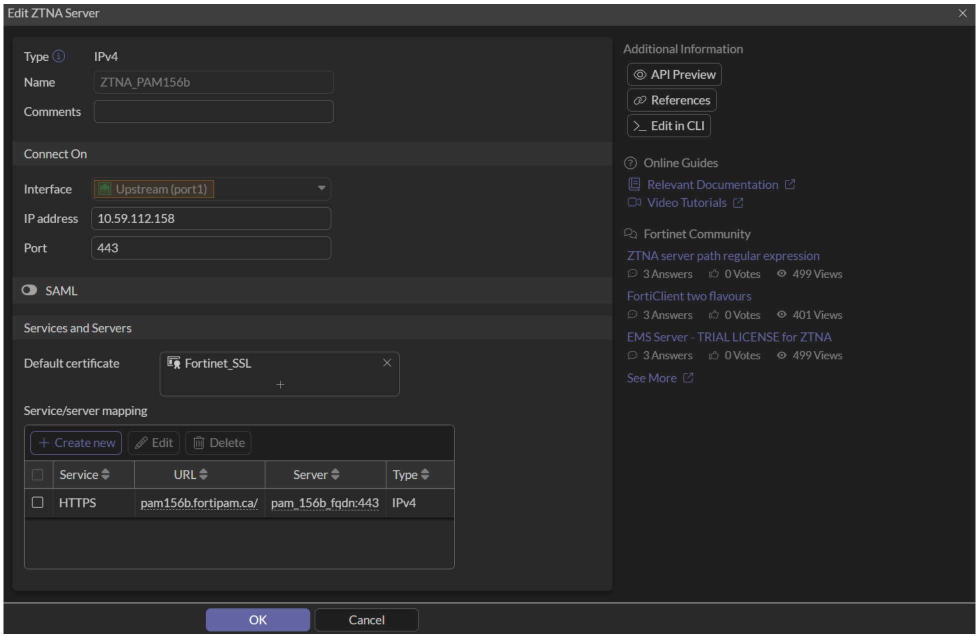
Server

Address type: FQDN

Address: pam_156b_fqdn

Port: 443

8. Click *OK*.



Edit ZTNA Server

Type: IPv4
Name: ZTNA_PAM156b
Comments:

Connect On

Interface: Upstream (port1)
IP address: 10.59.112.158
Port: 443

SAML

Services and Servers

Default certificate: Fortinet_SSL

Service/server mapping

	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
```

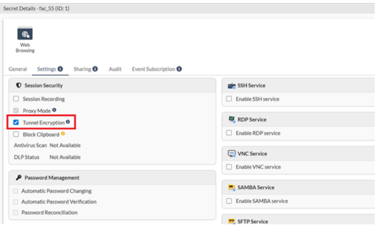
2. In the CLI console, enter the following commands to change the `proxy-fqdn` to the FortiGate GUI FQDN:

```
config web -proxy global
 set proxy-fqdn "fos58.fortipam.ca"
end
```

3. 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
```

4. In the FortiPAM GUI, go to *Secrets* > *Secrets*, from the list, open a secret:
   a. Go to the *Settings* tab, enable *Tunnel Encryption*, and click *Save*.



☐ Session Recording
☑ Proxy Mode
☑ Tunnel Encryption
☐ Block Clipboard
Antivirus Scan Not Available
DLP Status Not Available

☐ Automatic Password Changing
☐ Automatic Password Verification
☐ Password Reconciliation

☐ Enable SSH service
☐ Enable RDP service
☐ Enable VNC service
☐ Enable SAMBA service

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