FortiSASE Endpoint Management and ZTNA Lab

4D Accelerator

Table of Contents

Introduction

1. Lab introduction

In this 4-D Accelerator lab, we switch gears from the secure internet access (SIA) configurations that the FortiSASE Basic Deployment Lab introduced and dive into advanced endpoint configuration and management options. We demonstrate different endpoint management features like endpoint profile assignment, VPN autoconnect, split tunnel, vulnerability scan, zero trust network access (ZTNA) tagging and rules, and SAML single sign on (SSO) authentication for SIA. We discuss how to leverage ZTNA tags and rules to access resources that a ZTNA application gateway hosts using SAML SSO authentication.

In summary, in this 4-D Accelerator lab guide, we configure and understand the following key FortiSASE endpoint management features:

Feature	Enables...
Custom endpoint profiles	Segregation of remote users based on endpoints belonging to different Active Directory (AD) groups and non-AD groups.
VPN autoconnect	Caching user credentials on FortiClient after user's initial login to FortiSASE SIA and enables FortiClient to automatically connect to SIA if endpoint reboots, during user login to OS and when endpoint's network connectivity changes from being unavailable to available, without any manual intervention.
Bypass FortiSASE	Disabling VPN autoconnect based on endpoint's on- and off-net status.
Split tunnel	Users to access the resources that split tunnel defines to be accessed via their local internet and not through FortiSASE SIA.
ZTNA tags, tagging rules, and application gateway	Sharing ZTNA tags with the corporate firewall (FortiGate_HQ) to allow or deny access to HTTP and SSH services that the ZTNA application gateway protects.

Intended audience

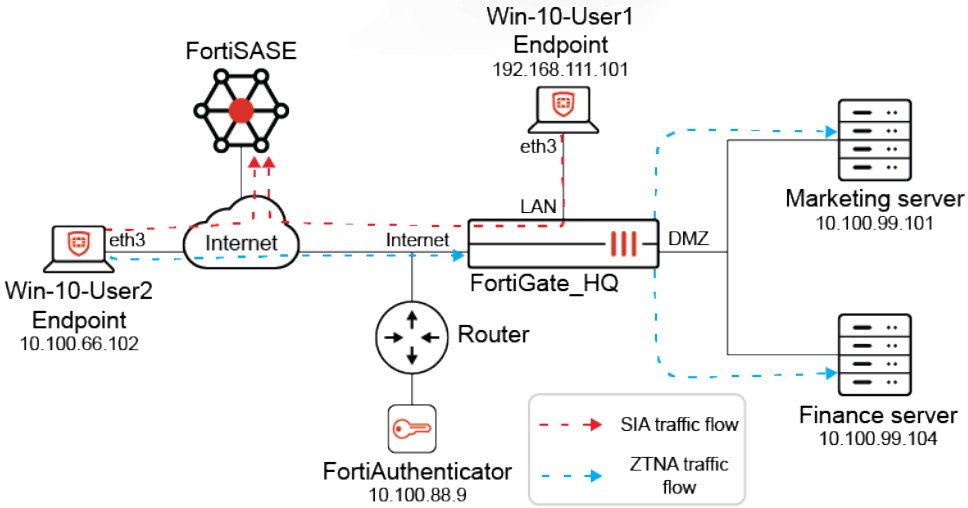
This 4-D Accelerator lab is aimed at anyone wanting to gain basic understanding and apply different use cases of FortiSASE endpoint management features. Expect to spend approximately one hour and thirty minutes depending on your familiarity with networking knowledge to complete this 4-D Accelerator lab. Midlevel network and security architects in companies of all sizes and verticals should find this guide helpful.

About this guide

This 4-D Accelerator lab primarily serves the purpose of walking through a working demonstration of the solution to help readers familiarize themselves with the basic configuration steps involved. Reviewing supplementary material found in product administration guides, example guides, cookbooks, release notes, and other documents where appropriate on the Fortinet Document Library is recommended.

1.1 Lab topology

Topology



The topology is of a company named Financial, which has recently acquired another company named Horizon to manage marketing services (i.e. Marketing Server) for Financial. The endpoint Windows10-User1 originally belongs to Financial and is integrated into Financial's Active Directory (AD) domain called financial.local. The endpoint Windows10-User2 belongs to a user from the acquired company, Horizon, that has not yet been integrated into Financial's AD environment. Thus, Window10-User1 is an AD endpoint, and Window10-User2 is a considered non-AD endpoint for the Financial company.

FortiClient is preinstalled on both endpoints. In addition, the user on the endpoint Windows10-User1 is situated in the office and considered on-premise (i.e. located behind the corporate firewall FortiGate_HQ). The user on endpoint Windows10-User2 works remotely and is considered off-premise (i.e. located on the internet). The notation of endpoint being on- or off-premise is always with respect to FortiGate_HQ in this lab guide.

As Windows10-User1 is belongs to Financial since the beginning, it is considered trusted, whereas endpoint Windows10-User2 is new and is considered not trusted as Windows10-User1.

To summarize the differences between Windows10-User1 and Windows10-User2 in this lab's context:

Windows10-User1	Windows10-User2
Part of AD domain financial.local. Is an AD-endpoint.	Not a part of any AD domain. Is considered a non-AD endpoint
On-premise or on-net (i.e. located behind FortiGate_HQ's LAN interface)	Off-premise or off-net (i.e. located on the internet)
Trusted	Not trusted
Username is: financial\johnlocus	Username is: local\fortinet

Financial owns two servers named Finance and Marketing that are running HTTP and SSH Services on them. According to the requirements of Financial company, user on endpoint Windows10-User1 must have access to Finance server only, whereas user on endpoint Windows10-User2 must have access to Marketing server only. These services must be accessed via ZTNA Application Gateway, which is configured on internet interface (port1) of FortiGate_HQ.

For the purpose of this lab, two different domains are used for ZTNA as follows:

- **financial.local**: simulation of private domain (resolvable by Windows endpoint used in this lab) that resolves marketing.financial.local and finance.financial.local to the actual original private IP address of marketing and finance servers respectively.
- **fortidemo.fortinet.com**: simulation of public domain (resolvable by Windows endpoint used in this lab), that resolves marketing.fortidemo.fortinet.com and finance.fortidemo.fortinet.com to 10.100.66.99, which is internet interface (port1) IP address of FortiGate_HQ.

There are two ways to access Finance and Marketing servers via ZTNA Application Gateway in this lab, which are by using:

- Web Access Proxy: access HTTP resources using public domain/FQDNs of Finance and Marketing server.
- TCP Forwarding: access SSH resources using private domain/FQDNs of Finance and Marketing server.

The table below shows the endpoints that are required to have access to either the Marketing or Finance server. Endpoints must use FQDNs given below to access HTTP and SSH service on these servers.

The Endpoint	Have access to	Via HTTP Service (using HTTP Access Proxy method) by using following FQDN	Via SSH Service (using TCP Forwarding method) by using following FQDN
Windows10-User1 (AD Endpoint)	Finance server	finance.fortidemo.fortinet.com:9443	finance.financial.local:22
Windows10-User2 (non-AD Endpoint)	Marketing server	marketing.fortidemo.fortinet.com:9443	marketing.financial.local:22

FortiAuthenticator is connected to FortiGate_HQ's internet interface and serves as SAML Identity Provider (IdP) in SAML Authentication flow.

Devices and networks

This lab uses the following devices and networks:

Device	Port/service	Address	Gateway
Marketing server	eth1 (DMZ)	10.100.99.101/24	10.100.99.1/24
Finance server	eth1 (DMZ)	10.100.99.104/24	10.100.99.1/24
FortiGate_HQ	port4 (LAN) port1 (internet) port2 (DMZ)	192.168.111.1/24 10.100.66.99/24 10.100.99.1	N/A 10.100.66.1 N/A
Windows10-User1	eth3	192.168.111.101/24	192.168.111.1
Windows10-User2	eth3	10.100.66.102	10.100.66.1

Users and endpoints

The following shows the user type, computer name, and credentials for the Windows 10 endpoints and for SAML user authentication to connect to FortiSASE SIA and ZTNA Application Gateway:

User type	Computer name	Domain\username	Password
AD user	Windows10-User1	financial\johnlocus	SecurityFabric
Non-AD user	Windows10-User2	local\fortinet	SecurityFabric

1.2 4-D Accelerator lab configuration modules

This table provides a list of configuration modules for this 4-D Accelerator lab. You can use the table to tailor a demonstration. Required modules take approximately one hour to one hour and thirty minutes. Optional modules build on the configuration completed in required modules. The time to complete each module may vary depending on user familiarity with networking knowledge and FortiSASE.

Use case	4-D Accelerator lab configuration modules	Type	Suggested time in minutes
	2.1 Checking FortiSASE EMS connectivity on page 7		
Basic SIA and endpoint profile features (custom endpoint profiles, VPN autoconnect, bypass FortiSASE, split tunnel)	2.2 Configuring FortiSASE with FortiAuthenticator as SAML IdP (required) on page 8	Required	40
	2.3 Creating SSO user group and VPN policy for SIA (required) on page 14		
	2.4 Configuring domains (required) on page 15		
	2.5 Configuring endpoint profiles (required) on page 17		
	2.6 Onboarding endpoint to connect it to FortiSASE (required) on page 19		
	2.7 Configuring and verifying tunnel autoconnect and bypass FortiSASE (required) on page 21		
	2.8 Configuring and verifying split tunneling (required) on page 25		
ZTNA tags, connection rules, and ZTNA access proxy	2.9 Configuring security posture tagging rules and ZTNA connection rules (required) on page 28	Required	30
	2.10 Configuring FortiClient Cloud connector and verifying ZTNA tag sync (required) on page 35		
	2.11 Configuring SAML SSO on		

Use case	4-D Accelerator lab configuration modules	Type	Suggested time in minutes
	FortiGate_HQ (required) on page 36		
	2.12 Configuring ZTNA tags in full ZTNA firewall policy (required) on page 39		
	2.13 Accessing services via a ZTNA application gateway (required) on page 41		
	2.14 Running a Vulnerability Scan and configuring application-based ZTNA tags (optional) on page 43	Optional	10
		Total	80

2. Deployment procedures

This 4-D Accelerator lab uses two endpoints that have FortiClient preinstalled. The endpoint Windows10-User1 is domain-joined and part of the financial.local domain. The other endpoint, Window10-User2, is a non-AD endpoint. Using these two endpoints, we demonstrate FortiSASE Endpoint Management features by following the tasks in this section.

2.1 Checking FortiSASE EMS connectivity

Prior to configuring FortiSASE, we ensure that FortiSASE successfully established connectivity with its Endpoint Management Service (EMS). This connectivity is crucial for SAML authentication, endpoint profile deployment, and endpoint monitoring.

In the demo lab environment, you will encounter one of these scenarios:

EMS connectivity is...	Probability
Provisioned and connected successfully.	Most scenarios
Not established. FortiSASE establishes EMS connectivity after user clicks **Retry Connection**.	Small percentage
Not provisioned properly. Another lab instance is required.	Rare

In the rare case where EMS connectivity is not provisioned properly, request a new lab instance from the trainer.

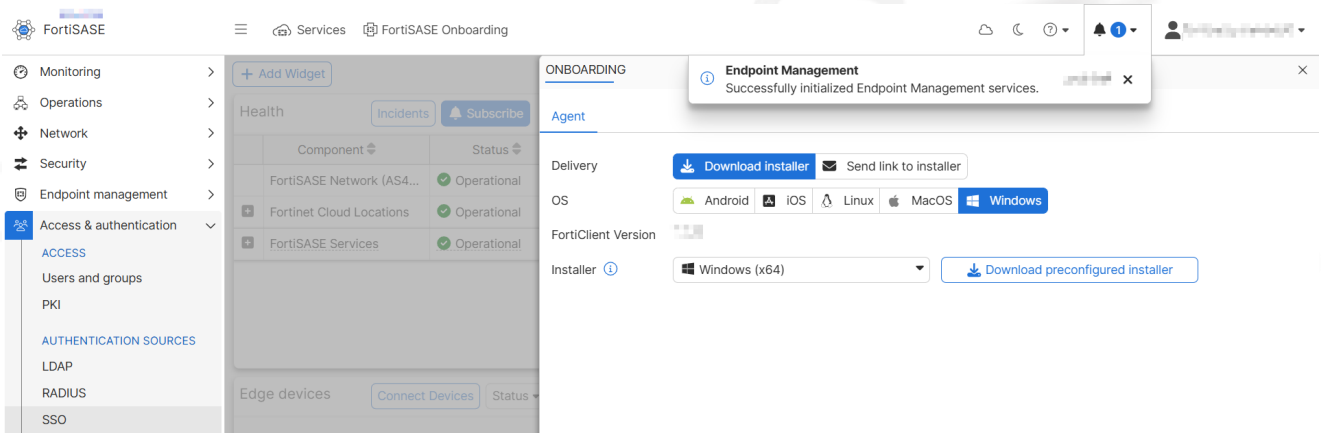
Task 1: Checking FortiSASE EMS connectivity

In the most common scenario, FortiSASE establishes EMS connectivity. Confirm by observing these:

- A notification appears under the bell icon in the header: **Endpoint Management: Successfully initialized Endpoint Management services**.
- **SSO** is visible in **Access & authentication > Authentication Sources**.

- The **Onboard Users** slide-in from the **Monitoring > Dashboards > Status > Remote Users** widget displays the installer links.

The screenshot below shows the scenario and observations made when FortiSASE establishes EMS connectivity:



If FortiSASE did not establish EMS connectivity, you observe these:

- **SSO** is missing from **Access & authentication > Authentication Sources**.
- The bell icon in the header displays the message **Endpoint Management: Failed to initialise Endpoint Management services. Please contact FortiCare support.**
- In **Monitoring > Dashboards > Status** in the **Remote Users** widget, the warning **Connection Issues – Retry Connection** displays.
- **Failed to fetch managed endpoints data** displays.
- The **Onboard Users** slide-in from the **Remote Users** widget does not display the installer links.

To resolve the issue:

1. Click **Retry Connection** next to **Connection Issues** in the **Remote Users** widget.
2. The warning changes to **Provisioning**. Wait for FortiSASE EMS to provision.
   If the provisioning succeeds, observe the following:
   - A notification appears under the bell icon in the header: **Endpoint Management: Successfully initialized Endpoint Management services**.
   - **SSO** is now visible in **Access & authentication > Authentication Sources**.
   - The **Onboard Users** slide-in from the **Remote Users** widget now displays the installer links or invitation code.
3. If the provisioning still fails, repeat step 1. Contact your trainer or workshop facilitator for assistance in accessing another lab instance if the issue is not resolved after two tries.

2.2 Configuring FortiSASE with FortiAuthenticator as SAML IdP (required)

In this section, we configure FortiSASE to act as a SAML service provider (SP) and FortiAuthenticator to act as a SAML identity provider (IdP) during the SAML authentication flow, when remote users connect to FortiSASE SIA. The configuration involves configuring specific SAML URLs from FortiAuthenticator in FortiSASE and vice-versa.

During the SAML authentication process, the SAML IdP must verify itself to the SAML SP. This verification happens using the SAML IdP certificate. FortiAuthenticator is preloaded with a server certificate (FortiDemo2024) that a well-known third-party certificate authority (CA) signed.

Task 1: Exporting IdP server certificate from FortiAuthenticator

This task exports the IdP server certificate from FortiAuthenticator.

To export the IdP certificate from FortiAuthenticator:

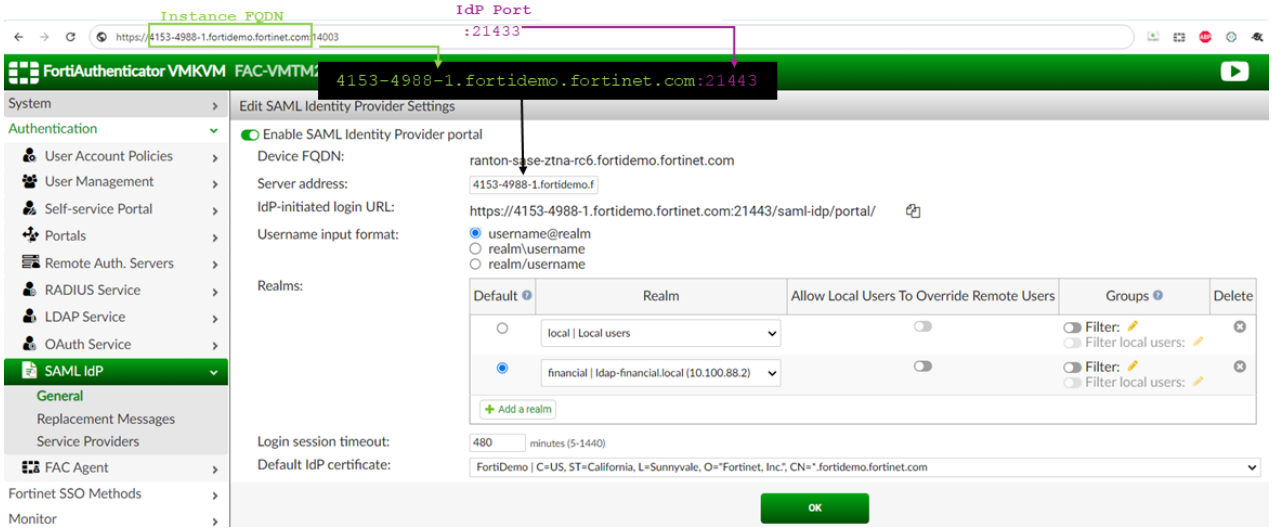
1. Log into FortiAuthenticator with the credentials provided for this lab.
2. Go to **Certificate Management > End Entities > Local Services**.
3. Select the active FortiDemo certificate, **FortiDemo**, by clicking the left checkbox for the certificate entry in the table and clicking **Export Certificate**.
4. Go to the file location on your local computer and click **Save**.

Task 2: Configuring FortiAuthenticator as SAML IdP - I

This task configures FortiAuthenticator to act as an IdP for SSO authentication.

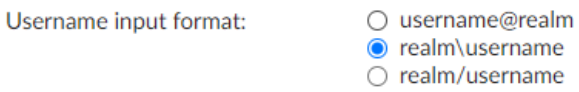
To configure FortiAuthenticator as SAML IdP:

1. In FortiAuthenticator, go to **Authentication > SAML IdP > General**.
2. Locate the instance FQDN and add port 21443 to the end. Enter this address in the **Server Address** field.



Note down the instance FQDN, as you use it in later steps.

3. For **Username input format**, select **realm\username**:



When using Chrome, ensure that an extra http:// or https:// is not added in these cases:

- Copying the instance address from the address bar and pasting it to FortiAuthenticator in **Authentication > SAML IdP > General > Server address**
- Copying the IdP values from FortiAuthenticator and pasting them to IdP fields in FortiSASE in **Access & authentication > Authentication Sources > SSO**

4. Confirm the default IdP certificate is preconfigured as **FortiDemo**. Click **OK**. You see **Successfully saved SAML Identity Provider Settings** at the top of the window.
5. Go to **Authentication > SAML IdP > Service Providers**.
6. Click **sase** to edit the preconfigured SP settings for FortiSASE.

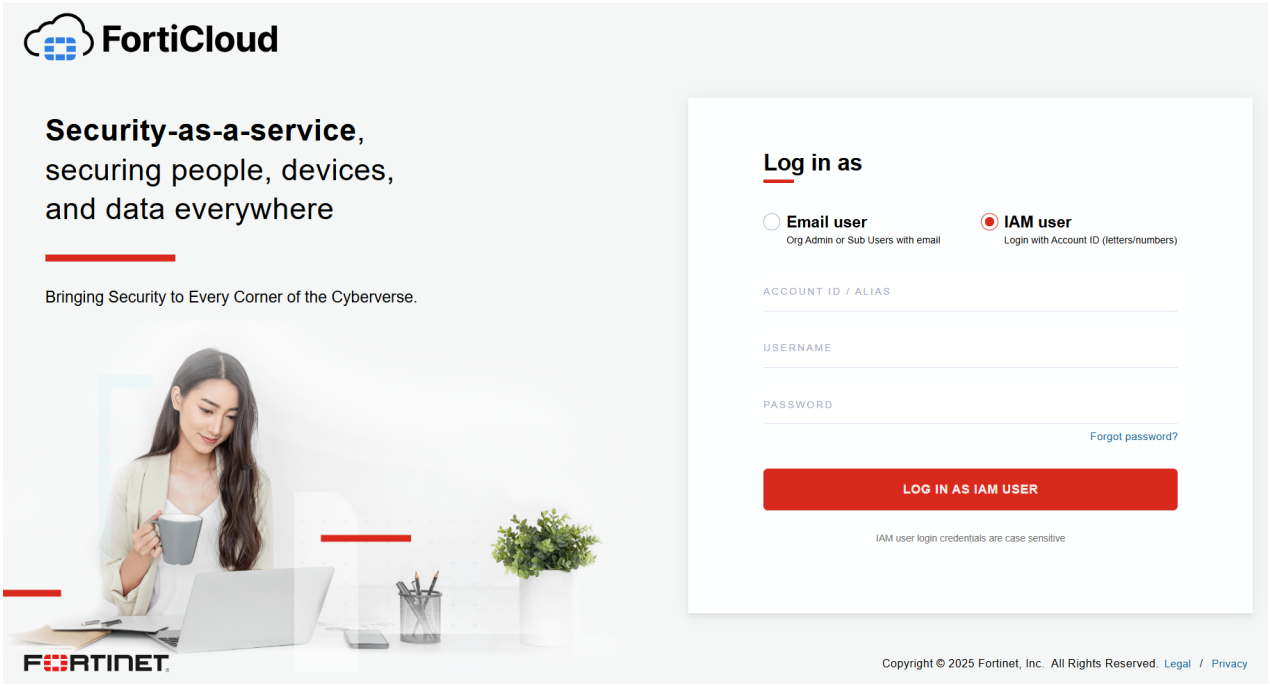
7. In **Edit SAML Service Provider**, observe the following fields:
   - **IdP entity id**
   - **IdP single sign-on URL**
   - **IdP single logout URL**
8. Keep this page open in your web browser since you will copy values from **Edit SAML Service Provider** to FortiSASE.

Task 3: Importing IdP server certificate into FortiSASE

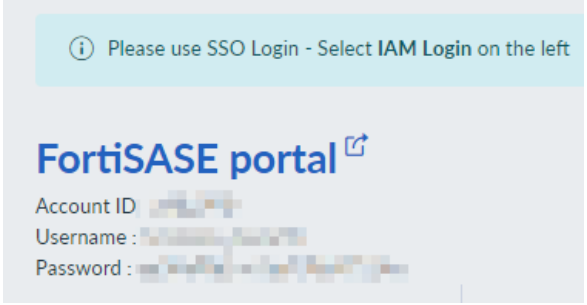
This task imports the saved IdP server certificate into FortiSASE.

To import the IdP certificate into FortiSASE:

1. Open Google Chrome and log into FortiSASE at https://portal.demo.fortisase.com. Ensure you click **Log in with FortiCloud SSO**, select **IAM user**, and enter the IAM credentials (account ID, username, password) provided for this lab.



In the FortiDemo details, you can find the FortiSASE portal link along with the IAM credentials:



2. When logging into the FortiSASE portal, you will see the multifactor authentication prompt asking to **Input Security Code**. You should input the security code received in the email address used for your FNDN sign-in.
3. Go to **System > Certificates**.
4. Click **Import > Remote Certificate**.

5. For **Import Remote Certificate**, configure the following settings:

Field	Value
Type	**Remote Certificate**
Certificate File	Click **+Upload** and select the saved certificate FortiDemo.cer from the saved file location on your local computer.
Certificate Name	By default, this field contains the certificate file name without the file extension, **FortiDemo**. You can modify it as desired. This example keeps the name as-is.

6. Click **OK**.

Task 4: Configuring FortiSASE as SAML SP

This task configures FortiSASE to act as an SP for SSO authentication.

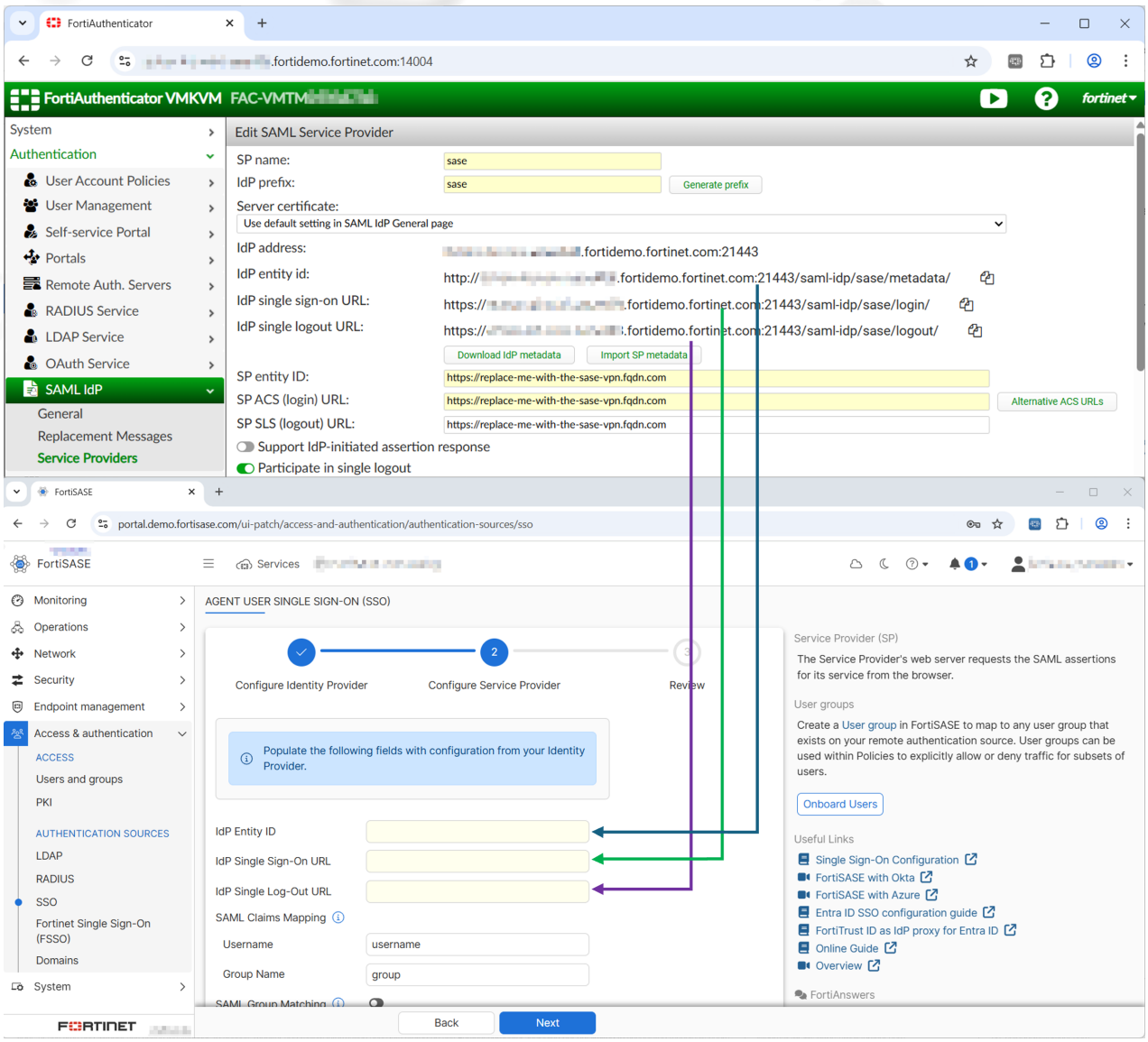
To configure FortiSASE as SAML SP:

When using Chrome, ensure that an extra http:// or https:// is not added in these cases:

- Copying the instance address from the address bar and pasting it to FortiAuthenticator in **Authentication > SAML IdP > General > Server address**
- Copying the IdP values from FortiAuthenticator and pasting them to IdP fields in FortiSASE in **Access & authentication > Authentication Sources > SSO**

1. In FortiSASE, go to **Access & authentication > Authentication Sources > SSO**. Click **Next** in the SSO wizard.
2. In **Configure Service Provider**, copy the FortiAuthenticator **SAML IdP > Service Providers** fields and paste them into matching IdP fields.

FortiAuthenticator > Edit SAML Service Provider	FortiSASE > Access & authentication > Authentication Sources > SSO
IdP entity id	**IdP Entity ID**
IdP single sign-on URL	**IdP Single Sign-On URL**
IdP single logout URL	**IdP Single Log-Out URL**

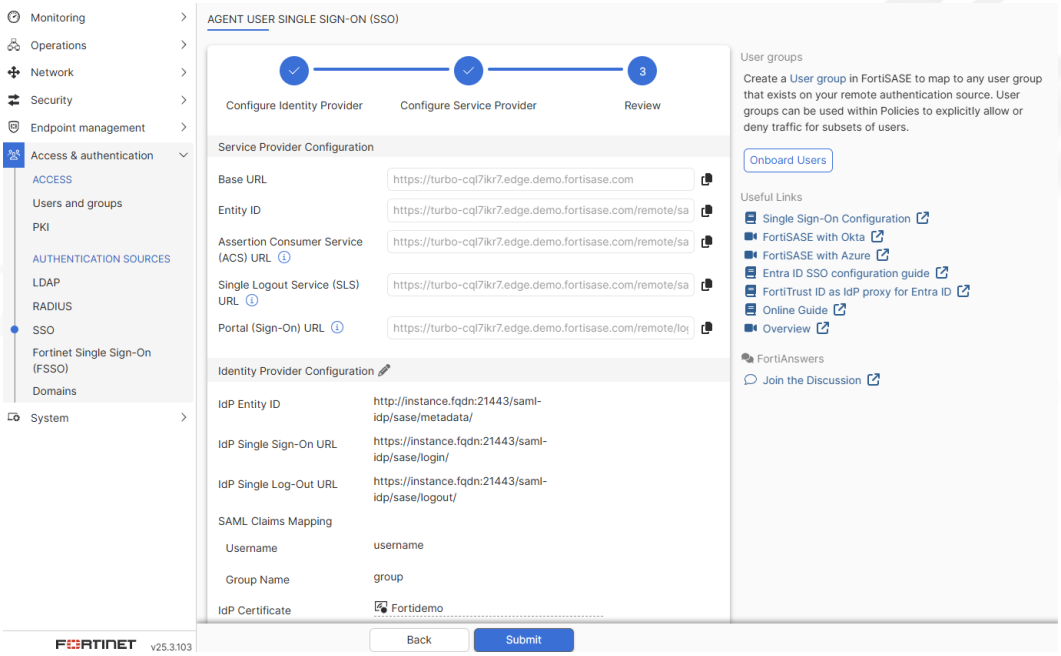


3. For **Configure Service Provider**, configure the remaining settings:

Field	Value
Username	username
Group Name	group
SAML Group Matching	Disabled
IdP Certificate	**Fortidemo**
Service Provider Certificate	**FortiSASE Default Certificate**
Digest Method	**SHA-1**

This lab uses SHA-1 for simplicity. For actual deployments, SHA-256 is recommended.

4. Click **Next**. For **Review**, click **Submit**.



A dialog informs you that SSO authentication takes priority over existing LDAP and RADIUS authentication methods. For this lab, only SSO authentication is configured so we can just acknowledge this notification. Click **OK**.

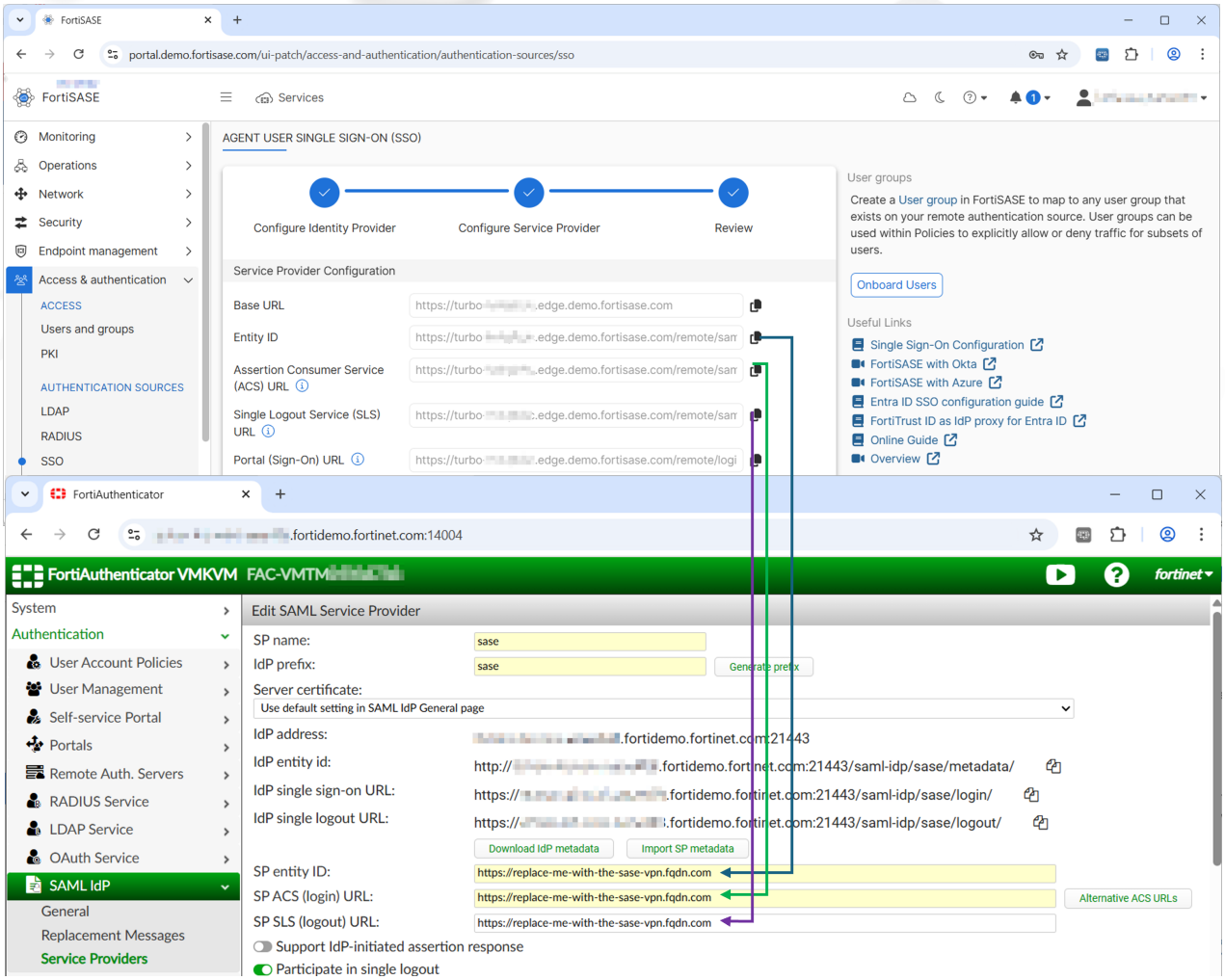
5. In **Service Provider Configuration**, observe the following fields:
   - **Entity ID**
   - **Assertion Consumer Service (ACS) URL**
   - **Single Logout Service (SLS) URL**
6. Keep this page open in your web browser since you will copy values from **Service Provider Configuration** to FortiAuthenticator.

Task 5: Configuring FortiAuthenticator as SAML IdP - II

To configure FortiAuthenticator as SAML IdP:

1. Go to the open web browser and continue configuring **Edit SAML Service Provider** in FortiAuthenticator.
2. Copy the SP fields from FortiSASE, which you will paste in the SAML SP fields. You can replace the placeholder values predefined in the FortiAuthenticator fields:

FortiSASE > Access & authentication > Authentication Sources > SSO	FortiAuthenticator > Edit SAML Service Provider
Entity ID	SP entity ID
ACS URL	SP ACS (login) URL
SLS URL	SP SLS (logout) URL



3. Click **OK**.

2.3 Creating SSO user group and VPN policy for SIA (required)

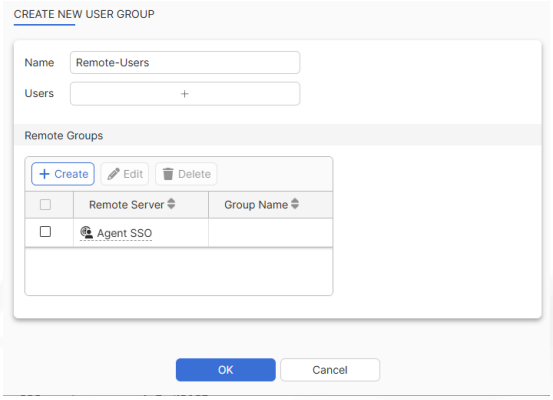
In this section, we create a user group called Remote-Users that references the SAML SSO server to authenticate remote users (both AD and non-AD endpoint) using SAML. We add the Remote-Users user group to the default Allow-All VPN policy that enables users to authenticate using SAML while connecting to FortiSASE SIA and access the internet via FortiSASE SIA.

Task 1: Creating user group for SAML SSO

To create a user group for SAML SSO:

1. On FortiSASE, go to **Access & authentication > Access > Users & Groups**.
2. Click **Create**.
3. Select **User Group** and click **Next**.
4. In the **Create New User Group** page, configure the following:
   a. In the **Name** field, enter **Remote-Users**.
   b. Under **Remote Groups**, click **Create**.
   c. In **Add Group Match**, for **Remote Server**, select **Agent SSO** under **SAML Server**.

d. Click **OK**.

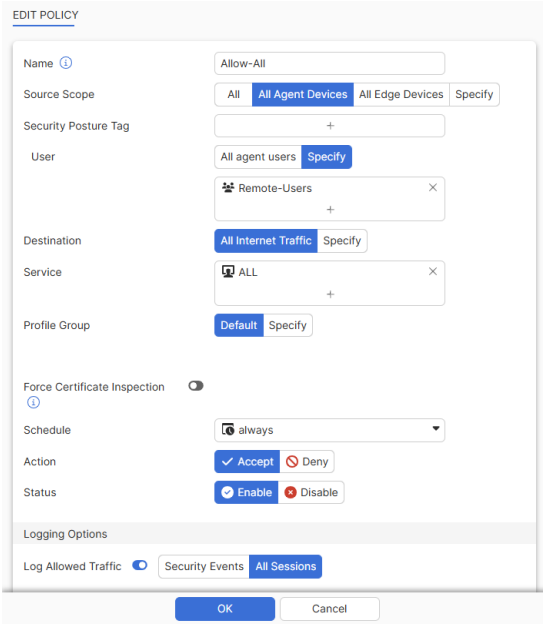


5. Click **OK**.
6. In **Onboarding**, click **Close**. In this lab, FortiClient is already installed on the endpoint machine so we ignore this step. Also, we copy the invitation code in a later task.

Task 2: Adding user group to Allow-All VPN policy

To add user group to Allow-All VPN policy:

1. Go to **Security > Traffic > Policies**.
2. Click the **Allow-All** policy, and select **Edit**.
3. For **Source Scope**, select **All Agent Devices**.
4. In the **User** field, click **Specify** and then select **Remote-Users**.



5. Click **OK**.

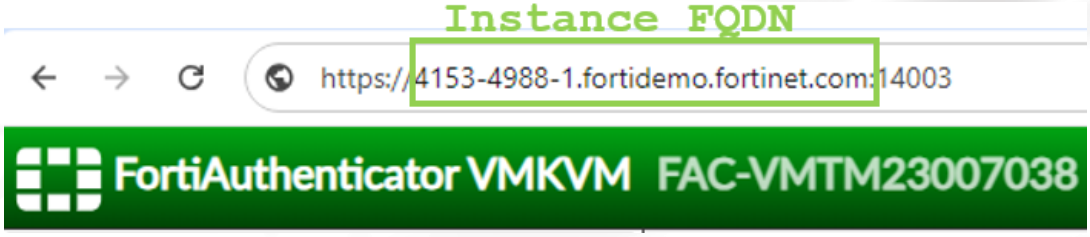
2.4 Configuring domains (required)

In this configuration, we configure a domain connector on FortiSASE that enables communication between FortiSASE and financial.local, the on-premise AD server hosted behind FortiGate_HQ. This configuration uses the domain connector to segregate endpoints based on whether the endpoint belongs to the financial.local domain or not (i.e. non-AD user) using custom endpoint profiles, as the later sections discuss.

Task 1: Configuring a domain connector

To configure a domain connector:

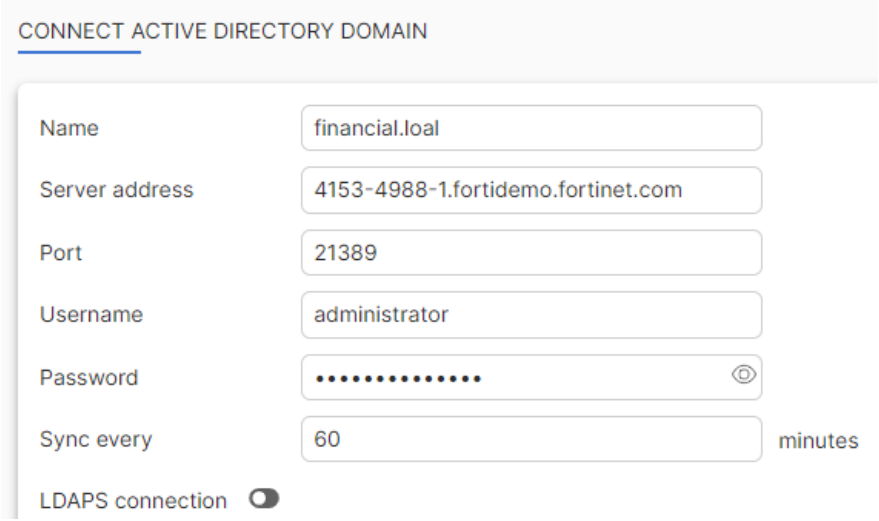
1. Retrieve the instance FQDN using your FortiAuthenticator login URL:



2. On FortiSASE, go to **Access & authentication > Authentication Sources > Domains**, and click **Create > Active Directory (AD) connection**. Enter details shown below:

Field	Value
Name	financial.local
Server address	Instance FQDN from step 1
Port	21389
Username	administrator
Password	SecurityFabric
Sync every	60
LDAPS connection	Disabled

3. After entering the above details, the configuration appears as shown below. The **Server address** is your unique instance FQDN found using step 1.



Enabling LDAPS connection for a domain connector is considered best practice, as it enables FortiSASE to check the certificate that the LDAP server presents against the LDAP server IP address or FQDN configured in **Server address**. LDAPS also provides an encrypted communication channel.

For simplicity, in our lab demonstration, we disable LDAPS connection.

4. Click **Create**.

2.5 Configuring endpoint profiles (required)

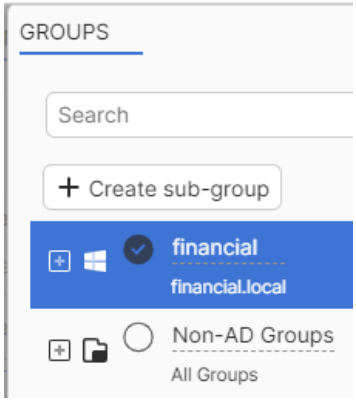
In this section, we segregate the two endpoints based on the criterion that one belongs to the domain financial.local (AD user) and the other does not (non-AD User). We achieve this by using two custom endpoint profiles on FortiSASE. Having two different endpoint profiles enables us to manage our endpoint security requirements differently for AD and non-AD users.

The first endpoint profile we configure is named Corporate and assigned to an endpoint only if it is integrated into domain financial.local (AD user). The second endpoint profile we configure is called NonCorporate and assigned to an endpoint only if it does not belong to any AD group (non-AD user).

Task 1: Configuring an endpoint profile

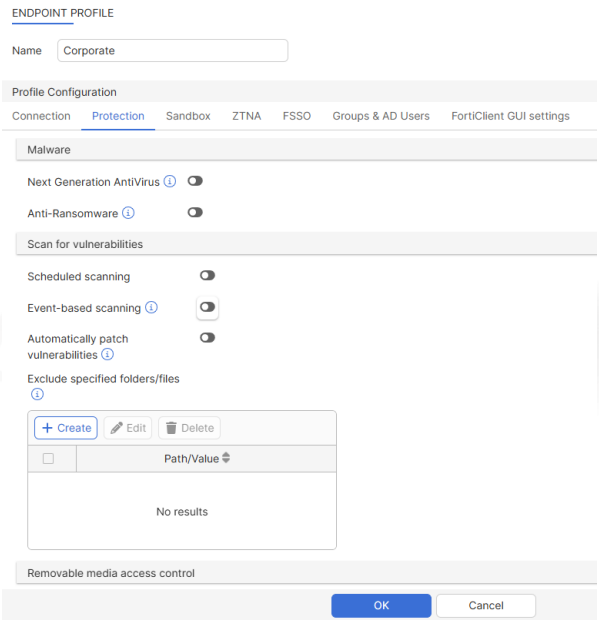
To configure an endpoint profile:

1. Configure the Corporate endpoint profile:
   a. In FortiSASE, go to **Endpoint management > Endpoint profiles**.
   b. Under the **Profiles** tab, click **Create**.
   c. In the **Name** field, enter **Corporate**.
   d. Under **Profile Configuration**, go to the **Connection** tab and set **Endpoint connects to FortiSASE Cloud Security** to **Manually**.
   e. Go to the **Groups & AD Users** tab.
   f. Click **Add > Groups**.
   g. Select the **financial** group.



   Click **OK**.
   h. Go to the **Protection** tab. Under **Malware** and **Scan for vulnerabilities**, disable the toggle for the following settings:
      - **Next-Generation AntiVirus**
      - **Anti-Ransomware**
      - **Scheduled scanning**
      - **Event-based scanning**

   These settings are later enabled in other sections when we need vulnerability scanning. For this section, keep them disabled.

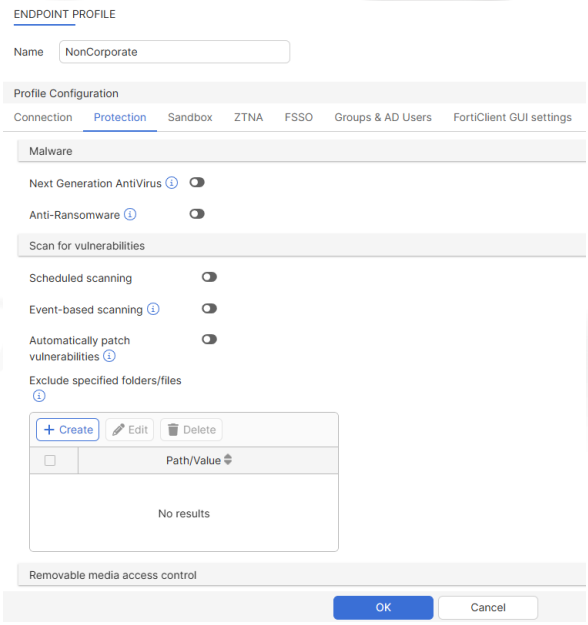


i. Click **OK** to save the endpoint profile.

You can also configure a more granular AD group rather than selecting an entire domain. However, in our lab, FortiSASE must assign a user that belongs to the AD domain financial.local to the Corporate endpoint profile. FortiSASE must assign users that do not belong to this domain or who are non-AD users to the NonCorporate endpoint profile.

2. On the same **Endpoint management > Endpoint profiles** page, click **Create**.
3. In the **Name** field, enter **NonCorporate**.
4. Under **Profile Configuration**, go to the **Connection** tab and set **Endpoint connects to FortiSASE Cloud Security** to **Manually**.
5. On the **Group & AD Users** tab, click **Add > Groups** and select **Non-AD Groups**.
6. Click **OK**.
7. Go to the **Protection** tab. Under **Malware** and **Scan for vulnerabilities**, disable the toggle for the following settings:
   - **Next-Generation AntiVirus**
   - **Anti-Ransomware**
   - **Scheduled scanning**
   - **Event-based scanning**

   These settings are later enabled in other sections when we need vulnerability scanning. For this section, keep them disabled.



8. Click **OK** to save the endpoint profile.

In the next section, when FortiClient on both Windows10-User1 and Windows10-User2 endpoints are onboarded to FortiSASE, FortiSASE evaluates the endpoint's AD membership to assign the configured endpoint profiles accordingly.

2.6 Onboarding endpoint to connect it to FortiSASE (required)

Endpoint onboarding requires deploying or installing FortiClient and registering it to FortiSASE EMS using a FortiSASE invitation code to obtain any configuration settings from this service. This service automatically updates FortiClient to include a SIA VPN connection to connect to FortiSASE SIA. The latest FortiClient version that FortiSASE supports is preinstalled on endpoints in the lab environment.

For other production environments, you can deploy the FortiClient installer to your endpoints using the methods below:

Installer deployment method	Description
Preconfigured installer	FortiSASE EMS automatically generates a preconfigured installer that is downloadable directly from the FortiSASE portal. This installer includes the invitation code. You can deploy the installer to all endpoints using Microsoft System Center Configuration Manager, group policy objects, or mobile device management.
Manual installer	User downloads installer using FortiClient general availability installer links. The installer does not include the invitation code

Task 1: Obtaining the FortiSASE invitation code for endpoint onboarding

To obtain the FortiSASE invitation code:

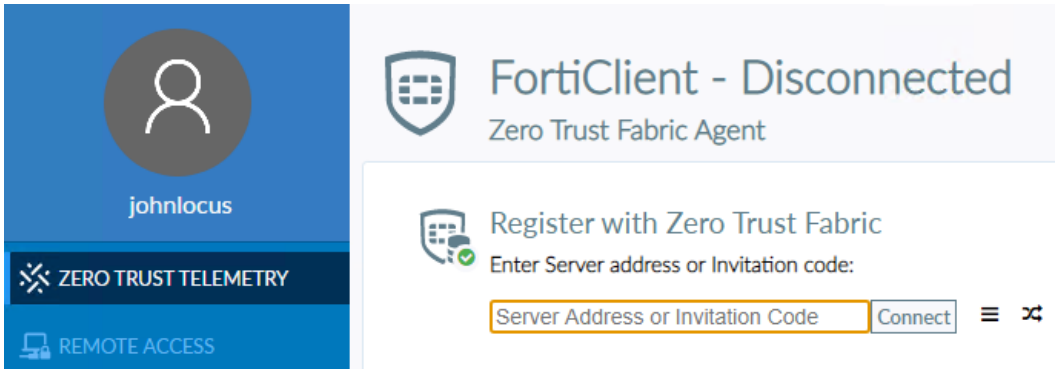
1. Go to **Monitoring > Dashboards > Status**.
2. Under the **Remote users** widget, click **Onboard Users**. If this widget does not exist, click **Add Widget** and add a new **Remote users** widget.

3. In **Onboarding**, under **OS** select **Android**, click the copy icon to the right of the **Default invitation code** text field to copy the invitation code to the clipboard.
4. Paste the invitation code to a text file for use in a later task.
5. Click **Close**.

Task 2: Using the FortiSASE invitation code in FortiClient on an endpoint

To use the FortiSASE invitation code in FortiClient on an endpoint:

1. Log into the Windows10-User1 endpoint with the credentials provided for this lab by doing one of the following:
   - In the FortiDemo details, find the FQDN and RDP port to access the endpoint via the Remote Desktop Connection application in Windows . RDP is the preferred method because it supports copying and pasting the invitation code.
   - Click **DISPLAY** to access the endpoint using VNC. This method does not support copying and pasting the invitation code.
2. On the desktop, double-click the **FortiClient** shortcut.
3. In FortiClient, go to **Zero Trust Telemetry**.



4. Under **Register with Zero Trust Fabric**, in the **Enter Server address or Invitation code** field, paste the FortiSASE invitation code obtained from the previous task and click **Connect**.
5. In **Zero Trust Telemetry**, the section displays **Managed by FortiClient Cloud** with a **Status** of **Connected**. Observe the following notification from the FortiClient system tray: **Configuration update was received from Endpoint Management Server (EMS).** This happens when there are configuration changes that FortiSASE EMS pushes to the FortiClient endpoints.

FortiSASE is by default configured to have a FortiClient Telemetry sync timer of 60 seconds, which means any endpoint specific changes that you make on FortiSASE take a minimum of 60 seconds to propagate and reflect on FortiClient.

Thus, you are advised to wait at least 60 seconds for the endpoint profile changes performed on FortiSASE to propagate to FortiClient endpoints.

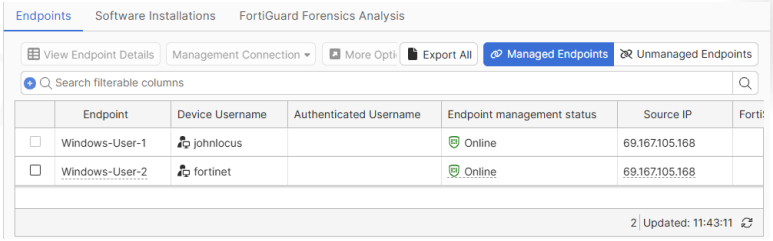
6. Repeat the above steps after logging into Windows10-User2 to connect it to FortiSASE.

Task 3: Verifying the endpoint profile assigned to endpoints

In this task, we verify whether endpoint is assigned the desired custom endpoint profile as per our configuration. In our lab, as Windows10-User1 belongs to the financial.local AD domain, FortiSASE must assign it the Corporate endpoint profile. The Windows10-User2 is not a part of any AD group, so FortiSASE must assign it the NonCorporate endpoint profile.

To verify the endpoint profile assignment:

1. On FortiSASE, go to **Operations > Connectivity > Endpoints**.
2. Under the **Endpoints** tab, verify that both endpoints are connected to FortiSASE and the **Endpoint management status** column shows them as **Online**.
3. Scroll to the right to see the **Profile** column. Confirm that Windows-User-1 is assigned the Corporate endpoint profile and Windows-User-2 is assigned the NonCorporate endpoint profile:



2.7 Configuring and verifying tunnel autoconnect and bypass FortiSASE (required)

In this section, we tweak a few settings in the Corporate and NonCorporate custom endpoint profiles to enable FortiSASE features such as tunnel autoconnect and bypass FortiSASE to demonstrate granular control of these features per endpoint profile.

The following summarizes use cases for the custom endpoint profiles:

Custom endpoint profile	User	Typical use case
Corporate	Windows10-User1 is already integrated into AD, thus, considered trustworthy.	Typical use case for AD endpoint requires them to: • Auto-connect to FortiSASE SIA when working remotely (i.e. they are off-premise or off-net) to secure and scan their browsing traffic. • If they work from office (i.e. on-premise or on-net) FortiClient must bypass the endpoint from using tunnel autoconnect to connect to FortiSASE SIA as they are already been behind and protected by corporate firewall (i.e. FortiGate_HQ). • AD endpoints must have an option and ability to disconnect from FortiSASE SIA.
NonCorporate	Windows10-User2 being a non-AD user cannot be trusted with their browsing activity.	• Enforce any non-AD endpoint to auto-connect to FortiSASE SIA and access all internet resources via FortiSASE SIA. • In addition, once the non-AD users connect to FortiSASE SIA, they also must not have the ability to disconnect from FortiSASE SIA.

The table below lists the summary of each Tasks needed to achieve and test the use cases stated above.

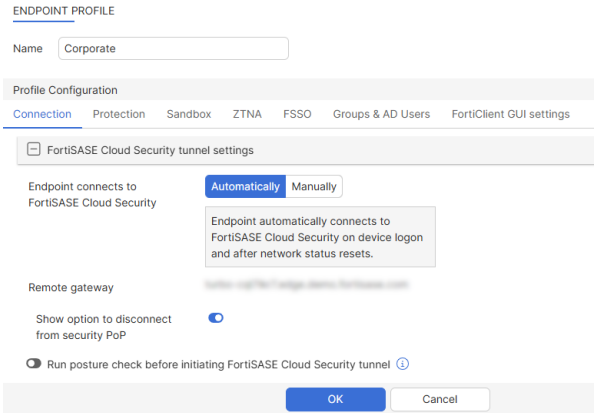
	Task on Windows10-User1	Task on Windows10-User2
Task 1	• Configure and test tunnel auto-connect	• Configure and test tunnel auto-connect

	Task on Windows10-User1	Task on Windows10-User2
	• Configure the option to let users disconnect from FortiSASE SIA using the disconnect button	• Configure the option to never let user disconnect from FortiSASE SIA
Task 2	Configure Bypass FortiSASE and test tunnel auto-connect.	N/A

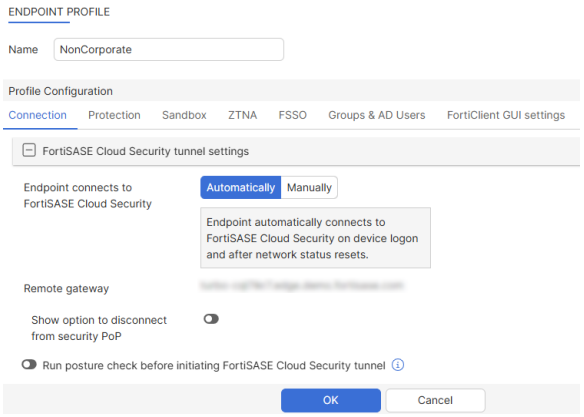
Task 1: Configuring and verifying tunnel autoconnect

To configure and verify tunnel autoconnect:

1. On FortiSASE, go to **Endpoint management > Endpoint profiles**.
2. Select **Corporate** profile and click **Edit**.
3. Under **Connection** tab, set the **Endpoint connects to FortiSASE Cloud Security** option to **Automatically**. Click **OK** on prompt that warns the configuration change will delete all alternative tunnels configured. Enable the **Show option to disconnect from security PoP** toggle that provides the **Disconnect** button on FortiClient.



   Click **OK** to save the profile.
4. Select the **NonCorporate** endpoint profile and click **Edit**.
5. Under **Connection** tab, set **Endpoint connects to FortiSASE Cloud Security** to **Automatically**. Click **OK** on prompt that warns the configuration change will delete all alternative tunnels configured. Disable the toggle for **Show option to disconnect from security PoP**. Disabling the toggle, will remove the **Disconnect** button on FortiClient. Thus, endpoints can no longer disconnect from FortiSASE SIA.



6. Click **OK** to save the profile.
7. Sign out and sign in from and to the Windows10-User1 and Windows10-User2 machines, respectively. Notice the FortiAuthenticator login page pops up due to the tunnel autoconnect feature that informs the endpoint to

continuously attempt to connect to FortiSASE SIA. You must provide the credentials manually for the initial attempt, after which FortiClient creates a cookie using the credentials and uses the cookie to autoconnect to FortiSASE SIA automatically on subsequent connections.

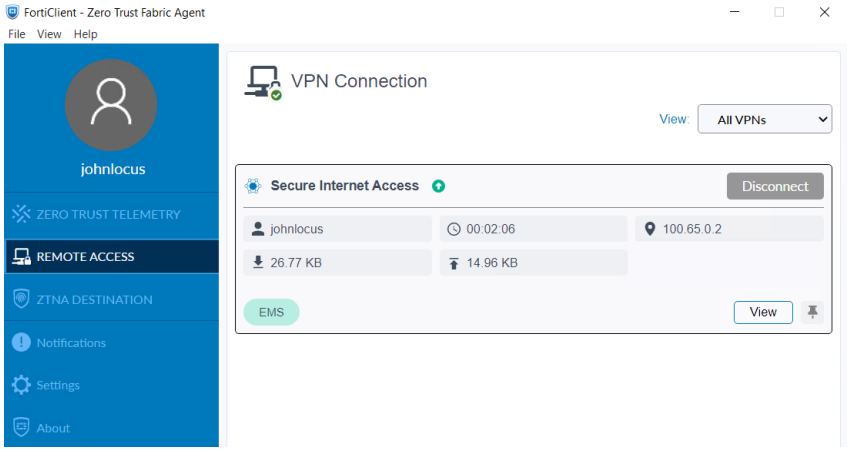
Use the credentials given to connect to SIA and confirm whether Windows10-User1 and Windows10-User2 are connected to SIA using the **Remote Access** tab on FortiClient.

User type	Computer name	FortiSASE SIA username	Password
AD User	Windows10-User1	financial\johnlocus	SecurityFabric
Non-AD User	Windows10-User2	local\fortinet	

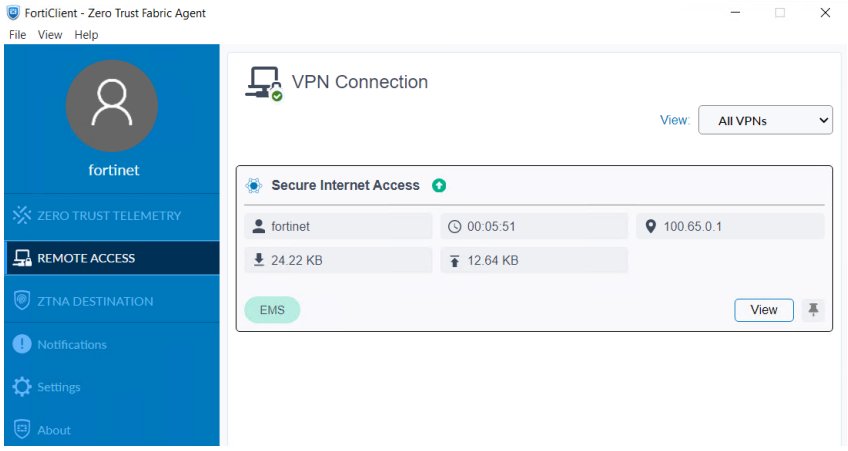
To troubleshoot SAML login errors and issues, see Appendix C - FAQs on page 48.

In the lab environment, it may happen that when FortiClient connects to FortiSASE SIA it may disconnect the RDP session abruptly and internet traffic gets re-routed through FortiSASE SIA. To fix the issue re-login into the Windows endpoint again.

8. Confirm from FortiClient's REMOTE ACCESS tab that Window10-User1 also has a **Disconnect** button to disconnect from VPN.



Whereas the Window10-User2 does not have that **Disconnect** button to disconnect from VPN as per our use case:

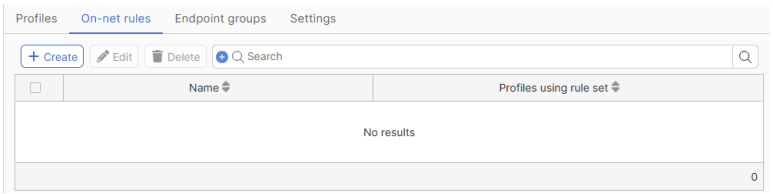


9. Verify the configuration:
   a. To confirm whether both endpoints are connected to FortiSASE SIA, on FortiSASE go to **Operations > Connectivity > Endpoints** and notice the user listed in the **FortiSASE agent session** column.
   b. To verify that tunnel auto-connects works reboot both Windows10-User1 and Windows10-User2 and login to both endpoints again and wait for tunnel auto-connect to connect to FortiSASE SIA without any manual intervention.
   c. Open FortiClient's REMOTE ACCESS tab to confirm it is connected to FortiSASE SIA by virtue of tunnel autoconnect.

Task 2: Configuring and verifying Bypass FortiSASE

To configure and verify Bypass FortiSASE:

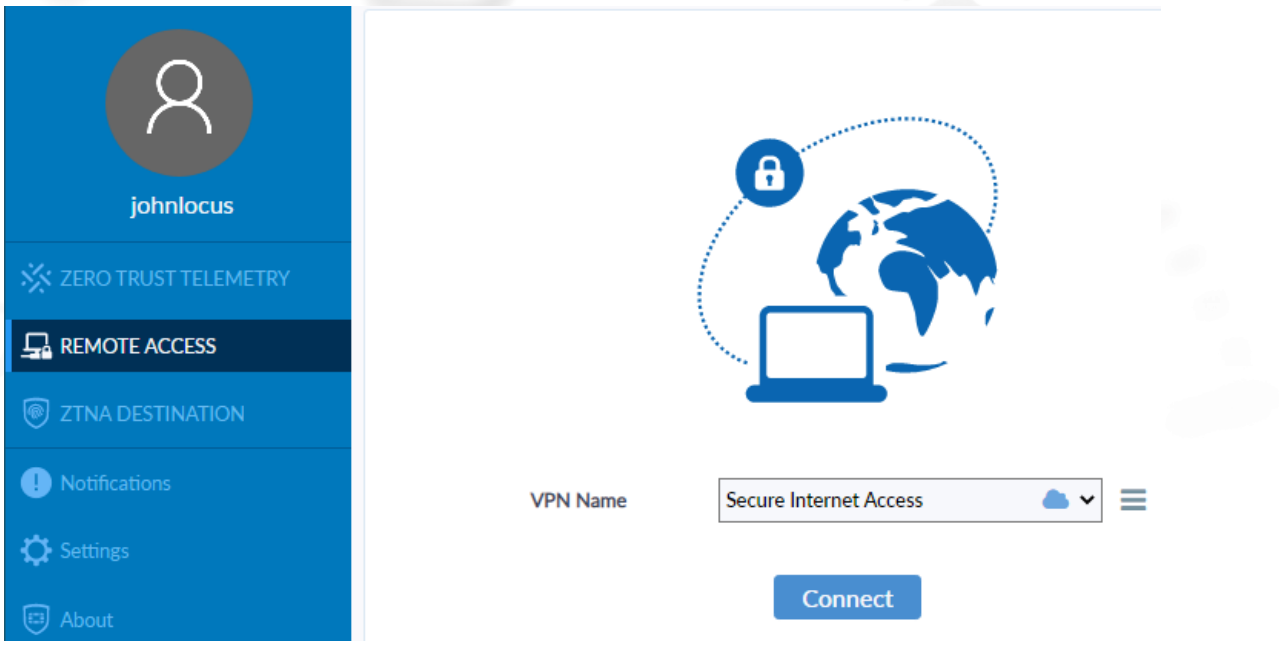
1. On FortiSASE, go to **Endpoint management > Endpoint profiles**. Switch to the **On-net rules** tab.



2. Click **Create**, in the slide in window enter the **Name** as **On-Premise**.
3. Enable the detection type **Can ping a known server**. In the **Known server IP addresses** field, enter 192.168.111.1, which is the FortiGate_HQ LAN IP address.

FortiSASE supports on-net rule sets of various detection types. To know more about how different detection mechanism work, see Connection.

4. Click **OK**.
5. Go to **Endpoint management > Endpoint profiles**. Select **Corporate** and click **Edit**.
6. In the **Profile Configuration** section, under **Connection** tab, set **On/off-net detection** to **Enable**. In the **On-net rule set** dropdown list, select **On-Premise**. Enable the toggle for **Exempt endpoint from FortiSASE auto-connect when endpoint is on-net**.
7. Click **OK**.
8. To verify bypassing FortiSASE works as expected, reboot the Window10-User1 and open FortiClient's **REMOTE ACCESS** tab to confirm that it no longer using tunnel auto connect to connect to FortiSASE SIA and relies on manually connecting to FortiSASE SIA using **Connect** button.



This is because Window10-User1 satisfies the **On-Premise** On-net rule set configured, as it is able to ping 192.168.111.1, which is the LAN IP of FortiGate_HQ as per our requirement.

2.8 Configuring and verifying split tunneling (required)

In this section, we configure and test Subnet-based and FQDN-based split tunneling on both endpoint profiles. For Subnet based split tunneling, we use an IP of 10.100.66.99/32 and for FQDN based split tunneling, we use ipchicken.com as the split tunneling destination address field. Thus, any traffic originating from endpoints destined to 10.100.66.99/32 and/or ipchicken.com goes directly to the internet rather than traversing through FortiSASE SIA.

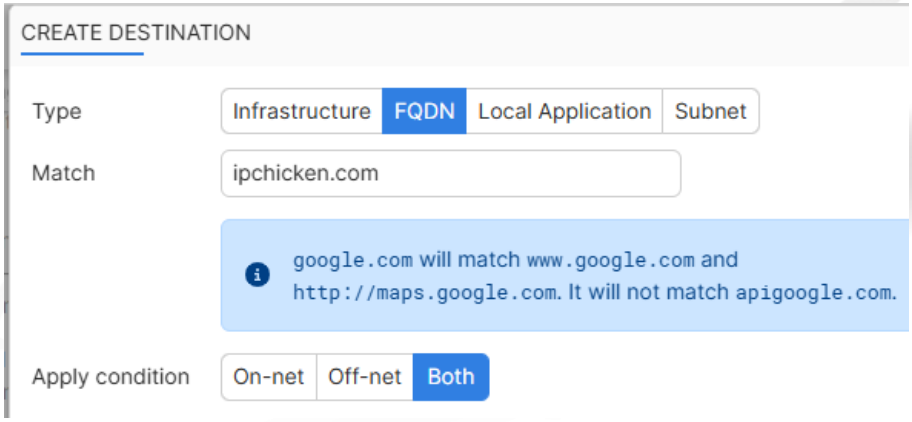
The IP 10.100.66.99 used for configuring Subnet based split tunneling is actually the IP assigned to internet interface (port1) of FortiGate_HQ. This internet port acts as the ZTNA Application Gateway on port 9443. We use subnet based split tunneling to bypass FortiSASE SIA and directly reach the ZTNA Application Gateway when endpoints access Marketing and Finance servers in later sections.

Task 1: Configuring FQDN-based and Subnet based split tunnel

To configure FQDN-based split tunnel:

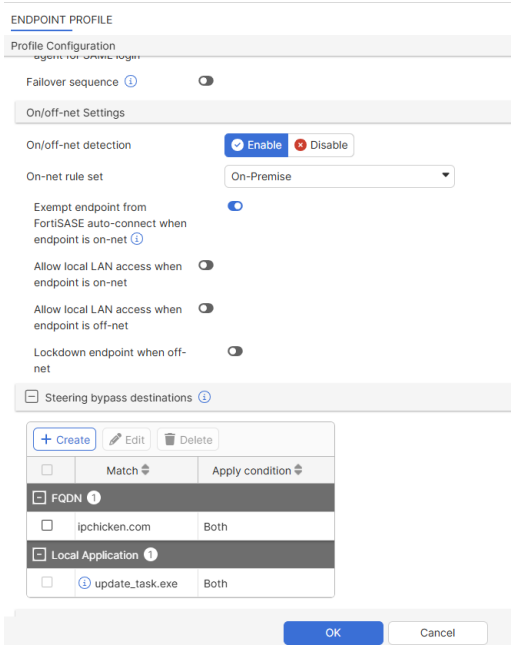
1. Add the ipchicken.com FQDN to the Corporate endpoint profile:
   a. Go to **Endpoint management > Endpoint profiles**, select **Corporate**, and click **Edit**.
   b. In **Profile Configuration** section, under **Connection** tab, expand the option **Steering bypass destinations**. Click **Create**.
   c. In the slide-in, for **Type**, select **FQDN**.
   d. For **Match**, enter **ipchicken.com**.

e. For **Apply condition**, select **Both**.



f. Click **OK**.

g. Click **OK** to save the changes to the endpoint profile.



2. To configure subnet-based split tunneling on the Corporate and NonCorporate profiles:

a. Under **Steering bypass destinations**, click **Create**.

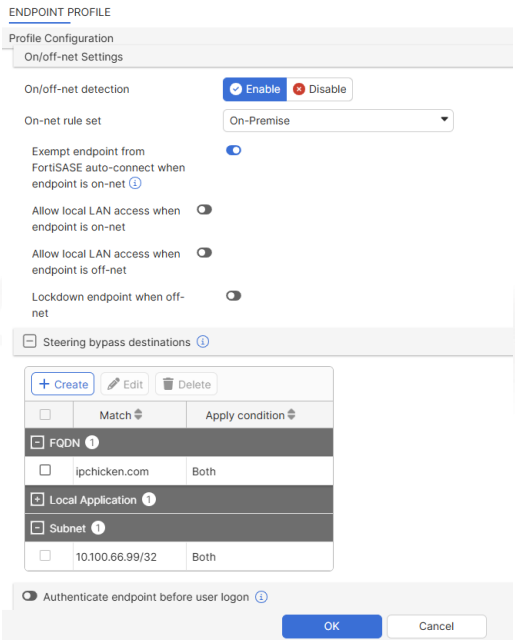
b. In the slide-in, for **Type**, select **Subnet**.

c. For **Match**, enter **10.100.66.99/32**.

d. For **Apply condition**, select **Both**.

e. Click **OK**.

f. Click **OK** to save the changes to the endpoint profile.



g. Repeat the above steps to add the ipchicken.com FQDN to the **NonCorporate** endpoint profile.

Task 2: Verifying subnet- and FQDN-based split tunnel

To verify subnet and FQDN-based split tunnel:

1. Log in to Windows10-User1 or Windows10-User2.

For subnet- and FQDN-based split tunnel configuration to take effect on endpoints, the endpoint must disconnect and reconnect to FortiSASE SIA.

You can disconnect the endpoint from FortiSASE SIA by using the **Disconnect** button on FortiClient for Windows10-User1 or via rebooting the endpoint for Windows10-User2.

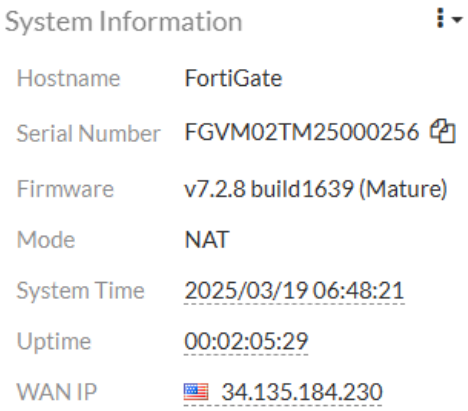
2. Do one of the following:
   - If you are using Windows10-User2 and it is already connected to FortiSASE SIA, reboot the endpoint so that it reconnects to FortiSASE SIA using tunnel autoconnect.
   - If you are using Windows10-User1, go to the **Remote Access** tab and click **Connect** to connect to FortiSASE SIA. As tunnel autoconnect was disabled in the previous steps for this endpoint by using the bypass FortiSASE feature, we must manually connect to FortiSASE SIA to test split tunneling.
3. On the **Remote Access** tab, confirm that FortiClient is connected to FortiSASE SIA.
4. To verify subnet-based split tunneling, open command prompt (CMD) from the toolbar and enter the following command: `route print 10.100.66.99`. From the output, see the `Active Routes` section from where we can confirm the route 10.100.66.99 being injected into the endpoint's routing table.
   The following shows the expected output of `route print 10.100.66.99` for Windows10-User1:

```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
     10.100.66.99  255.255.255.255    192.168.111.1  192.168.111.101     25
===========================================================================
```

   The following shows the expected output of `route print 10.100.66.99` for Windows10-User2:

```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
     10.100.66.99  255.255.255.255      10.100.66.1    10.100.66.102     25
===========================================================================
```

5. Open an incognito window in the Chrome browser. Go to ipinfo.io by entering the URL in the navigation bar or use the ipinfo.io bookmark. You can use this website to verify the public IP address. This IP address is the public IP address of the FortiSASE PoP as the traffic flows through the FortiSASE PoP.
6. For comparison, open another incognito Chrome window. Go to ipchicken.com by entering the URL in the navigation bar or use the ipchicken.com bookmark. Notice the public IP address shown differs since this traffic going directly to the internet via split tunneling.
7. (Optional) To verify that this IP address is the same as your lab instance public IP address, do the following:
   a. Log into FortiGate_HQ using the credentials provided.
   b. Go to the **Dashboard > System Information** widget and verify the WAN IP address mentioned.



The public IP addresses differ. Thus, traffic to ipchicken.com flows directly through the lab instance and not through FortiSASE SIA.

Task 3: Exploring split tunneling further (optional)

Our examples above demonstrate the necessary split tunneling configuration to reach the ZTNA application gateway (10.100.66.99) and the ipchicken.com FQDN directly. You can explore split tunneling further using other cases where performing split tunneling is useful, such as the following:

- For trusted clients such as AD users, it may be okay to bypass FortiSASE scanning for certain trusted websites like a banking website. Edit the Corporate endpoint profile to configure FQDN-based split tunneling so that traffic to the website hsbc.com does not go through FortiSASE.
- For untrusted clients such as non-AD users in our scenario, they may still require direct access to some shared resources such as printers without going through the tunnel or through ZTNA. Edit the Default endpoint profile to configure Subnet based split tunneling that allows a non-AD user access to the subnet x.x.x.x (make up a new subnet for printers). Verify the same using CMD using the command route print x.x.x.x

2.9 Configuring security posture tagging rules and ZTNA connection rules (required)

Security posture tags are labels assigned to the endpoints based on the criteria defined by the tagging rules.

In this section, we configure security posture tagging rules and tags. The security posture tags, Vulnerable and WindowsDefenderEnabled, are assigned to endpoints if they satisfy the configured tagging rules.

Lastly, we configure ZTNA connection rules that install the ZTNA destinations for SSH access to the Marketing and Finance servers.

We define the following ZTNA connection rules to grant SSH access to endpoints for their respective servers.

Endpoint	Server for SSH access	FQDN	Port
Windows10-User1	Financial server	finance.financial.local	22
Windows10-User2	Marketing server	marketing.financial.local	

Later steps use ZTNA tags configured on FortiSASE on FortiGate_HQ inside firewall policies to allow or deny access to the resources that the ZTNA application gateway protects.

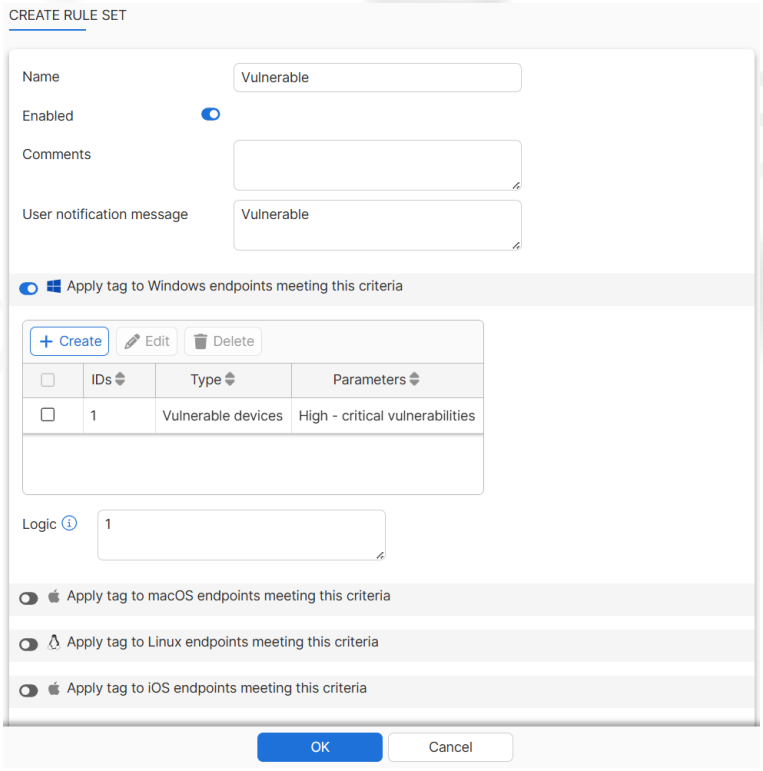
Task 1: Configuring security posture tagging rules

To configure security posture tagging rules:

1. On FortiSASE, go to **Endpoint management > Security posture tags**.
2. On the **Tagging rules** tab, click **Create**.
3. Enter the **Name** as **Vulnerable**.
4. In **User notification message**, enter a message.
5. Enable **Apply tag to Windows endpoints meeting this criteria**.
6. Click **Create** and configure the criteria for the security posture rule and configure the following:

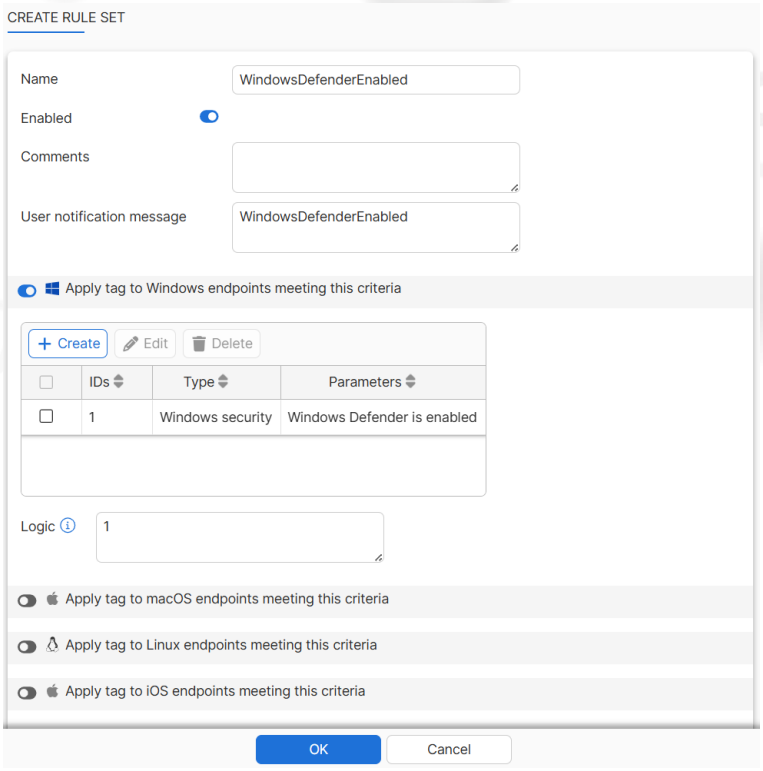
Field	Value
Operating system	**Windows**
Rule type	**Vulnerable devices**
Vulnerable devices	**With, High - critical vulnerabilities**

7. Click **OK**.



8. Click **OK**. A security posture tag with the same name will be created and applied to any endpoints matching the rule criteria.
9. Repeat the same steps to configure a security posture rule with the following configuration:

Field	Value
Name	WindowsDefenderEnabled
Operating system	**Windows**
Rule type	**Windows security**
Windows security	Keep **Negate** as-is (disabled). **Windows Defender is enabled**



Task 2: Configure private applications for Agent-based ZTNA

To configure private application for Agent-based ZTNA

1. On FortiSASE, go to **Security > Traffic > ZTNA**.
2. Under **Agent-based > Private applications**, click **Create**.
3. Configure the following settings for the ZTNA application named finance, that is used for endpoints belonging to Corporate endpoint profile in later steps.

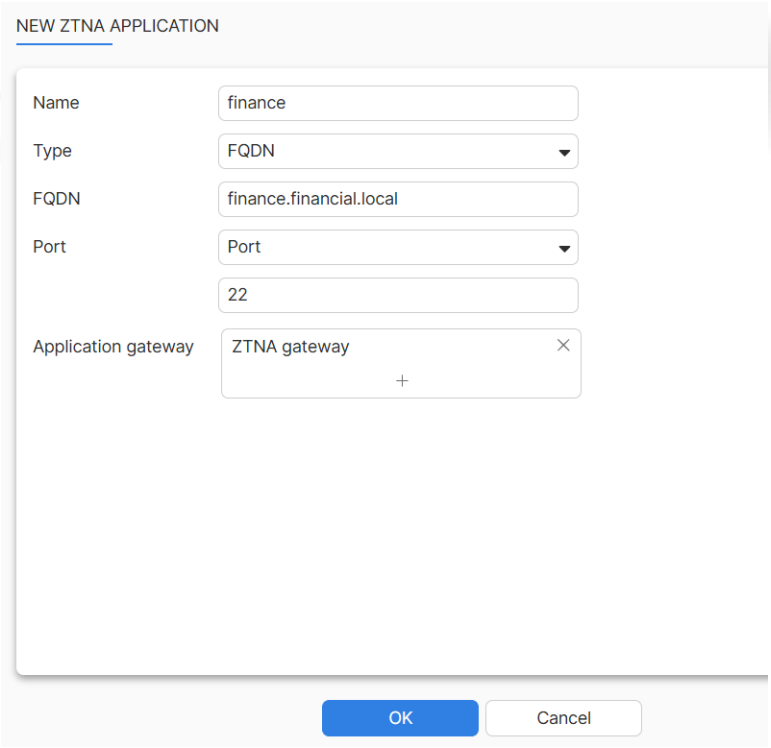
Field	Value
Name	finance
Type	FQDN
FQDN	finance.financial.local
Port	Port, then enter 22.

4. Under **Application gateway**, click **+** and click **+** again to configure the following for the ZTNA application gateway:

Field	Value
Name	ZTNA gateway
Address	access.fortidemo.fortinet.com The ZTNA application gateway address access.fortidemo.fortinet.com resolves to 10.100.66.99/32, which is the internet interface of FortiGate_HQ. Any traffic to this IP address is bypassed from flowing through FortiSASE SIA as per our subnet-based split tunnel configuration.

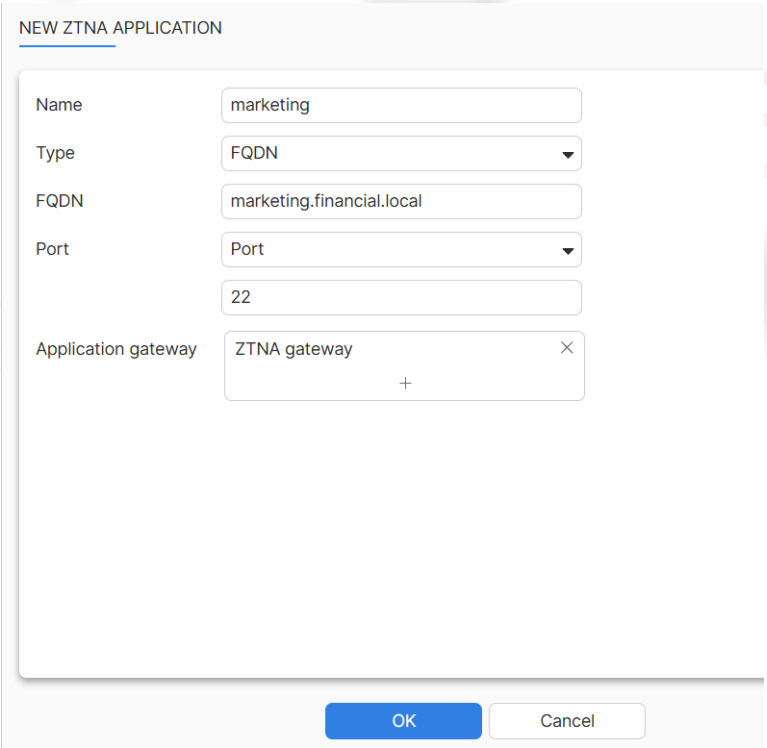
Field	Value
Port	9443

5. Click **OK**.
6. In the **Confirm** prompt, select **OK** to use the new entry.



7. Click **OK**.
8. Click **Create** again to configure the ZTNA application named marketing, that is used for endpoints belonging to NonCorporate endpoint profile in later steps.

Field	Value
Name	marketing
Type	FQDN
FQDN	marketing.financial.local
Port	Port, then enter 22.
Application gateway	ZTNA gateway

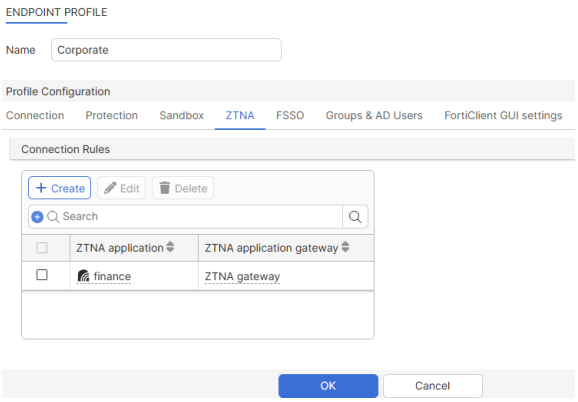


9. Click **OK**.

Task 3: Configuring ZTNA connection rules

To configure ZTNA connection rules:

1. On FortiSASE, configure the Corporate profile:
   a. Go to **Endpoint management > Endpoint profiles**, select **Corporate** and click **Edit**.
   b. On the **Connection** tab, under **Tunnel settings**, set **Use advanced SAML engine for FortiClient built-in browser** to **Web browser**.
   c. Switch to the **FortiClient GUI settings** tab in the same Corporate endpoint profile and enable **Show security posture tags**. This enables FortiClient to display security posture tags assigned to the endpoint.
   d. Switch to the **ZTNA** tab and under **Connection Rules**, click **Create**.
   e. From the **Agent-based ZTNA application** dropdown list, select **finance**.
   f. Click **OK**.
   g. Click **OK** to save the endpoint profile.

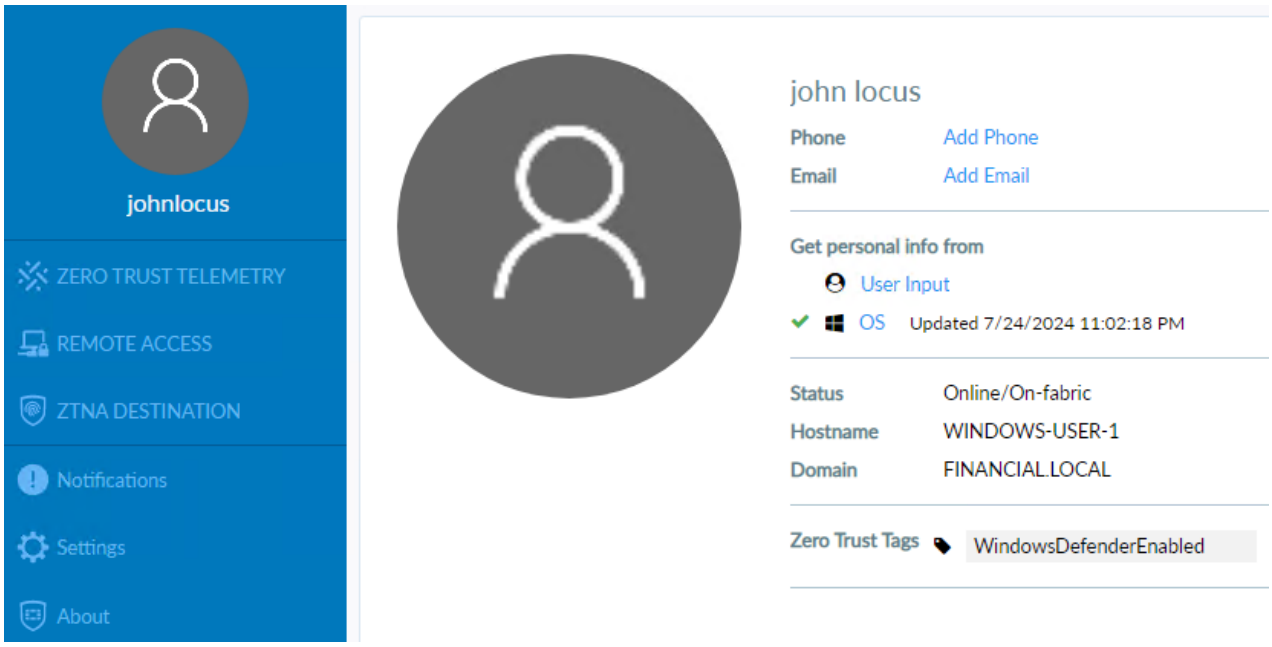


2. Edit the NonCorporate profile:
   a. On the same **Endpoint management > Endpoint profiles** page, select **NonCorporate** and click **Edit**.
   b. On the **Connection** tab, under **Tunnel settings**, set **Use advanced SAML engine for FortiClient built-in browser** to **Web browser**.
   c. Switch to the **FortiClient GUI settings** tab in the same NonCorporate endpoint profile and enable **Show security posture tags**. This enables FortiClient to display security posture tags assigned to the endpoint.
   d. Switch to the **ZTNA** tab and under **Connection Rules**, click **Create**.
   e. From the **Agent-based ZTNA application** dropdown list, select **marketing**.
   f. Click **OK**, then click **OK** to save the endpoint profile.

Task 4: Verifying ZTNA tags and connection rules on endpoints

To verify ZTNA tags assigned and ZTNA connection rules deployed on FortiClient endpoints:

1. Log in to the Windows10-User1 endpoint and open the FortiClient console.
2. Click the **johnlocus** user avatar at the top left of FortiClient console, which opens the user profile.
3. Under **Zero Trust Tags** of the user profile on FortiClient, confirm the ZTNA tags that are assigned. You can see the **WindowsDefenderEnabled** ZTNA tag, as both endpoints have Windows Defender enabled by default.



4. Similarly, to view the ZTNA tags assigned to endpoints on FortiSASE, go to **Operations > Connectivity > Endpoints**. Use scrollbar at the bottom to move to right until you see **ZTNA Tags (Simple)** column.
5. To view the **ZTNA Connection Rules** on FortiClient, click the **ZTNA DESTINATION** tab on FortiClient. On Windows10-User1, you see the **finance** SSH access ZTNA connection rule.
6. Follow the steps above to verify the ZTNA tags and connection rules for the fortinet user on the Windows10-User2 endpoint. On Windows10-User2, you see the **marketing** SSH access ZTNA connection rule on the **ZTNA DESTINATION** tab.

By default, FortiSASE is configured to have a FortiClient telemetry sync timer of 60 seconds, which means that any endpoint-specific change performed on FortiSASE takes a minimum of 60 seconds to propagate and reflect on FortiClient.

Thus, users are advised to wait at least 60 seconds for endpoint profile changes performed on FortiSASE to propagate to FortiClient endpoints.

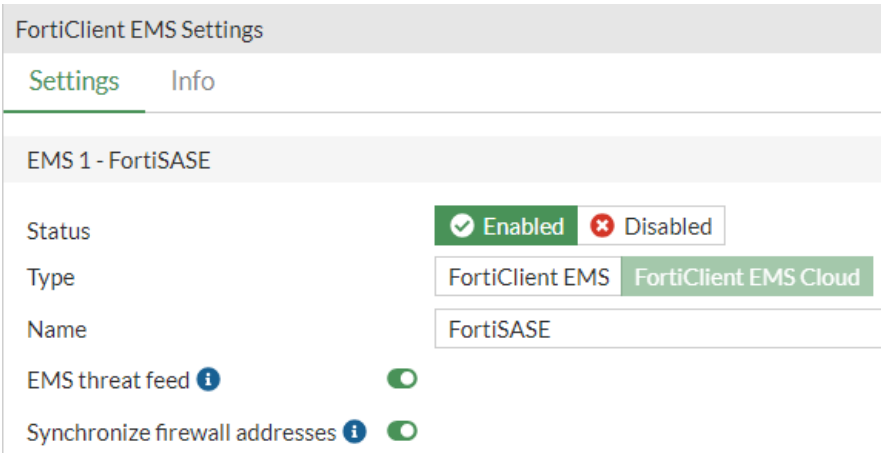
2.10 Configuring FortiClient Cloud connector and verifying ZTNA tag sync (required)

In this section, we configure connectivity between FortiGate_HQ and the FortiSASE Endpoint Management (FortiClient Cloud) service using a Security Fabric FortiClient EMS connector. Once the connection succeeds, ZTNA tags that are configured on FortiSASE are visible and available for use on FortiGate_HQ. You can use ZTNA tags to restrict access to a ZTNA application gateway on FortiGate_HQ.

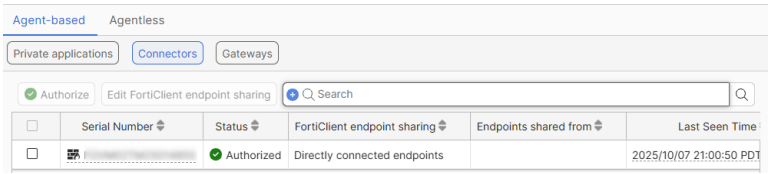
Task 1: Configuring a FortiClient Cloud connector

To configure a FortiClient Cloud connector on FortiGate_HQ:

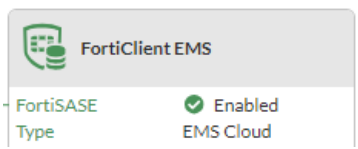
1. Configure the connector in FortiOS:
   a. Go to **Security Fabric > Fabric Connectors**.
   b. Click **FortiClient EMS** and select **Edit**.
   c. For **EMS 1**, set **Status** as **Enabled**.
   d. For **Type**, select **FortiClient EMS Cloud**. In the **Name** field, enter **FortiSASE**. Click **OK**.



2. Do the following:
   a. FortiSASE presents an EMS server certificate. Click **Accept**.
   b. Click **Close** for the warning of FortiGate not being authorized on FortiClient EMS.
3. On FortiSASE, go to **Security > Traffic > ZTNA**. Go to the **Connectors** tab.
4. Select the FortiGate serial number, and click **Authorize**. Click **OK** on the confirmation prompt.
5. Confirm that the FortiGate **Status** displays as **Authorized**.



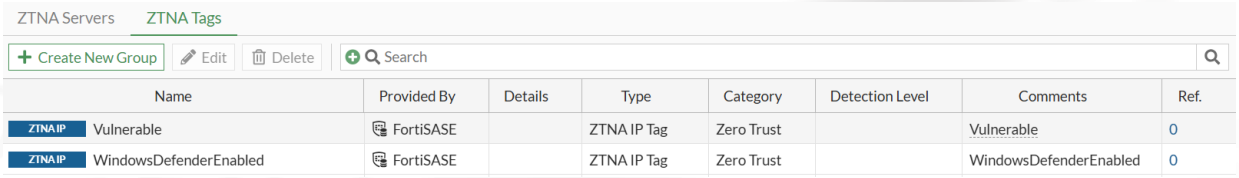
6. On the FortiGate, under **Security Fabric > Fabric Connectors**, the **FortiClient EMS** card shows as **Connected** with a green check.



Task 2: Verifying ZTNA tag sync on FortiGate_HQ

To verify ZTNA tag sync on FortiGate_HQ:

1. On the FortiGate, go to **Policy & Objects > ZTNA** and switch to the **ZTNA Tags** from the toolbar.
2. Verify that **[ZTNA IP] Vulnerable** and **[ZTNA IP] WindowsDefenderEnabled** tags are visible.



2.11 Configuring SAML SSO on FortiGate_HQ (required)

For this section, in Task 1 we complete the remainder steps of configuring SAML SSO using FortiAuthenticator as IdP on FortiGate_HQ. This SSO configuration is used for user authentication to ZTNA Application Gateway.

In the (optional) Task 2, we review and get familiar with the following pre-configured settings that are used for configuring ZTNA Application Gateway on FortiGate_HQ.

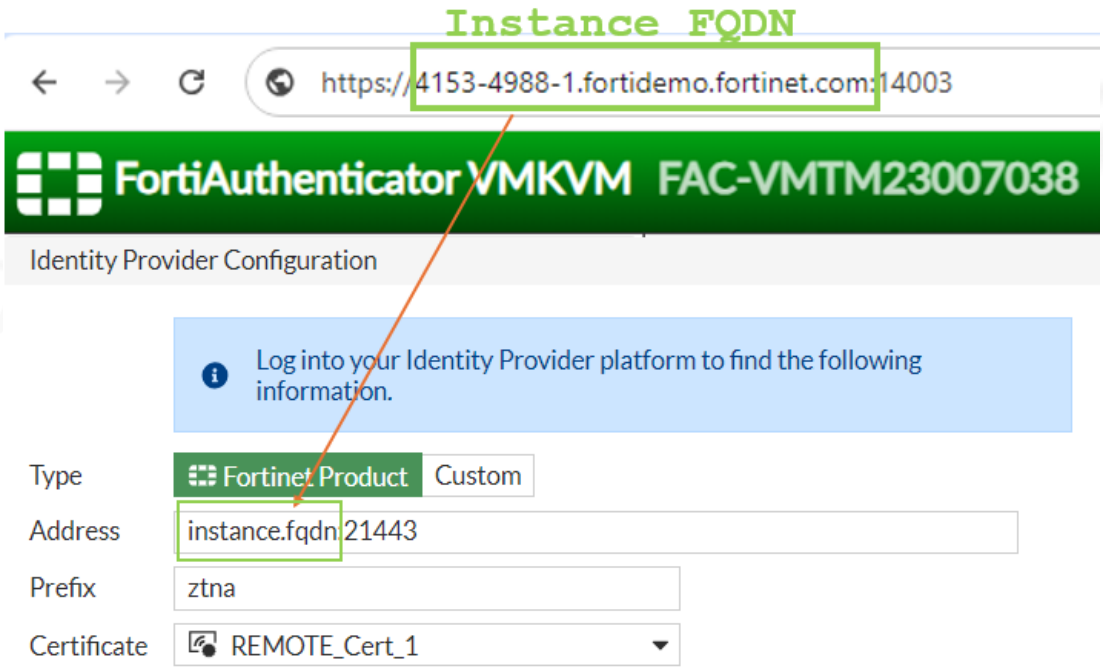
- SAML User Group
- ZTNA Authentication Rules & Schemes
- ZTNA Server
- Full ZTNA firewall policy

Task 1: Configuring SAML SSO on FortiGate_HQ

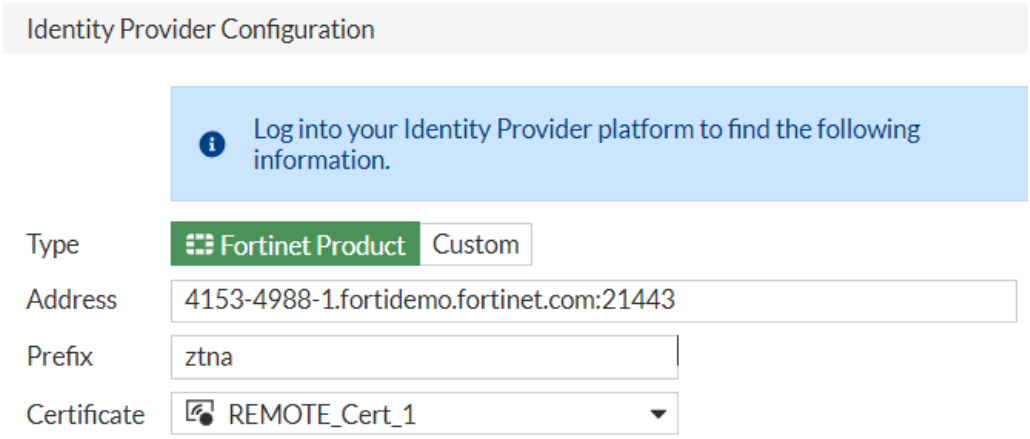
To configure SAML SSO on FortiGate_HQ:

1. On FortiGate_HQ, go to **User & Authentication > Single Sign-On**.
2. Select **SAML-FAC** and click **Edit**.
3. Under **Identity Provider Configuration**, in the **Address** field, replace the **instance.fqdn** with your unique instance FQDN.Keep the port 21443 as it is.
4. To get the instance.FQDN use your FortiAuthenticator's login URL as shown below.

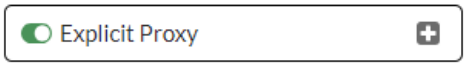
5. Use the instance FQDN from FortiAuthenticator and replace **instance.fqdn** on FortiGate_HQ as shown below.



6. For example, after entering the instance FQDN the **Address** field should then appear as shown below. Note: The **Address** field will be unique to your instance as your instance FQDN is unique.



7. Click **OK** to save the SAML SSO configuration.
8. On FortiGate_HQ, go to **System > Feature Visibility** and enable **Explicit Proxy** for Full ZTNA Policies to be visible on GUI.

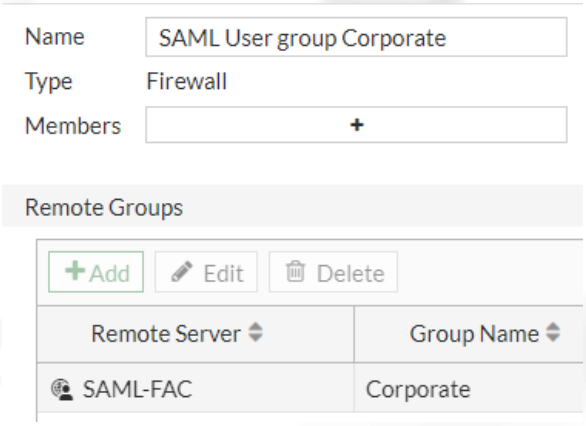


9. Click **Apply**.

Task 2: Reviewing ZTNA Application Gateway configuration (Optional)

To review the pre-configured ZTNA configuration for ZTNA Application Gateway on FortiGate_HQ:

1. To review SAML User groups, go to **User & Authentication > User Groups**.
   a. Select **SAML User group Corporate** and click **Edit**. Notice SAML server configured in Task 1 called SAML-FAC, is used in the **Remote Groups** configuration. This user group has a **Group Name** called **Corporate**.

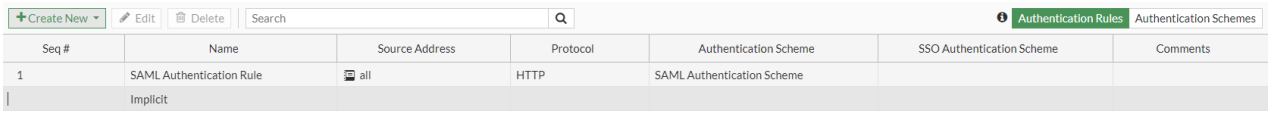


The **Group Name** configuration is used as a filter by FortiGate_HQ to achieve SAML group matching by filtering out SAML Assertions sent by FortiAuthenticator. This configuration enables segregation of users into different user groups.

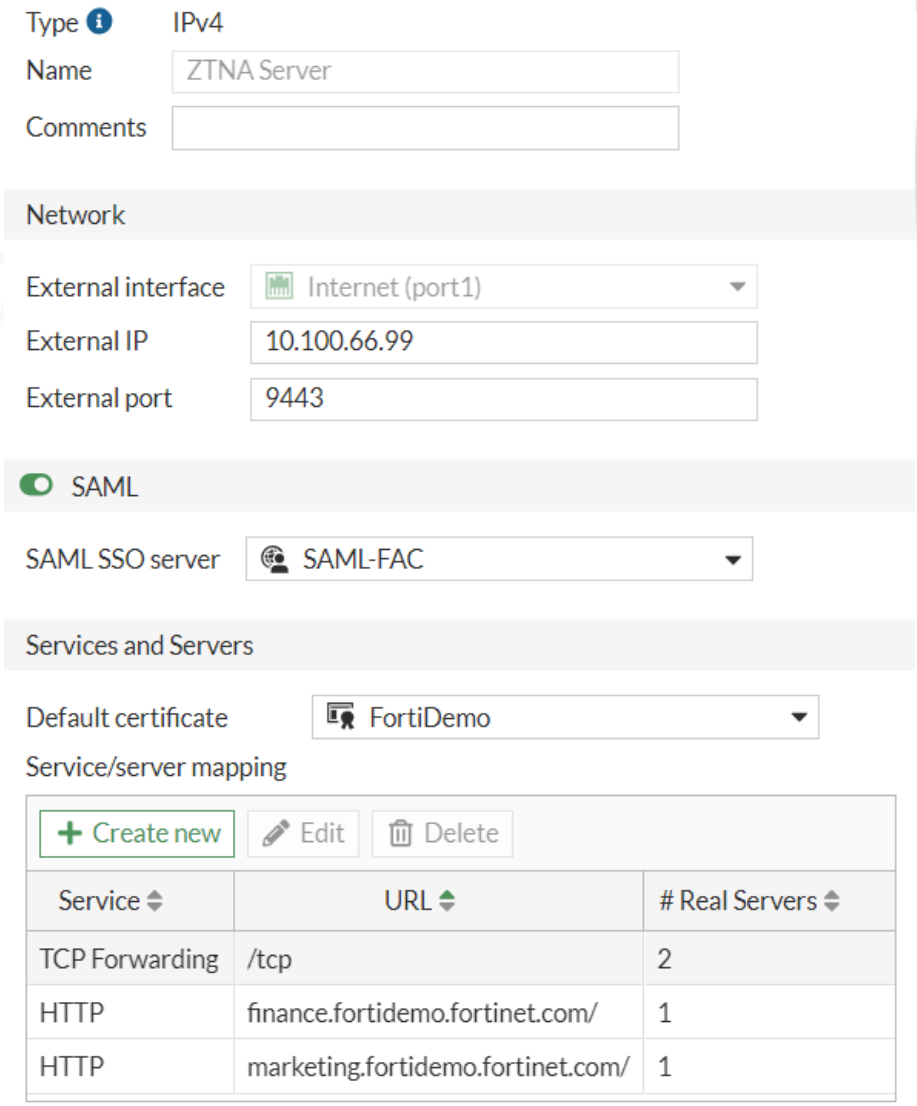
b. Click **Cancel**, and similarly, review the other User group i.e. **SAML User group NonCorporate**.

2. To review Authentication Rules and Schemes, go to **Policy & Objects > Authentication Rules**.
3. Select the **Authentication Schemes** tab and notice the **Method** used is configured as **SAML** for ZTNA Application Gateway.

4. Select **Authentication Rules** tab and notice the **Authentication Rule** uses the **Authentication Scheme**.



5. To review ZTNA Server configuration, go to **Policy & Objects > ZTNA**. Select **ZTNA Server** and click **Edit**.



6. To review Full ZTNA Firewall policy, go to **Policy & Objects > Proxy Policy**.

ID	Name	Type	To	Source	Destination	Schedule	Action	Security Profiles	Log	Bytes
1	Deny Vulnerable Endpoint	ZTNA		all SAML User group Corporate SAML User group NonCorporate	all	always	DENY		All	0 B
2	ZTNA Policy Corporate	ZTNA		all SAML User group Corporate	Finance Server	always	ACCEPT	no-inspection	All	0 B
3	ZTNA Policy NonCorporate	ZTNA		all SAML User group NonCorporate	Marketing Server	always	ACCEPT	no-inspection	All	0 B
0	Implicit Deny		any	all	all	always	DENY		Disabled	0 B

For more information about ZTNA, see ZTNA.

2.12 Configuring ZTNA tags in full ZTNA firewall policy (required)

This section demonstrates how to use ZTNA tags on FortiGate_HQ to allow role based access control to resources protected by ZTNA Application Gateway.

In our lab, ZTNA Application Gateway uses Web Access Proxy and TCP Forwarding method to expose the HTTP and SSH services on Finance and Marketing servers. These services are reachable by endpoints using the FQDNs below:

Service Name	Server FQDN:Service Port
HTTP	marketing.fortidemo.fortinet.com:9443 finance.fortidemo.fortinet.com:9443
SSH	marketing.financial.local:22 finance.financial.local:22

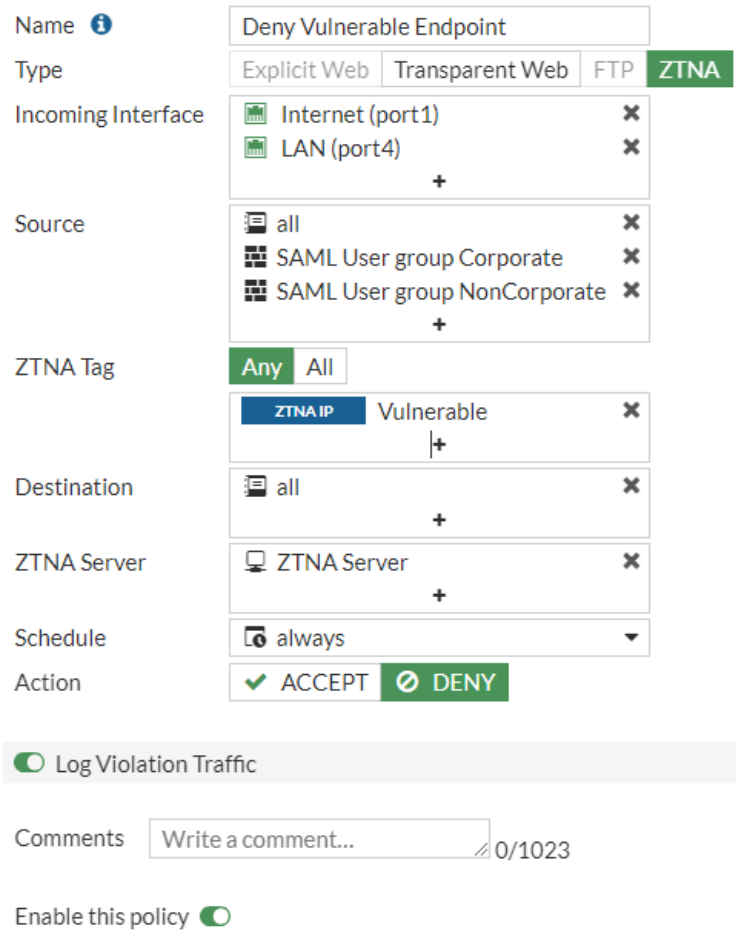
When endpoint accesses these services, it must authenticate itself to the ZTNA Application Gateway. SAML SSO is used by ZTNA Application Gateway for user authentication. These settings are pre-configured on FortiGate_HQ.

We configure ZTNA tags inside Full ZTNA firewall policies of FortiGate_HQ to test the role based access control of these resources:

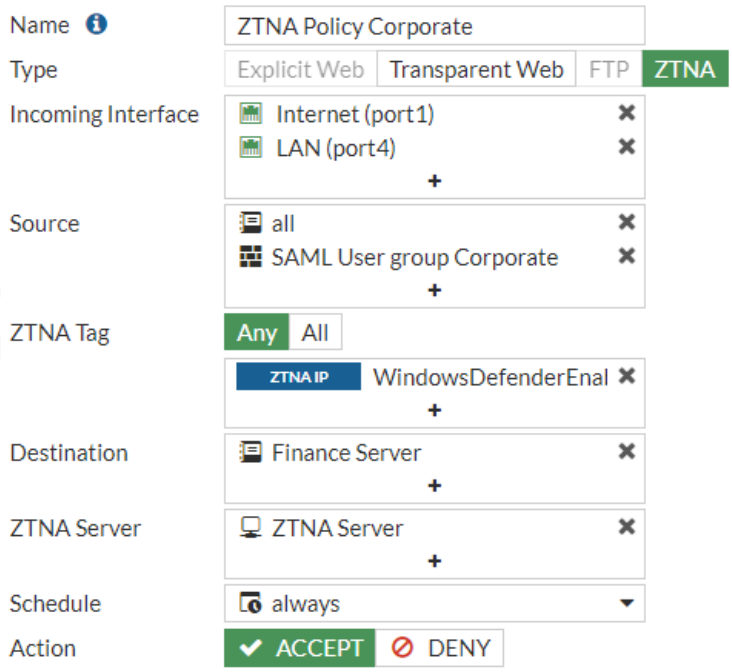
Task 1: Configuring ZTNA tags in Full ZTNA firewall Policy

To configure ZTNA tags in Full ZTNA firewall Policy:

1. On FortiGate, go to **Policy & Objects > Proxy Policy**.
2. Select policy **Deny Vulnerable Endpoint** and click **Edit**.
3. In the **ZTNA Tag** field, click **+** to add a ZTNA tag and select **[ZTNA IP] Vulnerable** tag from the **FortiSASE – IP** tag group.



4. Click **OK** to save it.
5. Similarly, from the same firewall policy page, edit **ZTNA Policy Corporate** to add **[ZTNA IP] WindowsDefenderEnabled** tag from the **FortiSASE – IP** tag group.



6. Click **OK** to save the firewall policy.
7. Repeat the same steps for **ZTNA Policy NonCorporate** to add **[ZTNA IP] WindowsDefenderEnabled** tag to it.

This configuration ensures if the endpoint is tagged with ZTNA Tag of Vulnerable, it will be denied access to resources protected by the ZTNA Application Gateway. It also ensures only the endpoints tagged with ZTNA Tag of WindowsDefenderEnabled will be able to access HTTP and SSH resources.

2.13 Accessing services via a ZTNA application gateway (required)

In this section, we will access the HTTP server and SSH server that the ZTNA application gateway protects to verify that FortiGate_HQ performs client certificate authentication, user authentication using SAML, and role-based access control using the WindowsDefenderEnabled ZTNA tag. We will go through the ZTNA logs to verify that logs conform to our requirements.

The table lists FQDNs that endpoints use to access the respective servers:

Endpoint	Can access	Via HTTP service (using web access proxy method) by using following FQDN	Via SSH service (using TCP forwarding method) by using following FQDN
Windows10-User1 (AD Endpoint)	Finance server	finance.fortidemo.fortinet.com:9443	finance.financial.local:22
Windows10-User2 (non-AD Endpoint)	Marketing server	marketing.fortidemo.fortinet.com:9443	marketing.financial.local:22

Task 1: Accessing HTTP and SSH services via ZTNA application gateway

To access HTTP and SSH services via ZTNA application gateway:

1. On Windows10-User1, open a Chrome incognito window and open the **Finance Server** bookmark or go to https://finance.fortidemo.fortinet.com:9443. Chrome presents a prompt to authenticate to the ZTNA application gateway using a client certificate. Select the certificate and click **OK**.

The FortiSASE Endpoint Management server generates, signs, and installs a client certificate on the endpoint's certificate store when it first connects to FortiSASE using the invitation code.

Whenever FortiClient disconnects and reconnects to FortiSASE using the invitation code, a new client certificate is automatically provisioned by FortiSASE's Endpoint Management. As FortiSASE's Endpoint Management server has signed that certificate, FortiSASE trusts that certificate whenever it is presented.

2. FortiAuthenticator presents a SAML login page. Enter the appropriate credentials, then click **Login**:

User Type	Computer Name	FortiSASE SIA Username	Password
AD User	Windows-User1	financial\johnlocus	SecurityFabric

3. Similarly, use another browser tab to open the Marketing server using the **Marketing Server** bookmark or visiting the URL https://marketing.fortidemo.fortinet.com:9443.
4. Verify that Windows10-User1 is allowed access to Finance server and denied access to Marketing server for HTTP service:

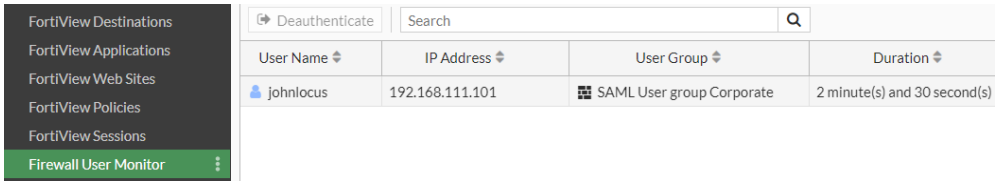
Computer Name	HTTP Service	HTTP Access (Allowed/Denied)
Windows10-User1	Finance Server	Allowed
	Marketing Server	Denied

An endpoint is prompted for SAML authentication while accessing the ZTNA Server only once, after which it not prompted for its credentials again until the authenticated entry times out on FortiGate_HQ.

To clear the authenticated sessions on FortiGate_HQ manually, login to FortiGate_HQ and perform the following steps in **Dashboard > Firewall User Monitor**:

- On the **Firewall** tab, select the user and click **Deauthenticate**.
- On the **Proxy** tab, select the user and click **Deauthenticate**.

If **Firewall User Monitor** is not visible on **Dashboard** option, click **+ Add Monitor**. Then search for Firewall Users and add.



5. To verify accessing the SSH service, open PuTTy using the shortcut from the taskbar.
6. From the **Saved Sessions**, click **Finance Server** shortcut and click **Load**. Alternatively, in **Session category**, in the **Host Name** (or **IP Address**) field, enter the finance server FQDN as finance.financial.local and set the **Connection type** as **SSH**.
7. Click **Open**.

8. If you are allowed to access the SSH service then you will be presented with a key pair. Click **Accept** to accept the key-pair.
9. Use the username as root and password as SecurityFabric to log in.
10. Similarly, to login to Marketing server open another PuTTy session by using the **PuTTy** shortcut from the taskbar. From the **Saved Sessions**, click **Marketing Server** shortcut and click **Load**. Alternatively, in **Session** category, in the **Host Name** (or **IP Address**) field, enter the marketing server FQDN as marketing.financial.local and set the **Connection type** as **SSH**.
11. Click **Open**.
12. Verify that Windows10-User1 is allowed access to Finance server and denied access to Marketing server for SSH service as per our requirement below:

Computer Name	SSH Service	SSH Access (Allowed/Denied)
Windows10-User1	Finance Server	Allowed
	Marketing Server	Denied

13. Now, login to Windows10-User2 endpoint and perform the same steps as above to access Marketing and Finance server using the SAML credentials below:

User Type	Computer Name	FortiSASE SIA Username	Password
Non-AD User	Windows-User2	local\fortinet	SecurityFabric

Verify whether Windows10-User2 is allowed or denied access to HTTP and SSH services on following servers, as per our requirement below:

Computer Name	HTTP & SSH Service	HTTP & SSH Access (Allowed/Denied)
Windows10-User2	Finance Server	Denied
	Marketing Server	Allowed

Task 2: Verifying ZTNA logs

To verify ZTNA logs:

1. Logging **All Sessions** is enabled in Full ZTNA firewall policy. To view these logs on FortiGate_HQ, go to **Log & Report > ZTNA Traffic**.
2. Verify the logs generated for the HTTP and SSH services that match the ZTNA policy using the **Service** and **Policy ID** columns.

2.14 Running a Vulnerability Scan and configuring application-based ZTNA tags (optional)

This section is an optional section for users who want to explore more FortiSASE endpoint management features.

In Task 1, we perform a Vulnerability Scan on the endpoint to verify if the endpoint is tagged with the Vulnerable ZTNA tag and whether FortiClient denies the endpoint access to the ZTNA resource because it is tagged as Vulnerable.

Next in Task 2, we configure a ZTNA tag called UnAuthorizedApps to prevent endpoints from running applications that Financial company did not authorize. In this task, we use an application called FileZilla that is used for FTP data

transfers. FTP data transfers can cause data loss and infect endpoints. Therefore, we want to restrict endpoints running FileZilla from accessing any resources that the ZTNA application gateway protects.

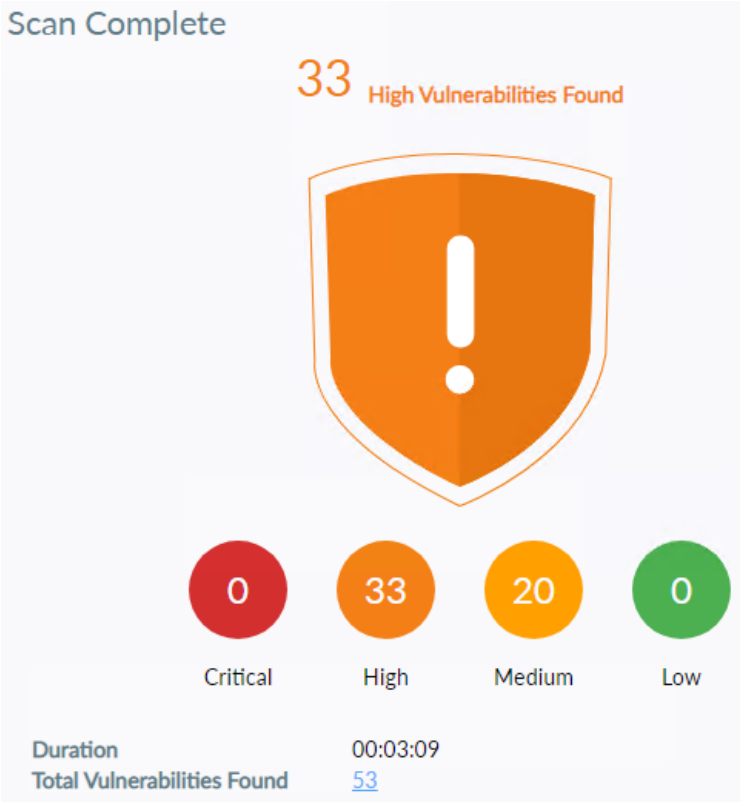
(Optional) Task 1: Running a Vulnerability Scan and verifying access to HTTP and SSH services

To run a Vulnerability Scan and verify access to HTTP and SSH services:

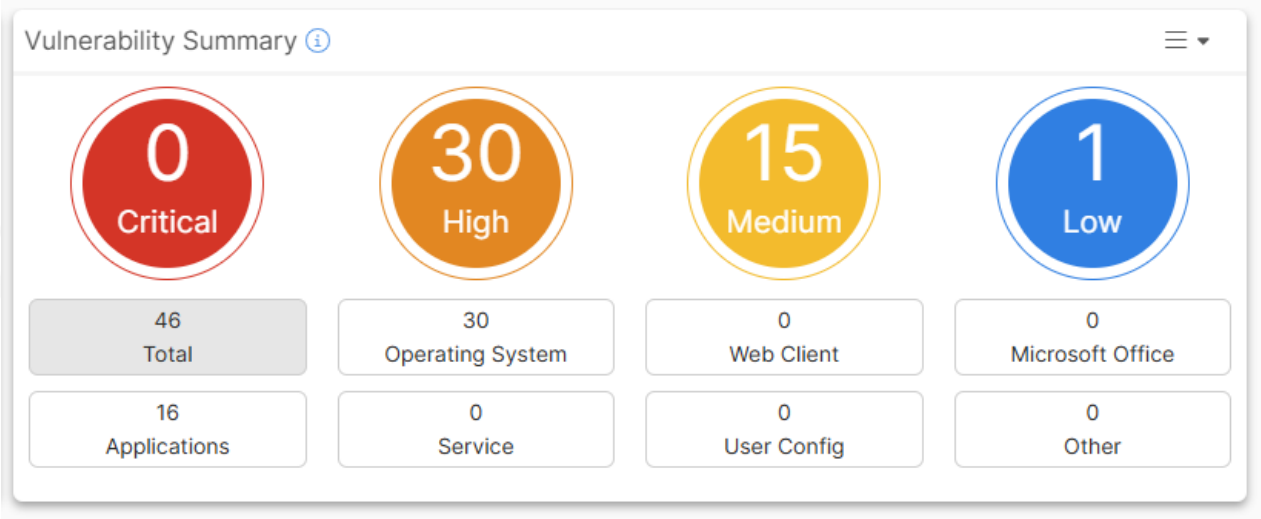
1. Enable Vulnerability Scan on the **Corporate** profile:
   a. In FortiSASE, go to **Endpoint management > Endpoint profiles**. Select **Corporate** and click **Edit**.
   b. On the **Protection** tab, do the following:
      - Enable **Scheduled scanning**.
      - From the **Schedule type** dropdown list, select **Daily**.
      - In the **Start at** field, configure a desired time.
      - Enable **Event-based scanning**.
   c. Click **OK** to save the profile.
2. Perform the same steps for the **NonCorporate** endpoint profile.

Users are advised to wait at least 60 seconds for the endpoint profile changes performed on FortiSASE to propagate to FortiClient endpoints due to the FortiClient telemetry sync timer.

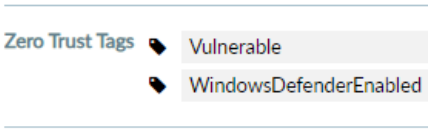
3. Open FortiClient on an endpoint.
4. On the **Vulnerability Scan** tab, you can see that the scan started automatically. Alternately, if **Scan Now** is visible, click it to activate a vulnerability scan manually. Wait for a few minutes for FortiClient to complete the scan. Under **Vulnerabilities Detected**, you will notice that FortiClient detected some high severity vulnerabilities.



5. To view the detected vulnerabilities on endpoints from FortiSASE, go to **Monitoring > Dashboards > Security > Vulnerability summary**. Click **Total** to see all vulnerabilities detected.



6. According to the tagging rules configured earlier on FortiSASE, whenever FortiClient detects a high or higher severity vulnerability on an endpoint, it is tagged with the **Vulnerable** security posture tag. To verify whether the security posture tag is assigned to an endpoint, click the user avatar at the top-left corner on FortiClient. In **Zero Trust Tags**, note the **Vulnerable** security posture tag.



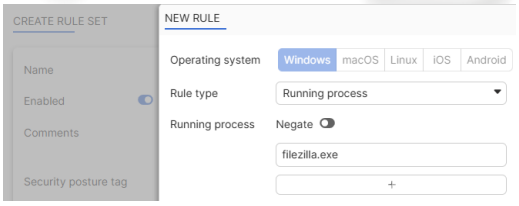
7. Retry access to the HTTP and SSH servers using the steps in Task 1: Accessing HTTP and SSH services via ZTNA application gateway on page 42.
8. You are presented with a ZTNA policy denied block page for the HTTP service and a network error for SSH access, which means that ZTNA has blocked access to the service due to the **Deny Vulnerable Endpoint** policy that denies any incoming request from an endpoint that has the **Vulnerable** tag assigned.
9. Verify the ZTNA logs using Task 2: Verifying ZTNA logs on page 43.

(Optional) Task 2: Configuring application-based security posture tags and verifying access to HTTP and SSH services

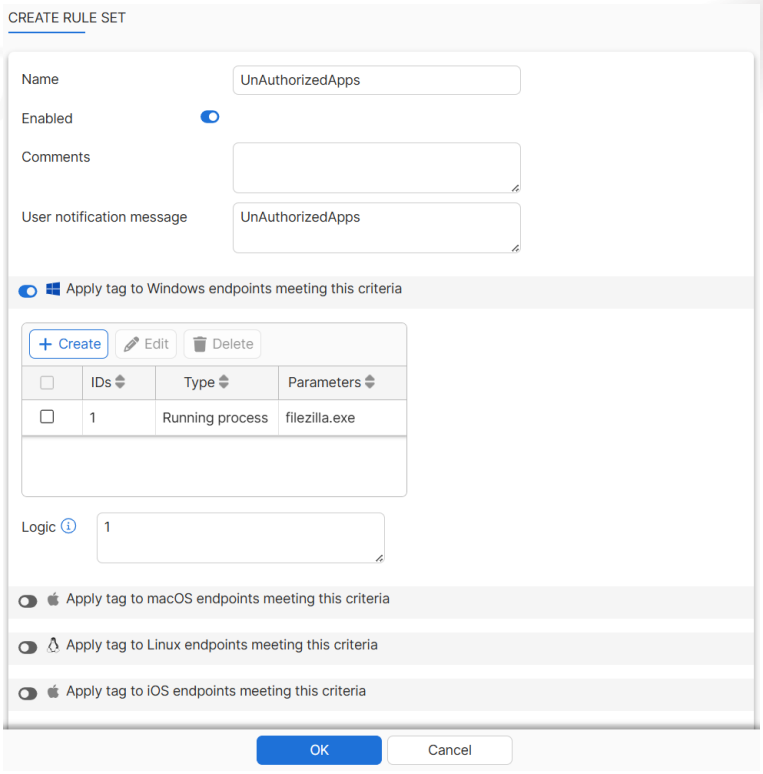
To configure an application-based security posture tag for the FileZilla application:

1. In FortiSASE, go to **Endpoint management > Security posture tags**.
2. Go to the **Tagging rules** tab.
3. Click **Create** and enter **Name** as **UnAuthorizedApps**.
4. In **User notification message**, enter a message.
5. Enable **Apply tag to Windows endpoints meeting this criteria**.
6. Click **Create** and enter the following details:

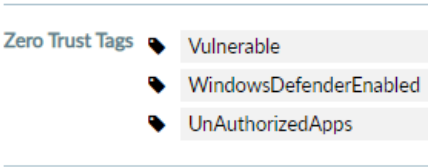
Field	Value
Operating system	Windows
Rule type	Running Process
Running process	filezilla.exe



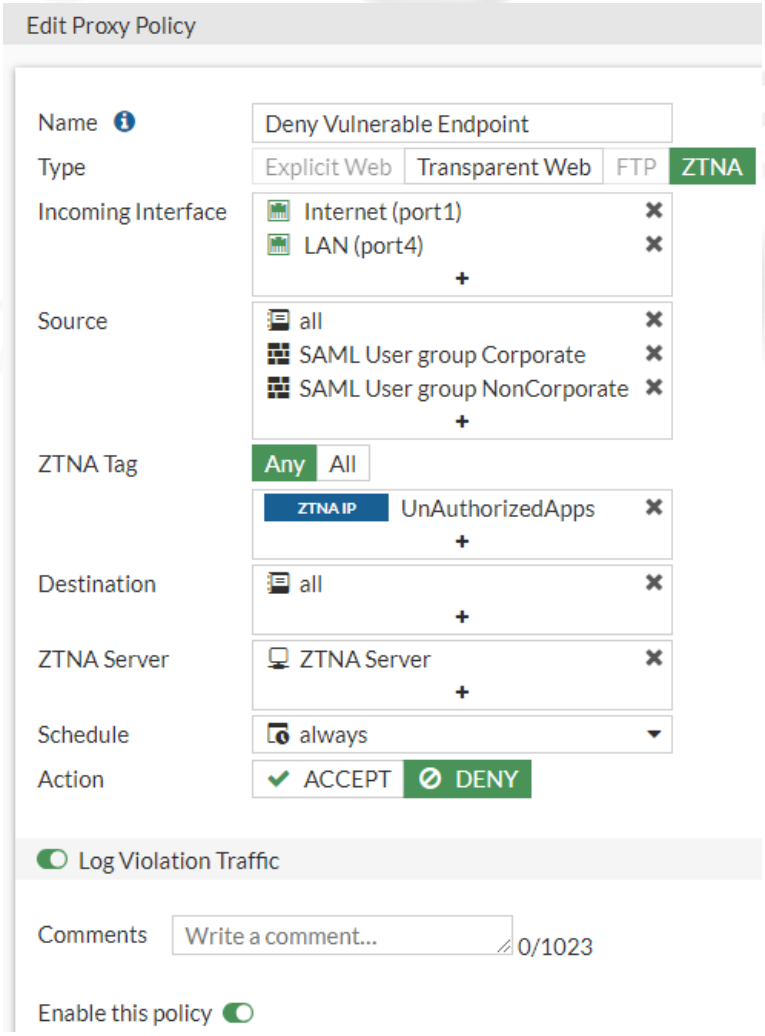
7. Click **OK**.



8. Click **OK** to save the security posture tagging rule.
9. Log in to an endpoint and open the FileZilla application shortcut from the Desktop or from the taskbar shortcut.
10. In FortiClient, click the user avatar and wait for the endpoint to be tagged with the UnAuthorizedApps ZTNA tag.



11. On FortiGate_HQ, go to **Policy & Objects > Proxy Policy**. Edit the **Deny Vulnerable Endpoints** policy to remove **Vulnerable** ZTNA tag and add **ZTNA IP UnAuthorizedApps** in **ZTNA Tag** as shown below.



12. Click **OK** to save the policy.
13. From the same FortiClient endpoint access HTTP and SSH Servers again using ZTNA Application Gateway and verify ZTNA logs using steps from Task 1: Accessing HTTP and SSH services via ZTNA application gateway on page 42 and confirm that you are blocked by ZTNA Application Gateway from accessing any resources because of Deny Vulnerable Endpoint Full ZTNA firewall policy as endpoint is tagged with UnAuthorizedApps tag.
14. Verify the same using ZTNA logs using Task 2: Verifying ZTNA logs on page 43.

3. Conclusion

In this 4-D Accelerator lab, we configured and tested different FortiSASE Endpoint Management features like custom endpoint profiles, VPN autoconnect, bypass FortiSASE, and split tunnel. We also configured ZTNA features like ZTNA tags and tagging rules and leveraged ZTNA application gateway configuration on FortiGate_HQ to access resources that the ZTNA server protects.

4. More information

Appendix A - Products used in this guide

Product	Model	Firmware
FortiGate	FortiGate-VM64-KVM	7.2.8 GA
FortiAuthenticator	FAC-VMTM23007138	6.1.1 GA
FortiSASE	N/A	See the FortiSASE Release Notes.
FortiClient		7.4.5

Appendix B - Documentation references

This 4-D Accelerator lab provides a quick and accelerated demonstration of basic use cases of FortiSASE endpoint management. For longer or more in-depth lab demonstrations, see the following product documentation:

Product documentation

- FortiSASE Administration Guide
- FortiSASE Reference Guide
- FortiOS Administration Guide

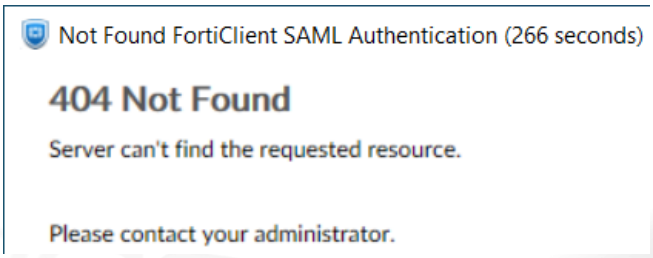
Appendix C - FAQs

After clicking SAML Login, I receive an error when the FortiClient SAML authentication prompt appears. What do the error messages mean and how can I resolve the issues?

If you have issues with displaying the SAML login prompt from FortiClient, examine the error message:

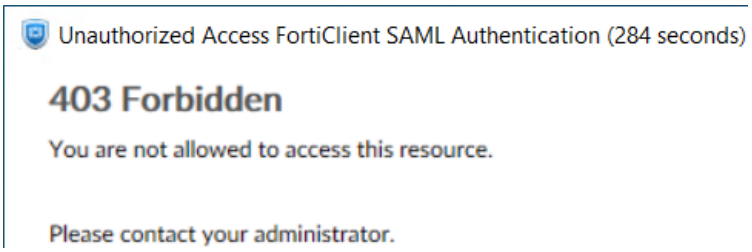
- A **404 Not Found** error in the SAML login prompt indicates FortiClient could not access the IdP single sign-on URL successfully. This error indicates an issue with configuring **IdP Single Sign-On URL** in the **Identity Provider Configuration** section of the **SSO** wizard in FortiSASE.

To resolve this issue, ensure that you copied this field correctly from **Edit SAML Service Provider** on FortiAuthenticator.

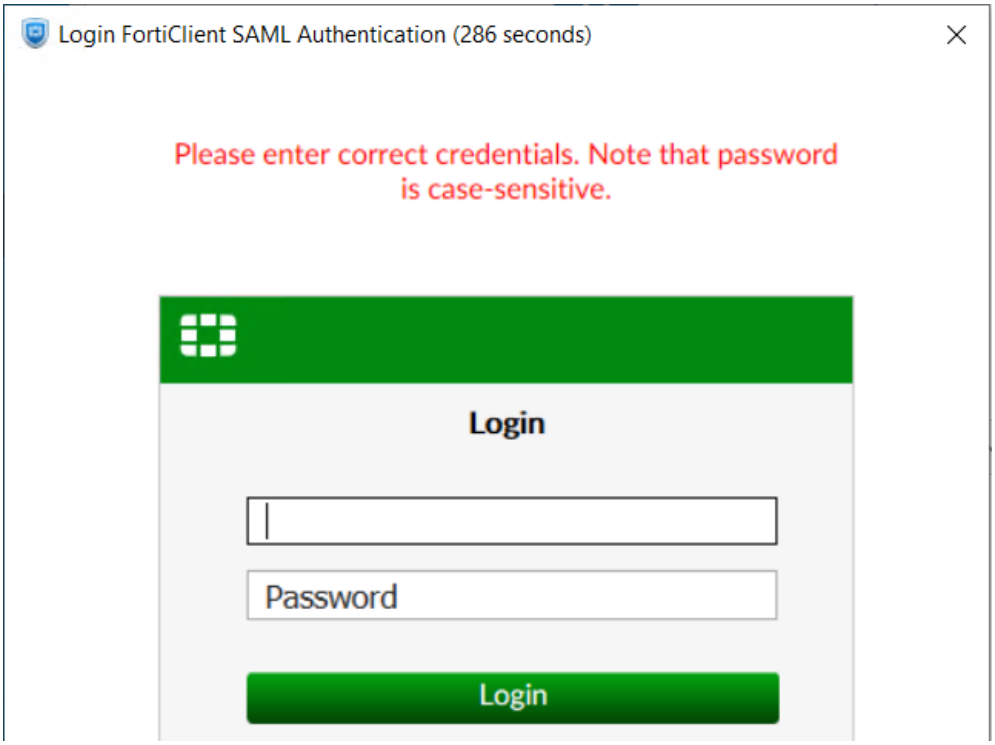


- A **403 Forbidden** error in the SAML login prompt indicates that the username provided does not have permission to log in to the SP, in this case, FortiSASE. This error indicates an issue with configuring **SP ACS (login) URL** in **Edit SAML Service Provider** in FortiAuthenticator.

  To resolve this issue, ensure that you have not left this field with the predefined placeholder value **https://replace-me-with-the-sase-vpn.fqdn.com** and replaced it with the correct URL in **Assertion Consumer Service (ACS) URL** in the **Service Provider Configuration** section of the **SSO** wizard in FortiSASE.



After clicking SAML Login, the FortiClient SAML authenticator prompt displays as desired. When I enter my credentials, I see the error message Please enter correct credentials. Note that password is case-sensitive. What does this mean and how can I resolve the issue?



This error indicates that you entered the username or password incorrectly. To resolve this issue, ensure that you correctly enter the **local\fortinet** or **financial\johnlocus** usernames and matching passwords. See Users and endpoints on page 6.

Change log

Date	Change description
2024-06-20	Initial release.
2024-07-26	Updated FortiClient version to 7.0.13.
2024-08-20	Added 2.1 Checking FortiSASE EMS connectivity on page 7.
2024-09-04	Updated 2.2 Configuring FortiSASE with FortiAuthenticator as SAML IdP (required) on page 8.
2024-10-07	Updated for 24.3.c GUI changes.
2024-11-26	Updated for 24.4.b GUI changes.
2025-01-17	Updated FortiClient to 7.2.6 and lab guide with 24.4.c GUI changes.
2025-02-18	Updated FortiClient to 7.2.8 and lab guide with 25.1.a GUI changes.
2025-03-19	Updated for 25.1.b GUI changes.
2025-08-15	Updated FortiClient to 7.2.11 and lab guide with 25.3.a GUI changes.
2025-10-10	Updated for Feature release and its new navigation/GUI.
2025-12-18	Updated for 25.4.b GUI changes.
2026-01-27	Updated FortiClient to 7.4.5.

www.fortinet.com

72-251-922291-20260127