

DO NOT REPRINT
© FORTINET



FortiAuthenticator Lab Guide

for FortiAuthenticator 6.4

DO NOT REPRINT

© FORTINET

Fortinet Training Institute - Library

<https://training.fortinet.com>

Fortinet Product Documentation

<https://docs.fortinet.com>

Fortinet Knowledge Base

<https://kb.fortinet.com>

Fortinet Fuse User Community

<https://fusecommunity.fortinet.com/home>

Fortinet Forums

<https://forum.fortinet.com>

Fortinet Product Support

<https://support.fortinet.com>

FortiGuard Labs

<https://www.fortiguard.com>

Fortinet Training Program Information

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

Fortinet | Pearson VUE

<https://home.pearsonvue.com/fortinet>

Fortinet Training Institute Helpdesk (training questions, comments, feedback)

<https://helpdesk.training.fortinet.com/support/home>



8/18/2022

TABLE OF CONTENTS

Change Log	6
Network Topology	7
Lab 1: Introduction and Initial Configuration	8
Lab 2: Basic Configuration	9
Exercise 1: Creating an Administrator Profile and User	10
Configure the FortiAuthenticator FQDN	10
Create an Administrator Profile	11
Create an Administrator User	12
Test Your Administrator User Permissions	15
Exercise 2: Configuring the Mail Server	16
Configure the Mail Server	16
Set Email Services to the FortiMail SMTP Server	17
Lab 3: Administering and Authenticating Users	18
Lab 4: User Authentication	19
Exercise 1: Configuring and Testing the Self-Service Portal	20
Configure the Self-Service Portal	20
Create a Self-Service Portal Policy	21
Modify the Replacement Message	22
Perform a Self-Registration	23
Approve the Self-Registration Request	24
Complete the Self-Registration	25
Exercise 2: Configuring FortiGate as a RADIUS Client of FortiAuthenticator	27
Configure the RADIUS Server on FortiGate	27
Create a Firewall User Group for Remote Administrators	27
Create a Wildcard Administrator User	28
Configure a Remote AD/LDAP Server on FortiAuthenticator	29
Create an Authentication Realm	30
Import Active Directory Users	30
Create a Remote LDAP User Group and Add a User	31
Link RADIUS Attributes to a Group	32
Configure FortiGate as a RADIUS Client of FortiAuthenticator	32
Configure a RADIUS Service Policy	33
Enable the RADIUS Service	33

Lab 5: Two-Factor Authentication	37
Exercise 1: Creating and Assigning a FortiToken Mobile Token	38
Obtain the Two Free FortiToken Mobile Tokens	38
Assign a Token to a User	39
Activate the FortiToken Mobile Token	39
Exercise 2: Testing Two-Factor Authentication	41
Lab 6: FSSO Process and Methods	42
Lab 7: Fortinet Single Sign-On	43
Exercise 1: Preparing FortiGate and FortiAuthenticator for FSSO	46
Create an FSSO Agent	46
Create an FSSO User Group	46
Enable FortiGate SSO Authentication	47
Create a FortiGate Filter	47
Add the FortiAuthenticator SSO Group to the FortiGate FSSO Agent	48
Exercise 2: Configuring RADIUS Accounting	50
Configure FortiGate as a RADIUS Accounting Client	50
Enable RADIUS Accounting SSO Clients	51
Configure FortiAuthenticator as the RADIUS Accounting Server	51
Test RADIUS Accounting	52
Exercise 3: Configuring Manual Portal Authentication	54
Add the SSL-VPN User Group to the AD Realm	54
Enable Portal Services	55
Test Manual Portal Authentication	55
Exercise 4: Configuring DC Polling (Event Log Polling)	57
Enable DC Polling	57
Create a DC	57
Test DC Polling	58
Exercise 5: Configuring FortiClient SSO Mobility Agent	60
Enable the FortiClient SSO Mobility Agent Service	60
Configure FortiClient to Send User Information to FortiAuthenticator	60
Validate FortiClient SSO Mobility Agent User Updates	61
Lab 8: Portal Services	62
Exercise 1: Configuring FortiGate for Credential-Based Authentication	64
Create a User Group for Portal Users	64
Enable a Captive Portal on FortiGate	64
Create a Firewall Policy for FortiAuthenticator	65
Exercise 2: Configuring FortiAuthenticator for Credential-Based Authentication	67
Create a User Group for Portal Users	67
Configure a Credential-Based Portal	67
Configure a Credential-Based Portal Policy	68

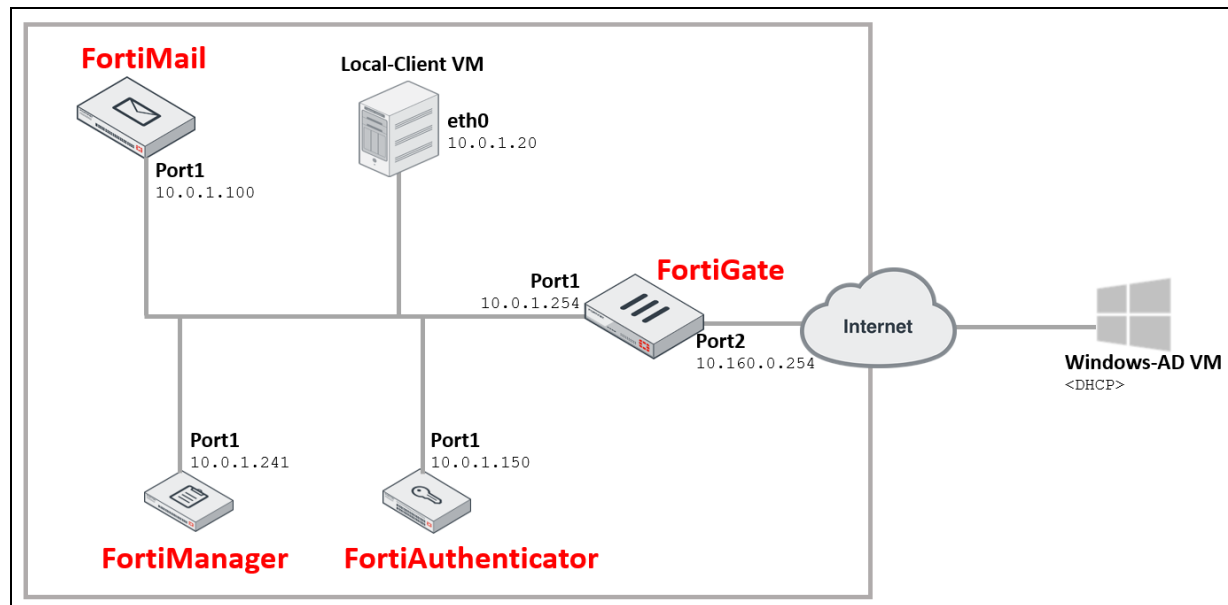
Exercise 3: Testing Authentication Through the Credential-Based Portal	71
Lab 9: PKI and FortiAuthenticator as a CA	73
Lab 10: Certificate Management	74
Exercise 1: Configuring SSL VPN User Groups	77
Create a User Group for SSL VPN Users	77
Add an SSL VPN Group to a RADIUS Client Policy	77
Add FortiAuthenticator to the Windows Domain	78
Exercise 2: Creating a CA Root Certificate and Importing It Into FortiGate	
Using SCEP	80
Create a CA Root Certificate	80
Enable the HTTP Service for SCEP	81
Import the Root Certificate Into FortiGate	81
Create a PKI User and Add the User to the Group	82
Exercise 3: Configuring User Certificate Authentication	84
Configure User Certificate Authentication	84
Export the User Certificate	84
Import the User Certificate to the VPN User's Certificate Store	85
Import the Certificate Into the Browser	85
Exercise 4: Using FortiAuthenticator to Create and Sign a CSR for FortiGate	
SSL Inspection	88
Generate a CSR on FortiGate	88
Sign the Certificate With FortiAuthenticator	89
Import the Signed Certificate Into FortiGate and Enable SSL Inspection	89
Import the Certificate Into the Browser	91
Lab 11: 802.1X Authentication	94
Lab 12: SAML	95
Exercise 1: Configuring IdP and SP Settings on FortiAuthenticator	96
Configure IdP Settings on FortiAuthenticator	96
Configure SP Settings on FortiAuthenticator	97
Exercise 2: Configuring FortiGate As an SP	99
Configure FortiGate As an SP	99
Complete the FortiAuthenticator SP Configuration for FortiGate	100
Exercise 3: Adding FortiManager As a Second SP	102
Add FortiManager As a Second SP	102
Complete the FortiAuthenticator SP Configuration for FortiManager	104
Exercise 4: Testing the SAML Authentication	105
Validate the SAML Authentication	105
Lab 13: FIDO2 Authentication	107

Change Log

This table includes updates to the *Lab Guide* dated 7/14/2022 to the updated document version dated 8/18/2022.

Change	Location
Added specific lab prerequisite instructions required for self-paced/on demand lab students only.	• To update the Windows-AD VM IP address on page 45 • To update the Windows-AD VM IP address on page 63 • To update the Windows-AD VM IP address on page 75
General copy edits	Entire guide

Network Topology



Lab 1: Introduction and Initial Configuration

At this time, there is no lab associated with the *Introduction and Initial Configuration* lesson.

Lab 2: Basic Configuration

While the initial configuration of FortiAuthenticator is already done for you, including the IP address and netmask, DNS servers, static routing (including the default gateway), and system time, there are some basic configurations that are still required. These configurations are most typically performed by customers and will also be used in future labs.

Objectives

- Create an administrator profile and administrator user
- Configure the mail server

Time to Complete

Estimated: 20 minutes

Exercise 1: Creating an Administrator Profile and User

In this exercise, you will create an administrator profile and administrator user, and then assign the administrator profile to the administrator user. As mentioned in the lesson, administrator profiles are useful for dividing responsibilities, as well as controlling administrative access.

To log in to the FortiAuthenticator GUI

1. Log in to the FortiAuthenticator GUI with the username `admin` and password `password`.



If a security alert appears, accept the self-signed certificate or security exemption.

HTTPS is the recommended protocol for administrative access to FortiAuthenticator. Other available protocols include SSH, ping, SNMP, HTTP, and Telnet (if they are enabled).



The factory default for FortiAuthenticator is the username `admin` and an empty password. You must set a password during initial login.

Configure the FortiAuthenticator FQDN

You must configure the FQDN so that administrators can access the FortiAuthenticator GUI outside of your network subnet.

To configure the FortiAuthenticator FQDN

1. On the FortiAuthenticator GUI, click **System > Dashboard > Status**.
2. In the **System Information** widget, click the pencil icon beside **Device FQDN**.

System Information	
Host Name	FortiAuthenticator 
Device FQDN	Not configured 
Serial Number	FAC-VMTM18002385
System Time	Wed Apr 6 06:43:26 2022 
Firmware Version	v6.4.1, build0958 (GA)
System Configuration	Last Backup: N/A
Uptime	0 day(s) 0 hour(s) 2 minute(s)

3. In the **Fully qualified domain name** field, type `fac.trainingad.training.lab`.
4. Click **OK**.
The GUI server restarts.

Create an Administrator Profile

You will create an administrator profile with read and write access to the **Users and Devices** permission set.

The **Users and Devices** permission set allows an administrator with this profile assigned to have access to all activities surrounding users and devices, but restricts the administrator from having read and write access to other FortiAuthenticator activities.

To create an administrator profile

1. Continuing on the FortiAuthenticator GUI, click **System > Administration > Admin Profiles**, and then on the main pane, click **Permission sets**.
2. Before you create an administrator profile with the **Users and Devices** permission set, examine the individual permissions associated with the permission set by performing the following:
 - a. In the list of permission sets, click **Users and Devices**.
 - b. View the individual permissions associated with the permission set—these are the tasks an administrator assigned this permission set can perform.
3. Return to **System > Administration > Admin Profiles**, and then on the main pane, click **Create New**.
4. On the **Create New Admin Profile** page, configure the following settings:

Field	Value
Name	Users-and-Devices
Users and Devices	Read & Write

5. Click **OK**.

Create New Admin Profile

Name:

Description:

Permission sets:

	None	Read-Only	Read & Write
Built-in	☐	☐	☐
Account Policy	☐	☐	☐
Administrators	☐	☐	☐
Authentication Monitor	☐	☐	☐
Certificate Management	☐	☐	☐
Local LDAP Service	☐	☐	☐
Logs	☐	☐	☐
Maintenance	☐	☐	☐
Messaging Configuration	☐	☐	☐
Network Configuration	☐	☐	☐
OAuth Service	☐	☐	☐
Portals	☐	☐	☐
RADIUS Accounting	☐	☐	☐
RADIUS Accounting Proxy	☐	☐	☐
RADIUS Services	☐	☐	☐
Remote Administrator	☐	☐	☐
Remote Servers	☐	☐	☐
SAML IdP	☐	☐	☐
SSO Monitor	☐	☐	☐
SSO Settings	☐	☐	☐
Self-Service Replacement Messages	☐	☐	☐
Self-Service Portal	☐	☐	☐
Sponsor	☐	☐	☐
System Administration	☐	☐	☐
TACACS+ Service	☐	☐	☐
Read-Only Users-and-Devices	☐	☐	☒
Websocket Authentication	☐	☐	☐
Widgets	☐	☐	☐

OK Cancel

You successfully added an administrator profile.

+ Create New Delete Permission sets

Successfully deleted 1 admin profile.

☐	Name
☐	Users-and-Devices
☐	Read-only Administrator
☐	Sponsor

3 / 1200 admin profiles

Create an Administrator User

You will create a new administrator user, and assign the **Users-and-Devices** administrator profile you created in the last procedure to this user.

On FortiAuthenticator, an administrator user is a standard user account (local or remote LDAP user) that is flagged as an administrator.

After you assign the **Users-and-Devices** administrator profile to your new administrator user, the account is limited by the permissions associated with that permission set.

To create an administrator user and assign an administrator profile

1. Continuing on the FortiAuthenticator GUI, click **Authentication > User Management > Local Users**, and then on the main pane, click **Create New**.
2. On the **Create New Local User** page, configure the following settings:

Field	Value
Username	admin2
Password creation	Specify a password
Password	fortinet
Password confirmation	fortinet

3. In the **Role** section, configure the following settings:

Field	Value
Role	Administrator
Admin profiles	Click the field, and then select the administrator profile you created: Users-and-Devices.

Ensure **Full permission** is *not* selected. If selected, it would give read and write access to all FortiAuthenticator permissions (that is, the same permissions as the default administrator user). For the purposes of this exercise, access must be limited.

4. Click **OK**.
5. Type the administrative password `password`, and then click **Validate**.
You successfully created an administrator user and assigned an administrator profile.

After the user is created, more user account configuration options become available.

The screenshot shows the 'Edit Local User' window. At the top, a green message bar states: 'The local user "admin2" was added successfully. You must edit it again below.' The 'Username' field contains 'admin2'. Under 'Authentication', 'Password authentication' is selected with a 'Change Password' button. Under 'User Rule', the 'Role' is 'Administrator' and the 'Admin profile' is 'xUsers-and-Devices'. A red box highlights the 'Web service access' section, which includes expandable options for 'User Information', 'Alternative Email Addresses', 'Password Recovery Options', 'Groups', 'Usage Information', 'Email Routing', 'TACACS+', 'Certificate Bindings', 'Devices', and 'RADIUS Attributes'. The 'OK' button is at the bottom right.

6. Click **User Information** to expand the section, and then in the **Email** field, type `admin2@training.lab`.

The screenshot shows the 'User Information' section. The 'Email' field is highlighted with a red box and contains 'admin2@training.lab'. Other fields include 'First name', 'Last name', 'Phone number', 'Mobile number' (with a dropdown for country code and a field for number), 'SMS gateway' (with a dropdown for gateway), 'Street address', 'City', 'State/Province', 'Country' (with a dropdown), 'Language' (with a dropdown), and 'FortiToken Logo' (with a dropdown). A 'Test SMS' button is also visible.

7. Click **OK**.
8. Type the administrative password `password`, and then click **Validate**.

The screenshot shows a password validation dialog. It has a text input field with the placeholder 'Please re-enter your password' and a 'Validate' button.

You successfully created an administrator user, assigned an administrator profile, and configured an email address.

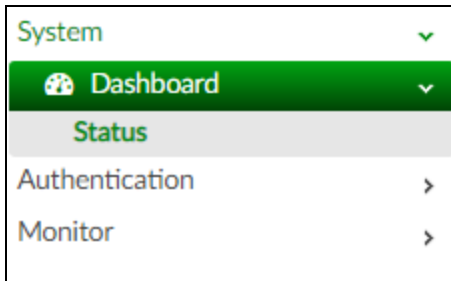
9. In the upper-right corner of the screen, click **admin**, and then select **Logout**.

Test Your Administrator User Permissions

The admin2 account should now be limited by the permission set associated with the **Users-and-Devices** administrator profile. You can test this by logging in as the new administrator user.

To test your administrator user permissions

1. Log in to the FortiAuthenticator GUI with the username `admin2` and password `fortinet`.
Note that the GUI menu items are restricted to those associated with the assigned administrator profile (**Users and Devices** permission set).



2. In the upper-right corner of the screen, click **admin2**, and then select **Logout**.

Exercise 2: Configuring the Mail Server

In this exercise, you will configure FortiAuthenticator to use FortiMail as the new default Simple Mail Transfer Protocol (SMTP) server. FortiAuthenticator sends email for several purposes, such as password reset requests, new user approvals, user self-registration, and two-factor authentication.

Configure the Mail Server

As mentioned in the lesson, by default, FortiAuthenticator uses the built-in SMTP server. This is provided for convenience, but is not necessarily optimal for production environments. Antispam methods, such as IP lookup, DKIM, and SPF, can cause mail from such ad hoc mail servers to be blocked. You should relay email through an official, external mail server for your domain.

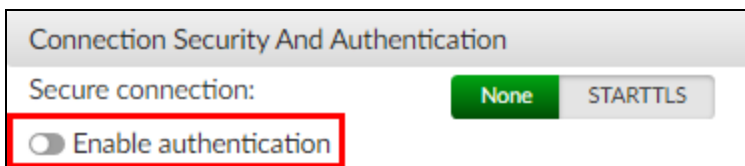
You will configure FortiMail as your mail server. You will use this mail server throughout the labs.

To configure an SMTP server

1. Log in to the FortiAuthenticator GUI with the username `admin` and password `password`.
2. Click **System** > **Messaging** > **SMTP Servers**, and then click **Create New**.
3. On the **Create New SMTP Server** page, configure the following settings:

Field	Value
Name	FortiMail
Server name/IP	10.0.1.100 <i>This is the IP address of FortiMail. For more information, see Network Topology.</i>
Port	25
Sender email address	IT@training.lab

4. In the **Connection Security And Authentication** section, turn off **Enable authentication**.



5. Click **OK**.
You successfully created a new mail server. However, note that the **Local Mail Server** (localhost:25) is still set as the default server.
6. To make your new FortiMail mail server the default server, select the checkbox for the **FortiMail** server, and then click **Set as Default**.

Name	Server	Default
FortiMail	10.0.1.100:25	☒
Local Mail Server	localhost:25	☐

You successfully set the new FortiMail mail server as the default server.

Set Email Services to the FortiMail SMTP Server

Now that you configured FortiMail as your mail server, you must specify that FortiAuthenticator use the FortiMail mail server for both administrators and users.

To set email services to the FortiMail SMTP server

1. Continuing on the FortiAuthenticator GUI, click **System > Messaging > Email Services**.
2. In the SMTP server drop-down list, select **FortiMail (10.0.1.100:25)** for both **Administrators** and **Users**.

Recipient	SMTP Server
Administrators	FortiMail (10.0.1.100:25)
Users	FortiMail (10.0.1.100:25)

3. Click **Save**.

You successfully specified that FortiAuthenticator use the FortiMail mail server for both administrators and users.



The SMTP server drop-down list contains the **Use default server** option, as well as all SMTP servers that were added manually. Because the **FortiMail** server is the default server, this setting was not necessary but demonstrates that you can configure FortiAuthenticator to use a selected server for the associated recipient type.

Lab 3: Administering and Authenticating Users

At this time, there is no lab associated with the *Administering and Authenticating Users* lesson.

Lab 4: User Authentication

In this lab, you will configure and test the self-service portal, and configure FortiGate as a RADIUS client of FortiAuthenticator.

Objectives

- Configure and test the self-service portal
- Configure FortiGate as a RADIUS client of FortiAuthenticator

Time to Complete

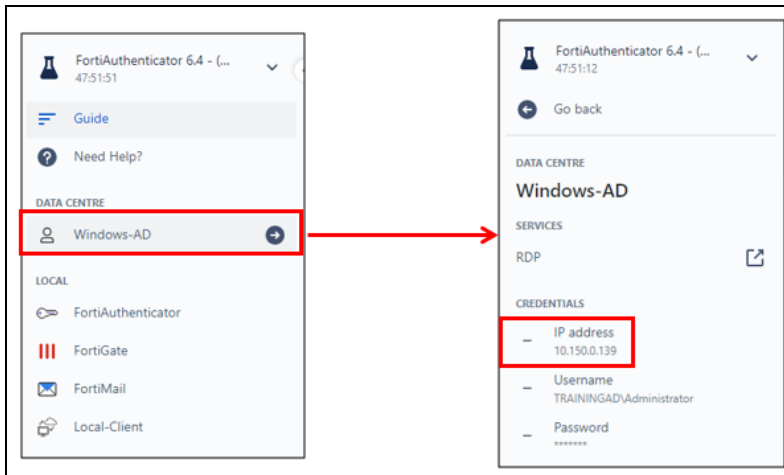
Estimated: 35 minutes

Prerequisites

Before beginning this lab, you must identify the Windows-AD VM IP address.

To identify the Windows-AD VM IP address

1. On the Fortinet Training Institute side bar, click **Windows-AD**.
2. In the **CREDENTIALS** section, under **IP address**, locate and make a note of the IP address. You will use this address where the lab asks for <Windows-AD IP>.



Exercise 1: Configuring and Testing the Self-Service Portal

In this exercise, you will configure and test the self-service portal. As mentioned in the lesson, you can configure the self-service portal to ease the administrative burden on the administrator, specifically in terms of adding new end users to FortiAuthenticator.

Configure the Self-Service Portal

FortiAuthenticator allows you to specify a name for the self-service portal. The name of the portal is used in communications with users who are self-registering. If you do not set a name, emails such as those for self-registrations, appear to be from the device FQDN or IP address instead of the self-service portal name.



You must perform this exercise from the Local-Client VM because of necessary DNS configurations in the lab environment.

To configure the self-service portal

1. On the Local-Client VM, open a browser, and then log in to the FortiAuthenticator GUI with the username `admin` and password `password`.
2. Click **Authentication > Portals > Portals**.
3. Click **Create New**, and then name the portal `TrainingPortal`.
4. In the **Pre-Login Services** section, configure the following settings:

Field	Value
Disclaimer	Enable
Account Registration	Enable

5. Under the account registration option, configure the following settings:

Field	Value
Require administrator approval	Enable
Enable email to freeform addresses	Enable
Administrator email addresses	<code>admin2@training.lab</code>

Field	Value
Password creation	Randomly generated
Account delivery options available to the user	Email

- Under **Required field configurations**, disable **Mobile number**.
- In the **Post-login Services** section, configure the following settings:

Field	Value
Profile	Enable Enable View and Edit
Password Change	Enable Local user
Token Registration	Enable Allow Fido token registration

- Click **OK**.

Create a Self-Service Portal Policy

Self-service portal policies determine the portal that is presented to a user.

To create a self-service portal policy

- Continuing on the FortiAuthenticator GUI, click **Authentication > Portals > Policies**.
- In the upper-right corner, click **Self-Service Portal**.



- Click **Create New**, and then in the **Policy type** view, configure the following settings:

Field	Value
Name	TrainingLab
Portal	TrainingPortal

- Click **Next**.
- In the **Identity sources** view, keep the default settings, and then click **Next**.

6. In the **Authentication factors** view, leave **All configured password and OTP factors** enabled, and then enable **FIDO authentication** and select the **FIDO token only**.
7. Click **Save and exit**.

Modify the Replacement Message

Based on your self-registration configuration, you must modify the default automatic message that is sent to users. The default message requires users to enter a password during self-registration. However, you set passwords to be randomly generated during the self-registration configuration in the previous exercise, so you must remove the password field in the replacement message.

To modify the replacement message

1. Continuing on the FortiAuthenticator GUI, click **Authentication > Portals > Replacement Messages**.
2. Click **TrainingPortal** to edit the messages for that portal.
3. Scroll to the **User Registration** section, and then select **Approved User Email Message**.
4. In the pane on the far-right, change `{{:email_signature}}` to the following:

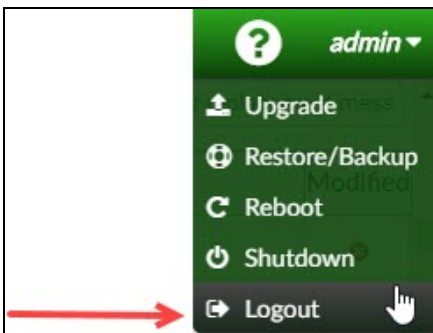
```
Please login and change your password here:  
https://fac.trainingad.training.lab/portal/selfservice/TrainingLab/
```

```
The IT team
```

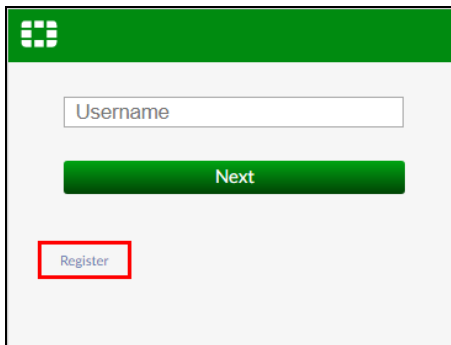
After you update the message, the left pane should look like the following example:

```
Welcome to fortinet.com, john!  
  
Your login information:  
Username: john  
Password: *****  
  
Please login and change your password Here:  
https://fac.trainingad.training.lab/portal/selfservice/TrainingLab/  
  
The IT team
```

5. Click **Save**.
6. Click **Authentication > Portals > Policies**, and then click **TrainingLab** to access the policy.
7. Click the **Copy url** icon  to copy the URL.
8. In the upper-right corner, click **admin**, and then select **Logout**.



9. Open a new browser tab, paste the portal URL, and then press **Enter**, or use the existing bookmark, to access the self-service portal.
The disclaimer screen opens.
10. Click **Yes, I agree**.
The login screen opens with a **Register** link for self-registration. Users use this link to self-register.



Perform a Self-Registration

Now that you have configured the self-service portal, you will test it by registering as an end user.

To self-register as an end user

1. On the FortiAuthenticator login screen, click the **Register** link.
2. On the registration page that opens, type the following information:

Field	Value
Username	student
First name	Student
Last name	User
Email address	student@training.lab
Confirm email address	student@training.lab

3. Click **Submit**.
A success page opens.

Registration Successful
Your information has been sent to the administrator for approval. You will receive an email once your account has been approved and activated.
[Go back to the login page](#)

Because you specified earlier that `admin2` must approve self-registrations, you must check the `admin2` email address and approve the self-registration.

Approve the Self-Registration Request

Because you configured the self-service portal to require administrator approval for user self-registrations, you will approve the user self-registration as an administrator. To approve the registration by email, log in to the FortiMail webmail GUI as `admin2`, view the email, and then accept the registration.

To approve a user self-registration as an administrator

1. Open a new browser tab, and then log in to the FortiMail webmail GUI with the username `admin2` and password `fortinet`.
2. Open the email from `IT@training.lab`.

User "student" has just registered and is waiting for approval.
Please go to the following link to approve or deny this user:
<https://fac.trainingad.training.lab/auth/register/3/approve/>

3. Follow the instructions in the email.
The **New User Approval** page opens.

New User Approval
Please review the following user information. You can approve or deny this user.

Username:	student
First name:	Student
Last name:	User
Email address:	student@training.lab
Address:	
City:	
State/Province:	
Country:	
Phone number:	
Mobile number:	

4. Review the content in the request, and then click **Approve**.
You successfully approved a self-registration request.

User registration complete
User "student" has been activated.

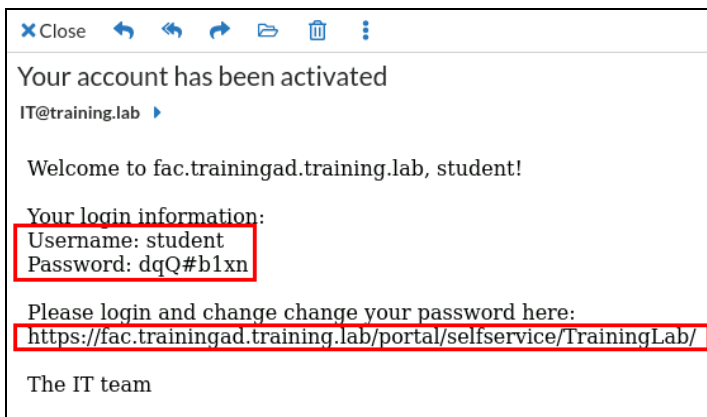
5. Close this tab, and then log out of FortiMail as `admin2`.

Complete the Self-Registration

After the administrator has approved the end-user self-registration request, the end user can complete the self-registration. You will complete the student registration and access the self-service portal.

To complete the self-registration as the student user

1. Log in to the FortiMail webmail GUI with the username `student` and password `fortinet`.
2. Open the email from `IT@training.lab`.



A few things to note are:

- The email welcomes the user to the **training.lab** and is signed by **The IT team**. These are the self-service portal settings you configured at the beginning of this exercise.
 - The password is randomly assigned. This is because when you configured self-registration, you set password generation to **Randomly generated**.
3. Copy the password.
 4. Highlight the link, right-click it, and then select **Open Link in New Tab**.
 5. At the login prompt, type the username `student`, and then click **Next**.
 6. In the **Password** field, paste the password you copied from the email, and then click **Login**.

The self-service portal page opens.



- Click **Password**, and then configure the following settings:

Field	Value
Old password	<randomly generated password in email>
New password	fortinet
Confirm new password	fortinet

- Click **OK**.
You successfully changed your password and are now registered.
- Log in again to validate the password change.
- Close all browser tabs to complete the exercise.

Exercise 2: Configuring FortiGate as a RADIUS Client of FortiAuthenticator

In this exercise, you will set up FortiGate as a RADIUS client of FortiAuthenticator. You will also set up Active Directory (AD) authentication on FortiAuthenticator. After you complete the configuration, you will test it.

The use case is an administrator account logging in to FortiGate using RADIUS and AD/LDAP authentication.

Configure the RADIUS Server on FortiGate

You will configure FortiAuthenticator as a remote RADIUS server on FortiGate.

To configure FortiAuthenticator as a RADIUS server on FortiGate

1. Log in to the FortiGate GUI with the username `admin` and password `password`.
2. Click **User & Authentication** > **RADIUS Servers**, and then click **Create New**.
3. Configure the following settings:

Field	Value
Name	FortiAuth-RADIUS
IP/Name	10.0.1.150 This is the IP address of FortiAuthenticator. For more information, see Network Topology on page 7 .
Secret	fortinet

4. Keep the default values for all other parameters, and then click **OK** to create the RADIUS server.



Attempting to test connectivity or user credentials at this time results in a failure. This is because you have not yet configured FortiGate as a RADIUS client on FortiAuthenticator.

Create a Firewall User Group for Remote Administrators

Firewall user groups are used locally as part of authentication. When a security policy allows access only to specified user groups, users must authenticate. If a user authenticates successfully, and is a member of one of the permitted groups, the session is allowed to proceed.

To create a firewall user group for remote administrators

1. Continuing on the FortiGate GUI, click **User & Authentication > User Groups**, and then click **Create New**.
2. On the **New User Group** page, configure the following settings:

Field	Value
Name	Remote-AD-admins
Type	Firewall

3. In the **Remote groups** section, click **Add**, and then configure the following settings:

Field	Value
Remote Server	FortiAuth-RADIUS This is the RADIUS server you configured in the previous procedure.
Groups	Specify Remote-AD-admins <i>The group name is case sensitive.</i>

4. Click **OK**.
5. Click **OK**.

Create a Wildcard Administrator User

When you use RADIUS authentication, you can use a wildcard administrator to allow multiple administrator accounts on RADIUS to use a single account on FortiGate. When you use the GUI, the wildcard administrator is the only type of remote administrator account that does not require you to designate a password during account creation. This password is normally used when the remote authentication server is unavailable during authentication. The benefit in this lab is fast configuration.

To create a wildcard administrator user

1. Continuing on the FortiGate GUI, click **System > Administrators**, click **Create New**, and then select **Administrator**.
2. On the **New Administrator** page, configure the following settings:

Field	Value
Username	*
Type	Match all users in a remote server group
Administrator Profile	super_admin
Remote User Group	Remote-AD-admins

3. Keep the remaining default settings, and then click **OK**.
4. Log out of the FortiGate GUI.

Configure a Remote AD/LDAP Server on FortiAuthenticator

In this environment, an LDAP server with Active Directory has been configured for you. As a result, FortiAuthenticator can connect to it for remote authentication, much like FortiOS remote authentication.

You will configure FortiAuthenticator to connect to the LDAP server.



Do not change or release the IP address of the Windows-AD VM for any reason—doing so will make your lab environment unusable.

To configure a remote AD/LDAP server on FortiAuthenticator

1. Log in to the FortiAuthenticator GUI with the username `admin` and password `password`.
2. Click **Authentication > Remote Auth. Servers > LDAP**, and then click **Create New**.
3. On the **Create New LDAP Server** page, configure the following settings:

Field	Value
Name	ADserver
Primary server name/IP	<Windows-AD IP> This is the IP address of the Windows-AD server. For more information, see the prerequisites at the beginning of this lab.
Base distinguished name	ou=training,dc=trainingAD,dc=training,dc=lab This is the domain name for Active Directory on the Windows-AD server. Active Directory has already been preconfigured, with all users located in the Training organizational unit (ou).
Bind type	Regular
Username	cn=ADadmin,cn=users,dc=trainingAD,dc=training,dc=lab You are using the credentials of an Active Directory user called ADadmin to authenticate to Active Directory. ADadmin is located in the Users organizational unit (ou).
Password	Training! This is the password preconfigured for the ADadmin user. You must use it to be able to bind.

4. Click **OK**.

Create an Authentication Realm

As mentioned in the lesson, realms allow multiple domains to authenticate on a single FortiAuthenticator device. Each RADIUS realm is associated with a name, such as a domain or company name, that is used during the login process to indicate the remote (or local) authentication server on which the user resides. FortiAuthenticator uses the specified realm to identify the back-end RADIUS or LDAP authentication server (or servers) that are used to authenticate the user.

You will create an authentication realm for the Active Directory server.

To create an authentication realm

1. Continuing on the FortiAuthenticator GUI, click **Authentication > User Management > Realms**, and then click **Create New**.
2. On the **Create New Realm** page, configure the following settings:

Field	Value
Name	Realm-ADserver
User source	ADserver (<Windows-AD IP> (for example, 10.150.0.60))

3. Click **OK**.

Import Active Directory Users

You will import Active Directory users into FortiAuthenticator. These users have been preconfigured for you.

To import Active Directory users

1. Continuing on the FortiAuthenticator GUI, click **Authentication > User Management > Remote Users**, and then click **Import**.
2. On the **Import Remote LDAP Users** page, configure the following settings:

Field	Value
Remote LDAP server	ADserver (<Windows-AD IP>) (for example, 10.150.0.60)
Action	Import users

3. Click **Go**.
4. In the **Import Remote LDAP Users** dialog box, select the two Active Directory users: **CN=aduser1** and **CN=aduser2**.
These users were preconfigured in Active Directory for the purposes of this lab.
5. Click **OK**.

✔ Successfully added 2 selected remote LDAP users from "ADserver (10.150.0.47)"					
☐	Username	Remote LDAP Server	Admin	Status	Token
☐	aduser1	ADserver (10.150.0.47)			
☐	aduser2	ADserver (10.150.0.47)			
2 / 100 remote LDAP users					

You successfully imported Active Directory users.

Create a Remote LDAP User Group and Add a User

You will create a user group for remote LDAP users and add **aduser1** to this group.

To create a remote LDAP user group and add a user

- Continuing on the FortiAuthenticator GUI, click **Authentication > User Management > User Groups**, and then click **Create New**.
- On the **Create New User Group** page, configure the following settings:

Field	Value
Name	Firewall Admin
Type	Remote LDAP
User retrieval	Set a list of imported remote LDAP users
Remote LDAP	ADserver (Windows-AD IP) (for example, 10.150.0.60)

- In the **LDAP users** section, click in the **search** box, and then select **aduser1**.

Create New User Group

Name:

Firewall Admin

type:

Local

Remote LDAP

Remote RADIUS

Remote SAML

MAC

User retrieval:

☐ Specify an LDAP Filter

☒ Set a list of imported remote LDAP users

Remote LDAP:

ADserver (10.0.1.0)

LDAP users:

search

x aduser1

Remove all

☐ Usage Profile

[Please select]

TACACS+ authorization rules:

[Please Select]

RADIUS Attributes

OK

Cancel

- Click **OK**.

Link RADIUS Attributes to a Group

You will add RADIUS attributes to the **Firewall Admin** group. This allows the RADIUS client to receive information about the users through vendor-specific attributes. When a RADIUS user successfully authenticates, FortiAuthenticator sends the users' RADIUS attributes and values to the RADIUS client.

To link RADIUS attributes to a group

1. Continuing on the FortiAuthenticator GUI, click the **Firewall Admin** group you created in the previous procedure, and then in the **RADIUS Attributes** section, click **Add Attribute**.
2. In the **RADIUS Attributes** section, configure the following settings:

Field	Value
Vendor	Fortinet
Attribute ID	Fortinet-Group-Name
Value	Remote-AD-admins The attribute has to exactly match what has been specified in the FortiGate Group. <i>This is case sensitive.</i>

3. Click **OK**.

Configure FortiGate as a RADIUS Client of FortiAuthenticator

You will configure FortiGate as a RADIUS client of FortiAuthenticator. In doing this, FortiAuthenticator will answer only to this specific RADIUS client (or any additional RADIUS clients you may add).

To configure FortiGate as a RADIUS client of FortiAuthenticator

1. Continuing on the FortiAuthenticator GUI, click **Authentication > RADIUS Service > Clients**, and then click **Create New**.
2. On the **Create New Authentication Client** page, configure the following settings:

Field	Value
Name	FortiGate
Client address	10.0.1.254 This is the IP address of FortiGate. For more information, see Network Topology on page 7 .
Secret	fortinet

3. Click **OK**.

Configure a RADIUS Service Policy

You will create a RADIUS service policy that defines how FortiAuthenticator responds to RADIUS requests. RADIUS service policies allow you to customize how RADIUS responses are processed for different RADIUS clients.

To configure a RADIUS service policy

1. Continuing on the FortiAuthenticator GUI, click **Authentication > RADIUS Service > Policies**, and then click **Create New**.
2. In the **RADIUS clients** settings, name the policy `FortiGate_Default`.
3. In the **RADIUS clients** section, under **Available RADIUS Clients**, select **FortiGate (10.0.1.254)**, and then use the forward arrow to move it under **Chosen RADIUS Clients**.
4. Click **Next**, and then leave all settings at the default values until you reach the **Identity source** settings.
5. In the **Realms** section, do the following:
 - a. In the **Realm** column, select **realm-adserver | ADserver (<Windows-AD IP>)**.
 - b. In the **Groups** column, enable **Filter**, and then click the edit icon.



Because of limitations in the lab environment, the edit pop-up window may not be scaled properly (it may be out of the window). Workaround: Make the screen full size, zoom out to configure it, and then click **OK**.

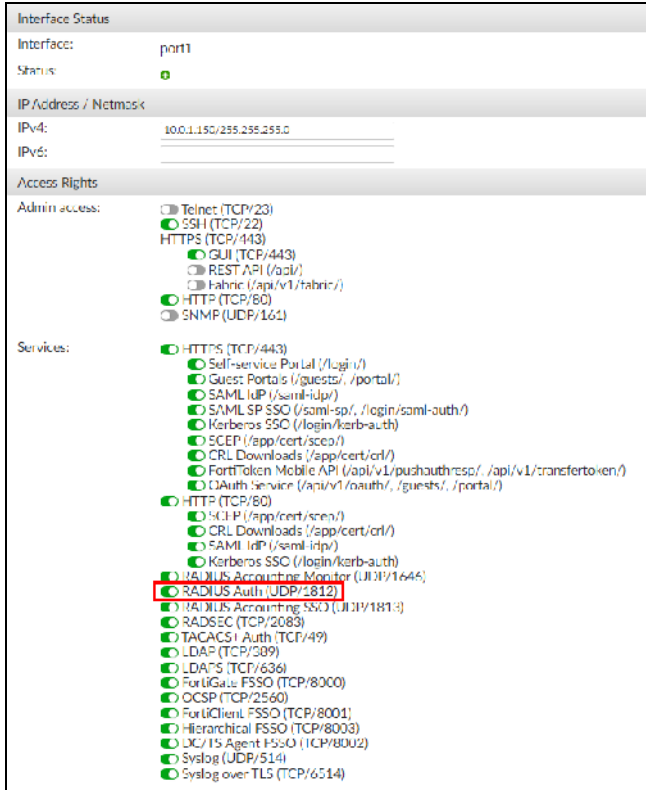
- c. Move the **Firewall Admin** group from **Available User Groups** to **Chosen User Groups**, and then click **OK**.
- d. Keep the default values for all other parameters, click **Next** until you get to the **RADIUS response** settings, and then click **Save and exit**.

Enable the RADIUS Service

You must enable the RADIUS service on FortiAuthenticator in order to authenticate using the RADIUS database. While this is enabled by default, it is a good idea to verify that it is enabled.

To enable the RADIUS service

1. Continuing on the FortiAuthenticator GUI, click **System > Network > Interfaces**, and then click the **port1** interface to view and edit it.
2. In the **Access Rights > Services** section, make sure that **RADIUS Auth (UDP/1812)** is enabled.



3. Click **OK**.

To test FortiGate as a RADIUS client of FortiAuthenticator and Active Directory authentication on FortiAuthenticator

1. Log in to the FortiGate GUI with the username `aduser1` and password `Training!`.
2. Click **Dashboard > Status**, and then locate the **Administrators** widget.
You should see `aduser1` listed as a **super_admin**.
3. Click `aduser1`, and then select **Show active administrator sessions**.
You will see more details about the administrative session.
4. Return to the FortiAuthenticator GUI, which you are logged in to as **admin**.
5. Click **Logging > Log Access > Logs**, and then look for a successful authentication from a remote LDAP user.
6. Click the log entry to open the **Log Details** window, and then examine the log details.

Log Details	
Log Record Detail	
ID	649
Timestamp	Fri Mar 18 14:14:25 2022
Level	Information
Action	Authentication
Status	Success
Source IP	10.0.1.254
Message	Remote LDAP user authentication with no token successful
User	aduser1
Log Type	
Type ID	20001
Name	Authentication OK No FTK
Sub Category	Authentication
Category	Event
Description	Authentication successful without Forti token

7. Return to the browser tab with the FortiGate GUI, log out, and then log in again with the username `aduser2` and password `password`.

This user was not added to the **Firewall Admin** group and therefore should not be allowed to authenticate.

Authentication failure

Login

8. Return to the browser tab with the FortiAuthenticator GUI, and then refresh the **Logs** page. You should see several authentication failed messages.

ID	Timestamp	Short Message	Level	Category	Sub Category	Log Type ID	Action	Status	User	Source IP
653	Fri Mar 18 14:19:...	Remote LDAP user authentication fail...	Information	Event	Authentication	20101	Authenticati...	Failed	aduser2	10.0.1.254
652	Fri Mar 18 14:19:...	Remote LDAP user authentication fail...	Information	Event	Authentication	20102	Authenticati...	Failed	aduser2	10.0.1.254
651	Fri Mar 18 14:19:...	Remote LDAP user authentication fail...	Information	Event	Authentication	20102	Authenticati...	Failed	aduser2	10.0.1.254
650	Fri Mar 18 14:19:...	Remote LDAP user authentication with...	Information	Event	Authentication	20102	Authenticati...	Failed	aduser2	10.0.1.254

9. Optionally, you can see the group's RADIUS Attribute being added and sent back from FortiAuthenticator through the FortiGate CLI:

a. Connect to FortiGate using SSH

b. Enter the following command:

```
diagnose test authserver radius <RADIUS server name> pap <ad admin user> <password>
```

Where:

- <RADIUS server name> is `FortiAuth-RADIUS`
- <ad admin user> is `aduser1`

- <password> is Training!

You should see something like the following example:

```
authenticate 'aduser1' against 'pap' succeeded, server=primary assigned_rad_session_  
id=810153440 session_timeout=0 secs!  
Group membership(s) - remote-AD-admins
```

If you are getting a successful authentication on FortiAuthenticator, but a `permission denied` error, then check your group attributes and FortiGate settings.

10. Log out of the SSH session.

Lab 5: Two-Factor Authentication

In this lab, you will configure a user for two-factor authentication, and then you will log in to the self-service portal using FortiToken Windows for two-factor authentication.

Objectives

- Create and assign a FortiToken Mobile token
- Test two-factor authentication

Time to Complete

Estimated: 20 minutes

Exercise 1: Creating and Assigning a FortiToken Mobile Token

In this lab, you will obtain two free FortiToken Mobile tokens, assign a token to a user, enforce two-factor authentication, and validate the configuration.

Obtain the Two Free FortiToken Mobile Tokens

Each FortiAuthenticator comes with two free FortiToken Mobile tokens. However, because all students are working on FortiAuthenticator VMs that are cloned from a master VM, the serial numbers of the FortiToken Mobile tokens are the same on each VM. Because FortiAuthenticator verifies the activation of tokens with FortiGuard, after one student activates the token, no other students can activate the token. The same token serial number cannot be activated more than once.

To prevent this from happening, each student must delete the existing FortiToken Mobile tokens, and then get new ones. This way, each student will be randomly assigned a new serial number and there will be no conflicts.



This exercise is also relevant in a real-world scenario. This procedure is required, for example, if you're upgrading an unlicensed FortiAuthenticator to a licensed one, because the old tokens associated with the unlicensed serial number won't be compatible with the new, licensed serial number. The tokens will still work, and you won't be able to reassign them to a new user. In this case, you must delete the old tokens, and then generate new ones.

To delete and create new FortiToken Mobile tokens

1. Log in to the FortiAuthenticator GUI with the username `admin` and password `password`.
2. Click **Authentication > User Management > FortiTokens**.
3. Select the existing FortiToken Mobile tokens, click **Delete**, and then when you are prompted to confirm that you want to delete them, click **Yes, I'm sure**.
4. Click **Create New** to obtain the two free FortiToken Mobile trial tokens.
5. On the **Create New FortiToken** page, complete the following:
 - a. In the **Token type** field, select **FortiToken Mobile**.
 - b. Enable **Get FortiToken Mobile free trial tokens**.
 - c. Click **OK**.

You successfully obtained the FortiToken Mobile trial tokens. Your token serial numbers are now different from the token serial numbers of the other students in your lab.

6. Optionally, you can click the token to add a comment to the token.
For example, you can click the token you are going to assign to the student user later, and then type a comment such as `For student user`.

If you want to assign a specific token to the student user, you should make a note of the serial number of the token now (the last three digits are sufficient).

Assign a Token to a User

Now that you have unique FortiToken Mobile tokens available, you can assign one to a user. You will assign a token to the student user.

To assign a FortiToken Mobile token to the student user

1. Continuing on the FortiAuthenticator GUI, click **Authentication > User Management > Local Users**, and then edit the **student** user.
2. Enable **One-Time Password (OTP) authentication**, select **FortiToken** to deliver the token code using FortiToken, and then select **Mobile**.
3. In the **Token** drop-down list, select one of the FortiToken Mobile tokens.
If you added a comment to one of the tokens earlier because you wanted to use that one for testing, ensure you assign that token to the student user.
4. In the **Activation Delivery method** field, select **Email**.
5. Click **OK**.

You successfully assigned a FortiToken Mobile token to a user for two-factor authentication.

Activate the FortiToken Mobile Token

When you assigned the token to the student user, an email containing activation instructions, including the activation code, was automatically sent to the student. You will log in to the FortiMail webmail GUI as the student user to access the activation instructions and activation code.

To activate the FortiToken Mobile token

1. Log in to the FortiMail webmail GUI with the username `student` and password `fortinet`.
2. Open the new email from `IT@training.lab`.

Hello student, welcome to FortiToken Mobile - One-Time-Password software token.

Please visit <https://docs.fortinet.com/product/fortitoken/> for instructions on how to install your FortiToken Mobile application on your device and to activate your token.

Activation Code for FortiToken Mobile FTKMO [REDACTED], which you will need to enter on your device later, is

"EEIM4QFW [REDACTED]" ← **Activation code**

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, May 20, 2022 10:28 PDT, after which you will need to contact your system administrator to re-enable your activation.

3. Access the Windows-AD VM.
4. From the task bar, open the FortiToken application.



5. On the bottom of the FortiToken application window, click **Add**.
6. In the **Add Account** page, configure the following settings:

Field	Value
Account Name	Student Token
Key	Activation code from email
Category (Fortinet or 3rd party)	Fortinet

7. Click **Done**.
8. In the **Set PIN** page, enter and confirm a PIN of 1111, and then click **Done**.
You are now ready to test two-factor authentication using FortiToken Mobile.

Exercise 2: Testing Two-Factor Authentication

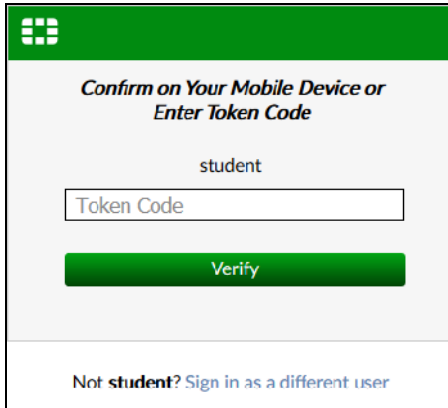
In this exercise, you will test logging in, using your two-factor authentication mechanism, as the student user.



You must perform this exercise from the Local-Client VM and Windows-AD VM.

To log in using two-factor authentication

1. On the Local-Client VM, open a browser, and then access the self-service portal.
2. Click **Yes, I agree**, and then log in with the username `student` and password `fortinet`.
The second-factor login window opens and prompts you to enter your token code.



3. On the Windows-AD VM, use the **Student Token** code from FortiToken to complete the log in to the self-service portal.
4. If the FortiToken application was closed, open the application, and then enter the PIN (1111).
5. Type the token code, and then click **Verify**.
The self-service portal loads.
6. Log out of the self-service portal, and then close the browser.

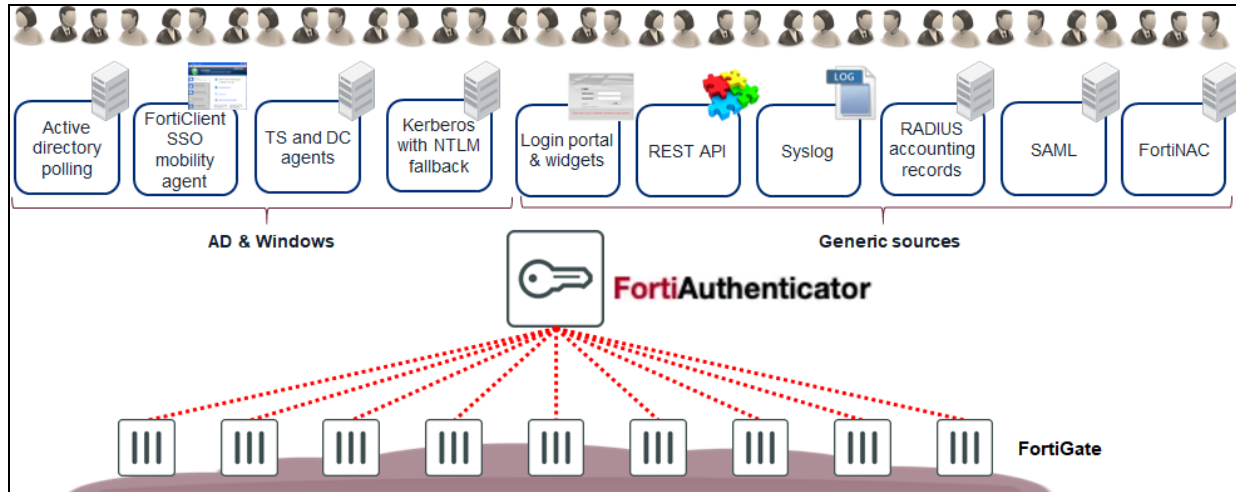
Lab 6: FSSO Process and Methods

At this time, there is no lab associated with the *FSSO Process and Methods* lesson.

Lab 7: Fortinet Single Sign-On

In this lab, you will examine how to configure three Fortinet single sign-on (FSSO) methods:

- RADIUS accounting
- Manual portal authentication
- DC polling



Objectives

- Prepare FortiGate and FortiAuthenticator for FSSO
- Configure RADIUS accounting
- Configure manual portal authentication
- Configure domain controller (DC) polling (event log polling)
- Configure FortiClient SSO Mobility Agent

Time to Complete

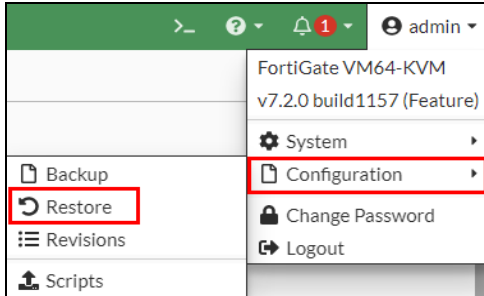
Estimated: 35 minutes

Prerequisites

Before beginning this lab, you must restore a configuration file to FortiGate, and note the IP addresses of the Windows-AD VM and the POD.

To restore the FortiGate configuration file

1. Log in to the Local-Client VM and open a browser.
2. Log in to the FortiGate GUI with the username `admin` and password `password`.
3. In the upper-right corner of the screen, click **admin**, and then click **Configuration > Restore**.

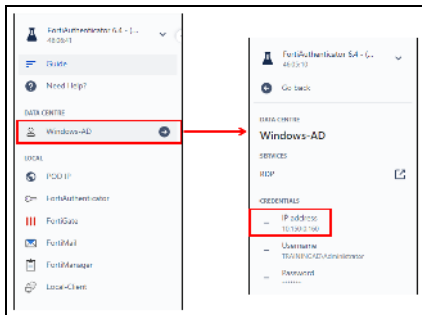


4. Click **Local PC**, and then click **Upload**.
5. Click **Desktop > Resources > FortiAuthenticator > LAB-7 > FortiGate_Lab-7.conf**, and then click **Select**.
6. Click **OK**.
7. Click **OK** to reboot.

This lab includes authenticating with a second-factor method through SSL-VPN, so you must configure the VPN settings on FortiGate. Because configuring VPN is out of scope for this lab, the configuration file includes the required VPN settings.

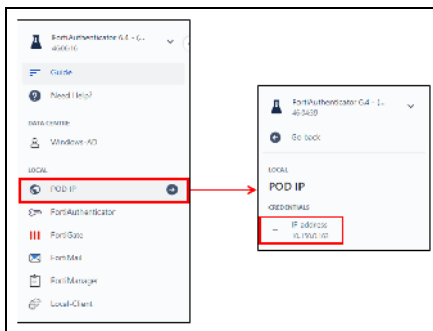
To identify the Windows-AD VM IP address

1. On the Fortinet Training Institute side bar, click **Windows-AD**.
2. Locate and note the IP address in the **CREDENTIALS** section, under **IP address**.
You will use this address where the lab asks for <Windows-AD IP>.



To identify the POD IP address

1. On the Fortinet Training Institute side bar, click **POD IP**.
2. Locate and note the IP address in the **CREDENTIALS** section, under **IP address**.
You will use this address where the lab asks for <POD IP address>.



To update the Windows-AD VM IP address



DO NOT perform these steps if you are taking an instructor-led class. This is only required if you are taking the self-paced labs.

1. Log in to the FortiAuthenticator GUI with the username `admin` and password `password`.
2. Click **Authentication > Remote Auth. Servers > LDAP**, and then edit the existing **ADserver** entry.
3. Update the **Primary server name/IP** field to match the Windows-AD VM IP address.

Edit LDAP Server

Name: `ADserver`

Primary server name/IP: `10.150.0.160` Port: `389`

☐ Use secondary server

Base distinguished name: `ou=training,dc=trainingAD,dc=training,dc=lab` [Browse](#)

Bind type: ☐ Simple ☒ Regular

Username: `cn=ADadmin,cn=users,dc=trainingAD` Password: `*****`

Server type: ☒ Microsoft Active Directory ☐ OpenLDAP/GSuite ☐ Novell eDirectory/Other [Apply template](#)

☐ Add supported domain names (used only if this is not a Windows Active Directory server)

4. Click **OK**.

Exercise 1: Preparing FortiGate and FortiAuthenticator for FSSO

Before you start working on each of the FSSO methods, you will examine how to enable some FSSO features on FortiGate and FortiAuthenticator.

Create an FSSO Agent

In this procedure, you will create an FSSO agent on FortiGate. You must configure every FortiGate that uses FortiAuthenticator to provide single sign-on authentication to use FortiAuthenticator as an SSO server.

To create an FSSO agent

1. Log in to the FortiGate GUI with the username `admin` and password `password`.
2. Click **Security Fabric > External Connectors**, and then select **Create New**.
3. Under **Endpoint/Identity**, select **FSSO Agent on Windows AD**.
4. Configure the following settings:

Field	Value
Name	FortiAuth-SSO
Primary FSSO Agent IP/Name	10.0.1.150 (This is the IP address of FortiAuthenticator.)
Password	fortinet (This is the same secret key you will later define on FortiAuthenticator.)

5. Keep the remaining settings, and click **OK**.

Create an FSSO User Group

In this procedure, you will create an FSSO user group on FortiGate.

When a user tries to access network resources, FortiGate selects the appropriate security policy for the destination. The selection consists of matching the FSSO group the user belongs to with the security policy that matches that group. If the user belongs to one of the permitted user groups associated with that policy, FortiGate allows the connection. Otherwise, FortiGate denies the connection.

In this procedure, you will create an FSSO user group. Later in this exercise, you will add members to this group.

To create an FSSO user group

1. Continuing on the FortiGate GUI, click **User & Authentication > User Groups**, and then click **Create New**.
2. Configure the following settings:

Field	Value
Name	FortiAuth-FSSO-Group
Type	Fortinet Single Sign-On (FSSO)

3. Click **OK**.

Enable FortiGate SSO Authentication

In this procedure, you will enable FortiGate SSO authentication on FortiAuthenticator. This allows FortiAuthenticator to listen for requests from authentication clients.

To enable FortiGate SSO authentication

1. Log in to the FortiAuthenticator GUI with the username `admin` and password `password`.
2. Click **Fortinet SSO Methods > SSO > General**.
3. In the **FortiGate** section, make sure the **Enable authentication** option is enabled, and then set the secret key to `fortinet`.
4. In the **Fortinet Single Sign-On (FSSO)** section, change **Log level** to **Debug**. This will help with troubleshooting if this lab is unsuccessful.
5. Click **OK**.

Create a FortiGate Filter

In order to provide FSSO only to specific groups on a remote LDAP server, you can filter the polling information so that it includes only those groups.

Complete the following procedure to filter on the AD group CN=AD-users.

To create a FortiGate filter

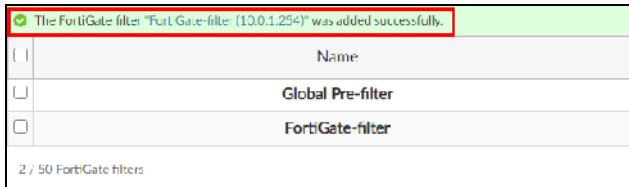
1. Continuing on the FortiAuthenticator GUI, click **Fortinet SSO Methods > SSO > FortiGate Filtering**, and then click **Create New**.
2. Configure the following settings:

Field	Value
Name	FortiGate-filter
FortiGate name/IP	10.0.1.254 (This is the FortiGate IP address.)

3. In the **Fortinet Single Sign-On (FSSO)** section, enable **Forward FSSO information for users from the following subset of users/groups/containers only**.
4. Click **Add Filtering Object**, and then configure the following settings:

Field	Value
Name	CN=AD-users,OU=Training,DC=TrainingAD,DC=training,DC=lab
Object Type	Group

- Click **OK**.



This configuration means that only this AD group will be pushed down to FortiGate as part of the FSSO information feed.

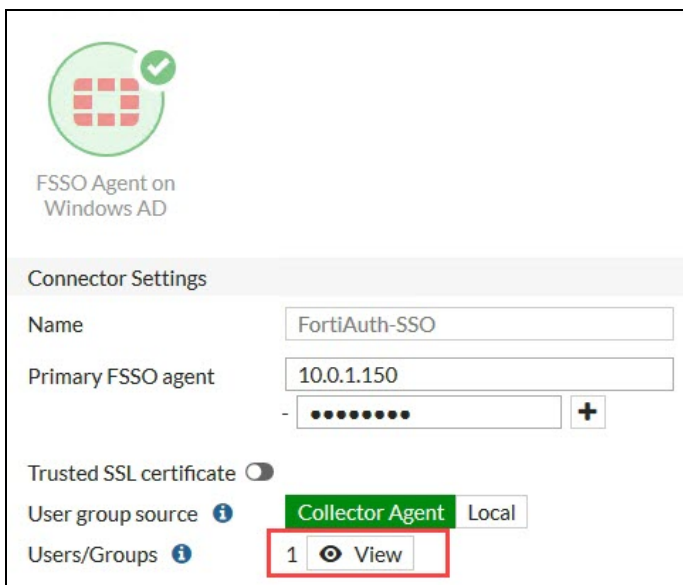
Add the FortiAuthenticator SSO Group to the FortiGate FSSO Agent

In this procedure, you will add the FortiAuthenticator SSO group (composed of the AD users you imported into the group) to the FSSO agent you created on FortiGate at the beginning of this exercise.

This allows FortiGate to receive a list of user groups from FortiAuthenticator (in this case, it is the FortiAuthenticator SSO group). When you open the server, you can see the configured group and, as with all configured groups, you can use it in firewall policies.

To add the AD user group to the FSSO agent

- Return to the browser tab that is running the FortiGate GUI.
- Click **Security Fabric > External Connectors**, and then edit **FortiAuth-SSO**.
- Click **Apply & Refresh**.
- Click the **View** button next to **Users/Groups**.



The single sign-on server settings should look the same as the following example:

Collector Agent Group Filters			
Delete Search			
	AD Group	User Groups	Ref.
	 CN=AD-USERS,OU=TRAINING,DC=TRAININGAD,DC=TRAINING,DC=LAB		

You are now ready to start configuring the three different FSSO methods.

Exercise 2: Configuring RADIUS Accounting

In this exercise, you will examine how to configure SSO based on RADIUS accounting records. FortiAuthenticator will receive RADIUS accounting packets from the RADIUS client (which you have already configured), collect additional group information, and then insert the information into FSSO to be used by FortiGate for firewall policies.

Then, you will test the configuration by logging in to SSL-VPN as aduser1. The SSL-VPN log in sends a RADIUS accounting packet from FortiGate to FortiAuthenticator every time a user successfully authenticates. RADIUS accounting and VPN are used only for generating FSSO logging events.

Configure FortiGate as a RADIUS Accounting Client

In this procedure, you will configure FortiGate as a RADIUS accounting client of FortiAuthenticator.

To configure FortiGate as a RADIUS accounting client

1. Log in to the FortiAuthenticator GUI with the username `admin` and password `password`.
2. Click **Fortinet SSO Methods > SSO > RADIUS Accounting Sources**, and then click **Create New**.
3. Configure the following settings:

Field	Value
Name	FortiGate
Client name/IP	10.0.1.254
Secret	fortinet
SSO user type	Remote users
Remote LDAP server	ADserver (<Windows-AD IP>) (for example, 10.150.0.60)

4. In the **RADIUS Attributes** section, make sure that the **Client IPv4 attribute** is set to **Calling-Station Id**.

RADIUS Attributes			
Username attribute:	User-Name	Browse	Default
Client IPv4 attribute:	Calling-Station-Id	Browse	Default
Client IPv6 attribute:	Framed-IPv6-Address	Browse	Default
User group attribute:	Fortinet-Group-Name	Browse	Default

5. Click **OK**.

Enable RADIUS Accounting SSO Clients

In this procedure, you will enable FortiAuthenticator to receive RADIUS accounting packets for FSSO.

To enable RADIUS accounting

1. Continuing on the FortiAuthenticator GUI, click **Fortinet SSO Methods > SSO > General**.
2. In the **Fortinet Single Sign-On (FSSO)** section, select **Enable RADIUS Accounting SSO clients**.

Fortinet Single Sign-On (FSSO)

Maximum concurrent user sessions: [Configure Per User/Group]

Log level: Error Warning Info Debug [Configure Log Filter]

☐ Enable Windows event log polling (e.g. domain controllers/Exchange servers)

☐ Enable FortiNAC SSO

☒ **Enable RADIUS Accounting SSO clients**

☐ Enable Syslog SSO [Configure syslog sources]

☐ Enable FortiClient SSO Mobility Agent Service

☐ Enable hierarchical FSSO tiering

☐ Enable DC/TS Agent Clients

3. Click **OK**.

Configure FortiAuthenticator as the RADIUS Accounting Server

Finally, you need to configure the RADIUS accounting server on FortiGate. This is configured on the CLI.

To configure FortiAuthenticator as the RADIUS accounting server

1. Open an SSH connection to the FortiGate.
2. Type the following commands:

The CLI commands are located on the Local-Client VM. Click **Desktop > Resources > FortiAuthenticator > Lab-7**, and then open the `FortiGate-RADIUS-config` text file. You can also copy and paste the commands. The first section should already be there.

```
config user radius
  edit "FortiAuth-RADIUS"
    set server "10.0.1.150"
    set secret fortinet
    set acct-interim-interval 600
config accounting-server
  edit 1
    set status enable
    set server "10.0.1.150"
    set secret fortinet
  next
end
next
end
```

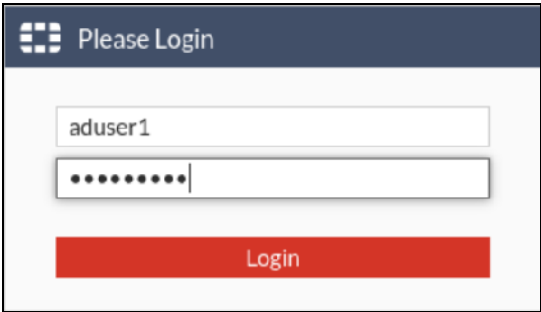
- 3. Enter `exit` to close the session.

Test RADIUS Accounting

Because the SSL-VPN is configured to send a RADIUS accounting packet from FortiGate to FortiAuthenticator every time a user successfully authenticates, you can test RADIUS accounting by logging in to the SSL-VPN as `aduser1`.

To test RADIUS accounting

- 1. On the Local-Client VM, open a browser, and navigate to the following URL: `https://10.0.1.254:10443` to open the SSL-VPN web portal.
- 2. Log in with the username `aduser1` and password `Training!`.

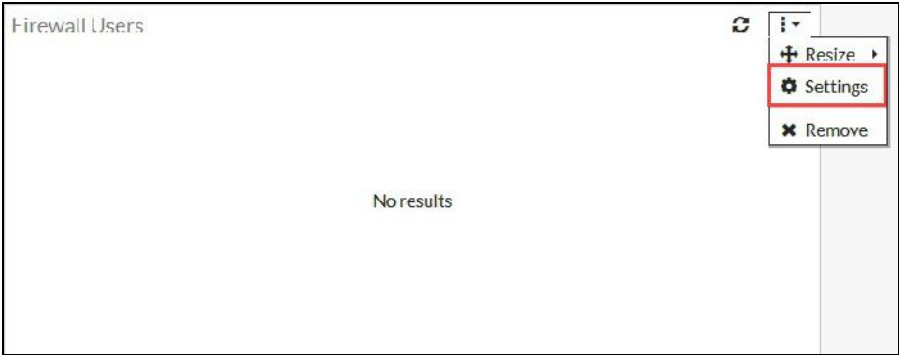


After a successful login and tunnel start, the VPN sends a RADIUS accounting packet to FortiAuthenticator. You can confirm this by running the `tcpdump` command on the FortiAuthenticator CLI (execute `tcpdump port 1813 -nnvvXS`).

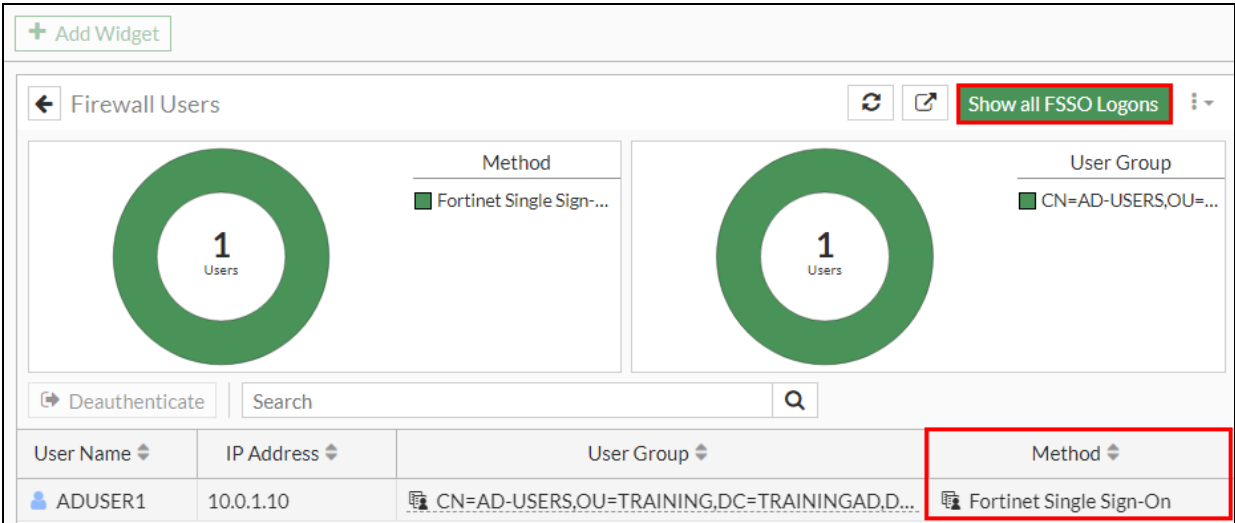
- 3. On the FortiAuthenticator GUI, click **Monitor > SSO > SSO Sessions**. You should see the SSL-VPN user, as shown in the following example:

Refresh Export Logoff All Logoff Selected Update Groups							
	Login Time	Update Time	Workstation	IP Address	Domain Grouping	Domain	Username
	Fri Apr 1 12:53:21 2022	Fri Apr 1 12:53:21 2022	10.0.1.10	10.0.1.10	DEFAULT	TRAININGAD.T...	ADUSER1
							Radius Accounting
1/100 sessions							

- 4. Log in to the FortiGate GUI, and then click **Dashboard > Users & Devices**.
- 5. Locate the **Firewall Users** widget, click the three dots in the upper-right corner of the widget, and then select **Settings**.



- 6. Enable **Show all FSSO Logons**, and then click **OK**.
The widget will refresh and display one firewall user.
- 7. Click inside the widget to view the user.



Using FortiAuthenticator and FSSO, you can populate the user information seamlessly across all FortiGate devices in the network. Remember, the RADIUS accounting packet does not always come from FortiGate. In wireless environments, the accounting packet could come from any third-party access point.

- 8. Return to the Local-Client VM and log out of the SSL-VPN web portal.

Exercise 3: Configuring Manual Portal Authentication

The basic premise of the login portal is that a redirect will send the user to the FortiAuthenticator login page. When used in conjunction with the FortiGate and FortiWiFi solutions, an unauthenticated user can be redirected to authenticate on FortiAuthenticator.

The SSO portal supports multiple authentication methods, including manual authentication, embeddable widgets, and Kerberos authentication.

In this exercise, you will examine manual authentication.

Add the SSL-VPN User Group to the AD Realm

In this exercise, you will add the AD realm the client will be associated with. Then, you will filter users based on the Firewall Admin user group.



This exercise must be performed from the Local-Client VM.

To add the SSL-VPN user group to the AD realm

1. On the Local-Client VM, open the Firefox browser, and then log in to the FortiAuthenticator GUI with the username `admin` and password `password`.
2. Click **Authentication > Portals > Policies**, and then select **Self-Service Portal** in the upper-right corner.
3. Click on **TrainingLab** to edit the policy, and then click **Next**.
4. In the **Identity sources** view, complete the following steps:
 - a. Click **Add a realm**, and then select **realm-adserver | ADserver (<AD server IP>)** (for example, 10.150.0.60).
 - b. Enable the **Filter** for that realm, click **Edit**, select **Firewall Admin**, and then move it under **Chosen groups**.
 - c. Click **OK**.
5. Set the realm you just added (**realm-adserver**) as the default realm, and then click **Update and exit**.

Default	Realm	Allow Local Users To Override Remote Users	Groups	Delete
☐	local Local users	☐	☐ Filter: ☐ Filter local users:	
☒	realm-adserver ADserver (10.0.1.10)	☐	☒ Filter: Firewall Admin ☐ Filter local users:	
Add a realm				

Enable Portal Services

Now, you must enable the SSO login portal on FortiAuthenticator.

To enable portal services

1. Continuing on the FortiAuthenticator GUI, click **Fortinet SSO Methods > SSO > Portal Services**.
2. On the **Edit Portal Services Setting** window, in the **User Portal** section, select **Enable SSO on self-service portals**.
3. In the **Self-service portal policies** section, click in the **search** box, and then select **TrainingLab**.
4. In the **SSO Web Service** section, enable the SSO web service.
5. Set the **SSO user type** to **Remote users**, and then in the drop-down list, select **ADserver (<AD server IP>)** (for example, 10.150.0.60).

User Portal

☒ Enable SSO on self service portals

Self-service portal policies:

search Remove all

x TrainingLab

Login timeout: minutes (-1-10080)

Maximum delay when redirecting to an external URL: seconds (1-10)

Kerberos User Portal

☐ Enable Kerberos login for SSO Import keytab and enable

Kerberos Principal:

SAML Portal

☐ Enable SAML portal

SSO Web Service

☒ Enable SSO Web Service

SSO user type:

☐ External ⓘ

☐ Local users ⓘ

☒ Remote users ⓘ ADserver (10.0.1.10) ▼

OK

6. Click **OK**.

Test Manual Portal Authentication

To test manual portal authentication, you need to log in to FortiAuthenticator as `aduser1` (the assumption is that the user has been redirected to FortiAuthenticator for the login). Because you also need to be able to monitor the active session of `aduser1` in FortiAuthenticator as the admin user, you must use two different browsers. You cannot log in to FortiAuthenticator as two different users at the same time because of the limitations in the lab environment.

To test manual portal authentication

1. On the Local-Client VM, open a **New private window** browser, and then access the self-service portal.
2. Click **Yes, I agree** and log in with the username `aduser1` and password `Training!`.
The self-service portal opens.
3. Return to the browser tab where you are logged in to the FortiAuthenticator GUI as admin, and then click **Monitor > SSO > SSO Sessions** to see the new user information.

					Search for SSO sessions				
☐	Logon Time	Update Time	Workstation	IP Address	Domain Grouping	Domain	Username	Source	Group
☐	Thu Apr 2 13:4...	Thu Apr 2 13:41...	10.0.1.10	10.0.1.10	DEFAULT	TRAINING...	ADUSER1	SSO Portal	CN=ADUSER1,OU=TRAINING,DC=TRAININGAD,DC=TRAINING,DC=L AB+CN=AD_USERS,OU=TRAINING, DC=TRAININGAD,DC=TRAINING, DC=LAB+CN=USERS,CN=BUILTIN, DC=TRAININGAD,DC=TRAINING, DC=LAB+CN=DOMAIN_USERS,CN =USERS,DC=TRAININGAD,DC=TR AINING,DC=LAB

4. Return to the tab with the self-service portal and log out, and then close the browser.

Exercise 4: Configuring DC Polling (Event Log Polling)

In this exercise, you will examine how to configure FortiAuthenticator to poll Active Directory (AD).



When you configured the AD/LDAP server on FortiAuthenticator in Lab 2, you defined the administrator account and used it for browsing the directory and configuring users and groups. From a user rights perspective, the account does not have to be an administrator—a basic account with directory browsing privileges is sufficient.

Enable DC Polling

In this procedure, you will enable DC polling so it is available for use as an FSSO method.

To configure DC polling

1. Log in to the FortiAuthenticator GUI with the username `admin` and password `password`.
2. Click **Fortinet SSO Methods > SSO > General**.
3. In the **Fortinet Single Sign-On (FSSO)** section, enable the following options:

- ☒ Enable Windows event log polling (e.g. domain controllers/Exchange servers) [\[Configure Events\]](#)
- ☒ Enable DNS lookup to get IP from workstation name
 - ☒ Directly use domain DNS suffix in lookup
- ☒ Enable reverse DNS lookup to get workstation name from IP
 - ☐ Do one more DNS lookup to get full list of IPs after reverse lookup of workstation name
 - ☐ Include account name ending with \$ (usually computer account)

4. Click **OK**.

Create a DC

In order to poll the Active Directory event log to track user logins, and also poll the Windows management instrumentation (WMI) logs to track user logouts, you must create a DC account. Again, administrator privileges are not essential; the account needs to be able to poll only the event and WMI logs.

To create a DC

1. Continuing on the FortiAuthenticator GUI, click **Fortinet SSO Methods > SSO > Windows Event Log Sources**, and then click **Create New**.
2. Configure the following settings:

Field	Value
NetBIOS name	TRAININGAD This is the NetBIOS name of your DC. You must use this name.
IP	<Windows-AD server IP> (for example, 10.150.0.60) This is the IP address of the Windows-AD server.
Account	Administrator This is a preconfigured user created for these labs that can authenticate on Active Directory.
Password	password

3. Click **OK**.

Ignore the warning prompt about *Administrator* not being a userPrincipalName.

Ignore the warning prompt about DNS. DNS is already configured for this particular environment.



The configured account does not need to have full administrator permissions on AD, but must have sufficient permissions to read the WMI logs. This can be configured on AD by adding the account to the Event Log Readers group.

Test DC Polling

Although this environment does not include a domain client PC to test logins and logouts, you can experiment with the administrator account by logging out of the Windows-AD VM and logging back in again.

To test DC polling

1. Sign out of the Windows-AD VM by opening the **Start** menu, clicking the user icon on the upper-right corner, and then selecting **Sign out**.
2. Log back in using the password `password`.
3. Log in to the FortiAuthenticator GUI with the username `admin` and password `password`.
4. Click **Monitor > SSO > SSO Sessions**.

You should see the administrator account that shows **Eventlog Polling** as the source.

Refresh		Export		Logoff All		Logoff Selected		Update Groups					
☐	Logon Time	Update Time	Workstation	IP Address	Domain Group	Domain	Username	Source	Group				
☐	Thu Apr 7 07:39:20...	Thu Apr 7 07:39:20...	10.0.1.10	10.0.1.10	DEFAULT	TRAININGAD.TRA...	ADMINISTRATOR	Eventing Polling	CN=ADMINISTRATOR,CN=USERS,DC=TRAININGAD,DC=TRAINING,DC=LAB+CN=SCHEMA ADMIN,CN=USERS,DC=TRAININGAD,DC=TRAINING,DC=LAB+CN=ENTERPRISE ADMIN,CN=USERS,DC=TRAININGAD,DC=TRAINING,DC=LAB+CN=ADMINISTRATORS,CN=BUILTIN,DC=TRAININGAD,DC=TRAINING,DC=LAB+CN=DOMAIN ADMIN,CN=USERS,DC=TRAININGAD,DC=TRAINING,DC=LAB+CN=DEFENDERS,DC=TRAININGAD,DC=LAB+CN=GROUP POLICY CREATOR OWNERS,CN=USERS,DC=TRAININGAD,DC=TRAINING,DC=LAB+CN=USERS,CN=BUILTIN,DC=TRAININGAD,DC=TRAINING,DC=LAB+CN=DOMAIN USERS,CN=USERS,DC=TRAININGAD,DC=TRAINING,DC=LAB				

1 WS20 server

5. Click **Monitor > SSO > Windows Event Log Sources**.

You should see that the DC is connected.

Refresh

Update Time	IP Address	Event Count	Event Processed	Last Event	Connected
Thu Apr 7 07:39:...	10.0.1.10	5	5 (100.0%) (See details)	4776;ADadmin;null;WIN-INT...	

1 Windows event log source

Exercise 5: Configuring FortiClient SSO Mobility Agent

In this exercise, you will examine how the FortiClient SSO Mobility Agent provides another method of user identity discovery over an FSSO framework. As part of FortiClient, the mobility agent is not dependent on a Windows AD infrastructure.

Enable the FortiClient SSO Mobility Agent Service

You will configure FortiAuthenticator to accept agent updates from endpoints.

To enable the FortiClient SSO Mobility Agent Service

1. Log in to the FortiAuthenticator GUI with the username `admin` and password `password`.
2. Click **Fortinet SSO Methods > SSO > General**.
3. In the **Fortinet Single Sign-On (FSSO)** section, enable **Enable FortiClient SSO Mobility Agent Service**. You will see the individual mobility agent service settings.
4. Enable authentication, and then set the **Secret key** to `fortinet`.
5. Leave the other settings at their default values, and click **OK**.



Configure FortiClient to Send User Information to FortiAuthenticator

You will configure FortiClient, which is installed on the Windows-AD server, to send user information updates to FortiAuthenticator.

1. From the Windows-AD VM, launch FortiClient from the task bar.
2. On the left side of the FortiClient window, select **Settings**.
3. In the bottom-left corner, click **Unlock Settings**.
4. Unlock the FortiClient settings page by clicking on the **Unlock Settings** icon in the upper-right corner.



5. Expand the **Advanced** tab, select the **Enable Single Sign-On mobility agent** setting, and then configure the following settings:

Setting	Value
Server address	<POD IP address> (for example, 10.150.0.46)
Port	8001
Pre-shared key	fortinet

6. Close FortiClient.

Validate FortiClient SSO Mobility Agent User Updates

After you configure the FortiClient SSO Mobility Agent settings on both FortiAuthenticator and FortiClient, the agent can begin to send user information updates to FortiAuthenticator.

To validate user information updates

1. Sign out of the Windows-AD server, and then log back in as administrator with the password `password`.
2. Log in to the FortiAuthenticator GUI with the username `admin` and password `password`.
3. Click **Monitor > SSO > SSO Sessions**.

You should see the SSO session information for the Windows-AD server, and the SSO source should be FortiClient.

Refresh	Export	Logoff All	Logoff Selected	Update Groups	Search for SSO sessions	
Workstation	IP Address	Domain Grouping	Domain	Username	Source	Group
WIN-TL0MJM116QB0...	10.0.1.10	DEFAULT	TRAININGAD...	ADMINISTRATOR	FortiClient	CN=ADMIN...

Lab 8: Portal Services

In this lab, you will configure a credential portal on FortiAuthenticator and FortiGate, and attempt to authenticate through the credential portal. Using this authentication method, you can restrict access to internal servers to authorized users only.

You will use the Local-Client VM as the captive portal client. Accordingly, after you configure credential authentication, any internet access through the browser will be subject to the captive portal settings. This is what any user will see when they attempt to connect to your internal servers.

To configure credential-based authentication, you must configure both FortiGate and FortiAuthenticator.

Objectives

- Configure FortiGate for credential-based authentication
- Configure FortiAuthenticator for credential-based authentication
- Test credential-based authentication

Time to Complete

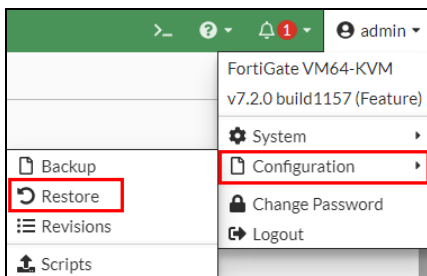
Estimated: 30 minutes

Prerequisites

Before beginning this lab, you must restore a configuration file to FortiGate.

To restore the FortiGate configuration file

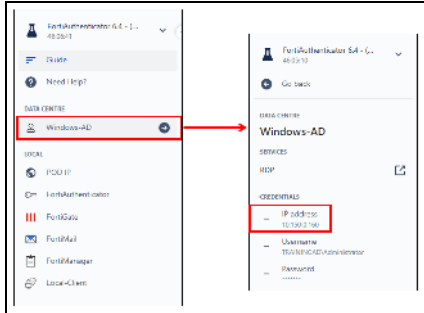
1. Log in to Local-Client VM and open a browser.
2. Log in to the FortiGate GUI with the username `admin` and password `password`.
3. In the upper-right corner of the screen, click **admin**, and then click **Configuration > Restore**.



4. Click **Local PC**, and then click **Upload**.
5. Click **Desktop > Resources > FortiAuthenticator > LAB-8 > FortiGate_Lab-8.conf**, and then click **Select**.
6. Click **OK**.
7. Click **OK** to reboot.

To identify the Windows-AD VM IP address

1. On the Fortinet Training Institute side bar, click **Windows-AD**.
2. Locate and note the IP address in the **CREDENTIALS** section, under **IP address**.
You will use this address where the lab asks for <AD server IP>.

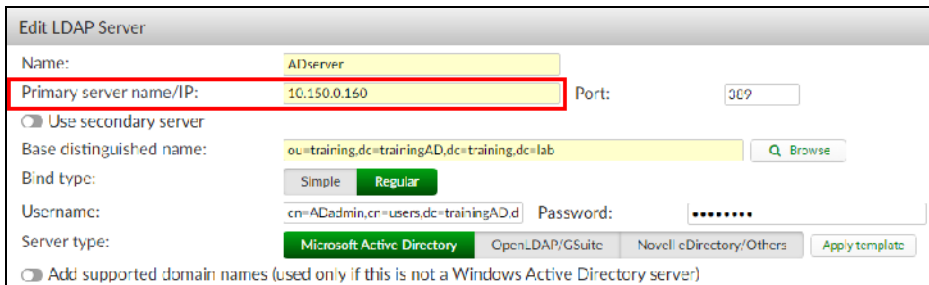


To update the Windows-AD VM IP address



DO NOT perform these steps if you are taking an instructor-led class. This is only required if you are taking the self-paced labs.

1. Log in to the FortiAuthenticator GUI with the username `admin` and password `password`.
2. Click **Authentication > Remote Auth. Servers > LDAP**, and then edit the existing **ADserver** entry.
3. Update the **Primary server name/IP** field to match the Windows-AD VM IP address.



4. Click **OK**.

Exercise 1: Configuring FortiGate for Credential-Based Authentication

When you configure credential-based authentication, you must configure both FortiGate and FortiAuthenticator. In this exercise, you will configure FortiGate only.



All procedures in this exercise are performed on FortiGate.

Create a User Group for Portal Users

In this exercise, you will create a user group on FortiGate for portal users called Portal_Users. This authentication user group is used to validate the user credentials as part of the captive portal login process.

To create a user group for portal users

1. Log in to the FortiGate GUI with the username `admin` and password `password`.
2. Click **User & Authentication** > **User Groups**, and then click **Create New**.
3. On the **New User Group** page, configure the following settings:

Field	Value
Name	Portal_Users
Type	Firewall

4. In the **Remote groups** section, click **Add**, and then configure the following settings:

Field	Value
Remote Server	FortiAuth-RADIUS
Groups	Any

5. Click **OK**.
6. Click **OK**.

Enable a Captive Portal on FortiGate

Now, you are ready to enable a captive portal as the security mode on FortiGate.

Because this lab uses a physical (wired) network interface, you can enable a captive portal through the network interface port 1.

You must configure the authentication protocol as external, and specify the Portal_Users user group you created in the previous procedure.

To enable a captive portal on FortiGate

1. Continuing on the FortiGate GUI, click **Network > Interfaces**, and then edit **LAN (port 1)**.
2. In the **Network** section, enable **Security Mode**, and then configure the following settings:

Field	Value
Security Mode	Captive Portal
Authentication Portal	External https://fac.trainingad.training.lab/portal/
User Access	Restricted to Groups
User Groups	Portal_Users

3. Click **Close**.
4. Click **OK**.

Create a Firewall Policy for FortiAuthenticator

Now, you will create a firewall policy on FortiGate. For credential-based authentication, you do not need a separate policy for FortiAuthenticator. However, for portals like the social portal, FortiAuthenticator requires unrestricted access to social websites. To learn how to allow traffic for FortiAuthenticator, you will create a policy and allow the traffic without any restrictions.

You will configure this firewall policy on the FortiGate GUI, but you can run the final `set captive-portal exempt enable` command only on the CLI.

To configure a firewall policy for FortiAuthenticator

1. Continuing on the FortiGate GUI, click **System > Feature Visibility**, and then enable **Policy Advanced Options** in the **Additional Features** column.
2. Click **Apply**.
3. Click **Policy & Objects > Addresses**, and then click **Create New > Address**. Configure the following settings:

Field	Value
Name	FortiAuthenticator
Type	Subnet
IP/Netmask	10.0.1.150/32

- Click **OK**.
- Click **Policy & Objects > Firewall Policy**, and then expand **LAN (port 1)→WAN (port2)**.
- Right-click the existing policy, select **Insert Empty Policy > Above**, and then double-click the policy you added to edit it.
- Set **Source** to **FortiAuthenticator**, turn on **NAT**, and then turn on **Exempt from Captive Portal**.

The screenshot shows the FortiGate Firewall Policy configuration page. The 'Source' field is set to 'FortiAuthenticator' and the 'Destination' field is set to 'all'. The 'Action' is set to 'ACCEPT'. The 'Inspection Mode' is set to 'Flow-based'. The 'Firewall / Network Options' section shows 'NAT' is enabled, 'IP Pool Configuration' is set to 'Use Outgoing Interface Address', 'Preserve Source Port' is disabled, and 'Protocol Options' is set to 'default'.

- Enable **Enable this policy**.
- Click **OK**.

Exercise 2: Configuring FortiAuthenticator for Credential-Based Authentication

When you configure credential-based authentication, you must configure both FortiGate and FortiAuthenticator. Now that you have configured FortiGate, you must configure FortiAuthenticator.



All procedures in this exercise are performed on the FortiAuthenticator GUI.

Create a User Group for Portal Users

You will create a user group on FortiAuthenticator and add AD users to that group. You are only required to create a group with users for credential-based portals.

To create a user group for portal users

1. Log in to the FortiAuthenticator GUI with the username `admin` and password `password`.
2. Click **Authentication > User Management > User Groups**, and then click **Create New**.
3. On the **Create New User Group** page, configure the following settings:

Field	Value
Name	Portal_Users
Type	Remote LDAP
User retrieval	Set a list of imported remote LDAP users
Remote LDAP	ADserver (<AD server IP>) (for example, 10.150.0.60)

4. In the **LDAP users** section, click in the search box and select **aduser1**.
5. Click **OK**.

Configure a Credential-Based Portal

You will create the captive portal page for credential-based user authentication. You will select this portal page during policy configuration.

To configure a credential-based portal

1. Continuing on the FortiAuthenticator GUI, click **Authentication > Portals > Portals**, and then click **Create New**.
2. In the **Name** field, type `CaptivePortal`, and then in the **Pre-login Services** section, enable **Disclaimer**.

Create New Portal Settings

General

Name: CaptivePortal

Description:

SMS gateway: Use default

Pre-Login Services

☒ Disclaimer

☐ Password Reset

☐ Account Registration

☐ FortiToken Revocation

☐ FIDO Revocation

☐ Usage Extension Notifications

3. Click **OK**.

Configure a Credential-Based Portal Policy

Now that you have configured a portal, you will create a portal policy. This policy defines the conditions in which the portal is presented to a user, and the authentication parameters that are used.

To configure a credential-based portal policy

1. Continuing on the FortiAuthenticator GUI, click **Authentication > Portals > Access Points**, and then click **Create New**.
2. In the **Create New Portal Access Point** view, configure the following settings:

Field	Value
Name	FortiGate_access_point
Client Address	10.0.1.254

3. Click **OK**.
4. Click **Authentication > Portals > Policies**, and then click **Create New**.
5. On the **Policy type** page, in the **Name** field, type `CaptivePortal_Policy`, select **Allow captive portal access**, and then select **CaptivePortal** in the **Portal** drop-down list.

Policy type: CaptivePortal_Policy

Description:

Type: ☒ Allow captive portal access
URL: https://fac.training.ad.training.lab/portal/
Portal: CaptivePortal
☐ Deny captive portal access

Dissect and exit Next

- 6. Click **Next**.
- 7. On the **Portal selection criteria** page, in the **Portal Rule Condition** section, configure the following settings:

Field	Value
HTTP Parameter	userip
Operator	[ip]in_range
Value	10.0.1.0/24

- 8. Click **Next**.
- 9. In the **Access points** section, select **FortiGate_access_point(10.0.1.254)**, and using the arrow, move it to the **Chosen Access Points** pane.
- 10. In the **RADIUS clients** section, select **FortiGate(10.0.1.254)**, and move it to the **Chosen RADIUS Clients** pane.

Access points:

Available Access Points:

Filter:

FortiCloud Sample access point (203.91.113.117)

FortiCloud Sample access point: 0 (ppau.forticloud)

Choose all

Chosen Access Points:

FortiGate_access_point(10.0.1.254)

Remove all

RADIUS clients:

Available RADIUS Clients:

Filter:

FortiCloud Sample (203.91.113.117)

Choose all

Chosen RADIUS Clients:

FortiGate(10.0.1.254)

Remove all

- 11. Click **Next**.
- 12. On the **Authentication type** page, validate that **Password/OTP authentication** has **Local/remote user** enabled, and then click **Next**.

Authentication type: ☒ Password/OTP authentication
☒ Local/remote user
☐ Social users
☐ MAC Authorization

13. On the **Identity sources** page, leave the **Username format** field set to **username@realm**.
14. In the **Realms** field, in the **Realm** column, select **realm-adserver | ADserver (<AD server IP>)** (for example, 10.150.0.60), and then in the **Groups** column, enable the **Filter**, and then edit it to contain the **Portal_Users** group.
15. Click **OK**.

Local/Remote Users:

Username format: ☒ username@realm
☐ realm/username
☐ realm/username

☐ Use default realm when user provided realm is different from all configured realms

Default	Realm	Allow Local Users To Override Remote Users	Groups	Delete
☒	realm-adserver ADserver (10.0.1.10)	☐	☒ Filter: Portal_Users ☐ Filter local users:	X

16. Click **Next**.
17. On the **Authentication factors** page, verify that **All configured password and OTP factors** is selected.
18. Click **Next**.
19. On the **RADIUS response** page, review the RADIUS response information, and then click **Save and exit**.

Exercise 3: Testing Authentication Through the Credential-Based Portal

You will now test the credential portal you set up. To test the credential portal, you will use the `aduser1` account to log in to the captive portal.

To test credential-based authentication

1. In the Local-Client VM, open a browser, and attempt to access <http://www.fortinet.com>.

The **Terms and Disclaimer Agreement** window opens.

Terms and Disclaimer Agreement

You are about to access Internet content that is not under the control of the network access provider. The network access provider is therefore not responsible for any of these sites, their content or their privacy policies. The network access provider and its staff do not endorse nor make any representations about these sites, or any information, software or other products or materials found there, or any results that may be obtained from using them. If you decide to access any Internet content, you do this entirely at your own risk and you are responsible for ensuring that any accessed material does not infringe the laws governing, but not exhaustively covering, copyright, trademarks, pornography, or any other material which is slanderous, defamatory or might cause offence in any other way.

Do you agree to the above terms?

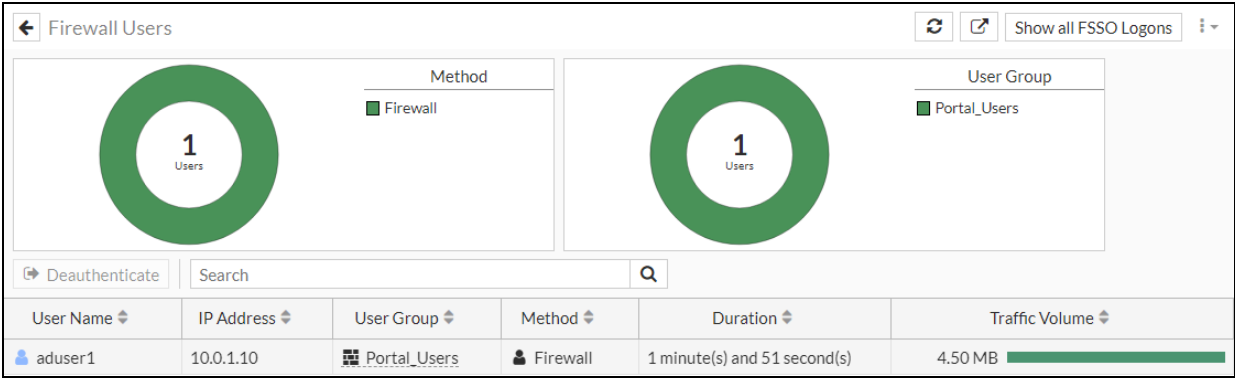


If a security alert appears, accept the self-signed certificate or security exemption.

2. Click **Yes, I agree**.
3. When prompted to log in, log in with the username `aduser1` and the password `Training!`.
After you successfully log in, you will be redirected to the page that you originally requested (www.fortinet.com), and the login and session details will be passed to FortiGate.

To monitor the user

1. Log in to the FortiGate GUI with the username `admin` and password `password`.
2. Click **Dashboard > Users & Devices**, and then click inside the **Firewall Users** widget.
You will see the connected user details.



If you want to walk through the testing process again with the same login credentials, you must deauthenticate yourself, and then close the private browsing window. To deauthenticate yourself, in the **Firewall Users** widget, select **aduser1**, and then click **Deauthenticate**.

- 3. Log out of FortiGate.

Lab 9: PKI and FortiAuthenticator as a CA

At this time, there is no lab associated with the *PKI and FortiAuthenticator as a CA* lesson.

Lab 10: Certificate Management

In this lab, you will add user certificate authentication to an SSL VPN, and then sign and deploy a certificate for SSL inspection on FortiGate.

To add certificate authentication, FortiAuthenticator must act as a certificate authority. You will configure FortiAuthenticator with a root certificate that will be used as the ultimate point of trust.

You will use the FortiAuthenticator root certificate to create a user certificate. You will then use the user certificate to authenticate on the SSL VPN.

Objectives

- Configure SSL VPN user groups
- Create a CA and user certificate
- Import the root CA certificate over SCEP
- Test certificate authentication over VPN
- Generate, sign, and deploy a certificate from a CSR

Time to Complete

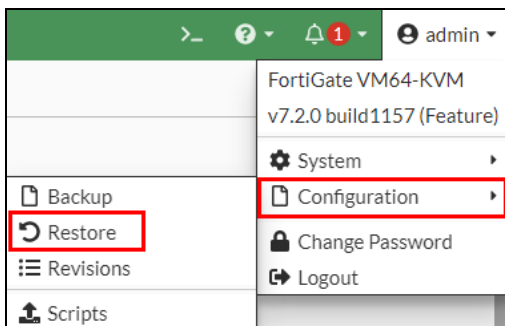
Estimated: 75 minutes

Prerequisites

Before beginning this lab, you must restore a configuration file on FortiGate.

To restore the FortiGate configuration file

1. Log in to the Local-Client VM, and then open a browser.
2. Log in to the FortiGate GUI with the username `admin` and password `password`.
3. In the upper-right corner of the screen, click **admin**, and then click **Configuration > Restore**.



4. Click **Local PC**, and then click **Upload**.
5. Click **Desktop > Resources > FortiAuthenticator > LAB-10 > FortiGate_Lab-10.conf**, and then click **Select**.

6. Click **OK**.
7. Click **OK** to reboot.

This lab includes authenticating with a two-factor method through VPN, so the VPN settings must be configured on FortiGate. Because installing and configuring VPN is out of scope for this lab, the configuration file includes the required VPN settings.

Important configuration items to know about

- The **SSL-VPN-Users** firewall group for the **FortiAuth-RADIUS** remote group (**User & Authentication > User Groups**)

Remote Groups	
Remote Server	Group Name
FortiAuth-RADIUS	SSL_VPN_Users

- The **SSL_VPN** firewall policy for **SSL-VPN-Users** (**Policy & Objects > Firewall Policy**)

Name	SSL_VPN
Incoming Interface	SSL-VPN tunnel interface (ssl.root)
Outgoing Interface	port2
Source	all, SSL-VPN-Users
Destination	all
Schedule	always
Service	ALL
Action	ACCEPT

To update the Windows-AD VM IP address



DO NOT perform these steps if you are taking an instructor-led class. This is only required if you are taking the self-paced labs.

1. Log in to the FortiAuthenticator GUI with the username `admin` and password `password`.
2. Click **Authentication > Remote Auth. Servers > LDAP**, and then edit the existing **ADserver** entry.
3. Update the **Primary server name/IP** field to match the Windows-AD VM IP address.

Edit LDAP Server

Name:

Primary server name/IP: Port:

☐ Use secondary server

Base distinguished name:

Bind type:

Username: Password:

Server type:

☐ Add supported domain names (used only if this is not a Windows Active Directory server)

4. Click **OK**.

Exercise 1: Configuring SSL VPN User Groups

In this exercise, you will create a user group for SSL VPN users, and then add the group to the RADIUS client policy.

Create a User Group for SSL VPN Users

You will create an SSL VPN user group on FortiAuthenticator called **SSL_VPN_Users**. You will then add **aduser1** from the remote LDAP server (**ADserver**) that you created in Lab 2: [User Authentication on page 19](#). After that, you will add a RADIUS attribute based on the group.

To create a user group for SSL VPN users

1. Log in to the FortiAuthenticator GUI with the username `admin` and password `password`.
2. Click **Authentication > User Management > User Groups**, and then click **Create New**.
3. Configure the following settings:

Field	Value
Name	SSL_VPN_Users
Type	Remote LDAP
User retrieval	Set a list of imported remote LDAP users
Remote LDAP	ADserver (<AD server IP>) (for example, 10.150.0.160)

4. Click in the **LDAP users** search box, and then select **aduser1**.
5. In the **RADIUS Attributes** section, click **Add RADIUS Attribute**, and then configure the following settings:

Field	Value
Vendor	Fortinet
Attribute ID	Fortinet-Group-Name
Value	SSL_VPN_Users

6. Click **OK**.

Add an SSL VPN Group to a RADIUS Client Policy

You must add the SSL VPN group you created in the previous procedure to the existing FortiGate RADIUS policy that you created in Lab 2: [User Authentication on page 19](#).

To add an SSL VPN group to a RADIUS client policy

1. Continuing on the FortiAuthenticator GUI, click **Authentication > RADIUS Service > Policies**, select **FortiGate_Default**, and then click **Edit**.
2. Click **Next** until the **Identity source** page appears.
3. On the **Identity source** page, in the **Realms** section, in the **Groups** column, edit the filter.

Username format:

- ☒ username@realm
- ☐ realm/username
- ☐ realm/username

Realms:

Default	Realm	Allow Local Users To Override Remote Users	Use Windows AD Domain Authentication	Groups	Delete
☒	realm:adserver ADserver (10.0.1.10)	☐	☐	☒ Filter: Firewall Admin Filter local users	☐

[Add a realm](#)

4. Move **SSL_VPN_Users** from the **Available User Groups** field to the **Chosen User Groups** field.

Available User Groups ?

Filter

Portal_Users

Choose all

Chosen User Groups ?

Firewall Admin
SSL_VPN_Users

Remove all

OK

5. Click **OK**.
6. Click **Update and exit**.

Add FortiAuthenticator to the Windows Domain

You will add FortiAuthenticator to the Windows domain. This allows FortiAuthenticator to proxy authentication requests using NTLM. This means that connections, such as IPsec or wireless networks using PEAP, can authenticate using CHAP and MSCHAPv2 instead of only PAP.

To configure FortiAuthenticator for domains

1. Continuing on the FortiAuthenticator GUI, click **Authentication > Remote Auth. Servers > LDAP**, and then edit the **ADserver** LDAP server.
2. In the **Windows Active Directory Domain Authentication** section, enable the **Enable** option, and then configure the following settings:

Field	Value
Kerberos realm name	trainingAD.training.lab
Domain NetBIOS name	TRAININGAD
FortiAuthenticator NetBIOS name	FAC
Administrator username	administrator
Administrator password	password

Windows Active Directory Domain Authentication

☒ Enable

Kerberos realm name:

Domain NetBIOS name:

FortiAuthenticator NetBIOS name:

Administrator username:

Administrator password:

☐ Allow Trusted Domain

Preferred Domain Controller Hostname:

- Click **OK**.
- Click **Monitor > Authentication > Windows AD**, validate the server information, and then ensure that the **Agent** is **running** and that the **Connection** is **joined domain, connected**.

Windows Active Directory Server #1	
Server name:	WindowsAD
Primary IP Address:	10.0.1.10
Secondary IP address	None
Authentication Realm:	trainingAD.training.lab
Agent:	running Reset
Connection:	joined domain, connected
Updated:	22 seconds ago



If the agent does not show as running or the domain has not been joined, click the **Refresh** button at the top of the page.

- Log out of FortiAuthenticator.

Exercise 2: Creating a CA Root Certificate and Importing It Into FortiGate Using SCEP

In this exercise, you will create a CA certificate and import it into FortiGate using SCEP. The CA is the ultimate point of trust in your public key infrastructure (PKI) environment.

Create a CA Root Certificate

To create a CA root certificate

1. Log in to the FortiAuthenticator GUI with the username `admin` and password `password`.
2. Click **Certificate Management > Certificate Authorities > Local CAs**, and then click **Create New**.
3. On the **Create New Local CA Certificate** page, configure the following settings:

Field	Value
Certificate ID	10.0.1.150
Name (CN)	FortiAuthCA

4. Leave the remaining settings at the default values, and then click **OK**.
For `aduser1` to log in to the VPN with a certificate, you must first create a user certificate for `aduser1`, which is signed by the root CA.

To enable SCEP on FortiAuthenticator

1. Continuing on the FortiAuthenticator GUI, click **Certificate Management > SCEP > General**, and then click **Enable SCEP**.
2. Configure the following settings:

Field	Value
Default CA	10.0.1.150 CN=FortiAuthCA
Default enrollment password	fortinet
Enrollment method	Automatic

3. Click **OK**.
Pay attention to the warning about enabling HTTP access on the network interface that will serve SCEP clients.

Successfully saved SCEP Settings.

Please remember to enable HTTP/HTTPS access on the network interface that is used to serve SCEP

☒ Enable SCEP

URL: /app/cert/scep/

Default CA: 10.0.1.150 | CN=FortiAuthCA

Default enrollment password:

Enrollment method: **Automatic** Manual and Automatic

☒ Revoke the old certificate on renewal

OK

Enable the HTTP Service for SCEP

The SCEP protocol runs over HTTP, so you must enable HTTP service access in the FortiAuthenticator interfaces that connect to the SCEP clients.

To enable the HTTP service for SCEP

1. Continuing on the FortiAuthenticator GUI, click **System > Network > Interfaces**, and then edit **port1**.
2. In the **Access Rights** section, under **Services**, ensure that **HTTP** and **SCEP (/app/cert/scep/)** are enabled, and then click **OK**.

Access Rights

Admin access:

- ☐ Telnet (TCP/23)
- ☒ SSH (TCP/22)
- ☒ HTTPS (TCP/443)
 - ☒ GUI (TCP/443)
 - ☒ REST API (/api/)
 - ☒ Fabric (/api/v1/fabric/)
- ☐ HTTP (TCP/80)
- ☐ SNMP (UDP/161)

Services:

- ☒ HTTPS (TCP/443)
 - ☒ Self-service Portal (/login/)
 - ☒ Guest Portals (/guests/, /portal/)
 - ☒ SAML IdP (/saml-idp/)
 - ☒ SAML SP SSO (/saml-sp/, /login/saml-auth/)
 - ☒ Kerberos SSO (/login/kerb-auth/)
 - ☒ SCEP (/app/cert/scep/)
 - ☒ CRL Downloads (/app/cert/crl/)
 - ☒ FortiToken Mobile API (/api/v1/pushauthresp/, /api/v1/transfertoken/)
 - ☒ OAuth Service (/api/v1/oauth/, /guests/, /portal/)
- ☒ HTTP (TCP/80)
- ☒ SCEP (/app/cert/scep/)
- ☐ CRL Downloads (/app/cert/crl/)
- ☐ SAML IdP (/saml-idp/)
- ☐ Kerberos SSO (/login/kerb-auth/)

Import the Root Certificate Into FortiGate

Now that SCEP is enabled, you will use the protocol to import the FortiAuthenticator root certificate into FortiGate. This is necessary for FortiGate to trust certificates that this root certificate issues.

To import the root certificate into FortiGate

1. Log in to the FortiGate GUI with the username `admin` and password `password`.
2. Click **System > Certificates**.
3. Click **Create/Import > CA Certificate**.
4. Select **Online SCEP**, and then in the **URL of the SCEP server** field, type `http://10.0.1.150/app/cert/scep`.
5. Click **OK**.

The FortiAuthCA certificate is added under **Remote CA Certificate**.

Remote CA Certificate 5						
CA_Cert_1	CN = FortiAuthCA		FortiAuth...	2025/10/25 18:19:02	Valid	User
Fortinet_CA	C = US, ST = California, L = Sunnyva...		Fortinet	2056/05/27 13:27:39	Valid	Factory
Fortinet CA Backup	C = US, ST = California, L = Sunnyva...		Fortinet	2030/01/19 15:34:39	Valid	Factory

Create a PKI User and Add the User to the Group

A PKI, or peer, user is a digital certificate holder who authenticates using a client certificate. A PKI user account on FortiGate contains the information required to determine which CA certificate to use to validate the user's certificate.

First, you must create a peer (PKI) user using the CLI, and then assign the CA certificate to the user. After that, you must assign the user to the SSL-VPN-Users group.

To create a peer (PKI) user

1. Open an SSH connection to the FortiGate.
2. Log in with the username `admin` and password `password`.
3. Enter the following commands to create a peer (PKI) user:

```
config user peer
  edit user1
    set ca CA_Cert_1
    set cn aduser1
  next
end
```

4. Close the SSH session.

To add the user to the group

1. Continuing on the FortiGate GUI, click **User & Authentication > User Groups**.
2. Select the **SSL-VPN-Users** group, and then click **Edit**.
3. In the **Members** field, click the **+** sign.
4. On the **Select Entries** page, select `user1`, and then click **Close**.

Edit User Group

Name:

Type:

Members: user1 +

Remote Groups

+ Add Edit Delete

Remote Server	Group Name
FortiAuth-RADIUS	SSL_VPN_Users

OK Cancel

5. Click **OK**.

Exercise 3: Configuring User Certificate Authentication

In this exercise, you will create a user certificate, export it as a PKCS#12 file, and then install it in the personal certificate store of aduser1. Then, you will authenticate on the VPN with your user credentials, with your user certificate as the second factor of authentication.

Configure User Certificate Authentication

FortiAuthenticator allows you to create end-entity certificates for users and local services. These certificates prove the authentication of the end entity.

To configure user certificate authentication

1. On the Local-Client VM, open the Firefox browser, and then log in to the FortiAuthenticator GUI with the username `admin` and password `password`.
2. Click **Certificate Management > End Entities > Users**, and then click **Create New**.
3. Configure the following settings:

Field	Value
Certificate ID	aduser1
Issuer	Local CA
Certificate authority	10.0.1.150 CN=FortiAuthCA
Name (CN)	aduser1

4. Click **OK**.

Export the User Certificate

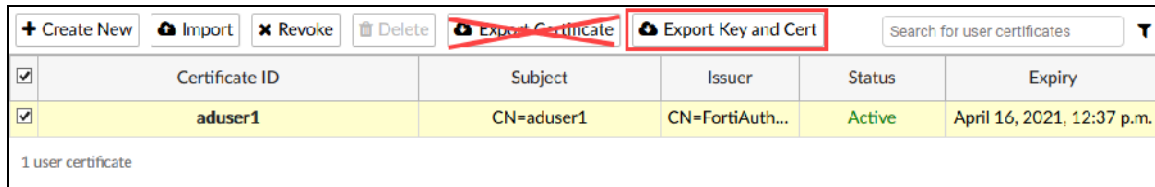
After you create the user certificate, you must issue the certificate to the user. You will export the user certificate as a PKCS#12 file. After you export it as a file, you can provide it to aduser1.

To export the user certificate

1. Continuing on the FortiAuthenticator GUI, click **Certificate Management > End Entities > Users**.
2. Select the **aduser1** client certificate, and then click **Export Key and Cert**.



Do not confuse the **Export Certificate** option with the **Export Key and Cert** option.



You are now prompted to give the file a passphrase.

3. Type the following passphrase:

Field	Value
Passphrase	fortinet
Confirm passphrase	fortinet

4. Click **OK**, and then click the **Download PKCS#12** file.
5. Click **Finish** to complete the export workflow.

Import the User Certificate to the VPN User's Certificate Store

Now that you have exported the user certificate for aduser1, you must install it in their personal certificate store. In this way, when aduser1 is prompted by the VPN for their certificate for authentication, the VPN automatically checks the personal certificate store.



You must install the user certificate in the **Personal** folder in the **Current User** store (not the **Local Machine** store). This is because the certificate is tied to a user (for example, for signing certificates and authenticating) and not a machine (for example, for SSL encryption on a website).

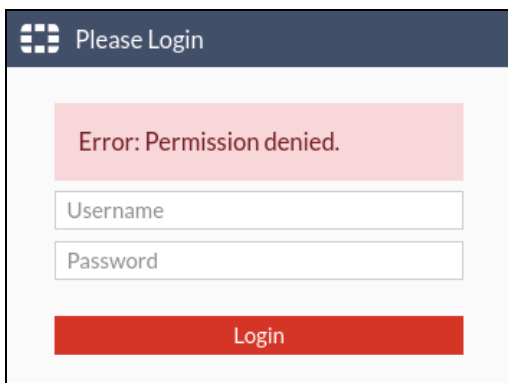
For the purposes of this lab, aduser1's computer (and therefore the location of aduser1's personal certificate store) is the Local-Client VM.

Import the Certificate Into the Browser

You will attempt to establish the SSL VPN connection before you install the certificate. Then, you will import the certificate you created earlier in this lab to the Firefox browser that is installed on the Local-Client VM.

To test before installing

1. On the Local-Client VM, open the Firefox browser.
2. Attempt to access `https://10.0.1.254:10443`.
A **Permission denied** error appears.



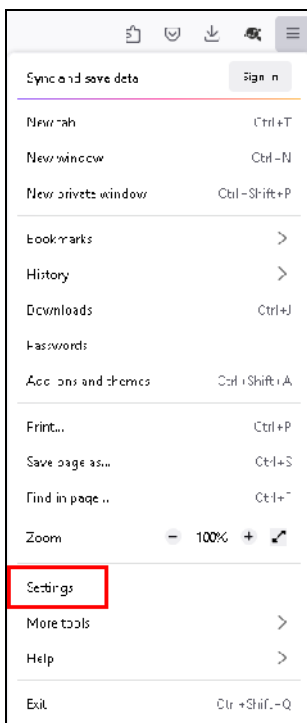
3. Close the browser.



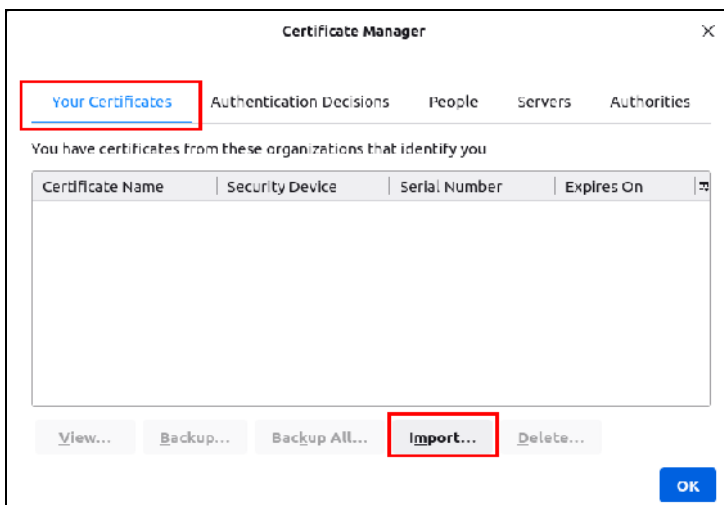
It is important to close the browser to prevent any browser caching issues while you perform these steps.

To import the certificate into the Firefox browser

1. On the Local-Client VM, open the Firefox browser.
2. In the upper-right corner of the browser, click the **Open menu** icon (three horizontal bars), and then click **Settings**.



3. In the left menu, click **Privacy & Security**.
4. Scroll down to the **Security** section, and then under **Certificates**, click **View Certificates**.
5. In the **Certificate Manager** window, click **Your Certificates** tab, and then click **Import**.

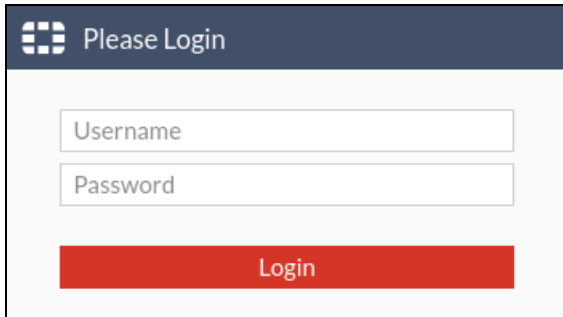


6. Navigate to the **Downloads** folder, select **aduser1.p12**, and then click **Select**.
7. Type `fortinet` as the password for the p12 file, and then click **Sign in**.
8. Click **OK**.

To test certificate-based authentication over SSL VPN

1. In the Firefox browser, open a new tab .
2. In the browser address field, enter: `https://10.0.1.254:10443`.

The login screen appears, without the error.



3. Log in to the SSL VPN with the username `aduser1` and password `Training!`.
You have successfully logged in to the SSL VPN using the selected certificate as the second factor of authentication.
4. Log out of the VPN session, and then close the browser.

Exercise 4: Using FortiAuthenticator to Create and Sign a CSR for FortiGate SSL Inspection

In this exercise, you will create a CSR on FortiGate and download it. You will then import the CSR to FortiAuthenticator for signing. After the certificate has been signed, you will import it into FortiGate for use in SSL inspection. Finally, you will import the certificate into your browser and validate successful SSL inspection.

Generate a CSR on FortiGate

You will generate a CSR on the lab FortiGate. You will then download the CSR so that FortiAuthenticator can import and sign it.

To generate and download a CSR on FortiGate

1. On the Local-Client VM, open a browser, and then log in to the FortiGate GUI with the username `admin` and password `password`.
2. Click **System** > **Certificates**, and then click **Create/Import**.
3. Click **Generate CSR**, and then configure the following settings:

Field	Value
Certificate Name	SSL_Inspection
ID Type	Host IP
IP	10.160.0.2
E-Mail	admin2@training.lab

4. Click **OK**.

The new certificate appears in the **Local Certificate** list, with a **Status** of **Pending**.

Name	Subject	Comments	Issuer	Expires	Status	Source
Fortinet_SSL_ECDSA256	C = US, ST = California, L = Sunn...	This certificate is embedd...	Fortinet	2030/01/09 07:58:15	Valid	Factory
Fortinet_SSL_ECDSA384	C = US, ST = California, L = Sunn...	This certificate is embedd...	Fortinet	2030/01/09 07:58:15	Valid	Factory
Fortinet_SSL_ECDSA521	C = US, ST = California, L = Sunn...	This certificate is embedd...	Fortinet	2030/02/24 13:11:57	Valid	Factory
Fortinet_SSL_ID448	C = US, ST = California, L = Sunn...	This certificate is embedd...	Fortinet	2030/02/24 13:11:57	Valid	Factory
Fortinet_SSL_ED25519	C = US, ST = California, L = Sunn...	This certificate is embedd...	Fortinet	2030/02/24 13:11:57	Valid	Factory
Fortinet_SSL_RSA1024	C = US, ST = California, L = Sunn...	This certificate is embedd...	Fortinet	2030/01/09 07:58:14	Valid	Factory
Fortinet_SSL_RSA2048	C = US, ST = California, L = Sunn...	This certificate is embedd...	Fortinet	2030/01/09 07:58:14	Valid	Factory
Fortinet_SSL_RSA4096	C = US, ST = California, L = Sunn...	This certificate is embedd...	Fortinet	2030/02/24 13:11:57	Valid	Factory
Fortinet_Wifi	C = US, ST = California, L = Sunn...	This certificate is embedd...	DigiCert Inc	2021/02/11 05:00:00	Valid	Factory
SSL_Inspection					Pending	User

5. Select the **SSL_Inspection** certificate, and then click **Download** to save the file in the **Downloads** folder.

Sign the Certificate With FortiAuthenticator

You will import the CSR into FortiAuthenticator and sign the certificate.

To import and sign the CSR with FortiAuthenticator

1. On the Local-Client VM, open a browser, and then log in to the FortiAuthenticator GUI with the username `admin` and password `password`.
2. Click **Certificate Management > Certificate Authorities > Local CAs**, and then click **Import**.
3. In the **Import Signing Request or Local CA Certificate** window, configure the following settings:

Field	Value
Type	CSR to sign
Certificate ID	SSL_Inspection_FG
CSR File (.csr, .req)	Click Upload a file . Navigate to Downloads , and then select <code>SSL_Inspection.csr</code> . Click Select .

4. Click **OK**.

The **SSL_Inspection_FG** certificate appears in the list of Local CAs.

✔ Certificate signing request "CN=192.168.150.155, emailAddress=admin2@fortinet.lab" was signed with CA certificate "CN=FortiAuthCA" ✔ CA certificate 'CN=192.168.150.155, emailAddress=admin2@fortinet.lab' was successfully imported					
☐	Certificate ID	Subject	Issuer	Status	CA Type
☐	10.0.1.150	CN=FortiAuthCA	CN=FortiAut...	Active	Root CA
☐	SSL_Inspection_FG	CN=192.168.150.155, ema...	CN=FortiAut...	Active	Intermediate (non-si...

5. Select the **SSL_Inspection_FG** certificate, and then click **Export Certificate**.

Import the Signed Certificate Into FortiGate and Enable SSL Inspection

You will import the signed certificate into FortiGate, and then enable SSL inspection in the firewall policy.

To import the signed certificate and enable SSL inspection in a firewall policy

1. On the Local-Client VM, open a browser, and then log in to the FortiGate GUI with the username `admin` and password `password`.
2. Click **System > Certificates**, and then select **Certificate** in the **Create/Import** drop-down list.
3. In the **Import Certificate** section, click **Import Certificate**.
4. In the **Import Certificate** section, verify that **Local Certificate** is selected, and then click **Upload**.
5. Navigate to the **Downloads** directory, select the `SSL_Inspection_FG` security certificate (make sure you select the file ending with `_FG`, not the `.csr` extension), and then click **Select**.

6. Click **Create**.
7. Click **OK**.

The **SSL-Inspection** certificate is now valid.

SSL_Inspection	CN = 10.160.0.2, emailAddress = a...	FortiAuthCA	2032/04/05 11:13:24	Valid	User
----------------	--------------------------------------	-------------	---------------------	-------	------

8. Click **Policy & Objects > Firewall Policy**.
9. Expand the **LAN (port1) → WAN (port2)** policy header, select the **Internet_Access** policy, and then click **Edit**.

+ Create New Edit Delete Policy Lookup Search Q Interface Pair View By Sequence									
Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
port1 → port2									
Internet_Access	all	all	always	ALL	✓ ACCEPT	✓ Enabled	SSL no-inspection	UTM	17.44 MB

10. In the **Edit Policy** window, in the **Security Profiles** section, enable **Application Control**, and then in the **SSL Inspection** drop-down list, select **custom-deep-inspection**.

Security Profiles	
AntiVirus	☐
Web Filter	☐
DNS Filter	☐
Application Control	☒ APP default
IPS	☐
SSL Inspection	SSL custom-deep-inspection

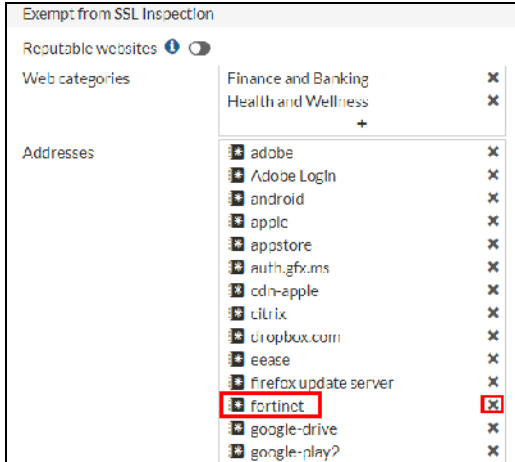


You enabled the **Application Control** option in the security profile because there must be at least one other profile enabled for the FortiGate to perform SSL inspection.

11. Click the pencil icon to the right of the **SSL Inspection** drop-down list to edit the **custom-deep-inspection** inspection profile.
12. In the **Edit SSL/SSH Inspection Profile** window, in the **SSL Inspection Options** section, select **SSL_Inspection** in the **CA certificate** drop-down list.

SSL Inspection Options	
Enable SSL inspection of	Multiple Clients Connecting to Multiple Servers Protecting SSL Server
Inspection method	SSL Certificate Inspection Full SSL Inspection
CA certificate	SSL_inspection Download
Blacklisted certificates	Allow Block View Blacklisted Certificates
Untrusted SSL certificates	Allow Block Ignore View Trusted CAs List

13. In the **Exempt from SSL Inspection** section, click the **X** to remove **fortinet** from the **Addresses** list.



14. Click **OK**.
15. Click **OK**.
16. On the Local-Client VM, open a new browser tab, and then attempt to navigate to `www.fortinet.com`.
You receive a security error and are not allowed to access the website. *Do not* accept the risk and continue if you are given the option.



You receive a security alert from the browser because the certificate (**SSL_Inspection**) that FortiGate is using for communication with the Local-Client VM is not trusted by the browser.

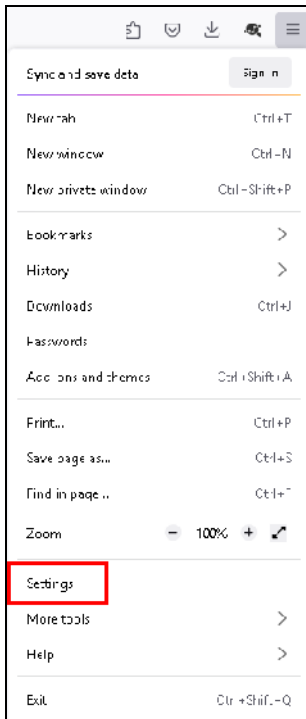
17. Close the browser tab.

Import the Certificate Into the Browser

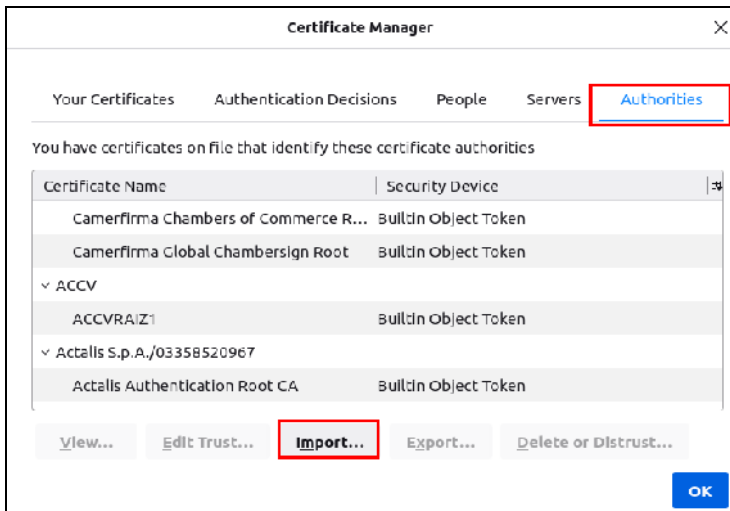
You will install the certificate you created earlier in this lab in the Firefox browser that is installed on the Local-Client VM.

To import the certificate into the Firefox browser

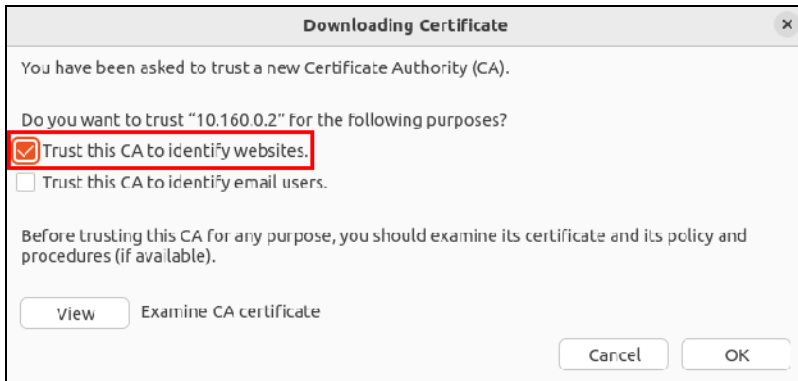
1. On the Local-Client VM, launch the Firefox browser.
2. In the upper-right corner of the browser, click the **Open menu** icon (three horizontal bars), and then click **Settings**.



3. In the left menu, click **Privacy & Security**.
4. Scroll down to the **Security** section, and then under **Certificates**, click **View Certificates**.
5. In the **Certificate Manager** window, click the **Authorities** tab, and then click **Import**.



6. Navigate to the **Downloads** folder, select `SSL_Inspection_FG`, and then click **Select**.
7. In the **Downloading Certificate** window, select **Trust this CA to identify websites**, and then click **OK**.



8. Click **OK**.
9. Close the **Options** tab, and then open a new browser tab.
10. In the new tab, browse to `www.fortinet.com`.
You will be able to access the page without security warnings.

By importing the **SSL_Inspection_FG** certificate into the browser, the browser now trusts that CA, which is the one that FortiGate is presenting (the CA is the FortiGate device).

Lab 11: 802.1X Authentication

At this time, there is no lab associated with the *802.1X Authentication* lesson.

Lab 12: SAML

In this lab, you will test Security Assertion Markup Language (SAML) single sign-on using two service providers (SPs) and one identity provider (IdP). You will configure FortiGate and FortiManager as the SPs, and FortiAuthenticator as the IdP.

- SPs:
 - FortiGate: `fgt.trainingad.training.lab`
 - FortiManager: `fmg.trainingad.training.lab`
- IdP:
 - FAC: `fac.trainingad.training.lab`

Objectives

- Configure FortiAuthenticator as an IdP
- Configure FortiGate and FortiManager as SPs
- Configure FortiAuthenticator to send SAML attributes

Time to Complete

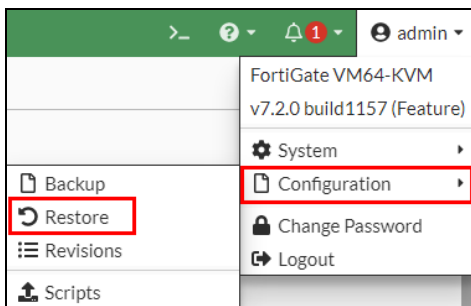
Estimated: 30 minutes

Prerequisites

Before beginning this lab, you must restore a configuration file to FortiGate.

To restore the FortiGate configuration file

1. Log in to the Local-Client VM, and then open a browser.
2. Log in to the FortiGate GUI with the username `admin` and password `password`.
3. In the upper-right corner of the screen, click **admin**, and then click **Configuration > Restore**.



4. Click **Local PC**, and then click **Upload**.
5. Click **Desktop > Resources > FortiAuthenticator > LAB-12 > FortiGate_Lab-12.conf**, and then click **Select**.
6. Click **OK**.
7. Click **OK** to reboot.

Exercise 1: Configuring IdP and SP Settings on FortiAuthenticator

In this exercise, you will configure FortiAuthenticator as an IdP server, with FortiGate and FortiManager as SPs.

Configure IdP Settings on FortiAuthenticator

You will create an IdP server certificate and configure FortiAuthenticator as an IdP.

To create and export a server certificate

1. On the Local-Client VM, open a browser, and then log in to the FortiAuthenticator GUI with the username `admin` and password `password`.
2. Click **Certificate Management > End Entities > Local Services**, and then click **Create New**.
3. On the **Create New Certificate** page, configure the following settings:

Field	Value
Certificate ID	IdP
Issuer	Local CA
Certificate authority	10.0.1.150 CN=FortiAuthCA
Name (CN)	IdP

4. Leave the remaining settings at the default values, and then click **OK**.
5. Select the **IdP** certificate, and then click **Export Certificate**.

+ Create New	Import	X Revoke	Delete	Export Certificate		
☐	Certificate ID	Subject	Issuer	Status		
☐	Default-Server-Certificate	C=US, ST=California, L=Sunnyvale, O=Fortinet, O...	Remote CA: C=US, ST=Cali...	Active		
☐	Fortinet_CA1_Factory	C=US, ST=California, L=Sunnyvale, O=Fortinet, O...	Remote CA: C=US, ST=Cali...	Active		
☐	Fortinet_CA2_Factory	C=US, ST=California, L=Sunnyvale, O=Fortinet, O...	Remote CA: C=US, ST=Cali...	Active		
☒	IdP	CN=IdP	CN=trainingod.training.lab	Active		
4 / 10 server certificates						

The certificate is exported to the **Downloads** folder.

To configure FortiAuthenticator as an IdP

1. Continuing on the FortiAuthenticator GUI, click **Authentication > SAML IdP > General**.
2. On the **Edit SAML Identity Provider Settings** page, enable the SAML identity provider portal, and then configure the following settings:

Field	Value
Server address	fac.trainingad.training.lab
Username input format	username@realm
Use default realm when user-provided realm is different from all configured realms	enable

3. In the **Realms** section, click **Add a realm**.
4. In the **Realm** column, ensure that **local | Local users** is selected.
5. In the **Default IdP certificate** drop-down list, select **IdP | CN=IdP**.
6. Leave the remaining settings at the default values, and then click **OK**.



You can use a group filter to limit the scope of the authentication to a specific user group.

Configure SP Settings on FortiAuthenticator

You will configure SP settings on FortiAuthenticator.

To configure SP settings on FortiAuthenticator

1. Continuing on the FortiAuthenticator GUI, click **Authentication > SAML IdP > Service Providers**, and then click **Create New**.
2. On the **Create New SAML Service Provider** page, configure the following settings:

Field	Value
SP name	FortiGate
IdP prefix	Click the green +. In the IdP prefix field, type <code>fgt</code> . Click OK .

Create New SAML Service Provider

IdP address: fac.trainingad.training.lab

SP name: FortiGate

IdP prefix: fgt x +

IdP entity id: http://fac.trainingad.training.lab/saml-idp/fgt/metadata/

IdP single sign-on URL: https://fac.trainingad.training.lab/saml-idp/fgt/login/

IdP single logout URL: https://fac.trainingad.training.lab/saml-idp/fgt/logout/

Server certificate: Use default setting in SAML IdP General page

IdP signing algorithm: Use default signing algorithm in SAML IdP General page

☐ Support IdP-initiated assertion response

☐ Participate in single logout

3. In the **Assertion Attributes** section, click **Add Assertion Attribute**, and then configure the following settings:

Field	Value
SAML attribute	username
User attribute	Username

Assertion Attributes

Assertion attribute:

SAML attribute: username

User attribute: Username

Add Assertion Attribute

4. Click **Save**.
5. Log out of FortiAuthenticator.

Exercise 2: Configuring FortiGate As an SP

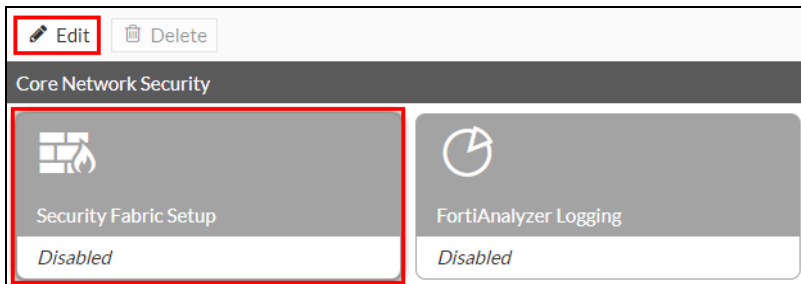
In this exercise, you will configure FortiGate to act as an SP for SSO. You will then configure FortiAuthenticator to act as the IdP for that SP.

Configure FortiGate As an SP

You will configure FortiGate as an SP and securely identify the IdP.

To configure FortiGate as an SP

1. On the Local-Client VM, open a browser, and then log in to the FortiGate with the username `admin` and password `password`.
2. Click **Security Fabric > Fabric Connectors**.
3. Select **Security Fabric Setup**, and then click **Edit**.



4. Click **Single Sign-On Settings**, and then configure the following settings:

Field	Value
Mode	Service Provider (SP)
SP address	fgt.trainingad.training.lab
Default login page	Single Sign-On
Default admin profile	super_admin
IdP type	Fortinet Product
IdP address	fac.trainingad.training.lab
Prefix	fgt

Field	Value
IdP certificate	Click Import , and then click Upload . Navigate to the Downloads directory, and then select the <code>IdP.cer</code> certificate file. Click Select , and then click OK . Select REMOTE_Cert_1 .

- Expand the **SP Details** tab, and then examine the entries.

SP Details	
SP portal URL	<code>https://fgt.trainingad.training.lab/saml/login/</code>
SP entity ID	<code>http://fgt.trainingad.training.lab/metadata/</code>
SP ACS (login) URL	<code>https://fgt.trainingad.training.lab/saml/?acs</code>
SP SLS (logout) URL	<code>https://fgt.trainingad.training.lab/saml/?sls</code>



The information shown in the **SP Details** tab is used to complete the SP configuration on FortiAuthenticator.

- Click **OK**.
- Click **OK**.

Complete the FortiAuthenticator SP Configuration for FortiGate

Now that you have the SP metadata, you must complete the SP configuration on FortiAuthenticator for the FortiGate SP.

To complete the FortiAuthenticator SP configuration for FortiGate

- On the Local-Client VM, open a browser, and then log in to the FortiAuthenticator with the username `admin` and password `password`.
- Click **Authentication > SAML IdP > Service Providers**.
- Edit the **FortiGate** SP, and configure the following settings:

Field	Value
SP entity ID	<code>http://fgt.trainingad.training.lab/metadata/</code>
SP ACS (login) URL	<code>https://fgt.trainingad.training.lab/saml/?acs</code>
SP SLS (Logout) URL	<code>https://fgt.trainingad.training.lab/saml/?sls</code>

- Click **OK**.

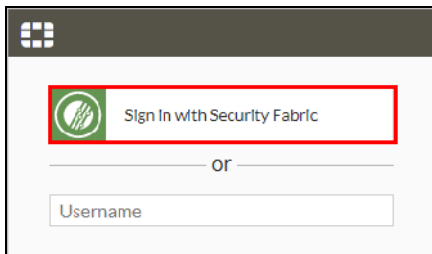


You can copy and paste the SP metadata you enter here from the FortiGate by expanding **SP Details**, which you configured earlier in this exercise, on the **Fabric Connector > Single Sign-On Settings** page.

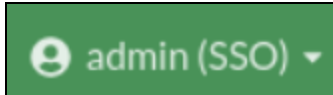
5. Log out of the FortiAuthenticator and FortiGate, and then close the browser.

To test the single sign-on configuration

1. Open a browser, and then access the FortiGate login screen.
2. Click **Sign in with Security Fabric**.



3. Log in with the username `admin` and password `password`.
A message appears stating that the single sign-on was successful and an SSO administrator account was created for the **admin** user.
4. Click **Continue**.
The SSO user that is currently logged in is **admin**.



5. Log out of the FortiGate GUI, and then close the browser.

Exercise 3: Adding FortiManager As a Second SP

In this exercise, you will add FortiManager as a second SP on FortiAuthenticator, import the IdP certificate on FortiManager, and configure the remaining settings. Finally, you will test SAML SSO on FortiGate and FortiManager.

Add FortiManager As a Second SP

You will configure the SP settings on FortiAuthenticator.

To add FortiManager as a second SP

1. Log in to the FortiAuthenticator GUI with the username `admin` and password `password`.
2. Click **Authentication > SAML IdP > Service Providers**.
3. Click **Create New**, and then configure the following settings:

Field	Value
SP name	FortiManager
IdP prefix	Click the green +. In the IdP prefix field, type <code>fmg</code> . Click OK .

Create New SAML Service Provider

IdP address: `fac.trainingad.training.lab`

SP name: `FortiManager`

IdP prefix: `fmg` ✖ +

IdP entity id: `http://fac.trainingad.training.lab/saml-idp/fmg/metadata/` 🔗

IdP single sign-on URL: `https://fac.trainingad.training.lab/saml-idp/fmg/login/` 🔗

IdP single logout URL: `https://fac.trainingad.training.lab/saml-idp/fmg/logout/` 🔗

Server certificate: `Use default setting in SAML IdP General page` ▼

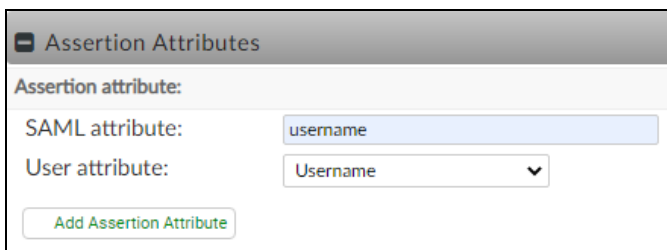
IdP signing algorithm: `Use default signing algorithm in SAML IdP General page` ▼

☐ Support IdP-initiated assertion response

☐ Participate in single logout

4. In the **Assertion Attributes** section, click **Add Assertion Attribute**, and then configure the following settings:

Field	Value
SAML attribute	username
User attribute	Username



Assertion Attributes

Assertion attribute:

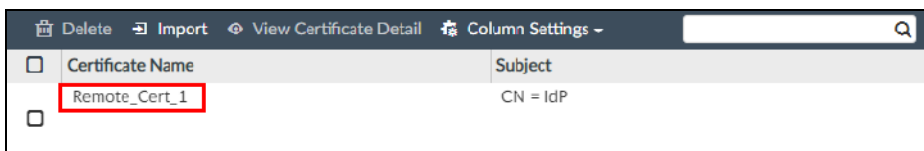
SAML attribute:

User attribute:

5. Click **Save**.
6. Log out of FortiAuthenticator.

To configure FortiManager for SAML SSO

1. On the Local-Client VM, open a browser, and then log in to the FortiManager GUI with the username `admin` and password `password`.
 2. Click **System Settings**.
 3. Click **Certificates > Remote Certificates**.
 4. Click **Import**, and then browse to the **Downloads** folder.
 5. Select the `IdP.cer` certificate file, and then click **Select**.
 6. Click **OK**.
- The IdP certificate appears as **Remote_Cert_1**.



☐	Certificate Name	Subject
☐	Remote_Cert_1	CN = IdP

7. On the **System Settings** page, click **Admin > SAML SSO**, and then configure the following settings:

Field	Value
Single Sign-On Mode	Service Provider (SP)
SP Address	fmg.trainingad.training.lab
Default Login Page	Normal
Default Admin Profile	Super_User
IdP Type	Fortinet
IdP Address	fac.trainingad.training.lab
Prefix	fmg
IdP Certificate	Remote_Cert_1 (FortiAuthCA, IdP)

8. Click **Apply**.



Note the **SP Entity ID**, **SP ACS (Login) URL**, and **SP SLS (Logout) URL**. These are used to complete the SP configuration on FortiAuthenticator.

9. Log out of FortiManager, and then close the browser.

Complete the FortiAuthenticator SP Configuration for FortiManager

You will use the information from the FortiManager SAML configuration to complete the FortiAuthenticator SP configuration.

To complete the FortiAuthenticator SP configuration for FortiManager

1. On the Local-Client VM, open a browser, and then log in to the FortiAuthenticator GUI with the username `admin` and password `password`.
2. Click **Authentication > SAML IdP > Service Providers**.
3. Edit the **FortiManager** SP, and then configure the following settings:

Field	Value
SP entity ID	<code>http://fmg.trainingad.training.lab/metadata/</code>
SP ACS (login) URL	<code>https://fmg.trainingad.training.lab/saml/?acs</code>
SP SLS (Logout) URL	<code>https://fmg.trainingad.training.lab/saml/?sls</code>

4. Click **OK**.



You can copy and paste the SP metadata you entered here from the FortiManager **Admin > SAML SSO** configuration page.

5. Log out of FortiAuthenticator, and then close the browser.

Exercise 4: Testing the SAML Authentication

In this exercise, you will test the SAML authentication with the two SPs that are configured on FortiAuthenticator. You will also use a SAML tracer add-on in Firefox to view the SAML message exchange.

Validate the SAML Authentication

You will test the SAML authentication by accessing the FortiGate login page, and then selecting the **Sign in with Security Fabric** option. This redirects your browser to the login portal on FortiAuthenticator. After you enter the login credentials, the browser is redirected to FortiGate. You will then connect to FortiManager. Because you already authenticated on FortiGate, you do not need to authenticate again on FortiManager.

To validate the SAML authentication

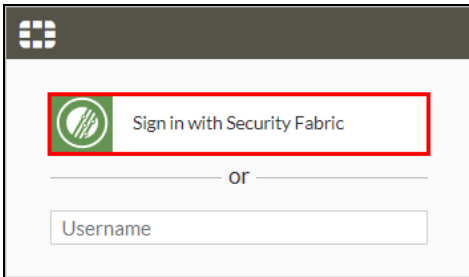
1. On the Local-Client VM, open a browser, and then in the upper-right corner, click the SAML tracer add-on icon.



2. In the browser, click the **FortiGate** bookmark, or you can type the following URL for the page:

`https://fgt.trainingad.training.lab/login`

3. Click **Sign in with Security Fabric**.



You are redirected to the FortiAuthenticator login portal.

4. Enter the following credentials for the SAML account:

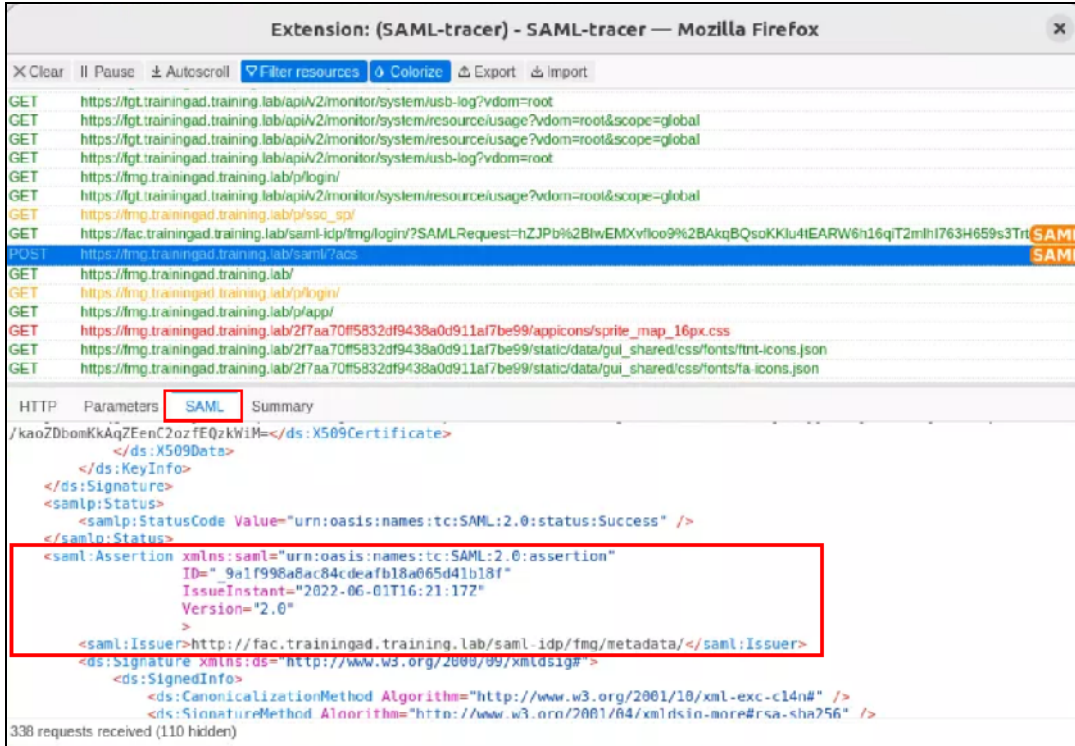
Username: admin

Password: password

5. Click **Login**.

You are redirected to the FortiGate landing page.

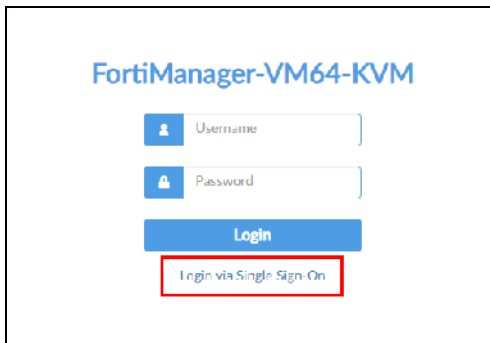
6. View the SAML assertion messages in the SAML tracer add-on window.



All SAML messages have an orange SAML tag. You can view the relevant information by selecting the individual message, and then clicking the SAML tab.

To validate SAML SSO

1. On the Local-Client VM, continue in the browser, and then open a new tab.
2. Click the **FortiManager** bookmark, or type the following URL for the page:
<https://fmg.trainingad.training.lab/>
3. Click **Login via Single Sign-On**.



You are automatically logged in to FortiManager without having to authenticate again.

4. Log out of FortiGate and FortiManager, and then close the browser.

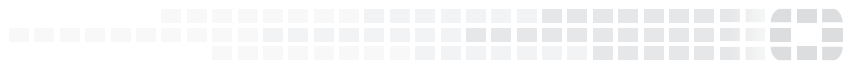
Lab 13: FIDO2 Authentication

At this time, there is no lab associated with the *FIDO2 Authentication* lesson.

DO NOT REPRINT
© FORTINET



FORTINET®



No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet Inc., as stipulated by the United States Copyright Act of 1976.

Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Fortinet Vouchers & Dumps are Available on [Brave-Dumps.com](https://bravedumps.com)