DO NOT REPRINT
© FORTINET
Passdumps.com



LAN Edge Study Guide

for FortiGate 7.0

Vouchers & Dumps are Available | WhatsApp +201224560923

FORTINET NSE Training Institute

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Fortinet Training

https://training.fortinet.com

Fortinet Document Library

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 Support

https://support.fortinet.com

FortiGuard Labs

https://www.fortiguard.com

Fortinet Network Security Expert Program (NSE)

https://training.fortinet.com/local/staticpage/view.php?page=certifications

Fortinet | Pearson VUE

https://home.pearsonvue.com/fortinet

Feedback

Email: askcourseware@fortinet.com

FORTINET

3/16/2022

Vouchers & Dumps are Available | WhatsApp +201224560923

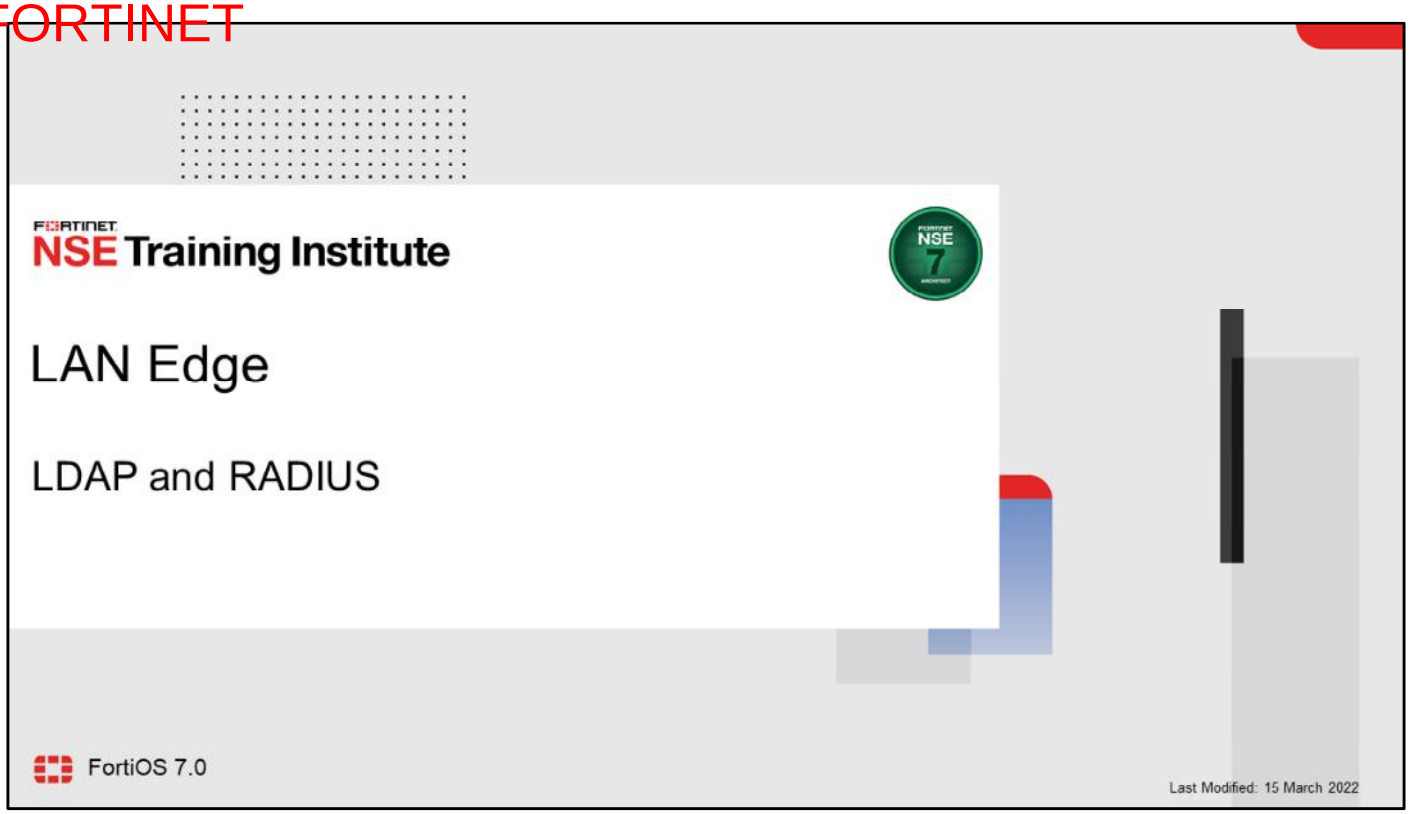
DO NOT REPRINT
© FORTINET
Brave-dumps.com

TABLE OF CONTENTS

01 LDAP and RADIUS **4**
02 Certificate-Based Authentication **58**
03 RADIUS and Syslog Single Sign-On **99**
04 Centralized Management **151**
05 FortiSwitch **202**
06 Port Security **253**
07 Integrated Wireless **295**
08 Guest Access **355**
09 Enhanced Wireless **391**
Solutions **459**

Vouchers & Dumps are Available | WhatsApp +201224560923

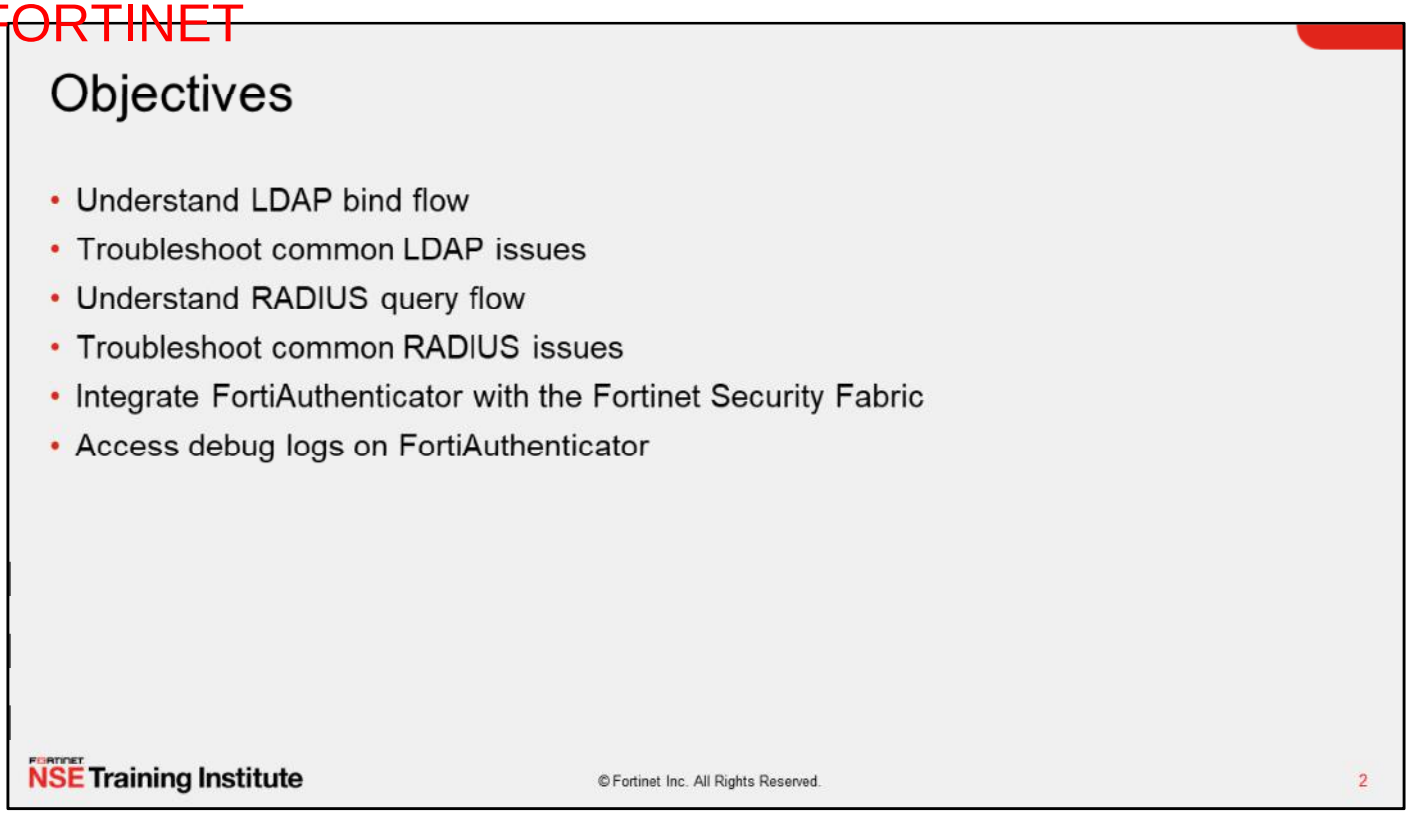
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn how to configure and troubleshoot LDAP and RADIUS authentication on FortiGate. You will also review some FortiAuthenticator basics.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

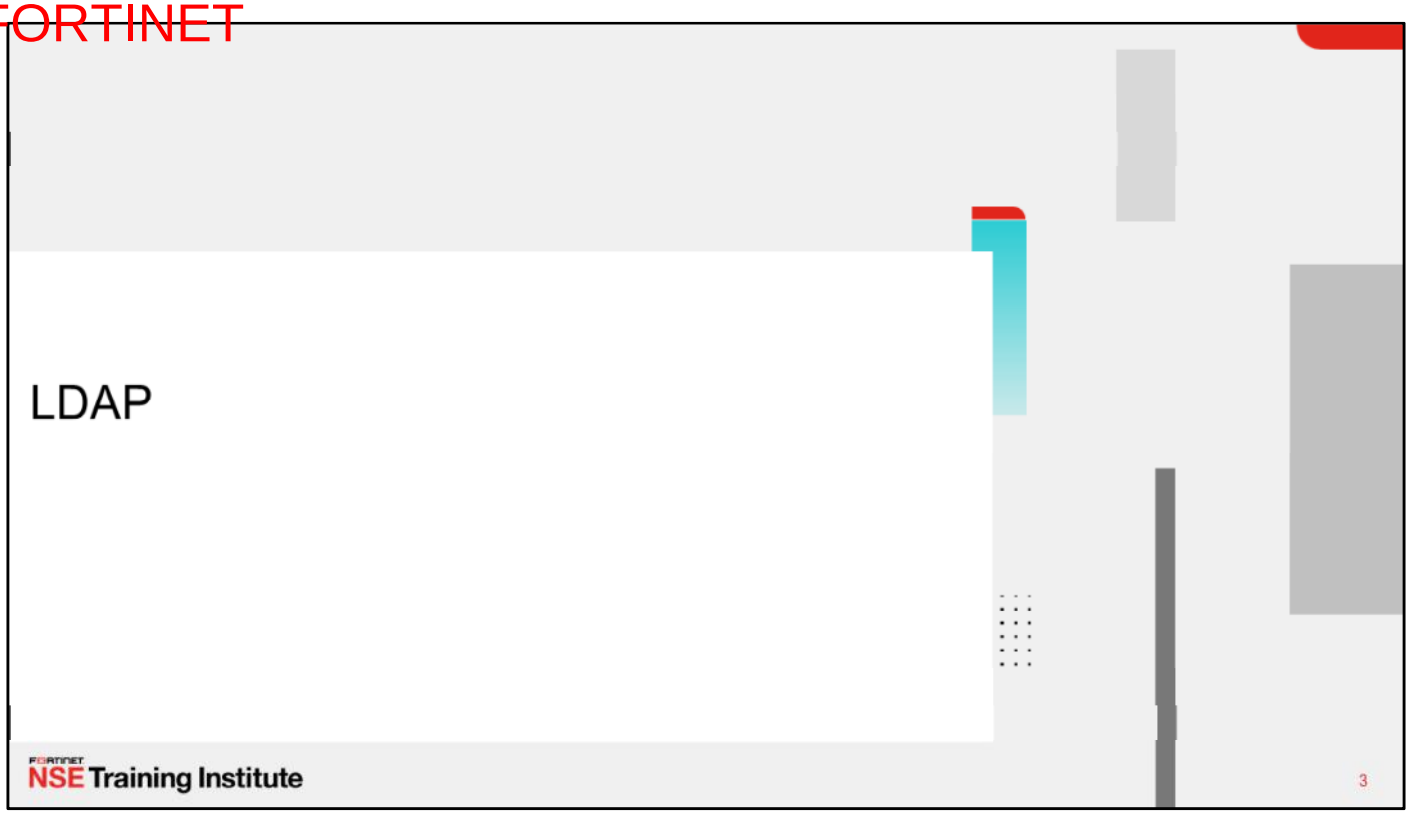


After completing this lesson, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in remote authentication and FortiAuthenticator, you will be able to understand and troubleshoot LDAP bind flow and RADIUS query flow, and integrating FortiAuthenticator with FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

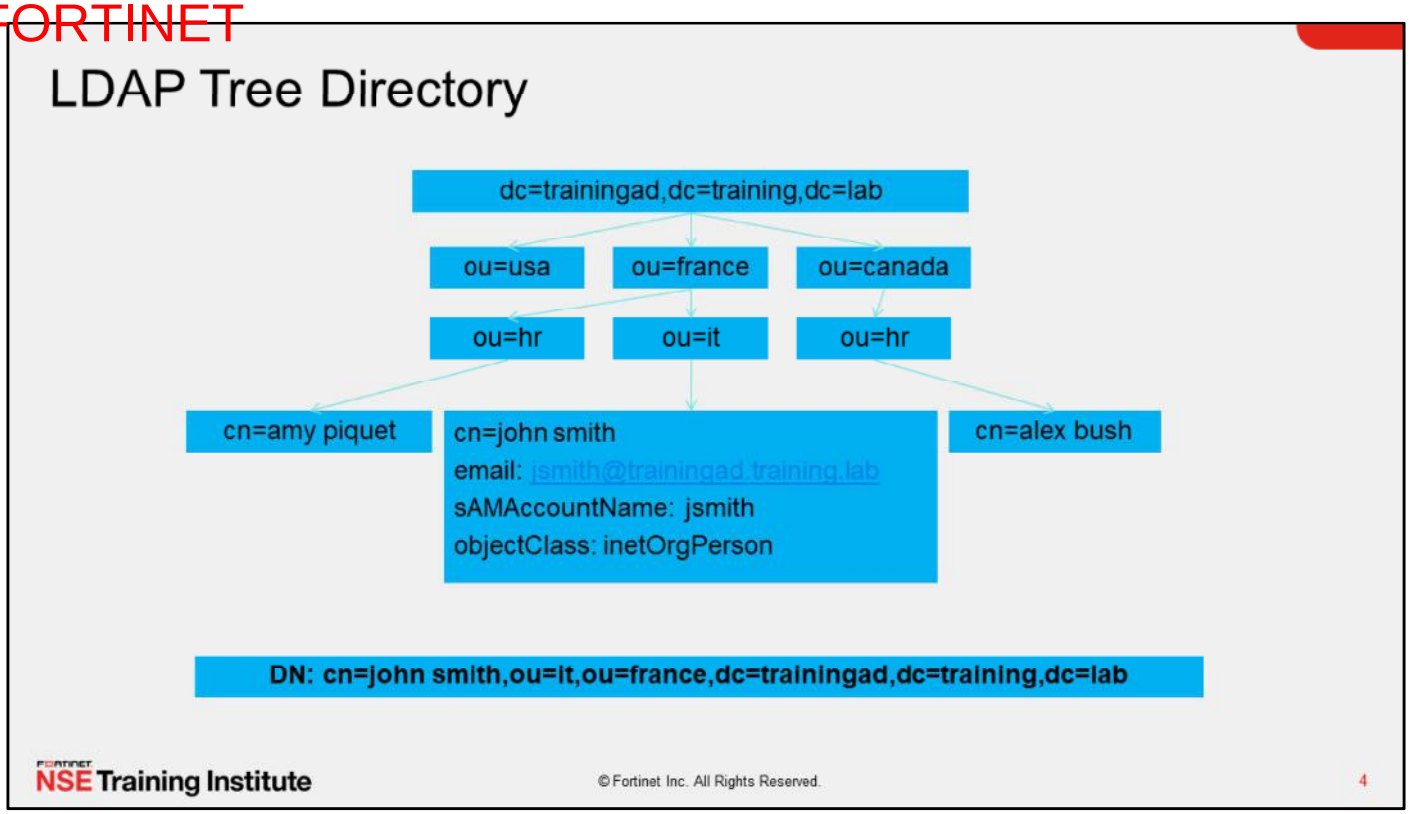
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn about LDAP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



To begin, you will review the LDAP protocol.

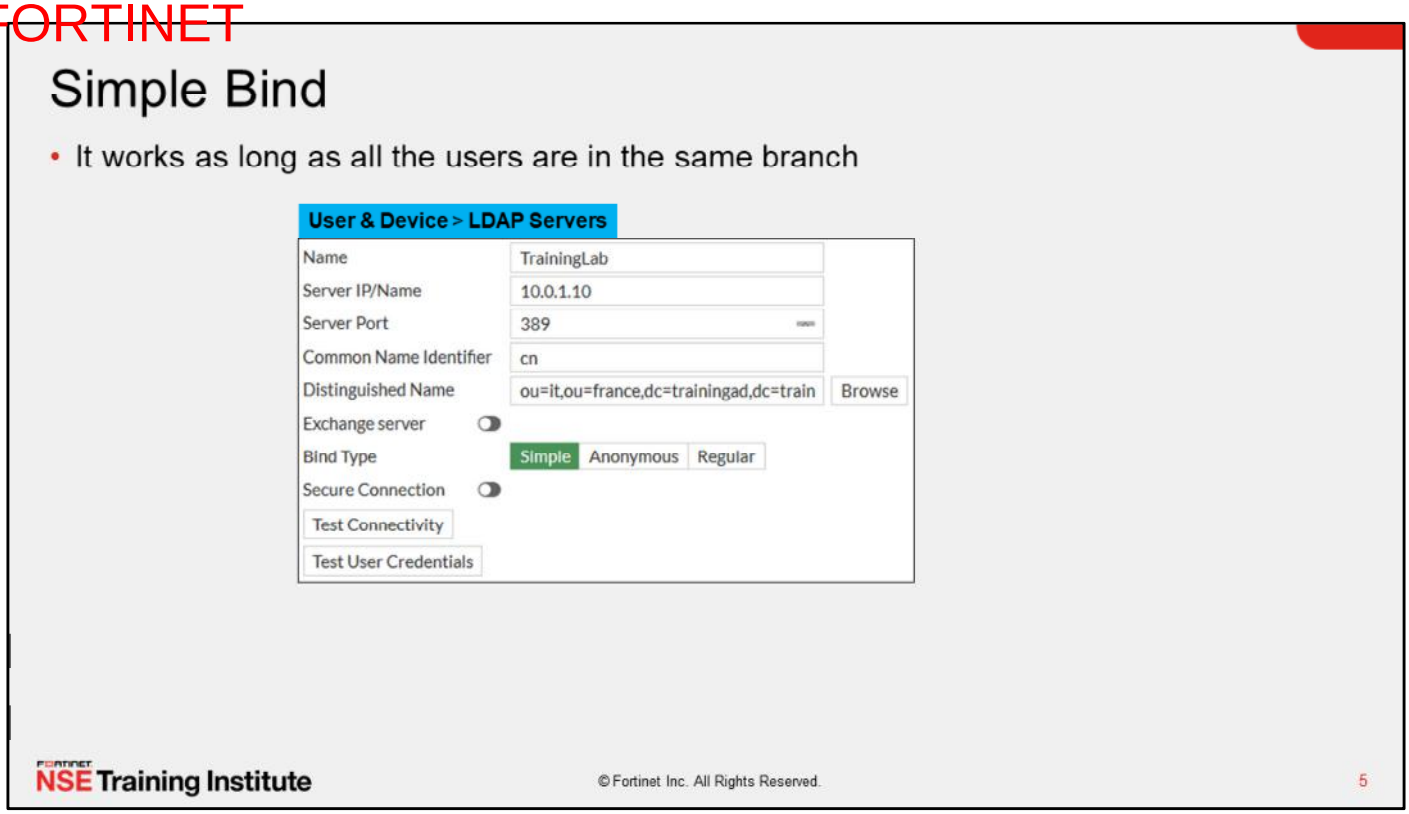
The hierarchy of an LDAP schema does not need to resemble the organizational hierarchy. However, the naming conventions and group structure usually match the company name and organizational hierarchy very closely.

At the top of the LDAP schema is the root, or DC. This is where an LDAP tree always starts, in any schema.

Next, the groups (or branches) are defined using CN or OU. The exact behavior and options used depend on the schema and what is being defined. Branches may contain objects, and each object contains attributes. Objects are uniquely identified by their distinguished names (DNs). The full DN specifies where the object is, and the name and value of an attribute that can be used to find it.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



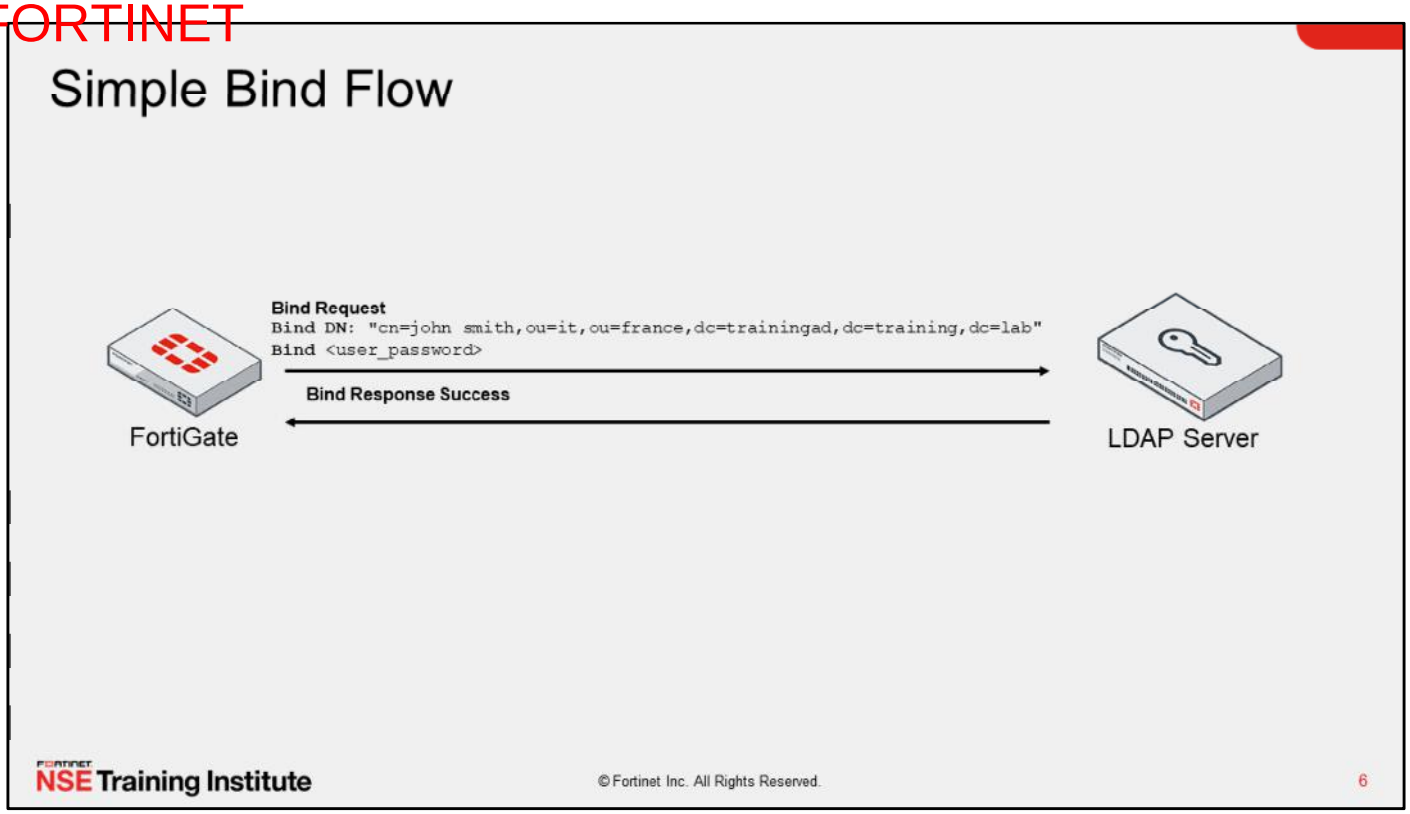
There are three different methods, or bind types, a FortiGate can use to access an LDAP server: simple, anonymous, and regular. In this lesson, you will learn about simple and regular binds.

A simple bind works as long as all accounts are in the same branch of the LDAP tree. The **Distinguished Name** field defines the scope of the LDAP lookup. For example, if your distinguished name is set to `ou=it, ou=france, dc=trainingad, dc=training, dc=lab`, only the users found under IT > France will be able to authenticate. However, you will not be able to authenticate the users under any of the other containers.

In the example shown on this slide, **Common Name Identifier** is set to `cn`. As a result, the DN of the LDAP queries will have the form cn=*id*, ou=it, ou=france, dc=trainingad, dc=training, dc=lab, where *id* refers to the user being authenticated.

Vouchers & Dumps are Available | WhatsApp +201224560923

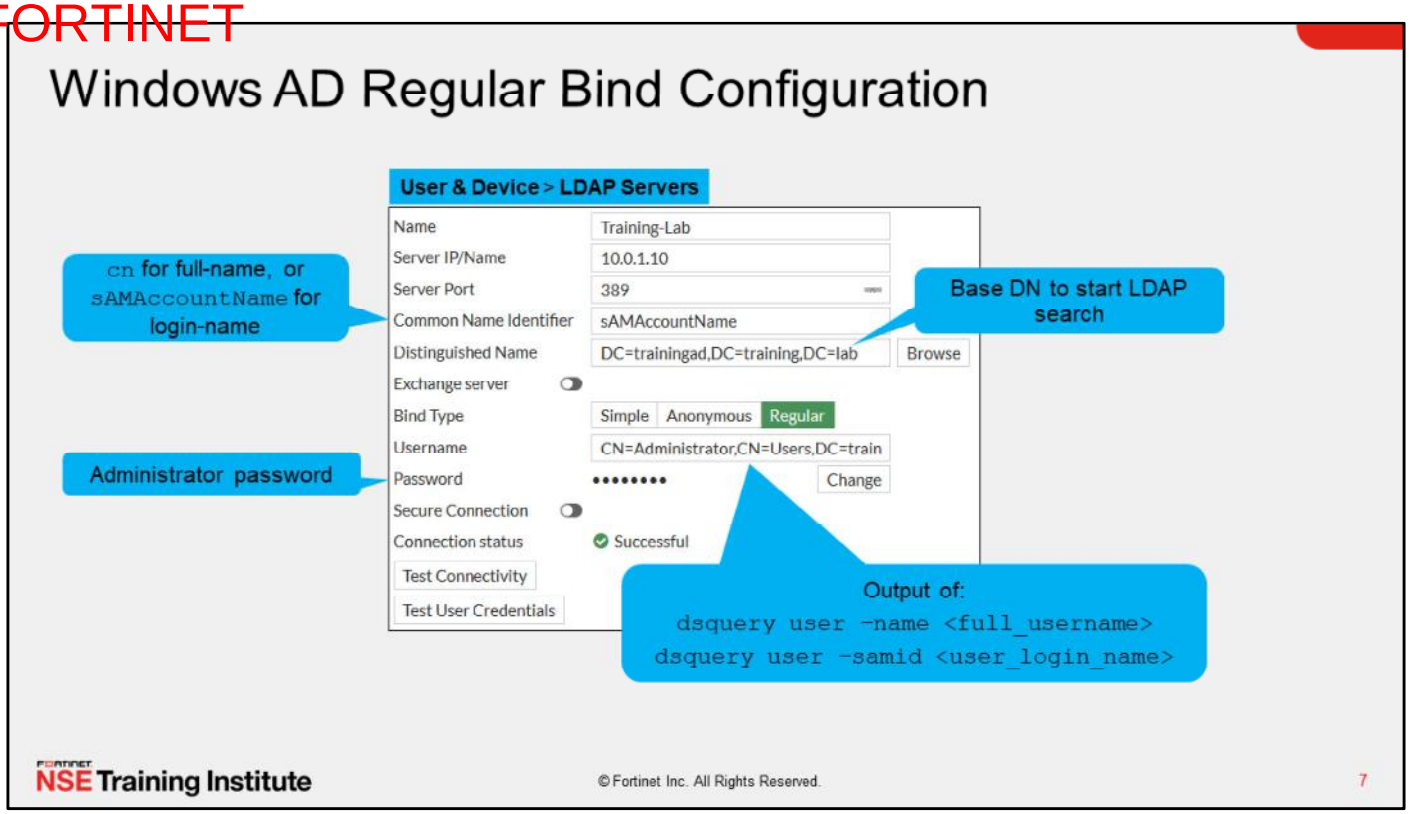
DO NOT REPRINT
© FORTINET
Brave-dumps.com



When you use simple bind flow, FortiGate sends a bind request for the user who wants to authenticate with the LDAP server. If the authentication is successful, the server responds to FortiGate with a Bind Response Success message.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows a summary of how to correctly configure regular bind for Windows AD. A different type of LDAP server might require a different approach.

First, the **Common Name Identifier** is usually either `cn` or `sAMAccountName`. If you set it to `cn`, users must authenticate using their full names (for example, `John Smith`). If you set it to `sAMAccountName`, users must authenticate using their login names (for example, `jsmith`).

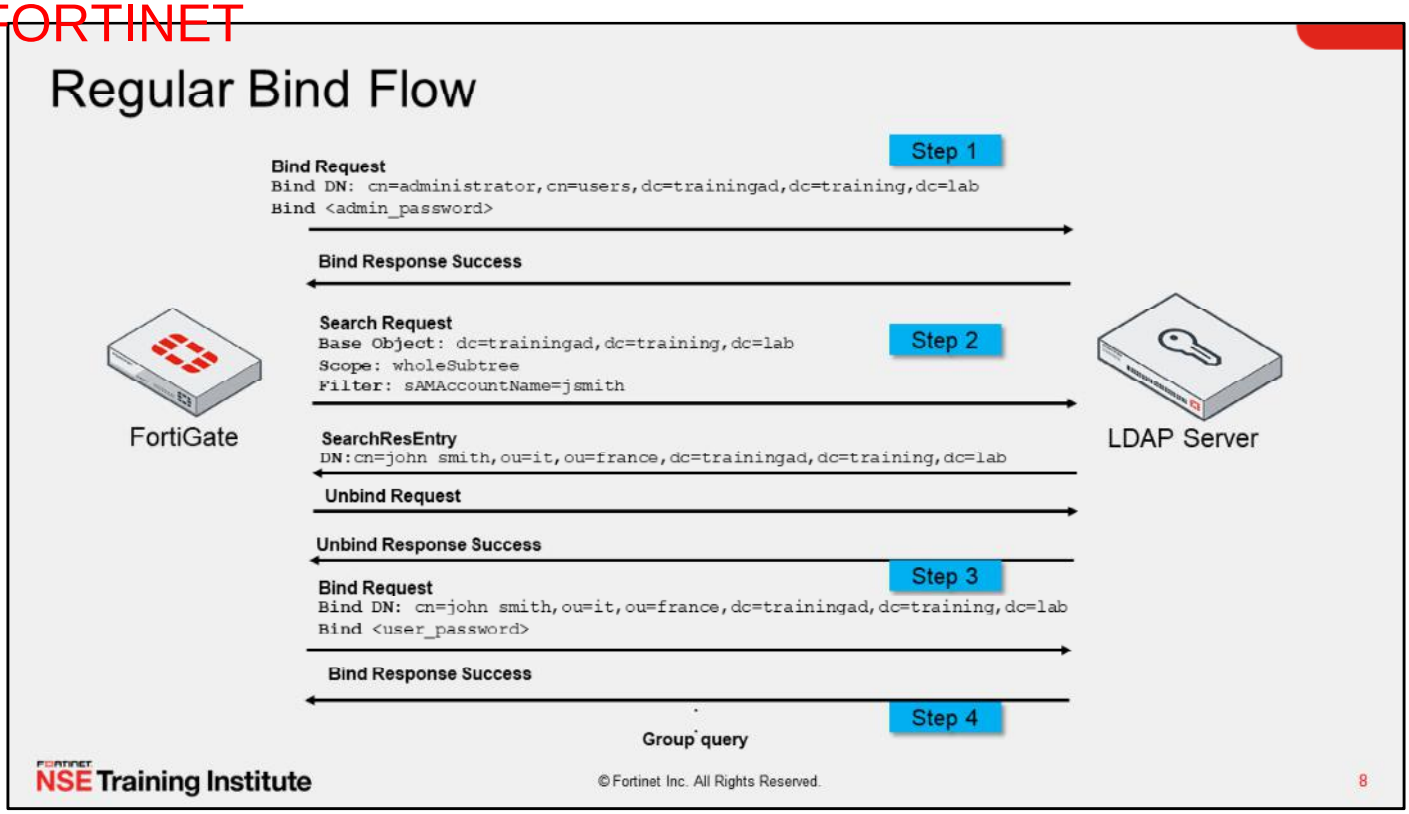
You can determine the **Distinguished Name** by querying the user DNs with the Windows AD command `dsquery`.

You can determine the **Username** by querying the administrator DN with the same Windows AD command `dsquery`.

Finally, the **Password** setting is the LDAP administrator password.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Regular bind is the most complex, versatile, and commonly used method. You complete LDAP authentication using regular bind in four steps:

1. FortiGate logs in to (binds to) the LDAP server, using an administrator account. After this step, FortiGate knows only the username. It doesn't know the branch where the user is located.
2. FortiGate performs a search query in the LDAP database to locate the user. In other words, to find the user's DN. If the user is found, the server replies with the user DN. Then, FortiGate logs out of (unbinds from) the LDAP server.
3. FortiGate binds to the LDAP server again, using the user credentials this time. It sends the DN it learned in step 2, along with the password.
4. FortiGate gets the user attribute and group information. The method it uses for this depends on the type of LDAP server, but it's usually an LDAP query.

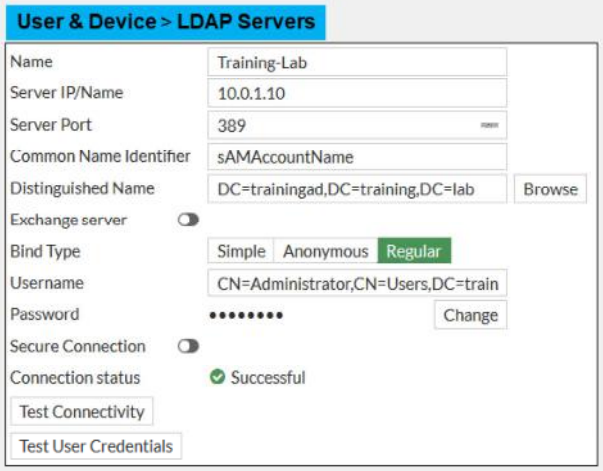
When isolating an LDAP problem, you must first identify which of these four steps is failing.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Regular Bind Configuration

- Misconfigurations usually happen in one of the following LDAP settings:
  - **Common Name Identifier**
  - **Distinguished Name**
  - **Username**
  - **Password**
- The attribute `cn` is typically used as the **Common Name Identifier**
  - For Windows AD deployments, you can also use `sAMAccountName`



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

9

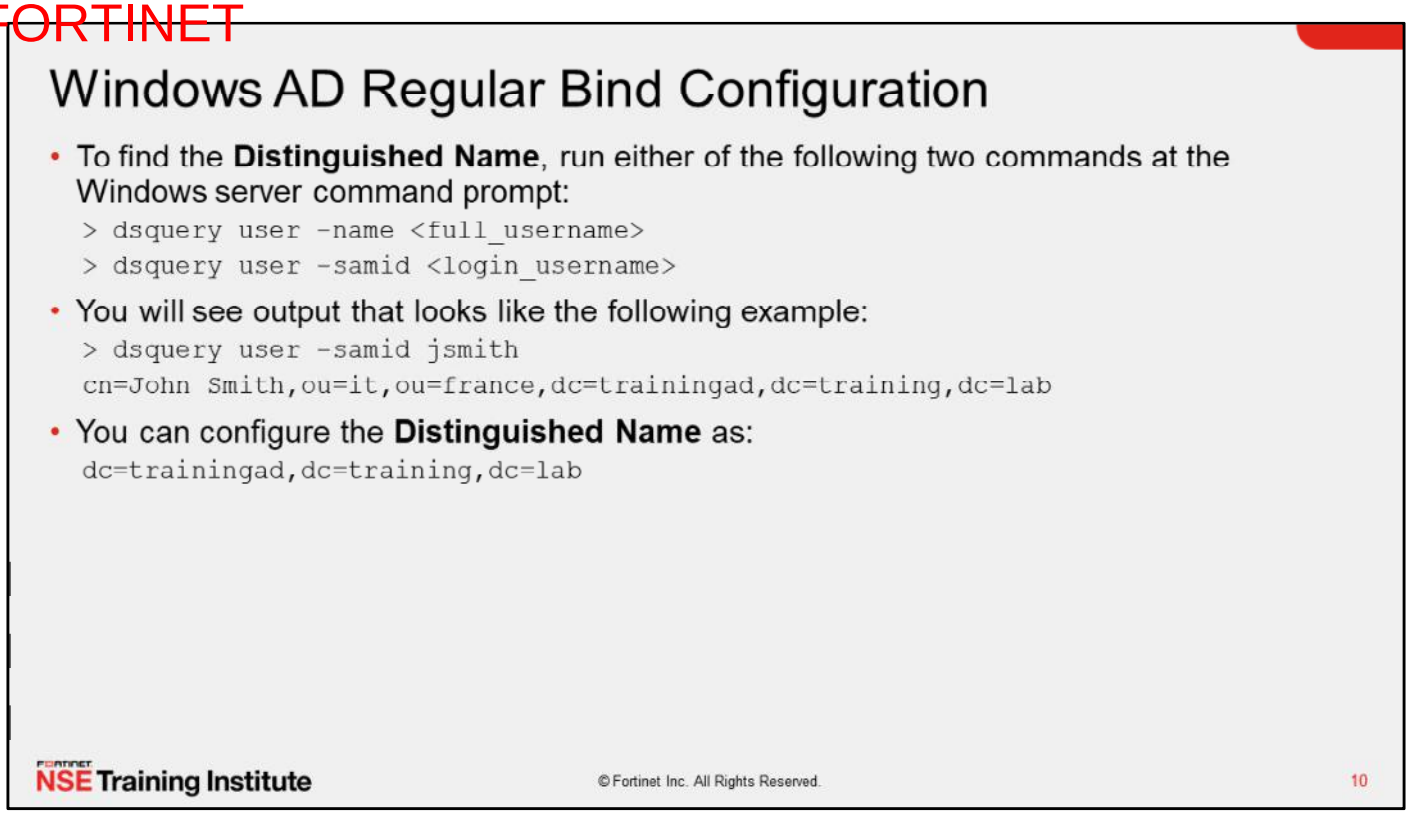
Most LDAP authentication problems are caused by misconfigurations, which usually happen in one of the following LDAP settings:

- **Common Name Identifier**
- **Distinguished Name**
- **Username**
- **Password**

Authentication problems most commonly occur on LDAP servers based on Windows AD. In this lesson, you will verify if the regular bind LDAP configuration on such a server is correct.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



How do you check if the *distinguished name* is correct? You can run either of the following two commands at the Windows AD server command prompt:

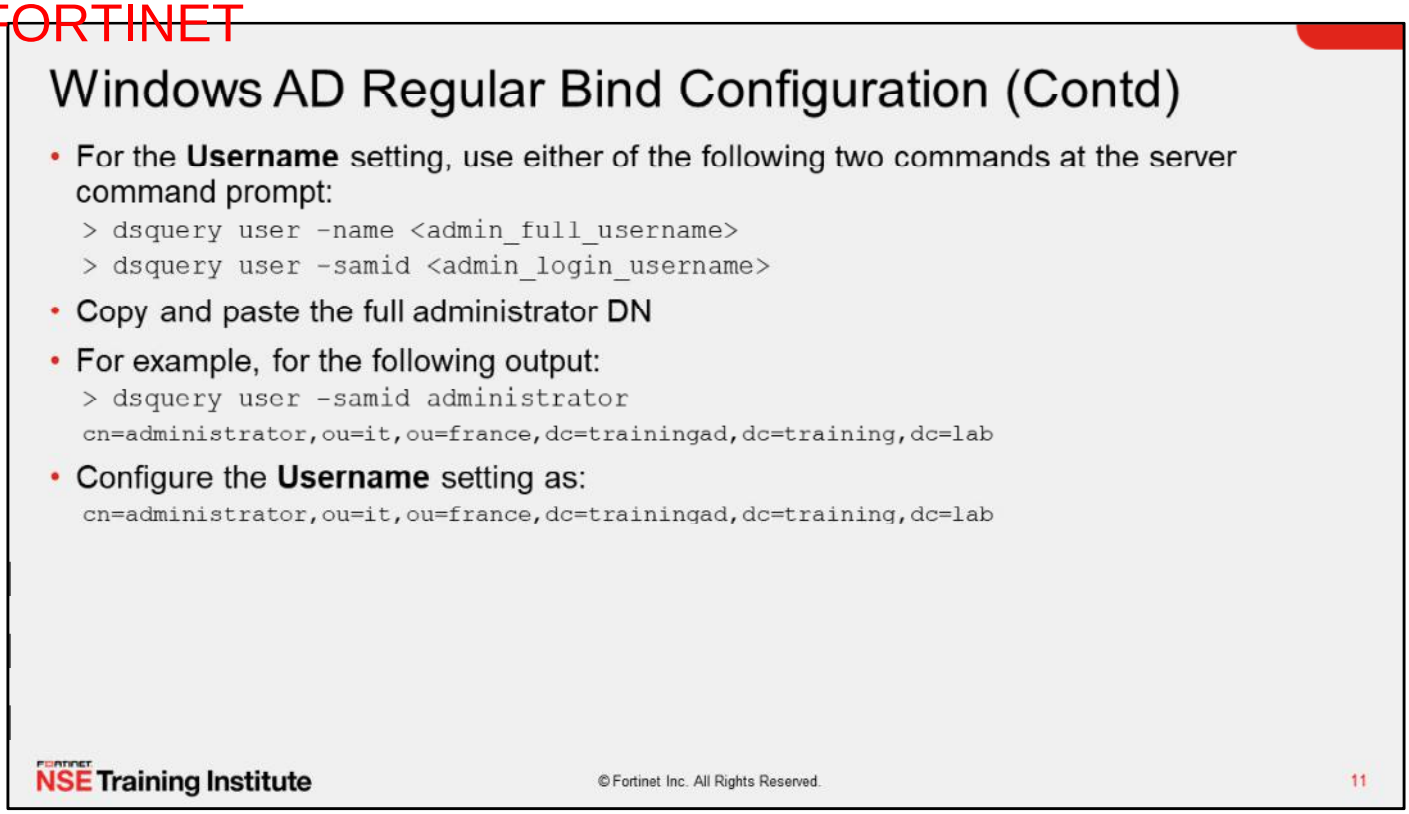
```
dsquery user -name <full_username>
dsquery user -samid <login_username>
```

The output displays the user DN. The **Distinguished Name** setting specifies a parent branch under which all users are located. FortiGate searches users in any sub-branch below this parent branch. For example, in the case shown on this slide, you can set the **Distinguished Name** setting to:

```
dc=trainingad,dc=training,dc=lab
```


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The **Username** setting is the full DN of the LDAP administrator account. You can use the same Windows LDAP server command (`dsquery`) to find that information.

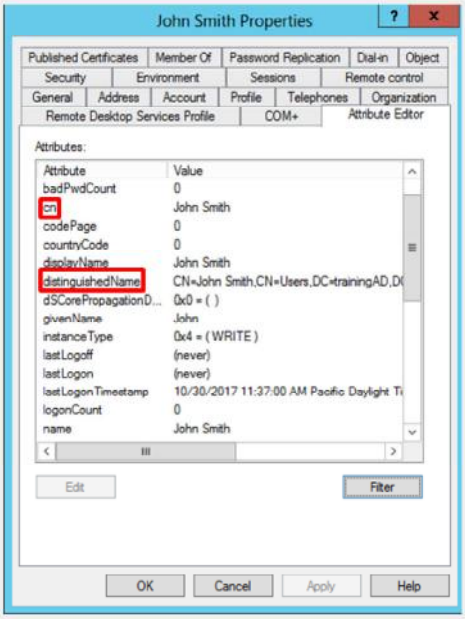
You can copy and paste the full DN output from the server command prompt to the FortiGate configuration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Attribute Editor

- Enable **Advanced Features** in Windows AD to:
  - Use the **Attribute Editor** tab to view all configured attributes under an object's properties
  - Configure additional attributes
- Any of the attributes can be used as the common name identifier



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

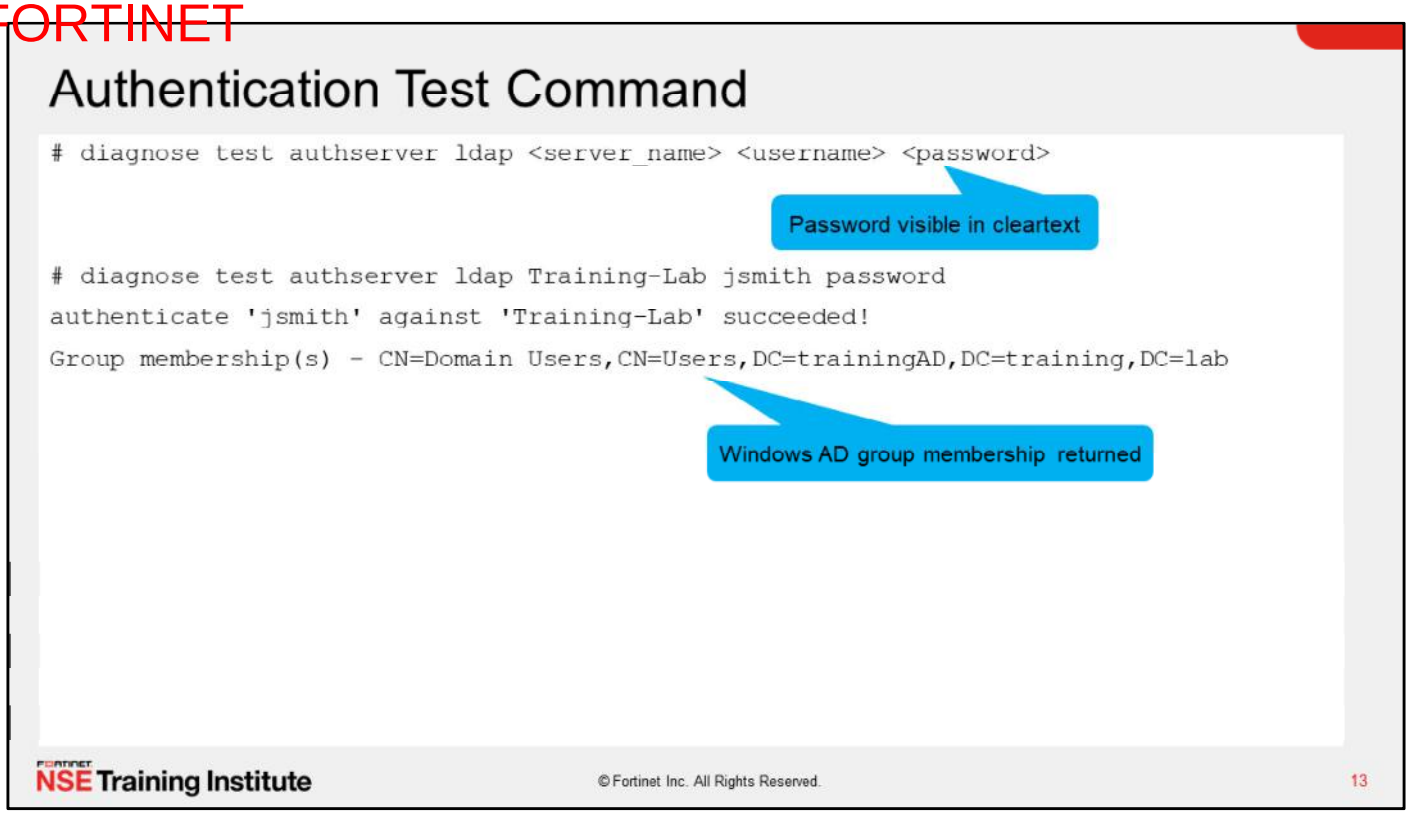
12

You can view the LDAP attributes in the **Attribute Editor** under the properties for each object. Here, you can see the value of all available LDAP attributes. For regular binds, you can use any attribute in the user object as the common name identifier. FortiGate then uses the attribute to perform an LDAP search to find the user in the directory.

Note that you must enable **Advanced Features** in Windows AD to have access to the **Attribute Editor** tab.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

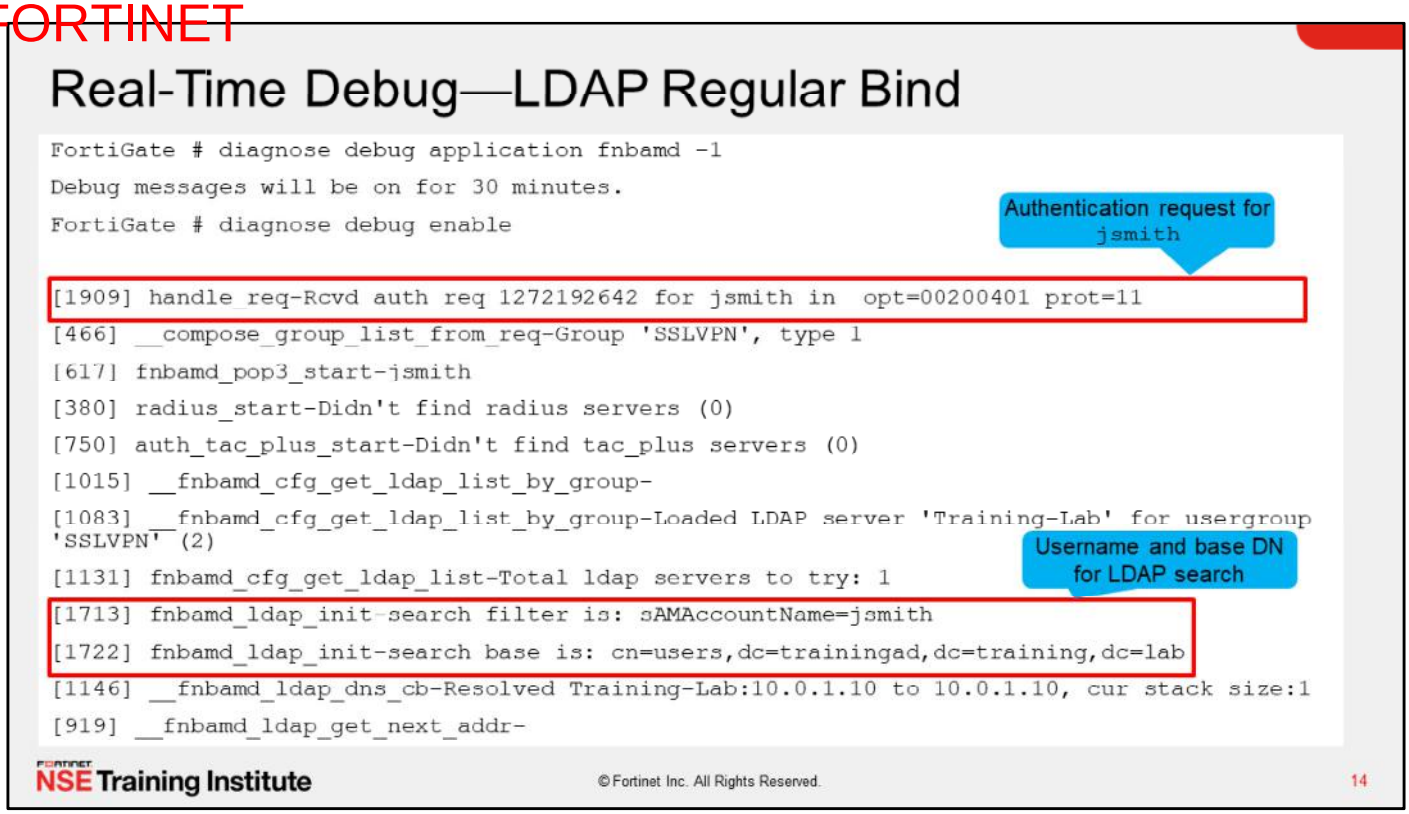


The CLI includes an LDAP authentication test command: `diagnose test authserver ldap`. If the credentials are correct, and if the LDAP configuration is correct, the LDAP server returns an authentication confirmation and a list of the user groups for that user.

You can run this test command as soon as you complete the LDAP server configuration, even before any user group or authentication firewall policy has been added to FortiGate. It tests only the LDAP server configuration and the LDAP communication between FortiGate and the server.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

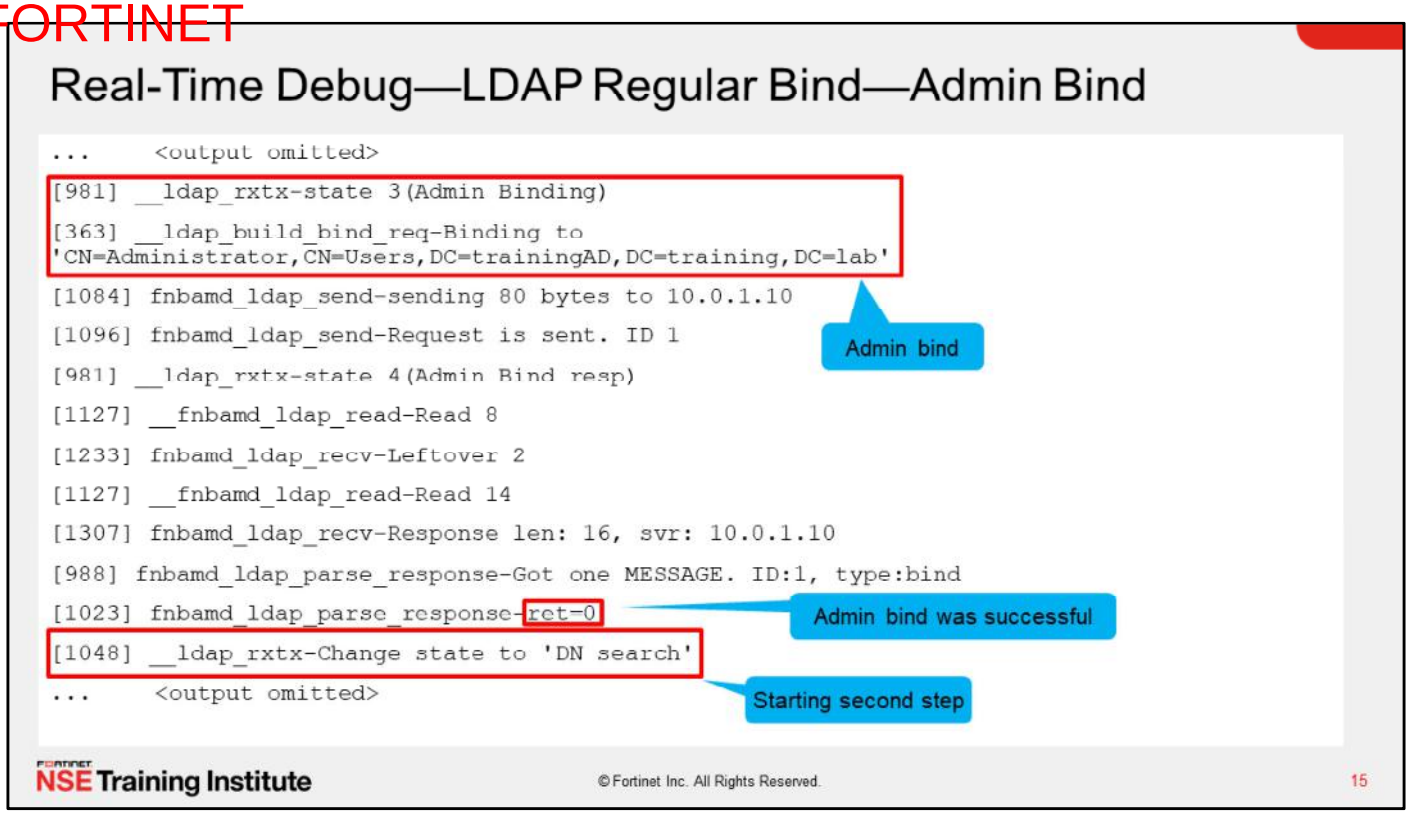


The Fortinet non-blocking authentication module daemon (`fnbamd`) is the process that handles LDAP and RADIUS authentication. This command enables the real-time debug for the `fnbamd` daemon.

In the example shown on this slide, the `handle_req-Rcvd auth` message indicates that FortiGate received a request for authentication for user `jsmith` on the `Training-Lab` LDAP server. Below the initial message, you will find more information, such as the attribute that you use to search the user in the LDAP tree, base DN, and server name/IP address.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

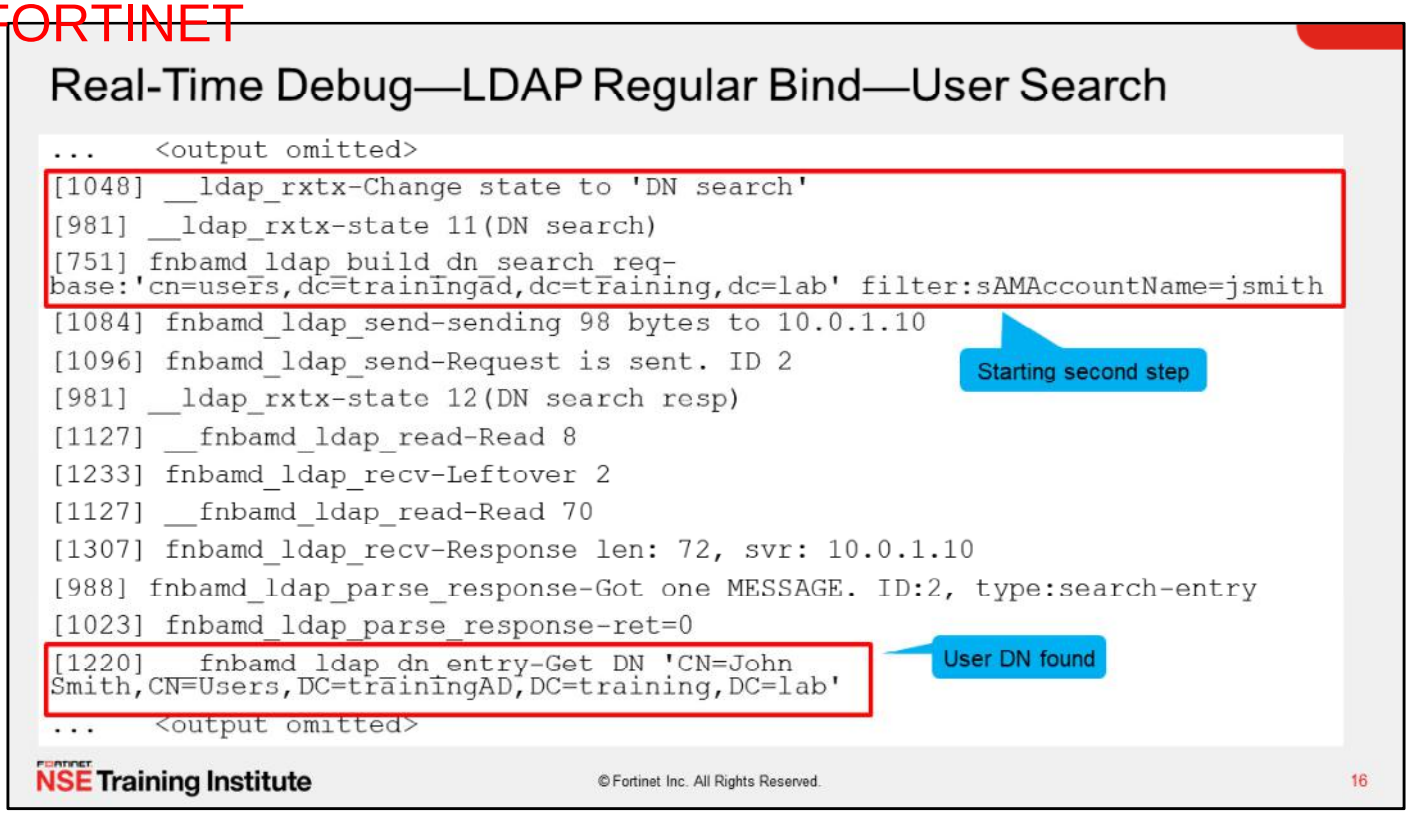


Continuing with the output, the next step for FortiOS is to perform an admin bind, since this example uses regular LDAP bind. This is the first step of the regular bind flow that starts with the `Admin Binding` heading. You can see that FortiOS is requesting authentication for the `administrator` user and message `ID 1`, which indicates that this is the first step of the regular bind process.

The `Change state to 'DN search'` message indicates that the first step was successful, and FortiOS is initiating the second step of the regular bind flow.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

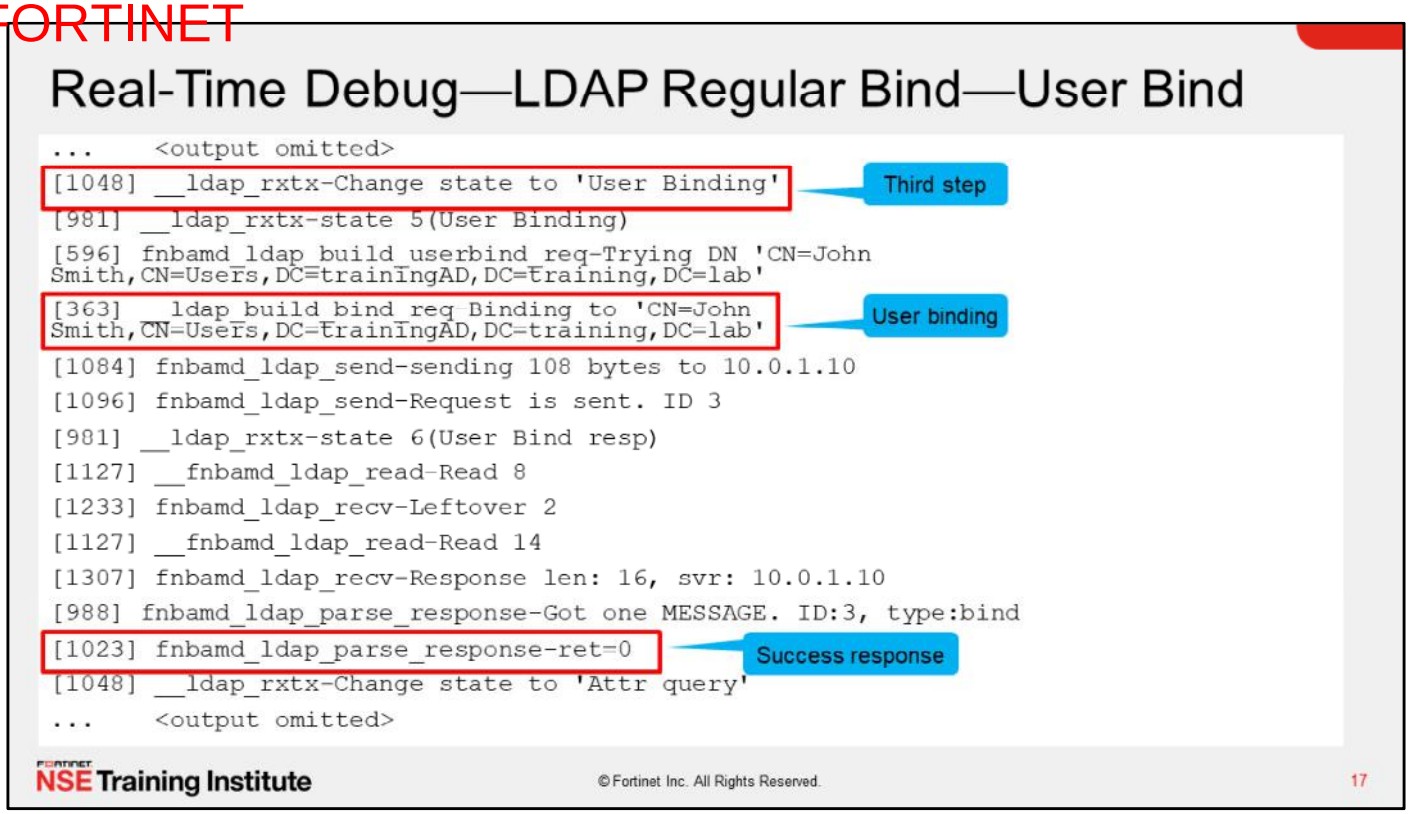


Continuing with the `fnbamd` output, this section indicates that FortiGate is performing the second step, which is searching for the user in the LDAP tree. The message includes the `base` branch (**Distinguished Name** setting) and the name of the attribute used to locate the user (**Common Name Identifier** setting).

If a user is located on the LDAP server, the LDAP server responds with the user DN.

Vouchers & Dumps are Available | WhatsApp +201224560923

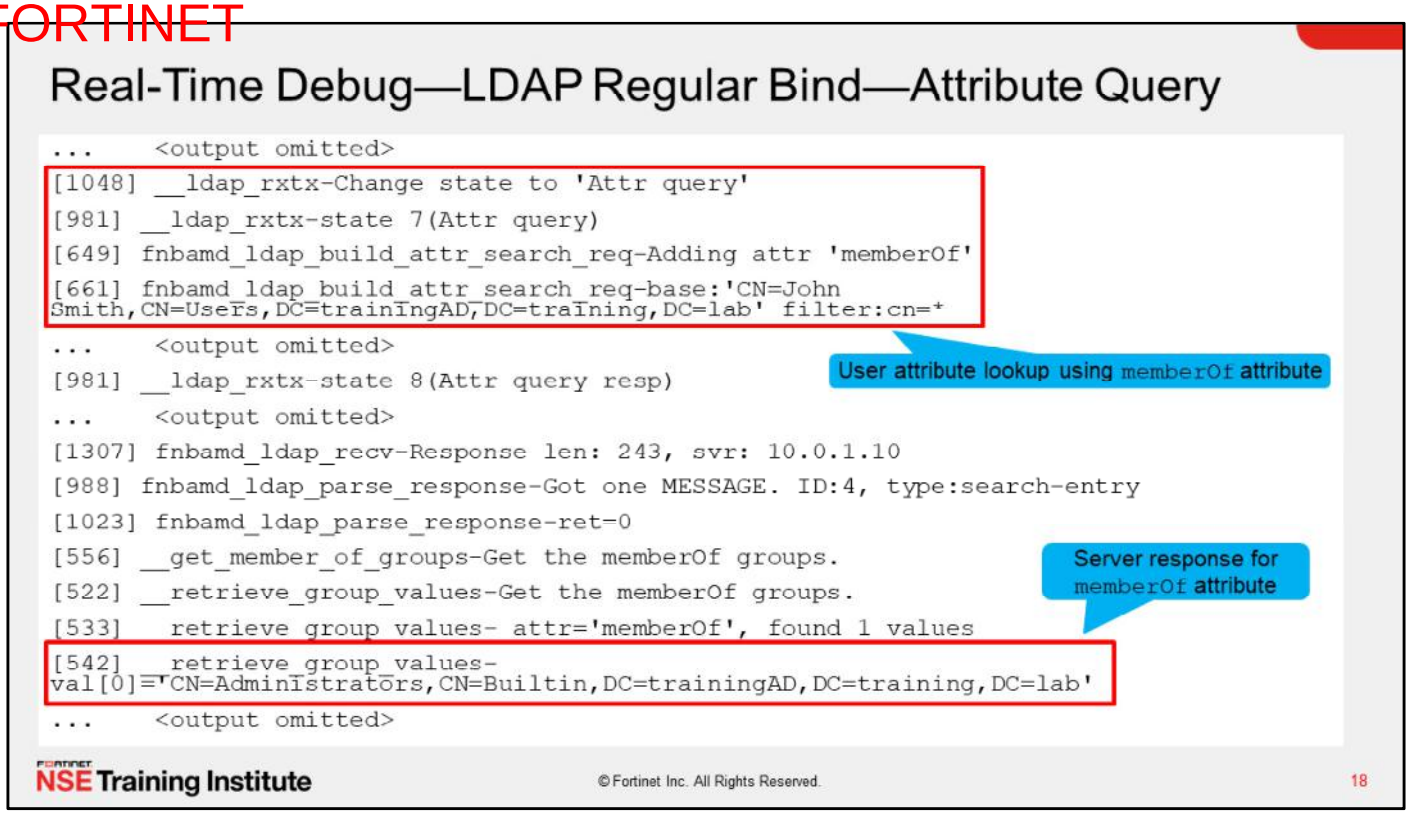
DO NOT REPRINT
© FORTINET
Brave-dumps.com



`Change state to 'User Binding'` indicates the third step in the regular bind. In this step, FortiGate requests authentication for user `John Smith`, and `User Bind resp` indicates the reply from the LDAP server. If user authentication is successful, the process moves on to the last step of the process.

Vouchers & Dumps are Available | WhatsApp +201224560923

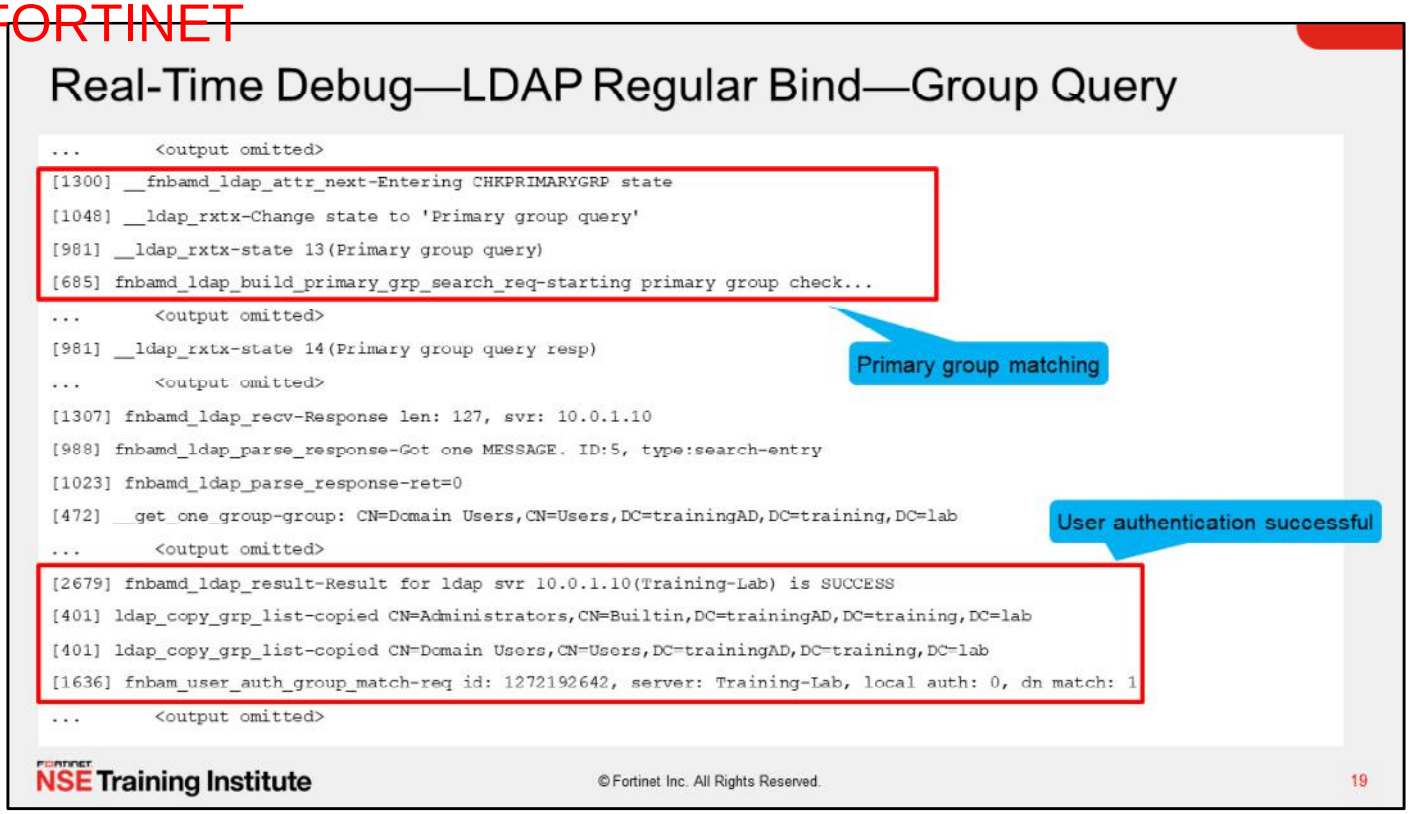
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The last step in the regular bind process is attribute and group query. In this example, FortiGate queries the `memberOf` attribute from the LDAP server, and the LDAP server replies with the information.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Next, is the `Primary group query` of the authenticating user. The server responds with the primary group of the user, which FortiGate binds to the user. This completes the steps in the LDAP regular bind process. `SUCCESS` indicates that authentication was successful and FortiGate now has all of the required information for the authenticated user.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Sniffer for LDAP Traffic

```
# diagnose sniffer packet any "port 389" 6
```

AD code	Description
0x525	user not found
0x52e	invalid credentials
0x530	not permitted to logon at this time
0x531	not permitted to logon from this workstation
0x532	password expired
0x533	account disabled
0x701	account expired
0x773	user must reset password
0x775	account locked out

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

20

If there is a problem with either step 1 (admin bind) or step 3 (user bind), you can sniff the traffic between FortiGate and the LDAP server to get the error code. Error codes provide an explicit description of why the bind is failing.

The table on this slide describes the codes returned by the Windows AD server.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

LDAP Result Codes

- Common industry-standard LDAP result codes

LDAP Error	Description
0	SUCCESS
2	PROTOCOL ERROR
7	AUTH METHOD NOT SUPPORTED
16	NO SUCH ATTRIBUTE
21	INVALID SYNTAX
32	NO SUCH OBJECT
34	INVALID DN SYNTAX
49	INVALID CREDENTIALS/ ACCOUNT DISABLED
50	LDAP INSUFFICIENT ACCESS

NSE Training Institute

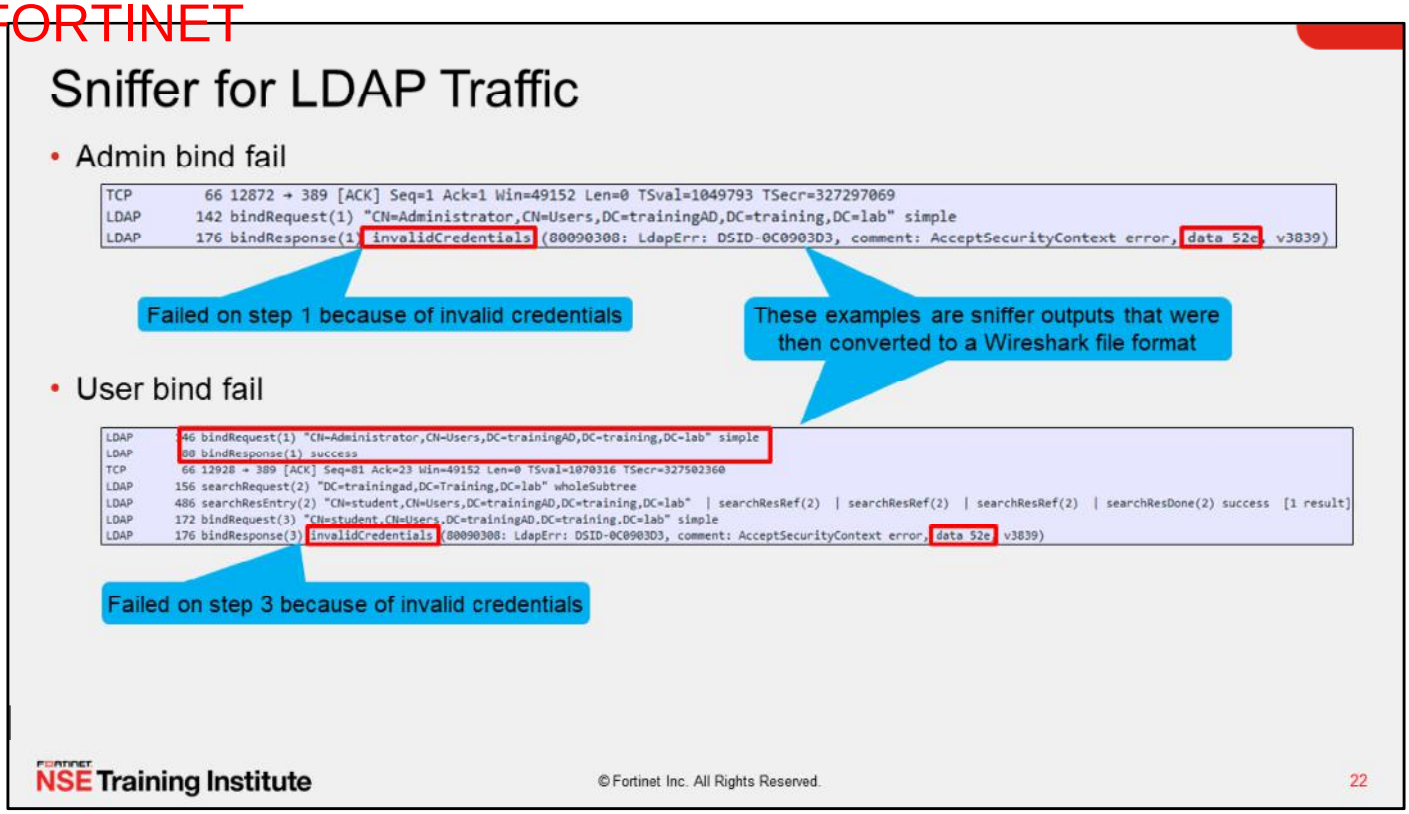
© Fortinet Inc. All Rights Reserved.

21

Here are a few industry-standard LDAP result codes. During LDAP authentication, the LDAP server returns a result code for both successful and unsuccessful authentication attempts, which can indicate why an authentication attempt was unsuccessful. For unsuccessful authentication requests, this error code can be used to understand why an authentication failed. To get the full list of LDAP result codes, review RFC 4511.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



If there is a problem with either step 1 (admin bind) or step 3 (user bind), you can sniff the traffic between FortiGate and the LDAP server to get the error code. Error codes provide an explicit description of why the bind is failing.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Common Problems: Incorrect Bind Password

```
...   <output omitted>
[977] __ldap_rxtx-state 3(Admin Binding)
[206] __ldap_build_bind_req-Binding to
'CN=Administrator,CN=Users,DC=trainingAD,DC=training,DC=lab'
...   <output omitted>
[977] __ldap_rxtx-state 4(Admin Bind resp)
...   <output omitted>
[831] fnbamd_ldap_parse_response-Got one MESSAGE. ID:1, type:bind
[853] fnbamd_ldap_parse_response-Error 49(80090308: LdapErr: DSID-
0C0903C5, comment: AcceptSecurityContext error, data 52e, v23f0)
[866] fnbamd_ldap_parse_response-ret=49
[784] __ldap_done-svr 'Training-Lab'
[725] __ldap_stop-Conn with 10.0.1.10 destroyed.
[190] fnbamd_comm_send_result-Sending result 1 (error 0, nid 0) for req
729206354, len=2060
...   <output omitted>
```

LDAP error code 49 for invalid credentials

Step 1

NSE Training Institute

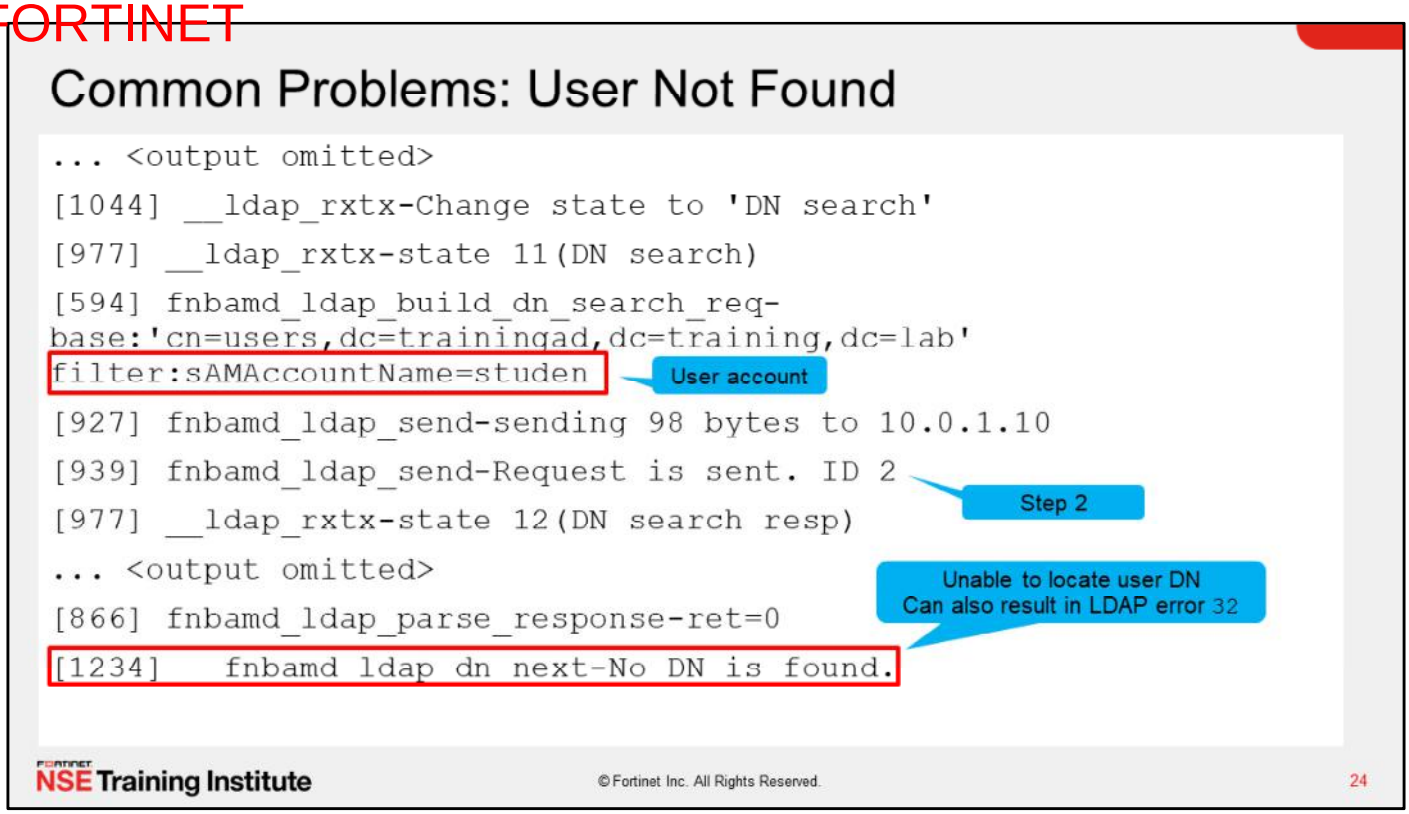
© Fortinet Inc. All Rights Reserved.

23

The real-time debug for LDAP displays `error 49` for invalid credentials.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The message `No DN is found` in step 2 refers to the fact that the authentication request was unable to locate the user in the LDAP tree. This indicates a problem with the username, or the user resides in an LDAP branch that is outside the scope of the LDAP search path.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Common Problems: Incorrect User Password

```
[1044] __ldap_rxtx-Change state to 'User Binding'
[977] __ldap_rxtx-state 5(User Binding)
[439] fnbamd_ldap_build_userbind_req-Trying DN
'CN=student,CN=Users,DC=trainingAD,DC=training,DC=lab'
[206] __ldap_build_bind_req-Binding to
'CN=student,CN=Users,DC=trainingAD,DC=training,DC=lab'
[927] fnbamd_ldap_send-sending 106 bytes to 10.0.1.10
[939] fnbamd_ldap_send-Request is sent. ID 3
[977] __ldap_rxtx-state 6(User Bind resp)
...   <output omitted>
[1150] fnbamd_ldap_recv-Response len: 104, svr: 10.0.1.10
[831] fnbamd_ldap_parse_response-Got one MESSAGE. ID:3, type:bind
[853] fnbamd_ldap_parse_response-Error 49 (80090308: LdapErr: DSID-
0C0903C5, comment: AcceptSecurityContext error, data 52e, v23f0)
[866] fnbamd_ldap_parse_response-ret=49
```

User DN

Step 3

Invalid credentials

NSE Training Institute

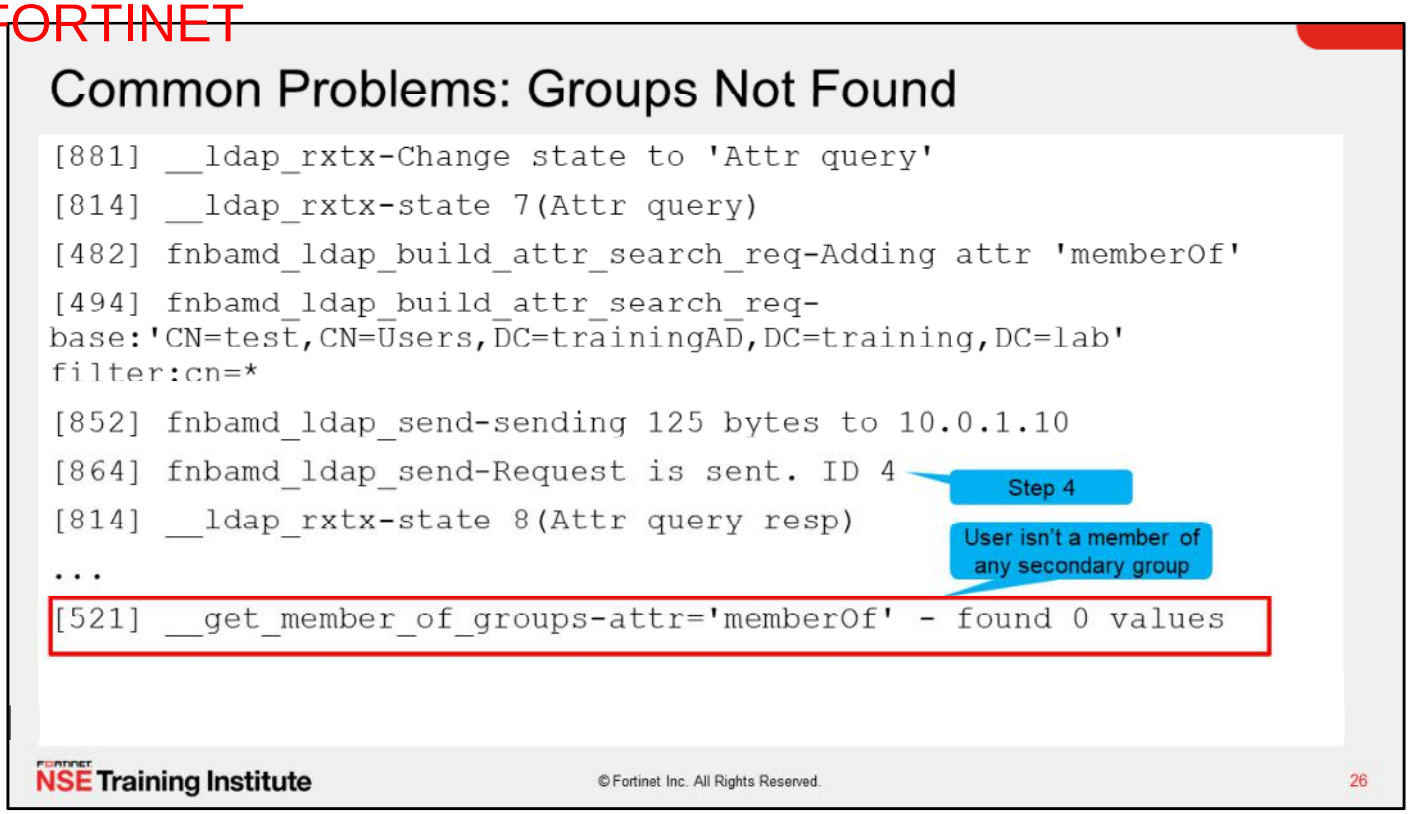
© Fortinet Inc. All Rights Reserved.

25

`Error 49` in step 3 indicates that the user credentials are invalid, or the user account is disabled on Windows AD.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Finally, the following error indicates a problem in step 4:

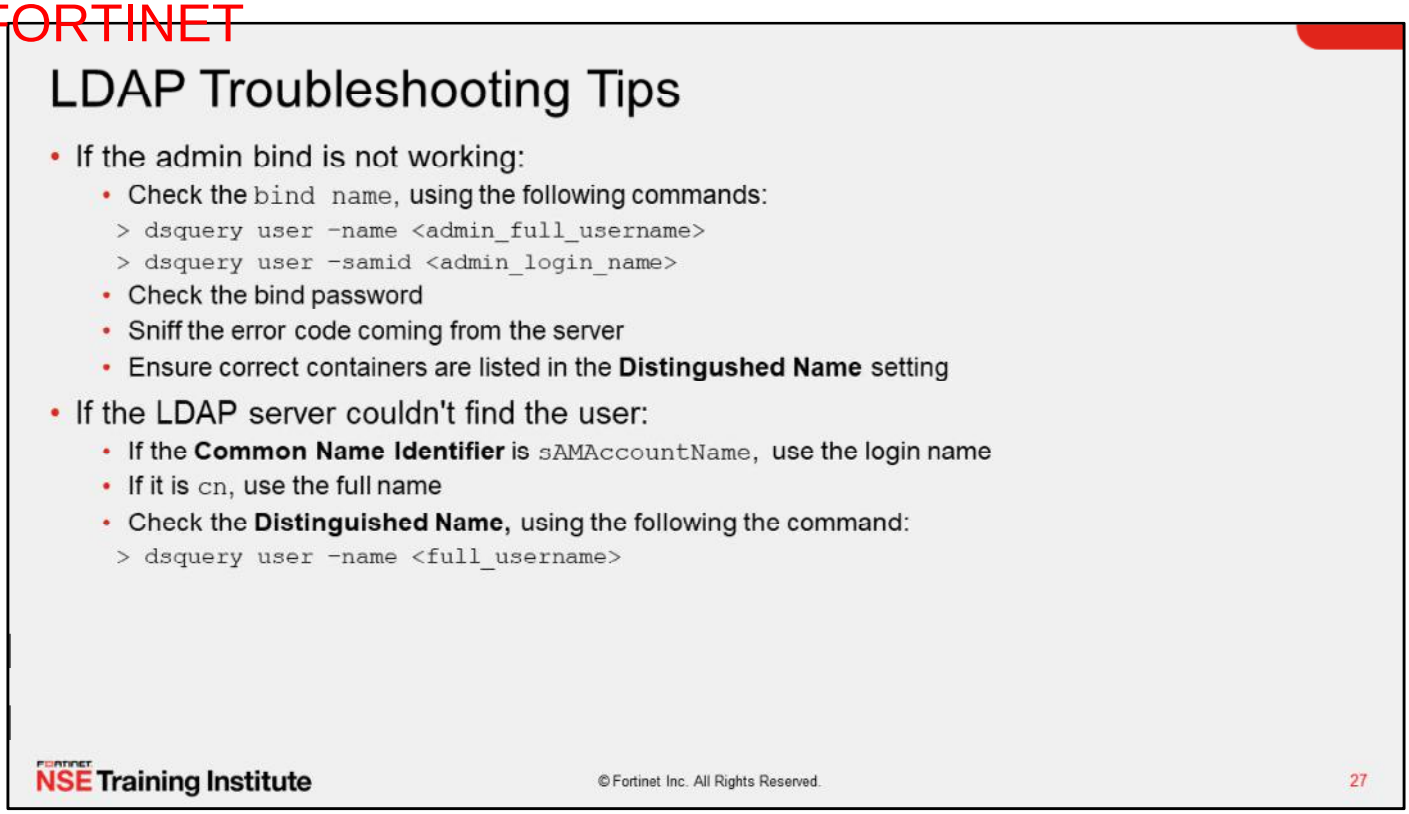
```
get_member_of_groups-attr=<attribute_name> found 0 values
```

The user credentials are correct, but no user group information was found.

In some LDAP implementations, the user group information is not an attribute of the user. Instead, the users are listed as an attribute of the group. In these instances, you need to query the group of the user. There is additional configuration that allows FortiGate to work with these implementations, but the debug does not reflect this, in these cases. In these implementations, you can ignore this error.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



What should you do if the problem is in step 1 (admin bind not working)?

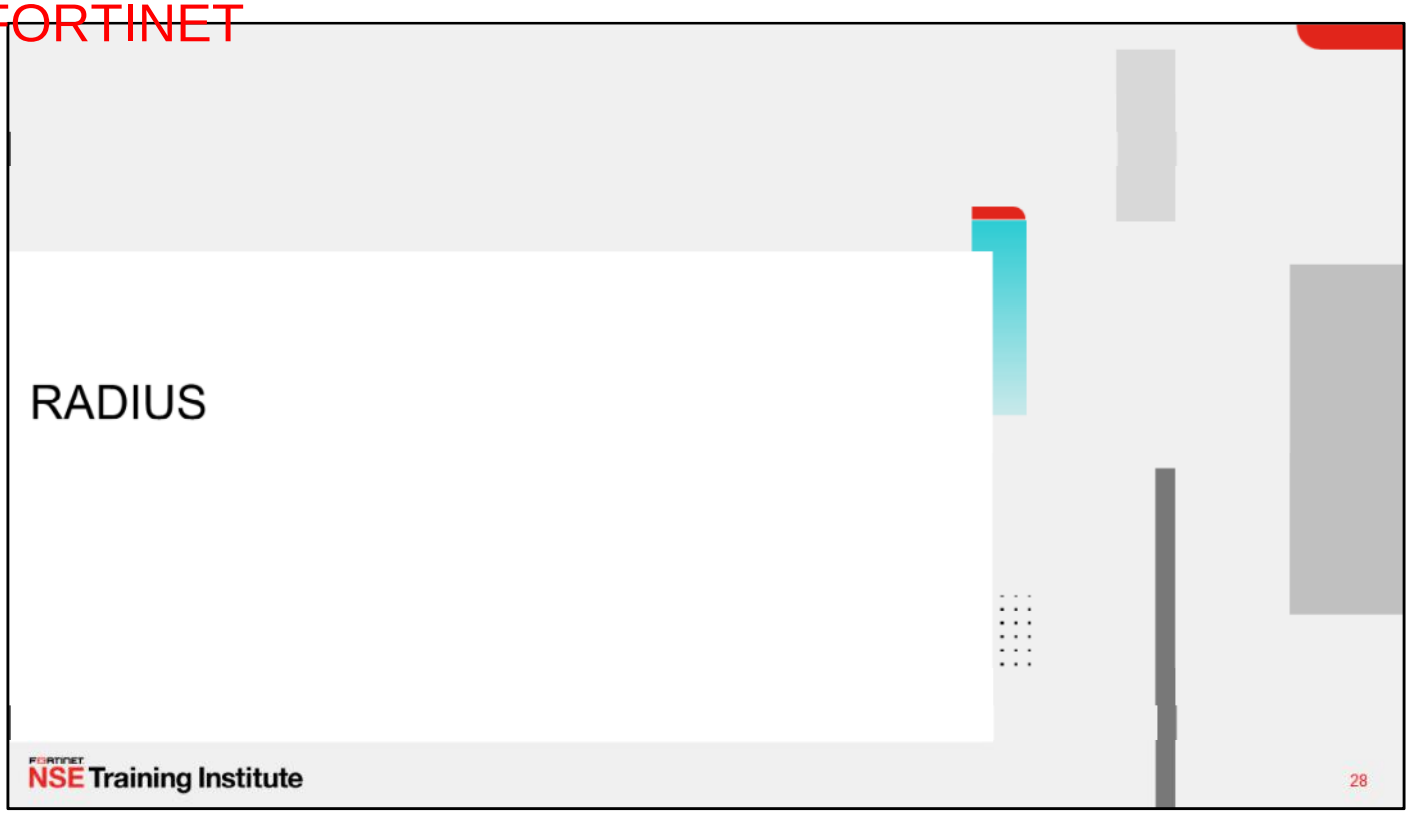
- Use the `dsquery` query to check the administrator DN
- Check the administrator password
- Sniff the error code coming from the server

What should you do if the problem is in step 2 (LDAP server could not find the user)?

- If the **Common Name Identifier** is set to `sAMAccountName`, the user must use the login name. If it is set to `cn` instead, the user must use the full name.
- Check the **Distinguished Name** setting, using the `dsquery` command

Vouchers & Dumps are Available | WhatsApp +201224560923

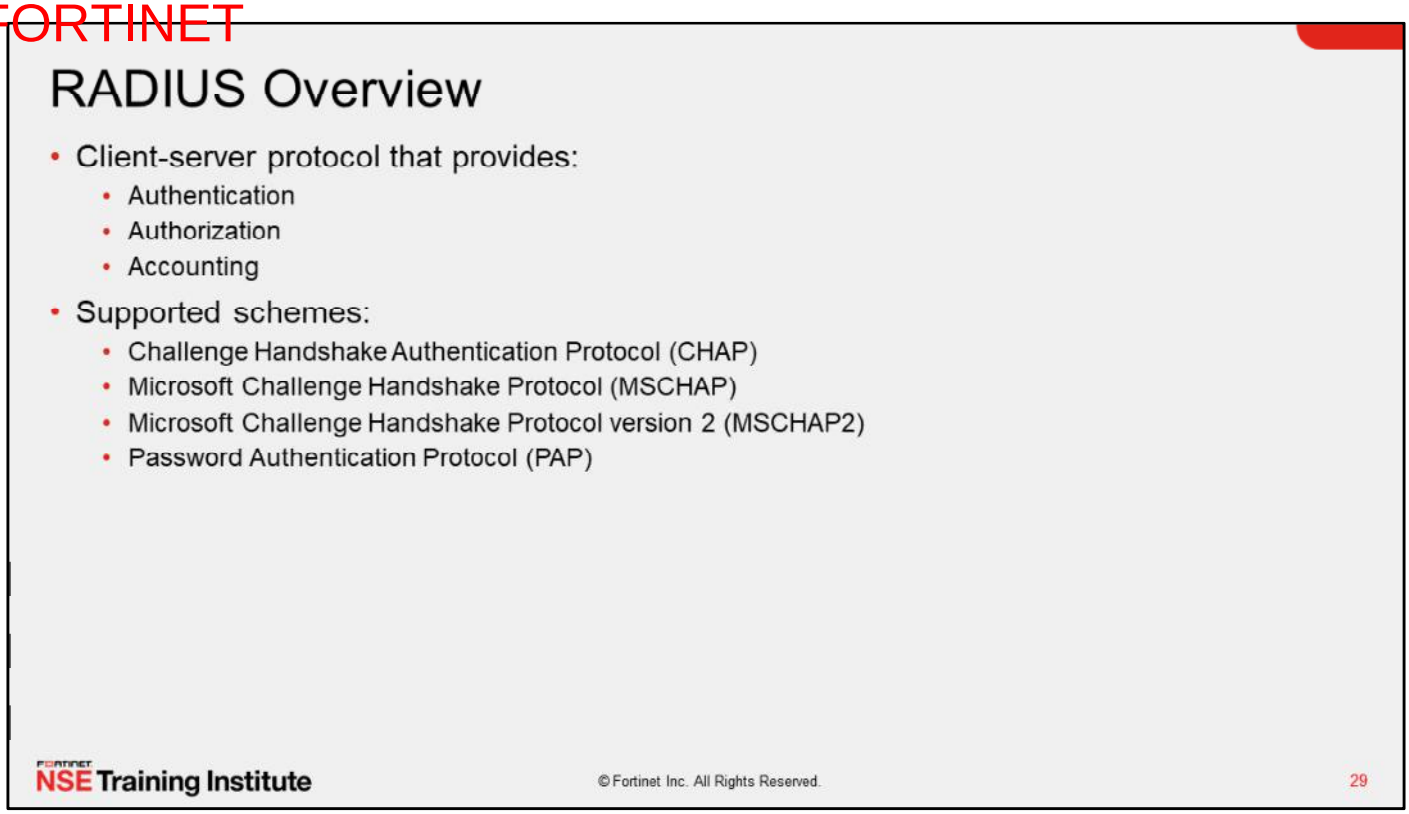
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn about RADIUS.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

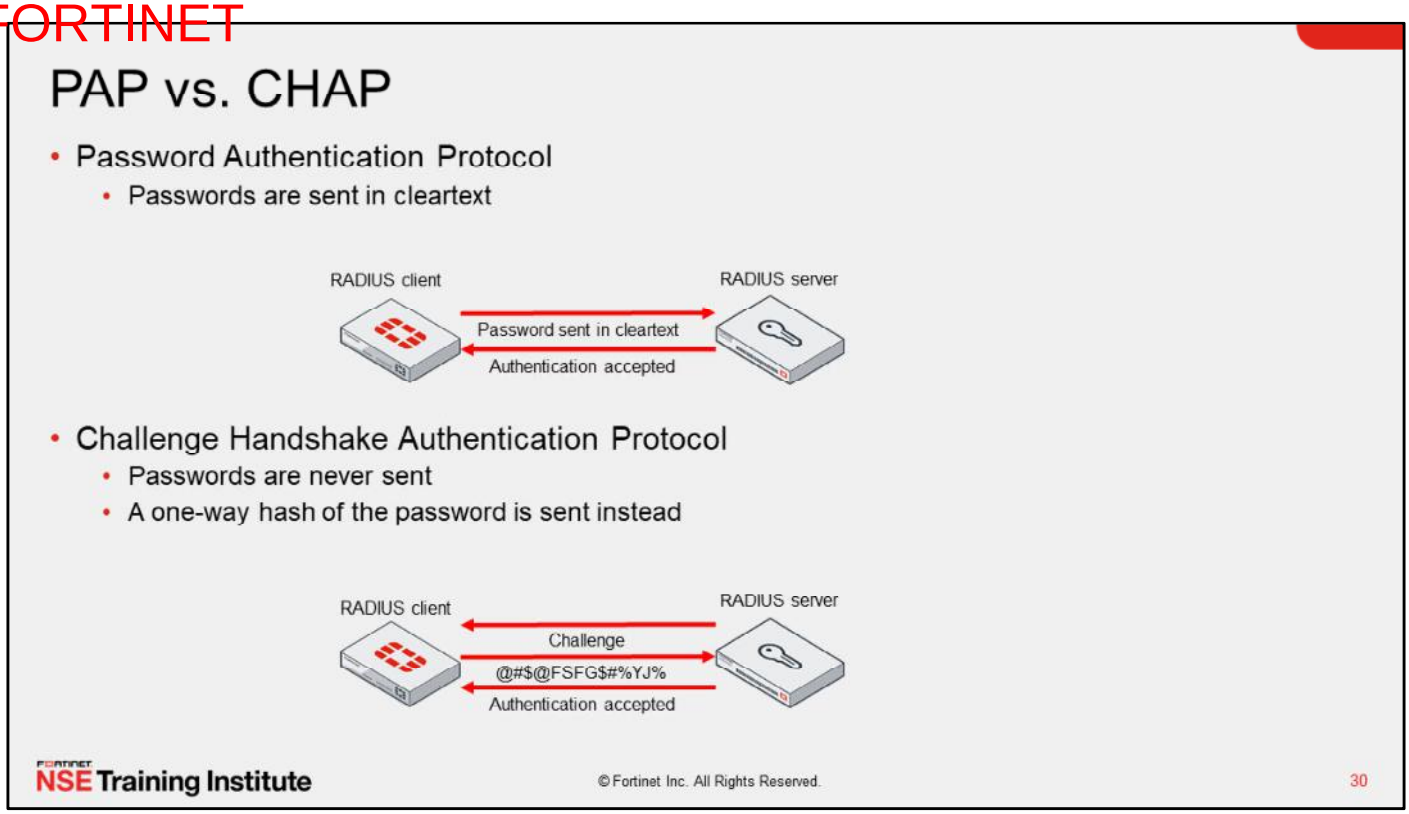


RADIUS is a broadly supported client-server protocol that provides centralized authentication, authorization, and accounting functions. RADIUS servers use UDP packets to communicate with the RADIUS clients on the network to authenticate users before allowing them to access the network, authorize access to resources by appropriate users, and account for the resources that are used.

You must configure the RADIUS server to accept FortiGate as a client. FortiGate uses the authentication and accounting functions of the RADIUS server. FortiGate supports the following RADIUS schemes: CHAP, PAP, MSCHAP, and MSCHAP2.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) are two common authentication schemes that are used with RADIUS.

PAP is a weak authentication scheme, because it transmits the password.

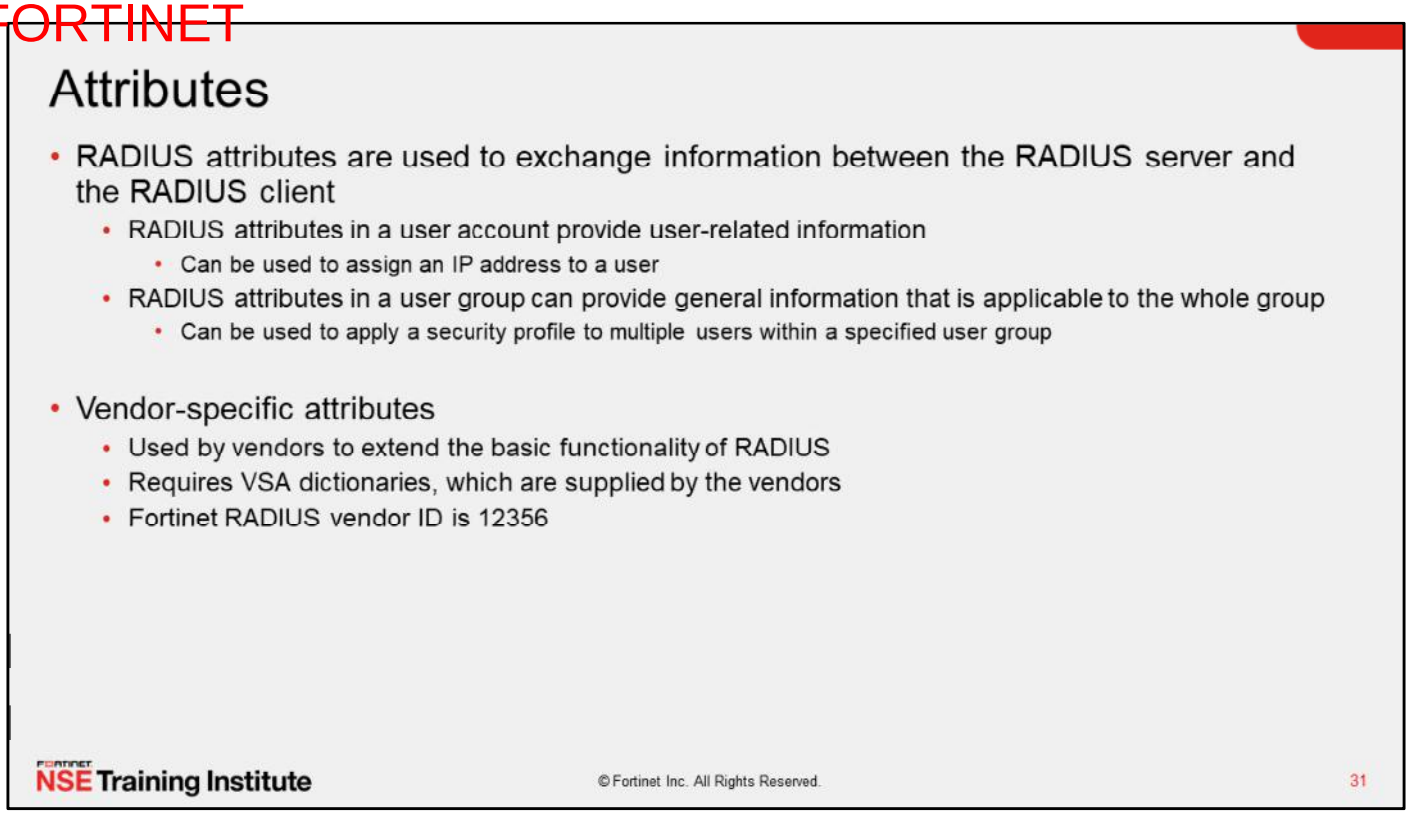
CHAP is a stronger authentication scheme, because it never sends the password. It uses hashing to perform the authentication.

After the link is established between the client and server, the following occurs:

1. The server sends a challenge message to the client, which includes a challenge value.
2. The client responds with a one-way hash of the password and the challenge value combined (note that the password itself is never actually sent).
3. The server also calculates the one-way hash using the stored user password and the challenge value combined.
4. The server compares the calculated hash with the hash received from the client.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

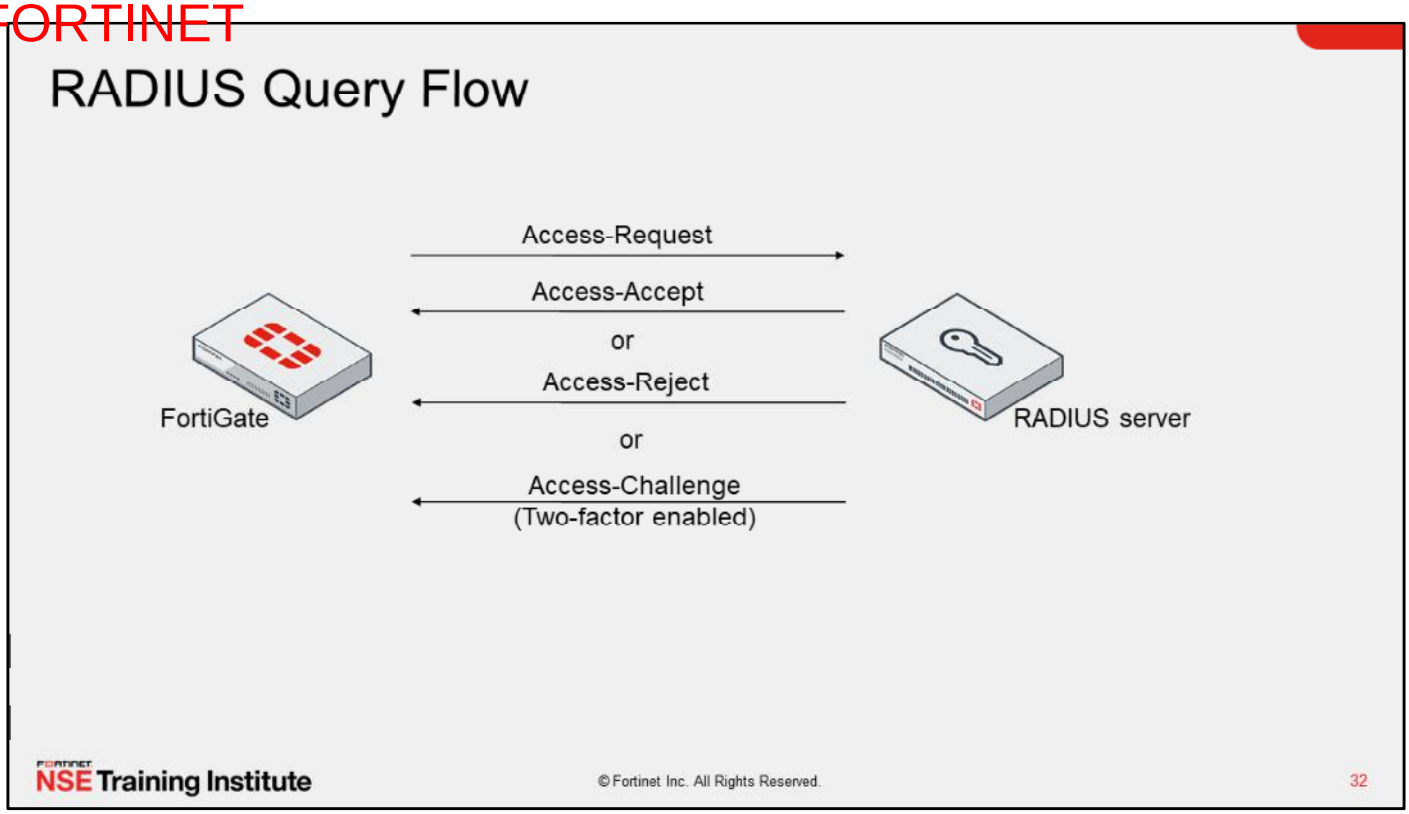


You can use RADIUS attributes to provide information about a user or a user group. RADIUS attributes configured at a user level can provide user-related information, such as IP addresses. Attributes configured at the user-group level are used to provide information that is applied to all the users within the specified group.

Vendors use vendor-specific attributes (VSA) to extend the basic functionality of RADIUS. Each vendor uses a unique VSA ID to transmit additional information, based on authentication success or failure. You must use VSA dictionaries to understand the proprietary VSA attributes that are supplied by the RADIUS vendors.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

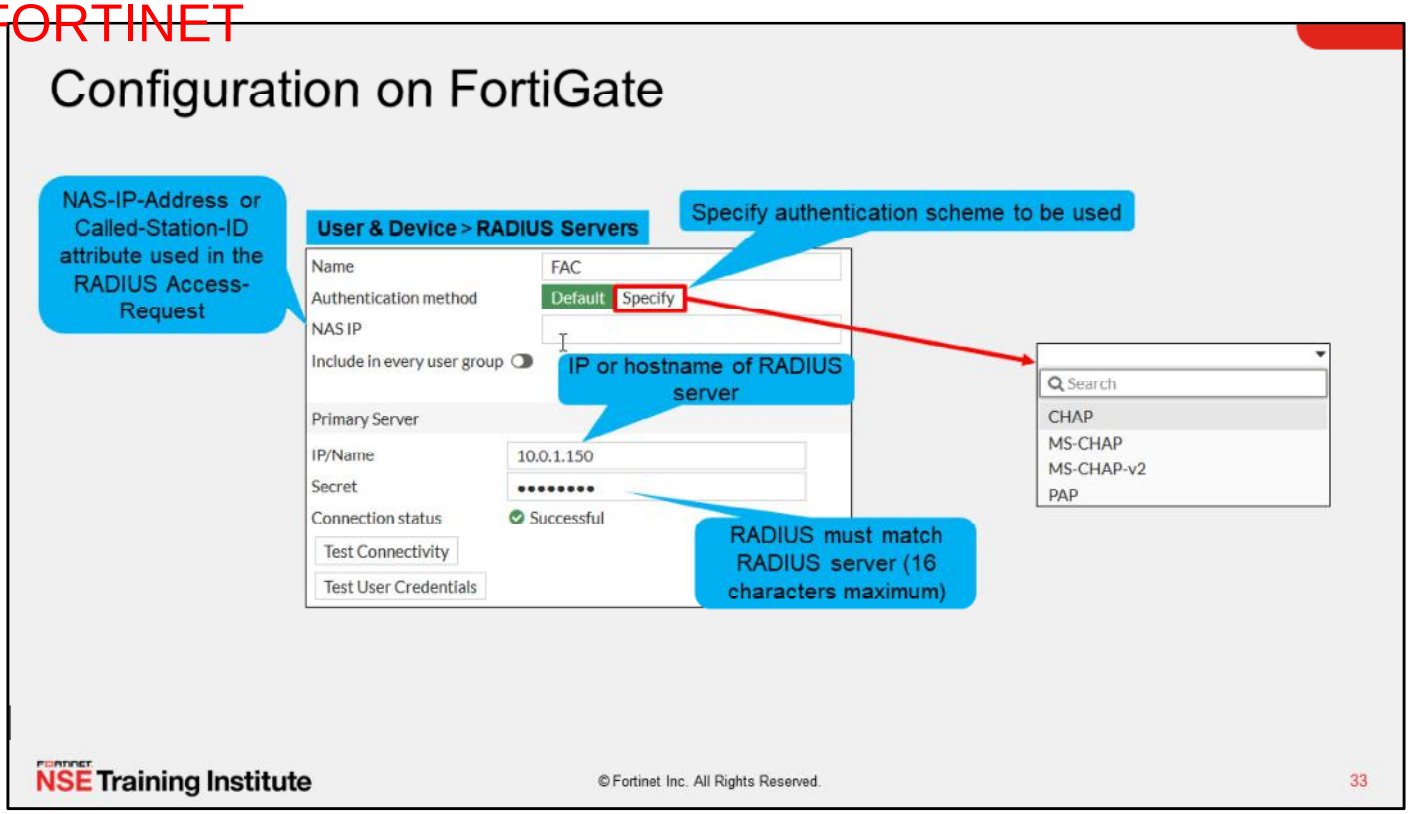


Normal authentication queries with the RADIUS protocol begin with an Access-Request being sent from FortiGate to the RADIUS server. Valid responses to this are Access-Accept and Access-Reject (yes and no, respectively).

If two-factor authentication is enabled on the server, the server returns an Access-Challenge message, to indicate it is looking for more information.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



When configuring the RADIUS server on FortiGate, you must provide the following information: **Name**, **Primary Server IP/Name**, **Primary Server Secret**, and **Authentication Method**. When **Authentication Method** is set to **Default**, FortiGate tries the different authentication schemes, starting with MSCHAP2, CHAP, and then PAP. You can also type an IP address in the **NAS IP** field**,** if you want to send the authentication request with the `NAS-IP-Address` or `Called-Station-ID` attribute attached to the RADIUS Access-Request.

Note that MSCHAP is never used when the authentication method is set to **Default**. If you want to use only MSCHAP as the authentication method scheme, you must specify MSCHAP manually.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Testing the RADIUS Secret

- Use the CLI command to test RADIUS secret between client and server:

```
# diagnose test authserver radius-direct <server_name or IP> <port
number> <secret> <chap | pap | mschap | mschap2>
# diagnose test authserver radius-direct 10.0.1.150 1812 secret
mschap2
RADIUS server '10.0.1.150' status is OK
```

- Three types of status results:

1. `Status is OK`: Secret is correct
2. `Status is Secret invalid`: Secret is incorrect
3. `Status is Server unreachable`: IP address or port is incorrect or RADIUS client used is not an authorized client on the RADIUS server

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

34

The `diagnose test authserver radius-direct` command is used to test the secret between the RADIUS client and server.

It can be the first check that you run when diagnosing RADIUS issues, and can reduce troubleshooting time significantly in many cases.

The RADIUS client is the FortiGate device here. There are two possible replies that you can see in the output, as listed on this slide. It is important to note that `Secret Invalid` is only displayed if the RADIUS client is an authorized client on the RADIUS server. If the RADIUS client is not authorized on the RADIUS server, you receive a `Server unreachable` status message. This is because the RADIUS server does not respond to requests sent by unauthorized RADIUS clients.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Testing RADIUS Queries

```
# diagnose test authserver radius <server_name> <chap | pap |
mschap | mschap2> <username> <password>

# diagnose test authserver radius FAC mschap2 student password
authenticate 'student' against 'mschap2' succeeded, server=primary
assigned_rad_
session_id=1014692435 session_timeout=0 secs idle_timeout=0 secs!
Group membership(s) - SSLVPN
```

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

35

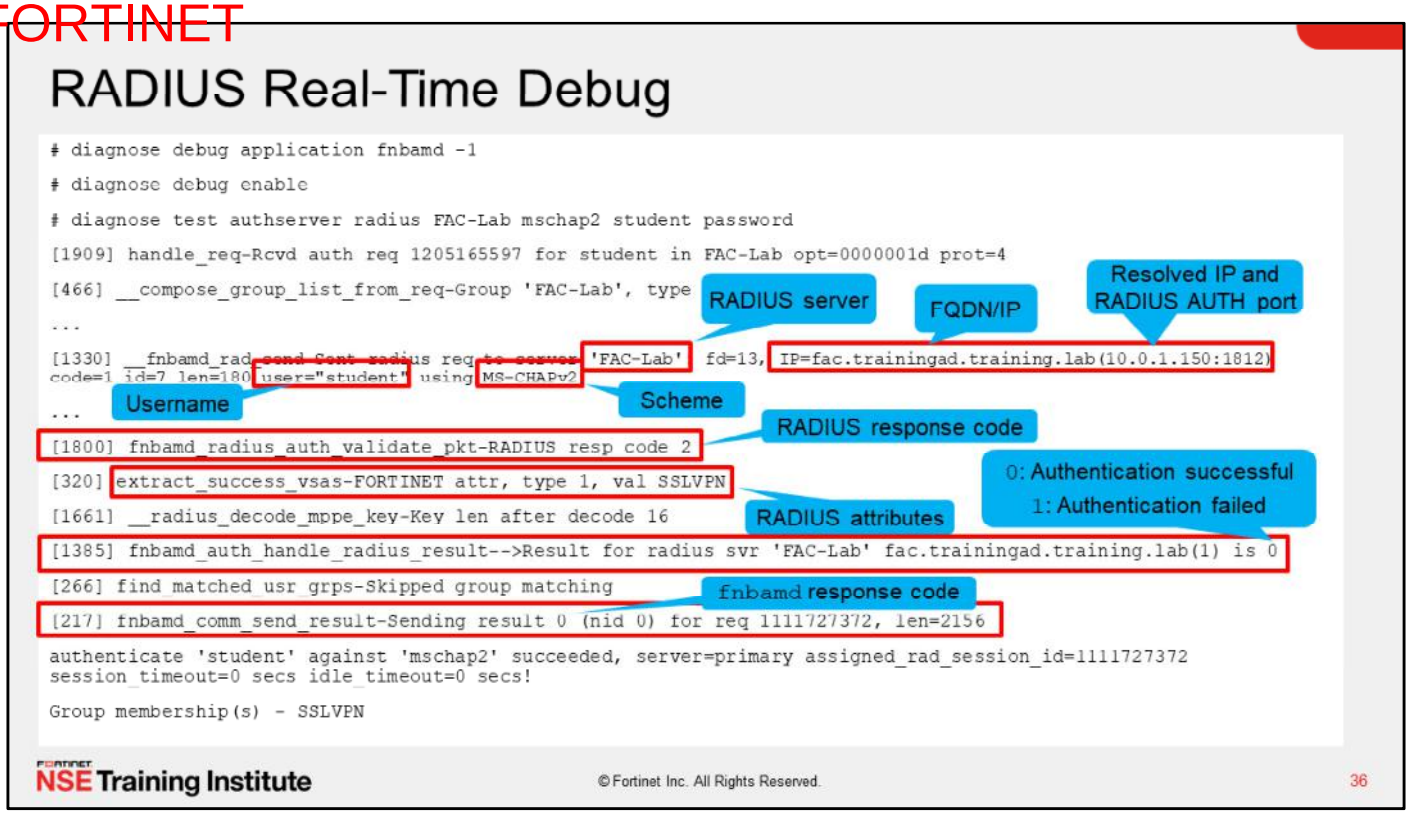
Similar to LDAP, there is a CLI test command for RADIUS.

When you use the CLI test command for RADIUS, you must provide not only the credentials for a test user, but also the authentication scheme.

Also, as in the case of LDAP, this command tests only the FortiGate RADIUS server configuration. It does not require the FortiGate configuration to contain a user group or firewall policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



RADIUS is either a one-step or two-step process (depending on the use of two-factor authentication). It is not as long as the four-step process that happens with LDAP regular bind. So, the output of the real-time debug is usually shorter. The output of the real-time command shows:

- The RADIUS server name, and IP/FQDN as defined on FortiGate
- Resolved IP, if FQDN is used, and RADIUS auth port
- The username requesting authentication
- The RADIUS scheme used
- Any RADIUS attribute sent by the RADIUS server
- The authentication results of `0` for successful and `1` for failed
- The RADIUS response code provides more detail as to why the authentication was successful or unsuccessful

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

fnbamd Response Codes

Response code	Description
0	Success
1	Deny
2	Challenged (password renewal or token is needed)
3	Unknown
4	Pending
5	Error
6	Framed IP Conflict
7	Token code is required
8	Need next token is required because token out of sync
9	Response buffer is too small
10	Authentication times out
11	Maximum concurrent authentication sessions are reached
12	Token code is already used

Most common ones

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

37

Here is the full list of the response codes provided by `fnbamd` debug. These codes can help you find the root cause of authentication issues.

Note that, in terms of token-related issues, the difference between response codes `2` and `7` is that the former involves RADIUS, while the latter does not. An example of a response code `2` is when you configure FortiGate to authenticate users against a RADIUS server that has two-factor authentication enabled. In such a case, after the user provides their credentials, FortiGate would then receive a RADIUS challenge response from the server requesting the user to provide the second factor.

An example of a response code `7` is when you configure FortiGate to perform two-factor authentication for a firewall user, but there is no RADIUS server involved. This could be a local FortiGate user configured with FortiToken as the second authentication factor. In this case, the request for the second factor is not triggered from a RADIUS response.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

RADIUS Response Codes

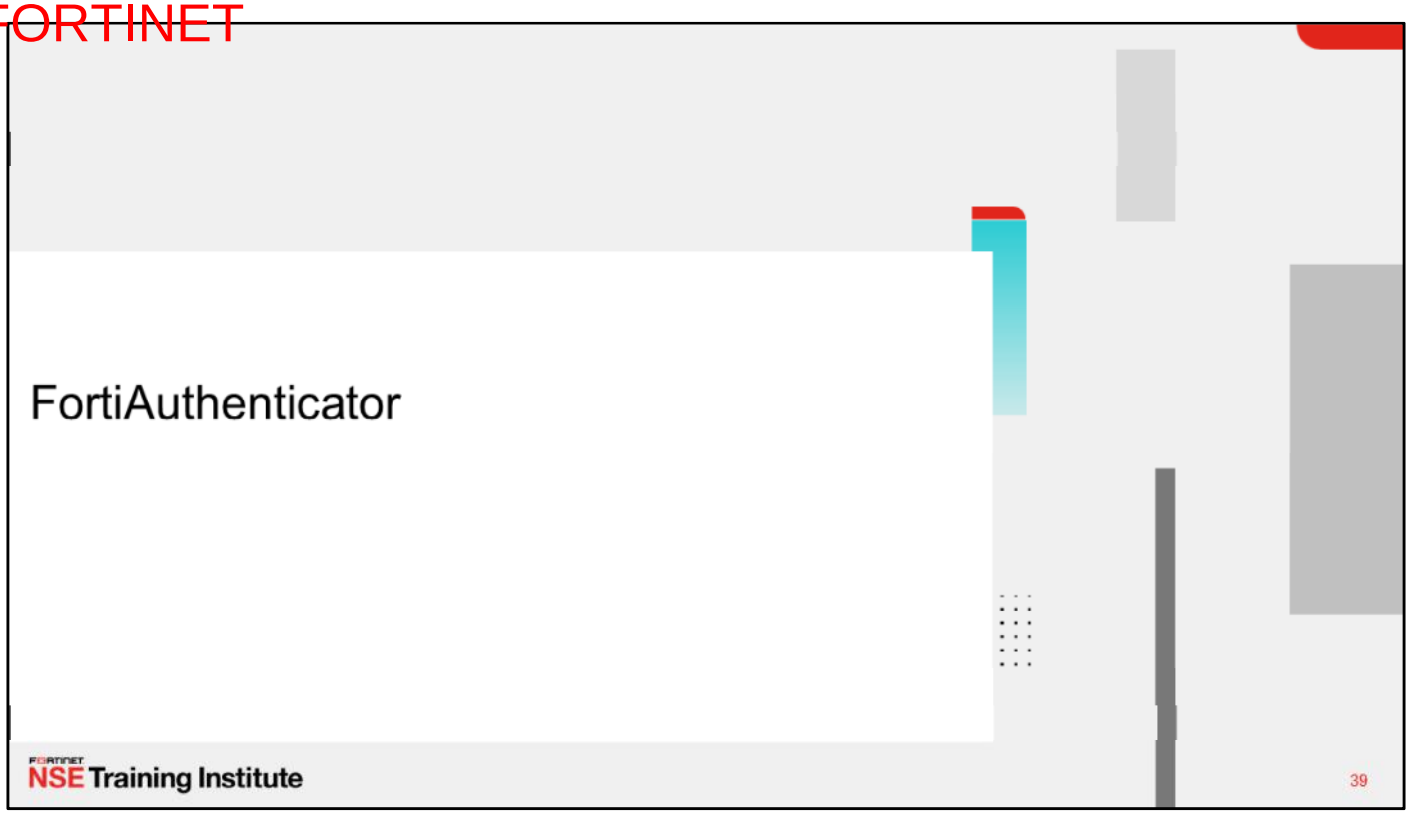
Code	Message Type
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge

NSE Training Institute
© Fortinet Inc. All Rights Reserved.

RADIUS code identifies the type of RADIUS packet. This slide shows RADIUS codes and the correspondent RADIUS messages.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn about FortiAuthenticator basics.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiAuthenticator

- FortiAuthenticator is a user authentication and identity manager
  - Provides standards-based secure authentication to a network
  - Centralizes the management and storage of user identity information
  - FortiAuthenticator serves as the gatekeeper of the Fortinet Security Fabric to establish identity at the entry points
- Some of the key features include:
  - RADIUS and LDAP services
  - Two-factor authentication
  - Wired/wireless authentication using the 802.1X standard
  - Certificate management
  - Captive portal
  - Self-serve portal
  - Fortinet single sign-on



NSE Training Institute

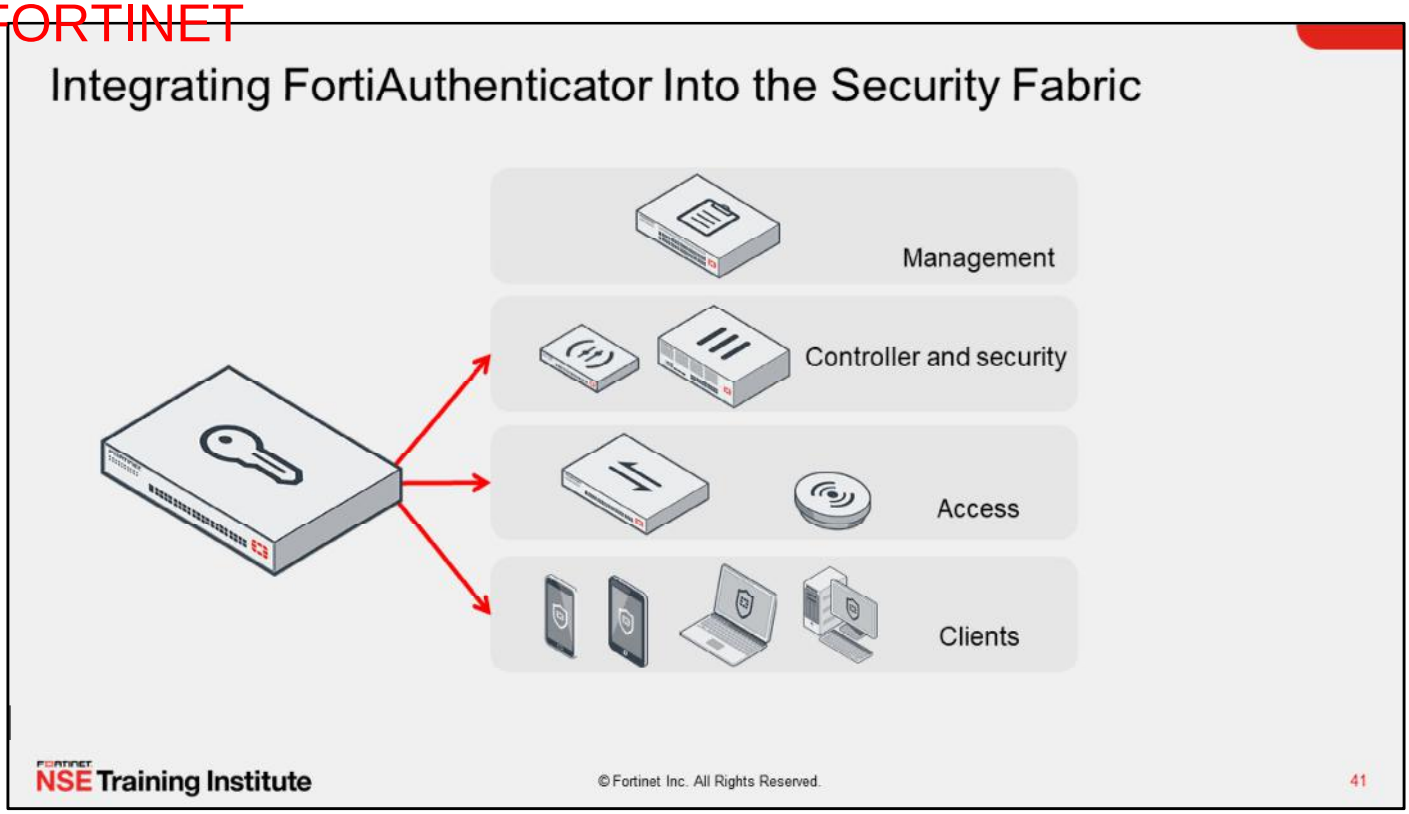
© Fortinet Inc. All Rights Reserved.

40

FortiAuthenticator is a user authentication and identity management device. It provides standards-based secure authentication to network devices. FortiAuthenticator provides RADIUS, LDAP, and 802.1X wireless authentication, certificate management, and Fortinet single sign-on (FSSO). FortiAuthenticator is compatible with FortiToken to provide two-factor authentication when using multiple FortiGate and third-party devices. Together, FortiAuthenticator and FortiToken deliver cost-effective, scalable, secure authentication to your entire network infrastructure.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiAuthenticator is a key component in the Fortinet LAN edge solution. FortiAuthenticator provides authentication, which is used by FortiGate and/or controllers to assign appropriate access to clients. Based on the configuration and roles defined on FortiGate, authentication rules can be enforced for wireless and wired clients.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiAuthenticator Key Differences

Feature	Key differences compared to FortiGate
RADIUS	RADIUS authentication and authorization server RADIUS authentication and accounting proxy Rule-based rewrite of RADIUS accounting packets for FSSO
Two-factor authentication	Centralized two-factor authentication for users and tokens
FSSO	Restrict number of devices per FSSO user FSSO user/group/IP filtering to FortiGate Kerberos FSSO (with NTLM fallback) SAML service provider SAML identity provider
Active Directory	Rule-based auto-sync with Windows Active Directory Reset Active Directory password
Wi-Fi/Hotspot	Social authentication: Facebook, Twitter, LinkedIn Google authentication
Guest/BYOD	Certificate authority (SCEP, OCSP, endpoint auto-enrollment)
CA	Certificate authority

NSE Training Institute

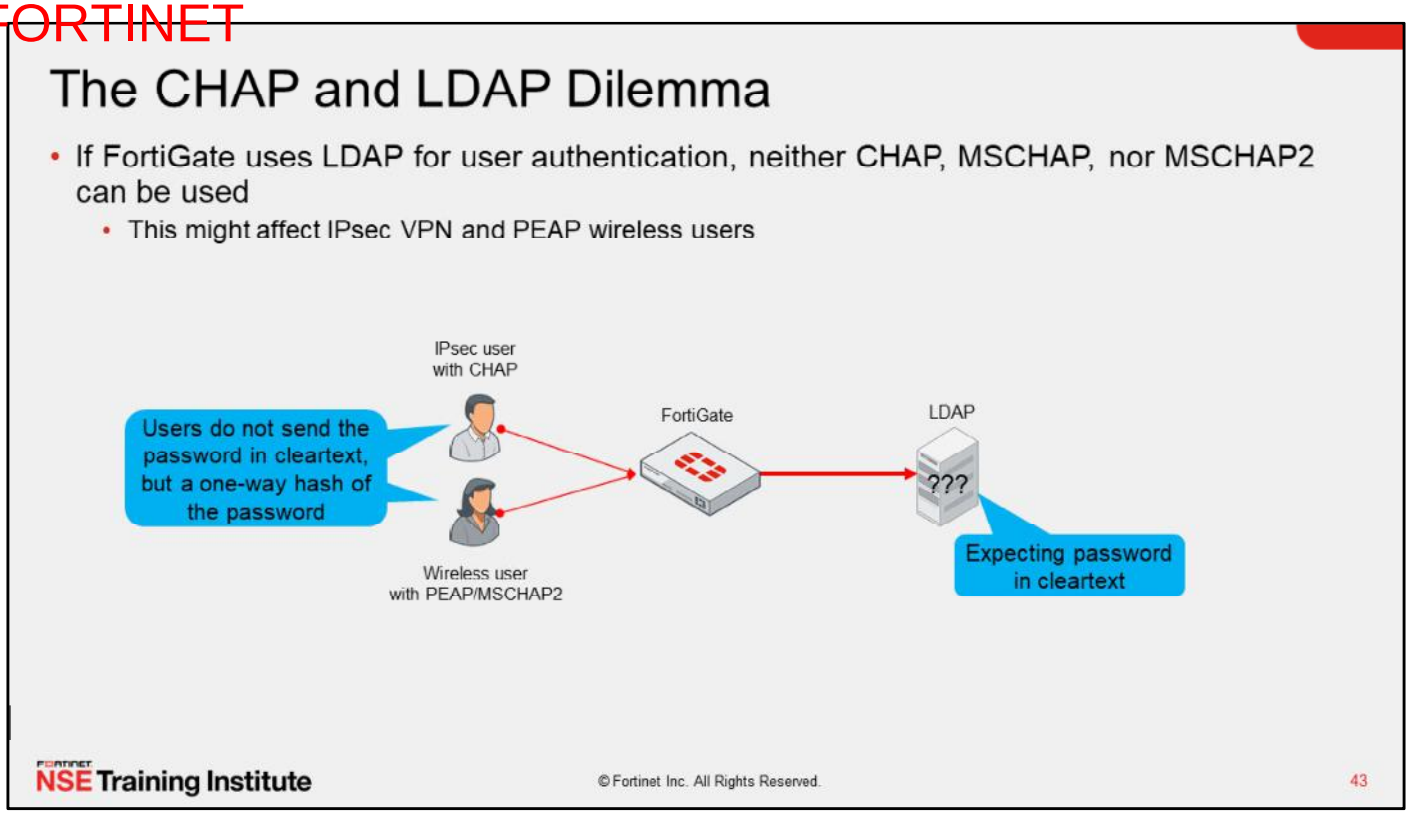
© Fortinet Inc. All Rights Reserved.

42

The list shown on this slide contains some of the key differences between FortiGate and FortiAuthenticator in terms of RADIUS, two-factor authentication, FSSO, Active Directory, Wi-Fi authentication, and guest management.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



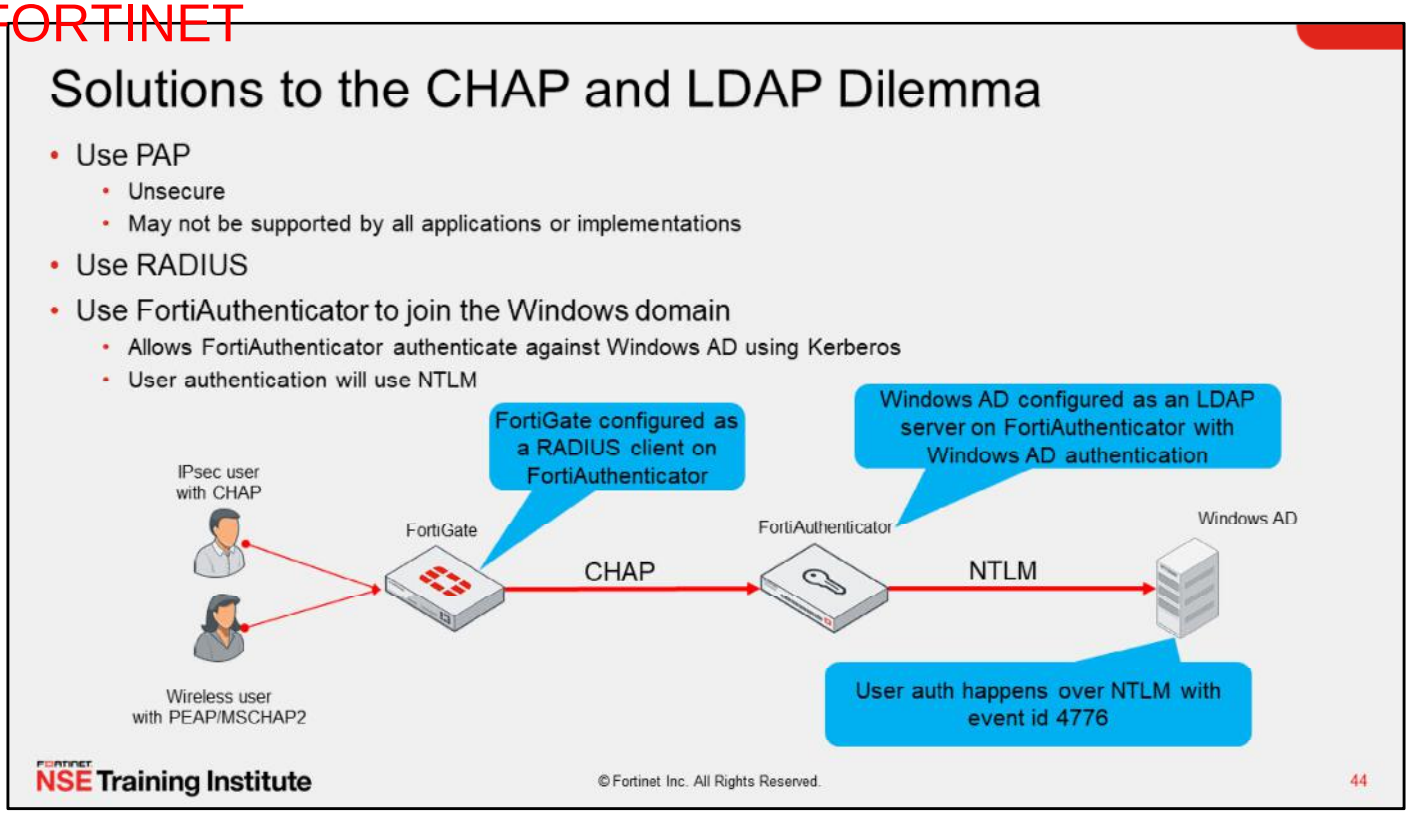
Now, you will explore another benefit of adding FortiAuthenticator to your LAN edge solution.

If FortiGate is configured to authenticate clients using a remote LDAP server, VPN and wireless clients using CHAP schemes are not able to authenticate. That is the case for wireless clients using PEAP/MSCHAP2 and IPsec VPN clients with extended authentication (XAuth) and CHAP. The same applies for any other device or application using CHAP, MSCHAP, or MSCHAP2 for authenticating against a FortiGate device that uses an LDAP server as the back end.

The reason is that during CHAP, MSCHAP, and MSCHAP2 authentication, a client sends a one-way hash of the password. However, the LDAP server, which is on the back end, is expecting the password itself. FortiGate, which is acting as the LDAP client, does not have the client passwords, nor can it convert a hashed password to a cleartext password.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



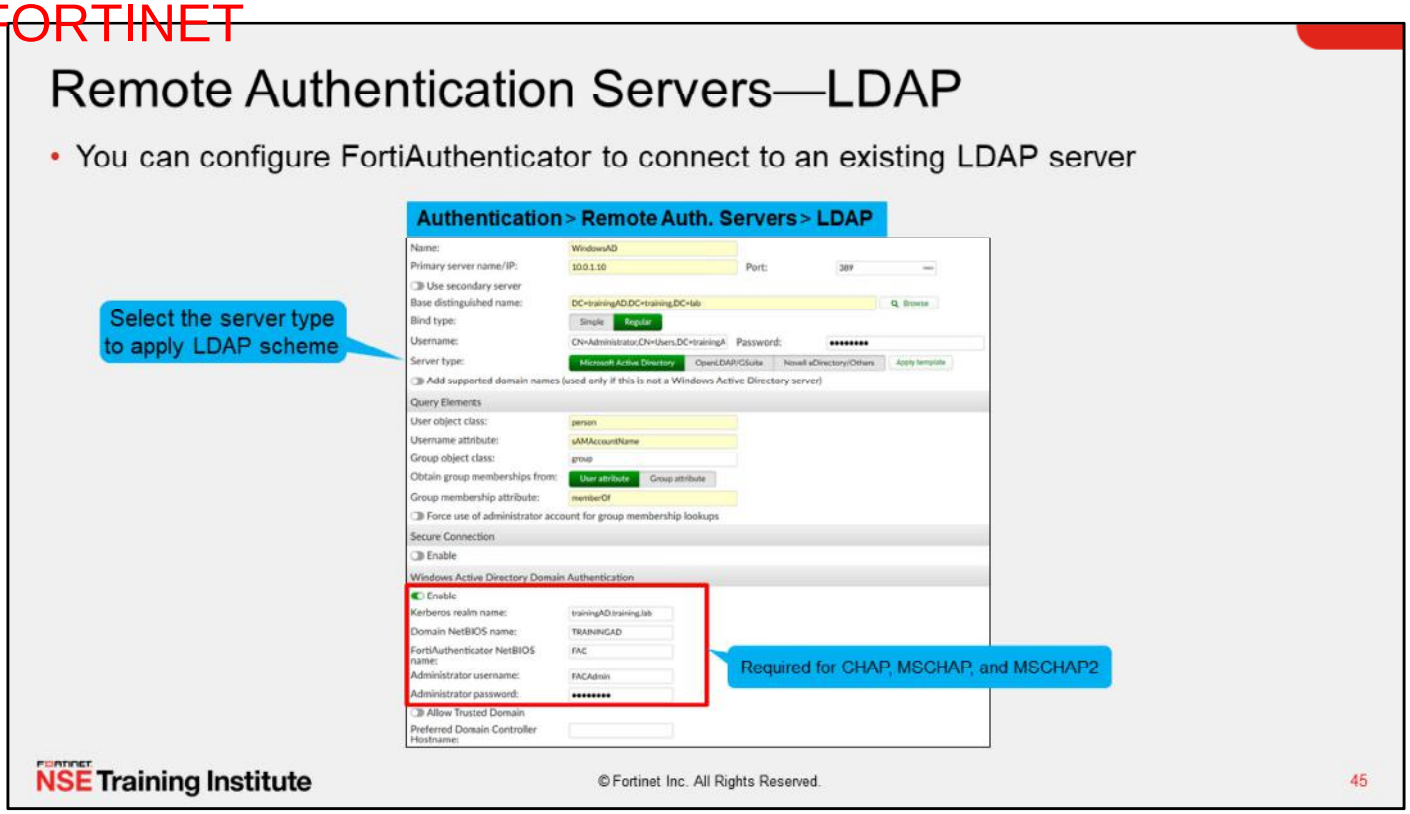
Two possible methods that you can use to solve the CHAP and LDAP problem are:

- Use PAP: You must configure FortiGate to use PAP instead of CHAP when authenticating clients. This approach is unsecure, because of the nature of the PAP protocol.
- Use RADIUS: Change your back-end server from LDAP to RADIUS.

If you are using Windows AD as your LDAP server, an alternative is to use FortiAuthenticator as an authentication proxy. FortiAuthenticator would be located between FortiGate and the Windows server. You must also configure FortiAuthenticator to log in to the Windows domain using the credentials of a Windows administrator. This adds FortiAuthenticator as a trusted device on the Windows AD domain, allowing FortiAuthenticator to proxy the password hash from the client to the Windows server, using NTLM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiAuthenticator can store the user database locally. It can also proxy authentication requests from a client to a back-end authentication server.

Now, you will learn how to configure FortiAuthenticator to proxy authentication requests to a remote LDAP server, which can be a Windows AD server.

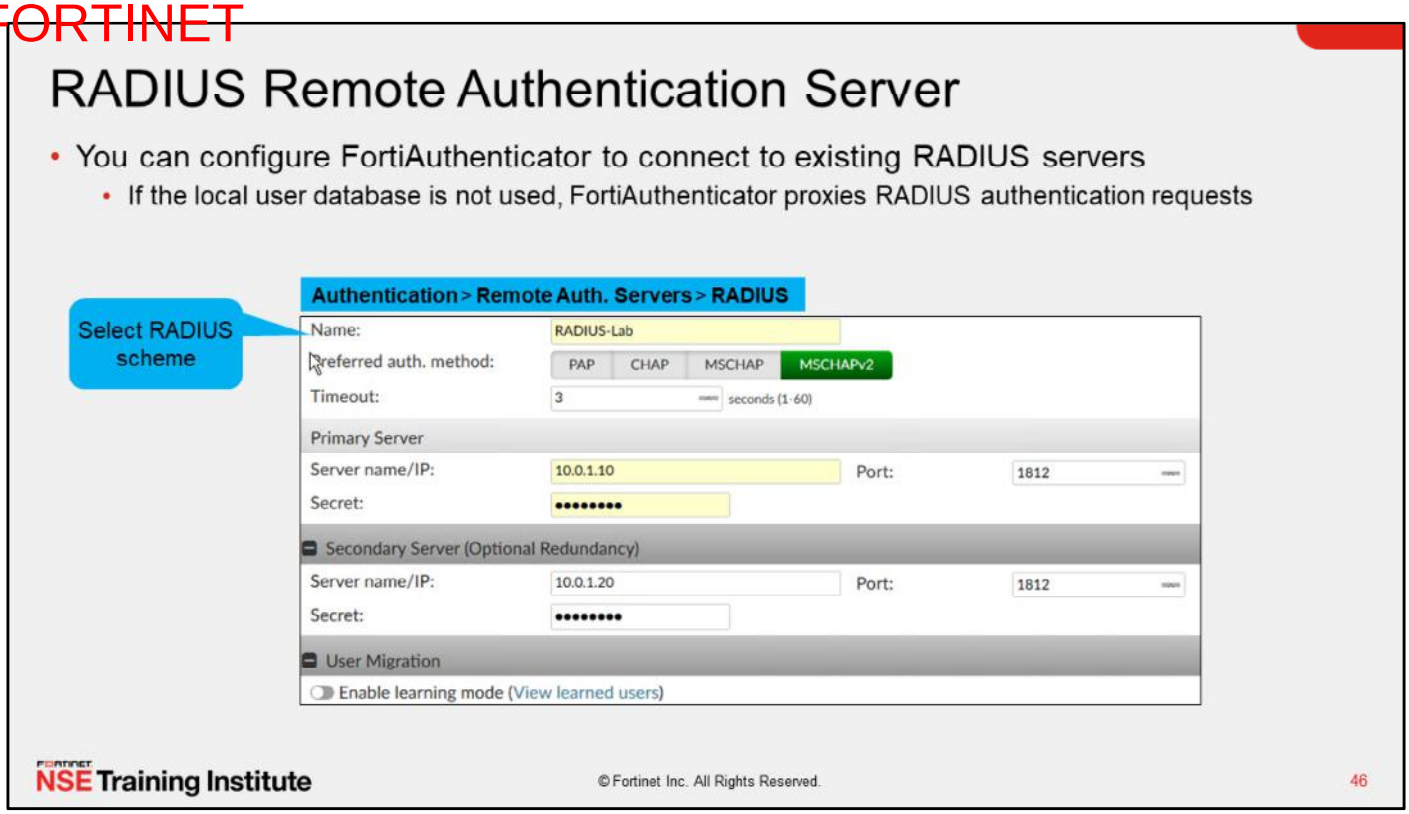
You must configure the following settings: **Name**, **Primary server name/IP**, **Base distinguished name**, **Bind type** and administrator **Username** and **Password** for regular bind type. Note that the **Base distinguished name** sets the root node where LDAP starts searching for user accounts.

There are predefined LDAP templates you can select in the **Server type** section. They include default attribute settings for well-known LDAP servers, such as Windows AD, OpenLDAP, and Novell eDirectory.

If you want FortiAuthenticator to relay CHAP, MSCHAP, and MSCHAPv2 authentication to a Windows AD server, you must enable **Windows Active Directory Domain Authentication** and enter the credentials for a Windows administrator. FortiAuthenticator logs in to the domain as a trusted device, allowing FortiAuthenticator to proxy CHAP, MSCHAP, and MSCHAP2 authentication, using NTLM.

Vouchers & Dumps are Available | WhatsApp +201224560923

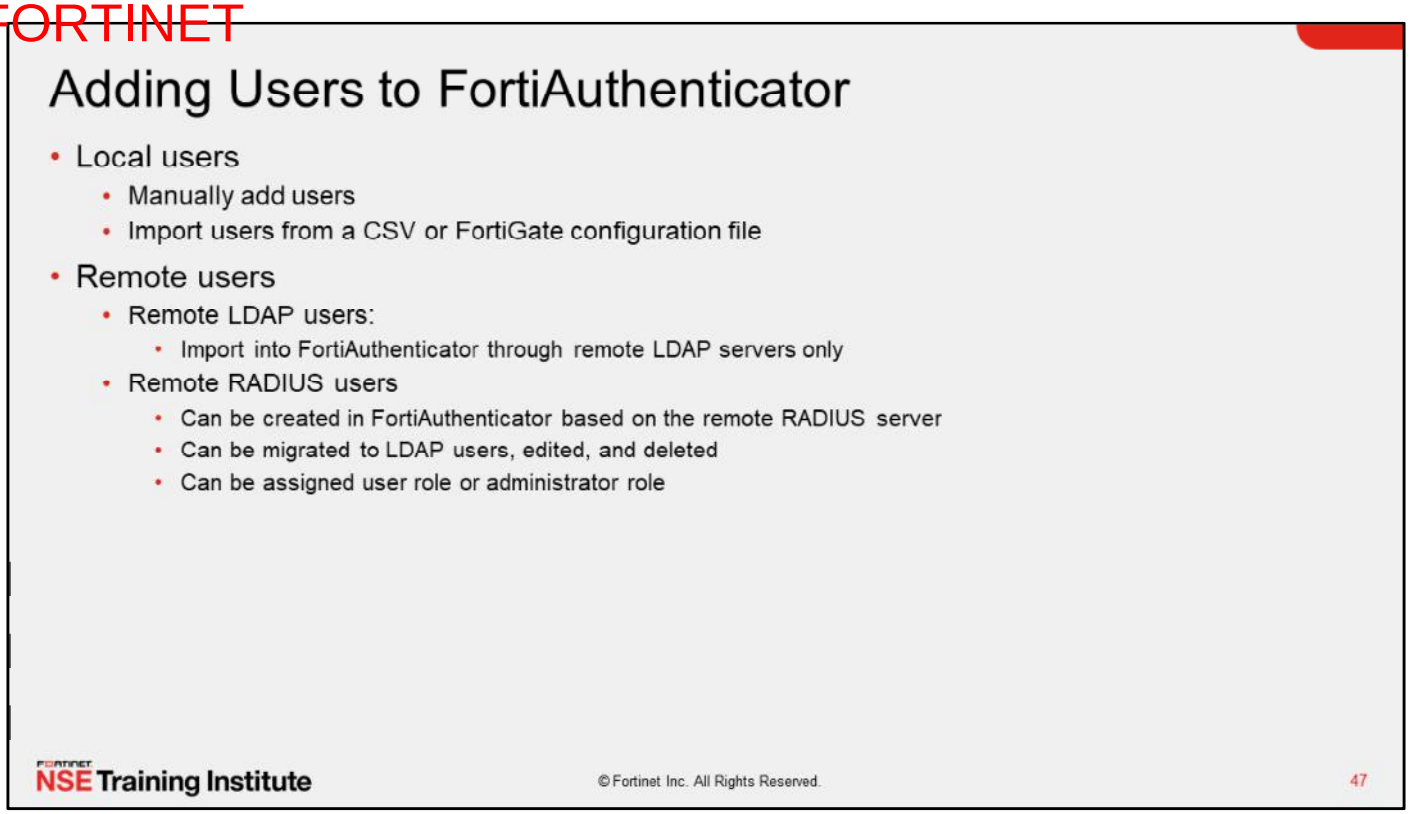
DO NOT REPRINT Brave-dumps.com
© FORTINET



The slide shows is an example of the configuration required for FortiAuthenticator to proxy authentication requests to a remote RADIUS server.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



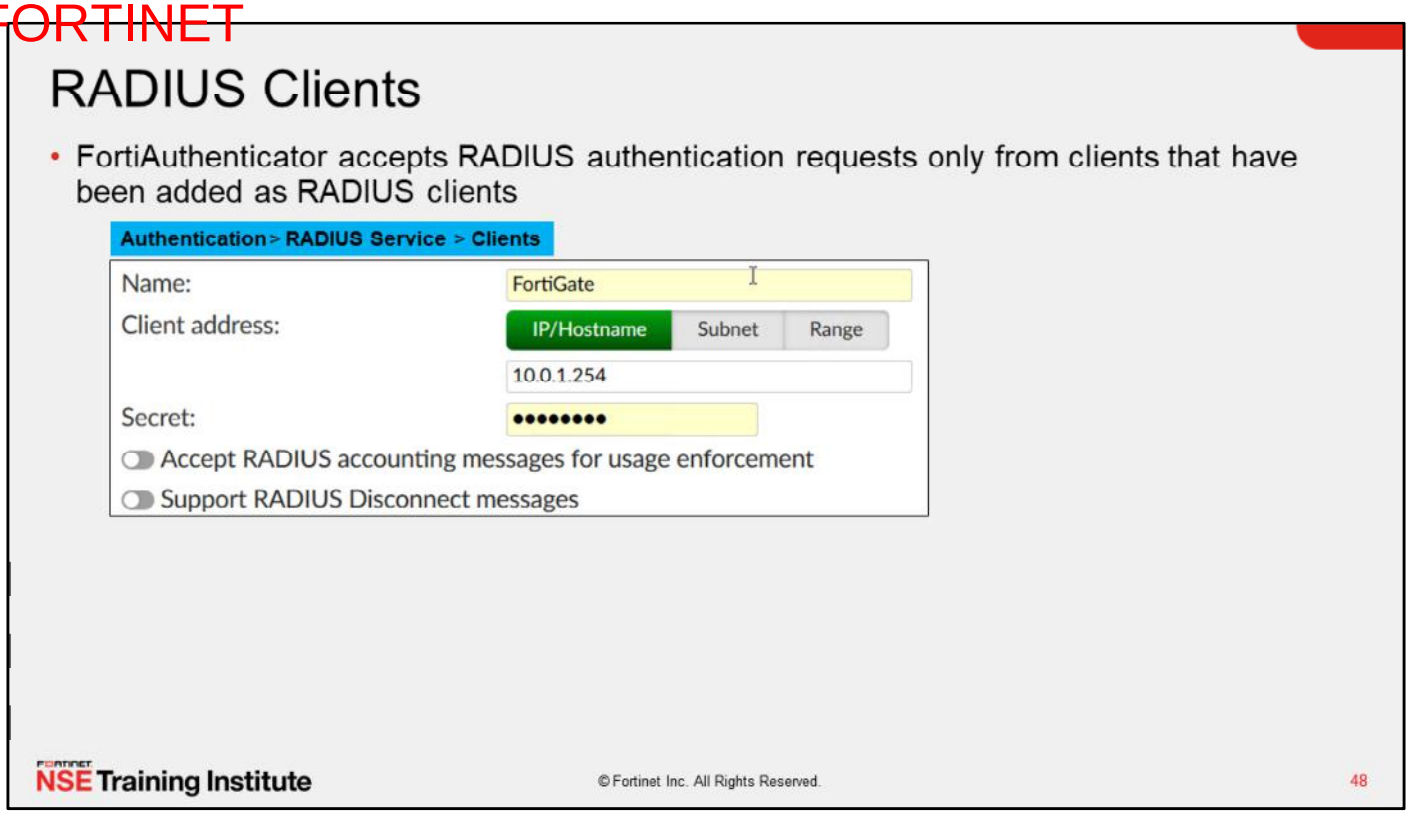
There are two ways you can add local users to FortiAuthenticator:
- Manually add users
- Import users from a comma-separated value (CSV) file or FortiGate configuration file

Note that FortiAuthenticator includes a self-service portal where users can register themselves.

You add remote LDAP and RADIUS users to FortiAuthenticator in different ways:
- For remote LDAP users, you must import users into the FortiAuthenticator user database from their remote LDAP servers.
- For remote RADIUS users, you can create them based on a remote RADIUS server. You can migrate remote RADIUS users to LDAP users, as well as edit and delete them. You can also flag remote RADIUS users with the user role or administrator role.

Vouchers & Dumps are Available | WhatsApp +201224560923

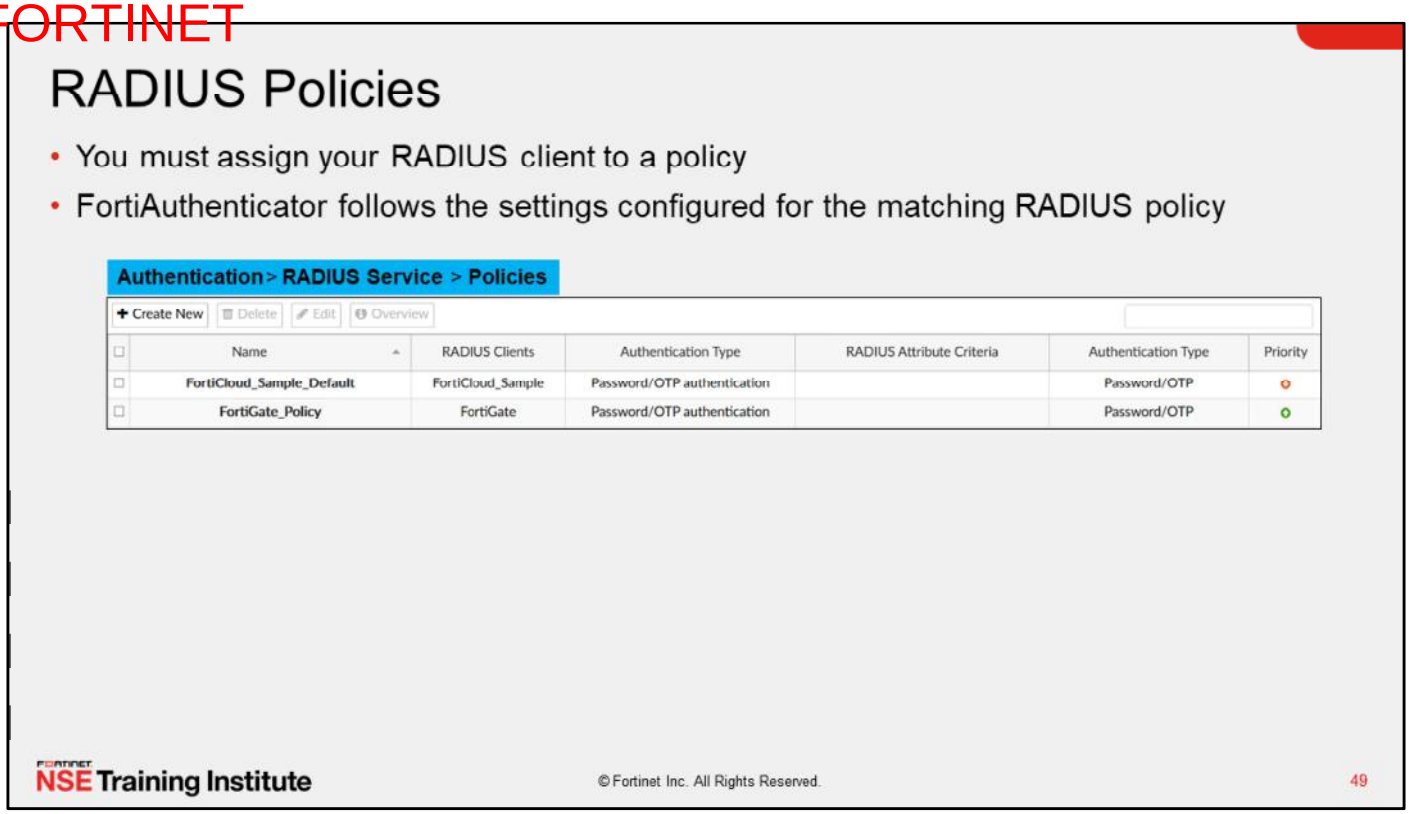
DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiAuthenticator accepts RADIUS authentication requests only from approved RADIUS clients. After you configure remote authentication servers or a local user database, you must allow FortiGate to make authentication requests to FortiAuthenticator. This is done under RADIUS clients on the FortiAuthenticator.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

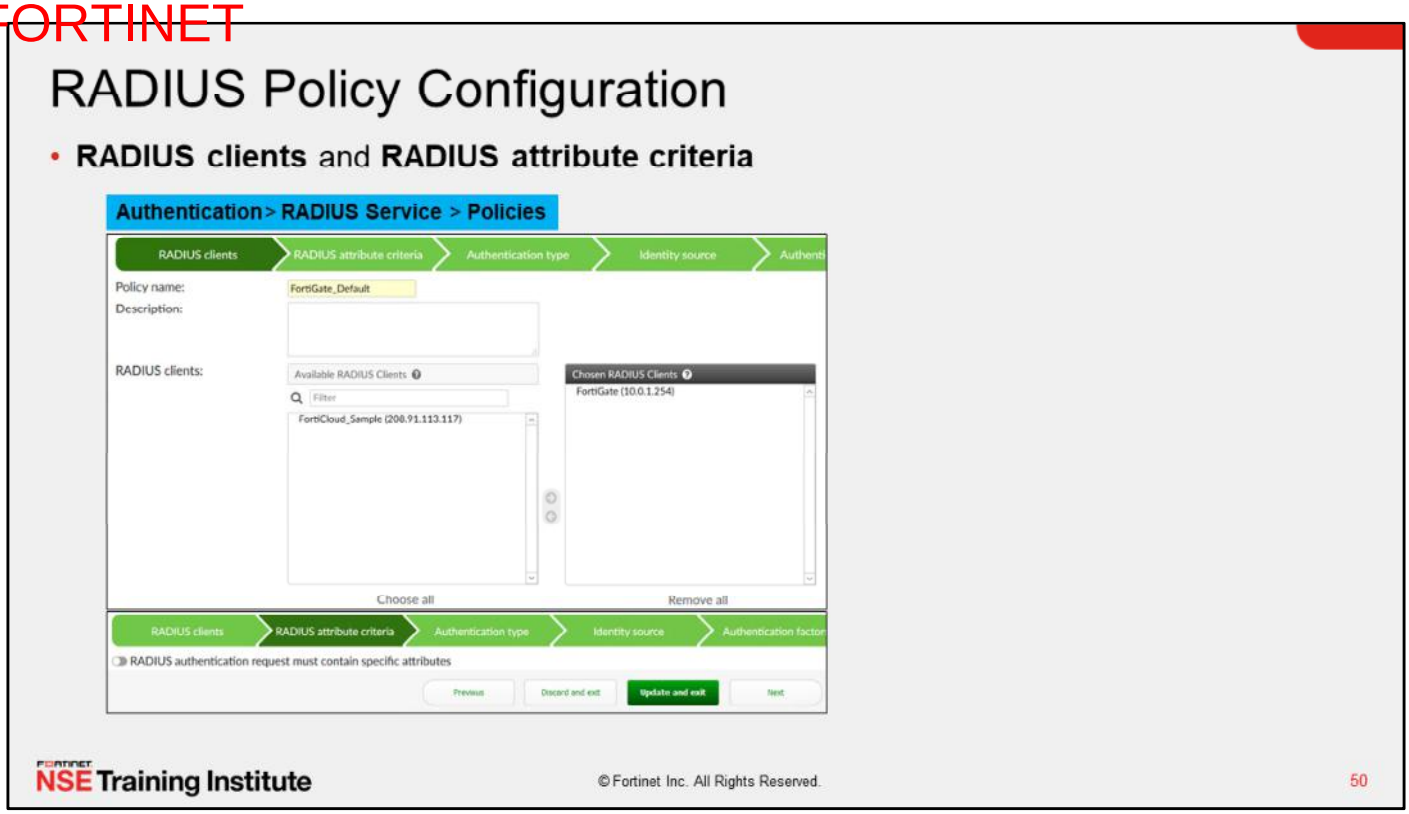


After you configure a RADIUS client, you must assign it to one or more RADIUS policies. A RADIUS policy contains the authentication settings that FortiAuthenticator follows when processing authentication requests sent by your RADIUS client.

When FortiAuthenticator receives a RADIUS authentication request, it looks at the request attributes and then finds a matching policy using a top-down approach. If there is no matching policy, FortiAuthenticator rejects the RADIUS authentication request.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

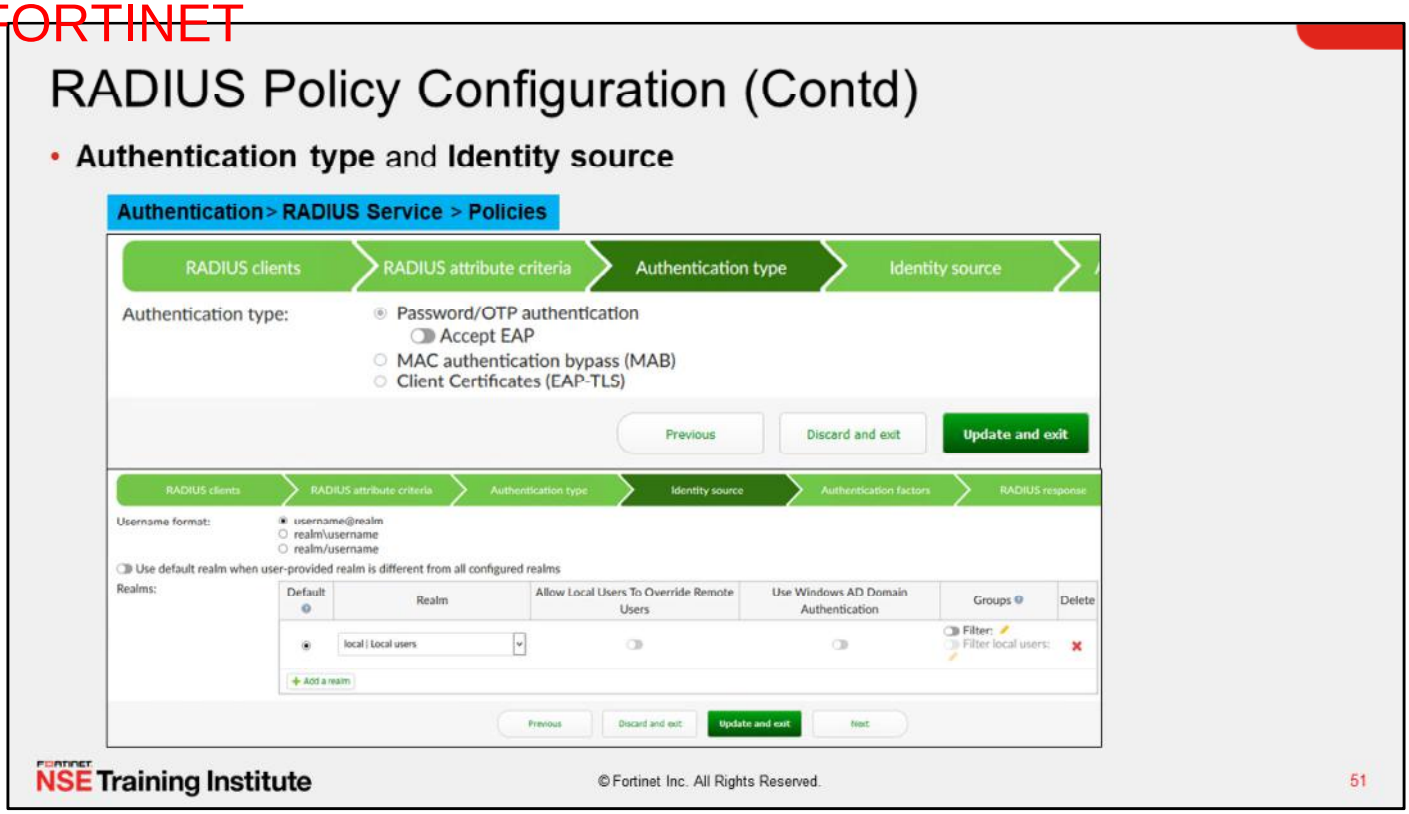


When you create or edit a RADIUS policy, FortiAuthenticator walks you through each of the six configuration sections comprising the policy.

The configuration example on this slide shows the **RADIUS client** and **RADIUS attribute criteria** sections. The example indicates that **FortiGate (10.0.1.254)** has been selected as the RADIUS client for the **FortiGate_Default** policy, and that no specific RADIUS attributes must be matched when processing the authentication requests sent by the RADIUS client.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The configuration example on this slide shows the **Authentication type** and **Identity source** sections.

The authentication type is set to **Password/OTP authentication**, which means that FortiAuthenticator authenticates the user's password and, if two-factor authentication is enabled for that user, FortiAuthenticator also verifies the user's one-time password (OTP).

The FortiAuthenticator RADIUS service also employs the concept of realms. Realms allow multiple domains to authenticate to a single FortiAuthenticator device. Each 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. For example, if you are a service provider that hosts multiple domains and you want each domain to have different permissions, you can set up a realm on FortiAuthenticator for each domain. So even though each domain is using the same RADIUS client, realms allow you to control access and permissions.

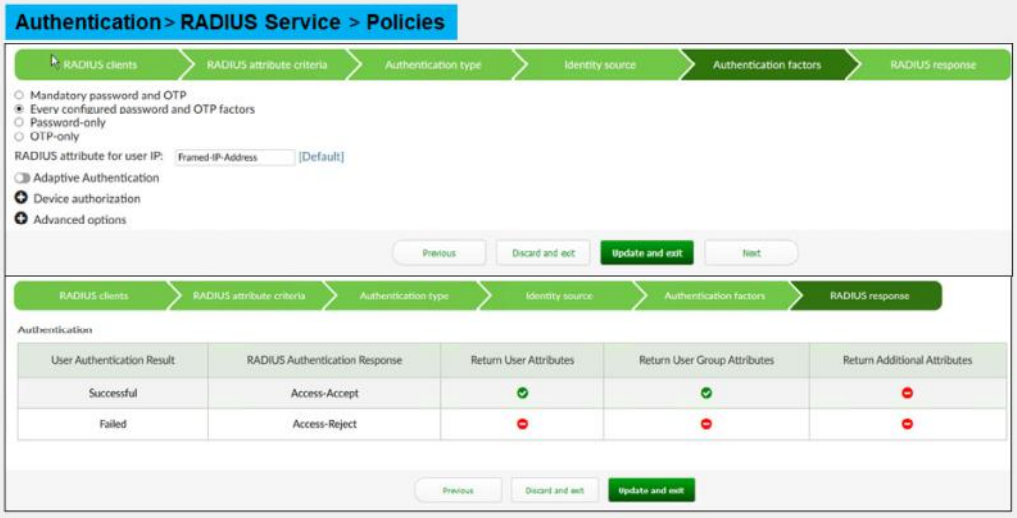
In the example shown on this slide, FortiAuthenticator expects the username to match the **username@realm** format. In addition, there's only one realm configured: **local | Local users**. In case the provided username does not contain a realm portion, FortiAuthenticator uses the default realm configured in the policy. Because the policy has only one realm configured, then that same realm becomes the default realm of the policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

RADIUS Policy Configuration (Contd)

- **Authentication factors** and **RADIUS response**



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

52

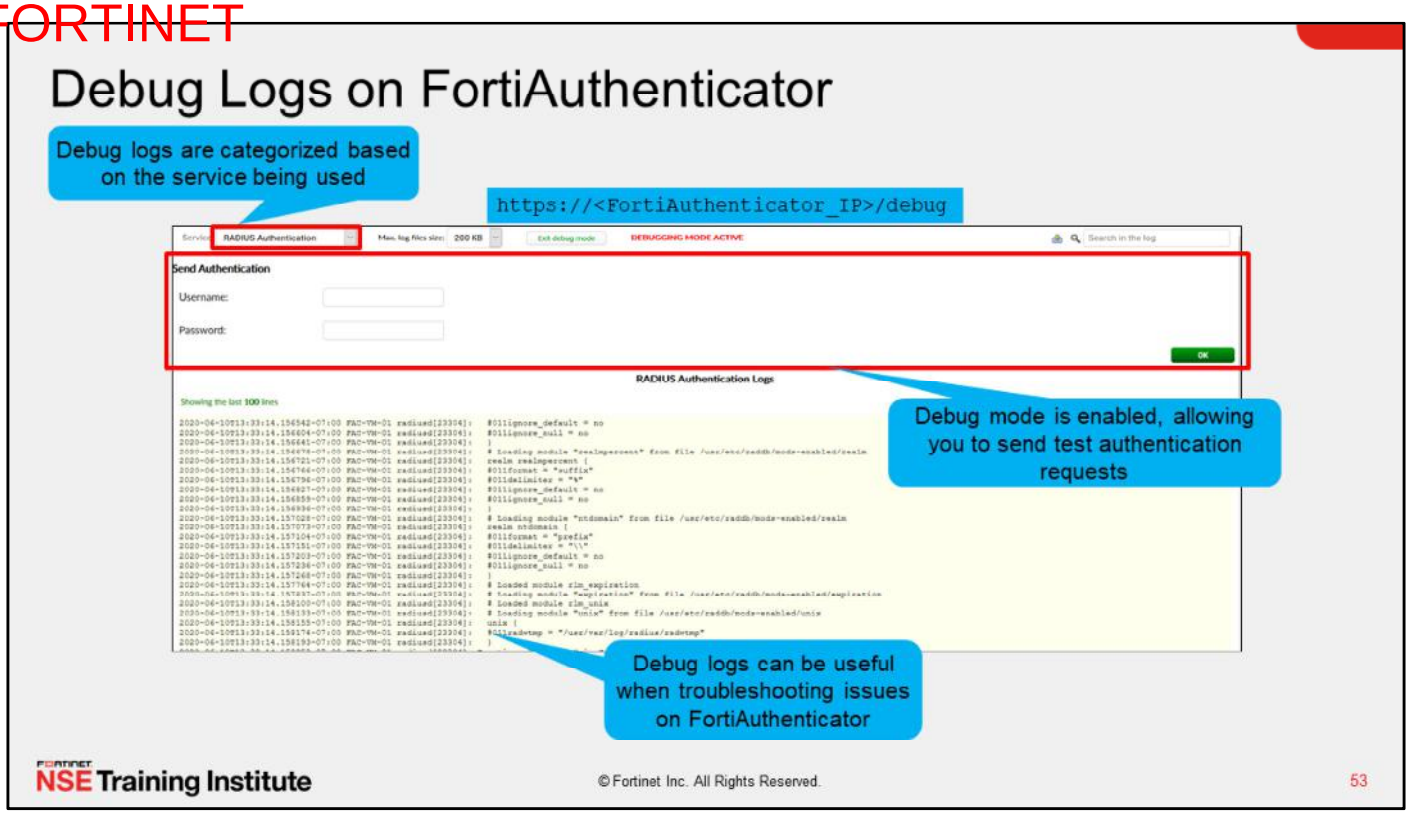
The configuration example on this slide shows the **Authentication factors** and **RADIUS response** sections.

Every configured password and OTP factors means that FortiAuthenticator will verify all configured factors, including regular and OTP passwords.

Finally, the **RADIUS response** section shows the different RADIUS attributes that are included in the response to a successful or failed authentication request.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

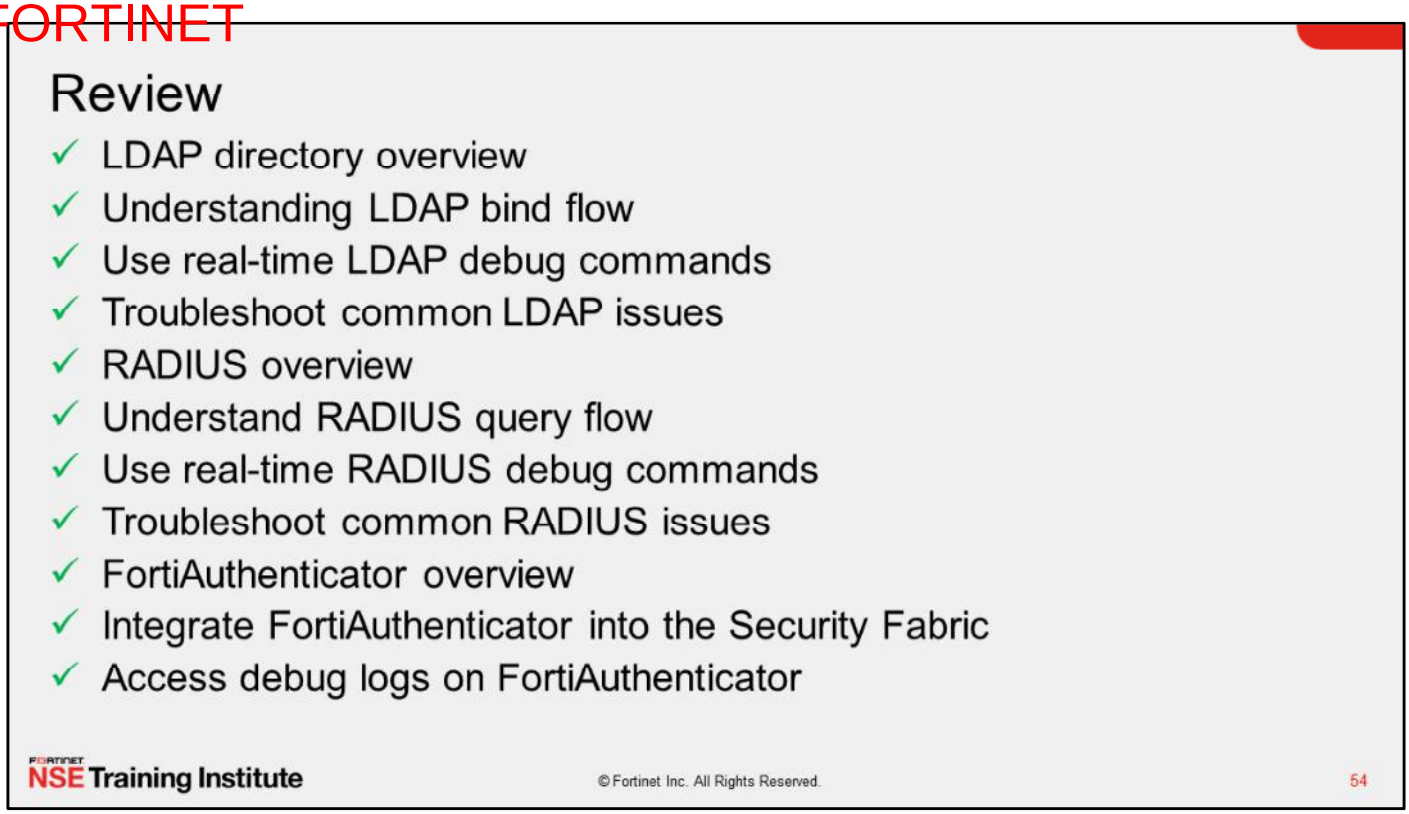


Unlike FortiGate, FortiAuthenticator does not have real-time debug commands. Instead, you can access extended logs for individual services. You can access the debug log page using the URL `https://<FortiAuthenticator_IP>/debug`. You can use these logs to troubleshoot issues with services running on FortiAuthenticator.

In the case of the debug logs for RADIUS authentication, there is the option of enabling **debug mode**, which allows administrators to test RADIUS authentication using the credentials of a test user from the debug logs window.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

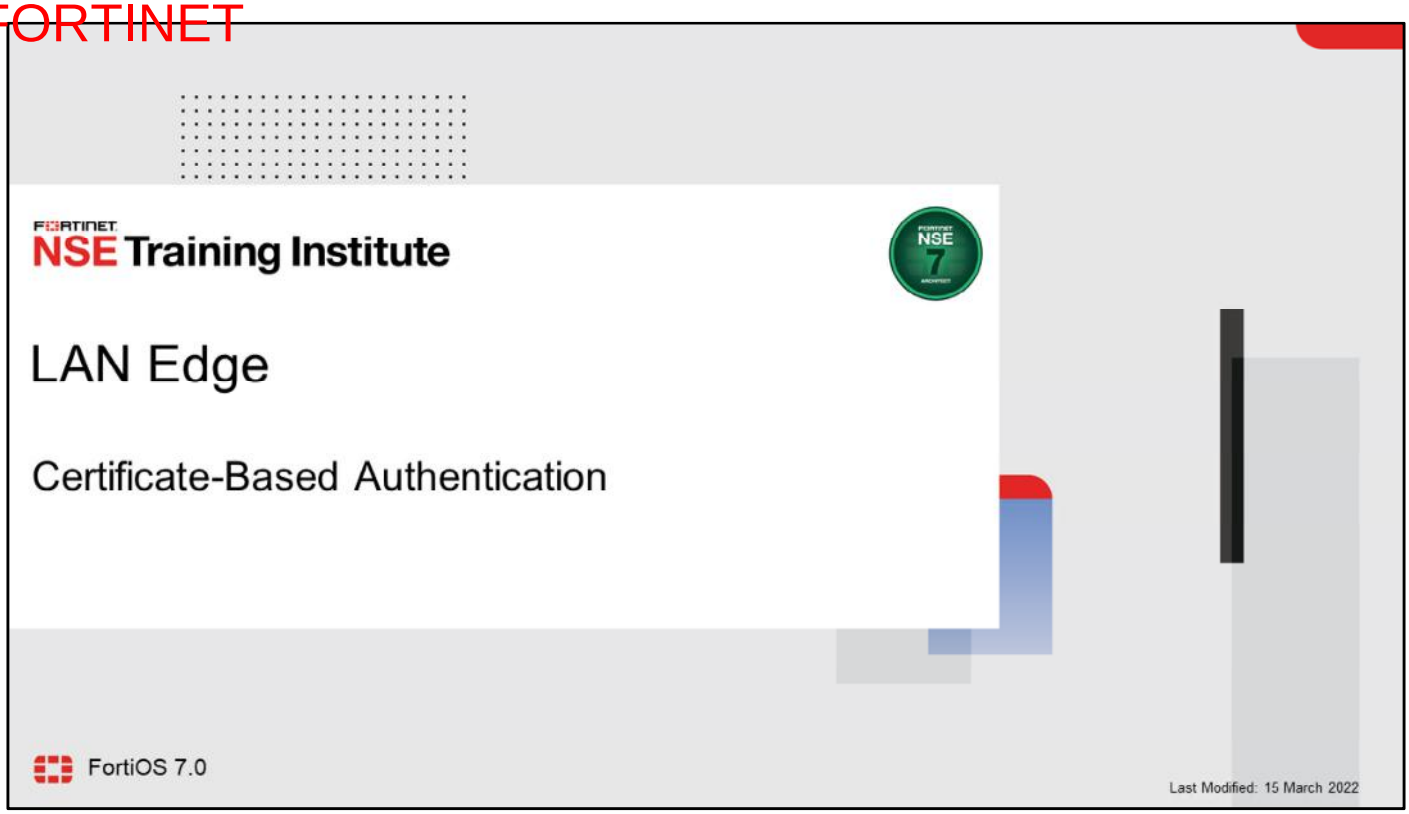


This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to configure and troubleshoot LDAP and RADIUS authentication on FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

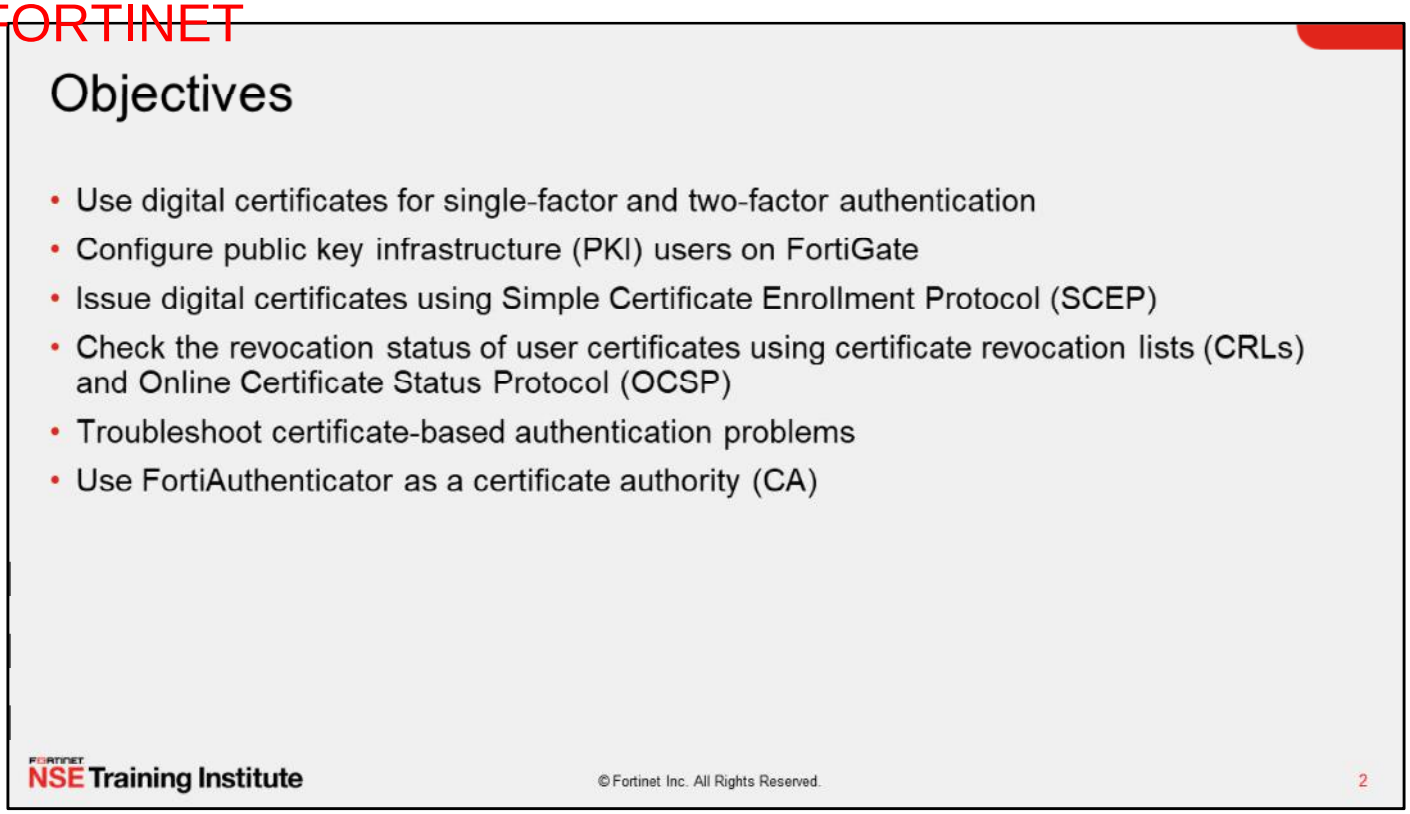
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn how to configure and troubleshoot certificate-based authentication.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

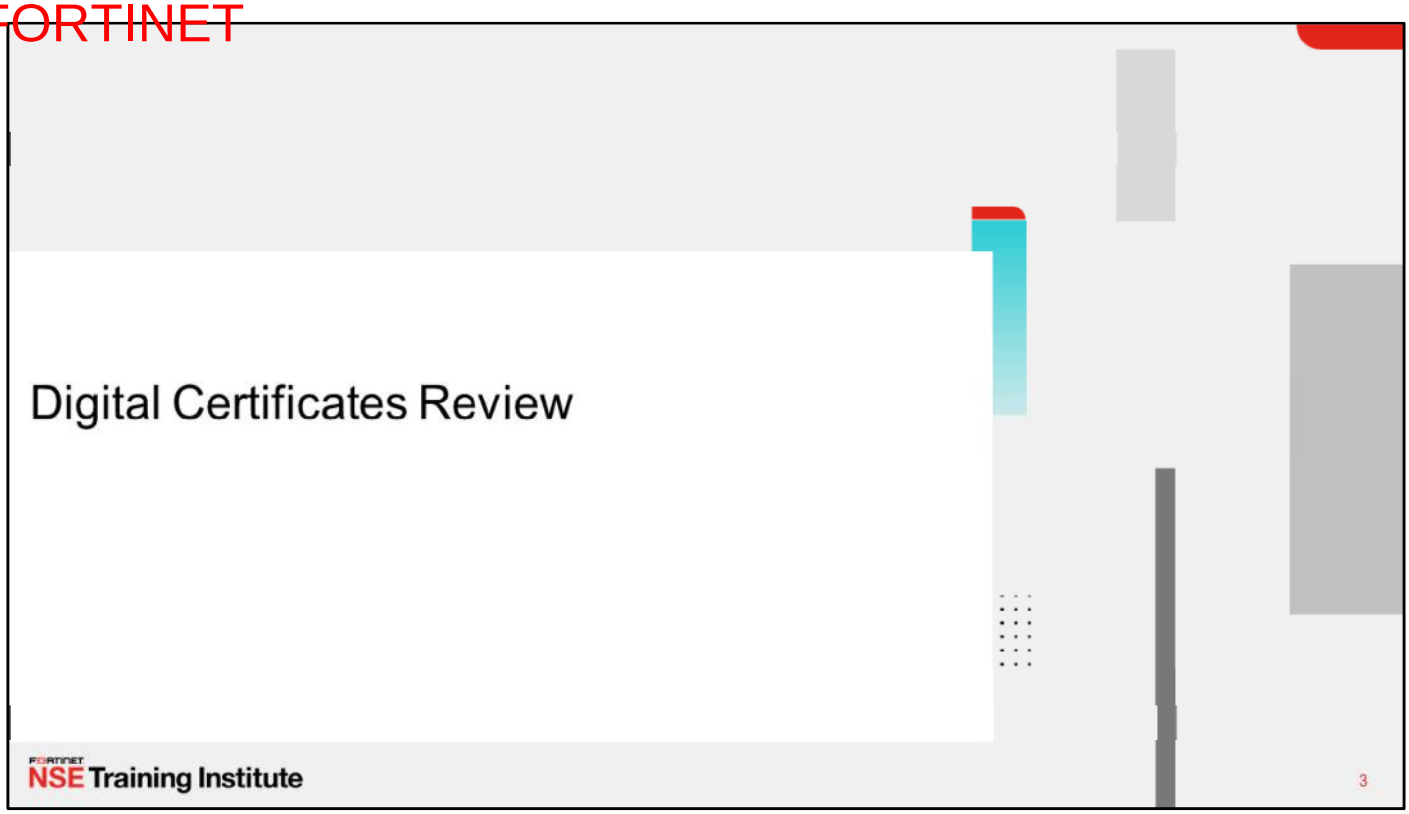


After completing this lesson, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in certificate-based authentication, you will be able to use and configure digital certificates on FortiGate and FortiAuthenticator.

Vouchers & Dumps are Available | WhatsApp +201224560923

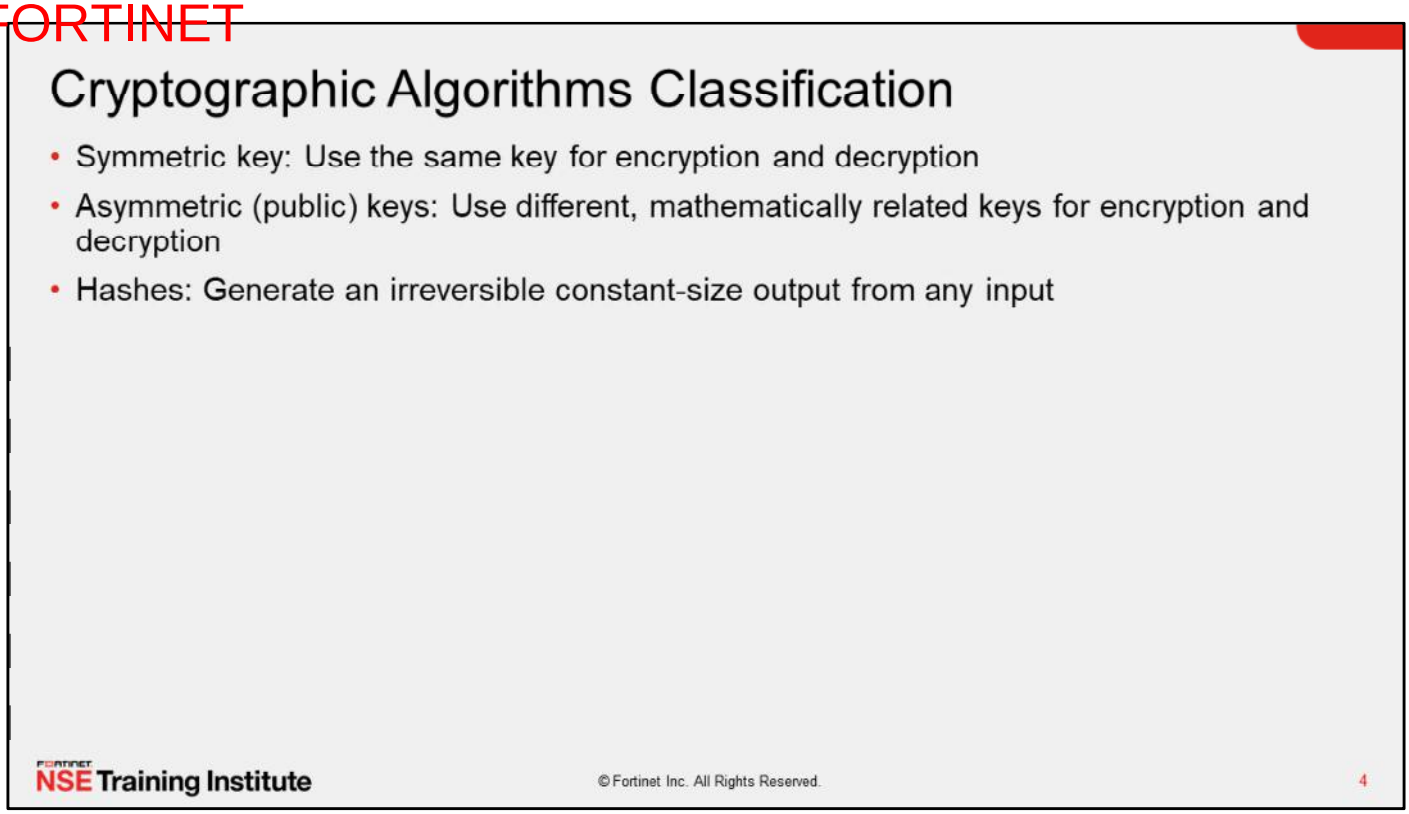
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will review the basics of digital certificates.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



There are two basic techniques for encrypting information: symmetric encryption and asymmetric encryption.

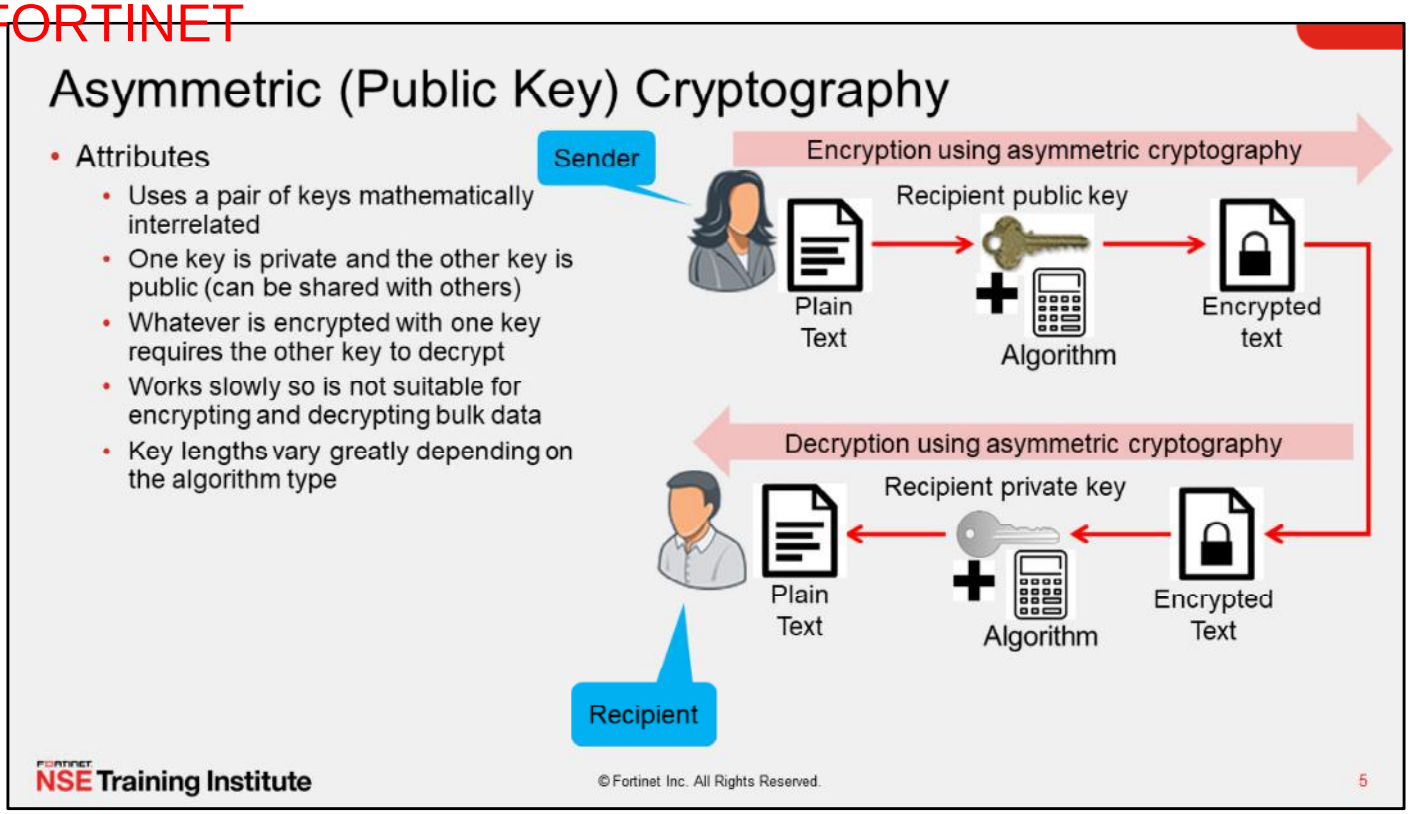
Symmetric encryption uses a single key for encrypting and decrypting. This key is shared by the parties that are exchanging encrypted information.

Asymmetric encryption uses a pair of keys. Both keys are mathematically related. One key is used for encrypting the information. The other key is used for decrypting the information.

Hashes, on the other hand, are not encrypted information because they cannot be decrypted. A hash algorithm generates an irreversible output from any input.

Vouchers & Dumps are Available | WhatsApp +201224560923

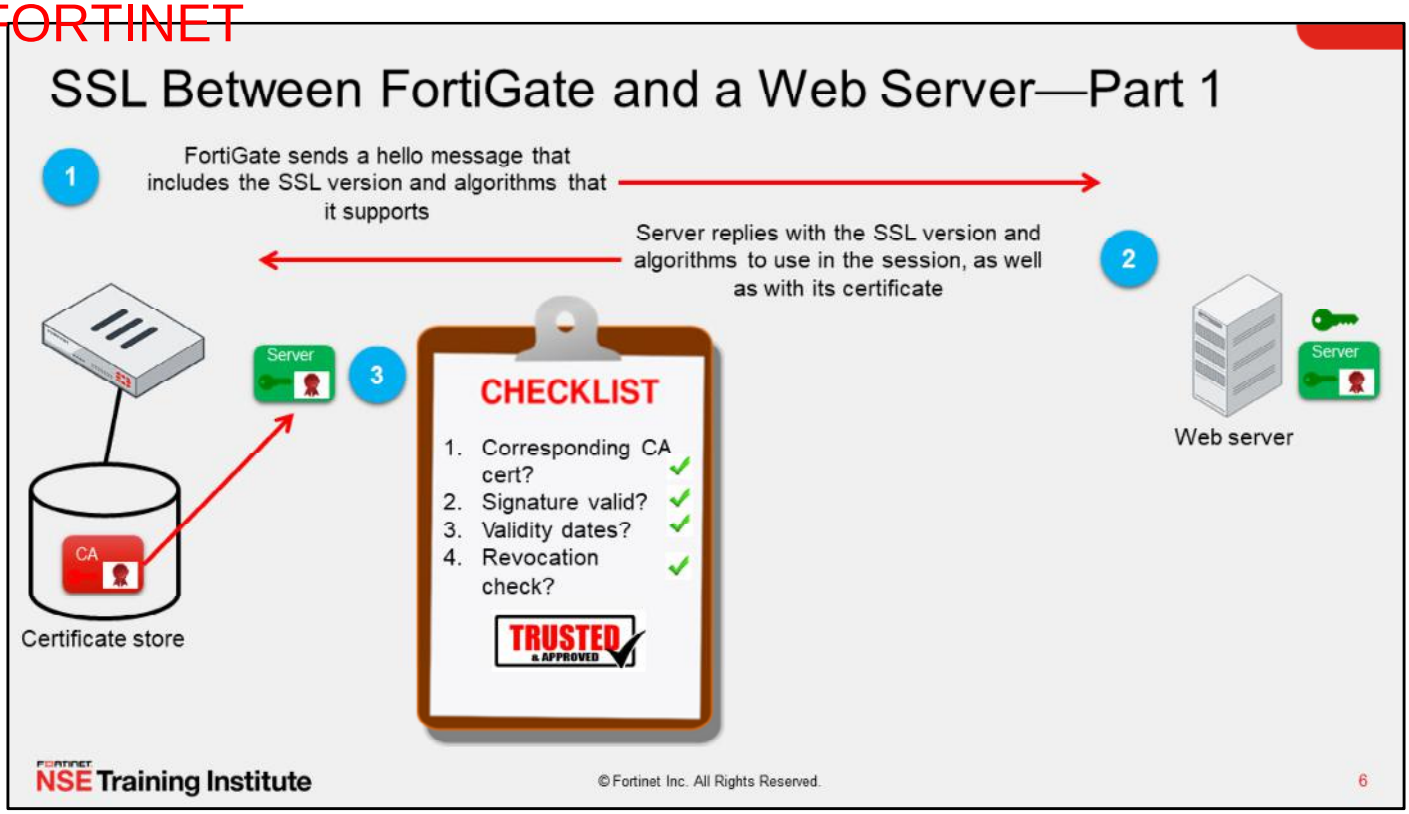
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Asymmetric cryptography, also known as public key cryptography, consists of a pair of keys that are mathematically interrelated and perform inverse functions. Whatever is encrypted with one key can be decrypted only with the other key. One key is made public (it can be distributed to others) and the other key is private. In the example shown on this slide, the sender knows the recipient public key. So, the sender uses the recipient public key to encrypt the information that is intended for the recipient only. Because the information was encrypted using the recipient public key, it can be decrypted using only the recipient private key, which only the recipient has. In this way, the sender ensures that only the intended recipient will be able to decrypt the information.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Now, you will learn more about the process of establishing an SSL session.

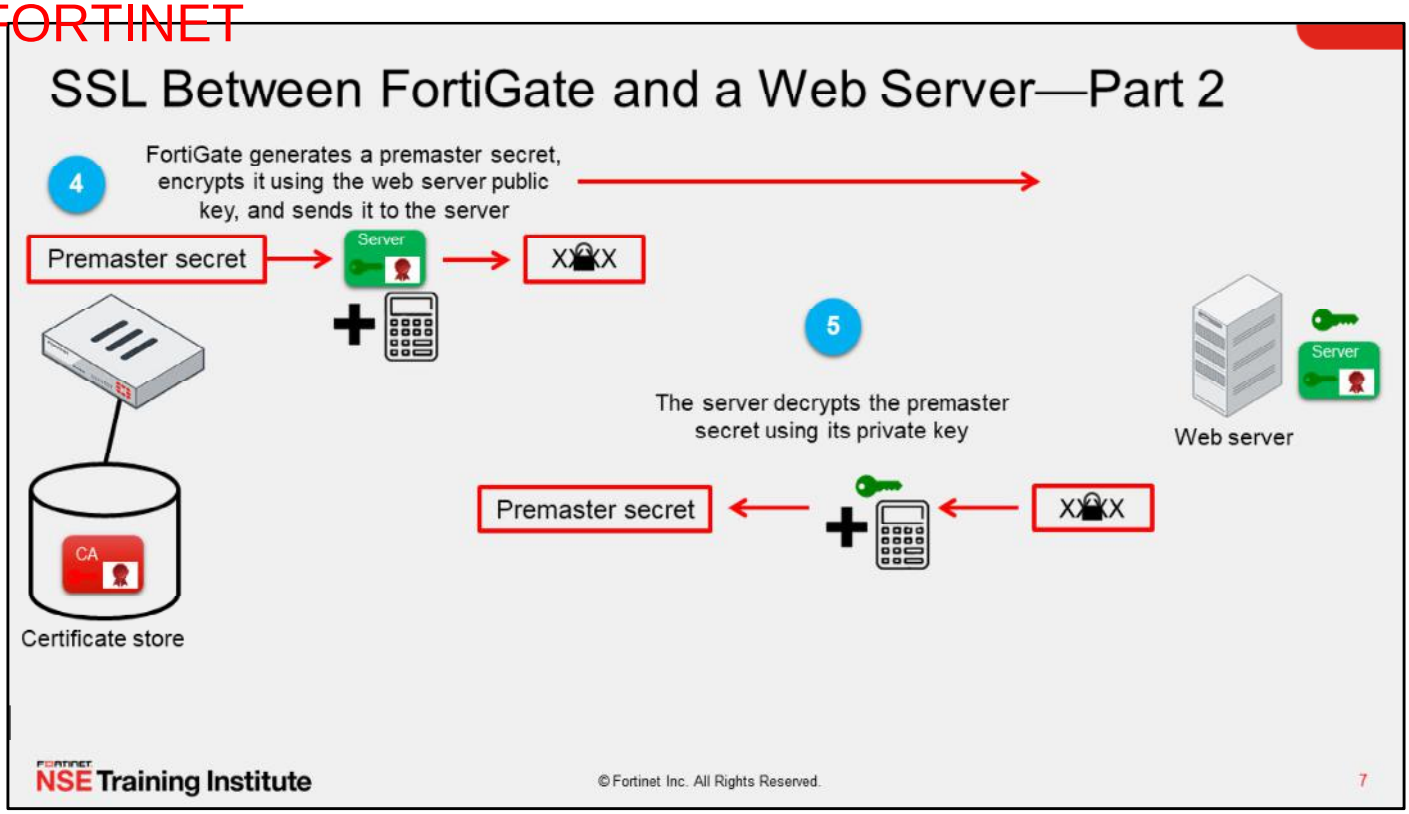
In the first step of the example shown on this slide, FortiGate connects to a web server that is configured for SSL. In the initial hello message, the browser provides critical information that is needed to communicate with the web server. This information includes the SSL version number and the names of the cryptographic algorithms that it supports.

In the second step, the web server receives the message from FortiGate and chooses the first suite of cryptographic algorithms included in the message, and verifies that it is also supported by the web server. The web server replies with the chosen SSL version and cipher suite, and then sends its certificate to FortiGate. Note that the certificate information is passed as cleartext over the public network. The information contained in a certificate is typically public, so this is not a security concern.

In the third step, FortiGate validates the web server certificate. The checklist shown on this slide represents the checks that FortiGate performs on the certificate to ensure that it can be trusted. If FortiGate determines that the certificate can be trusted, then the SSL handshake continues.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

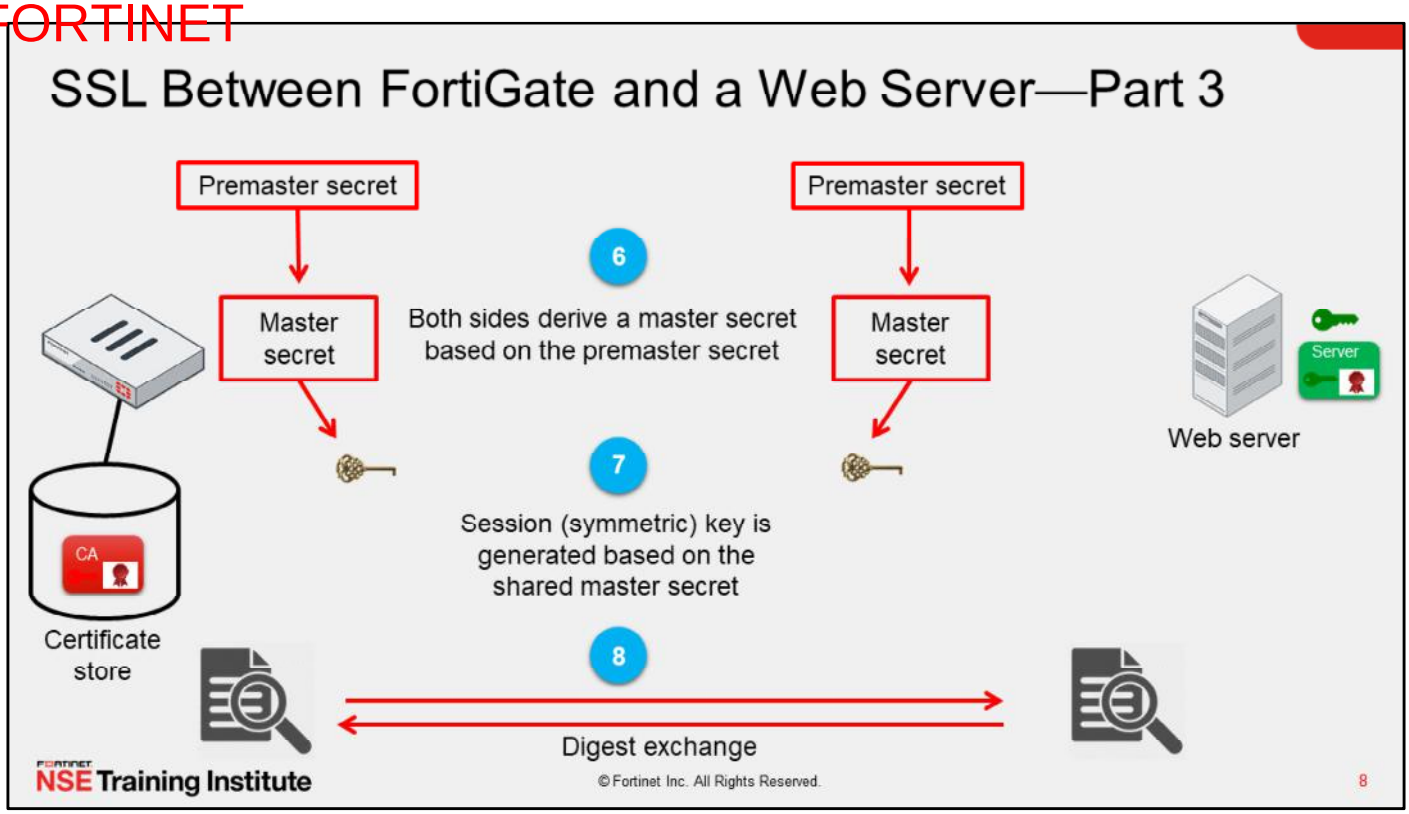


In the fourth step, FortiGate generates a value known as the premaster secret. FortiGate uses the server public key, which is in the certificate, to encrypt the premaster secret. FortiGate then sends the encrypted premaster secret to the web server. If a third-party intercepted the premaster secret, they would be unable to read it, because they do not have the private key.

In the fifth step, the web server uses its private key to decrypt the premaster secret. Now, both FortiGate and the web server share a secret value that is known by only these two devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



In the sixth step, both FortiGate and the web server derive the master secret based on the premaster secret.

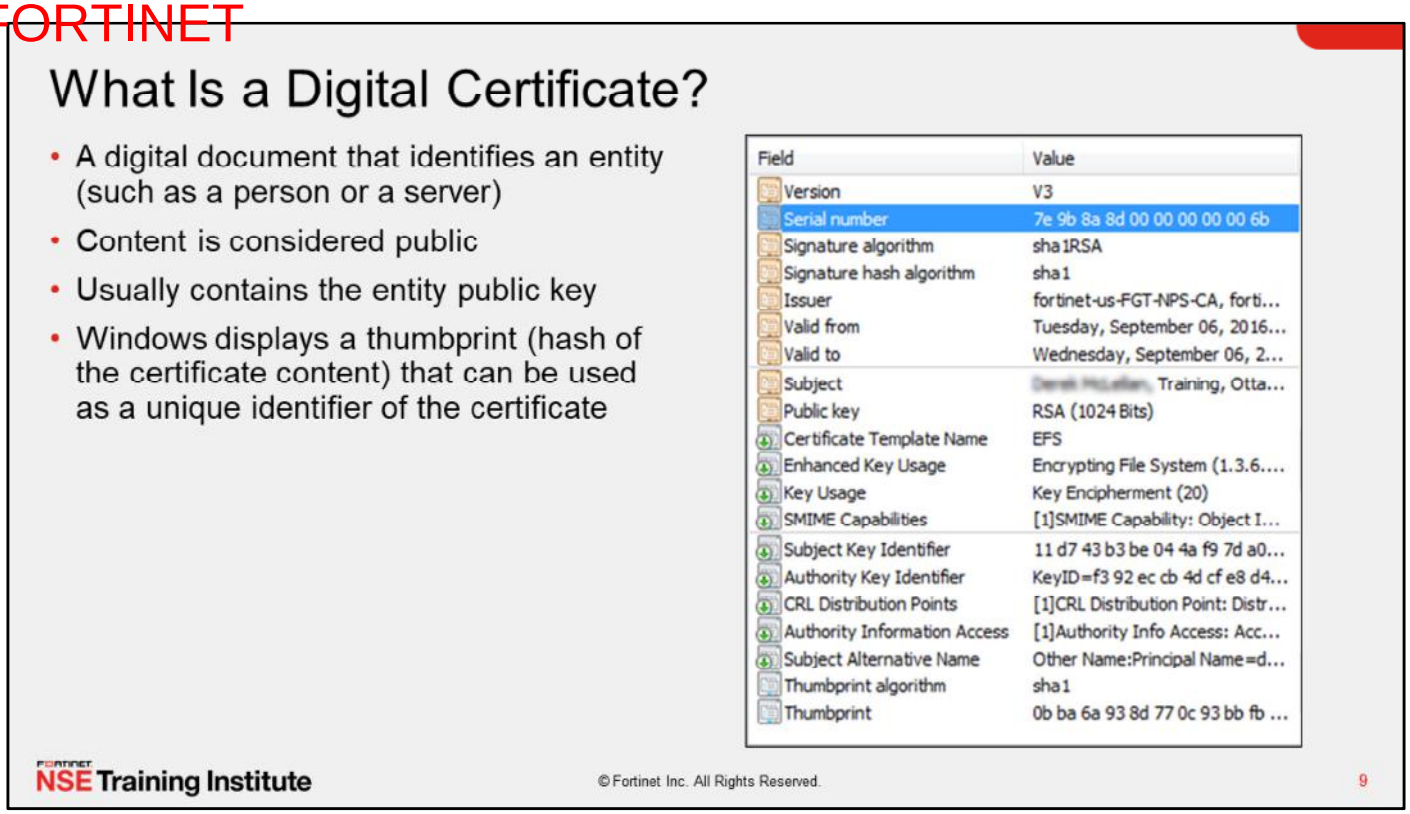
In the seventh step, based on the master secret value, FortiGate and the web server generate the session key. The session key is a symmetric key. It is required to encrypt and decrypt the data. Because both sides have the session key, both sides can encrypt and decrypt data for each other.

In the eighth and final step before these two entities establish the secure connection, both FortiGate and the web server send each other a summary (or digest) of the messages sent so far. The digests are encrypted with the session key. The digests ensure that none of the messages exchanged during the creation of the session have been intercepted or replaced. If the digests match, the secure communication channel is established.

The SSL handshake is now complete. Both FortiGate and the web server are ready to communicate securely, using the session keys to encrypt and decrypt the data they send over the network or internet.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



What is a digital certificate? It is a digital document that identifies an entity (such as a person or device). It usually contains the entity public key.

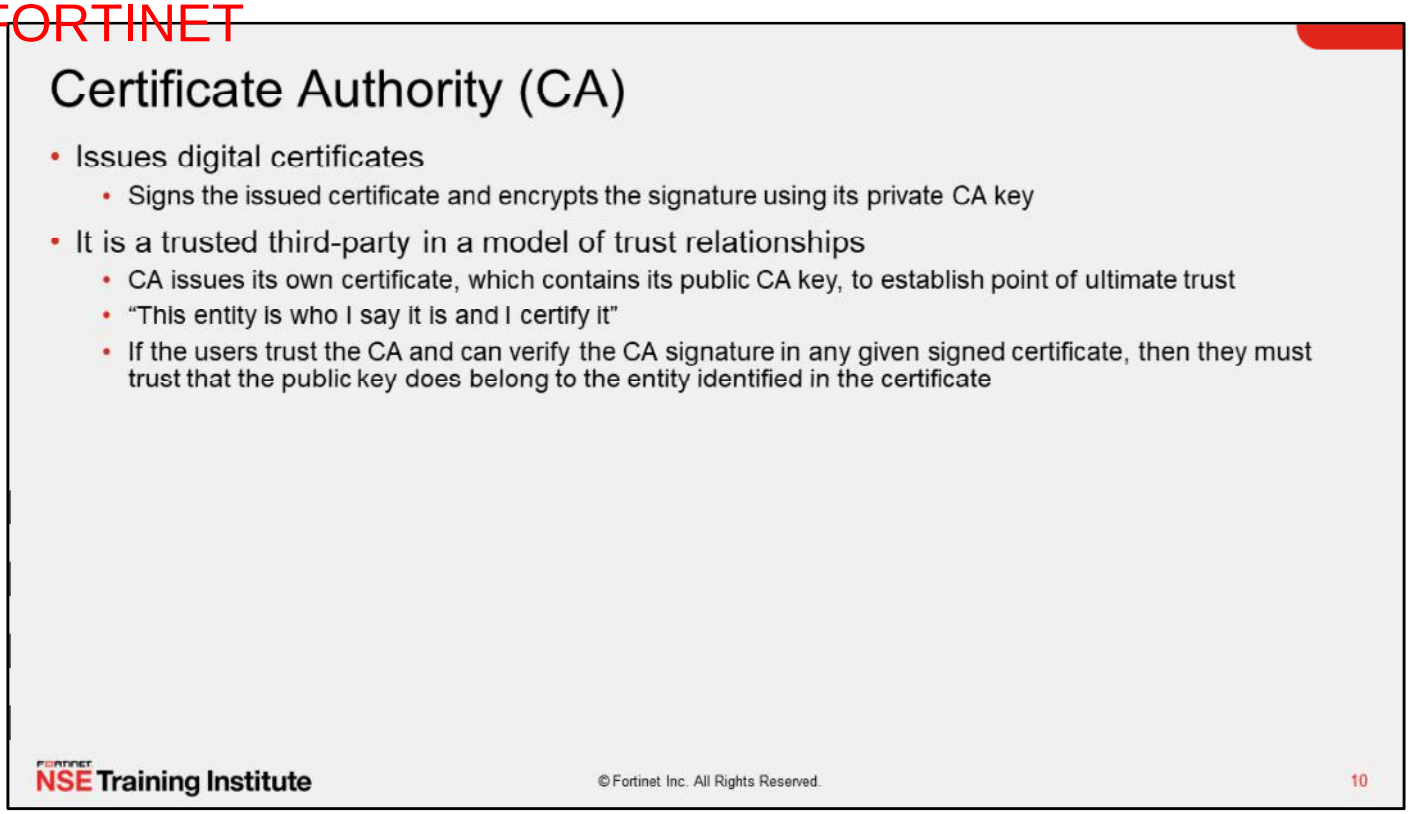
Other important information contained in a certificate is:

- **Serial number**: A unique number for the issuing CA that identifies the certificate.
- **Signature algorithm**: Identifies the hashing and asymmetric algorithms used to produce the digital signature that secures this certificate.
- **Issuer** and **Subject**: Identify the CA that produced the certificate and the entity to whom the certificate is issued. The values are typically expressed using the X.500 or LDAP formats.
- **Valid from** and **Valid to**: Just like a passport or driver's license, a certificate has a validity period—explicit dates on which it is valid. The certificate is invalid on the dates that occur before and after the validity period.
- **CRL Distribution Points**: Identifies to the application where it should retrieve the revocation list from.

In addition, note that some information displayed for a certificate is not actually part of the certificate, but computed from it. This is the case of the **Thumbprint** (or fingerprint), which is a hash of the certificate calculated by Windows, that can be used by applications as a unique identifier for certificates when making trust decisions.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



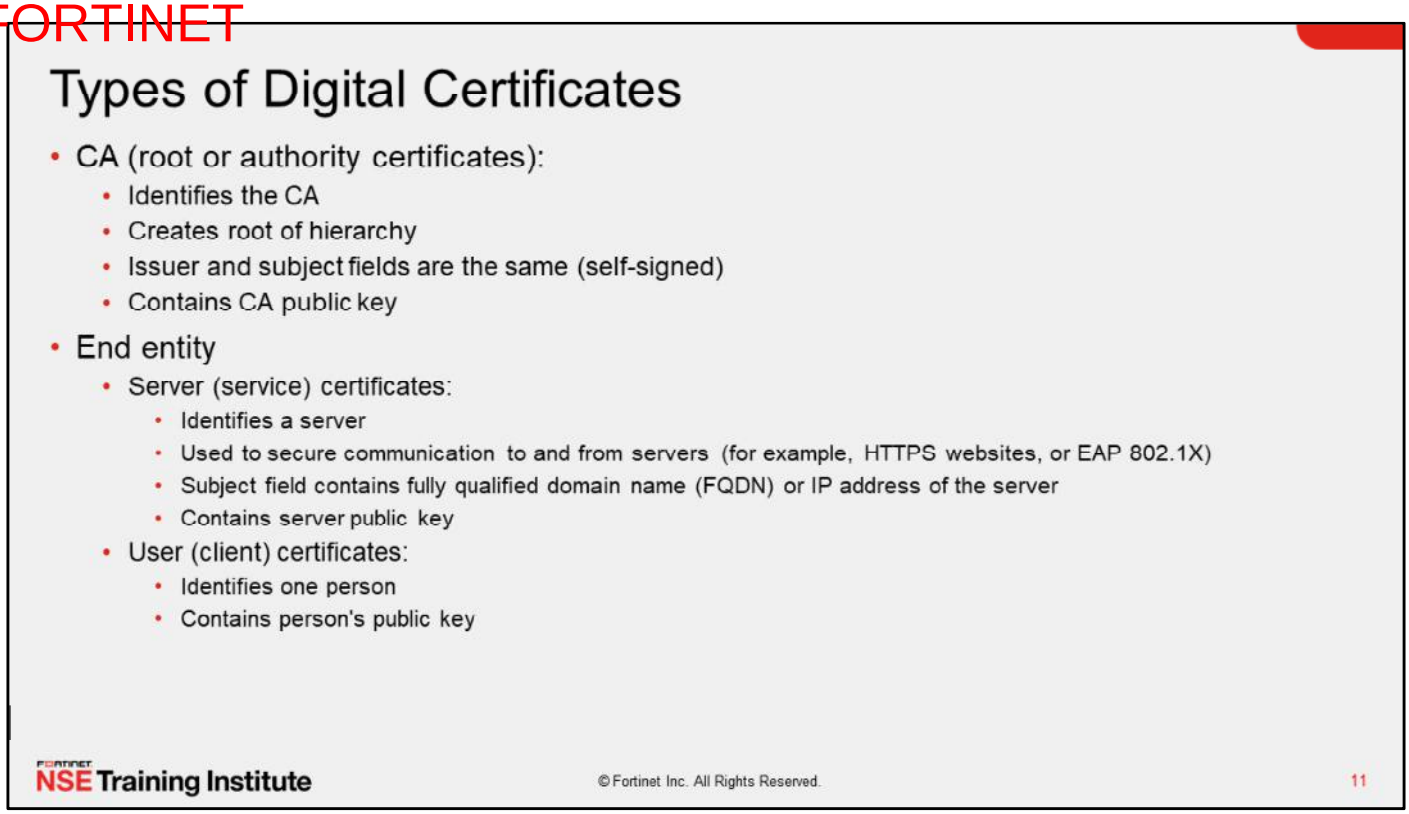
CAs issue and sign digital certificates for end entities. When a CA issues and signs a digital certificate, the CA is essentially proclaiming, "This is the entity who I say it is and I certify it." The CA signature in the digital certificate is encrypted using the CA private key.

PKI uses a relationship trust model, and the CA is at the root of the hierarchy as the trusted third party: everything begins with the CA. A CA issues its own digital certificate—known as the root certificate—in order to establish this point of ultimate trust. After the root certificate is established, the CA can generate digital certificates that are issued and signed by the root.

Accordingly, if users trust the CA and can verify the CA signature as authentic, then they must trust that the public key does belong to the entity identified in the digital certificate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



There are many different types of certificates, each with different functions (and sometimes, confusingly, with different names). A few common certificate types include:

CA certificates (also called root or authority certificates): These certificates identify the CA and create the root of a CA hierarchy. As such, the certificate details have the same input for both the Issuer and Subject fields. These certificates are self-signed and contain the CA public key needed to decrypt signatures in the signed certificates.

Server certificates (also called service certificates): These certificates identify services and are used to secure communication to and from servers, such as HTTPS websites, or Extensible Authentication Protocol (EAP) 802.1X authentication servers. The certificate details have the FQDN (or IP address) of the server in the subject field. The public key of the server is included.

User certificates (also called client certificates): These certificates identify one person to another, a person to a device or gateway, or one device to another device. The certificate includes the public key associated with the identity.

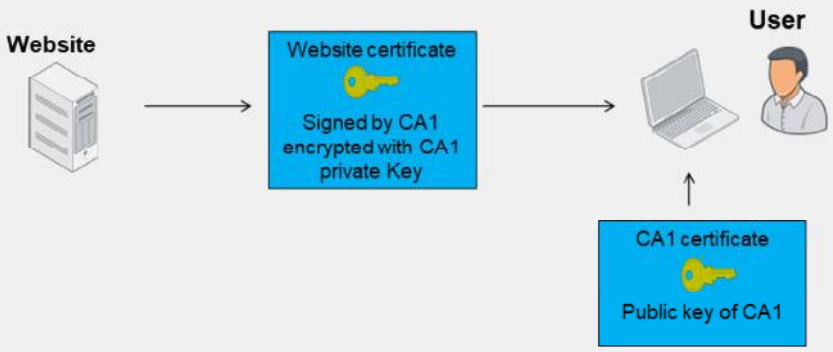
Both user and server certificates belong to the category of end-entity certificates.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Server Authentication

- When a browser is connecting to an HTTPS web page, it receives the website certificate signed by a CA
- The browser must have the CA certificate, containing the CA public key, to decrypt and validate the signature in the website certificate



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

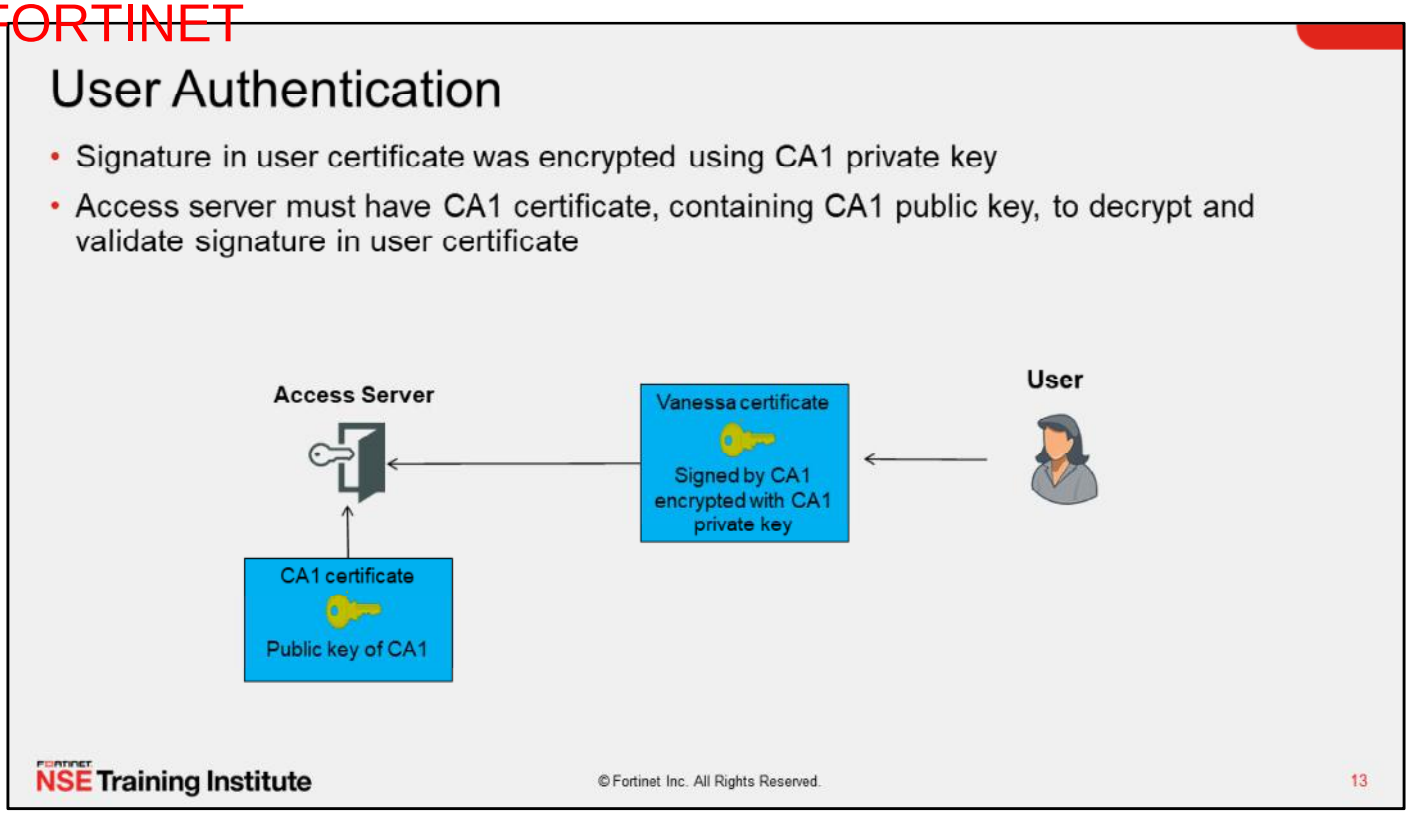
12

In the example shown on this slide, a user with a web browser is connecting to an HTTPS website. The website sends its certificate, which contains its public key and is signed by a CA named CA1. The website certificate signature is encrypted with the CA1 private key. The browser must have the CA1 public key to decrypt and validate the signature in the digital certificate. The CA1 public key is installed in the browser by importing the CA1 digital certificate, which contains its public key.

Most browsers already have preinstalled the CA certificates of the most well-known public CAs. However, if the server certificate is signed by a private CA, the public CA certificate must be installed in the browser. In this way, the browser *trusts* the private CA and can verify the digital certificates that the CA has signed.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



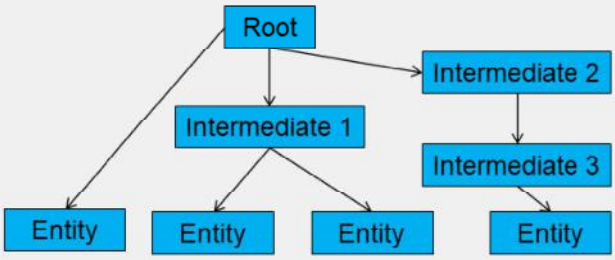
In a similar way, digital certificates can be used to authenticate users. They can be combined with user credentials for two-factor authentication. In this case, when the user is authenticating against an access server, the user sends the digital certificate, which is signed by a CA. In the example on this slide, the CA is CA1. The user certificate signature is encrypted with the CA1 private key. The access server must have the CA1 certificate installed (which contains the CA1 public key) for decrypting and validating the user certificate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Chain of Trust

- **Root**: A self-signed certificate that identifies a CA
- **Intermediate**: A subordinate CA certificate signed by a root or by another intermediate CA
- Both can issue (sign) end-entity certificates



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

14

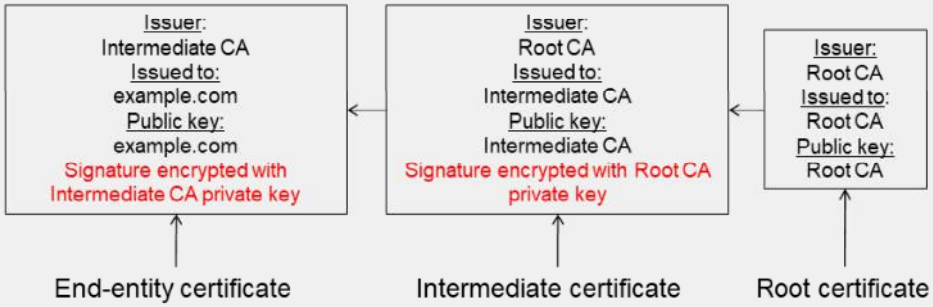
Digital certificates are validated through a chain of trust. The simplest chain of trust occurs when the root CA is directly signing the end-entity certificates. However, a chain of trust can include one or more intermediate CAs. Both root and intermediate CAs can sign end-entity certificates.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Chain of Trust (Contd)

- The path that must be followed to validate a certificate is called a chain of trust or certification path



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

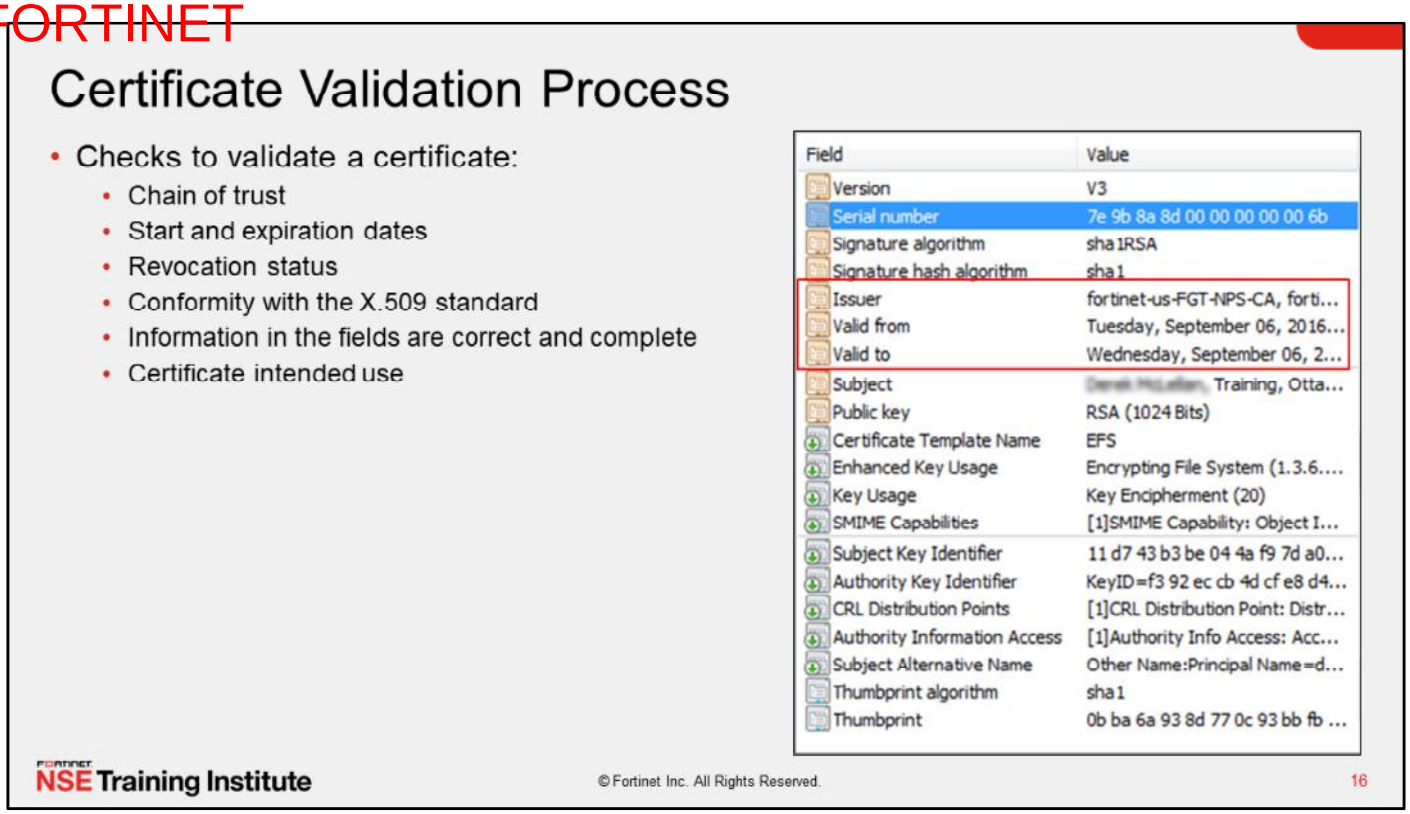
15

In the example shown on this slide, the end-entity certificate was signed by an intermediate CA. The intermediate CA certificate was signed by the root CA.

The process of validating the end-entity certificate goes from top to bottom on the chain of trust. The public key of the intermediate certificate (included in the intermediate CA certificate) is used to validate the signature in the end-entity certificate. Additionally, the root public key (included in the root certificate) is used to validate the signature in the intermediate CA certificate. For this reason, the validation of the end-entity certificate requires the certificates of both the root CA and the intermediate CA.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

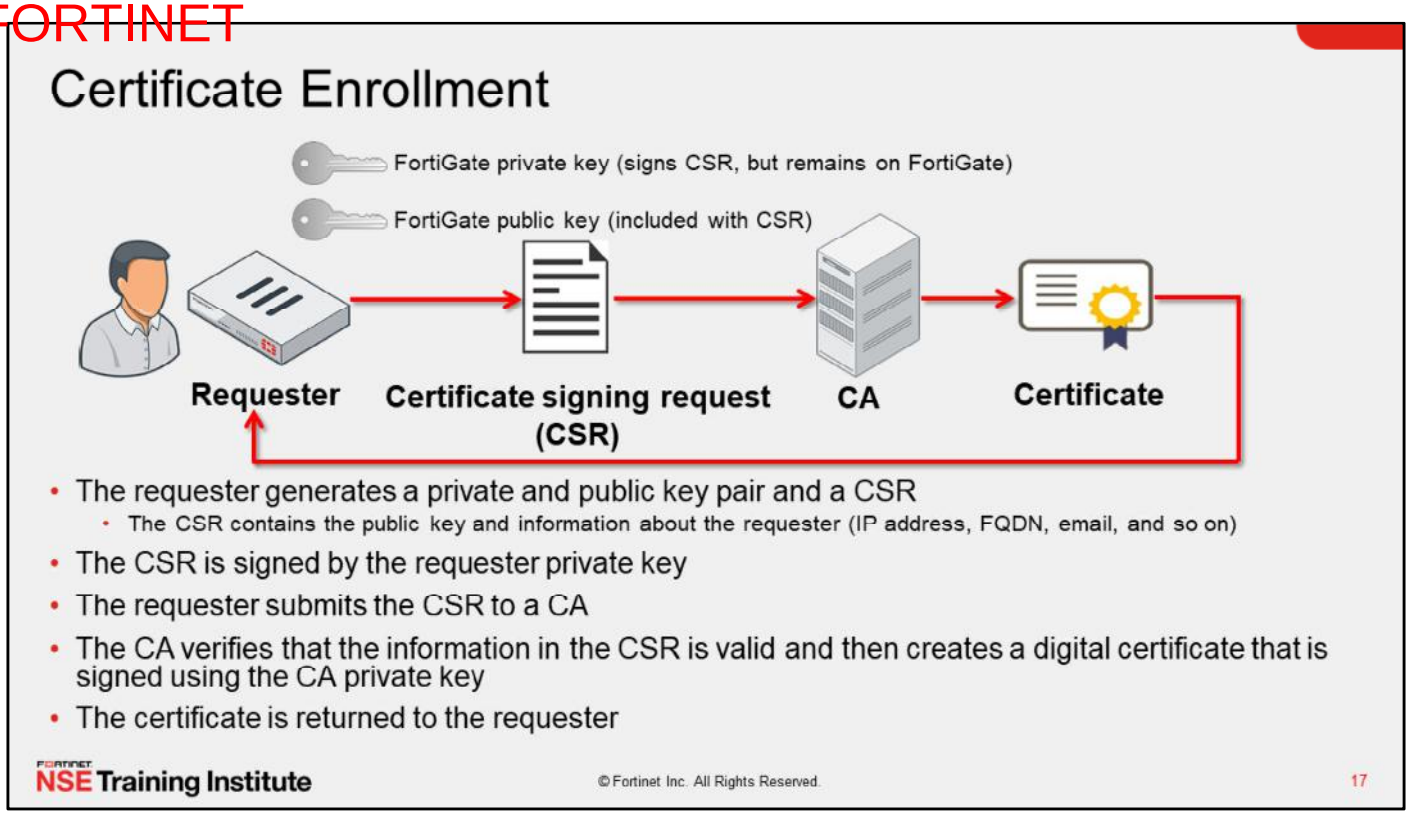


For each step in the chain of trust, the following checks are run to validate a certificate:

- Chain of trust
- Valid period (start and expiration dates)
- Revocation status
- Conformity with the X.509 standard
- Information in the fields are proper and complete
- Certificate intended use

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

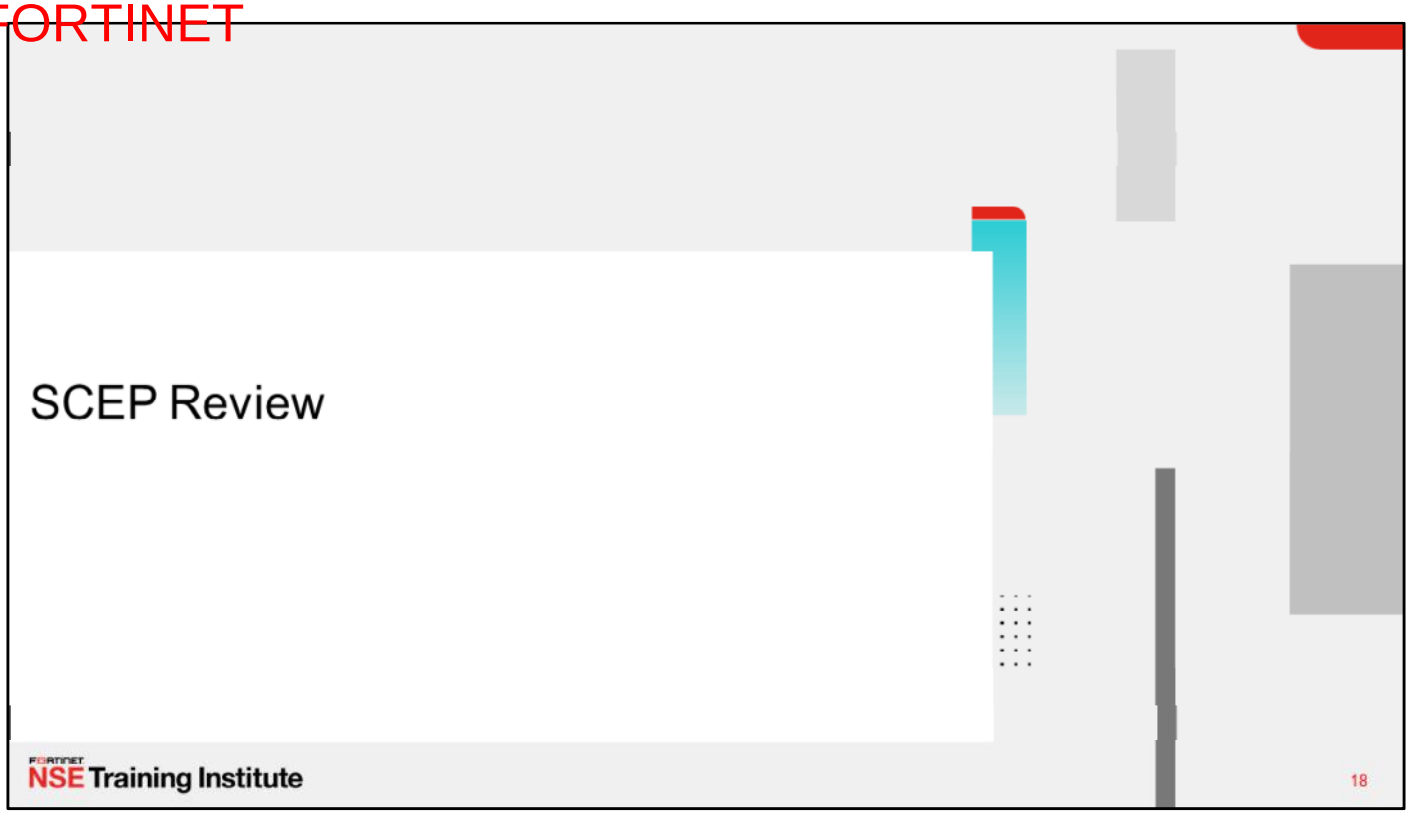


The process of obtaining a digital certificate begins with the creation of a CSR. The process is as follows:

1. The requester generates a private and public key pair and a CSR. The CSR includes the requester public key and specific information about the requester (IP address, distinguished name, email address, and so on). Note that the private key remains confidential.
2. The CSR is signed by the requester private key.
3. The requester submits the CSR to a CA
4. The CA verifies that the information in the CSR is valid and then creates a digital certificate for the requester. The certificate is digitally signed using the CA private key.
5. The certificate is returned to the requester.

Vouchers & Dumps are Available | WhatsApp +201224560923

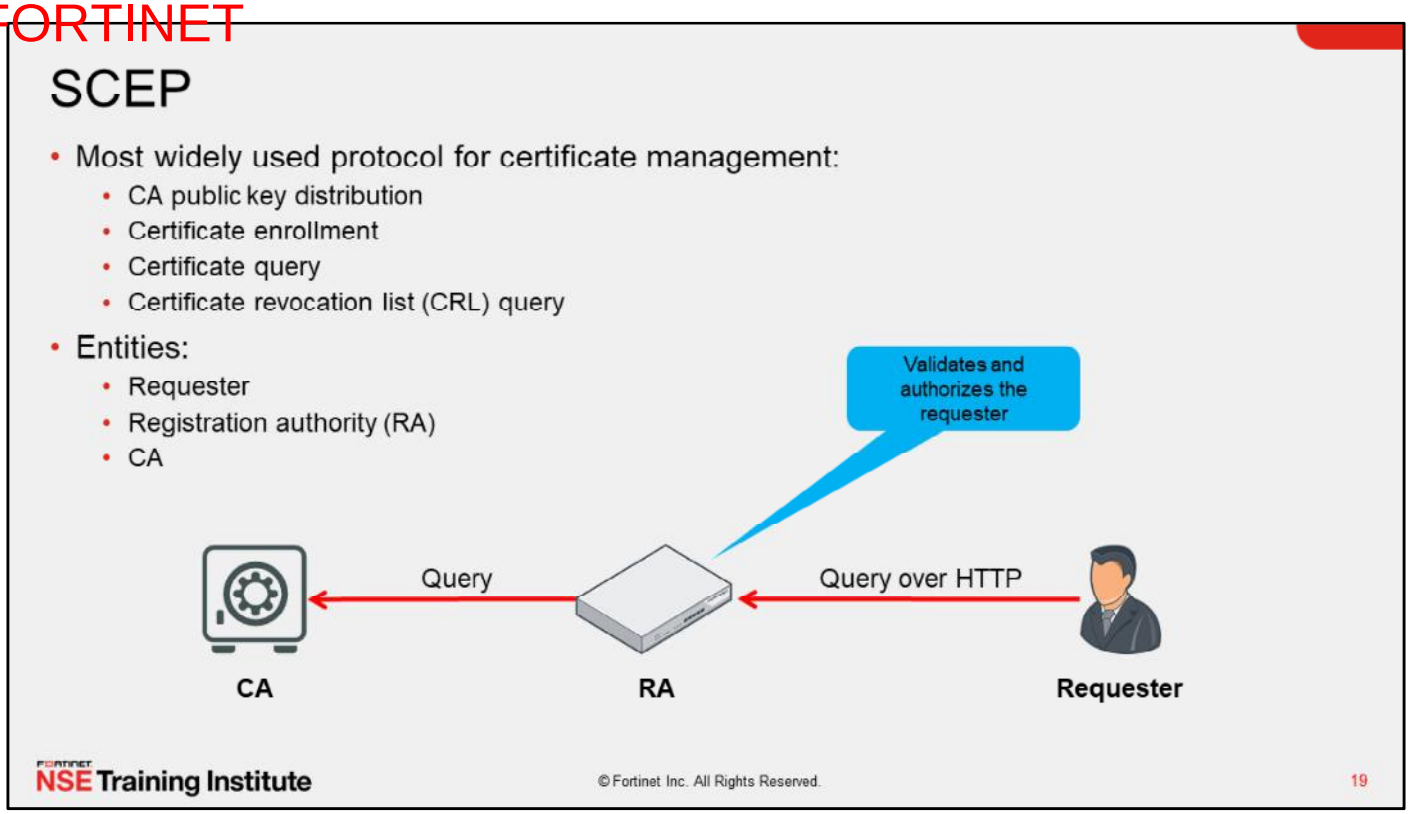
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will review SCEP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

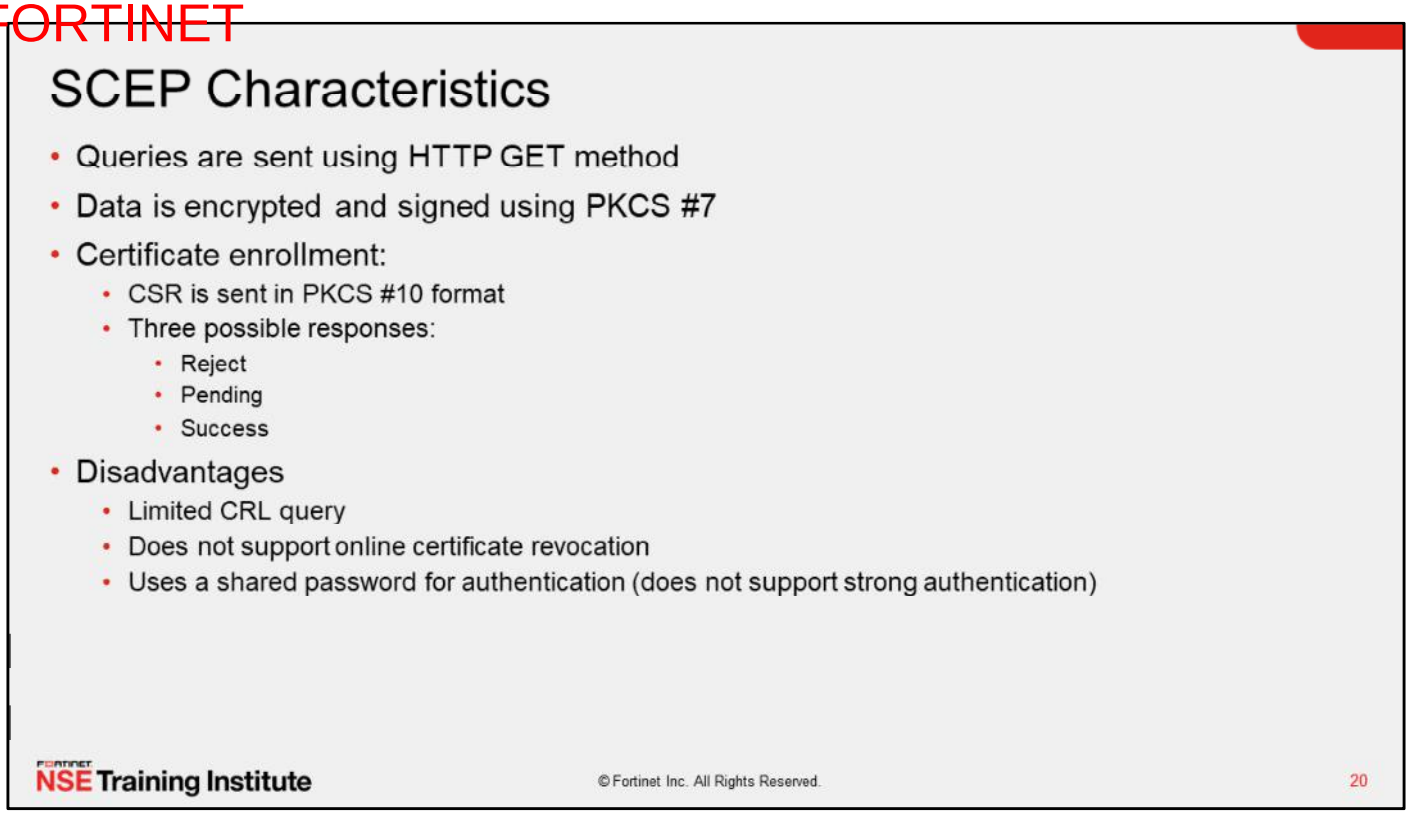


SCEP is probably the most widely used protocol for certificate management. It allows a requester to query a registration authority (RA) to get CA certificates, revocation lists, and submit CSRs.

The RA forwards the query to the CA to get the information for the requester.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



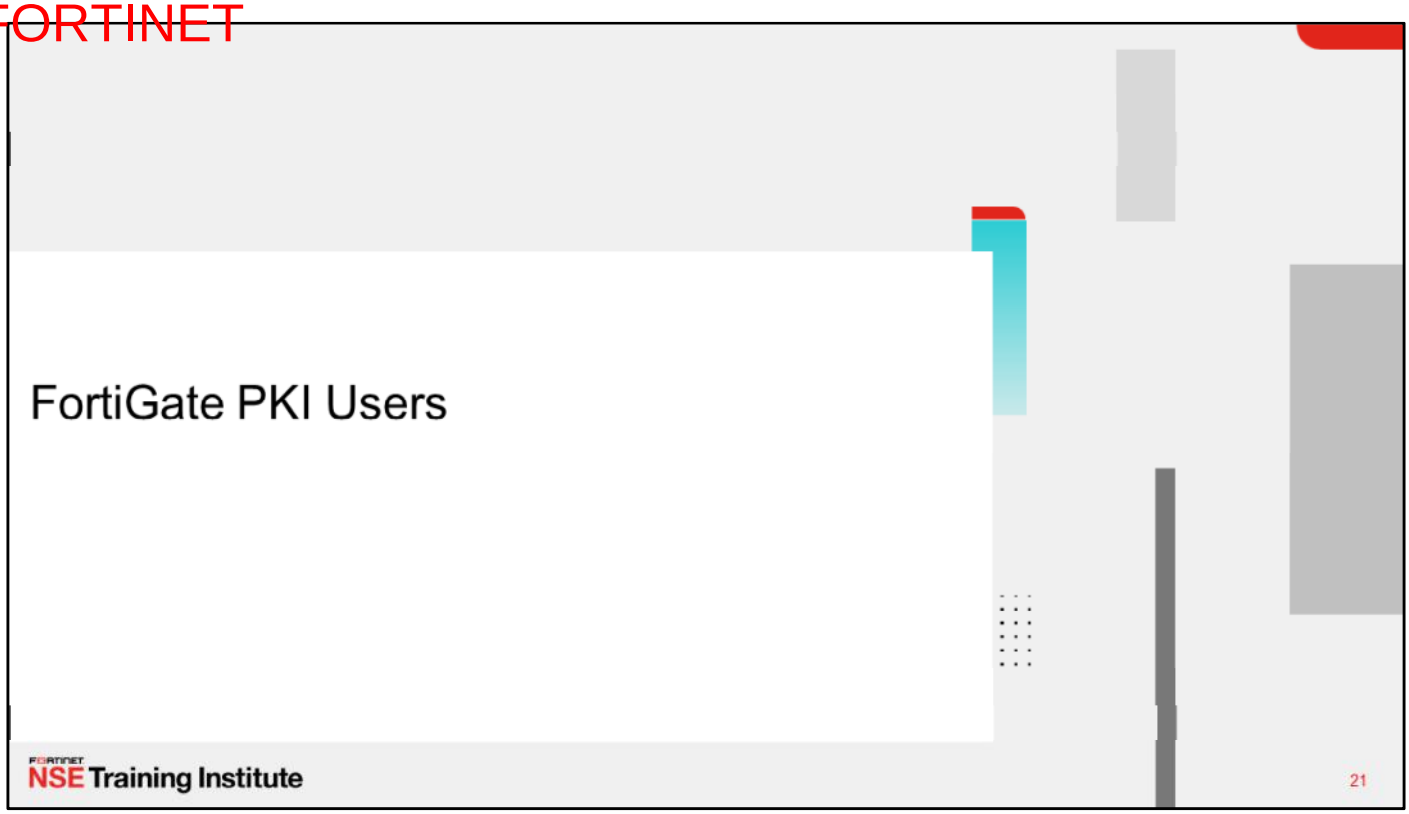
SCEP is based on HTTP. It uses the regular HTTP GET method to send queries to the RA. Data, though, is encrypted and signed using the standard PKCS #7.

CSRs sent by requesters follow the PKCS #10 format. When the RA receives a CSR, it replies with one of the following three answers: reject, pending, or success. When the CSR is received successfully (and if it has already been preapproved by an administrators) the RA issues, signs, and sends the requester certificate back to the requester.

SCEP has some disadvantages though. It supports a very limited number of CRL queries, does not support online certificate revocation checks, and does not support strong authentication.

Vouchers & Dumps are Available | WhatsApp +201224560923

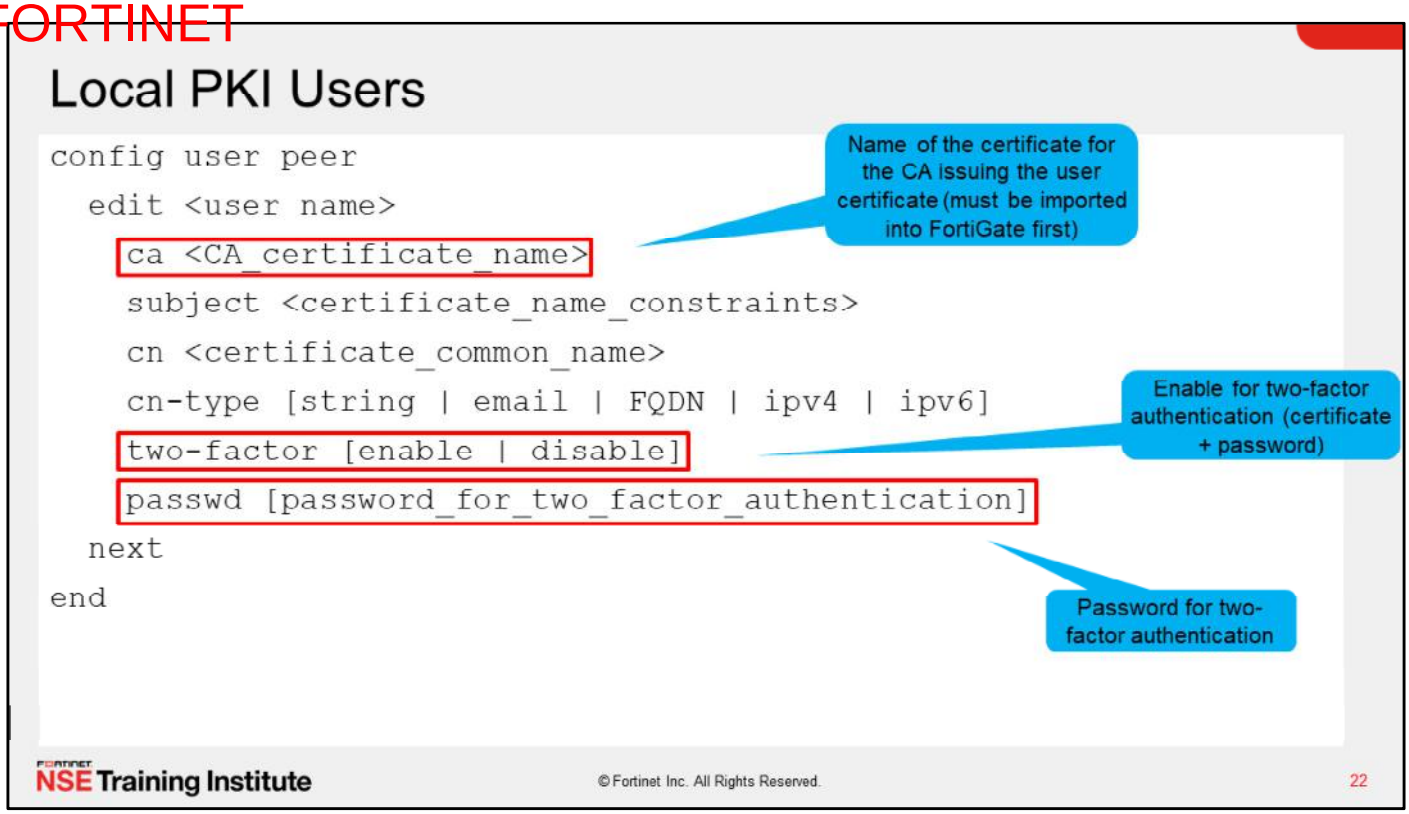
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn how to create PKI users on FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You must use the CLI to create the first PKI user. After you create the first PKI user, and as long as there is at least one PKI user, the menu option to create and administrate more PKI users will appear on the GUI.

This slide shows the CLI commands for creating a PKI user. One of the most important settings (`ca`) defines the digital certificate of the CA that signed the end-entity certificate for this PKI user. This CA certificate must have been installed previously on FortiGate.

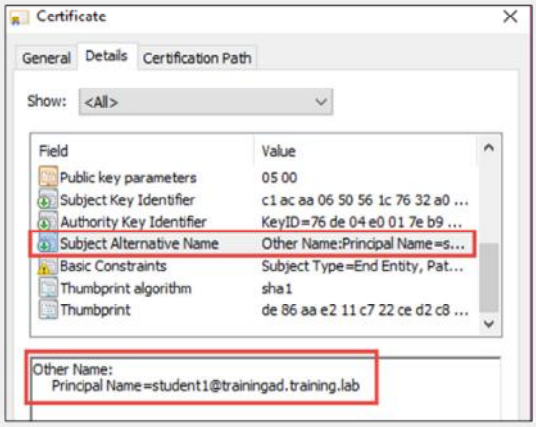
You can combine certificate-based authentication with user credentials to offer two-factor authentication. After you enable two-factor authentication for a PKI user, you must add the PKI user password.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Authorizing PKI Users Using Principal Name

- FortiGate can use LDAP to validate the information in the certificate user principal name (UPN) field
  - Authentication fails if no valid user has a UPN that matches the UPN in the certificate



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

23

On some occasions, the user certificate might include the UPN, which is a user attribute in Windows AD that you can use to identify the user. You can configure FortiGate to use LDAP to validate this field against a Windows AD server. The authentication fails if no valid user has a UPN that matches the user certificate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Authorizing PKI Users Using UPN

```
config user peer
  edit "student"
    set ldap-mode principal-name
    ca CA_Cert_1
    subject student
    cn trainingad.training.lab
    cn-type string
    set ldap-server "Training-Lab
  next
end
```

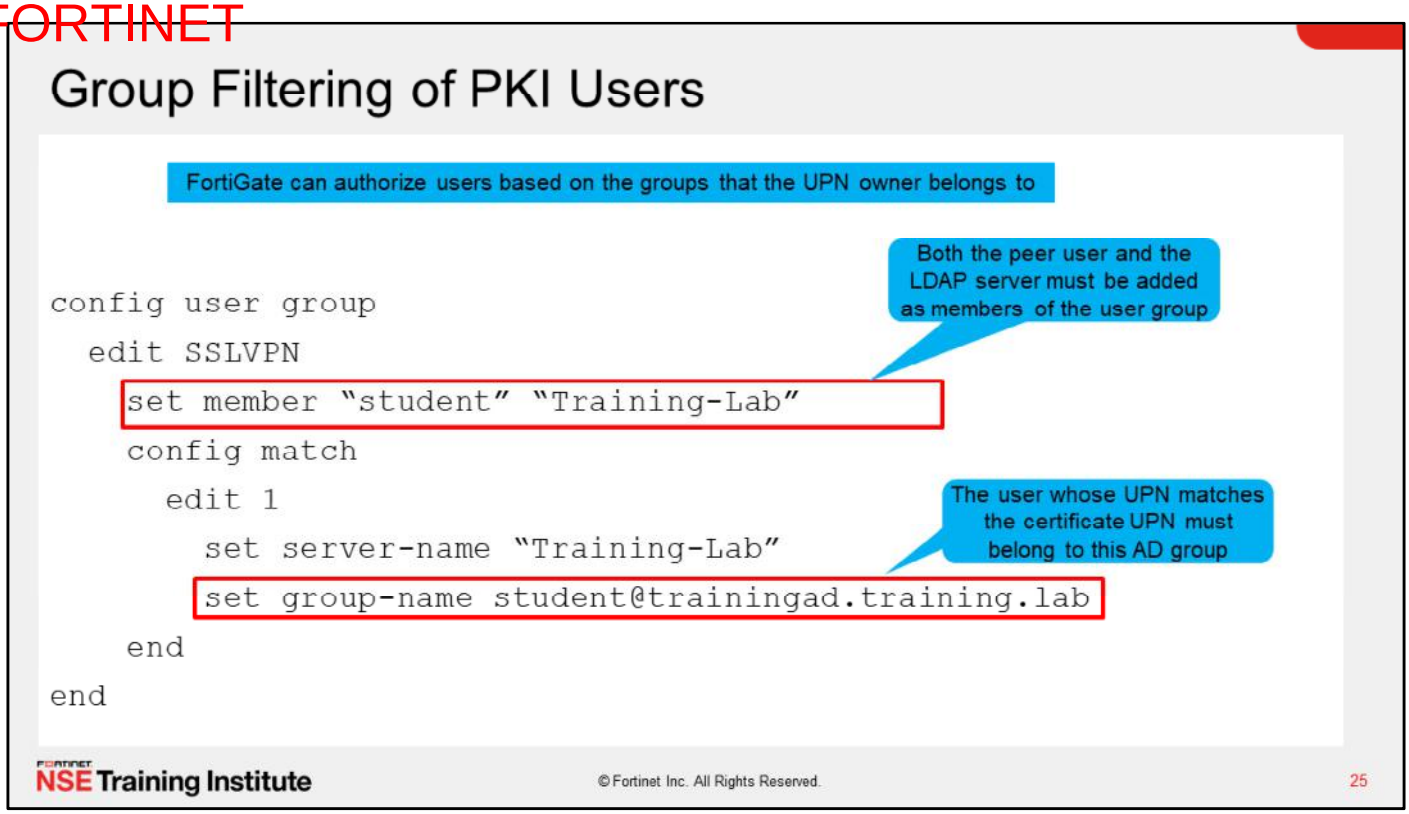
- Enable UPN checking
- To match subject name on user certificate
- Certificate common name
- It can be string, email, FQDN, ipv4, ipv6
- Name of the LDAP server

NSE Training Institute © Fortinet Inc. All Rights Reserved. 24

To configure FortiGate to check the UPN in a user certificate, you must change the `ldap-mode` setting to `principal-name`. Additionally, you must enter the name of the LDAP server previously configured on FortiGate, that will be used to validate the UPN.

Vouchers & Dumps are Available | WhatsApp +201224560923

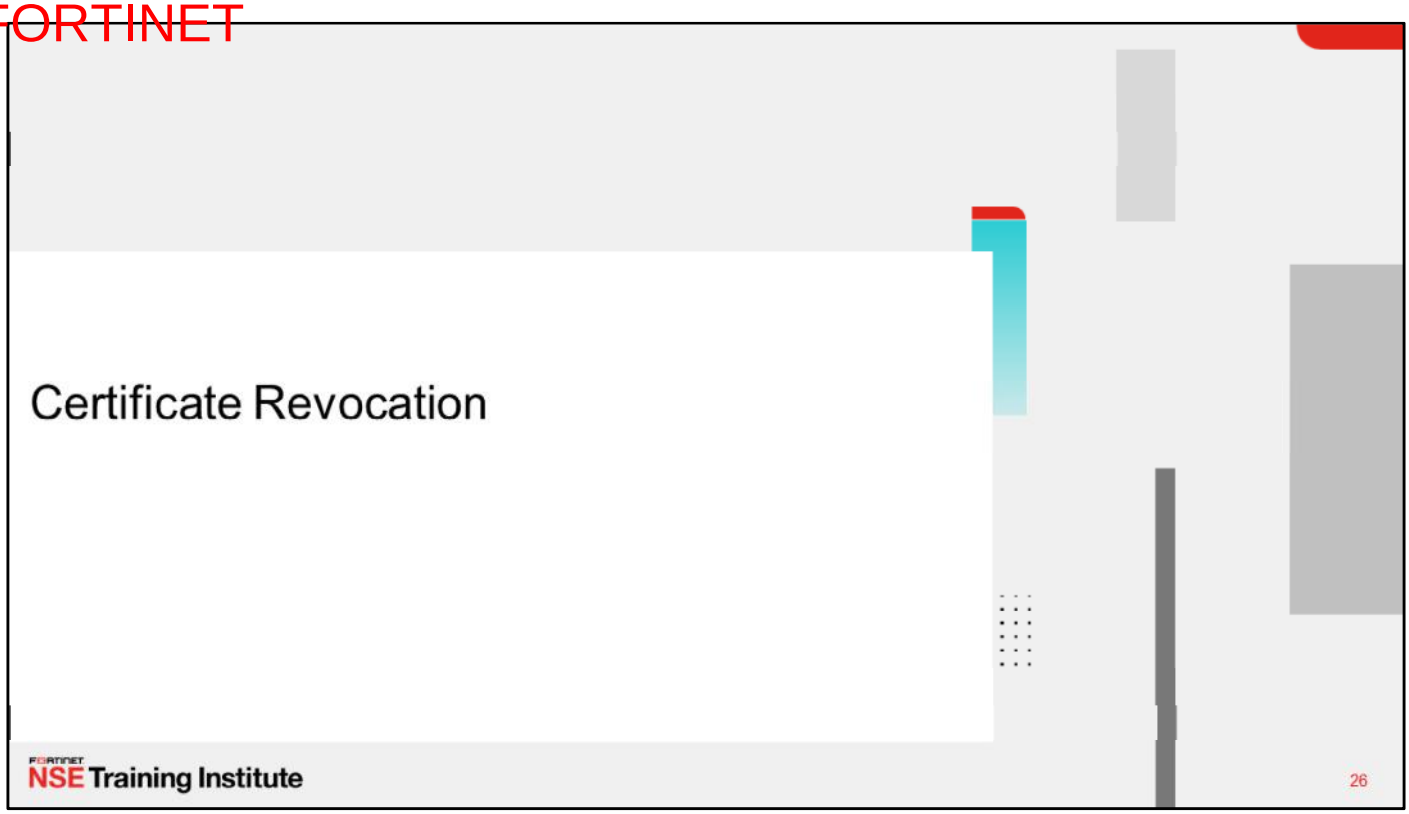
DO NOT REPRINT Brave-dumps.com
© FORTINET



When you configure UPN validation for a PKI user, and the UPN belongs to a valid user, FortiGate queries the LDAP for the user groups. You can use that information to authorize access only to users that belong to specific groups.

Vouchers & Dumps are Available | WhatsApp +201224560923

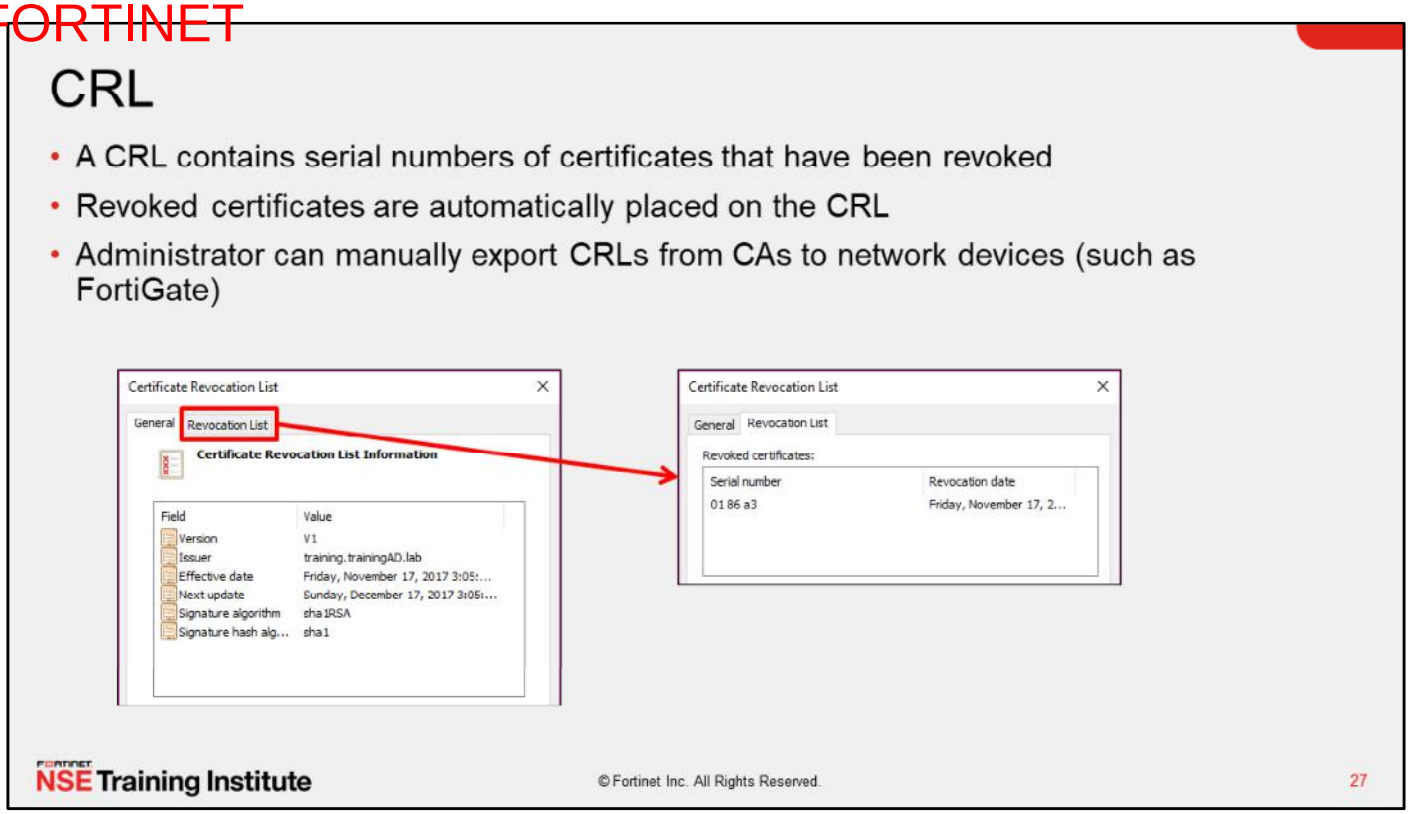
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will review CRLs and learn how to use OCSP for certificate revocation checks.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

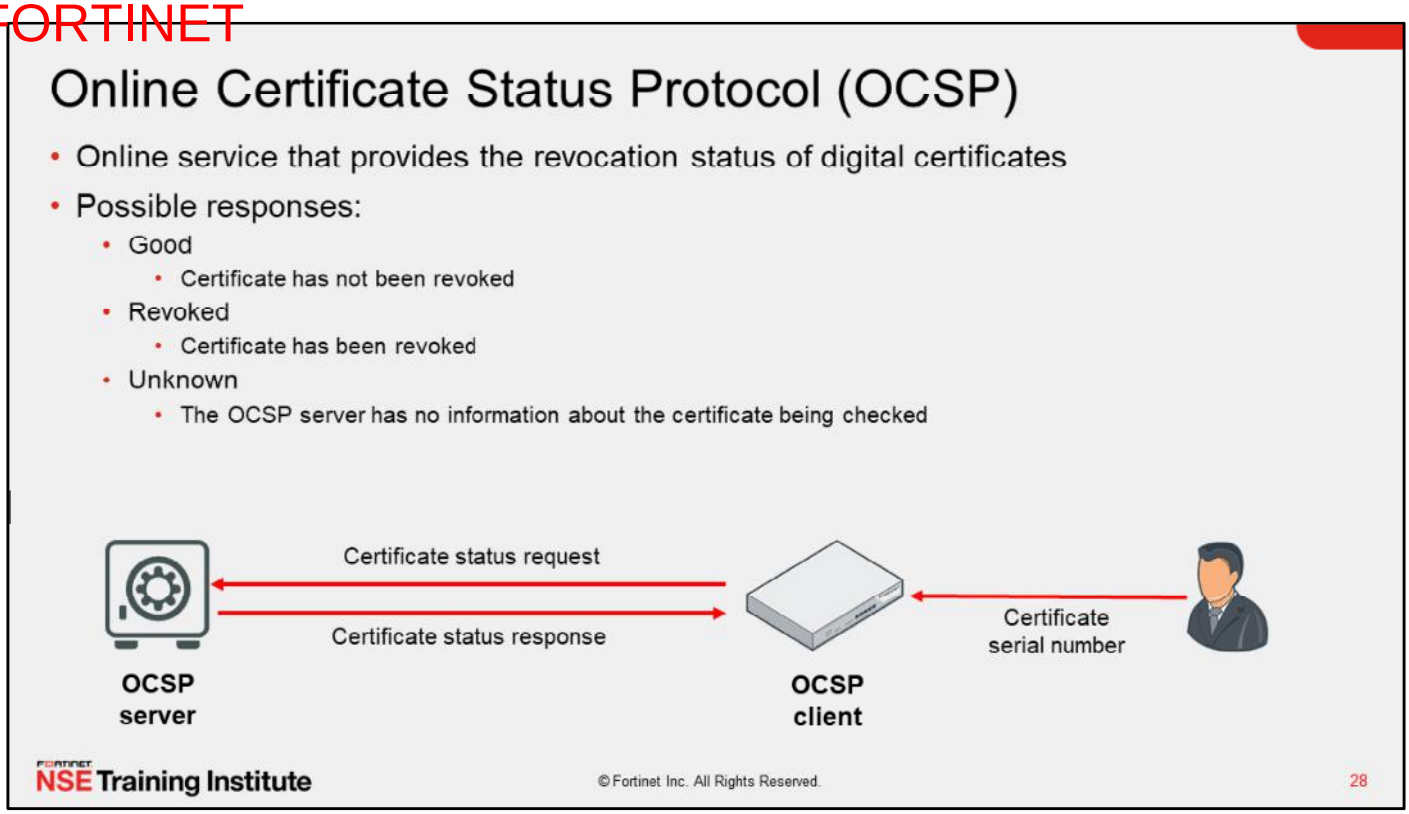


A CRL contains the serial numbers of certificates that have been revoked. There is usually one CRL per root CA.

Administrators can manually download a CRL from a CA and import it on FortiGate. Each time a user presents a certificate, FortiGate checks that the serial number of the certificate is not in the CRL of the CA that signed the certificate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

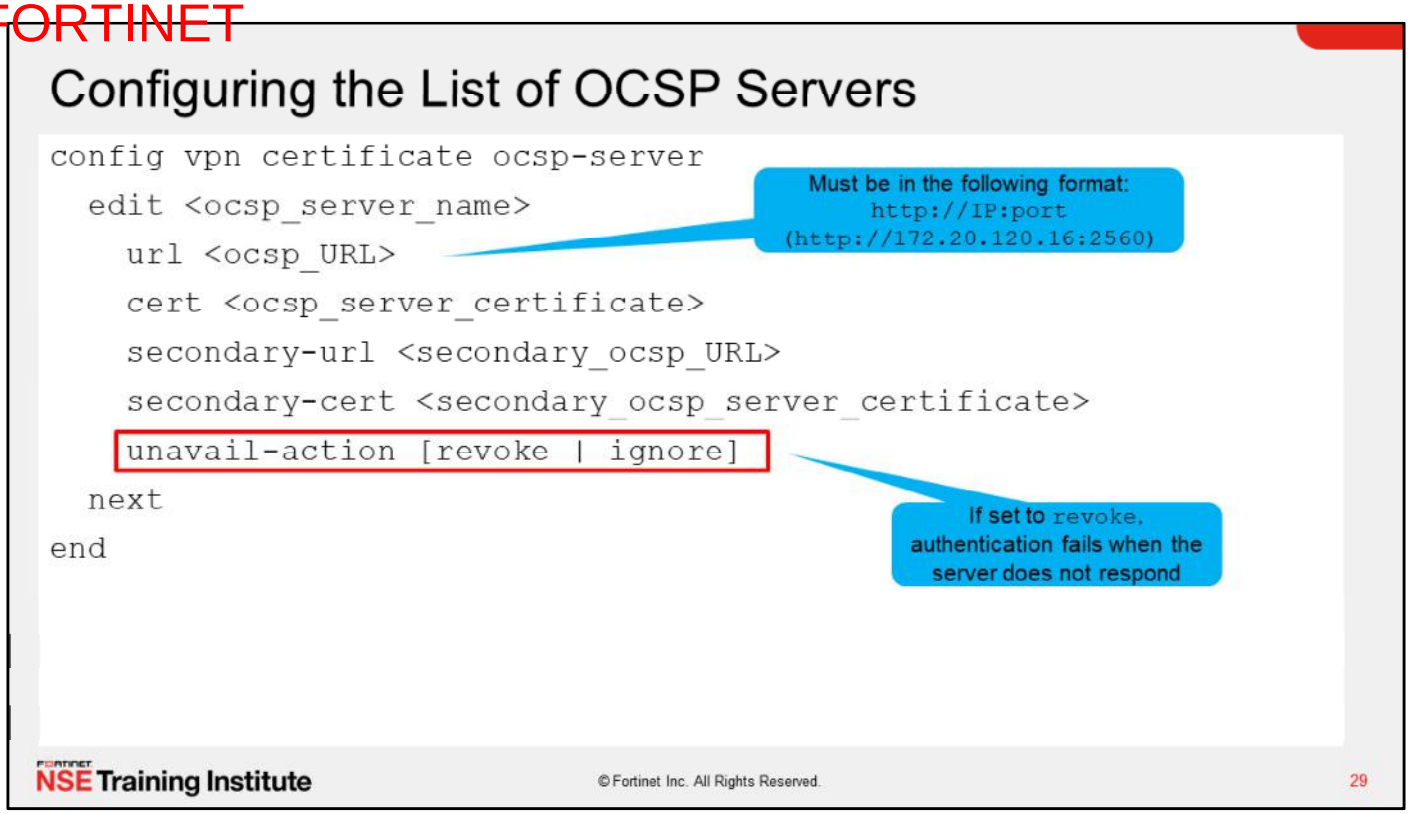


The OCSP offers an online service that provides the revocation status of a digital certificate. Using this protocol, administrators do not need to manually import the CRL into FortiGate. Each time a user presents a certificate, FortiGate uses OCSP to send the certificate serial number to an OCSP server. The OCSP server replies with one of three possible answers:

- **Good**: The certificate has not been revoked.
- **Revoked**: The certificate has been revoked.
- **Unknown**: The OCSP server has no information about the certificate being checked, usually because the certificate was issued by an unrecognized CA that is not served by the OCSP server.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



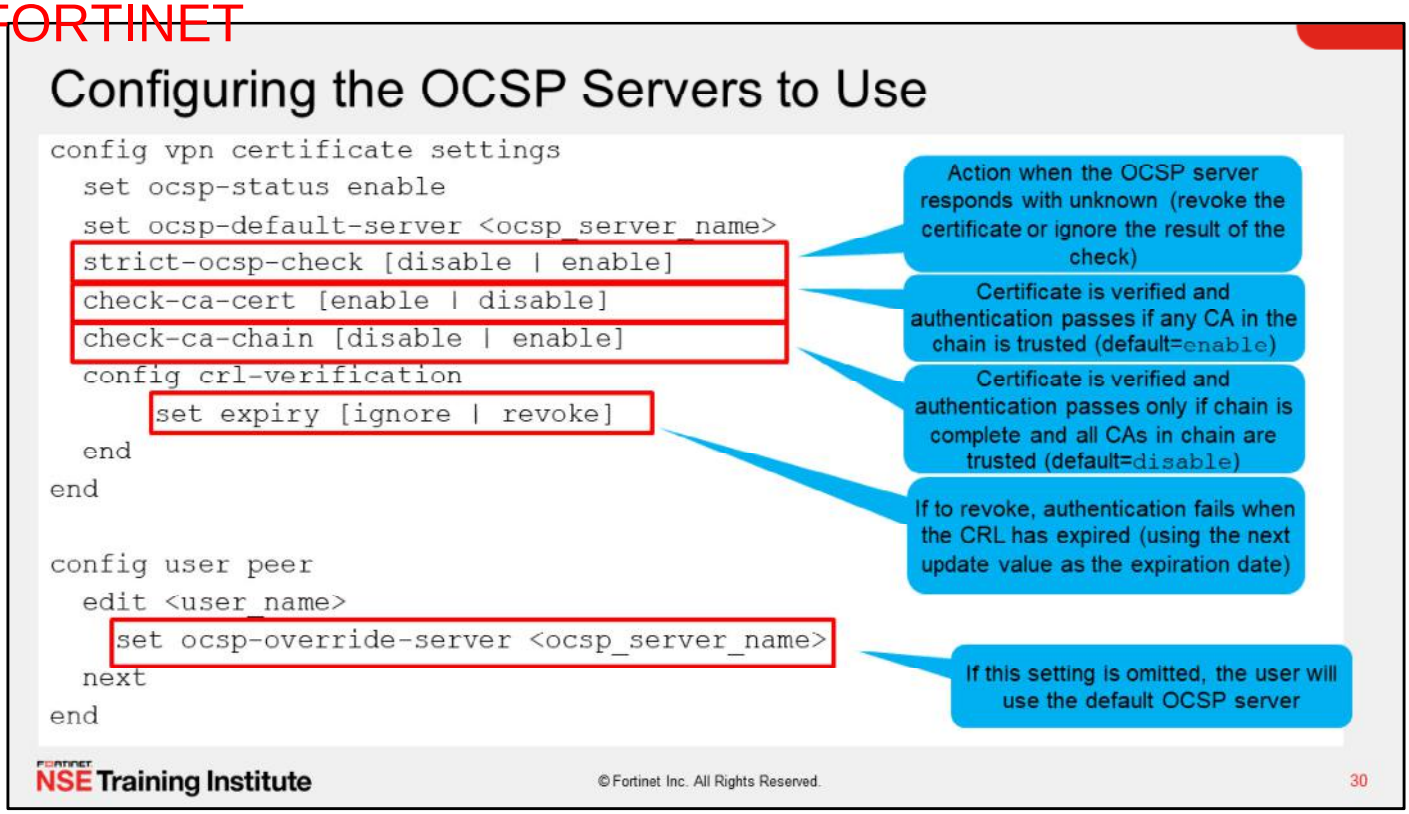
You can configure FortiGate with a list of OCSP servers that can be used to validate the revocation status of user certificates. For each OCSP server, you configure its URL and the CA certificate (`cert`) of the CA that signed the OCSP certificate (this is used for authenticating the OCSP server). Optionally, you can configure a secondary (backup) OCSP server, for cases where the primary server does not reply.

If the `unavail-action` setting is set to `revoke`, the certificate is rejected if the OCSP server does not respond.

If the `unavail-action` setting is set to `ignore`, the certificate is accepted, even for cases when the OCSP server does not respond.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Under `config vpn certificate settings`, you select which OCSP server (from the previous list) will be the default server used for checking revocation status. You can override that setting per user using the `ocsp-override-server` setting under `config user peer`.

If `strict-ocsp-check` is enabled, the certificate is rejected if the OCSP server responds with a certificate unknown state.

If you are using a CRL list instead of OCSP, the `expiry` setting under `config crl-verification` defines the action to take when the CRL has expired.

Vouchers & Dumps are Available | WhatsApp +201224560923

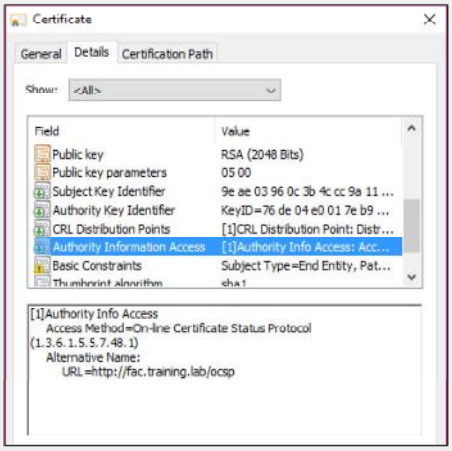
DO NOT REPRINT
© FORTINET
Brave-dumps.com

OCSP URL Embedded in the Certificate

- Certificates can include the OCSP URL
- You can configure FortiGate to use the OCSP URL in the certificate (if present), instead of the one statically configured:

```
config vpn certificate setting
  set ocsp-option [certificate | server]
end
```

  - `certificate`: Use URL from certificate (if present)
  - `server`: Always use URL in FortiGate configuration



NSE Training Institute

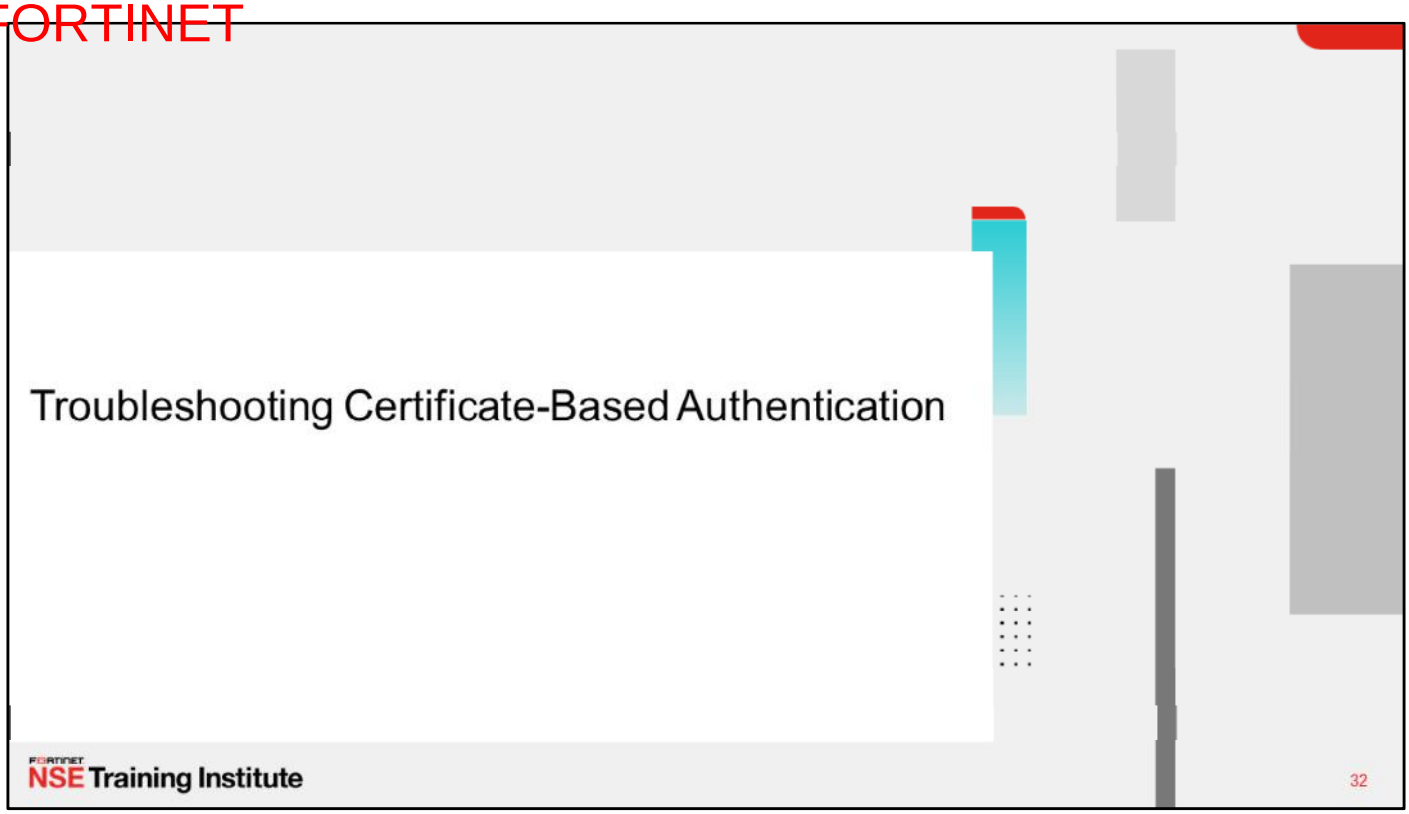
© Fortinet Inc. All Rights Reserved.

31

In some cases, the user certificates contain the URL of an OCSP server that can be used to check the revocation status. You can configure FortiGate to either use this information (if available in the certificate), or ignore it (and keep using the OCSP server configured in the FortiGate configuration).

Vouchers & Dumps are Available | WhatsApp +201224560923

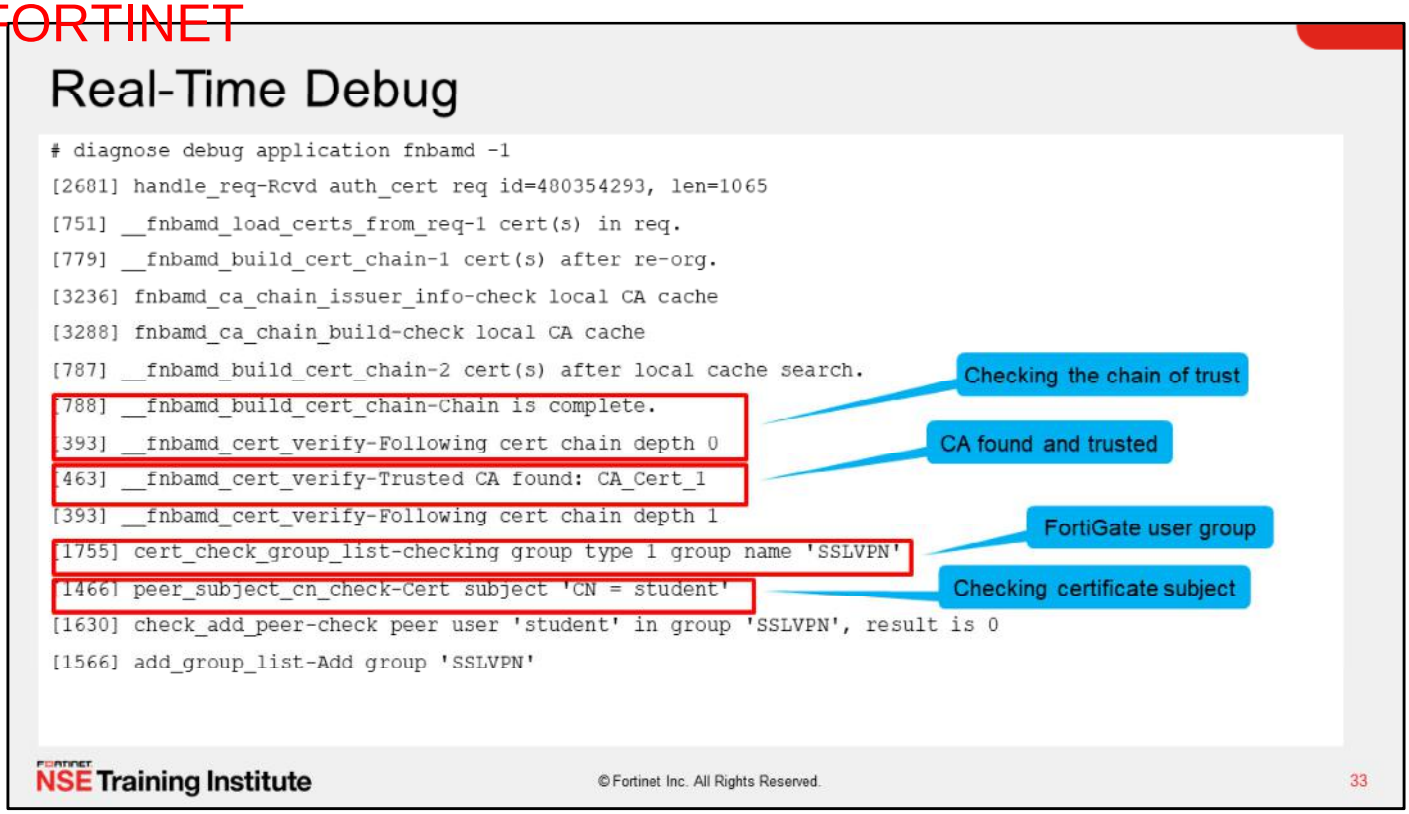
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn how to troubleshoot certificate-based authentication problems.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

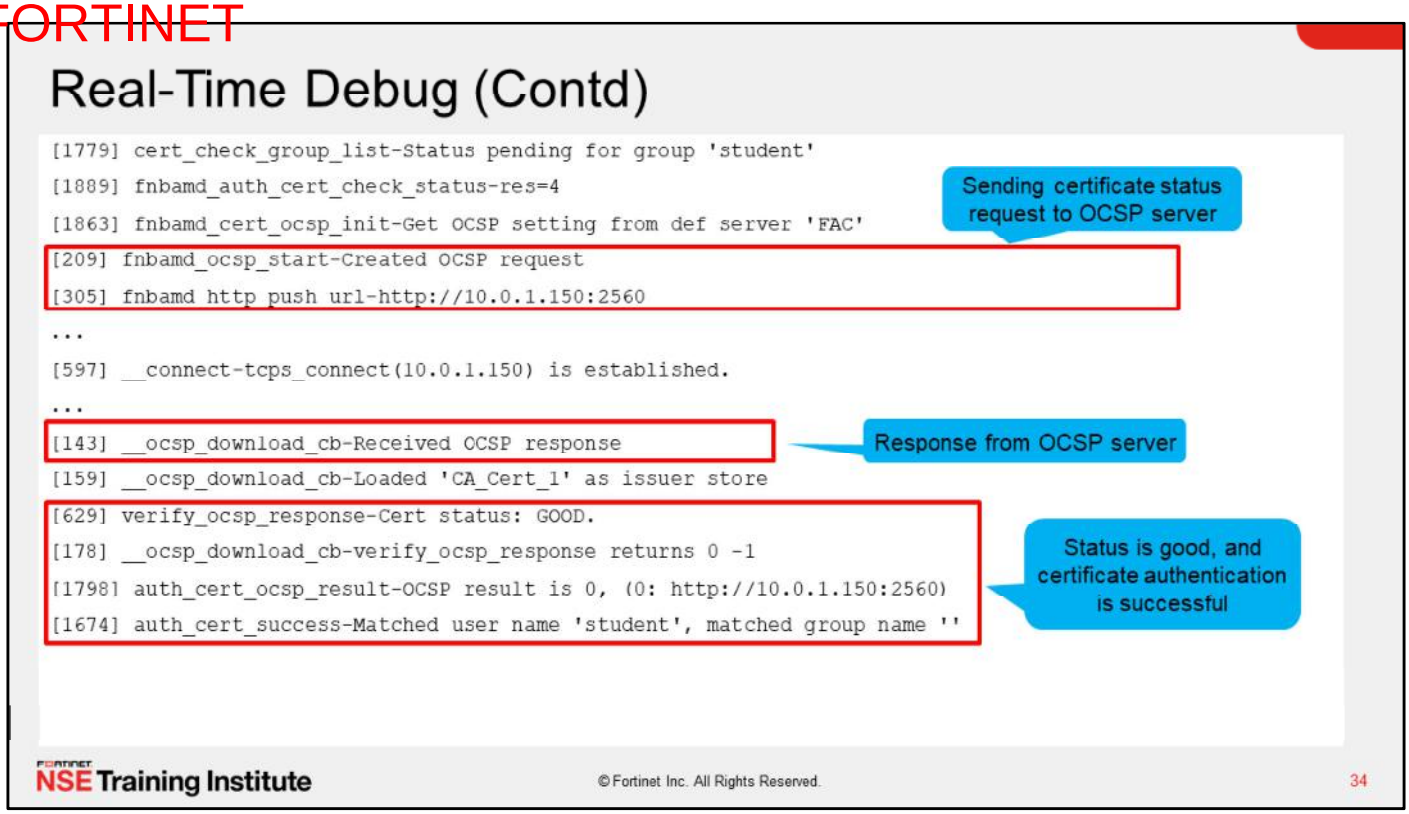


The Fortinet non-blocking authentication daemon (`fnbamd`) is the process that validates user certificates. The output of its real-time debug shows, step-by-step, what the non-blocking authentication daemon does when a user certificate is received and must be validated.

In the output shown on this slide, FortiGate checks the chain of trust first, until it finds that the certificate is signed by a trusted CA. Then, FortiGate finds the user group that the PKI user belongs to and checks the certificate subject.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In the example shown on this slide, FortiGate is configured to validate the certificate revocation status using OCSP. The output of the real-time debug shows the OCSP URL and a log entry indicating that the OCSP request has been sent.

Then, the output shows the response from the OCSP server, which, in this case, indicates that the certificate is good. It has not been revoked yet.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Common Real-Time Debug Errors

```
"Subject issuer mismatch."
"Certificate signature is invalid."
"Certificate is not yet valid."
"Certificate has expired."
"Certificate chain length exceeds limit."
"Certificate group information is invalid."
"CRL signature failure."
"CRL has expired."
"Certificate is revoked by CRL."
"OCSP server connection error."
"Certificate has been revoked by OCSP."
```

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

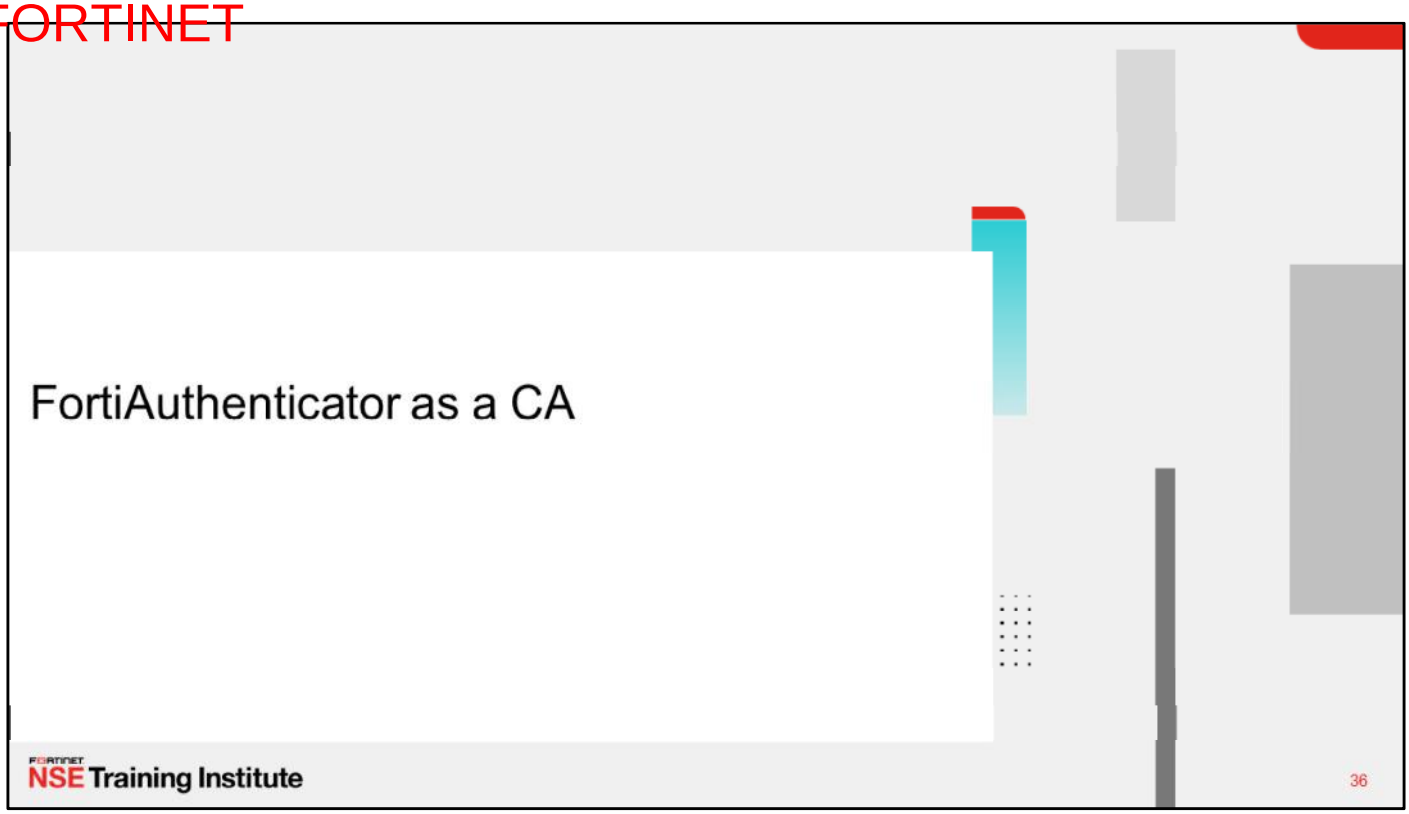
35

If a problem occurs during the validation of a user certificate, the output of the non-blocking authentication real-time debug displays an error explaining why the certificate validation failed. The possible reasons are listed on this slide. Some of them include:

- The subject does not match the subject in the PKI user configuration.
- The certificate is not valid yet or has expired.
- The CRL has expired.
- The certificate has been revoked.

Vouchers & Dumps are Available | WhatsApp +201224560923

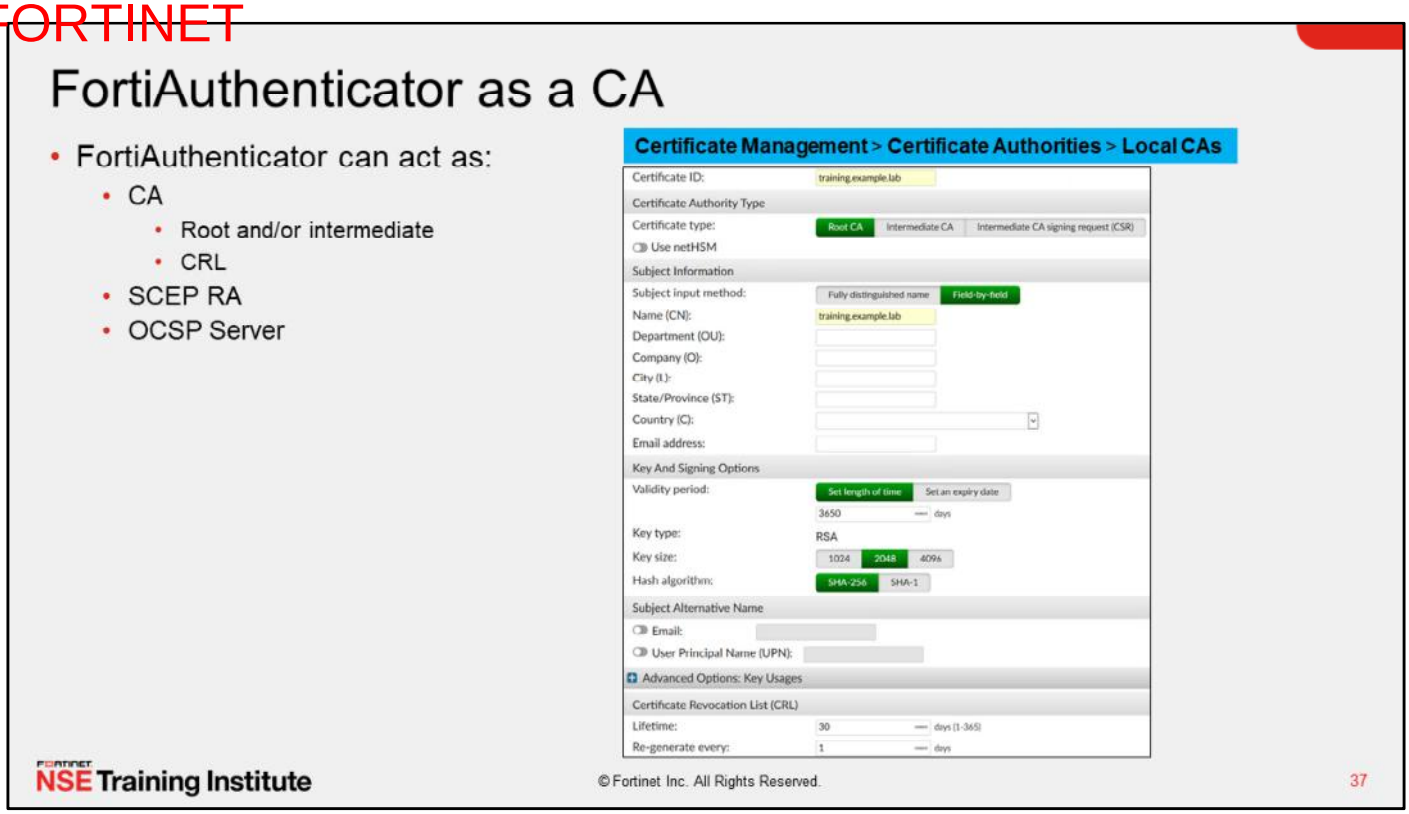
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will review how FortiAuthenticator can act as a CA.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



FortiAuthenticator can act as a self-signed or local CA for issuing and revoking digital certificates.

As a CA, the administrator can also import trusted CA certificates and certificate revocation lists.

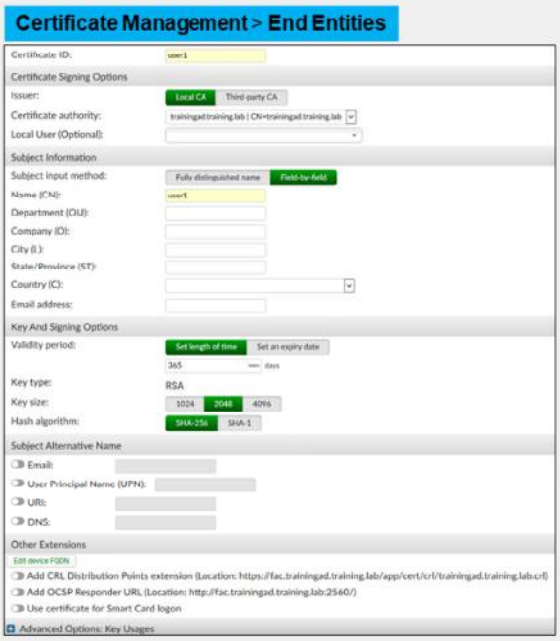
FortiAuthenticator can also act as an OCSP server (for certificate revocation checks) and a SCEP RA (for receiving CSRs and issuing certificates).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Generating Certificates

- FortiAuthenticator can generate the following types of certificates:
  - User certificates
    - Clients/end users
    - Used to identify users, services, and devices
    - Allows download of private key (one time only)
  - Local service certificates
    - Server certificate
    - Used to identify servers
    - Applies to local services enabled on the FortiAuthenticator only
    - Cannot retrieve the private key



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

38

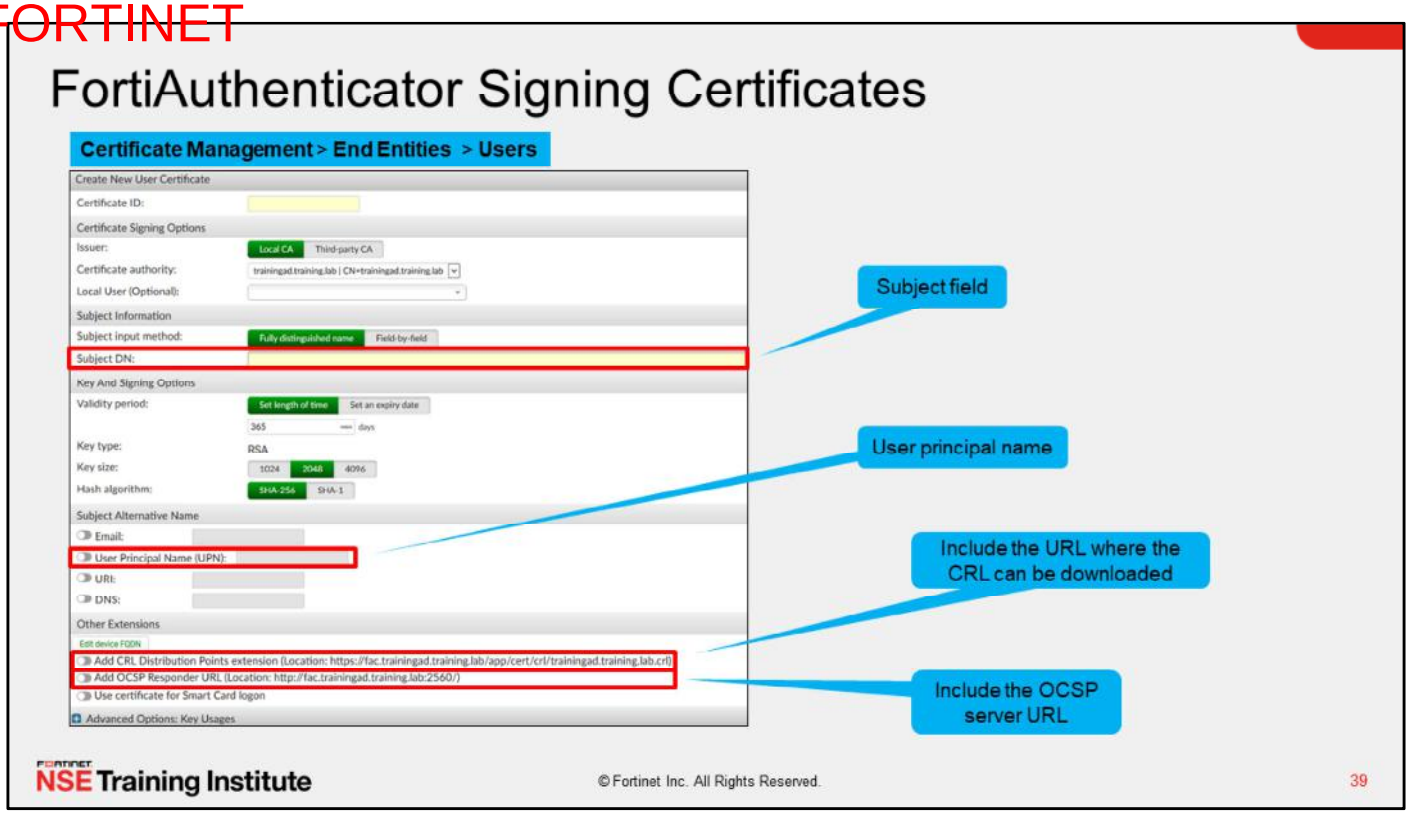
User and server certificates are required for mutual authentication on many HTTPS, SSL, and IPsec VPN network resources.

You can create a user certificate on FortiAuthenticator, or import and sign a CSR. User certificates, external service certificates, and device certificates are all the same type of certificate.

Note that **End Entities** certificates can be used only to verify client identity and cannot be used to sign other certificates.

Vouchers & Dumps are Available | WhatsApp +201224560923

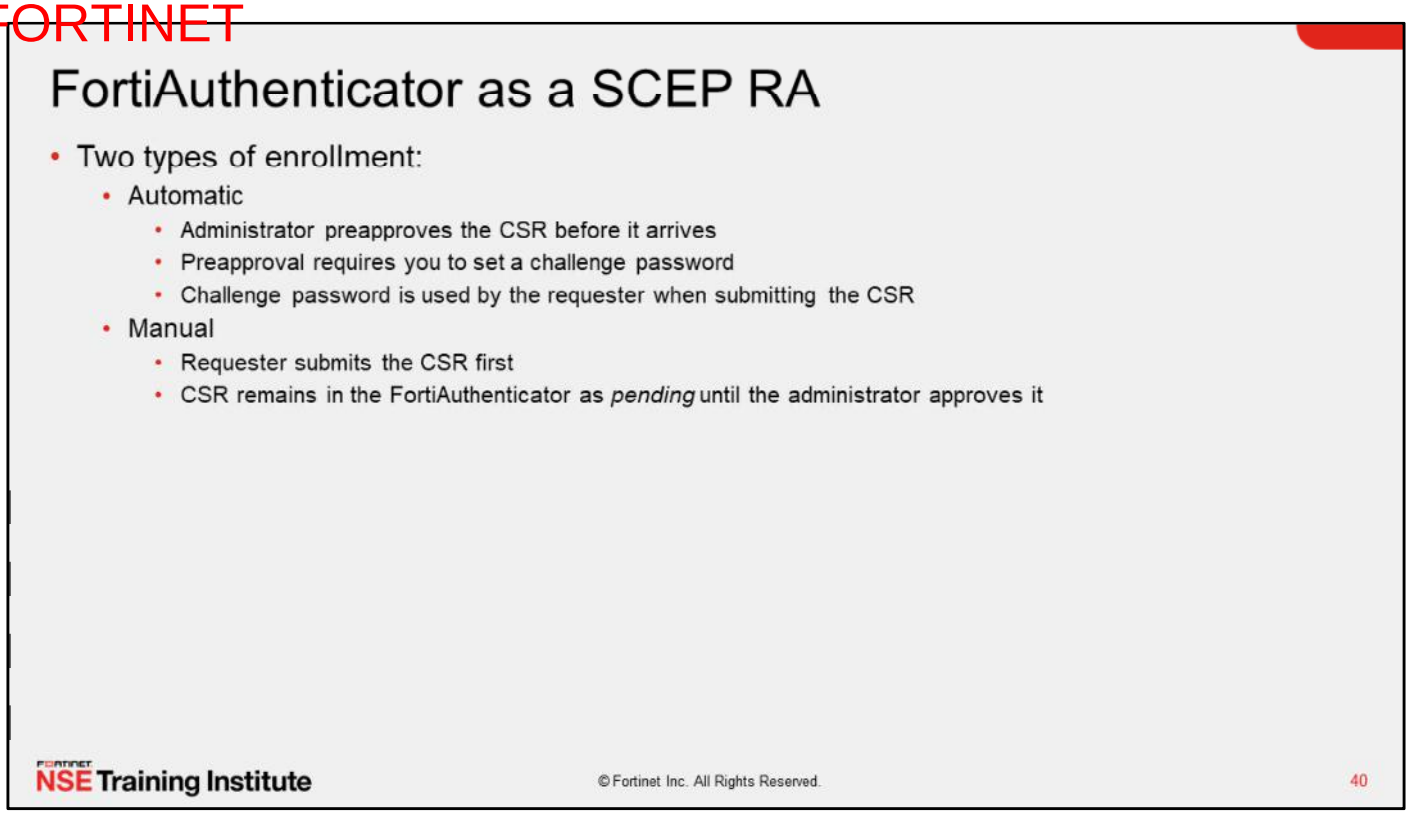
DO NOT REPRINT
© FORTINET
Brave-dumps.com



After you create a CA certificate, FortiAuthenticator can start issuing certificates to users. In each user certificate, you can define the subject field, expiration date, UPN, URL where the CRL can be downloaded, and the OCSP URL.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

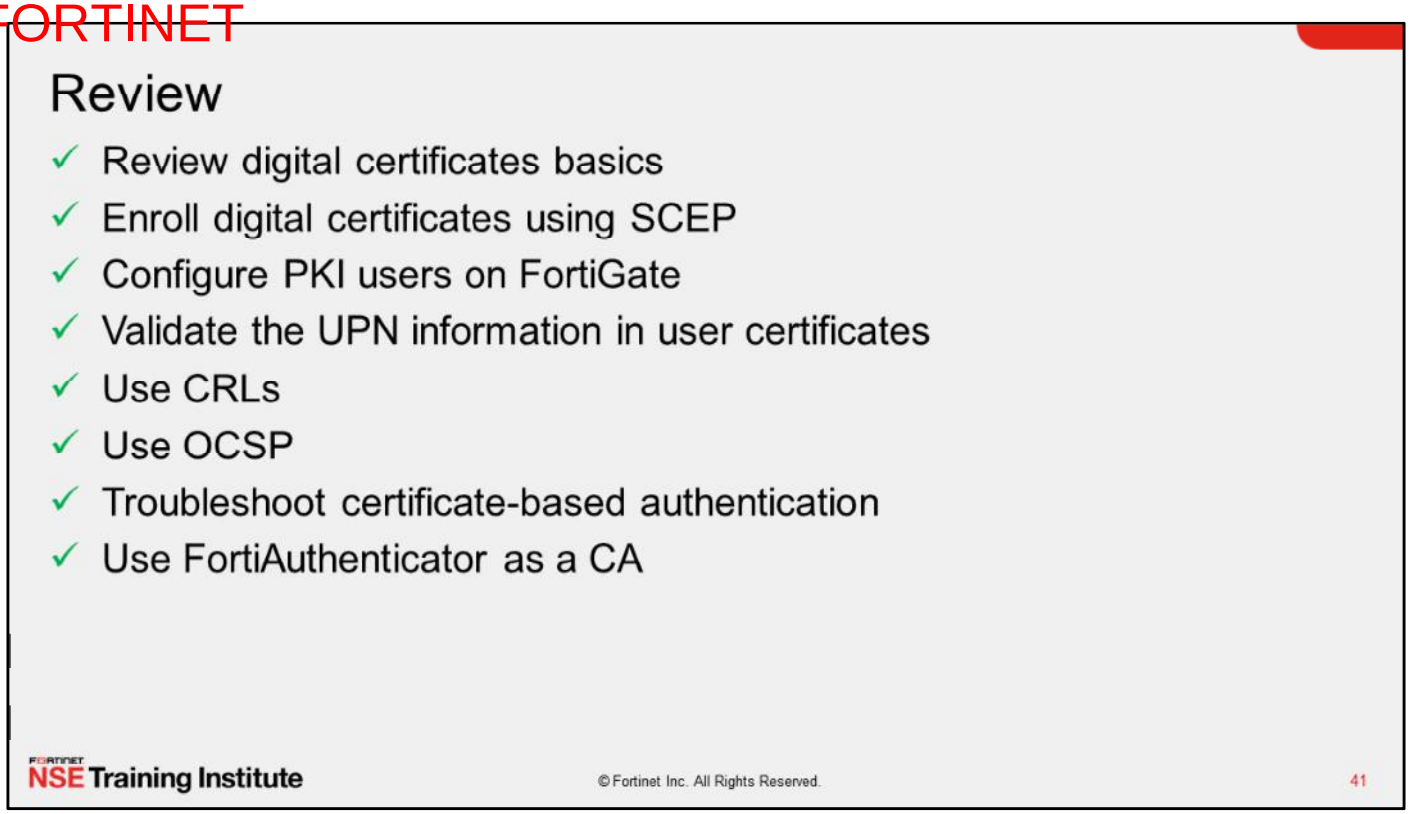


FortiAuthenticator supports SCEP. When acting as a SCEP server, FortiAuthenticator can receive CSRs coming from any device in your network. There are two types of SCEP enrollments:

- **Automatic**: Administrators preapprove the CSR before it arrives. After it arrives, FortiAuthenticator replies with the signed certificate.
- **Manual**: The requesters submit the CSRs first. The CSRs remain on FortiAuthenticator as *pending* until the administrator approves them.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

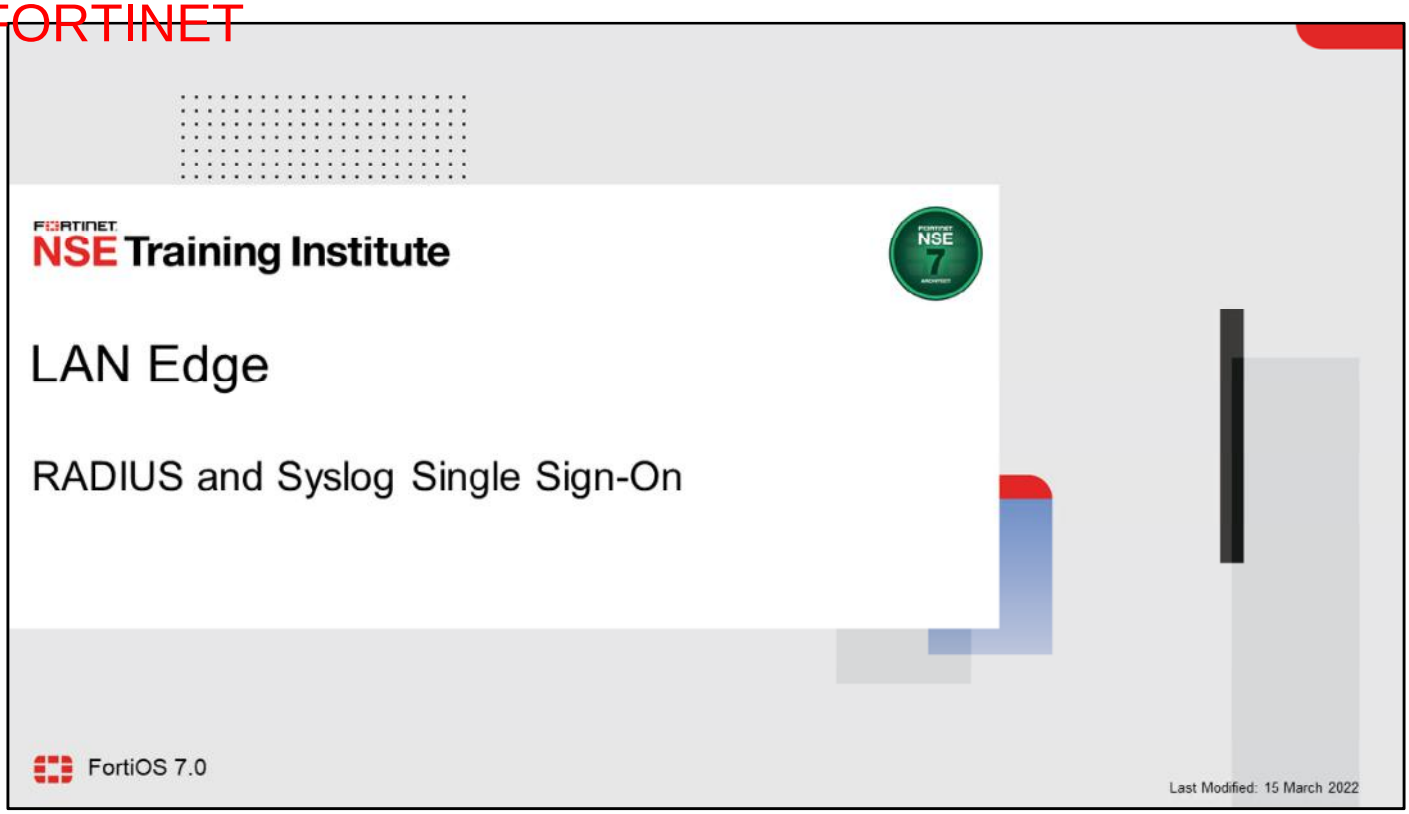


This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to configure and troubleshoot certificate-based authentication.

Vouchers & Dumps are Available | WhatsApp +201224560923

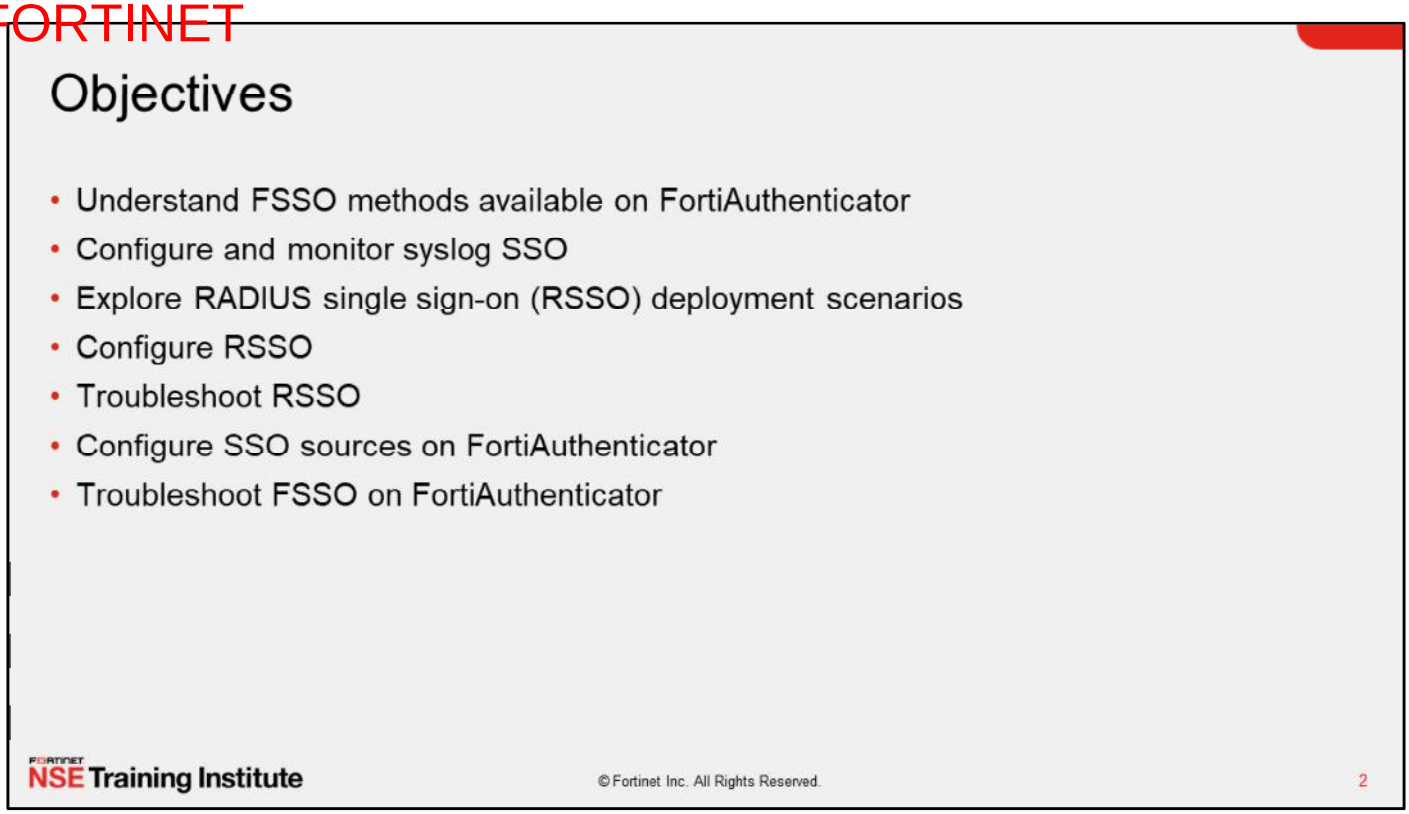
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about different ways to collect logon events and convert them to Fortinet single sign-on (FSSO) events. You will focus on RADIUS and syslog single sign-on and their relevant configurations.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this lesson, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in RADIUS and syslog SSO, you will be able to configure and use different SSO methods on FortiAuthenticator.

Vouchers & Dumps are Available | WhatsApp +201224560923

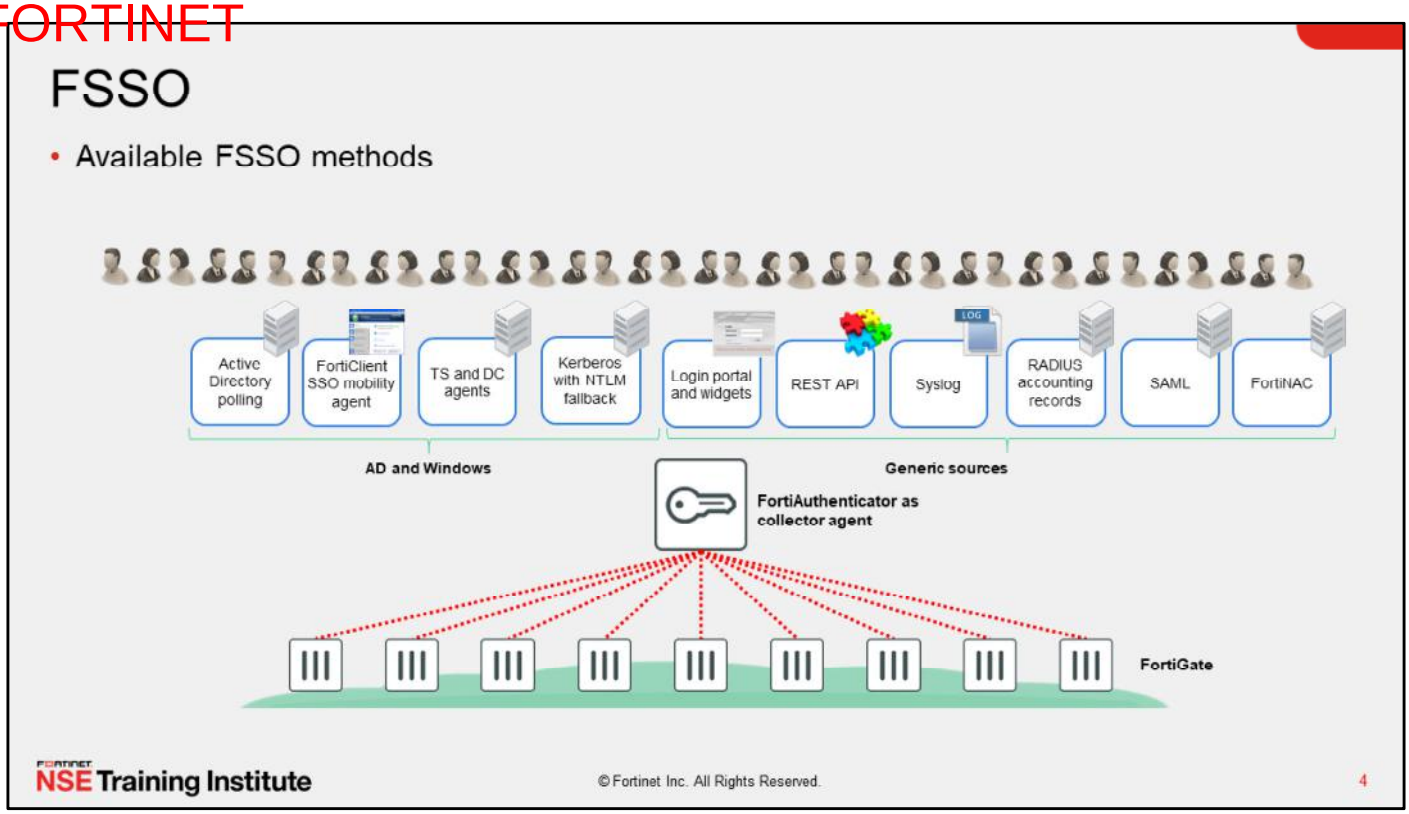
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn about FSSO collection methods.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

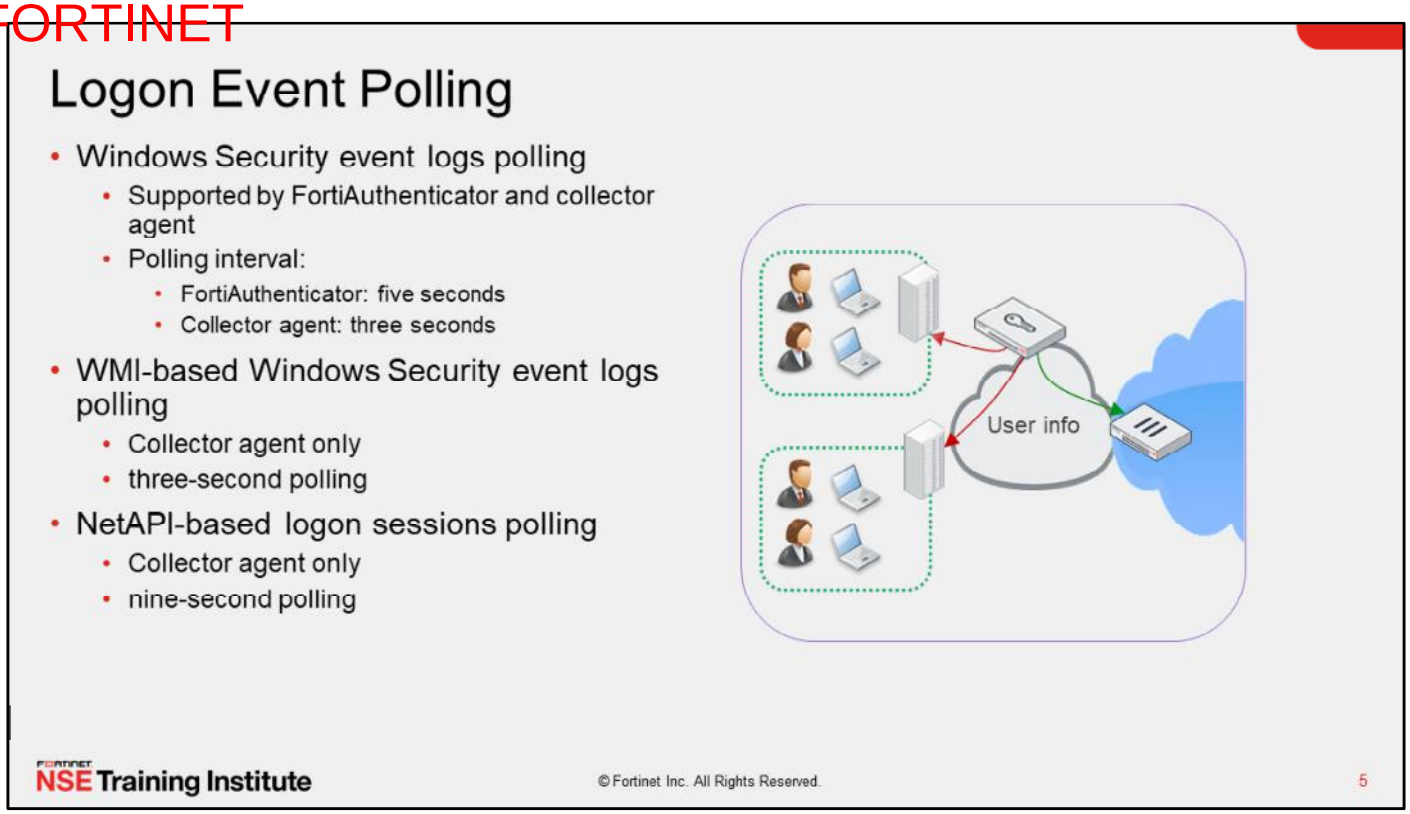


This slide shows the methods you can use to collect sign-on (or logon) information from, and convert it to, FSSO. You can divide sign-on methods into two groups: Active Directory (AD) and Windows, and generic sources. Sign-on information is sent to FortiAuthenticator, which acts as a collector agent to FortiGate. FortiAuthenticator then maintains a record of all the sign-ons learned from different methods and forwards them to FortiGate as FSSO. FortiGate can then use this information to provide accessibility to resources based on FSSO information.

Fortinet also provides a standalone collector agent (or FSSO agent) that can be installed on a Windows host to collect sign-on information through different methods. Unless otherwise stated, all references to the collector agent on this lesson refer to the standalone collector agent.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can poll the logon events from the domain controller (DC) using three methods:

- Windows security event polling: Uses server message block (SMB) to get the event logs from the DC. It is supported by both FortiAuthenticator and the collector agent. FortiAuthenticator polls the DC every five seconds, and the collector agent every three seconds. Polling may run a bit slower but will not miss events. By default, FortiAuthenticator ignores logon events from usernames ending with a $ sign.

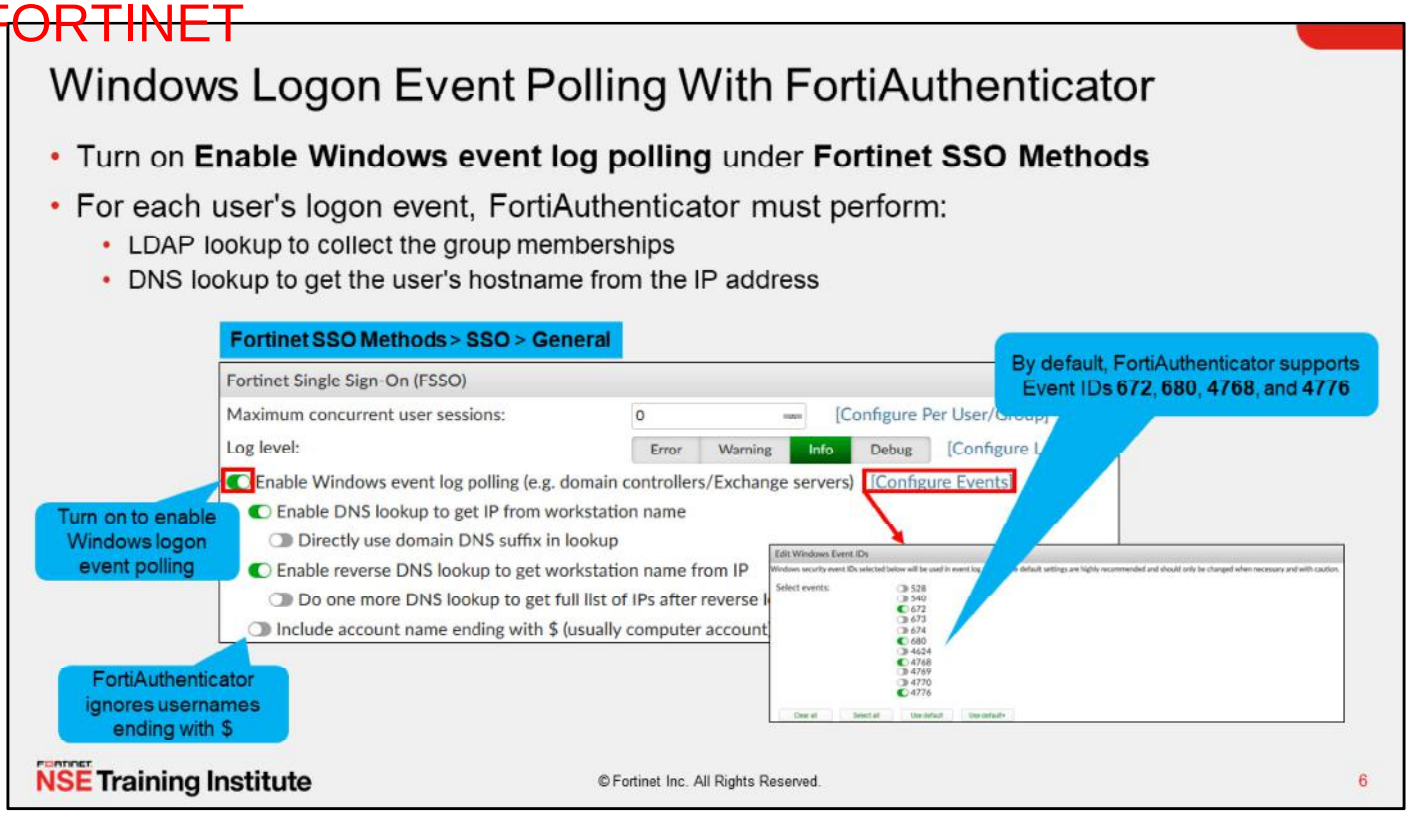
- WMI-based Windows Security event polling: Uses Windows Management Instrumentation (WMI) to extract the logon events. It is supported by the collector agent only, which polls the DC every three seconds. The main advantage of this method is that the collector agent does not need to search security event logs on the DC for user logon events. Instead, the DC returns all requested logon events through WMI.

- NetAPI-based logon sessions polling: Supported only by the collector agent. NetAPI, which is a Windows API that provides access to network services, is used to retrieve server logon sessions. NetAPI runs faster than security event log polling, but it may miss user logon events under heavy system load. Polling takes place every 9 seconds, and it requires a query round-trip time of less than 10 seconds.

Note that while logon events can be detected from the security event logs and login sessions, you can't detect logout events. This is because logout events can be triggered in different ways, not just the logout action. While some methods natively support logout detection (like the FortiClient SSO Mobility Agent), others, such as DC polling, do not. To enable logout detection, both FortiAuthenticator and the collector agent support WMI-based workstation IP address verification (or workstation check) to check the current logged-in user state for a device. For this, FortiAuthenticator and the collector agent periodically connect to each workstation to get the user login state. If the user is no longer logged in to the workstation, FortiAuthenticator and the collector agent remove the user from the list of active FSSO users.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can enable Windows logon event polling on FortiAuthenticator by clicking **Fortinet SSO Methods** > **SSO** > **General**. FortiAuthenticator uses LDAP lookup to collect user group memberships, and DNS lookup to resolve the workstation IP address. DNS plays a big role in ensuring the overall reliability of FSSO events. If DNS resolution is slow or not working properly, FSSO event information is not accurate or even valid.

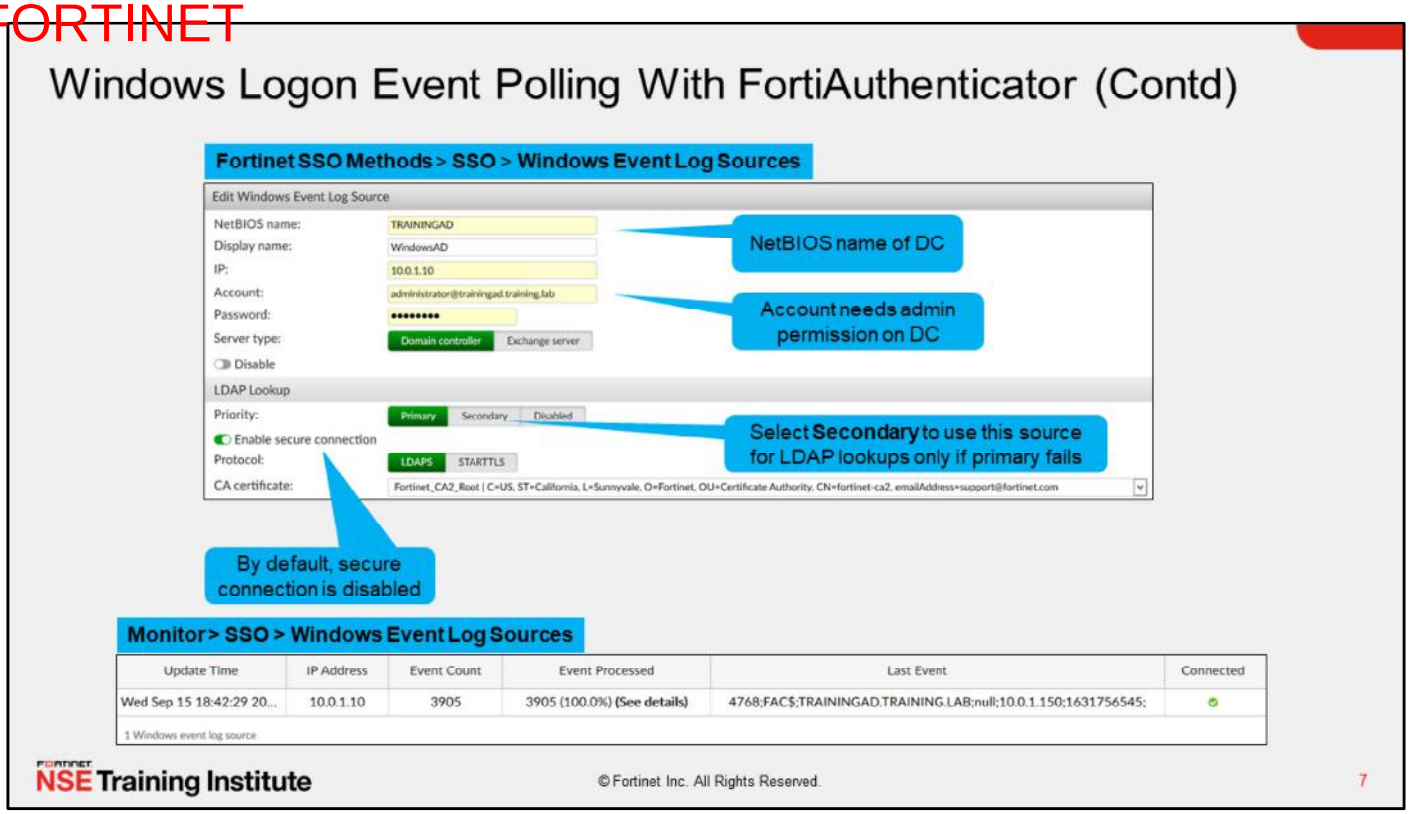
By default, FortiAuthenticator supports event IDs 672, 680, 4768, and 4776; however, you can also enable support for the following event IDs by clicking **Configure Events**:

528, 540, 673, 674, 4624, 4769, 4770

Note that FortiAuthenticator ignores usernames ending with a $ sign.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



After you enable Windows logon event polling, you must configure the logon event source in the **Windows Event Log Sources** section. When you configure a new source, you must type values in the **NetBIOS name**, **IP**, **Account**, and **Password** fields to use to poll events from that source. Use an account with administrator privileges in the DC so that logon events can be retrieved.

If you configure multiple sources for polling logon events from the same domain, for each source, you must select the LDAP lookup priority. If you select **Primary**, the source becomes the primary server for *LDAP lookups* for that domain. If you select **Secondary** instead, FortiAuthenticator uses that source to perform LDAP lookups only when the primary LDAP source fails.

For enhanced security, you can turn on **Enable secure connection**, and then select **LDAPS** or **STARTTLS**, so FortiAuthenticator securely connects to the LDAP server.

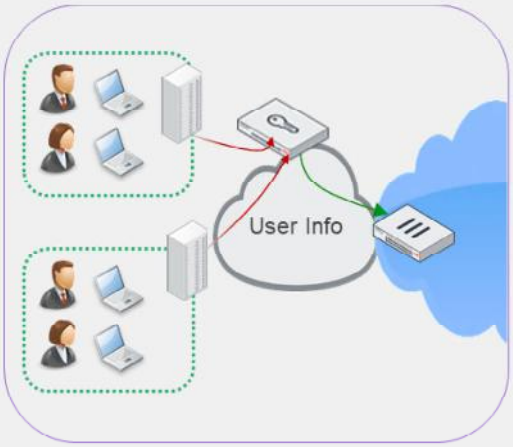
After you configure a Windows event log source, you can check the **Windows Event Log Sources** monitor section to verify that FortiAuthenticator can poll logon events from that source.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

DC and TS Agent

- DC agent
  - DC agent is installed on all DCs
  - Monitors user logins in real time
  - Logon events pushed to FortiAuthenticator in real time
- TS agent
  - Installed on Citrix terminal servers
  - Monitors user logins (TS users) in real time
  - Similar to DC agent



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

8

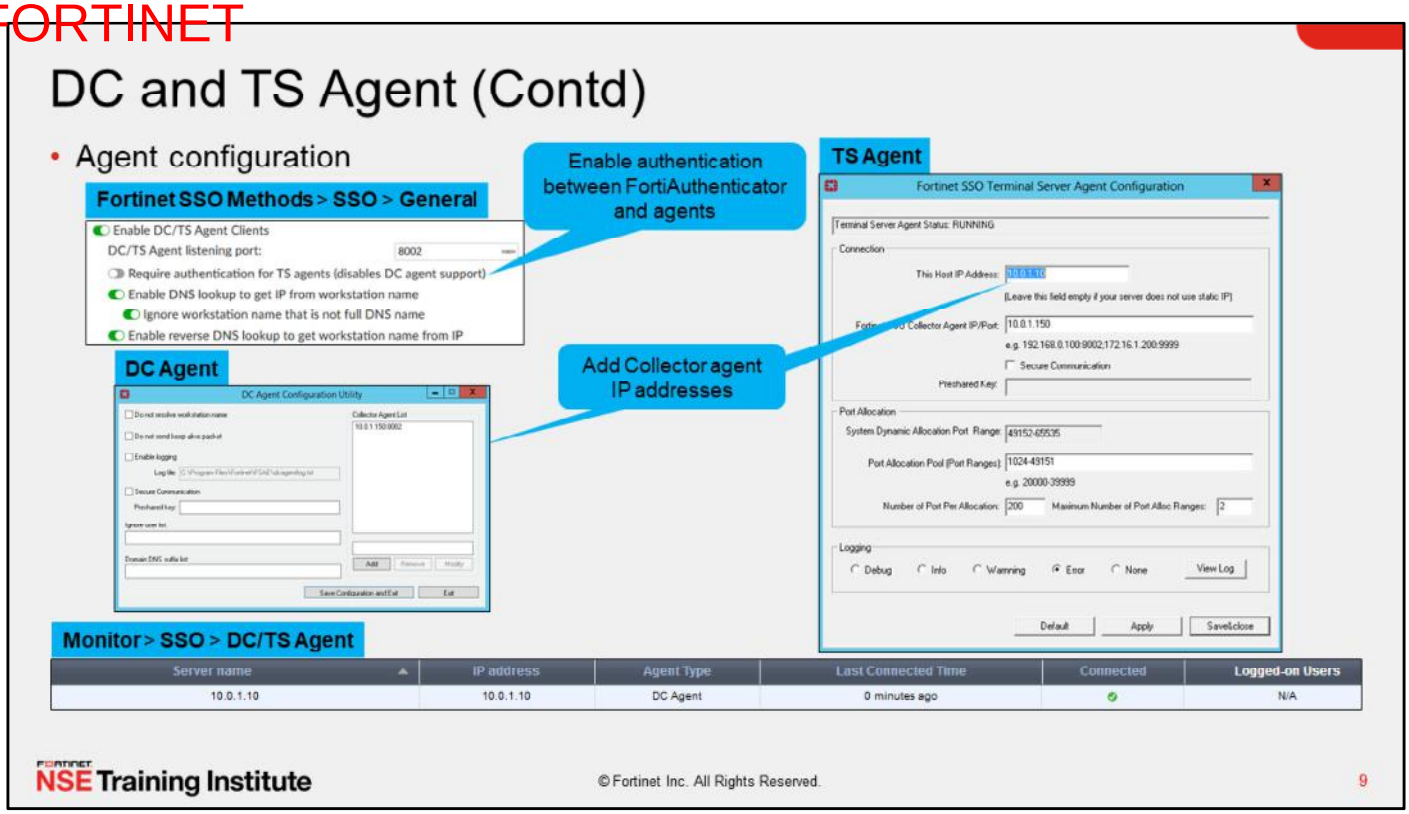
Instead of polling the login information from the DCs, you can deploy DC and TS agents that send real-time logon events to your FortiAuthenticator device. You can download DC and TS agent installers from the Fortinet support site.

You must install a DC agent on each DC and then restart the DC after you install the agent. The DC agents monitor user logon events and pass the information to FortiAuthenticator (which acts as a collector agent), which stores the information and sends it to FortiGate. The DC agent is not a service like the collector agent—it is a DLL file called `dcagent.dll` that is installed in the Windows\system32 directory.

The Citrix/Terminal Server (TS) agent is installed on a Citrix terminal server (which runs on Windows) to monitor user logins in real time. It functions much like the DC agent on a Windows DC, in that it sends real-time login information to the collector agent. However, unlike the DC agent, which sends logon events generated by users that log in to the domain from their workstations (unique IP address), the TS agent sends login information generated by users that log in to a TS (shared IP address). Because TS users share the same IP address, each of them is assigned a unique port range to access the domain network resources. To distinguish between TS users and, therefore, for FortiGate to be able to track the different TS users, the TS agent also includes the port range assigned to each user in the login information sent to the collector agent.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



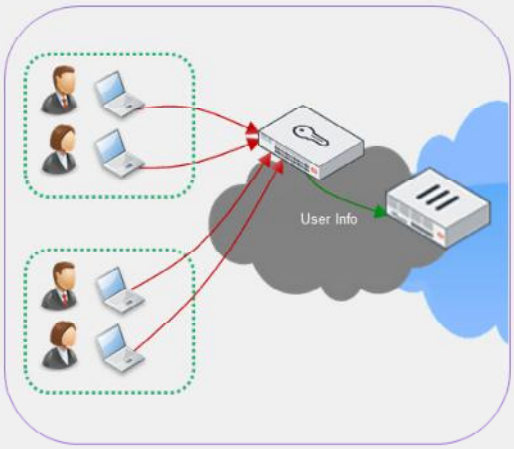
You must enable the DC/TS agent in FSSO methods on FortiAuthenticator to allow communication between DC/TS agents and FortiAuthenticator. You can also enable optional authentication for added security. You must configure both the DC/TS agent and FortiAuthenticator with the same password.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Single Sign-On Mobility Agent (SSOMA)

- SSOMA:
  - FortiClient user identification
    - Detects login/logout/IP address change
    - Sends hello packets every five minutes to detect improper shutdown, hibernation, and so on
  - Standalone (background service installer option too)
  - Most scalable FSSO ID method
  - Supports multiple forests, domains, and cross-domain groups
  - *Most accurate method for detecting logouts*



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

10

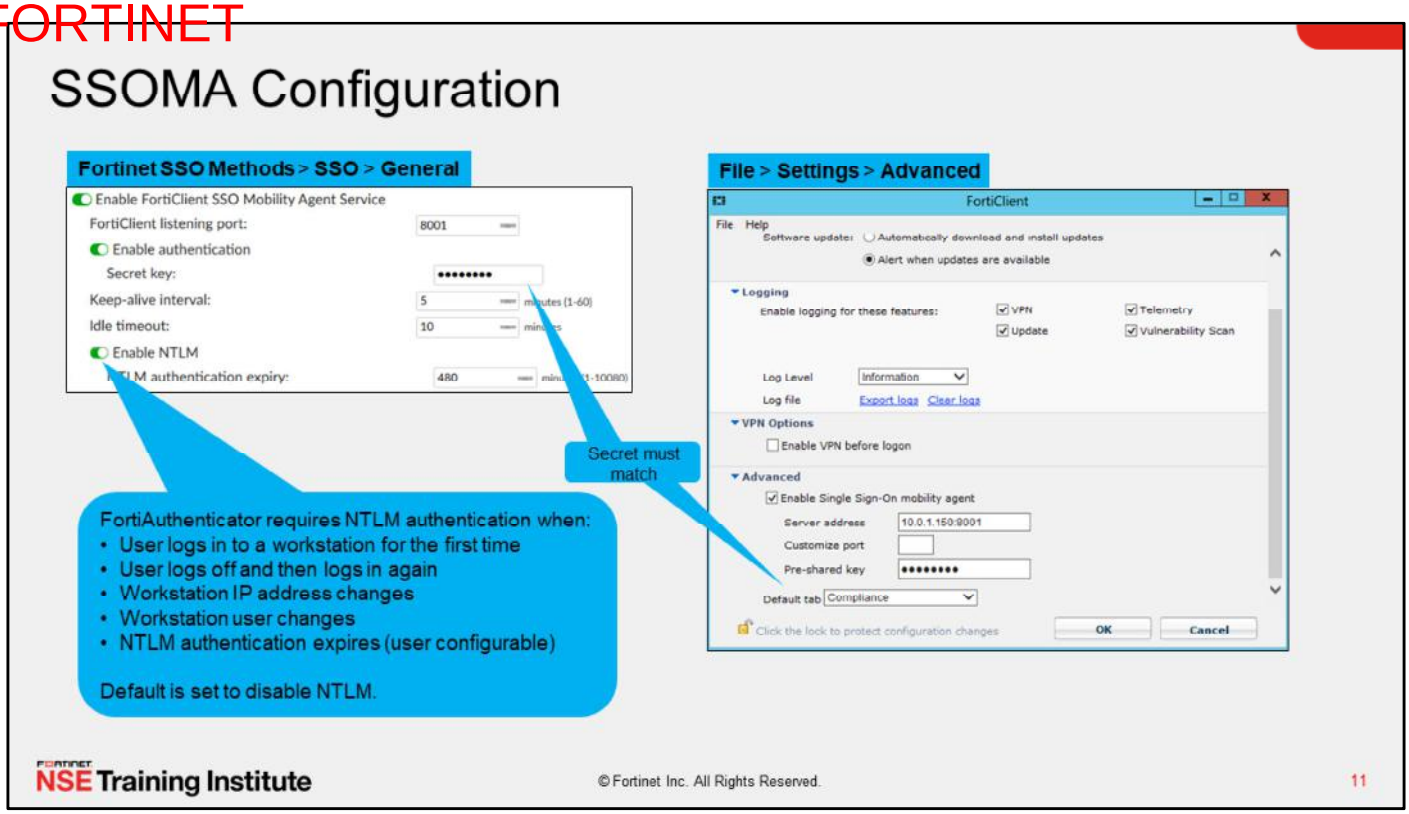
SSOMA is a FortiClient feature that can also be installed as a standalone feature. SSOMA identifies the logged in domain user and IP address, and communicates this information to FortiAuthenticator.

FortiClient SSOMA has several benefits over other FSSO detection methods:

- FortiClient sends regular HELLO packets. If FortiAuthenticator detects X number of missing HELLO packets, the user is deauthenticated.
- If the device IP address stack changes, for example, roaming on the wireless network, the update is sent to FortiAuthenticator.
- If the user logs out, FortiClient notifies FortiAuthenticator during the logout process and deauthenticates the user.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Like other SSO methods, you must enable SSOMA in the FSSO methods settings on FortiAuthenticator. By default, SSOMA will connect to FortiAuthenticator on port 8001, but that can be changed to another port if required. You can also enable optional authentication with secret keys, as well as configure keepalive and idle timeout intervals.

Optionally, you can enable NTLM within SSOMA settings so that NTLM works in conjunction with FSSO. When enabled, FortiAuthenticator requires NTLM authentication when:

- A user logs in to a workstation for the first time
- A user logs out and then logs in again
- The workstation IP address changes
- The workstation user changes
- NTLM authentication expires (user configurable)

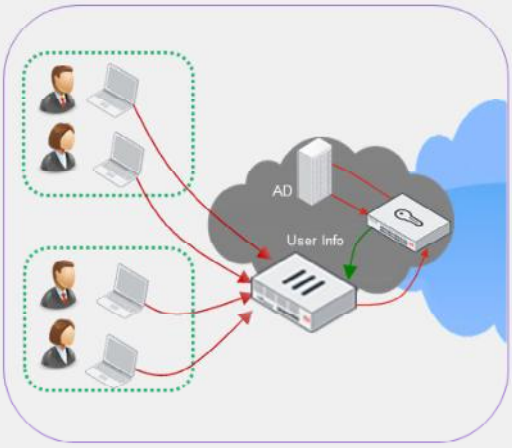
By default, NTLM is disabled.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Kerberos SSO

- Redirect unauthenticated users from FortiGate to FortiAuthenticator
  - FortiAuthenticator requests service ticket
  - Browser obtains ticket from ticket granting service and forwards to FortiAuthenticator
  - FortiAuthenticator decrypts and uses ticket to validate user identity



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

12

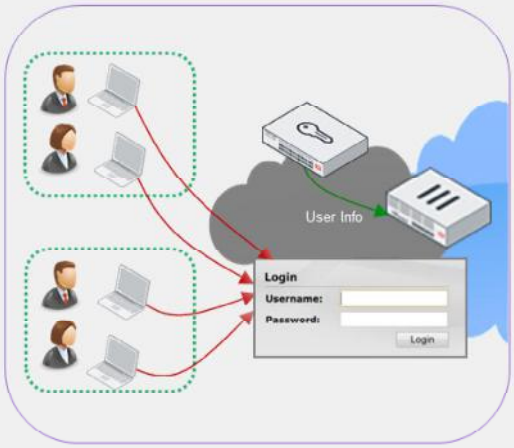
To avoid the need to poll the DC while retaining the ability to transparently authenticate Windows users, FortiAuthenticator supports the use of Kerberos tickets passed by the browser and validated against the Kerberos DC to identify users. In the example shown on this slide, unauthenticated users are redirected from FortiGate to FortiAuthenticator. FortiAuthenticator requests the service ticket from the browser, and then decrypts and uses the ticket to validate the user identity.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FSSO Method—Portal Authentication and Widgets

- Portal authentication and widgets
  - Login portal for manual authentication
    - Catches systems not supported by other methods
    - Widgets can be embedded into an organization's intranet homepage
    - User *token* stored in cookie to identify user on subsequent access (valid for up to 30 days)



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

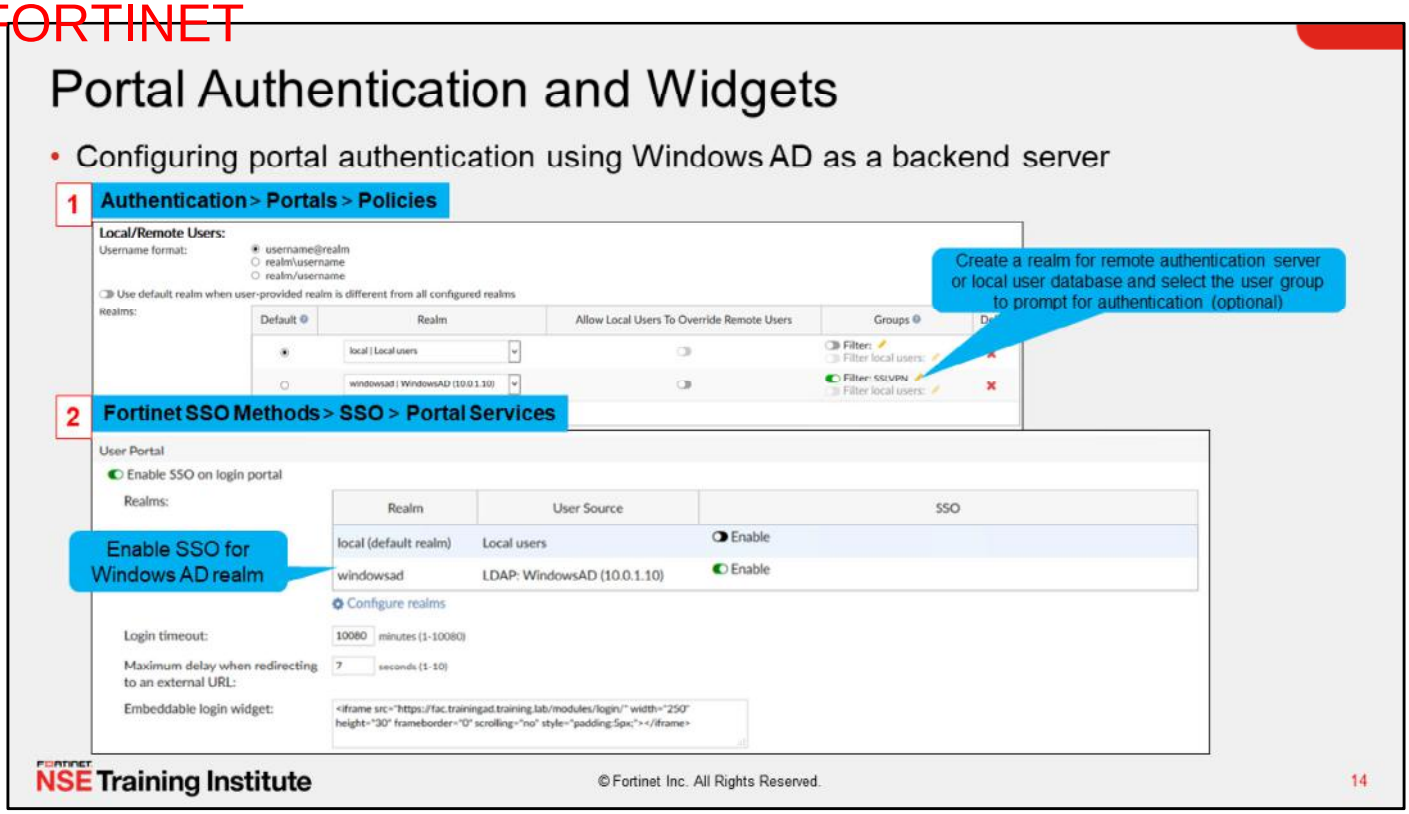
13

In situations where the device or user identity cannot be established transparently, such as for non-domain BYOD devices or shared kiosk machines, you can use a web portal to prompt users to log in. Often this method is used with other transparent method and is used as a *catch-all*.

Once authenticated, the user *token* is stored in a cookie to identify the user on subsequent access (valid for up to 30 days) or until they log out using the browser.

Vouchers & Dumps are Available | WhatsApp +201224560923

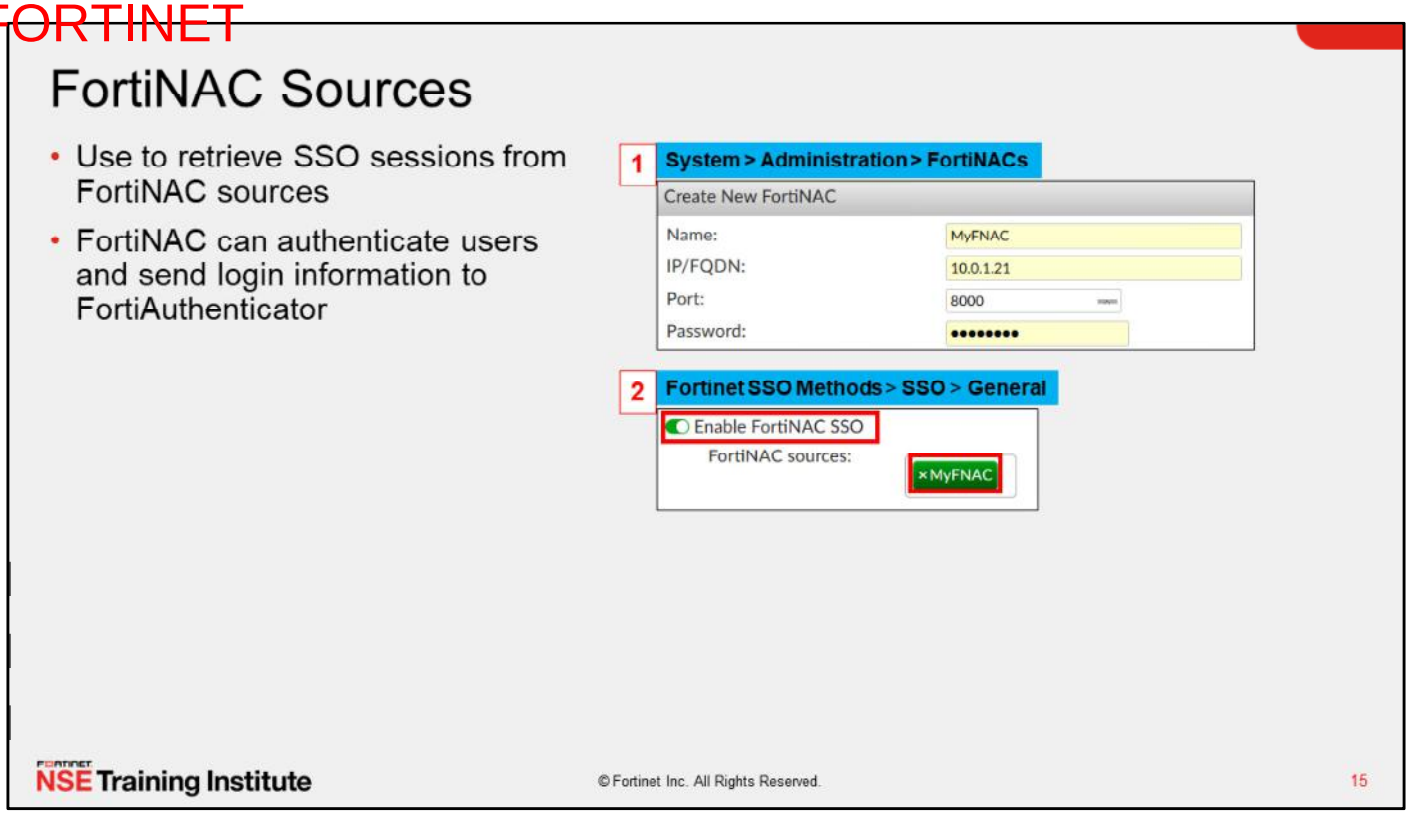
DO NOT REPRINT Brave-dumps.com
© FORTINET



Portal authentication and widgets require you to configure a portal policy and portal services on FortiAuthenticator. You must have a remote authentication server or local user database configured to validate authentication requests. You must also create a realm that SSO will use to authenticate users through portal authentication. Optionally, you can select specific user groups that you want to use for portal authentication. After you create and configure a realm, you must enable portal services in **Fortinet SSO Methods**, and select the realms to use.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



FortiNAC is a Fortinet network access control (NAC) solution that provides visibility of all devices and users connected to the network.

FortiNAC can authenticate network users, and their login information can be sent to FortiAuthenticator when you configure FortiNAC as an SSO source. The login information provided includes the username, group, and IP address.

To configure FortiAuthenticator to use FortiNAC as an SSO source:

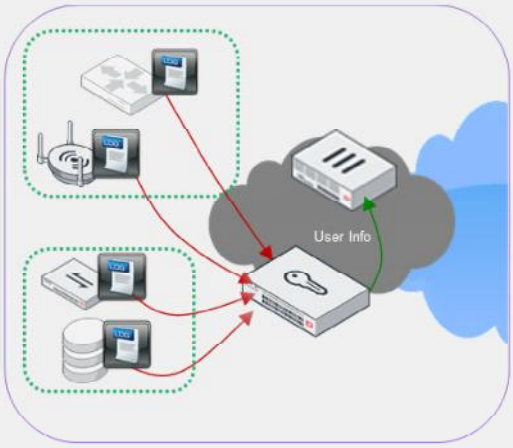
1. Create a FortiNAC source in **System** > **Administration** > **FortiNACs**.
2. Click **Fortinet SSO Methods** > **SSO** > **General**, select **Enable FortiNAC SSO**, and then select the FortiNAC source you just configured.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

External Syslog

- Syslog SSO
  - Receive external syslog feeds to learn user login information
    - Configurable logon, update, and logoff rules
    - Debug logs give full visibility into log and rule extraction
  - Extract user details from any third-party syslog feed



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

16

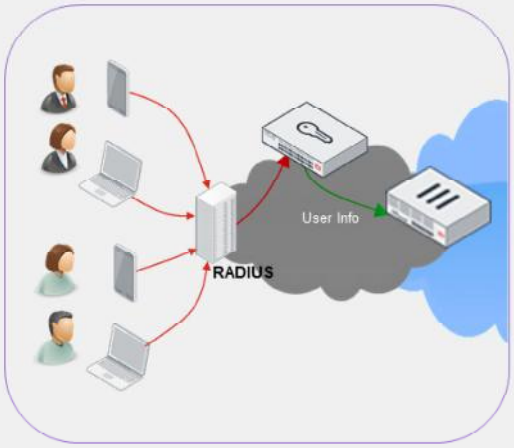
FortiAuthenticator can also parse username and IP address information from a syslog feed from a third-party device, and inject this information into FSSO so it can be used in FortiGate firewall policies. You can use the syslog feed to trigger logon, update, or logoff rules on FortiAuthenticator. You can use any syslog server to send the username and IP address information to FortiAuthenticator, as long as you have configured a corresponding matching rule.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

RADIUS Accounting Packets SSO

- RADIUS accounting
  - RADIUS accounting start, interim, and stop packets used as a source of user identification
  - Can come from any third-party source that is capable of sending RADIUS accounting packets
    - VPN gateways
    - Wireless controller/APs
    - Switches
- RSSO is used with third-party integration usually when FortiGate or FortiAuthenticator is not used for user/device authentication



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

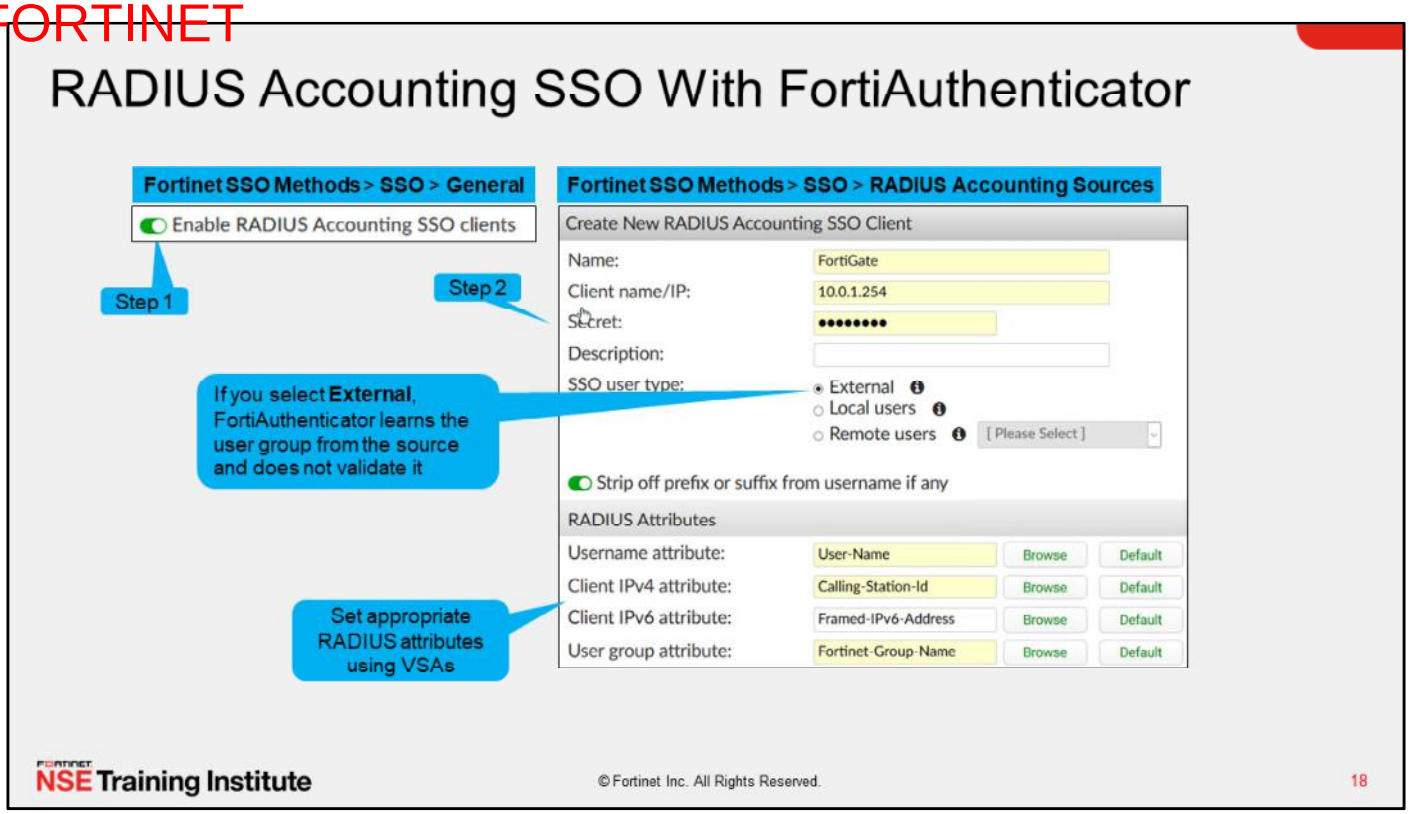
17

The RADIUS accounting method uses RADIUS start, interim, and stop accounting packets to trigger logon and logoff events to FSSO. Such RADIUS packets are commonly sent by networking devices, such as SSL VPN devices, wireless controllers, switches, and so on.

The benefit of using this method is that vendors who support sending such packets do not require any direct support from FortiAuthenticator (they use standard RADIUS which is already supported) and require minimal change to enable the input of user authentication data into FSSO.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



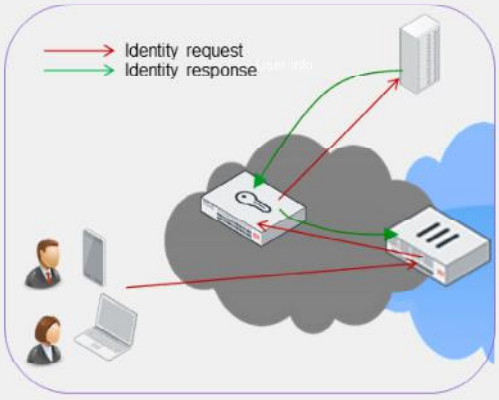
You must enable the RADIUS accounting SSO method in the FSSO methods section. You must also create a RADIUS accounting source that will be used to learn sign-on information using RADIUS accounting messages. FortiAuthenticator can look up group membership information for the user accounts that are learned through RADIUS accounting, as long as they reside on the remote authentication server or local database on the device. If you select **External** as **SSO user type**, FortiAuthenticator extracts only the information that is included in the accounting message, including the user group, and does not validate the group membership. If you select the **Local users** or **Remote users** as **SSO user type**, FortiAuthenticator retrieves the user group information from its local user database or the selected back-end server, respectively.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Security Assertion Markup Language (SAML)

- SAML
  - An XML standard for maintaining a single repository for authentication among internal and/or external systems
  - Requires a service provider (SP) and an identity provider (IDP)
  - IDP sends SAML assertions to the SP
  - SP relays the information provided by the IDP
- Authentication flow
  1. A user attempts to connect to the internet through FortiGate
  2. The user is not authenticated in FSSO, so is redirected to FortiAuthenticator
  3. FortiAuthenticator (a service provider) asks the user (principal) for SAML assertion
  4. FortiAuthenticator pushes identity and group information to FSSO
  5. FortiAuthenticator redirects the user to the original URL
  6. FortiGate locates the user in FSSO and allows the user to pass



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

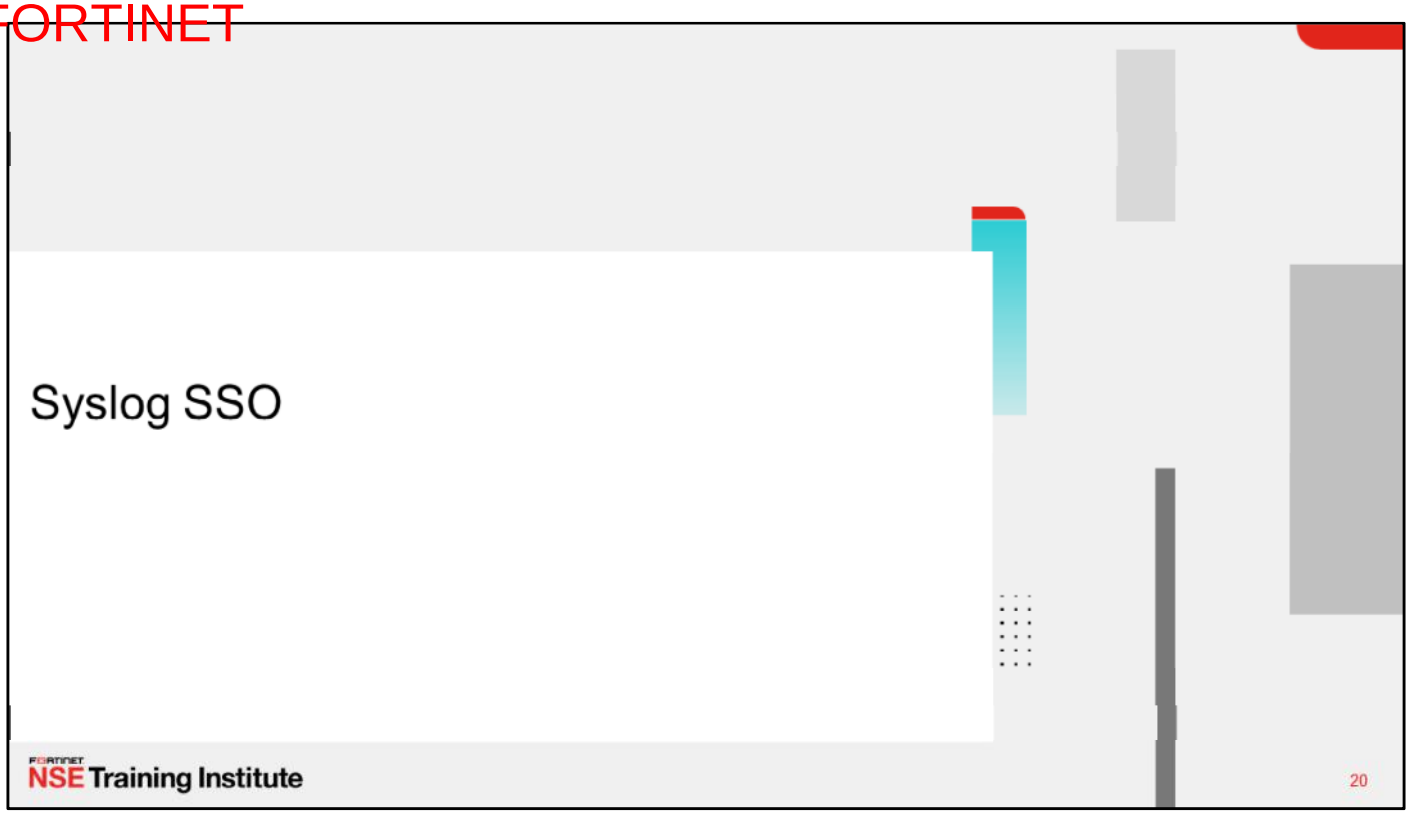
19

FortiAuthenticator can use SAML assertions to generate FSSO events when you use FortiAuthenticator as a SAML service provider. SAML assertions are messages that contain the user authorization information, and that are sent by the IDP to the SP.

In service provider mode, FortiAuthenticator can use SAML assertions to extract the username, IP address, and other available SAML attributes to generate FSSO events. These events are then used to allow users to access resources within and outside the network using FortiGate devices. All the authentication information is validated and inserted in the cookie by an IDP, and FortiAuthenticator then uses the information for FSSO events.

Vouchers & Dumps are Available | WhatsApp +201224560923

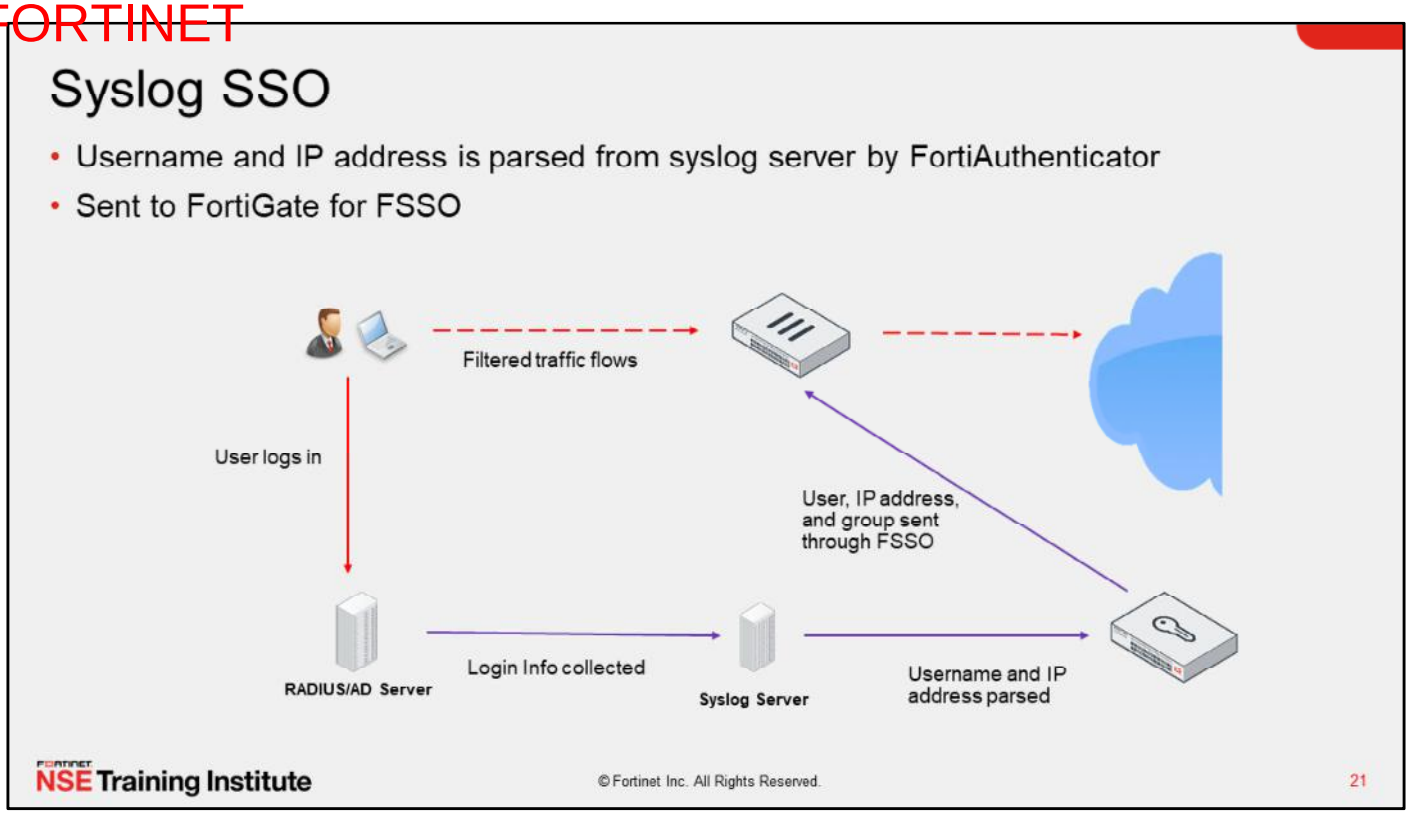
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn about syslog SSO using FortiAuthenticator.

Vouchers & Dumps are Available | WhatsApp +201224560923

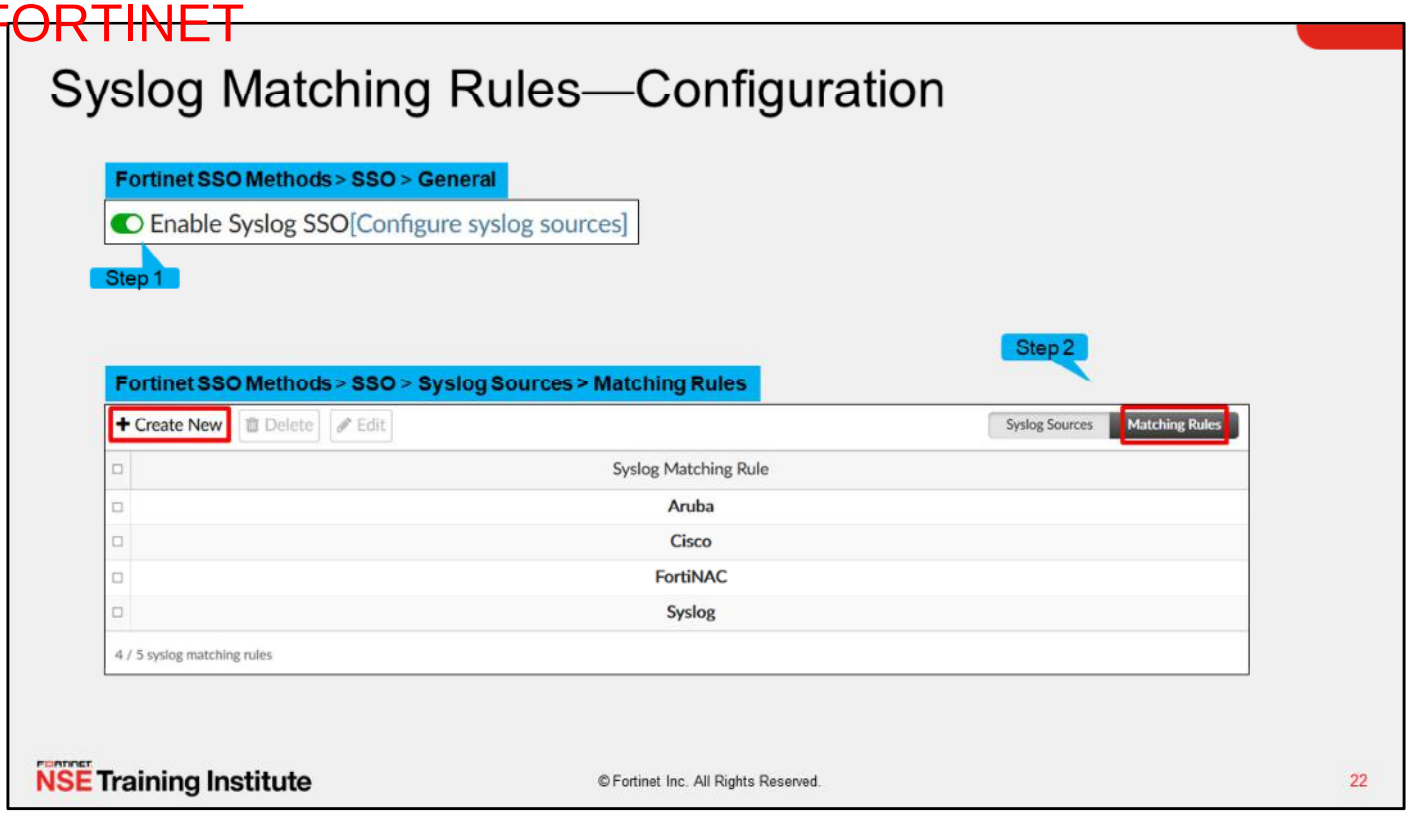
DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiAuthenticator can parse username and IP address information from a syslog feed from a third-party device, and inject this information into FSSO so it can be used in FortiGate authentication policies.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

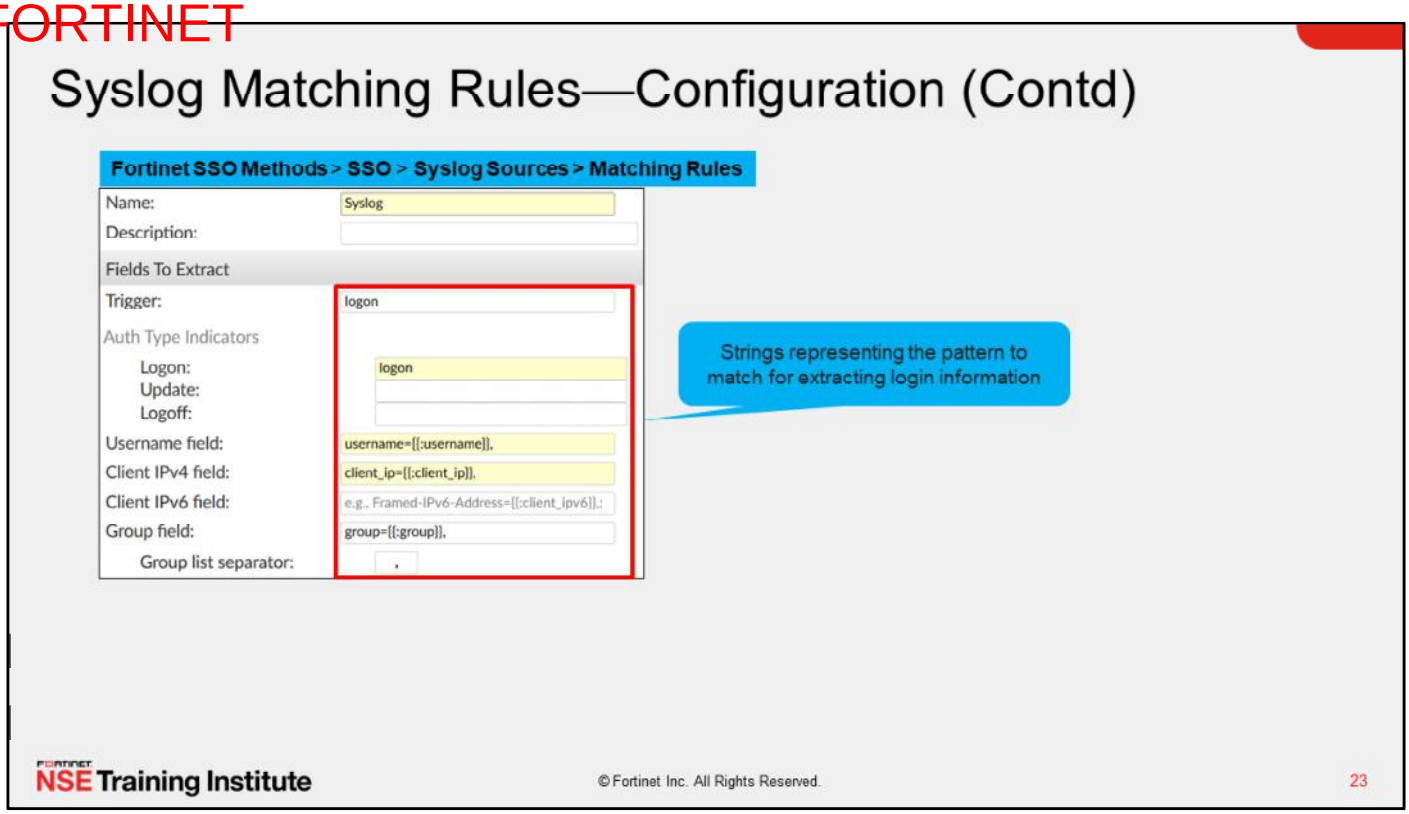


Syslog objects include sources and matching rules. Sources identify the entities sending the syslog messages, and matching rules are used to extract the events from the syslog messages. FortiAuthenticator ignores messages coming from nonconfigured sources.

After you enable the **Enable Syslog SSO** option, the next step is to create a matching rule to be used by your syslog source.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

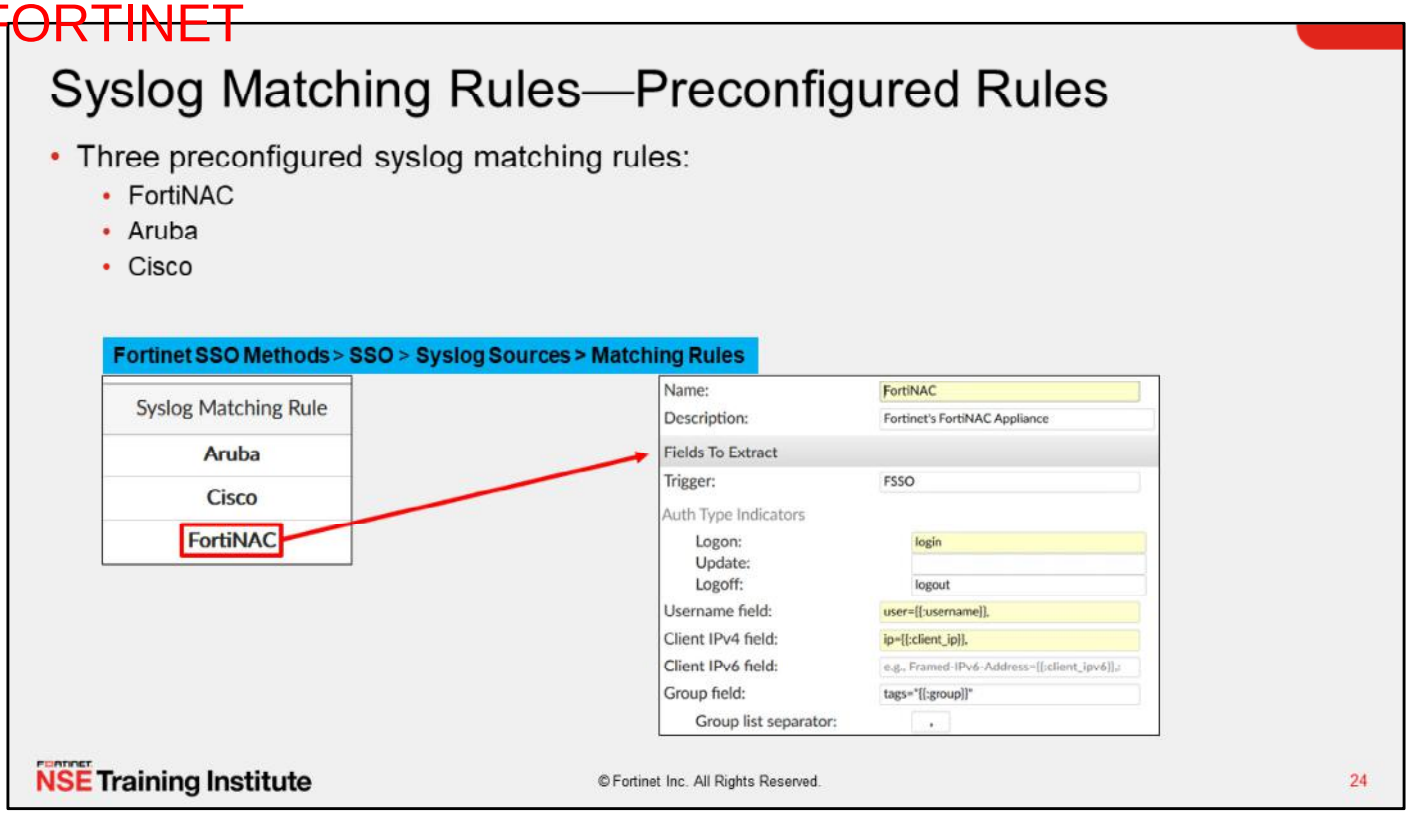


There are preconfigured matching rules for some third-party syslog server formats, but you can create custom matching rules to match the format of any syslog server feed.

In the **Fields To Extract** section, you can specify the string patterns that FortiAuthenticator uses to trigger logon, update, and logoff messages. FortiAuthenticator uses these fields to extract the username and IP address from the messages to convert them to FSSO events.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

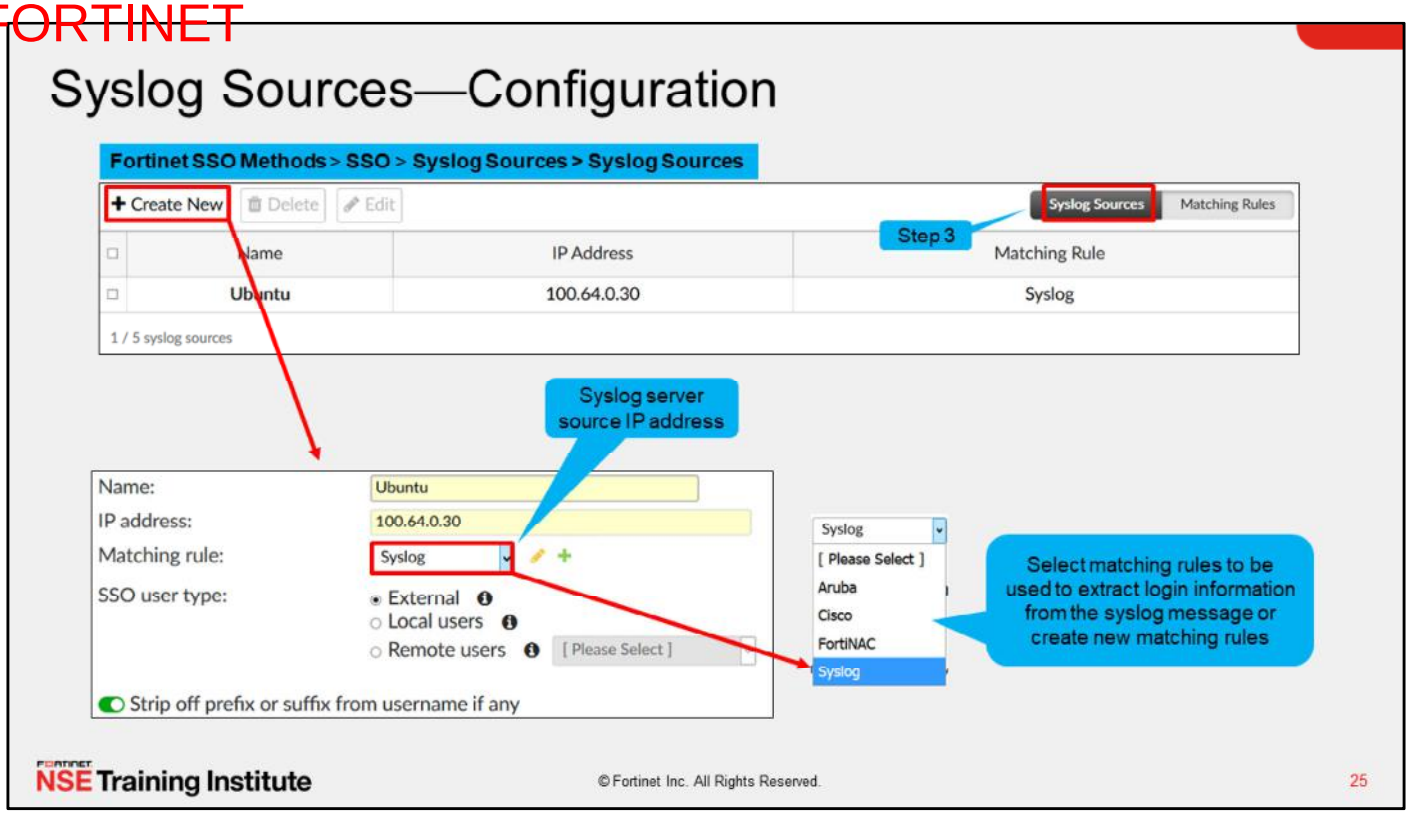


Three preconfigured matching rules for some third-party syslog server formats are:

- FortiNAC
- Aruba
- Cisco

Vouchers & Dumps are Available | WhatsApp +201224560923

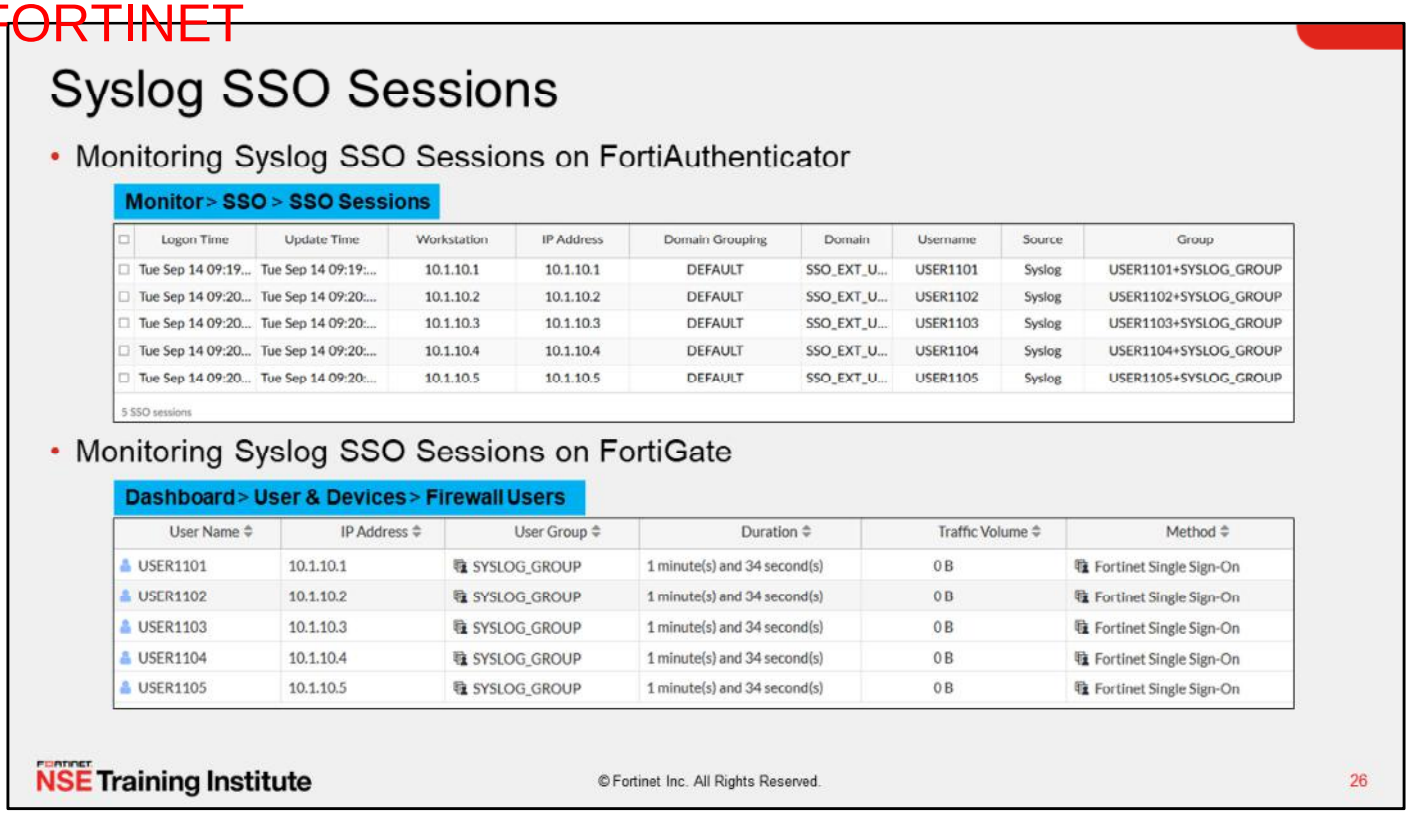
DO NOT REPRINT Brave-dumps.com
© FORTINET



The next step is to create a syslog source. You must type values in the **Name** and **IP address** fields, and then select a rule in the **Matching rule** drop-down list.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can view syslog SSO sessions on FortiAuthenticator by clicking **Monitor** > **SSO** > **SSO Sessions**.

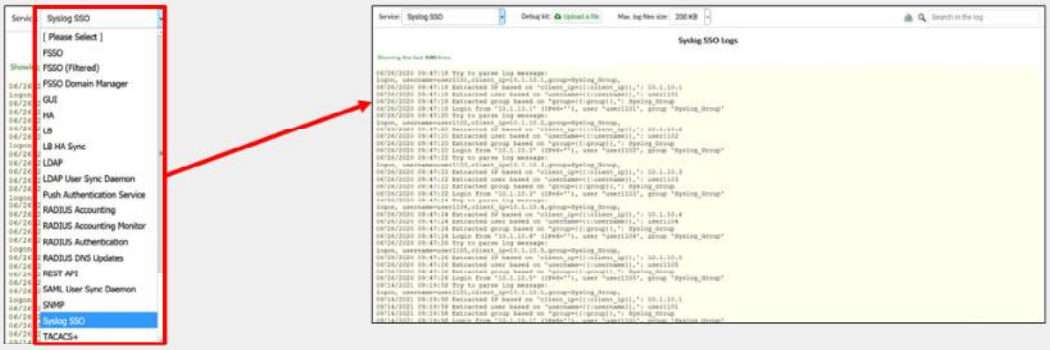
On FortiGate, you click **Dashboard** > **User & Devices** > **Firewall Users** to view the FSSO logs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Debug Logs

- Viewing debug logs from a specific service



- Debug logs can be helpful when troubleshooting SSO-related issues
  - Display information-level logs from the selected service
  - View service logs that are relevant to the FSSO method that is encountering issues
  - Most recent logs are at the bottom

NSE Training Institute

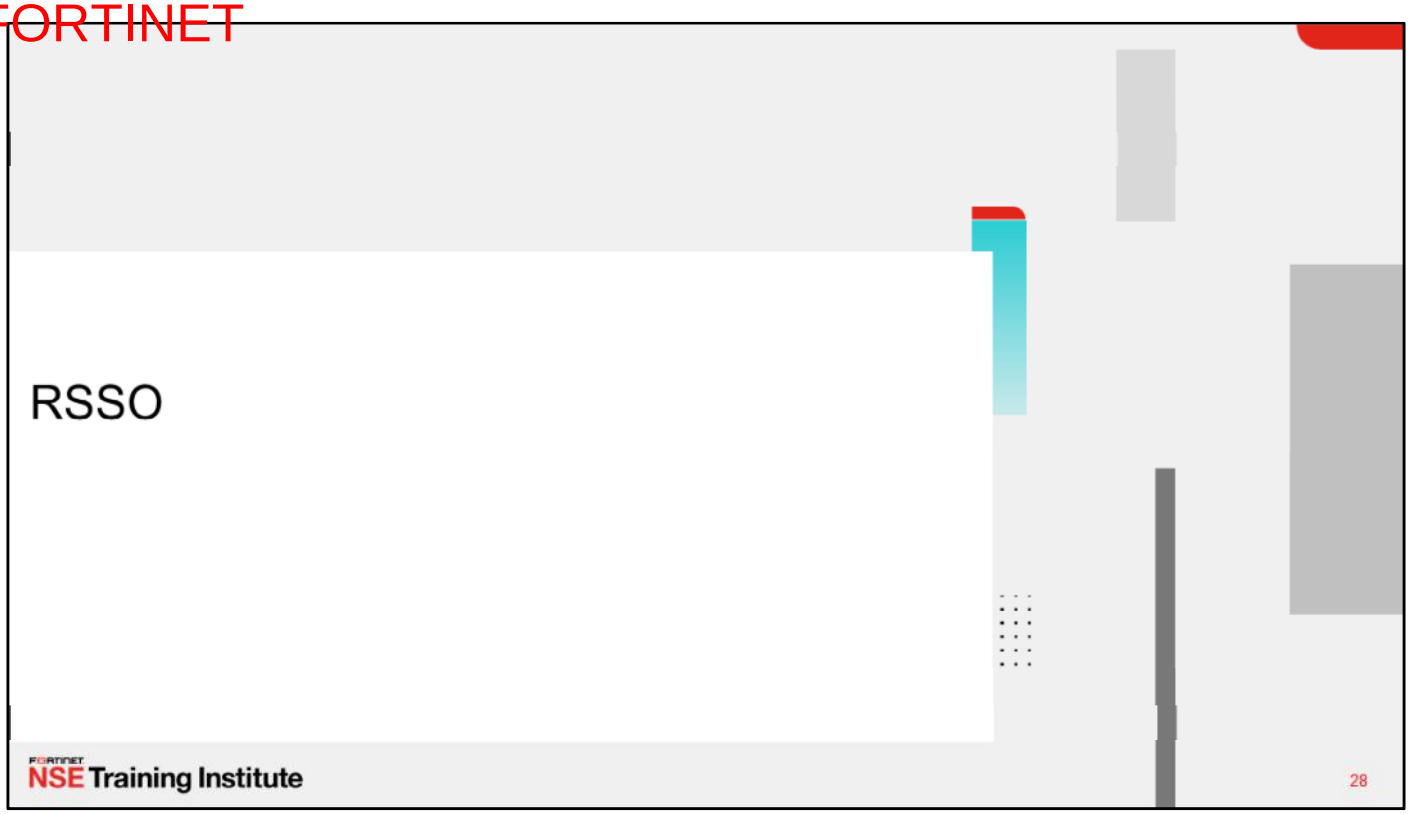
© Fortinet Inc. All Rights Reserved.

27

You can also view SSO-related logs that are specific to a single SSO source, such as RADIUS accounting or the syslog feed. For example, you can view the RADIUS attributes that are sent in the accounting message, or view the raw syslog feed that FortiAuthenticator is receiving.

Vouchers & Dumps are Available | WhatsApp +201224560923

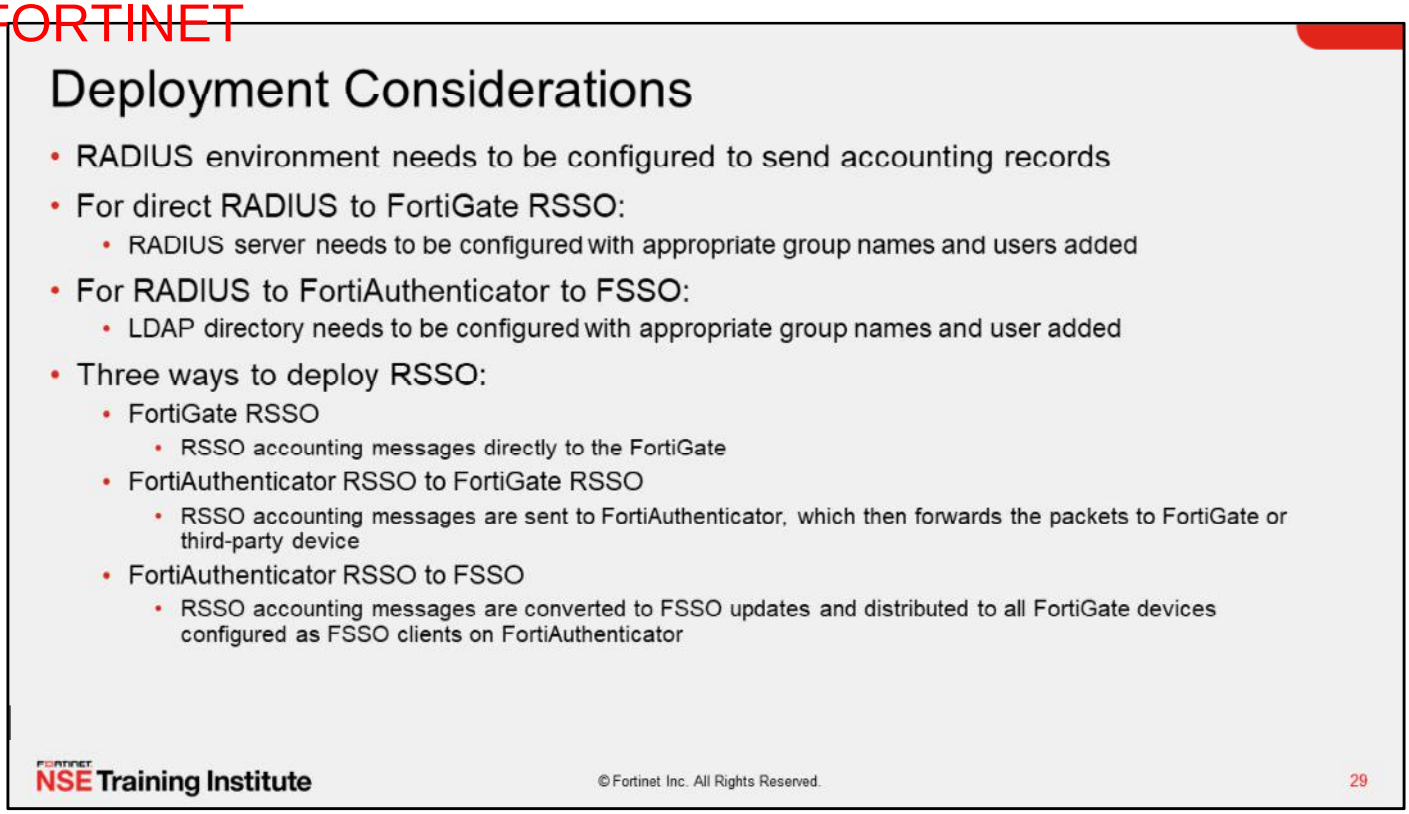
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn how to implement RSSO to be used with FortiAuthenticator and FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Consider the following important aspects before using RSSO:

- You must configure the RADIUS environment to send accounting records. How to configure every possible RADIUS server is beyond the scope of this lesson.
- For direct RADIUS to FortiGate RSSO, you must configure the RADIUS server with appropriate group names and users added to them.
- For RADIUS to FortiAuthenticator to FSSO, you must configure your LDAP directory with appropriate group names and users added to them.

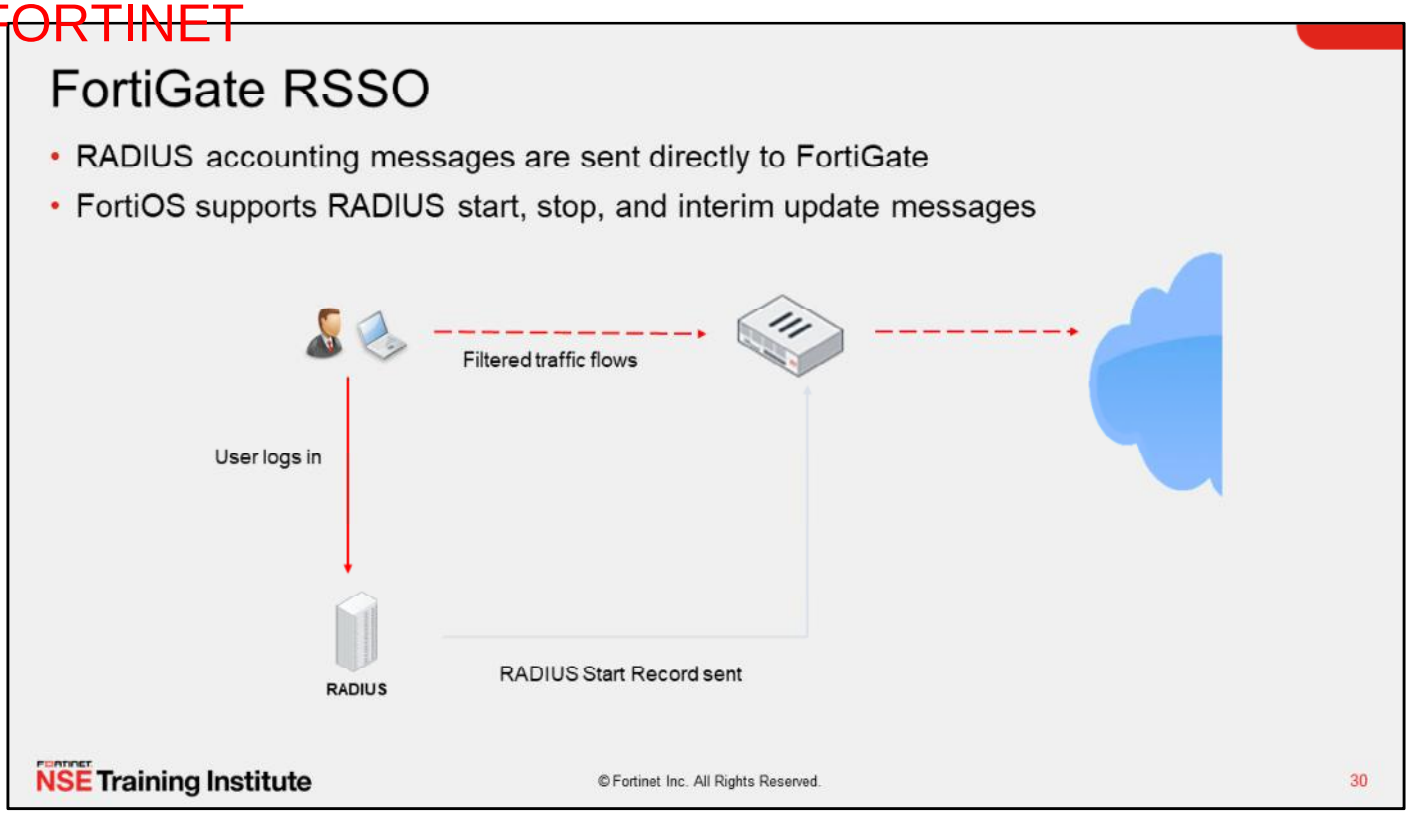
There are three different ways to deploy RSSO:

- FortiGate RSSO: RSSO accounting messages directly to FortiGate.
- FortiAuthenticator RSSO to FortiGate RSSO: RSSO accounting messages are sent to FortiAuthenticator, which then forwards the packets to FortiGate or a third-party device.
- FortiAuthenticator RSSO to FSSO: RSSO accounting messages are converted to FSSO updates and distributed to all FortiGate devices configured as FSSO clients on FortiAuthenticator.

Now, you will look at each of the three methods in more detail.

Vouchers & Dumps are Available | WhatsApp +201224560923

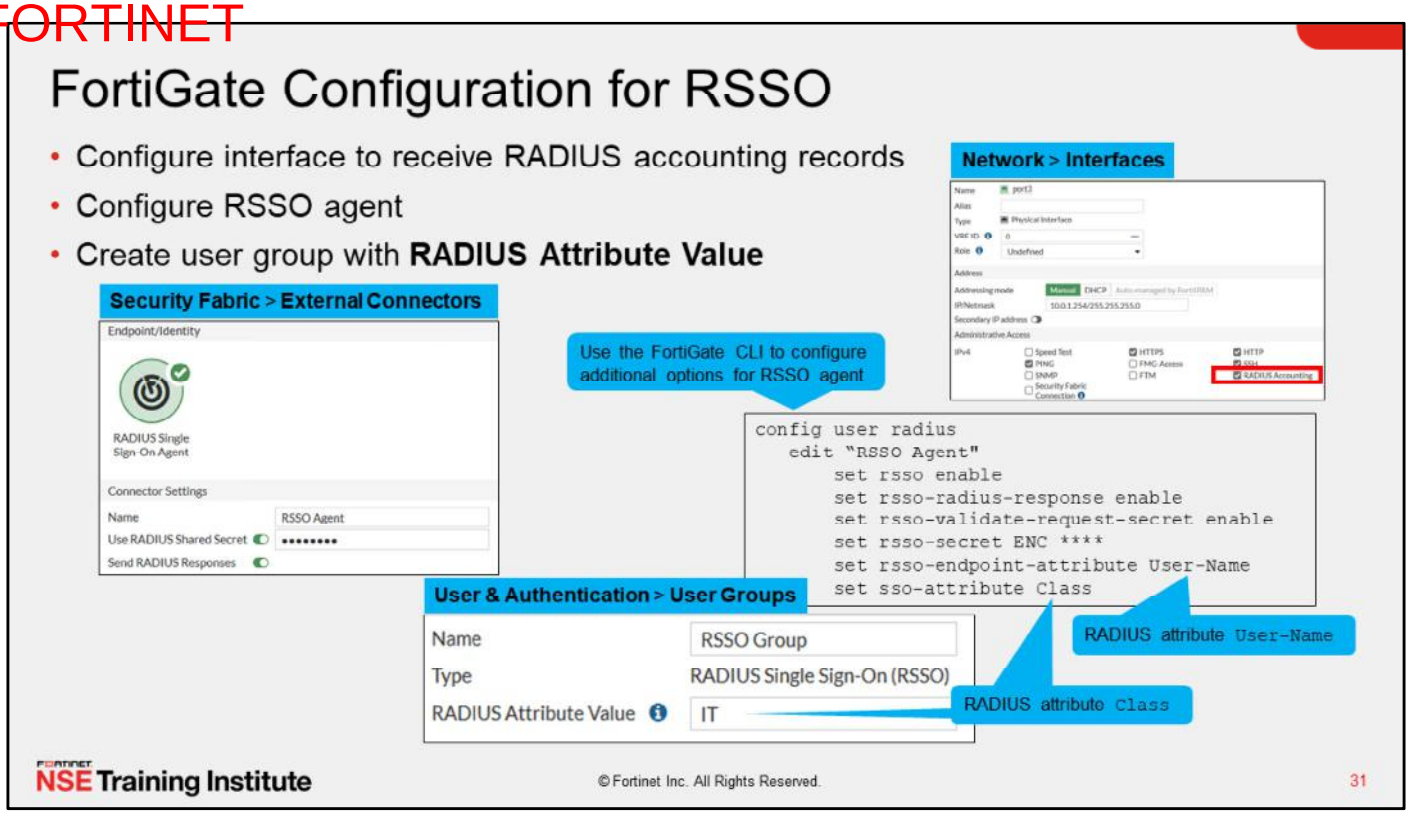
DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiOS supports the use of RADIUS start, stop, and interim update messages to authenticate and manage active users transparently. You can configure FortiGate to receive and use these messages.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You must perform a few configuration steps to enable RSSO on FortiGate. First, you must enable **RADIUS Accounting** in the **Administrative Access** section on the FortiGate interface where you expect to receive RSSO messages. Then, you must click **Security Fabric** > **Fabric Connectors**, define an RSSO agent, and configure it with a unique name and RADIUS shared secret that matches the one configured on the RADIUS accounting server. This enables a form of authentication between the RSSO agent (FortiGate) and the RADIUS accounting server (or RSSO server). You also need to create an RSSO user group locally on FortiGate. In the RSSO user group, you must set the **RADIUS Attribute Value**, which is used for user group matching. You can then use the RSSO user groups on a firewall policy to enable access for RSSO users.

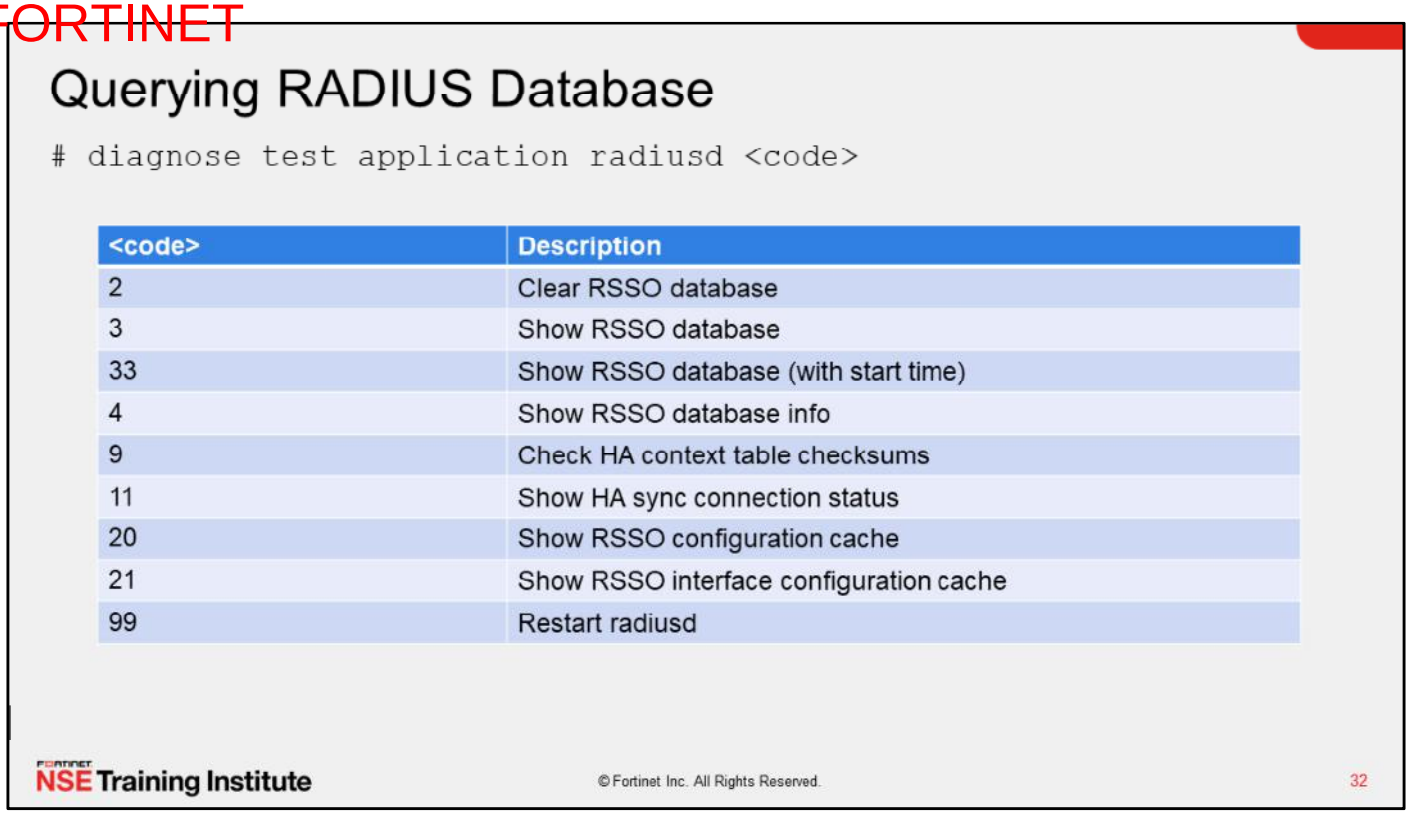
RSSO user group matching works as follows:

1. When FortiGate receives the RADIUS accounting message, FortiGate checks the value for the attribute set as `sso-attribute` in the RSSO agent configuration. In the example shown on this slide, the `sso-attribute` is set to `Class`.
2. FortiGate checks its local RSSO user groups. If the value of the `Class` attribute contained in the accounting message matches the value set as **RADIUS Attribute Value** in the RSSO user group, then FortiGate associates the RADIUS user with the RSSO user group. In the example shown on this slide, the configured **RADIUS Attribute Value** is `IT`.

In addition, FortiGate extracts the username from the attribute set as `rsso-endpoint-attribute`. In the example shown on this slide, the attribute is set to `User-Name`.

Vouchers & Dumps are Available | WhatsApp +201224560923

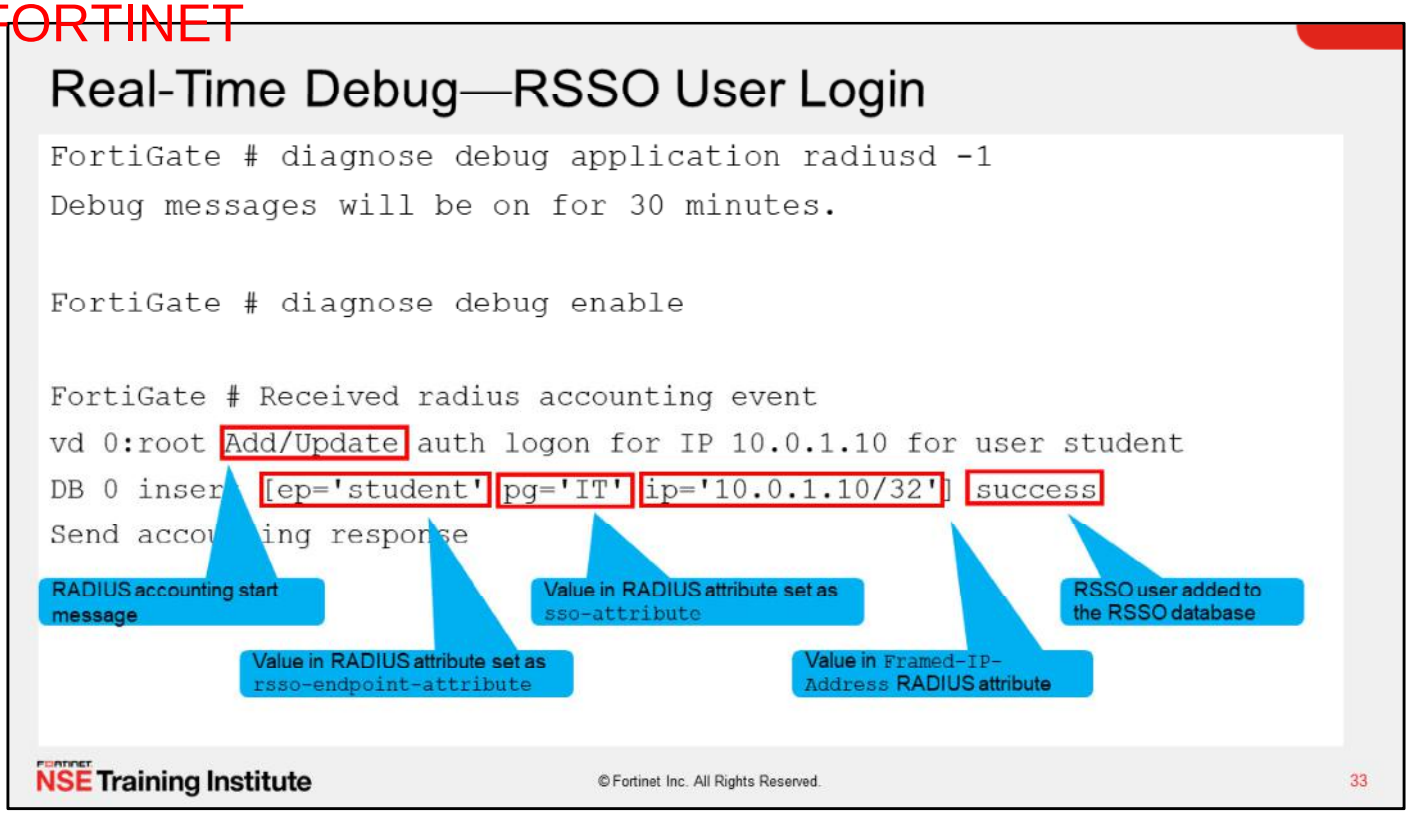
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The command `diagnose test application radiusd` allows you to perform additional actions on the RSSO service, include restarting the radiusd process. When you restart radiusd, the RSSO database is also cleared.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

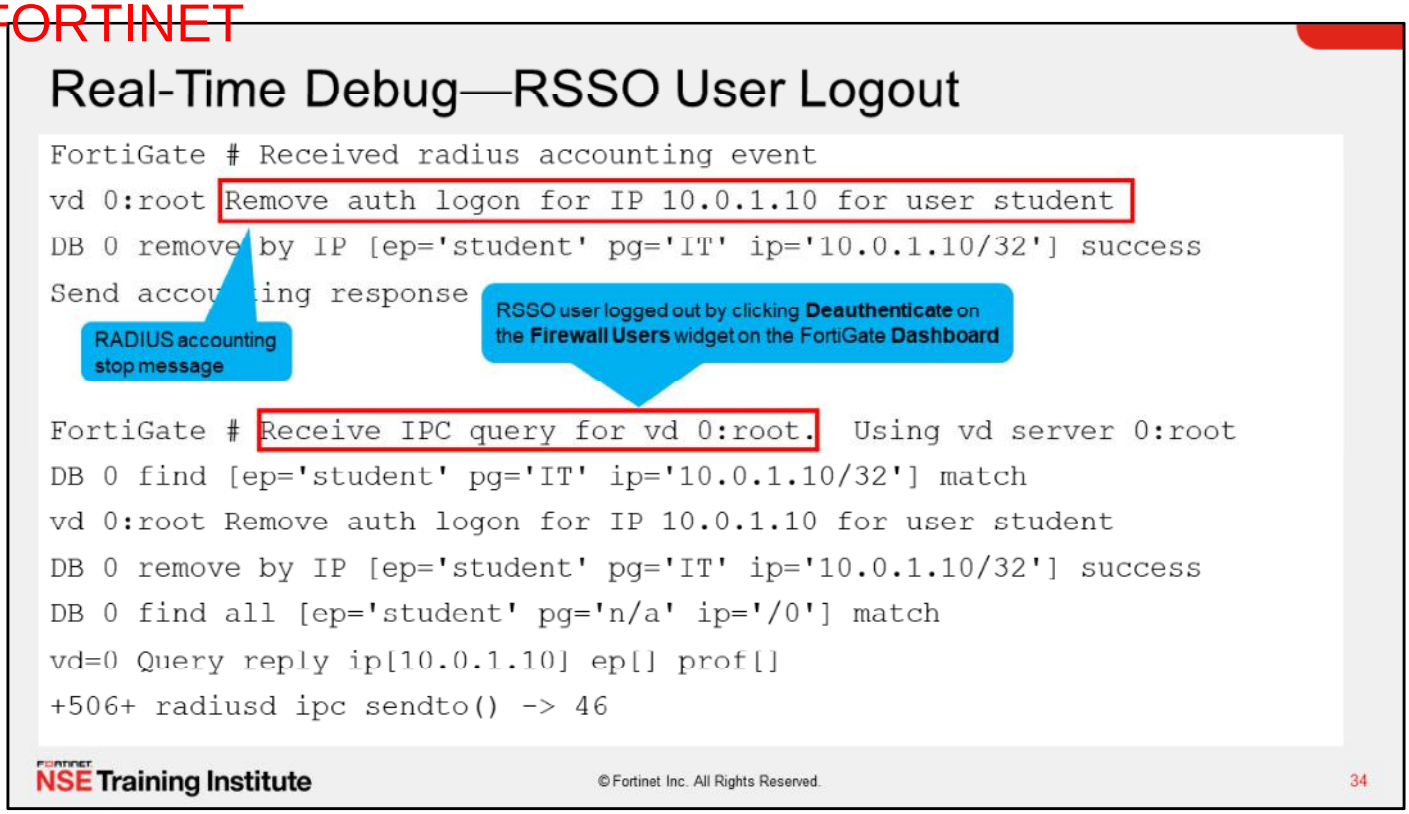


This slide shows real-time debugging when FortiGate receives a RADIUS accounting start message from the RADIUS server.

When FortiGate receives the RADIUS accounting start message, it extracts the username and user group information based on the RADIUS attributes set in the RSSO agent configuration for `rsso-endpoint-attribute` and `sso-endpoint-attribute` options, respectively. FortiGate then checks if the `sso-endpoint-attribute` value matches any of its local RSSO groups. If there is a match, FortiGate then adds the RSSO user to the RSSO database. The RSSO user entry contains the username, user group, as well as the user IP address, which is extracted from the `Framed-IP-Address` attribute that should also be present in the RADIUS accounting message.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

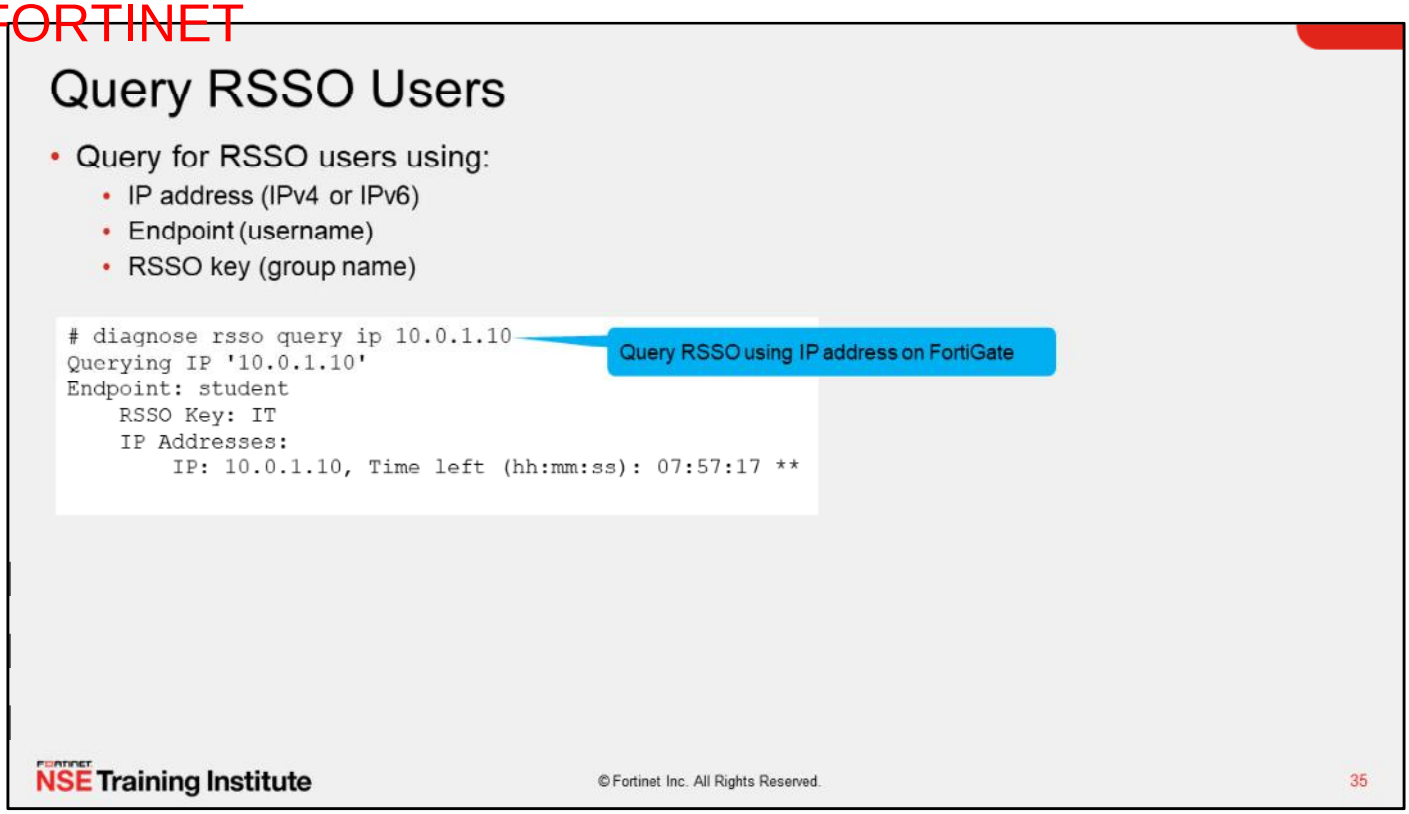


This slide shows two different debug outputs, both resulting in the RSSO user being logged out:

1. FortiGate receives a RADIUS accounting stop message from the RADIUS server.
2. The RSSO user is logged out of FortiGate using the **Deauthenticate** button on the **Firewall Users** widget on the FortiGate **Dashboard**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



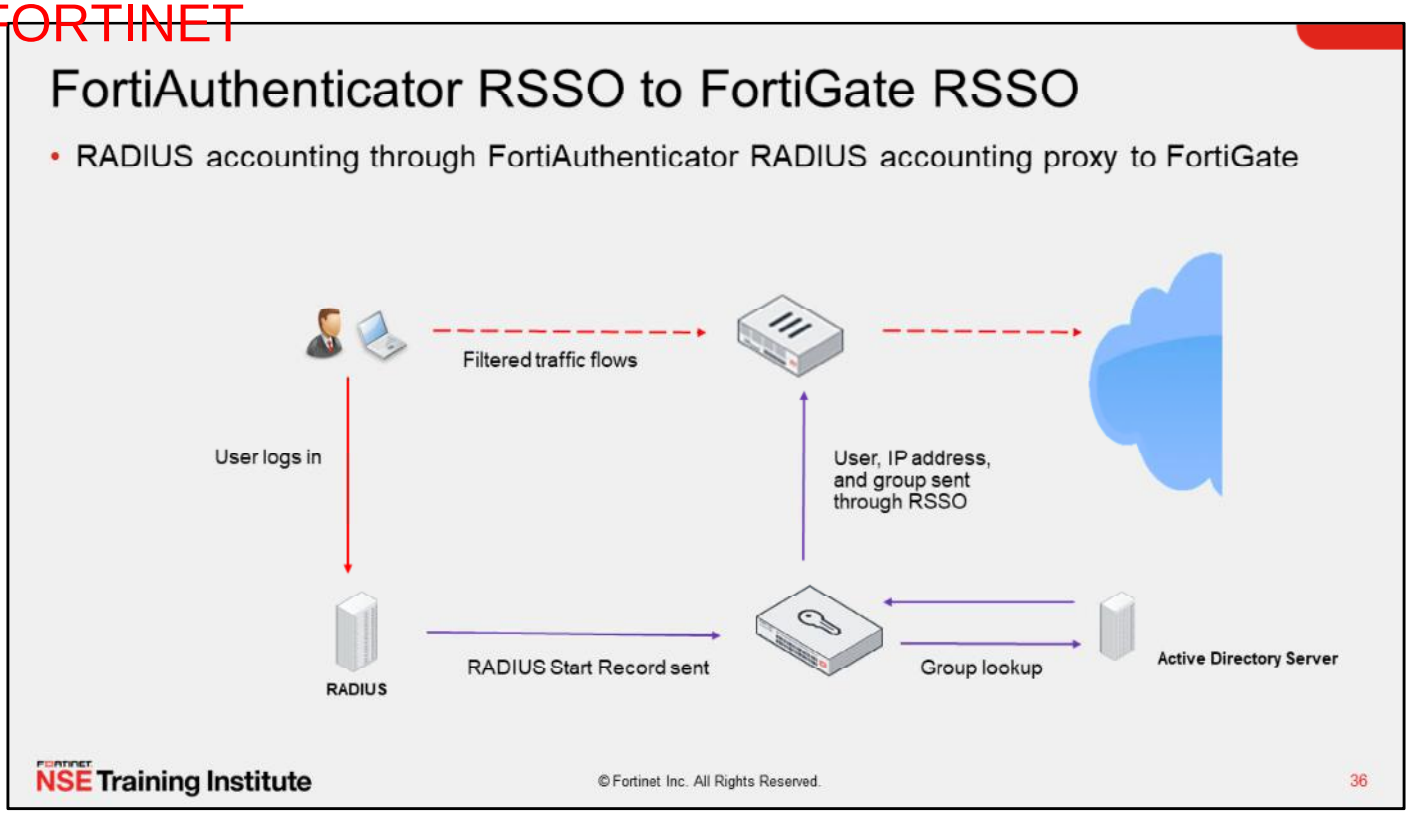
The command `diagnose rsso query` queries the RSSO database on FortiGate.

You can query RSSO users by IP address, username, or group name.

This slide shows an example of a query using the IP address.

Vouchers & Dumps are Available | WhatsApp +201224560923

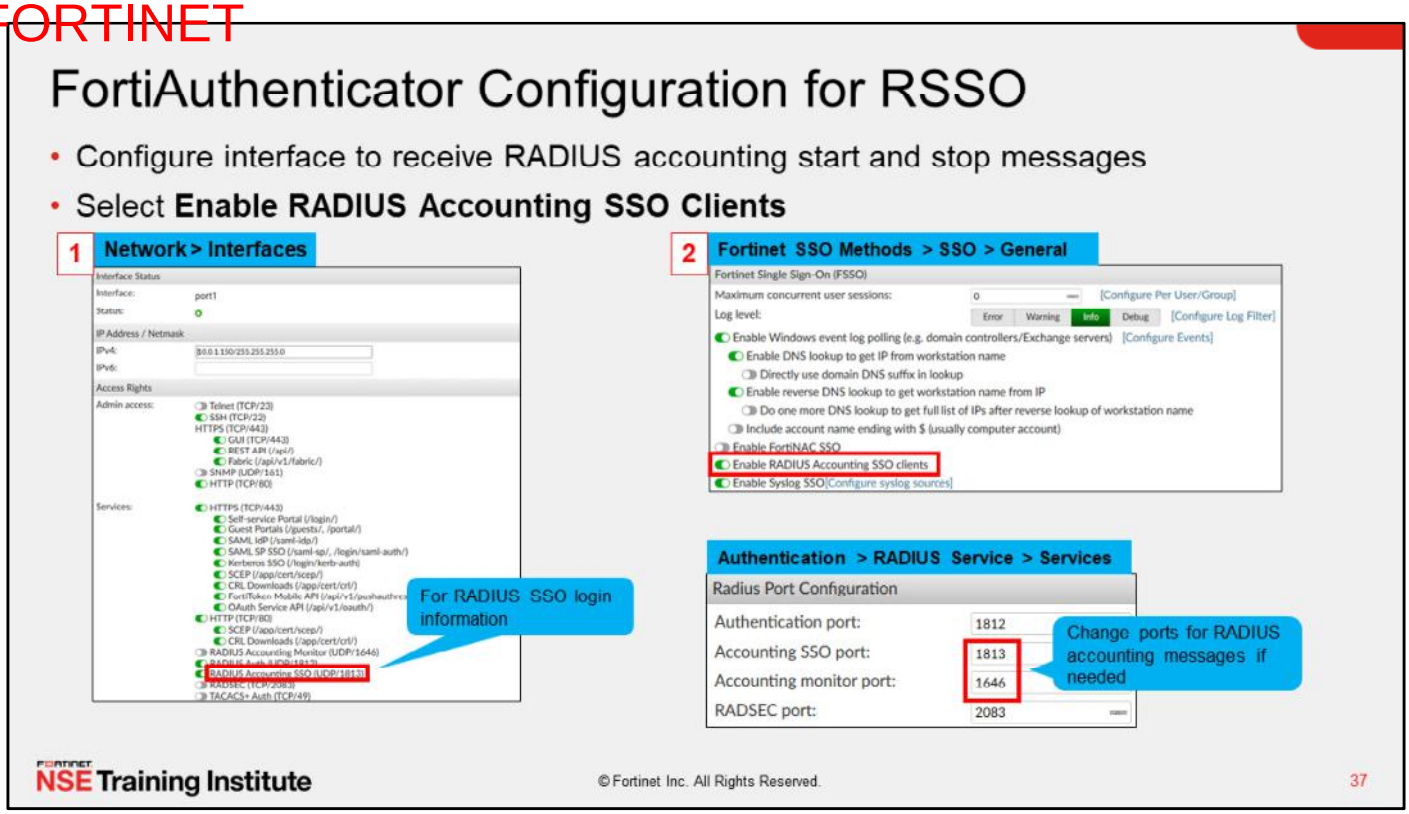
DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiAuthenticator supports the use of RADIUS start, stop, and interim update messages to authenticate and manage active users transparently. It receives RADIUS accounting messages, performs lookups against the LDAP server for group membership, and then forwards the RADIUS message to the FortiGate RSSO agent. This is useful when group membership information is handled by Active Directory, or when the RADIUS server is business-critical IT infrastructure, limiting the changes that can be made to the server configuration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Use the steps on this slide and the next to configure FortiAuthenticator when you want to implement a FortiAuthenticator RSSO to FortiGate FSSO solution:

1. Enable **RADIUS Accounting SSO** on the interface that will receive RADIUS accounting start and stop messages.
2. Turn on **Enable RADIUS Accounting SSO clients**.

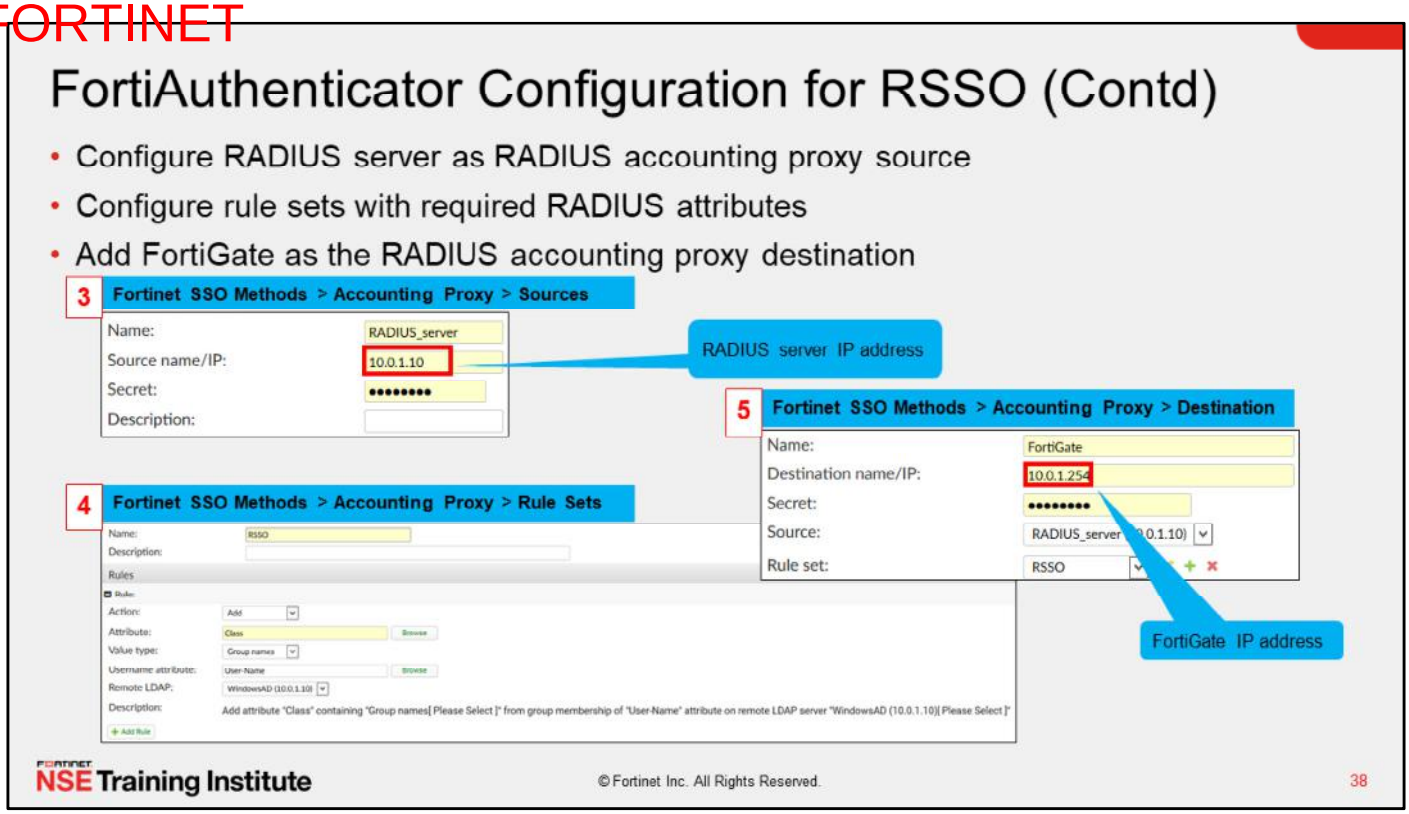
When you enable **RADIUS Accounting SSO**, FortiAuthenticator starts to listen on UDP port 1813 by default for incoming RADIUS accounting *start* and *stop* messages. The attributes on these messages are then used by FortiAuthenticator to create SSO sessions that can be shared with registered FortiGate devices through FSSO.

If you want FortiAuthenticator to track data and time usage for the RADIUS SSO users, then you must enable **RADIUS Accounting Monitor** on the interface. When you enable this option, FortiAuthenticator starts to listen on UDP port 1646 by default for incoming RADIUS accounting *interim* messages containing the user data and time usage information.

Note that you can change the default ports for both **RADIUS Accounting SSO** and **RADIUS Accounting Monitor** services if required. However, per design, FortiAuthenticator requires different ports for each service.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



3. Configure the RADIUS server as a RADIUS accounting proxy source.

4. Configure rule sets with the required RADIUS attributes.
Select **Add** for a new attribute, and click **Browse** to select the attribute. FortiAuthenticator uses the RADIUS attribute set as **Username** to perform an LDAP search on the selected LDAP server, and to retrieve group membership information. FortiAuthenticator then adds the attribute set as **Attribute** to the accounting messages it forwards to FortiGate.

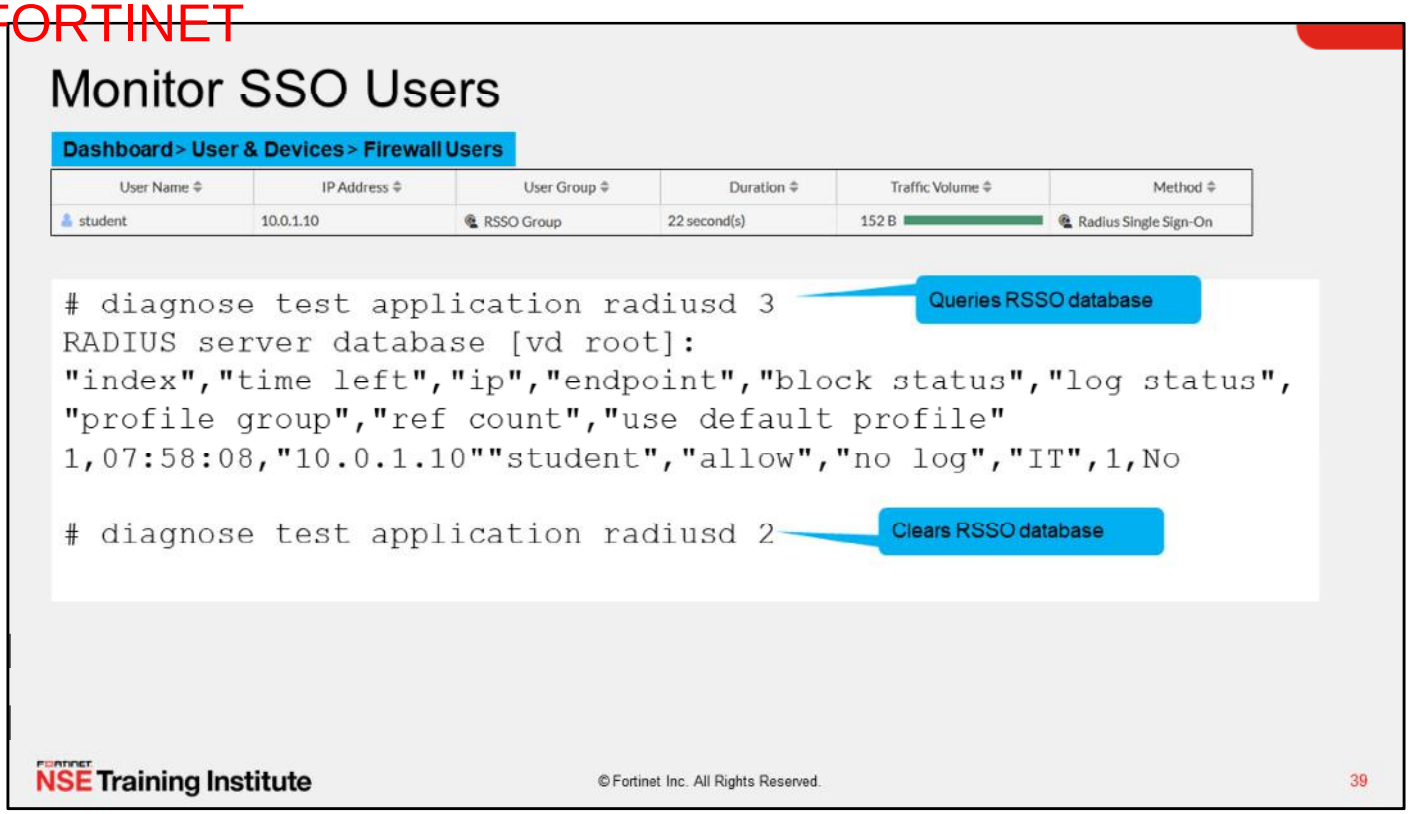
In the example shown on this slide, rule number 1 instructs FortiAuthenticator to add the attribute `Class` to the accounting message forwarded to FortiGate. The `Class` attribute contains the user groups retrieved from the LDAP server for the username set as `User-Name` attribute in the RADIUS accounting message received by FortiAuthenticator.

5. Add FortiGate as the RADIUS accounting proxy destination.
This is the target for the translated accounting message. Usually, this is the FortiGate device you want to send the accounting messages to, but it can be any RADIUS server configured to listen for accounting messages. Make sure you assign the rule set and source correctly.

Note that the FortiGate configuration is the same as described on the slide titled *FortiGate Configuration for RSSO*.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Various commands are available on FortiGate to view and clear information about RSSO users.

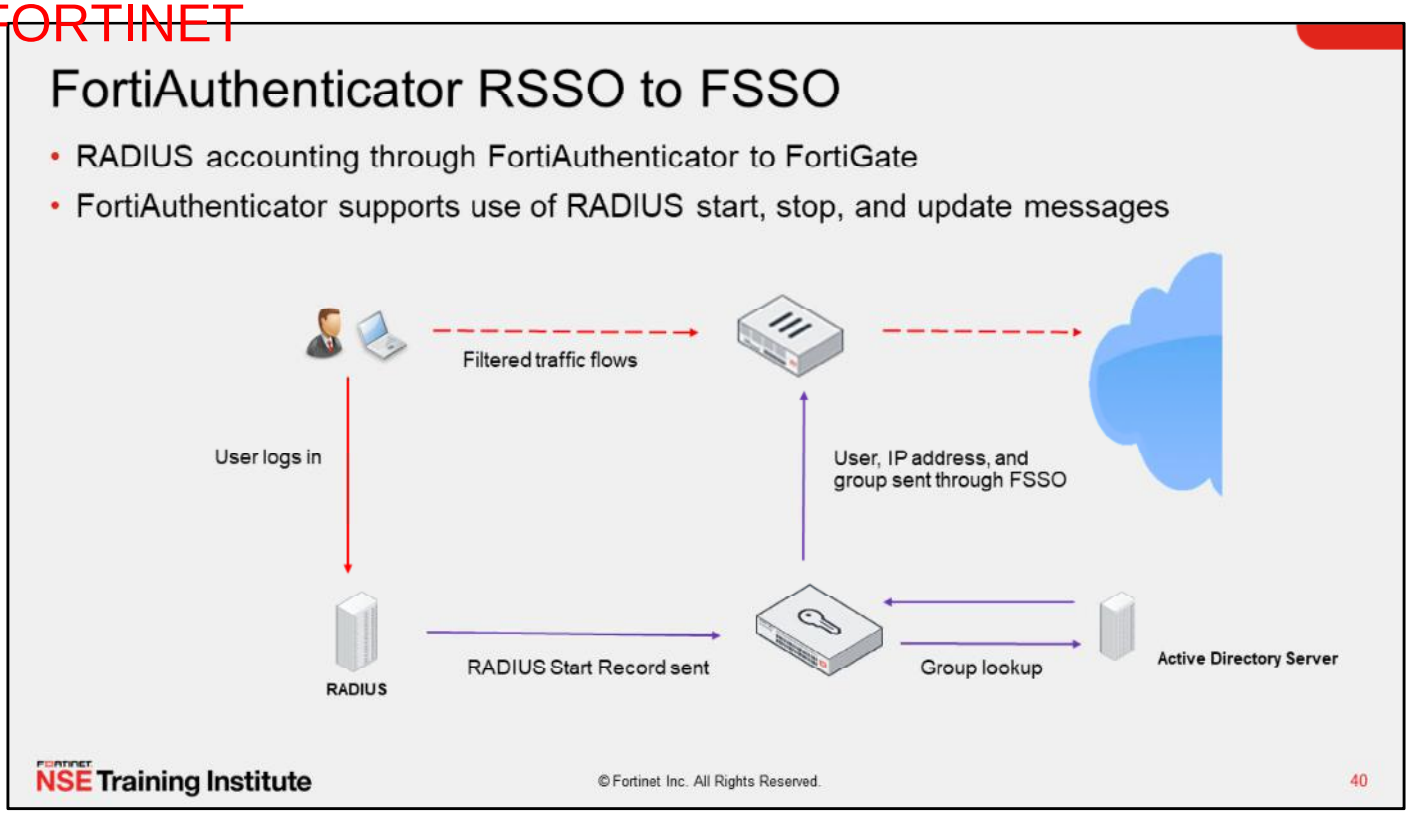
You can use the **Firewall Users** widget available on the FortiGate **Dashboard**.

Alternatively, you can use the command `diagnose test application radiusd 3`, which queries the RSSO database maintained by the radiusd process for all RSSO users currently logged in. radiusd is the FortiOS process responsible for the RSSO service operation.

You can also use the command `diagnose test application radiusd 2` to clear all the users in the RSSO database. To clear an individual user you must send an accounting stop message for that user.

Vouchers & Dumps are Available | WhatsApp +201224560923

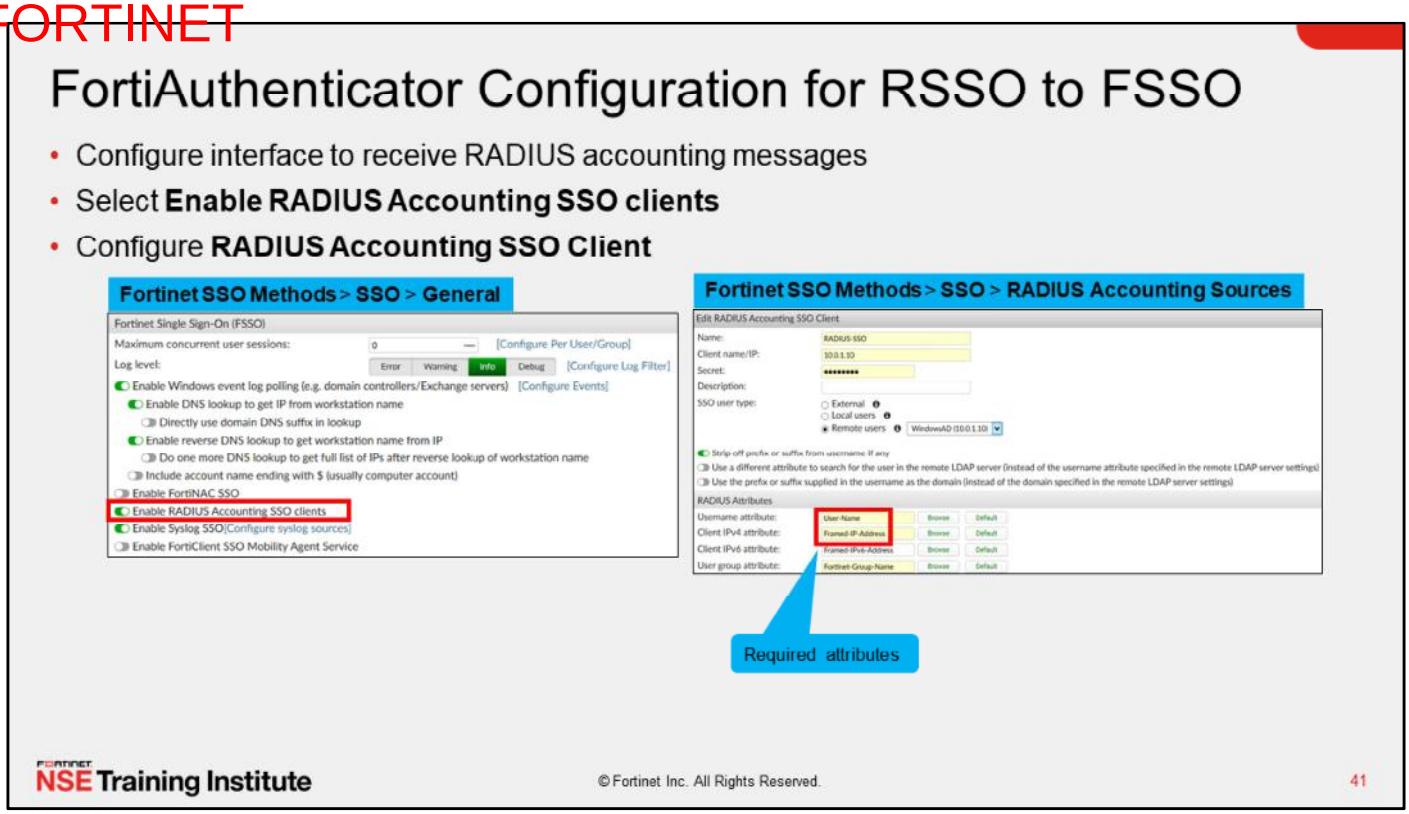
DO NOT REPRINT Brave-dumps.com
© FORTINET



FortiAuthenticator supports the use of RADIUS start, stop, and interim update messages to authenticate and manage active users transparently. It receives RADIUS accounting messages, performs lookups against the LDAP server for group membership, and then populates its FSSO cache with the correct information. This information is then sent to FortiGate as an FSSO login. This is useful when group membership information is handled by Active Directory, or when the RADIUS server is business-critical IT infrastructure, limiting the changes that can be made to the server configuration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can convert RSSO messages to FSSO using FortiAuthenticator. This can be very useful in environments that have multiple FortiGate devices deployed. FortiAuthenticator can distribute FSSO events to all FortiGate devices that have been configured to receive FSSO updates in the network.

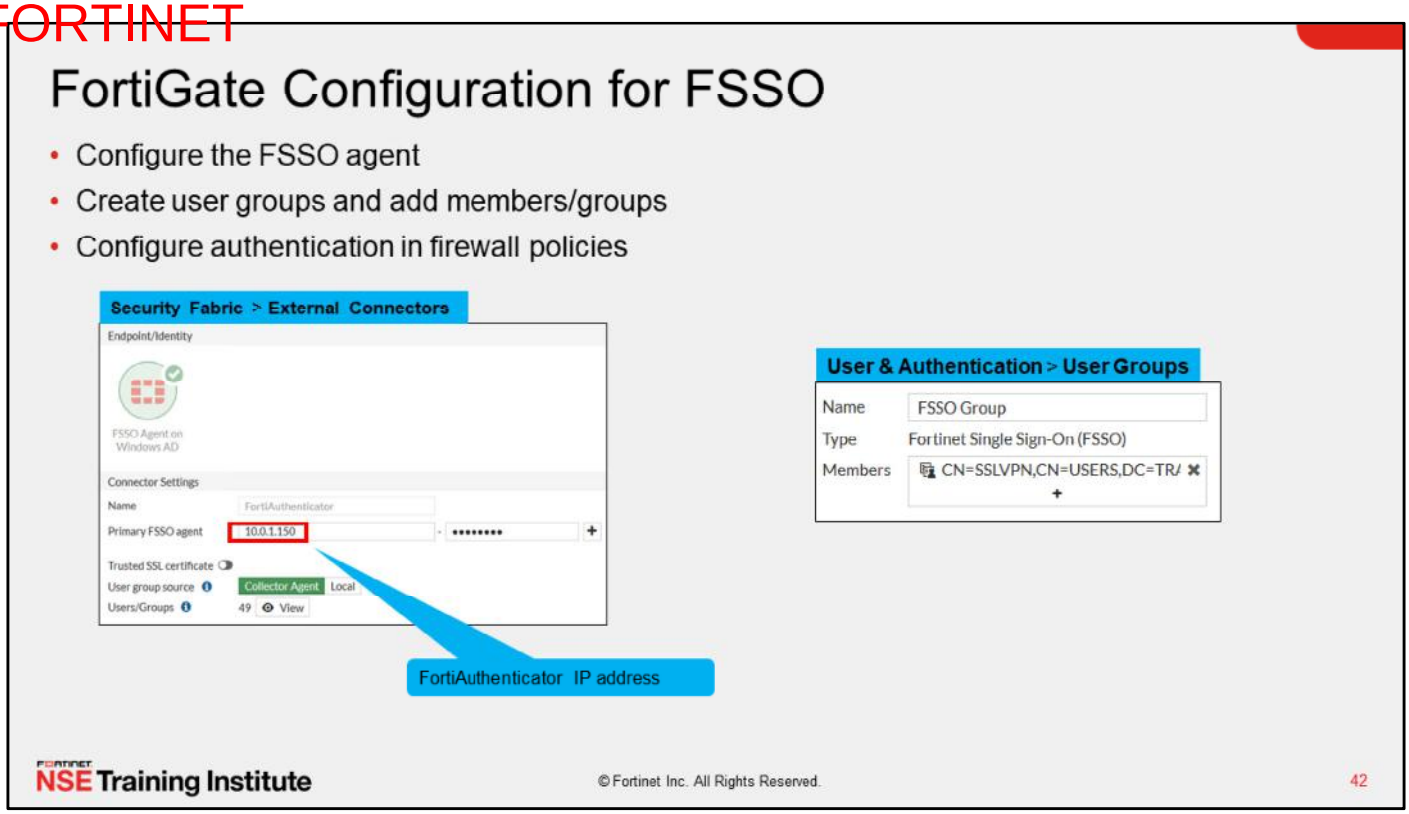
Use the following steps to configure FortiAuthenticator for FSSO:

1. Configure the interface to receive RADIUS accounting messages.
2. Select **Enable RADIUS Accounting SSO Clients**.
3. Configure the **RADIUS Accounting SSO Client**.

You must select the LDAP server from the drop-down list if you want to validate remote users using a back-end LDAP server. FortiAuthenticator can retrieve group memberships from the LDAP server to verify that the RSSO user account resides on the LDAP server. You can also categorize the user as **External**, which means that the user account is not expected to be configured in the local or remote database. The RADIUS **Username attribute** (default **User-Name**) and **Client IPv4 attribute** (default **Framed-IP-Address**) fields are required. The **User group attribute** field is not required.

Vouchers & Dumps are Available | WhatsApp +201224560923

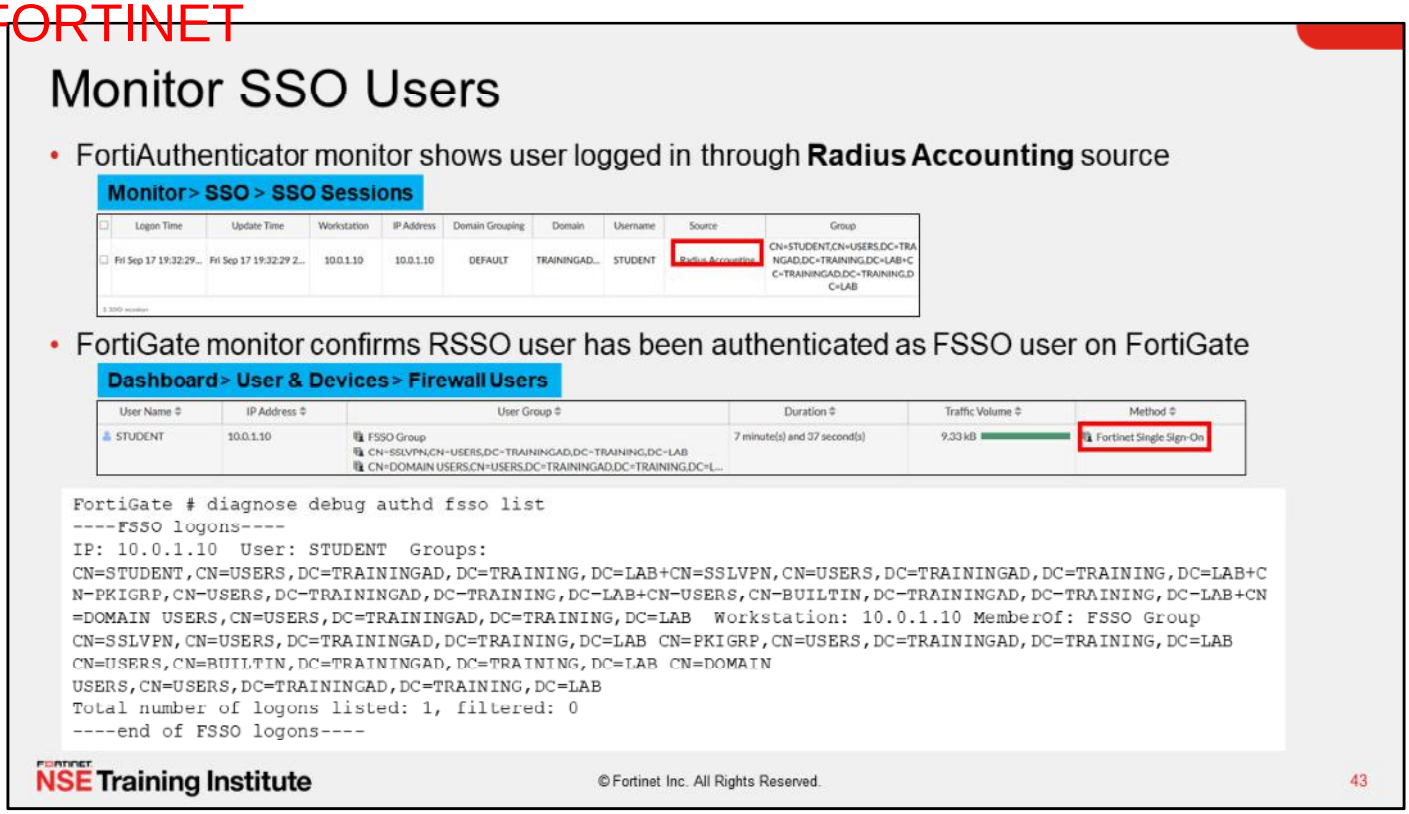
DO NOT REPRINT
© FORTINET
Brave-dumps.com



You must configure FSSO on FortiGate to receive the FSSO updates from FortiAuthenticator. First, you configure a **Fortinet Single Sign-On Agent** in **External Connectors**. Then, you can pull or create an FSSO user group, and assign remote members to the group. You can then refer to the FSSO user group on a firewall policy to provide network access to FSSO users.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



While the FortiAuthenticator **Monitor** page records that the user logged in through a **Radius Accounting** source, you can confirm that the user was authenticated on FortiGate using the **Fortinet Single Sign-On** method by looking at the **Firewall Users** widget.

You can also confirm this by running the `diagnose debug authd fsso list` command.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Real-Time Debug on FortiGate

```
FortiGate # diagnose debug application authd -1
Debug messages will be on for 30 minutes.
FortiGate # diagnose debug enable

FortiGate # fsae_io_ctx_process_msg[FortiAuthenticator]: received heartbeat 0
authd_epoll_work: timeout 33140
[_process_logon:1064]: STUDENT (10.0.1.10, 0) logged on from FortiAuthenticator.
authd_epoll_work: timeout 28060
[authd_admin_read:1007]: called
authd_epoll_work: timeout 28050
```

FortiGate receives login message from FortiAuthenticator through FSSO

NSE Training Institute

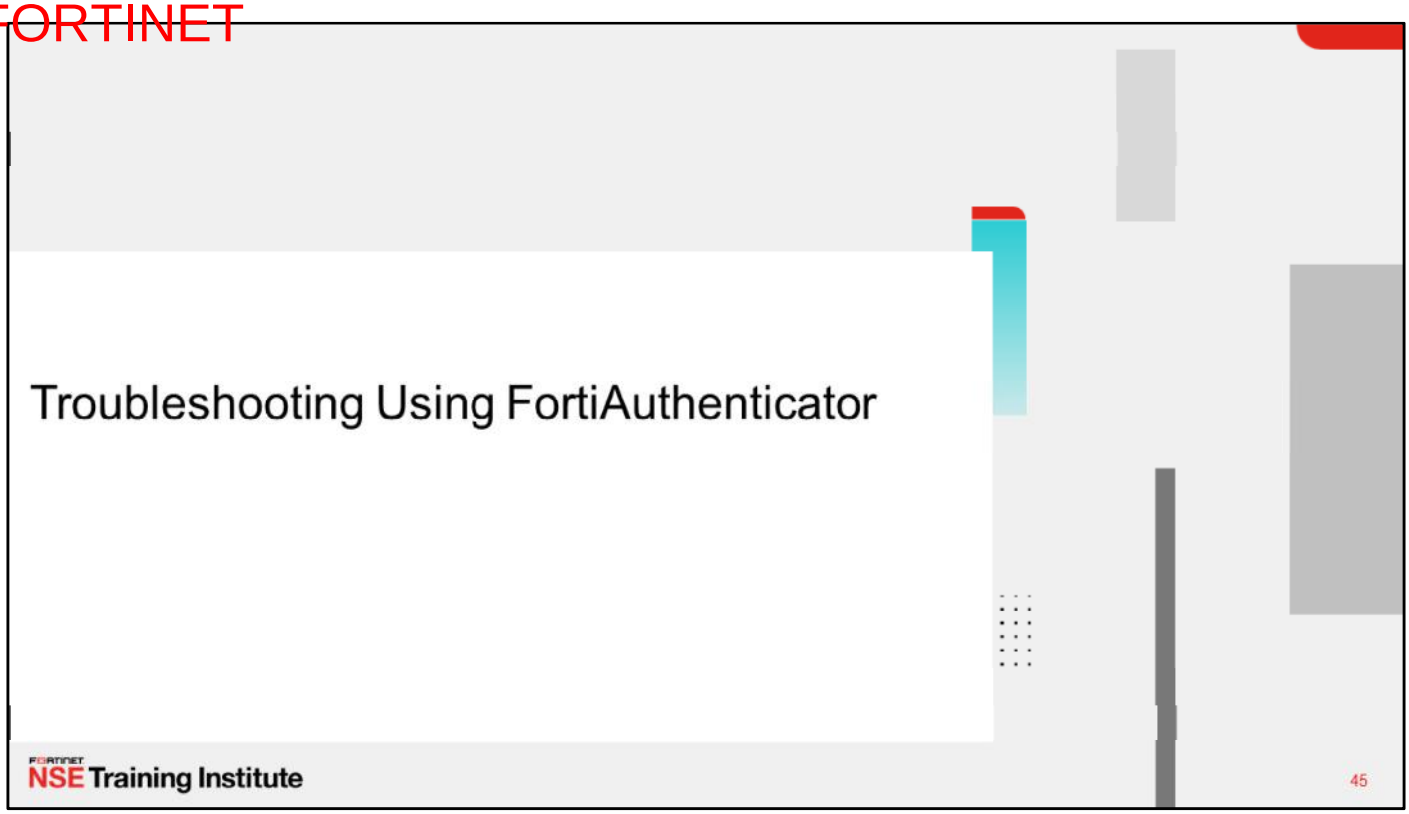
© Fortinet Inc. All Rights Reserved.

44

This slide shows the real-time debugging of the FortiGate device that receives a login message from FortiAuthenticator through FSSO.

Vouchers & Dumps are Available | WhatsApp +201224560923

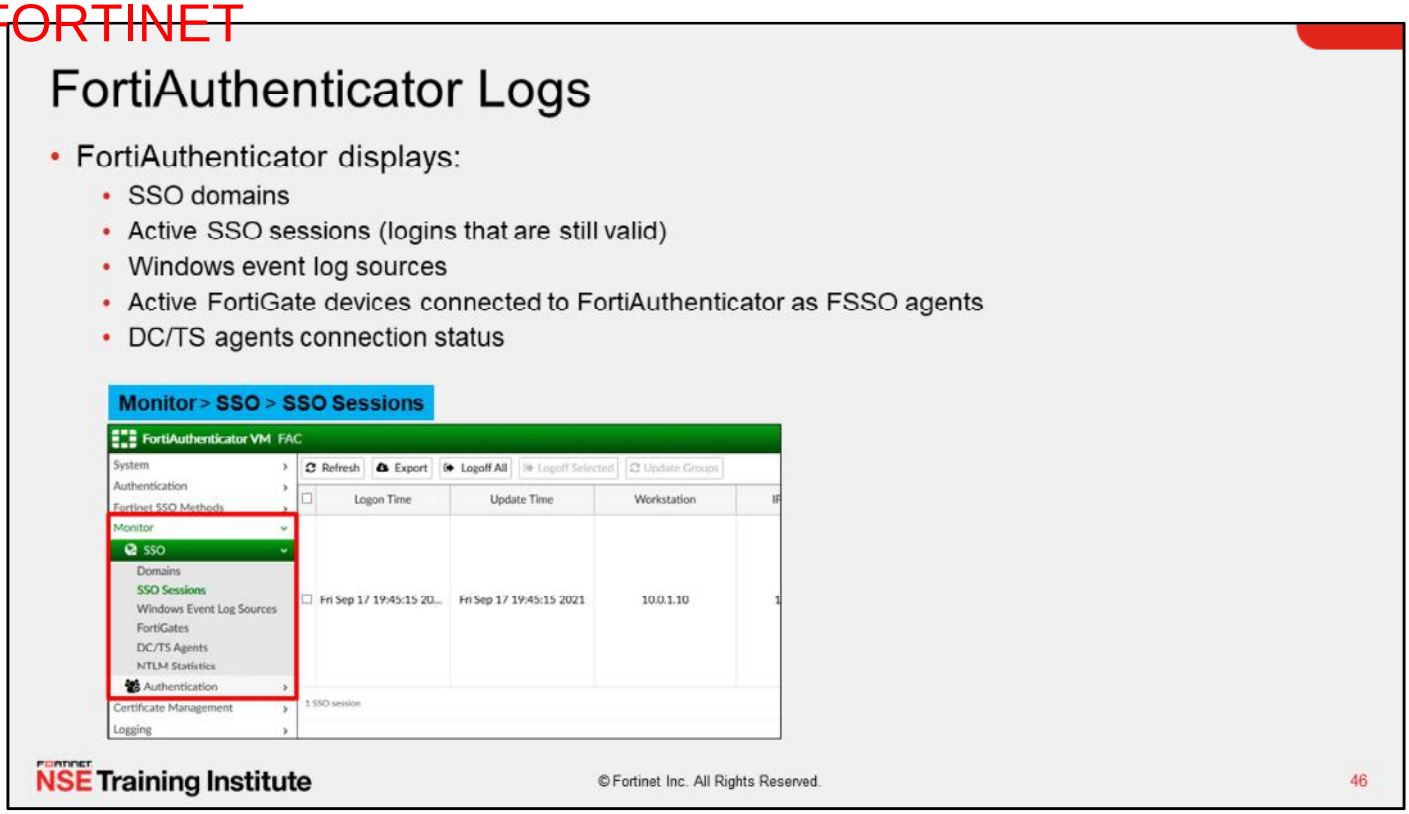
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn about troubleshooting FSSO using FortiAuthenticator.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiAuthenticator makes troubleshooting easier because all the tools required to check the status of different components in FSSO are available on the GUI. By clicking **Monitor** > **SSO**, you can view information, such as SSO domains, active SSO sessions, Windows event log sources status, currently active FortiGate connections, and DC/TS agents connection status.

If you have trouble distinguishing SSO sessions from TS/DC agents, you can view whether the DC/TS agents are connected to FortiAuthenticator. If not, ensure that the correct IP address, port, and secret are configured on both FortiAuthenticator and the DC/TS agents.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Monitoring SSO Sessions on FortiAuthenticator

- Administrator can log out all current SSO sessions or specific entries

Monitor > SSO > SSO Sessions

Refresh | Export | Logoff All | Logoff Selected | Update Groups

Logon Time	Update Time	Workstation	IP Address	Domain Grouping	Domain	Username	Source	Group
Mon Sep 20 05:08:11 2...	Mon Sep 20 05:08:11 2021	WINDOWSAD.TRAININ...	10.0.1.10	DEFAULT	TRAININGAD.T...	JSMITH	Eventlog Polling	CN=JOHN SMITH,CN=USERS,DC=TRAININGAD,DC=TRAINING,DC=LAB+CN=ADMINISTRATORS,CN=BUILTIN,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
Mon Sep 20 05:36:15 2...	Mon Sep 20 05:36:15 2021	10.1.10.1	10.1.10.1	DEFAULT	SSO_EXT_USER	USER1101	Syslog	USER1101+SYSLOG_GROUP
Mon Sep 20 05:36:33 2...	Mon Sep 20 05:36:33 2021	10.1.10.10	10.1.10.10	DEFAULT	SSO_EXT_USER	USER11010	Syslog	USER11010+SYSLOG_GROUP
Mon Sep 20 05:36:35 2...	Mon Sep 20 05:36:35 2021	10.1.10.11	10.1.10.11	DEFAULT	SSO_EXT_USER	USER11011	Syslog	USER11011+SYSLOG_GROUP
Mon Sep 20 05:36:37 2...	Mon Sep 20 05:36:37 2021	10.1.10.12	10.1.10.12	DEFAULT	SSO_EXT_USER	USER11012	Syslog	USER11012+SYSLOG_GROUP
Mon Sep 20 05:36:39 2...	Mon Sep 20 05:36:39 2021	10.1.10.13	10.1.10.13	DEFAULT	SSO_EXT_USER	USER11013	Syslog	USER11013+SYSLOG_GROUP
Mon Sep 20 05:36:41 2...	Mon Sep 20 05:36:41 2021	10.1.10.14	10.1.10.14	DEFAULT	SSO_EXT_USER	USER11014	Syslog	USER11014+SYSLOG_GROUP
Mon Sep 20 05:36:43 2...	Mon Sep 20 05:36:43 2021	10.1.10.15	10.1.10.15	DEFAULT	SSO_EXT_USER	USER11015	Syslog	USER11015+SYSLOG_GROUP
Mon Sep 20 05:36:45 2...	Mon Sep 20 05:36:45 2021	10.1.10.16	10.1.10.16	DEFAULT	SSO_EXT_USER	USER11016	Syslog	USER11016+SYSLOG_GROUP
Mon Sep 20 05:36:47 2...	Mon Sep 20 05:36:47 2021	10.1.10.17	10.1.10.17	DEFAULT	SSO_EXT_USER	USER11017	Syslog	USER11017+SYSLOG_GROUP
Mon Sep 20 05:36:49 2...	Mon Sep 20 05:36:49 2021	10.1.10.18	10.1.10.18	DEFAULT	SSO_EXT_USER	USER11018	Syslog	USER11018+SYSLOG_GROUP
Mon Sep 20 05:36:51 2...	Mon Sep 20 05:36:51 2021	10.1.10.19	10.1.10.19	DEFAULT	SSO_EXT_USER	USER11019	Syslog	USER11019+SYSLOG_GROUP

NSE Training Institute

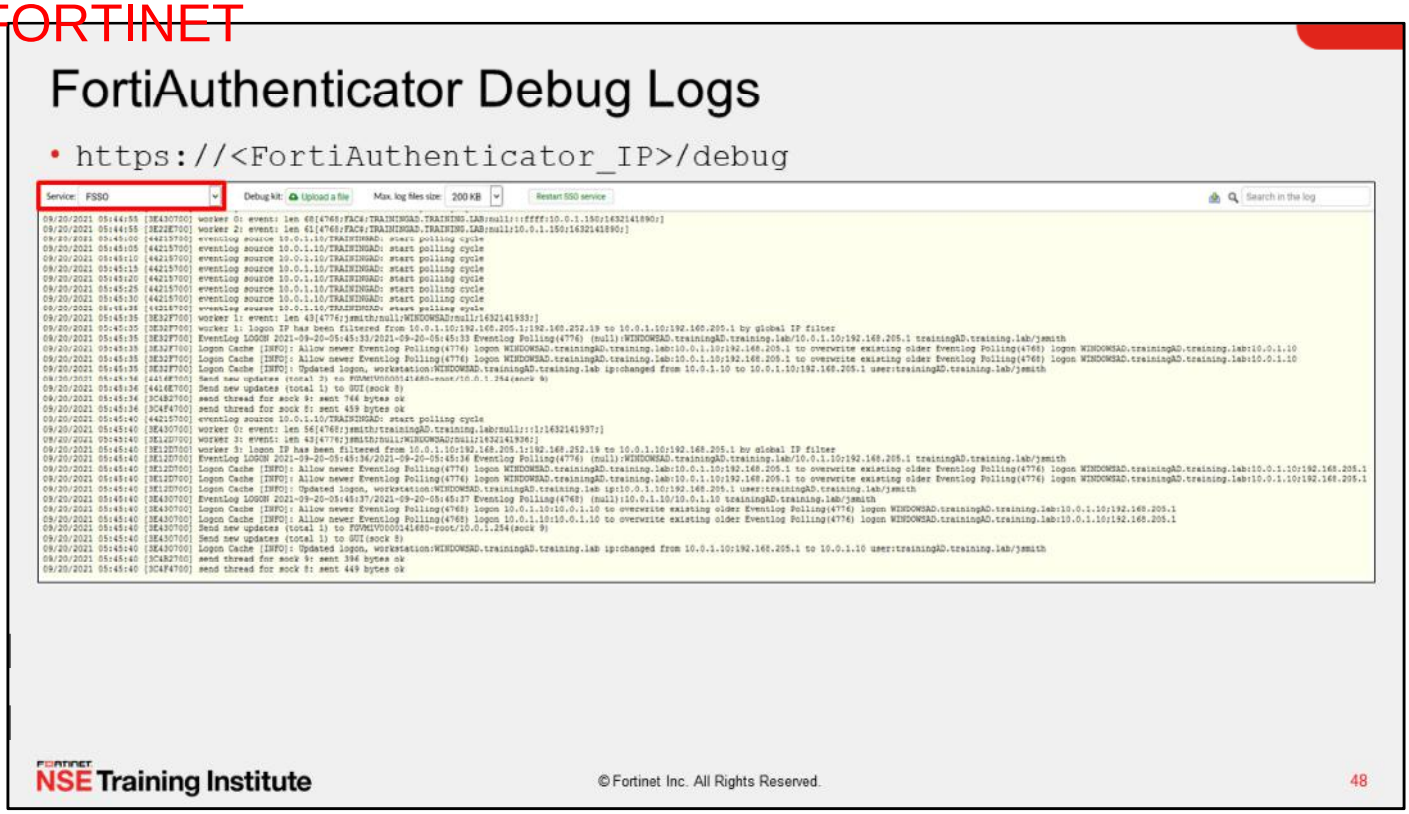
© Fortinet Inc. All Rights Reserved.

47

FortiAuthenticator displays all the active SSO sessions on the **Monitor** tab. This tab displays detailed information about SSO sessions that are currently active on FortiAuthenticator. On this tab, you can view SSO-related information, such as login time, logout time, username, IP address, workstation name (AD), domain, group, and SSO source. In the example shown on this slide, there are two SSO sources that are currently in use, **Eventlog Polling** and **Syslog** feed.

Vouchers & Dumps are Available | WhatsApp +201224560923

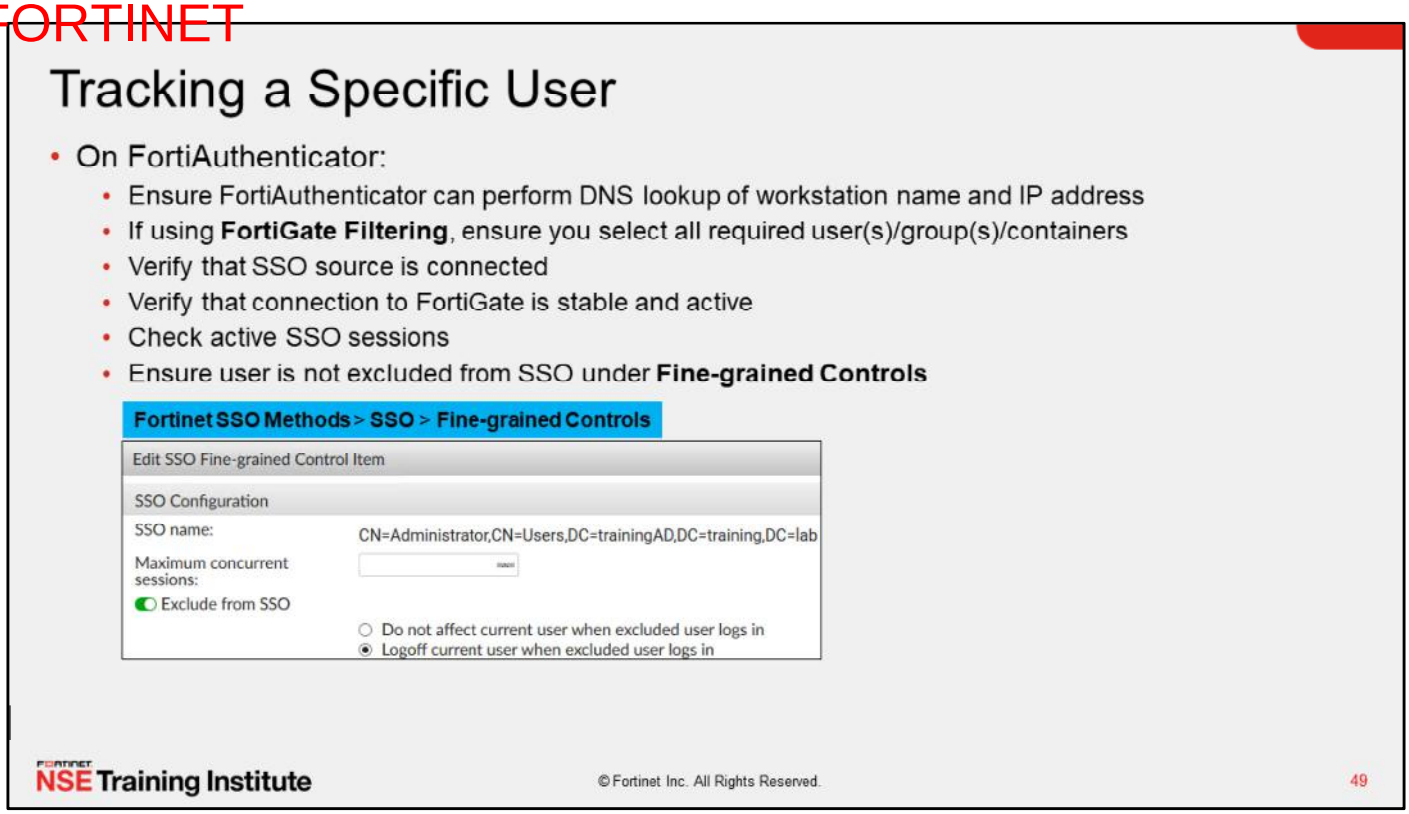
DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can also view debug-level logs on FortiAuthenticator by connecting to `https://<FortiAuthenticator_IP>/debug` and selecting the **FSSO** service. The debug log page enables you to view detailed connection logs, as well as basic information about configuration mismatches between FortiAuthenticator and the SSO source. You can also view information that is exchanged between the FSSO source and FortiAuthenticator, which can be useful when troubleshooting FSSO-related issues.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



If you are having FSSO issues for a specific user, you can start troubleshooting by following these steps:

- Ensure FortiAuthenticator can perform a DNS lookup of the workstation name and IP address.
- If using **FortiGate Filtering**, ensure you select all required users, groups, and containers.
- Verify that the SSO source is connected.
- Ensure the user is not excluded from SSO in **Fine-grained Controls.**
- Check the active SSO sessions.
- Verify that the connection to FortiGate is stable and active.

When troubleshooting FSSO issues related to the DC agent mode (Windows AD) environment, the steps are the same for the standalone collector agent and FortiAuthenticator. The only difference between the two is that all the DC agents point to FortiAuthenticator instead of to the standalone collector agent.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Listing Active FSSO Users

```
# diagnose debug authd fsso filter ?
clear       Clear all filters.
Source      Source IP address.
user        User name.
group       Group name.
server      FSSO agent name.

# diagnose debug authd fsso list
----FSSO logons----
IP: 10.0.1.10  User: JSMITH  Groups: CN=DOMAIN
USERS,CN=USERS,DC=TRAININGAD,DC=TRAINING,DC=LAB  Workstation: 10.0.1.10
IP: 10.1.10.1  User: USER1101  Groups: SYSLOG_GROUP  Workstation:
10.1.10.1
Total number of logons listed: 2, filtered: 0
----end of FSSO logons----
```

NSE Training Institute © Fortinet Inc. All Rights Reserved. 50

To retrieve the list of active FSSO users from FortiGate, use the command `diagnose debug authd fsso list`. You can set up a filter first using the command `diagnose debug authd fsso filter`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The CLI command `diagnose debug authd fsso refresh-logons` refreshes the active FSSO user list on FortiGate by retrieving this information again from the collector agent.

The CLI command `diagnose debug authd fsso clear-logons` flushes the list of active FSSO users on FortiGate.

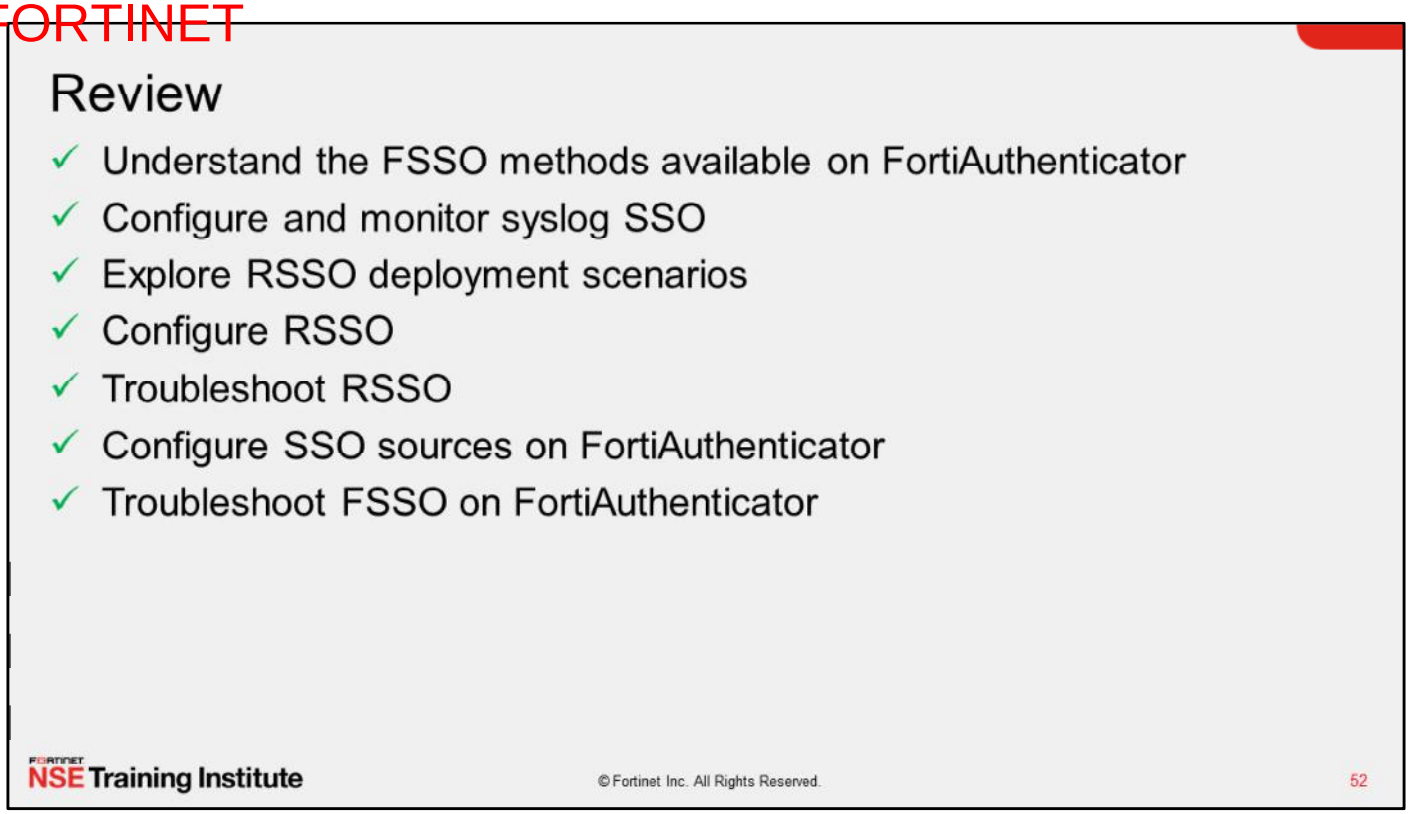
The CLI command `diagnose debug authd fsso refresh-groups` refreshes the user group information on FortiGate by retrieving this information again from the collector agent.

The CLI command `execute fsso refresh` will refresh the FSSO user group information.

To list the monitored user groups, use the command `get user adgrp`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

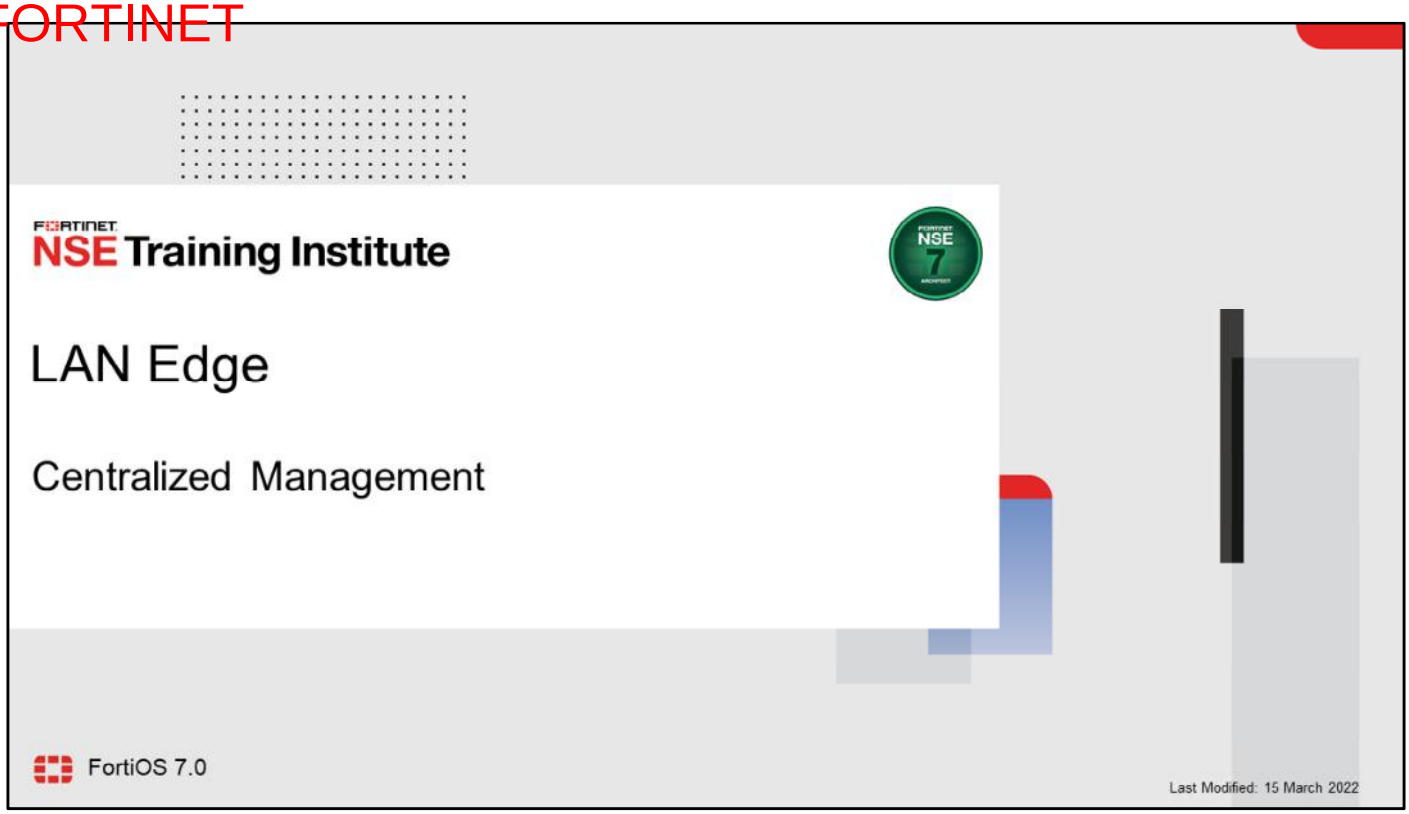


This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned about different ways to collect login events and convert them to Fortinet single sign-on (FSSO) events. You also focused on RADIUS and syslog single sign-on and their relevant configurations.

Vouchers & Dumps are Available | WhatsApp +201224560923

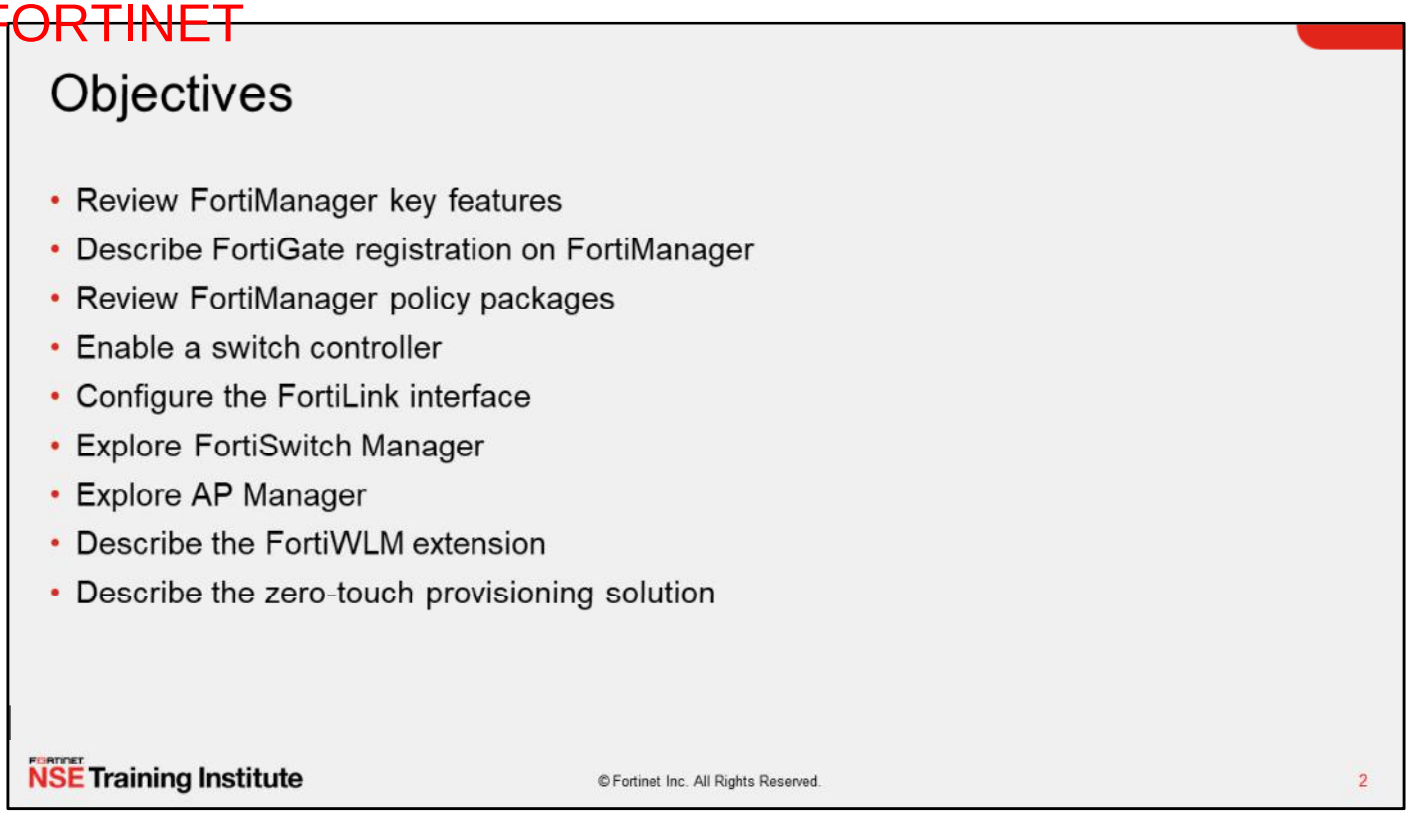
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about FortiSwitch and FortiAP management on FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

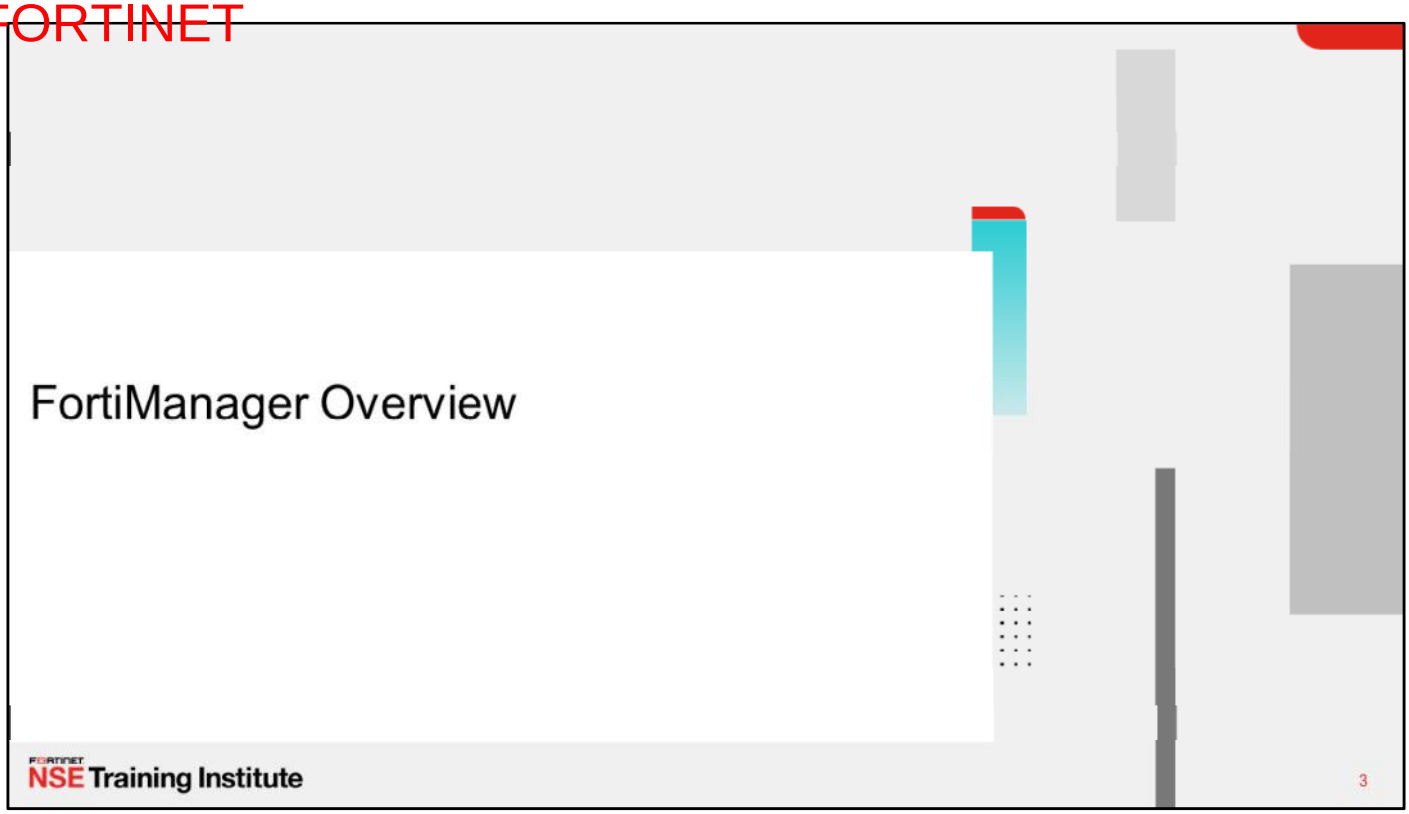


After completing this lesson, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in centralized management, you will be able to manage FortiGate using FortiManager, configure the FortiLink interface to manage FortiSwitch, and enable a Security Fabric connection to manage FortiAP.

Vouchers & Dumps are Available | WhatsApp +201224560923

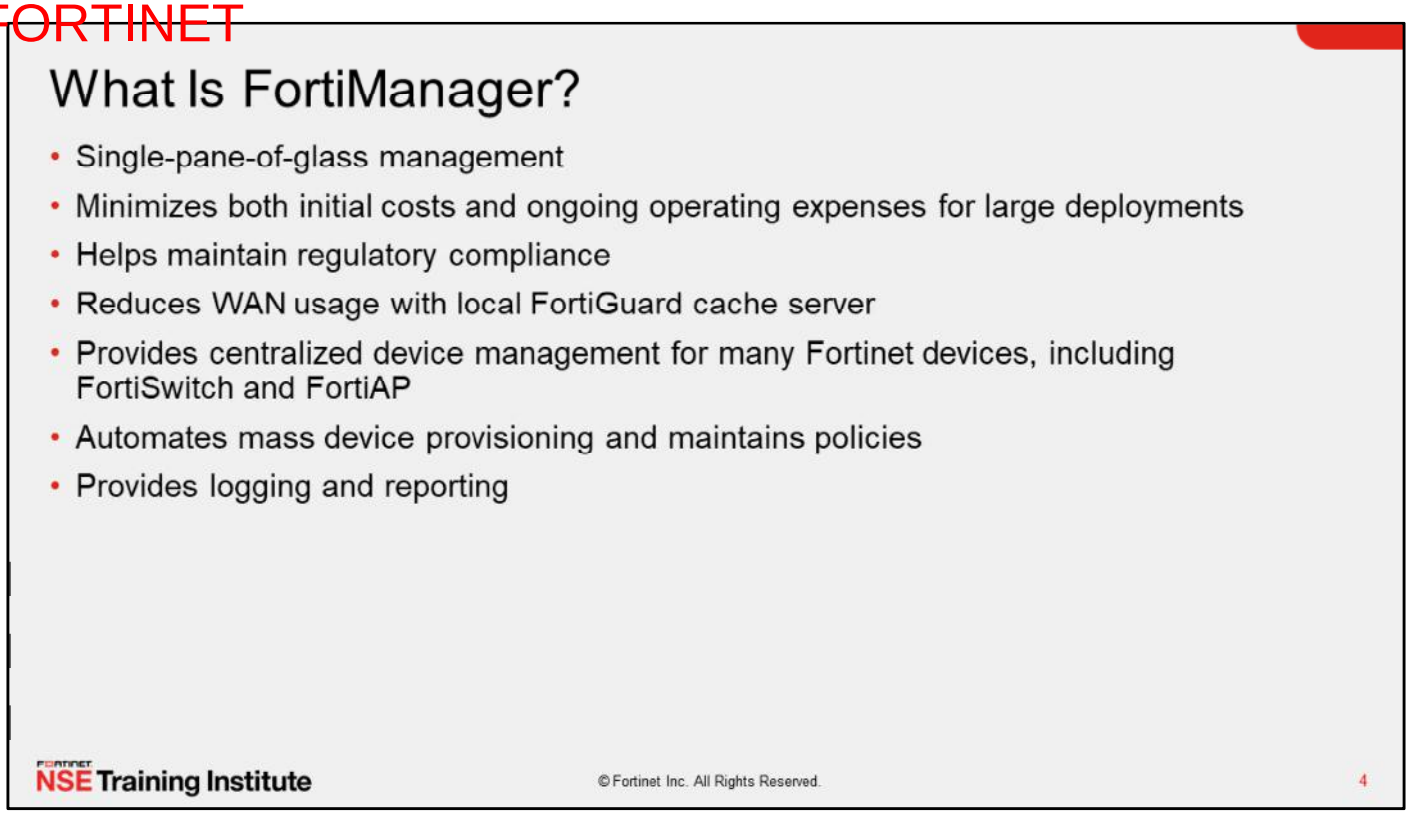
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will review FortiManager basics.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



When should you use FortiManager in your network?

In large enterprises and managed security service providers (MSSPs), the size of the network introduces challenges that smaller networks don't have: mass provisioning; scheduling rollout of configuration changes; and maintaining, tracking, and auditing many changes.

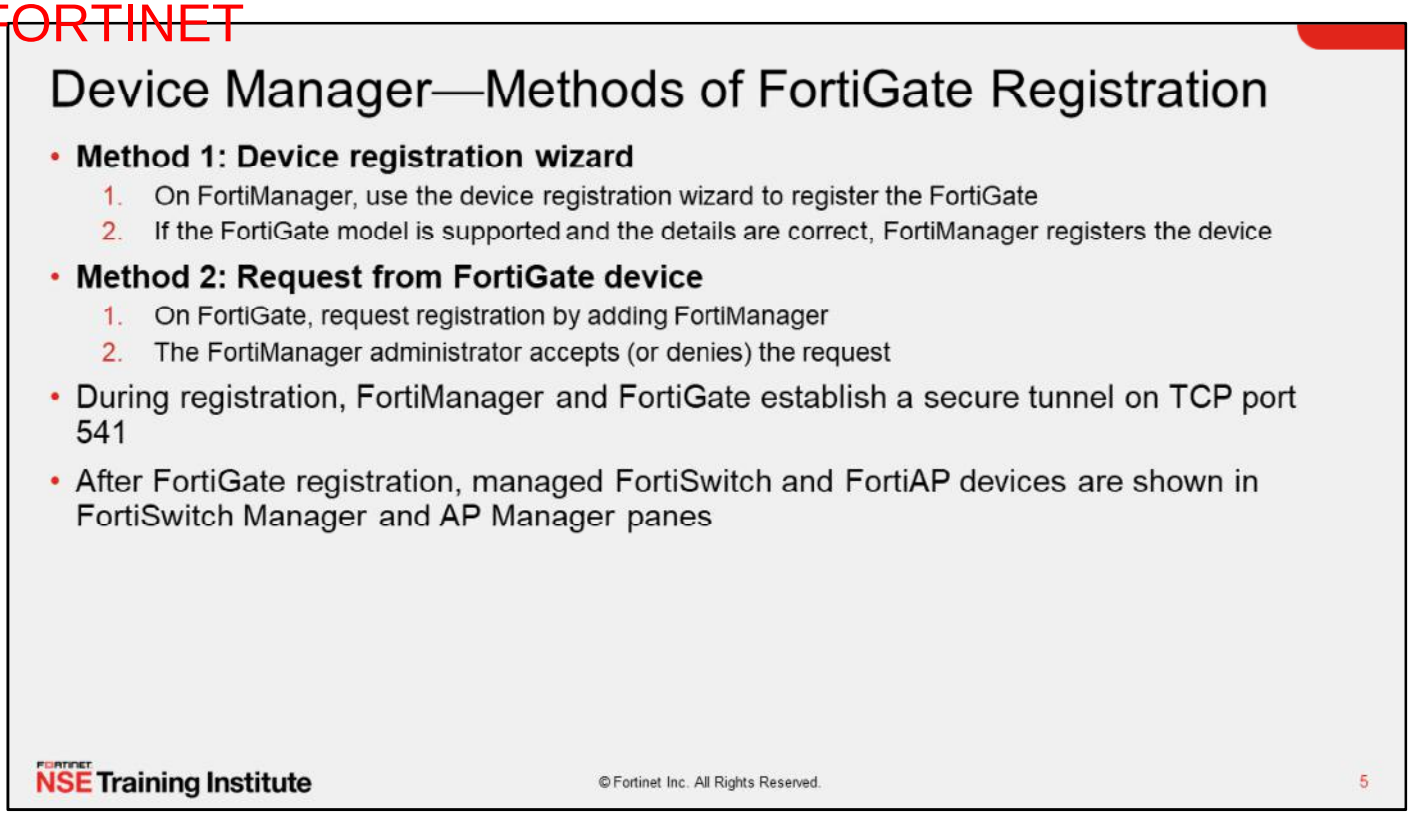
Centralized management through FortiManager can help you to more easily manage many deployment types with many devices, and to reduce the cost of operation.

What can FortiManager do?

- Provision firewall policies across your network.
- Act as a central repository for configuration revision control and security audits.
- Centrally manage of FortiSwitch and FortiAP devices.
- Act as a private FortiGuard distribution server (FDS) for your managed devices.
- Script and automate device provisioning, policy changes, and more, with JSON APIs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



There are two ways you can register a FortiGate device using FortiManager.

The first method involves the FortiManager device registration wizard. If the FortiGate device is supported and all the details of the device are correct, FortiManager registers the device. This method is the one used in the lab, and you'll learn more about this method in this lesson.

The second method involves a request for registration from the FortiGate device. This happens after you add FortiManager on the FortiGate GUI. Then, when the FortiManager administrator receives the registration request, the request is accepted (though it can be denied).

During device registration, FortiManager and FortiGate create a secure tunnel on TCP port 541. The tunnel is used for checking device status and configuration, as well as configuration installation.

After FortiGate is registered on FortiManager, any FortiSwitch or FortiAP devices that are managed by that FortiGate device are displayed on the FortiSwitch Manager and AP Manager panes, respectively.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Device Manager—Device Registration Wizard

- Add a device through Device Manager



NSE Training Institute © Fortinet Inc. All Rights Reserved. 6

When using the device registration wizard, the FortiManager administrator proactively initiates and, ultimately, performs the registration. When this method is used, the administrator must have specific details about the FortiGate device that they are registering.

You can launch the wizard from the **Device Manager** pane by clicking **Add Device** from the menu bar.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Device Manager—Viewing Authorized Devices

- **Device Manager** lists all authorized devices



NSE Training Institute

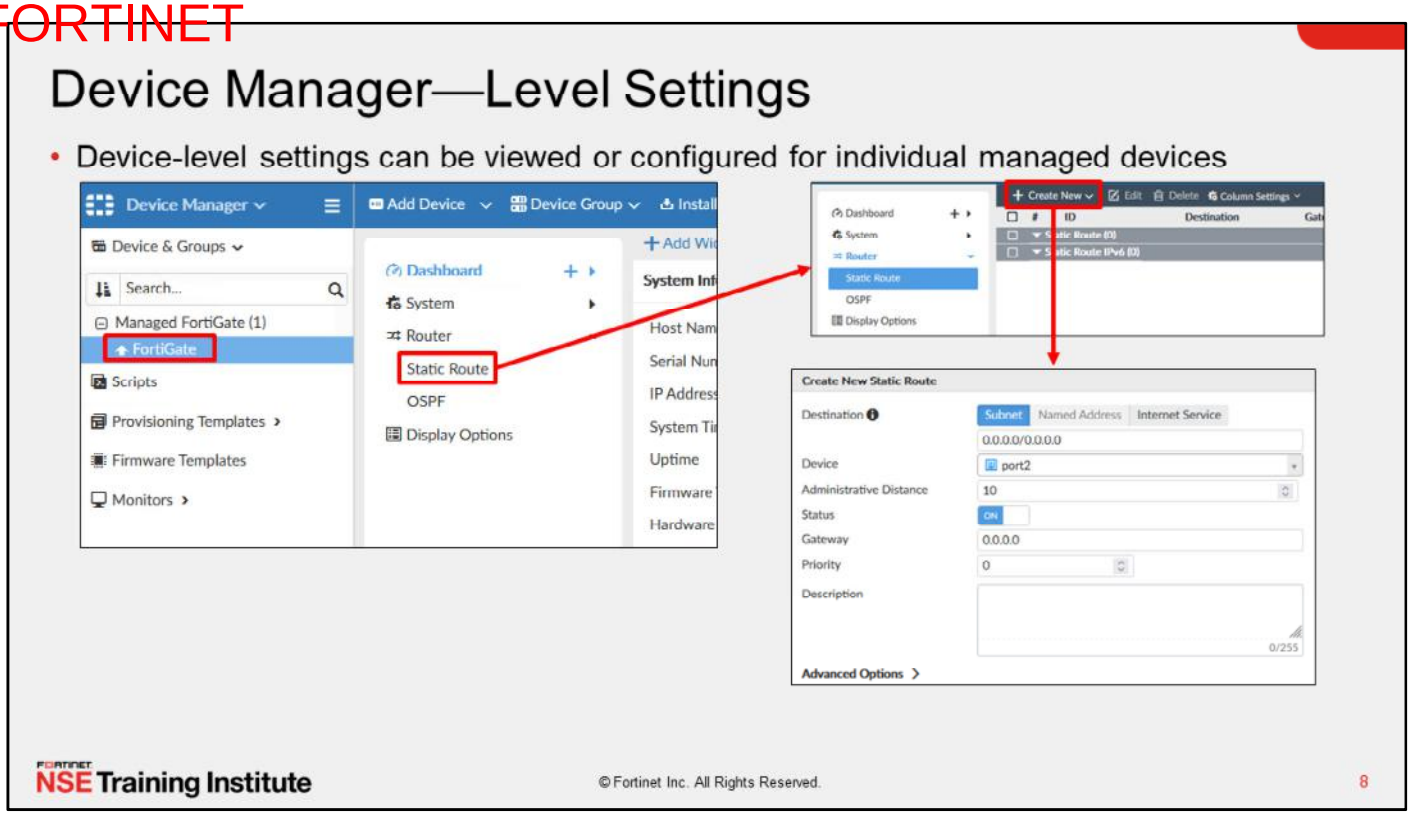
© Fortinet Inc. All Rights Reserved.

7

After you register a FortiGate device, it appears on **Device Manager** > **Device & Groups**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



To configure the device-level settings of your FortiGate devices, select the device or VDOM in the **Device Manager**. In the example shown on this slide, the FortiGate device named **FortiGate** is selected.

The device-level settings of a managed FortiGate can be viewed and configured from the toolbar at the top of the **Dashboard**. This enables you to view or configure interfaces, HA, DNS, and log settings, to name a few. To configure or view routes, click **Router** > **Static Route**.

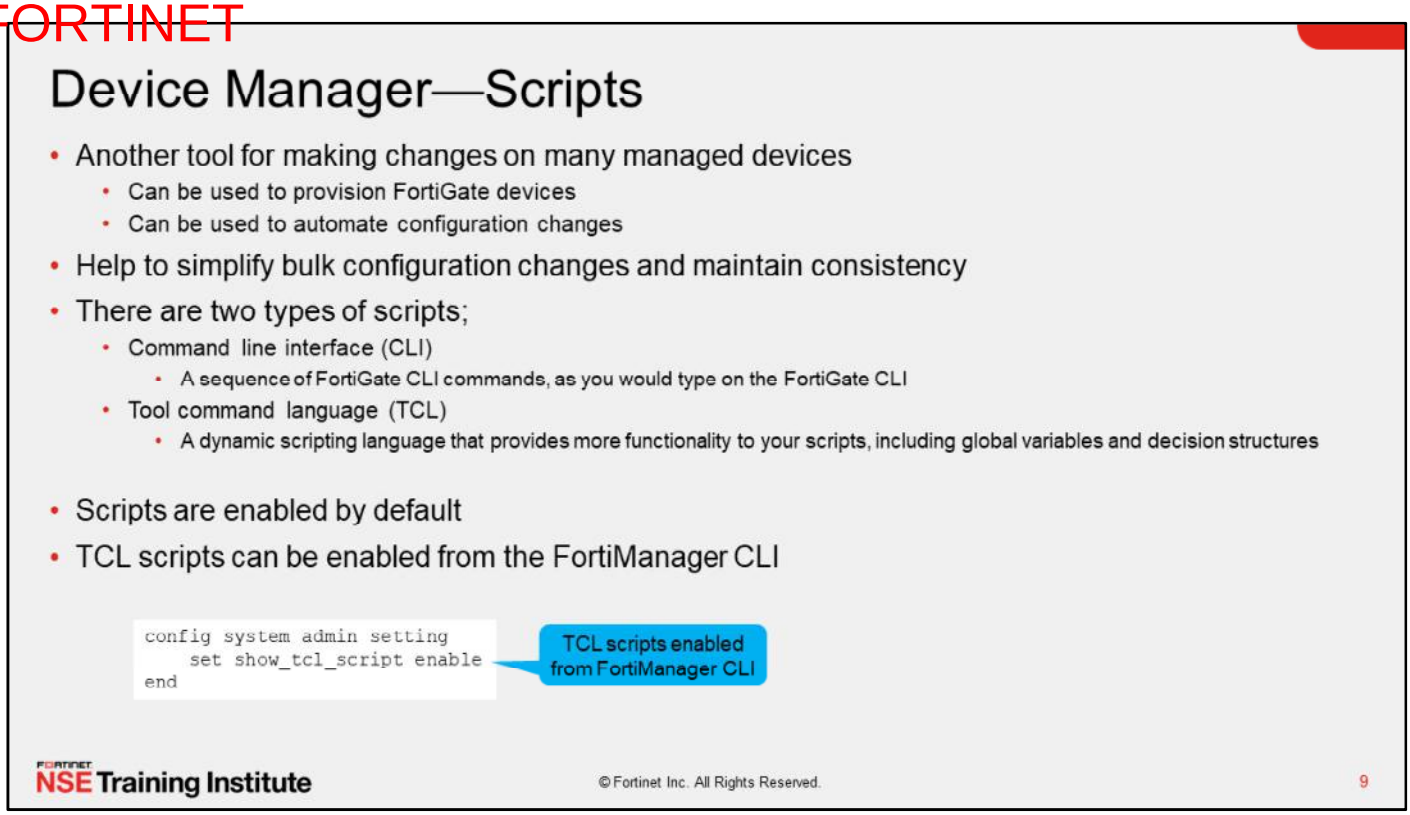
In the example shown on this slide, a new static route is created.

Most of the settings that you see in this example have a one-to-one correlation with the device configuration that you would see if you logged in locally using the FortiGate GUI or CLI.

Note that there are only a few options in the **Display Options** section to customize the global display as needed.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



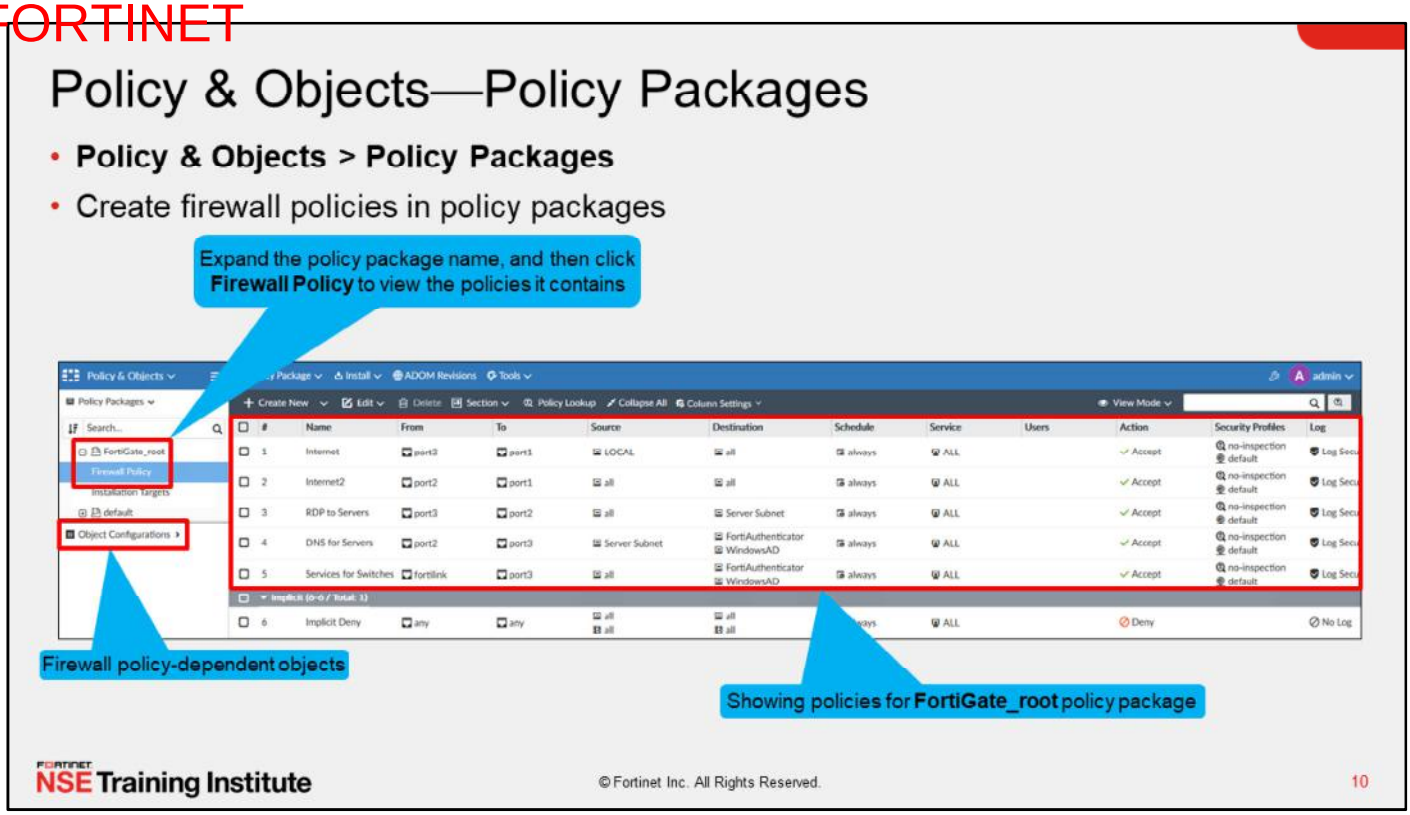
Another way to change device-level settings on devices is by using FortiManager scripts. Scripts are useful for bulk configuration changes and consistency across multiple managed devices.

FortiManager supports two types of scripts:
- CLI: CLI scripts include only FortiOS CLI commands as they are entered at the command line prompt on a FortiGate device.
- TCL: TCL is a dynamic scripting language that extends the functionality of CLI scripting. You must be familiar with the TCL language and regular expressions. For more information about TCL scripts, visit the official TCL website: http://www.tcl.tk

Scripts are enabled by default. For TCL scripts, you also need to enable the show command from the FortiManager CLI.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



If you want to edit the firewall policies and dependent objects on FortiManager, you go to the **Policy & Objects** pane.

FortiManager organizes firewall policies in policy packages. You can then customize the policy packages for each device or VDOM, or apply a single policy package for multiple devices that require the same set of firewall policies.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

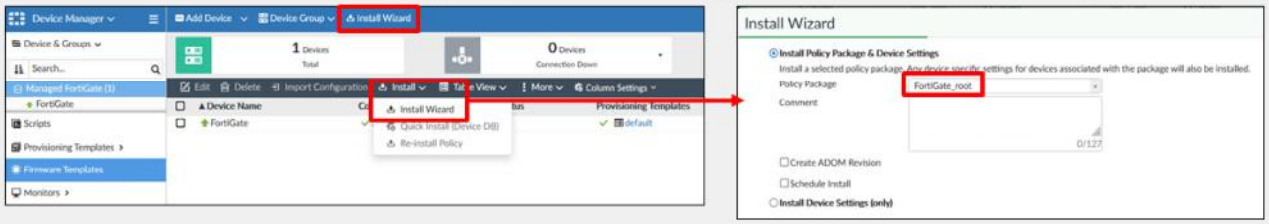
Device Manager—Install Wizard

- Installs settings on one or more FortiGate devices
- Two options on **Install Wizard**

Install Device Settings (only)
- Install only device settings for a select set of devices
- Policy and object changes are not installed

Install Policy Package & Device Settings
- Install a selected policy package
- Any device-specific settings for devices associated with the package are also installed

- Launch the **Install Wizard** from **Device Manager**
- Select **Install Device Settings (only)** or **Install Policy Package & Device Settings**



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

11

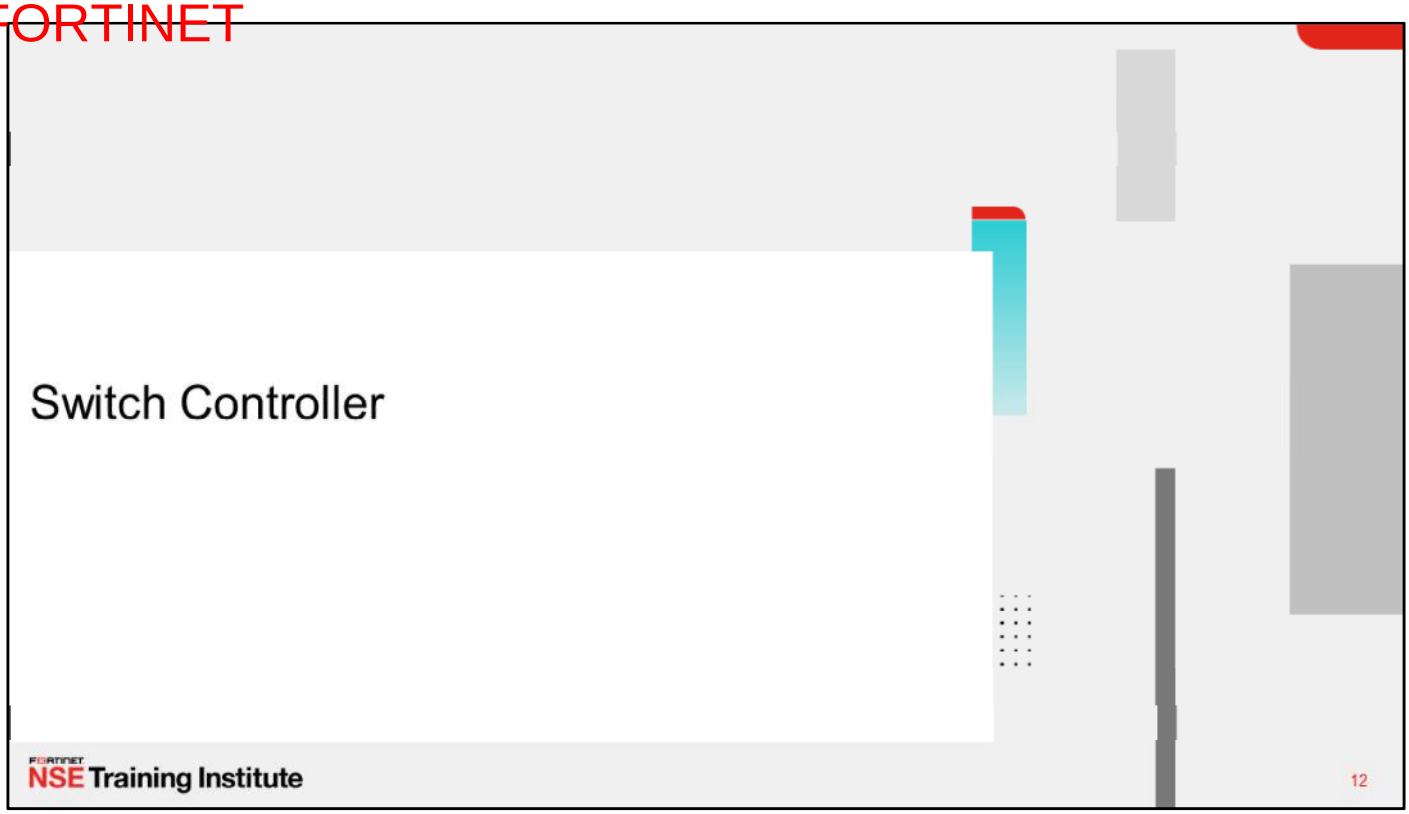
After you configure the FortiGate device-level settings and firewall policies on FortiManager, the changes do not take immediate effect—they must be *installed*. Therefore, you must install the changes to FortiGate by using the **Install Wizard** on **Device Manager**.

During installation, you must choose between two different installation types. If you choose **Install Device Settings (only)**, the wizard installs only device-level configuration changes made from FortiManager. If you have made changes to the device-level configuration and policies in the policy packages, you can choose **Install Policy Package & Device Settings**, which installs policy package changes and any device-level settings.

In the example shown on this slide, the **Install Policy Package & Device Settings** option is selected, which also requires choosing the policy package to install.

Vouchers & Dumps are Available | WhatsApp +201224560923

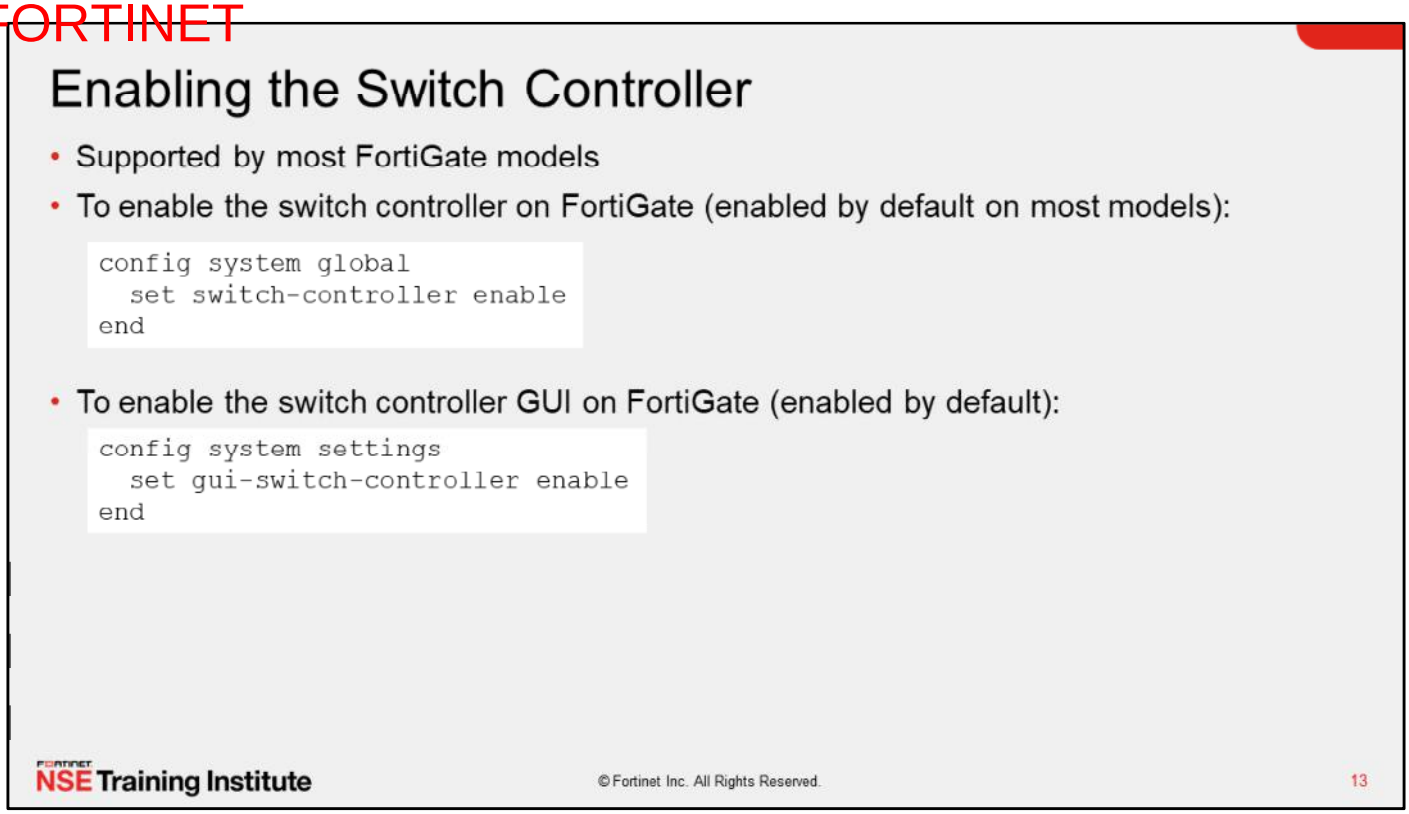
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn how to enable the switch controller feature.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

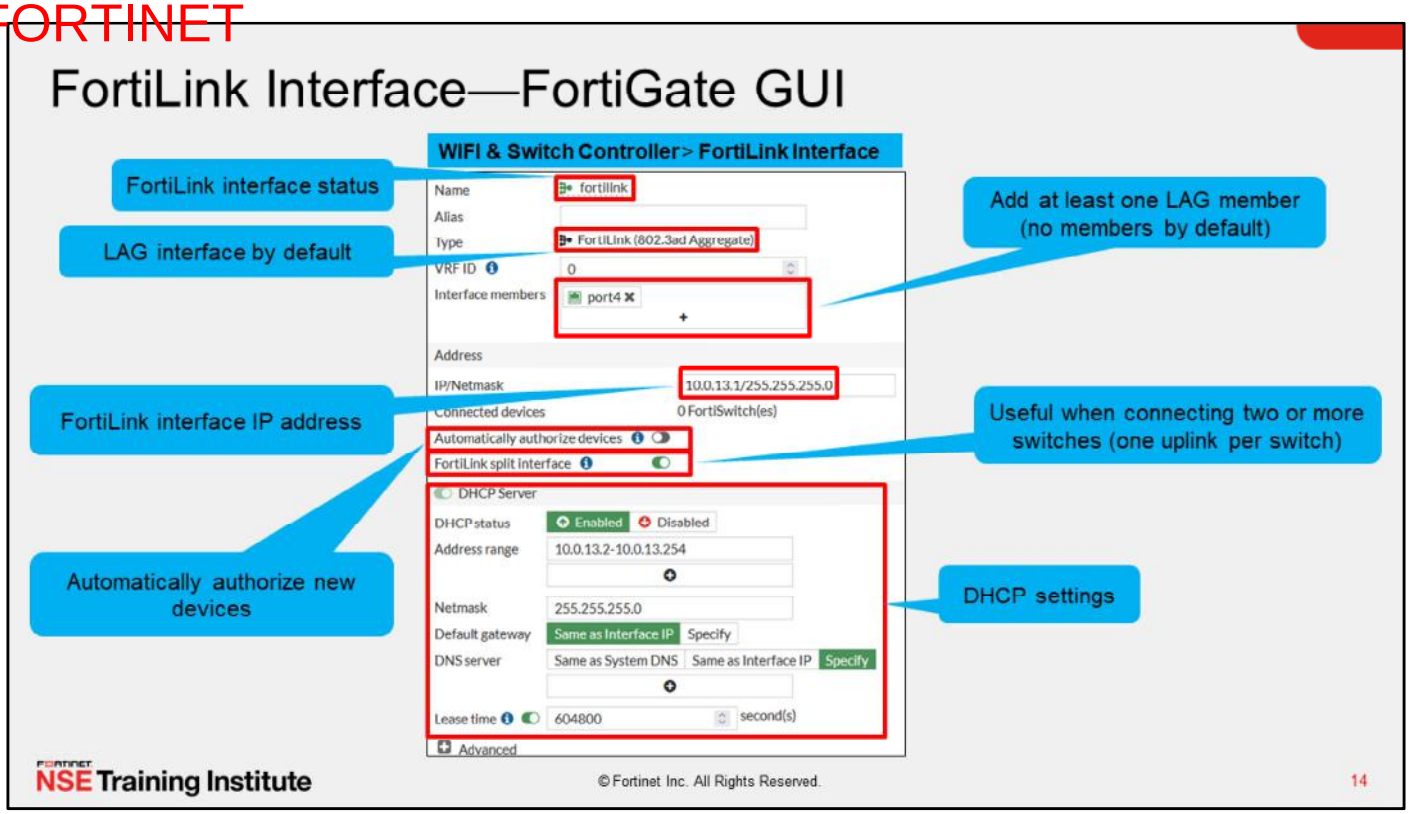


By default, the switch controller feature is enabled on most FortiGate models. In FortiGate VM models, however, it is not enabled by default, but you can enable it by running the CLI commands shown on this slide.

After you enable the switch controller feature, the related switch controller settings are shown on the GUI by default. If the GUI settings are not shown, make sure `gui-switch-controller` is enabled under system settings.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



All FortiGate devices come with a factory default FortiLink interface in the root VDOM dedicated to communication between the switch controller (FortiGate) and the managed switches. By default, the interface is created as a link aggregation group (LAG) interface.

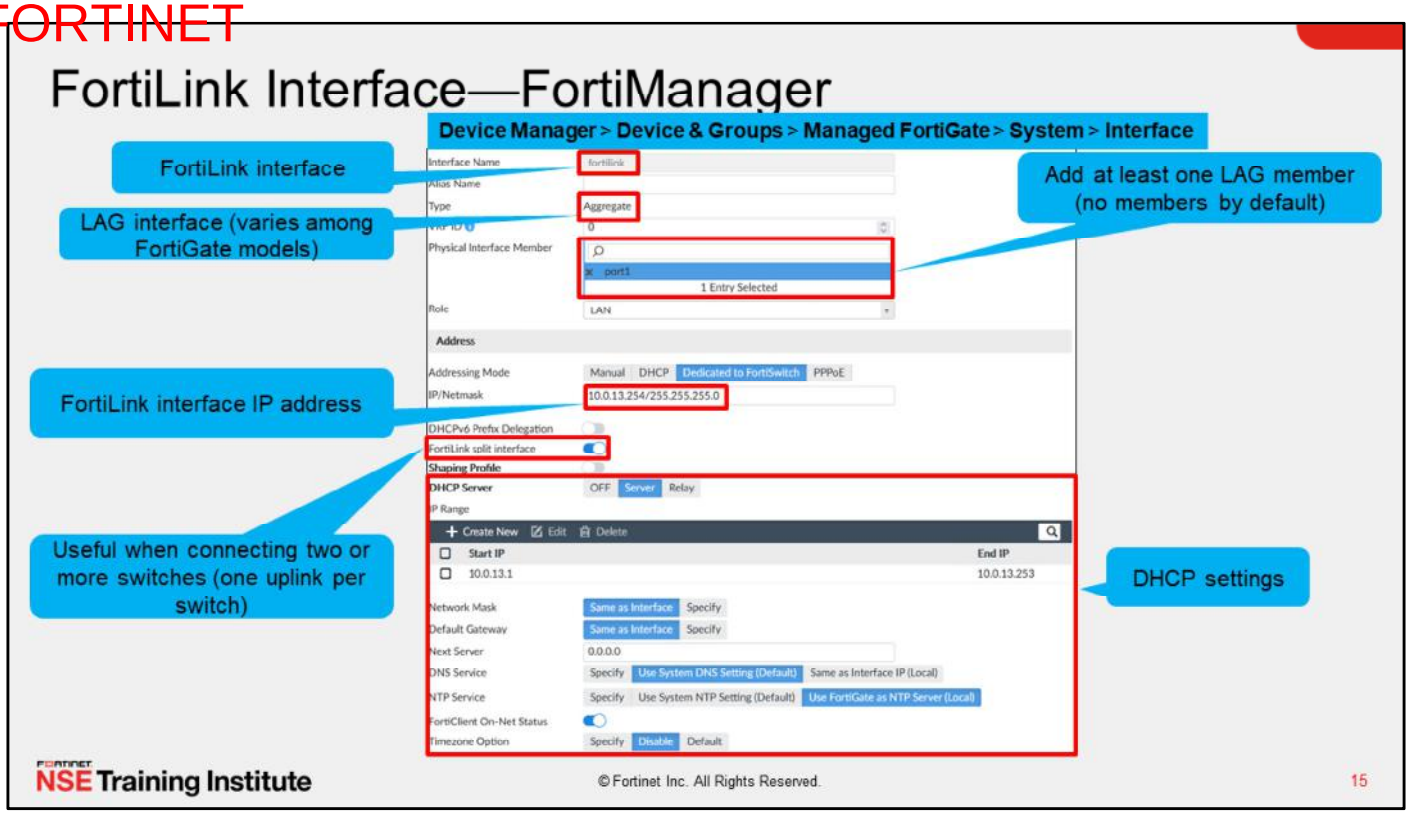
The FortiLink interface comes with no LAG members by default. Therefore, you must add at least one member to the FortiLink LAG interface and assign an IP address to it. FortiGate then uses the configured IP address and netmask to configure a DHCP scope for assigning IP addresses and other network parameters to managed switches.

By default, you must authorize the switches discovered by FortiGate before being able to manage them. Alternatively, you can enable **Automatically authorize devices** to automatically authorize discovered switches.

In addition, **FortiLink split interface** is enabled by default. If a FortiLink interface has two or more members, this option instructs FortiGate to keep only one FortiLink interface port member active. This behavior is useful when you connect your FortiLink interface from one FortiGate device to two or more switches, and the switches do not support multi-chassis link aggregation (MCLAG) or MCLAG has not been configured yet. Under this scenario, you lose management to one or more switches if FortiLink split interface is disabled. You will learn more about FortiLink in another lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

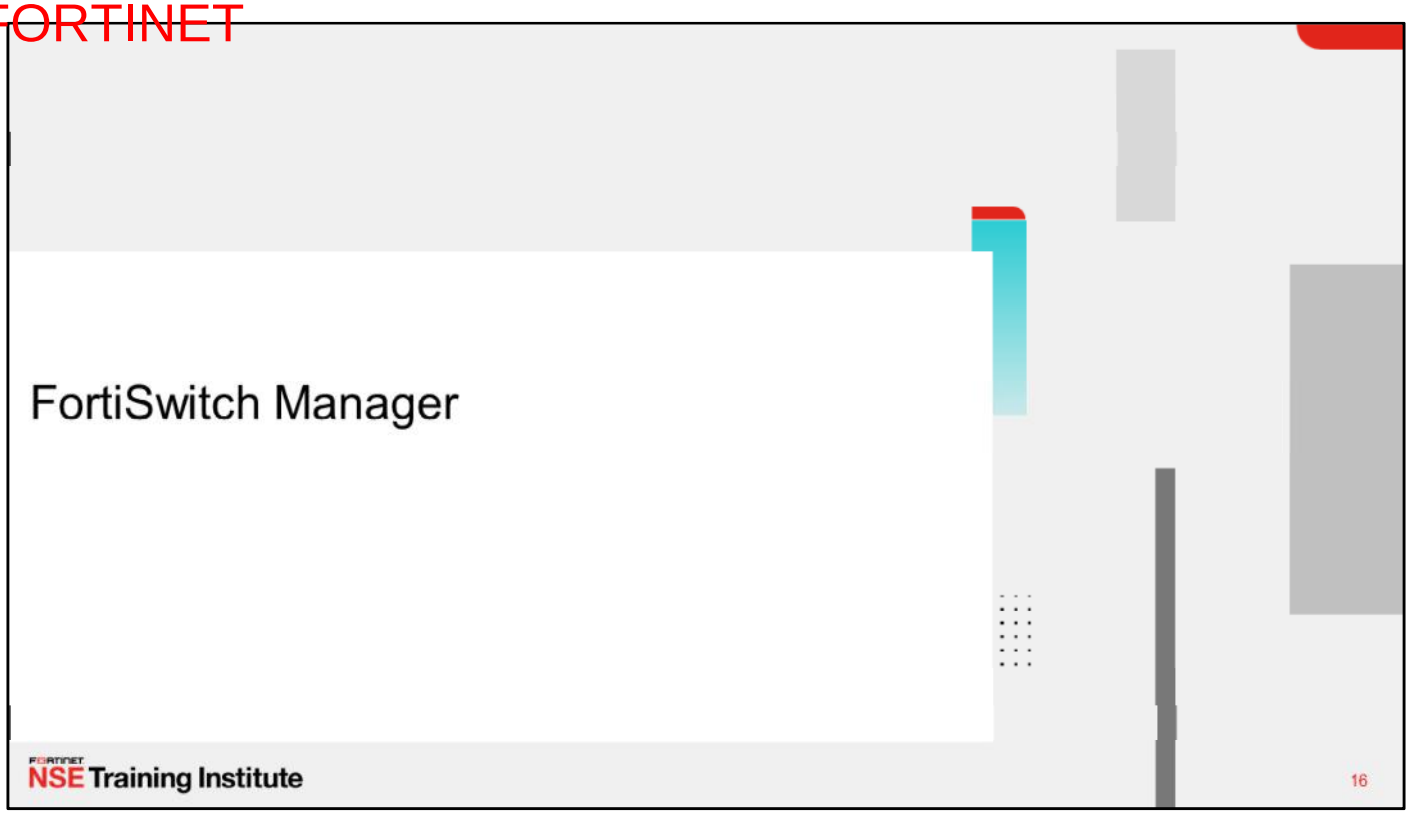


You can also edit the FortiLink interface on FortiManager by accessing the device interface settings on **Device Manager**.

The layout and options available on FortiManager are very similar to the ones displayed by the FortiGate GUI. The option **Automatically authorize devices** you see on FortiGate is not available on FortiManager, but you can use scripts or CLI-only objects to configure the setting.

Vouchers & Dumps are Available | WhatsApp +201224560923

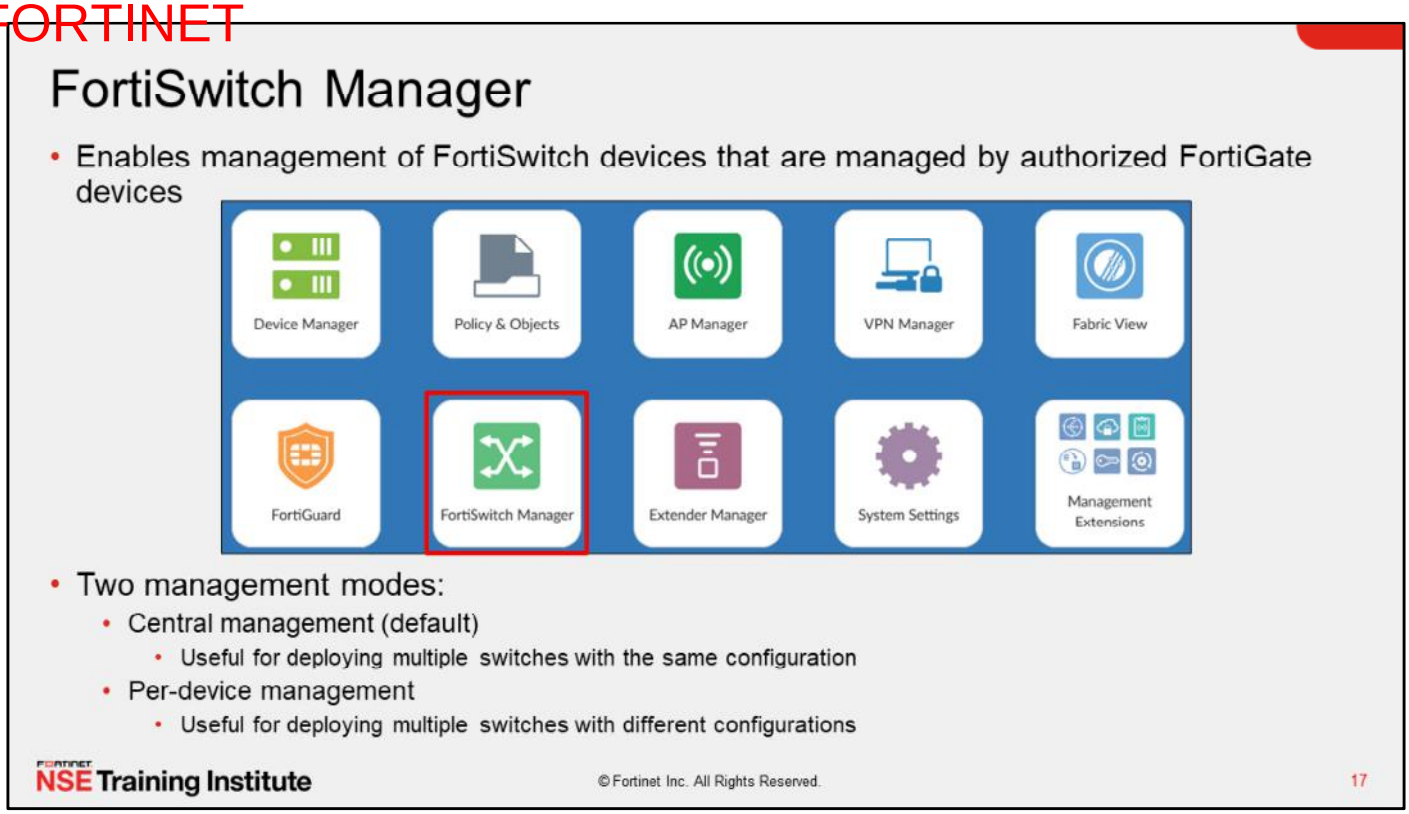
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn about the FortiSwitch Manager pane, which enables you to manage FortiSwitch devices on FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiGate can act as a switch controller, which enables you to manage FortiSwitch devices from FortiGate rather than having to individually access each FortiSwitch for management purposes.

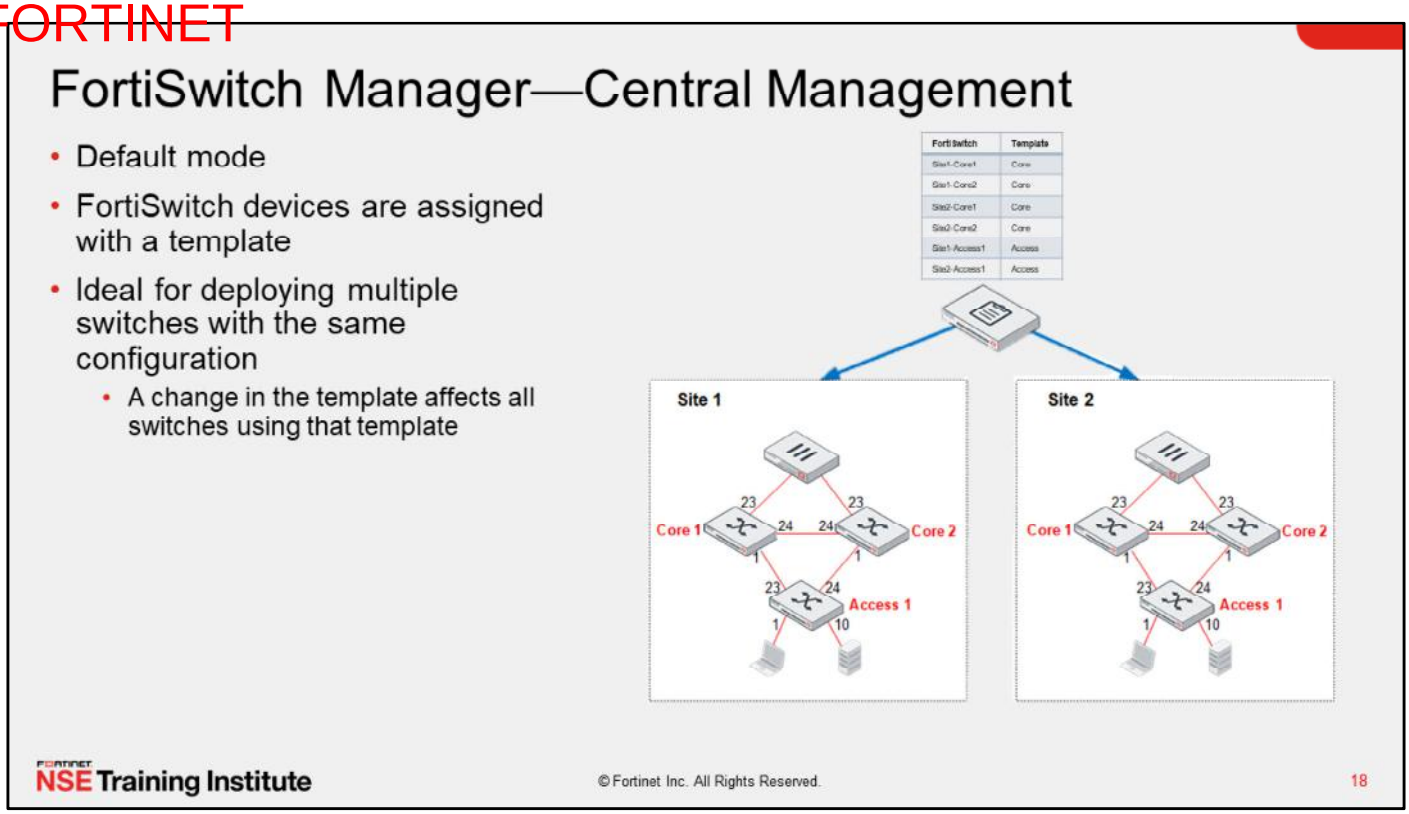
On FortiManager, when you register a FortiGate device acting as a switch controller, the FortiSwitch devices that are discovered by FortiGate are also used by FortiManager and displayed on the **FortiSwitch Manager** pane.

FortiSwitch Manager enables you to centrally manage FortiSwitch devices discovered by all authorized FortiGate devices on FortiManager. Instead of accessing each FortiGate device to manage its FortiSwitch devices, you can manage all FortiSwitch devices controlled by all FortiGate devices from a single pane on FortiManager. This can considerably reduce the operating expenses for your network, especially for large networks that have tens or hundreds of switches deployed.

FortiSwitch Manager supports two management modes: central management and per-device management. In central management mode (default mode), you maintain templates and assign them to FortiSwitch devices. Central management mode is convenient for deploying multiple devices that use the same configuration. In per-device management mode, you apply settings and profiles to individual FortiSwitch devices, which enables you to deploy sites that use different configurations.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



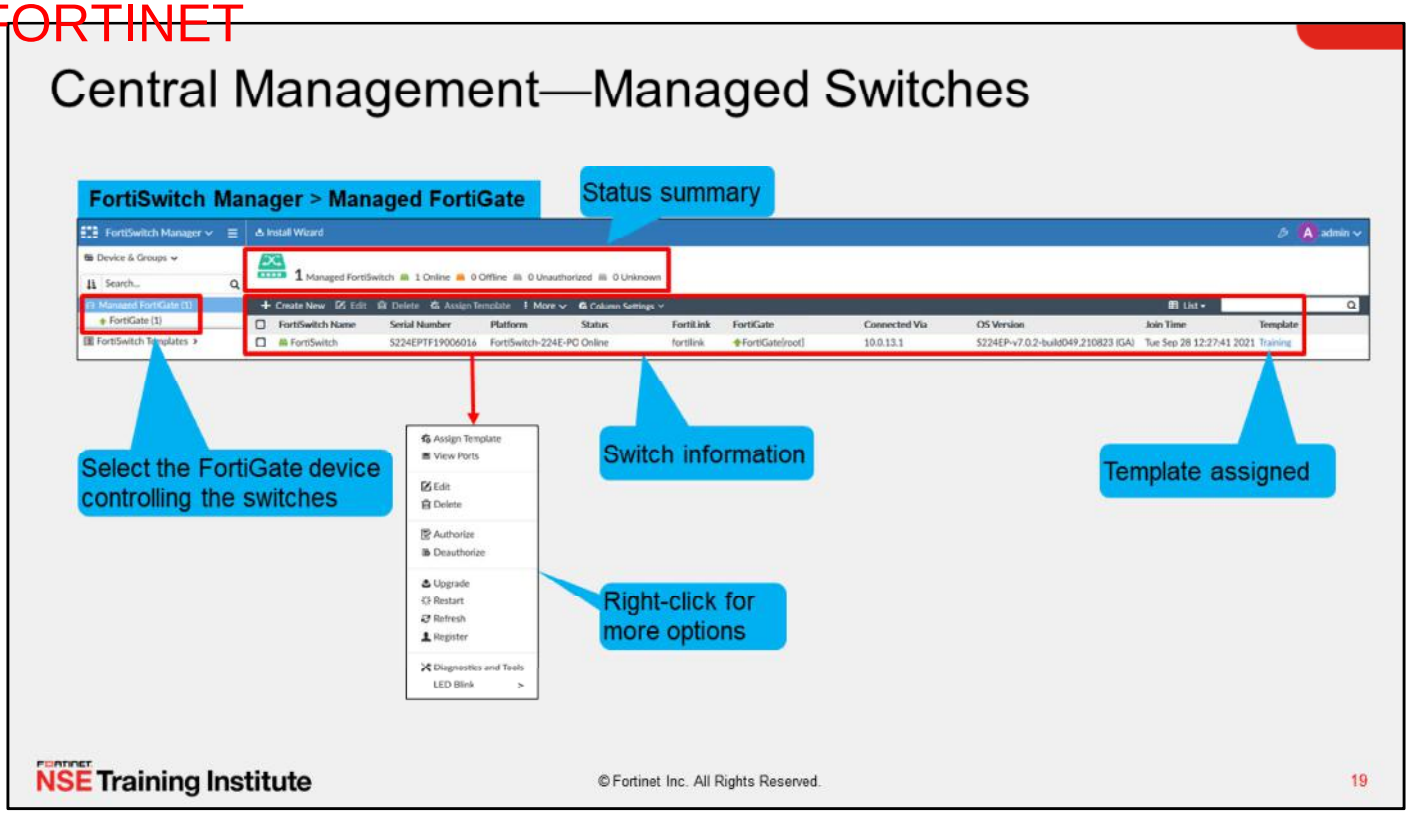
Central management mode is the default mode used by FortiSwitch Manager. You first configure a template and then assign it to one or more FortiSwitch devices that require the same deployment. You make configuration changes on the template, instead of on the individual FortiSwitch devices. Changes made on a single template result in a configuration change on multiple devices. For this reason, central management mode is best suited for deployments that use the exact same configuration on all FortiSwitch devices.

A FortiSwitch template is specific to a FortiSwitch model, and therefore, different switch models require different templates.

In the example shown on this slide, site 1 and site 2 have identical network topologies. FortiManager is configured with two FortiSwitch templates: core and access. The core template is assigned to devices acting as a core switch on site 1 and site 2, while the access template is applied to devices acting as access switches. The result is that you can manage six switches across two sites with only two templates. If you need to deploy more identical sites, you can continue to use the same existing templates, resulting in even greater scalability.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



When you access the **FortiSwitch Manager** pane, the managed switches page opens by default. This page displays a table containing all the switches discovered by all FortiGate devices registered on FortiManager. For each authorized switch, the page displays its name, serial number, model (or platform), the current status, the FortiLink interface used (on the controlling FortiGate), the controlling FortiGate and VDOM, IP address (connected via), OS version, and join time. This is the same information that you would see on the FortiGate GUI for a switch.

On the left menu, click **Managed FortiGate** if you want to view all switches discovered by all FortiGate devices. Otherwise, click the FortiGate device that controls the switches you want to view. The page lists all discovered FortiSwitch devices, including those that have not been authorized. Each switch displays an icon to the left of its name that reports its current status, which is obtained by FortiManager by polling FortiGate REST API every three minutes. The different statuses mean:

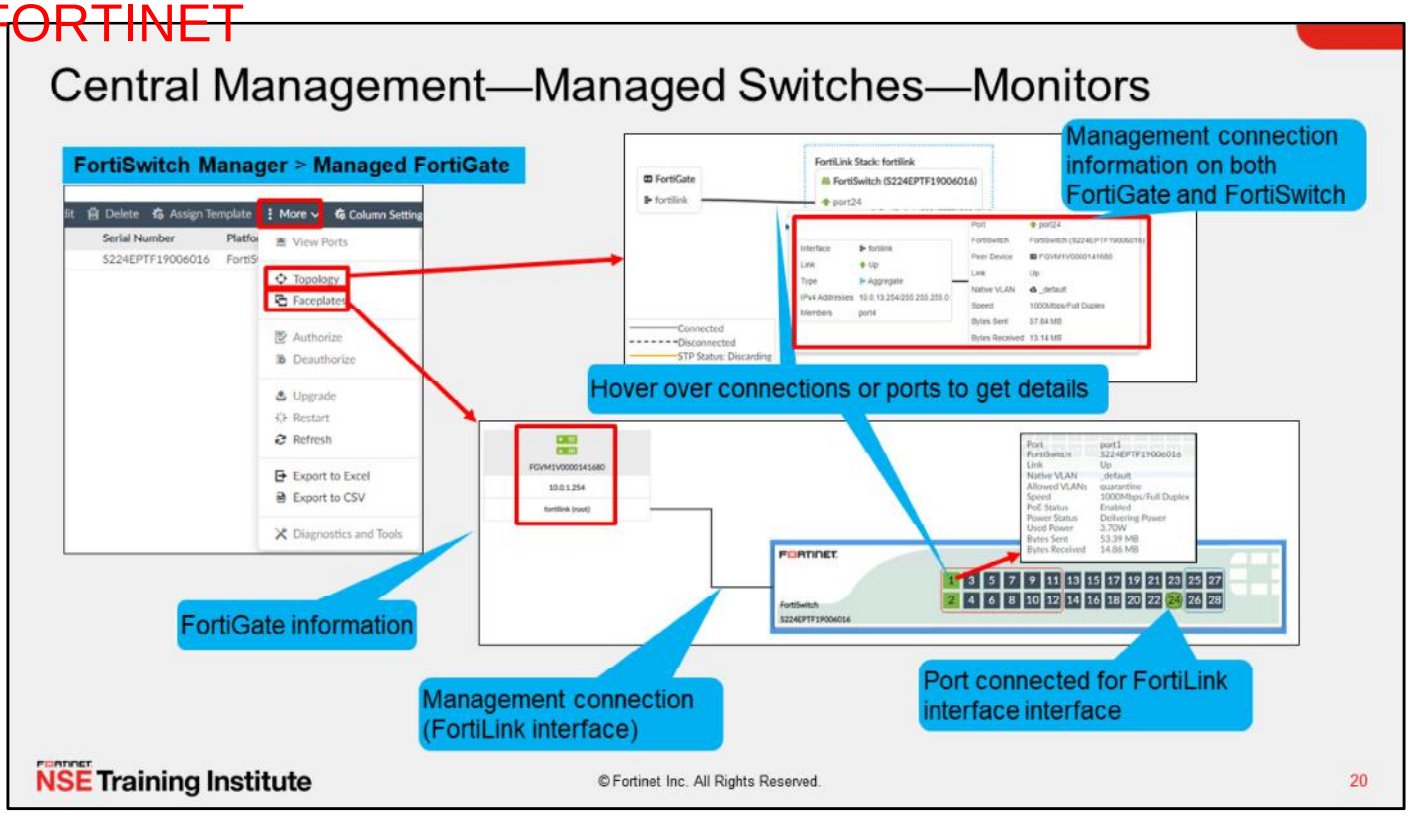
- **Online**: The switch is authorized and the management link with FortiGate is up.
- **Offline**: The switch is authorized but the management link with FortiGate is down.
- **Unauthorized**: The switch has been discovered by FortiGate, but it has not been authorized.
- **Unknown**: The switch is authorized but its status cannot be determined. This is usually the case when the controller (FortiGate) is also offline.

The page also displays the template that has been assigned to the switch. On the example shown on this slide, the switch has been assigned with the **Training** template and its status is **Online**.

When you right-click a switch, a menu with additional management actions, such as switch authorization or firmware upgrade, is displayed.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



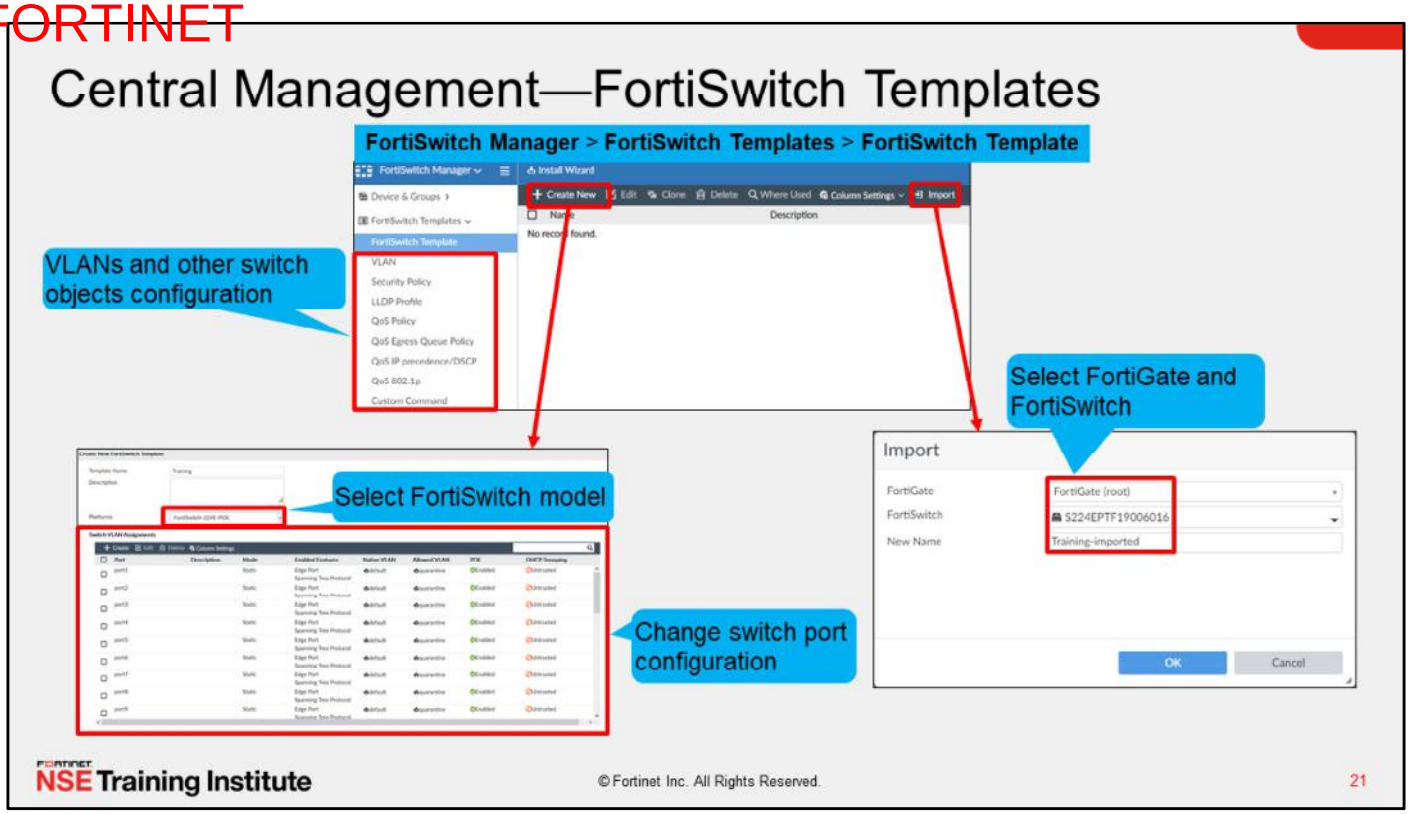
When you click the **More** tab on the **Managed FortiGate** page, you can click **Topology** to view the block-style topology representation of the connected FortiSwitch devices. On the topology, you can hover over connection links or ports to get more details.

Another monitor tool you can click on is **Faceplates**. Faceplates displays a diagram of the management connection between FortiGate and its controlled FortiSwitch devices. It also displays the status of each port on the managed switches. The FortiGate interface used for managing switches is called *FortiLink*. FortiLink is also the name of one of the protocols used by FortiGate for switch management. The protocol operates over the switch uplink connected to FortiGate, and between switches for switch discovery. You will learn more about FortiLink in another lesson. On the diagram, the switch port connected to the FortiLink interface is circled in black (port24 in the example shown on this slide).

Both monitor tools display some information about the FortiGate device controlling the switch. The information includes the serial number, management IP address, as well as the VDOM and the FortiLink interface name. In the example of faceplates shown on this slide, the FortiLink interface name is **fortilink** and it belongs to the **root** VDOM. Also note that the FortiGate management IP address refers to the IP address that FortiManager uses to communicate with FortiGate through the secure tunnel on TCP port 541.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The **FortiSwitch Templates** section is where you configure the templates, VLANs, and other switch object configurations for FortiSwitch devices. You can create a new template from scratch by clicking **FortiSwitch Template** on the left menu, then clicking **Create New**, and then selecting the FortiSwitch model the template will be based on. After you select the FortiSwitch model, FortiManager automatically populates the template with the ports available in the selected switch model. In addition, FortiManager assigns a default configuration to each switch port, which you can then change to suit your needs.

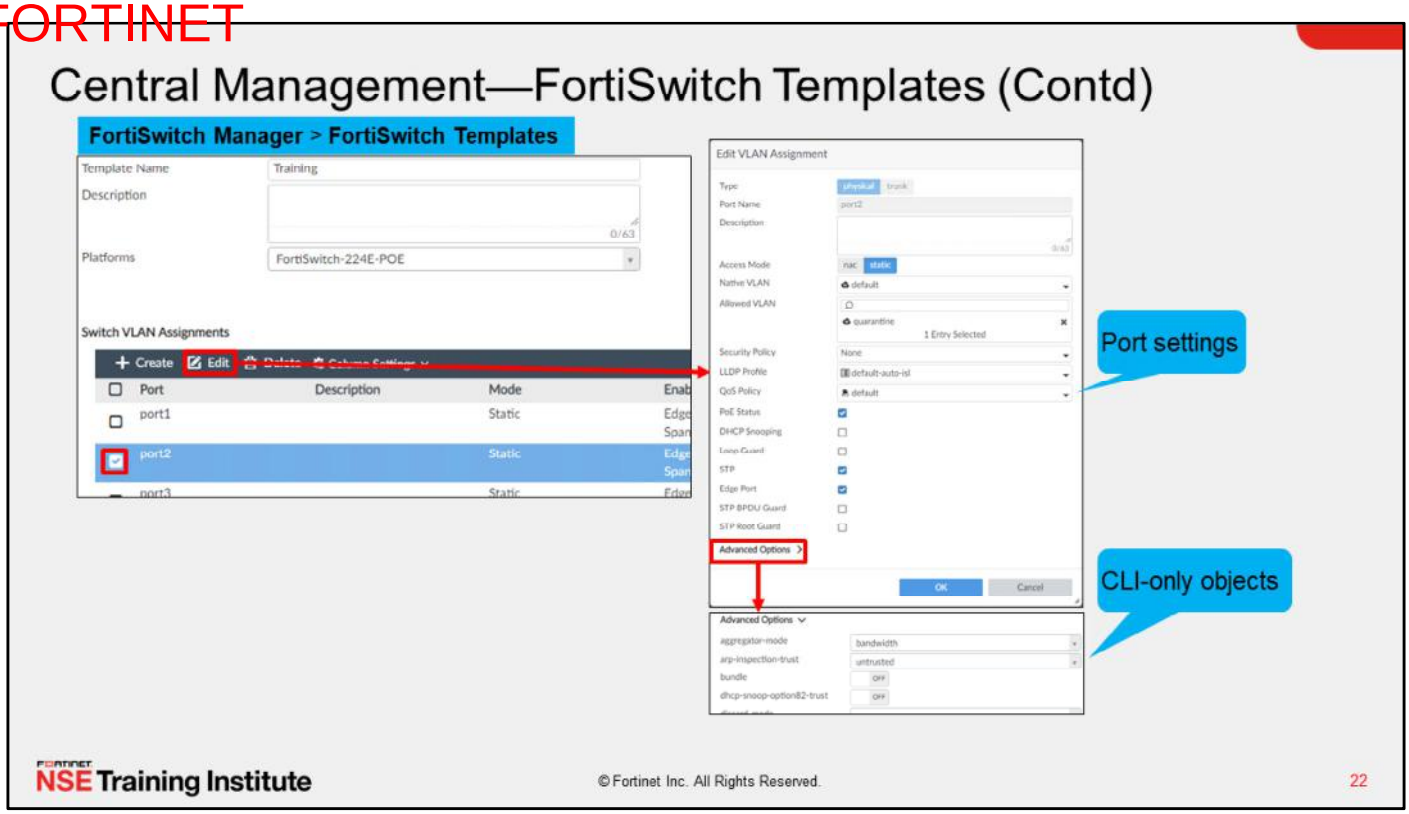
Another way to create a template is by importing its settings from the current configuration on a switch. This option is useful when you want to build your template from the existing configuration on a production switch, and then apply that configuration to other switches that require the same setup. To import a template, click **Import**, and then select the FortiGate device and the switch you want to import the template settings from.

Before you create the template, you may want to configure the objects used by the template:

- **VLAN**: A FortiSwitch VLAN is a FortiGate VLAN interface bound to the FortiLink interface. The VLANs can then be selected as the native VLAN and allowed VLANs on a switch port.
- **Security Profiles**: FortiSwitch supports 802.1X authentication. You configure the 802.1X authentication policy in a security profile, and then assign the security profile to a switch port in the template.
- **LLDP Profiles**: FortiSwitch supports Link Layer Discovery Protocol (LLDP) and its extension LLDP for Media Endpoint Discovery (LLDP-MED). An LLDP profile enables you to configure the type length values (TLVs) to advertise on a port, as well as the LLDP-MED network policy used for auto VLAN configuration on endpoints (usually phones).
- **QoS Policy**: FortiSwitch supports quality of service (QoS) policies, which enable you to classify and mark packets entering a port for egress priority queuing purposes.
- **Custom Command**: Some FortiSwitch settings and diagnostic commands are available on the FortiSwitch device only by creating custom commands.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



To configure a port on a template, click **Edit** to modify the port settings. FortiManager displays a new window showing the port settings. From there, you can select the native and allowed VLANs on the port, as well as change its LLDP profile or security policy. You can also change some STP settings.

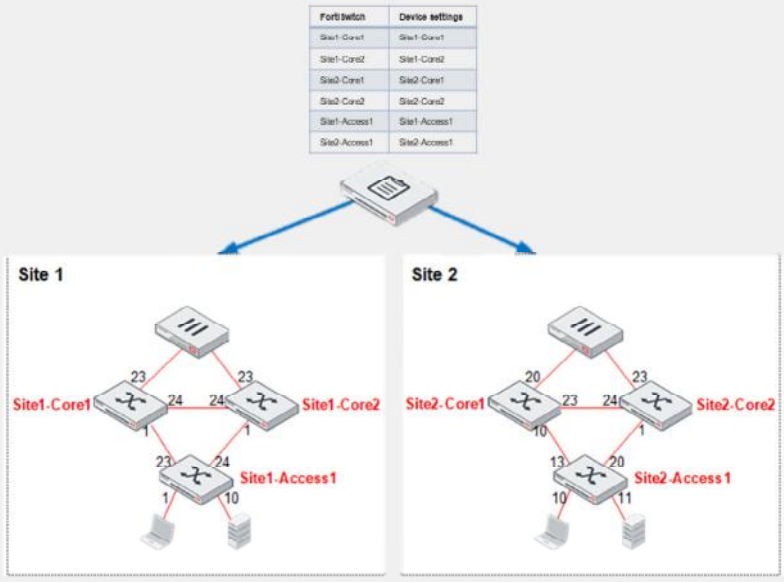
If you click **Advanced Options**, FortiManager shows the additional CLI-only objects available for the port.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiSwitch Manager—Per-Device Management

- Configuration is maintained on a per-device basis
- Ideal for deploying switches with different configurations
  - A change in the switch configuration affects only that switch



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

23

Per-device management is the alternative mode available for FortiSwitch Manager. Unlike central management mode, in which you configure templates, in per-device management mode you configure FortiSwitch devices in the same way you would if you were configuring them on the FortiGate GUI.

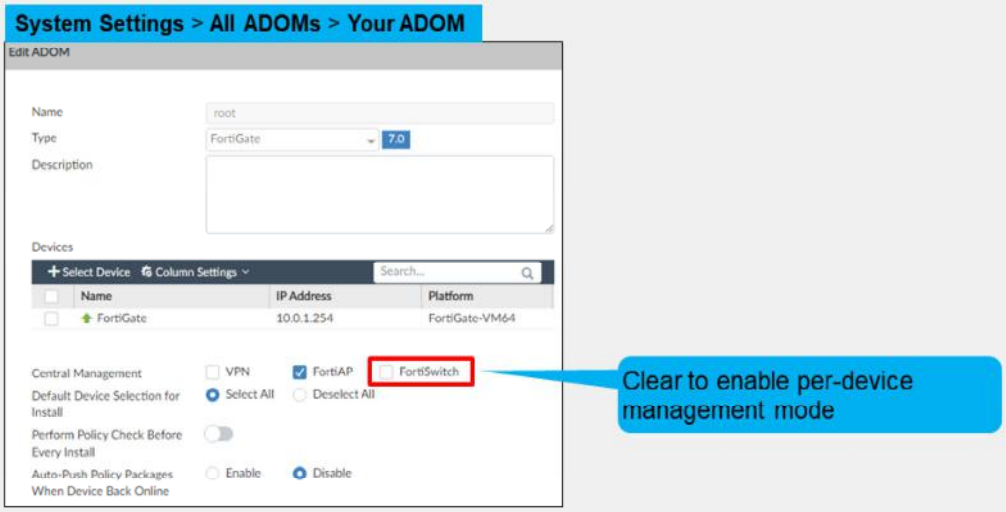
The advantage of per-device management mode is that you can configure each switch differently. This makes it an ideal option when you need to deploy switches that don't necessarily require the same setup. In addition, because FortiManager maintains separate device settings for each switch, any changes made on a switch affect only that switch.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiSwitch Manager—Per-Device Management (Contd)

- Clear the **FortiSwitch** option in ADOM settings to enable per-device management



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

24

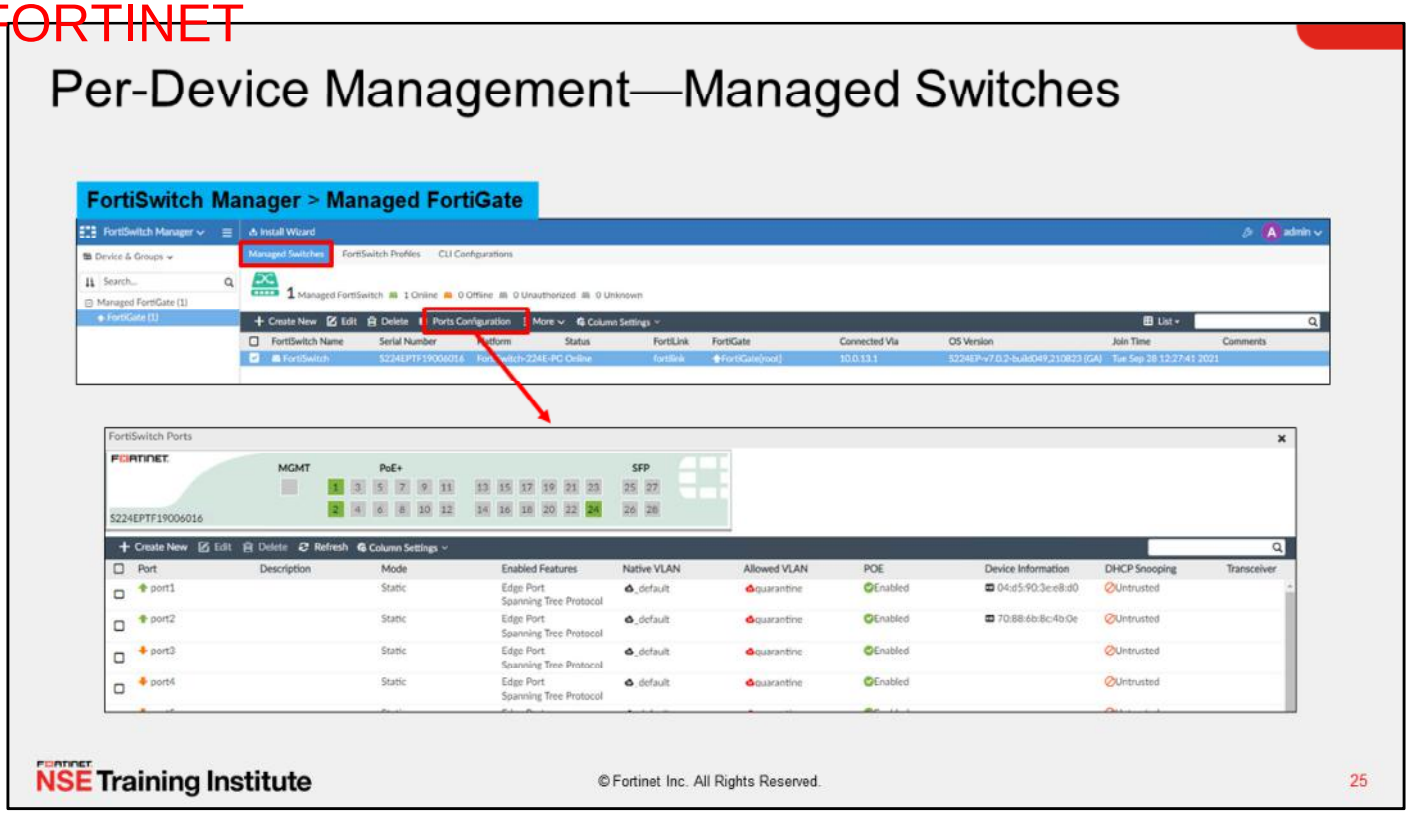
Central management mode is the default FortiSwitch Manager mode in an administrative domain (ADOM). ADOMs enable you to create groupings of devices for administrators to monitor and manage. The purpose of ADOMs is to divide administration of devices by ADOM and to control (restrict) administrator access.

To enable per-device management, you edit the settings of the ADOM you manage your FortiSwitch devices on, and you uncheck the **FortiSwitch** option.

In the example shown on this slide, **FortiSwitch** has been cleared on the **root** ADOM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

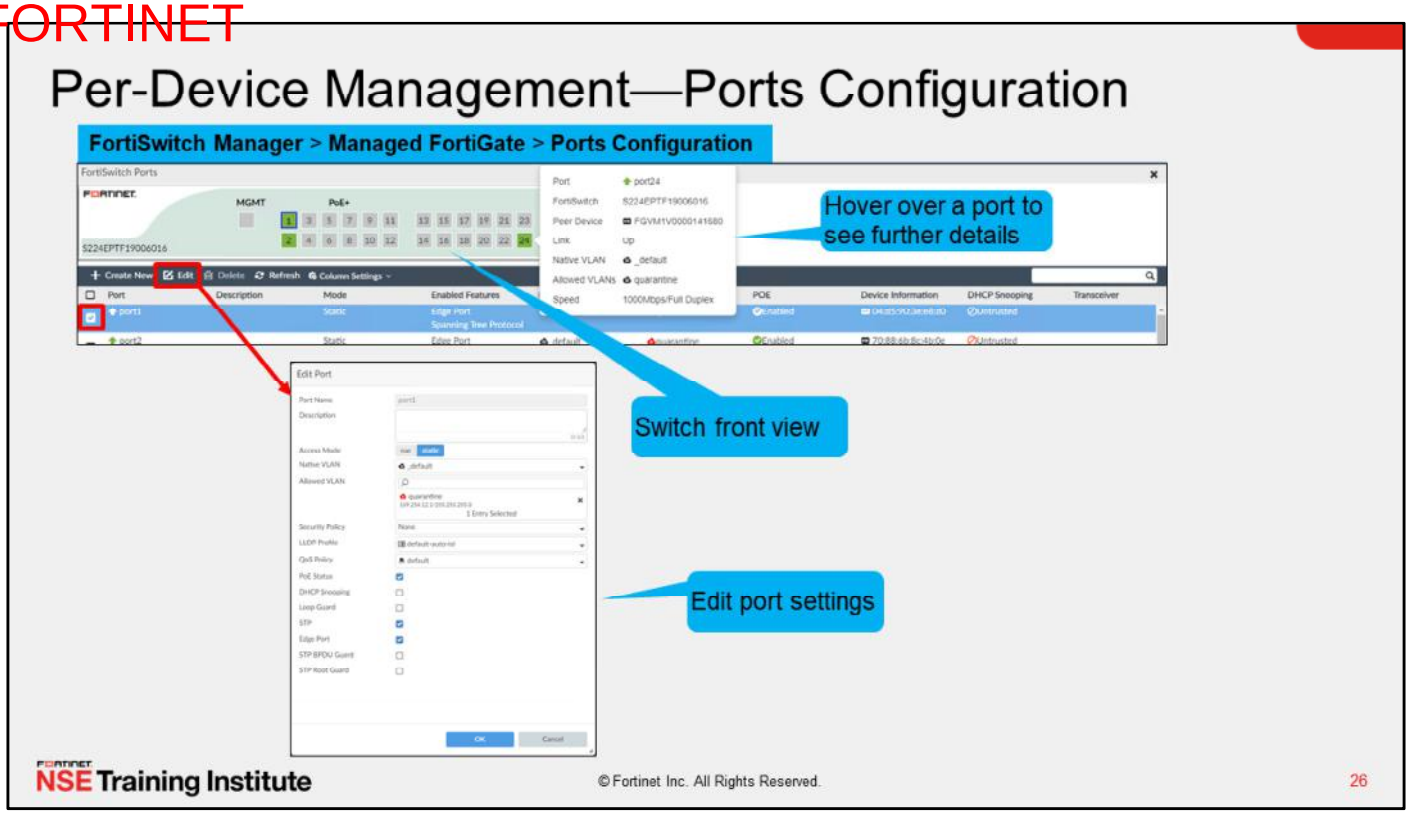


After you enable per-device management mode, you can click **Ports Configuration** to edit the port configuration of a switch instead of assigning a template to it. Also, the template column is no longer shown as part of the information displayed for a switch.

In addition, the FortiSwitch Manager pane shows a **FortiSwitch Profiles** tab. You can use the other tab, **CLI Configurations**, to access settings that are not available to configure directly within the FortiSwitch Manager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

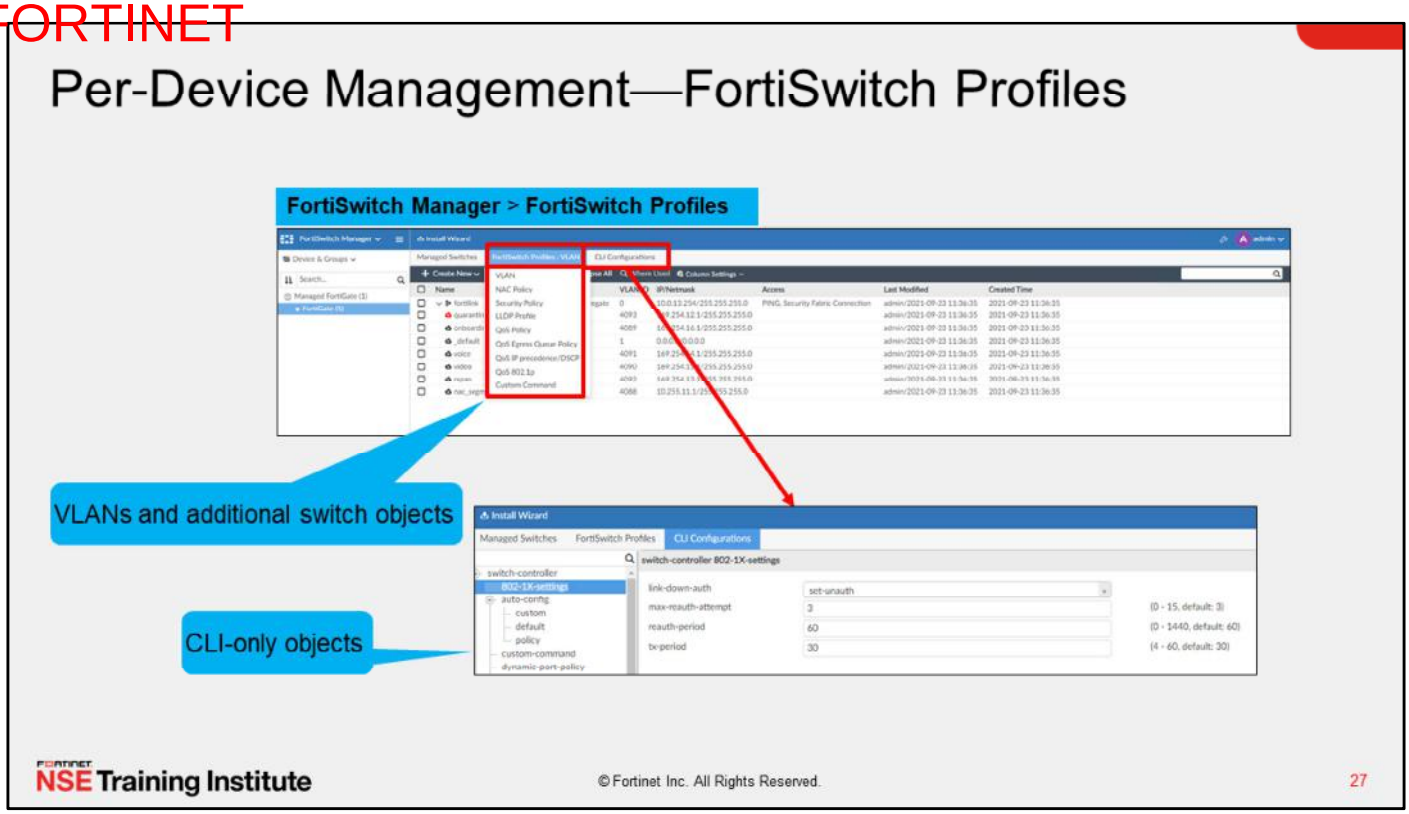


The **Ports Configuration** page displays all the ports available on the switch. From the page, you can view or edit the configuration of each port. Select a port and then click **Edit** to change its settings. After you click **Edit**, a new window opens showing the port settings available.

In addition, on the **Ports Configuration** page, FortiManager displays the switch front view, indicating the status of all ports on the switch. Hover over a port to see more information about it, such as its link status, the FortiSwitch device it belongs to, its assigned VLANs, or even the name of its peer device discovered through LLDP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



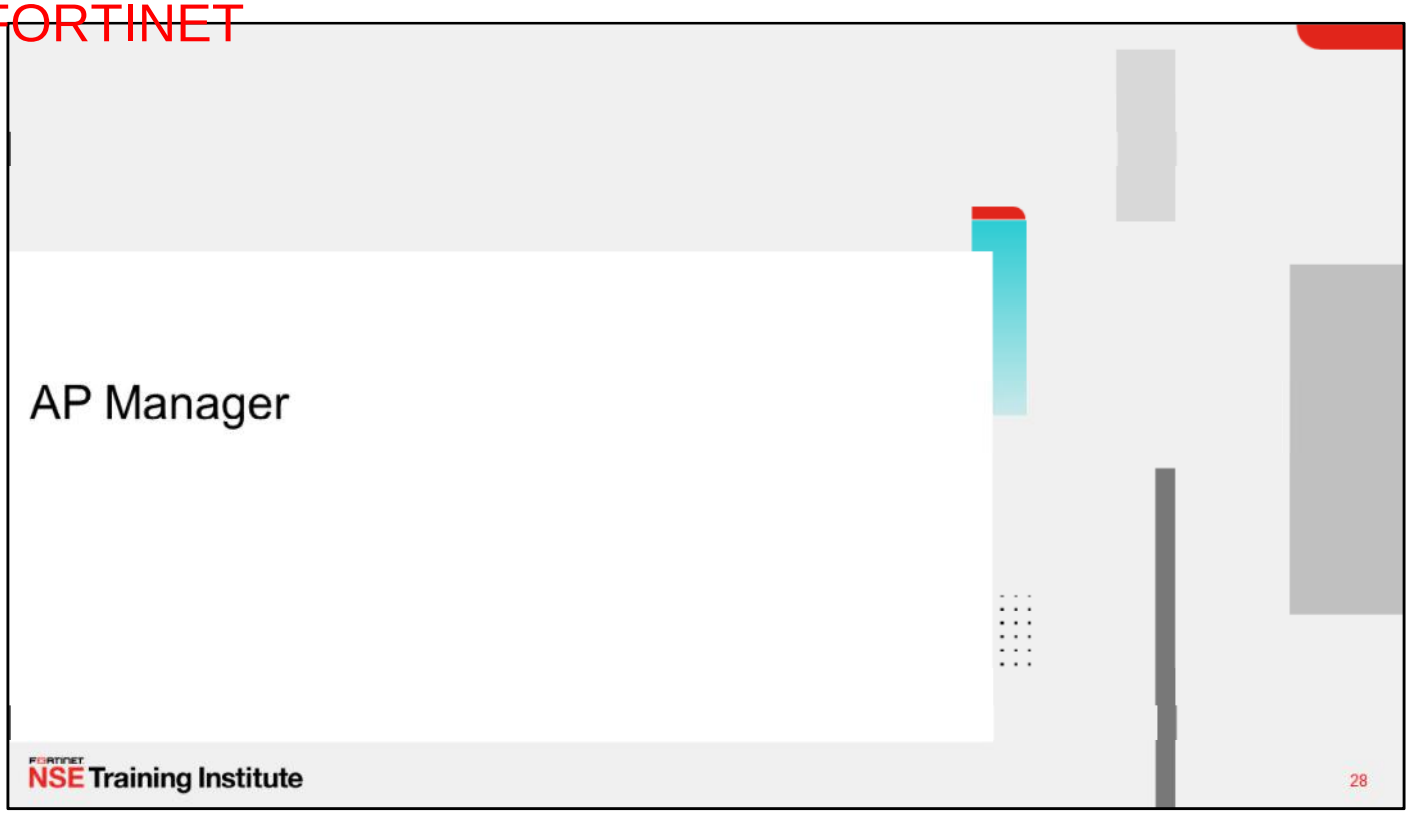
The **FortiSwitch Profiles** tab is where you configure additional switch objects. When compared to the FortiSwitch templates section, you find the same configuration objects plus **NAC Policy**.

Network access control (NAC) policies enable you to assign a VLAN and other settings to ports that connect to devices matching a certain criteria such as the MAC address, operating system, or type. The purpose is to automatically configure a switch port with the correct settings based on the type of device connected.

In addition, you can configure additional CLI-only objects on the switch by clicking the **CLI Configurations** tab.

Vouchers & Dumps are Available | WhatsApp +201224560923

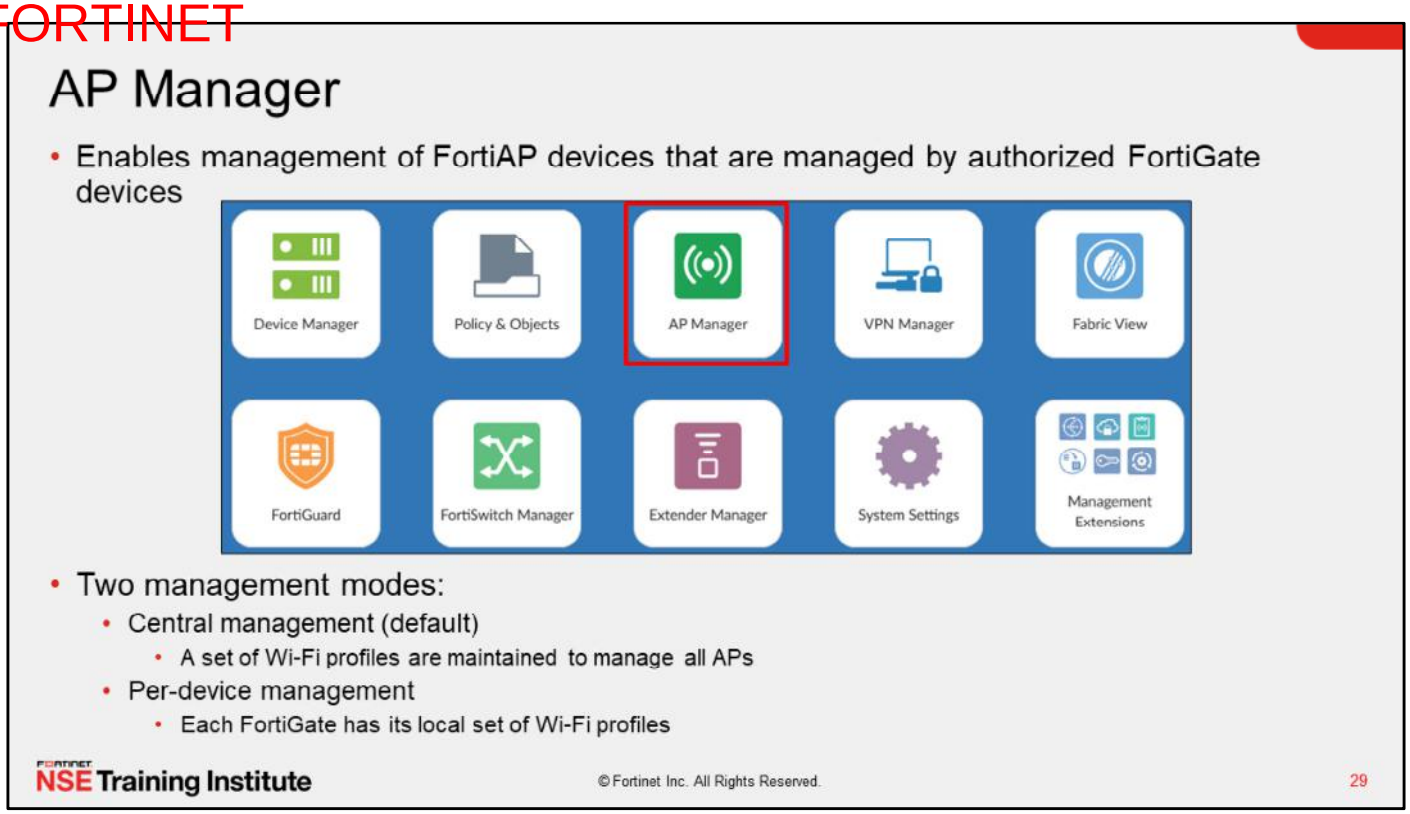
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn about the AP Manager pane, which enables you to manage FortiAP devices on FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



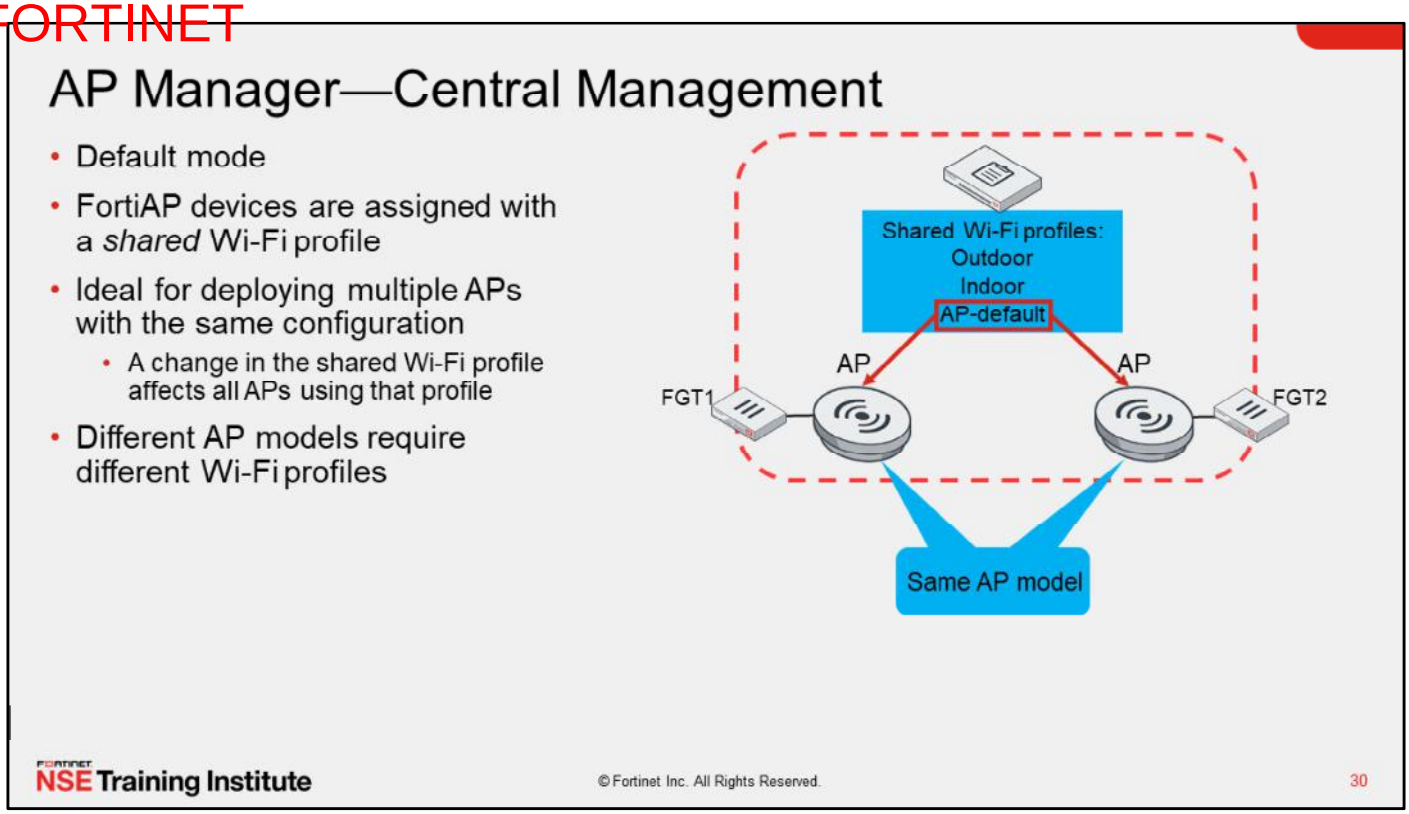
The **AP Manager** pane enables you to centrally manage FortiAP devices discovered by all authorized FortiGate devices on FortiManager.

AP Manager is very similar to FortiSwitch Manager. For example, AP Manager supports two management modes: central management and per-device management. In central management mode (default mode), you maintain a set of shared Wi-Fi profiles and assign them to FortiAP devices, which makes it an ideal mode for deploying multiple devices that use the same configuration. In per-device management mode, each FortiAP has its own set of Wi-Fi profiles, which are not shared with other APs.

Because the information displayed and the options available in AP Manager are very similar to the ones in FortiSwitch Manager, the lesson focuses on the differences.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



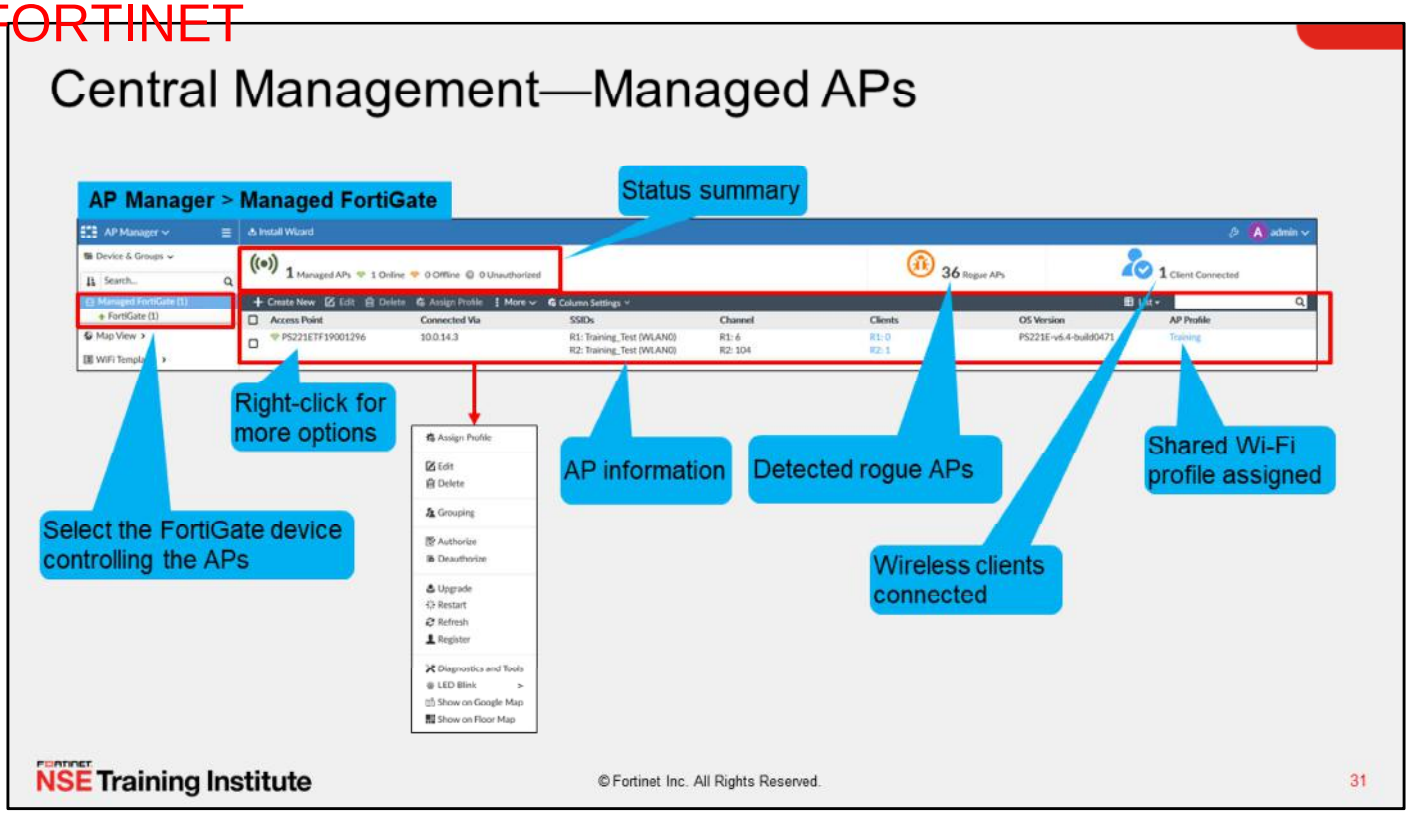
Central management mode uses *shared* Wi-Fi profiles to deploy the configuration to controlled APs. Changes made on a Wi-Fi profile result in a configuration change on multiple APs.

A Wi-Fi profile is specific to a FortiAP model, and therefore, different AP models require different Wi-Fi profiles.

In the example shown on this slide, the two APs are the same model and are deployed with the same shared Wi-Fi profile.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The example on this slide shows the managed APs in the **AP Manager** pane when using the central management mode.

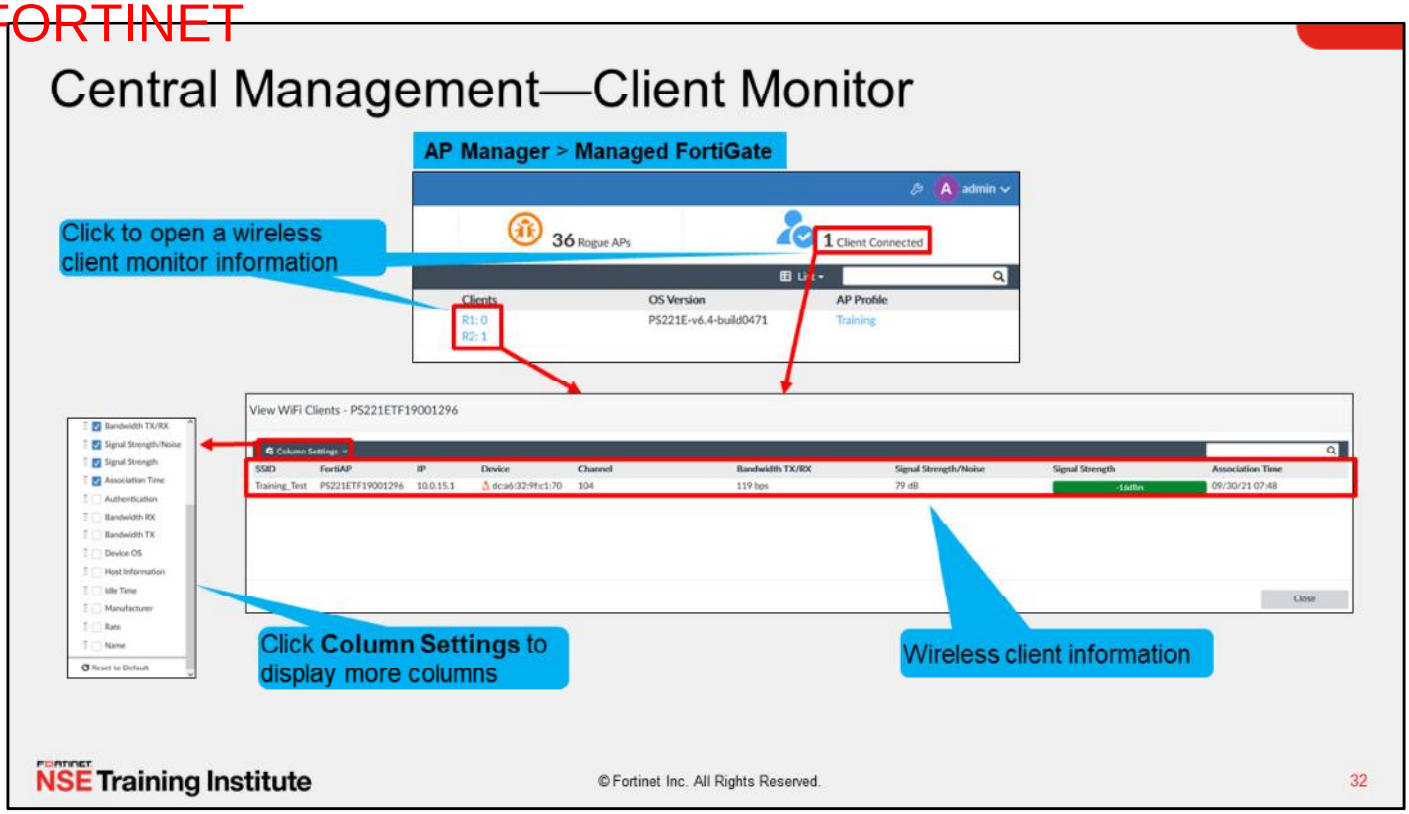
It shows wireless-related information, such as **SSIDs**, **Channel**, **Clients**, and **AP Profile** (or Wi-Fi profile). It also displays the status for each AP, but, unlike FortiSwitch Manager, there is no **Unknown** status. The other statuses (**Online**, **Offline**, **Unauthorized**) have the same meaning as in FortiSwitch Manager.

In addition, the page indicates the number of detected **Rogue APs** as well as the number of wireless clients connected (**Client Connected**).

When you right-click an AP, a menu with more management actions is displayed.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

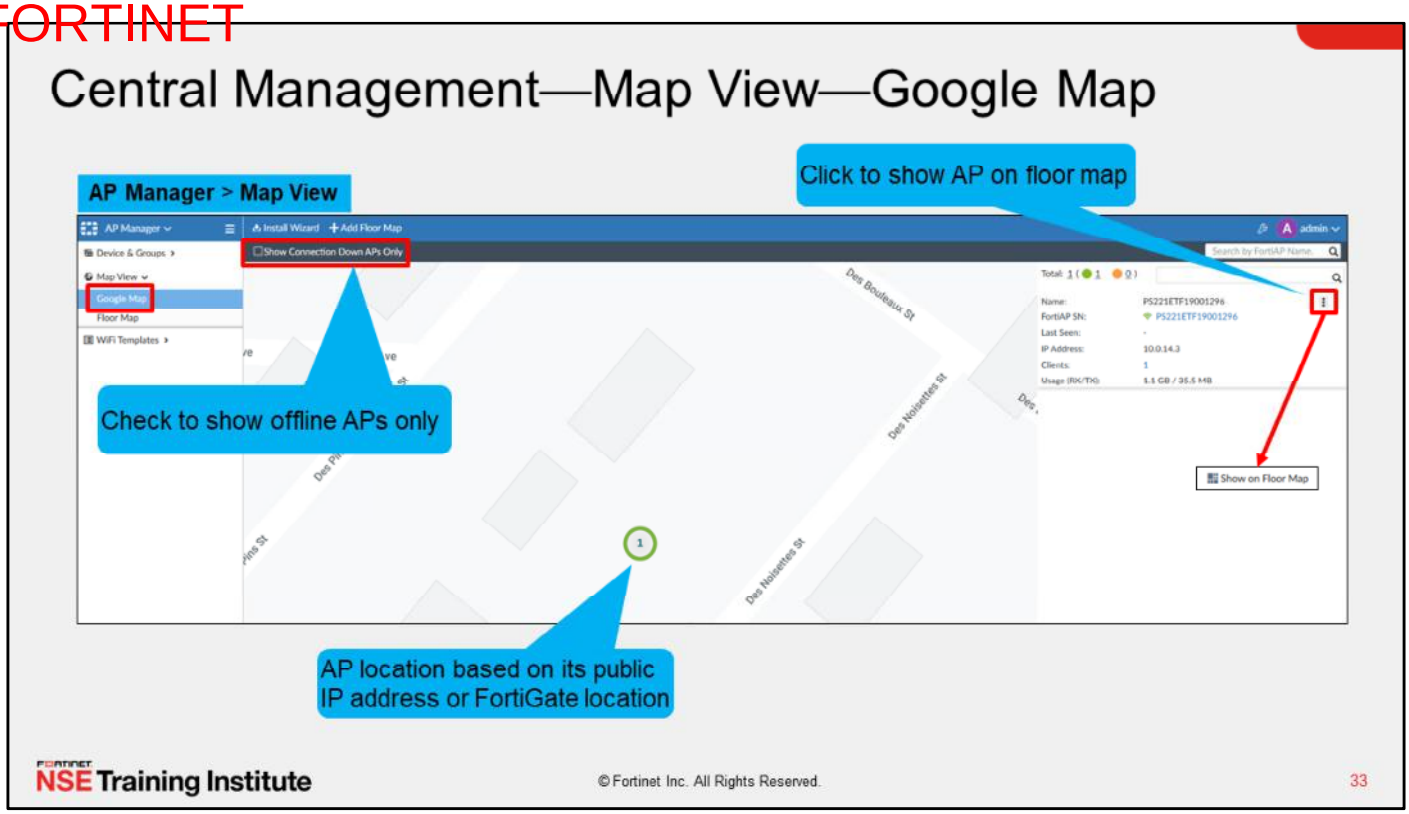


You can click a number in the **Clients** column or click the **Client Connected** icon to display a table with the list of wireless clients currently connected to the APs. For each client, the page displays some important wireless information, such as the SSID and the FortiAP it is connected to, or the signal-to-noise ratio (or signal strength/noise) and the signal strength. The last two values are key to determining the quality of the wireless signal.

If device detection is enabled on the SSID that the client is connected to, then FortiGate attempts to identify the device using various detection methods. You can click **Column Settings** to display additional columns containing device-related information.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



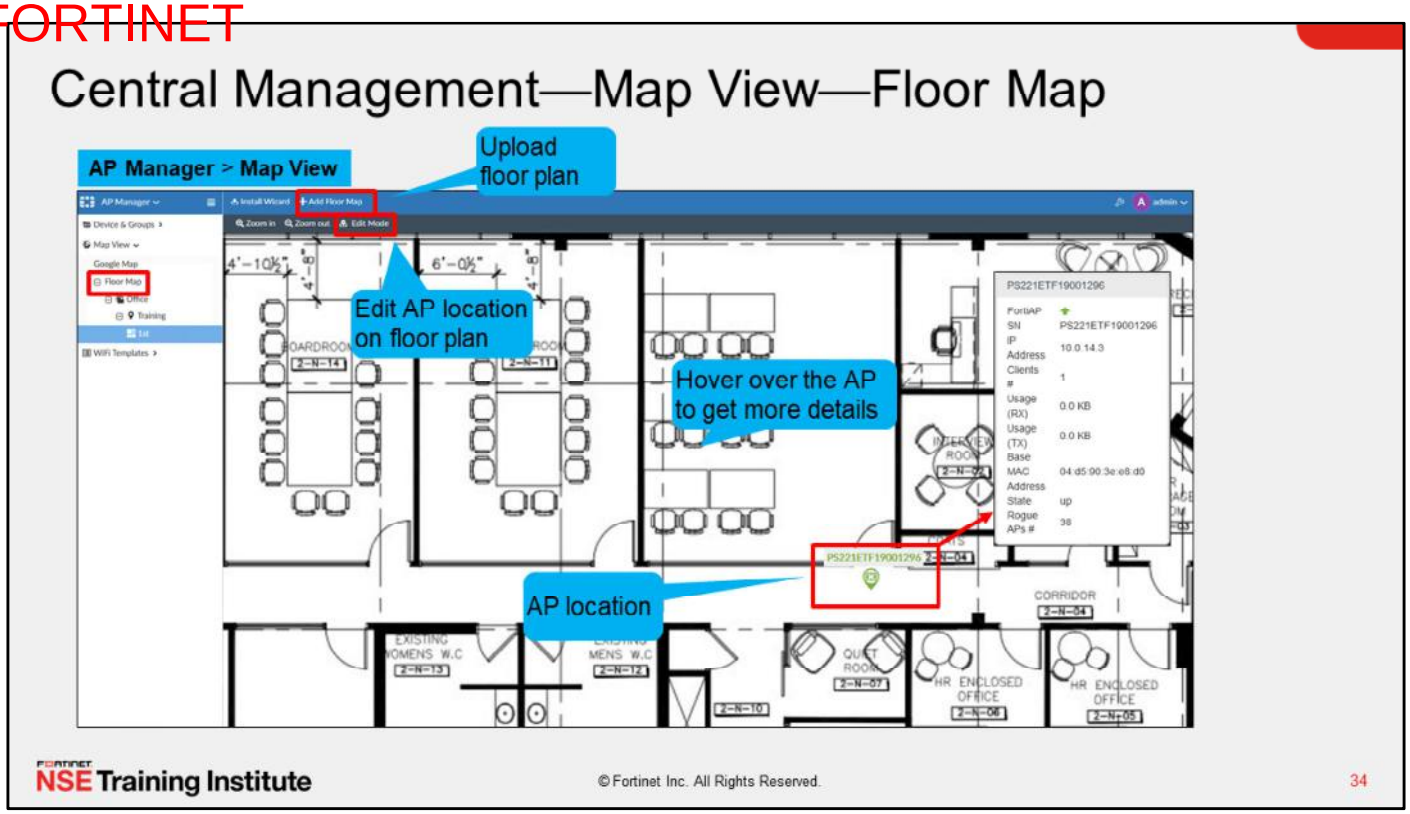
The **Map View** section in AP Manager displays the location of an AP on a **Google Map**, or its location on a **Floor Map**. FortiManager determines the AP location on Google Maps based on the AP public IP address. If the AP has a private IP address, FortiManager uses the controlling FortiGate location as the AP location. In the example shown on this slide, FortiManager uses the FortiGate location because the AP has a private IP address.

You can check **Show Connection Down APs Only** to display only the APs that are currently offline. This is useful when you need to locate failed APs that require an on-site presence to restore the service.

In addition, when you click **Show on Floor Map**, FortiManager displays the floor map view for the selected AP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

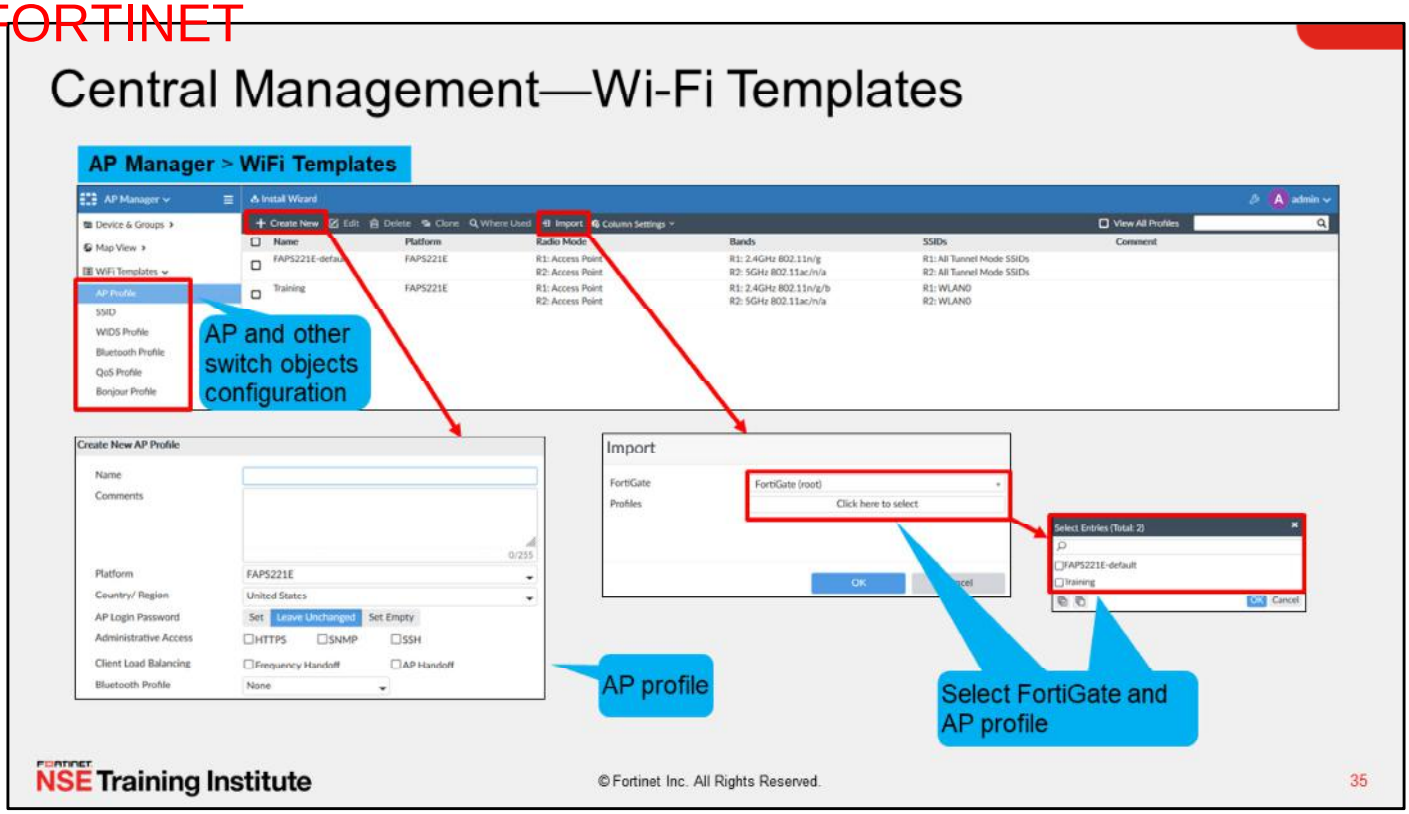


The **Floor Map** view enables you to upload the floor plan on the site where your APs are located. After that, you must manually place each AP on the floor plan.

Hover over each AP to get more details about the device such as IP address, serial number, data usage, or MAC address.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The **WiFi Templates** section is where you configure the profiles for your APs. A Wi-Fi profile contains all the wireless settings for your AP, such as the AP operation mode, enabled channels, power control, client load balancing options, and enabled SSIDs. It also contains the AP remote management settings.

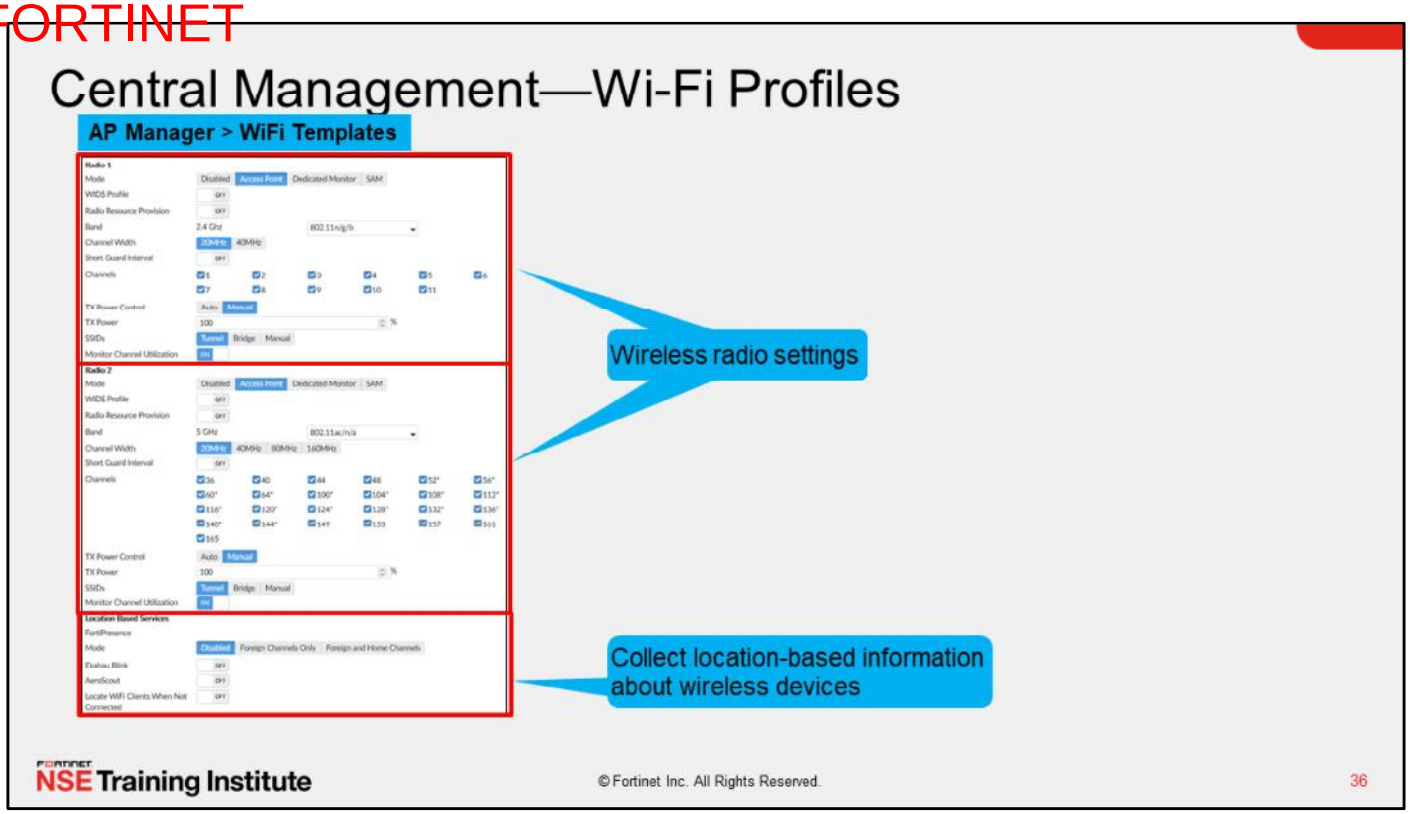
You can create a new Wi-Fi profile from scratch by clicking **AP Profile** on the left menu, and then clicking **Create New**. Alternatively, you can import a profile from an authorized FortiAP by clicking **Import**, and then selecting the FortiGate device and the AP profile you want to import the profile settings from.

You can also configure the following objects that can be used in your Wi-Fi profile:

- **SSID**: This is where you configure your wireless service set identifiers (SSIDs).
- **WIDS Profile**: A wireless IDS (WIDS) profile enables you to configure rules to detect intrusion attacks on the wireless network. It also enables you to detect rogue APs. A rogue AP is an AP that has not been authorized on your network, or just an AP that is unknown.
- **Bluetooth Profile**: Enables you to configure FortiAP to scan for wireless devices using the Bluetooth low energy (BLE) standard.
- **QoS Profile**: Used for controlling the amount of bandwidth generated through the AP or by a wireless client.
- **Bonjour Profile**: Bonjour profiles are used to allow forwarding of Bonjour traffic sourced from wireless devices to other FortiGate interfaces. The purpose is to allow the discovery and operation of Bonjour-based services running on your wireless devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The image on this slide shows more settings available in a Wi-Fi profile for a dual-radio AP model. You can configure different settings for each radio.

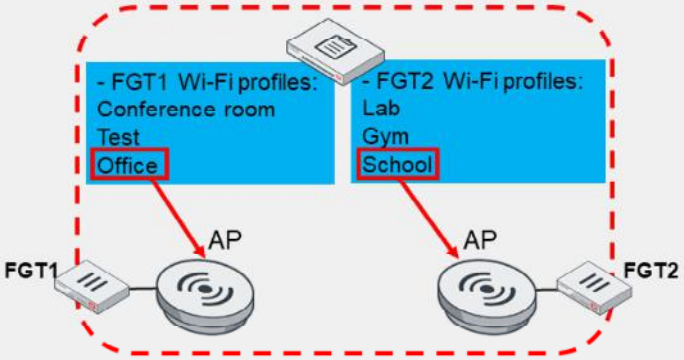
The **Location Based Services** section is where you configure the AP to collect information about wireless devices detected by your AP. The information collected is then used by FortiPresence to provide presence and positioning analytics for your locations.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

AP Manager—Per-Device Management

- Each FortiGate maintains its own set of Wi-Fi profiles
  - Wi-Fi profiles are not shared with other FortiGate and FortiAP devices
- Same settings in central management are available



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

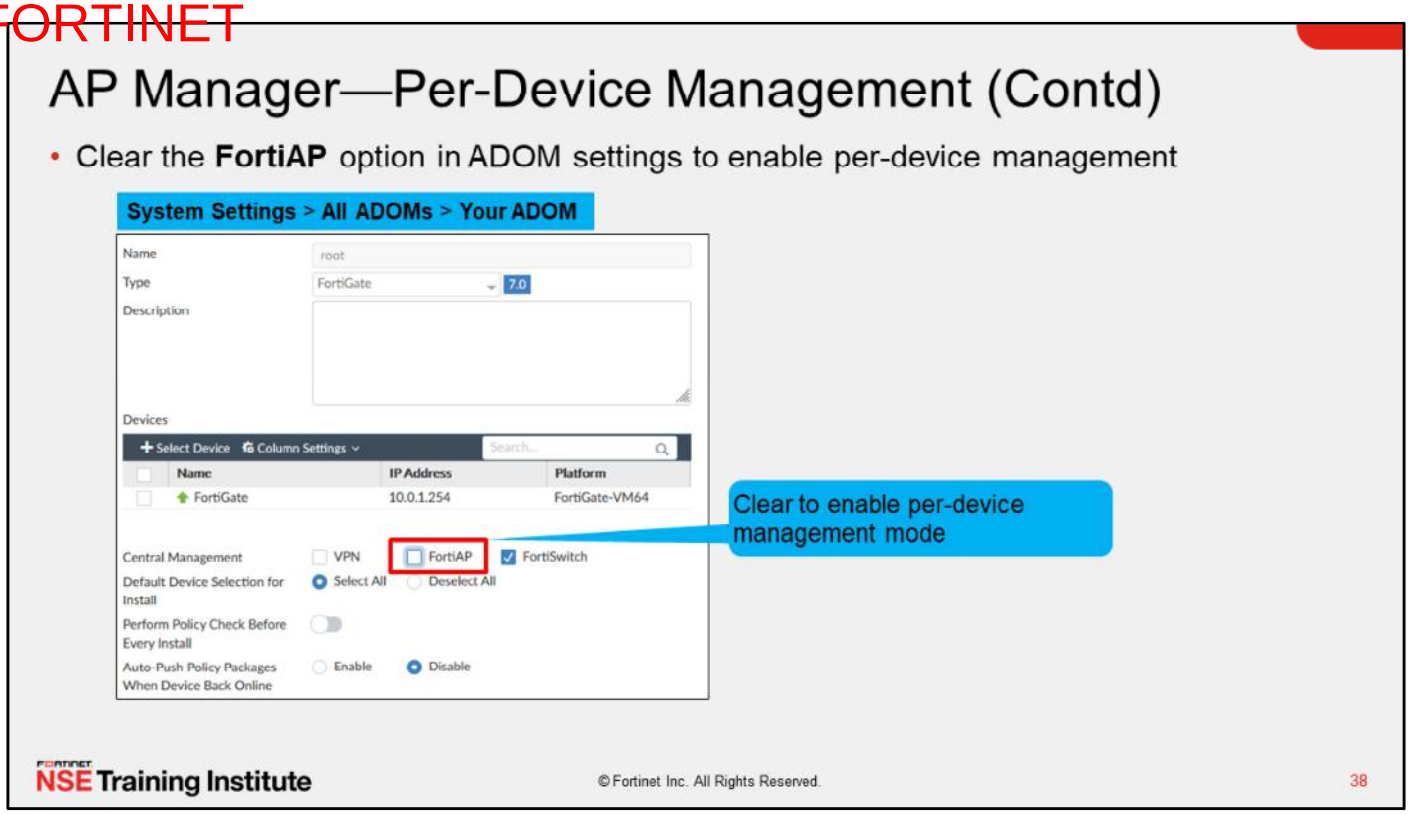
37

Per-device management mode supports the same configuration options as in central management mode. The only difference is that on per-device management mode, FortiManager maintains a set of Wi-Fi profiles for each wireless controller (FortiGate), instead of having a set of profiles that are shared among all APs controlled by all FortiGate devices.

In the example shown on this slide, FortiManager maintains three different Wi-Fi profiles for each FortiGate device, and one of those profiles is applied to the controlling AP.

Vouchers & Dumps are Available | WhatsApp +201224560923

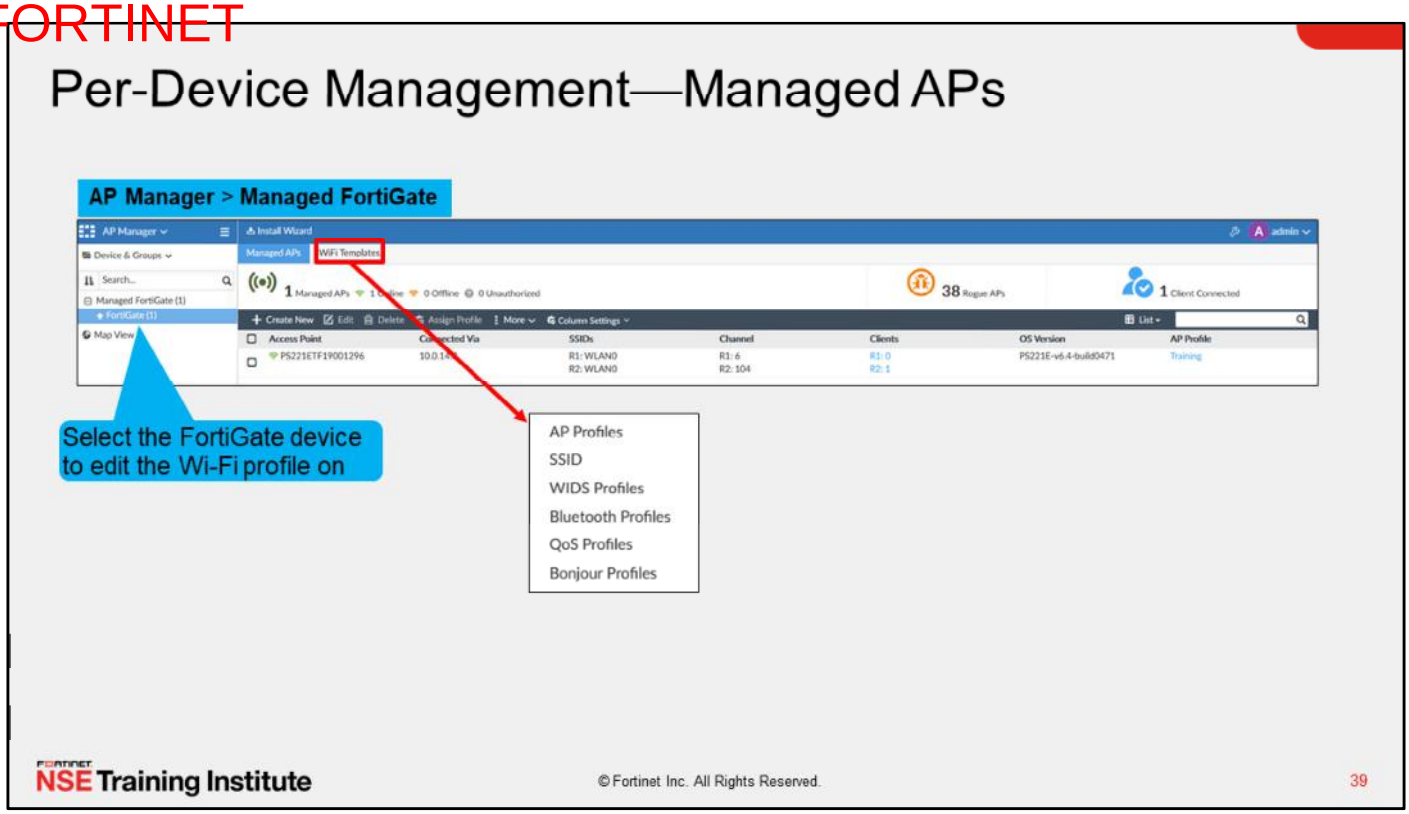
DO NOT REPRINT
© FORTINET
Brave-dumps.com



To enable per-device management, edit the settings of the ADOM you manage your FortiAP devices on, and clear the **FortiAP** option.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

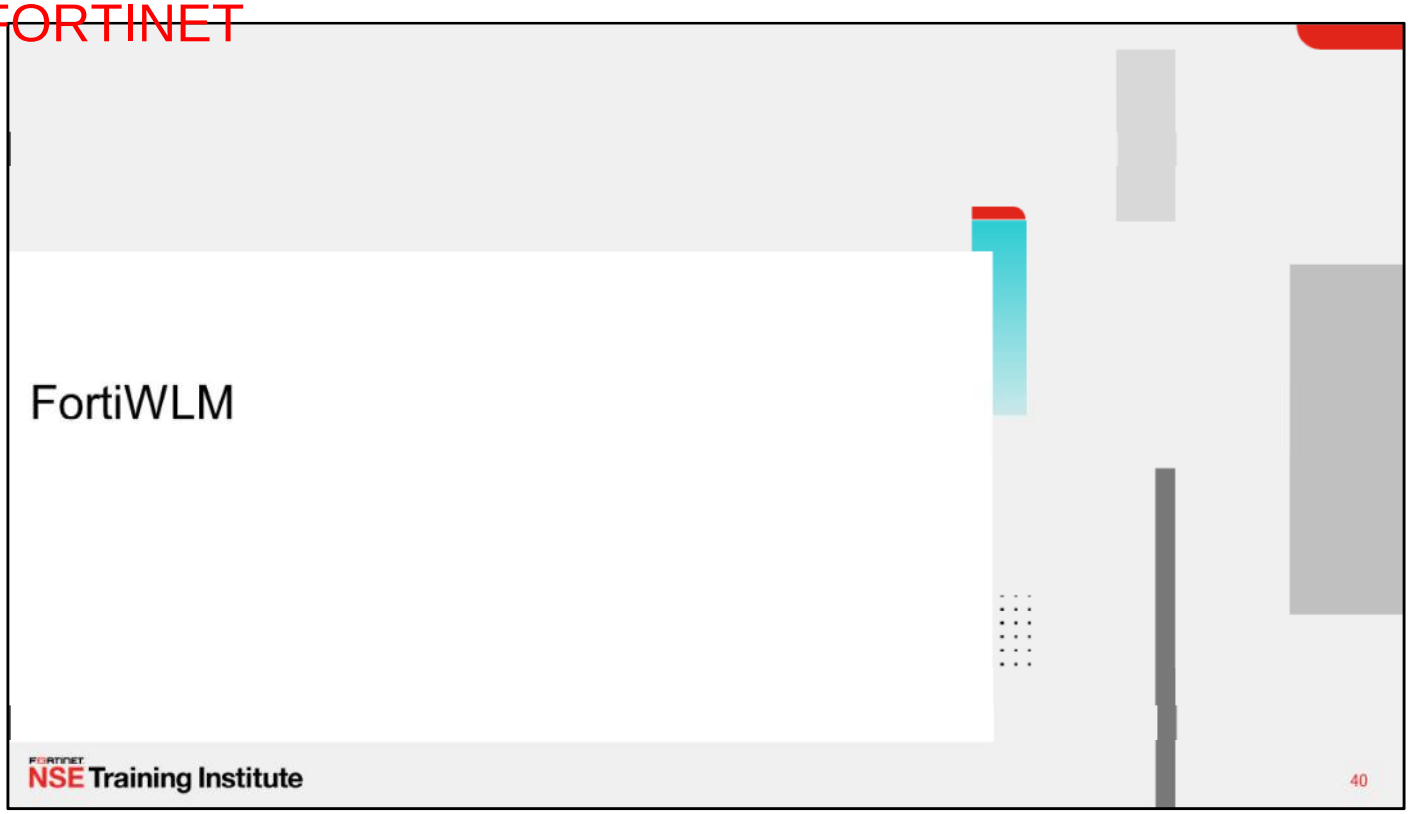


In per-device management mode, all tabs look the same as in central management mode. The only difference is the addition of the **WiFi Template** tab. Click this tab to edit the Wi-Fi profiles on the selected FortiGate device.

The example on this slide shows only one FortiGate device. When there are multiple FortiGate devices, you see a set of Wi-Fi profiles for each managed FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

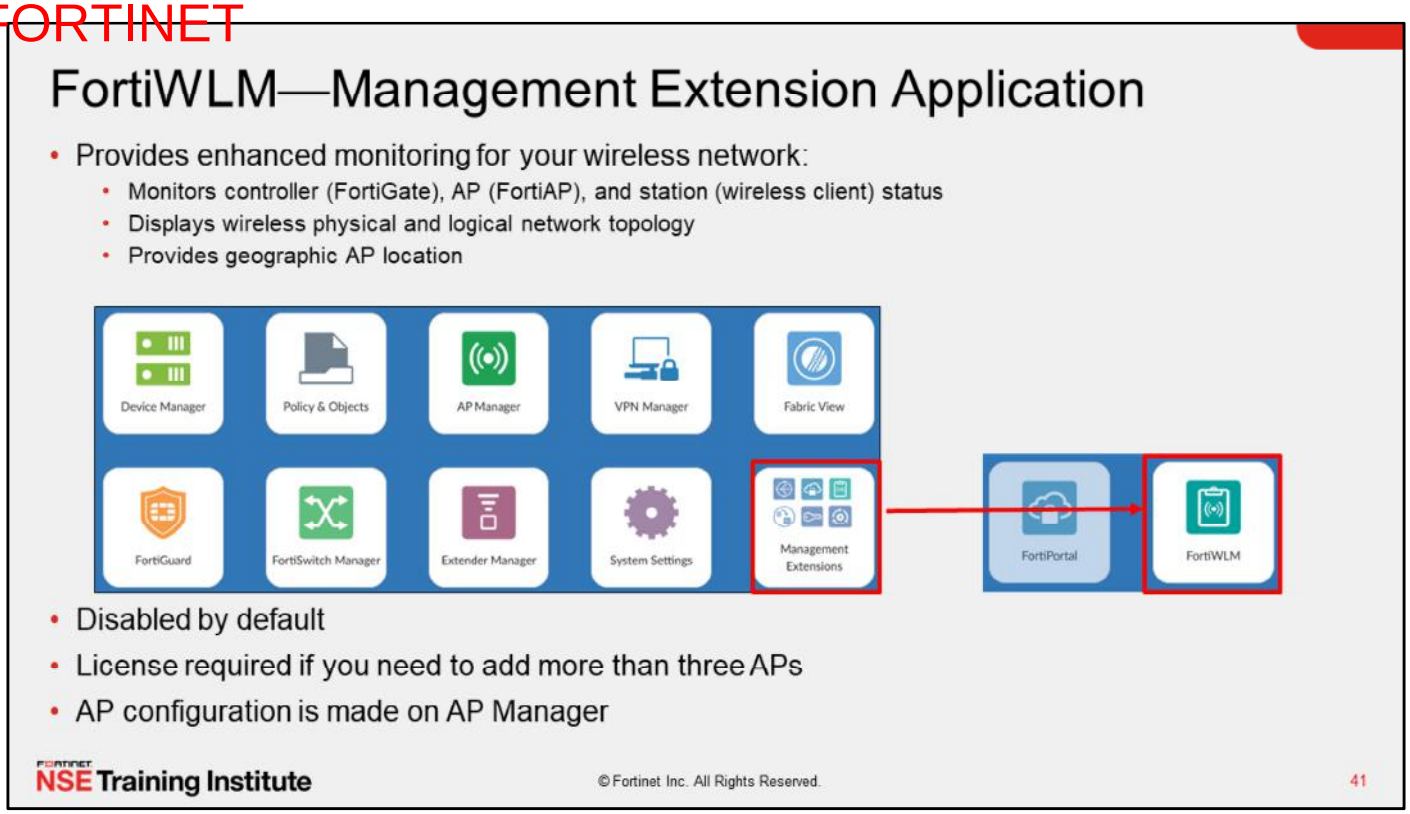
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn about the FortiWLM extension on FortiManager, which provides you with enhanced monitoring for your wireless network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



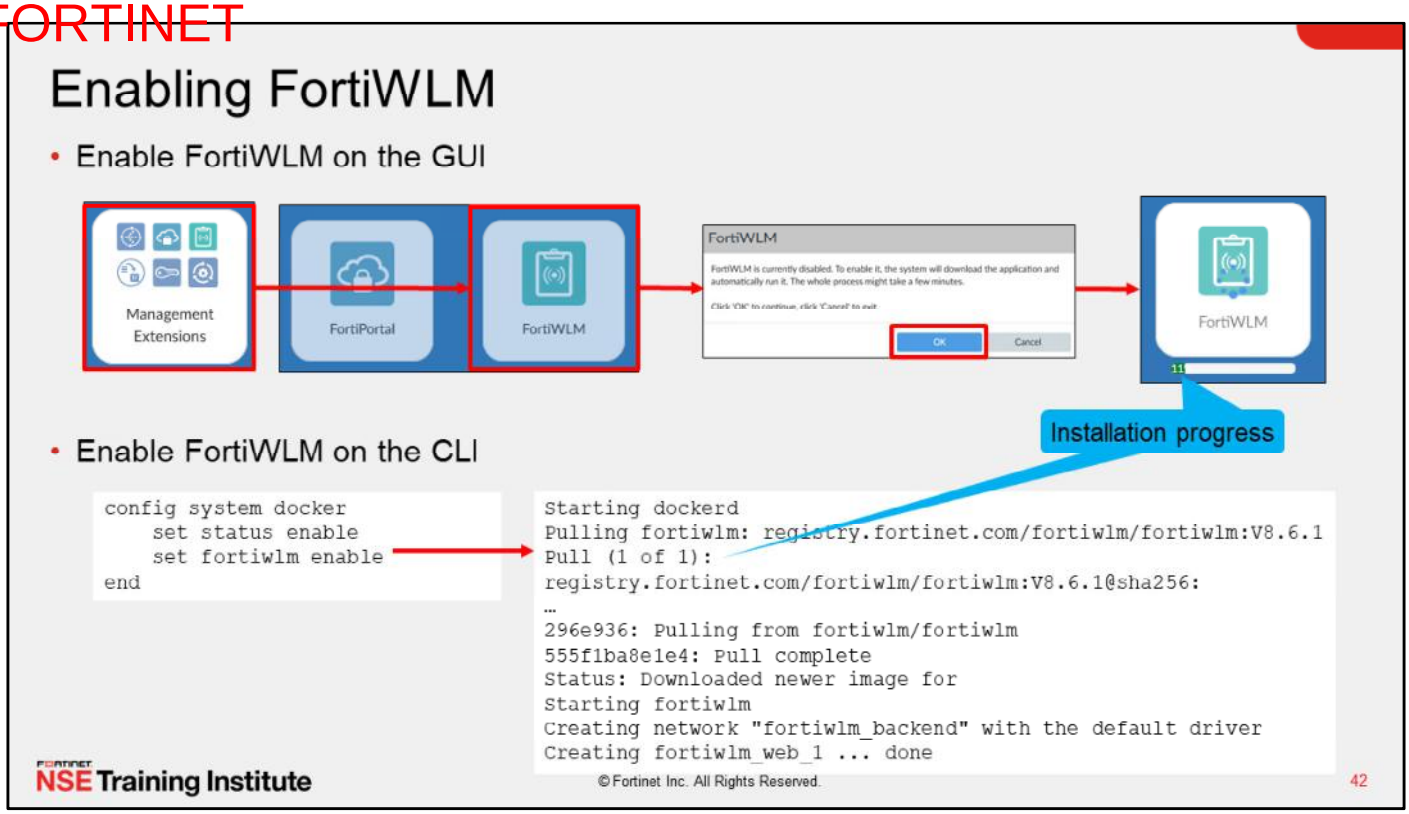
The **FortiWLM** management extension application (MEA) is a complement to AP Manager. While AP Manager supports a monitor tab, with FortiWLM you get an enhanced monitoring view of your wireless network. For this, FortiManager contacts the wireless controller (FortiGate) periodically to poll wireless-related information, which is then used to report on the status of your wireless devices, build graphs and network topologies, determine AP location, and generate alarms, among other things.

FortiWLM is disabled by default. When enabled, you require a valid FortiWLM license to monitor more than three APs.

FortiWLM MEA provides monitoring services only. You still need to use AP Manager to deploy your APs and change their configuration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



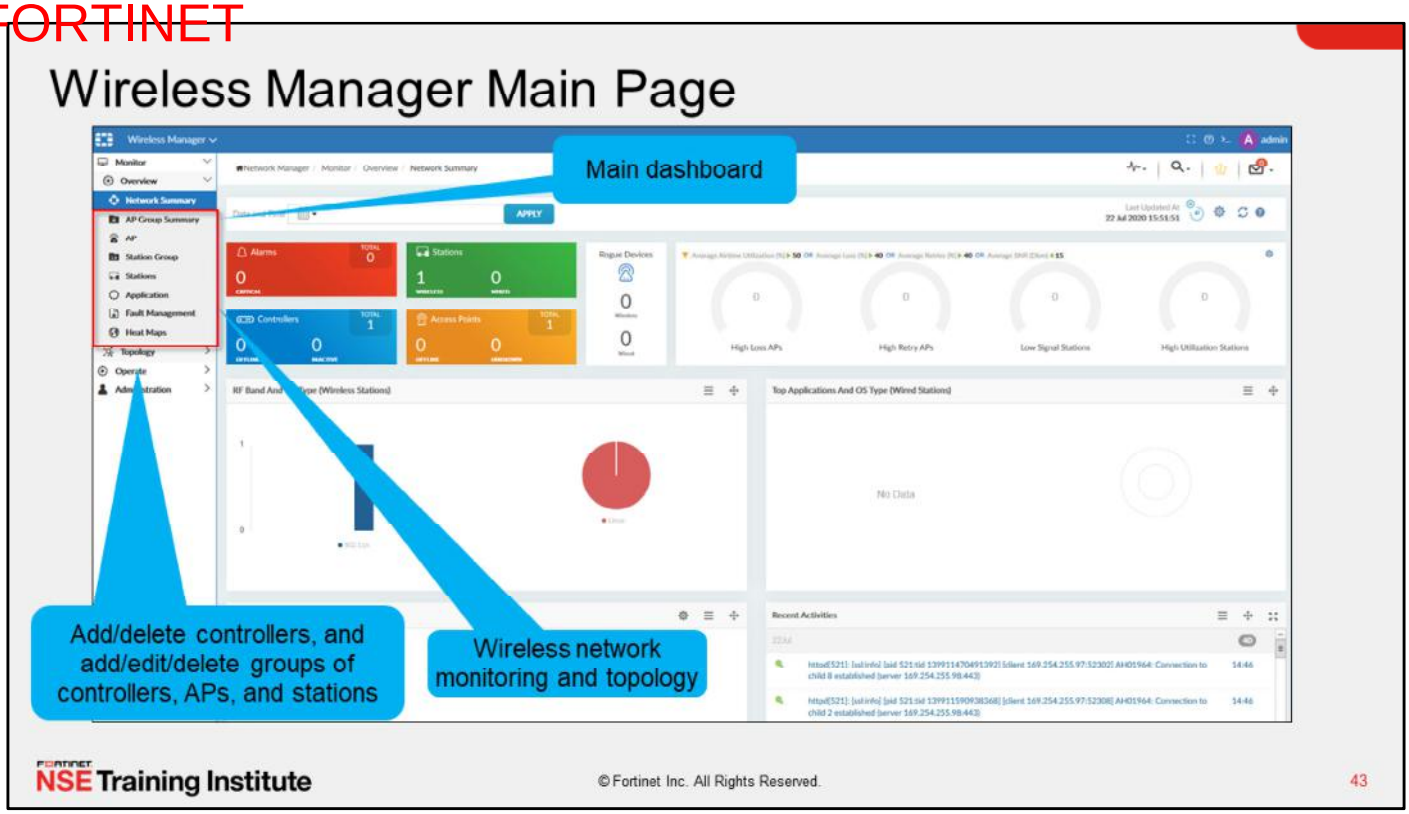
FortiWLM is disabled by default. You can enable it on the GUI or on the CLI.

To enable FortiWLM on the GUI, click **Management Extensions** and then **FortiWLM**, upon which FortiManager prompts you to enable the extension. To enable FortiWLM, FortiManager needs to download the application files from the internet, so you must make sure your FortiManager device has internet access. While FortiManager is downloading and installing FortiWLM, it displays a progress bar under the FortiWLM icon.

Alternatively, you can enable FortiWLM on the CLI by entering the commands shown on this slide. The CLI also displays the progress of the application installation.

Vouchers & Dumps are Available | WhatsApp +201224560923

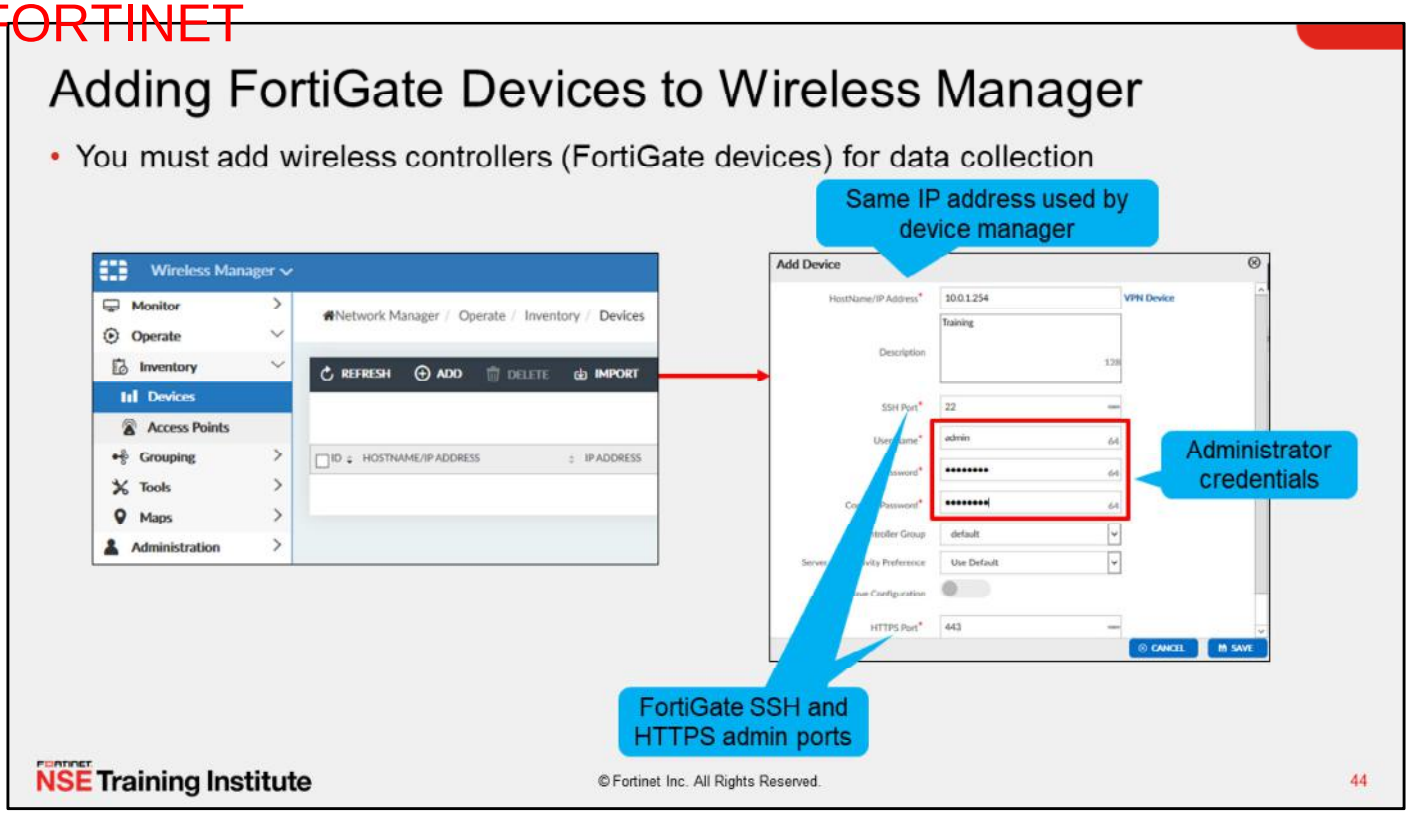
DO NOT REPRINT Brave-dumps.com
© FORTINET



The image on this slide shows the FortiWLM main page (or dashboard) after it is enabled.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

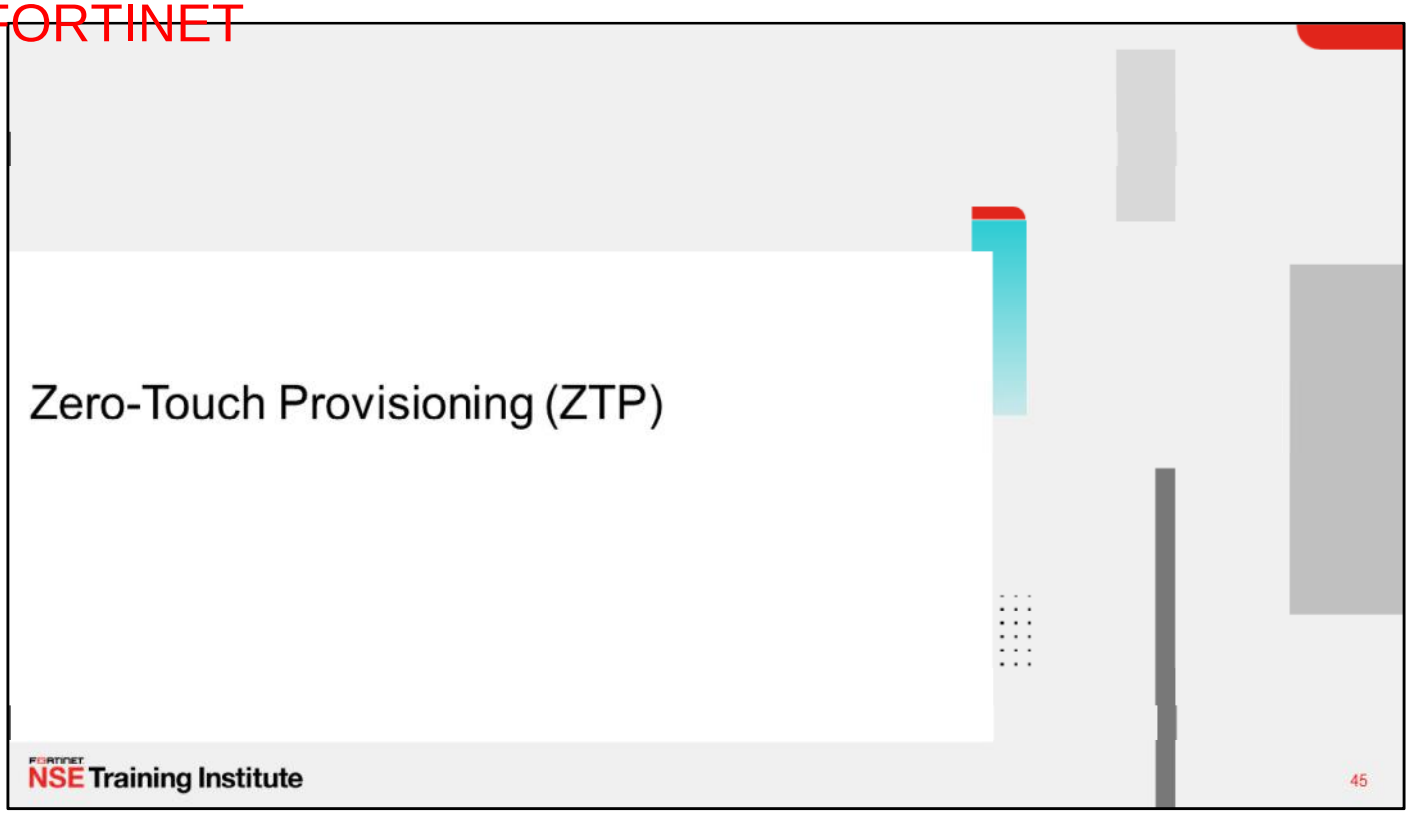


You must add wireless controllers (FortiGate devices) to FortiWLM before it can start collecting data for monitoring purposes. Note that before doing this, the FortiGate devices must have been already registered on the root ADOM on FortiManager. Also note that you can add only FortiGate devices registered on the root ADOM to FortiWLM.

To add the wireless controller to FortiWLM, click **Inventory** > **Devices**, and then click **ADD**. FortiWLM requests the device IP address, administrator credentials, and the ports it uses for SSH and HTTPS administration.

Vouchers & Dumps are Available | WhatsApp +201224560923

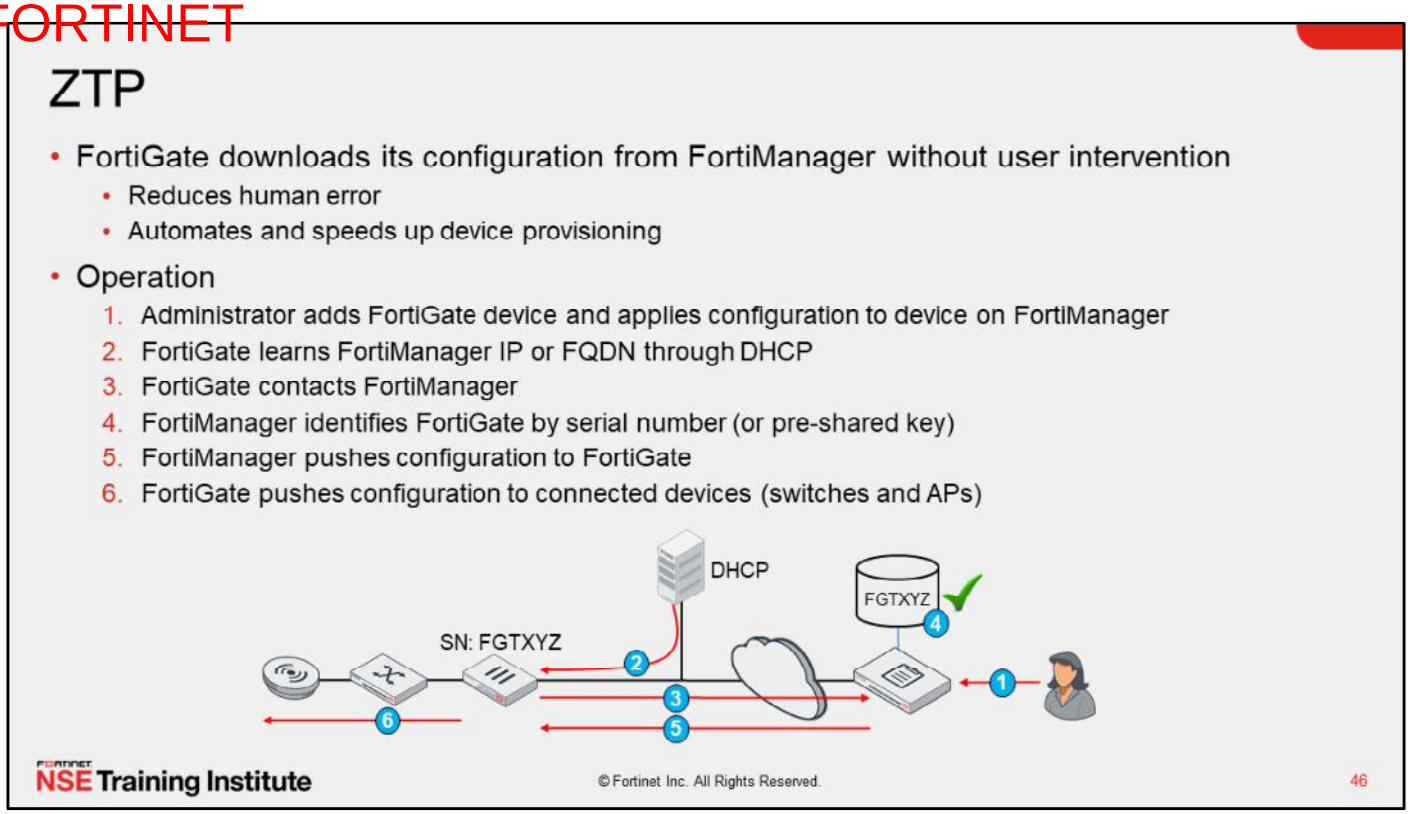
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn about the ZTP solution available on FortiManager, which enables you to configure your FortiGate and its connected devices without user intervention on the managed devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



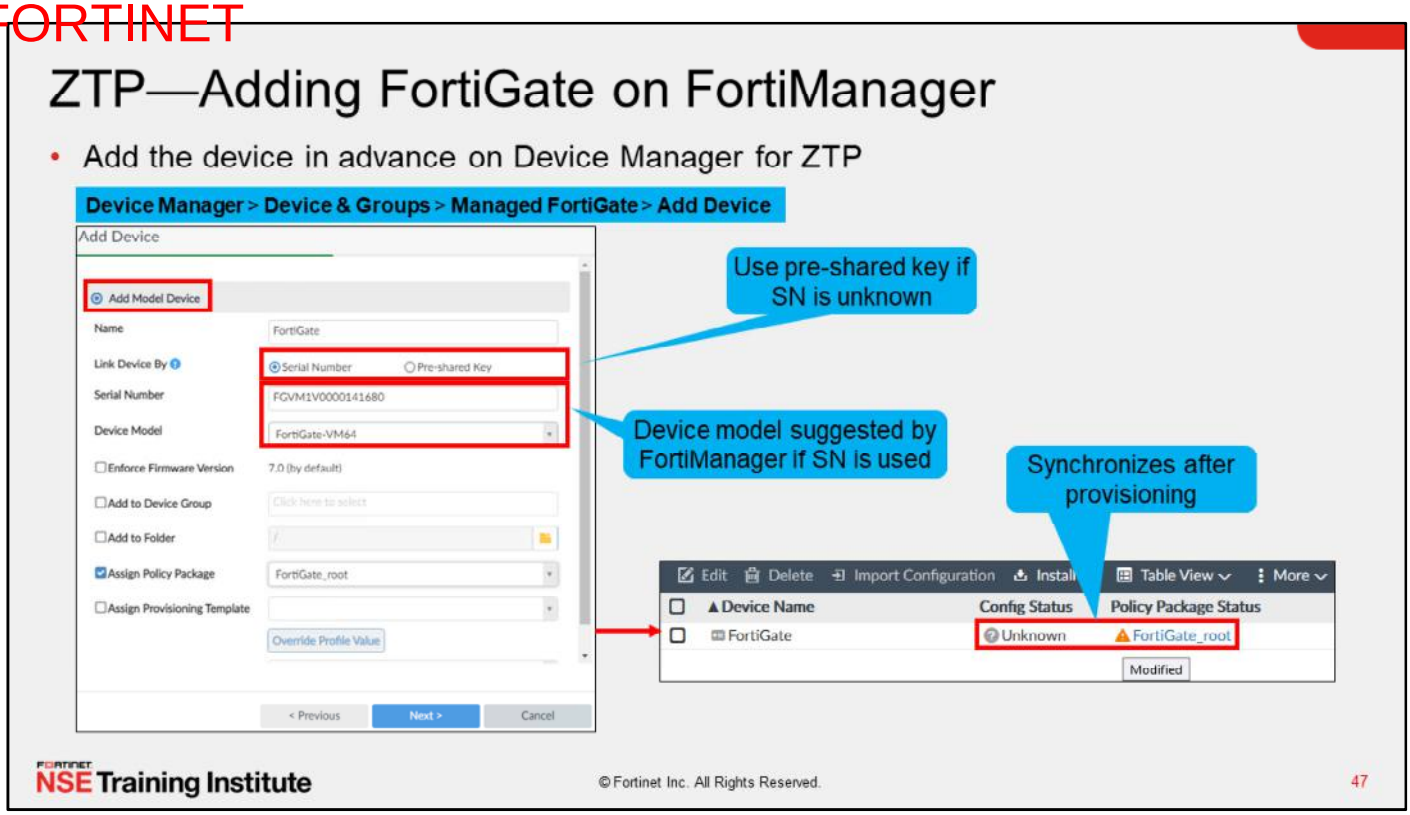
ZTP enables you to provision devices without having to change their configuration onsite. The local technician needs to make only the necessary network physical connections and power up the devices. This approach reduces human error while speeding up deployments thanks to automation.

ZTP works as follows:

1. The administrator adds the FortiGate device on FortiManager and configures all of its settings. The configured settings include the device settings, policy package, and the configuration for its connected switches and APs.
2. When FortiGate is connected to the network, FortiGate retrieves the FortiManager IP address or FQDN through DHCP options 240 or 241 respectively, provided the DHCP server in the local network has been preconfigured with such options.
3. FortiGate contacts FortiManager using the network parameters provided by the DHCP server.
4. FortiManager checks the FortiGate serial number against its local database. If the serial number matches a preconfigured device, then device registration is completed. Optionally, you can configure a pre-shared key on both FortiManager and FortiGate for identifying the managed device.
5. FortiManager pushes the preconfigured device settings to FortiGate.
6. If there are connected devices, such as switches and APs, FortiGate also pushes the configuration provided by FortiManager for those devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The first step to achieve ZTP is to add the device on FortiManager before it is deployed on the field.

When you add the device on FortiManager, you must select **Add Model Device**, and then type the device details. Usually you want to match the device based on its serial number, but you could also use a pre-shared key if the device serial number is unknown.

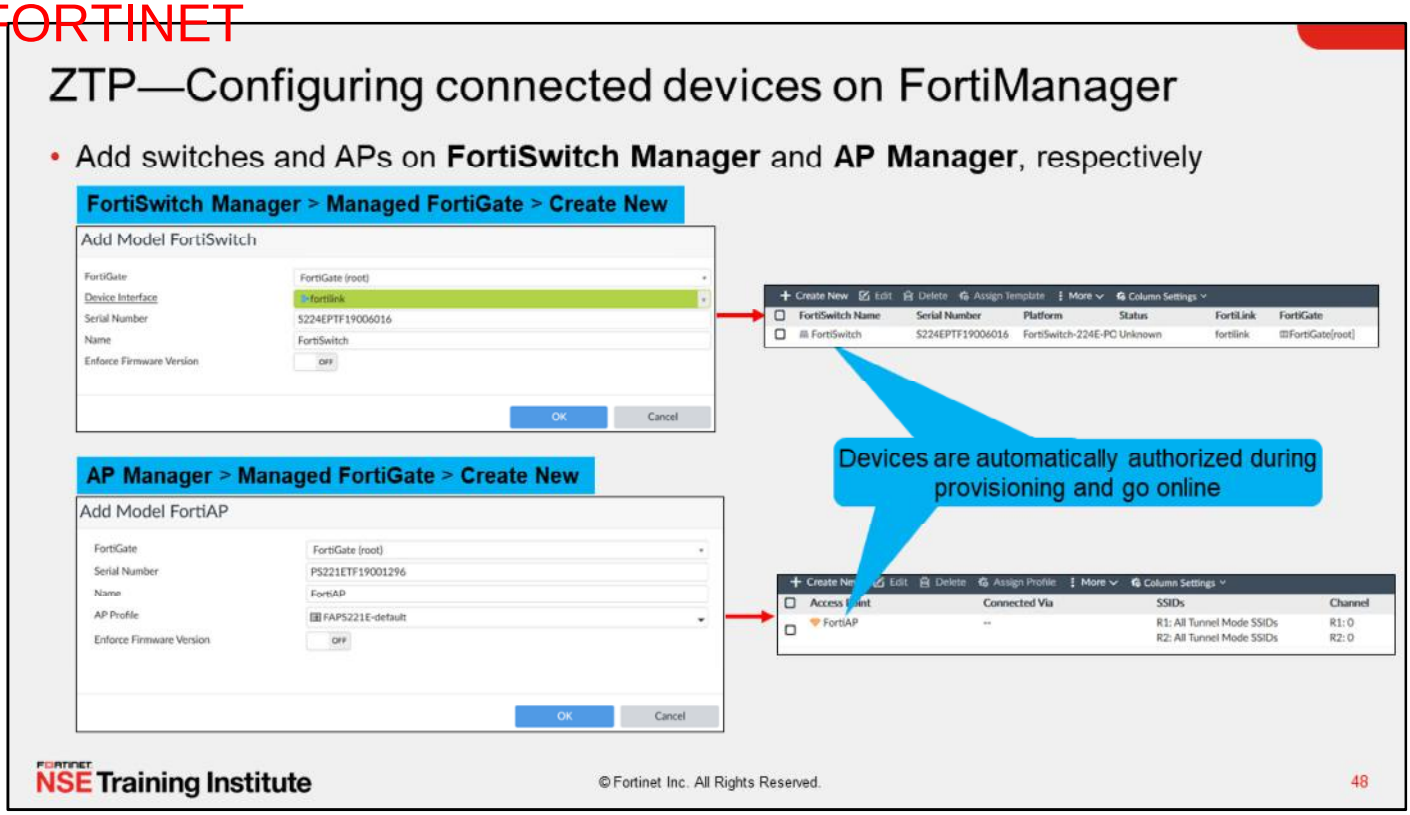
You must also indicate the device model. However, if you use a serial number for device matching, then FortiManager suggests a device model based on the serial number.

After you add the device, its **Config Status** and **Policy Package Status** are shown as **Unknown** and **Modified**, respectively. Both statuses change after the device downloads the settings from FortiManager during provisioning.

After the device is added, you may want to configure its required settings and policies on the **Device Manager** and **Policy & Objects** panes, respectively. Otherwise, FortiManager uses the device factory default configuration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can use ZTP to provision FortiSwitch and FortiAP devices that are connected to FortiGate by adding the devices to their FortiManager panes.

When you add the connected devices ahead of time on FortiManager, they do not appear as online. However, after FortiGate downloads the configuration from FortiManager, which also includes the settings for its connected switches and APs, the devices are automatically authorized and eventually appear online.

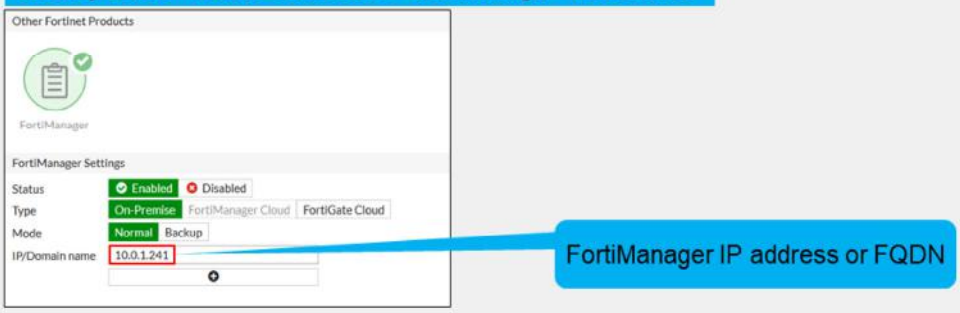
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

ZTP—Adding FortiManager on FortiGate

- FortiGate learns FortiManager address through DHCP:
  - Option 240: IP address
  - Option 241: FQDN
- Alternatively, you can set FortiManager address on FortiGate GUI

Security Fabric > Fabric Connectors > FortiManager > Add Device



- If pre-shared key is used instead of serial number, you must also run on the CLI:

```
# execute central-mgmt register-device <fmg-sn> <psk-key>
```

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

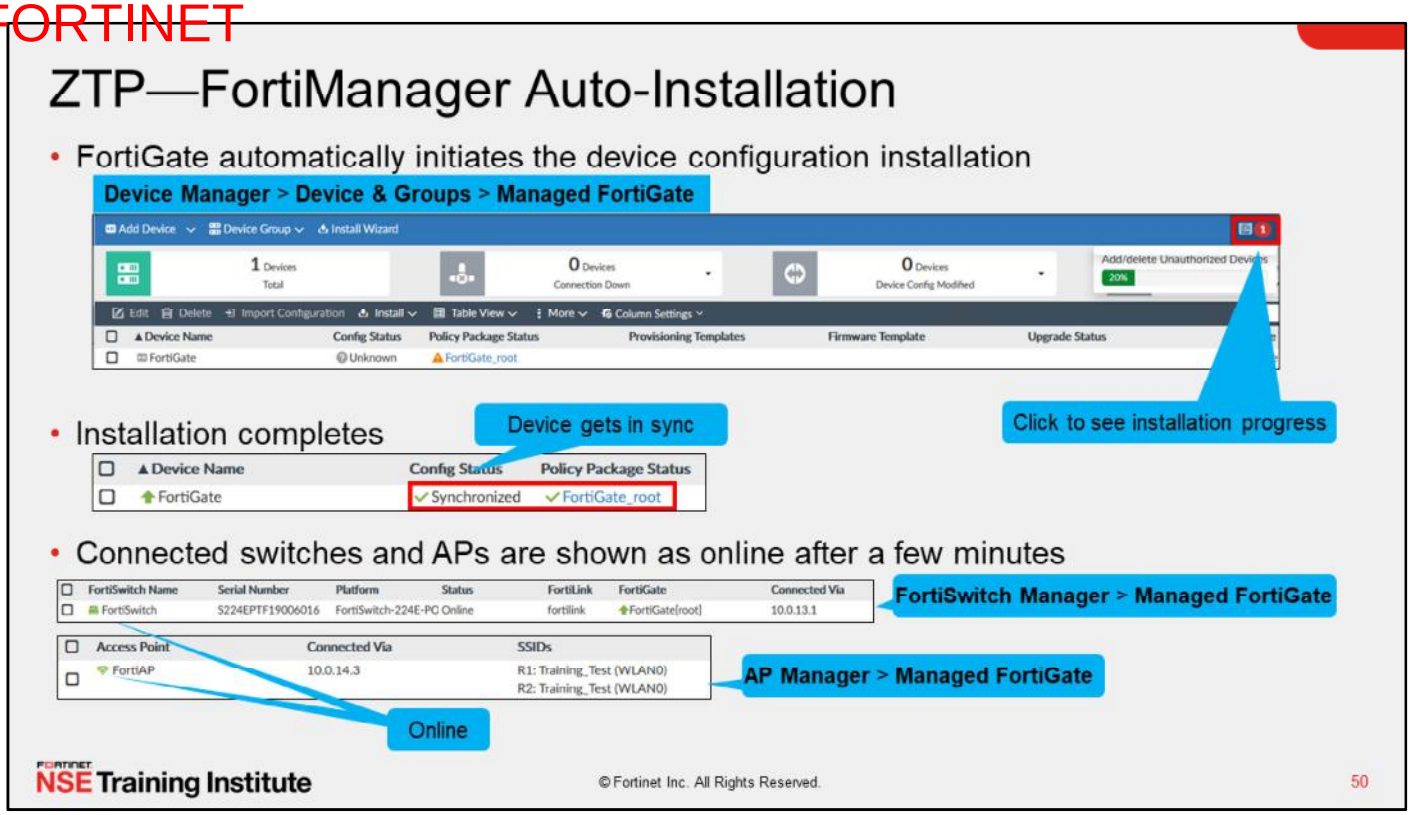
49

FortiGate can obtain the FortiManager address through DHCP options 240 and 241. If the local DHCP server is not configured with such options, you can manually set the FortiManager address on the GUI instead. *Do not* configure the FortiManager address on the CLI because that does *not* initiate the secure tunnel between FortiGate and FortiManager. This is a behavior by design.

If you have configured device matching based on pre-shared key instead of serial number, then you must also run the CLI command shown on this slide. The command requires the user to provide the FortiManager serial number and the configured pre-shared key.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



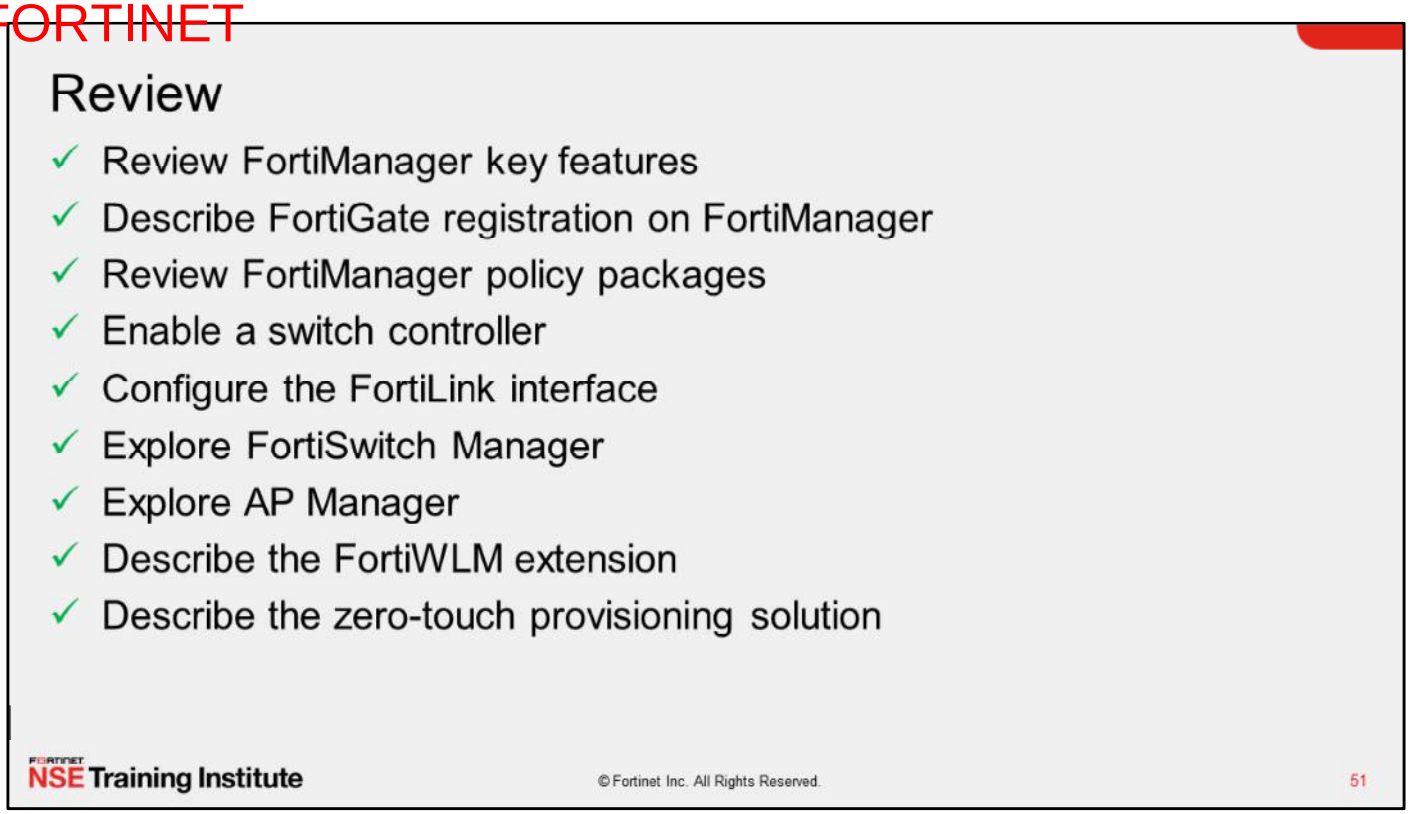
After FortiGate retrieves the FortiManager address, it contacts FortiManager to initiate the secure tunnel on TCP port 541. After the tunnel is established and the device is identified, FortiManager automatically initiates the device configuration installation and shows a notification on **Device Manager**. Click the notification button to view the installation progress.

After a few seconds, the installation is completed, and the device is shown as in sync.

If you have configured connected devices, they are also shown as online in their respective FortiManager panes. Just keep in mind that FortiManager may need a few minutes before displaying them as online because the devices are rebooted upon authorization and FortiManager queries their status every three minutes.

Vouchers & Dumps are Available | WhatsApp +201224560923

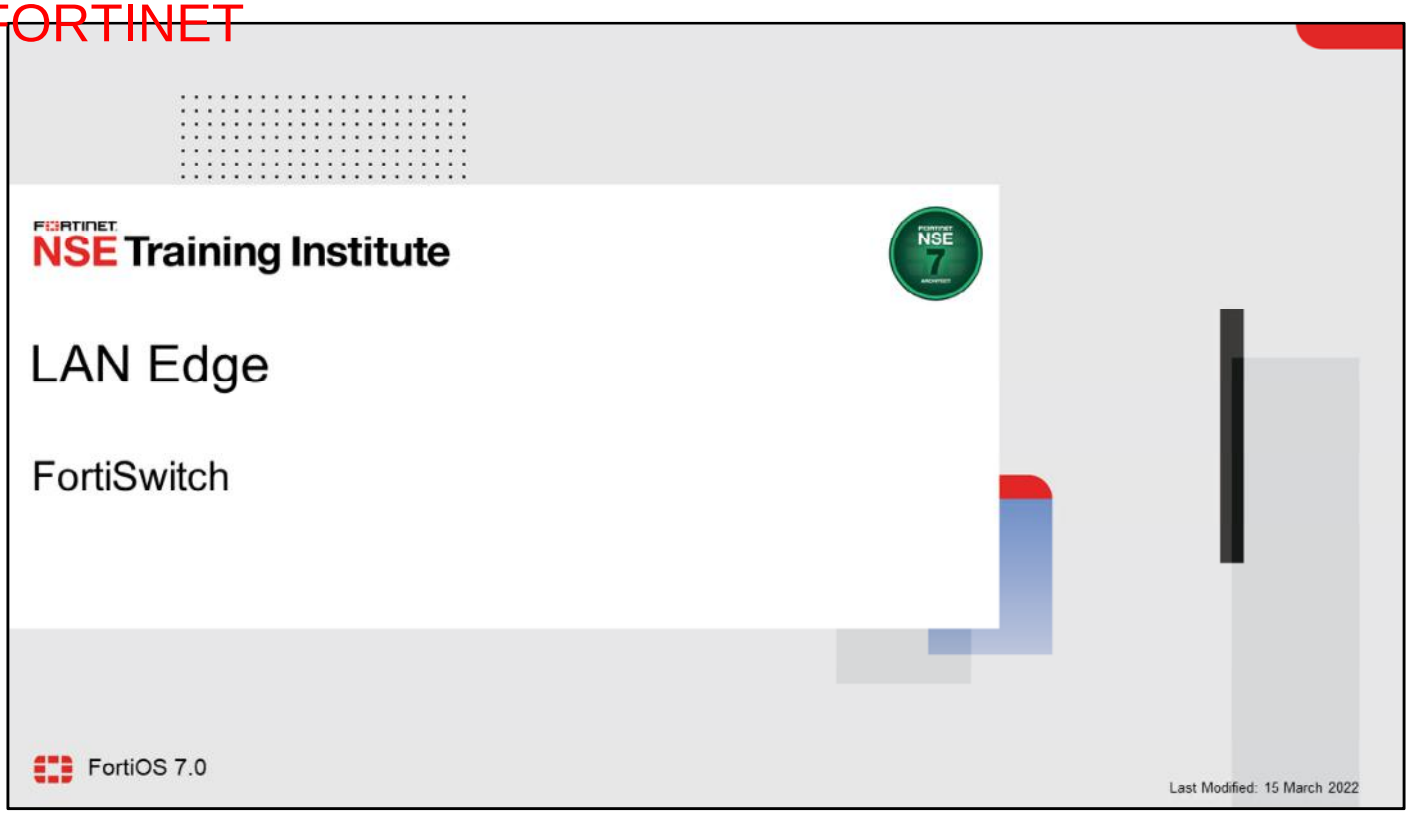
DO NOT REPRINT
© FORTINET
Brave-dumps.com



By mastering the objectives covered in this lesson, you learned how to use FortiManager to deploy FortiSwitch and FortiAP devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

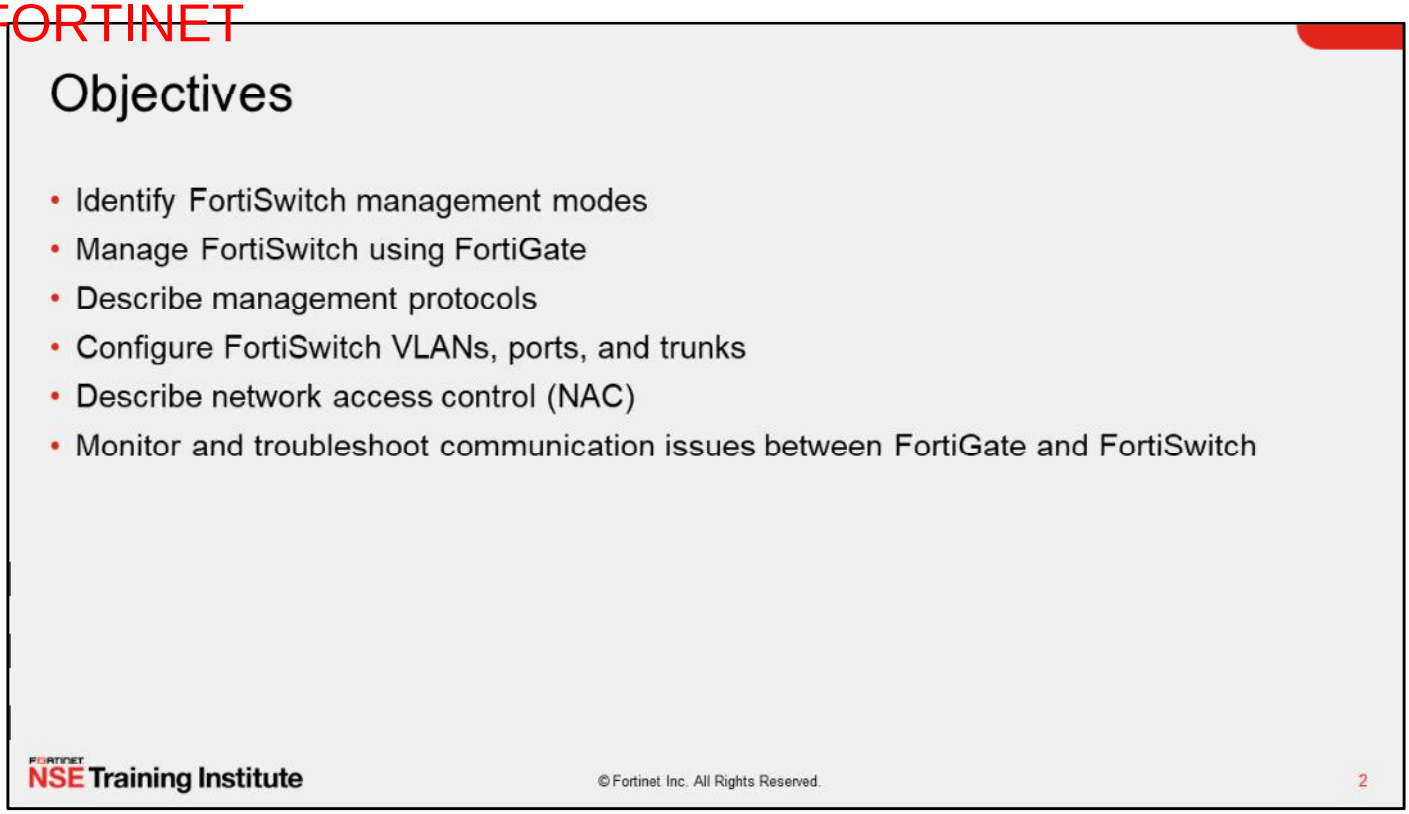
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn about FortiSwitch configuration and troubleshooting when managed by FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

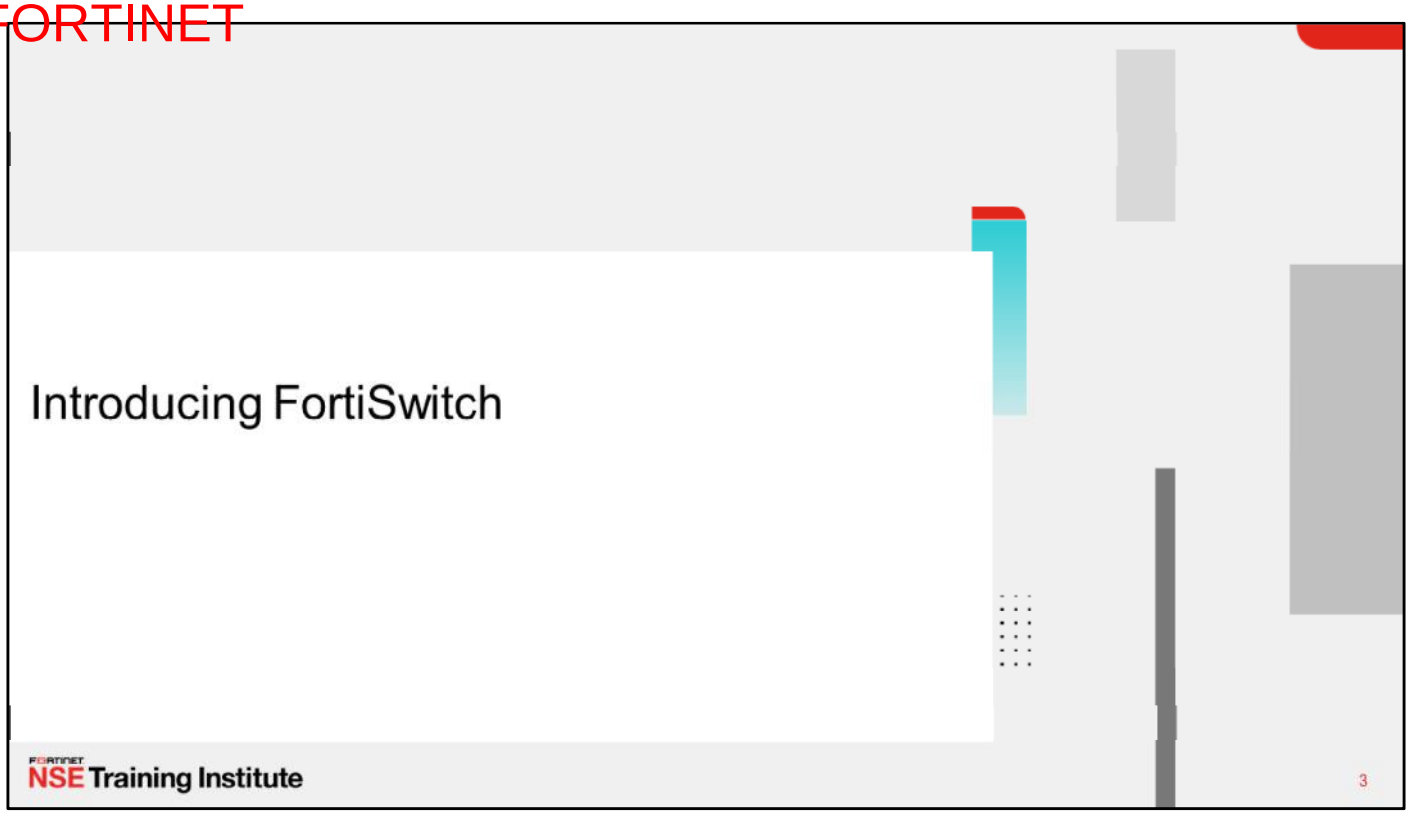


After completing this lesson, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in FortiSwitch, you will be able to configure FortiSwitch VLANs, ports, and trunks, and troubleshoot communication issues between FortiGate and FortiSwitch.

Vouchers & Dumps are Available | WhatsApp +201224560923

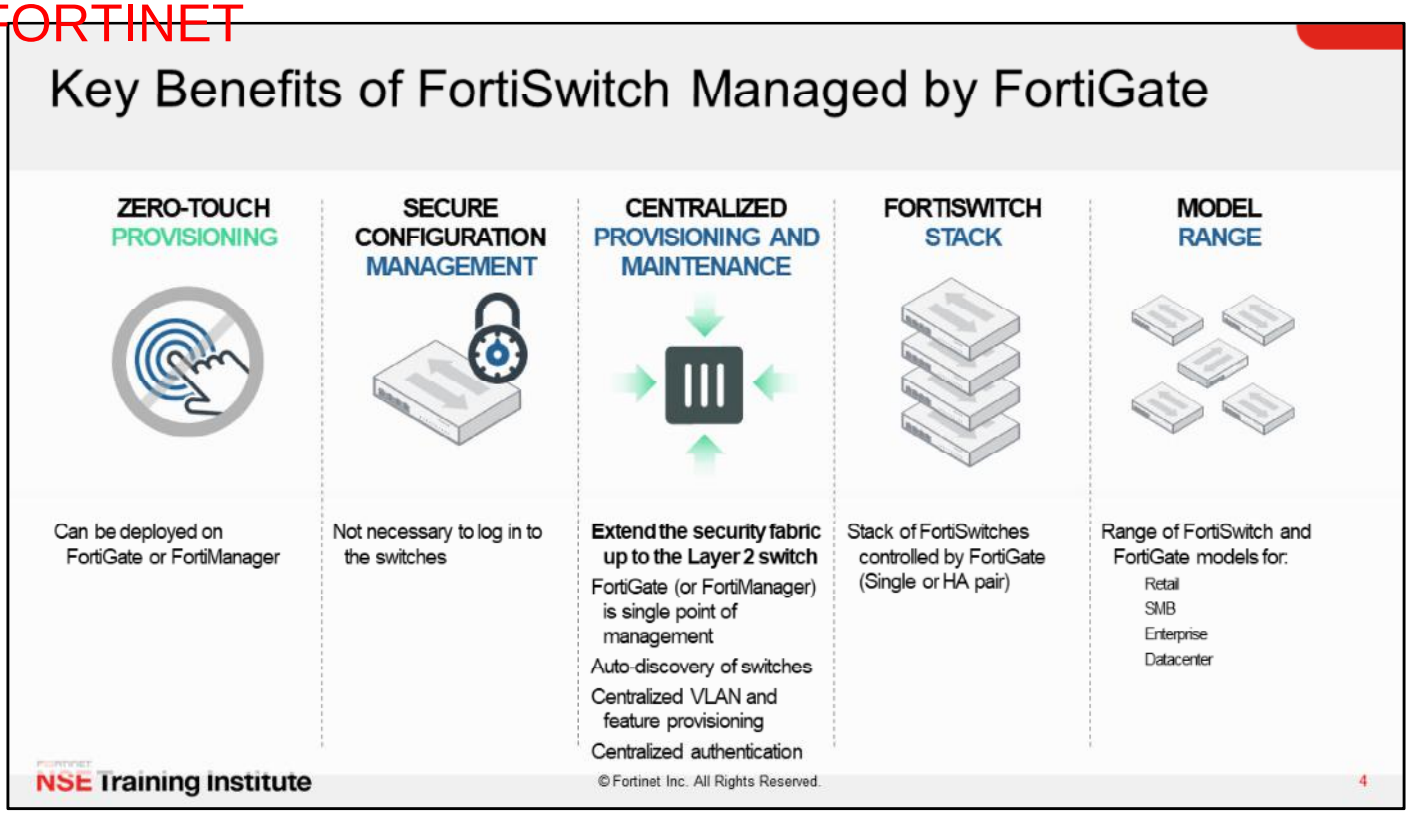
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn about FortiSwitch when it is managed by FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Managing FortiSwitch devices using FortiGate offers the following important key benefits:

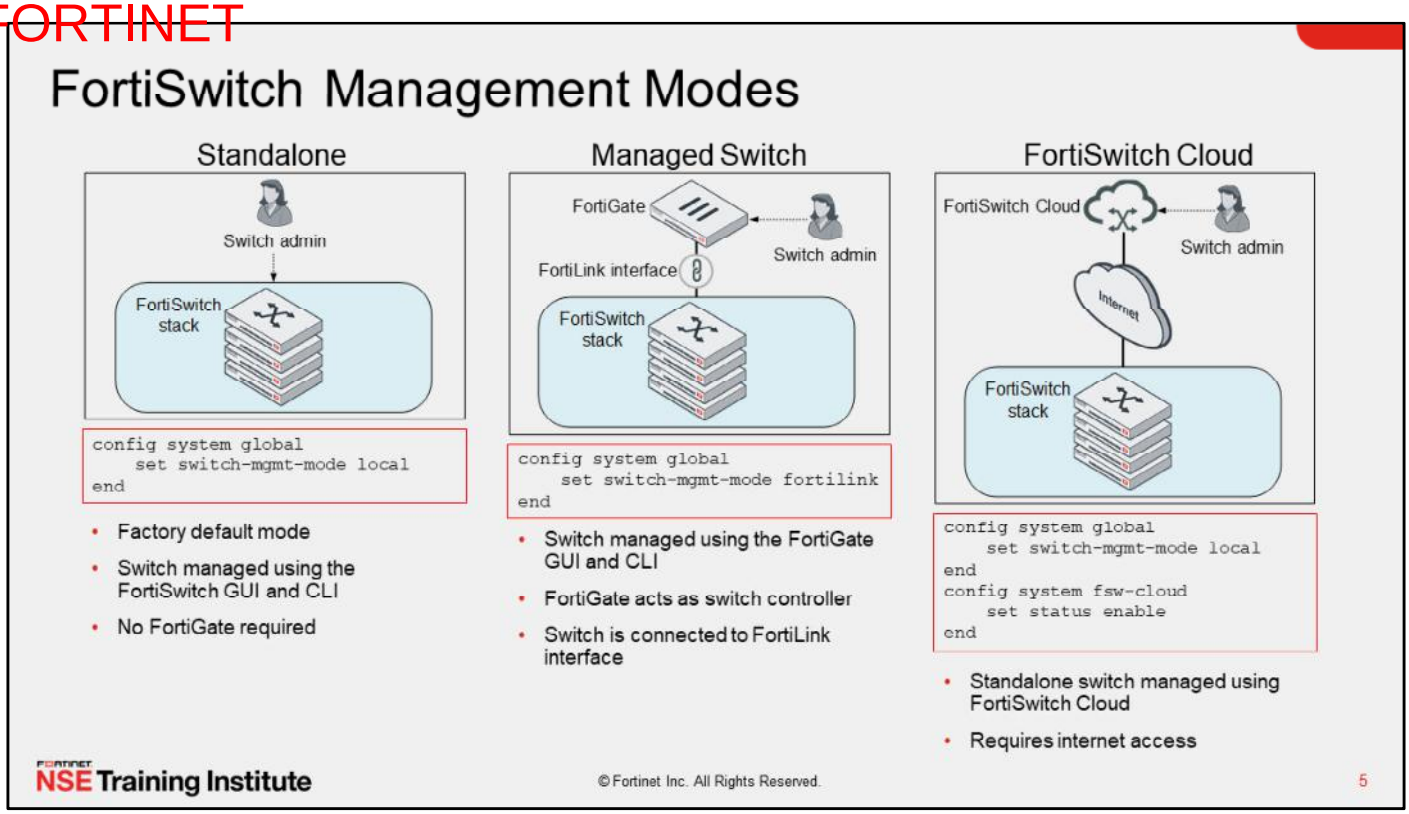
- Zero-touch provisioning: When you connect FortiSwitch to a FortiGate interface that has FortiLink enabled, FortiGate automatically discovers and provisions FortiSwitch. You can also use zero-touch provisioning by configuring the FortiGate settings on FortiManager.
- Secure configuration management: You manage FortiSwitch using the FortiGate GUI and CLI, or on FortiManager. Administrators are not required to log in to FortiSwitch.
- Centralized provisioning and maintenance: FortiSwitch becomes an extension of FortiGate. You configure firewall policies using FortiSwitch VLANs in the same way as for FortiGate VLANs. Authentication and authorization are also handled centrally on FortiGate or FortiManager.
- FortiSwitch stack: FortiGate can manage multiple FortiSwitch devices stacked in different ways to offer scalability and redundancy.
- Model range: FortiGate and FortiSwitch devices come in many sizes to accommodate the needs of customers, from retail and SMB up to data centers.

Although you can manage FortiSwitch directly on FortiGate, for the purpose of implementing a more enterprise-level approach, most of the instructions and references in this lesson are based on the FortiSwitch manager pane on FortiManager. In this scenario, FortiSwitch is still managed by FortiGate, except that the changes are made on FortiManager instead of on FortiGate. When you push the changes to FortiGate from FortiManager, FortiGate then pushes the changes to FortiSwitch.

In addition, the information displayed for FortiSwitch manager is based on per-device management mode. Per-device management mode provides you with a more friendly and practical way to achieve the objectives outlined in this lesson. The lesson also refers to some features and settings on the FortiGate CLI or GUI, only when these options are not supported by FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can deploy FortiSwitch as a standalone switch or as a managed switch.

The factory default management mode on FortiSwitch is standalone, also known as local mode. When in standalone management mode, you can manage the switch through the FortiSwitch GUI and CLI interfaces, or from FortiSwitch Cloud. FortiSwitch Cloud is a management as a service (MaaS) solution that provides centralized discovery, visibility, and configuration for standalone FortiSwitch devices. FortiSwitch Cloud requires every switch to have internet access.

When deployed as a managed switch, the switch is controlled by FortiGate, which acts as the switch controller and uses its FortiLink interface to communicate with the switch. Under this mode, you manage the switch from FortiGate. The managed switch mode is also known as FortiLink mode. This lesson covers the managed switch mode only.

This slide also shows the FortiSwitchOS CLI settings that control the switch management mode. When `switch-mgmt-mode` is set to `local`, the switch operates in standalone mode. If you also want to manage your standalone switch from FortiSwitch Cloud, ensure that the feature is enabled in `config system fsw-cloud` (it is enabled by default). When `switch-mgmt-mode` is set to `fortilink`, the switch operates in managed switch mode. Under managed switch mode, the FortiSwitch Cloud-related settings are hidden on the FortiSwitchOS CLI.

Note that when you change the `switch-mgmt-mode` setting, the switch requires a reboot.

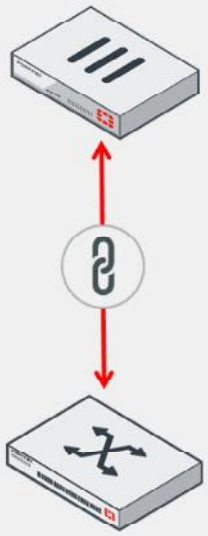
Finally, unless otherwise stated, all references in this lesson are for managed switch mode. You will learn more about standalone switch and FortiSwitch Cloud in another lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Management Protocols

- FortiLink
  - Default FortiSwitch discovery method
    - In standalone, discovery frames are sent on specific ports
  - Also used for heartbeats
    - Between FortiGate and FortiSwitch only (FortiLink interface)
  - Discovery frames include switch serial number and port information
  - Ethernet type 0x88FF
- Link Layer Discovery Protocol (LLDP)
  - Alternative method for FortiSwitch discovery
  - Used for auto-ISL configuration (switch stack)
  - Ethernet type 0x88CC
- CAPWAP
  - Switch authentication and authorization
  - Also used for heartbeats
  - Alternative firmware upgrade method
  - LLDP neighbor information
  - FortiSwitch logs export
  - UDP port 5246



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

6

FortiGate uses multiple protocols to control FortiSwitch. The protocols listed on this slide are used mainly for switch discovery, authorization, and health checks.

For discovery, FortiGate uses the FortiLink protocol by default. The FortiLink discovery frames include the switch serial number, as well as the port information on the switch. Note that when FortiSwitch is in standalone mode, only specific ports send FortiLink discovery frames by default. FortiLink is also used by managed switches that are directly connected to FortiGate to send heartbeats.

You can also use LLDP as an alternative switch discovery method. LLDP is also used when setting up a switch stack, because it enables the links connecting the switches to be automatically configured as trunks (auto-ISL). You will learn more about trunks and auto-ISL in another lesson.

CAPWAP is another control protocol that FortiGate uses to manage FortiSwitch devices. CAPWAP performs switch authentication, authorization, and health checks (heartbeats) by establishing a Datagram Transport Layer Security (DTLS) tunnel between FortiGate and the switch. It is also used as the alternative and legacy method for sending a firmware image file to a switch when you use the FortiGate GUI firmware upgrade tool. FortiSwitch also uses CAPWAP to send LLDP neighbor information and switch logs to FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Management Protocols (Contd)

- DHCP
  - Management IP address assignment
  - UDP port 67
- DNS
  - Name resolution
  - UDP port 53
- NTP
  - Time synchronization (critical for CAPWAP DTLS tunnel)
  - UDP port 123
- HTTPS
  - Configuration and diagnostics using REST API
  - Default firmware upgrade method
  - TCP port 443
- SSH
  - CLI connection tool on the GUI
  - TCP port 22



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

7

DHCP, DNS, NTP, and HTTPS are used for provisioning the switch with a management IP address, its time, name resolution, and configuration, respectively.

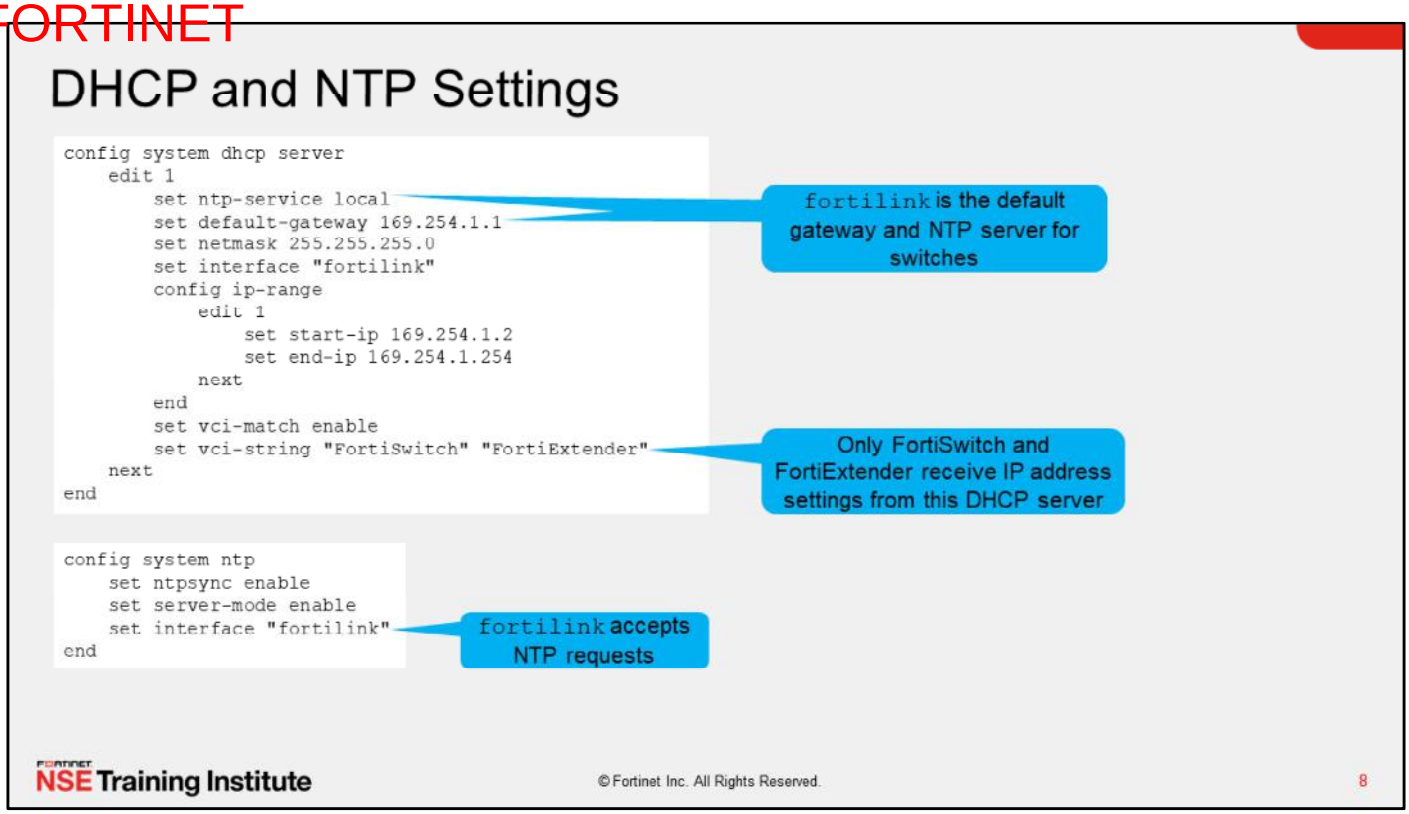
FortiGate acts as the DHCP, DNS, and NTP server for the switch. FortiSwitch uses DHCP to get an IP address from the same subnet as the FortiLink interface. In addition, FortiGate is configured to respond to DNS and NTP requests received at the FortiLink interface by default. The use of NTP is very important because the time on FortiGate and FortiSwitch *must be* in sync. Otherwise, the CAPWAP DTLS tunnel won't be established and therefore the switch won't come online.

FortiGate uses HTTPS for pushing switch configuration, collecting diagnostics, and as the switch default firmware upgrade method. For this, FortiGate uses the FortiSwitch REST API to communicate with the switch. For example, when you change the port configuration of a switch on FortiGate, FortiGate uses the FortiSwitch REST API to apply the changes on the switch. When you check the FortiSwitch ports on the GUI, FortiGate also uses the FortiSwitch REST API to obtain the current port status information from the switch. When you use the FortiSwitch firmware upgrade tool on the FortiGate GUI or CLI, FortiGate uploads the firmware image file to the switch through HTTPS.

Finally, FortiGate also uses SSH to access the switch CLI. When you use the CLI connection tool available on the GUI, FortiGate establishes an SSH connection to the switch management IP address.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

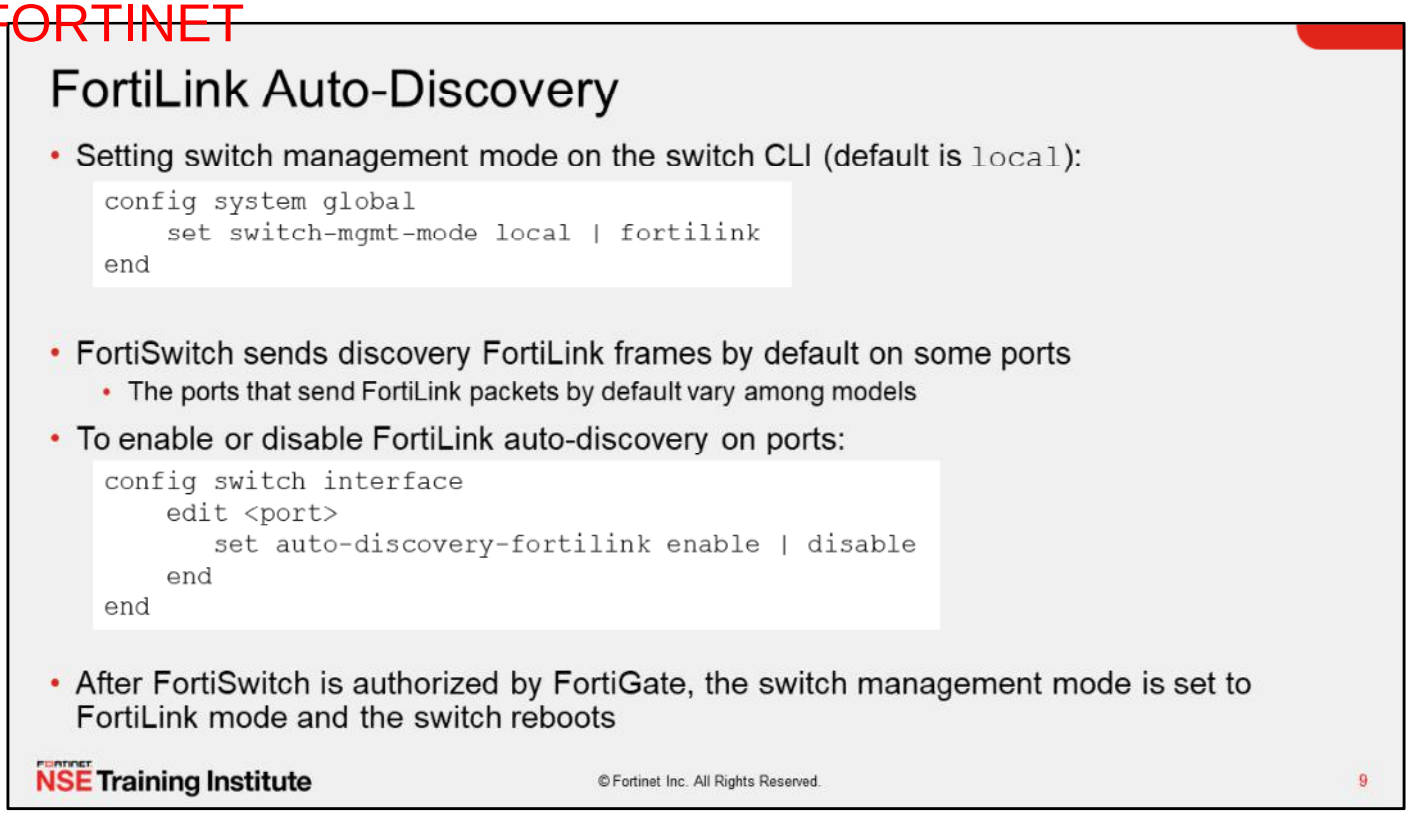


The default DHCP scope for the default FortiLink interface sets FortiGate as the default gateway, NTP server, and DNS server for its managed switches. The DHCP scope is automatically configured based on the IP address and netmask assigned to the interface. By default, the default FortiLink interface is assigned the IP address `169.254.1.1` and netmask `255.255.255.0`. In addition, the DHCP scope is also restricted to Vendor Class Identifiers (VCIs) `FortiSwitch` and `FortiExtender`. This means that only FortiSwitch and FortiExtender devices can obtain addresses from that scope.

For NTP, FortiGate is configured to respond to NTP requests received at the FortiLink interface.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



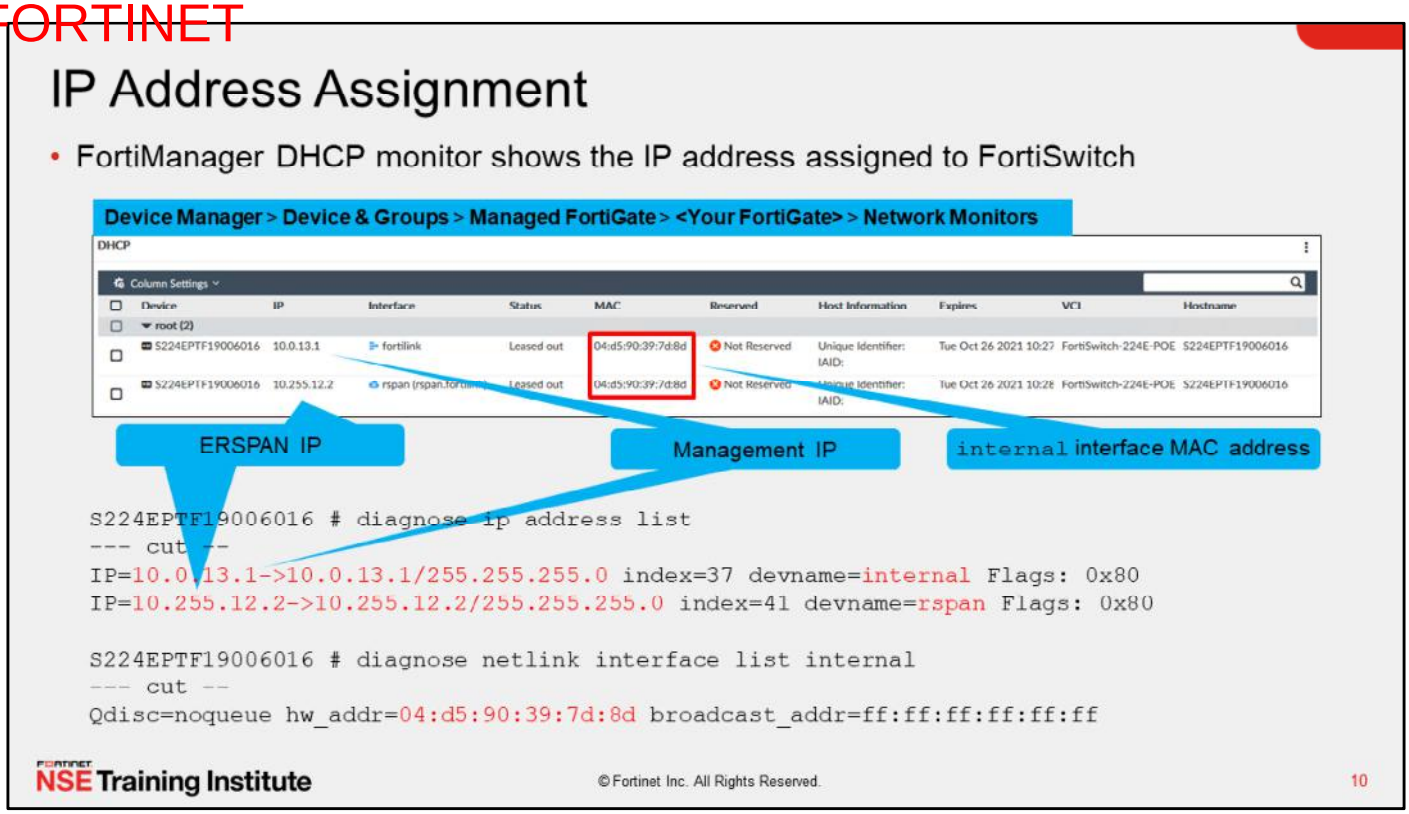
By default, the switch management mode is set to `local` (also known as standalone). The slide shows how to change the management mode directly on the switch CLI. However, despite the switch operating in local management mode by default, some of the switch ports are also configured to broadcast FortiLink discovery frames by default. This set of ports varies among switch models. For example, in a FortiSwitch 224E-POE, these ports are 21 to 28.

If you want a port to send out FortiLink discovery frames, you can enable `auto-discovery-fortilink` on the port.

When FortiGate receives FortiLink discovery frames on any of its FortiLink interface port members, FortiGate adds the switch to the list of managed switch and displays it as unauthorized. After you authorize the switch on FortiGate, the switch management mode is changed to `fortilink`, which causes the switch to reboot.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiGate assigns two IP addresses to FortiSwitch through DHCP. The network monitors on FortiManager displays the DHCP records table, which includes the FortiSwitch hostname, MAC address, and assigned IP addresses.

The two IP addresses assigned over DHCP are:

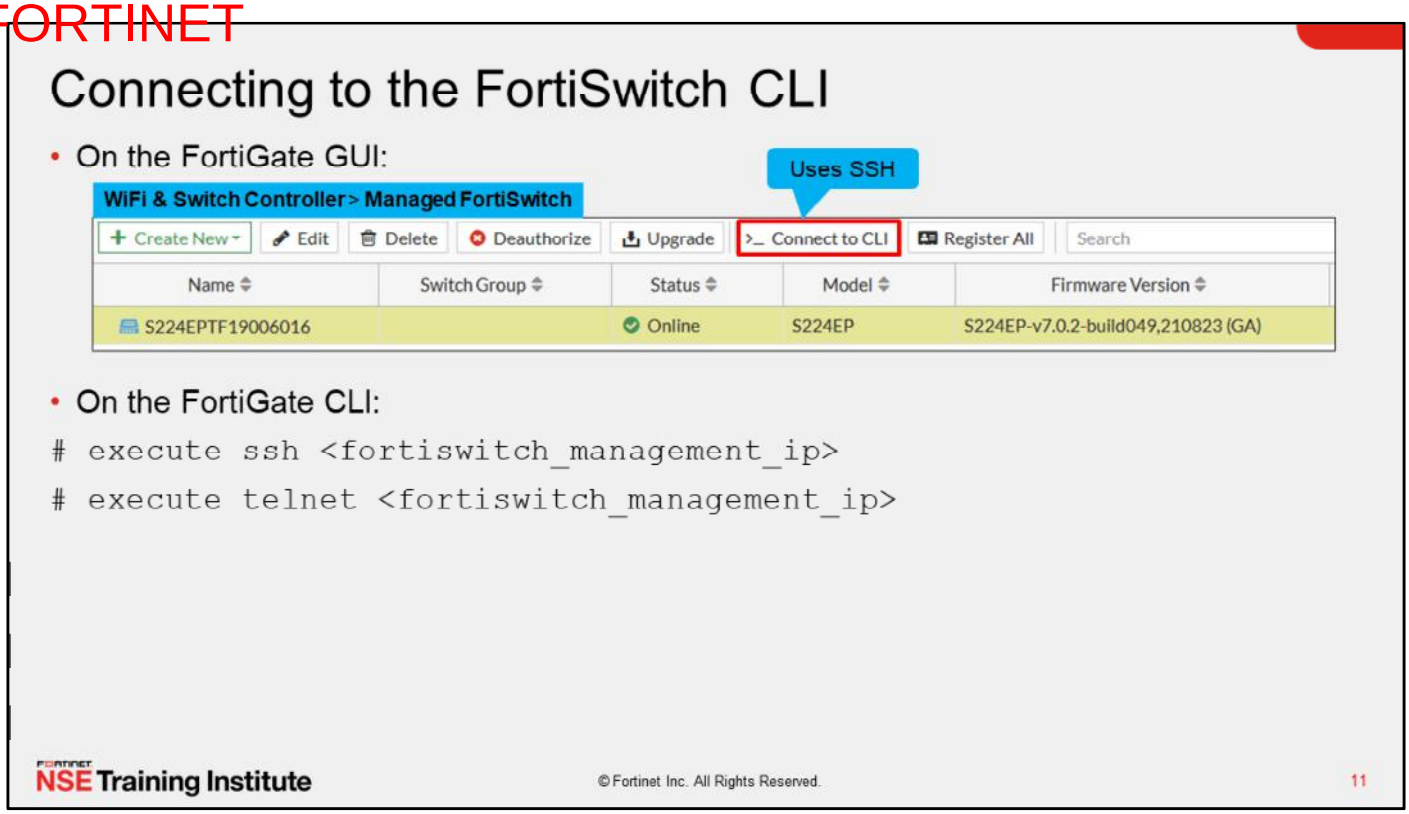
- Management IP address: The IP address is on the same subnet as the FortiLink interface. It is used for management communication between FortiGate and the switch.
- ERSPAN IP address: Encapsulated remote SPAN (ERSPAN) enables FortiSwitch to encapsulate mirrored traffic into GRE and send it across a Layer 3 network. The ERSPAN IP address is used as the source IP address of the encapsulated traffic. Note that FortiSwitch also supports remote SPAN (RSPAN), but this IP address is used by ERSPAN *only*.

On the FortiSwitch side, the management and ERSPAN IP addresses are assigned to the `internal` and `rspan` interfaces, respectively. Because `rspan` is a VLAN interface bound to `internal`, both interfaces share the same MAC address.

The `internal` interface is a logical in-band management interface that is accessed through the switch ports. Some FortiSwitch models also come with a dedicated physical management port named `mgmt`, that provides you with out-of-band management for the switch.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

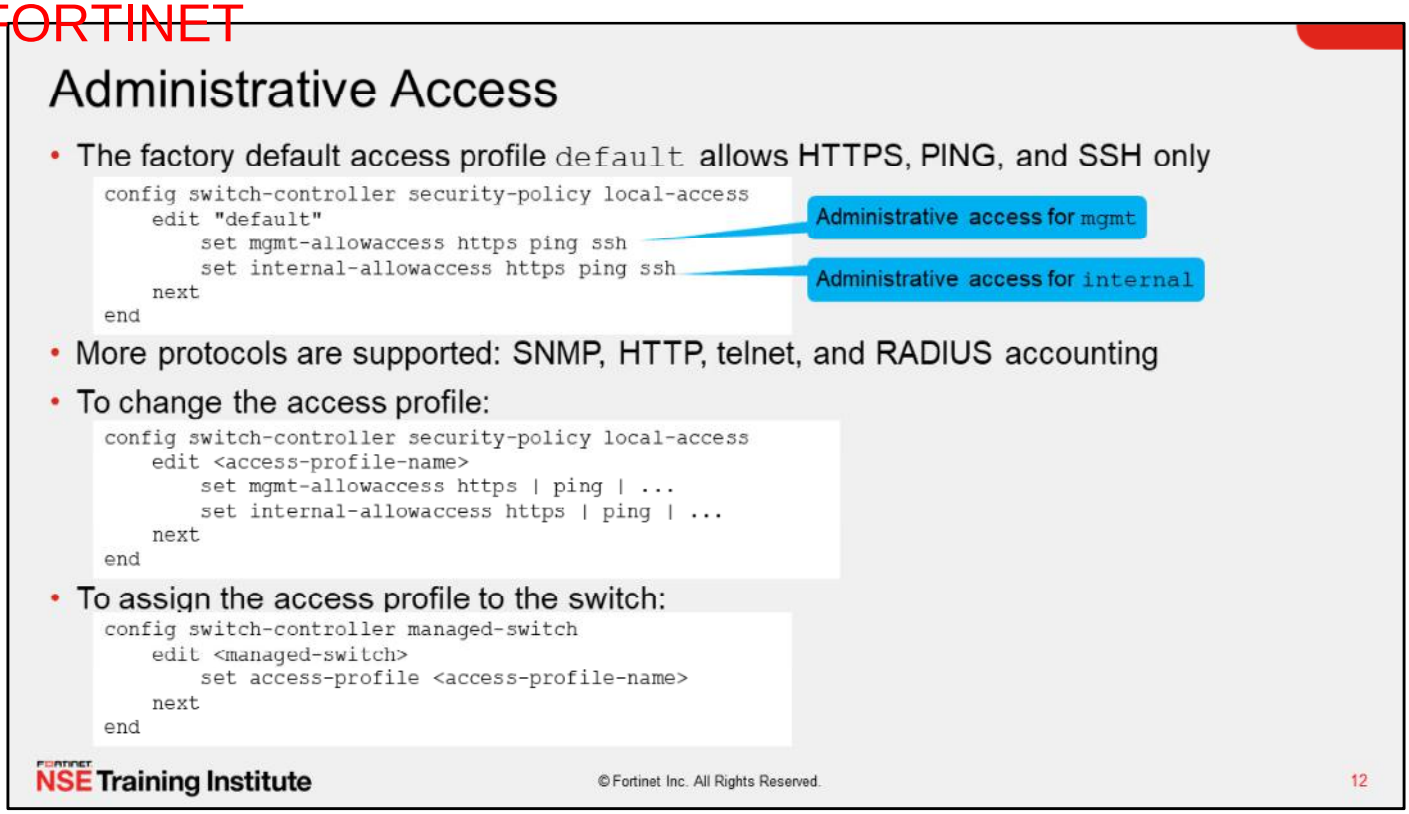


Once FortiSwitch is managed by FortiGate, you usually do not need to connect to the FortiSwitch GUI or CLI. All the administration is done on FortiGate or FortiManager. However, if access to the FortiSwitch CLI is required, you can connect to it over SSH or telnet by running the commands shown on this slide. Just keep in mind that, by default, only SSH, HTTPS, and PING access is enabled on the switch `internal` interface. Therefore, you must first enable telnet access on the switch if you want to connect to its CLI over telnet.

You can also connect to the FortiSwitch CLI using the FortiGate GUI. When you use this method, FortiGate establishes an SSH connection to the switch management IP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

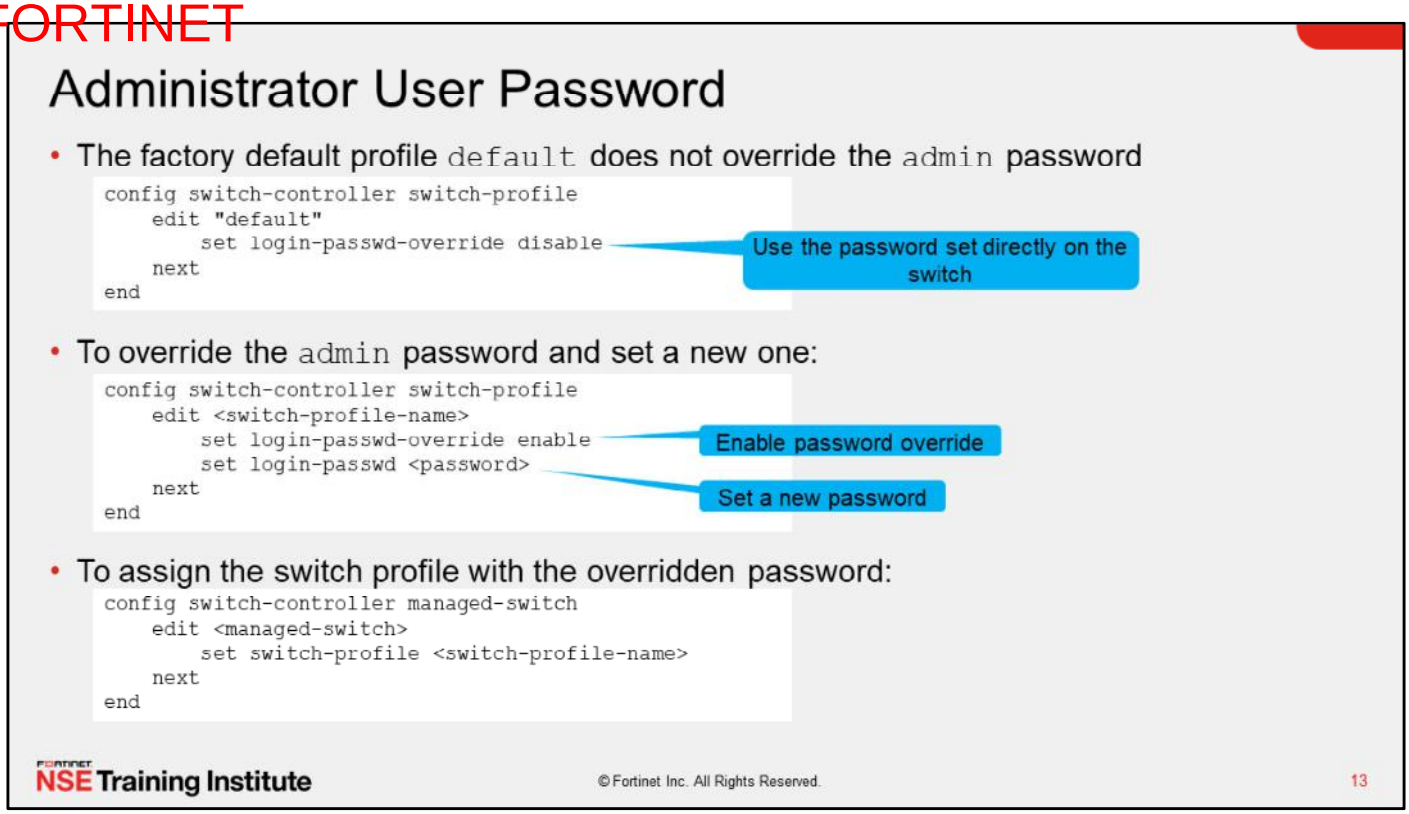


The administrative access on a managed switch is controlled by the access profile assigned to the switch. A factory default access profile named `default` is assigned to the switch after it is authorized on FortiGate. The `default` access profile has HTTPS, PING, and SSH administrative access enabled for both the `mgmt` and `internal` interfaces.

If you need to edit the administrative access on a switch, you must create a new access profile and assign it to the switch, or edit the existing default access profile to suit your needs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

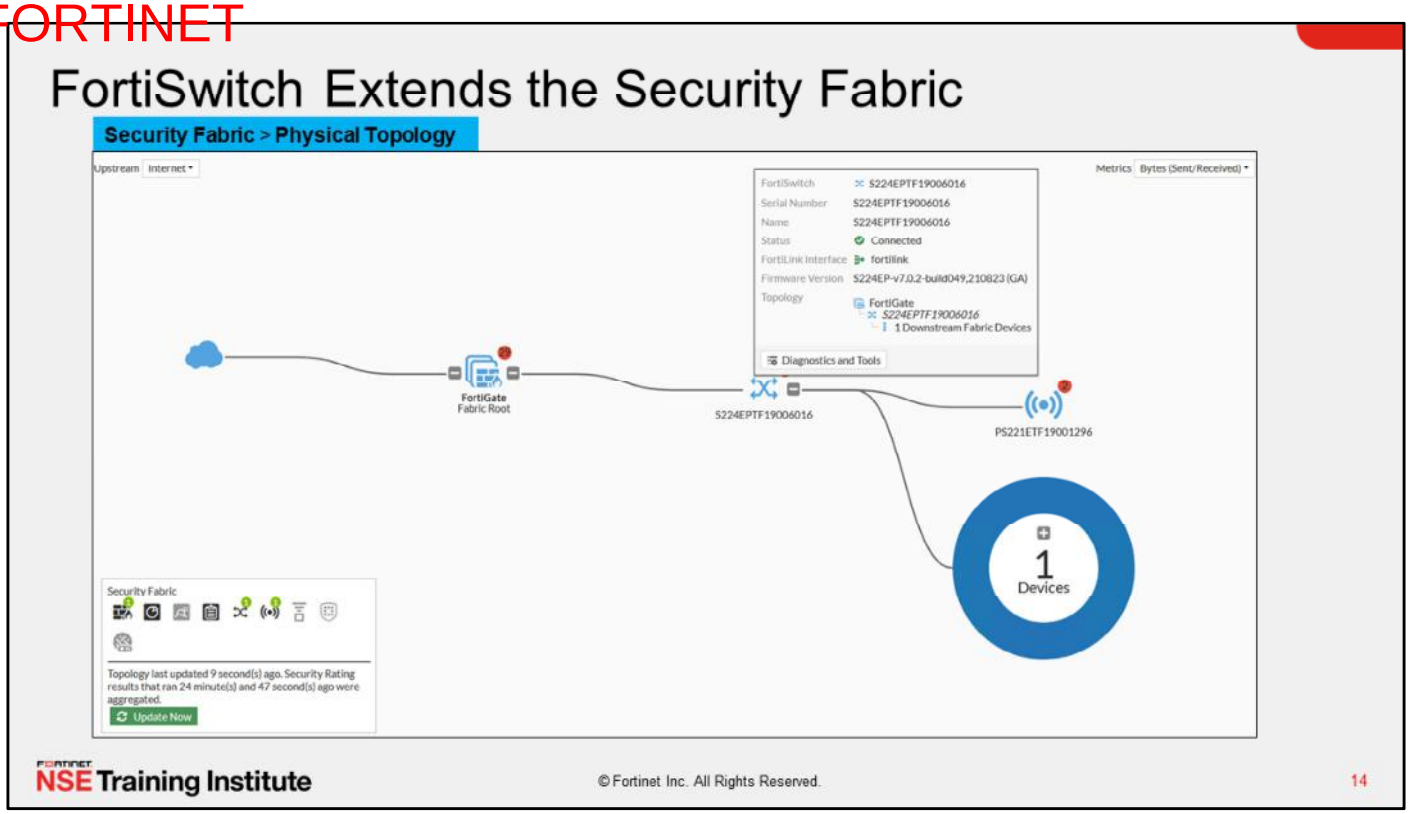


The `admin` password on a managed switch is controlled by the switch profile assigned to the switch. A factory default switch profile named `default` is assigned to the switch after it is authorized on FortiGate. The `default` switch profile does not change the `admin` user password set directly on the switch.

If you need to override the `admin` password on the switch with one of your preferences, you must create a new switch profile and assign it to the switch, or edit the existing default switch profile.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

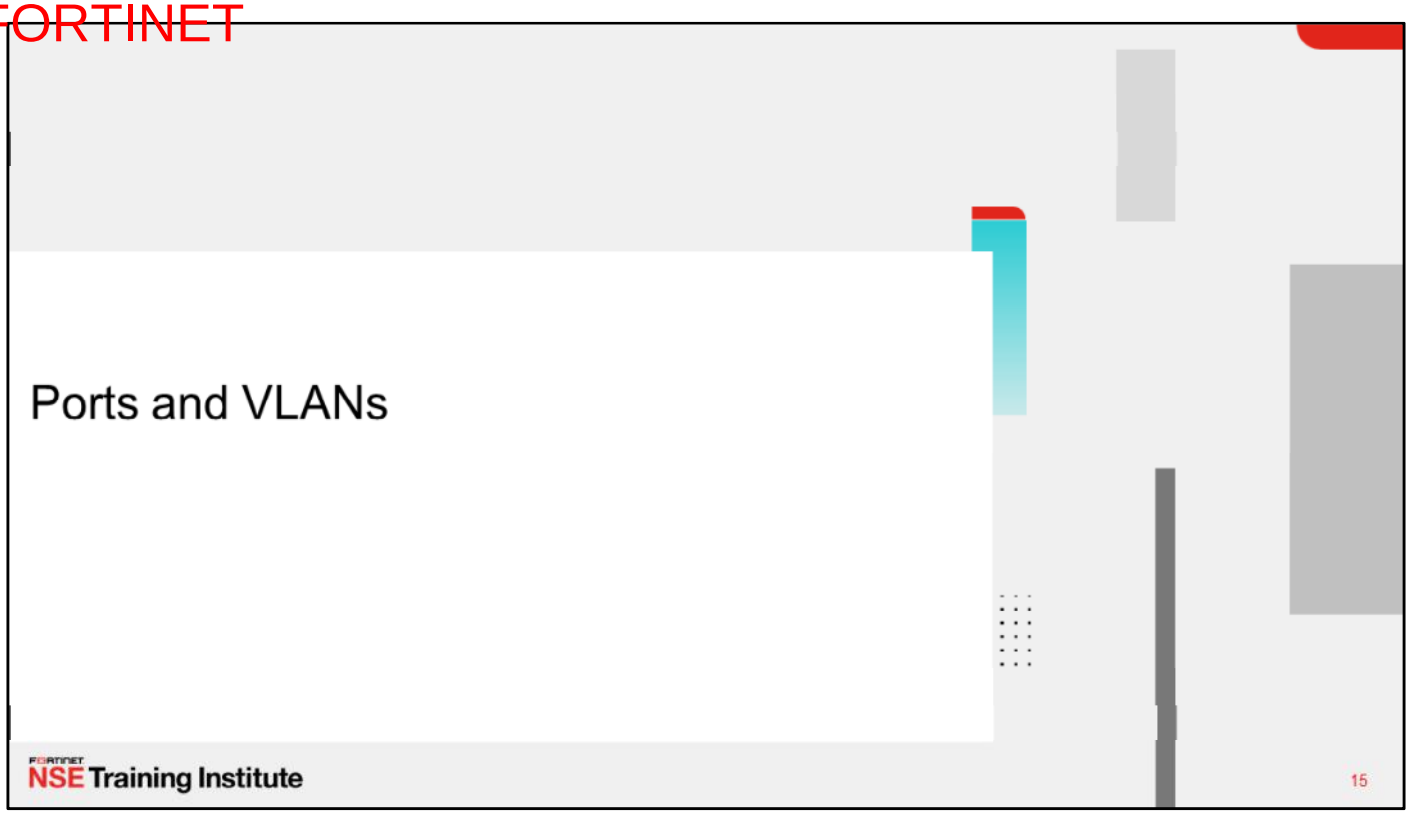


A managed FortiSwitch is an extension of a FortiGate device. In this way, FortiSwitch extends the visibility of the Fortinet Security Fabric up to Layer 2. Using FortiView physical and logical topology views, you can visualize different security segments together with the stacked FortiSwitch and connected end devices.

In the example shown on this slide, the Security Fabric physical topology view shows the FortiSwitch location in the network, as well as its directly connected FortiAP device.

Vouchers & Dumps are Available | WhatsApp +201224560923

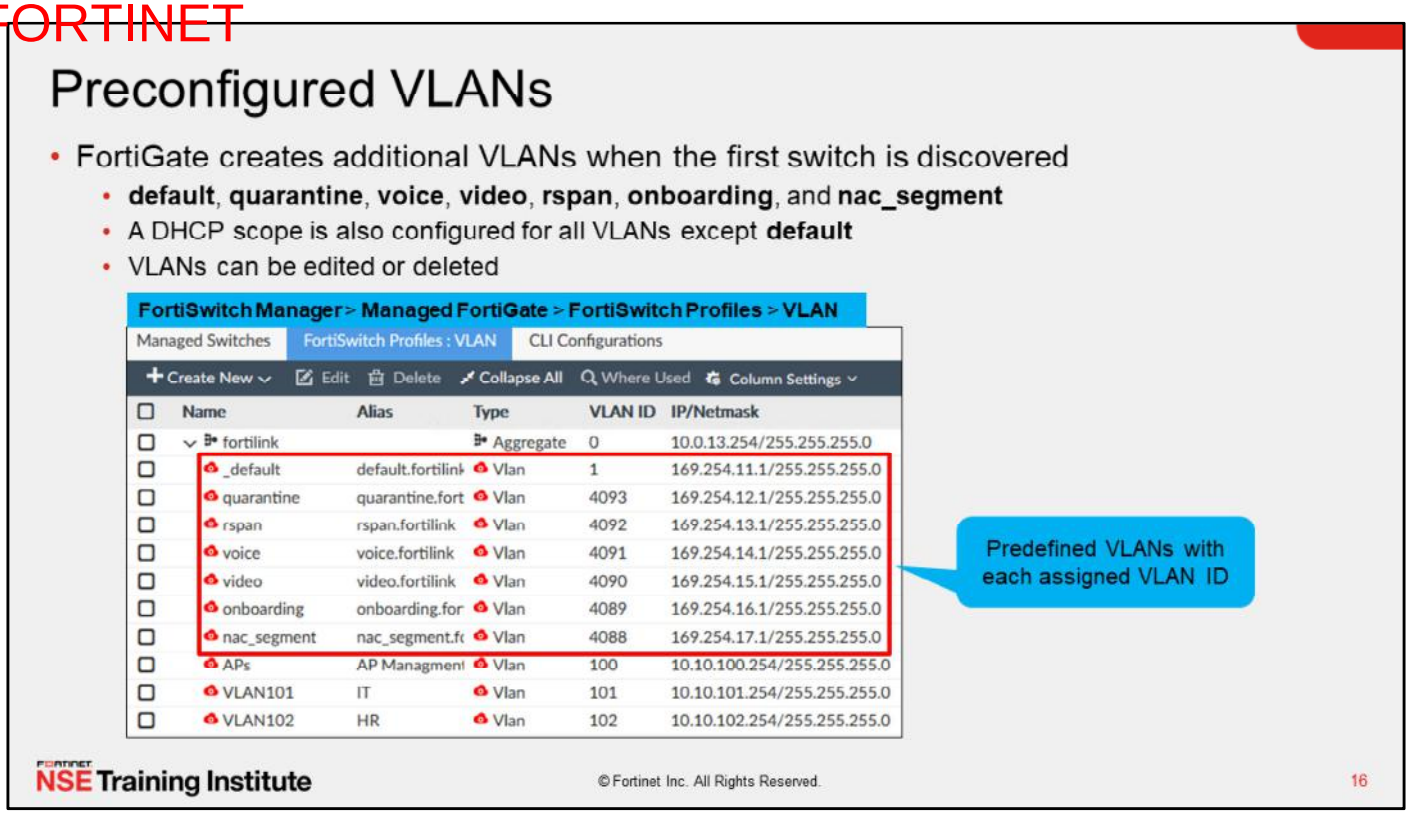
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn how to configure FortiSwitch ports and VLANs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



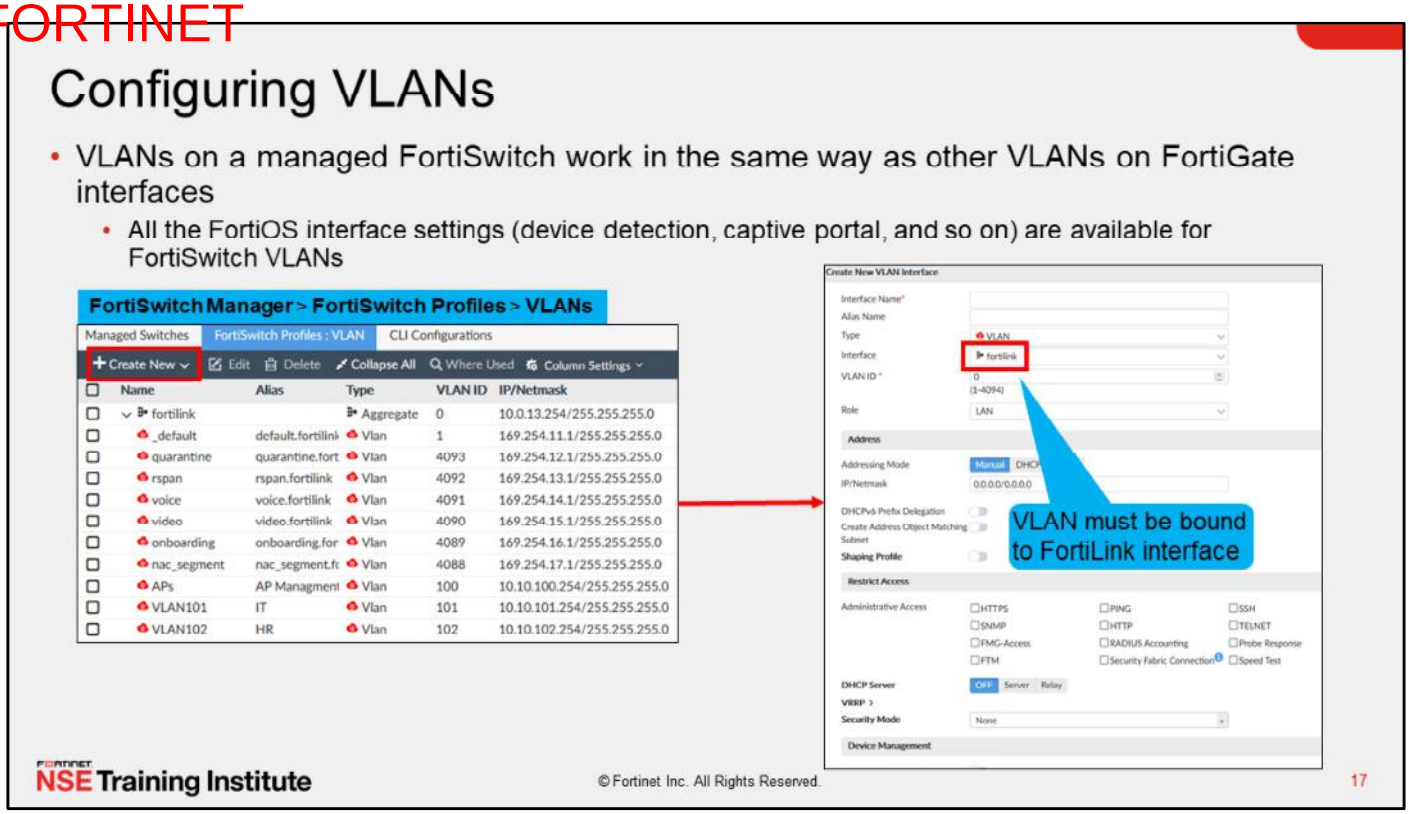
When FortiGate discovers the first switch, it automatically adds to its configuration some settings that are needed for switch management. These settings include the following VLANs:

- Default: This is the default native VLAN assigned to all switch ports.
- Quarantine: This is the default VLAN used for quarantined traffic. On FortiGate, you can quarantine a device connected to a switch, upon which the device is placed in the quarantine VLAN.
- RSPAN: It is used for sending encapsulated mirrored traffic across the network.
- Voice: When using LLDP-MED, you can assign the switch port to this VLAN if the endpoint is detected as a voice device.
- Video: Same as the voice VLAN, but used when the endpoint is detected as a video device.
- Onboarding: When network access control (NAC) policies are enabled, this is the VLAN where devices that do not match any of the configured NAC policies are placed. You will learn more about NAC policies in this lesson.
- NAC segment: Used to prevent hosts from having to renew IP addresses when moving to another VLAN.

In addition, a DHCP scope is configured for all the preconfigured VLANs except the default VLAN. The VLANs are also assigned with the predefined VLAN IDs shown in the example on this slide, and they can be edited or deleted if required.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

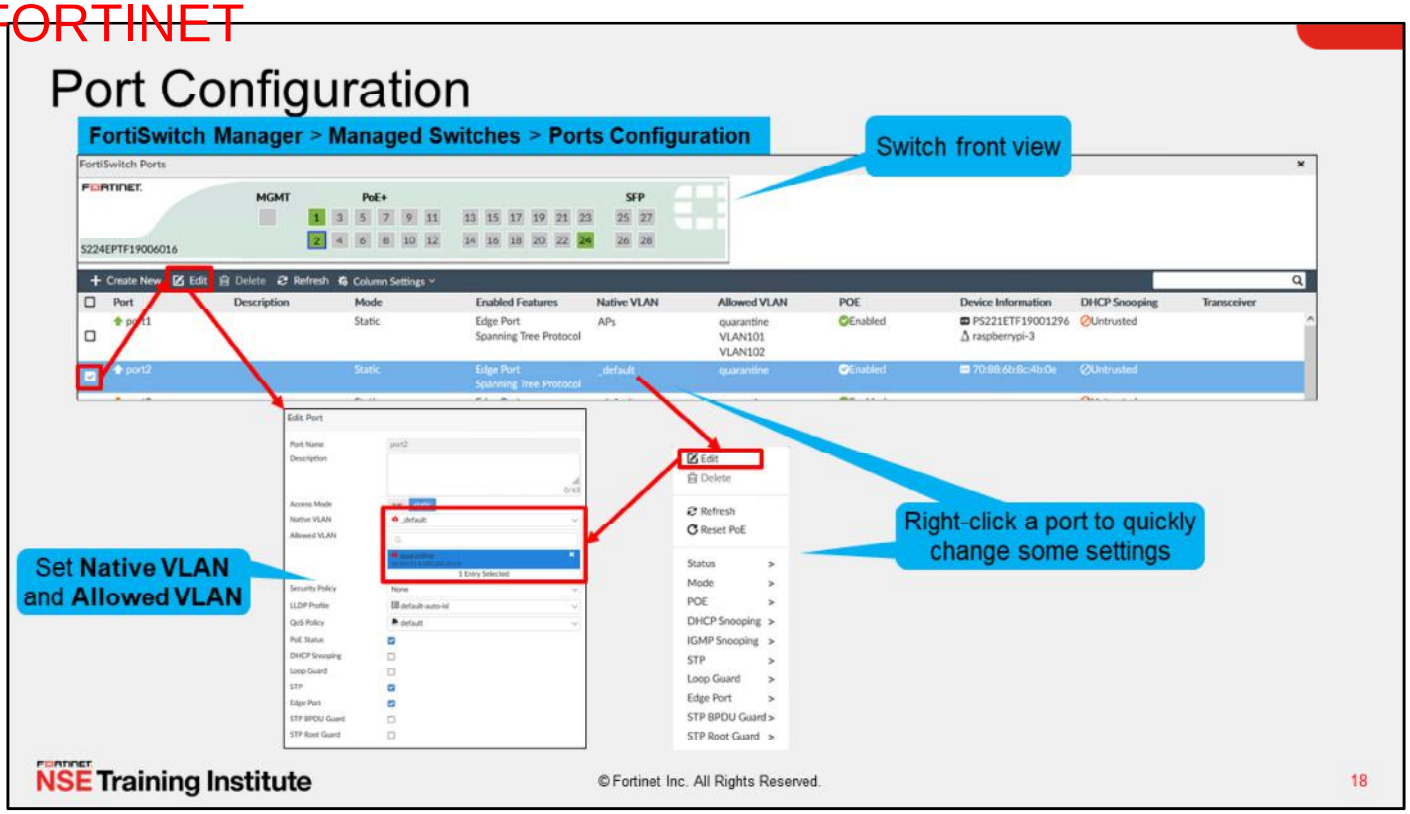


When you manage a switch from FortiGate, the switch becomes an extension of FortiGate. You configure and use FortiSwitch VLANs in the same way as FortiGate VLANs. Just keep in mind that a FortiSwitch VLAN *must be* bound to the FortiLink interface. Otherwise, you won't be able to select the VLAN when configuring the VLAN settings on a switch port.

In addition, all interface settings usually available on FortiGate VLANs are available on FortiSwitch VLANs, such as device detection, captive portal, and so on.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



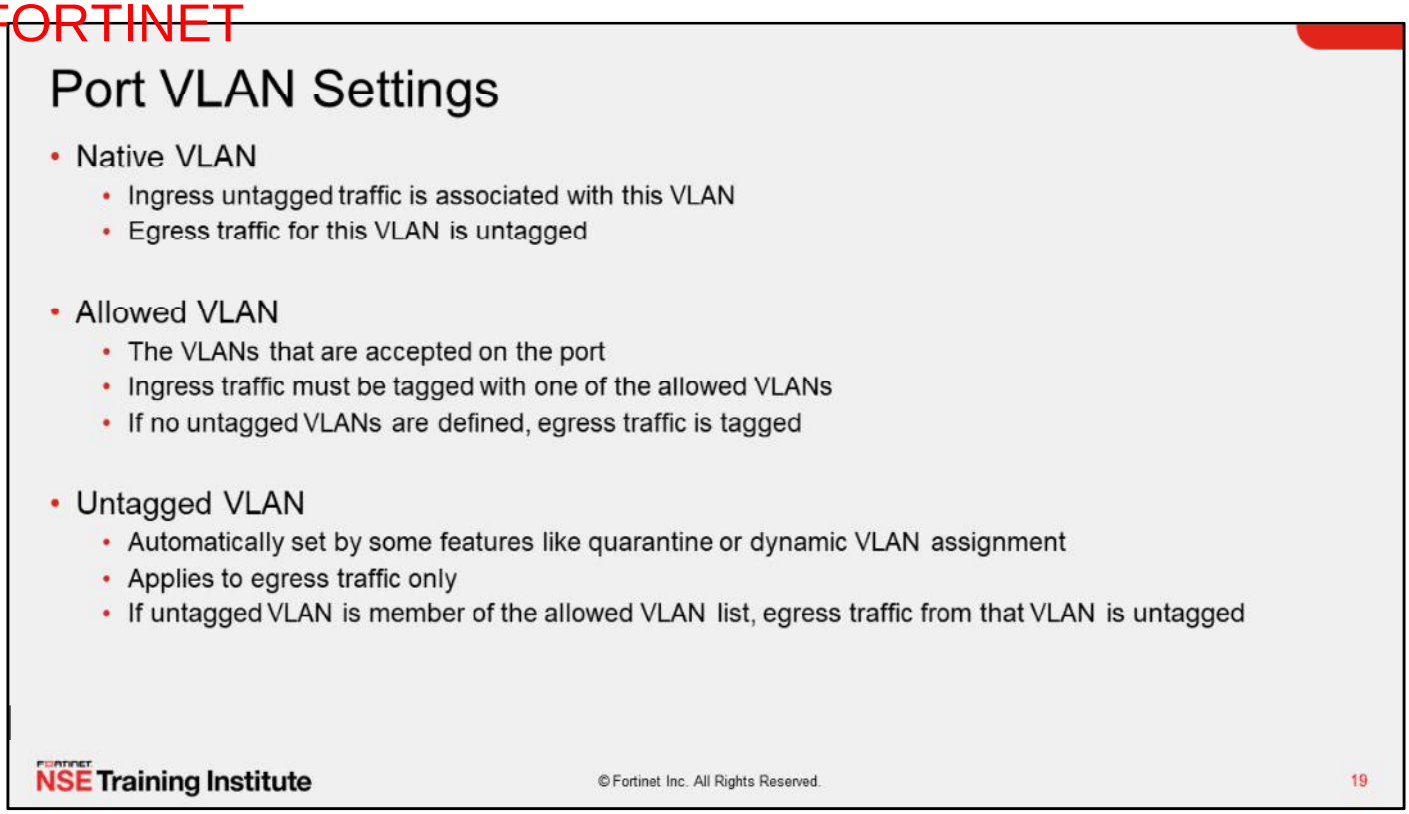
Ports Configuration on FortiSwitch manager displays all the ports available on the switch. On FortiSwitch manager, you can view or edit the configuration of each port.

To edit the settings on a port, select the port and click **Edit** to display a new window showing the port settings available. On this window, you can assign the **Native VLAN**, as well as the **Allowed VLAN** list for the port. You will learn more about these VLANs in this lesson.

In addition, when you right-click a port, a context menu is shown with some settings available for the port. Moreover, on the ports configuration page, FortiManager also displays the switch front view, indicating the status of all ports on the switch.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiSwitch can process both tagged and untagged Ethernet frames. When you configure a port, you must ensure that the port VLAN settings match the VLAN tagging required by the connected device for ingress and egress traffic. Below are the VLAN settings that define how the port handles tagged and untagged traffic. Note that the ingress and egress traffic refers to the traffic entering and leaving the switch port, respectively.

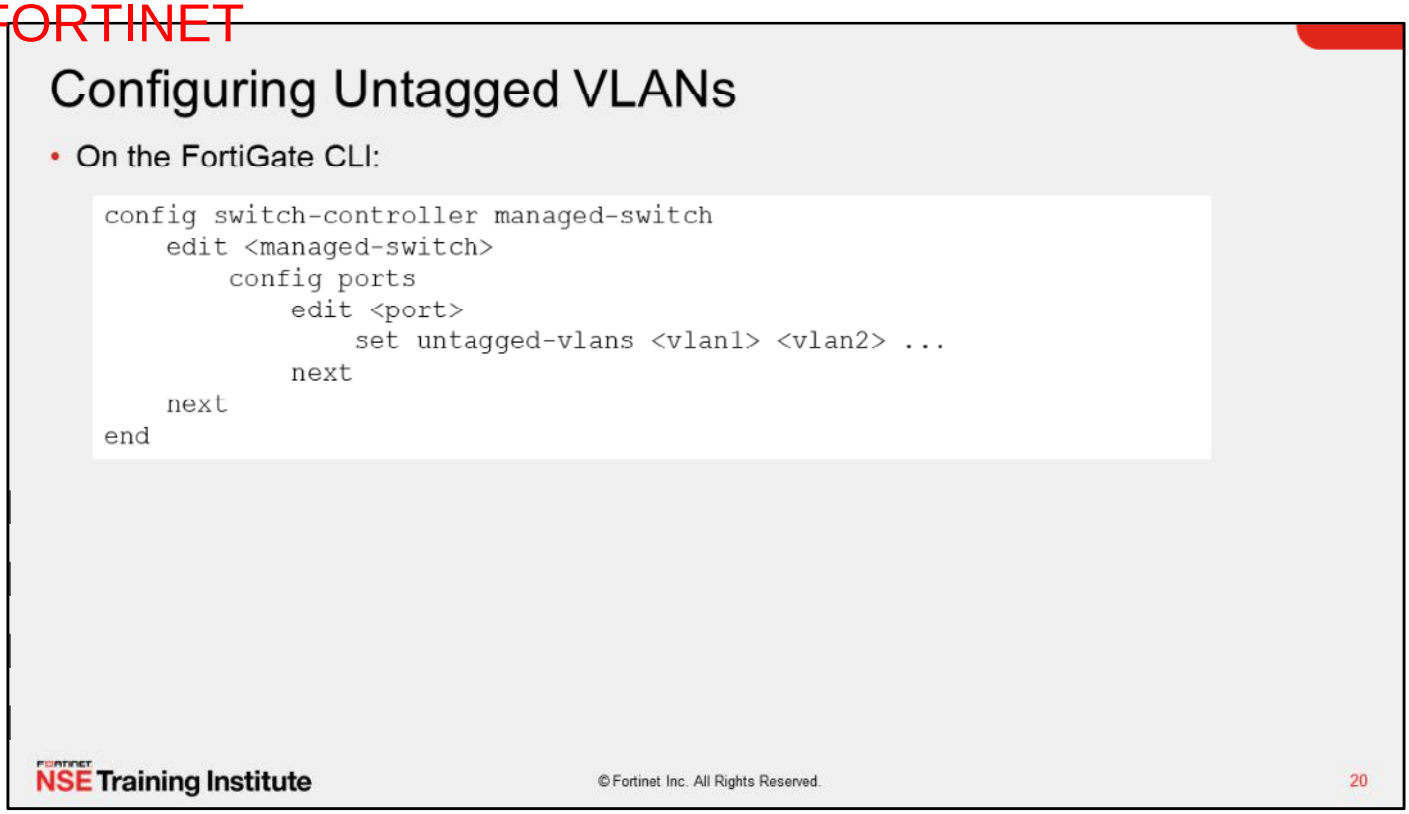
- Native VLAN: In most cases, this refers to the VLAN assigned to the endpoint. The native VLAN can be defined as the default VLAN for untagged ingress traffic. Because most endpoints send traffic without VLAN tag, then the endpoint traffic is placed in the VLAN defined as the native VLAN. Frames for egress traffic matching the native VLAN are also sent untagged.

- Allowed VLAN: Defines the list of VLANs that are allowed on the port for both ingress and egress traffic, and for both tagged and untagged traffic. The native VLAN is implicitly allowed on the port, and therefore, you don’t need to include it in the allowed VLANs list. For the port to accept incoming frames tagged with VLANs other than the native VLAN, the frames must be tagged with one of the VLANs defined in the allowed VLAN list. When there are no VLANs defined as untagged VLANs, the egress traffic for an allowed VLAN is tagged. The allowed VLAN settings is key on inter-switch links (ISLs), and in the FortiLink trunk, because the traffic forwarded between the switches, and between the switch and FortiGate, are usually tagged with multiple VLANs. You may also need to adjust the allowed VLAN settings on ports connecting endpoints that send and expect to receive tagged traffic. This is the case for some IP phones or servers that leverage the use of VLAN tags for their applications.

- Untagged VLAN: Usually, you don’t have to configure this setting. However, some features like quarantine MAC or dynamic VLAN assignment, require it for the feature to work. The setting applies only to egress traffic, and defines a list of VLANs for which the egress traffic is sent untagged. In order for the setting to take effect, the untagged VLAN must also be a member of the allowed VLAN list.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can configure the `untagged-vlans` setting by running the commands shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Power Over Ethernet (PoE)

- Display PoE status:
  - On **FortiSwitch Manager** > **More** > **Faceplates**



  - On the FortiGate CLI

```
FortiGate # diagnose switch-controller switch-info poe detail S224EPTF19006016 port1
VDOM: root
Managed Switch : S224EPTF19006016     0

Port(1) Power:3.90W,    Power-Status: Delivering Power
Power-Up Mode: Normal Mode
Remote Power Device Type: IEEE802.3AF PD
Power Class: 3
Defined Max Power: 16.2W, Priority: Low.
Voltage: 54.01V
Current: 74mA
Temperature: 31.25 Centigrade
```

- Reset PoE on the FortiGate CLI:

```
FortiGate # execute switch-controller switch-action poe reset S224EPTF19006016 port1
Toggling power on port1.........
```

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

21

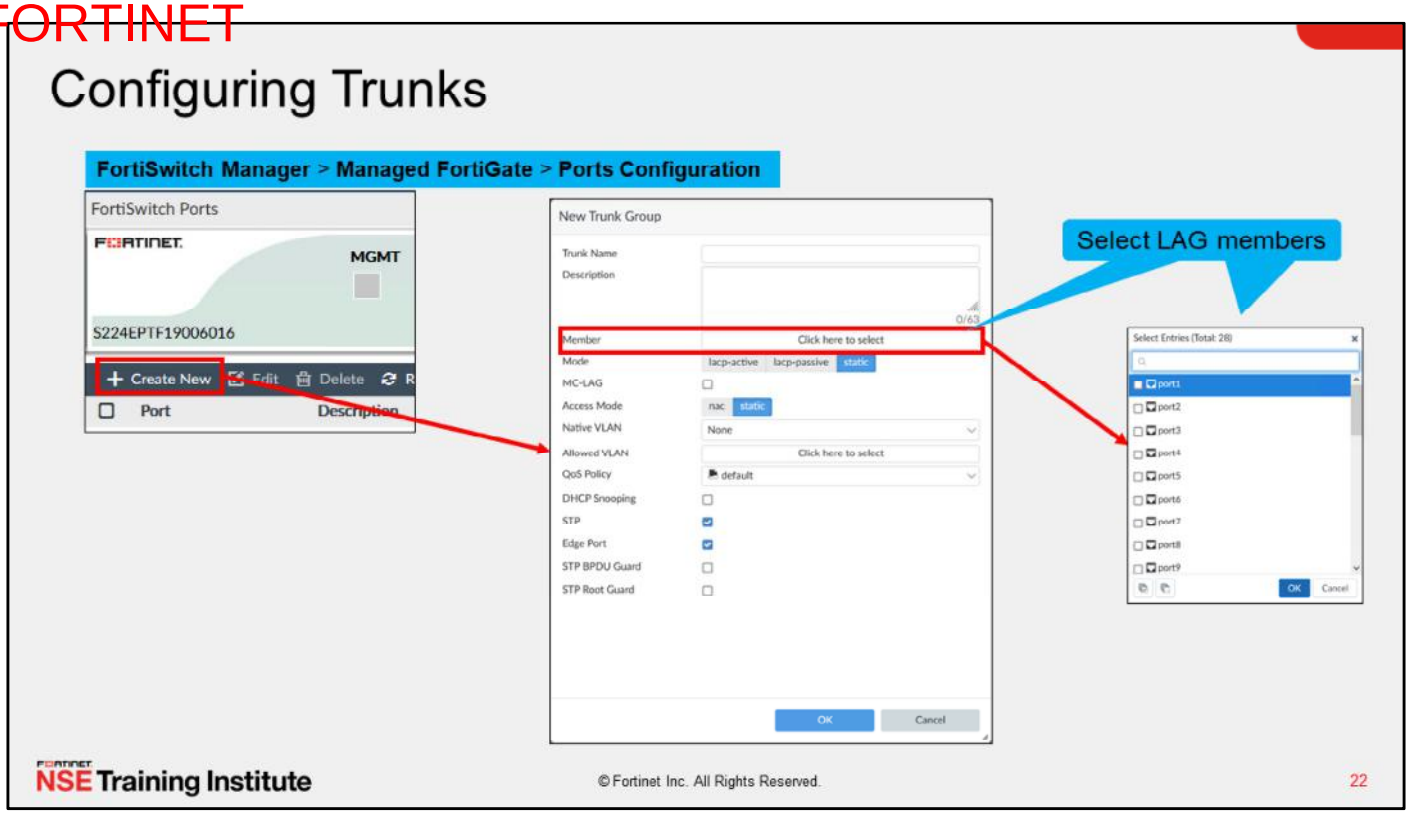
If you have PoE-powered devices connected to PoE-enabled switch ports, you can check the current PoE status on the switch port from the faceplates section on FortiSwitch manager. Hover over the port to get the amount of power delivered by the port.

Alternatively, you can also display the PoE information from FortiGate CLI by running the command shown on the slide. Compared to FortiSwitch manager, the command displays more details about PoE, such as the power class, voltage, current, and maximum power.

In case you want to reset the PoE delivery on a port, you can run a FortiGate CLI command like the one shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



In FortiSwitch, a trunk is a link aggregation group (LAG) interface. Although other vendors use the term trunk when referring to interfaces that accept tagged Ethernet frames, for FortiSwitch, a trunk is just a LAG interface.

When you connect two FortiSwitch devices together, or when you connect FortiSwitch to the FortiGate FortiLink interface, a trunk is automatically formed on the switch by the auto-ISL feature used by LLDP. Other devices connecting to FortiSwitch using a LAG require that you manually configure a trunk on FortiSwitch. You can manually configure a trunk on FortiSwitch manager by clicking **Create New** on the **Ports Configuration** page, to display a new window with the settings available for the trunk.

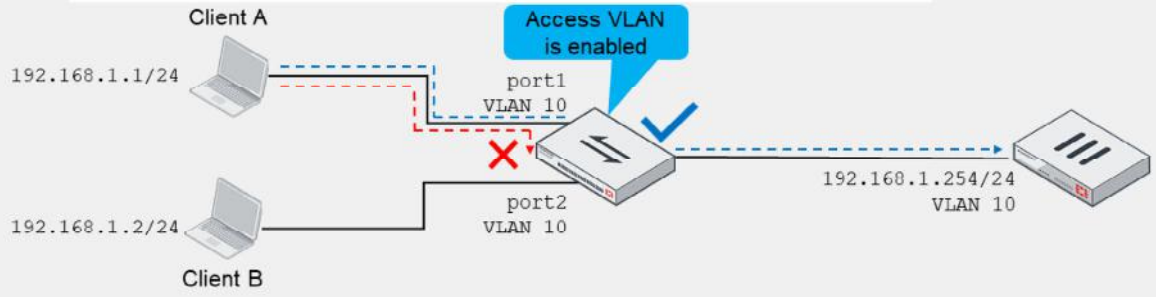
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Access VLANs

- Prevent intra-VLAN communication
  - Devices can communicate only with FortiGate
  - Can be used for isolating devices before authentication or detection is completed
  - FortiGate CLI setting (enabled on the quarantine and onboarding VLANs by default):

```
config system interface
    edit <vlan>
        set switch-controller-access-vlan enable | disable
    next
end
```



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

23

Access VLANs enable FortiSwitch to prevent direct communication among devices in the same VLAN. Devices can communicate only with FortiGate. Traffic destined for other devices in the same VLAN is dropped by FortiSwitch. Although other vendors use the term “access VLAN” when referring to the native or untagged VLAN on a switch port, in FortiSwitch, “access VLAN” just refers to a VLAN that allows traffic to the switch controller only.

Access VLANs can be used to place devices in a temporary or onboarding VLAN before they are authenticated or identified by FortiGate, upon which FortiGate moves the device to the corresponding production VLAN. Another use case for access VLANs is when you want to drop intra-VLAN traffic because the devices don’t require client-to-client communication. This could prevent the spread of malware by compromised hosts, reduce the amount of traffic in the network, or prevent an attacker from gathering network information that can be later used to attack vulnerable hosts in the same VLAN.

You can enable access VLANs on a FortiSwitch VLAN by running the CLI commands shown on this slide. Note that access VLAN is enabled on the quarantine and onboarding VLANs by default.

In the network diagram shown on this slide, port1 and port2 on FortiSwitch are placed in VLAN 10, which is a FortiSwitch VLAN configured on FortiGate with access VLAN enabled. As a result, when client A sends traffic destined to devices other than the VLAN 10 interface on FortiGate, FortiSwitch drops the traffic.

Vouchers & Dumps are Available | WhatsApp +201224560923

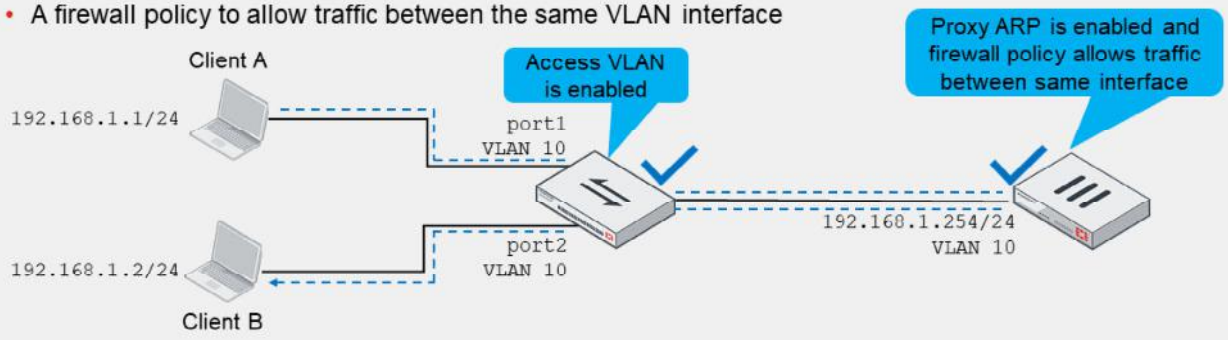
DO NOT REPRINT
© FORTINET
Brave-dumps.com

Access VLANs—Allow Intra-VLAN Traffic

- Intra-VLAN communication *through* FortiGate can be allowed by configuring:
  - Proxy ARP in FortiGate, for example:

```
config system proxy-arp
    edit 1
        set interface "VLAN 10"
        set ip 192.168.1.1
        set end-ip 192.168.1.253
    next
end
```

  - A firewall policy to allow traffic between the same VLAN interface



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

24

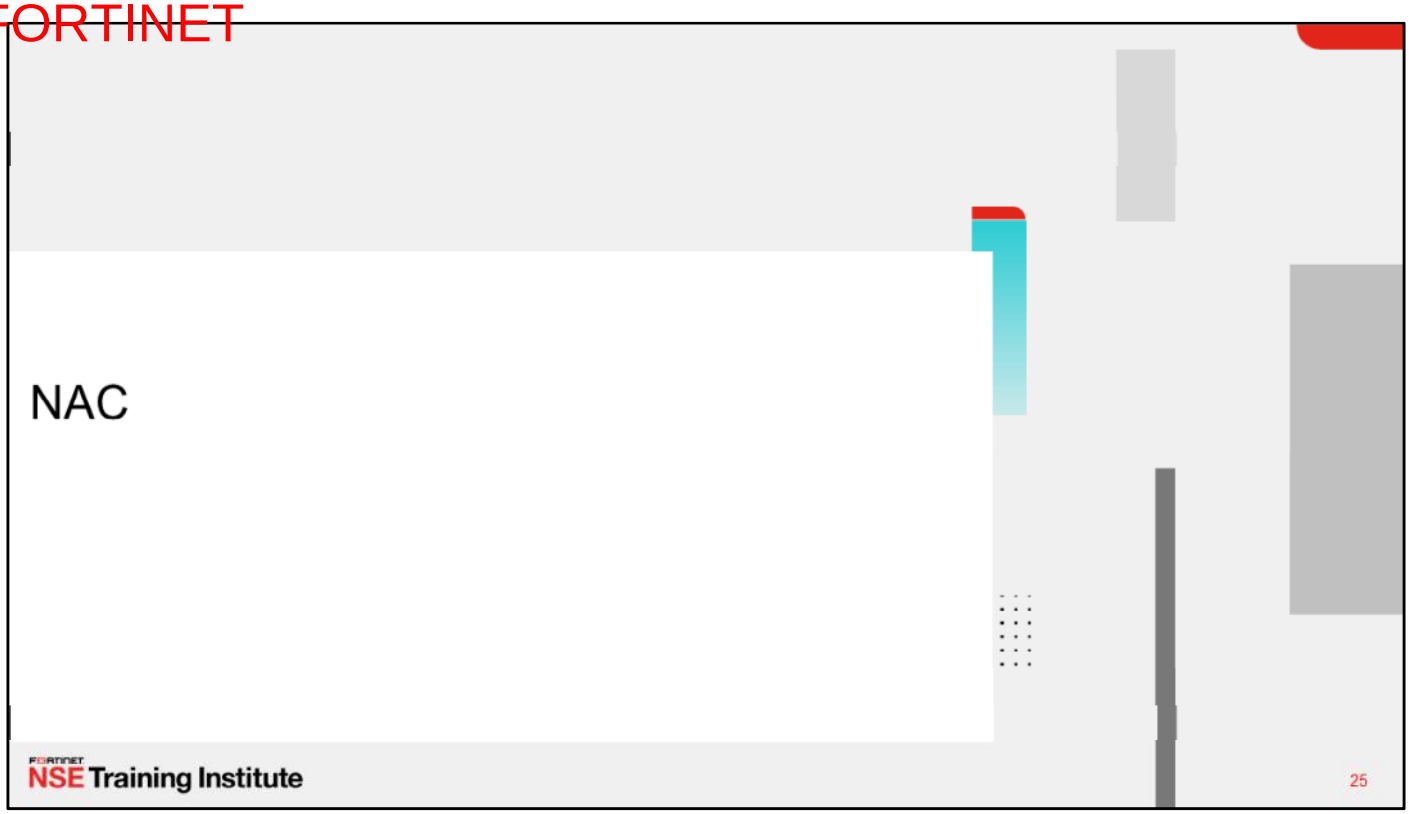
When access VLAN is enabled, you can still allow intra-VLAN traffic *through* FortiGate by having FortiGate perform proxy ARP for other hosts in the VLAN, and by having firewall policies allowing the intra-VLAN traffic.

This slide shows an example of the proxy ARP configuration needed on FortiGate based on the network diagram shown on the slide. When client A sends ARP requests for resolving the MAC address of client B, FortiGate responds to ARP requests on behalf of client B. As a result, when client A communicates with client B, packets from client A to client B are sent through FortiGate, which is a traffic that is allowed by FortiSwitch. When traffic arrives at FortiGate, the traffic is then forwarded to client B because FortiGate has a firewall policy allowing the intra-VLAN traffic.

When you configure the firewall policy, you must select the same VLAN interface as the incoming interface and the outgoing interface. You can also enable security profiles to perform inspection if required.

Vouchers & Dumps are Available | WhatsApp +201224560923

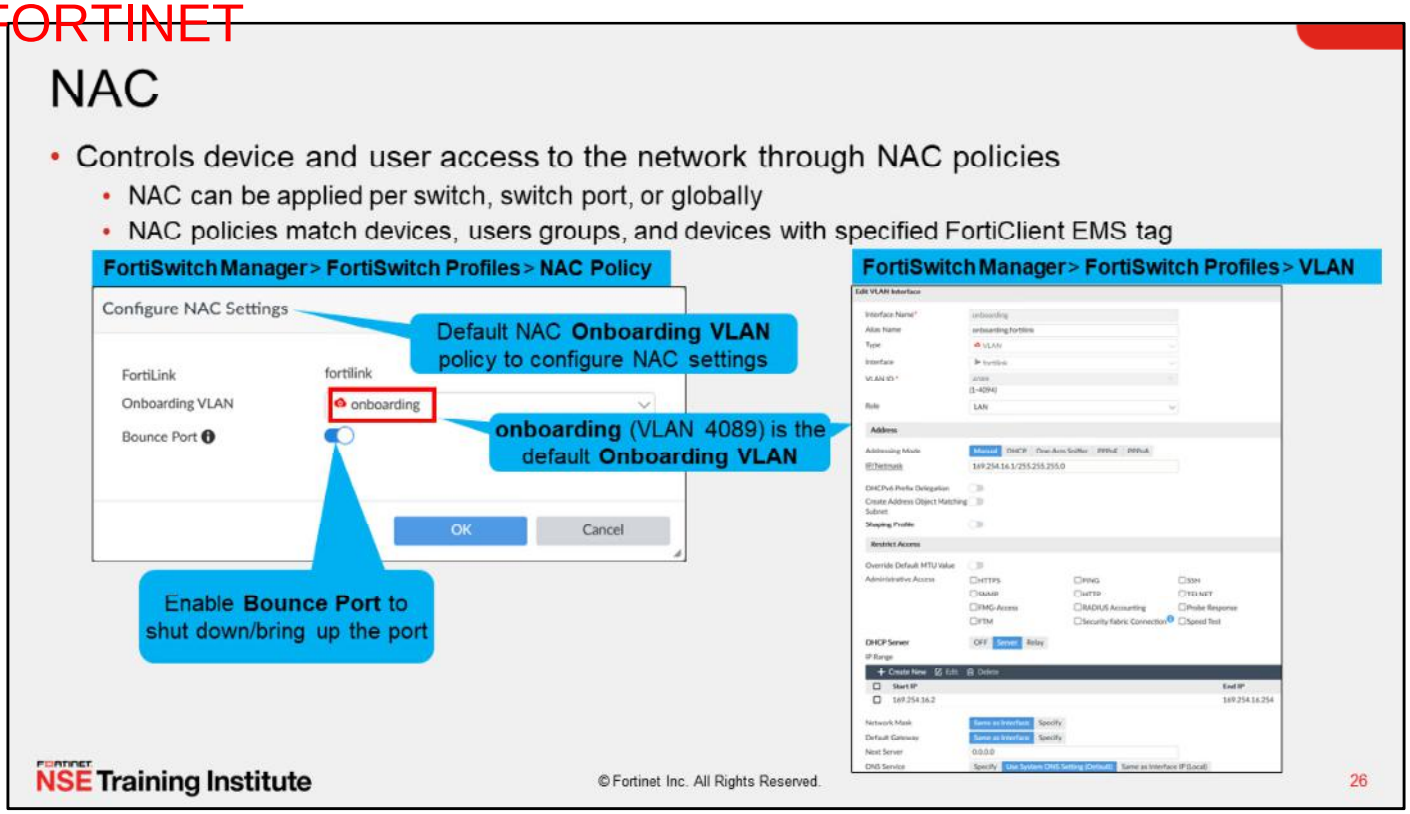
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn how to configure NAC on FortiSwitch.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



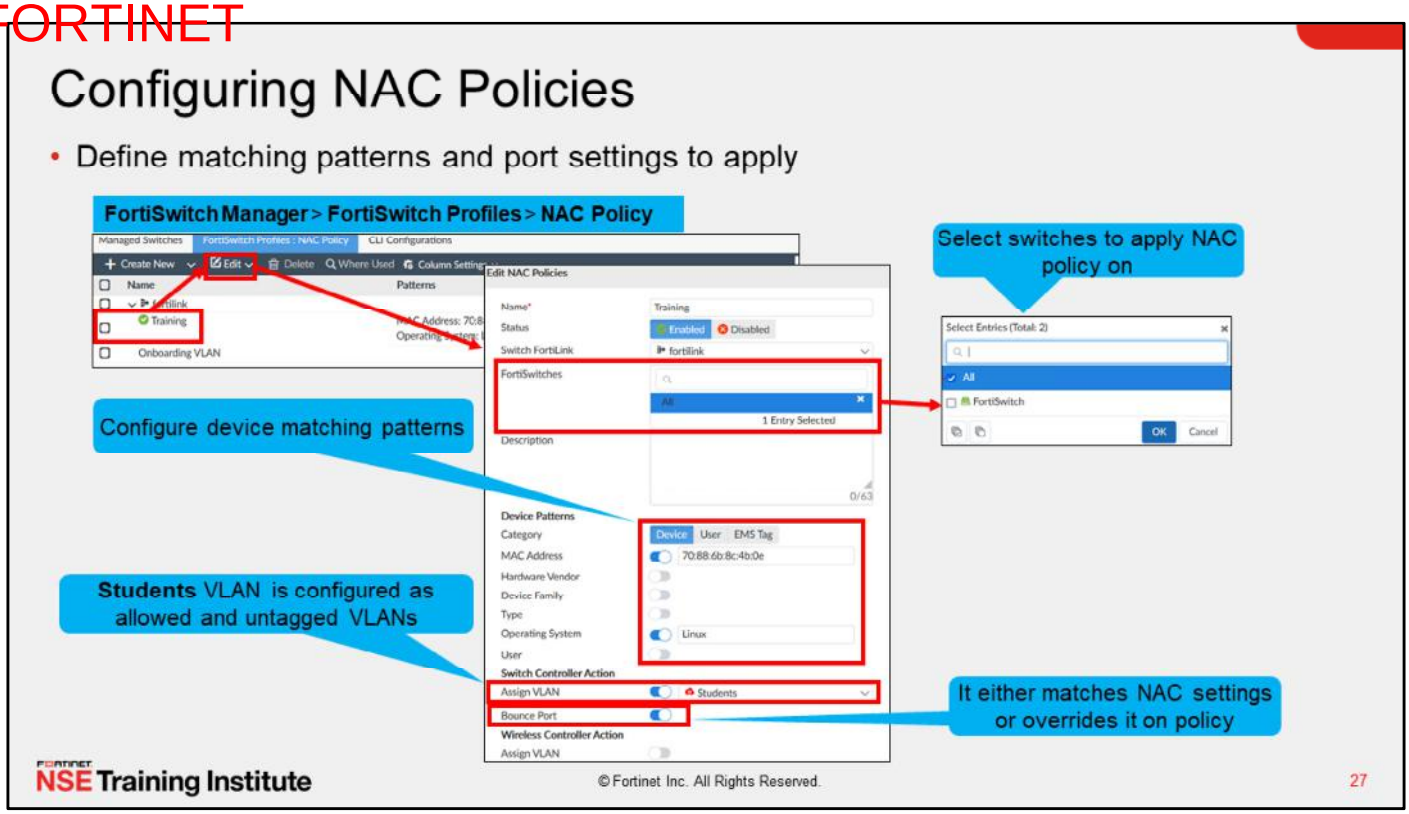
NAC enables a managed FortiSwitch to assign a VLAN or some specific settings to the port to which a device is connected, based on the device, user groups, or devices with specified FortiClient EMS tag detected on that port. For this, FortiGate uses NAC policies that define the criteria (or patterns) that match a device or user, as well as the settings to apply on the corresponding switch port.

NAC settings are, by default, configured to use the default onboarding VLAN which is assigned with the VLAN ID 4089. However, you can select any of the existing FortiSwitch VLANs if required. The onboarding VLAN is assigned as the native VLAN on a port that is subject to NAC based on the NAC settings configured. As a result, the traffic for the device connected on the port is placed on the onboarding VLAN initially. The onboarding VLAN typically has minimum or no network access, device identification enabled, a DHCP server, and optionally a captive portal. After the device or user is identified, FortiGate applies the VLAN or port settings configured in the matching NAC policy. If there are no matching NAC policies, the device stays in the onboarding VLAN.

After the VLAN or port settings are applied on the port, you may want to shut down and bring up the port to restart the DHCP process on the device, because the device may have been moved to a different VLAN with different DHCP settings. To have FortiGate automatically bounce the port after detection, **Bounce Port** on NAC settings is enabled by default. You can also enable or disable **Bounce Port** settings for each NAC policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



NAC policies contain the device, user patterns, and FortiClient EMS tag to check on a device, before the VLAN or settings are applied on the port. Like firewall policies, NAC policies are checked from top to bottom until a policy that matches *all* the defined patterns is found.

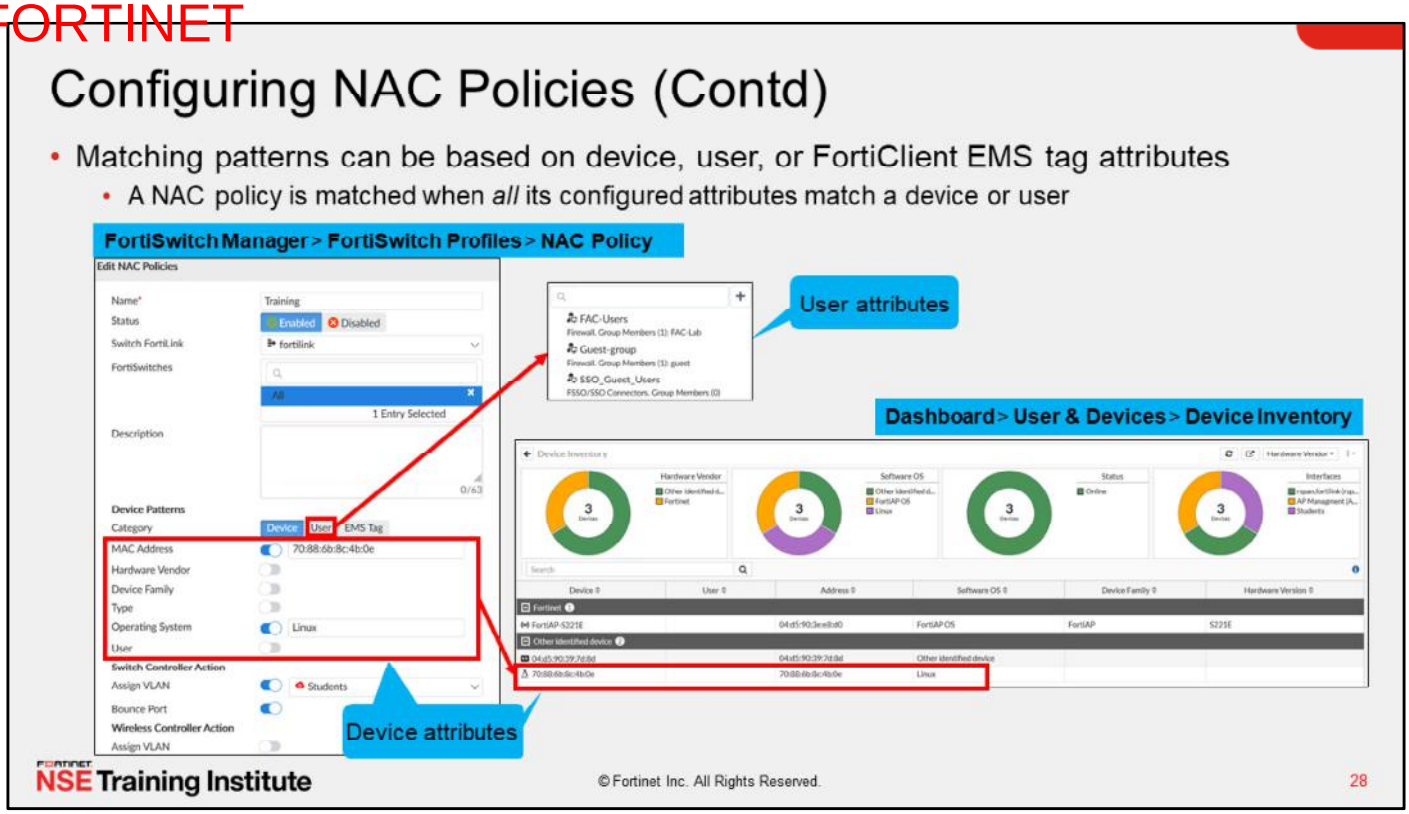
When you configure a NAC policy, you can select if you want the policy to apply to all managed switches or specific ones. Note that the list of switches selected on a NAC policy takes precedence over the list of switches selected on the FortiLink interface.

After the device or user is detected and a NAC policy is matched, FortiGate assigns the port to the VLAN selected in the **Assign VLAN** drop-down list. The assigned VLAN is also configured as part of the allowed and untagged VLANs of the port.

You can enable or disable **Bounce Port** settings to match the default NAC settings or to override it on the NAC policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



When you configure the NAC policy patterns, you must first select the category: **Device**, **User**, or **EMS Tag**. **Device** category leverages the device detection feature of FortiGate, which means that you must enable device detection on the onboarding VLAN for it to work. Device detection uses various detection methods to identify the following information about the device: MAC address, hardware vendor, device family, type, OS, and user. You can configure NAC policies to match any of these device attributes.

You can also view the device detection details by accessing the **Device Inventory** widget on the FortiGate dashboard. Note that not all attributes apply for all detected devices. For example, the **Linux** shown in the example on this slide has no information in the **Device Family** and **Hardware Version** columns.

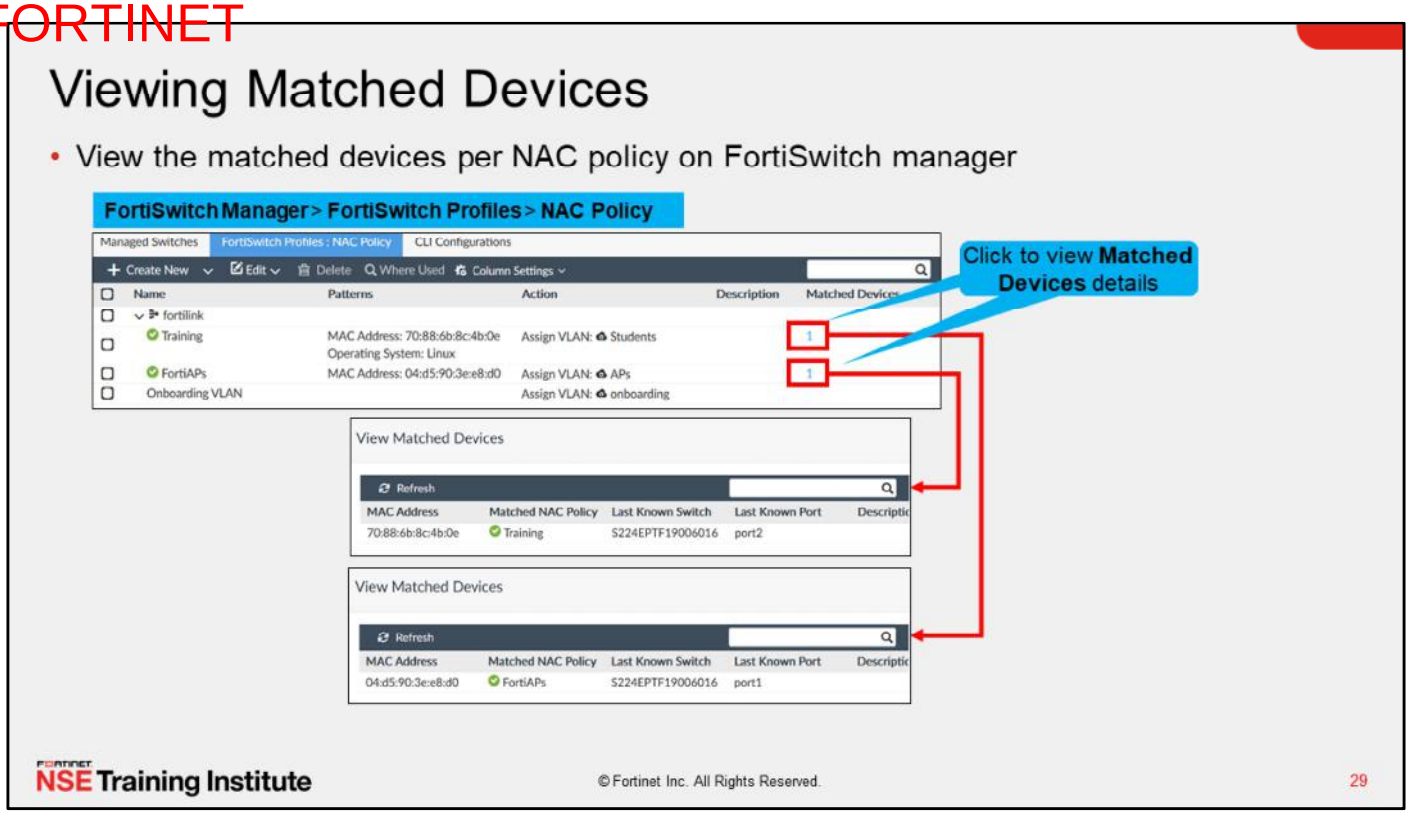
Alternatively, you can select the **User** category for pattern matching. This category instructs FortiGate to match a device based on the user information obtained by FortiGate for that device through passive or active authentication. Do not confuse the **User** *category* with the **User** *field* available under the **Device** category. The **User** field refers to the user identified by FortiGate through device detection techniques, while the user category makes use of the firewall user authentication information maintained by FortiGate.

Moreover, you can create the NAC policy based on **EMS Tag** device patterns to match devices with a specified MAC address. The MAC address is derived from the FortiClient endpoint management server (EMS).

Note that a NAC policy is matched when *all* its configured attributes match a device or user. Otherwise, FortiGate evaluates the next NAC policy in the list. If there are no matching NAC policies, the device stays in the onboarding VLAN.

Vouchers & Dumps are Available | WhatsApp +201224560923

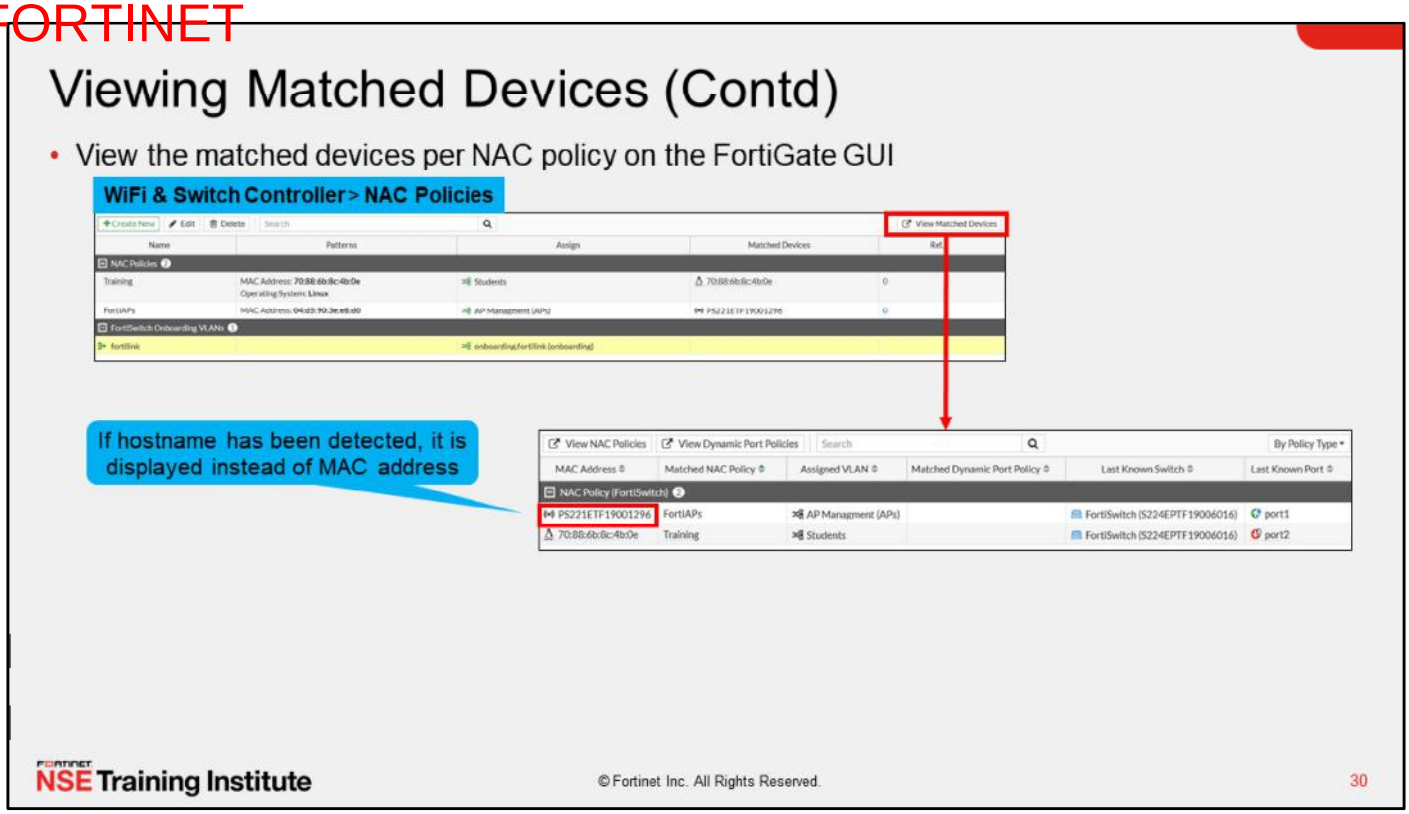
DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can see the list of devices that matched any of the NAC policies configured. The device details include the port and switch the device is connected to, the timestamp of the match event, and the device MAC address, among other things.

Vouchers & Dumps are Available | WhatsApp +201224560923

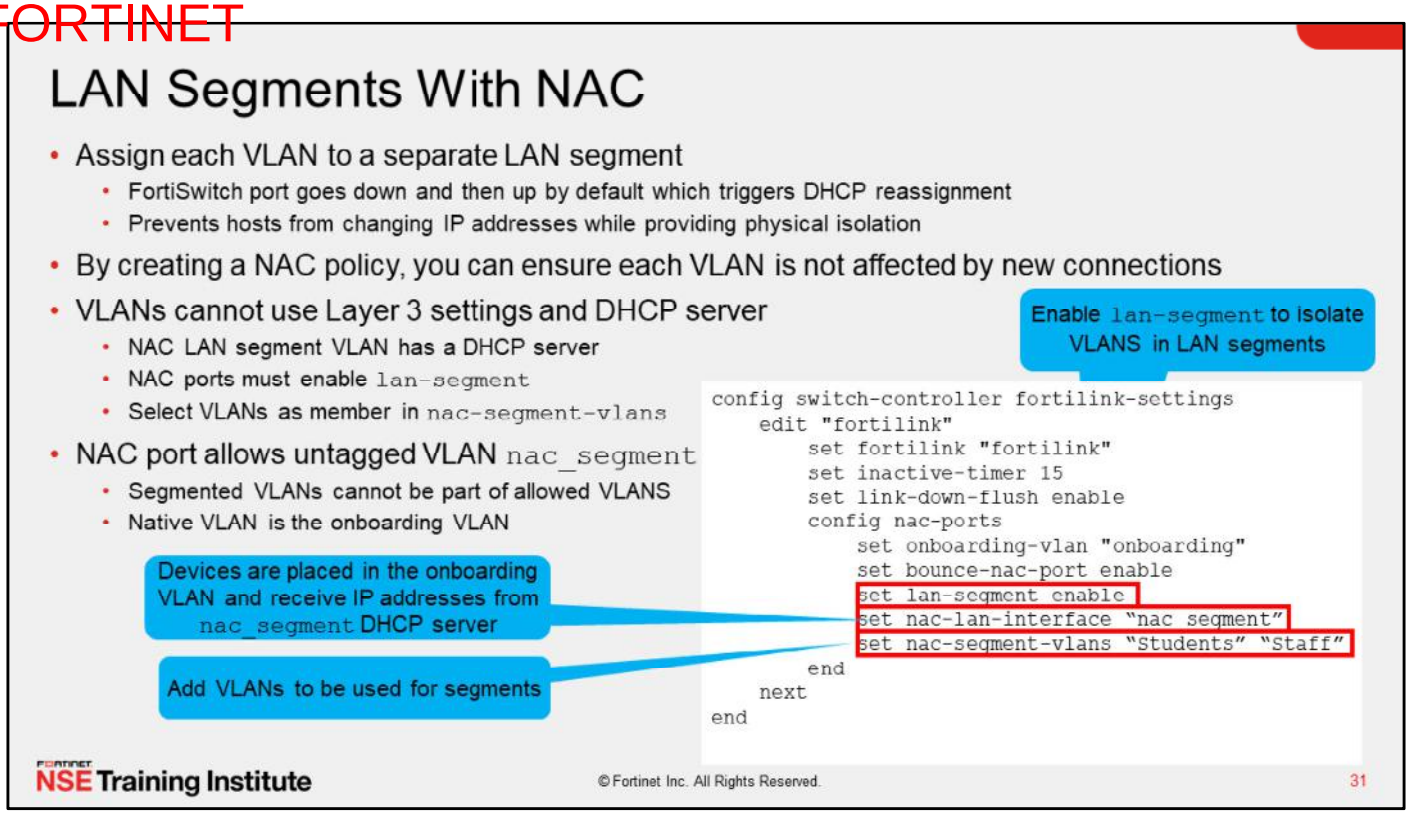
DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can also see the list of matched devices on the FortiGate GUI and CLI. Note that if the device hostname has been detected by FortiGate, the GUI will display the device hostname instead of its MAC address.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



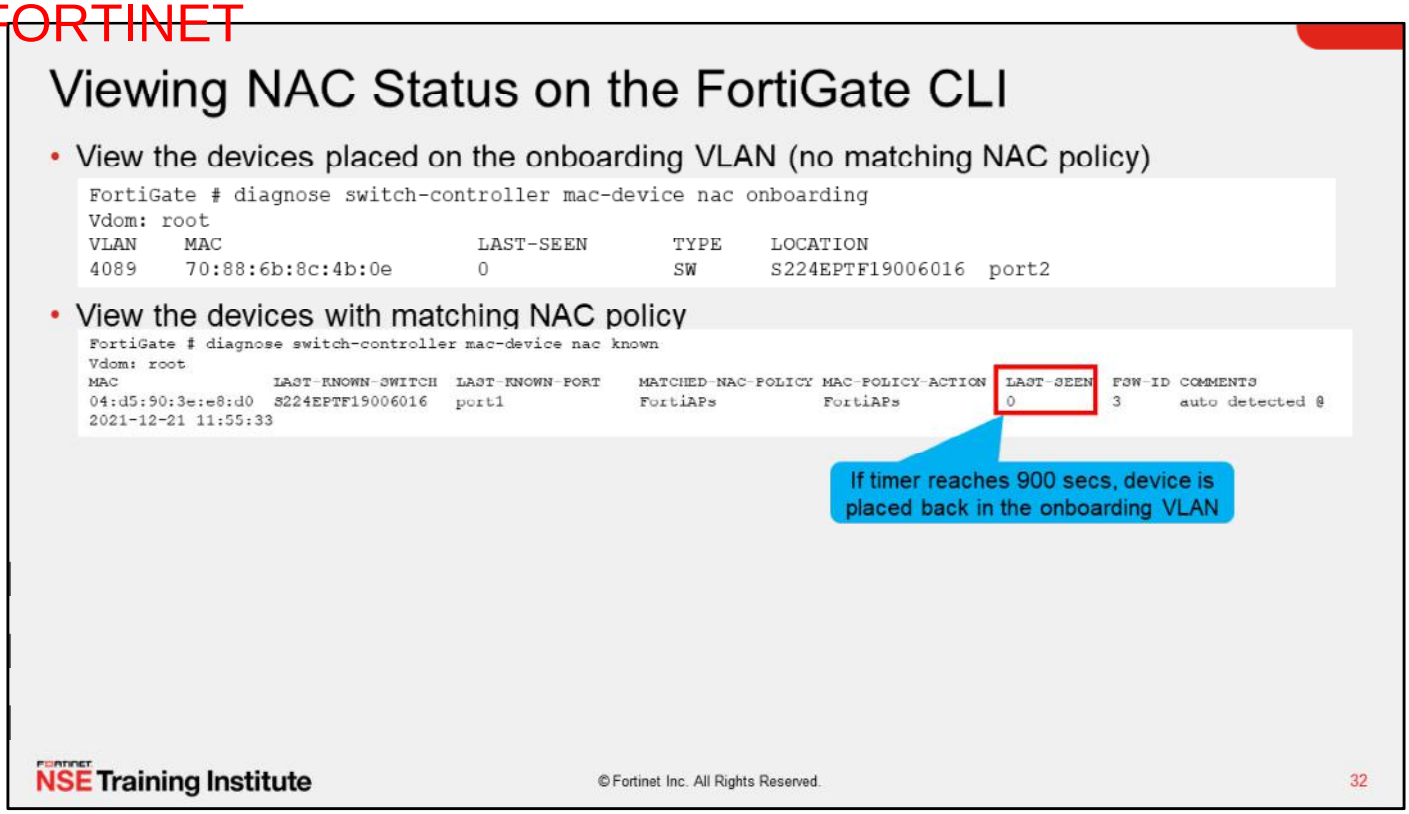
For FortiSwitch ports acting as a NAC interface, the default behavior for new connections to the port is that the link disconnects and then reconnects. This causes connected hosts to restart the DHCP process, which in turn makes these devices obtain new IP addresses. The hosts lose existing firewall sessions, which is an issue for using a NAC policy on FortiSwitch ports with dynamic changes to the physical connections.

NAC LAN segments prevent the IP addresses of hosts from changing while providing physical isolation. The NAC policy takes effect when existing connected devices are in isolated segments where they are assigned IP addresses by the `nac_segment` interface. This in turn preserves ongoing firewall sessions instead of resetting traffic connections for the devices.

To configure the NAC LAN segment globally, VLANs that require segmentation must not have any Layer 3 settings such as IP address and DHCP server. The `nac_segment` interface assigns an IP address to each device in its VLAN LAN segment. The NAC port should allow only the untagged `nac_segment` VLAN. Do not add the segmented VLANs to the NAC port setting because they are part of global LAN configuration and do not offer Layer 3 services, such as DHCP server.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

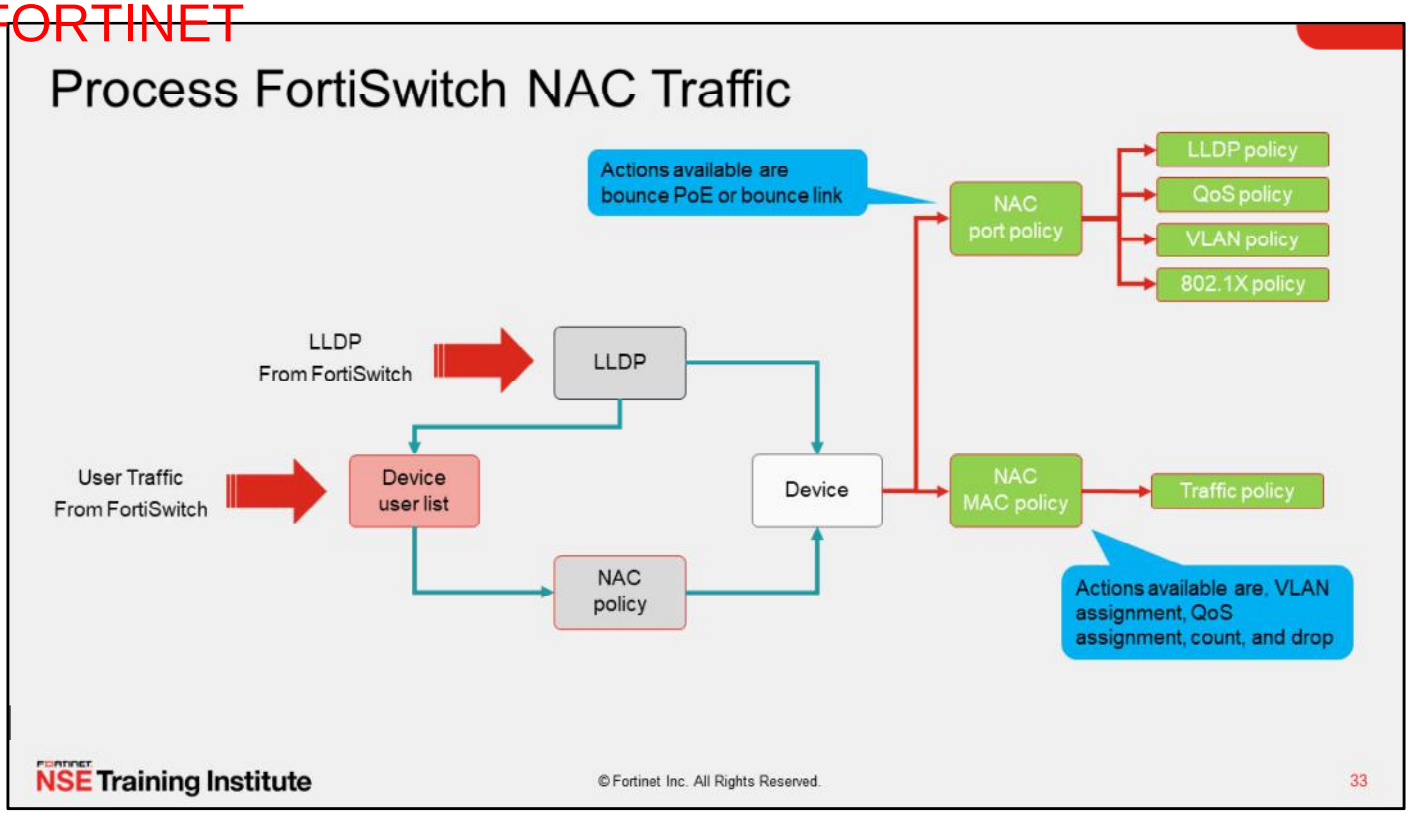


Before a device matches a NAC policy, it is placed in the onboarding VLAN. You can view the list of devices placed in the onboarding VLAN by running the `diagnose switch-controller mac-device nac onboarding` command on the FortiGate CLI.

You can also view the list of devices that have matched a NAC policy, and their location on the network, by running the `diagnose switch-controller mac-device nac known` command. FortiSwitch synchronizes the MAC address table of its managed switches every five seconds. If the MAC address of the NAC device is not listed in the MAC address table for the last 900 seconds (15 minutes), the device is considered inactive and is placed back in the onboarding VLAN.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



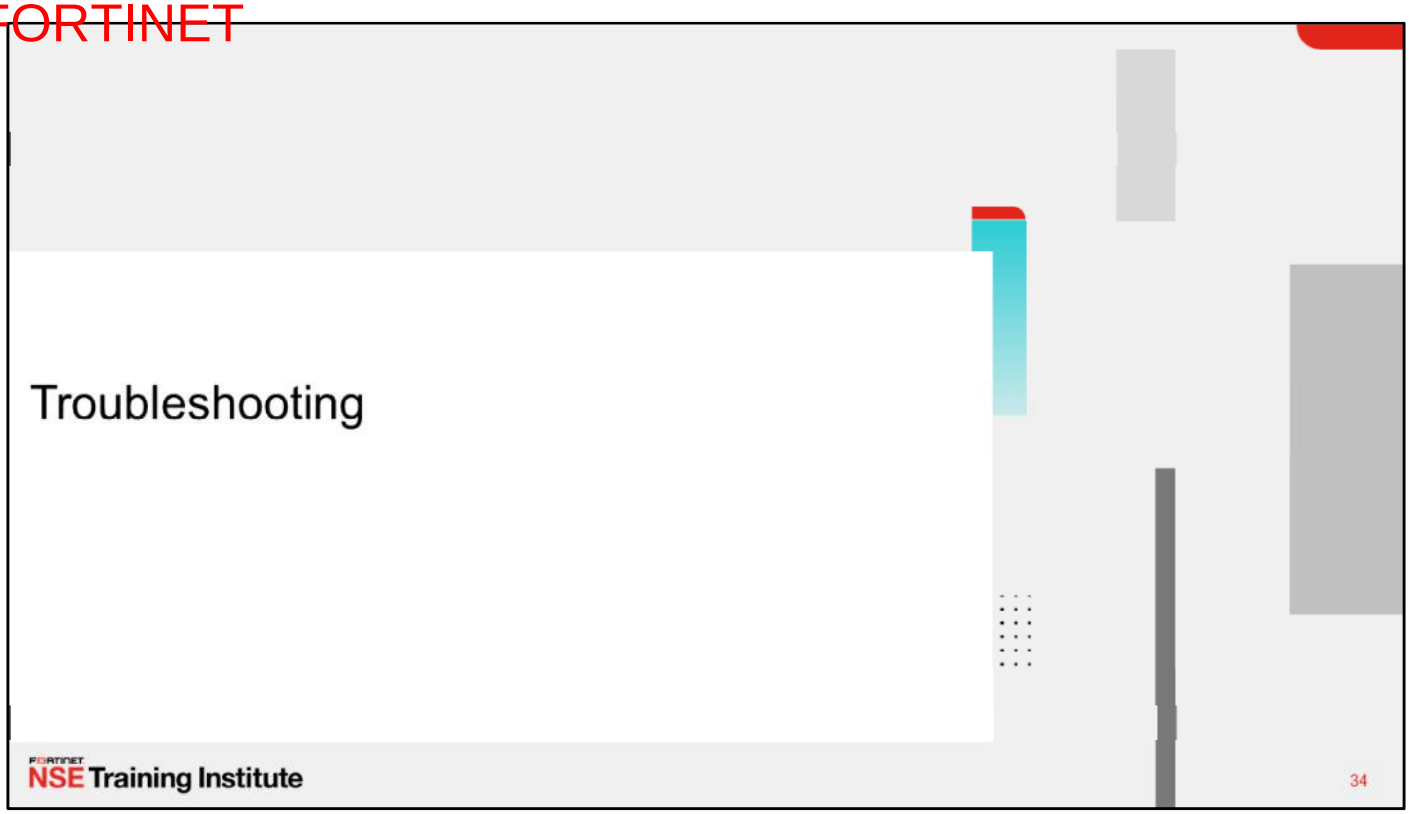
This slide shows the steps performed on the traffic received from FortiSwitch on ports configured as NAC mode.

Implementing policies for controlling devices and user access to your networks for resource, role, device and location-based access, and enforce security compliance with security and patch management policies, among other controls.

The NAC policy is defined based on any significant field with the user device list entry. Devices within the list may have NAC policy applied and are using the IoT device identification database or LLDP from FortiSwitch.

Vouchers & Dumps are Available | WhatsApp +201224560923

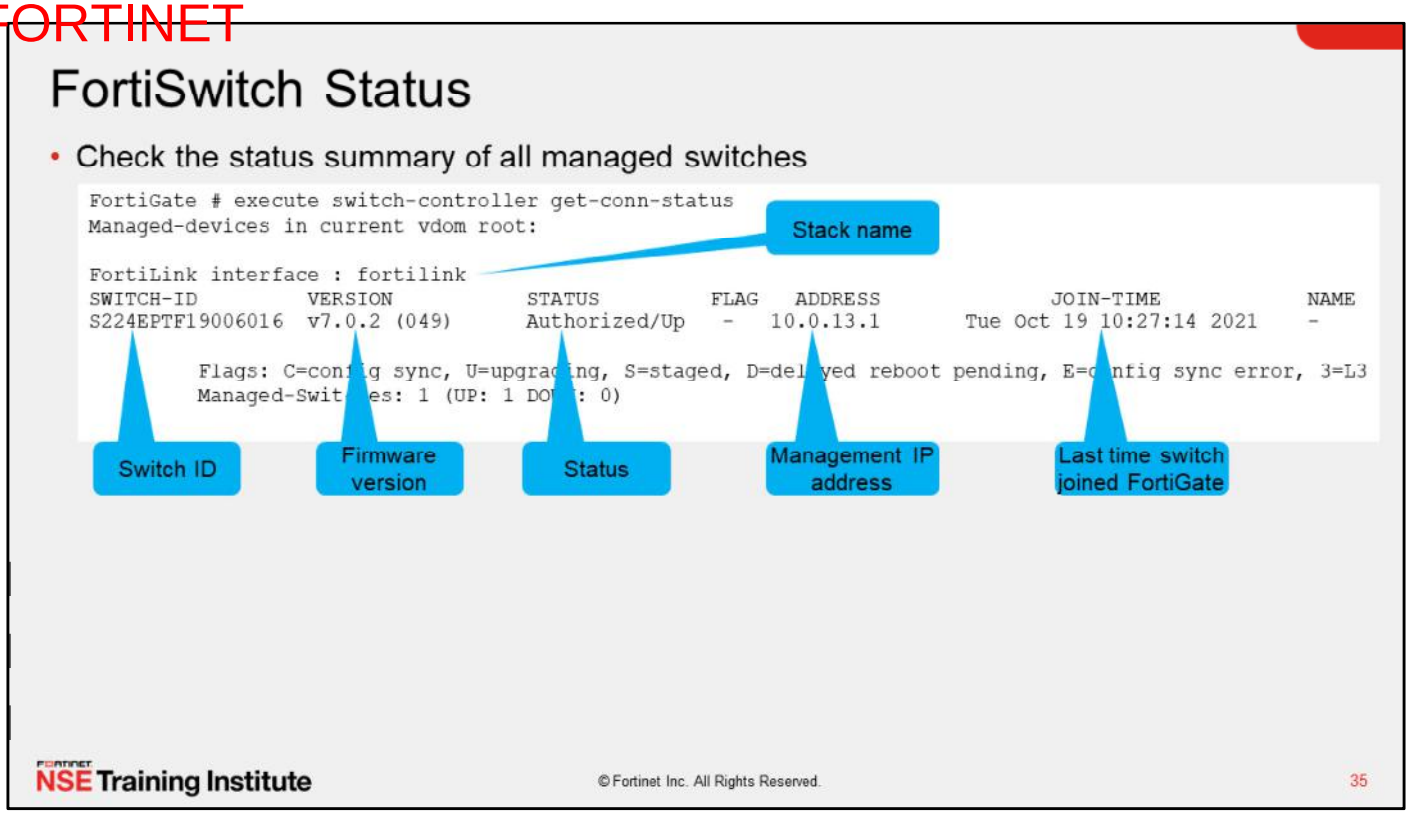
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn about troubleshooting communication issues between FortiGate and FortiSwitch.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

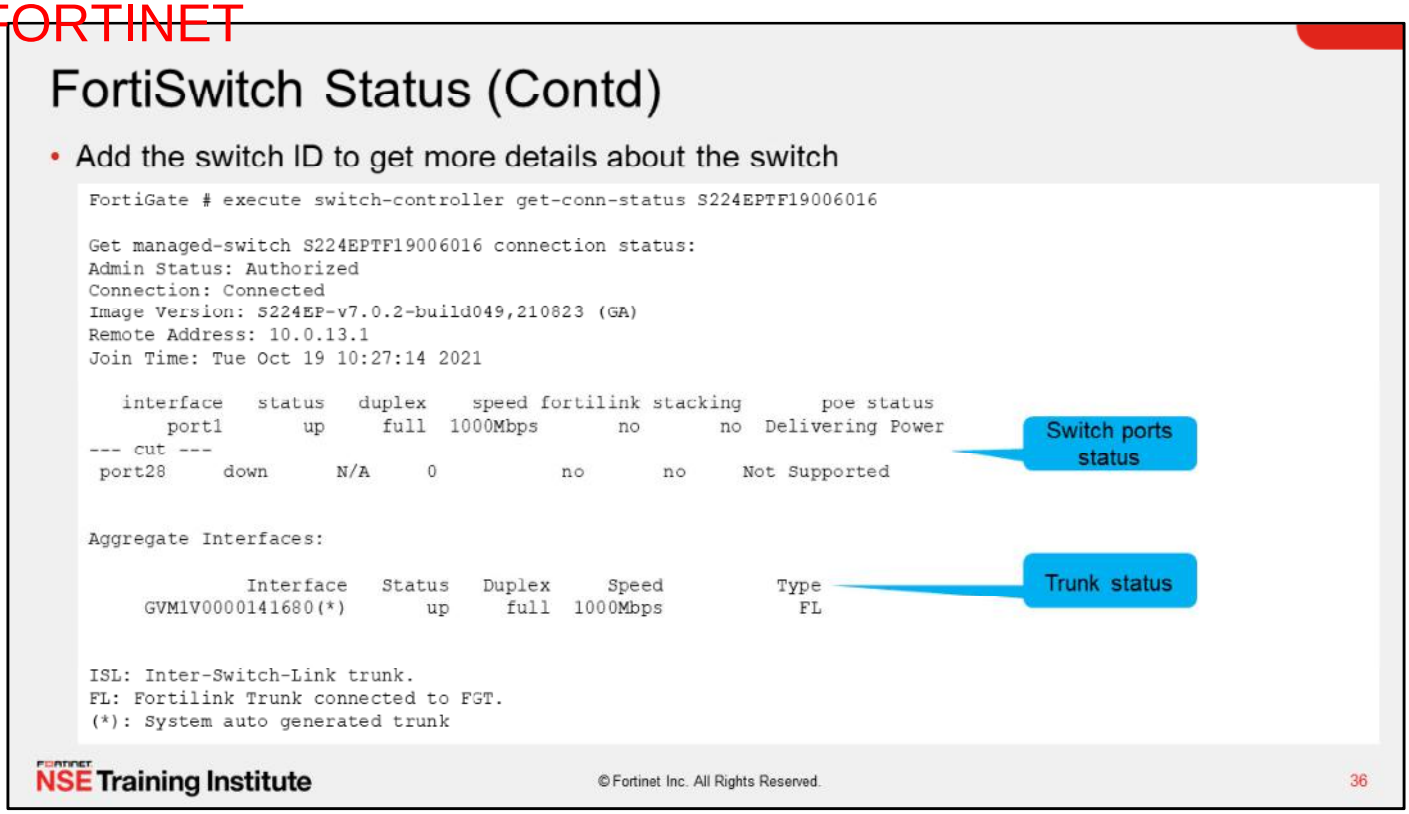


When troubleshooting managed switches, start by running the `execute switch-controller get-conn-status` command on the FortiGate CLI. The command provides you with key information for all managed switches, such as their current status, management IP address, firmware version, as well as the last time the switches successfully connected to (or joined) FortiGate. Under normal operation, a switch join time should remain the same because it is the first time the switches joined FortiGate. However, a switch join time that is frequently updated may indicate connectivity issues between the switch and FortiGate.

The output also provides you with two pieces of information that you will likely need to troubleshoot further: stack name and switch ID. Because FortiGate supports management of multiple switch stacks, and given that each stack can have multiple switches, knowing the stack name and the switch ID of a problematic switch allows you to filter the output when running some troubleshooting commands. This is particularly useful when dealing with large FortiSwitch deployments because reviewing the output of all managed switches can be overwhelming. Note that all stack names start with `FortiSwitch-Stack-` followed by the FortiLink interface the stack is connected to. In the example shown on this slide, the FortiLink interface is `fortilink`.

Vouchers & Dumps are Available | WhatsApp +201224560923

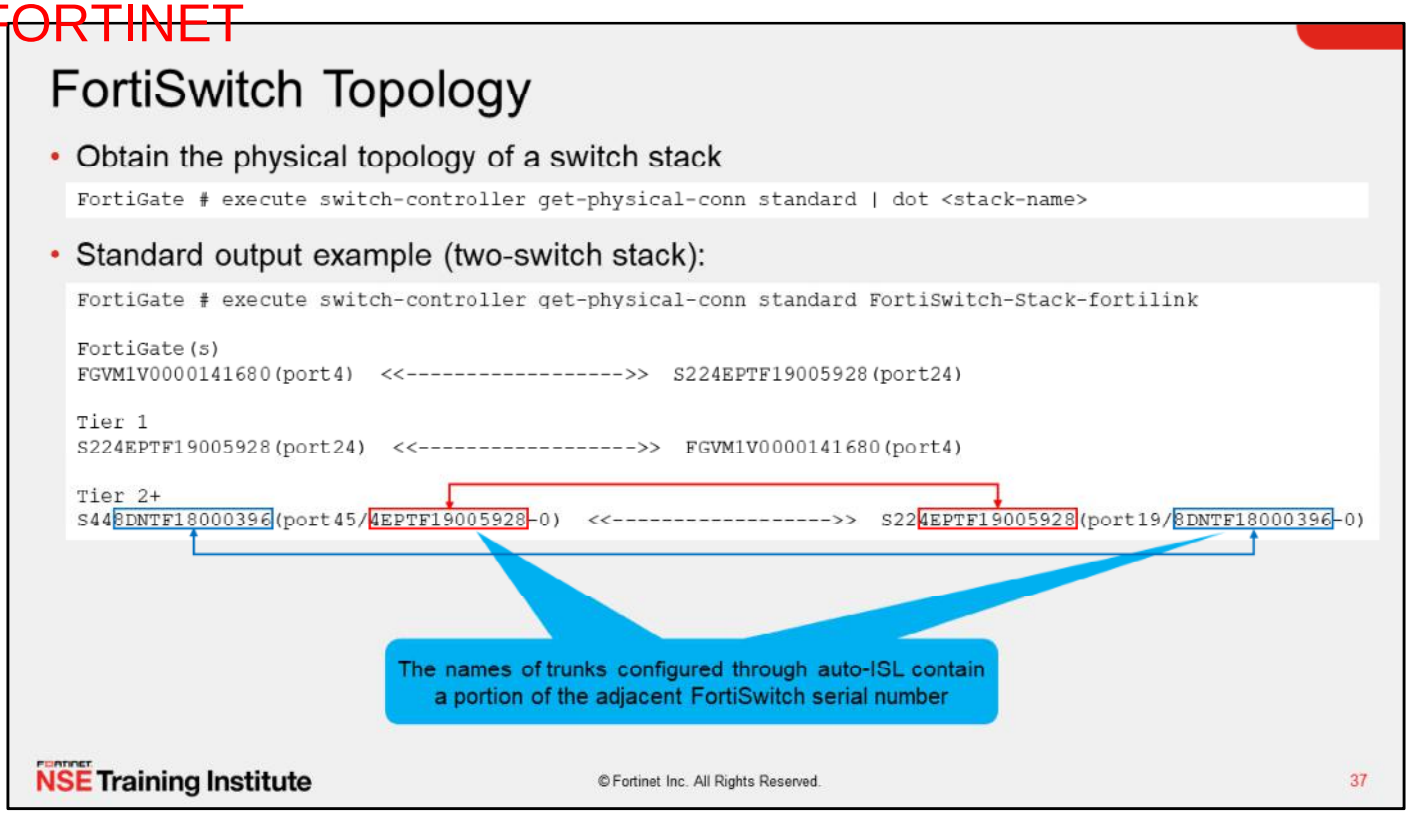
DO NOT REPRINT
© FORTINET
Brave-dumps.com



If you add the switch ID to the `execute switch-controller get-conn-status` command, you get further details about the switch, including the status summary of all of its ports and aggregate interfaces (or trunks).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The next step in troubleshooting a switch is to obtain the physical connection details of the stack. This is especially helpful when troubleshooting instability issues caused by incorrect physical connections.

You can get the current physical topology of a stack by running the `execute switch-controller get-physical-conn` command. The command can display the output in standard format or dot format. The standard format is more suited for small deployments, because the output for these cases is usually easier to read. The standard output organizes the switches per tier (or level), and indicates the ports used for each connection between switches, and between switches and FortiGate devices. For example, the standard format output shown on this slide corresponds to a two-switch stack. The switch that is directly connected to FortiGate is classified as tier 1.

In addition, the output also includes the names of the trunks automatically configured through auto-ISL. In auto-ISL, the trunk names contain a portion of the adjacent switch serial number.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiSwitch Topology (Contd)

- Dot output example (two-switch stack):

```
FortiGate # execute switch-controller get-physical-conn dot FortiSwitch-Stack-fortilink
 FortiLink interface : FortiSwitch-Stack-fortilink
digraph {

graph [layout = dot, rankdir = TB]

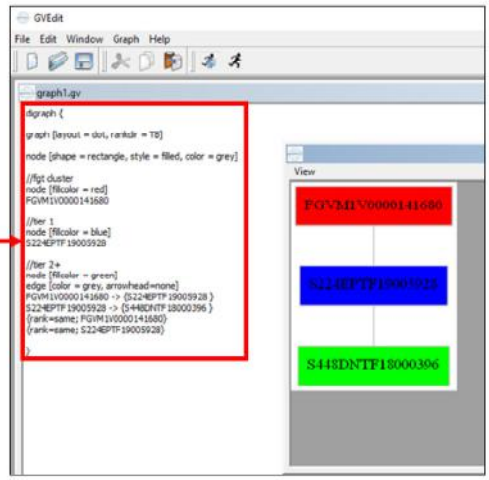
node [shape = rectangle, style = filled, color = grey]

//fgt cluster
node [fillcolor = red]
FGVM1V0000141680

//tier 1
node [fillcolor = blue]
S224EPTF19005920

//tier 2+
node [fillcolor = green]
edge [color = grey, arrowhead=none]
FGVM1V0000141680 -> {S224EPTF19005928 }
S224EPTF19005928 -> {S448DNTF18000396 }
{rank=same; FGVM1V0000141680}
{rank=same; S224EPTF19005928}

}
```



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

38

For large deployments, you may want to use the dot format output instead. The output can be loaded into an image editor that supports graphviz format, such as GVedit, so the output is displayed as a graph. Alternatively, you can upload the output into a graphviz converter website such as `www.webgraphviz.com`, to generate the graph.

In the example shown on the slide, the dot output has been loaded into GVEdit. GVEdit then generates a graph depicting the physical topology of the stack.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiSwitch Synchronization Status

```
FortiGate # execute switch-controller get-sync-status
all           Get FortiSwitch sync status.
group         Get FortiSwitch sync status by group.
name          Get FortiSwitch sync status by switch name.
switch-id     Get FortiSwitch sync status by switch.

FortiGate # execute switch-controller get-sync-status all
Managed-devices in current vdom root:

STACK-NAME: FortiSwitch-Stack-fortilink
SWITCH (NAME)                  STATUS CONFIG         MAC-SYNC       HTTP-UPGRADE
S224EPTF19005928               Up     Idle           Idle           Idle
```

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

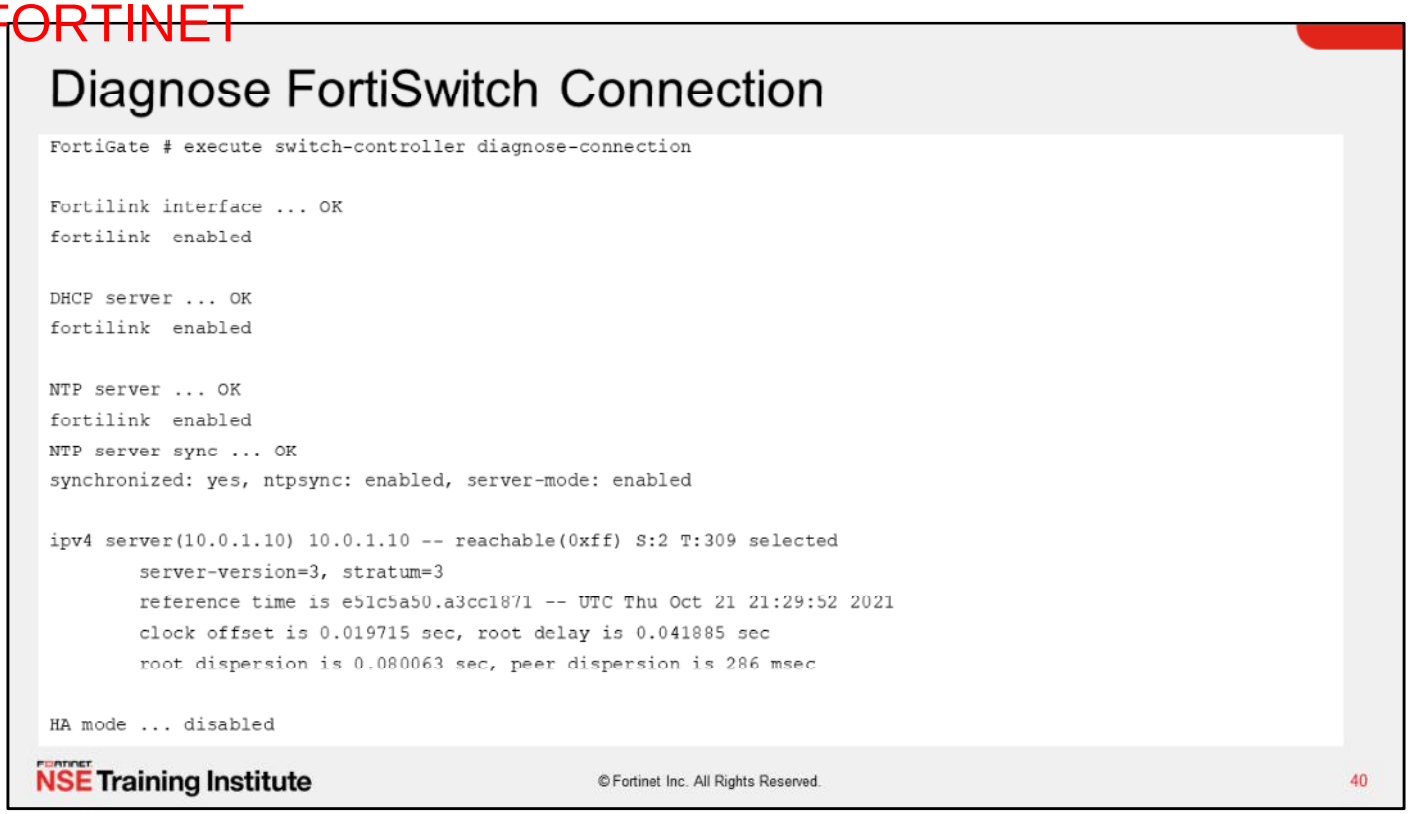
39

Each time you change the FortiSwitch configuration on FortiGate, the change is saved in the FortiGate configuration first, and then FortiGate pushes the configuration change to FortiSwitch through HTTPS and using the FortiSwitch REST API. FortiSwitch then saves the changes locally. The command `execute switch-controller get-sync-status` shows the status of the configuration synchronization between FortiGate and FortiSwitch.

The command also displays the MAC address synchronization and HTTP firmware upgrade status. FortiGate frequently polls the MAC address table from all managed switches to get the physical address listed on each port. This information is then used by FortiGate to provide visibility, control, and ultimately security of the network. In addition, FortiGate supports two methods for pushing firmware image files to managed switches: CAPWAP and HTTPS. The upgrade status information displayed by the `execute switch-controller get-sync-status` command is for the HTTPS method *only*.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



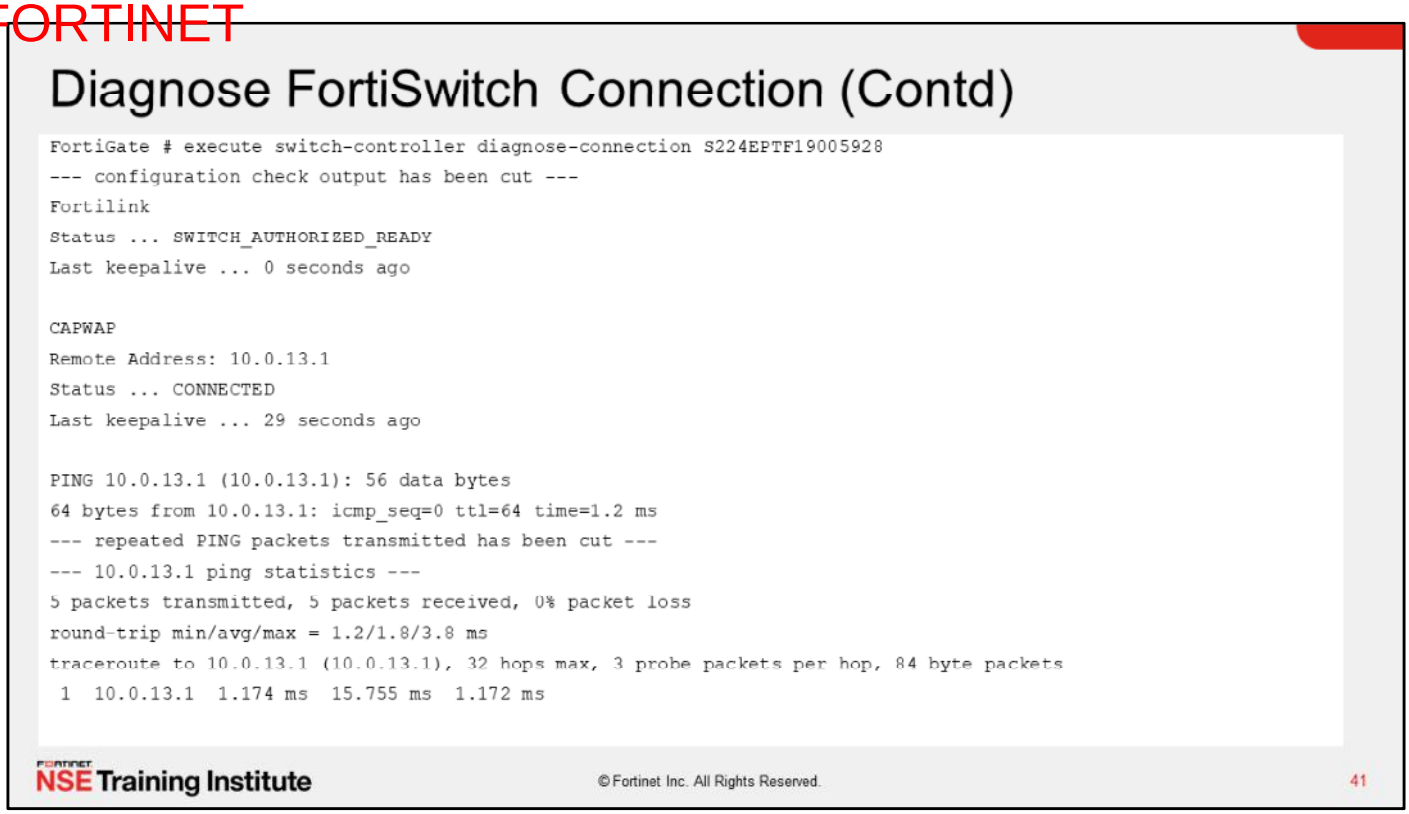
To verify that all the configuration needed for switch management is in place, you can run the `execute switch-controller diagnose-connection` command. FortiGate checks that the following settings are present:

- The FortiLink interface has the `fortilink` setting enabled
- There is a DHCP server scope for the FortiLink interface
- The NTP server is enabled on the FortiLink interface

The command also provides the latest NTP status information, as well as the FortiGate high availability (HA) mode in use.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



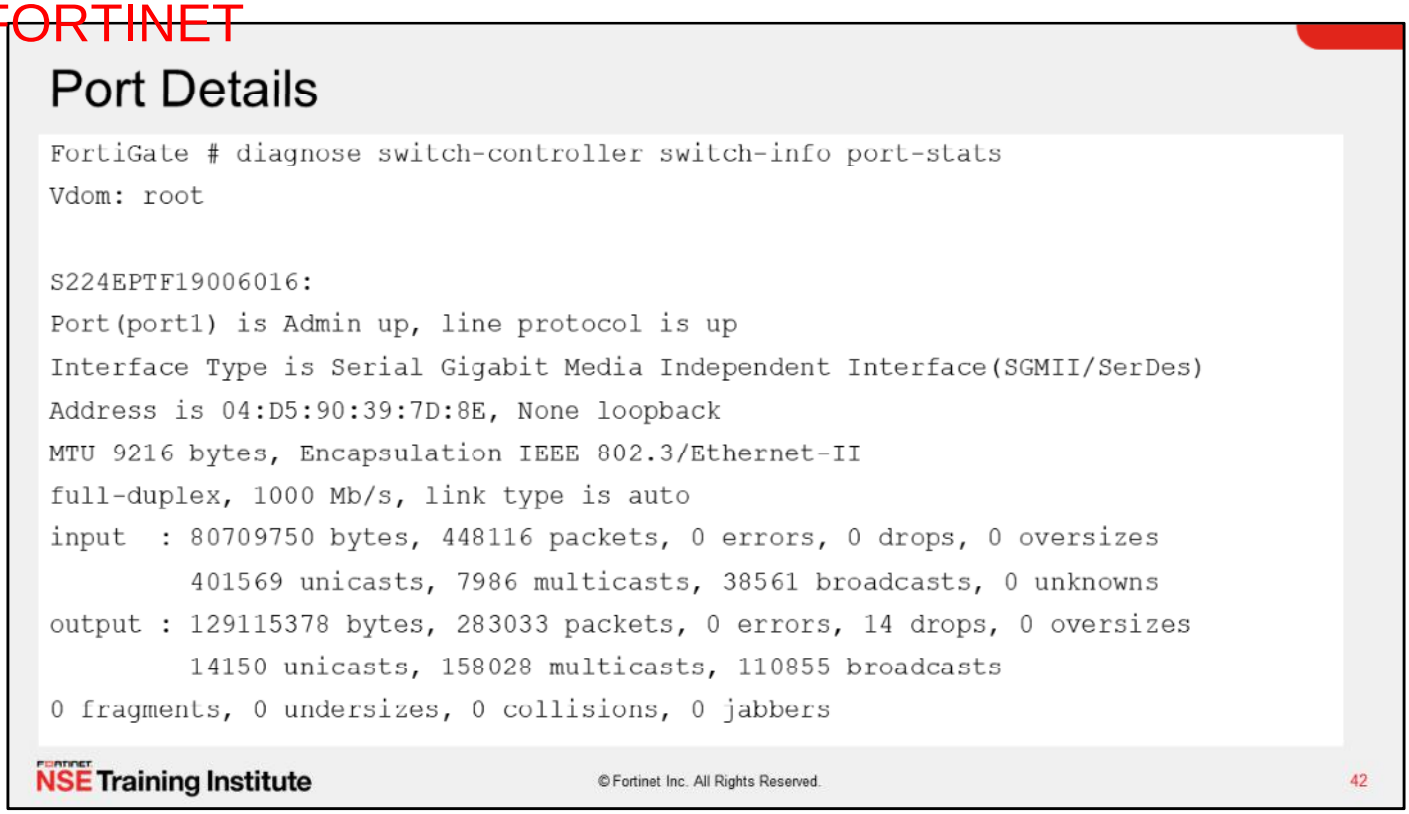
When you specify a switch, the `execute switch-controller diagnose-connection` command also includes in the output the following connectivity checks between FortiGate and the switch:

- FortiLink and CAPWAP connection status, including the last keepalive (or heartbeat) received
- The results of FortiGate sending pings to the switch

Note that this command also displays the output for the configuration check, which is described on the previous slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The command shown on this slide lists specific port information, such as its status, speed, MTU, as well as multiple input and output counters. The output has been cut to include the information for port1 only.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

MAC Address Table

```
FortiGate # diagnose switch-controller switch-info mac-table
Vdom: root
Managed Switch : S224EPTF19006016 0
flag bit pattern: 0x00000000
flag bit Mask:    0x00000000
vlan map: 0-4094
port-id map: 0-29
trunk-id map: 0-127

MAC: 04:d5:90:3e:e8:d0  VLAN: 100 Port: port1(port-id 1)
  Flags: 0x00010441 [ hit dynamic src-hit native ]
MAC: 04:d5:90:39:7d:8d  VLAN: 4094 Port: internal(port-id 29)
  Flags: 0x00010470 [ static hit l3-lookup src-hit native ]
MAC: 00:0c:29:e9:10:a9  VLAN: 4094 Trunk: GVM1V0000141600(trunk-id 0)
  Flags: 0x000104c1 [ hit trunk dynamic src-hit native ]
MAC: 70:88:6b:8c:4b:0e  VLAN: 1 Port: port2(port-id 2)
  Flags: 0x00000001 [ dynamic ]1
MAC: 00:0c:29:e9:10:a9  VLAN: 100 Trunk: GVM1V0000141680(trunk-id 0)
  Flags: 0x000104c1 [ hit trunk dynamic src-hit native ]

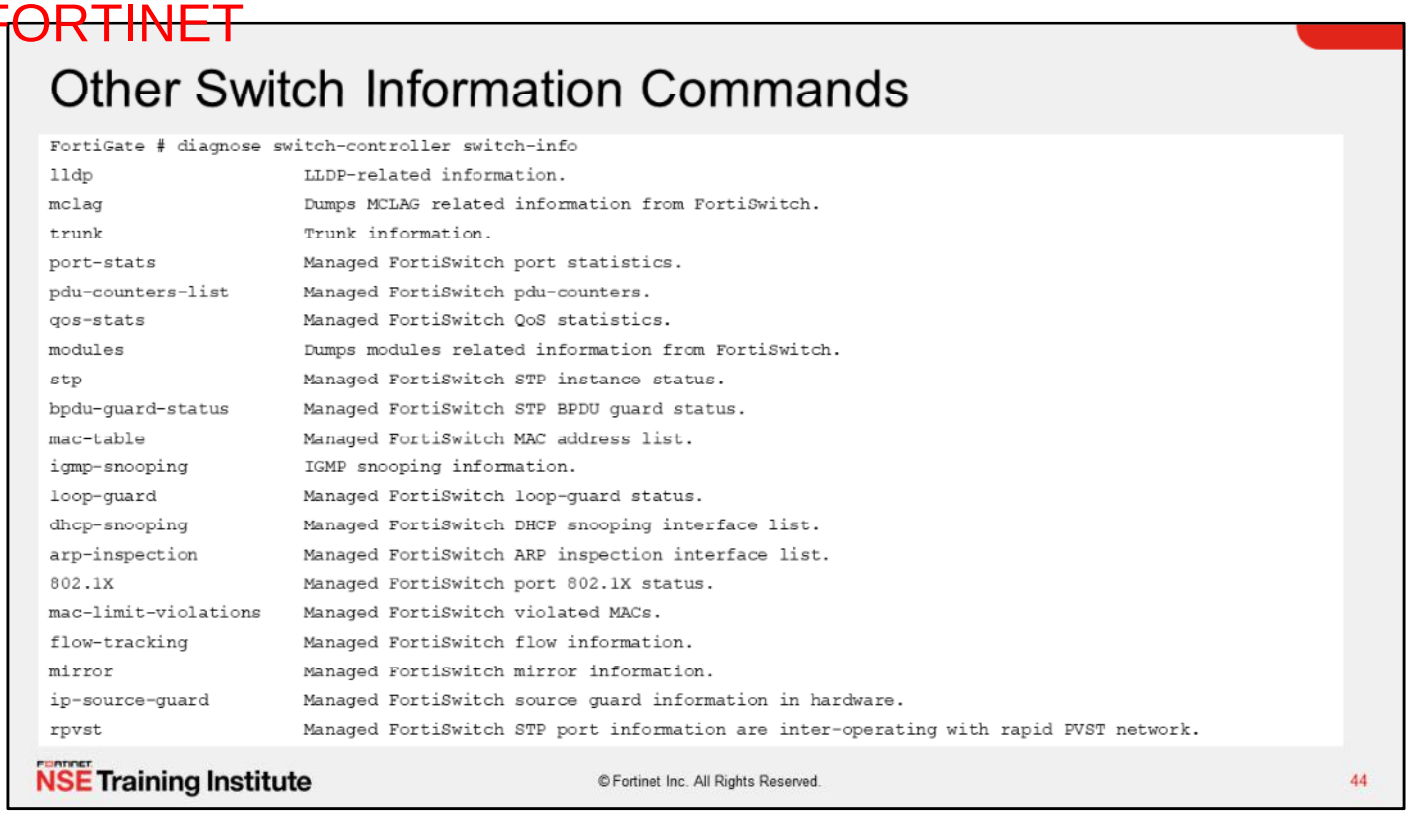
Total Displayed: 6
```

NSE Training Institute © Fortinet Inc. All Rights Reserved. 43

The command `diagnose switch-controller switch-info mac-table` displays the FortiSwitch MAC address table.

Vouchers & Dumps are Available | WhatsApp +201224560923

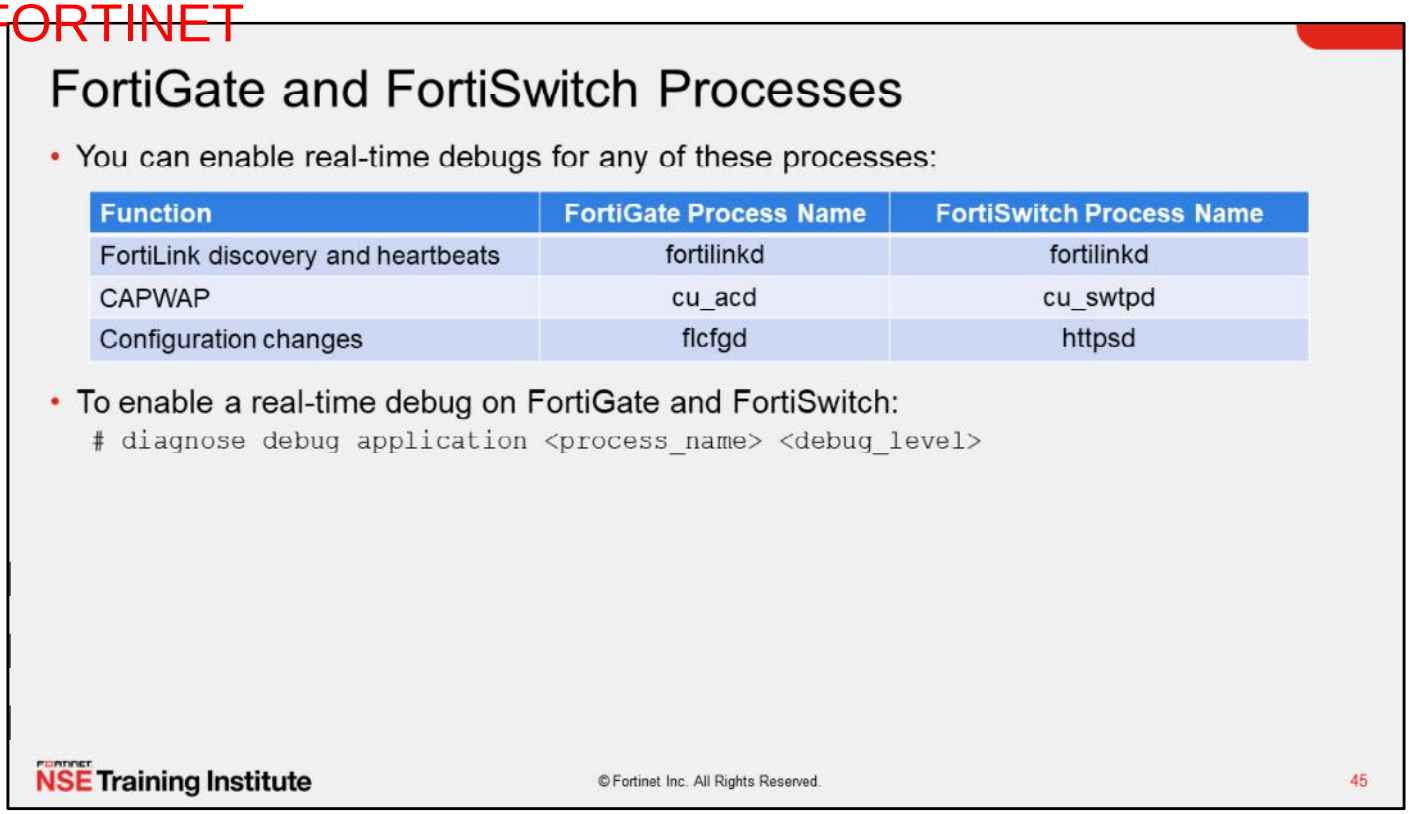
DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows a list of additional CLI commands that you can use for FortiSwitch diagnostics and troubleshooting.

Vouchers & Dumps are Available | WhatsApp +201224560923

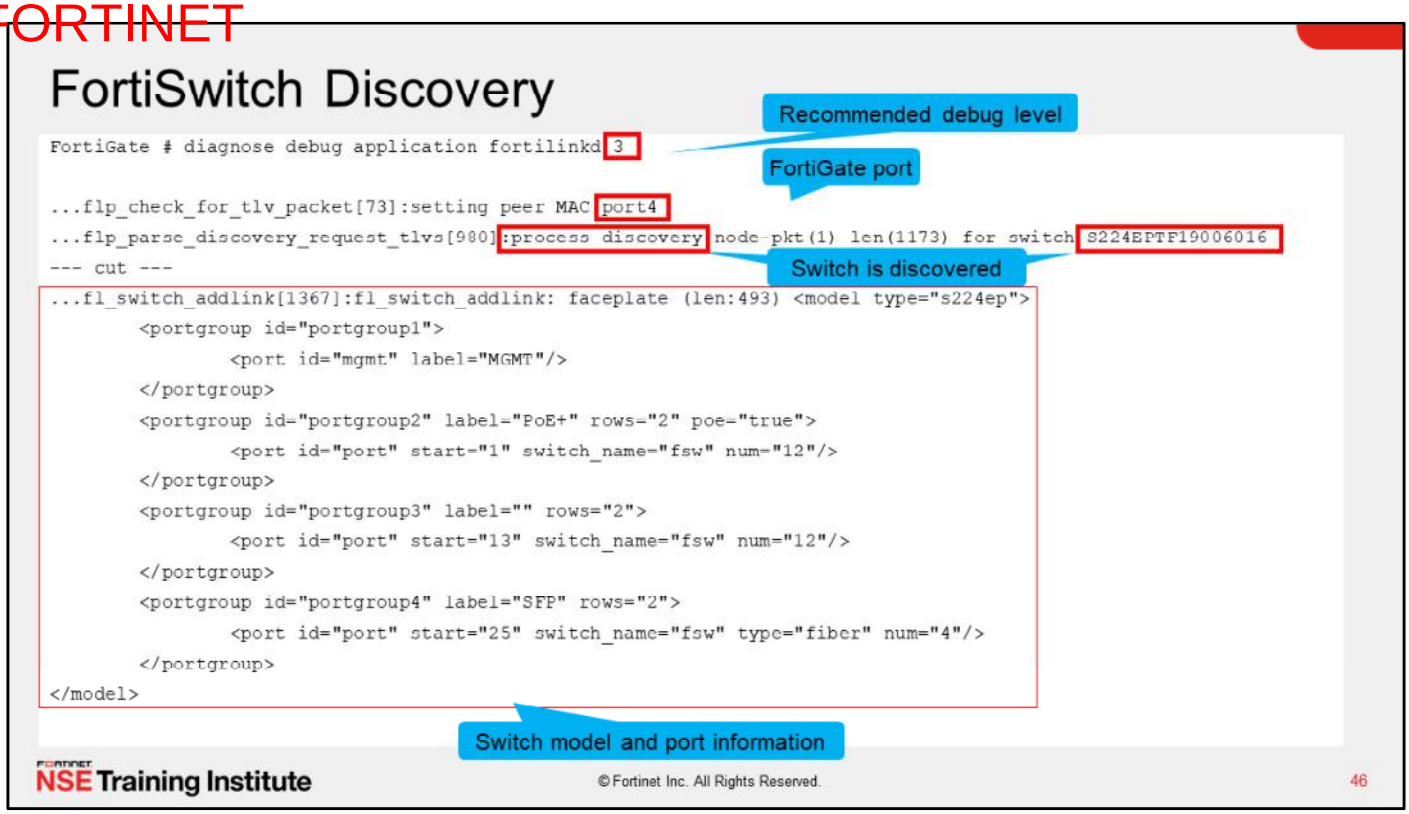
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The table on this slide shows the processes that handle the discovery, heartbeats, and configuration changes on a managed FortiSwitch. The table includes the respective processes for both FortiGate and FortiSwitch.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



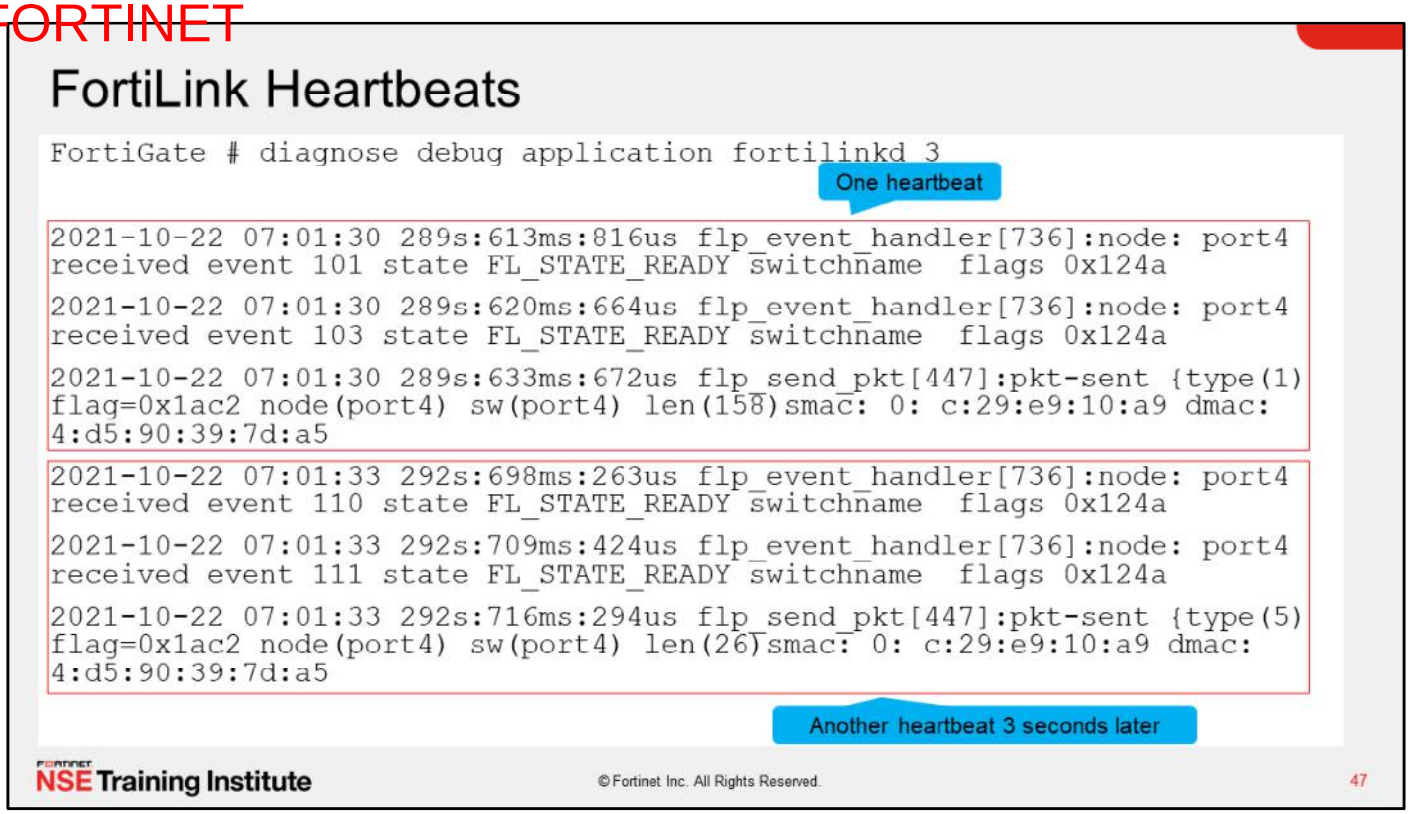
You can enable debug of the `fortilinkd` process for monitoring and troubleshooting the discovery of FortiSwitch devices.

When a new FortiSwitch is discovered, the debug output shows the FortiSwitch serial number as well as the FortiGate port where the FortiLink frames that triggered the switch discovery were received.

In addition, because the FortiLink discovery frames include the switch port information, FortiGate reads this information from the frames to build the switch faceplate image shown on the GUI.

Vouchers & Dumps are Available | WhatsApp +201224560923

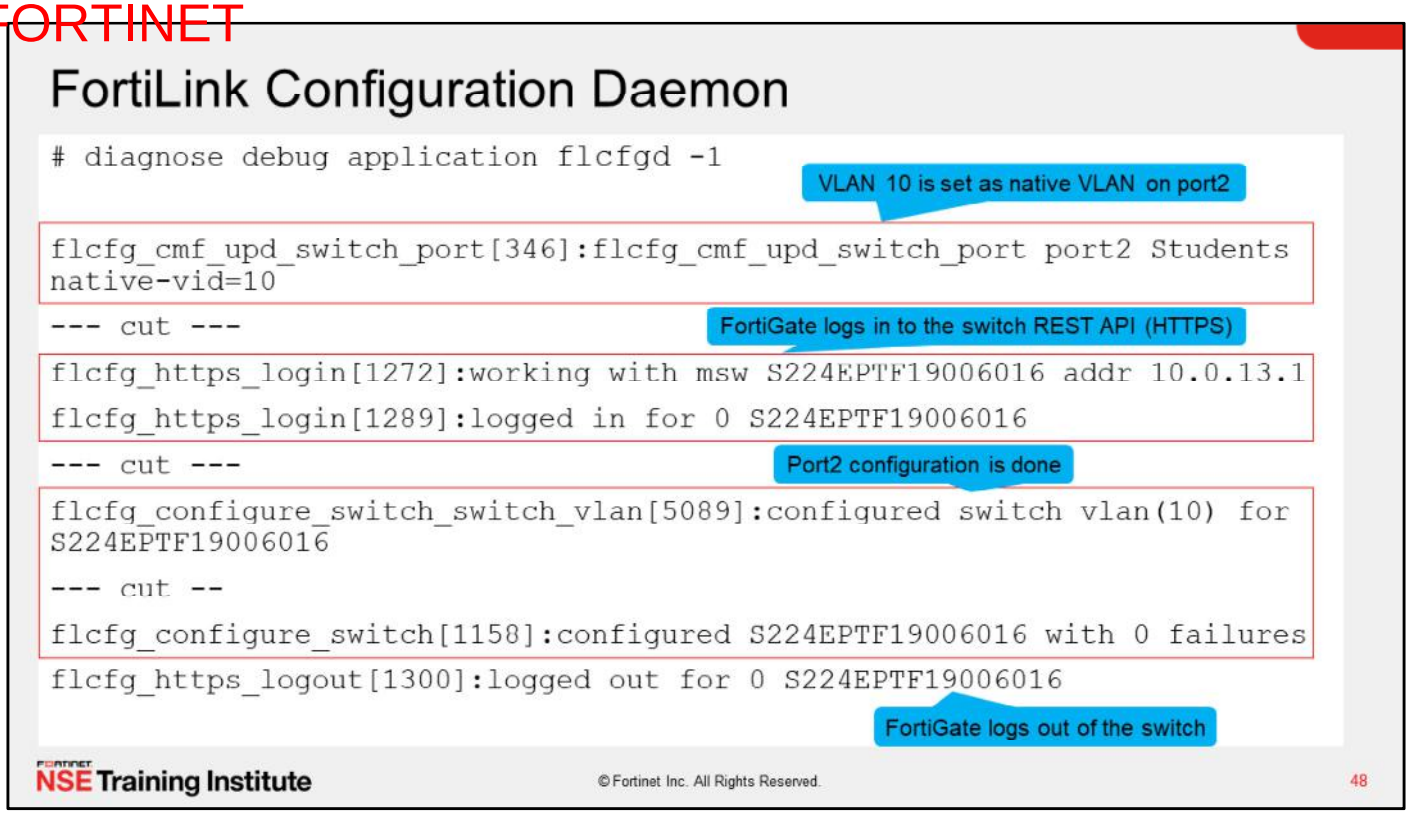
DO NOT REPRINT
© FORTINET
Brave-dumps.com



After you authorize a switch and it comes online, the switch starts sending FortiLink heartbeats to FortiGate every 3 seconds. FortiGate then acknowledges the heartbeats by sending a reply to the switch. The debug output for the `fortlinkd` process also shows these heartbeats.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

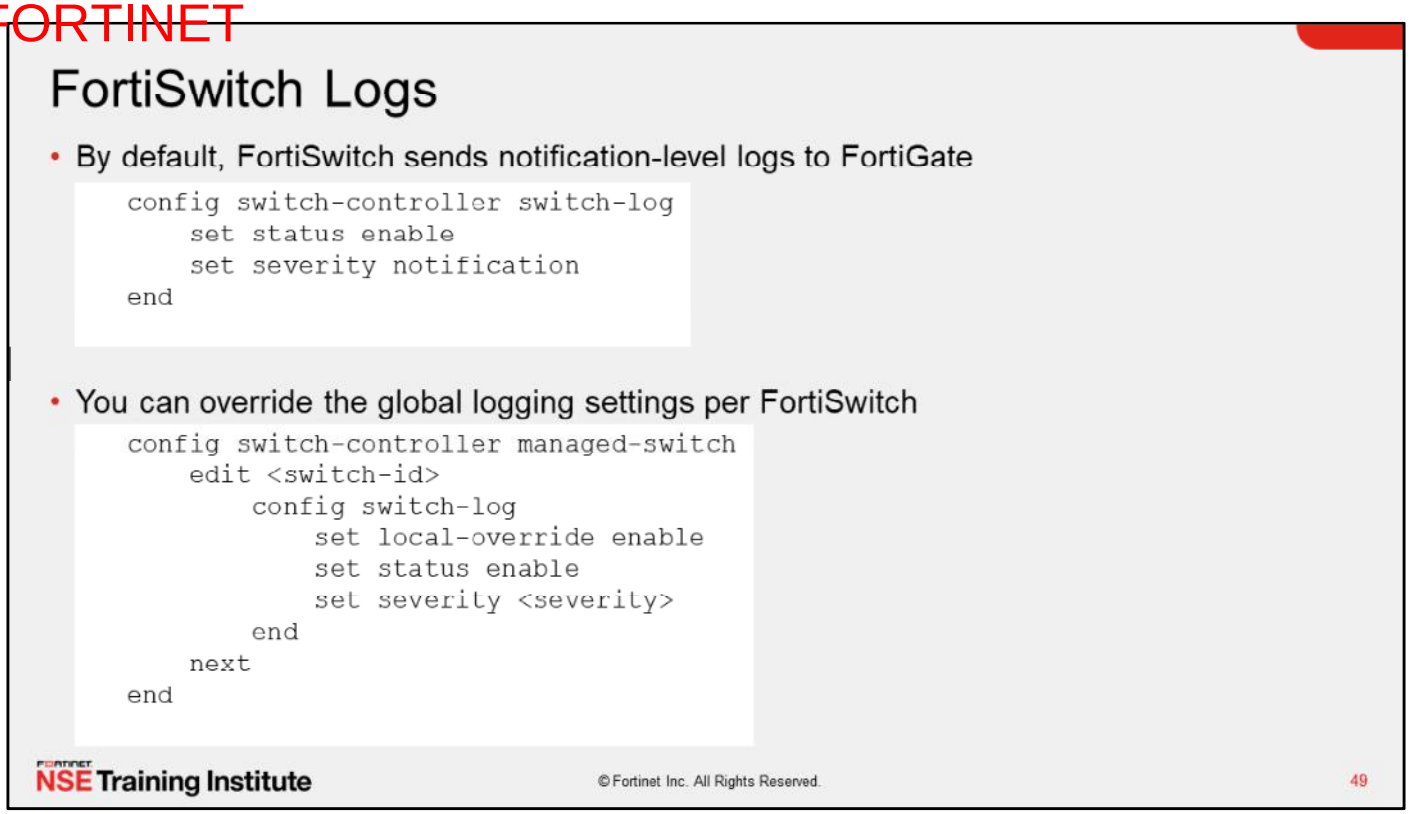


To troubleshoot or monitor the configuration changes applied by FortiGate to the switches, you can enable debug for the FortiLink configuration daemon.

In the example shown on this slide, the administrator sets the native VLAN for `port2` on the switch to `Students`. The `Students` VLAN uses VLAN ID 10. Because the change is made on FortiGate, it triggers a configuration push to the managed switch. FortiGate first logs in to the managed switch REST API through HTTPS, and then applies the configuration changes required for port2. After it finishes applying the changes, FortiGate logs out of the switch.

Vouchers & Dumps are Available | WhatsApp +201224560923

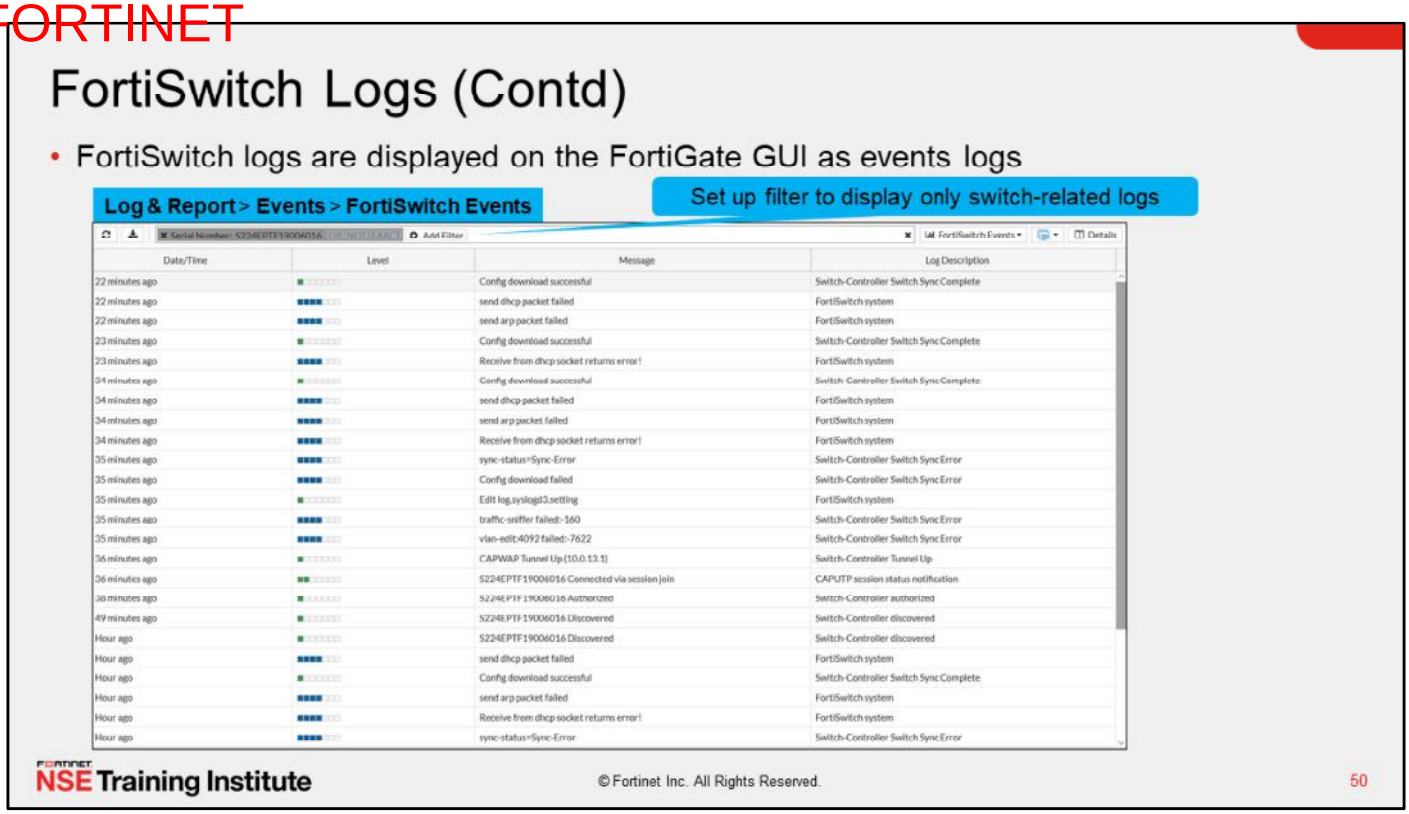
DO NOT REPRINT
© FORTINET
Brave-dumps.com



By default, all managed switches send notification-level logs, including information-level logs, to FortiGate so they can be displayed on the FortiGate GUI. You can set a different log severity level either globally or for each FortiSwitch.

Vouchers & Dumps are Available | WhatsApp +201224560923

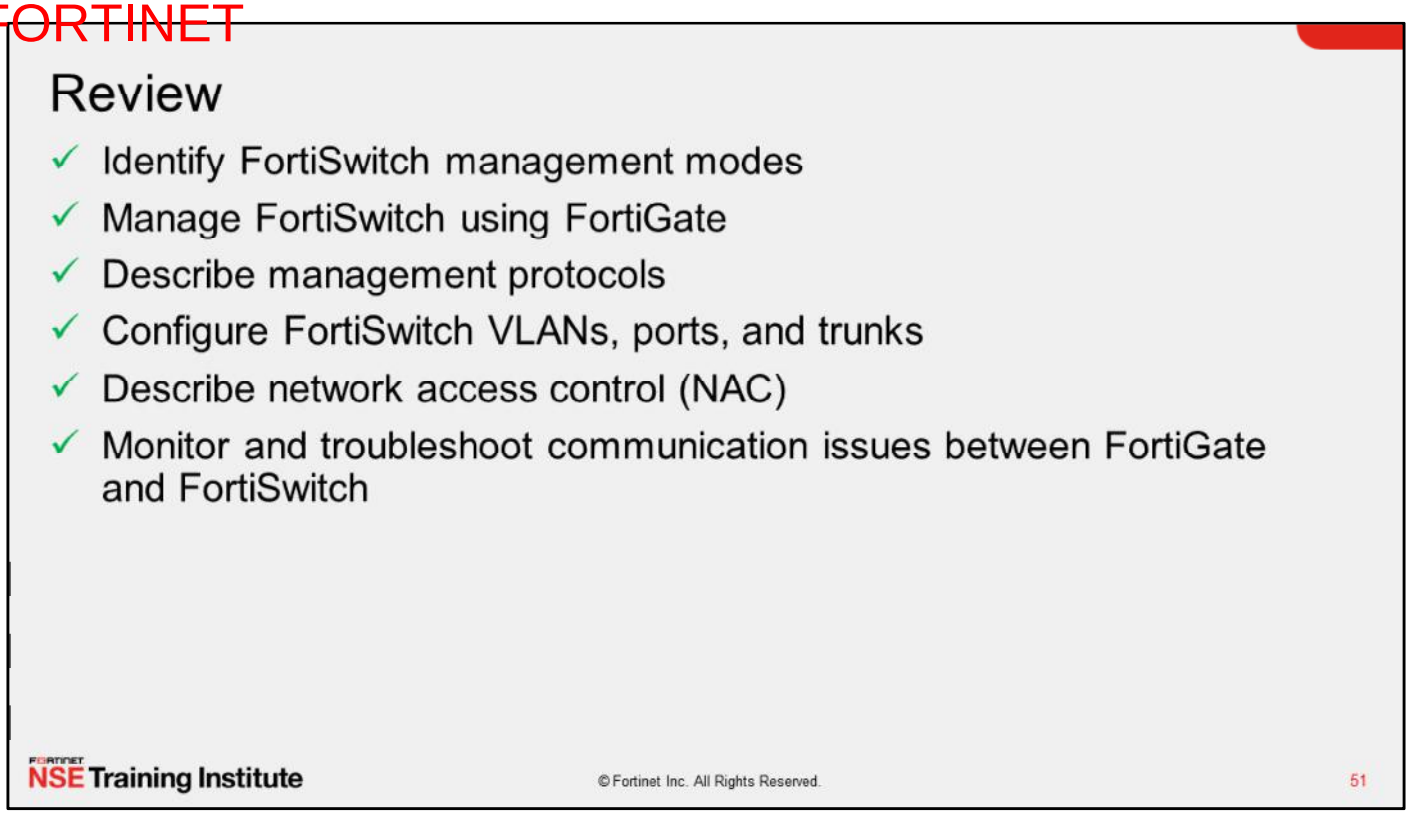
DO NOT REPRINT Brave-dumps.com
© FORTINET



This slide shows an example of FortiSwitch-related logs available on the FortiGate GUI. FortiSwitch logs are available as events logs on the FortiGate GUI. Because the event logs page also includes logs for other system-related events, the logs in this example are filtered to display only the logs for the managed FortiSwitch using the serial number.

Vouchers & Dumps are Available | WhatsApp +201224560923

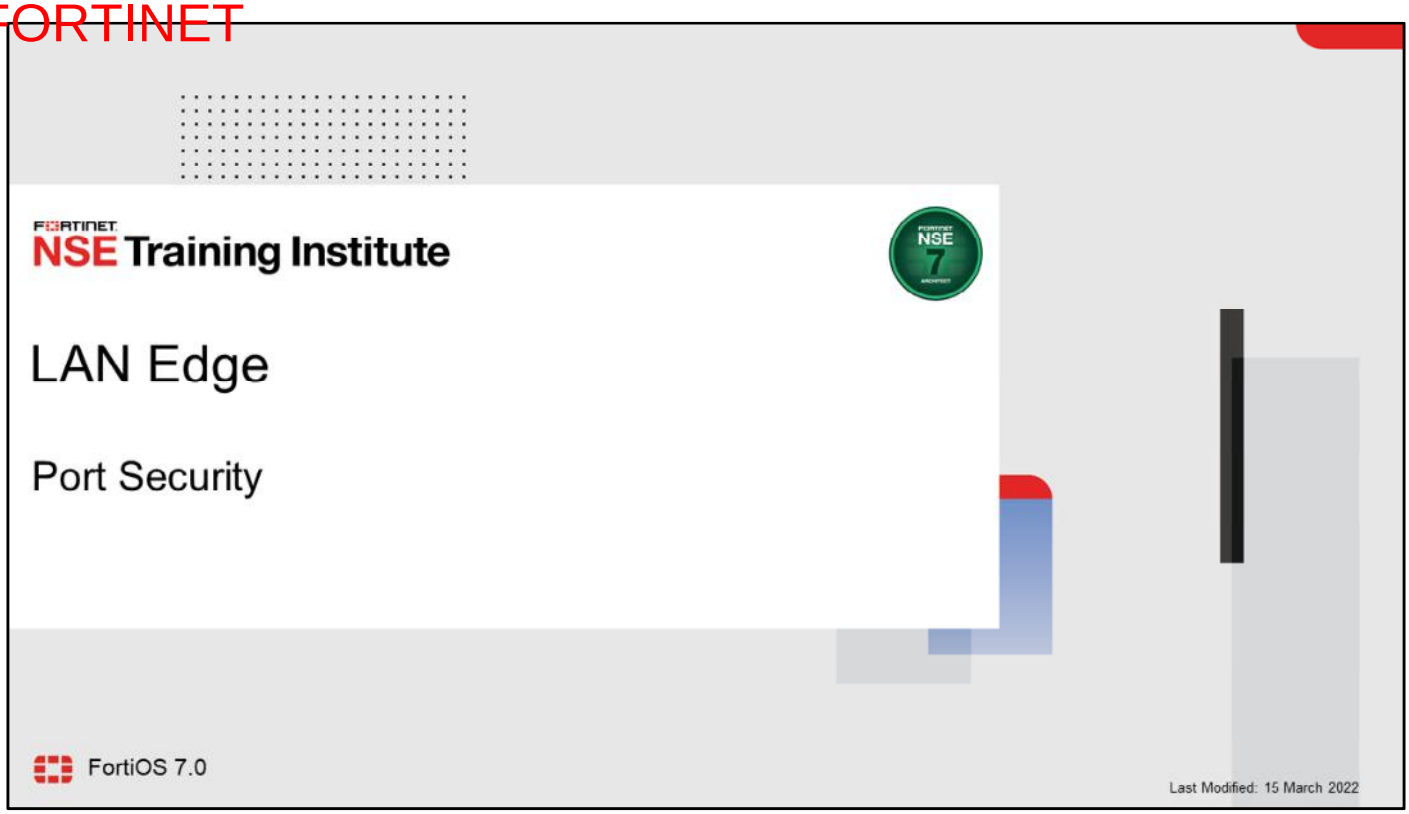
DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows the objectives that you covered in this lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

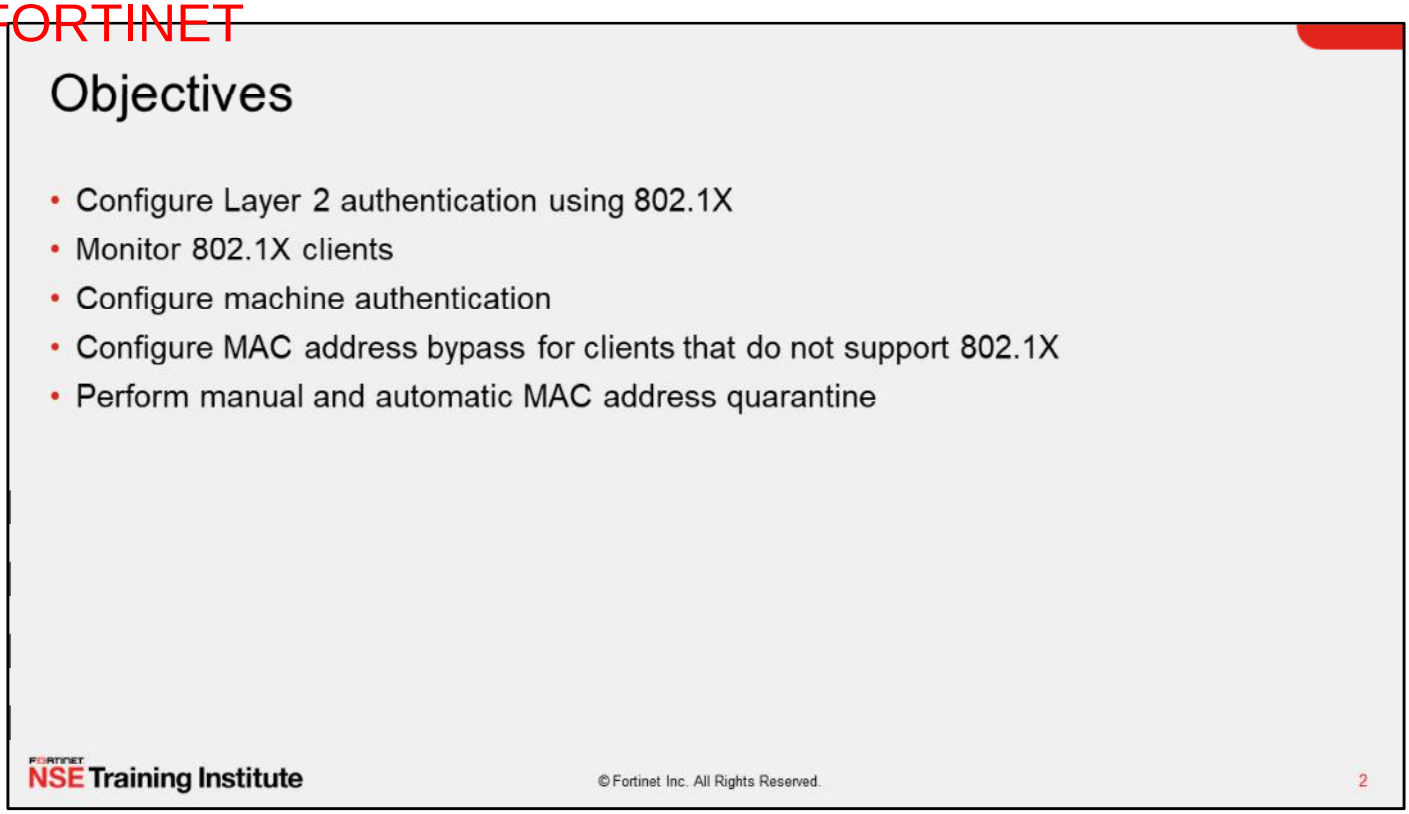


In this lesson, you will learn how to configure port authentication on FortiSwitch and FortiAuthenticator.

To maintain an enterprise-level approach, most of the information, instructions, and references are based on the FortiSwitch manager pane on FortiManager. In addition, the information displayed for FortiSwitch manager is based on *per-device management mode*. The lesson refers to some features and settings on the FortiGate CLI or GUI, only when these options cannot be easily configured on FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

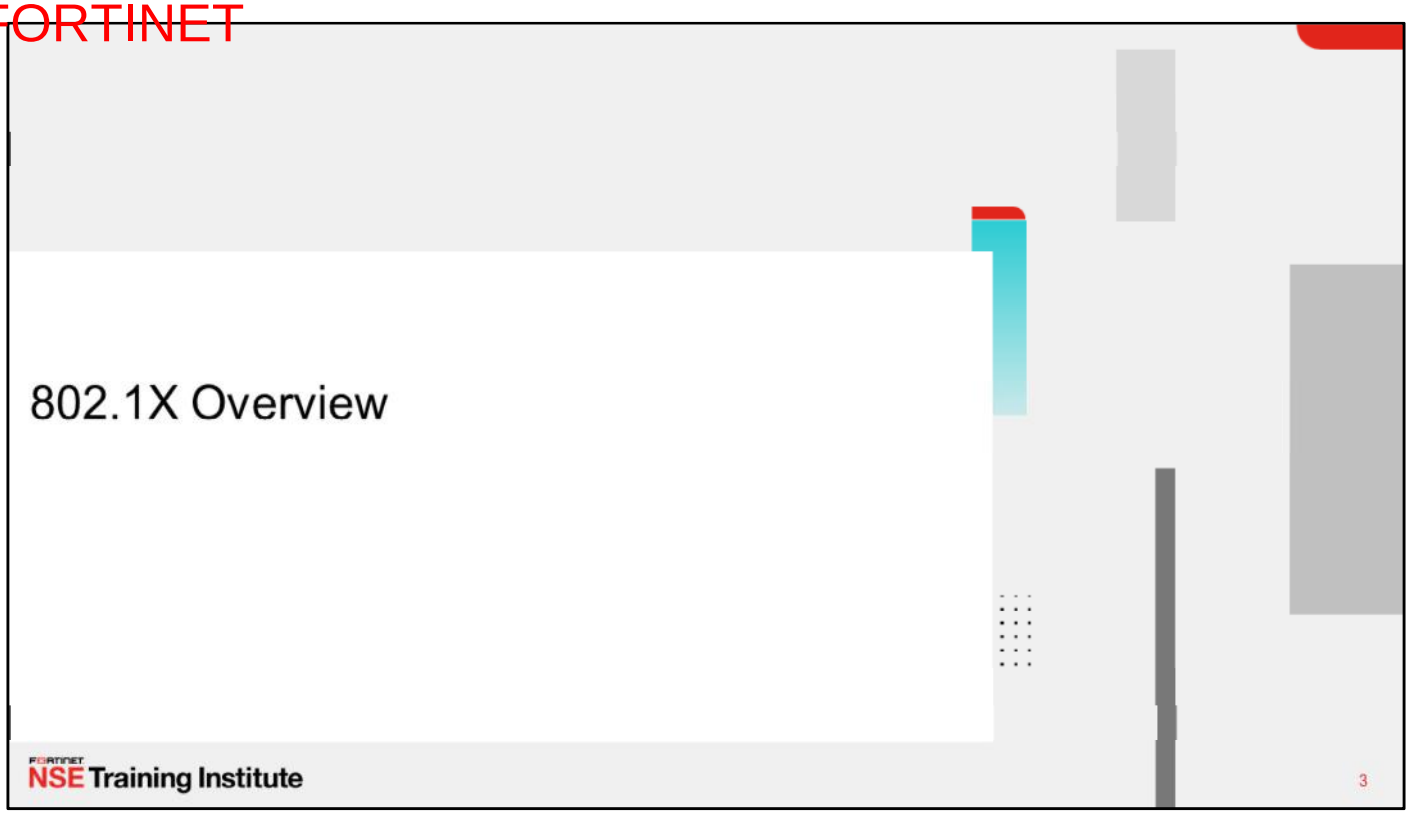


After completing this lesson, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in configuring port authentication, you will be able to control network access for devices connecting to FortiSwitch.

Vouchers & Dumps are Available | WhatsApp +201224560923

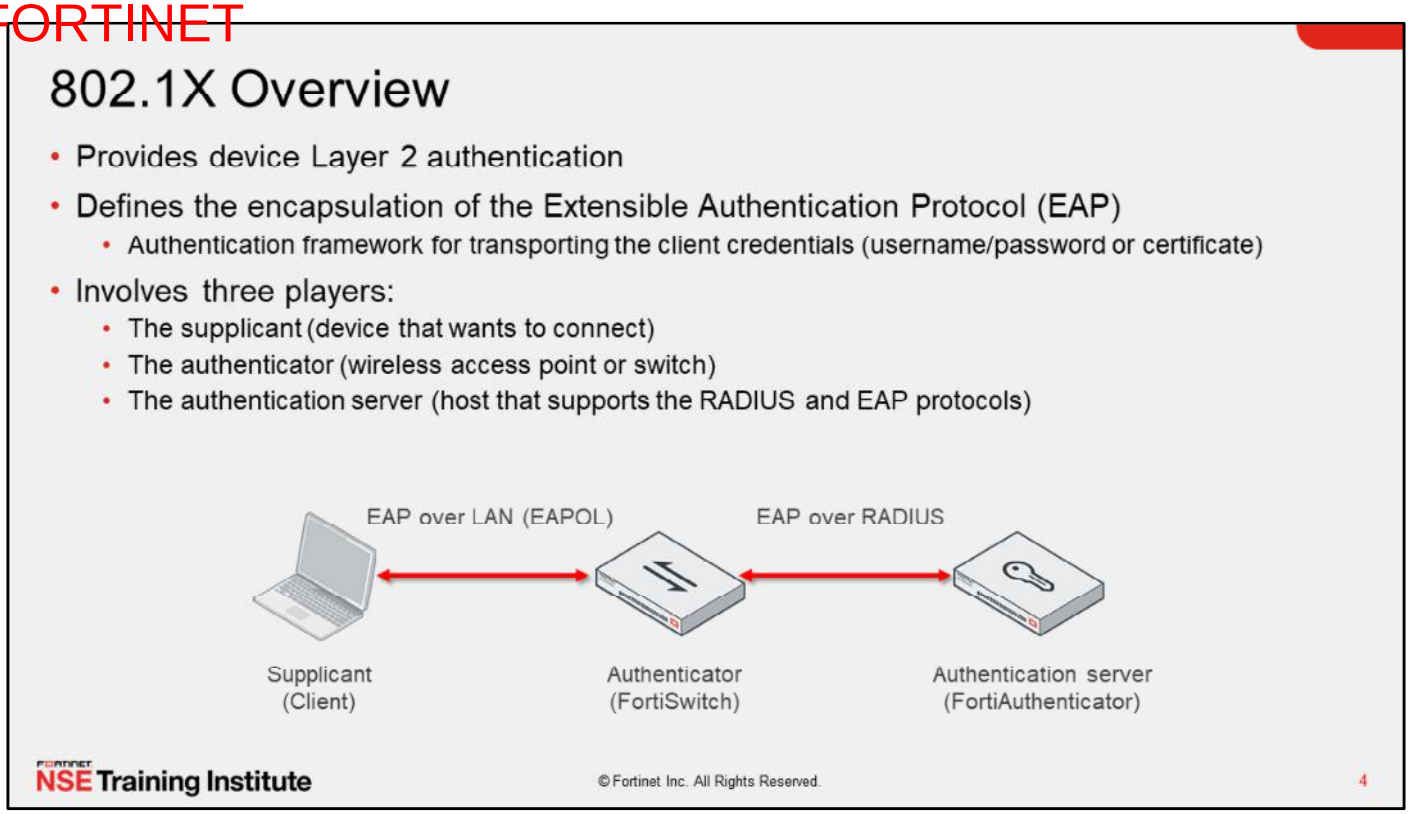
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn about 802.1X.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



802.1X is a standard that is designed to provide authentication services to network devices that want to join a wired or wireless network. The 802.1X standard defines an authentication protocol called EAP. It also defines how EAP is encapsulated over the LAN (the EAPOL protocol) and over RADIUS.

802.1X involves the following three parties:

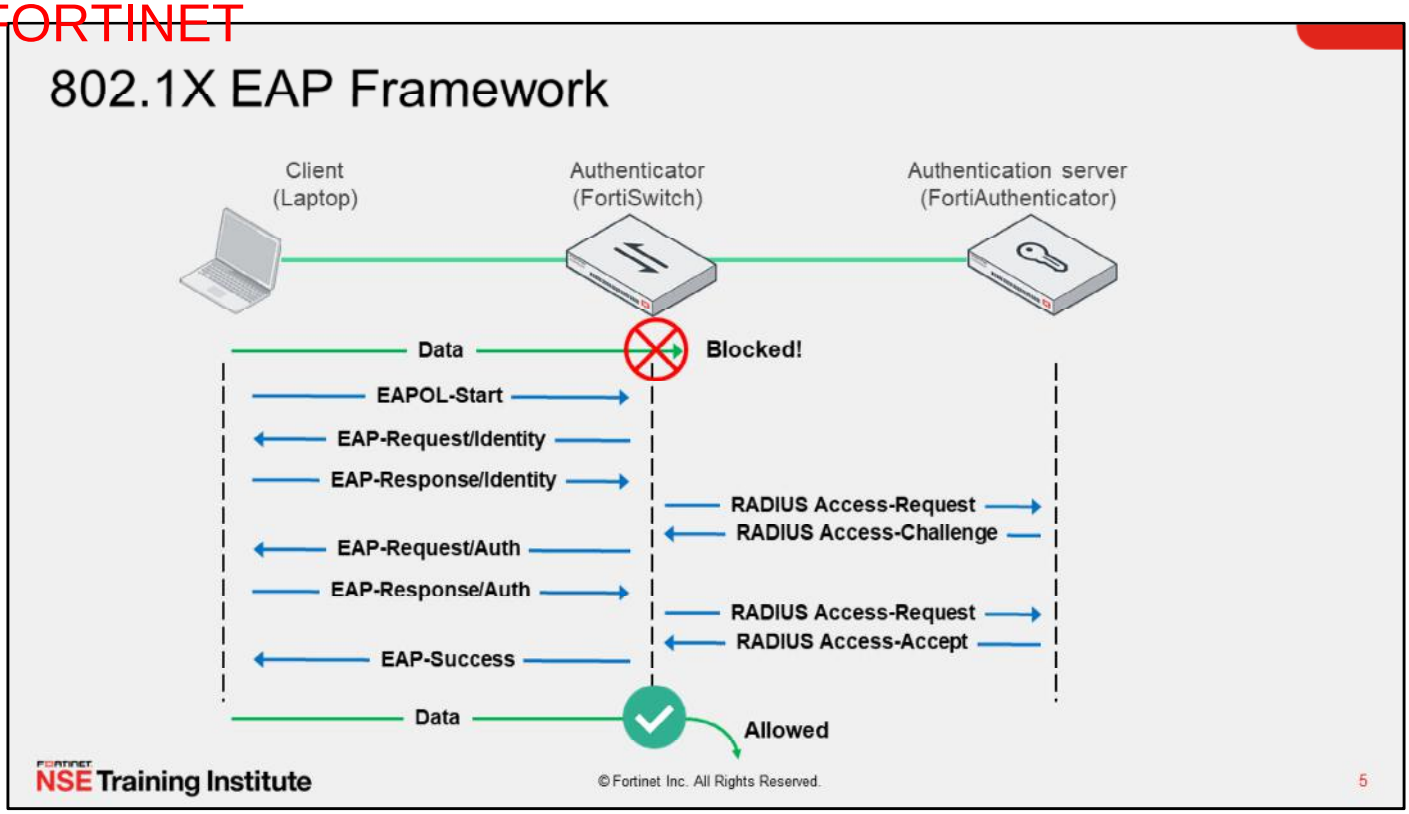
- The client, also known as the supplicant, is the device that wants to join the network. Its network stack must support 802.1X.
- The authenticator is a network device, such as a wireless access point or a switch, that acts as the broker in the authentication process. The authenticator allows or denies network access to the supplicant based on the response received from the authentication server.
- The authentication server is a host that supports the RADIUS and EAP protocols, such as FortiAuthenticator, that verifies the client credentials. The client credentials can be a username and password, or a digital certificate. The authentication server also grants the supplicant with a level of network access based on the existing network policies.

The client is not allowed to access the network until the client credentials are validated and authorized. Using 802.1X authentication, the client provides their credentials to the authenticator, which then passes on the information to the authentication server for verification. If the authentication server determines that the credentials are valid, the client device is granted access to the network.

Note that the authenticator does not need to store the client credentials or have knowledge of the authentication method (for example, PEAP or EAP-TLS). The authentication messages are tunneled from the client to the authentication server over the RADIUS protocol.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



When a client (laptop) connects to a LAN switch that requires 802.1X authentication, the client sends its credentials to the authenticator (FortiSwitch) using EAP over LAN (EAPOL) frames. The authenticator then forwards the EAP messages to the authentication server (FortiAuthenticator), which is a RADIUS server that supports EAP.

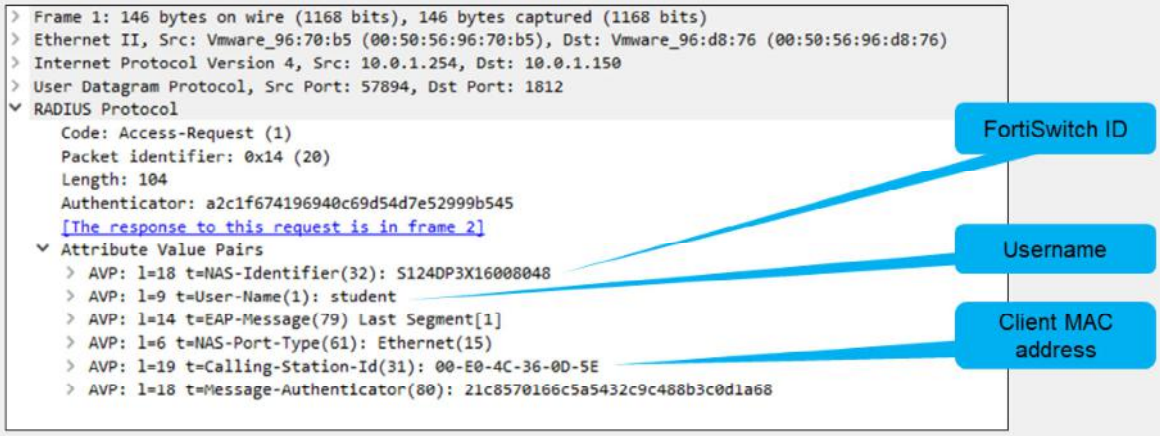
Before the client is authenticated, any non-EAPOL traffic sent by the client is blocked by the authenticator. The client authentication process is as follows:

1. The client sends an EAPOL-Start frame to initiate the EAP authentication.
2. The authenticator replies with an EAP-Request/Identity message to request identification. All EAP messages exchanged between the client and the authenticator are encapsulated into EAPOL frames.
3. The client responds with an EAP-Response/Identity message that contains the client identity (usually the username).
4. The authenticator forwards the EAP-Response/Identity message to the authentication server in a RADIUS Access-Request packet. All EAP messages exchanged between the authenticator and the authentication server are encapsulated into RADIUS packets.
5. The authentication server replies with a RADIUS Access-Challenge packet containing an EAP-Request message indicating the authentication method to use by the supplicant.
6. If the supplicant agrees on the requested EAP method, it responds with an EAP-Response message.
7. The client and the authentication server exchange multiple EAP-Request and EAP-Response messages for credentials verification.
8. The authentication process finishes when the authentication server sends to the client an EAP-Success message encapsulated into a RADIUS Access-Accept message.
9. At this point, any non-EAPOL traffic, such as IP traffic, is allowed by the authenticator.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

RADIUS Access-Request Packet

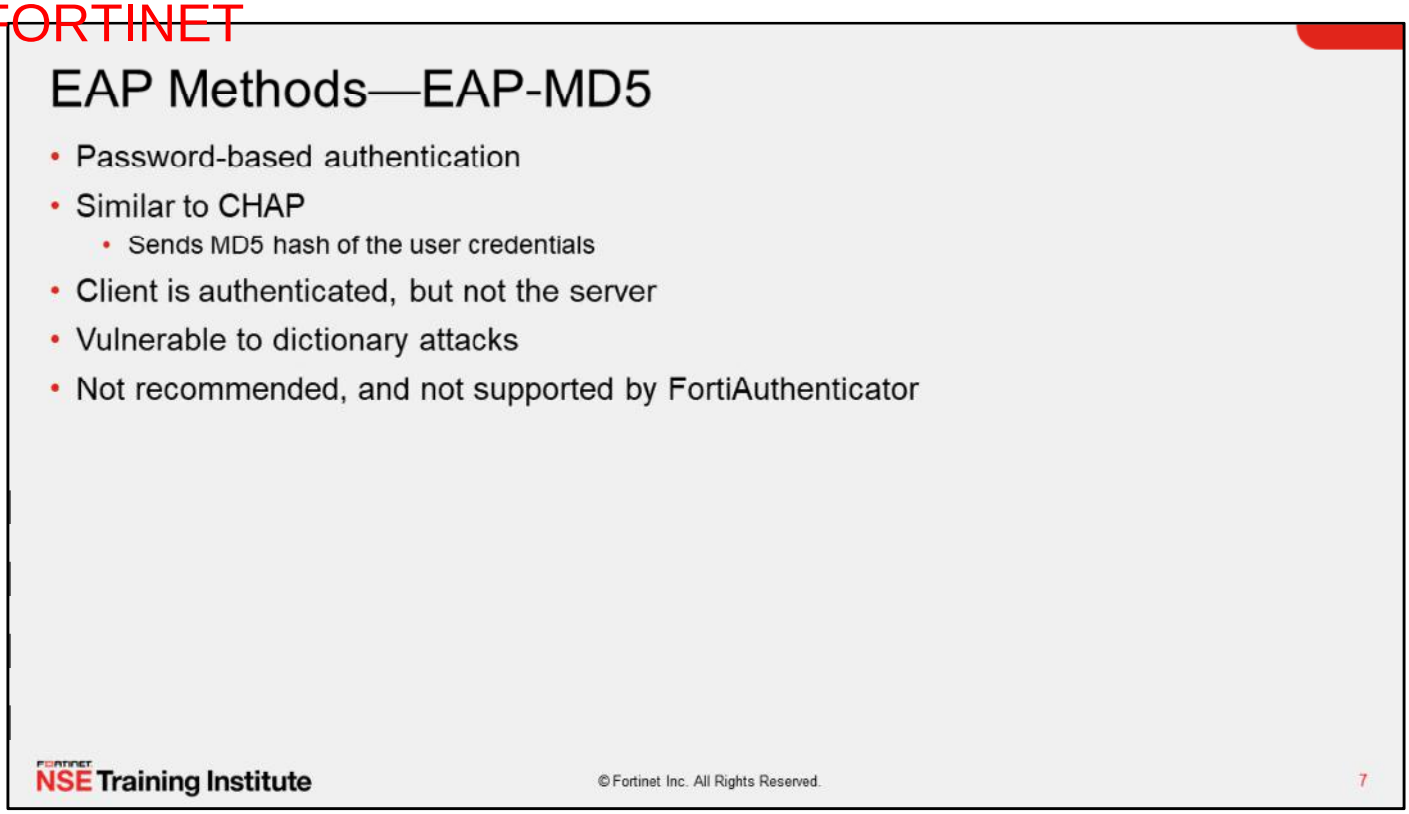


NSE Training Institute
© Fortinet Inc. All Rights Reserved.

The packet capture on this slide shows the RADIUS Access-Request that is sent from a Layer 2 switch (acting as an authenticator) to the authentication server. It contains the switch ID, username, and switch MAC address.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



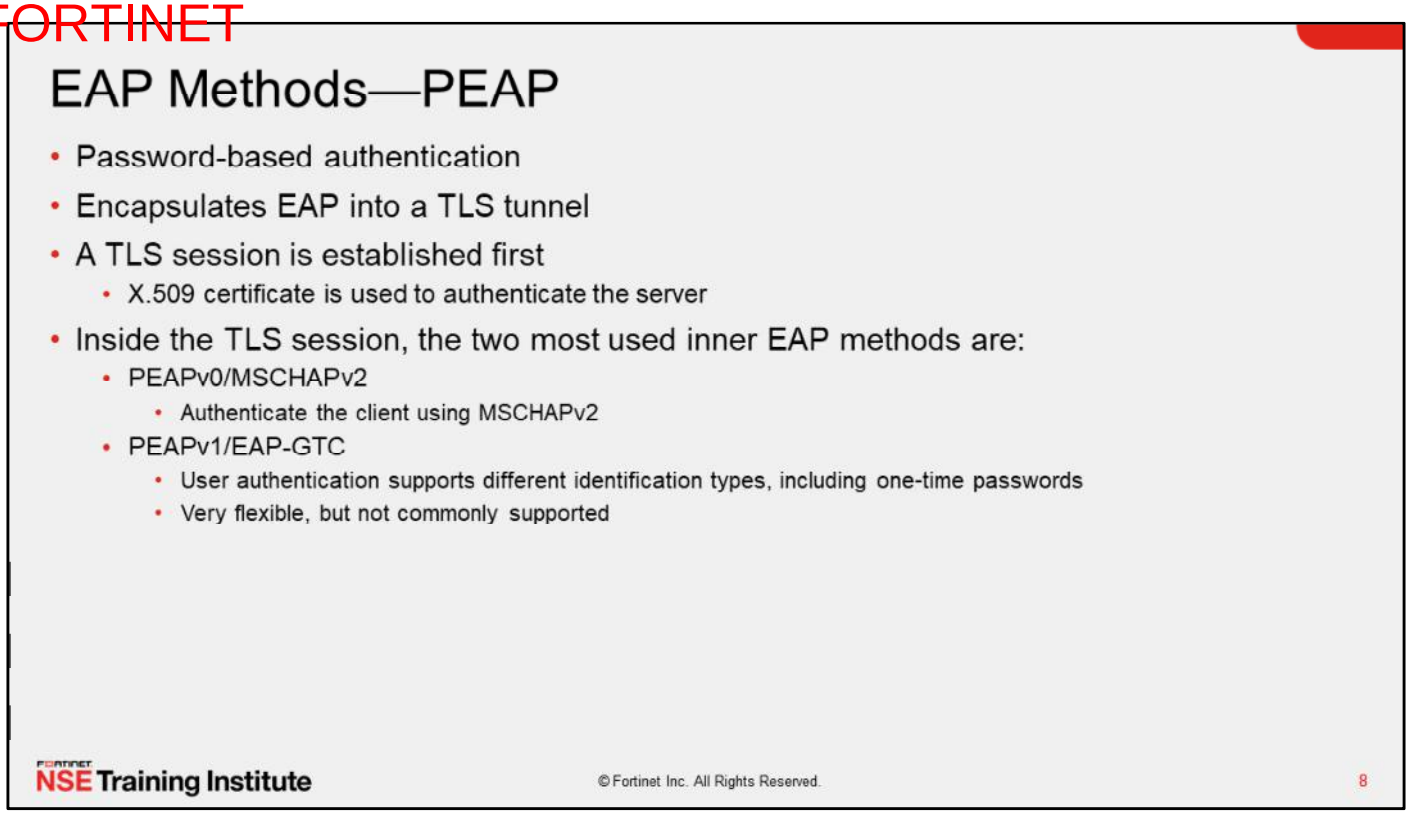
EAP-MD5 operates like Challenge Handshake Authentication Protocol (CHAP). The authentication server sends an MD5 challenge message, to which the client replies with an MD5 hash of its credentials.

As a result, EAP-MD5 can only authenticate clients, and does not offer a mechanism for authenticating servers. EAP-MD5 is also known to be vulnerable to dictionary attacks.

This method is not recommended and is not supported by FortiAuthenticator.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

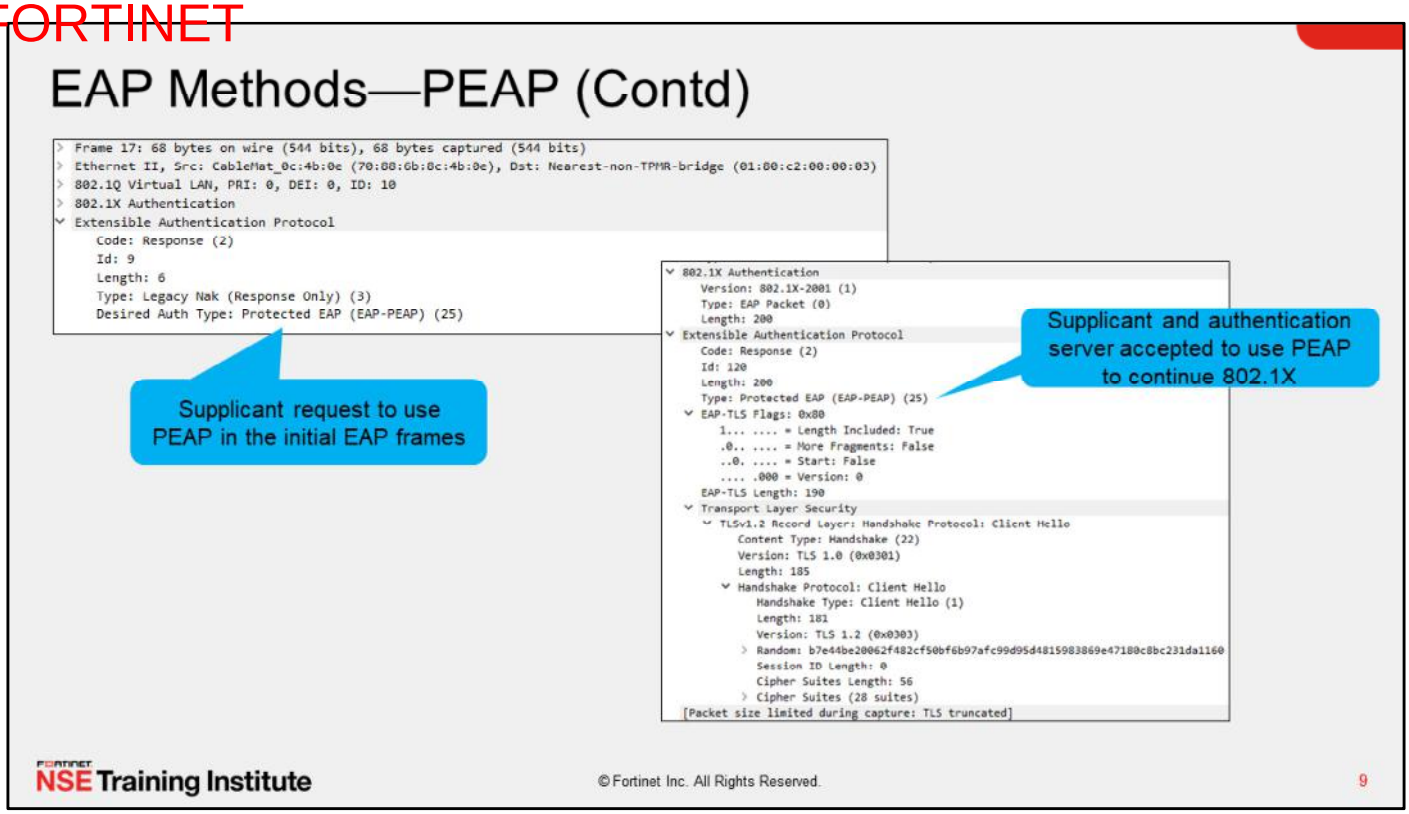


In Protected EAP (PEAP), a TLS tunnel is established first. During the TLS tunnel setup, the server is authenticated using a digital certificate. After the TLS tunnel is established, the client and authentication server can use any inner EAP method for authentication. However, the two most used inner EAP methods are:

- PEAPv0/MSCHAPv2: authenticates the client using MSCHAPv2.
- PEAPv1/EAP-GTC: sometimes referred to as simply EAP-GTC. Uses different identification mechanisms (including one-time passwords) for authenticating clients, which makes it very flexible. FortiAuthenticator supports it, but it is not commonly supported by other vendors.

Vouchers & Dumps are Available | WhatsApp +201224560923

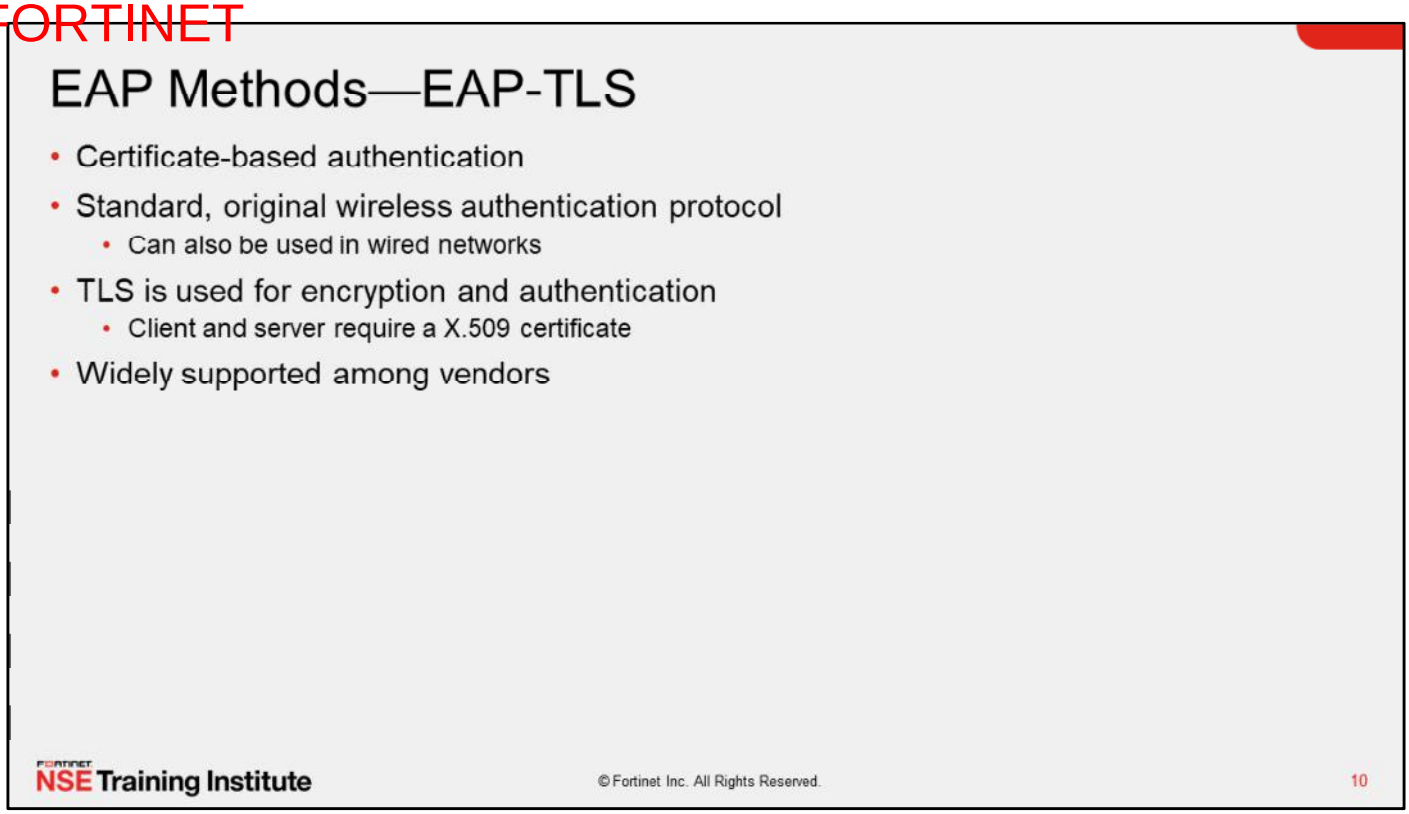
DO NOT REPRINT Brave-dumps.com
© FORTINET



The supplicant (client) starts the communication by sending an EAPOL frame that includes the identity as well as the desired authentication type to use in the EAP protocol. This is shown in the example PEAP type on the slide. The response from the authentication server to challenge the supplicant will initiate the process to select which EAP method to use and supported by all devices. You can see that the subsequent frame includes the type of EAP frame—**Protected EAP (EAP-PEAP)**—which is the method that will be used by all devices: the supplicant, the authenticator, and the authentication server.

Vouchers & Dumps are Available | WhatsApp +201224560923

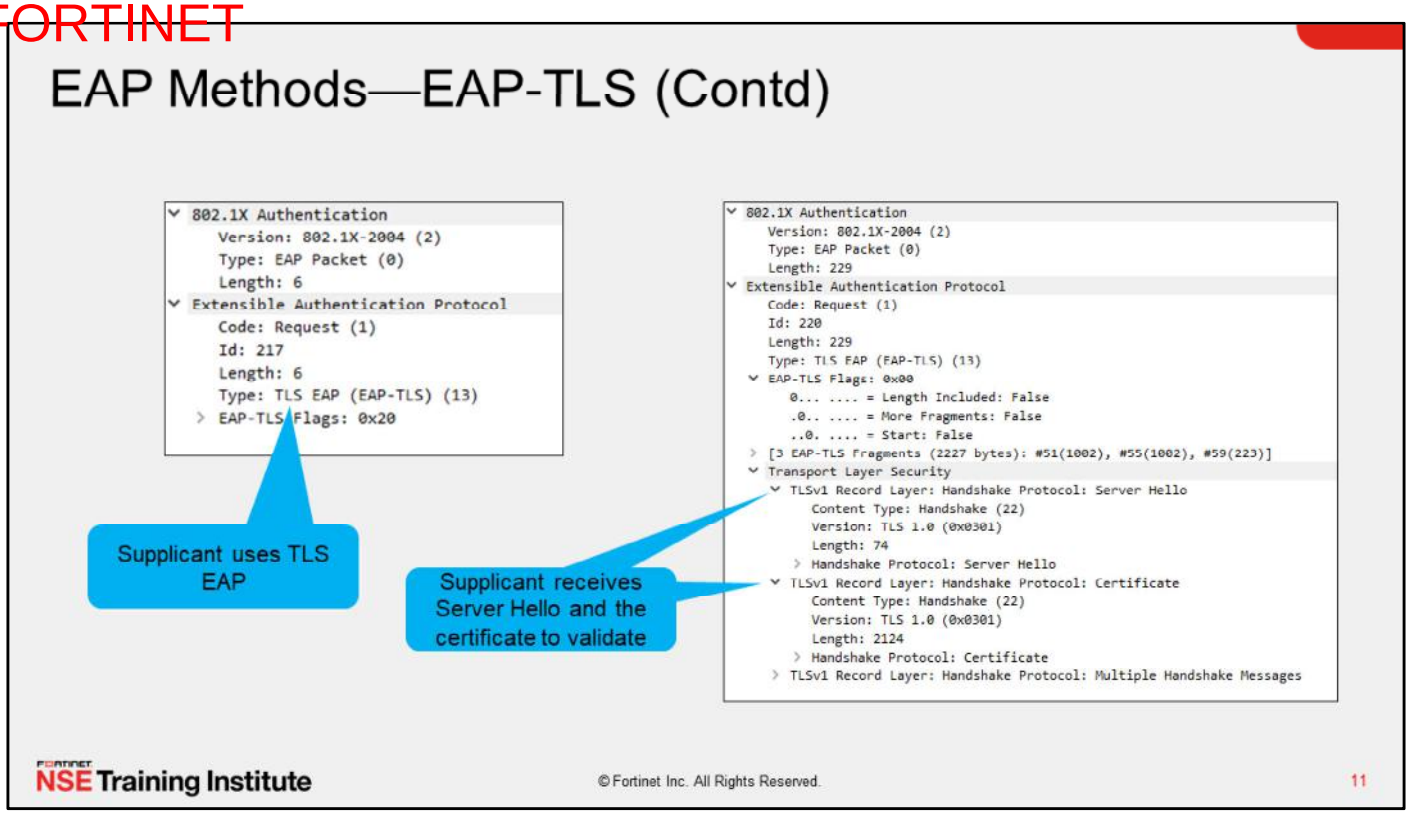
DO NOT REPRINT
© FORTINET
Brave-dumps.com



EAP-TLS is one of the most popular EAP methods for authenticating both wireless and wired devices. It is also considered one of the most secured methods, mainly because besides using TLS to encrypt messages exchanged between the client and the authentication server, it also authenticates both client and server using digital certificates.

Vouchers & Dumps are Available | WhatsApp +201224560923

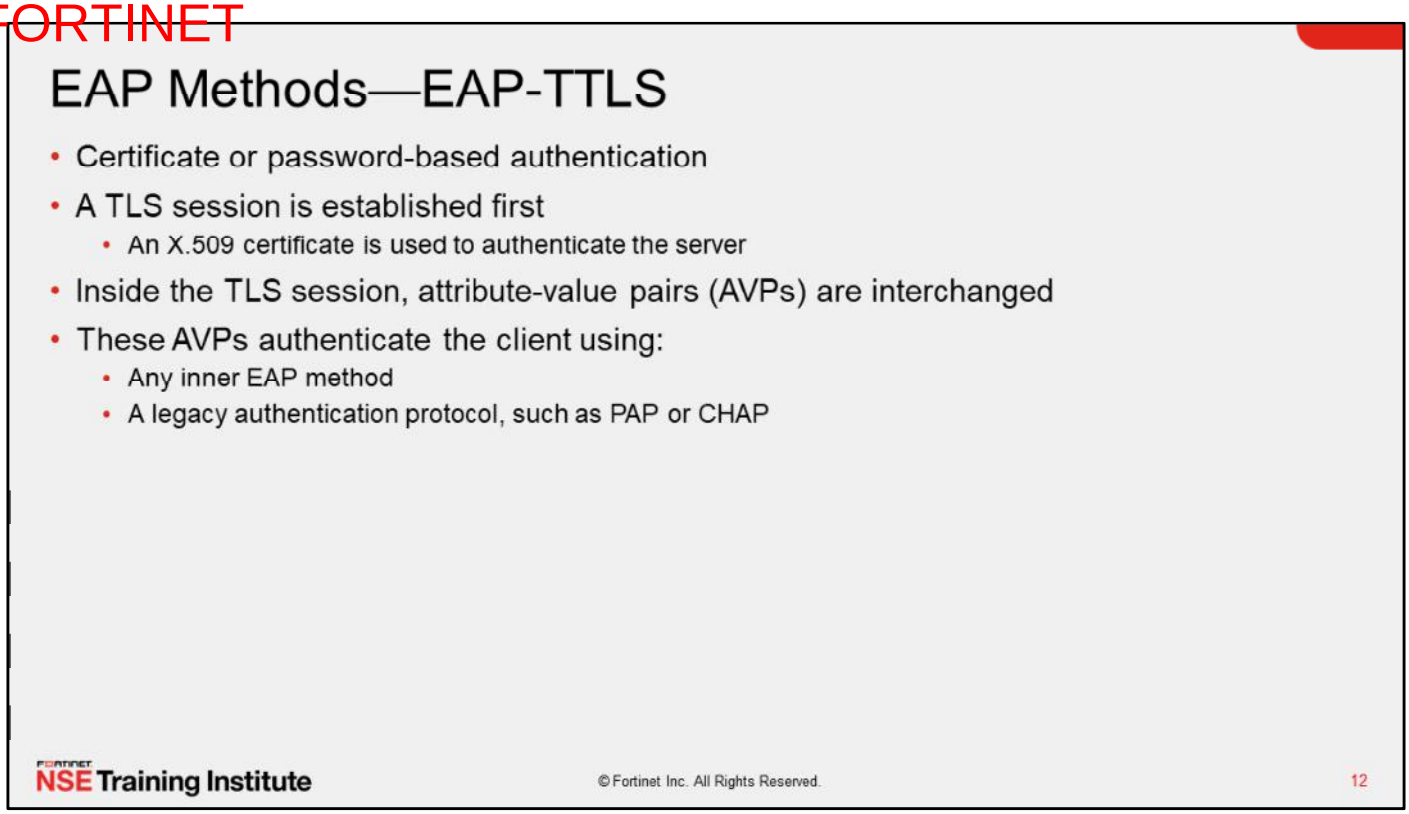
DO NOT REPRINT
© FORTINET
Brave-dumps.com



When the supplicant uses TLS EAP (EAP-TLS), it starts validating the server certificate (the authentication server) with a Client Hello frame after it establishes EAP communication with the authenticator. The authentication server then responds with a Server Hello, along with the certificate for the client to validate. The rest of the process follows the client-authenticated TLS handshake encapsulated within EAP frames. The client follows by providing its certificate for validation and so on.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Another method is EAP tunneled TLS (EAP-TTLS). With this method, AVPs authenticate clients using either any inner EAP method or a legacy authentication protocol, such as PAP or CHAP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

EAP Methods Supported by FortiAuthenticator

	EAP-TLS	EAP-TTLS	PEAP
Protocol	TLS session that validates server and client certificates	Establishes a TLS session, and exchanges AVPs	Establishes a TLS session, and supports two versions: • PEAPv0/EAP-MSCHAPv2 (PEAP in GUI) • PEAPv1/EAP-GTC (EAP-GTC in GUI)
Server certificate	Required	Required	Required
Client certificate	Required	Optional	Optional
Server authentication	X.509 certificate	X.509 certificate	X.509 certificate
Client authentication	X.509 certificate	Various identification types over AVPs	• MS-CHAPv2 • Various identification types over GTC

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

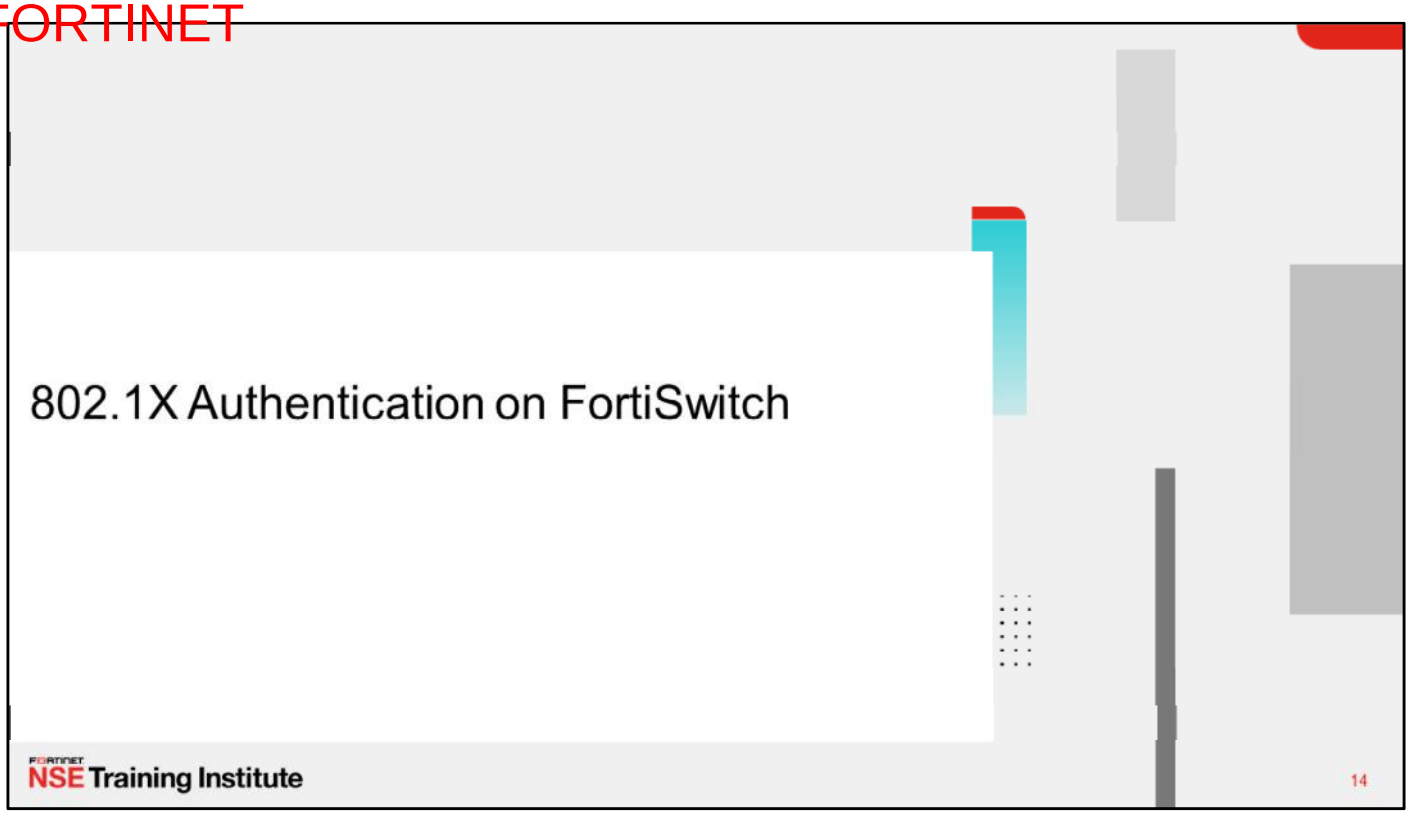
13

FortiAuthenticator supports EAP-TLS, EAP-TTLS, and PEAP. Although on its GUI, FortiAuthenticator displays EAP-TLS, EAP-TTLS, PEAP, and EAP-GTC, note that PEAP and EAP-GTC refer to PEAPv0/EAP-MSCHAPv2 and PEAPv1/EAP-GTC, respectively.

In all these methods, a TLS session is established first, and a digital certificate is used for authenticating the server. The way clients are authenticated varies from one method to another.

Vouchers & Dumps are Available | WhatsApp +201224560923

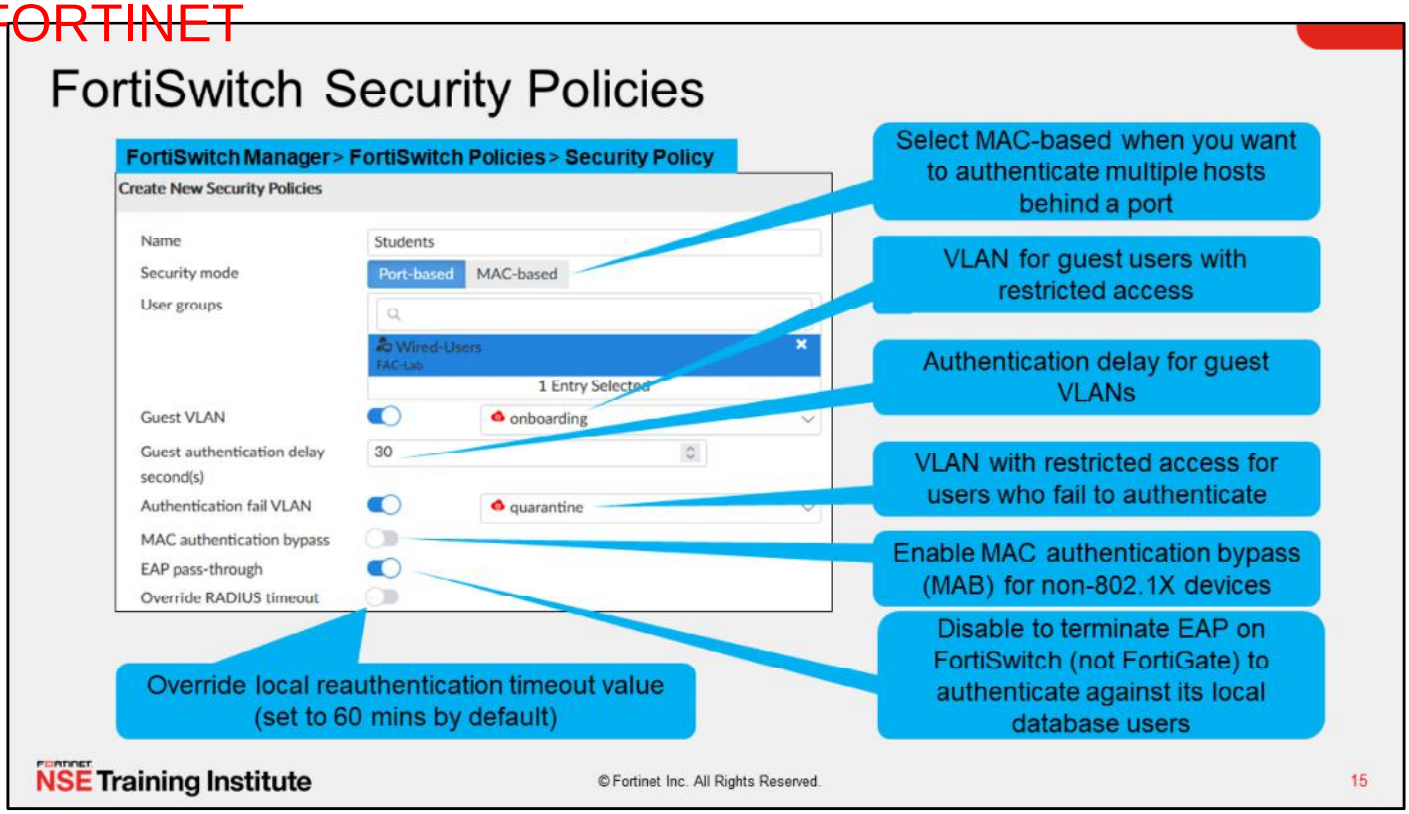
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn about 802.1X authentication on FortiSwitch.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



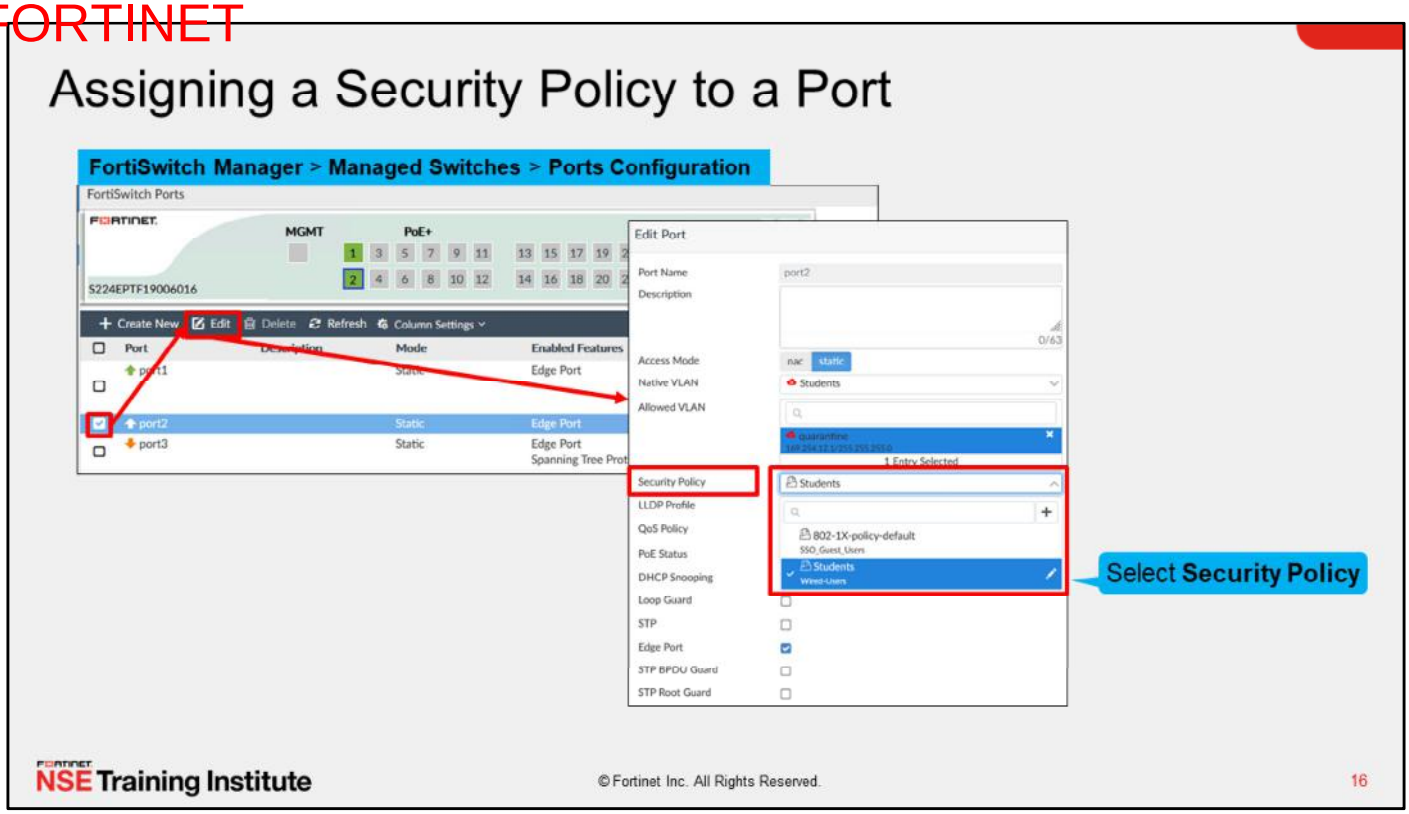
To configure 802.1X port authentication on FortiSwitch, you must first create a security policy. When you configure a security policy, you must select **Port-based** or **MAC-based** as the **Security mode**. **Port-based** is preferred when you expect a single host per port to authenticate, even though there may be multiple hosts connecting to the same port. Under this scenario, FortiSwitch authenticates a single host, and opens the port to other devices behind the port. A use case for this scenario could be an AP. After the AP authenticates against the switch, any of its connected devices can access the network despite using a different MAC address from the one used by the AP during authentication. In addition, all devices will be granted the same access level assigned to the AP during authentication. However, if you want to authenticate each device behind a port, and optionally, grant each device with a different access level based on the credentials provided, then **MAC-based** is required. Security-wise, MAC-based is also preferred because all hosts (or MAC addresses) behind the port must authenticate for accessing the network. Performance-wise, port-based is better because only a single host is required to authenticate.

In cases where a device does not support 802.1X, you can configure the security profile to place that device in the VLAN selected as **Guest VLAN**. Alternatively, you can enable **MAC authentication bypass** to allow network access to a non-802.1X device, provided the device MAC address is authorized on the authentication server. You can also place devices that try to authenticate through 802.1X, but fail, in the VLAN selected as **Authentication fail VLAN**.

You can disable **EAP pass-through** if the FortiSwitch role is to authenticate users against its local users database, or if the authentication server does not support EAP. The authentication process is only performed by FortiSwitch. FortiGate only pushes the settings to route EAP to the authentication server. As an 802.1X authentication server, FortiSwitch supports EAP-PEAP, EAP-TTLS, EAP-TLS, and EAP-MD5. Finally, if you enable **Override RADIUS timeout**, the switch overrides the local reauthentication timer with the session-timeout attribute value received from the RADIUS server.

Vouchers & Dumps are Available | WhatsApp +201224560923

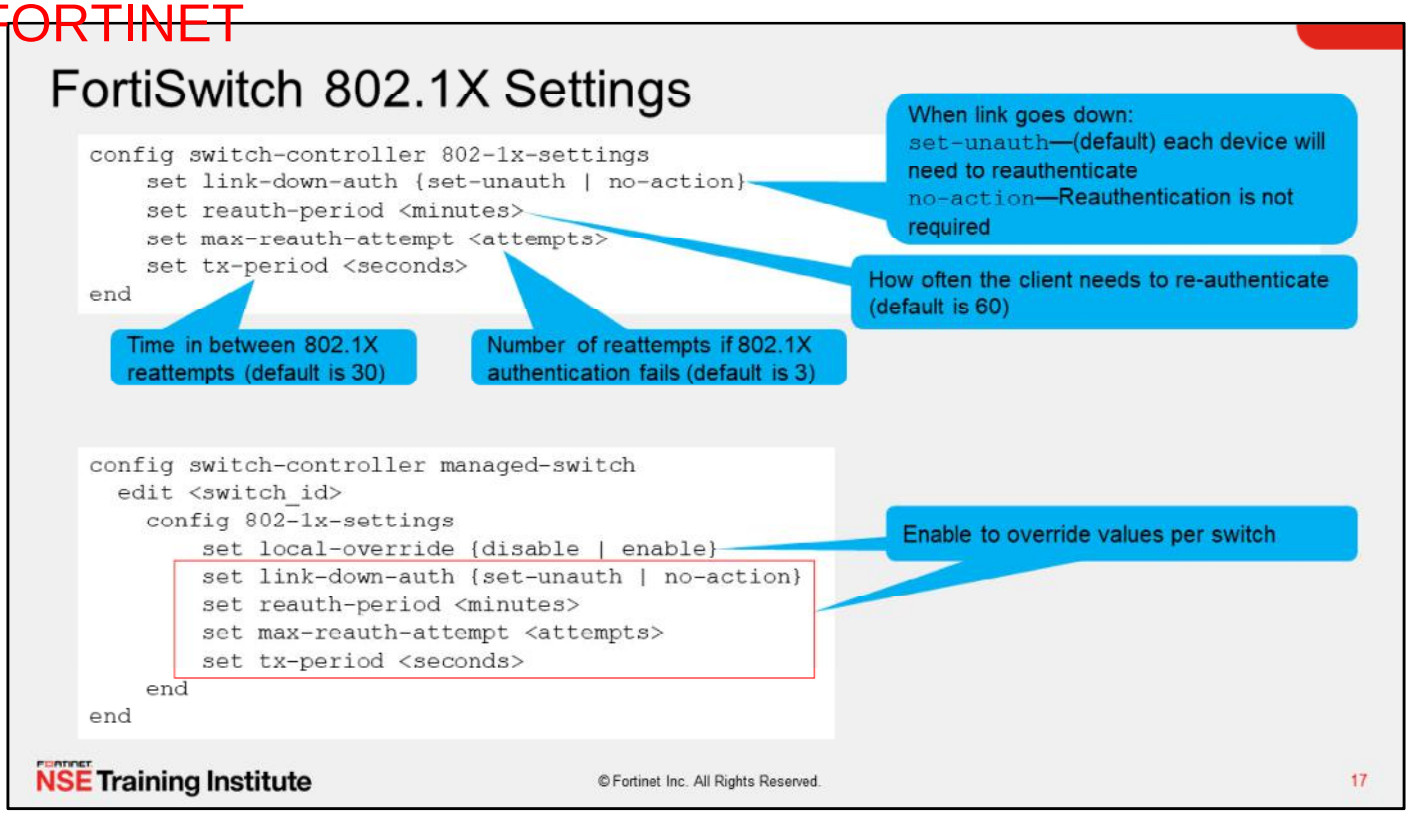
DO NOT REPRINT Brave-dumps.com
© FORTINET



After creating the security policies, you define which policy is applied to a FortiSwitch port. 802.1X authentication is enabled only on ports that have a security policy assigned to them.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



There are four 802.1X settings that can be configured either globally or per switch on the FortiGate CLI:

- `link-down-auth`: By default, FortiSwitch clears the 8021.X authentication information for a device after the port the device is connected to bounces, which results in the device having to authenticate again. However, you can configure FortiSwitch to skip reauthentication if the port bounces.
- `reauth-period`: FortiSwitch requests authenticated devices to reauthenticate every hour by default. This option allows you to adjust this timer if needed.
- `max-reauth-attempt`: Defines how many times FortiSwitch tries to authenticate a device *after* the first failed authentication attempt.
- `tx-period`: Sets the amount of time between 802.1X reauthentication attempts.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Monitoring 802.1X Ports

```
FortiGate # diagnose switch-controller switch-info 802.1X
Managed Switch : S224EPTF19006016

   port2 : Mode: port-based (mac-by-pass disable)
           Link: Link up
           Port State: authorized: (  )
           Dynamic Authorized Vlan : 0
           Dynamic Allowed Vlan list:
           Dynamic Untagged Vlan list:
           EAP pass-through : Enable
           EAP egress-frame-tagged : Enable
           EAP auto-untagged-vlans : Enable
           Allow MAC Move : Disable
           Dynamic Access Control List : Disable
           Quarantine VLAN (4093) detection : Enable
           Native Vlan : 10
           Allowed Vlan list: 10,4093
           Untagged Vlan list: 4093
           Guest VLAN :
           Auth-Fail Vlan :
           AuthServer-Timeout Vlan :

           Sessions info:
           70:88:6b:8c:4b:0e     Type=802.1x,PEAP,state=AUTHENTICATED,etime=0,eap_cnt=11 params:reAuth=3600
```

802.1X security mode

Authentication state

VLAN-related settings

Device MAC address

EAP method

Authentication state

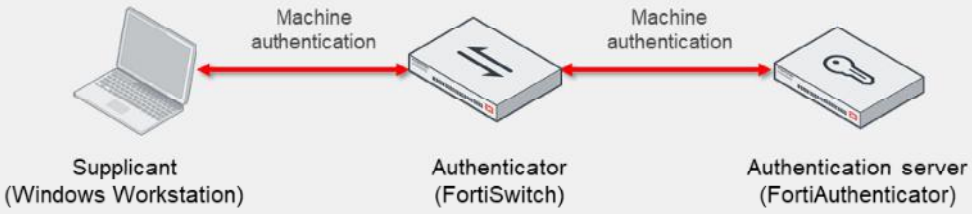
The FortiGate CLI command on this slide displays the 802.1X status for each switch port performing 802.1X authentication. The output indicates the 802.1X security mode in use, whether the device has been authorized or not, as well as the EAP method used for authentication. The output also shows important information, such as the device MAC address, quarantine VLAN, native VLAN, allowed VLANs, guest VLAN, and authentication fail VLAN.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Active Directory (AD) Machine Authentication

- AD machine authentication is performed by a Windows workstation, even before the Windows login screen appears
  - Commonly occurs on startup
- FortiAuthenticator supports machine authentication
  - It caches authenticated devices based on MAC address, for a configurable period (480 mins by default)



NSE Training Institute
© Fortinet Inc. All Rights Reserved.
19

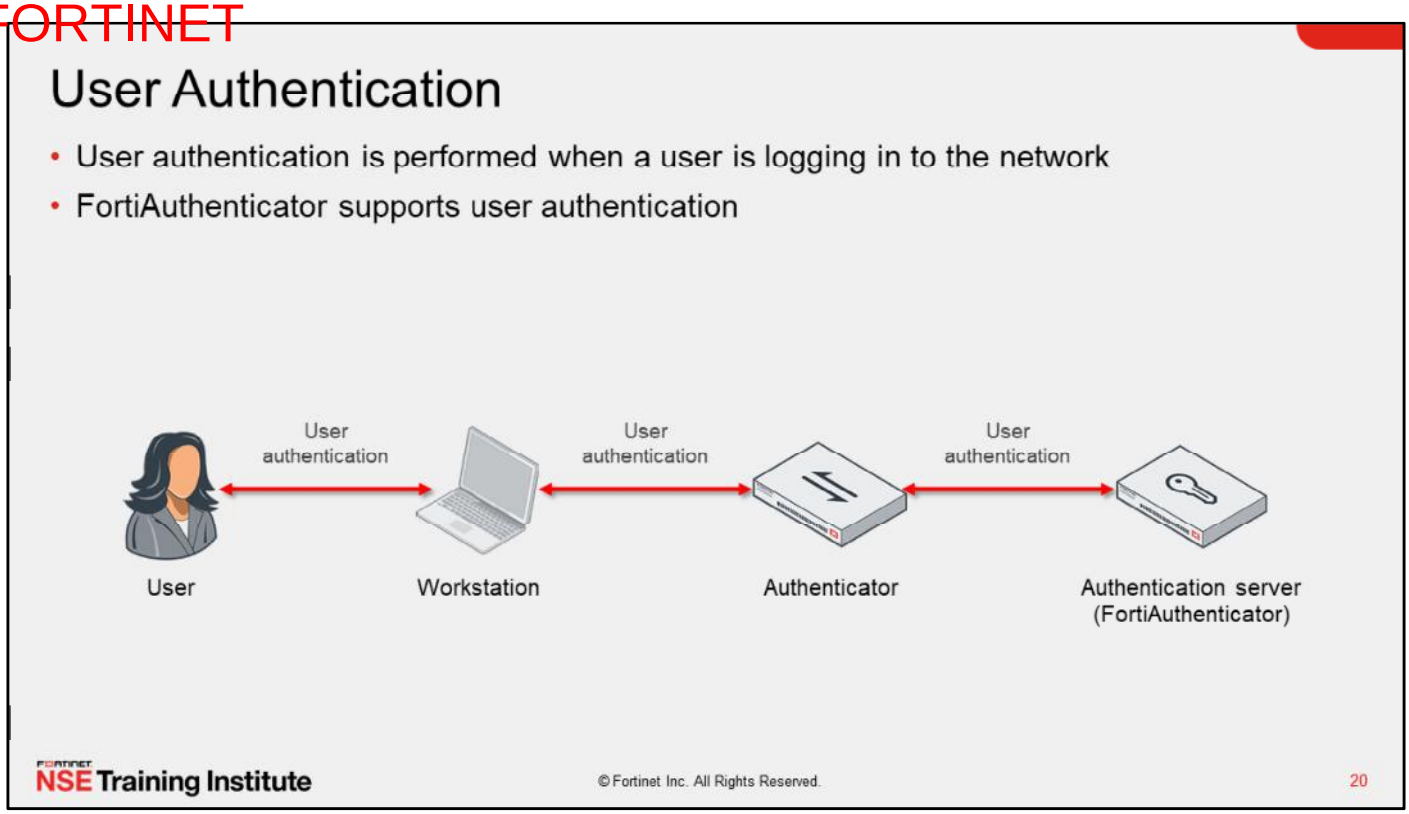
In Windows environments, there are two types of 802.1X authentication: AD machine authentication, and user authentication.

AD machine authentication is performed by the Windows OS, which sends its computer object credentials before the Windows login screen appears. Machine authentication commonly occurs on startup or logout, but not when Windows devices resume from sleep or hibernation states. To ensure previously authenticated devices continue to have access to the network after they resume from sleep or hibernation states, FortiAuthenticator caches authenticated devices based on their MAC addresses, for a configurable period of time.

Machine authentication is supported only by Windows workstations in Windows AD environments.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



User authentication is performed by a user when that user is logging in to the network.

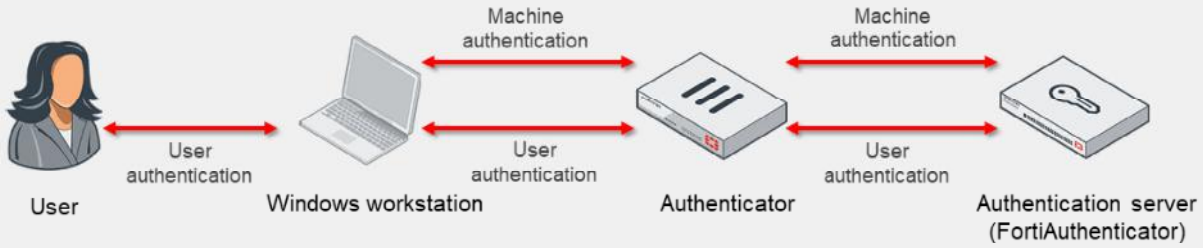
This is the traditional type of 802.1X authentication that is not restricted to Windows workstations. It is supported by almost all operating systems.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Machine and User Authentication

- FortiAuthenticator also supports the use of both machine and user authentication
  - You can limit access to the network based on machine credentials
  - User authentication can occur after machine authentication
  - You can grant further access to the network based on user credentials



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

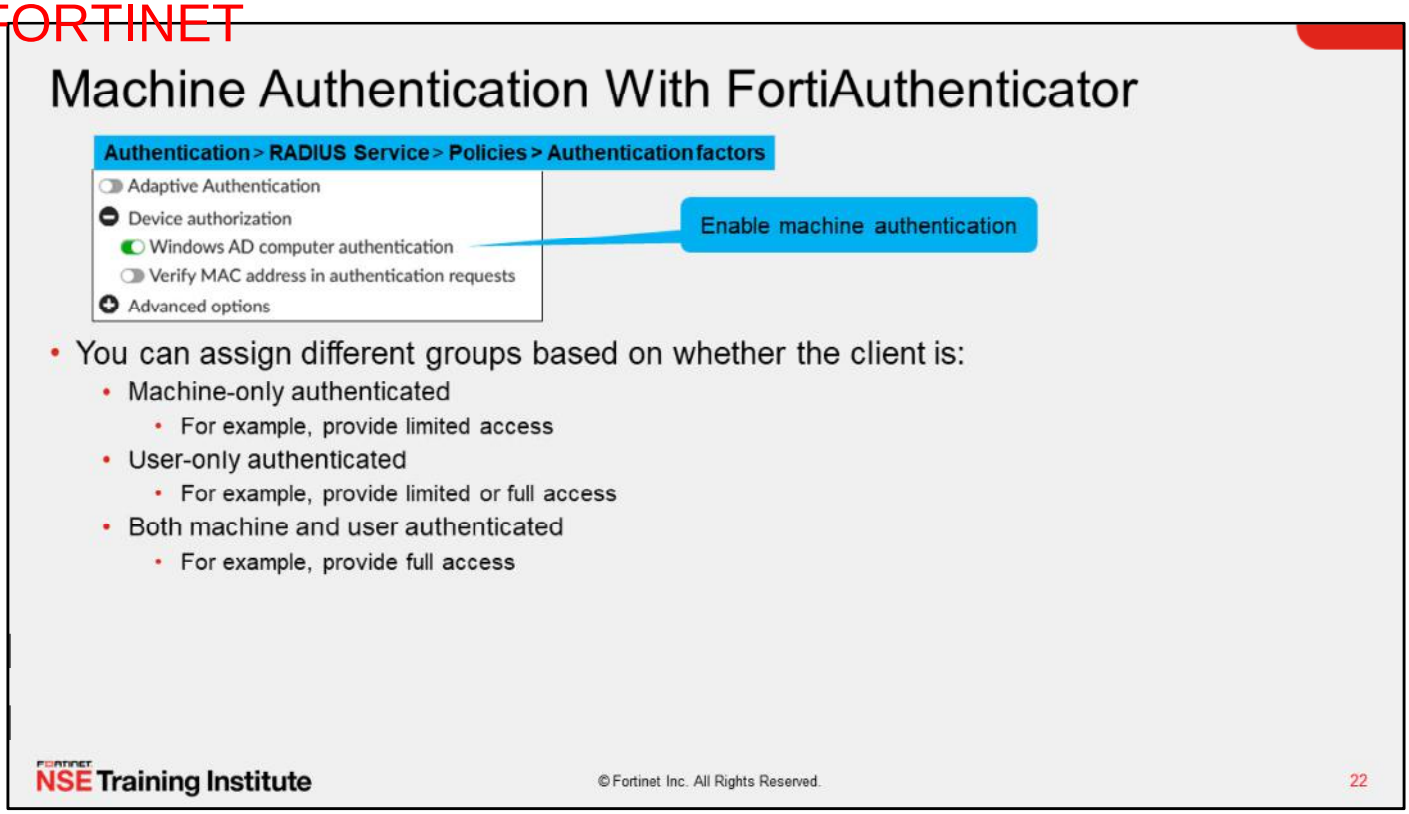
21

Windows environments can combine machine and user authentication. In these cases, you can use FortiAuthenticator to override the user group based on which type of authentication was used by each client.

For example, you can provide limited network access to clients (for example, only Active Directory servers) that have done machine authentication, but have not done user authentication yet. After user authentication is successful, you can then grant further access to the network, based on user credentials. In the meantime, you can block access to users that have done user authentication, but have not done machine authentication (which indicates that they are connecting from unauthorized devices).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

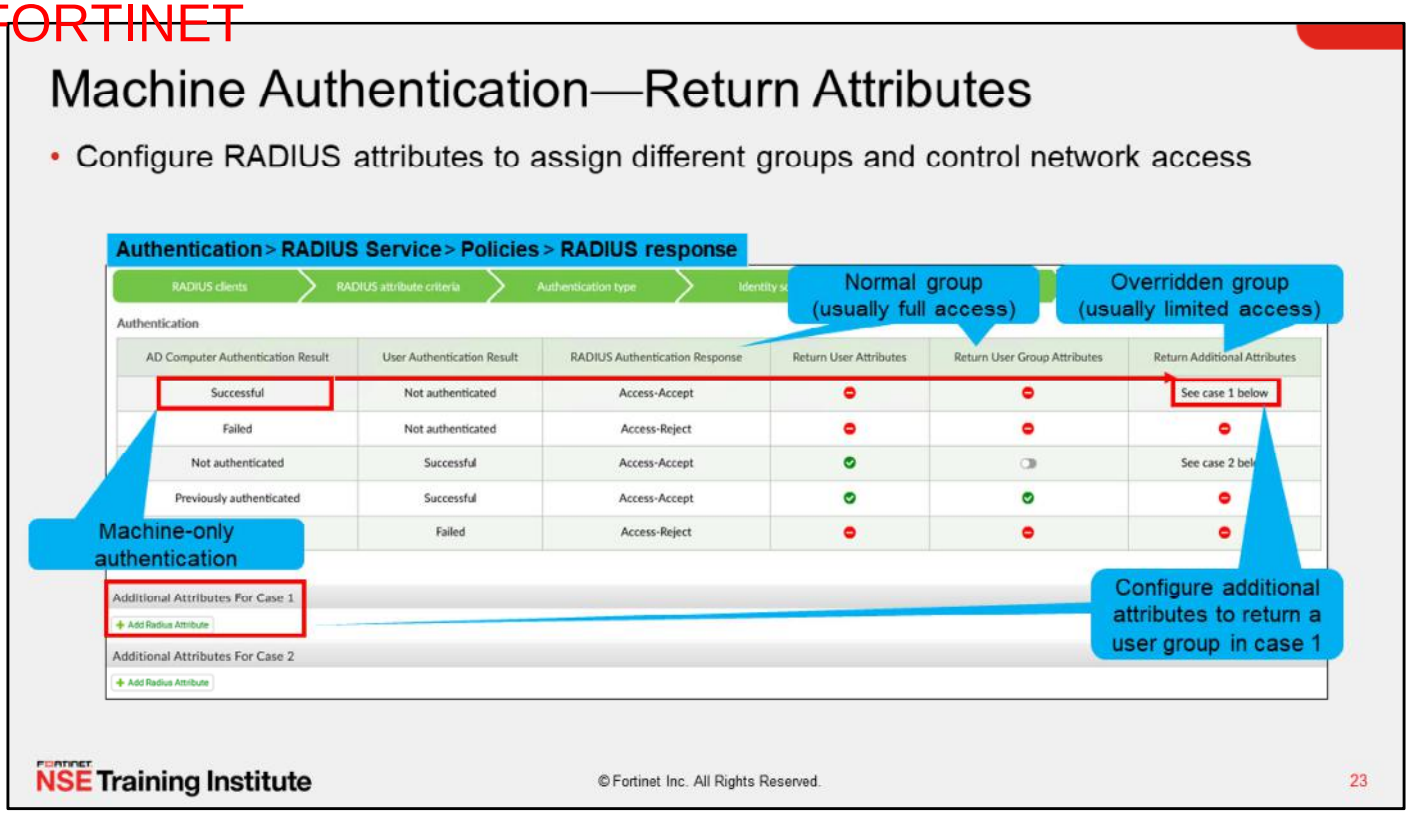


On FortiAuthenticator, you enable machine authentication by enabling **Windows AD computer authentication** in the **Authentication factors** section of the matching RADIUS policy.

After you enable machine authentication, you can override the user group that is returned by FortiAuthenticator for clients that have done either machine-only or user-only authentication. Because the user group that is returned by FortiAuthenticator is commonly used by the authenticator, such as FortiSwitch, to determine the VLAN for the device, this enables you to control the level of network access granted to the device based on the returned user group. Usually, you want to grant full access to devices that have performed both machine authentication and user authentication, and limited access to devices that have done machine authentication only or user authentication only.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

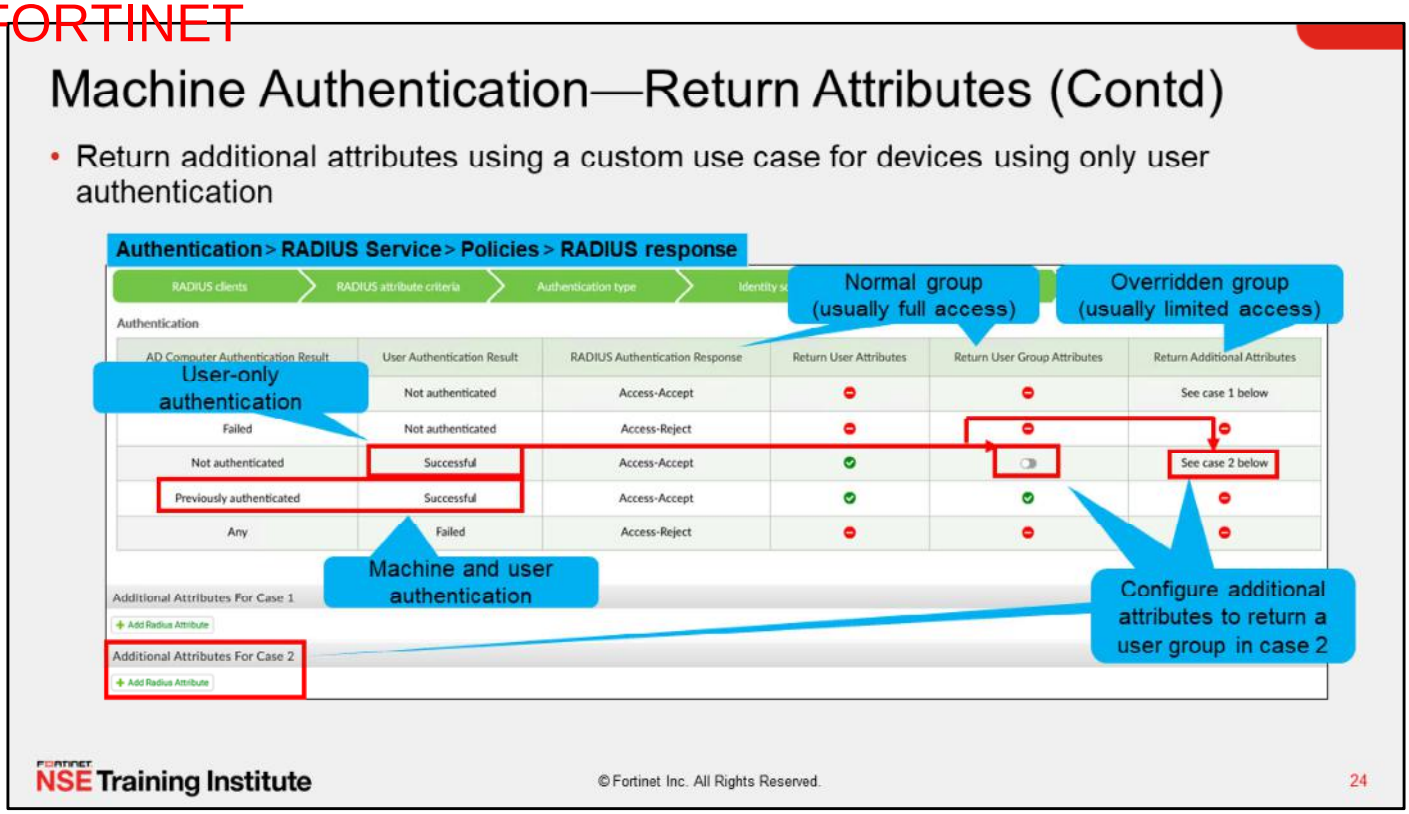


The list of returned attributes, which can include a user group, are configured in the **RADIUS response** section of the matching RADIUS policy. The following are examples of controlling network access on devices based on their authentication status:

- Devices that do both machine authentication and user authentication are assigned their normal user groups, and therefore, granted full network access.
- Devices that do only machine authentication can be assigned a user group that grants limited network access. FortiAuthenticator does not return the configured (or normal) user group as a RADIUS attribute. Instead, it offers you the option to return additional RADIUS attributes, including a different user group, which can have limited access to the network.

Vouchers & Dumps are Available | WhatsApp +201224560923

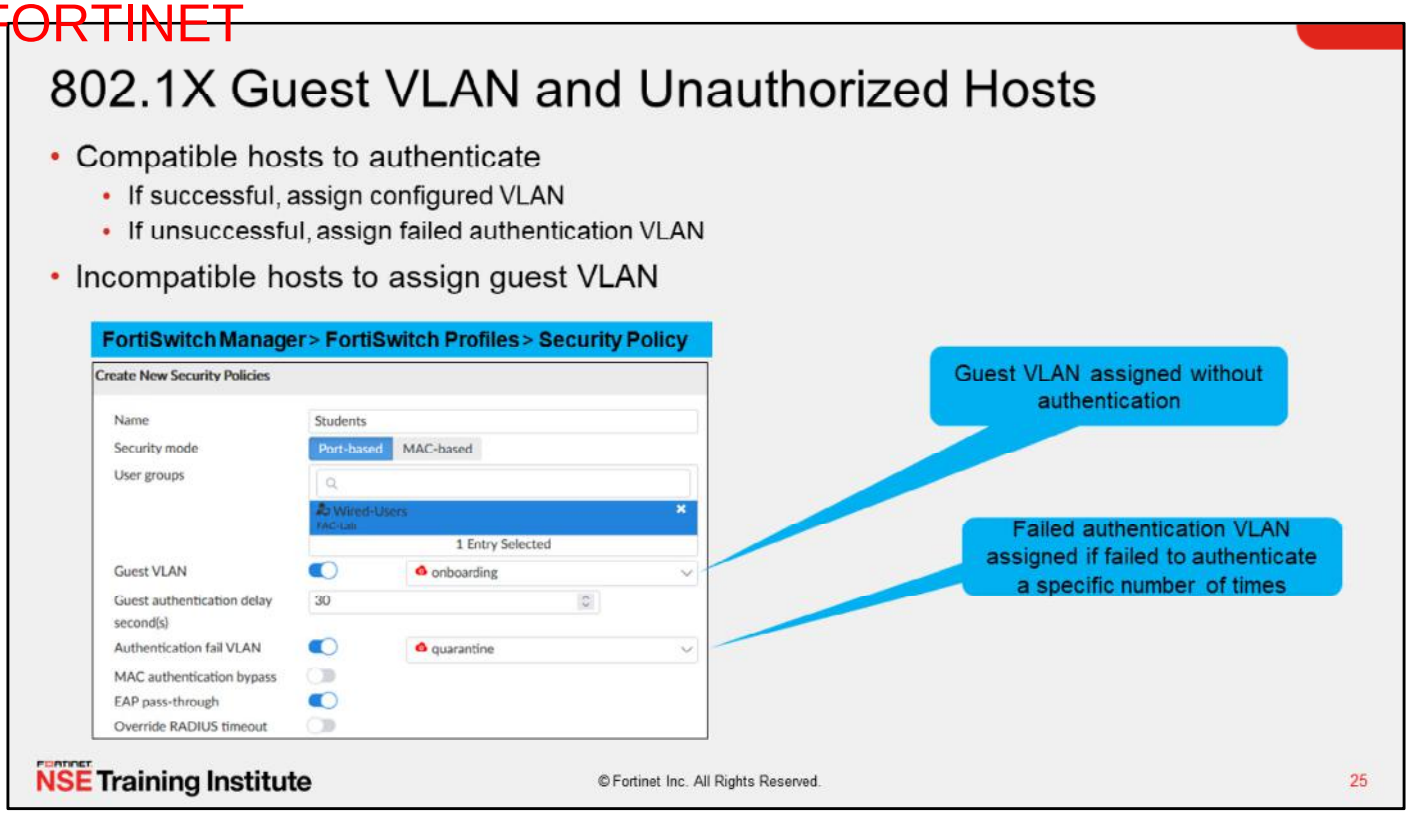
DO NOT REPRINT
© FORTINET
Brave-dumps.com



To limit access for unauthenticated users, you can configure additional attributes to return based on custom use cases. Devices that do only user authentication can be assigned the normal user group, which provides full network access, or with a different user group that grants limited access.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Create a guest VLAN and a failed authorization VLAN to dynamically assign them to hosts when they attempt to access the network.

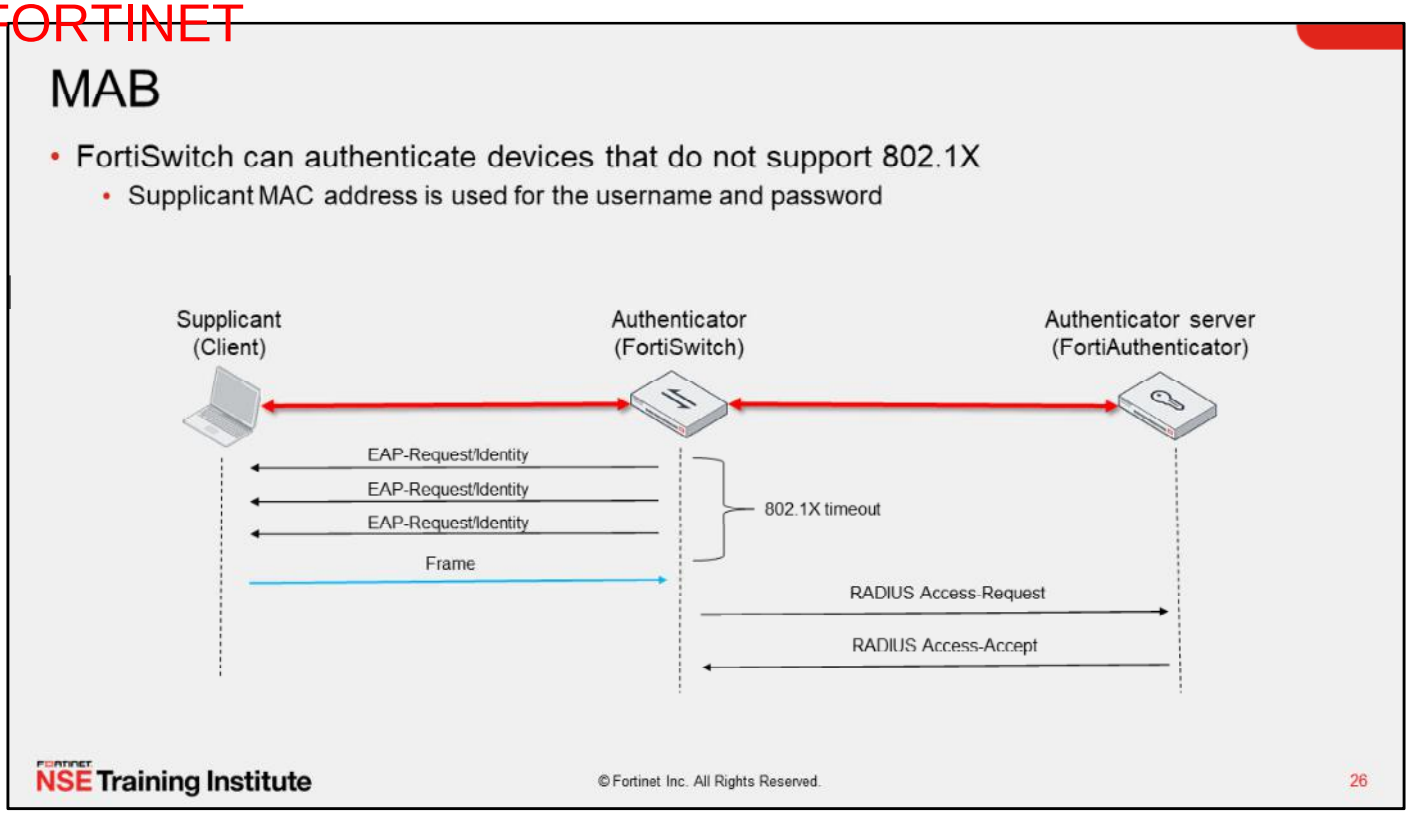
Unauthenticated hosts will be assigned to the **Guest VLAN** after the 802.1X authentication times out.

In addition, hosts that fail to authenticate (for example, compatible host with incorrect credentials), will be assigned to the **Authentication fail VLAN**.

Each VLAN may provide DHCP service to allocate IP addresses to hosts.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

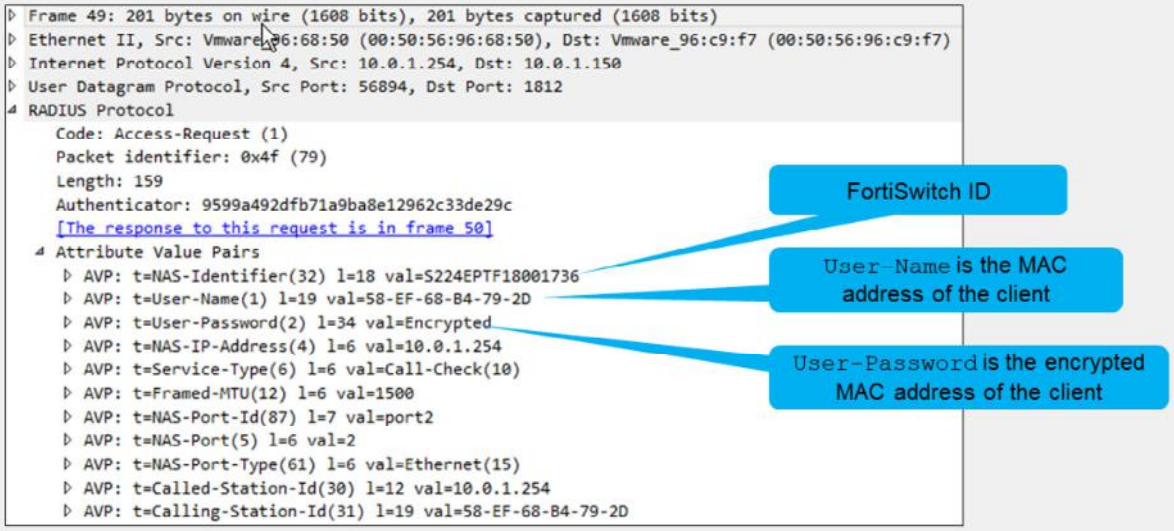


MAC authentication bypass (MAB) allows access to devices that do not support 802.1X authentication. When MAB is enabled in the security policy, and the 802.1X authentication times out, FortiSwitch performs the authentication on behalf of the connected device. For this purpose, FortiSwitch sends a RADIUS Access-Request, using the MAC address of the device as the username, and the encrypted MAC address of the device as the password. FortiAuthenticator can be configured with a list of MAC addresses that are allowed to access the network without 802.1X authentication. If the MAC address of the device is included in this list, the device is authorized.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

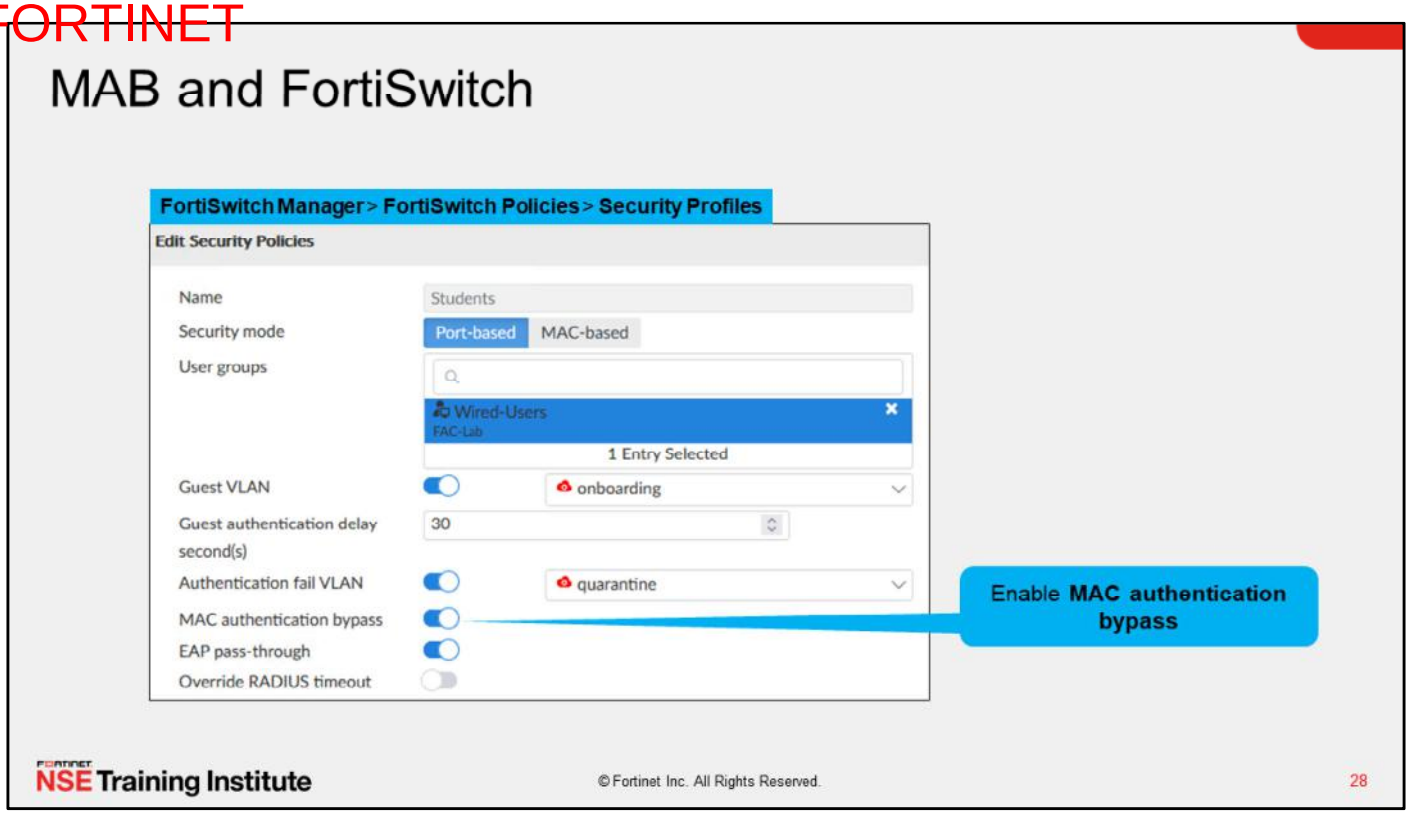
RADIUS Access-Request Sniffer for MAB



This packet capture shows the RADIUS Access-Request when MAB is used. It includes the FortiSwitch ID, client MAC address (as the username), encrypted client MAC address (as the password), and the client MAC address (as the `Calling-Station-ID`).

Vouchers & Dumps are Available | WhatsApp +201224560923

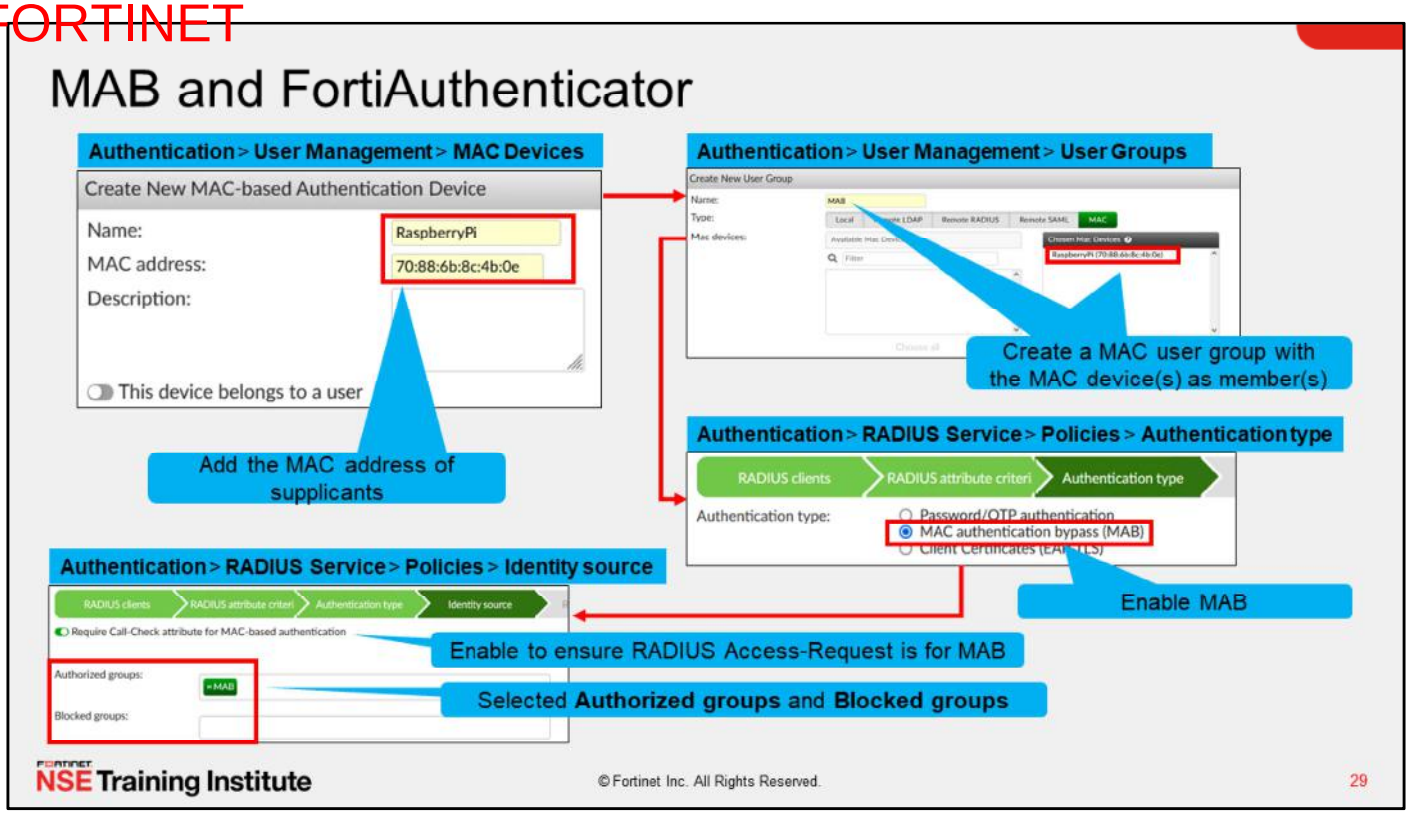
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In FortiSwitch, you enable **MAC authentication bypass** for each security policy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



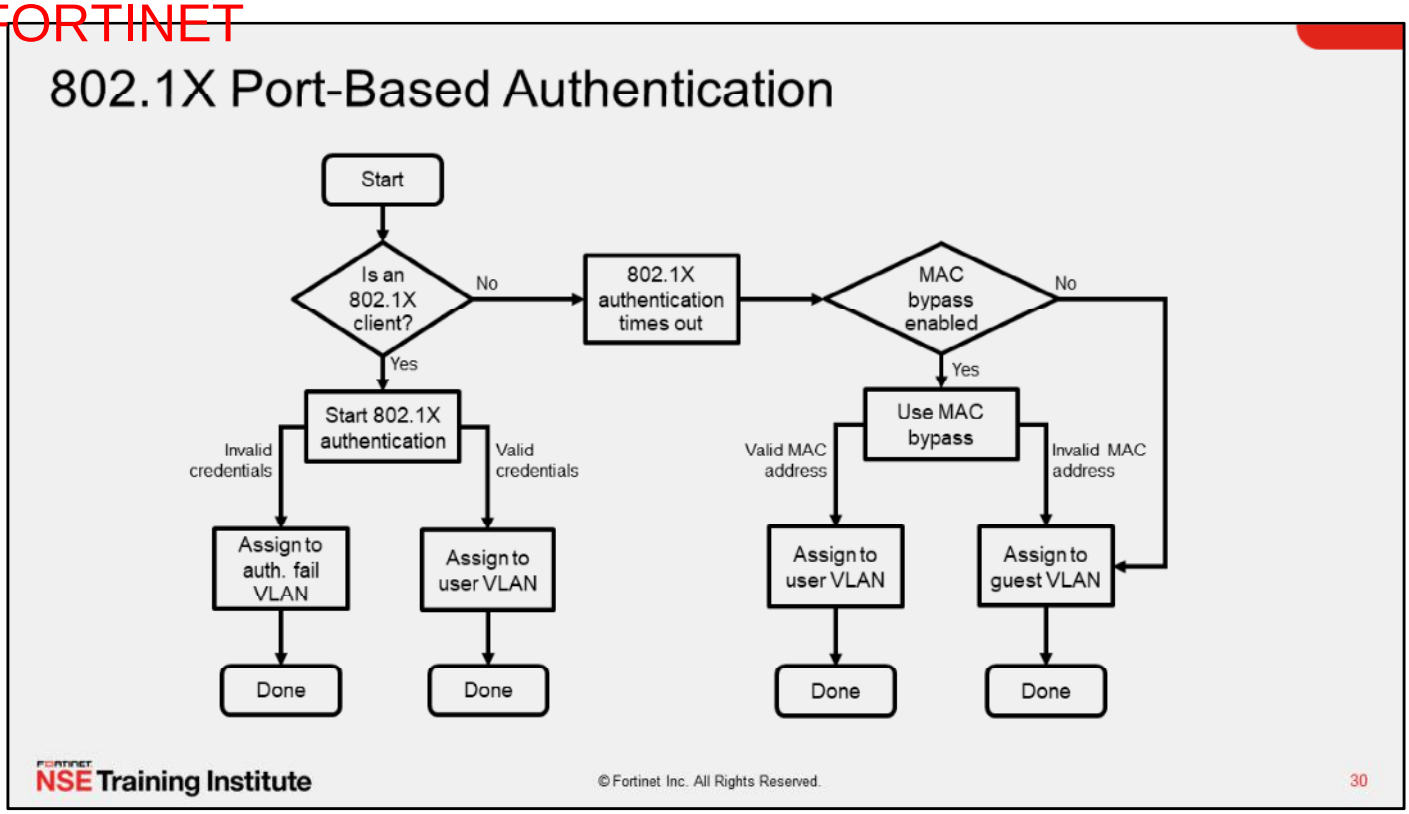
To have FortiAuthenticator work with MAB, you must add the MAC address of every supplicant on the FortiAuthenticator **MAC Devices** page. After that, you must create one or more MAC groups on the **User Groups** page, and then add the MAC devices to their respective MAC groups.

The next step is to enable **MAC authentication bypass (MAB)** in the **Authentication type** section of the matching RADIUS policy. Then, in the **Identity source** section, select the MAB groups that are part of the **Authorized groups** or the **Blocked groups**.

Finally, it is recommended that you enable the **Require Call-Check attribute for MAC-based authentication**. Because MAB uses the device MAC address as the username and password, enabling this option instructs FortiAuthenticator to also check that the RADIUS Access-Request received from the NAS includes the **Service-Type** attribute, and it is set to **Call-Check**. By performing this additional verification, FortiAuthenticator prevents processing non-MAB requests, which may also contain the device MAC address in a RADIUS attribute, as MAB requests. Enabling **Require Call-Check attribute for MAC-based authentication** does not require additional configuration on FortiSwitch. FortiSwitch always includes the **Service-Type** attribute set to **Call-Check** in all its MAB requests.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide shows the authentication process when 802.1X is combined with MAB. When a physical device is connected to an 802.1X port, FortiSwitch waits for the EAPOL-Start packet.

If FortiSwitch receives an EAPOL-Start packet from the connected device, the 802.1X authentication starts. FortiSwitch checks the credentials against a RADIUS server, with the following results:

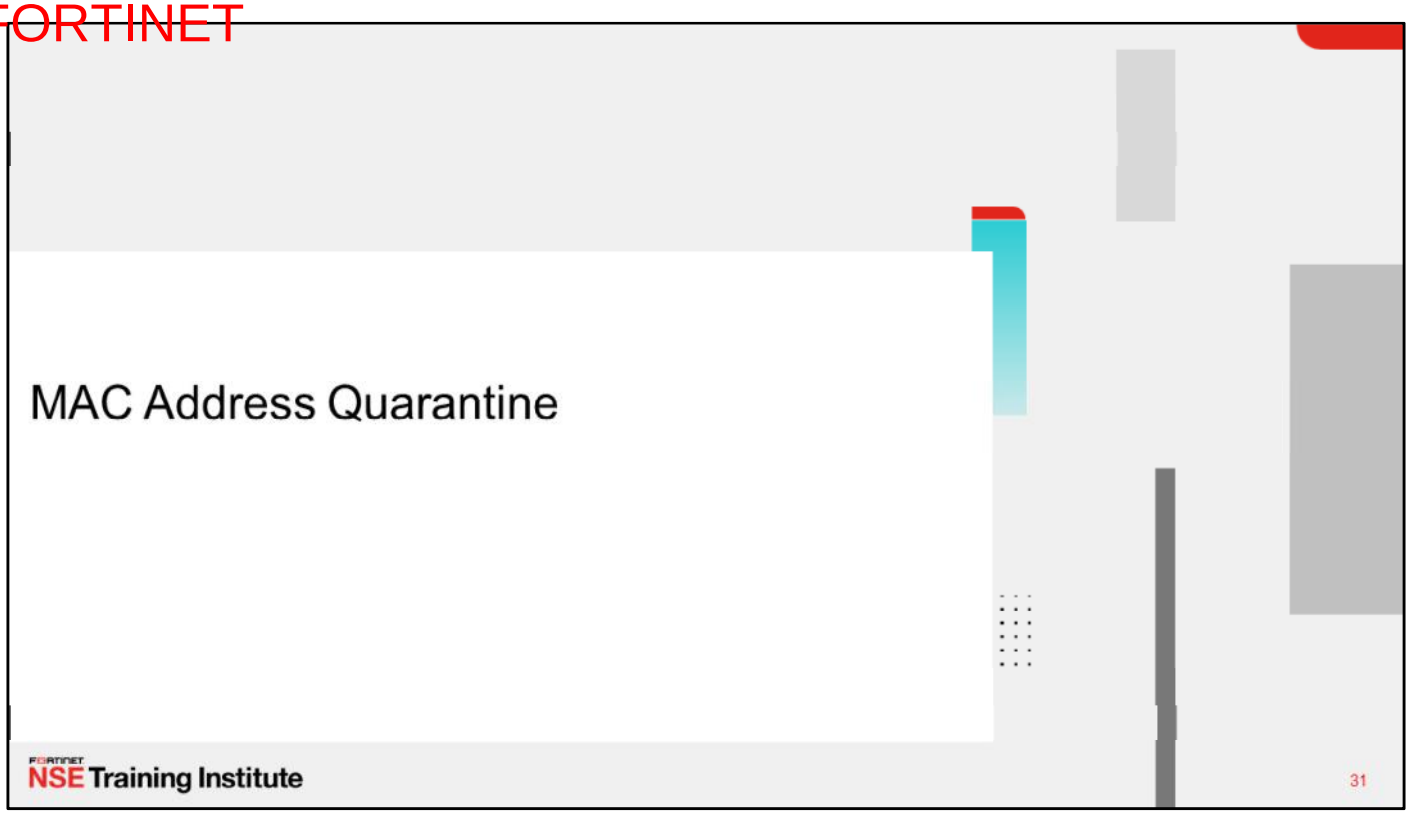
- If the credentials are invalid, and **Authentication fail VLAN** is enabled, traffic from the device is allowed and assigned to the authentication fail VLAN.
- If the credentials are invalid, and **Authentication fail VLAN** is disabled, traffic from the device is blocked.
- If the credentials are valid, traffic from the device is allowed and assigned to the respective user VLAN.

If FortiSwitch does not receive EAPOL-Start packets after a certain amount of time, the 802.1X authentication times out. After that, the source MAC address of the device is checked, with the following results:

- If MAC bypass is disabled, the traffic is assigned to the guest VLAN (or blocked, if **Guest VLAN** is disabled).
- If MAC bypass is enabled, but the source MAC address is not in the MAB table, the traffic is assigned to the guest VLAN (or blocked, if **Guest VLAN** is disabled).
- If MAC bypass is enabled, and the source MAC address is in the MAB table, the traffic is allowed and assigned to the respective user VLAN.

Vouchers & Dumps are Available | WhatsApp +201224560923

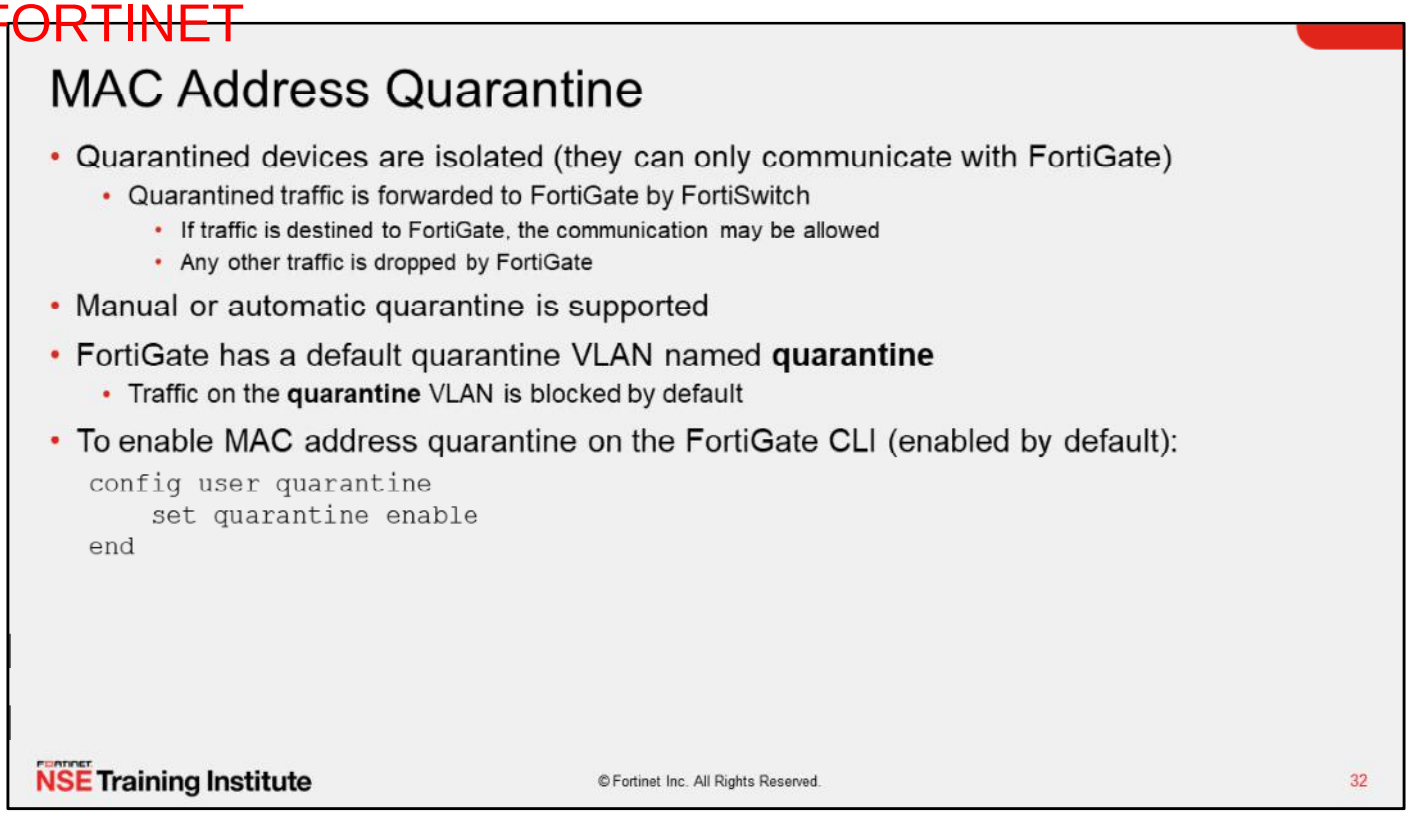
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn how to quarantine MAC addresses with FortiGate and FortiSwitch.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



To quarantine a MAC address, FortiSwitch and FortiGate work together to isolate a device. Isolation means that a quarantined device can communicate only with FortiGate. If the device tries to communicate with any other host on the network, the communication is blocked. To isolate a quarantined device, FortiSwitch forwards all its traffic to FortiGate. The traffic can be any of the following destinations:

- FortiGate local: The destination is a FortiGate interface.
- Intra-VLAN: The destination is a device in the same VLAN.
- Inter-VLAN: The destination is a device in a different VLAN or network that is reached through FortiGate.

For the FortiGate local traffic, the communication is allowed if FortiGate is configured to allow the connection. For example, a quarantined device can ping a FortiGate interface if ping access is enabled on that interface. For other traffic, the communication is blocked by FortiGate.

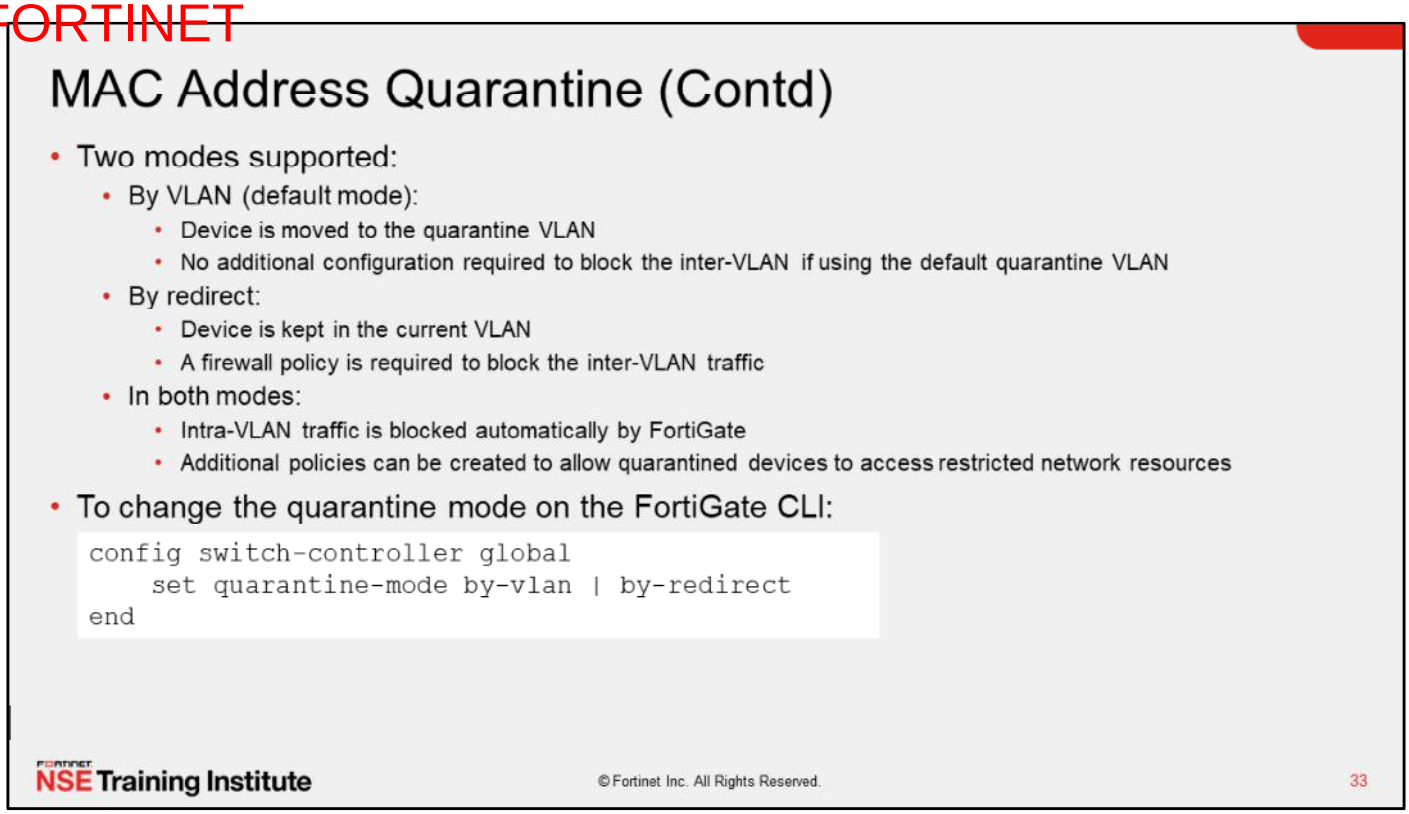
You can quarantine devices by MAC address, either manually or automatically. MAC address quarantine works as follows:

1. FortiGate monitors the device activity based on the traffic and security logs generated for the device.
2. If FortiGate determines that the device must be quarantined, either because an automated rule has been triggered, or because of user intervention, FortiGate adds the device MAC address to its local quarantine list.
3. FortiGate applies the quarantine-related configuration for the quarantined device to FortiSwitch using the FortiSwitch REST API.
4. The pushed configuration instructs FortiSwitch to block the traffic from the quarantined MAC address.

To enable MAC address quarantine on the FortiGate CLI, run the commands shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



FortiGate supports two MAC address quarantine modes: by VLAN and by redirect. In both modes, FortiGate blocks the traffic from the quarantined MAC address provided the correct configuration is in place.

In by VLAN mode, FortiGate moves the quarantined MAC address to the **quarantine** VLAN. If you are using the default **quarantine** VLAN as your quarantine VLAN, the inter-VLAN traffic from the device is automatically blocked because the **quarantine** VLAN does not have any firewall policies configured. Note that the device can still get an IP address through DHCP because the **quarantine** VLAN has the DHCP server enabled by default. However, this would require the device to restart its DHCP client, which typically requires user intervention. This could make it difficult for an administrator to perform remediation on the device.

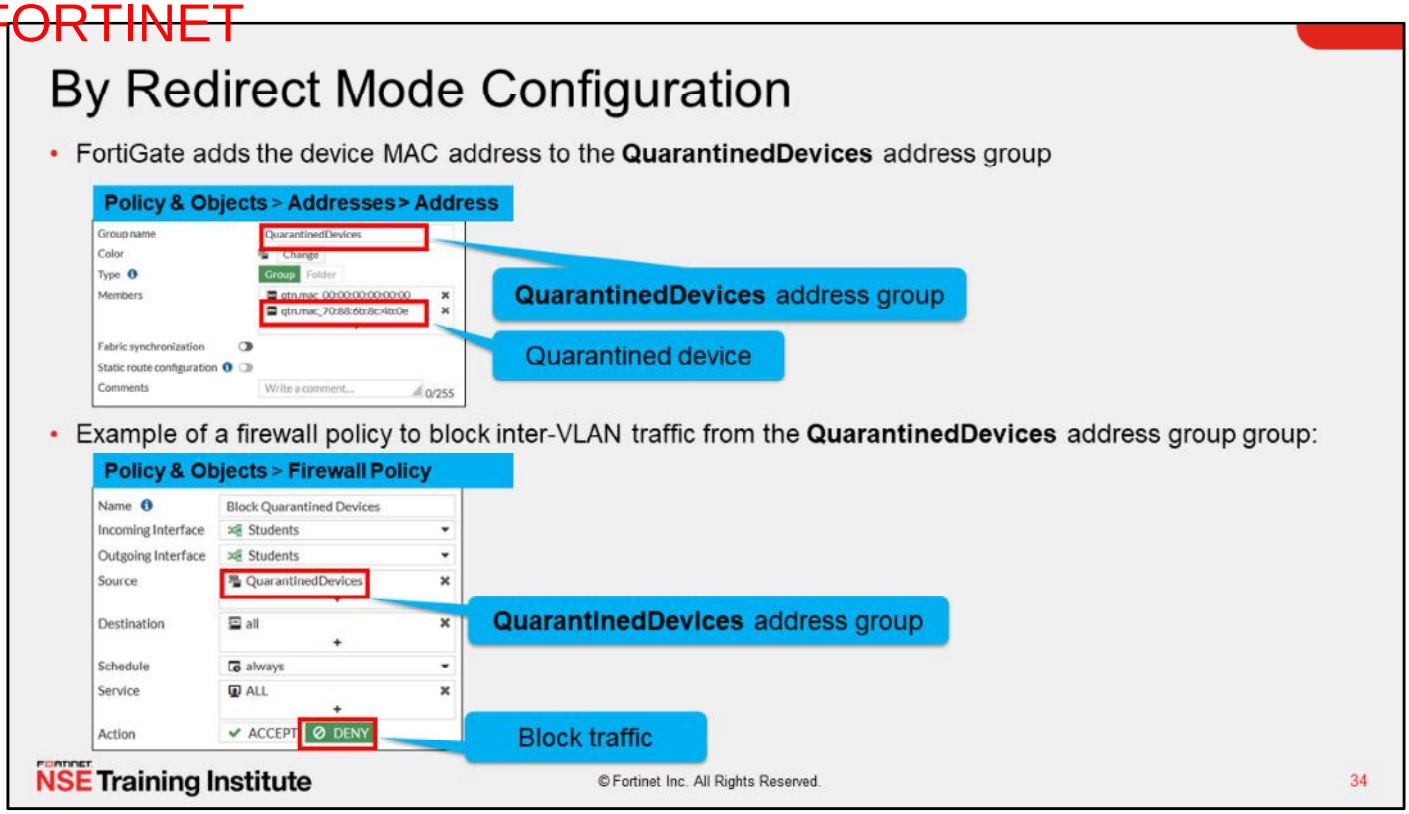
In by redirect mode, FortiGate keeps the device in its current VLAN, and adds the device MAC address to the **QuarantinedDevices** firewall address group. The device IP address does not change, which is useful for performing remediation. However, to block the inter-VLAN traffic, you must configure a firewall policy to explicitly block the traffic from the **QuarantinedDevices** address group.

In both modes, the intra-VLAN traffic is dropped automatically by FortiGate because the destination MAC address of the traffic does not match the FortiGate interface. The destination MAC address of the traffic is the MAC address of the target device located in the same VLAN. In addition, communication between the quarantined devices and FortiGate is allowed. You can also configure additional firewall policies to explicitly allow quarantined devices to access limited network resources, such as servers with Windows updates and other security-related software updates, which are required for remediation.

To change the MAC address quarantine mode on the FortiGate CLI, run the commands shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

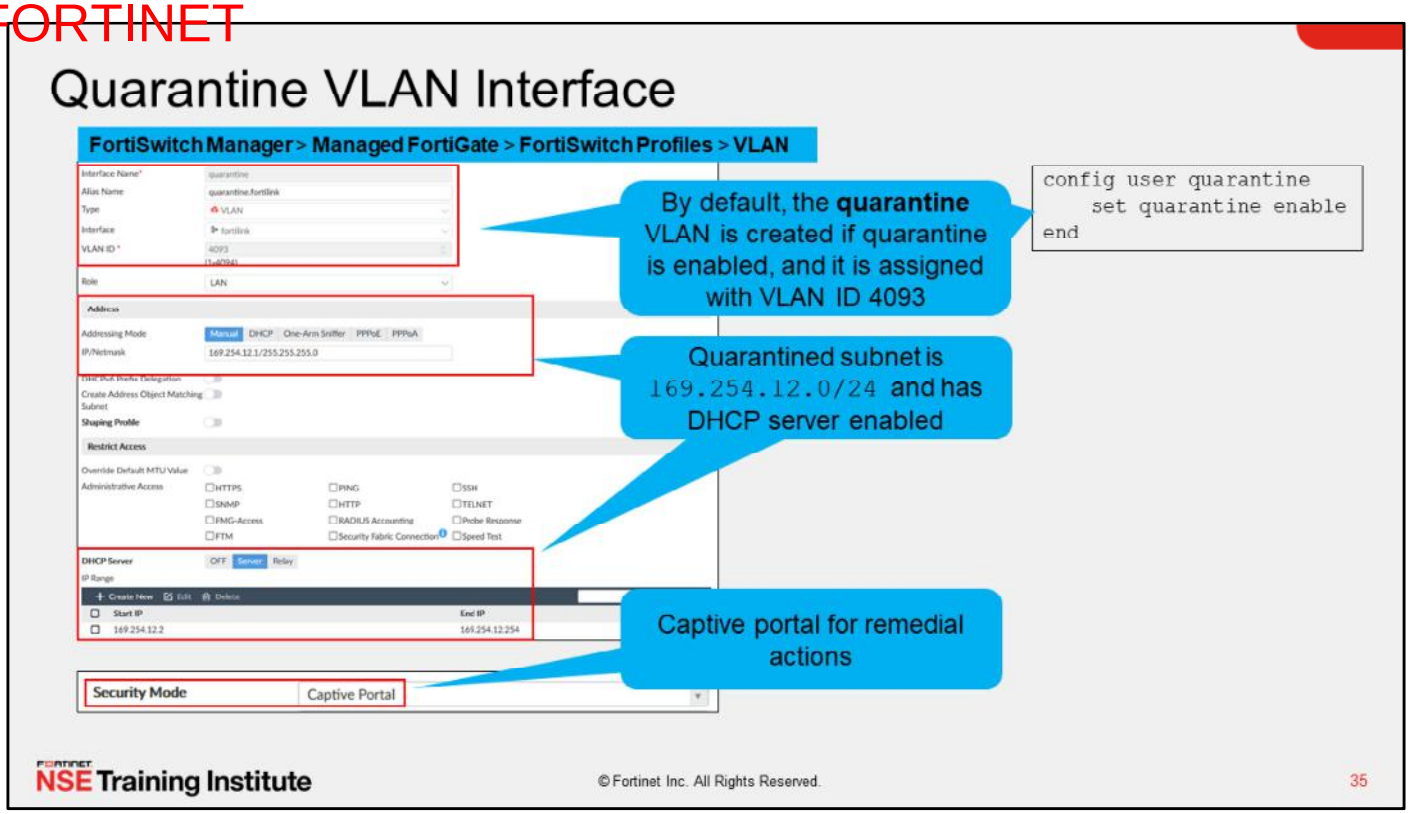


In by redirect mode, FortiGate quarantines a device by creating a firewall address object that contains the quarantined device MAC address. FortiGate then adds the firewall address object to the **QuarantinedDevices** address group.

However, FortiGate *does not* add a firewall policy to block the inter-VLAN traffic from the **QuarantinedDevices** address group. For this reason, the administrator must manually create a firewall policy like the one shown on this slide. Like with any firewall policy, the administrator must also make sure that the policy is placed in the correct position in the firewall policy list, so that the quarantined traffic matches the block policy instead of the regular firewall policies that are used for production traffic.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



If you are using by VLAN mode, then you might want use the default **quarantine** VLAN as your quarantine VLAN. The **quarantine** VLAN gets created when the first switch is discovered by FortiGate, provided the quarantine feature is enabled under `config user quarantine`.

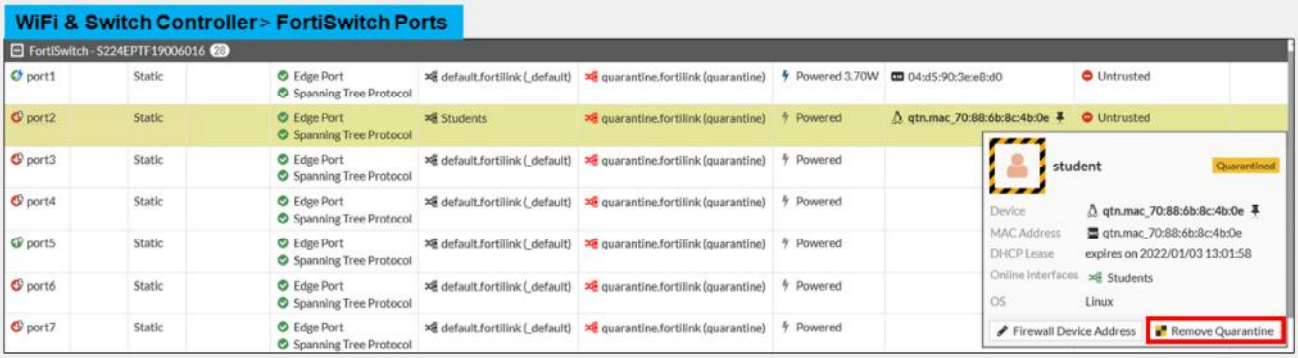
The **quarantine** VLAN is assigned with VLAN ID 4093, and configured with the subnet `169.254.12.0/24` by default. In addition, the interface has **DHCP Server** enabled to assign IP addresses to quarantined devices. By default, this VLAN is part of the allowed VLANs on a managed FortiSwitch, which is needed for the quarantine feature to work. Moreover, to isolate quarantined devices from each other, access VLAN is enabled on the **quarantine** VLAN by default. The access VLAN option is only visible on the FortiGate GUI, and not on the FortiManager GUI.

In addition, the **quarantine** VLAN has captive portal enabled for device remediation. Part of the role of quarantining devices is to challenge connectivity with the captive portal, which can be configured to present custom messaging to the organization.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Quarantine a MAC Address Manually

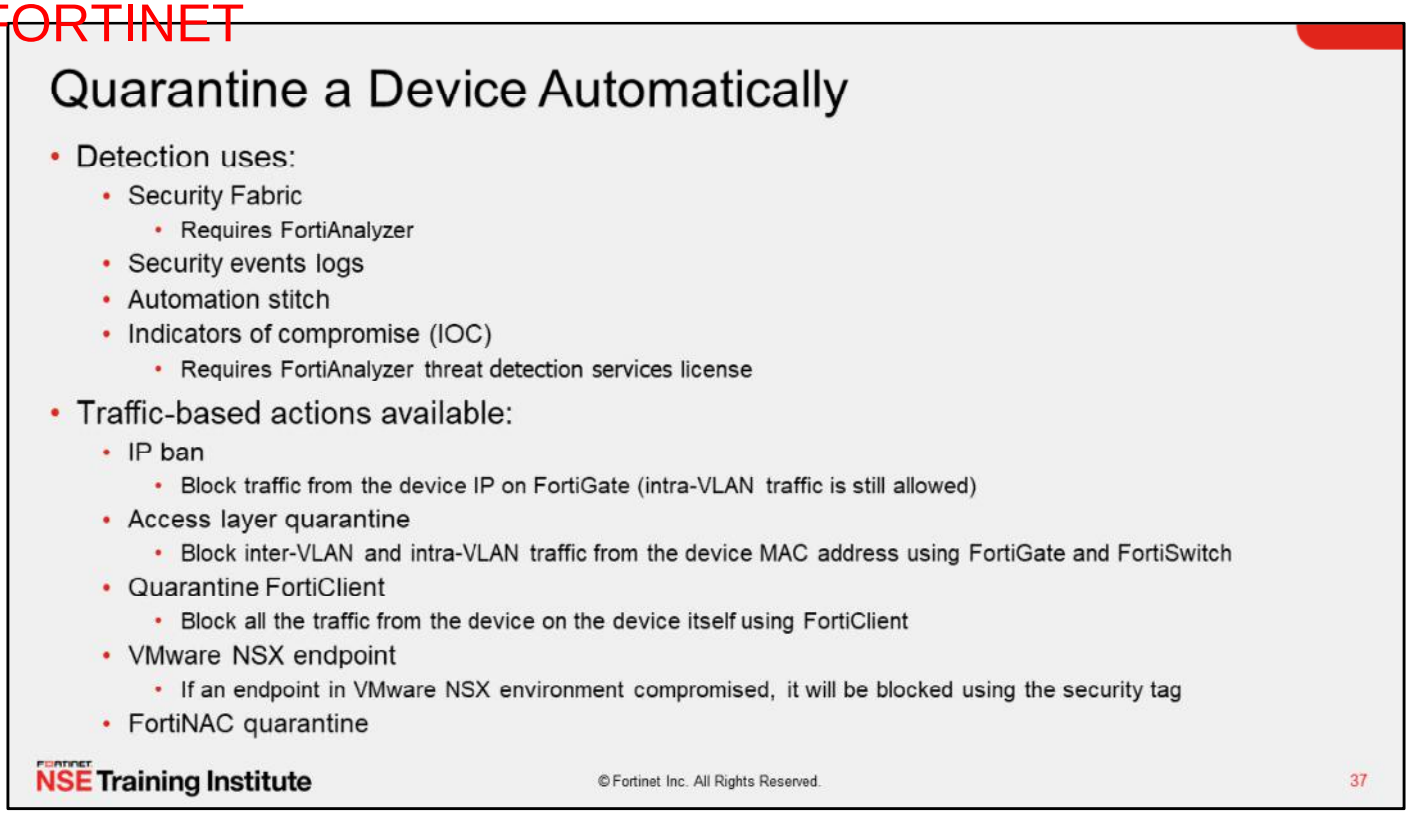


NSE Training Institute
© Fortinet Inc. All Rights Reserved.
36

To manually quarantine a MAC address on the FortiGate GUI, browse to **FortiSwitch Ports** on the **WiFi & Switch Controller** page, click the device listed in the **Device Information** column, and then select **Quarantine Host**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



When FortiGate is a member of a Security Fabric group, the Security Fabric can quarantine devices automatically using automation stitches.

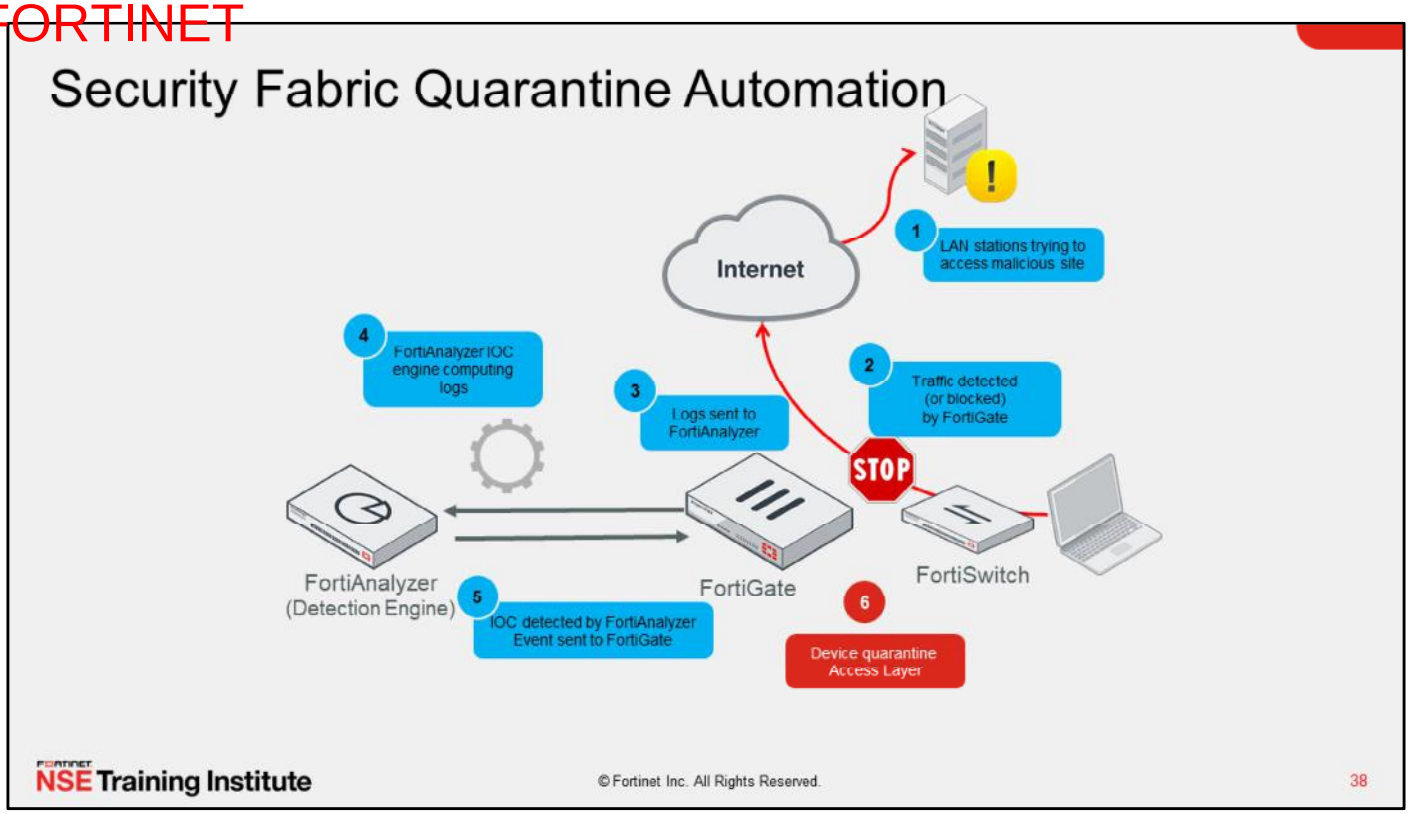
In addition to requiring a FortiAnalyzer device to configure the Security Fabric, you also need a valid threat detection services license on FortiAnalyzer. The license enables FortiAnalyzer to use IOCs to detect compromised devices on the network. IOCs are events or characteristics collected about a device that indicate, with high confidence, that the device has been compromised.

After FortiAnalyzer determines that the device has been compromised, you can configure the Security Fabric to perform the following actions:

- IP ban: Traffic from the compromised device IP is blocked on FortiGate, but intra-VLAN traffic is still allowed.
- Access layer quarantine: Inter-VLAN and intra-VLAN traffic from the compromised device MAC address is blocked using FortiGate and FortiSwitch.
- Quarantine FortiClient: All traffic from the compromised device is blocked on the device itself provided the device has FortiClient installed.
- VMware NSX security tag: An endpoint in VMware NSX environment that is compromised to be blocked based on the security tag.
- FortiNAC quarantine: The PC is quarantined and its MAC address is disabled in the configured FortiNAC.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

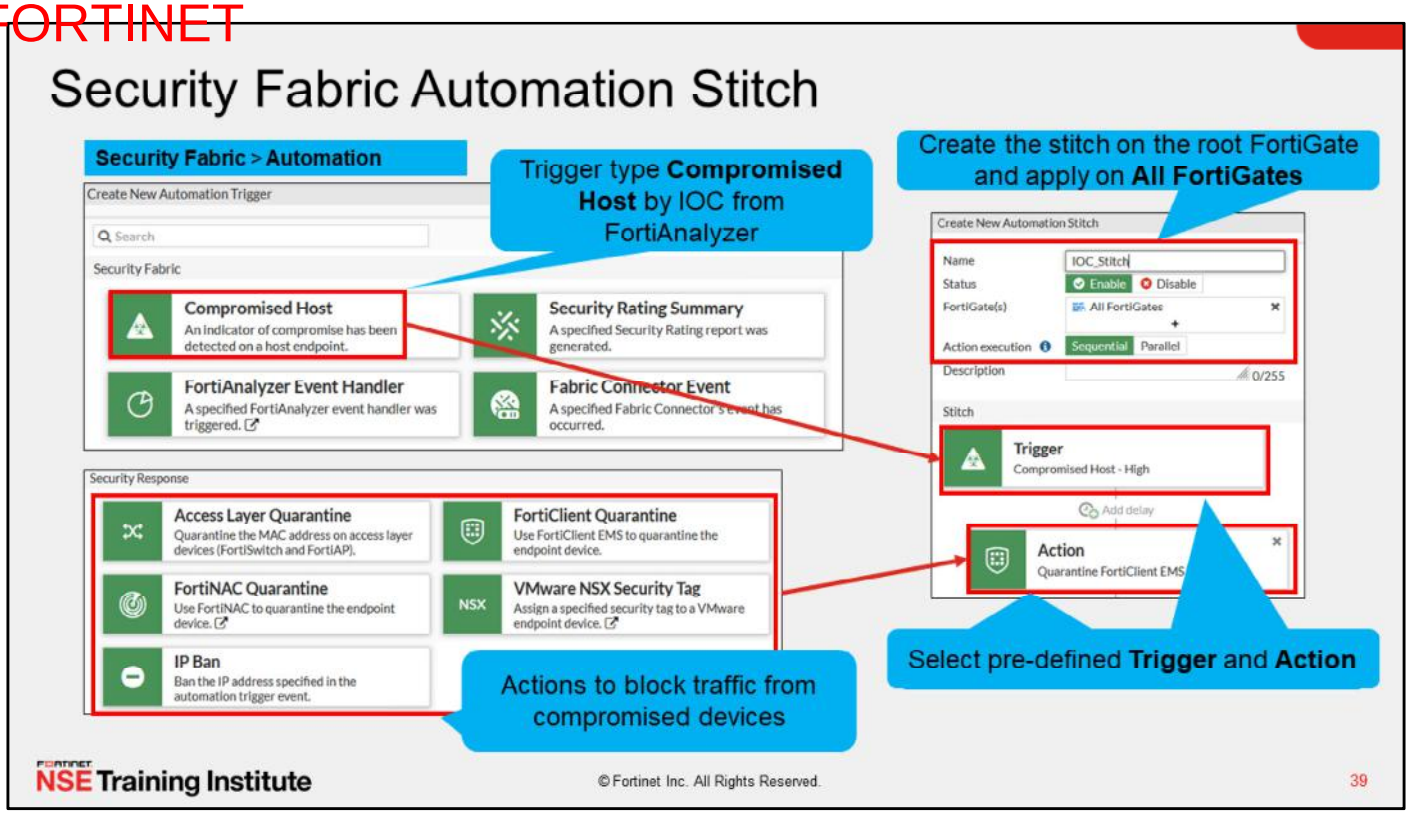


Known and unknown threat information is easily and efficiently shared among all elements and locations within the Security Fabric. User-defined automation on FortiGate to quarantine compromised devices can be strengthened with IOC services on FortiAnalyzer. This slide shows how compromised devices are quarantined automatically, using IOC and the Security Fabric:

1. A device attempts to access content that is a security risk, such as malicious websites.
2. FortiGate blocks access to the site based on the firewall policy defined with the web filter profile.
3. FortiGate sends a log record to FortiAnalyzer regarding the violation committed.
4. FortiAnalyzer processes the logs using IOC services.
5. FortiAnalyzer makes a security risk verdict and sends it back to FortiGate.
6. User-defined automation takes action to quarantine the compromised device and place it in isolation.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



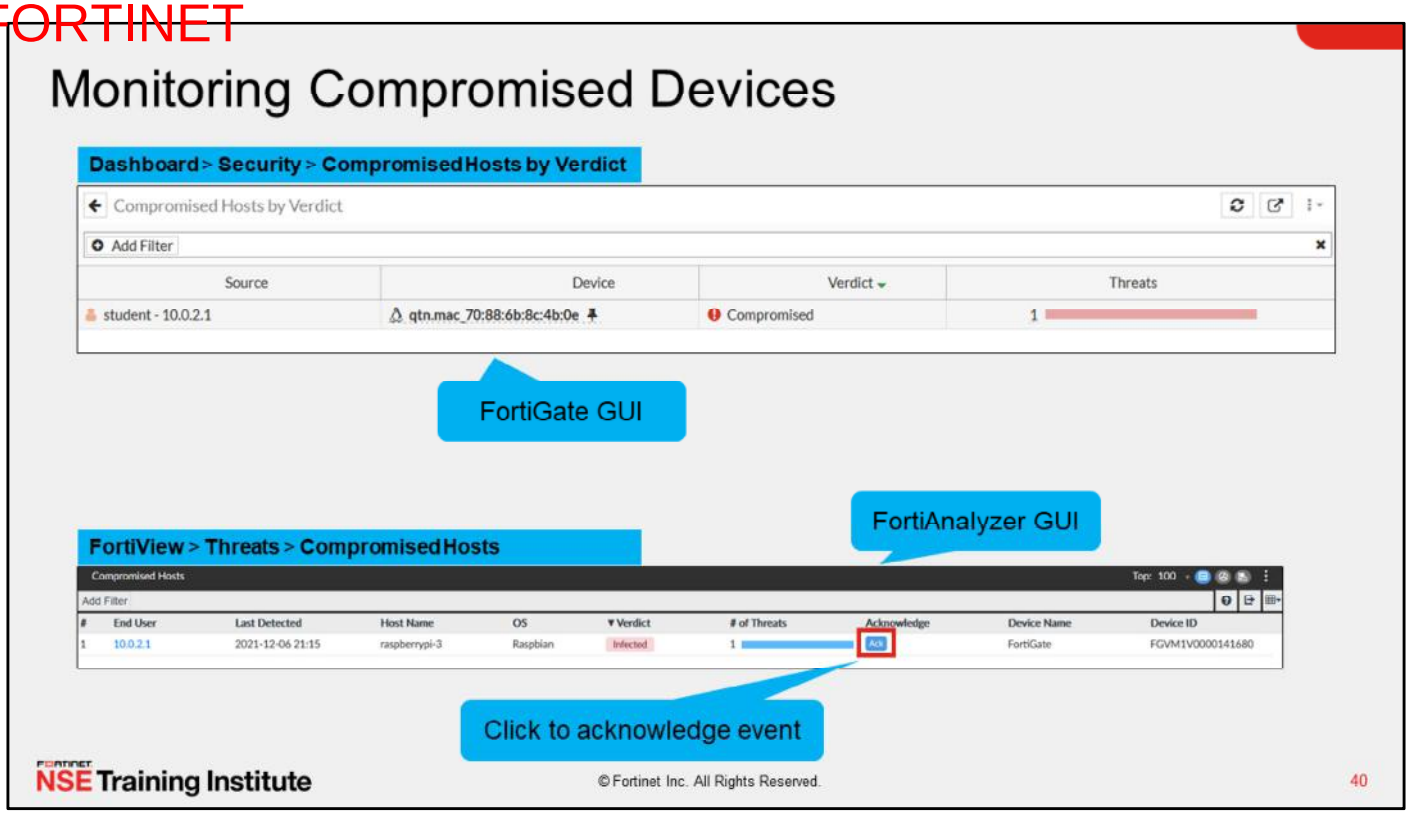
Compromised devices are identified by FortiAnalyzer using threat detection services. IOC verdicts are sent to the root FortiGate of the Security Fabric group, in case there is an automation stitch configured for compromised devices.

You can create the automation stitch only on the root FortiGate, and then select which of the FortiGate devices in the Security Fabric the stitch will be applied to when triggered.

After the stitch is triggered, there are many actions available. From the actions shown on the slide, the following can block the traffic from the device: **Access Layer Quarantine**, **FortiNAC Quarantine**, **IP Ban**, **FortiClient Quarantine**, and **VMware NSX Security Tag**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

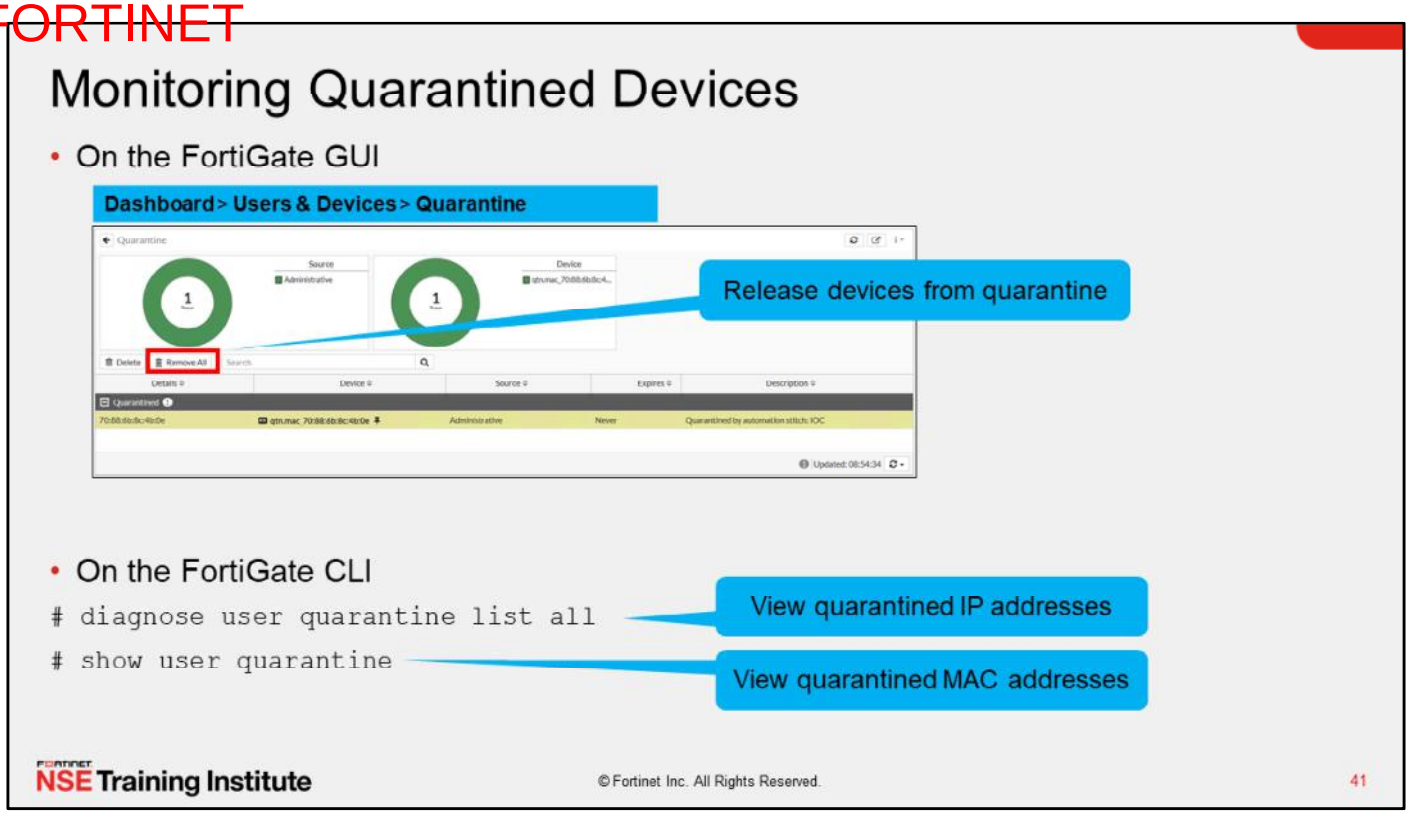


On the FortiGate GUI, you can view the compromised devices by IOC verdict by accessing the **Compromised Hosts by Verdict** widget available on the dashboard.

You can also display the compromised devices on the FortiAnalyzer GUI by accessing the **Compromised Hosts** section on the **FortiView** pane. On this page, you can click **Ack** to acknowledge the event. After you acknowledge an event, the event is removed from both the **Compromised Hosts** page on FortiAnalyzer, and the **Compromised Hosts by Verdict** widget on FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

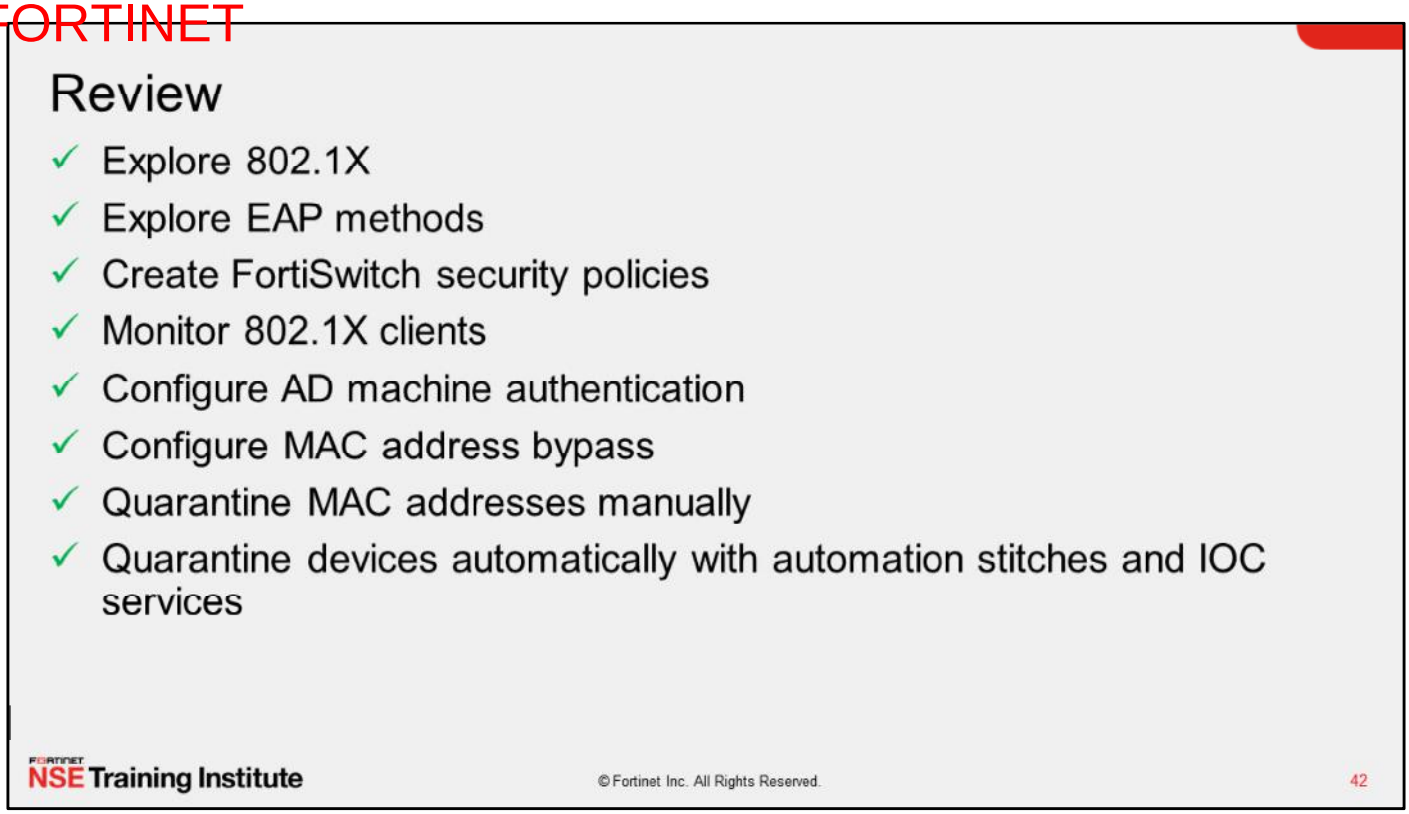
DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can view the list of quarantined devices on the FortiGate GUI by accessing the **Quarantine** widget available on the dashboard. Alternatively, you can display them on the FortiGate CLI by running the commands shown on the slide. Note that the list of quarantined IP addresses (IP ban action) and the list of quarantined MAC addresses (access layer quarantine action) are obtained using different CLI commands.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

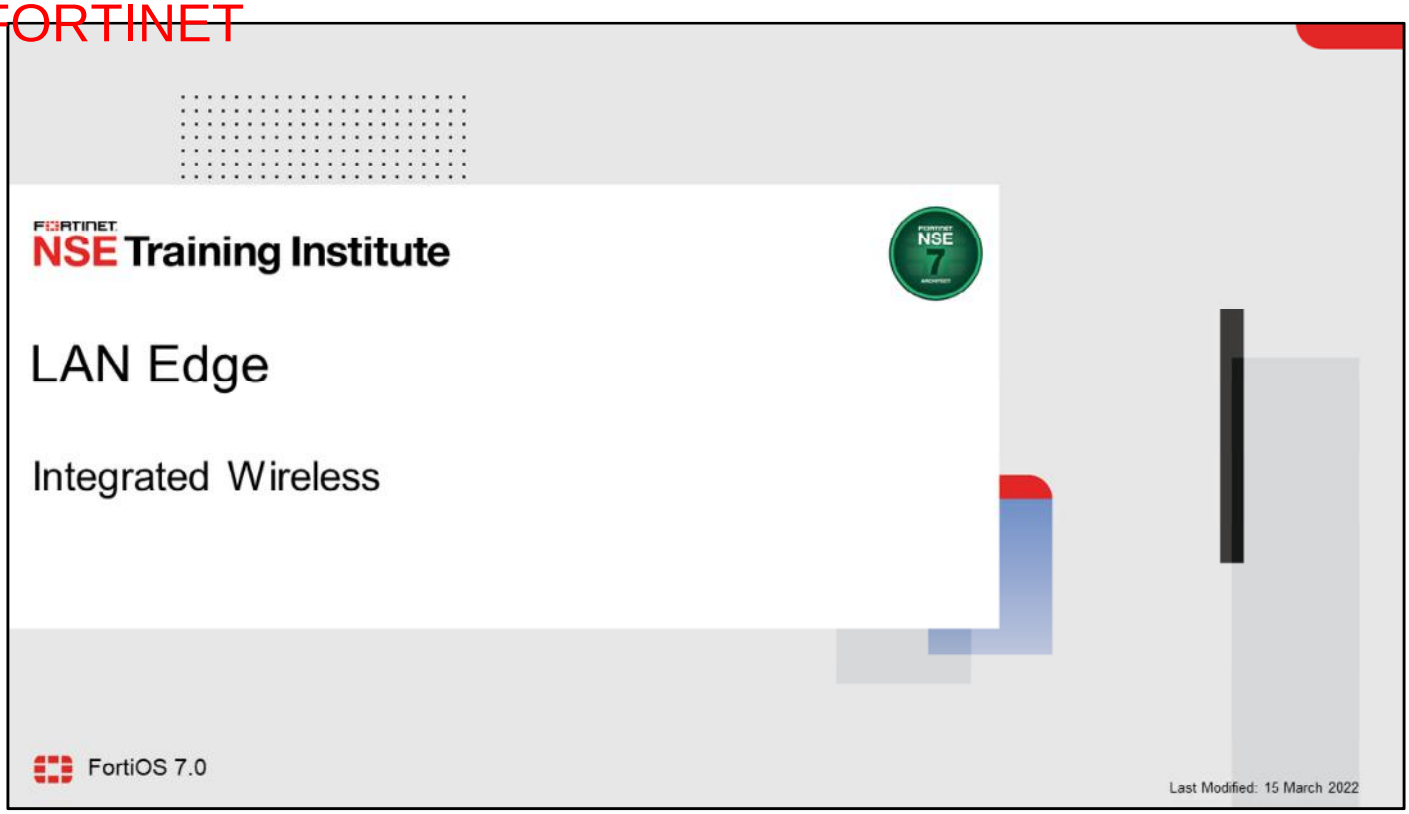


This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to configure port authentication on FortiSwitch and FortiAuthenticator.

Vouchers & Dumps are Available | WhatsApp +201224560923

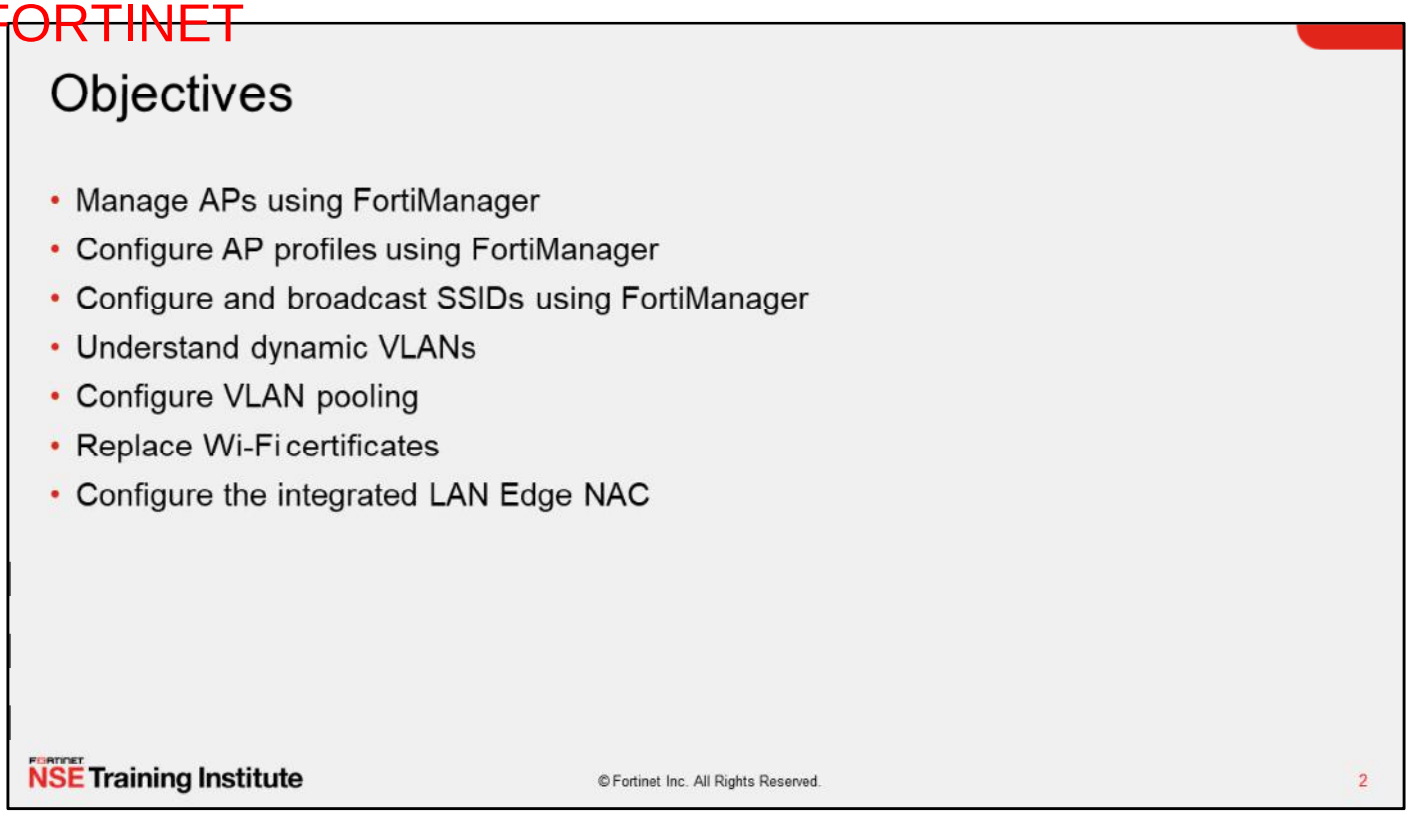
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn how to configure and use integrated wireless features on FortiOS using FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

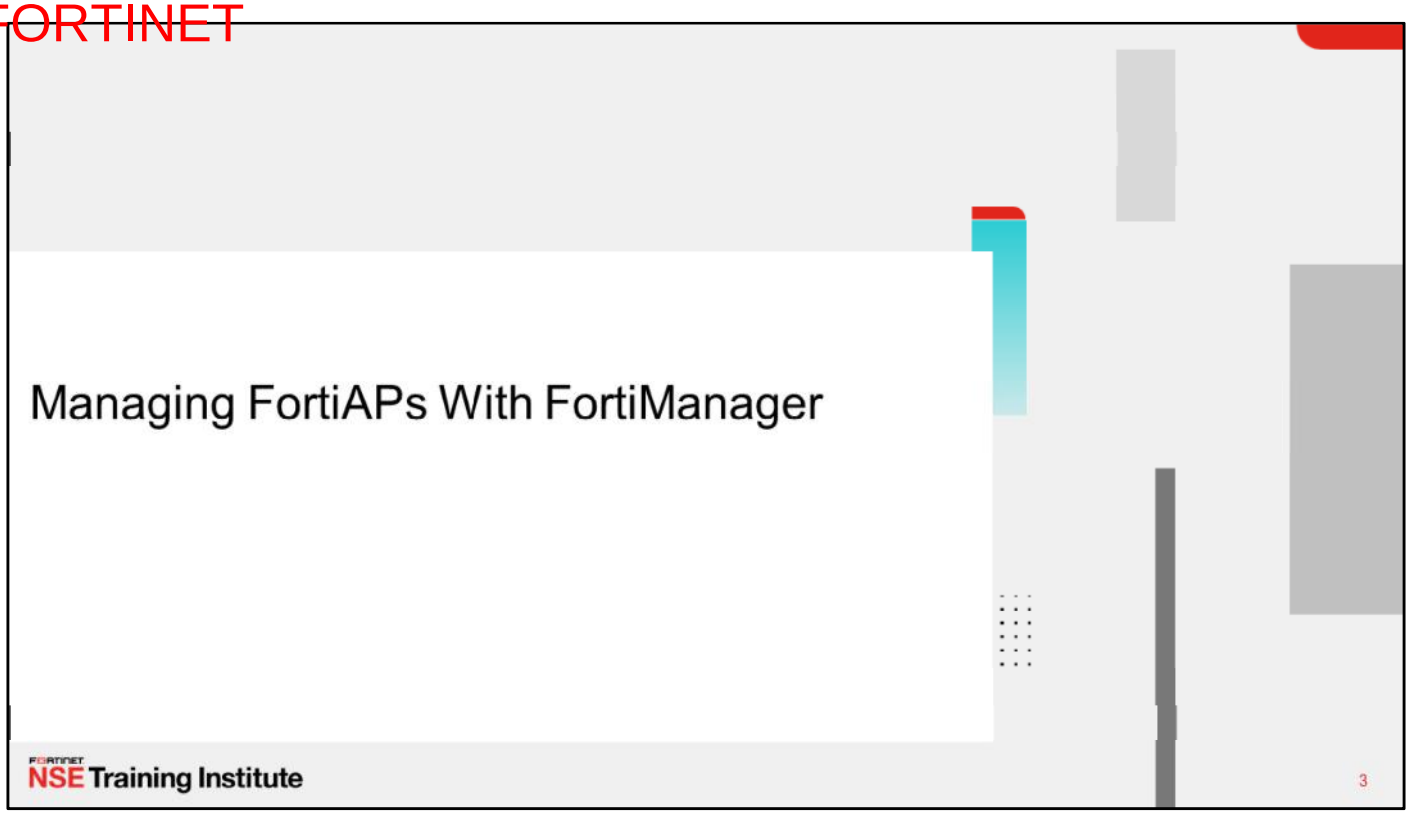
DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this lesson, you should be able to achieve the objectives shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

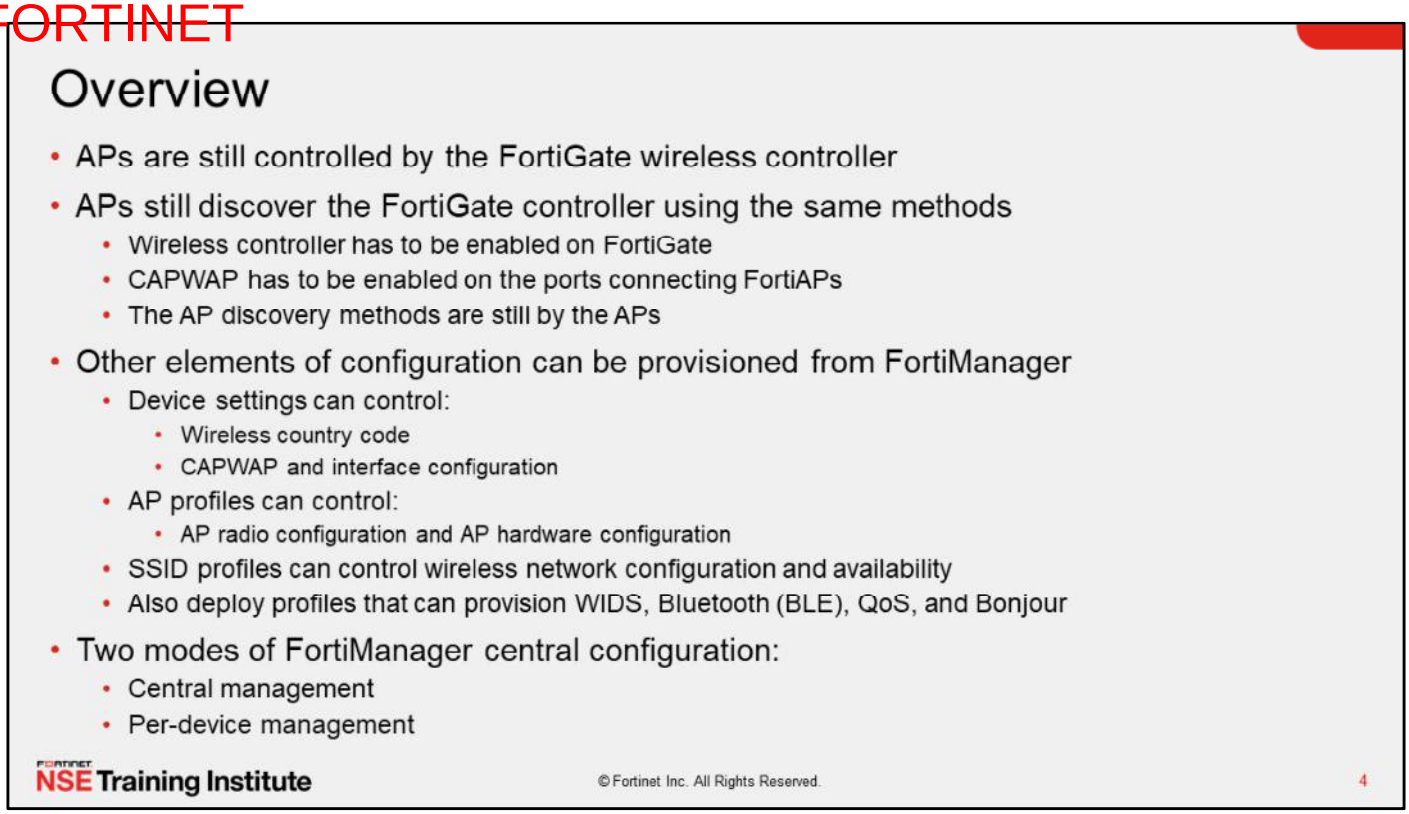
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn how to provision and update FortiAPs centrally using FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can provision many aspects of wireless configuration on FortiGate using FortiManager. It is important to note that it is still FortiGate that supports the AP wireless network. All the required configuration for AP discovery and CAPWAP configuration must be in place.

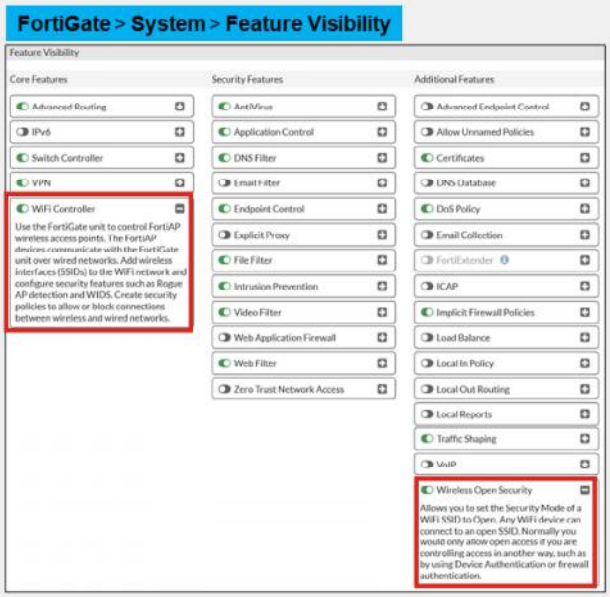
FortiManager can provision the majority of settings required to publish a wireless network and configure the APs. FortiManager uses profiles to control AP configuration, SSID configuration, and other profiles to control other wireless-related functions. These profiles are stored on FortiManager and can be applied to multiple FortiGate wireless controllers and APs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Enabling and Configuring the Wireless Controller

- On some FortiGate devices, the wireless controller functionality is disabled by default
- If the Wi-Fi and switch controller options are not available on the GUI, they can be enabled on FortiGate or using FortiManager
  - Configure individual controllers centrally using a **CLI Configuration** on FortiManager
  - Or enable at FortiGate in **Feature Viability**
- Optional: Enable wireless open security to allow the broadcast of completely open wireless networks
  - Configure using FortiManager script



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

5

Before starting to install and configure APs, you may need to perform some prerequisite configuration.

By default, some FortiGate devices do not show the Wi-Fi controller option in the menu. If you don't see the option on the main configuration menu, you can enable it using the **System Visibility** option in the **System** menu.

You can also configure this option using FortiManager. It is not possible to use a provisioning template, but a CLI configuration can be enabled for the wireless controller. This can be found by clicking:

Device Manager > **Device & Groups** > **Device** > **CLI Configuration** > **system** > **settings** > **gui-wireless-controller**.

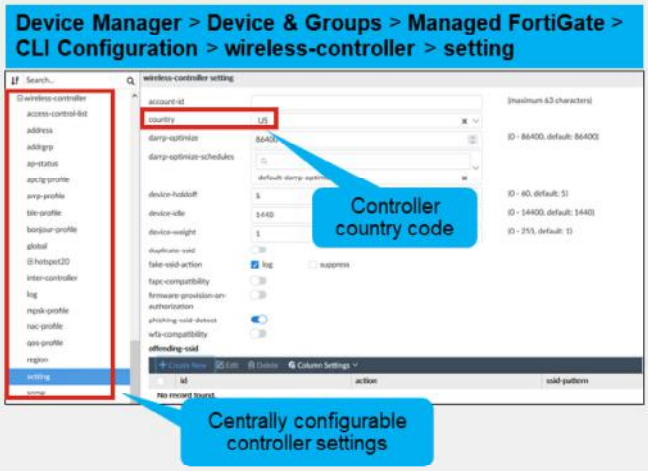
If you plan to broadcast completely open wireless networks (networks without any form of encryption or authentication), you will also need to enable the **Wireless Open Security** option under **Additional Features**. If you do not enable this feature, the open network options will not be shown.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Configuring the Country Code Using FortiManager

- Before creating wireless networks or AP profiles, the controller must be configured for the correct country code
  - Country code controls the allowed wireless channel and power setting
- Configure directly at the controller
  - CLI configuration only
- Configure using **CLI Configurations** through FortiManager
  - Individual FortiGate can be configured
  - **Provisioning Templates** cannot deliver this setting
- Delivered as part of **Device Settings**



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

6

When configuring wireless AP radio settings, it is important to know what regulatory domain you are operating in. By default, the wireless controller uses the North American regulations that govern channel usage and transmission power. If you are operating APs in any other part of the world, you will need to change the country code *before* creating any AP profiles or adding any APs.

The country code can be configure on the controller CLI using the following commands:

```
# config wireless-controller setting
(setting) # set country GB
(setting) # end
```

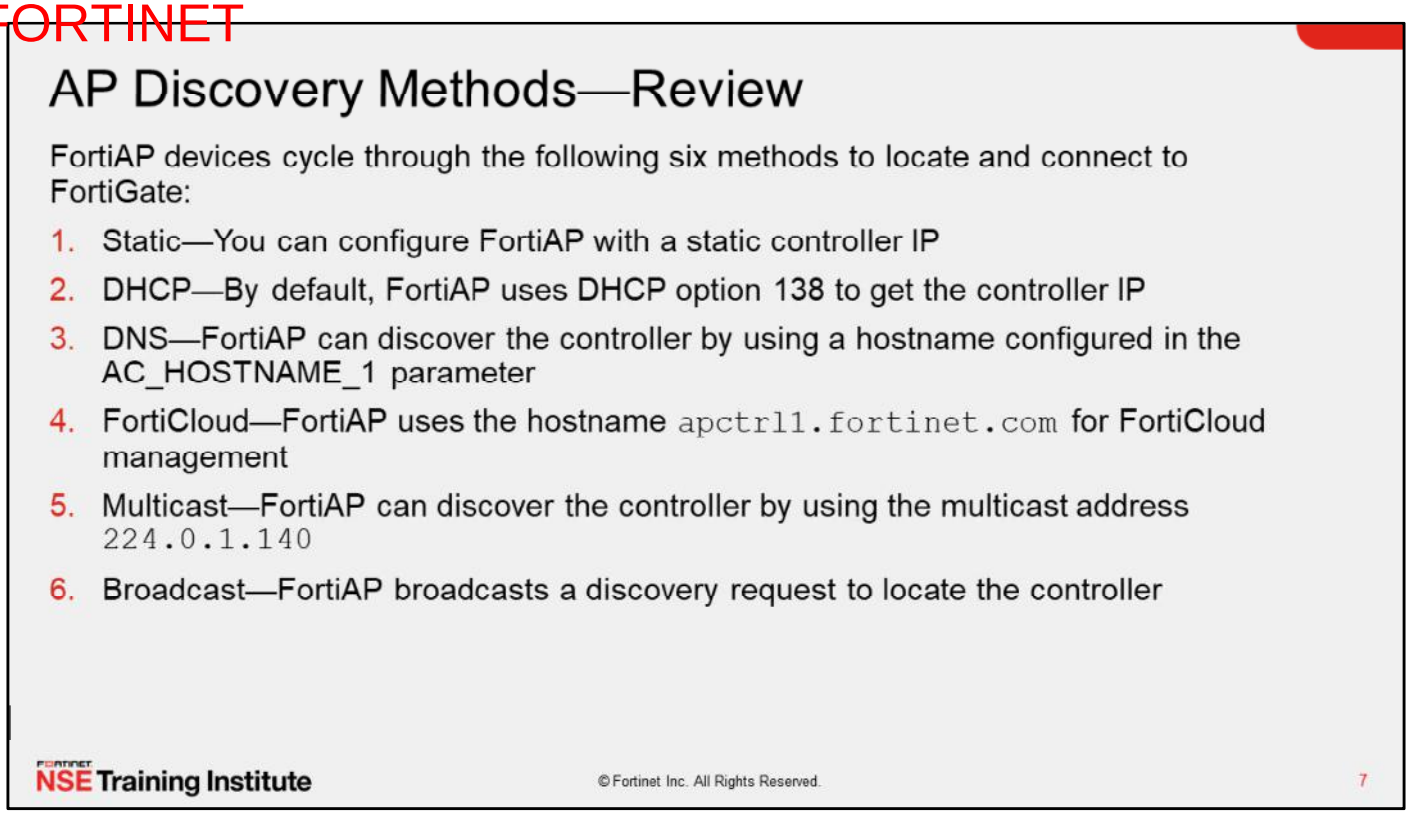
To see a full list of country codes, use the help option.

FortiManager can configure individual controllers with a country code using the **CLI Configurations** option for individual devices. By default, the **CLI Configurations** option is not visible until you it enable it through **Display Options**, either at the ADOM level or by customizing. Many aspects of the wireless controller can be configured here.

It is not possible to apply the country code setting as part of a provisioning template. Only a small set of CLI configuration settings are available in a template, and there are no wireless controller settings included.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



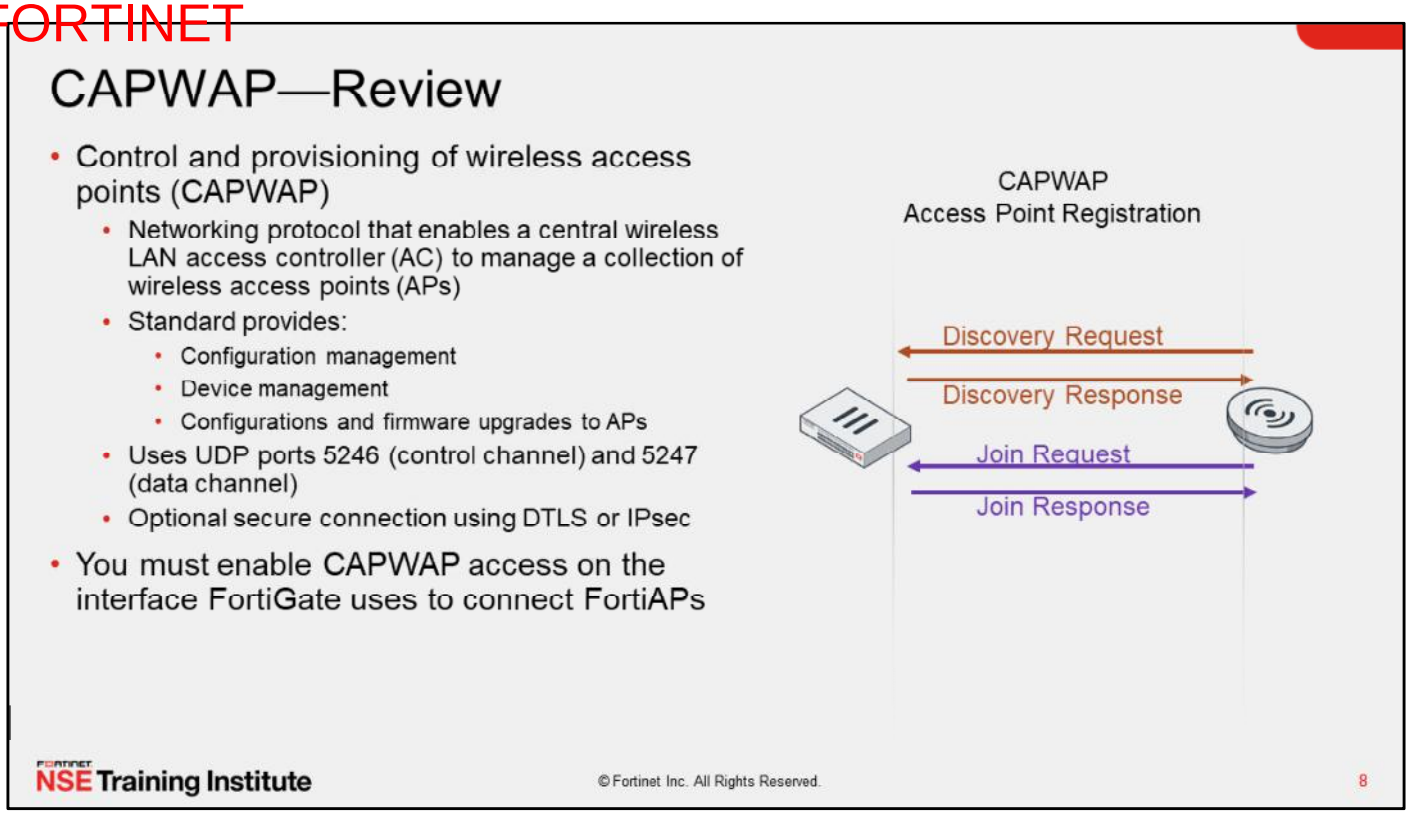
Before an AP can be managed by FortiGate, the AP and controller have to discover each other. The process is initiated by the AP during its start-up process. The AP will use multiple methods to try and determine the IP address of the local controller to connect to, or, if intending to use the cloud, the cloud-based host. By default, the FortiAP discovery method is set to auto, which means the AP will cycle through the discovery methods in the sequence shown on this slide, to locate a wireless controller. For every discovery type, FortiAP sends out discovery requests and sets a configurable timeout of between 2 and 180 seconds. The default setting is 5 seconds.

If the FortiAP times out and fails to connect to the controller, it will switch to the next discovery type and repeat the process until the last discovery method fails. This will lead to the SULKING state. After approximately 30 seconds, FortiAP will enter the `AC_IP_DISCVER` state. After the AC IP is found, it will enter the IDLE state, and will eventually enter the DISCOVERY state, then repeat the process.You can use static IP or DNS hostname methods when the AP is not deployed on the same subnet as the wireless controller, and cannot be reached by the multicast or broadcast method. You must make this configuration change on FortiAP devices manually, before deploying them. You can configure a static IP or DNS on a FortiAP using the GUI or CLI. You can also use the serial port on FortiAP to make this configuration change.

By default, FortiAP uses DHCP option 138 to receive the wireless controller's IP address. You need to convert the IP address of the wireless controller into hexadecimal. Convert each octet value separately, from left to right, and concatenate them. For example, `192.168.0.1` converts to `C0A80001`. If option `138` is used for some other purpose on your network, you can use a different option number, if you configure the AP units to match. The AP unit sends a multicast discovery request and the controller replies with a unicast discovery response message to the AP. The AP and the controller do not need to be in the same broadcast domain if multicast routing is correctly configured. The default multicast destination address is `224.0.1.140`. You can change it using the CLI, but you must make the changes to both the controller and AP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



CAPWAP is the network protocol that is used to provision and manage FortiAPs using FortiGate. CAPWAP allows an AC to manage a collection of wireless APs. In the Fortinet Integrated Wireless Solution, CAPWAP enables you to manage configuration, manage the device, and push firmware upgrades to FortiAPs.

CAPWAP uses UDP port 5246 as the control channel and 5247 as the data channel.

CAPWAP-enabled devices can, optionally, create a secure data channel to the controller using DTLS encryption or IPsec. Using IPsec will benefit FortiGate devices that can offload CAPWAP to hardware, resulting in greatly increased performance. DTLS encrypted CAPWAP *cannot* be offloaded. Where APs are located in a LAN, data plane encryption is not usually required, however if an AP is remotely based across a public WAN link data plane encryption is strongly recommended. Enabling encryption can impact throughput, particularly when using DTLS, which requires encryption/decryption in the CPU. IPsec performance can be far greater if FortiGate can offload to an NP.

CAPWAP provides direct administrator access to a FortiGate interface, so it must be enabled on the interface that the FortiAPs will be connecting to.

The CAPWAP discovery process:

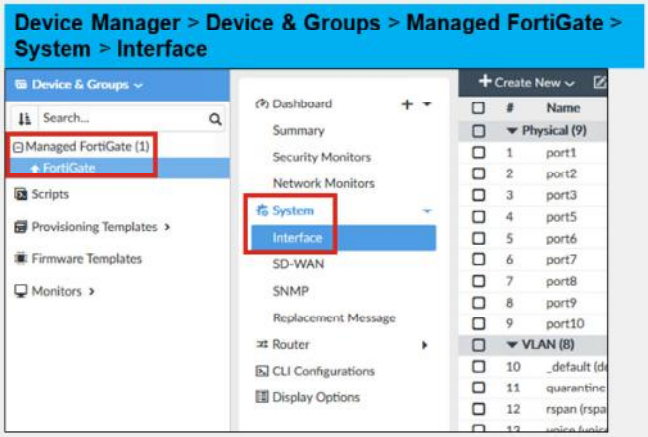
1. FortiAP sends a discovery request.
2. FortiGate responds with a discovery response.
3. Both devices establish a secure DTLS session.
4. After FortiGate authorizes the FortiAP, the CAPWAP discovery and join phase takes place.
5. After the CAPWAP tunnel is established, FortiGate sends all required management and WLAN-related configuration to FortiAP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Enabling CAPWAP Using FortiManager

- You must enable CAPWAP access on the interface FortiGate uses to connect FortiAPs
- It opens ports for communication for CAPWAP on UDP ports
  - 5246 control channel
  - 5247 data channel
- CAPWAP is enabled as part of the **Security Fabric Connection** access
- Enabled using **Device Manager** for FortiGate physical interfaces and VLANs
- Enabled on FortiSwitch VLANs using **FortiSwitch Manager**
  - On either a **FortiSwitch Profile** or **FortiSwitch Template**



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

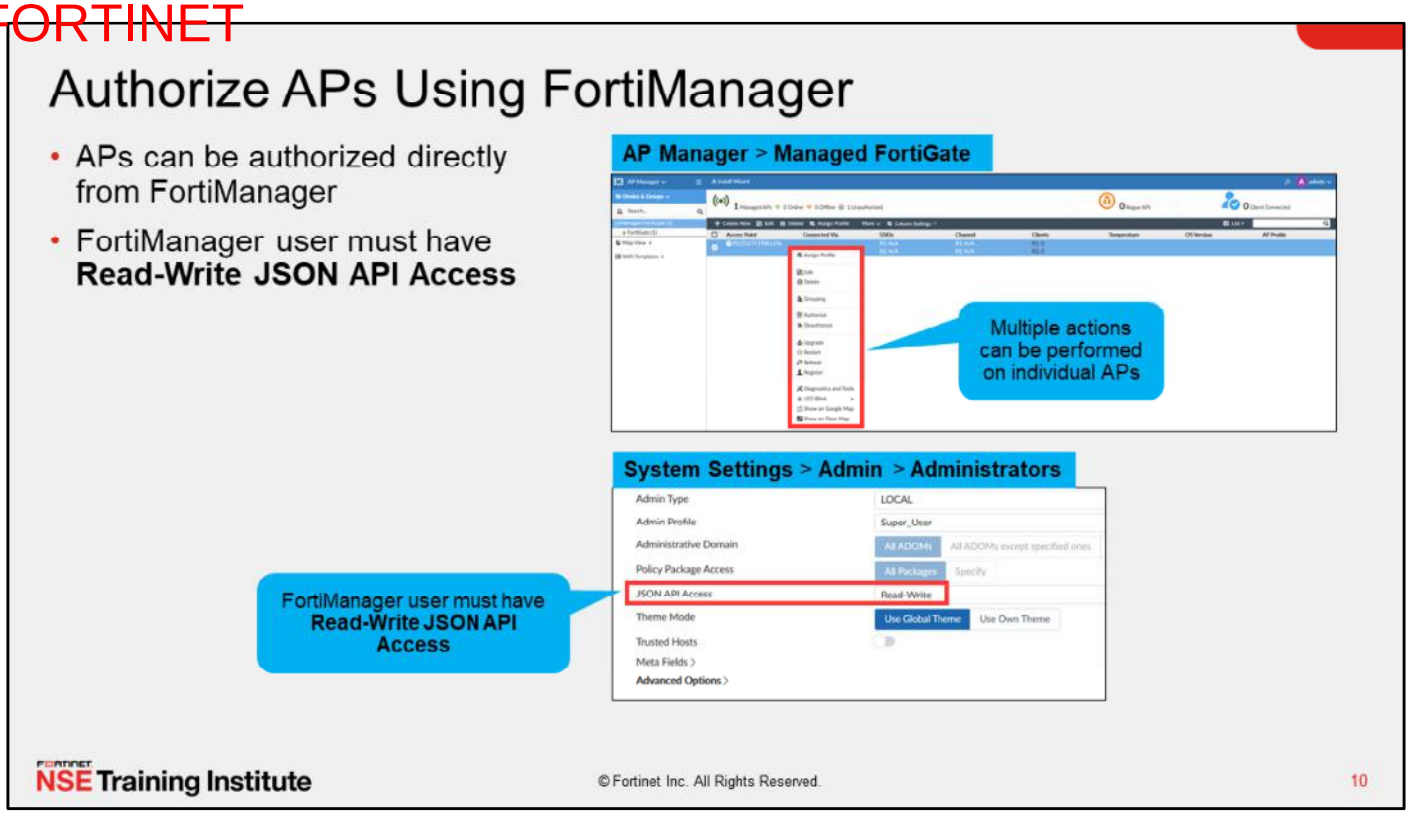
9

On FortiGate, choose an interface to which you will connect FortiAPs. You must enable CAPWAP access on any interface that will connect FortiAPs, even if they have intervening switched or routed links. CAPWAP access is now included as part of the **Security Fabric Connection** administrative access. Access has to be configured on a per-device basis, access can not be assigned using a provisioning template.

If required, enable the DHCP server option to allow FortiGate to assign IP addresses to FortiAPs. It is also possible to use other DHCP servers (such as Microsoft DHCP), but those servers must be configured to pass DHCP options, when required.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



After you have configured the appropriate discovery method on FortiGate (if configuration is required), and you have enabled CAPWAP, you can turn the AP on, and it will begin trying to discover the controller.

After FortiGate receives a discovery from an AP, you must authorize FortiAP to establish a CAPWAP tunnel between an AP and FortiGate. This indicates to the controller that it is now responsible for the management of the AP. When you authorize a FortiAP, it uses the default FortiAP profile that is determined by AP model and applies a default configuration based on the AP hardware.

When the ADOM managing FortiGate is in **Central Management** mode, it is possible to authorize the AP directly from FortiManager. The user requires the **Read-Write** JSON API access right configuring in their account details before they can authorize APs using FortiManager.

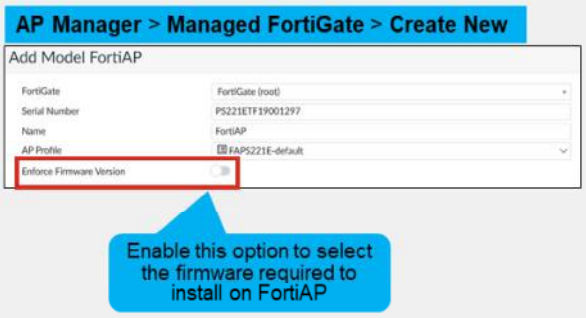
If the ADOM is in **Per-device Management** mode, the APs have to be authorized from FortiGate before they become visible in FortiManager

After a CAPWAP tunnel is established between the two devices, you will see a green check mark beside the listed FortiAP. The green check mark indicates that FortiAP can communicate with FortiGate and has received the initial configuration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Preauthorizing APs



- You can preauthorize APs by specifying the:
  - AP serial number
  - Name
  - AP profile
- These settings are mandatory
- After connecting to the network, the APs will be automatically authorized and moved to an online status

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

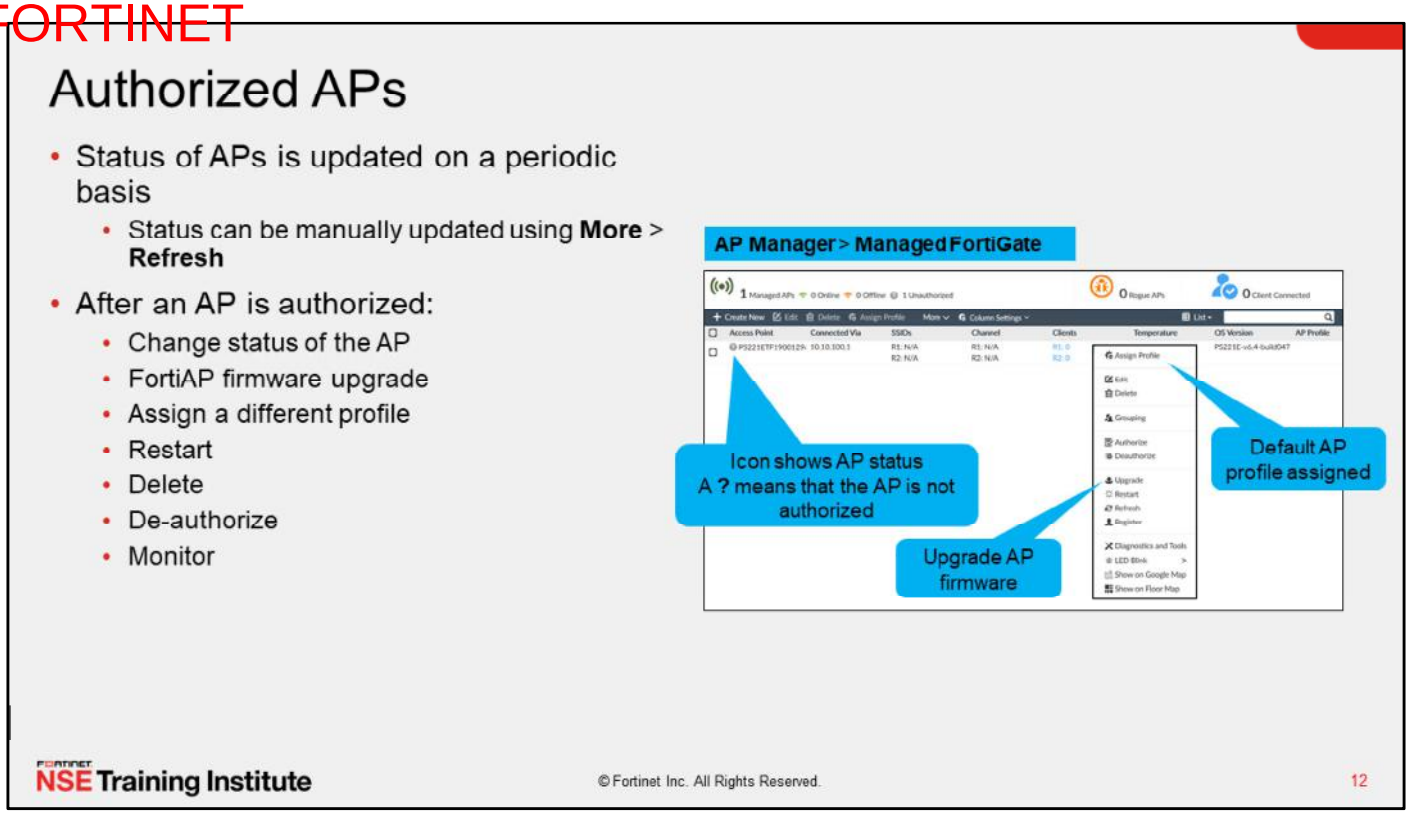
11

FortiManager allows you to preauthorize FortiAPs that will be added to your network. You must add all FortiAPs manually, one-by-one, to FortiManager using the AP serial number and specifying the name (which can be the serial number) and AP profile.

After the preauthorized FortiAPs come online and are discovered by FortiGate, FortiManager/FortiGate authorizes the FortiAPs automatically. FortiGate will establish a CAPWAP tunnel to the FortiAP devices and push the configuration to them, based on the assigned AP profile.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



After an AP is authorized, you can perform various tasks using the FortiGate GUI. On the **Managed FortiAPs** page, you can:

- Change the status of an AP (authorized to de-authorized)
- Perform an AP firmware upgrade
- Change the assigned AP profile
- Restart FortiAP
- Show the AP on a map
- View the spectrum and client information.

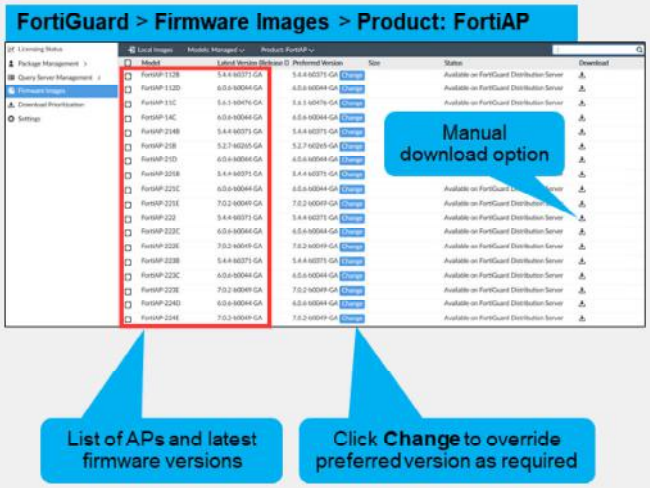
The table is updated approximately every three minutes. As a result, changes in an AP may not be displayed immediately.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Updating APs Using FortiManager

- Before continuing to set up an AP, you should ensure that it has appropriate firmware installed
- Locate the AP firmware images on the Fortinet support website
  - Review the *FortiAP and FortiOS Compatibility Matrix* for recommended firmware
  - Review the relevant release note for the AP
- FortiManager can centrally manage firmware updates for APs
  - List of supported APs and firmware synchronized with FortiGuard
  - Downloaded on demand or manually
  - Can be overridden to specify a version



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

13

Before continuing with the AP setup process, it is a good idea to confirm the current recommended firmware version for use with the release of FortiOS installed on FortiGate. The Fortinet support website contains up-to-date copies of the firmware for APs and a compatibility matrix, which allows you to select the appropriate version of FortiAP firmware for use with FortiGate. Ensure that you review the release notes for the version of firmware you're planning to install because it may include important information relating to the upgrade.

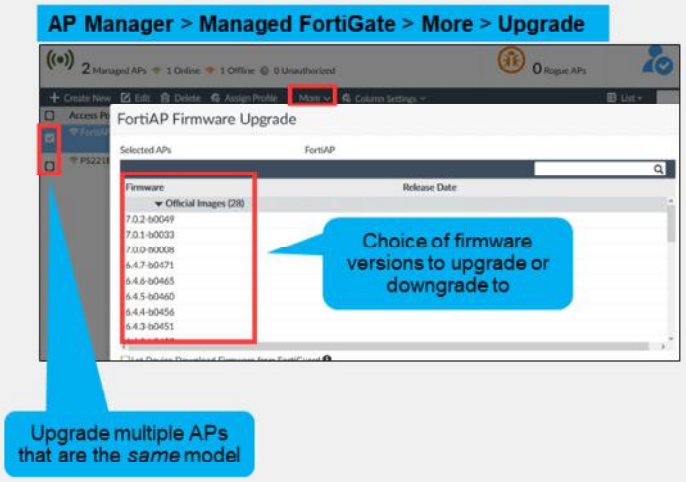
FortiManager maintains a repository of the AP and switch firmware versions. You can update the APs directly from FortiManager, either individually or in groups of APs of the same type. You can find the list of supported APs by clicking **FortiGuard** > **Firmware Images** and selecting **FortiAP** from the **Product** tab. FortiManager does not automatically download all the firmware versions; it downloads only when an update is requested or if you click the **Download** icon next to the AP. You can also change the AP firmware version that is used by clicking **Change**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Updating APs Using FortiManager (Contd)

- APs can be centrally upgraded in both **Per-Device** and **Central Configuration** mode
- Multiple APs can be upgraded at once if they are the same model number
- Option to allow AP to download firmware directly from FortiGuard if AP is remote
- Upgrade task can take many minutes or hours, depending on number of APs upgraded
  - Progress of upgrade task can be monitored in **System Settings** > **Task Manager**



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

14

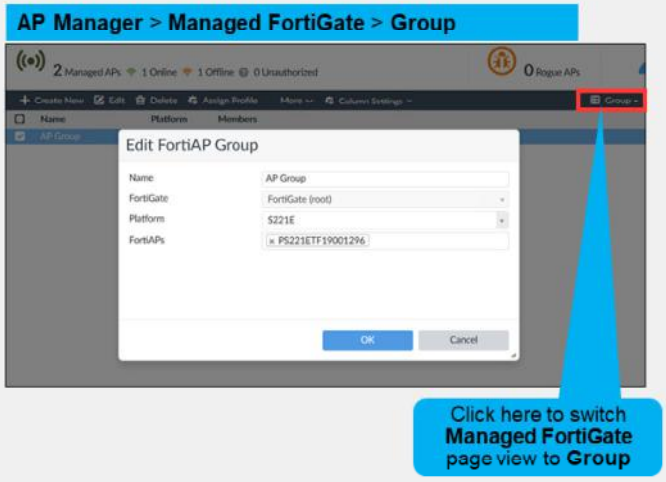
You update APs managed in per-device or central configuration mode in the same way. You can update single APs or multiple APs that are the same model number. When you upgrade, FortiManager shows a choice of AP firmware images with the latest image listed at the top. Select the image you require and then click **Upgrade Now** to start the upgrade. The upgrade process will display a real-time progress report, which you can close if required, and you can also monitor the process from **System Settings** > **Task Manager**. If the AP is remotely located, you can download the upgrade image directly from FortiGuard instead of the FortiManager server.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiAP Groups

- FortiManager allows the grouping of FortiAPs
- You can group FortiAPs based on the FortiGate device that supports them and the AP model
  - FortiAPs can belong to only one group at a time
- Can be used to selectively monitor FortiAPs by location



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

15

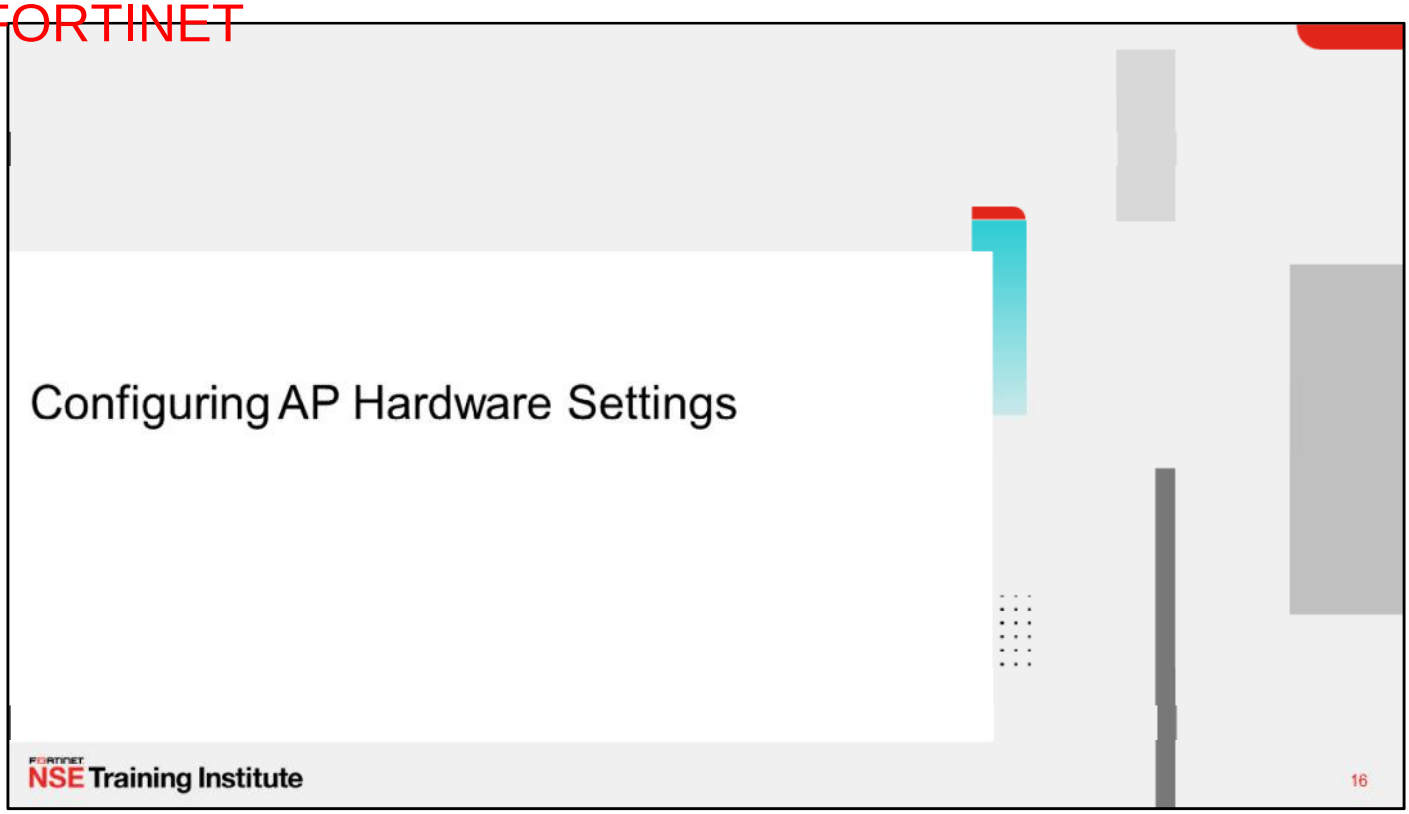
You can group FortiAPs in FortiManager. APs of the same type and APs that are connected to the same controller can be part of the same group but can be members of only one group.

You can use groups to organize APs geographically. For example, all the FortiAP U431F APs located in the canteen can be organized in a group. Grouping APs by location can help with the monitoring and troubleshooting of issues.

In wireless networks, many issues are related to the physical location of the APs and clients. You can use groups to help focus on geographical sets of APs.

Vouchers & Dumps are Available | WhatsApp +201224560923

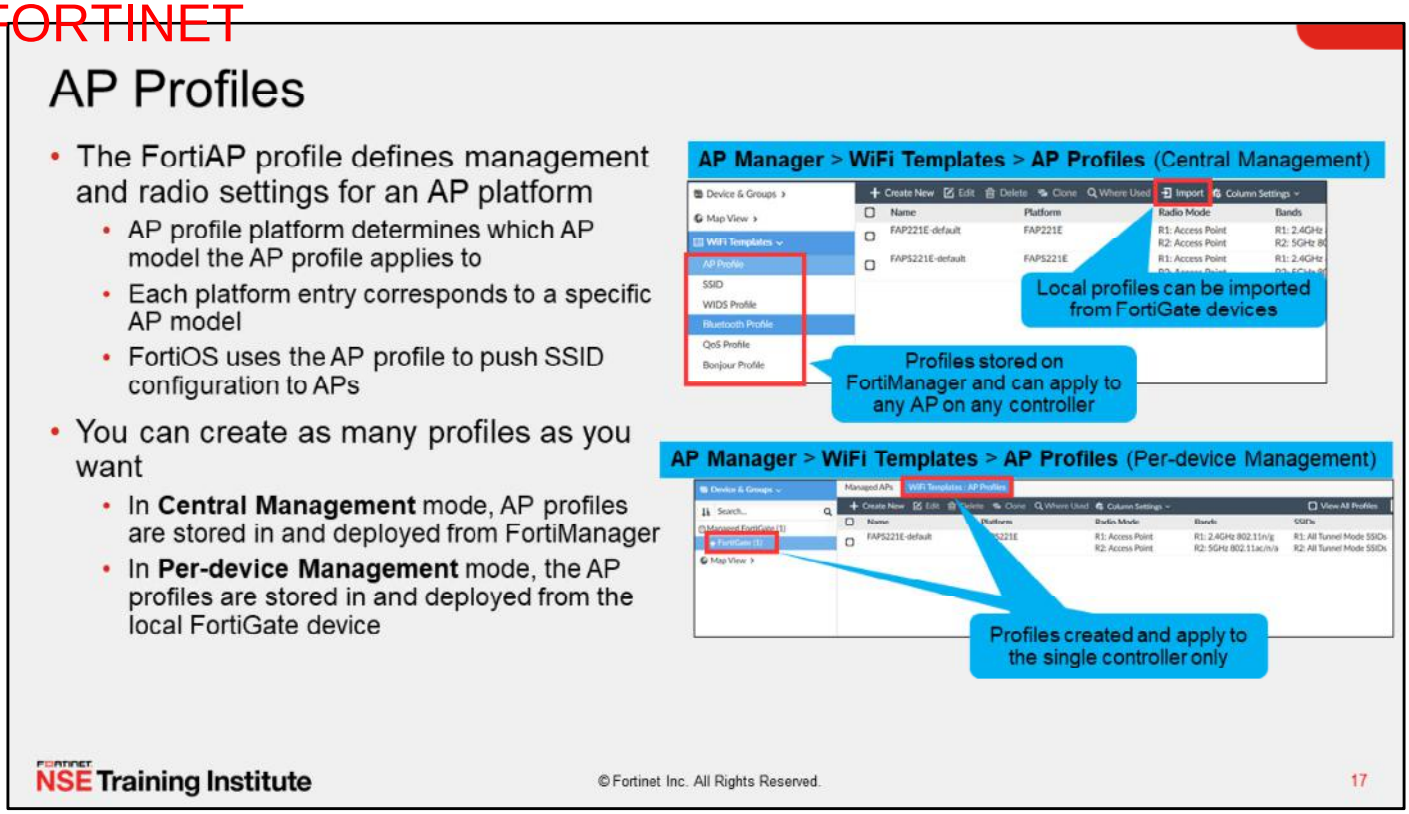
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn how to configure FortiAP radio settings using FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



To view and manage FortiAP profiles in FortiManager, click **AP Manager** > **WiFi Profiles** > **AP Profile**. The layout you see depends on the ADOM mode, In **Central Management** mode, only the profiles available on FortiManager are shown. You have the option to import a profile from a managed FortiGate. In **Per-device Management** mode, you can view profiles stored on *each* FortiGate. Changes in profiles are synchronized.

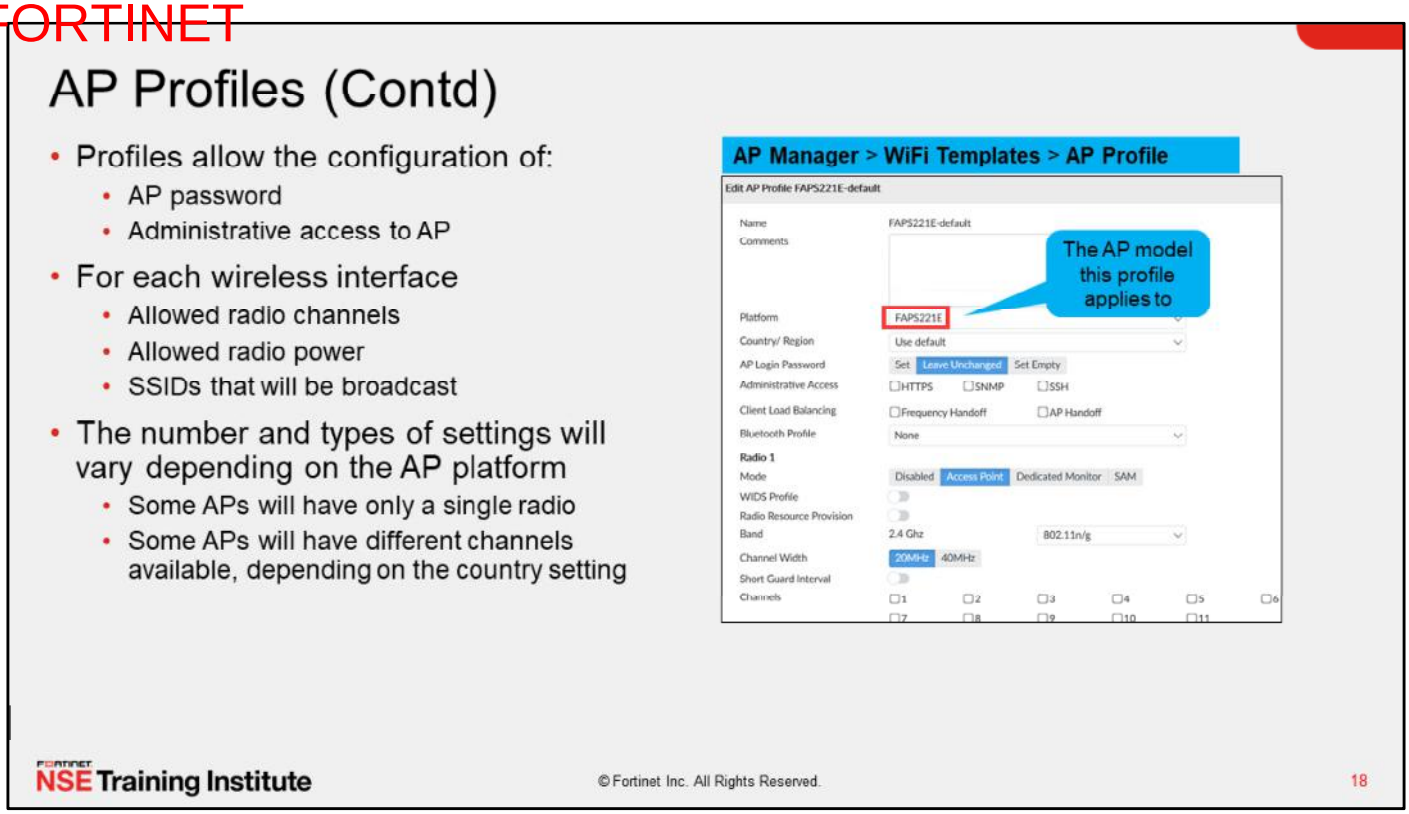
Not all profiles are displayed. By default, only those profiles that are compatible with the installed FortiAPs are displayed. In **Central Management** mode, you can view a full list of support AP profiles by selecting **View all Profiles**.

When an AP is assigned a profile, that profile controls the management and radio settings used for the channel setting, channel widths, transmission power levels, and wireless networks broadcast.
Because there are many types of APs, there are many types of hardware in use. Each type of hardware may require slightly different configuration settings, which requires that each type of AP has its own default profile to define the scope of the settings allowed.

You can create multiple profiles by creating new ones or cloning existing ones. You can have multiple profiles for the same AP type, but each profile may specify slightly different configuration settings. When APs are no longer using a profile, you can delete any unused profile.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



AP profiles control the various configuration options for APs and their radios.

Because different AP models have different capabilities, one profile type cannot control all AP models. Each profile has different options depending on the capability, type, and number of the radios.

The AP profile is where you decide which channels and power levels the AP will use when it is assigned the AP profile.

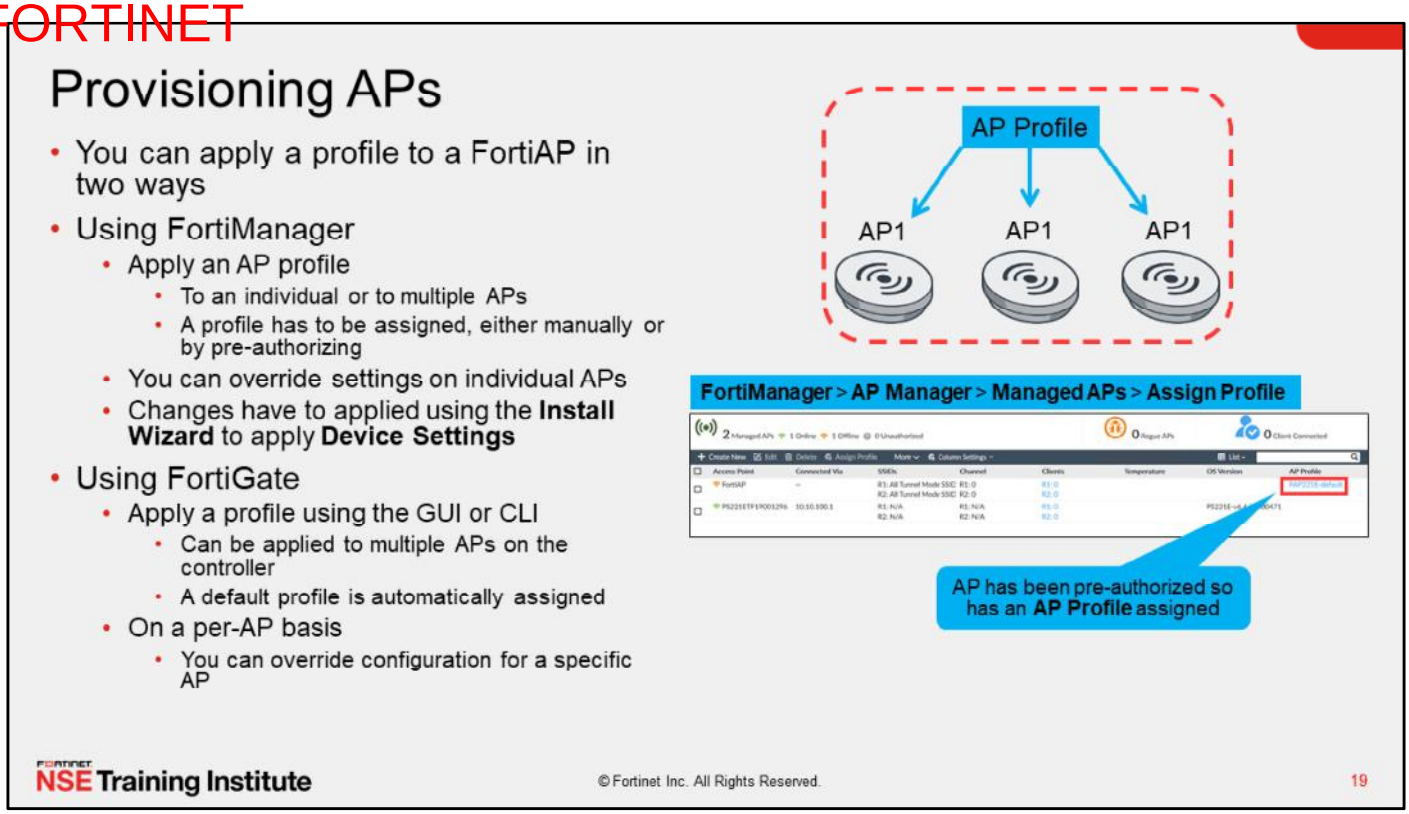
You also control which wireless networks broadcast on which wireless interfaces. For example, it is possible to broadcast a network *only* on the 5 GHz interface by configuring it only on radio interface 2.

Other profiles, such as the WIDS profile, may also be referenced by the AP profile.

Changes to a profile will apply to all APs that are assigned that profile. The changes are applied as part of the device settings that can be applied to a FortiGate device from FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



FortiGate automatically assigns a *default* AP profile to an AP when it is discovered and authorized. The profile is assigned based on the AP model detected during discovery.

FortiManager does not automatically assign a profile. You can define the profile by configuring it or by pre-authorizing the AP. After you apply a profile, because device settings are not automatically applied, you will need to apply them through the install wizard.

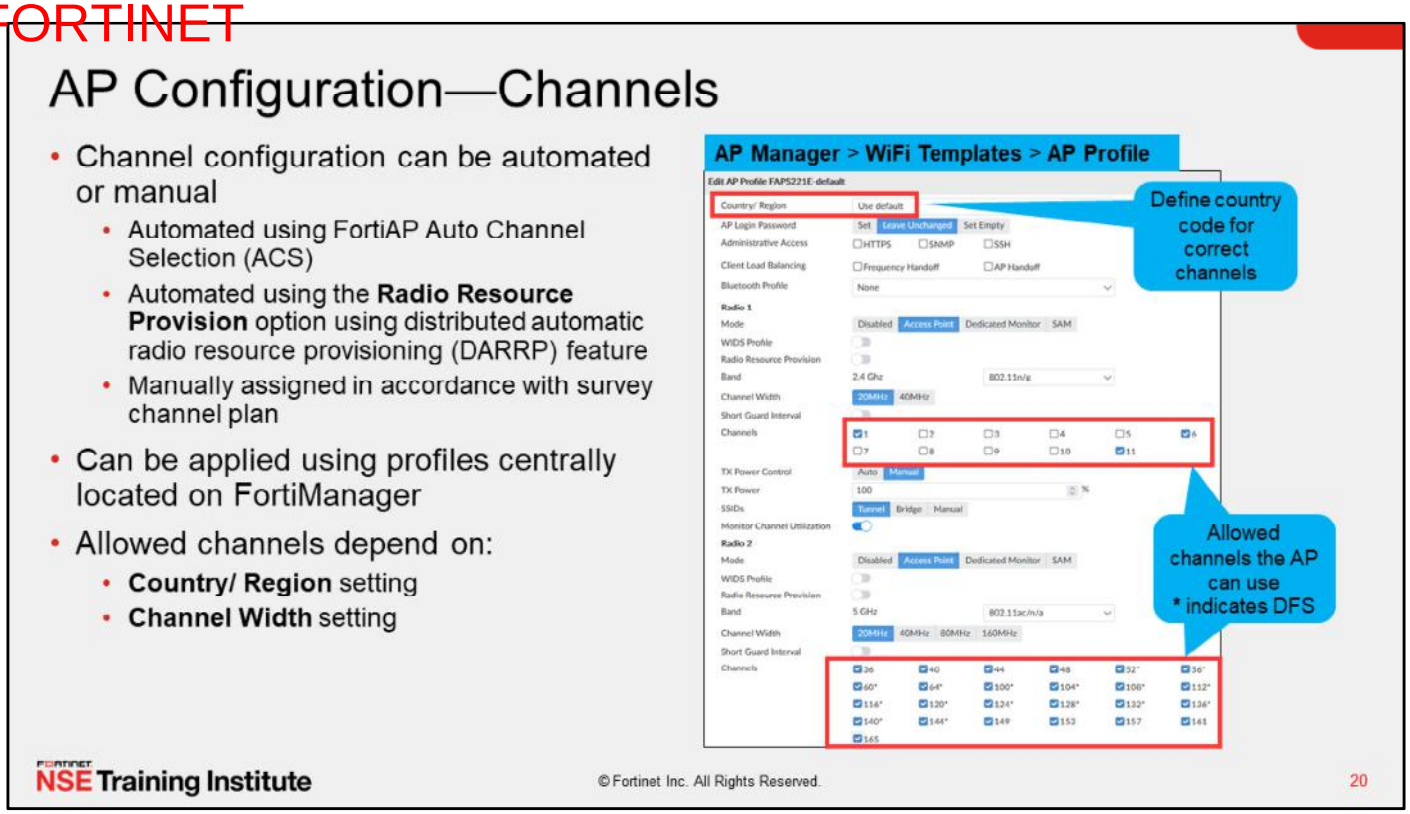
Both FortiGate and FortiManager have a set of default profiles based on the model of the AP. These are contained and updated as part of FortiOS. ADOM **Central Management** mode uses profiles located on FortiManager. **Per-device Management** mode uses profiles located on FortiGate.

After a CAPWAP tunnel is established between FortiGate and an AP, FortiGate uses the CAPWAP control channel to push all AP profile parameters to the AP. You will likely want to assign an AP profile that is different from the default, because you will have specific channel settings or AP settings you will want to deploy. It is important to note that you can assign an AP profile to one or multiple APs, but you *cannot* assign multiple profiles to a *single* AP. All APs that use the same AP profile receive the same configurations from FortiGate.

For more flexibility and granularity, you can override the AP profile configuration on a per-AP basis. You *must* assign an AP profile to an AP, but you can modify the settings on an individual AP basis using the GUI on FortiManager, or using the CLI and GUI on FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



An essential part of the profile configuration is the setting of the wireless radio channels. You define the channels that the AP can use by selecting the correct country code and required channel width. By default, 40 MHz channels are recommended for the 5 GHz range, and 20 MHz channels for the 2.4 GHz range.

After you select the channel width and country code, the legally allowed radio channels that the AP can use are indicated by the selected checkboxes. You will see that some of the 5 GHz channels have an asterisk (*****). The asterisk indicates channels that are subject to DFS regulations.

The use of DFS channels is a design decision. In some countries, the use of certain DFS channels is regulated, so you should be familiar with any local requirements. Many low-cost wireless clients are not DFS certified. As a result, they are not able to see APs configured for DFS channels. APs using DFS channels can also suffer from DFS events, causing them to change channels. This can cause issues for networks that support latency-sensitive applications, such as voice over IP (VOIP).

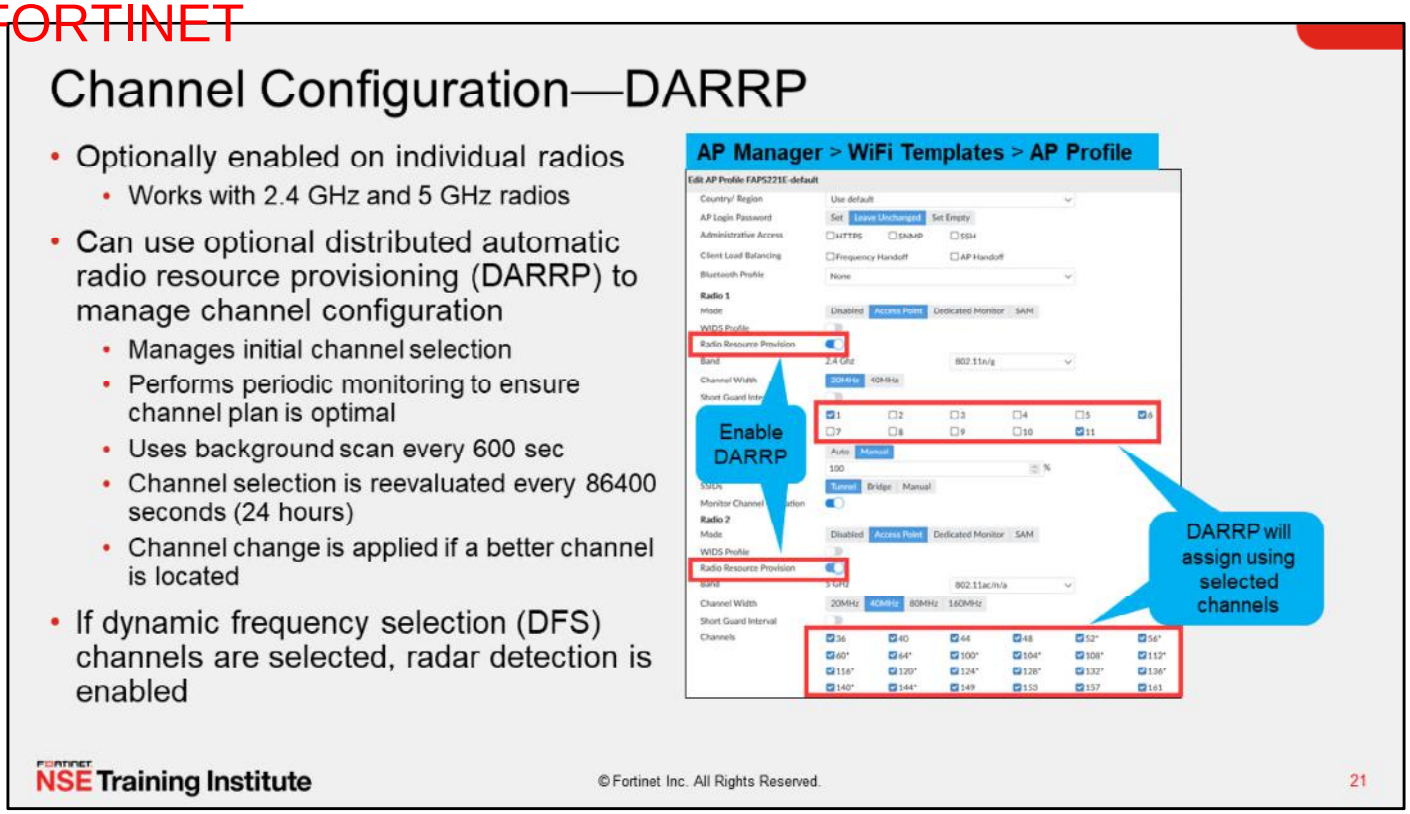
FortiAP automatic channel selection (ACS) is used when either *no* channels, or *multiple* channels are selected. The AP will perform a channel quality assessment on AP startup. It will assess the number of APs in each channel, measure the noise level and channel utilization, and then choose the channel with the least. It will perform a second check somewhere between 2 and 15 minutes later and change channel if a better channel is available. After that point, no further selection process takes place.

The optional distributed radio resource provisioning mechanism (DARRP) can manage initial channel allocation *and* ongoing channel optimization. It is an enhanced method of channel selection that uses the central information stored on FortiGate. It is optional and has to be enabled.

If a *single* channel is selected, the APs configured with that profile will use the channel selected.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The easiest method for allocating channels to APs is to use the distributed automatic radio resource provisioning mechanism (DARRP). This automated function runs on FortiGate and collects information from the RF environment to enable efficient planning of channels. It will then automatically assign channels to the interfaces, based on the channels allowed in the profile. Other than setting the allowed channels in the AP profile, it requires little management and runs automatically. It works well for small to medium-sized wireless networks.

When using DARRP, the AP selects the best channel available to use based on the scan results of BSSID/Received Signal Strength Indicator (RSSI) to AC. To prevent interference between APs, DARRP measures utilization and interference on the available channels and selects the clearest channel at each AP. DARRP uses AP background scan results as input, scans occur every 600 seconds and can be overridden and adjusted by configuring the **ap-bgscan-period** timer in the appropriate FortiManager WIDS profile in **AP Manager** > **WiFi Profiles** > **WIDS Profile**.

The data from the scans is used in the DARRP calculation. A large number of APs results in a complex calculation that will consume resources. If the calculation determines that there are more suitable channels to use, FortiGate performs a channel change. By default, the DARRP calculation runs every 86400 seconds (or 24 hours) and will run for a variable amount of time, depending on the number of APs. You can configure the **darrp-optimize** timer to reduce the interval as part of the **Device Manager** > **Devices & Groups** > **Device** > **CLI Configurations** > **wireless-controller** > **setting** on FortiManager.

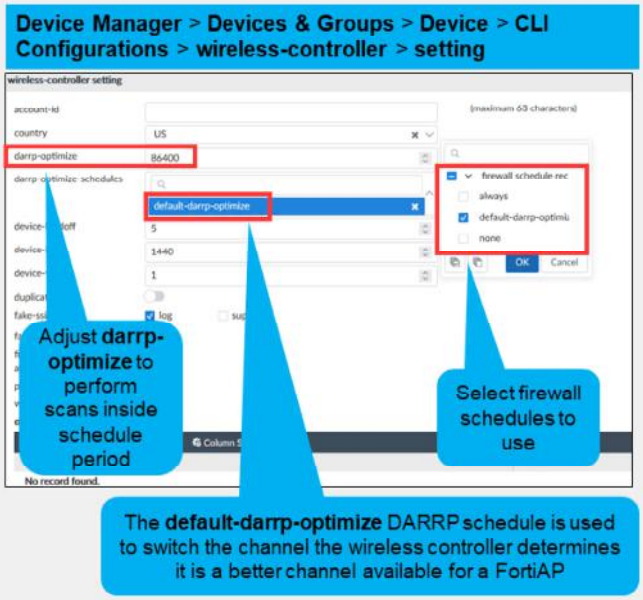
Note that DARRP doesn't do a continuous spectrum analysis, so it may not detect intermittent interference sources such as microwave ovens.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Scheduling DARRP Scans

- In a large wireless network the default DARRP settings can cause disruption
  - Many APs can cause long calculation times when planning channels
  - Multiple channel changes through the day
  - Can be disruptive in busy networks
- DARRP scans can be scheduled for a quieter time
  - You can apply a firewall schedule to control when DARRP scans and changes to the channel plan occur
  - Default schedule will scan between 1 AM and 1:30 AM each day of the week
  - Multiple schedules can be defined and deployed as part of a CLI configuration
- You can define scans as part of the CLI configuration



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

22

In more extensive networks with many APs, the DARRP process can consume significant resources when planning channels. After the calculation is complete, FortiGate will change the AP channels. Both of these processes can be disruptive. The computation takes resources on the controller, and a complex RF environment can generate multiple channel changes, which can be disruptive to client connectivity.

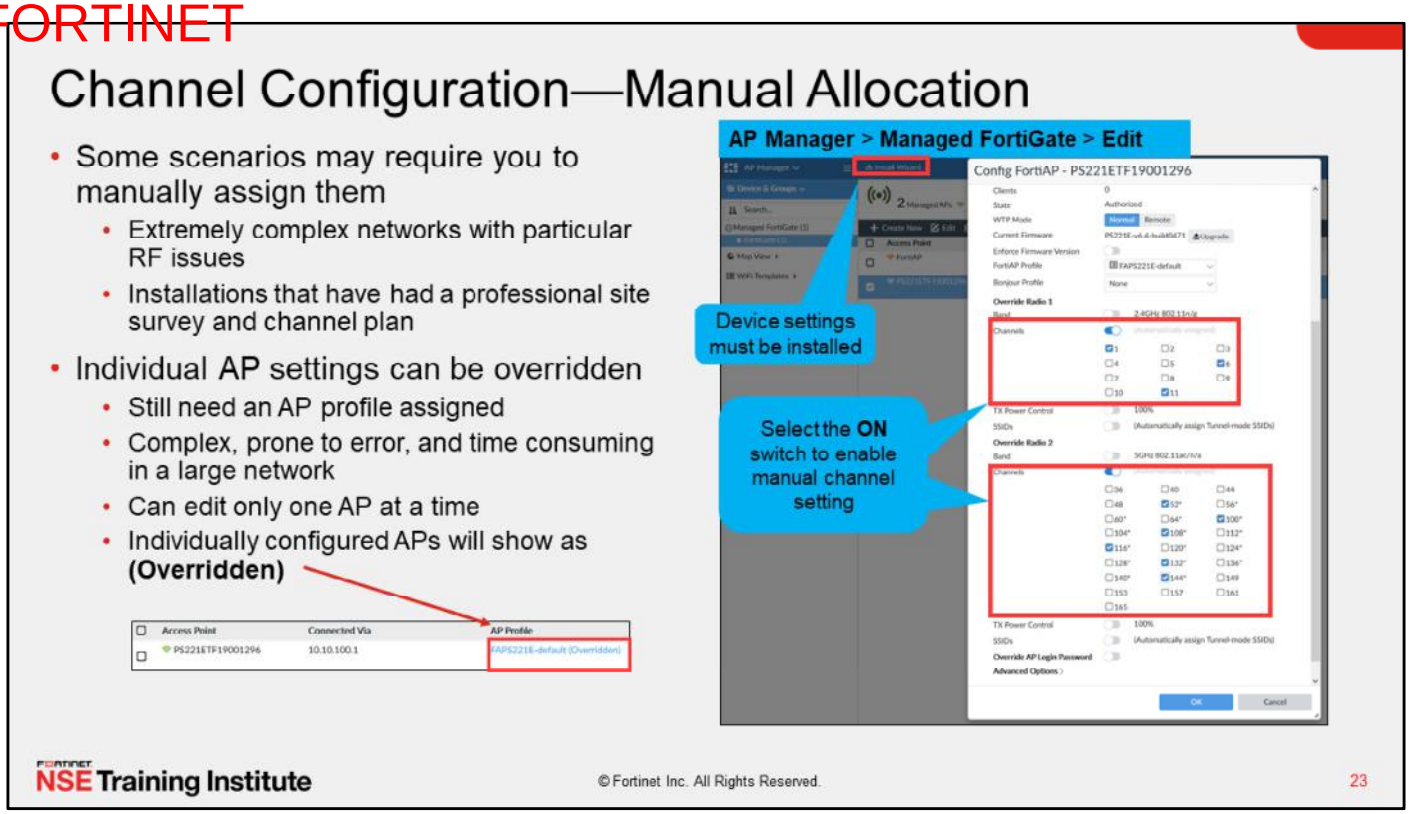
You can enable scheduling to control when the DARRP calculation occurs. You can configure a firewall schedule to limit the time during which the DARRP calculation and subsequent channel changes are made. A common practice is to schedule these activities to occur overnight, when the network is quieter.

You can use the default schedule, or, you can create a custom schedule. When limiting calculations to a small number of hours, you must ensure that the **darrp-optimize** timer is adjusted to allow at least one calculation attempt inside the period defined.

You can deploy firewall schedules from FortiManager as part of **Policy & Objects** > **Object Configurations** > **Firewall Objects** > **Schedules**. You can use FortiManager to enable DARRP scheduling under **Device Manager > Devices & Groups > Device > CLI Configurations > wireless-controller > setting**. DARRP scheduling is enabled on a per-controller basis; you cannot enable it as part of a provisioning template.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The DAARP process is usually the most efficient method for managing the AP channels. However, on occasion, it is necessary to control the channel configuration more precisely. You can set channels on each individual AP or override them manually.

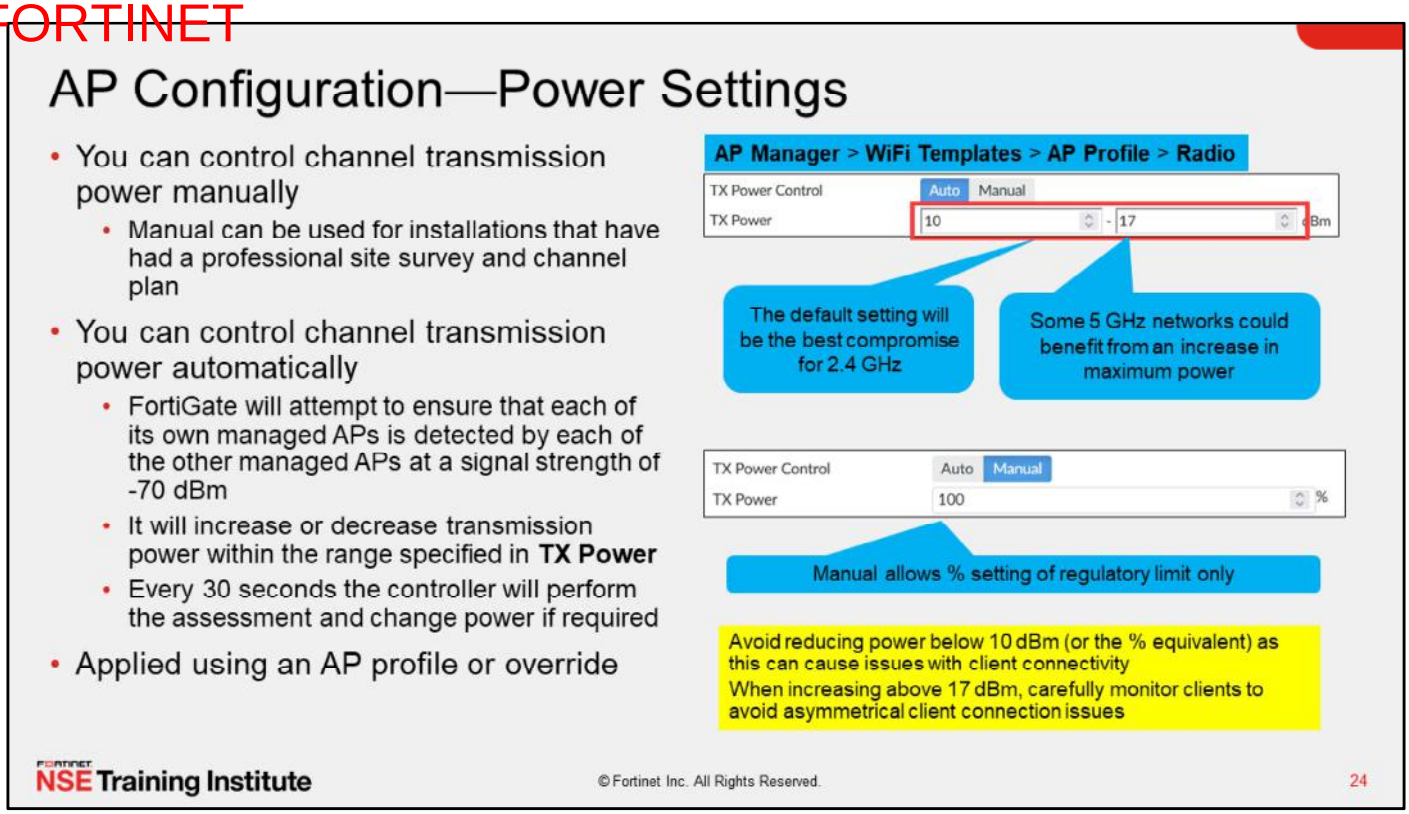
Assigning channels manually may be necessary if parts of the radio spectrum are suffering continued interference, or if a site survey is performed. Typically, surveys will specify channel settings and power levels after a full passive or active scan. Sometimes, implementing the survey design recommendations instead of using DARRP is required.

APs still require an AP profile, which defines the majority of the AP settings. You can configure individual APs through the AP manager by selecting an AP in turn and editing its configuration. You will notice that not all AP settings can be overridden. For example, it is not possible to override the **AP Mode** or **Client Load Balancing** settings; the AP profile sets these. You can selectively enable override on the radios and then select the channel required. Note that you should choose only the channel required. Any change that you make is not applied until the **Device Settings** are applied using the **Install Wizard**.

After you override an AP, you will see a message in the **AP Profile** column of the **Managed APs** table that indicates that you have applied manual settings. If you change the profile, the override will persist until the changes are reverted manually.

Vouchers & Dumps are Available | WhatsApp +201224560923

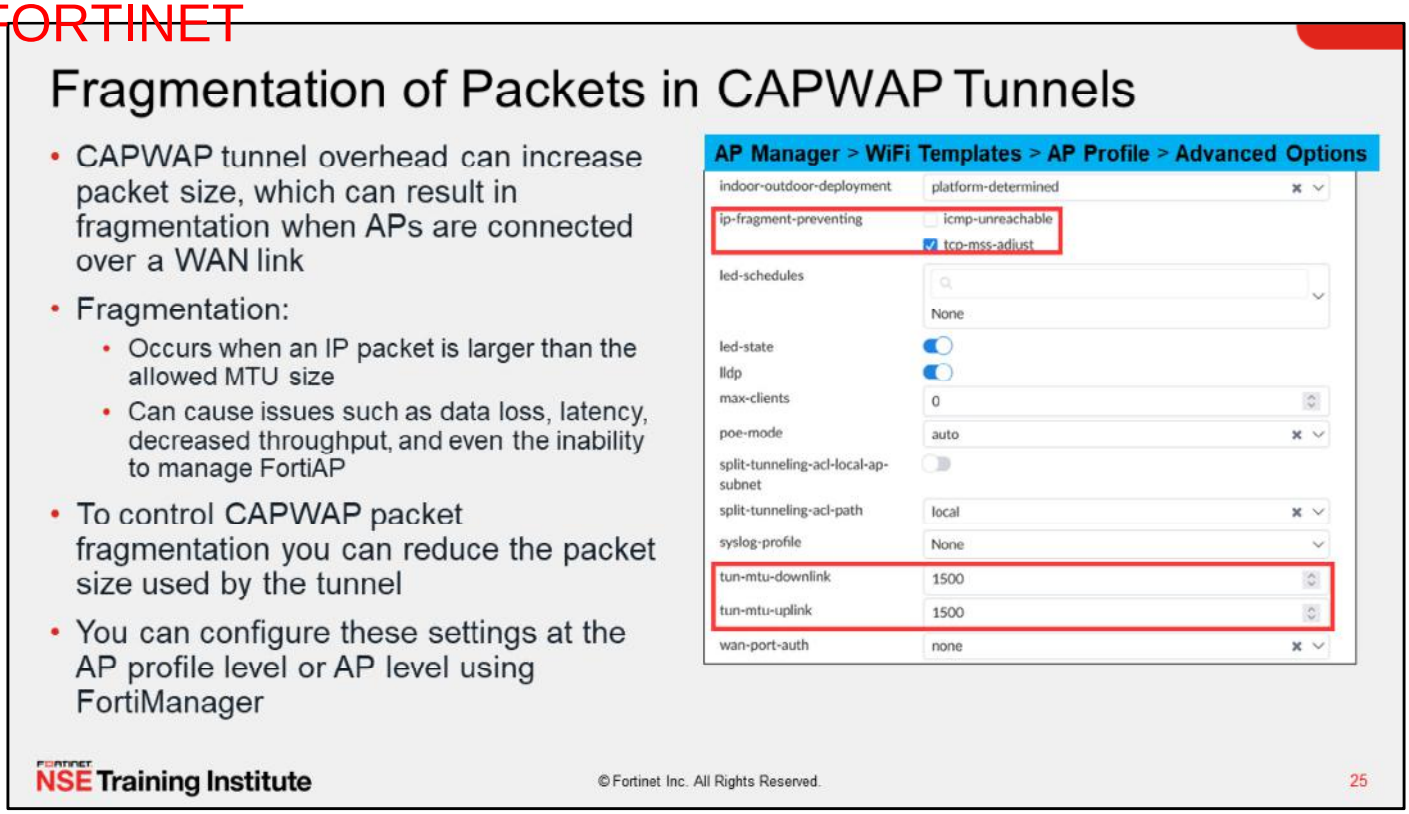
DO NOT REPRINT Brave-dumps.com
© FORTINET



It is crucial to ensure that the transmission power of your AP radios is optimized. A physical site survey is the best way to perform power measurements in each of the locations that require wireless coverage. However, this is not often practical for cost or other reasons. A simulated survey can provide suggested power settings based on a predictive design, which simulates the RF propagation through the building where you are installing the APs. If you are deploying your network using power settings and channels defined by a site survey, you can use the **TX Power Control** in manual mode to set the transmission power as a percentage. The percentage is based on the maximum transmission power that is allowed in the regulatory domain for the AP. The maximum allowable transmission power for 2.4 GHz radios might be 20 dB, so 70% power would equal approximately 14 dBm. Be aware that setting the power too high or too low in many 2.4 GHz environments will cause significant issues. Automatic power control will use signal strength measurements made between the APs that FortiGate is supporting. Every 30 seconds, the wireless controller will measure the signal strength of any *other* APs connected to FortiGate. Other APs not connected, not broadcasting an SSID, or advertising an infrastructure mode network, will not be used in the calculation. The wireless controller is only interested in its own APs, not any neighboring ones. If the detected signal strength of the measured FortiGate managed AP is above or below a target of -70 dBm, the controller will adjust the transmission power of that AP. By default, the range of adjustment is between 10 and 17 dBm. This range of adjustment is sufficient for the majority of 2.4 GHz networks. Because 5 GHz networks are configurable with a greater number of channels, the chance of overlap is less. Therefore, depending on the number of channels configured, it is possible to increase the maximum transmission power and still avoid co-channel interference. For the majority of installations, automatic transmission power control is recommended and can be configured using an AP profile or by override. You must be careful setting the power level on 5 GHz radios. Some channels have different power level settings, so setting a profile that is too high for some channels will cause the profile to fail installation.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



CAPWAP tunnel overhead can increase packet size which can result in fragmentation. Fragmentation occurs when an IP packet is larger than the allowed MTU size. Fragmentation can cause issues such as data loss, latency, decreased throughput, and, in some cases the inability to manage FortiAPs. One of the solutions to this problem is to control the packet size on the managed APs. You can decrease the MTU size for CAPWAP tunnels by modifying the uplink and downlink tunnel MTU size in the AP profile configuration on the CLI. You can also override this setting for a specific AP.

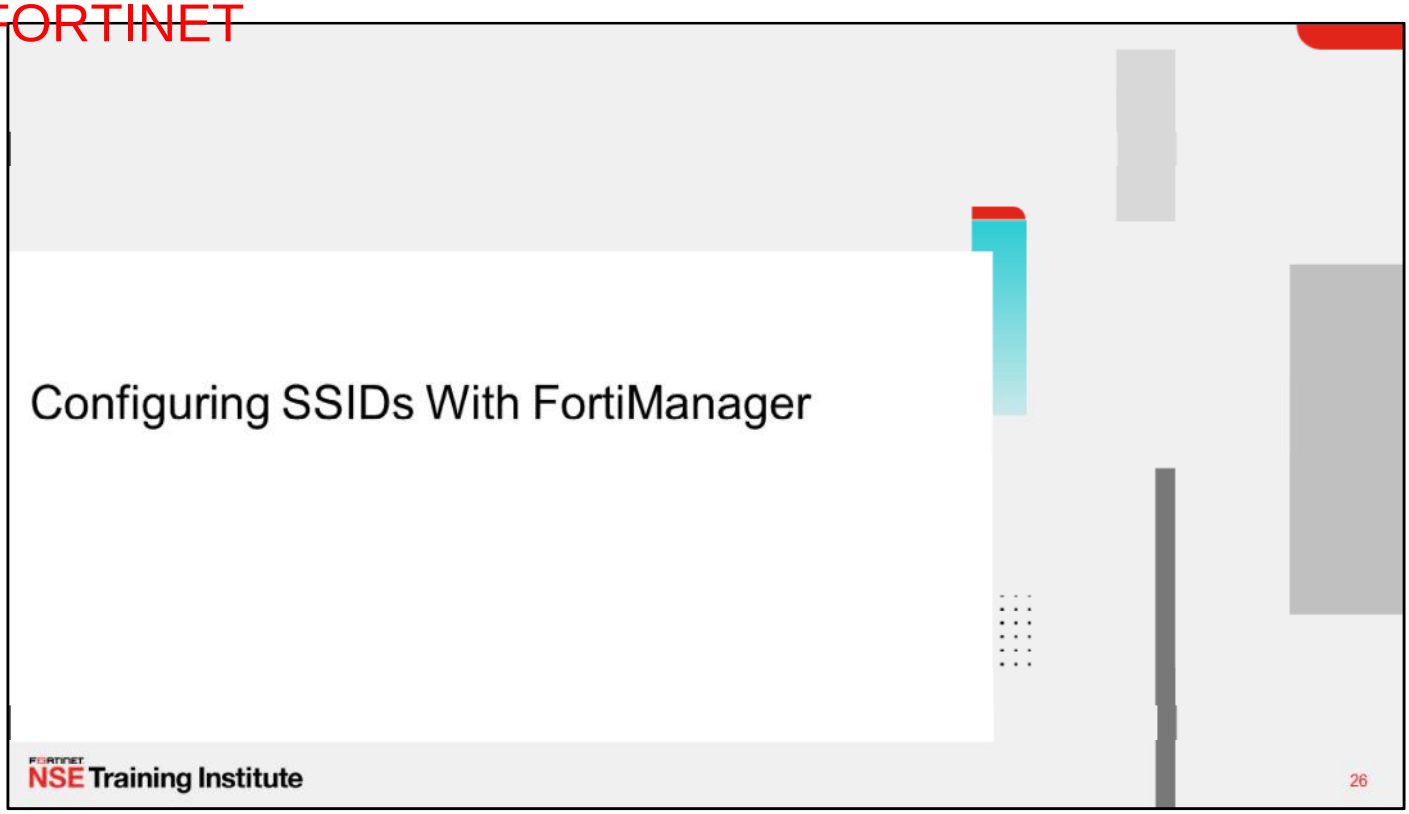
The **tcp-mss-adjust** option is set by default. It causes FortiAP to limit the maximum segment size (MSS) of TCP packets sent by wireless clients. FortiAP does this by adding a reduced MSS value to the SYN packets sent by FortiAP when negotiating with a wireless client to establish a session. This results in the wireless client sending packets that are smaller than the **tun-mtu-uplink** setting, so that when the CAPWAP headers are added, the CAPWAP packets have an MTU that matches the **tun-mtu-uplink** size. To enable, enter the required maximum byte size that the link will support before fragmentation. Start with a default value of 1500 and, if fragmentation is still an issue, reduce this value.

The **icmp-unreachable** option affects all traffic (UDP and TCP) between wireless clients and FortiAP. This option causes FortiAP to drop packets that have the *Don't Fragment* bit set in their IP header and that are large enough to cause fragmentation and then send an ICMP packet—type 3 **ICMP Destination unreachable** with code 4 **Fragmentation Needed** and **Don't Fragment was Set** back to the wireless controller. This should cause the wireless client to send smaller TCP and UDP packets.

In a LAN environment, fragmentation is not likely to be an issue because of the nature of the infrastructure. However, remotely based APs could suffer fragmentation where different WAN link configurations are used in between the AP and FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

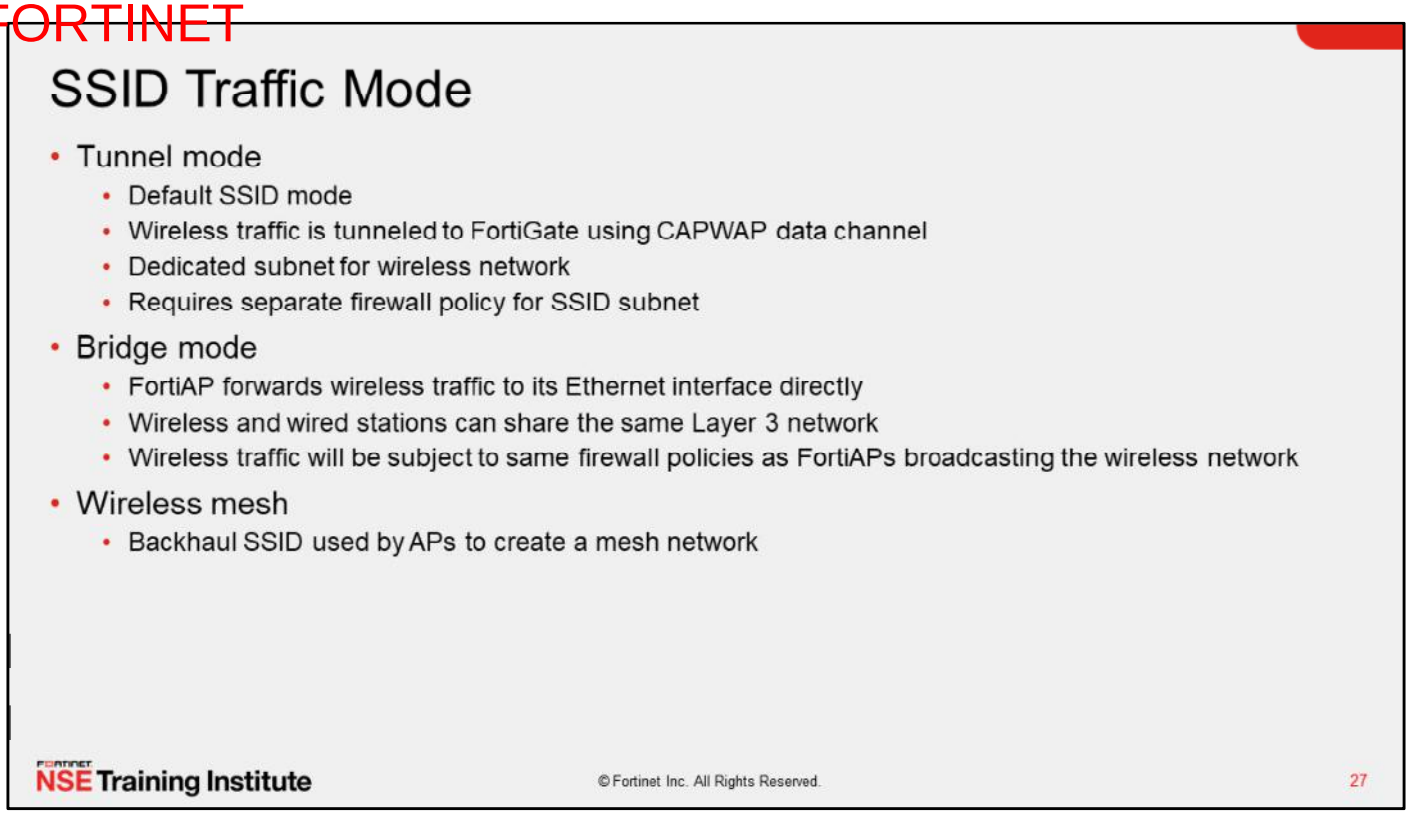
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn how to configure and broadcast SSID from a FortiGate using FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You can configure three types of SSIDs on FortiGate: tunnel mode, bridge mode, and wireless mesh.

By default, tunnel mode SSID is selected when you define an SSID on FortiGate. In this mode, all traffic within CAPWAP DTLS or non-DTLS tunnels is sent to FortiGate before it is allowed on the LAN or internet.

There are two main advantages to using this mode:

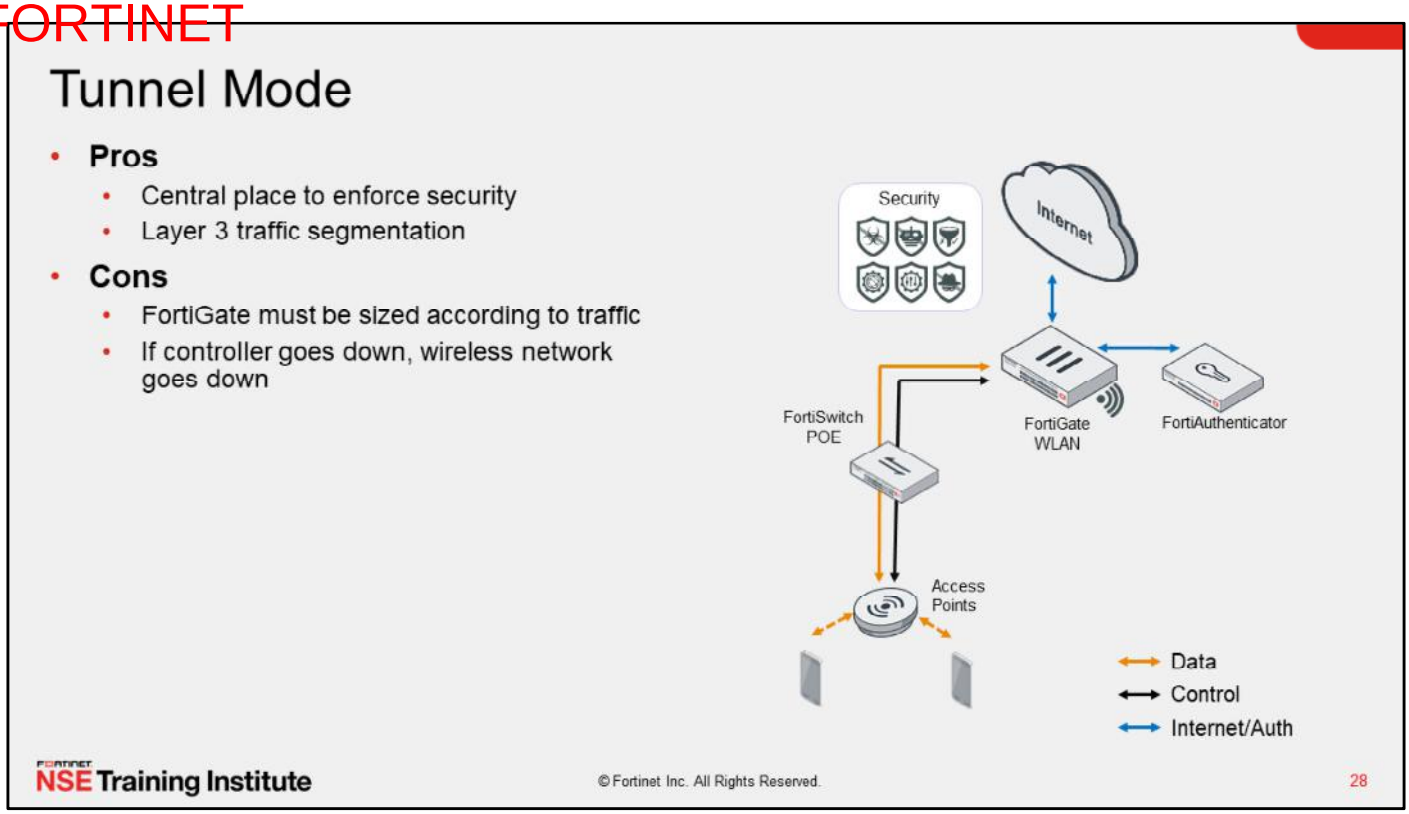
- Traffic is subject to firewall policies and security threat scanning. Traffic must go through a security profiles inspection and firewall policies examination before it is placed on the egress interface. This ensures that all security threats are addressed before a device is given access to internal or external resources.
- Traffic is processed at the session level. This gives FortiGate complete visibility of user and device activities on the network. FortiGate can track and log user activities, and control access at the user level.

In local bridge mode SSID, wireless traffic is bridged directly to the local LAN that the AP is connected to. This mode is useful when deploying APs at remote locations that connect to a wireless controller over a WAN link. To ensure all traffic is scanned for security threats, consider deploying compatible APs in this type of deployment.

Wireless mesh SSID is used strictly as a backhaul SSID to connect to the root AP in a mesh deployment.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



By default, tunnel mode SSID is selected when you define an SSID on FortiGate. In this mode, all traffic within CAPWAP DTLS or non-DTLS tunnels is sent to FortiGate before it is allowed on the LAN or the internet. There are two main advantages to using this mode:

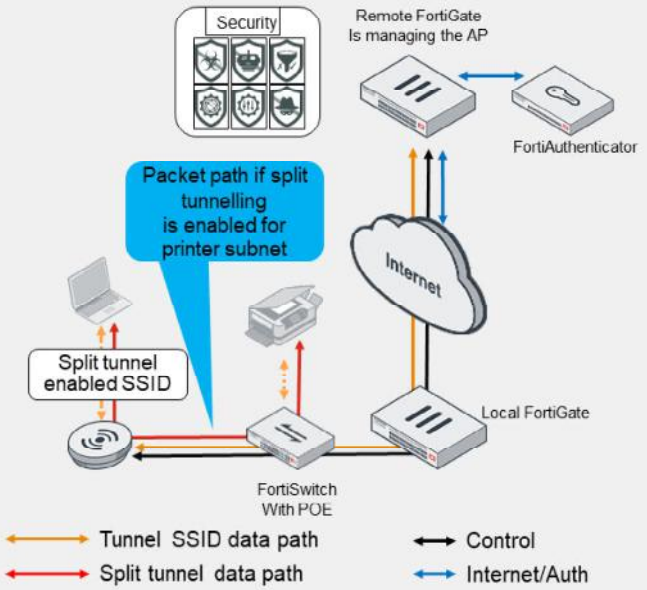
- Traffic is subject to firewall policies and security threat scanning. Traffic must go through a security profiles inspection and firewall policy examination before it is placed on the egress interface. This ensures that all security threats are addressed before a device is given access to internal or external resources.
- Traffic is processed at the session level. This gives FortiGate complete visibility of user and device activities on the network. FortiGate can track and log user activities, and control access at the user level.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Tunnel Mode—Split Tunneling

- Applies to APs deployed remotely or managed by FortiLAN Cloud
- By default, in tunnel mode, all traffic from the remote FortiAP is sent to the FortiGate Wi-Fi controller
- When split tunneling is enabled, selected traffic is sent to a local gateway, and not FortiGate
- Enabled on a per-subnet basis
- Subnets need to be defined in an ACL
  - AP subnet can be added automatically
  - Other local subnets can be added manually
  - Subnets defined in ACL will either be tunneled back to controller or locally egressed



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

29

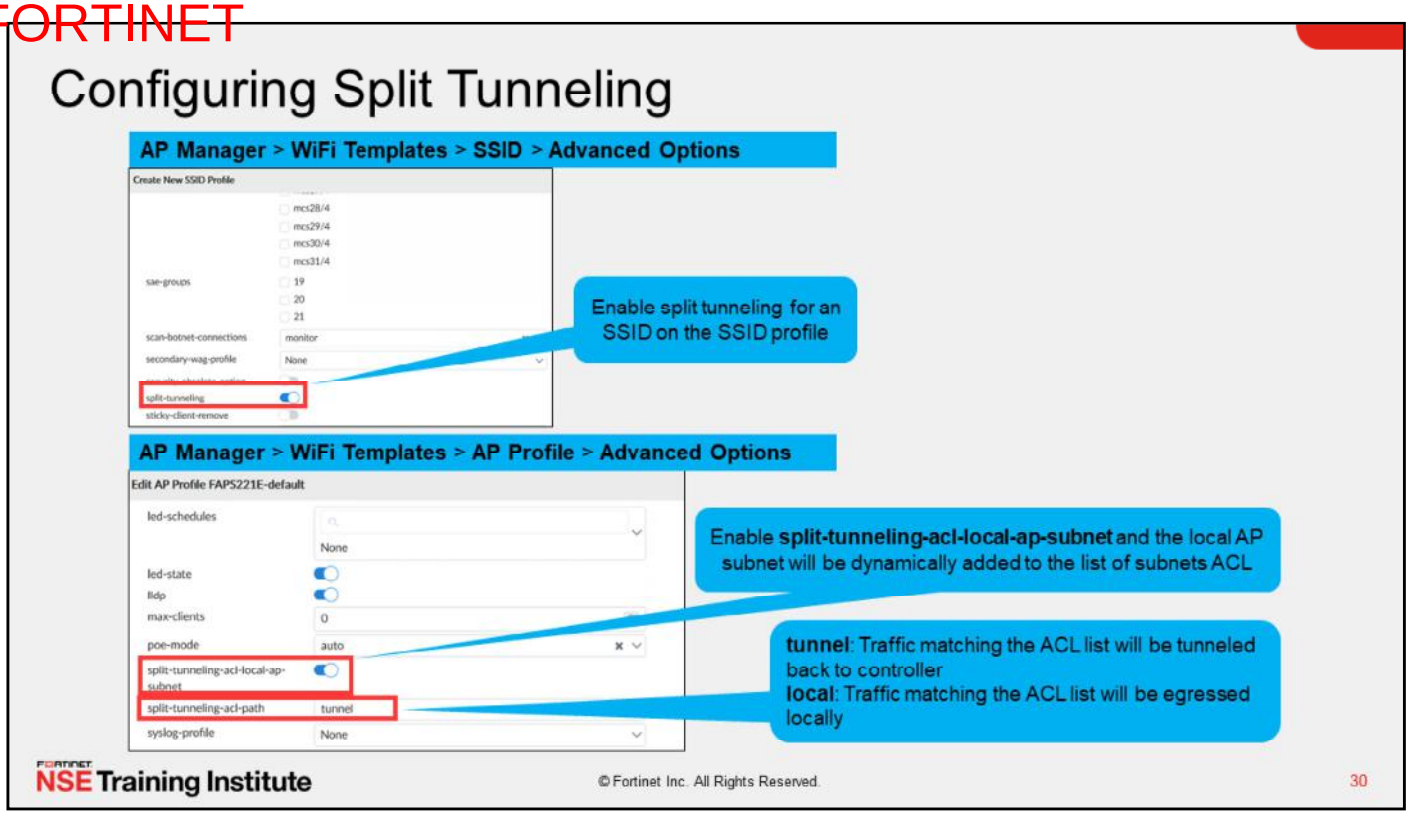
In tunnel mode, all traffic from the SSID is sent to the FortiGate Wi-Fi controller. If you locate the AP in a remote office, all the traffic is sent to FortiGate, even if it is destined for a remote office resource. The packets sent to a local resource, such as an office printer, will hairpin, crossing the WAN link needlessly.

When you enable split tunneling on an SSID profile, you can configure a different egress point for the traffic. You can *split* traffic; some traffic is sent to the local network, and some tunnels back to the managing FortiGate. Split tunneling eliminates loading FortiGate with unnecessary traffic and allows direct access to local private networks at the location of the FortiAP, even if the connection to the Wi-Fi controller goes down.

You can configure the subnets in an ACL. You then configure the ACL as the list of subnets that the SSID tunnels to, or will bridge locally. You can also configure the AP to automatically add its own subnet to the ACL.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Split tunneling is enabled on a per-SSID basis. However, split tunneling ACLs must be defined on the FortiAP profile or override settings on a per-AP basis.

The traffic is tunneled or bridged depending on the subnets configured in the **split-tunneling-acl** list. If the **split-tunneling-acl-local-ap-subnet** option is enabled, the AP's local subnet is dynamically added to the list.

When `split-tunneling-acl-path` is set to `local`, traffic matching the ACL remains local, instead of being tunneled.

If `split-tunneling-acl-path` is set to `tunnel`, `split-tunnel-acl` defines subnet(s) that will be tunneled back to the controller.

If you need to add additional subnets to the list, it has to be configured using a CLI configuration on an individual AP (or wtp). To do this, navigate to **Device Manager** > **Devices & Groups** > **CLI Configurations**. If the **CLI Configurations** option is not available, enable it from **Display Options**.

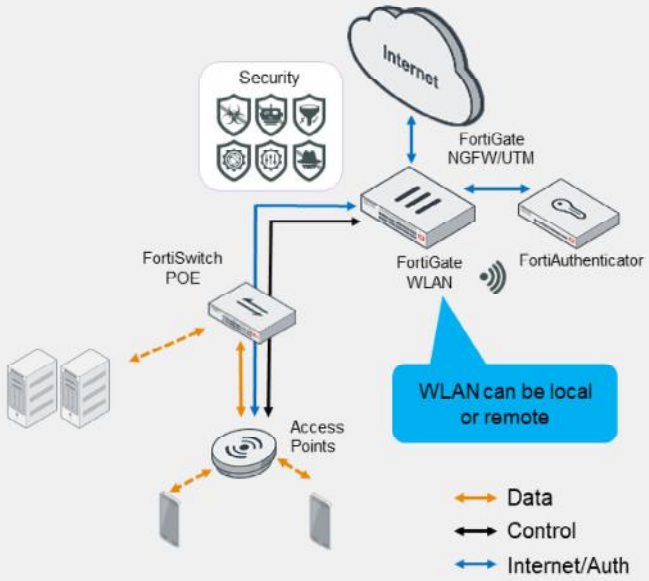
In **CLI Configurations**, navigate to **wireless-controller** > **wtp** and edit the AP requiring changes to the ACL. At the bottom of the options, you will find the **split-tunneling-acl** table where subnets can be added for this individual AP. This setting has to be applied to individual controllers and then installed using the **Install Wizard**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Bridge Mode

- **Pros**
  - Both wired and wireless stations can be in same subnet
  - Potential 1 Gbps or more (if using link aggregation on supported APs) LAN throughput per FortiAP
- **Cons**
  - Security profiles are available only with compatible APs
  - Limited VLAN pooling options



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

31

In local bridge mode SSID, wireless traffic is bridged directly to the local LAN that the AP is connected to. This mode is useful when deploying APs at remote locations, that connect to a wireless controller over a WAN link. To ensure all traffic is scanned for security threats, consider deploying compatible APs in this type of deployment.

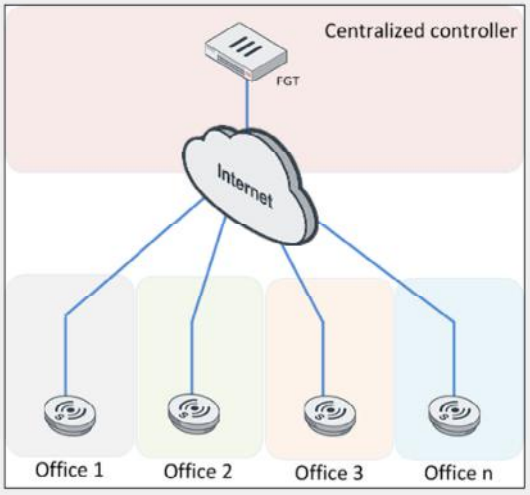
Local traffic is switched at FortiSwitch, but CAPWAP control traffic still goes to the wireless controller.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Bridge Mode—Security Profile Support

- Only available in bridge mode deployments
- Available on specific FortiAP models
- Ideal for remote deployments
  - Can also be used in complex networks
- Supports FortiGate and FortiCloud deployments
- Supported profiles:
  - AV
  - IPS
  - App control
  - Web filtering
- Requires a separate FortiGuard subscription per AP



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

32

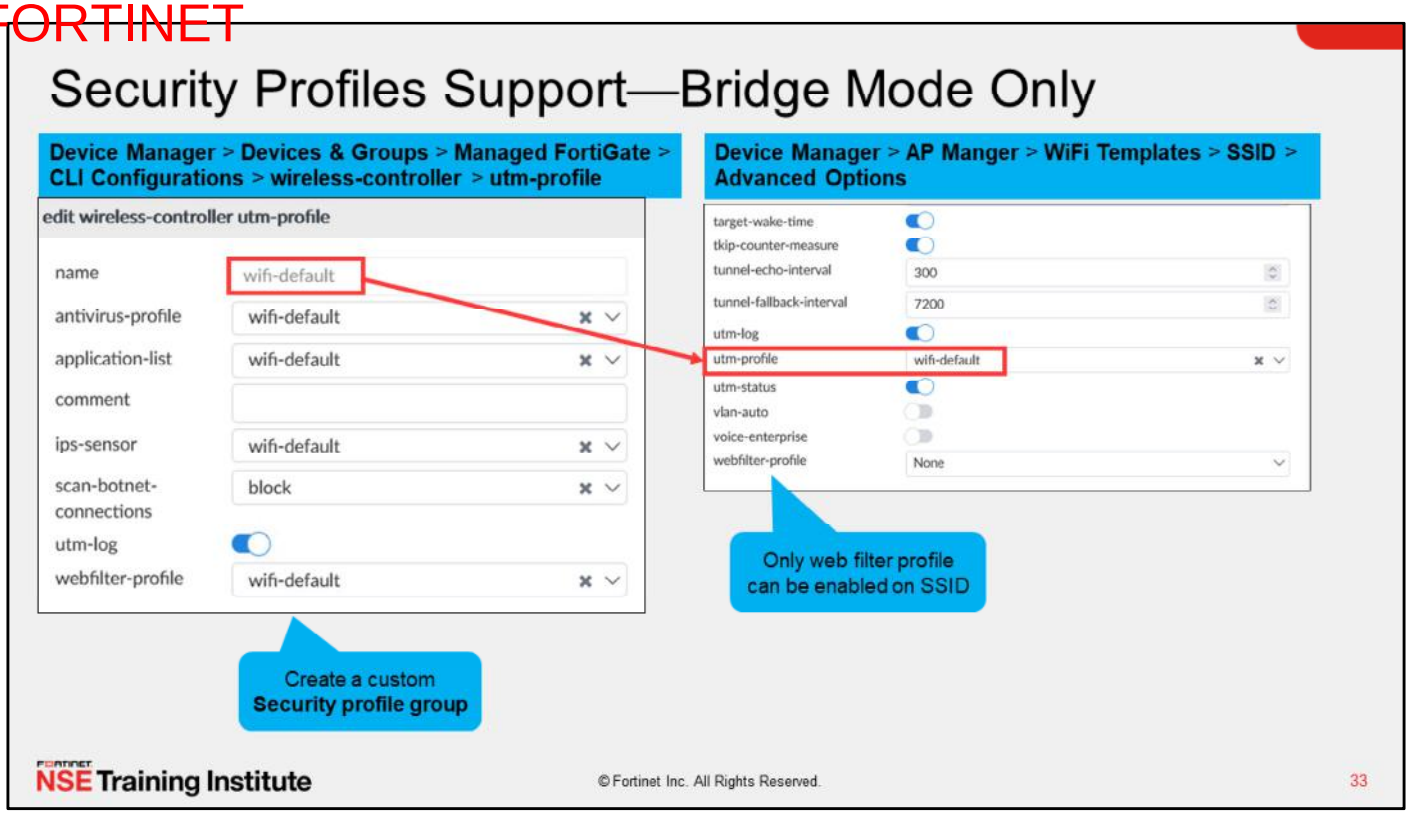
If a bridge mode SSID is configured for a managed FortiAP model which supports security profiles, you can add a security profile group to the wireless controller. This configuration allows you to apply the following security profile features to the traffic over the bridge SSID:

- Antivirus (including botnet protection)
- Intrusion prevention
- Application control
- Web filter

This is supported only in bridge mode. Tunneled SSID traffic will be inspected by FortiGate, as usual.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can create a security profile group and then apply it to an SSID. You can apply a web filter profile as a standalone security profile to an SSID, but the other security profiles can only be applied as part of a security profile group that can be applied only to a bridge mode SSID.

The security profile group is created using a CLI configuration and is applied on individual controllers. It cannot be applied using a template

Once the new or updated security profile has been installed on the controller it can be configured in an SSID profile.

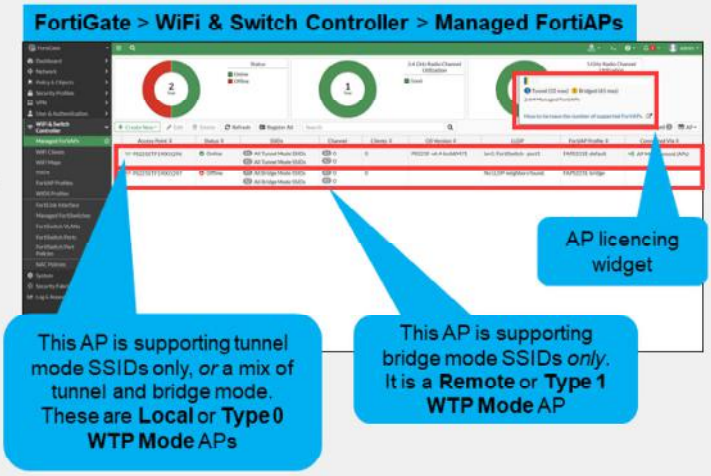
Only supported FortiAP models get security profile updates from FortiGuard by a FortiGuard subscription.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Supported Number of FortiAPs and Traffic Mode

- Controllers have a different supported number of APs for each type
  - Varies according to controller specification and type. Refer to the appropriate data sheet for the maximum number of APs supported
  - Count can be found in **Managed FortiAPs** on FortiGate
- On FortiManager, AP profiles will be deployed as:
  - **Tunnel**: Deploys tunnel networks only—causes AP to use a **Local** or **Type 0 WTP Mode** AP
  - **Bridge**: Deploys bridge mode networks only—causes AP to use **Remote** or **Type 1 WTP Mode** AP
  - **Manual**: Mix of the two—if a tunnel mode is selected, AP will become **Local** (**Type 0**)



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

34

The traffic mode used on the APs has a performance impact on the controller, and tunnel mode SSIDs will consume more resources than bridge mode. As a result, APs that transmit tunnel mode SSIDs will consume more resources at the controller. Controllers typically support different numbers of APs depending on the type of networks they broadcast, and the datasheet will include the mix of APs, listing the total number of APs supported, and then a reduced number when supporting tunneled networks.

FortiGate will display the current number of APs supported in **FortiGate** > **WiFi & Switch Controller** > **Managed FortiAPs**. Hovering over the managed text will show the total number of APs the FortiGate devices can support, how many of those can support bridged or tunneled networks, and how many are currently supported. You cannot find this number on FortiManager.

If an AP broadcasts *only* bridge mode SSIDs, it will be classified in FortiManager as a **Remote** or **Type 1 WTP Mode**. Then you will be able to support the upper number of APs quoted for FortiGate.

As soon as you configure an AP to broadcast a tunnel network, it is known as a **Local** or **Type 0 WTP Mode** AP, and you will be able to support the lower number of APs. APs that broadcast a *mix* of tunnel and bridge mode are classed as **Local Type 0 WTP Mode** APs.

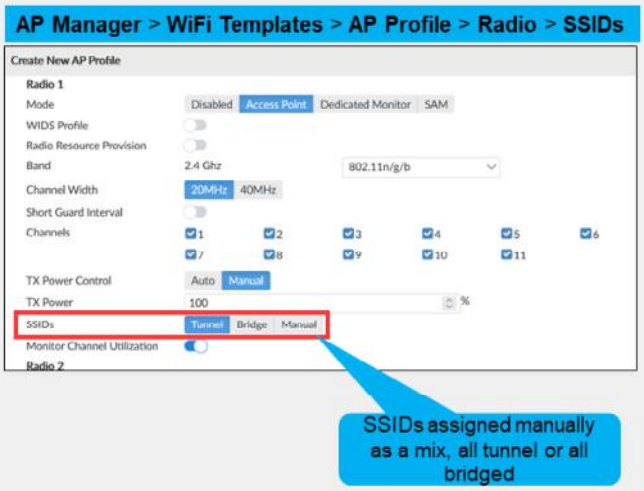
The mode the AP is using can be displayed in FortiManager by adding a **WTP Mode** column in the AP Manager under **AP Manager** > **Managed APs** > **Column Settings** > **WTP Mode**. This shows the type number. Individual APs can also be edited to view the **WTP Mode**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Configuring SSIDs With FortiManager

- SSIDs are defined using an **SSID Profile**
  - In **Central Management** mode, the profiles are available on FortiManager. A single profile is applied to multiple FortiGates
  - In **Per-device Management** mode, profiles are defined and available on FortiManager, but applied to individual FortiGate devices
- APs transmit new SSIDs when the new SSID profile is associated with the AP profile
  - **Manual** will install the SSID profile on the controller *and* broadcast the SSID
  - **Tunnel** and **Bridge** will automatically broadcast SSID profiles that are *already* installed on the controller



NSE Training Institute
© Fortinet Inc. All Rights Reserved.
35

Profiles are managed differently, depending on the management mode that you are using.

In **Central Management** mode, profiles are created and stored on FortiManager. An AP profile is distributed to a controller when at least one of its supported APs is assigned the profile *and* the device settings are installed. SSID profiles are delivered *only* when you select **Manual** in the **SSID** drop-down list.

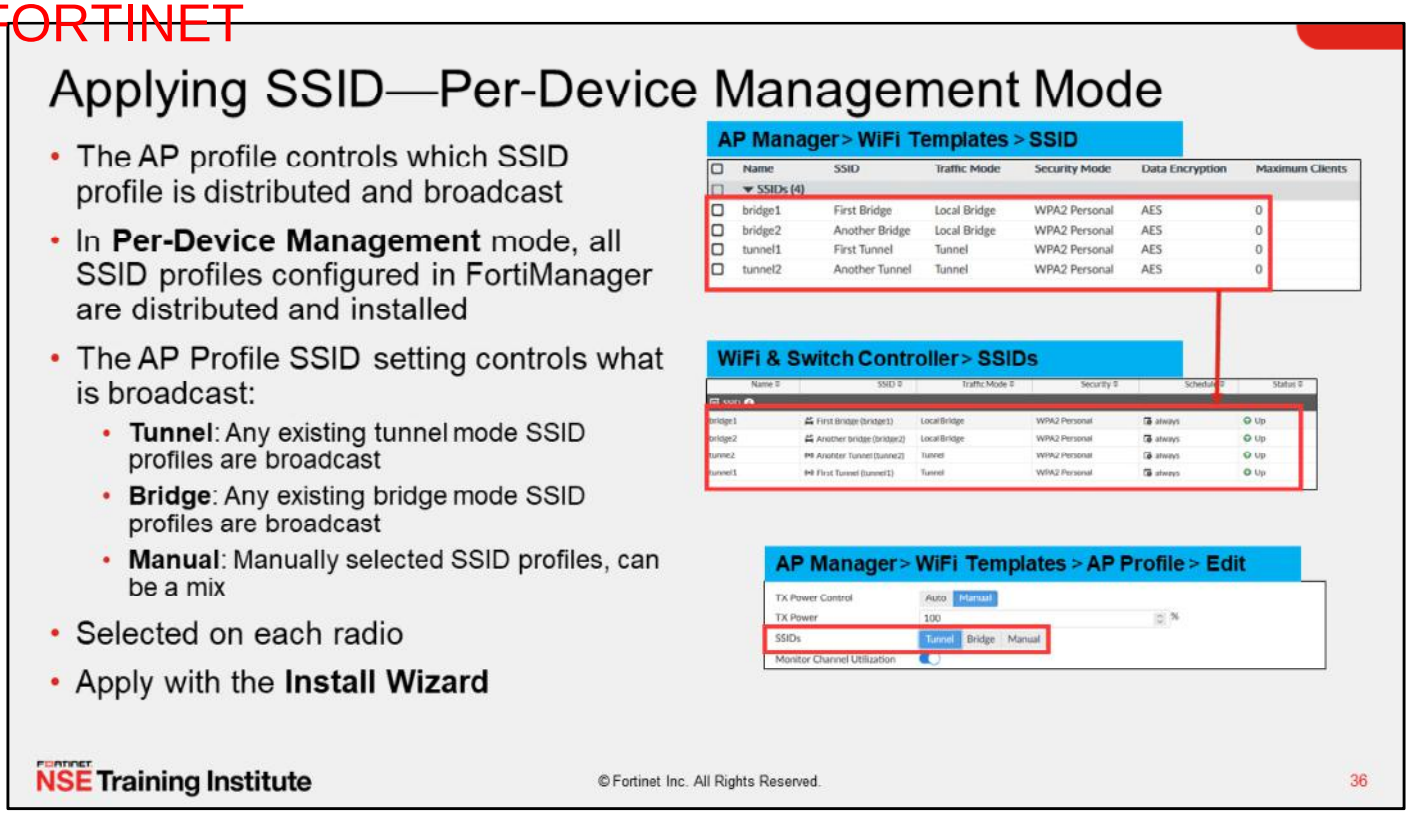
If you create an SSID profile centrally and configure all of the AP profiles to be tunnel or bridge, the SSID profile will *not* be delivered to FortiGate. FortiManager does not know which of the SSID profiles to distribute to which FortiGate. Setting **Tunnel** or **Bridge** on the AP profile instructs the AP to broadcast any *existing* tunnel or bridge SSID profile on the controller. A manual SSID explicitly tells FortiManager *which* SSID profile to broadcast on the AP and, as a result, the required SSID profile is delivered to the controller.

Other profiles, such as the **WIDS Profile,** are distributed when referenced.

In **Per-device Management** mode, profiles are created and stored on FortiManager. You specify profiles on a per-controller basis, FortiManager automatically distributes all profiles, regardless of whether they are used or not.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



There are differences in how wireless networks are published when using the two ADOM management modes.

In **Per-device Management** mode, you manage each FortiGate individually. Profiles are unique to each FortiGate but stored centrally on FortiManager. When you create an SSID profile in **Per-device Management** mode, you are creating for a specific FortiGate, and FortiManager knows this.

When you create profiles for a controller and when you install the device settings, FortiManager will automatically push them all to FortiGate regardless of whether they are used or not.

When you want to broadcast an SSID, you need to configure the AP profile that is being used by the APs that are to transmit it. You can broadcast SSIDs on a per-interface basis; each interface has an **SSIDs** option that can you can set to one of three modes:

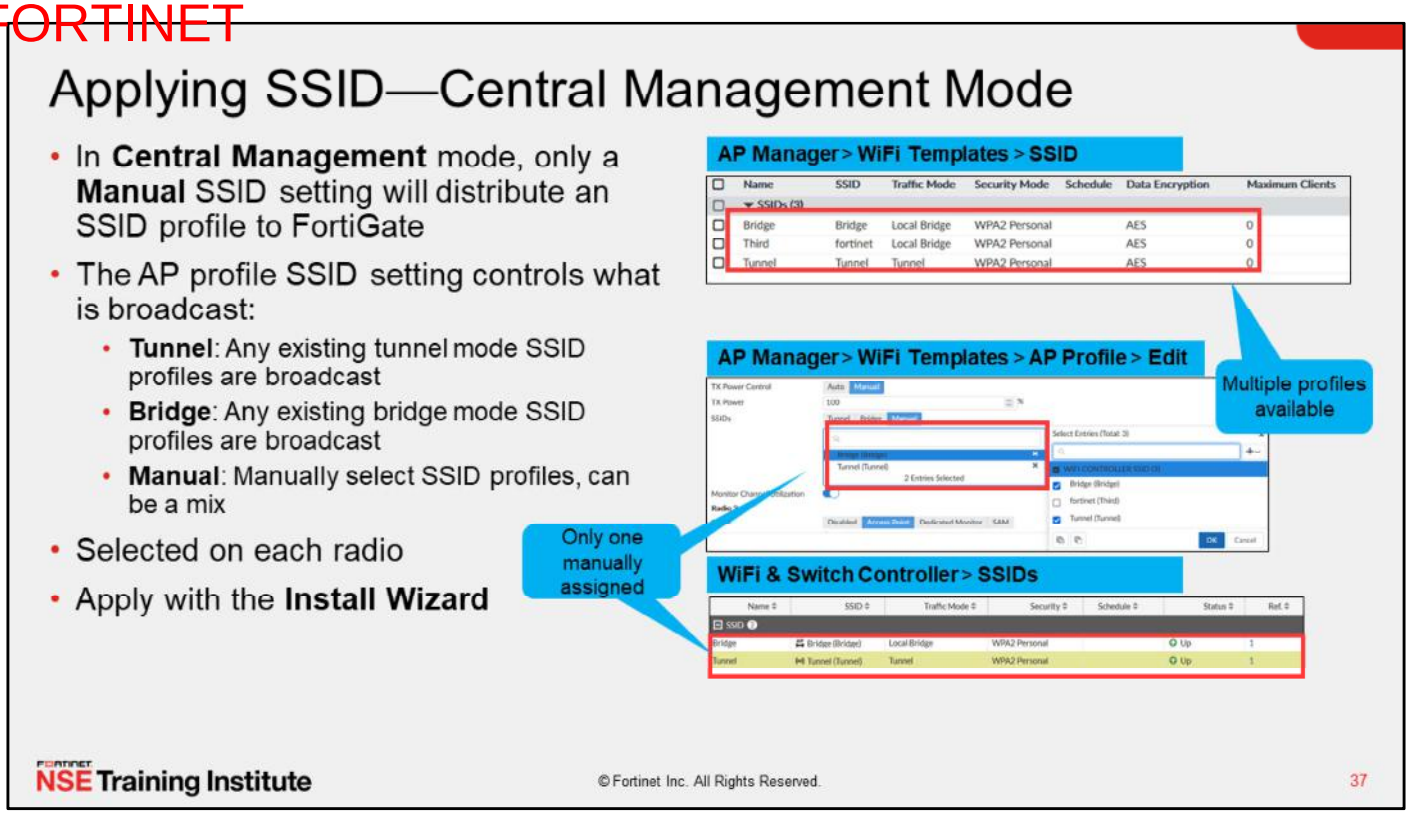
Tunnel: Any tunnel mode SSID profiles installed on FortiGate will broadcast.
Bridge: Any bridge mode SSID profiles installed on FortiGate will broadcast.
Manual: You can select a mix of SSIDs to broadcast.

Where you have the same model of AP broadcasting different combinations of SSID, you will need to clone or create separate AP profiles.

To make the profile changes active, they need to be installed on FortiGate using the **Install Device Settings** option in the **Install Wizard**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



When you create profiles in **Central Management** mode, you are creating profiles that you can apply to multiple controllers. They are stored on FortiManager, but FortiManager will not know which FortiGate will need which profiles. As a result, by default, no profiles are pushed to FortiGate when using the **Tunnel** or **Bridge** options.

The profiles are pushed when you make a specific link between an AP and an SSID. You do this by defining a manual SSID mapping in an AP Profile. The **Tunnel** and **Bridge** options will still work for any SSID profiles that are *already* on FortiGate, but these options will not cause all the profiles that exist on FortiManager to be pushed. In a sizeable FortiManager installation, a large number of SSID profiles can exist. Automatically pushing all of these profiles to each FortiGate, would not be desirable.

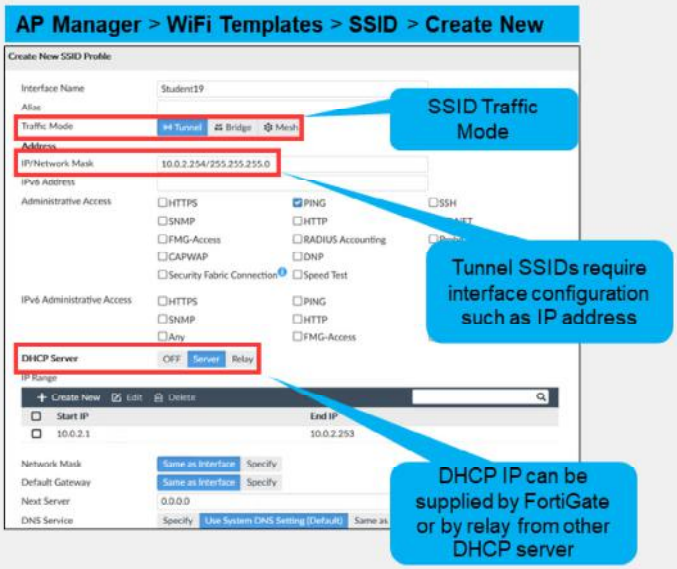
Older versions of FortiOS use a slightly different SSID assignment mechanism. **Auto** would automatically assign all tunnel mode SSID profiles, while **Manual** would allow a manual selection.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Configuring Tunnel SSIDs

- **Central Configuration** or **Per-Device Configuration** modes
- SSIDs are created as tunnel, bridge, or mesh:
  - Traffic mode cannot be changed
  - Interface name cannot be changed
- Tunnel SSID is treated as a separate virtual interface:
  - IP/network mask is required
  - Appropriate firewall policy needed
- DHCP services can be supplied using FortiGate DHCP server or relay to another third-party DHCP server
  - DHCP scope is automatically provisioned when SSID profile is applied to the FortiGate



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

38

The creation of tunnel mode SSID profiles is the same for both modes of management; however the interface for creating profiles differs slightly.

After you create the SSID profile, you *cannot* change the traffic mode or interface name. To do this, you will need to delete and recreate the profile.

Tunnel SSID is treated as a separate virtual interface on FortiGate. Because of this, you must configure the IP address, mask, and an appropriate firewall policy, before clients can connect to the tunnel SSID and pass traffic.

You may want to consider adding administrative access services, depending on your requirements.

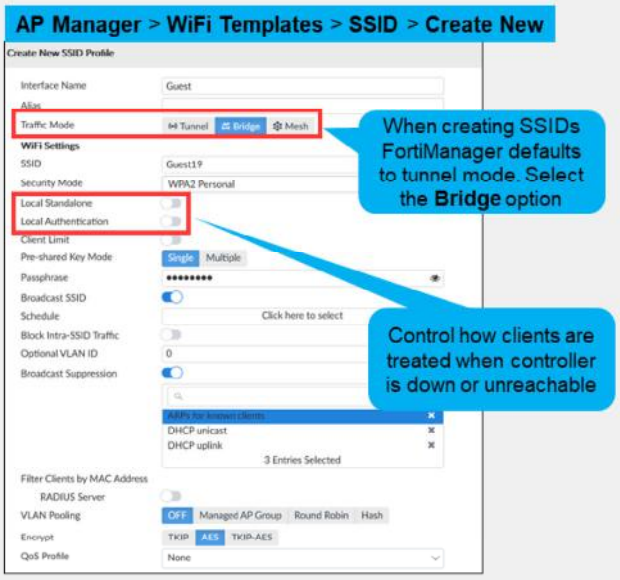
Clients attaching to a tunnelled SSID will require an IP address. This can be supplied by enabling the onboard DHCP server and either enabling a local scope or enabling DHCP relay to another third-party server.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Configuring Bridge SSIDs

- Bridge mode has many fewer options
- No requirement for IP or policy as traffic is egressed from the AP wired port
- Options to allow clients to connect or stay connected in the event of controller outage
  - Available only on bridged networks



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

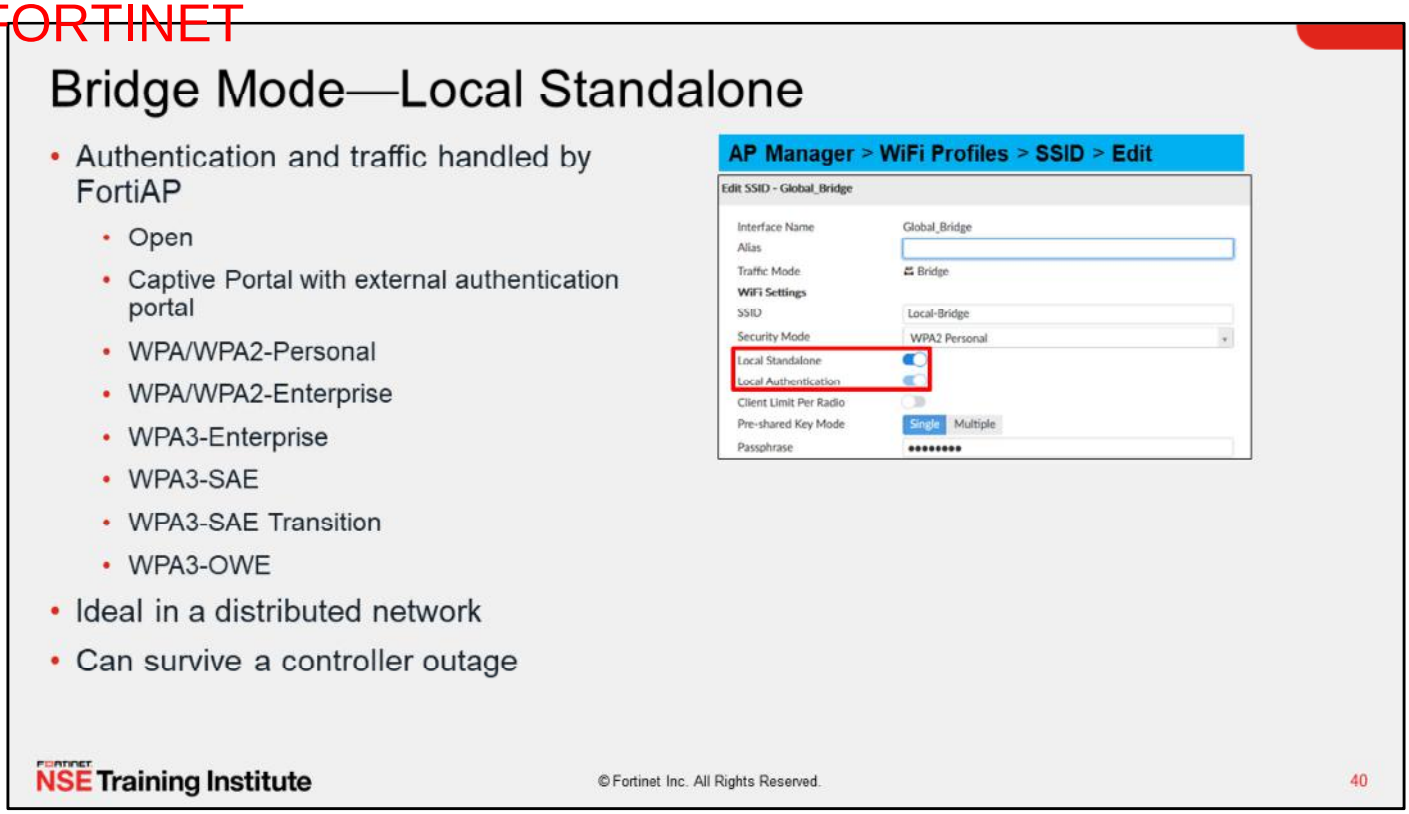
39

Bridge modes SSID are significantly easier to configure because they simply bridge the wireless traffic to the local Ethernet interface.

Additional options that you will see here control what happens to the wireless connection, if the FortiGate wireless controller becomes unavailable. There are options to allow clients to connect and authenticate locally, in the event the controller becomes unavailable.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The wireless controller, or the connection to it, might occasionally become unavailable, especially when FortiAPs are deployed remotely or over a congested network. During such an outage, clients already associated with a bridge mode FortiAP device can continue to have network access. Optionally, FortiAP can also continue to authenticate users, if the SSID meets these conditions.

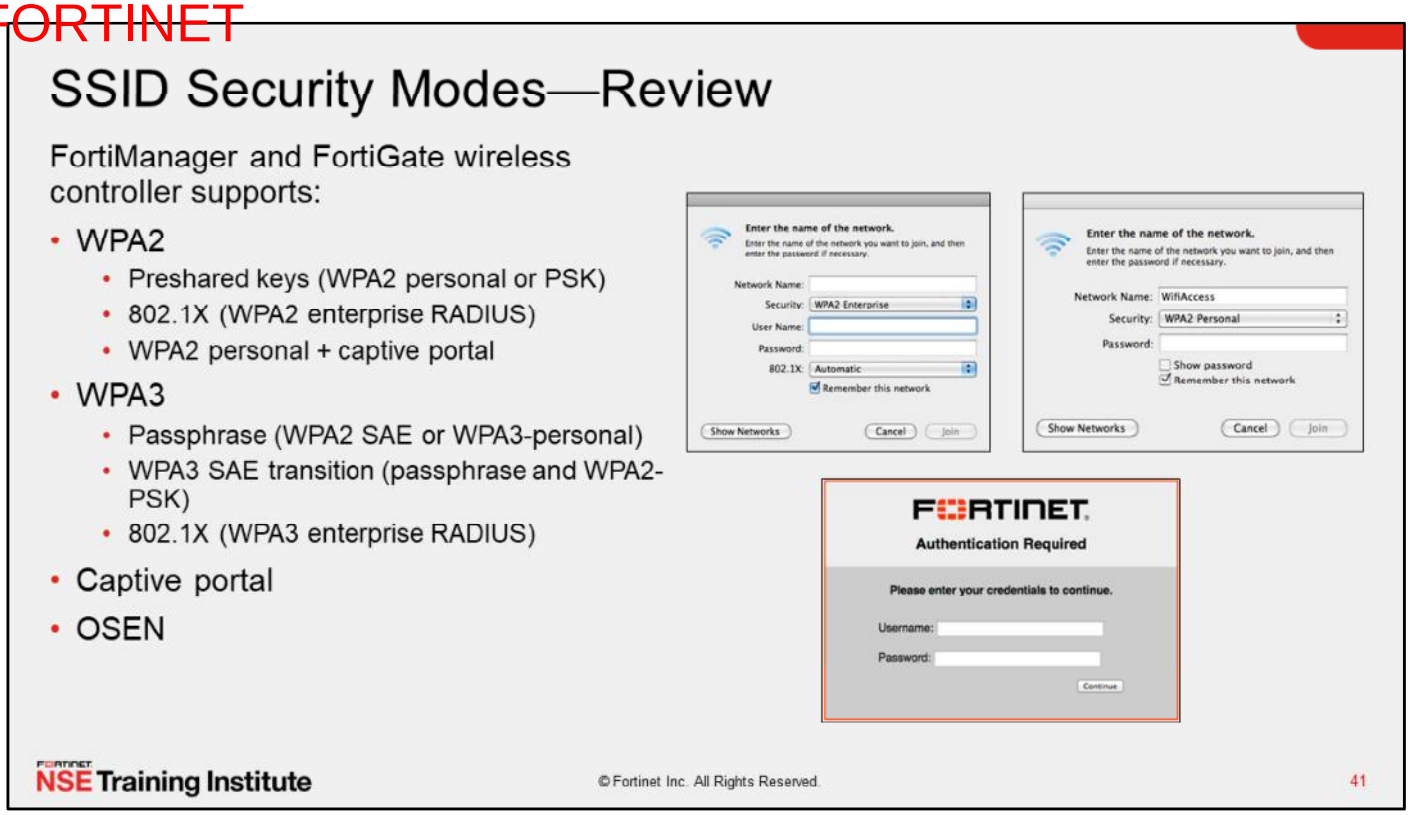
Authentication and traffic is handled by FortiAP, regardless of the connection status between FortiAP and FortiGate. Authentication methods have expanded to include:

- Open
- Captive Portal with external authentication portal
- WPA/WPA2-Personal
- WPA/WPA2-Enterprise
- WPA3-Enterprise
- WPA3-SAE
- WPA3-SAE Transition
- WPA3-OWE

This assumes that the AP can reach the required captive portal or authentication server.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Configuring the SSID profile requires the setup of the security mode. Security modes are settings for client authentication and traffic encryption between the wireless client and the AP. Remember, wireless is a shared medium, so there are even more vectors of attack than for wired connections. The FortiGate wireless controller supports multiple authentication methods:

- Username and password (WPA2/WPA3 enterprise or captive portal)
- Pre-shared keys (WPA2 personal)
- Simultaneous authentication of equals (WPA3 SAE)

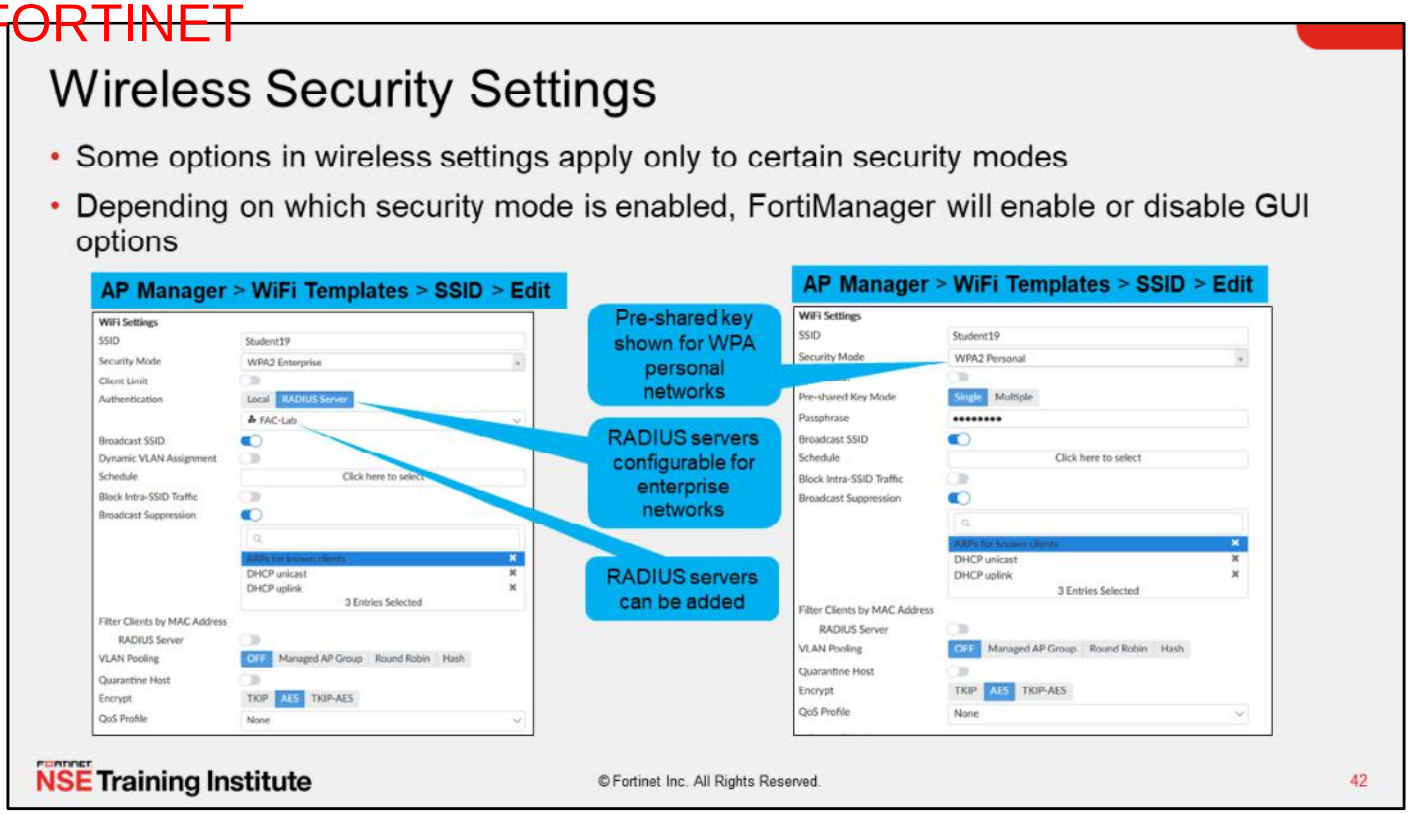
Alternatively, if you need to provide guest access without authentication, you can use captive portal as the security mode and disclaimer only as the portal type. Here is a complete list of supported formats:

- Captive portal: user authentication only and no connection encryption
- WPA2 personal: static pre-shared key-based authentication and AES connection encryption
- WPA2 personal with captive portal: key-based connection encryption and user authentication
- WPA2 enterprise: RADIUS-based user authentication and connection encryption
- WPA3 enterprise: RADIUS-based user authentication and connection encryption
- WPA3 SAE or officially referred to as WPA3 personal
- WPA3 SAE transition
- Completely unencrypted and unauthenticated
- OSEN: secure on-boarding used for hotspot 2.0

WPA3 SAE transition mode is a temporary stepping stone that allows support of both WPA3-SAE and WPA2-PSK on the *same* SSID. The older WPA standards (based on TKIP) are no longer supported. The open network option will be available only if enabled in feature visibility.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



It is important to note that, depending on the settings configured, FortiManager will hide or display applicable settings on the GUI automatically.

For example, if **WPA2 Personal** security mode is selected, FortiGate will not display the option to configure authentication and show only the options for pre-shared keys.

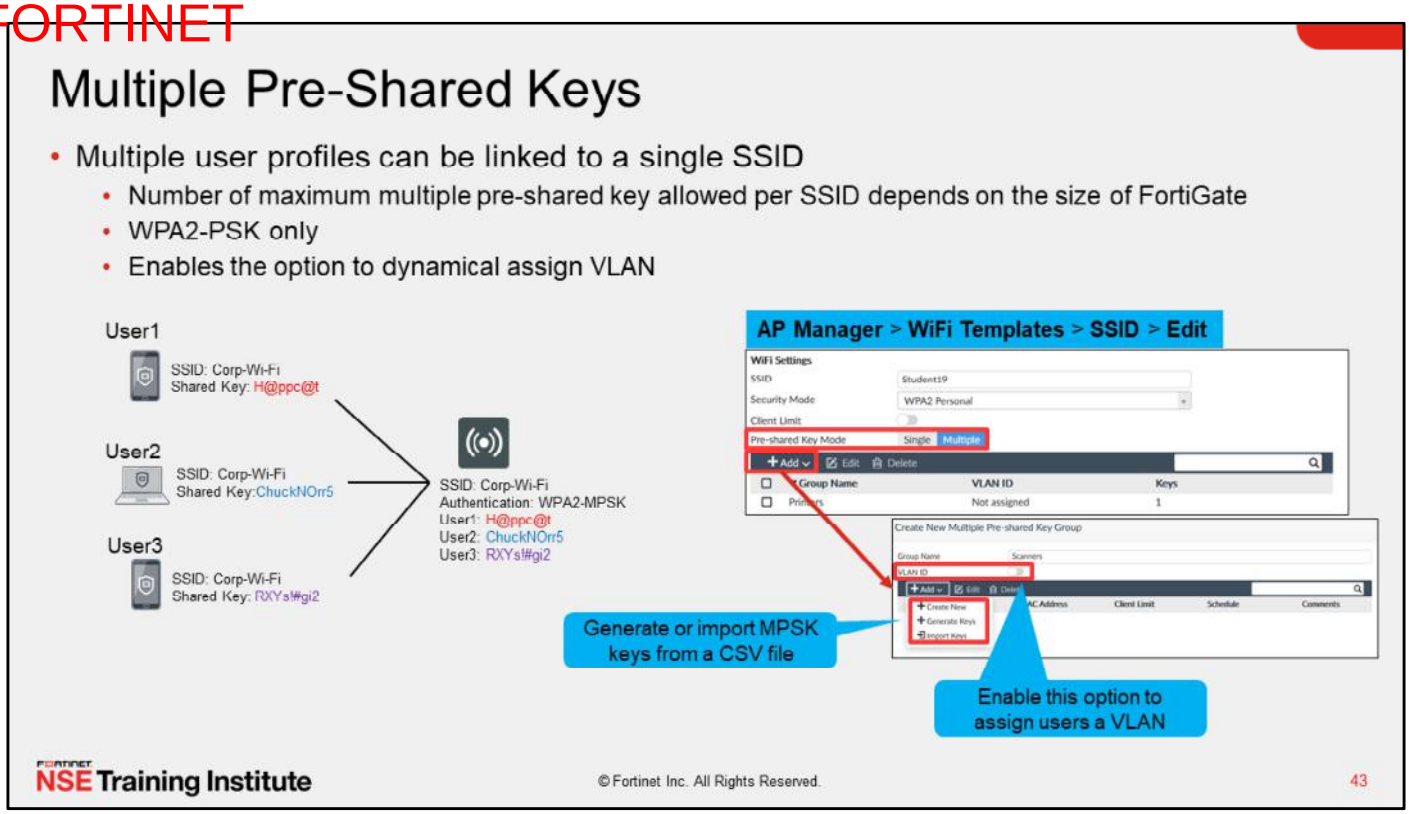
This also applies to options such as local or RADIUS authentication, multiple pre-shared keys, and so on, that are available only for the WPA2 personal option.

Some elements of additional configuration, for example, the RADIUS server entry shown on the slide, are directly configurable for the interface. The additional configurations set up here will be applied when the profile is applied to the controller using the Install Wizard. If you configure a RADIUS server entry here, as part of an SSID configuration, it will not be removed if the SSID profile is subsequently removed. It will remain configured at FortiGate.

The RADIUS server can also be configured as a separate item as part of a CLI configuration. This is defined by configuring an entry using **Device Manager** > **Device & Groups** > **Device** > **CLI Configurations** > **user** > **radius**.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



As an extension of the original PSK standard, it is possible to enable multiple PSKs (MPSK) for a wireless network. MPSK allows the use of multiple security keys to allow access to the *same* wireless network. Traditionally, pre-shared key networks would only allow one key. It often meant that these keys became well known and, as a result, the administrator could lose control over who had access to the network.

Enabling MPSK allows the wireless controller to dynamically assign a VLAN to each group based on its key and, if configured, based on the MAC address.

MPSK can make key management more straightforward because all users and devices have unique credentials. If a user leaves, a device is lost, or if a key becomes well-known, you can change the multiple pre-shared key for that one user or device without having to change all devices that connect to that network. It is also possible to limit the number of times each MPSK is used, which can now limit the number of devices that can use that key to connect to the network.

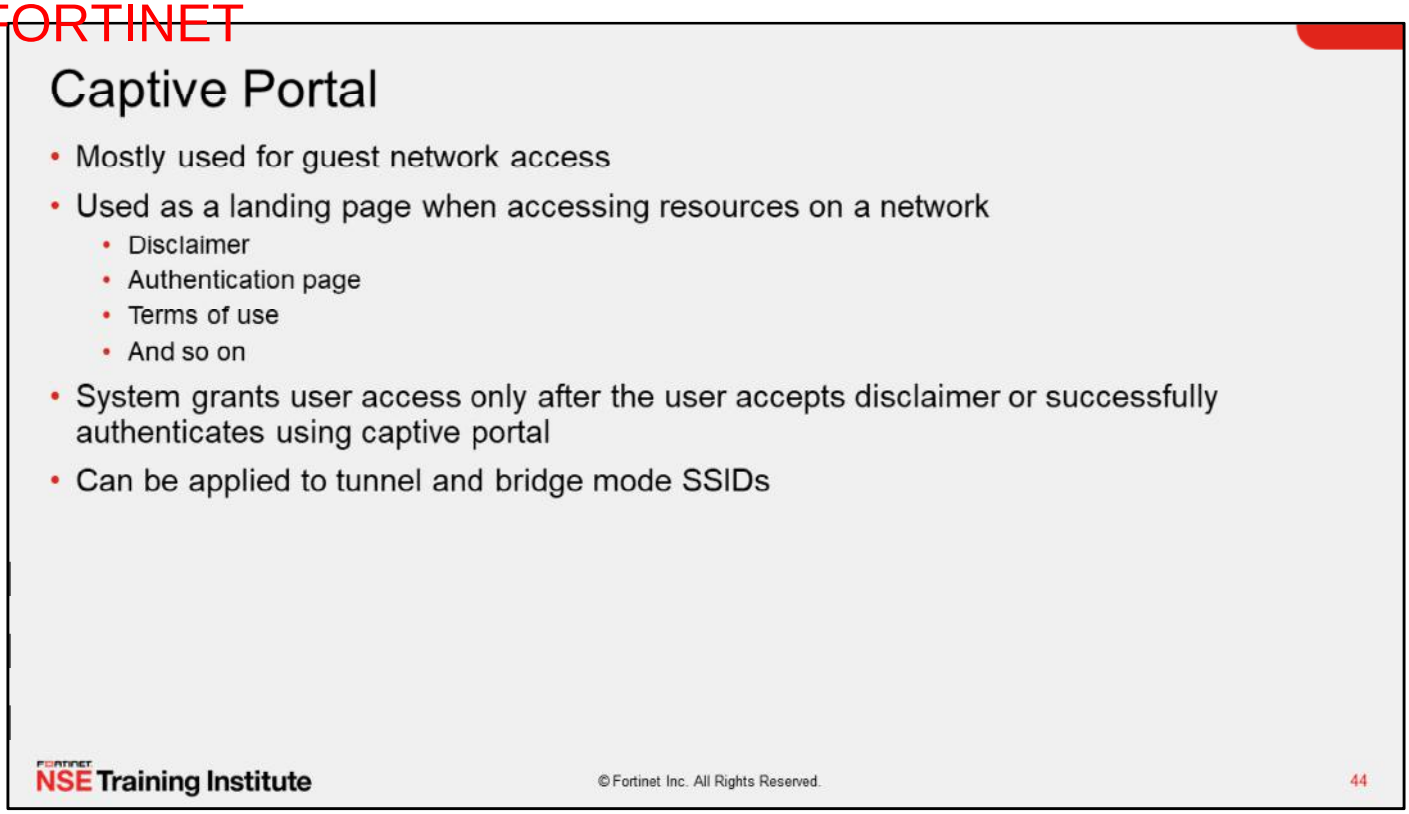
The number of PSKs allowed depends on the specification of FortiGate.

You can generate the keys for each user connecting or import the keys from a CSV file.

The MPSK can be configured centrally from FortiManager using an SSID profile but is available only on wireless networks that allow WPA2-PSK authentication.

Vouchers & Dumps are Available | WhatsApp +201224560923

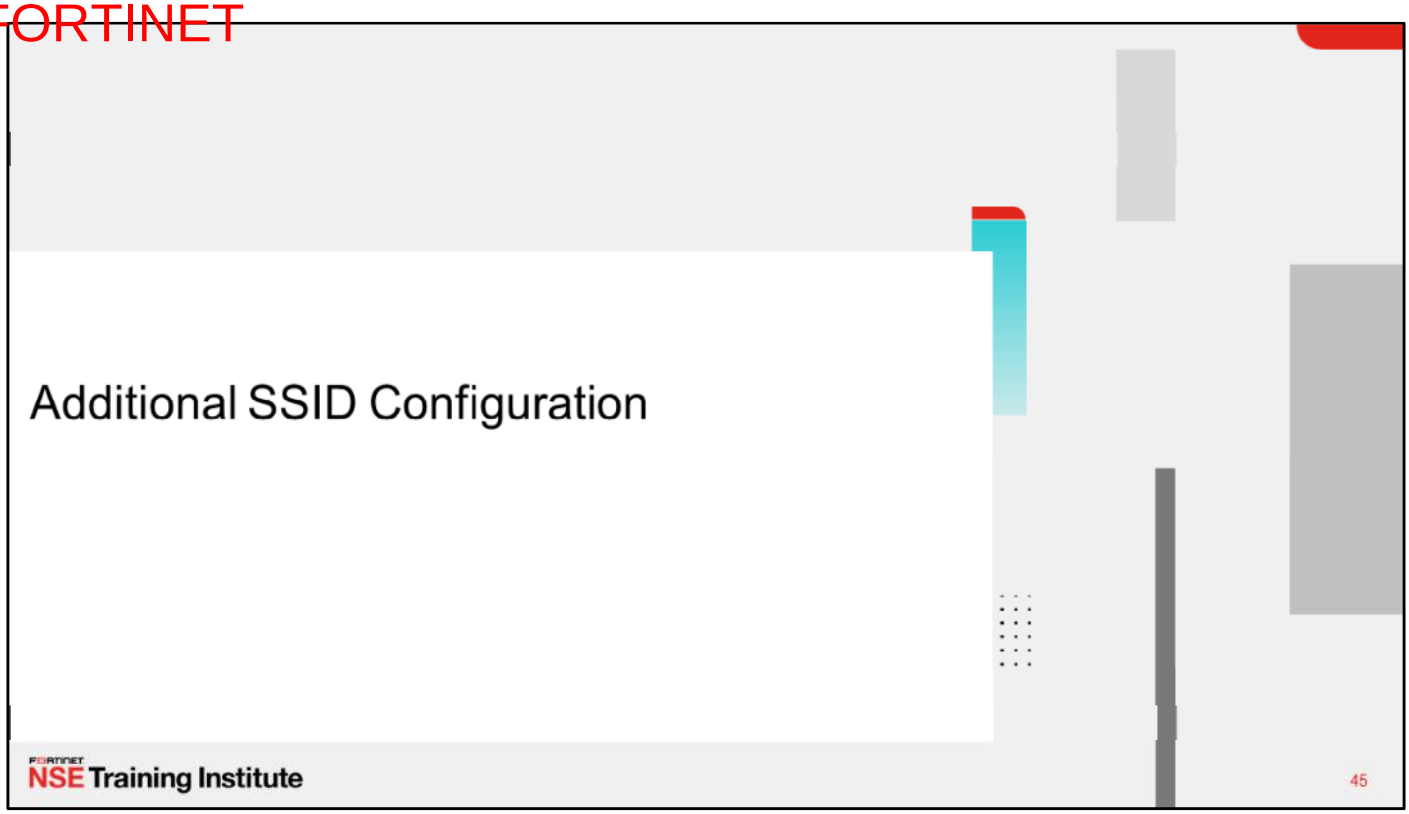
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The captive portal is used as a landing page after a user connects to a network. This is mostly used for guest access and networks that require a disclaimer. You can also authenticate your users on a captive portal page that requests the user's name and password. Until the user authenticates successfully, the authentication page is returned in response to any HTTP request. After successful authentication, the user accesses the requested URL and can access other web resources, as permitted by security policies. Optionally, the captive portal itself can allow web access to only the members of a specified user group.

Vouchers & Dumps are Available | WhatsApp +201224560923

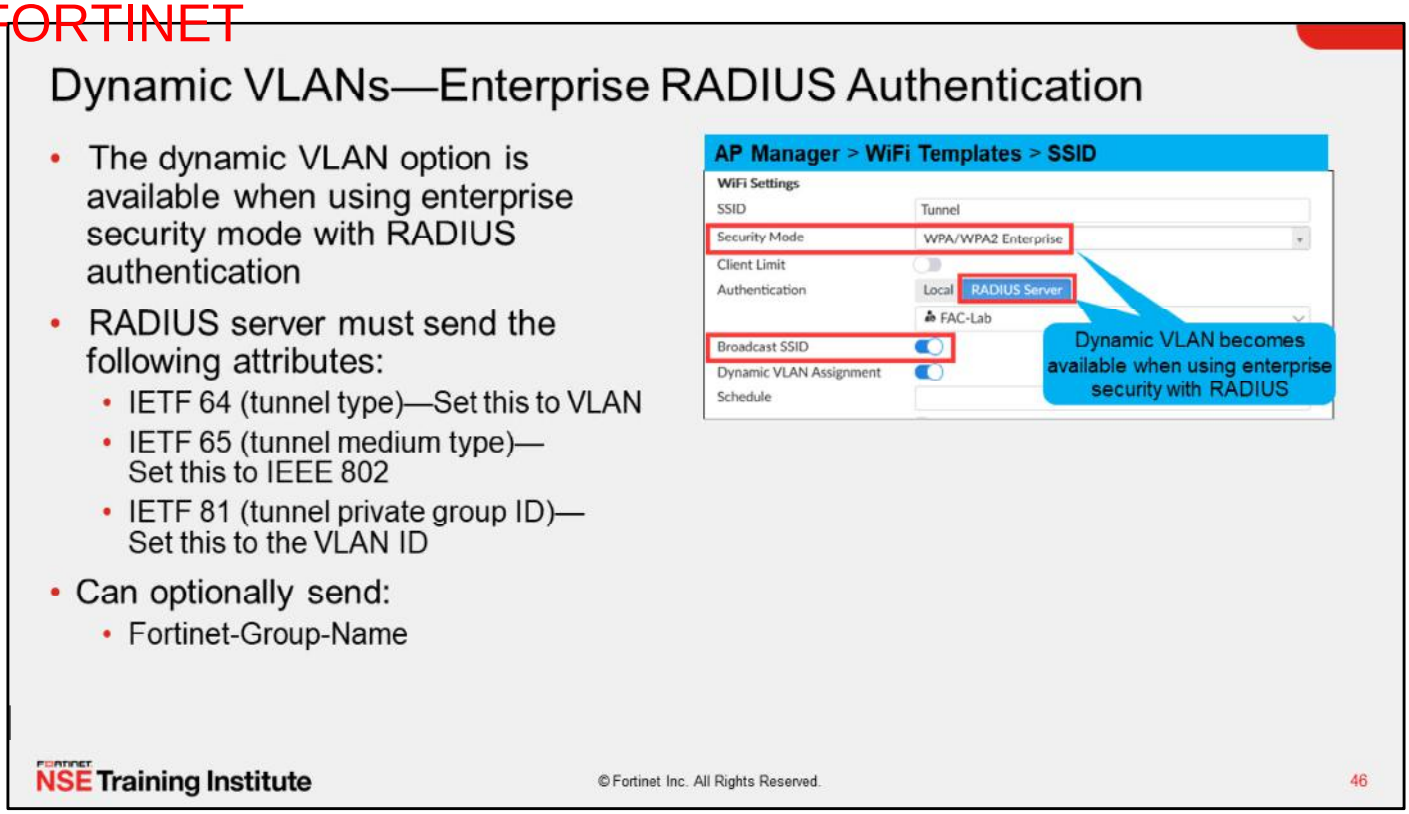
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn how to configure some additional, optional wireless network features using FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The option to add dynamic VLANs to SSID is available on FortiGate in both tunnel and bridge mode. You can apply a dynamic VLAN to SSIDs in which **WPA2 Enterprise** or **WPA3 Enterprise** have been selected in the **Security Mode** drop-down list, and **RADIUS Server** has been enabled in the **Authentication** field.

The RADIUS server is responsible for sending all the required attributes after a successful authentication. The RADIUS server must send the following attributes to FortiGate:

- IETF 64 set it to VLAN: This attribute tells FortiGate that VLAN information is attached to the RADIUS response.
- IETF 65 set it to IEEE 802: This attribute tells FortiGate that the IEEE 802 attribute is attached to the RADIUS response.
- IETF 81 set it to VLAN ID: This attribute tells FortiGate to attach the user to the specified VLAN ID interface.

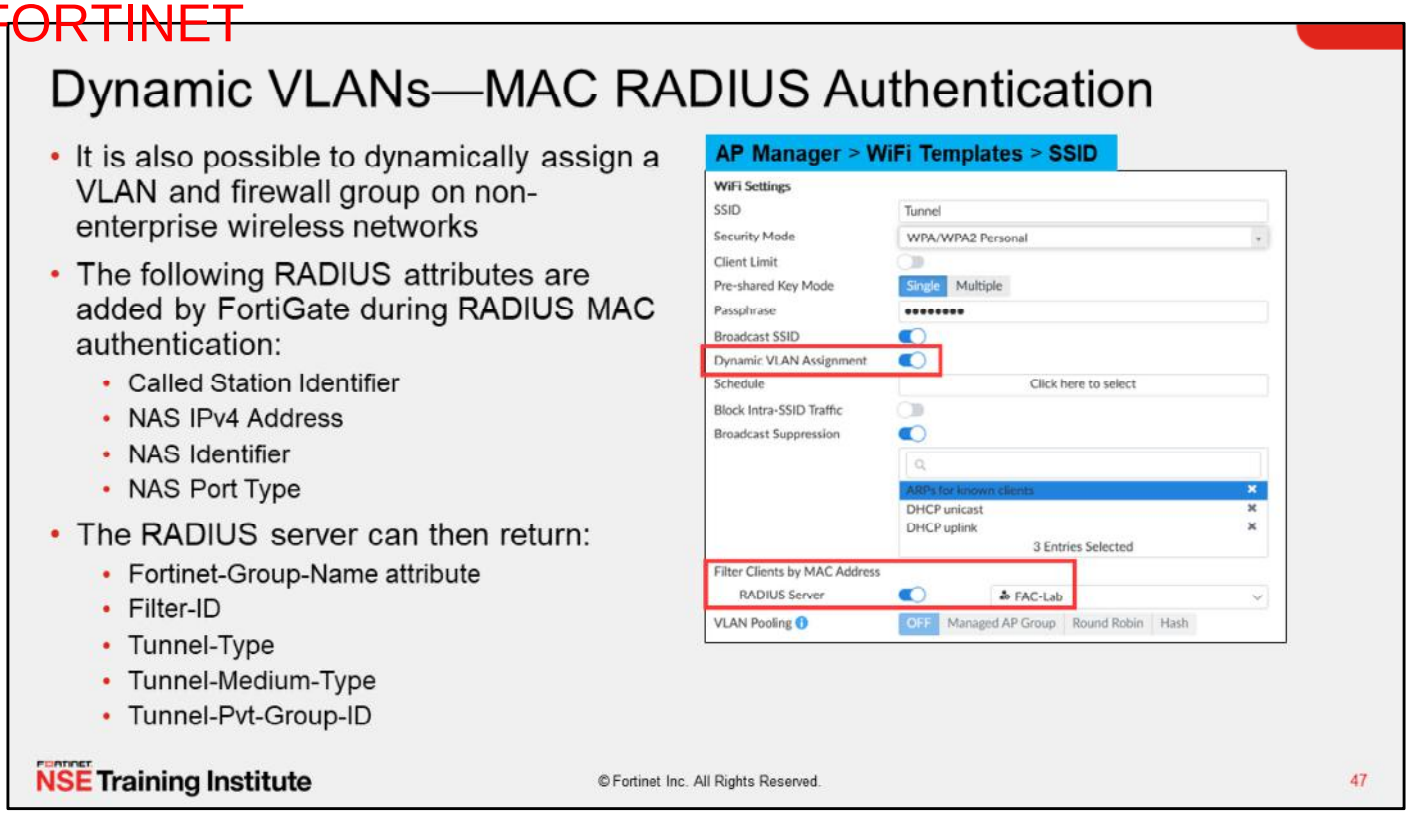
The RADIUS server can then pass back the following optional attributes as part of the RADIUS accept response.

- Fortinet-Group-Name attribute
- Filter-ID
- Tunnel-Type
- Tunnel-Medium-Type
- Tunnel-Pvt-Group-ID

You must configure all the VLANs on FortiGate along with corresponding firewall polices either directly or by using FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



It is also possible to add dynamic VLANs to a non-enterprise network. Traditionally, open or pre-shared key networks did not allow for the dynamic allocation of VLANs. But, MAC filtering using RADIUS, it is now makes it possible to pass back the following attributes to the RADIUS server when authenticating clients using their MAC addresses:

- Called Station Identifier
- NAS IPv4 Address
- NAS Identifier
- NAS Port Type

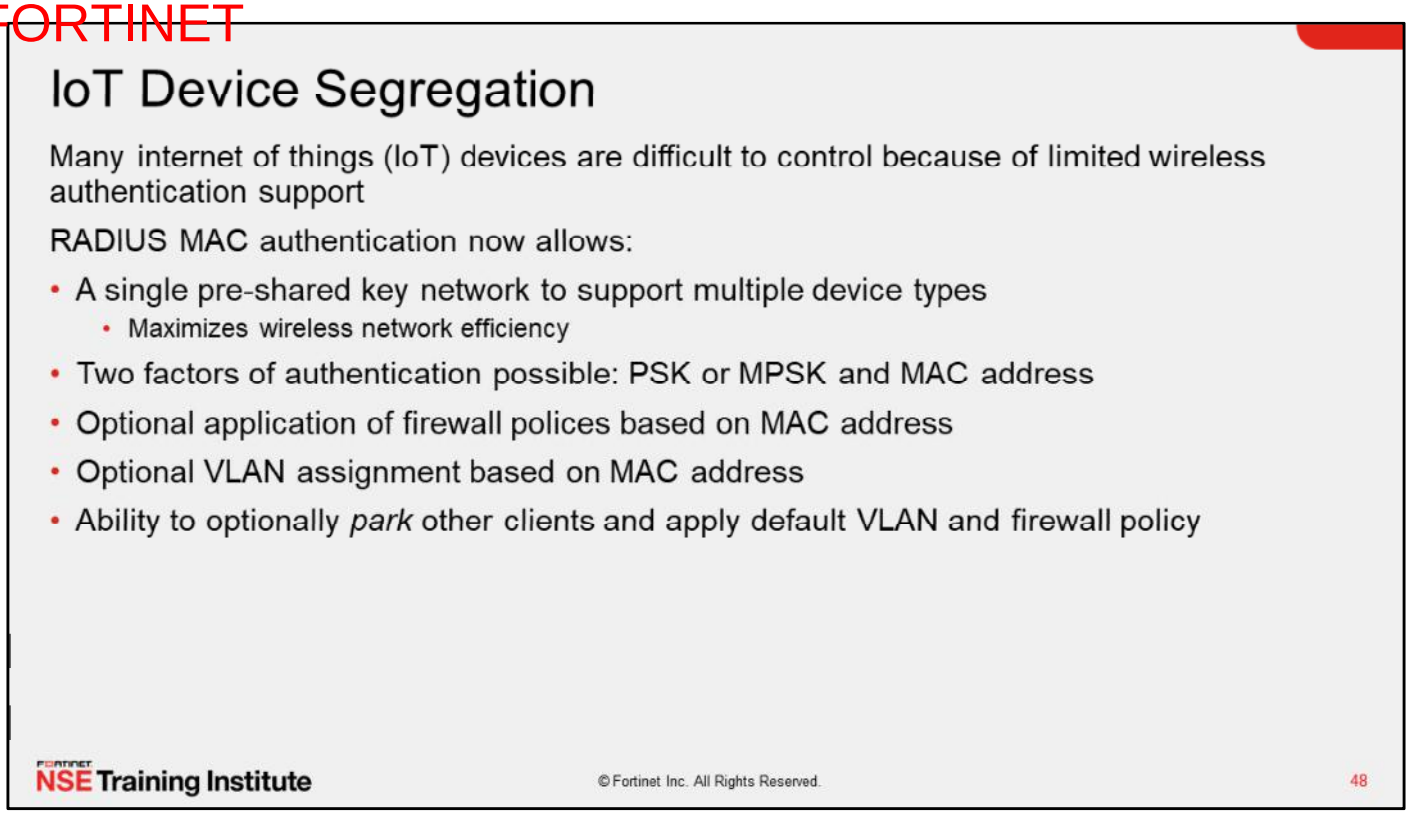
This allows the RADIUS server to authenticate a device using its MAC address and a pre-shared key, resulting in two factors of authentication. The RADIUS server can then pass back the following optional attributes as part of the MAC authentication RADIUS response:

- Fortinet-Group-Name attribute
- Filter-ID
- Tunnel-Type
- Tunnel-Medium-Type
- Tunnel-Pvt-Group-ID

This allows the client to be assigned a VLAN and a Fortinet group name attribute to allow dynamic VLANs and dynamic firewall policies.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Many simple IoT devices are not capable of supporting a full WPA2 enterprise supplicant. Many smart plugs, thermostats and other wirelessly connected devices support connecting to a wireless network using a pre-shared key. While this level of security may be sufficient for small home-based networks, in enterprise environments with many devices, using only a single pre-shared key can be a significant issue to manage and troubleshoot IoT devices.

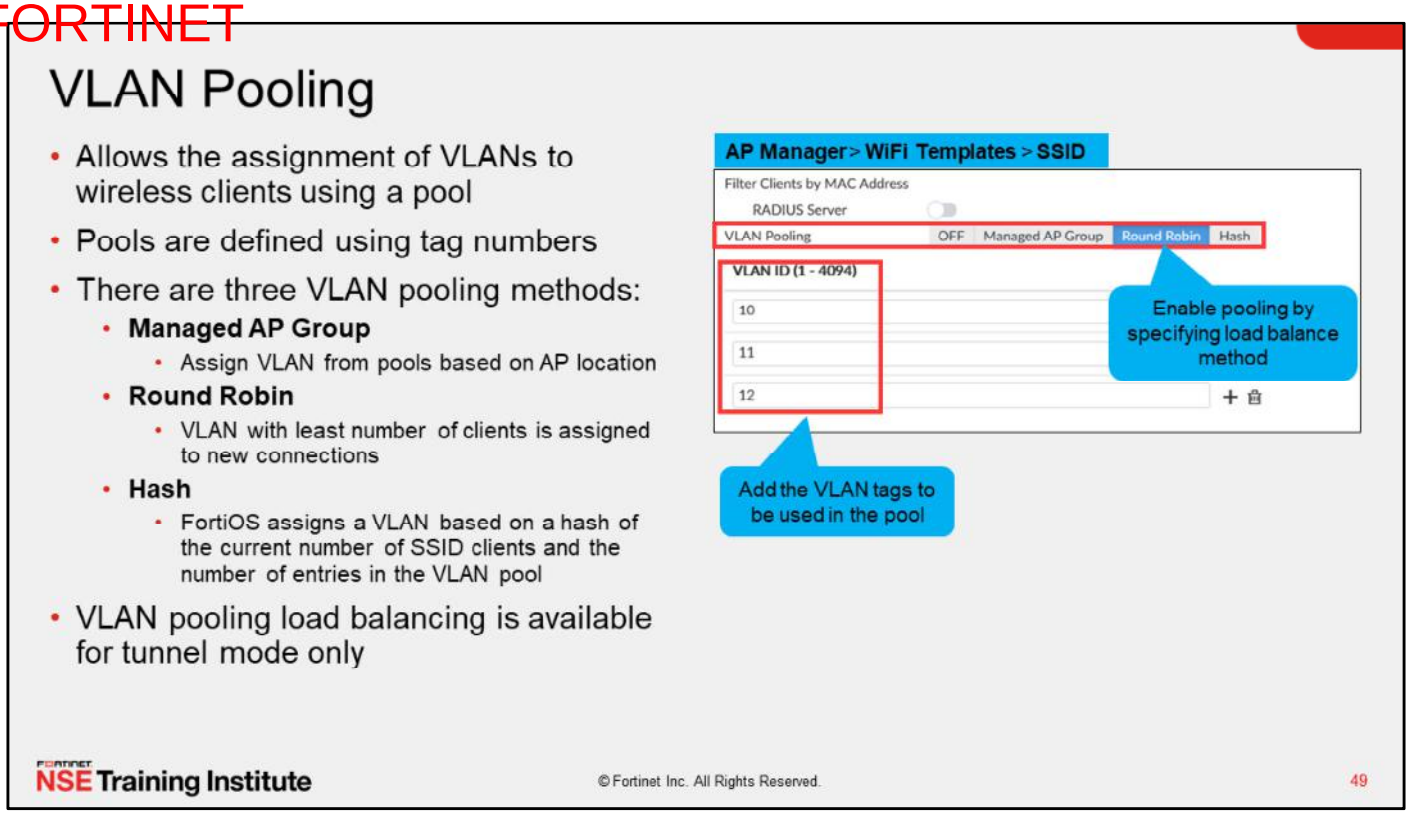
In an attempt to control IoT devices, enterprises will often publish multiple pre-shared key wireless networks, assigning each of them their own VLAN. Doing this can cause significant management overhead and potential wireless performance issues, because of the number of networks being broadcast.

RADIUS MAC authentication now allows you to control the access of IoT devices. FortiGate now sends and receives RADIUS attributes to allow the dynamic allocation of both a VLAN and a firewall policy using a suitably configured RADIUS server. In addition to MAC authentication, a second factor can be added in the form of a pre-shared key or, if multiple pre-shared keys are enabled, a choice of key. This enables connection encryption and a second factor of identity.

It is now possible to publish a single, pre-shared key-based network that serves multiple purposes. It could allow printers and IoT devices to be connected and controlled, assigning them to their own VLANs and firewall policies, while still allowing normal pre-shared clients, such as guests to connect and gain access.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



VLAN pooling is a mechanism that allows a single SSID to egress traffic into multiple VLANs. This feature is useful in large deployments and can break down the broadcast domain, rather than putting all wireless clients into a single subnet. Large broadcast domains can potentially cause performance problems in a wireless network, and traditionally /24 subnets are used to control the size of the domain. However, this can limit the number of clients that can connect to an SSID if it only supported one VLAN. With VLAN pooling, you can assign multiple VLANs to a single SSID removing any client limit and preserving an efficient IP network.

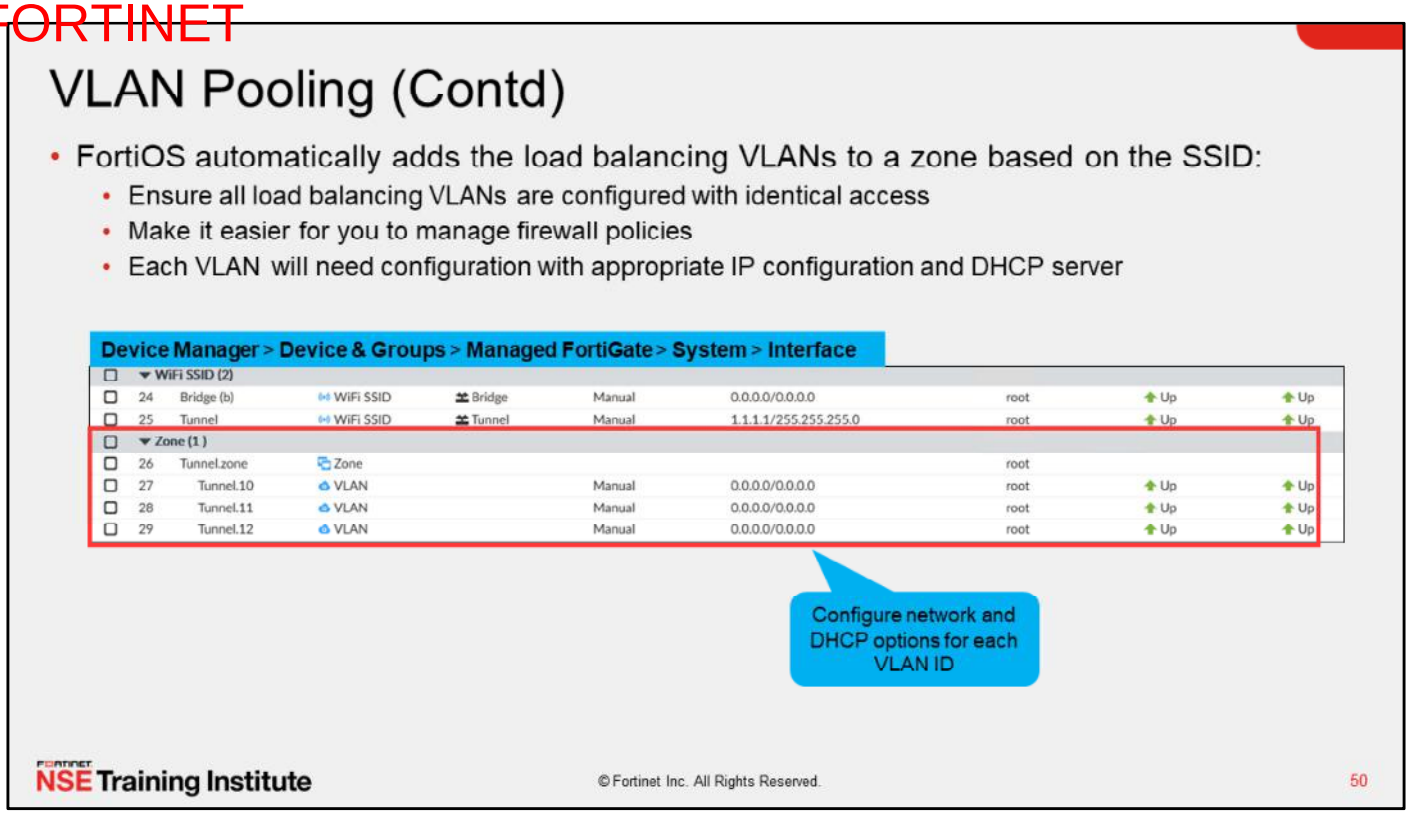
VLANs are added to each SSID profile using their tag number. The VLANs are automatically created when the SSID profile is assigned to a controller. There are two options available in the VLAN pooling configuration that provide load balancing options for wireless clients: round robin and hash.

The **Managed AP Group** load balance method assigns VLANs from pools based on AP location. When you enable the **Round Robin** option, the least busy VLAN is assigned to new clients. When you enable the **Hash** option, a VLAN is assigned based on the hash value of the current number of clients connected to the SSID and the number of VLANs available in the pool.

VLAN pooling load balancing is available for SSIDs operating in tunnel mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



FortiManager will automatically create the VLANs specified in the SSID profile when you apply it to FortiGate.

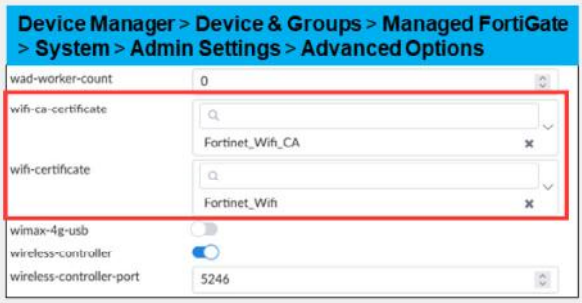
However, you must configure each VLAN with its own interface option, such as subnet, DHCP, and so on.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Replacing Wi-Fi Certificates

- The controller has a preloaded certificate that is used for wireless client connectivity
  - Used to secure WPA2/3 enterprise connections when using the local database
- Certificates can be updated
  - When they expire
  - If a different common name (CN) from the default `auth-cert.fortinet.com` is required
- Can be updated using the GUI or CLI of FortiGate
- Can be configured from FortiManager
  - Not as a provisioning template



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

51

FortiGate uses certificates when connecting wireless clients.

The Fortinet_Wi-Fi certificate is a factory-installed certificate that is used principally to identify and authenticate the controller when it is operating as the authentication server, as well as the authenticator. This happens when *local* authentication is selected. It is installed on FortiGate, not on FortiManager

When using an external RADIUS server, the clients will use the certificate installed on the RADIUS server instead.

The Fortinet_Wi-Fi certificate is issued to Fortinet Inc. by DigiCert with the common name (CN) `auth-cert.fortinet.com`. The Fortinet_Wi-Fi certificate can be updated automatically through the FortiGuard service certificate bundle update, but requires manual replacement, if FortiGuard is not available.

If a company or organization needs their own CN in their Wi-Fi deployment, they must *replace* the Fortinet_Wi-Fi certificate with their own certificate. Some client OS and supplicant configurations may display an error message when presented with the DigiCert certificate. They may require some acceptance or override.

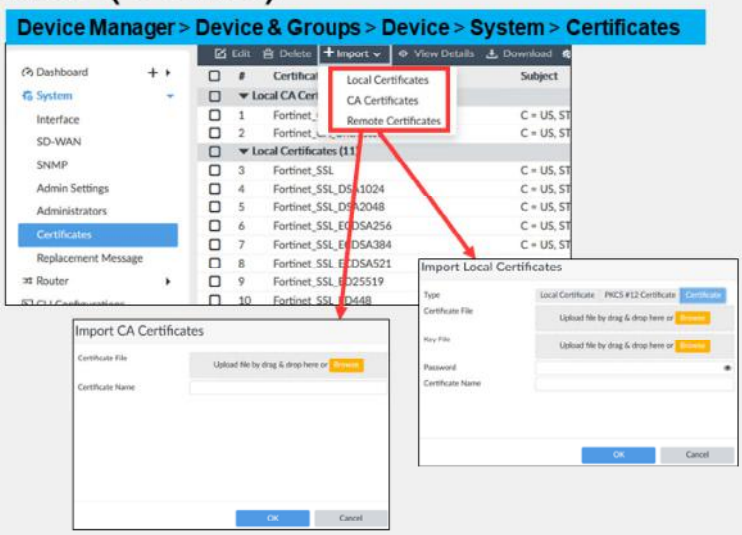
Certificates can be updated locally or deployed centrally from FortiManager to individual controllers. Provisioning templates don't support specifying certificates.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Replacing Wi-Fi Certificates (Contd)

- Certificates can be managed from FortiManager
- Applied on a per-FortiGate basis
- Import the updated or replacement certificate as required
- Create and import the CA certificate to be used
- Specify updated certificate and CA as shown on the previous slide



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

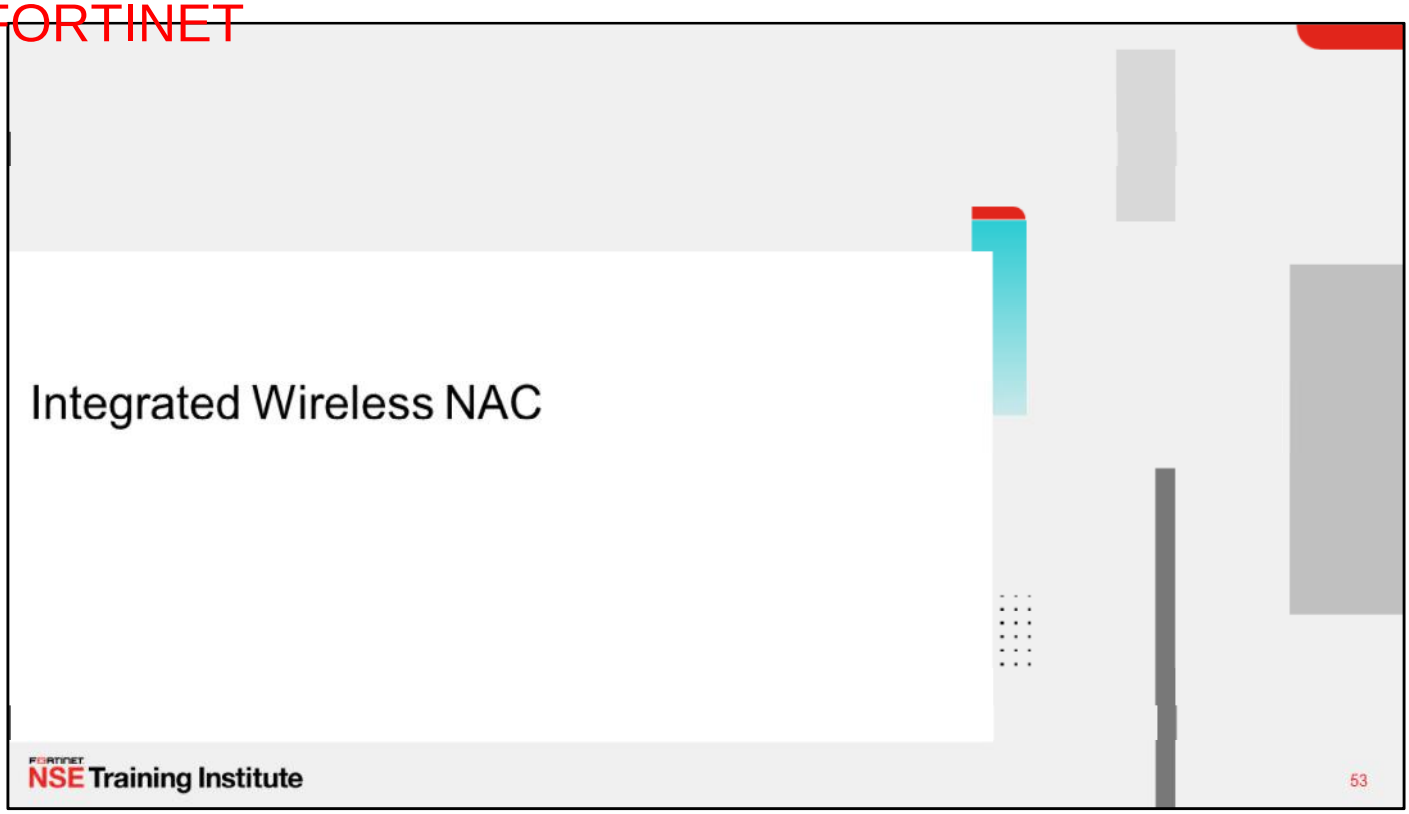
52

Certificates can be imported into FortiManager and then distributed to individual controllers using the device manager.

After you distribute the updated certificate and CA it can be specified as shown on the previous slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

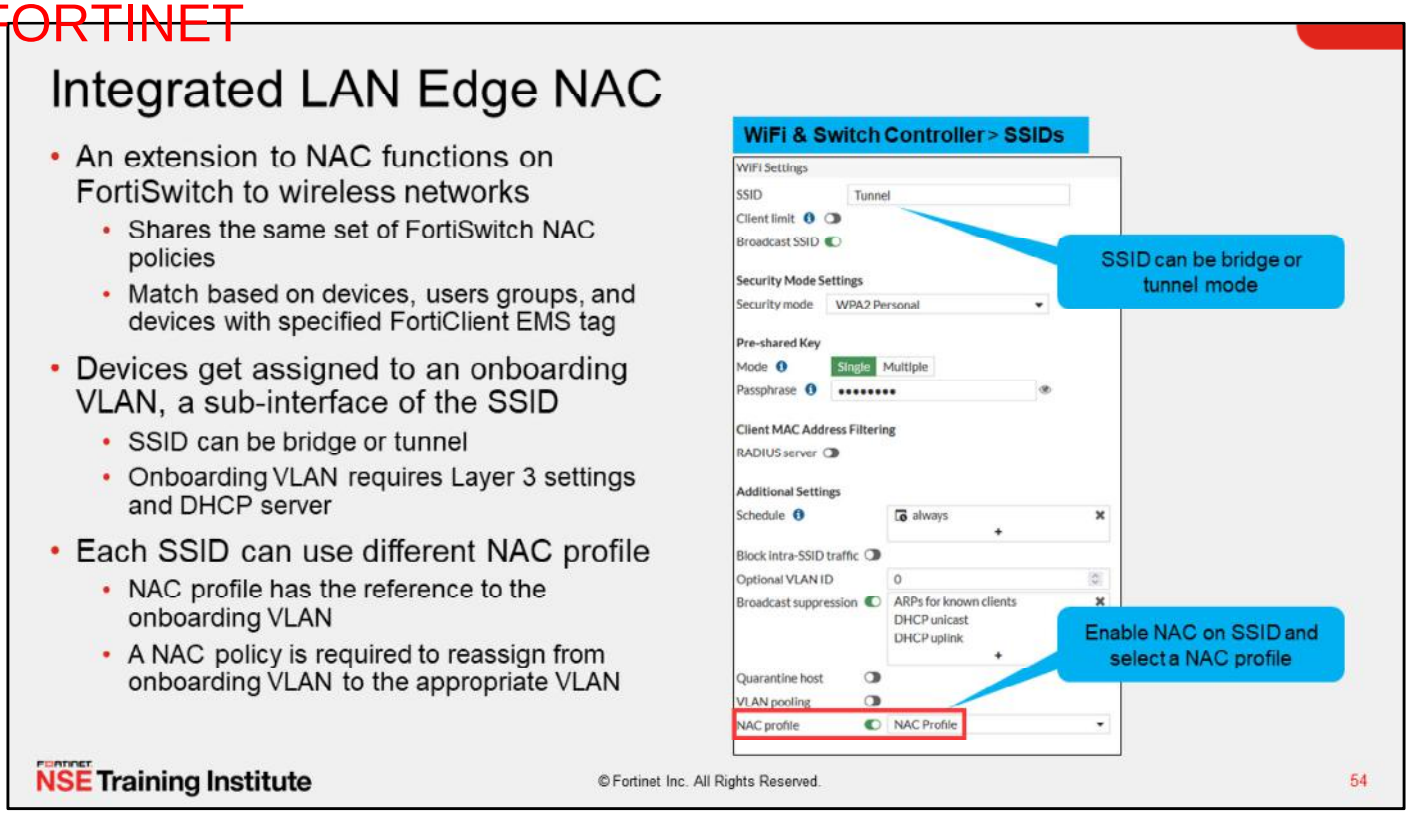
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn how to configure wireless network access control.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Network access control (NAC) helps you to implement policies to control devices on and users of your network. The integrated LAN Edge NAC, or wireless NAC, provides NAC functions that are similar to FortiSwitch NAC discussed in a previous lesson. However, it covers wireless networks that are controlled by FortiGate. Wireless NAC policy is defined based on patterns users and devices can be identified with. Such patterns can be user groups and device hardware information.

Wireless NAC can be enabled on bridge or tunnel mode SSIDs and require at least two VLANs to configure the onboarding segment as well as the appropriate VLAN for the wireless devices. These VLANs must be configured with Layer 3 settings, including DHCP and network device detection services.

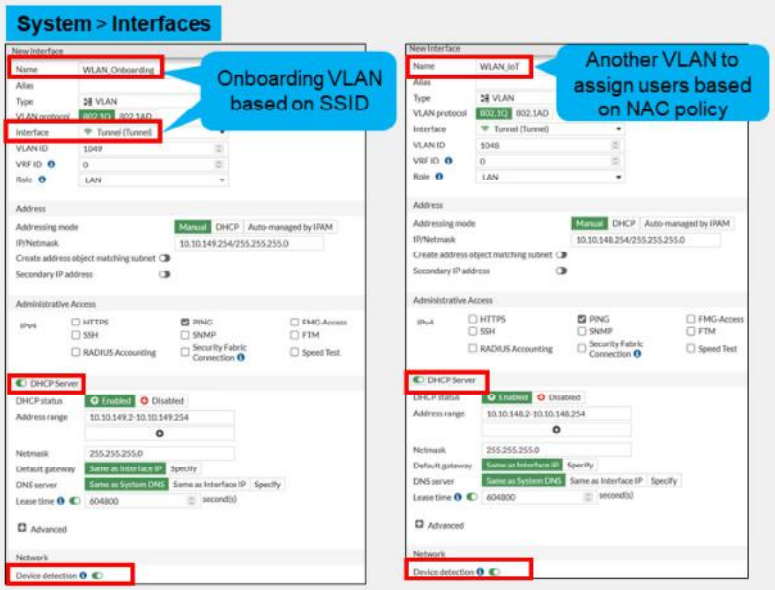
A NAC profile is the setting to enable on the SSID where you specify the onboarding VLAN while a NAC policy is to specify the matching condition and the wireless VLAN assignment should these conditions meet the devices connected to the wireless network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Integrated LAN Edge NAC—SSID and VLAN

- Once SSID configured as NAC access mode, a minimum of two VLANs must be created
- Onboarding VLAN
  - To onboard wireless clients if connected for the first time
  - Requires **DHCP Server** and **Device detection**
  - NAC profile must select this onboarding VLAN when SSID set as NAC access mode
- Another VLAN to reassign for matched device
- VLAN ID scope is only within the SSID interface broadcast domain



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

55

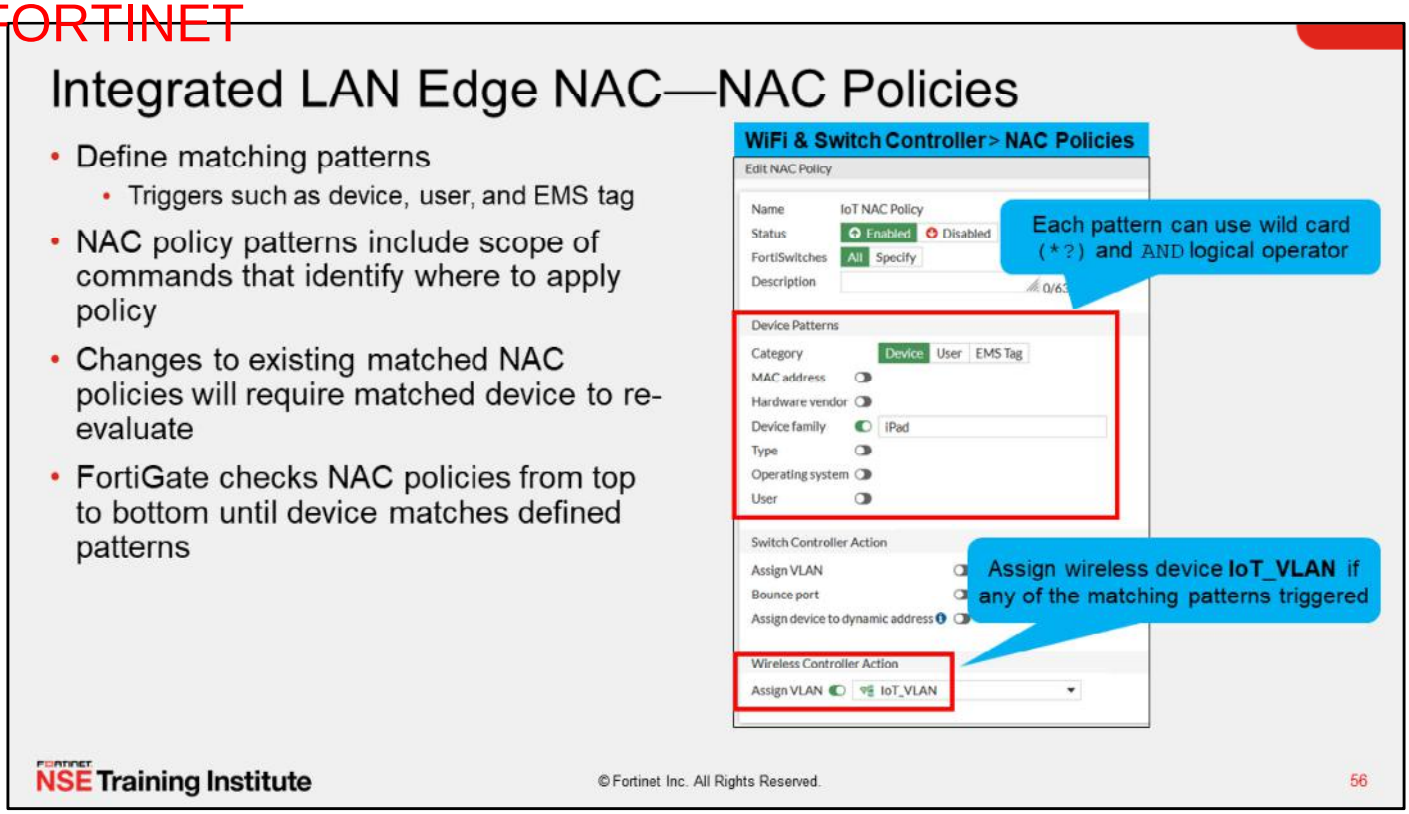
Unlike FortiSwitch NAC, there is no default onboarding VLAN. If the SSID is configured to become a NAC wireless, there are a minimum of two VLANs to be available to configure the remaining wireless NAC settings for this SSID.

The first VLAN is the onboarding VLAN which will be required to select when creating the NAC profile, which means to enable NAC on the SSID. The onboarding VLAN must have Layer 3 settings including DHCP and network device detection services.

Devices that match a NAC policy will be assigned the VLAN configured within the NAC policy for wireless controller section. The NAC policy can still be evaluated for FortiSwitch NAC operation should it has VLAN assignment for FortiSwitch.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

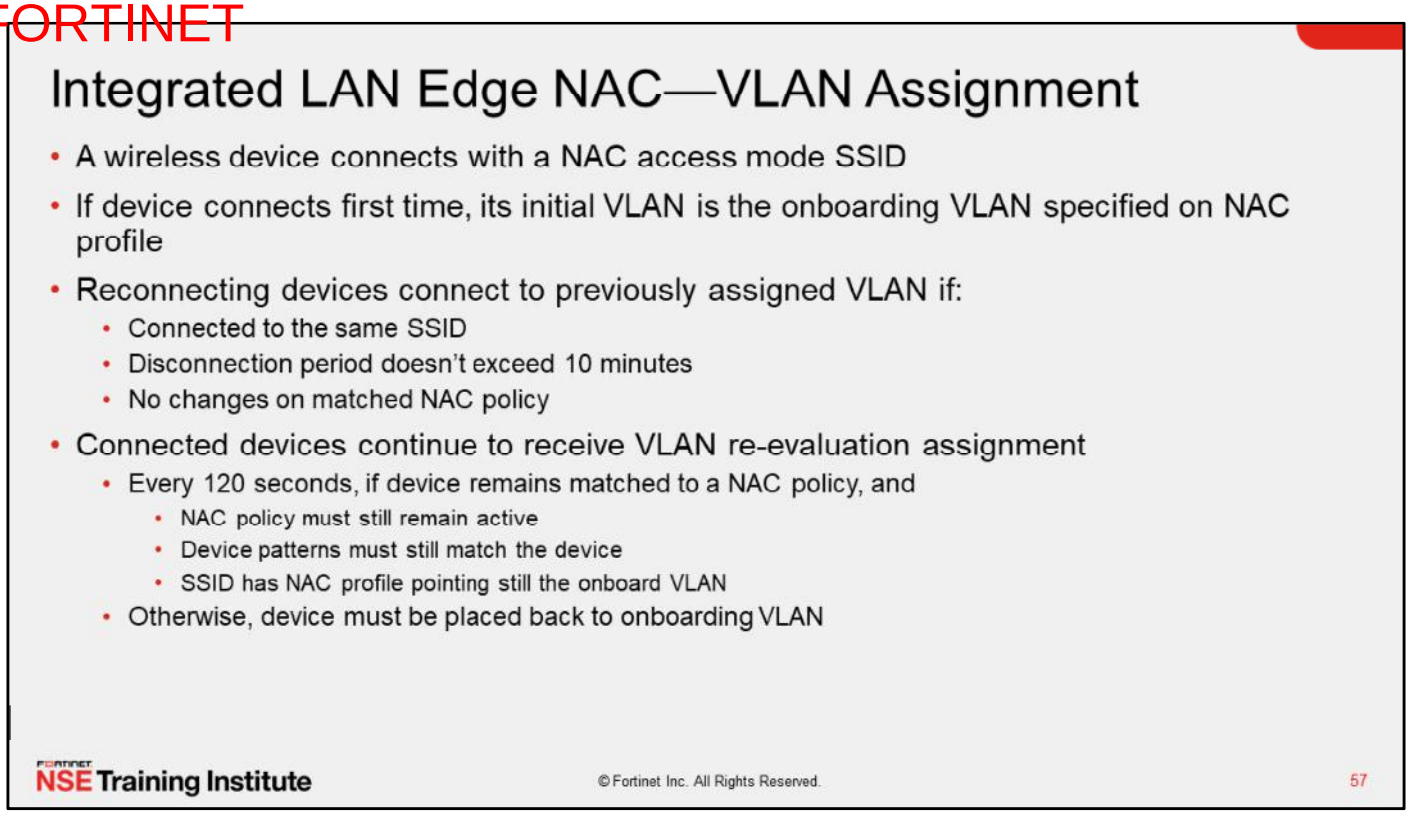


NAC policies contain the device, user patterns, FortiClient EMS tag to check on a device, before the VLAN. Like firewall policies, NAC policies are checked from top to bottom until a policy that matches *all* the defined patterns is found.

After the device or user is detected and a NAC policy is matched, FortiGate assigns the device the VLAN selected in the **Assign VLAN** drop-down list in the **Wireless Controller Action** section. Note that if changes are made on the NAC policy, all previously matched NAC devices will be deleted and re-evaluated through the list of NAC policies.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



When a wireless device is connecting to an SSID that has a NAC profile enabled, the VLAN ID to assign this device depends on the previous status of the connecting device. To avoid assigning a new IP address by multiple DHCP servers, if the device was connected to the same SSID and got disconnected for less than 10 minutes, it would be assigned the same VLAN it had prior to disconnecting, given the condition that no changes were made to the matched NAC policy.

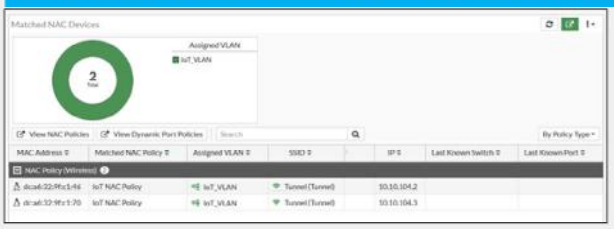
Connected devices undergo a re-evaluation process every 120 seconds to determine the VLAN ID for each device. As long the NAC policy exists on the same virtual domain (VDOM), the NAC policy must remain active and device patterns must match the connected device. This is, of course, as long the SSID in question still has a NAC profile enabled and is pointing to the same onboard VLAN.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Integrated LAN Edge NAC—Monitor and Debug

WiFi & Switch Controller > NAC Policies > View Matched Devices



- To display devices on CLI connected to a NAC access mode SSID

```
FortiGate # diagnose wireless-controller wlac_hlp -c sta-nac
STA (001/002) vfid,mac: 0, dc:a6:32:9f:c1:46
    ip                    : 10.10.104.2
    wlan                  : Tunnel(tunnel)
    vlan-id(oper/dflt)    : 104/1049
    matched nac-policy    : IoT NAC Policy
```

- To list configured NAC profiles

```
FortiGate # diagnose wireless-controller wlac_hlp -c nacprof
NACPROF (001/001) vdom,name: root, NAC Profile
    ob-vlan     : WLAN_Onboarding(1049)
```

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

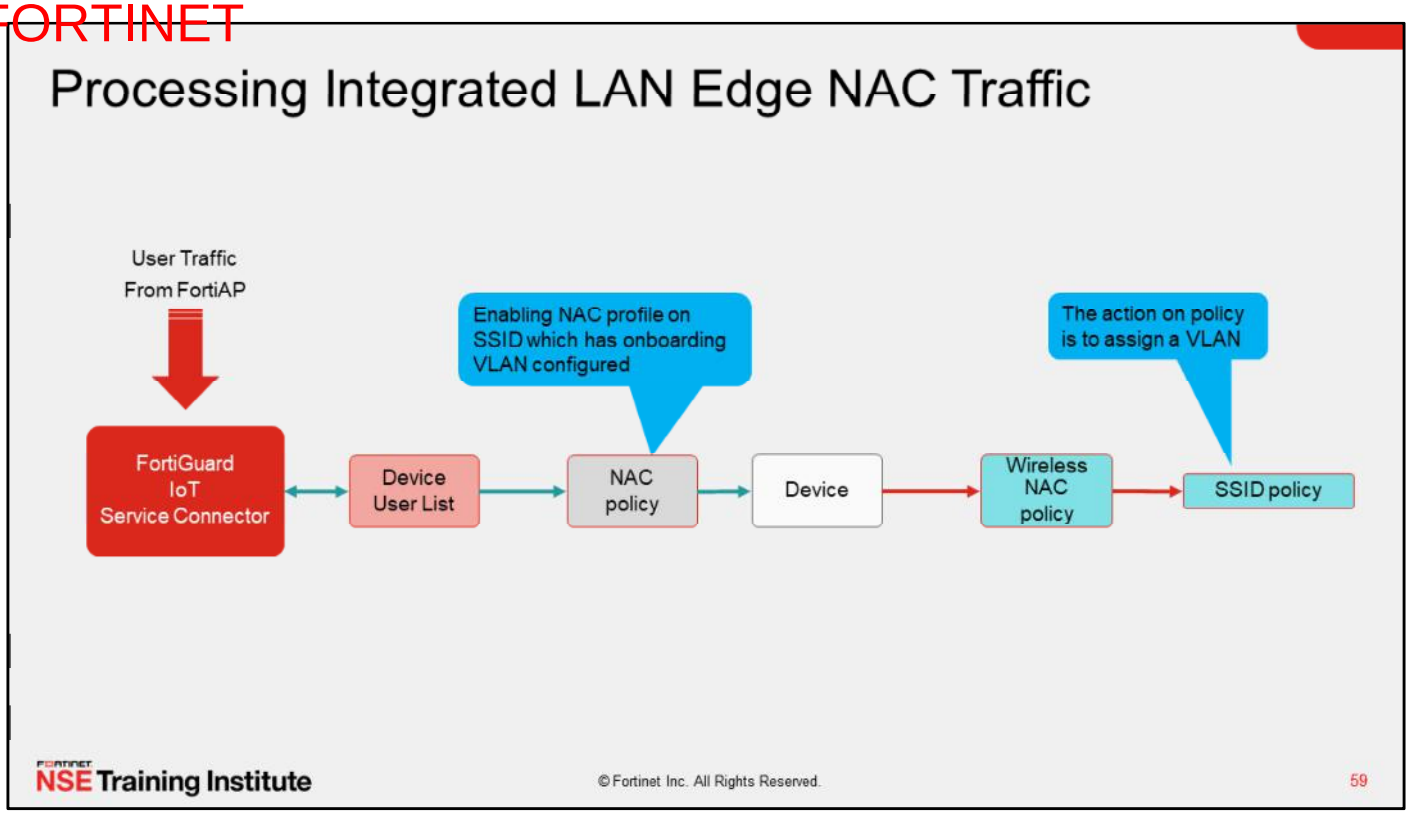
58

You can see the list of matched devices on the FortiGate GUI and CLI. By navigating to **NAC Policies**, you can switch the view to display devices that matched NAC policies for both FortiSwitch and FortiAP. Note that if the device hostname has been detected by FortiGate, the GUI will display the device hostname instead of its MAC address.

Other CLI commands, such as `wlac_hlp -c sta-nac`, display the information about the device that matched the wireless NAC policies in particular. You can also use `wlac_hlp -c nacprof` to display configured wireless NAC profiles each with its onboarding VLAN reference.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

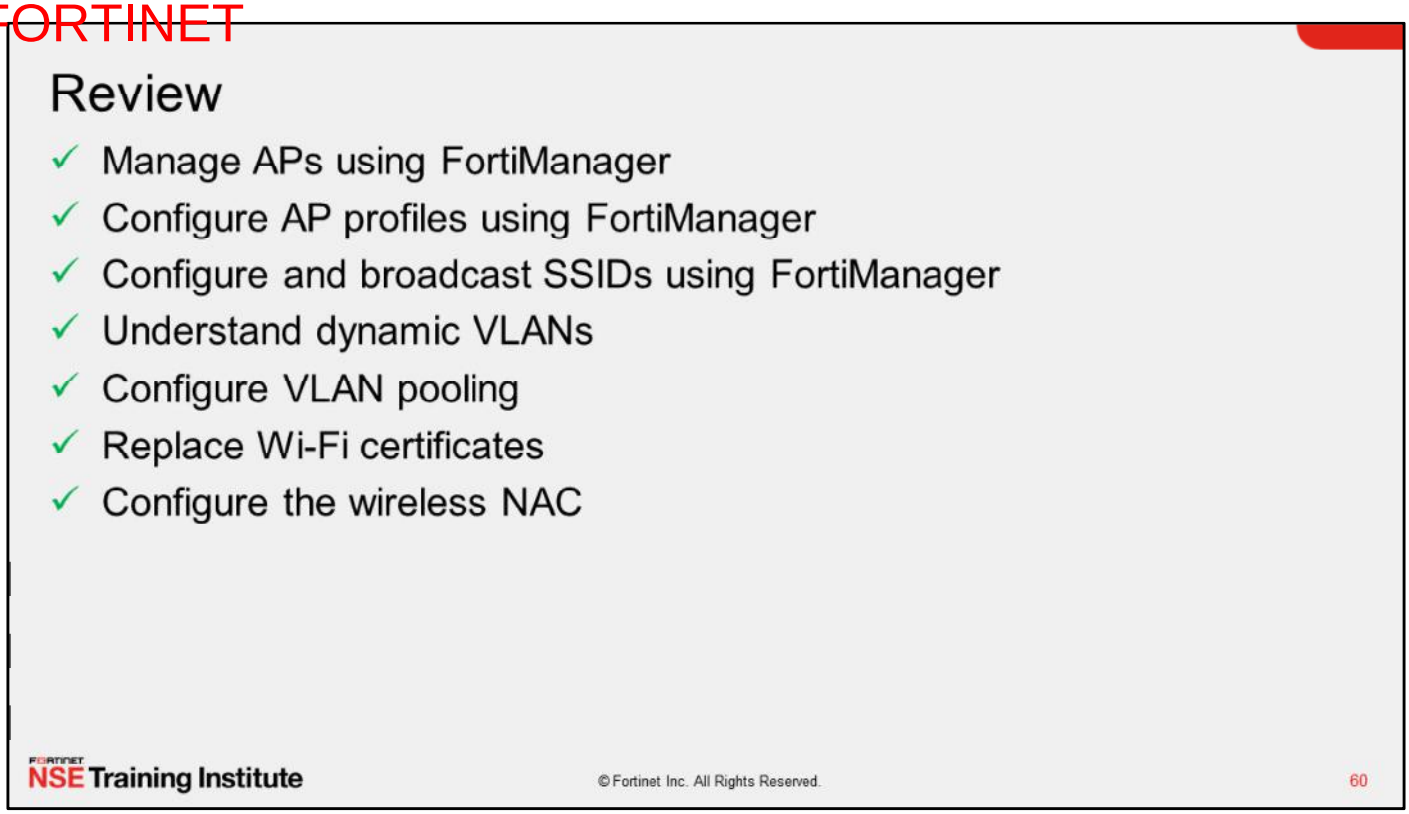


This slide shows the steps performed on the traffic received from FortiAP on SSID configured as NAC wireless network.

The NAC policy is defined based on any significant field with the user device list entry. Devices within the list may have a NAC policy applied and are using the IoT device identification database.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

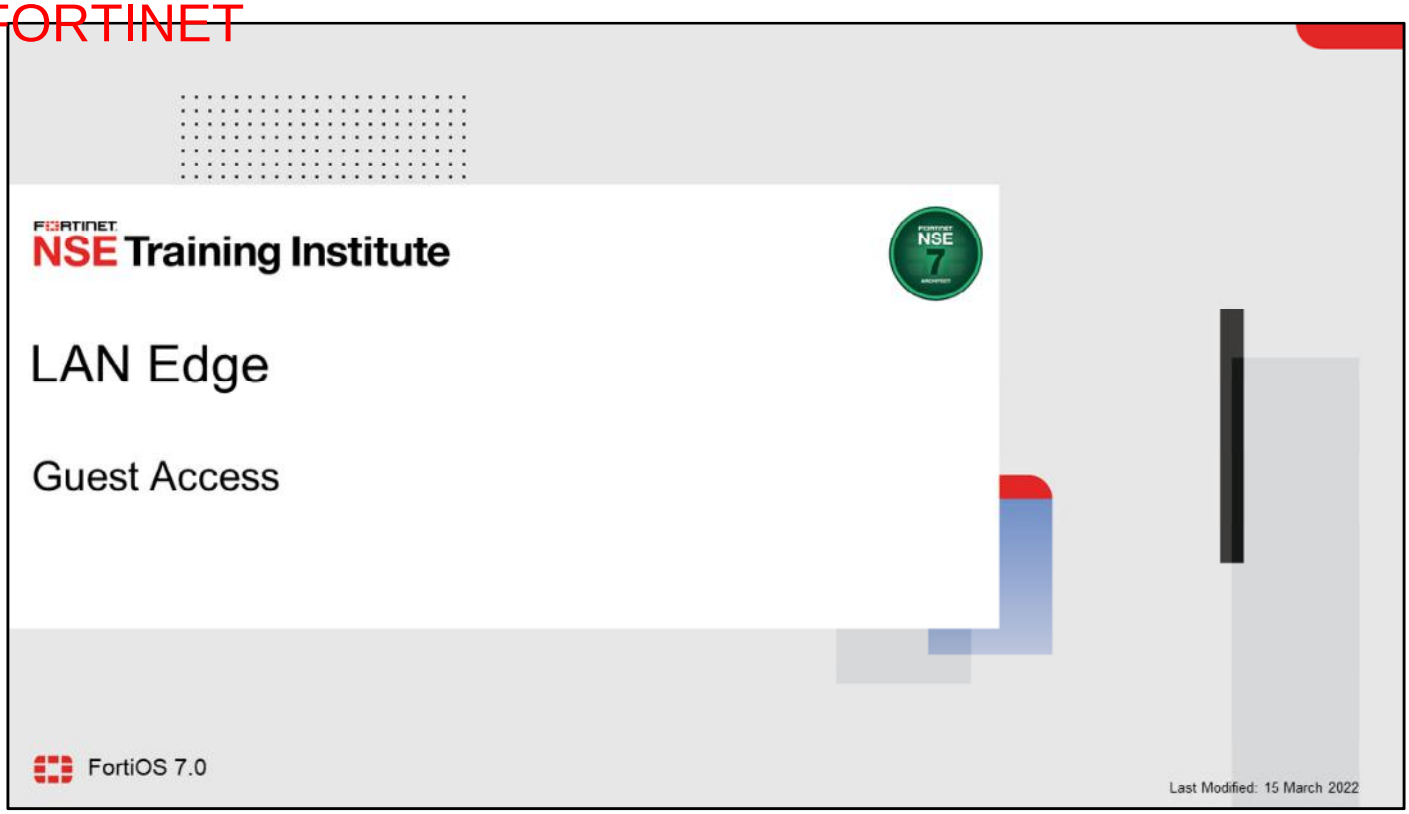


This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to configure and use FortiManager to centrally configure the integrated wireless features of FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

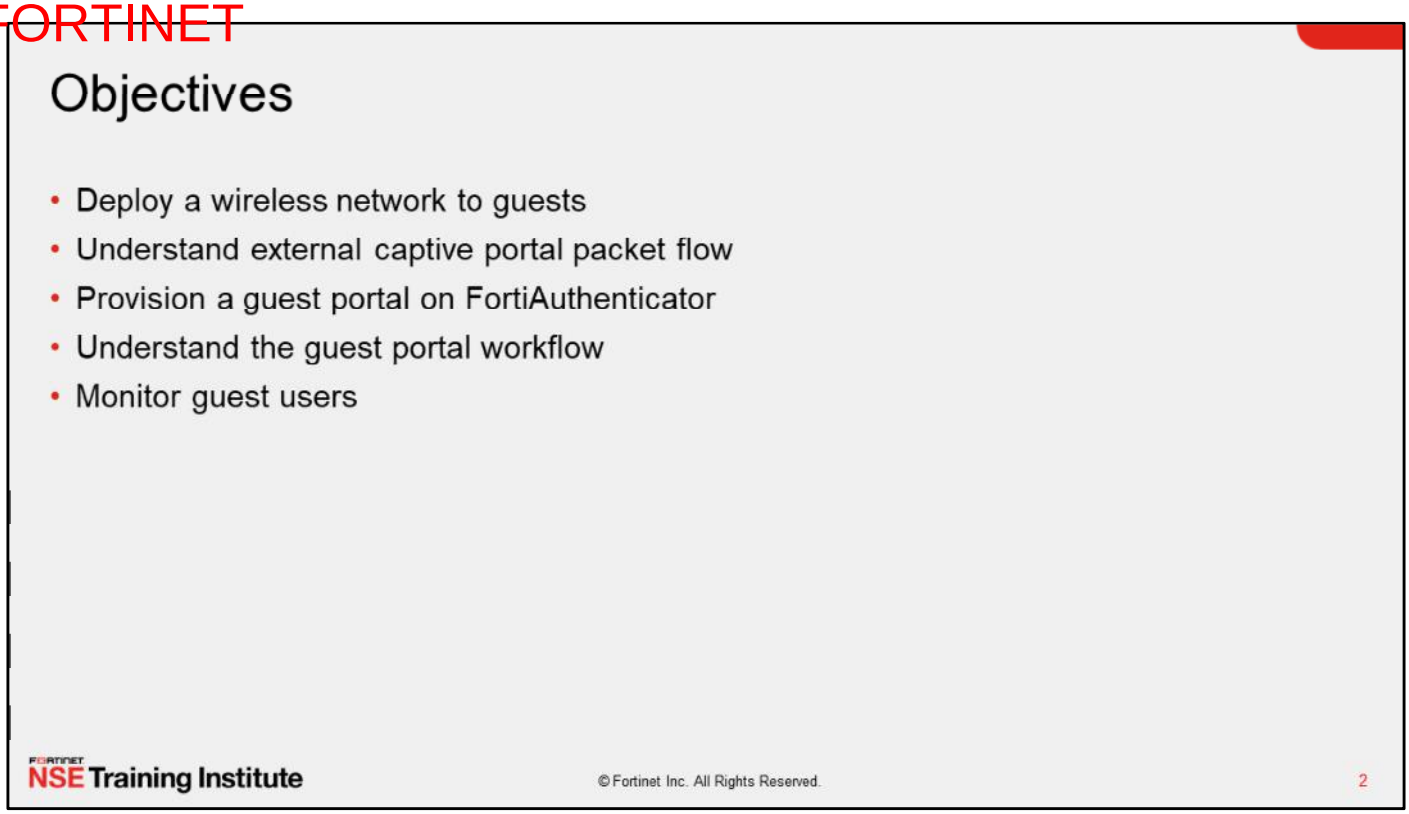
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn how to configure and use integrated wireless features on FortiOS and FortiAuthenticator to deploy a captive portal guest network.

Vouchers & Dumps are Available | WhatsApp +201224560923

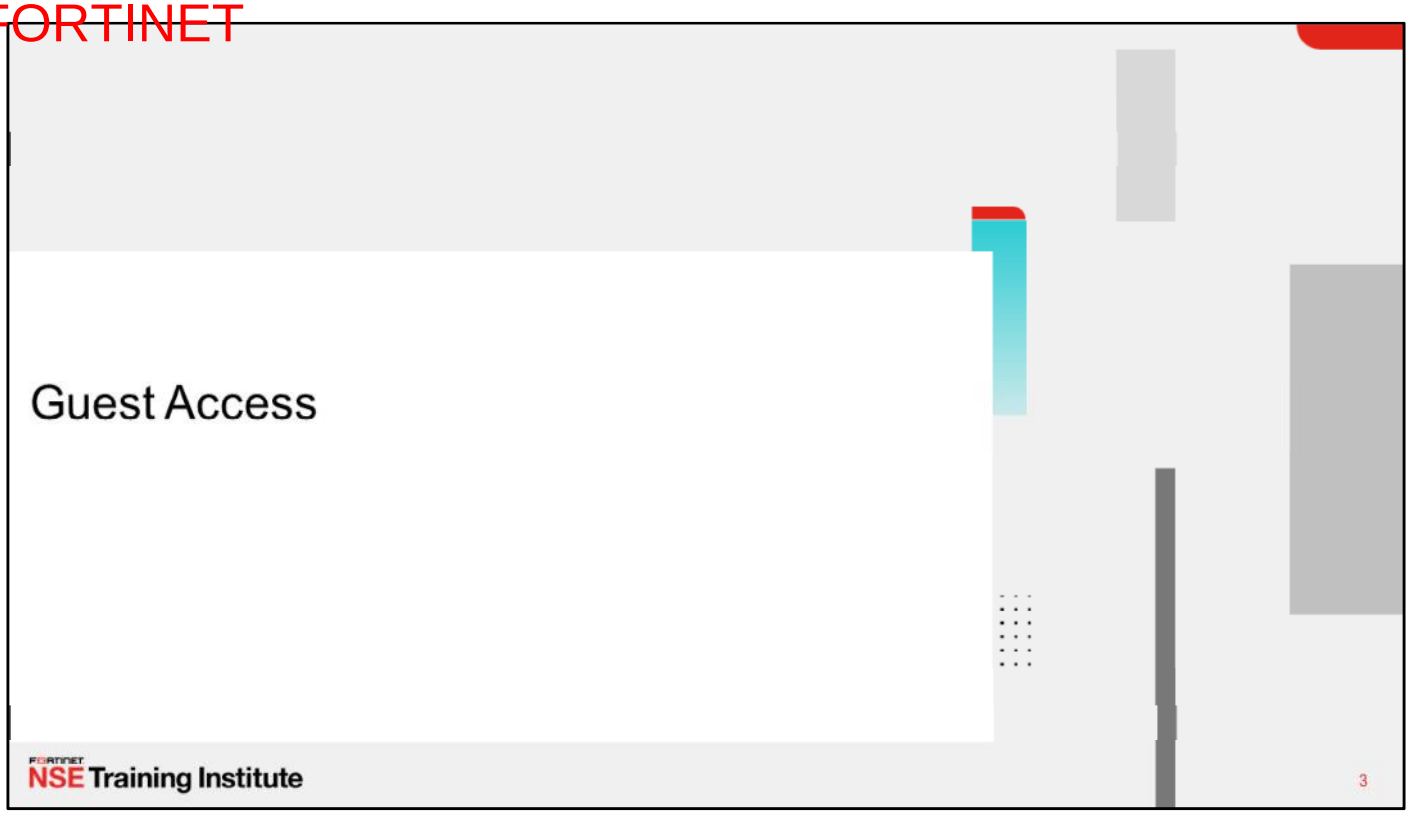
DO NOT REPRINT
© FORTINET
Brave-dumps.com



After completing this lesson, you should be able to achieve the objectives shown on this slide.

Vouchers & Dumps are Available | WhatsApp +201224560923

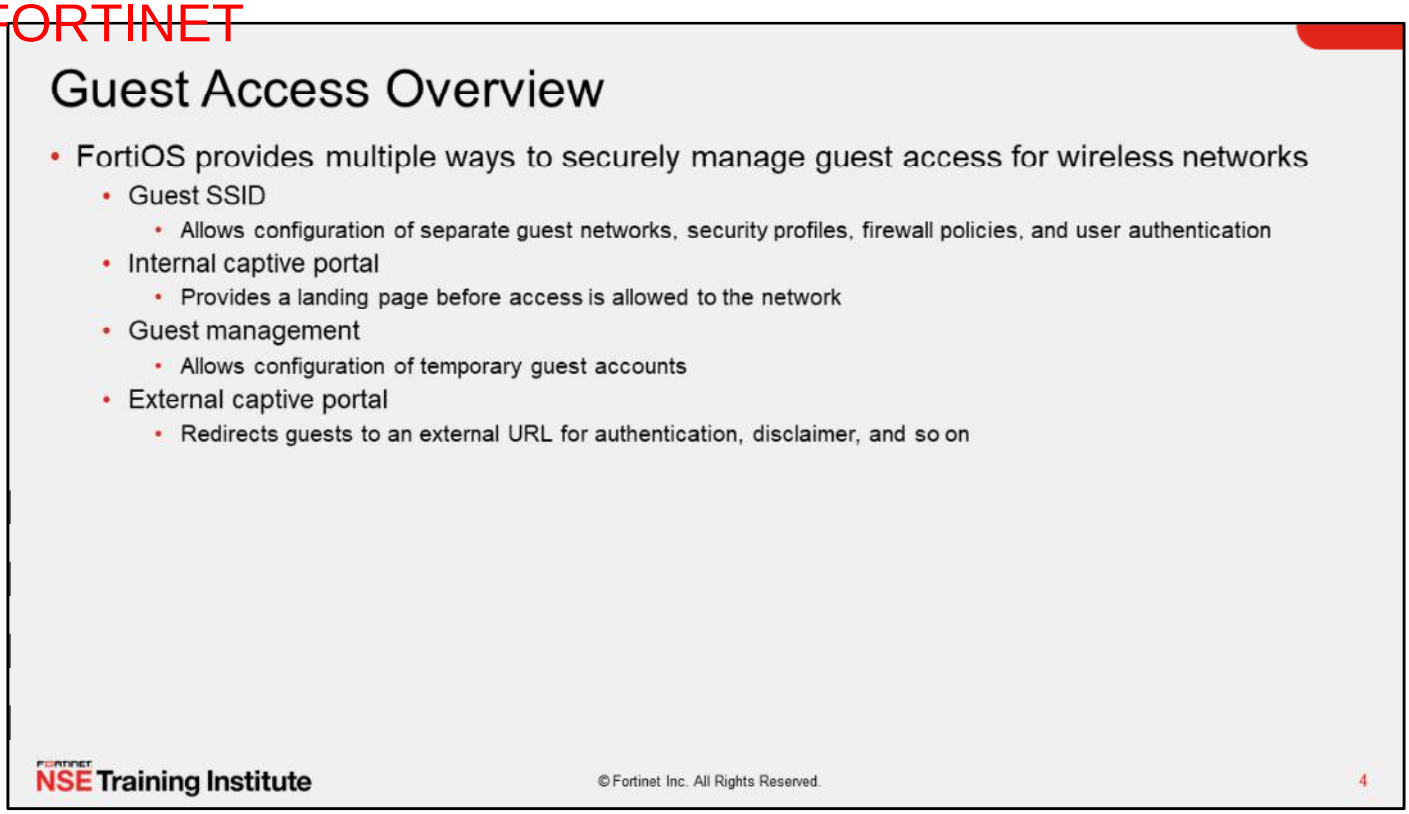
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn about managing guest access using FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

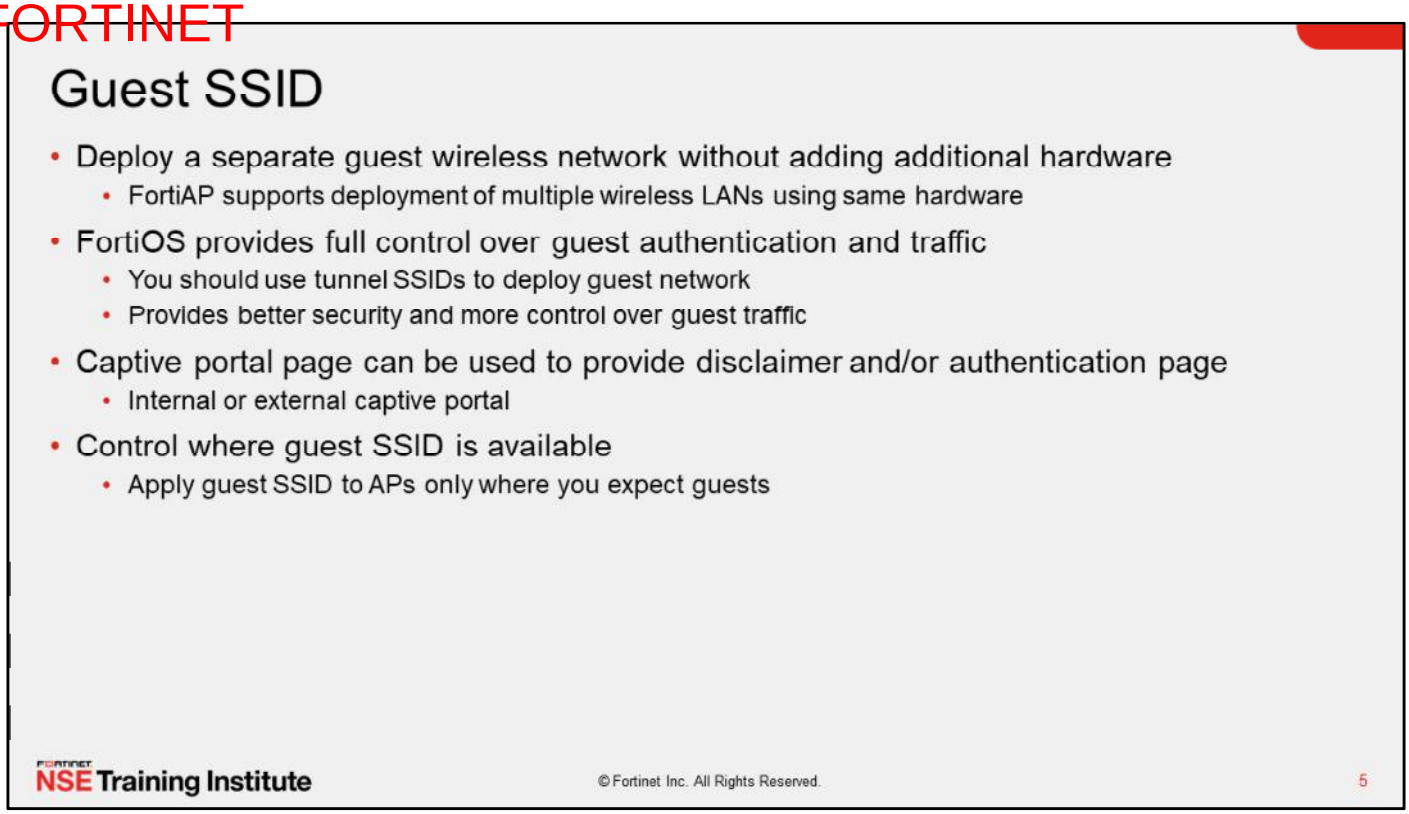


FortiGate provides multiple ways to securely manage guest access for wireless networks. You can deploy a completely separate wireless network using the existing hardware. FortiGate uses virtual AP (VAP) to deploy multiple SSIDs that are completely isolated from each other. This allows you to have complete control over the traffic, including the ability to assign firewall policies, security profiles, and so on.

FortiGate also has a local captive portal that you can use as a landing page for guests before they are allowed to access the network or local resources. To manage secure guest access, FortiGate offers local guest management tools that you can use to temporarily create and distribute guest accounts. Alternatively, you can redirect guests to an external captive portal server for authentication, disclaimer, and so on. FortiGate will allow access to resources only after it receives a valid response from the external server.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



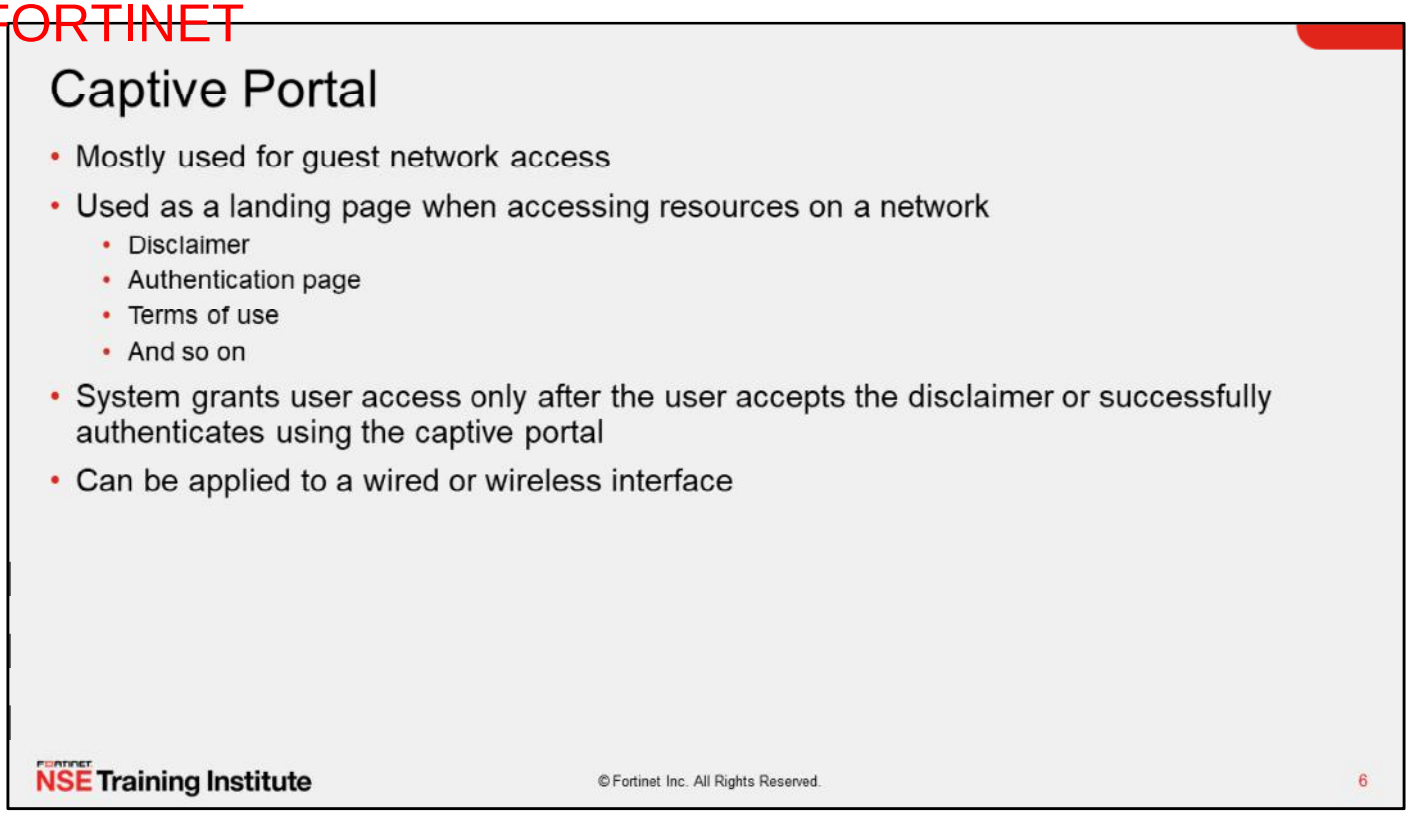
You should deploy a separate SSID server to guests that do not require access to a corporate or private network. You can deploy multiple SSIDs using the same hardware. Separate SSIDs mean that you will have full control over network traffic flow. You should deploy a guest access SSID in tunnel mode to ensure that all traffic is sent to FortiGate using a CAPWAP data control channel. This ensures that FortiGate maintains full control over the traffic flow, and can apply security profiles to eliminate security threats before placing traffic on the egress interface.

You can use a local or external captive portal to provide guests with a landing page. You can also use a captive portal to display a disclaimer, or authenticate guest users using guest accounts, or both. Because you will be using a separate wireless network for guest access, you can choose to broadcast the network on APs that are installed in locations where you expect guest users to be.

Be careful not to transmit too many SSIDs. Excessive numbers of SSIDs can impact wireless performance, and you should carefully plan the number and use of wireless networks. This subject is covered in another lesson.

Vouchers & Dumps are Available | WhatsApp +201224560923

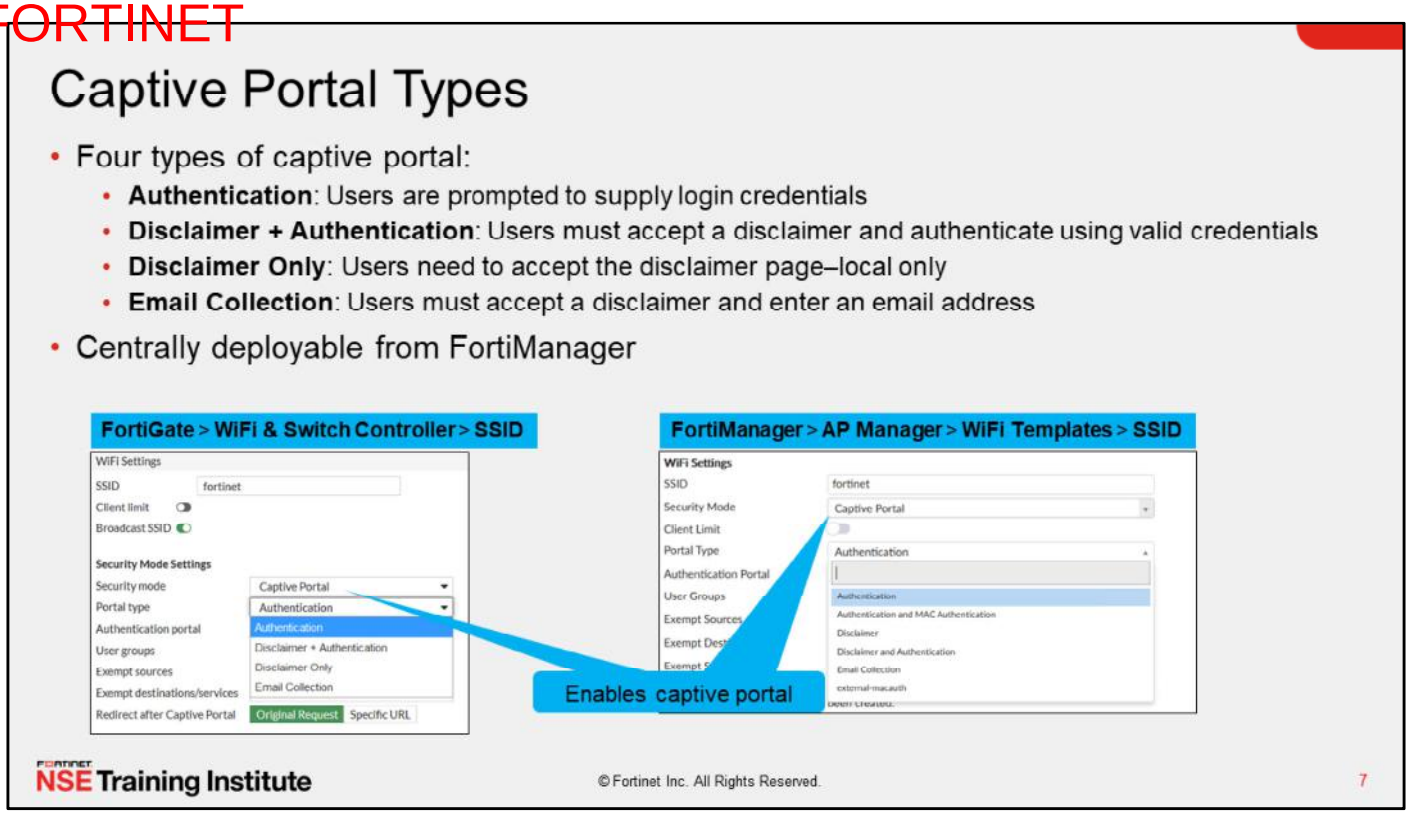
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The captive portal is used as a landing page after a user connects to a network. This is mostly used for guest access and networks that require a disclaimer. You can also authenticate your users on a captive portal page that requests the user's name and password. Until the user authenticates successfully, the authentication page is returned in response to any HTTP request. After successful authentication, the user can access the requested URL and can access other web resources, as permitted by security policies. Optionally, the captive portal itself can allow web access only to the members of a specified user group.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



There are four types of captive portals that you can enable on an interface: **Authentication**, **Disclaimer + Authentication**, **Disclaimer Only**, and **Email Collection**.

Authentication type captive portals request users to authenticate before they are allowed access to the network.

Disclaimer + Authentication type captive portals present users with a disclaimer page and an authentication page. The user must accept a disclaimer and authenticate successfully in order to get network access.

Disclaimer Only captive portals present users with a disclaimer page. Users do *not* have to authenticate using a username and password; they are allowed to access the network after they accept the disclaimer.

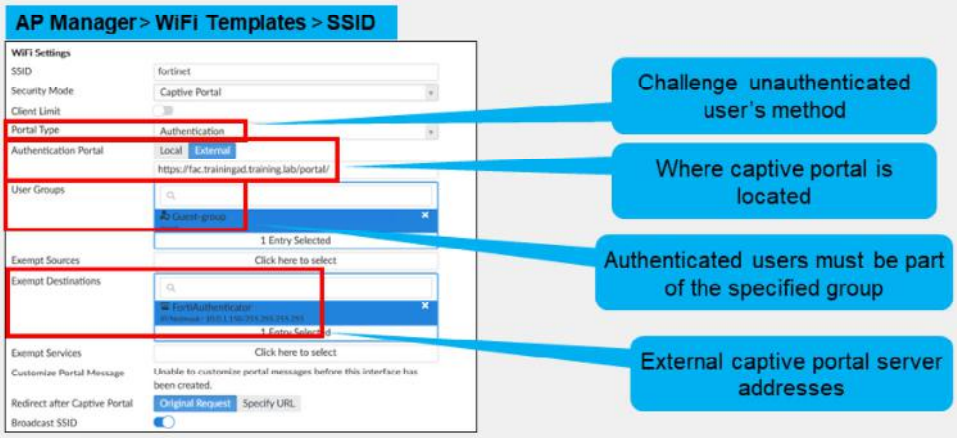
Email Collection captive portals present users with a disclaimer page together with a mandatory email request field. Users cannot gain access without entering an email address. The emails are collected and are displayable in the **FortiGate Dashboard** > **Users & Devices** > **Collected Email**. You have to enable **Email Collection** in feature visibility, or use FortiManager to deploy a CLI configuration from Device Manager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Captive Portal Authentication Types

- Authentication types:
  - **Local**: FortiGate presents the user with a login page and processes authentication requests
  - **External**: FortiGate redirects users to an external URL where the external captive portal server presents the user with a login page and validates authentication



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

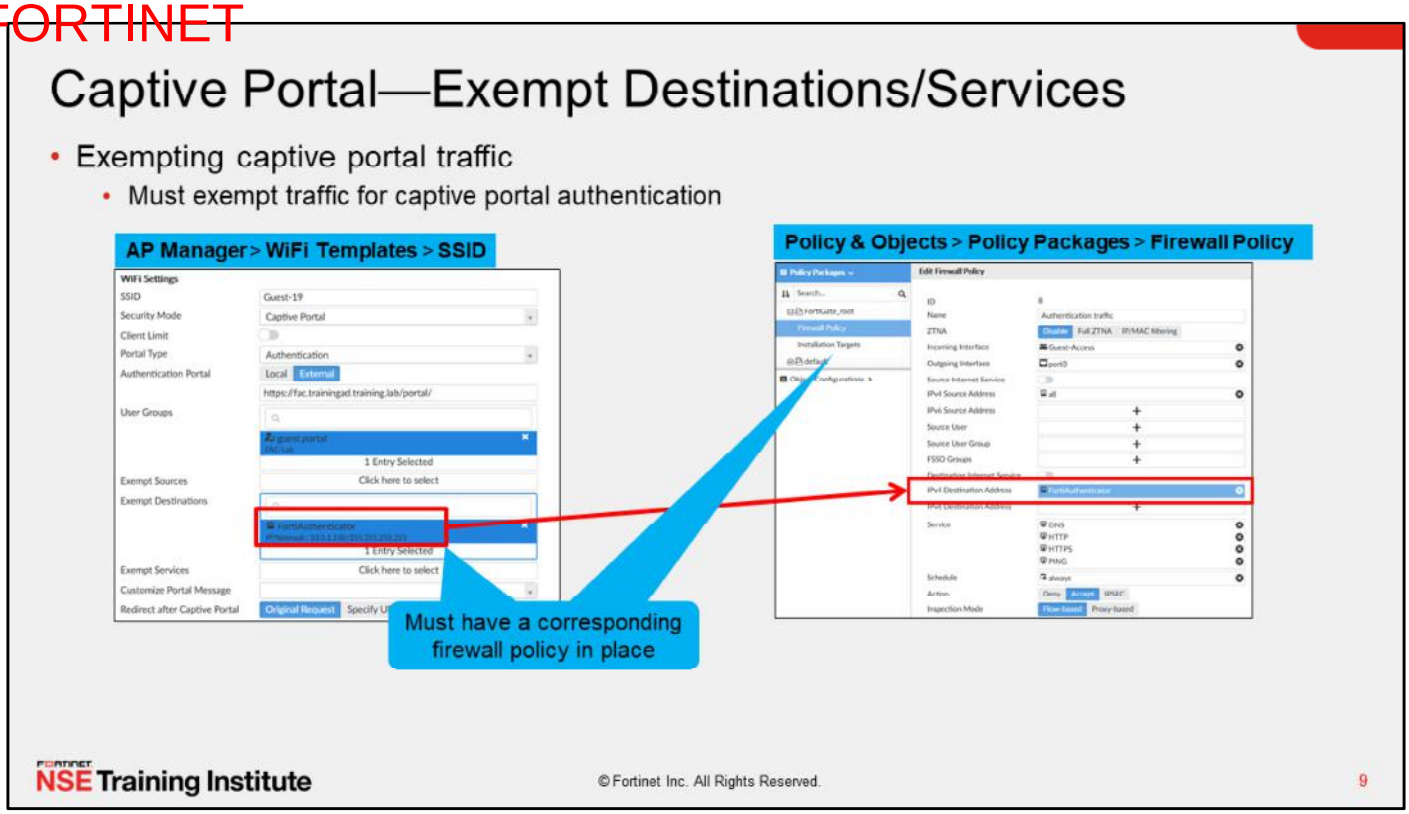
8

If you select **Authentication** in the **Portal Type** drop-down list, you will have the option to select **Local** or **External** in the **Authentication Portal** field. If you select **Local** in the **Authentication Portal** section, the FortiGate built-in portal page is used. All the portal configuration, including the web page that is presented to the users as a landing page, are hosted on FortiGate.

For external captive portals, you can select **External** in the **Authentication Portal** section, and enter the FQDN or IP address of the external captive portal server. When you do this, FortiGate redirects users to the specified server address. After the user meets the requirements of the external captive portal server, FortiGate allows user access based on the firewall policy configurations.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



By default, FortiGate blocks all user traffic behind an interface that has the security mode set to captive portal. All HTTP traffic redirects to the captive portal page, and all other traffic is blocked. However, there is an option to exempt certain traffic, allowing it to flow through FortiGate without fulfilling captive portal condition(s) (disclaimer and/or authentication).

If you are using an external captive portal server, you must configure a firewall policy and exempt web traffic to the external captive portal IP address. You can exempt destination IP addresses and services on the SSID using FortiManager. When you create the **SSID**, add the address objects of the destination(s) that you want to exempt in the **Exempt Destinations** or **Exempted Services** field.

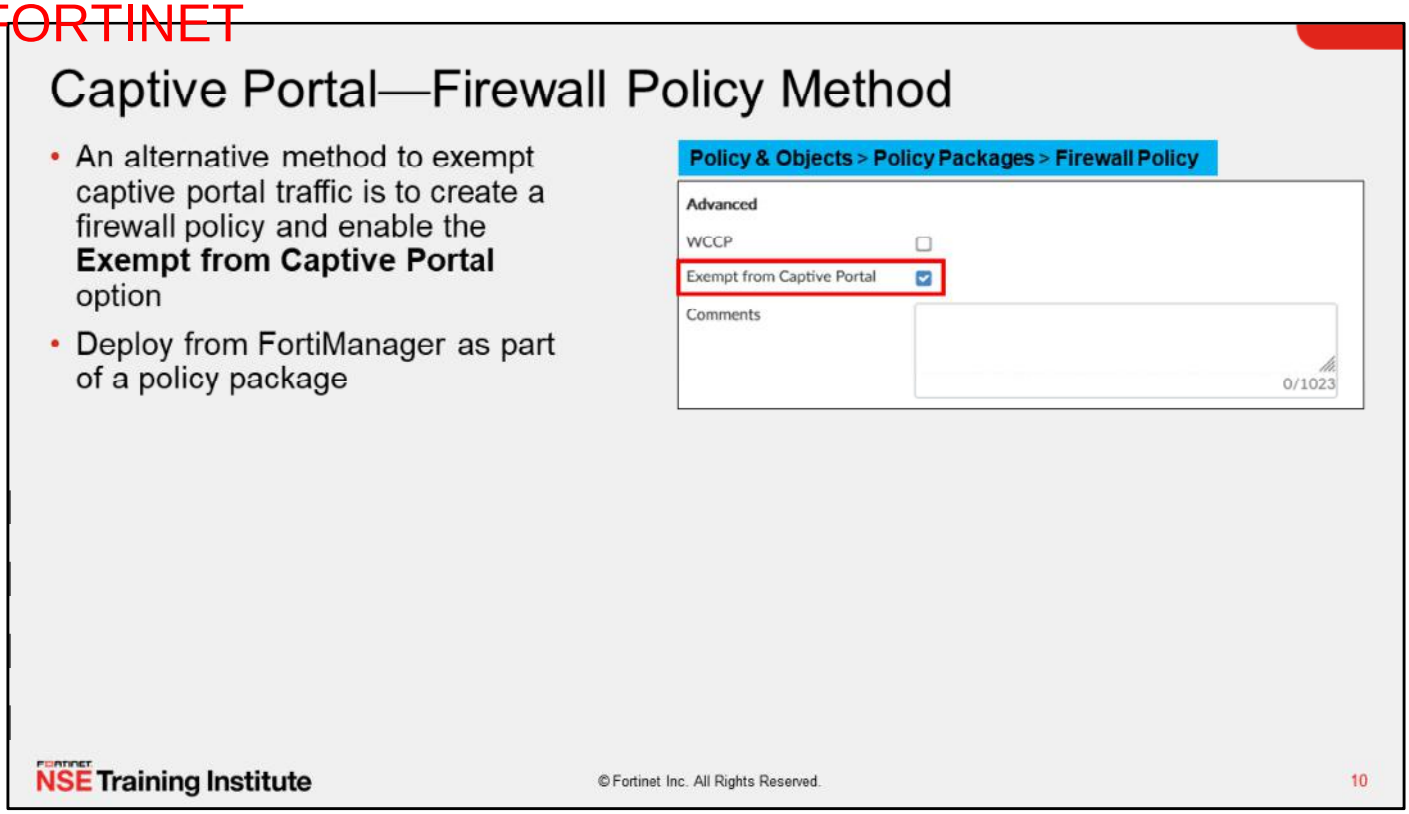
Just selecting and applying the address object and selecting the services is not enough to allow the traffic to pass through FortiGate. You must also have a corresponding firewall policy in place that allows the pinhole traffic to pass through FortiGate. Therefore, this is a two-step process:

1. Select the destination and services on the SSID in the **Exempt Destinations** or **Exempted Services** section.
2. Use FortiManager to deploy a firewall policy on the captive portal interface connected to the interface where the external captive portal server is located. You do not have to specify destination objects on the firewall policy.

You can also specify source IP addresses that you would like to exempt from the captive portal. This can be useful for devices that are unable to accept captive portal conditions using HTTP/HTTPs, but do require an internet connection. For example, a printer might need to access the internet for firmware upgrades, and so on.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



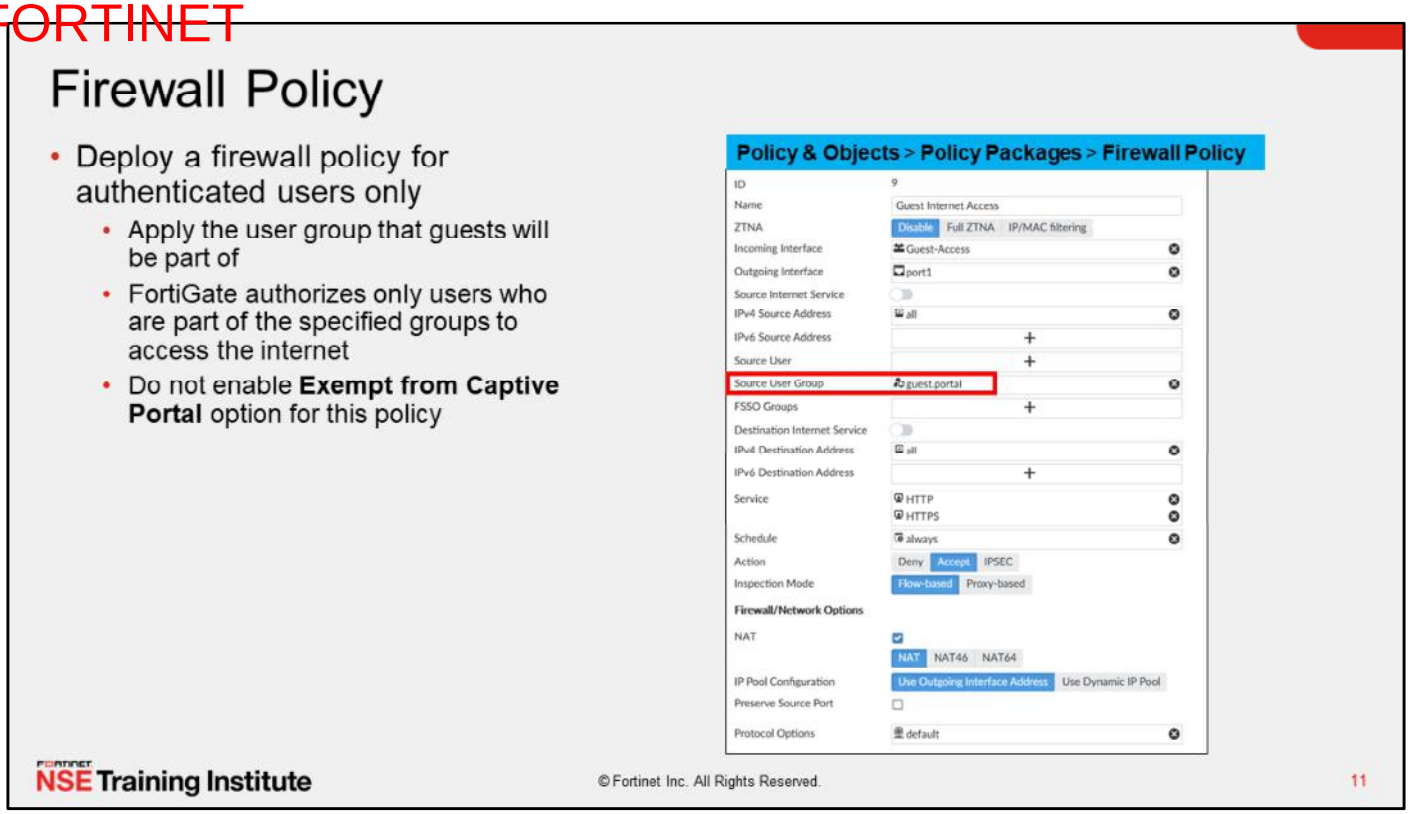
Alternatively, you can configure a separate firewall policy to allow traffic to reach the external captive portal server without authenticating on the captive portal interface.

Create a FortiManager firewall policy package and set the destination to your captive portal server, and any other required servers such as DNS or Windows AD. On the CLI, edit the firewall policy rule and enable the **Exempt from Captive Portal** option on the policy. This option instructs FortiGate to allow traffic to pass through to the specified destination(s), without forcing users to authenticate first.

You can use an IP address or an FQDN to point to the captive portal server. If HTTPs is being enforced, the portal address needs to be an FQDN, and match the CN on the certificate that is being used on FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

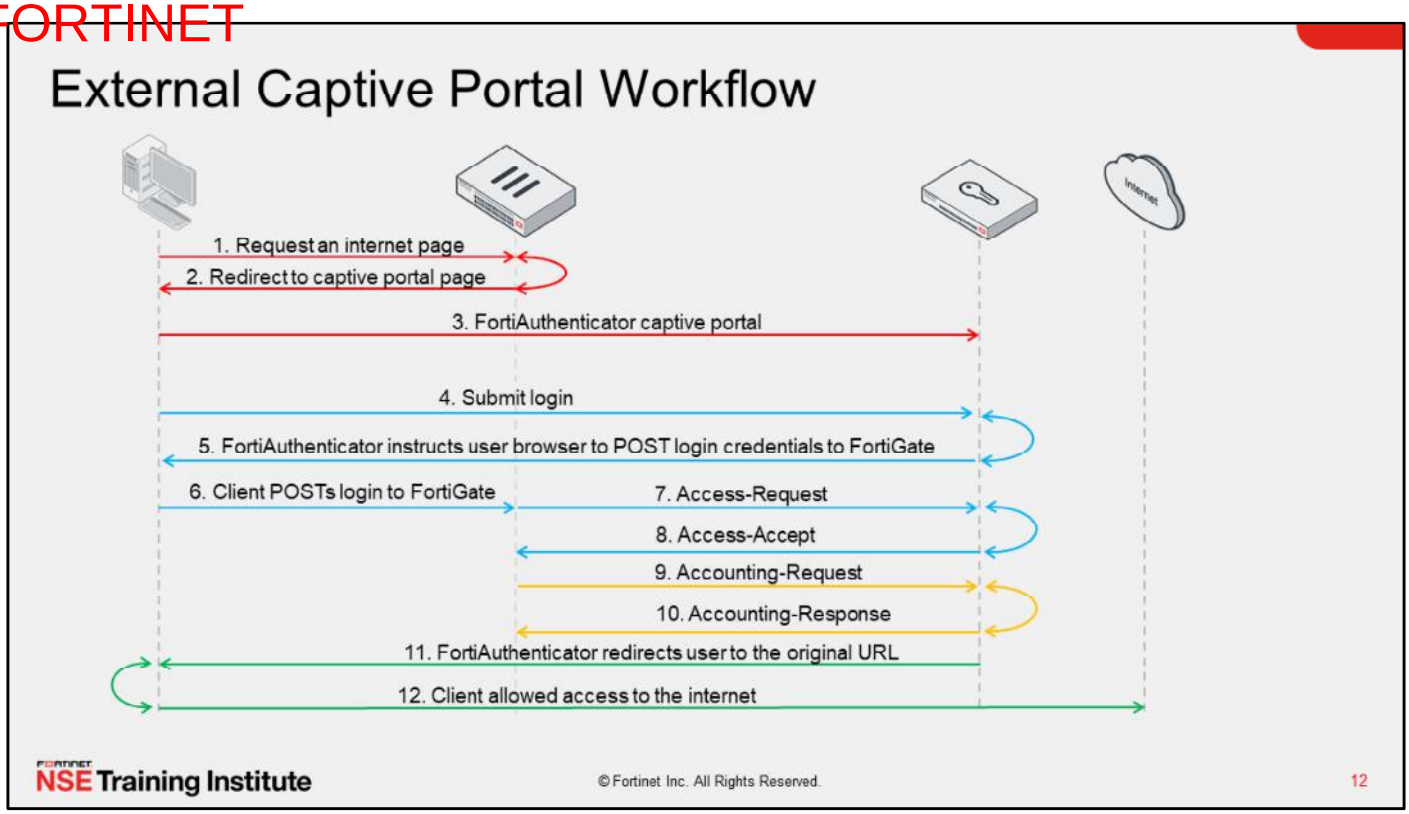


Create a firewall policy from the guest interface to the internet. If you are using a guest user group, make sure you assign it to the firewall policy as the **Source User Group**. When you do this, FortiGate allows access to the internet only for authenticated users who are part of that group.

Do not enable the **Exempt from Captive Portal** option on this firewall policy; otherwise, all the traffic to the internet will be allowed without the users being presented with a captive portal page.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



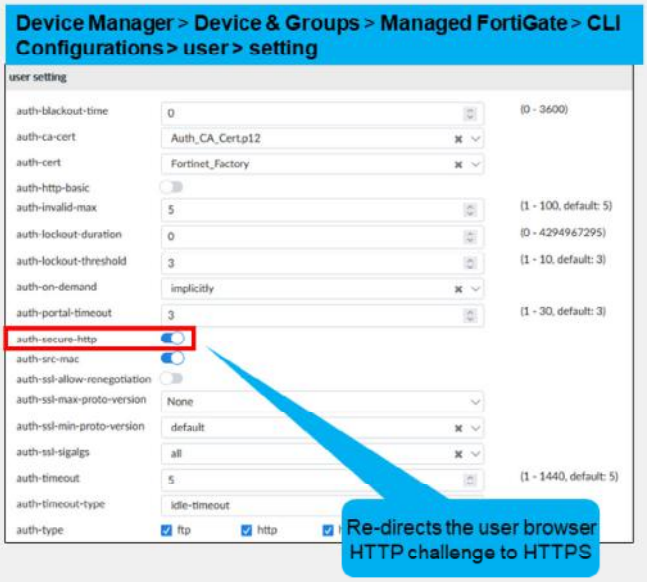
1. The client tries to access a website.
2. The initial HTTP traffic is intercepted by the FortiGate wireless controller and redirected to the FortiAuthenticator web login page defined in the FortiGate captive portal profile.
3. FortiAuthenticator presents the user with a login page.
4. The client enters their user credentials on the FortiAuthenticator web login page.
5. The login message instructs the guest user's browser to submit the user credentials directly to the FortiGate as an HTTPS POST for authentication processing.
6. When FortiGate receives the client credentials in the HTTPS POST, it sends a RADIUS Access-Request to the FortiAuthenticator RADIUS server to authenticate the user.
7. FortiAuthenticator validates the Access-Request message using its user database, which can be local or remote (LDAP/RADIUS).
8. Based on the results of the authentication and authorization processing, FortiAuthenticator responds with either an Access-Accept or Access-Reject message. If the authentication is successful, the Access-Accept message contains one or more RADIUS attributes to define the context of the client session. These attributes can include, but are not limited to: session duration, bandwidth, and access permissions. When FortiGate receives the Access-Accept message, it changes the role of the client session allowing the device access to the network.
9. A RADIUS accounting request is sent by FortiGate to FortiAuthenticator to verify whether the user has already established a session, or if an existing session in progress.
10. A RADIUS accounting response is sent back after the accounting record is written on FortiAuthenticator after the request has been verified.
11. Following a successful authentication and initiation of the user session, the client is redirected to the originally requested URL, which should now be accessible.
12. The user should be able to access the website and a countdown for the captive portal session timeout begins.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

HTTPS POST

- Uses HTTPS instead of HTTP for user authentication
  - Users credentials are protected by an SSL tunnel
- Configurable from FortiManager on a per device basis
  - Using a CLI Configuration
- The default port used for HTTPS authentication is 1003
  - If required, you can change this port using a FortiManager **System : Admin Settings** configuration



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

13

During the redirection process, user credentials can be communicated, secured, and encrypted, to the captive portal server. You can configure authentication to use HTTP over SSL by deploying a CLI Configuration from FortiManager.

The default port used for HTTPS authentication is 1003. If you need to change the port, you can change the **auth-https-port** value located in **Device Manager** > **Device & Groups** > **Device** > **System : Admin Settings** > **Advanced Options**.

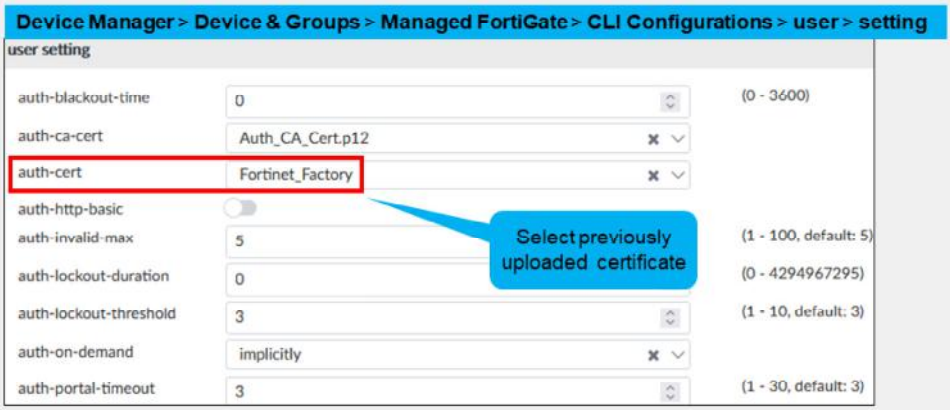
Both of these settings are configurable centrally, but only on a per-device basis. You cannot use a provisioning template.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Authentication Certificate

- By default, FortiGate presents users with a factory default certificate on the authentication page
- An alternative certificate can be specified from FortiManager



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

14

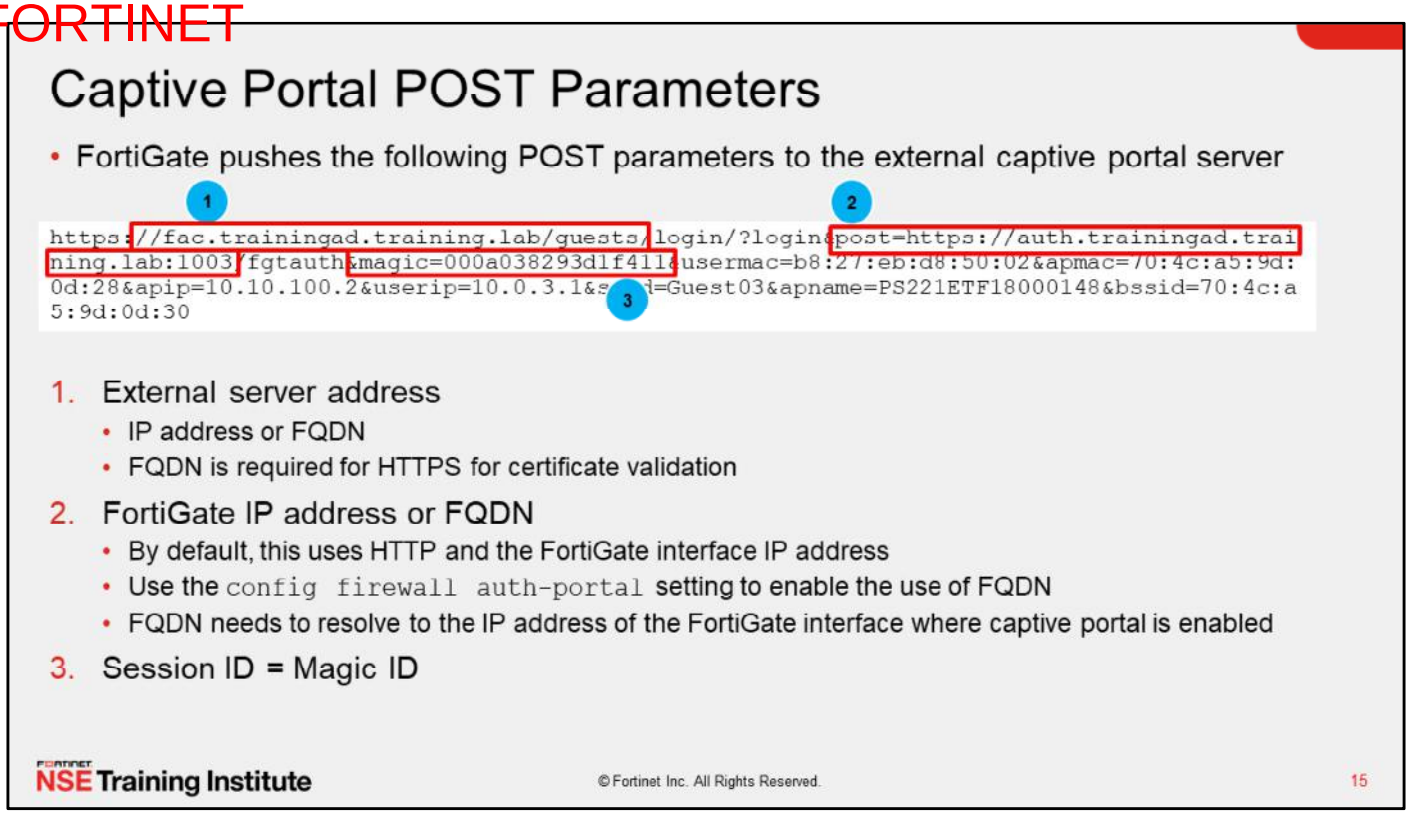
If you redirect the authentication page to an HTTPS page, FortiGate presents the currently configured server certificate.

Note that this certificate is different from the Wi-Fi certificate covered in the previous lesson. This certificate secures the captive portal webpage; the Wi-Fi certificate identifies and authenticates the controller when it is operating as the authentication server.

The FortiGate factory certificate is self signed and will generate a certificate warning in the guest's browser. Most administrators would want to avoid this. In the previous module, you saw how you could install certificates on FortiGate using FortiManager. You can use the same process to install a publicly signed certificate that you can specify here. Assuming the browser trusts this certificate, this will prevent the worrying certificate warnings.

Vouchers & Dumps are Available | WhatsApp +201224560923

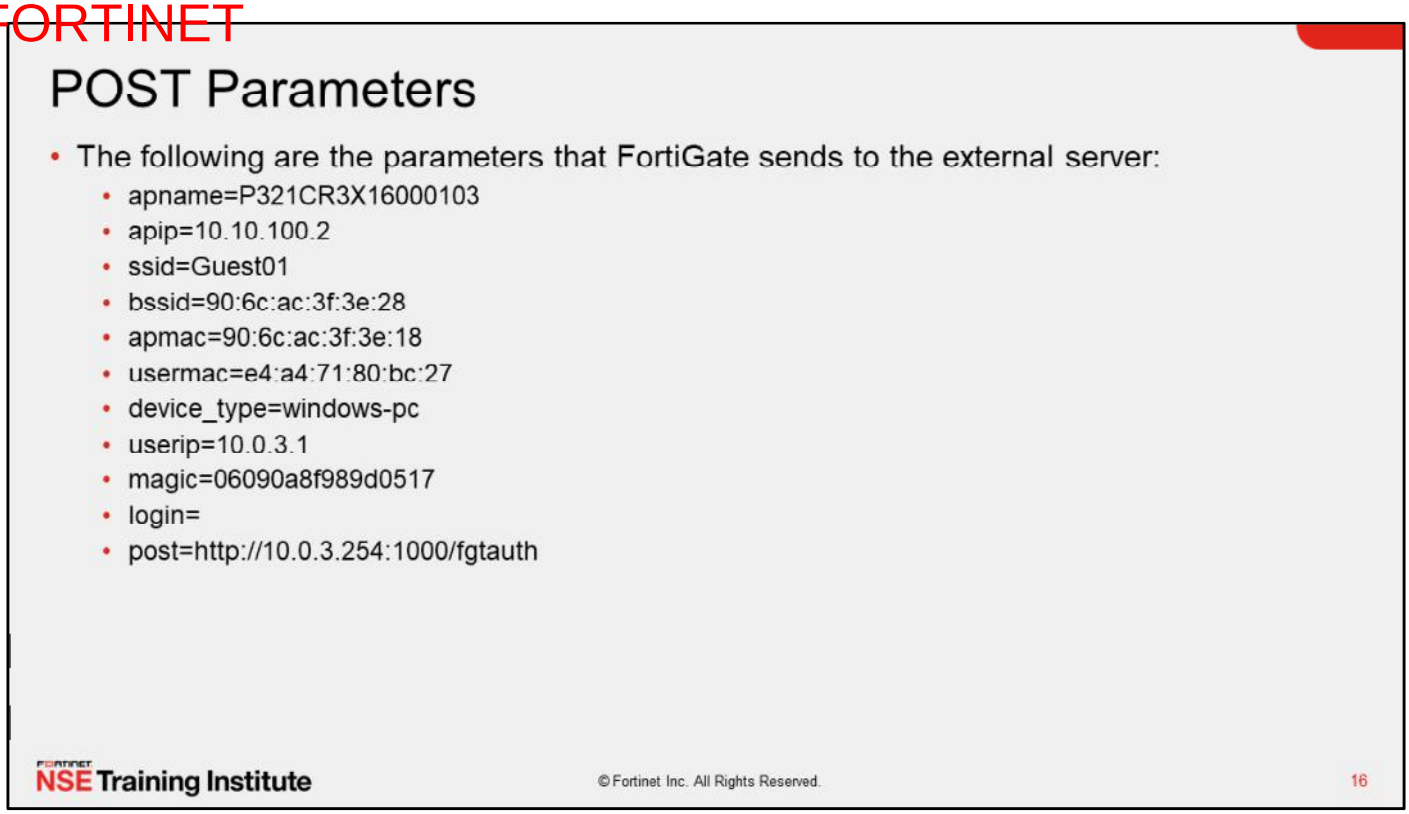
DO NOT REPRINT
© FORTINET
Brave-dumps.com



When FortiGate redirects a user to the external captive server, it adds the parameters shown on this slide to the HTTPS request. You can easily decode the information that FortiGate provides to the external captive portal server. The first part of the redirected URL includes the external server's address, followed by the address of the FortiGate interface address that has the captive portal enabled on it. The magic parameter is the session ID that is used to track the request information.

Vouchers & Dumps are Available | WhatsApp +201224560923

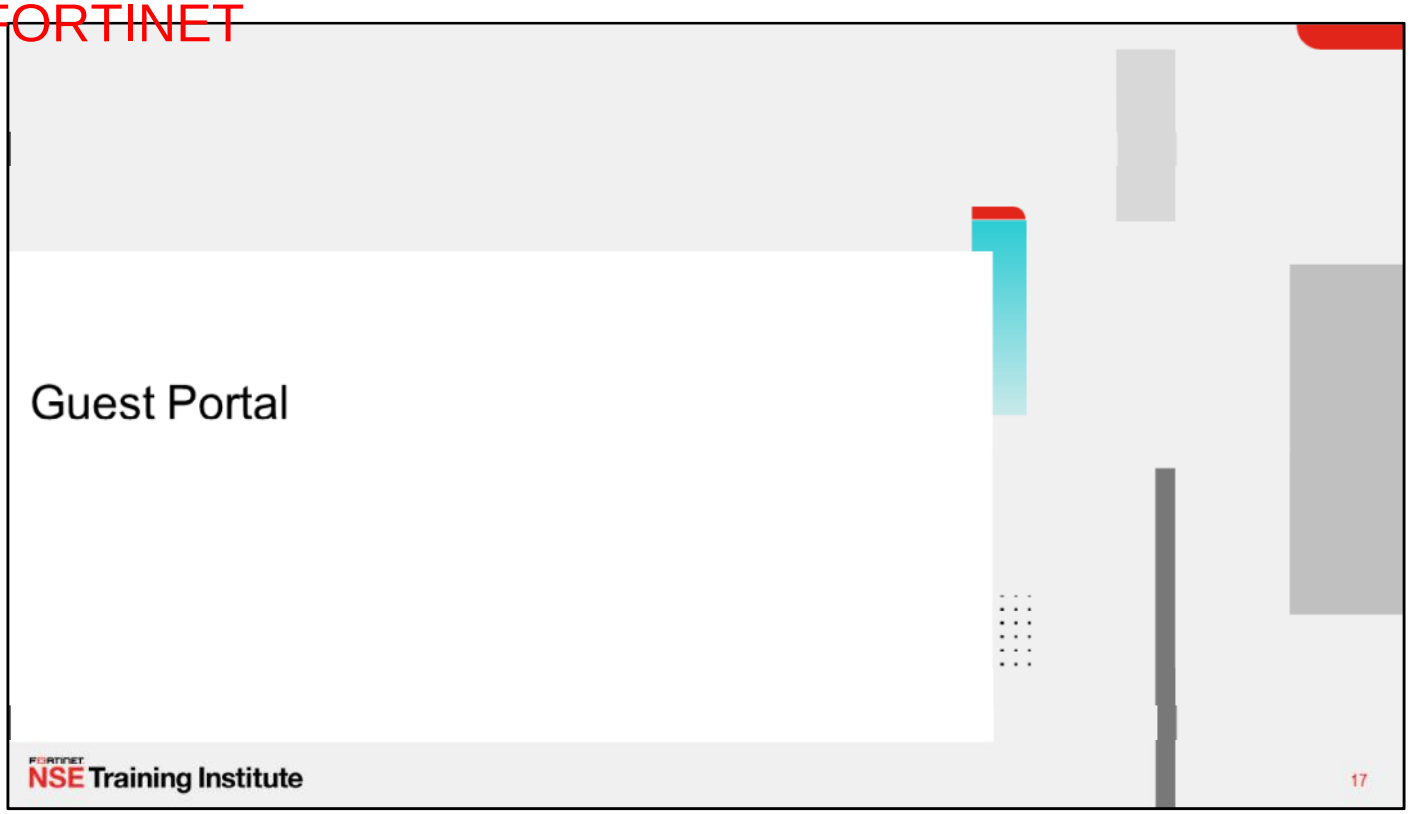
DO NOT REPRINT
© FORTINET
Brave-dumps.com



This slide contains a list of all the parameters that are sent to the external captive portal from a wireless network on FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

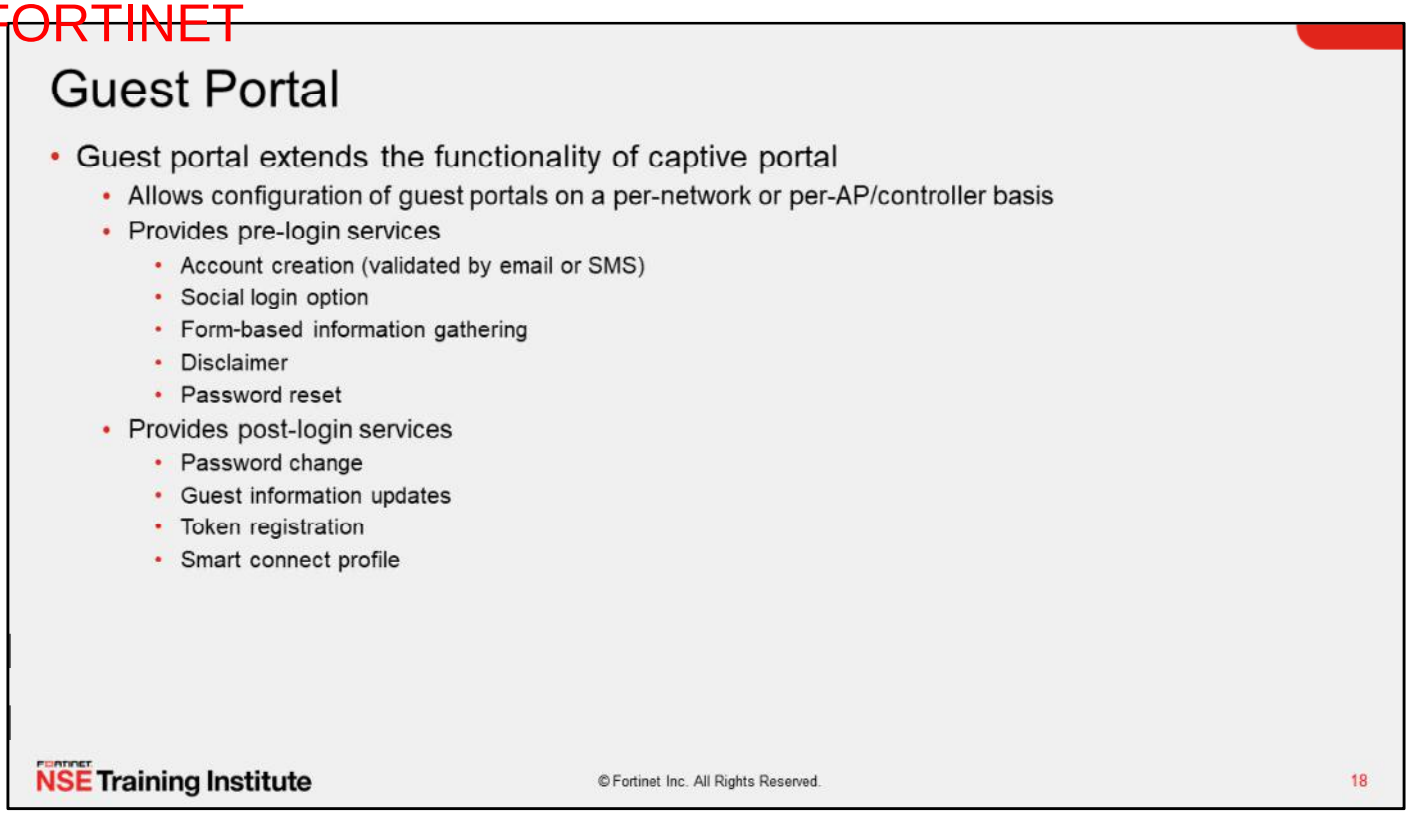
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn about the guest portal options available on FortiAuthenticator.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The guest portal on FortiAuthenticator extends the functionality of the captive portal available on FortiGate. The FortiAuthenticator captive portal is available through only one URL; however, portal match is based on the mapping rules and RADIUS client profile, which makes this type of configuration very flexible and scalable. You can configure multiple guest portals on FortiAuthenticator that can serve users connecting to different FortiGate devices or networks. FortiAuthenticator uses HTTP POST parameters that are sent by FortiGate in the captive portal request, along with RADIUS client configurations, to map incoming captive portal requests to their respective guest portals. You can define mapping rules based on the subnet address, AP MAC address, SSID, AP location, and so on. All these parameters are sent by FortiGate to FortiAuthenticator using HTTP POST.

The guest portal offers pre-login and post-login services for users who are authenticating using FortiAuthenticator. As the name suggests, pre-login services are available to users without authentication, and post-login services are offered after successful authentication. Pre-login services include creating guest accounts with the option to validate by email or SMS, a social login option, form-based information gathering, disclaimer, password reset, and so on.

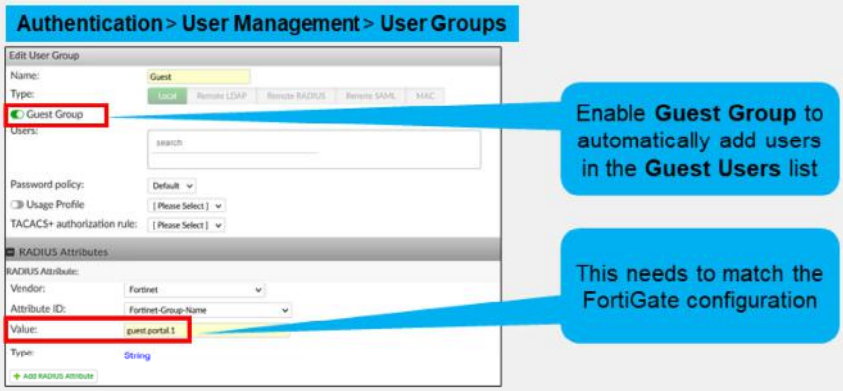
After the user logs in successfully, they can access the post-login services page by visiting FortiAuthenticator login page. On that page, users can make changes to their account, such as updating their information, changing their password, downloading a smart connect profile, and performing token registration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Guest Group

- Create a guest user group
  - Reference this group in the guest portal for automatic mapping of new users
- Configure the RADIUS attribute that is sent to FortiGate after a successful authentication
  - FortiGate uses the group name sent to assign authorization to users



NSE Training Institute

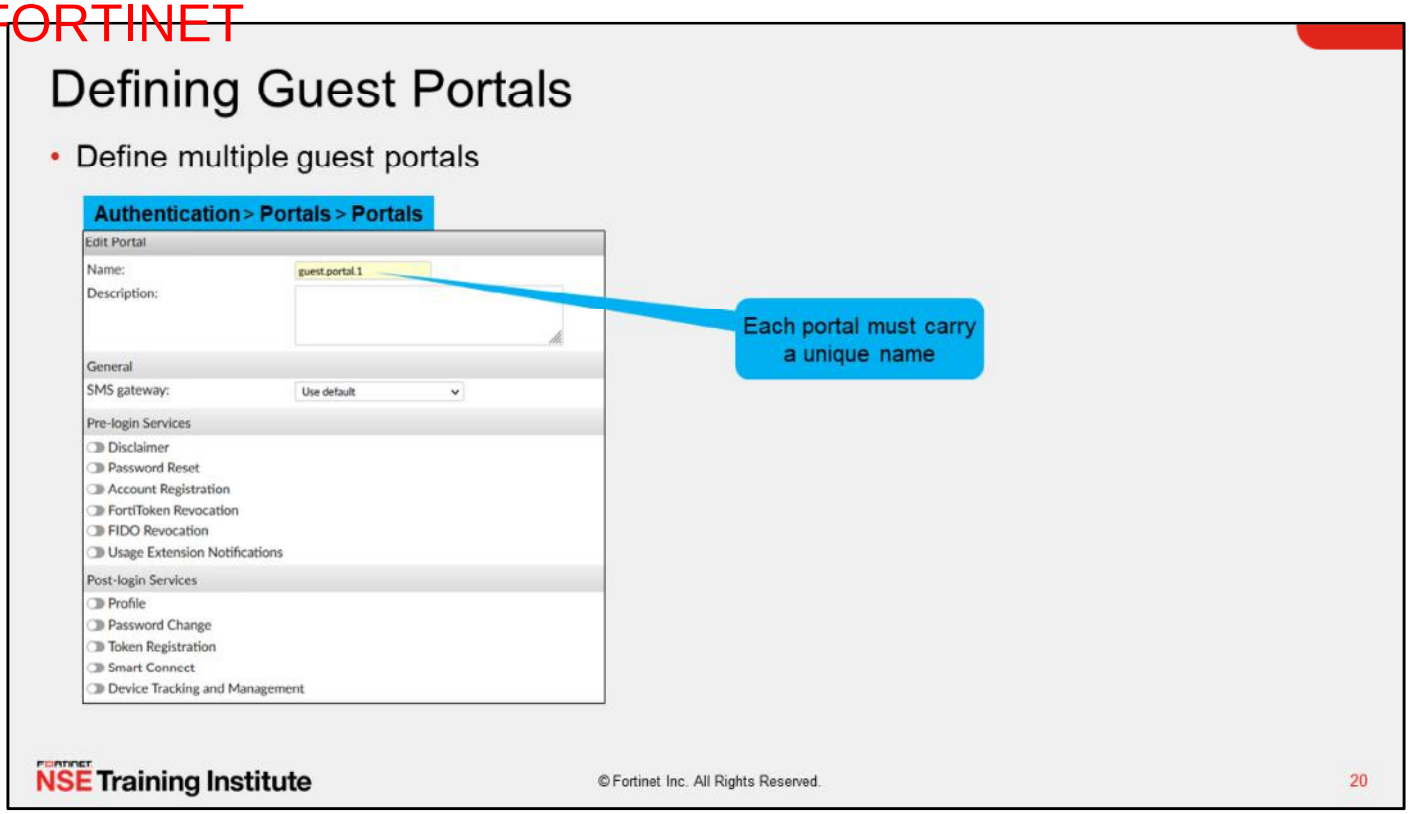
© Fortinet Inc. All Rights Reserved.

19

When configuring the guest portal, you should start by creating a guest user group on FortiAuthenticator. You can reference this group to the guest portal configuration, so that any user who registers through the guest portal will be put in this group. You can enable **Guest Group** to add newly self-registered users to the guest user list for another level of administrative management. You can use RADIUS attributes, such as group name, to associate users with a group on FortiGate. This will act as an authorization tag and you can reference that group in a firewall policy configuration. The RADIUS attribute value is case sensitive and must match the FortiGate guest group configuration.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



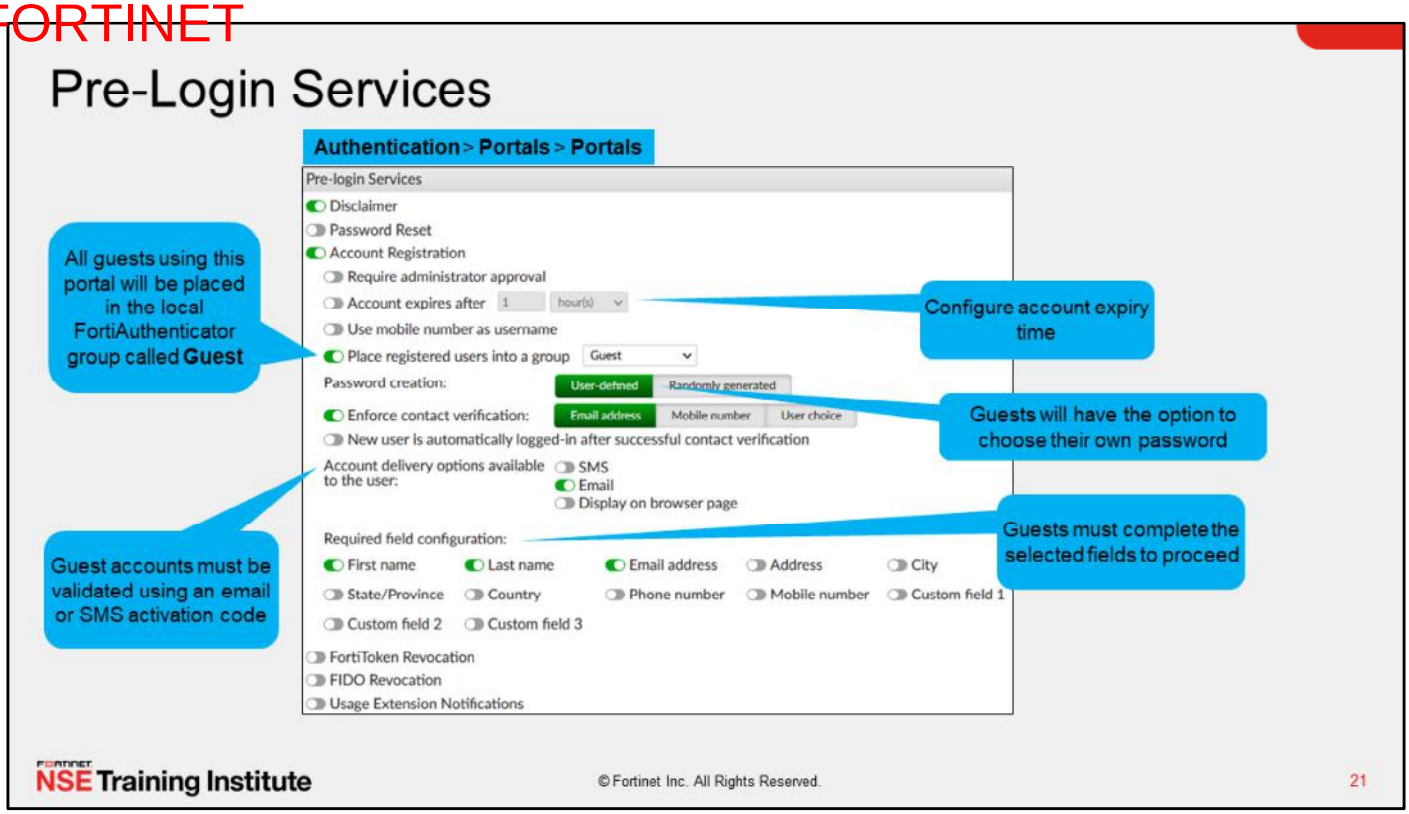
You start by defining the guest portals on the **Portals** configuration page, using the FortiAuthenticator GUI. The portal policy will then configure how the portal is used.

All portals will be accessible on the same URL, but the mapping of the portals will depend on the portal policy.

Portal creation consists of assigning a unique name to the portal and, if desired, an SMS gateway for end-user notifications. If you don't have an SMS gateway, you can use the FortiGuard Messaging Service, if you have valid licensing for the service.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



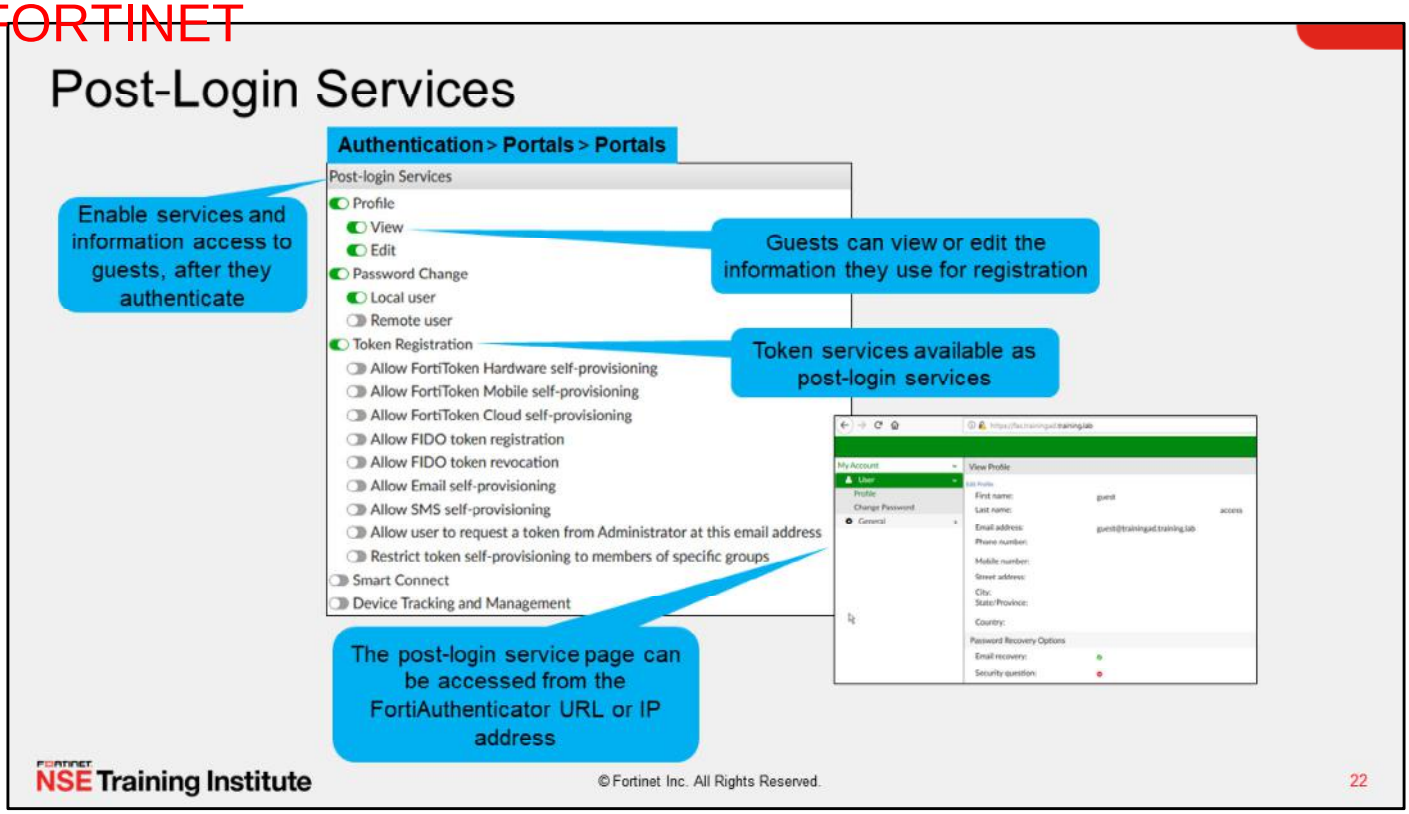
You can enable the pre-login services that you would like to use for this guest portal. The **Account Registration** option enables guest users to create and validate their account using a form-based web page. The **Account expires after** option allows you to configure the account validity period. You can apply this to all self-registered accounts. You can also enable the administrator approval option, which would require an administrator to enable all self-registered accounts manually.

All guest accounts created using the **Account Registration** option will be placed in the group defined by the **Place registered users into a group** option. FortiAuthenticator can randomly generate a password for the guest user, or you can let users pick their own password. All accounts registered through the guest portal must be validated through SMS or email before they can be used to log in. FortiAuthenticator will send the guest user an activation code that will be used to activate their account. In this case, administrators do not have to manually activate each self-registered account request.

You can select the mandatory field that a user must fill out at the time of account registration. The selected field cannot be left empty. The **FortiToken Revocation** option adds a **"Lost my token"** link to the guest portal token verification page. Users can click this link if they need to request that their existing mobile token be re-provisioned, switch to an email token, or disable their account.

Vouchers & Dumps are Available | WhatsApp +201224560923

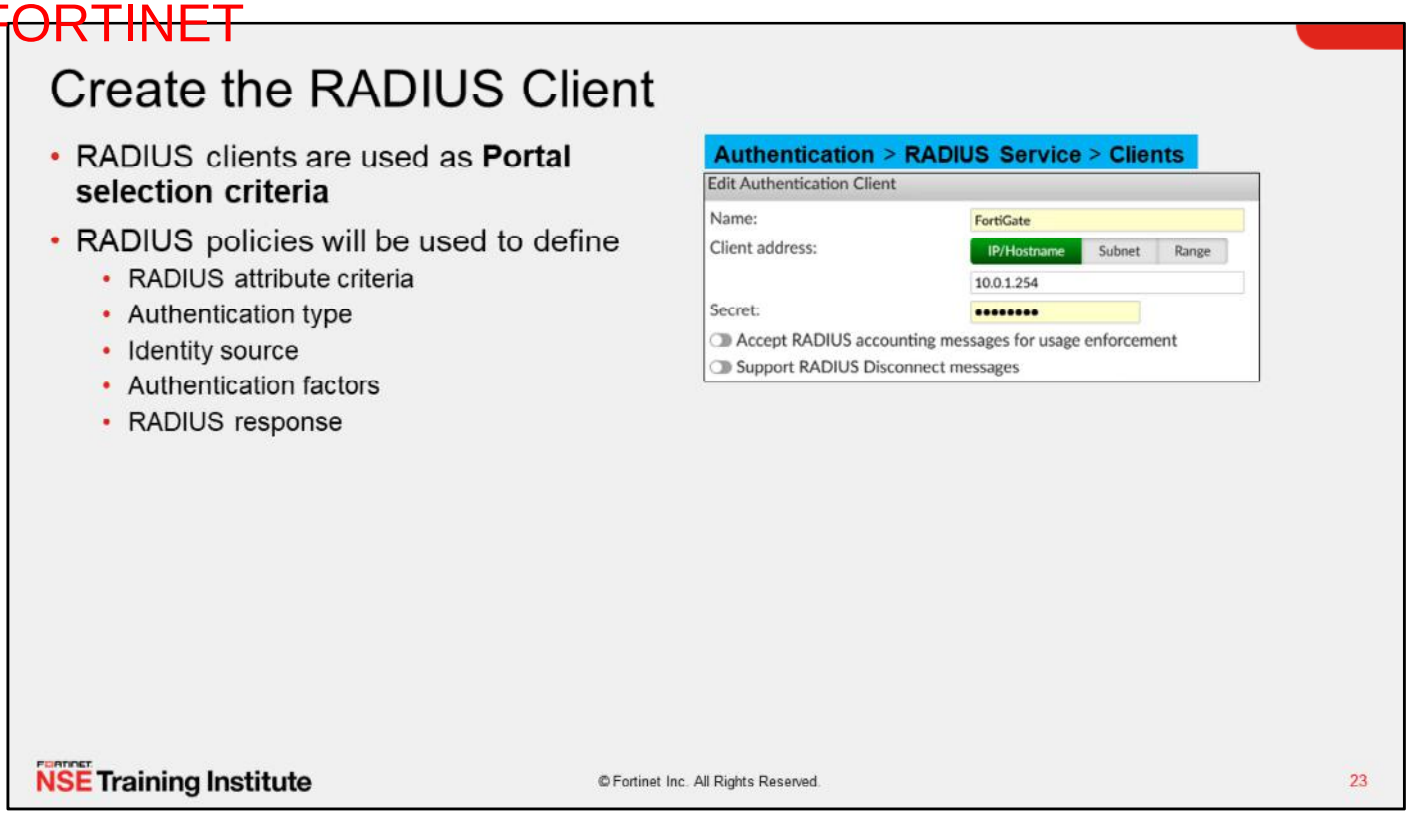
DO NOT REPRINT Brave-dumps.com
© FORTINET



On the same configuration page, you can also select what post-login services users will have access to. Post-login services will be available only to users after they authenticate. **Profile** options will allow users to view or edit their account information, such as name, email, phone number, and so on. You can also give users the ability to change their password. **Token Registration** options allow users to self-provision or request a new token from the administrator. The **Smart Connect** option allows users to download a smart connect profile for their networks. The **Device Tracking and Management** option allows administrators to assign all guest devices to a device group. Users must register all their devices before they are allowed to access the network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



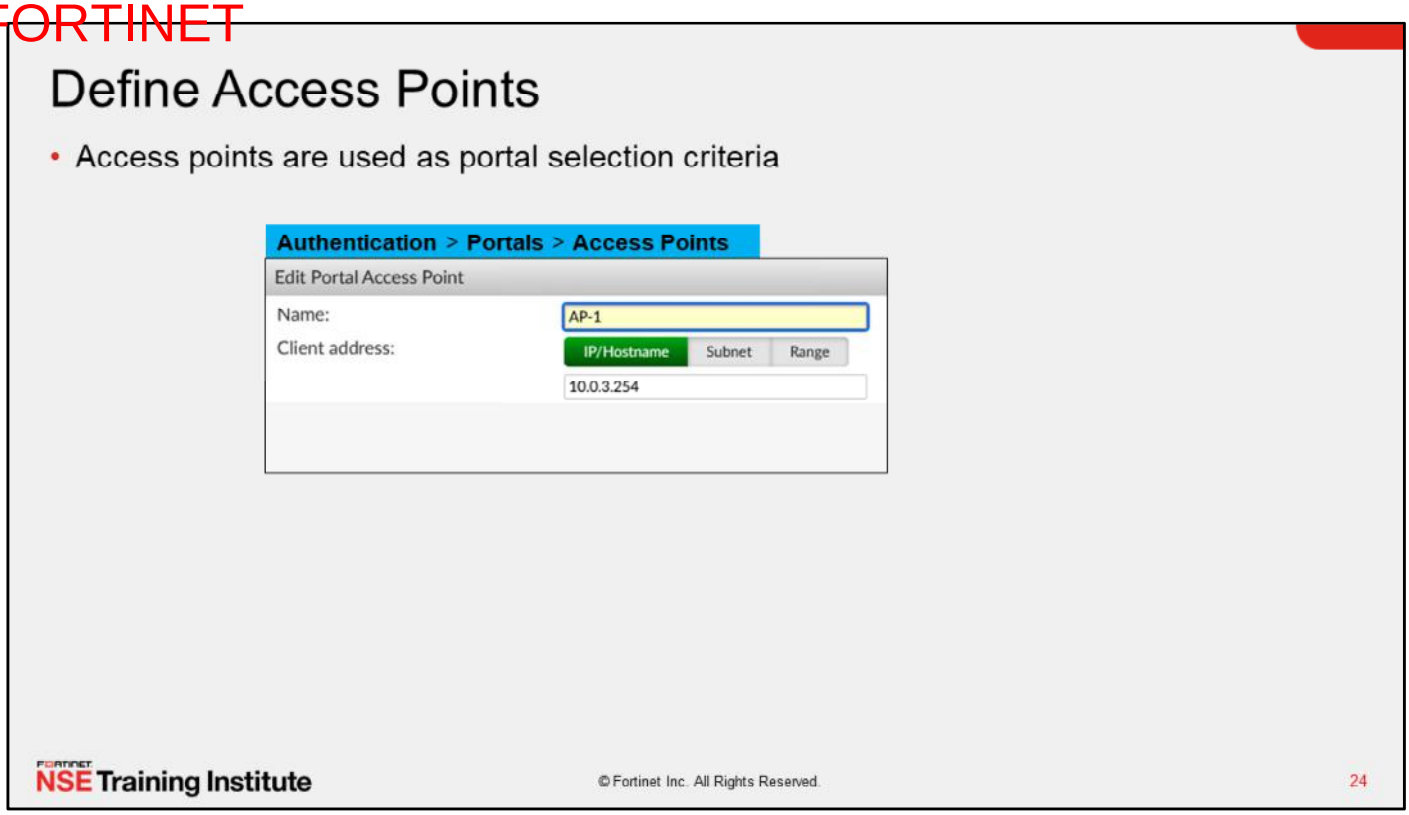
Before you can enable captive portal, you must create a RADIUS client. You do this on the **Clients** page. The RADIUS client is necessary so that FortiAuthenticator can accept RADIUS authentication requests from FortiGate. (FortiGate becomes registered as an authentication client.)

You will also need to create a RADIUS policy and assign the RADIUS client to that policy. The policy defines the way that FortiAuthenticator processes RADIUS communications with the client, including **Authentication type**, **Identity source**, **Authentication factors**, and so on.

Note that self-registered guest users will be added to the local FortiAuthenticator database. Make sure that the RADIUS profile is configured to use a realm that allows the processing of local user authentication.

Vouchers & Dumps are Available | WhatsApp +201224560923

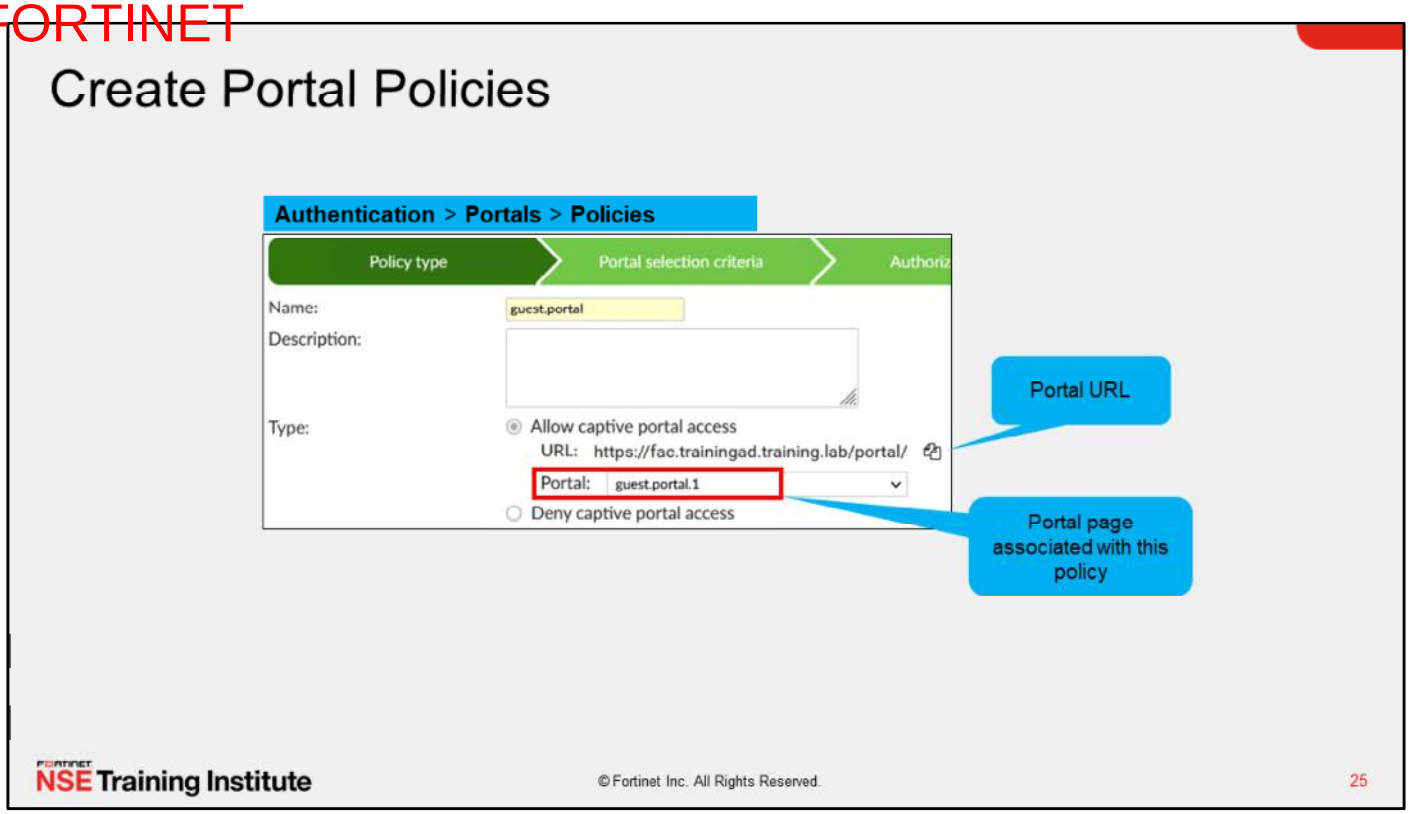
DO NOT REPRINT
© FORTINET
Brave-dumps.com



An access point (AP) is configured for use as a portal selection criteria in an access policy. The APs will define where an end user is being redirected from, in order to be directed to a specific portal.

Vouchers & Dumps are Available | WhatsApp +201224560923

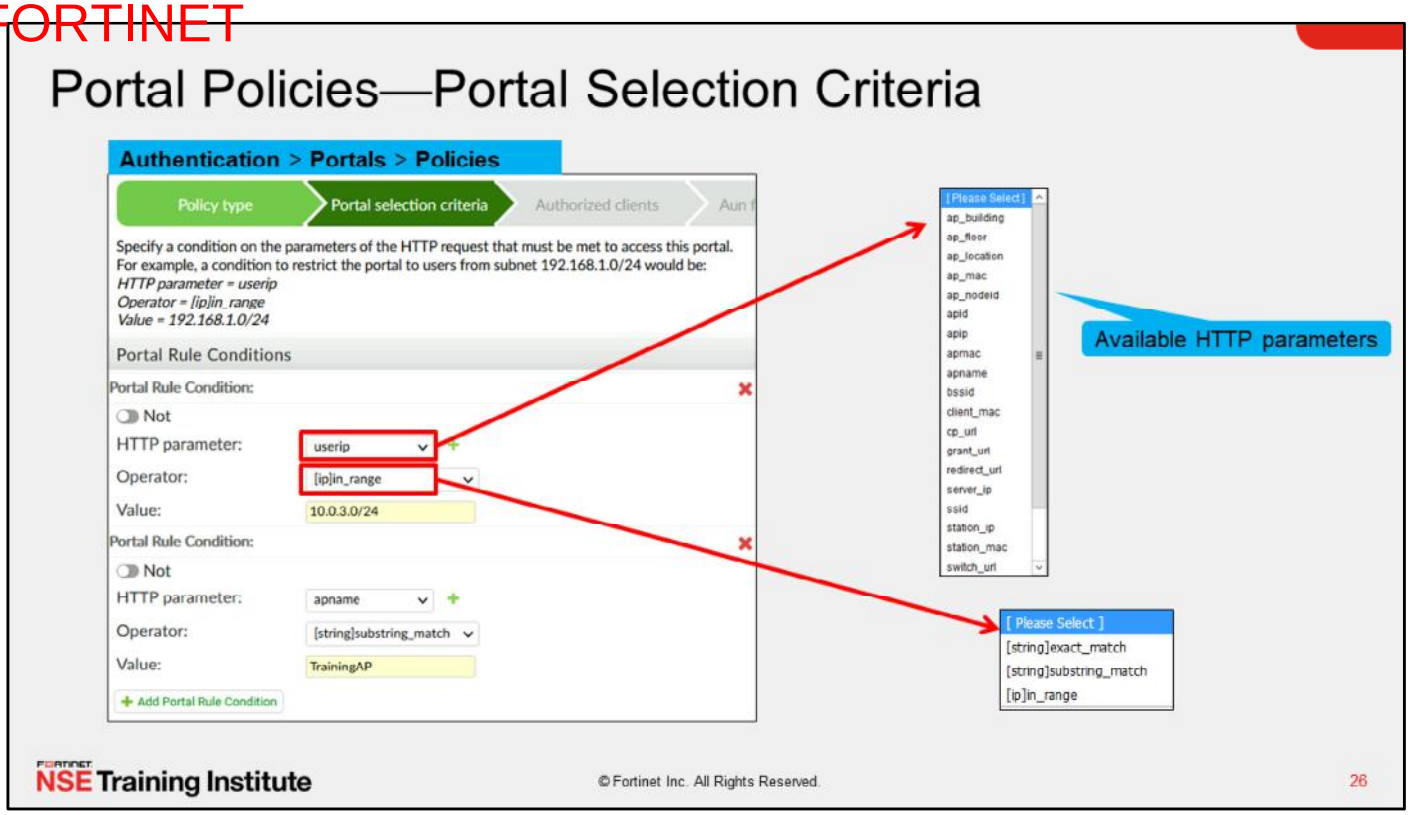
DO NOT REPRINT Brave-dumps.com
© FORTINET



Portal policies are used to both determine the appropriate portal, and the means in which the user is authenticated. Portal polices are configured using a multi-step policy wizard. The initial step, **Policy type**, is used to provide a name and description for the policy, as well as the type of access that will be enforced. The settings in the **Type** field allow you to direct users to a designated portal, which you select in the drop-down list, or select **Deny captive portal access** to deny portal access. The policy match criteria are defined by the configuration options that you set in other policy wizard steps.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



You must configure a portal policy to present the portal page to the guest.

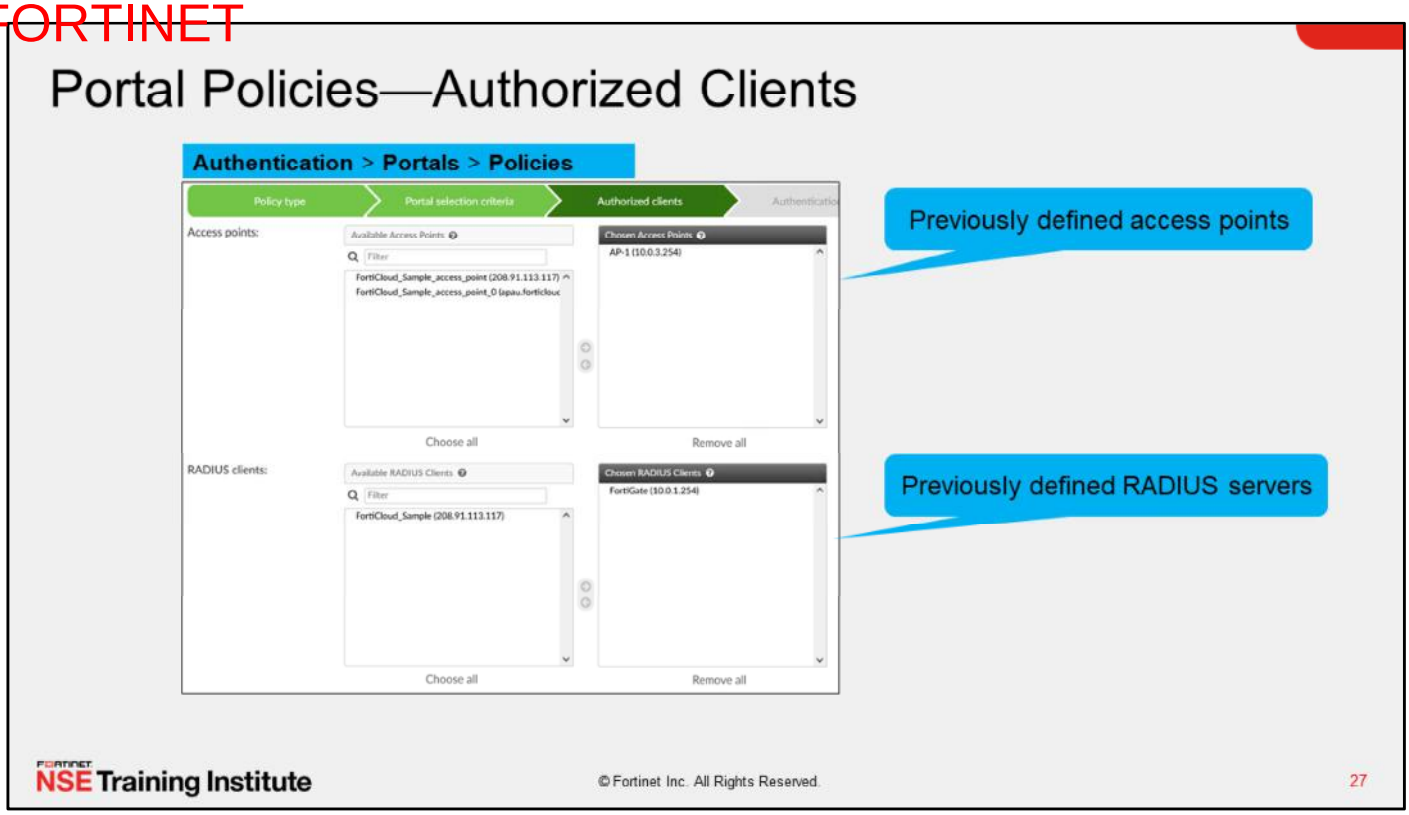
Guest portal rules use the incoming POST parameters and conditions defined within the rules to map the request to guest portals. You can define one or multiple conditions that must be matched to the POST parameter before a captive portal request is mapped to a guest portal login. You can select an HTTP parameter and use one of the three predefined operators (**exact_match**, **substring_match** or **in_range**) to add a condition. You must define values of a condition manually.

For example, if you would like to present a portal to users who connect from an IP address in the range of `10.0.3.0/24`, you would set the following conditions:

HTTP parameter: **userip**
Operator:[ip] in_range
Value: `10.0.3.0/24`

Vouchers & Dumps are Available | WhatsApp +201224560923

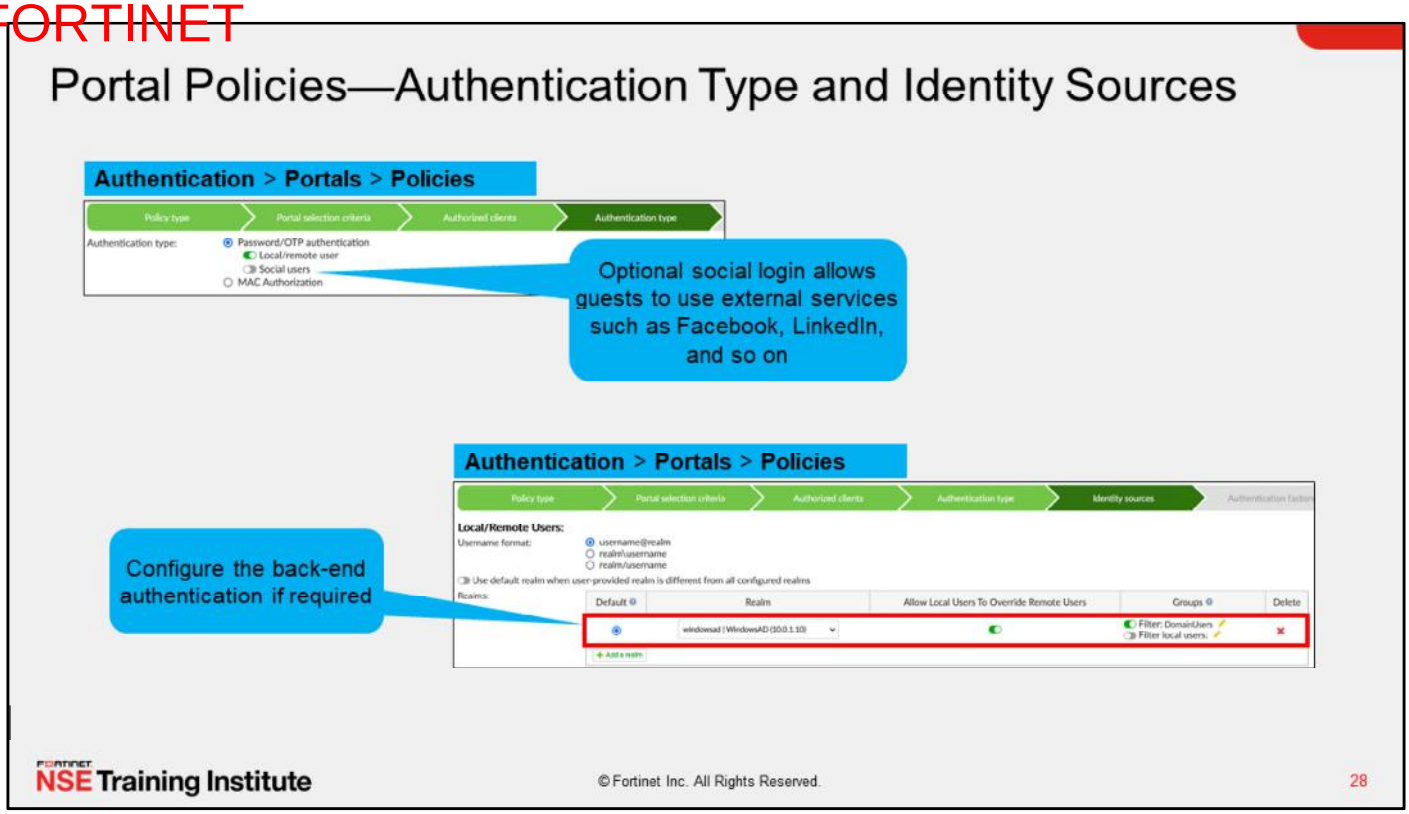
DO NOT REPRINT Brave-dumps.com
© FORTINET



In addition to the POST parameters, page presentation can be dependent on point of connection (the AP) and RADIUS message source. You define the access points and RADIUS clients on the **Authorized clients** page, by moving existing entries for each type to the **Chosen Access Points** and **Chosen RADIUS Clients** lists.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Within the **Authentication type** option, you can also define the type of authentication (user or device) as well as whether you want to use it for account login and/or social login.

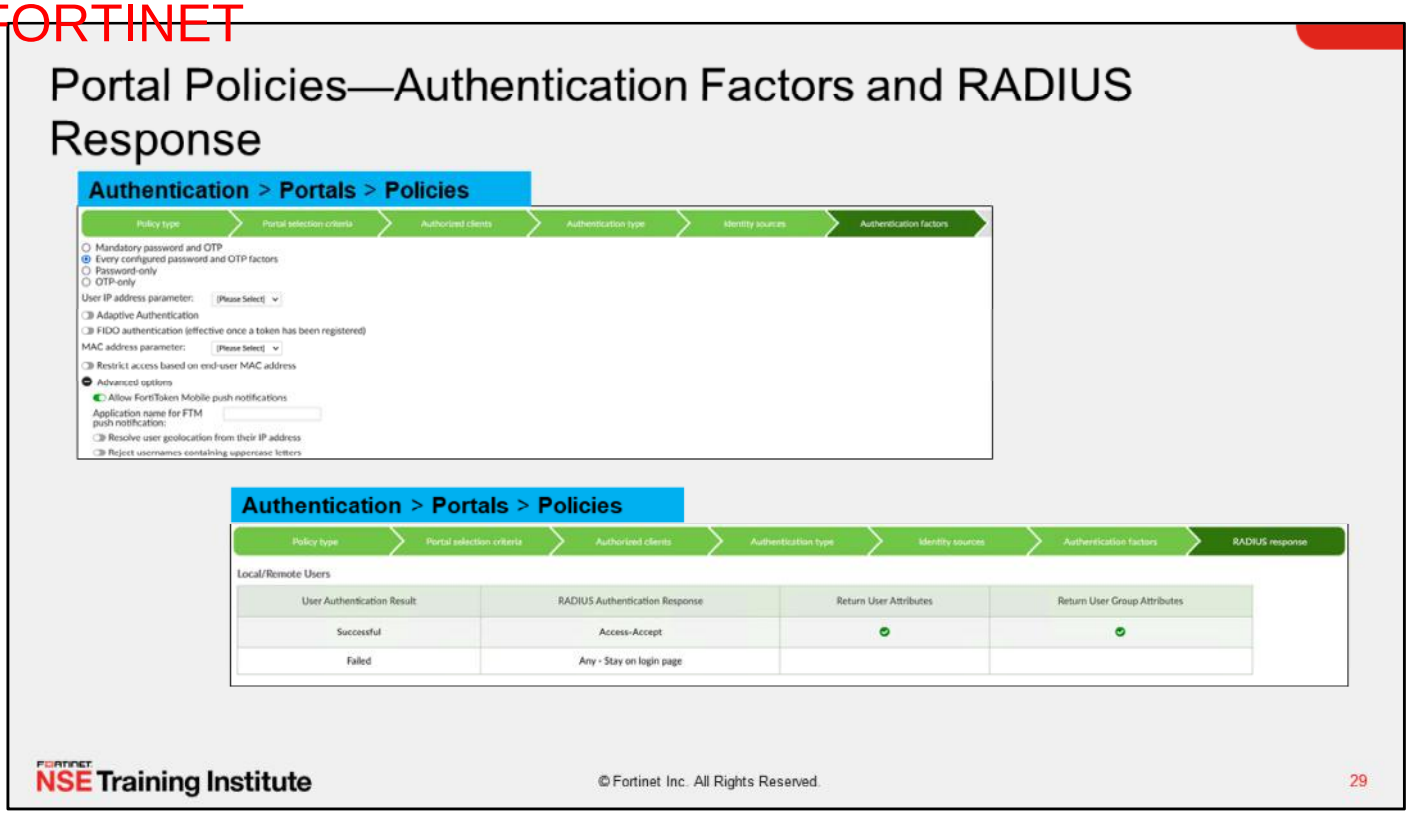
The social user login option allows users to authenticate using third-party SSO services such as Facebook, LinkedIn, and so on. You must configure social login profiles to use this method. Account login means that user credentials will be provided by FortiAuthenticator's internal database or remote authentication server.

You configure the back-end authentication details on the **Identity sources** page. If you have enabled social users as an authentication type, you will select the social platforms that will be available for user authentication. The options are **Facebook**, **Google**, **Twitter**, **Linkedin**, **Phone number**, and **Email**. For each option, other than phone number and email, you will need to configured a remote OAUTH server.

In the **Local/Remote Users** section, you will select the desired username format and realms. Each selected realm can be filtered down to the group level.

Vouchers & Dumps are Available | WhatsApp +201224560923

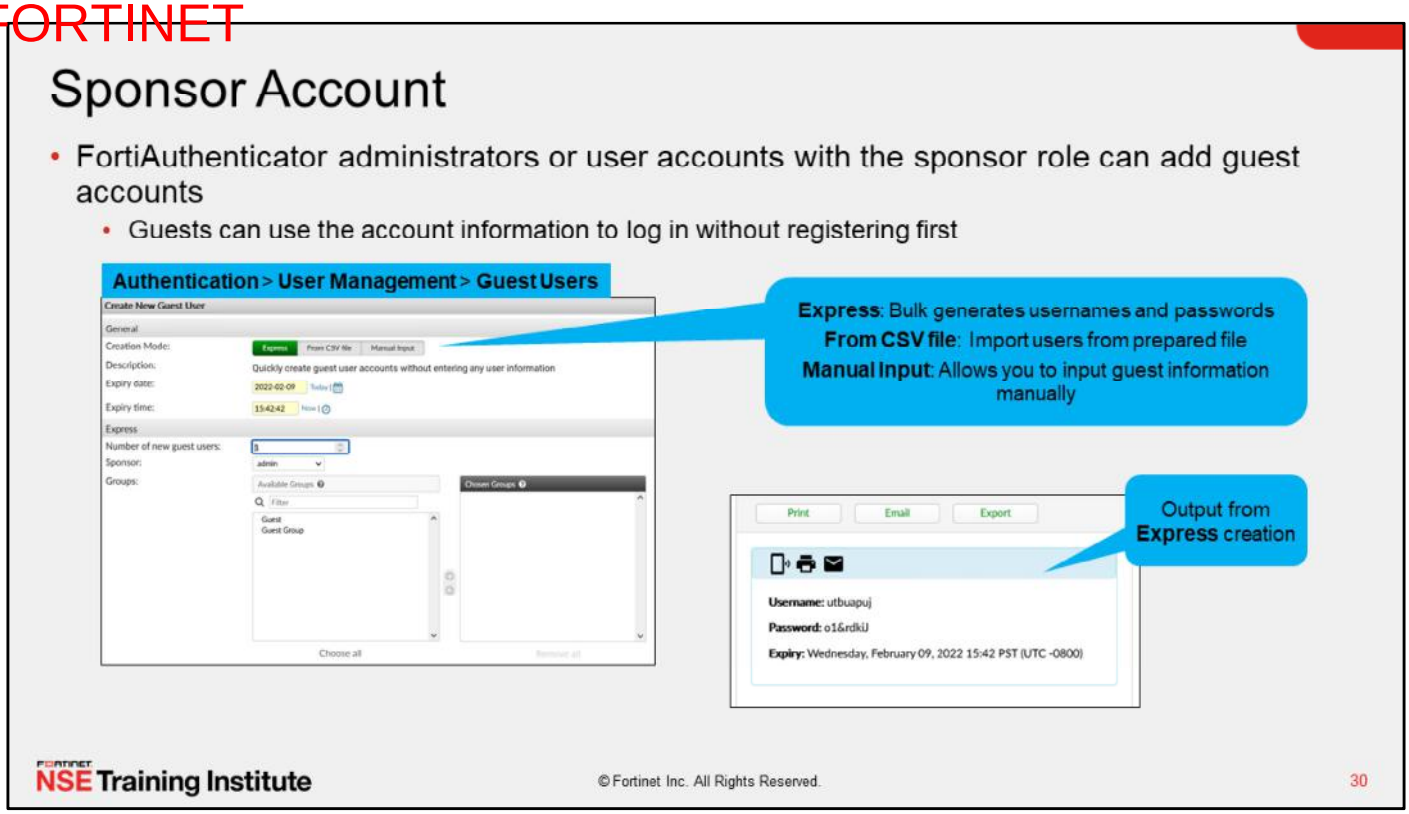
DO NOT REPRINT
© FORTINET
Brave-dumps.com



You define authentication requirements, such as mandatory two-factor authentication, password-only authentication, and so on, on the **Authentication factors** page. The **RADIUS response** page provides a summary of the RADIUS response for each authentication result.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



FortiAuthenticator allows administrator and user accounts that have sponsor permission to sponsor guest accounts for their visitors. Sponsor accounts are temporary accounts that are created by an administrator or user for visitors. Local users can log in to FortiAuthenticator and sponsor one or more guest accounts. There are three creation modes: **Express**, **From CSV file,** and **Manual Input**.

Express mode bulk creates multiple users and their login details automatically. Users must define the account expiry date and time before they can create a guest account. You can also select the number of guest account, and the sponsor and groups assigned to them. When you create the accounts, FortiAuthenticator will display the login information in a table. You can choose to send this information to guests directly using SMS or email. Alternatively, you can print or export the login information to a CSV file.

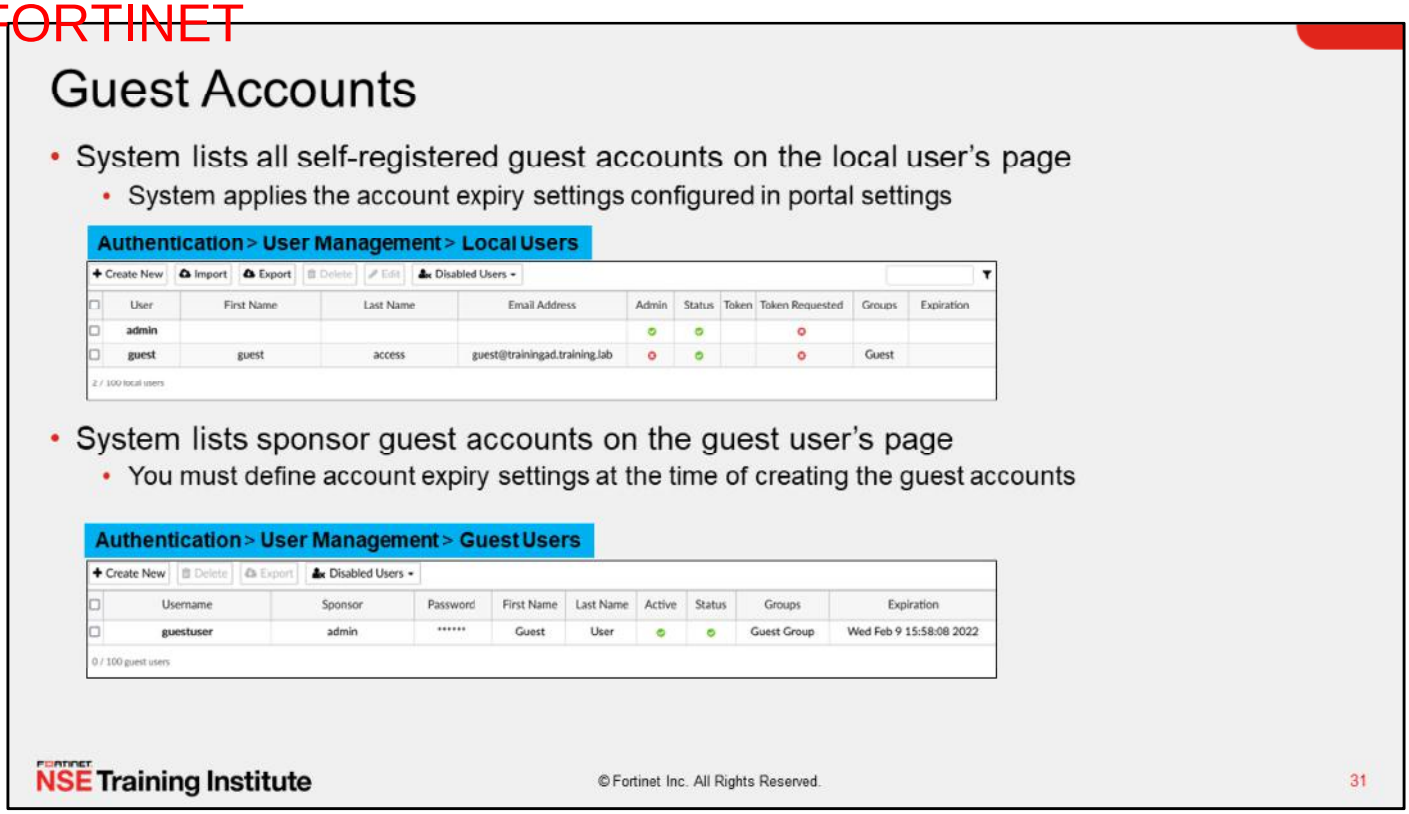
From CSV file creation mode allows administrators to create one or more guest accounts using parameters from a CSV file. Format each line of the CSV with the following values:

```
<first name>, <last name>, <email>, <mobile>, <group>
```

Manual Input mode requests the administrator or users to manually fill in the information for their guests, such as name, address, phone number, and so on. They must also manually define the username and password when using this mode.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



It is important to note that all the self-registered guest accounts will be listed on the **Local Users** page on the FortiAuthenticator GUI. The system will automatically assign an expiry date to all self-registered users as defined in the guest portal settings.

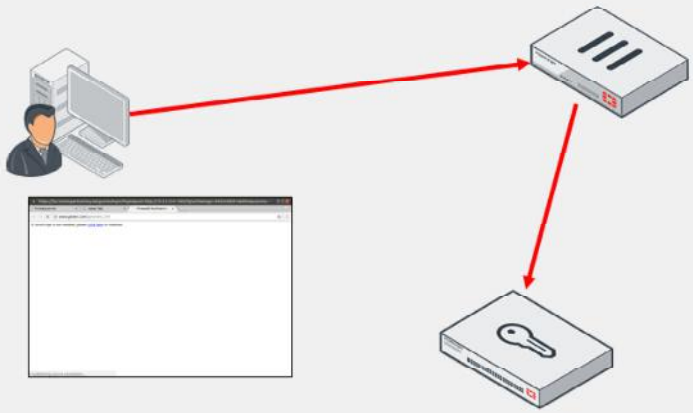
Sponsor accounts will be listed on the **Guest Users** GUI page on the FortiAuthenticator GUI. These accounts will expire according to the expiry date and time selected at the time of account creation.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Guest Portal Workflow

- FortiGate receives HTTP GET requests from users
- Redirects them to FortiAuthenticator
- FortiGate collects and sends the following POST parameters to FortiAuthenticator:
  - apname=P321CR3X16000103
  - apip=10.10.100.2
  - ssid=Guest01
  - bssid=90:6c:ac:3f:3e:28
  - apmac=90:6c:ac:3f:3e:18
  - usermac=e4:a4:71:80:bc:27
  - device_type=windows-pc
  - userip=10.0.3.1
  - magic=06090a8f989d0517
  - login=
  - post=http://10.0.3.254:1000/fgtauth



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

32

Now, you'll review the guest portal workflow. A client connects to a captive portal network on FortiGate. The client tries to visit a website. FortiGate receives an HTTP GET request from an unauthenticated user. It redirects the user to the captive portal URL along with the POST parameters.

Vouchers & Dumps are Available | WhatsApp +201224560923

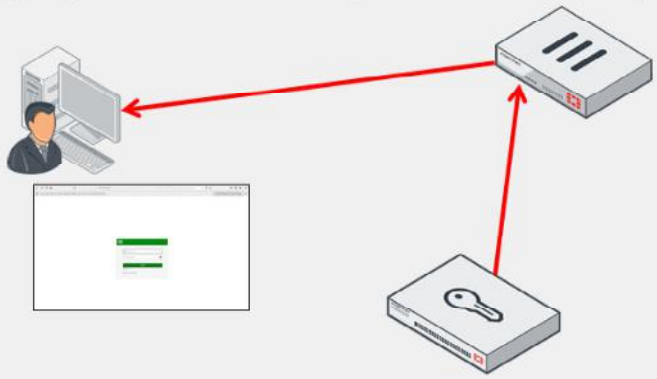
DO NOT REPRINT
© FORTINET
Brave-dumps.com

Guest Portal Workflow (Contd)

- FortiAuthenticator uses POST parameters and RADIUS client configuration to map the request to a guest portal for authentication

```
https://fac.trainingad.training.lab/guests/login/?login&post=https://auth.trainingad.training.lab:1003
/fgtauth&magic=000a038293d1f411&usermac=b8:27:eb:d8:50:02&apmac=70:4c:a5:9d:0d:28&apip=10.10.100.2&use
rip=10.0.3.1&ssid=Guest03&apname=PS221ETF18000148&bssid=70:4c:a5:9d:0d:30
```

- If mapping conditions are met, FortiAuthenticator presents the login page to the user



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

33

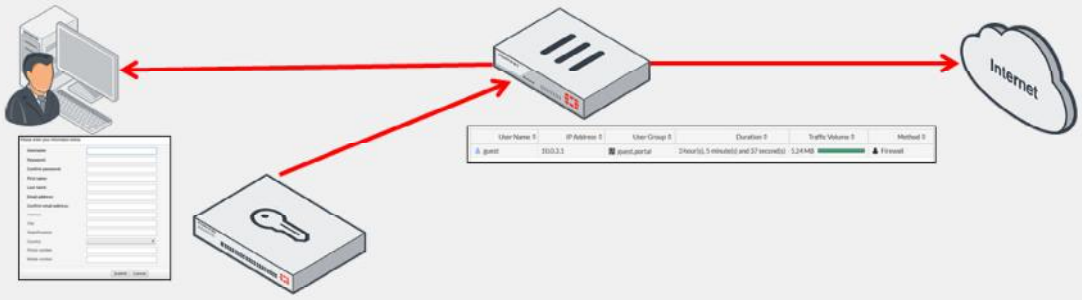
FortiAuthenticator uses the provided POST parameters and RADIUS client configuration to search the mapping rules. If all the conditions defined in a mapping rule are met, FortiAuthenticator uses the mapped guest portal and presents the login page to the user.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Guest Portal Workflow (Contd)

- Guest user registers and activates account
  - If account was a sponsored guest, you can use that account to log in directly
- Account is added to FortiAuthenticator's local user database
- Guest user logs in
- FortiGate verifies if the user group is allowed access to the requested page
- Guest user is allowed access based on the firewall policy configuration



NSE Training Institute

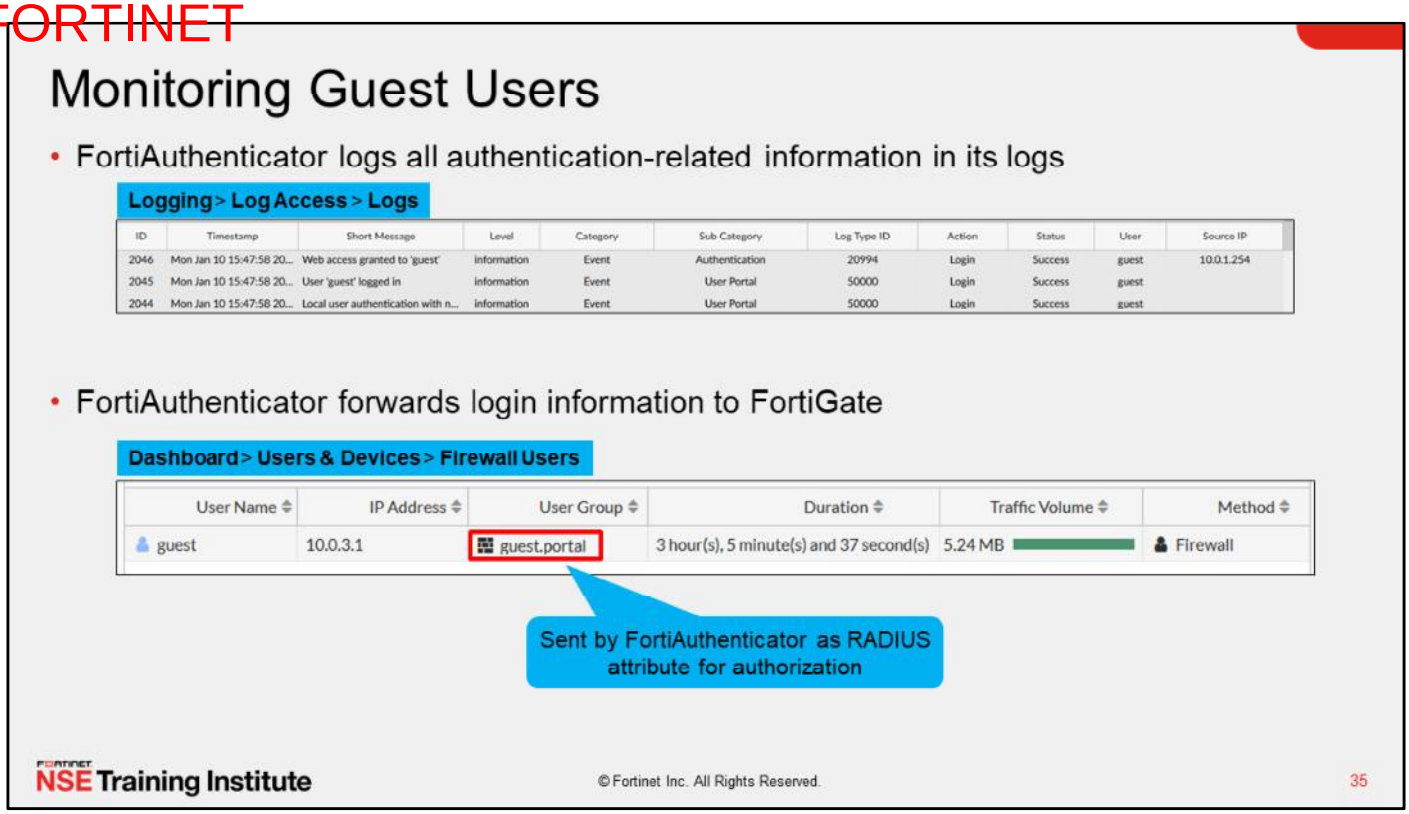
© Fortinet Inc. All Rights Reserved.

34

If the guest user does not have an account, they can click the link on the login page to register for an account. FortiAuthenticator will present them with a form-based web page to fill in. After the user fills in all the required information, including their email or phone number, or both, FortiAuthenticator will send them an activation code. This activation code is a request to finish the self-registered account creation process. After they enter a correct activation code, FortiAuthenticator will automatically add the account to its local user database and redirect the user to the login page. The user can now log in using their login credentials. After a user is authenticated, FortiAuthenticator will place them in the guest group and send the FortiGate group name using the RADIUS attribute. FortiGate will use the attribute as authorization and allow the user to access resources based on the firewall policies configuration.

Vouchers & Dumps are Available | WhatsApp +201224560923

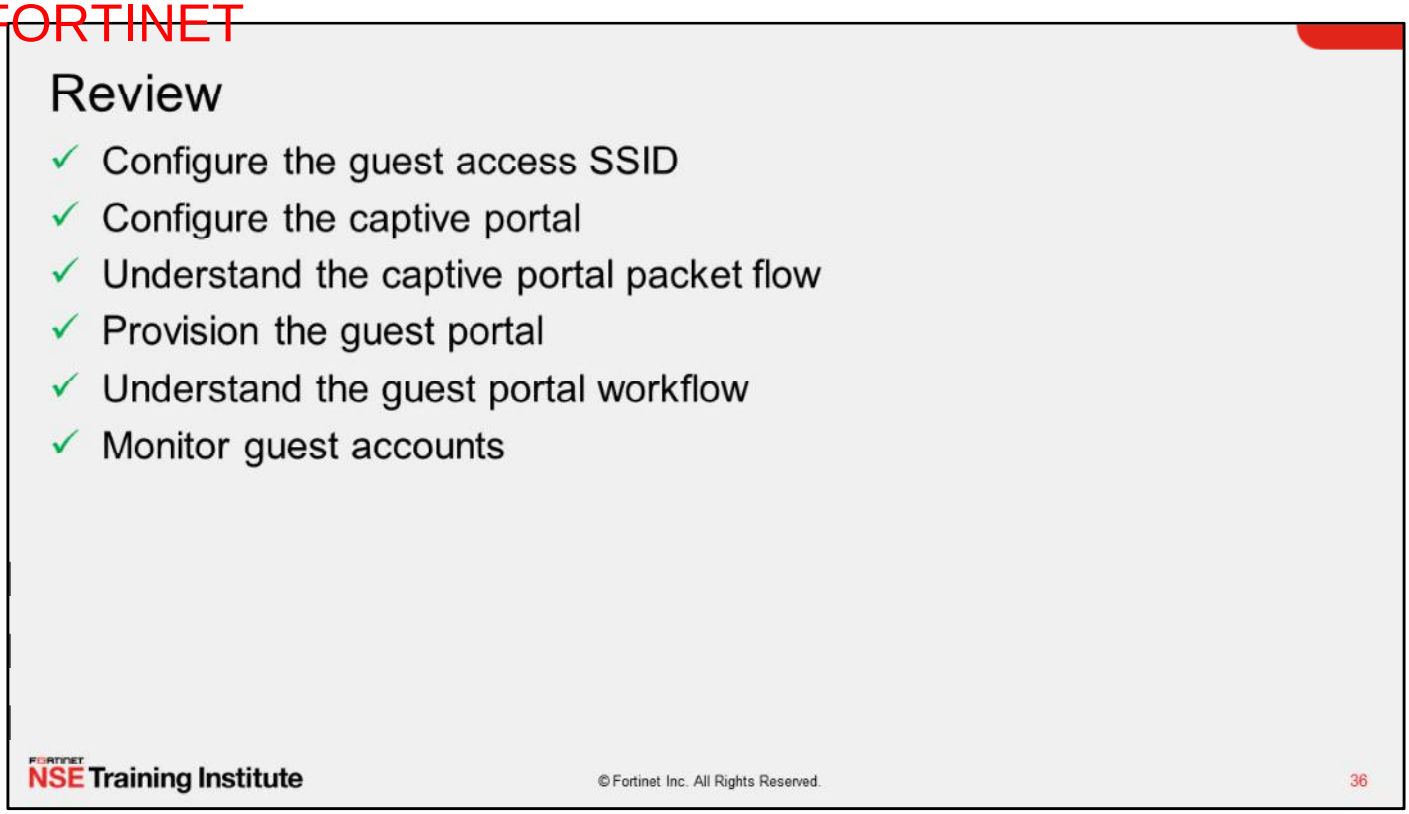
DO NOT REPRINT Brave-dumps.com
© FORTINET



FortiAuthenticator logs all authentication-related information. This information includes username, time of authentication, status, IP address, guest portal used to authenticate, and so on. You can view active user sessions on FortiGate on the **Firewall Users** monitor, which lists the username, user group, duration of the session, and IP address.

Vouchers & Dumps are Available | WhatsApp +201224560923

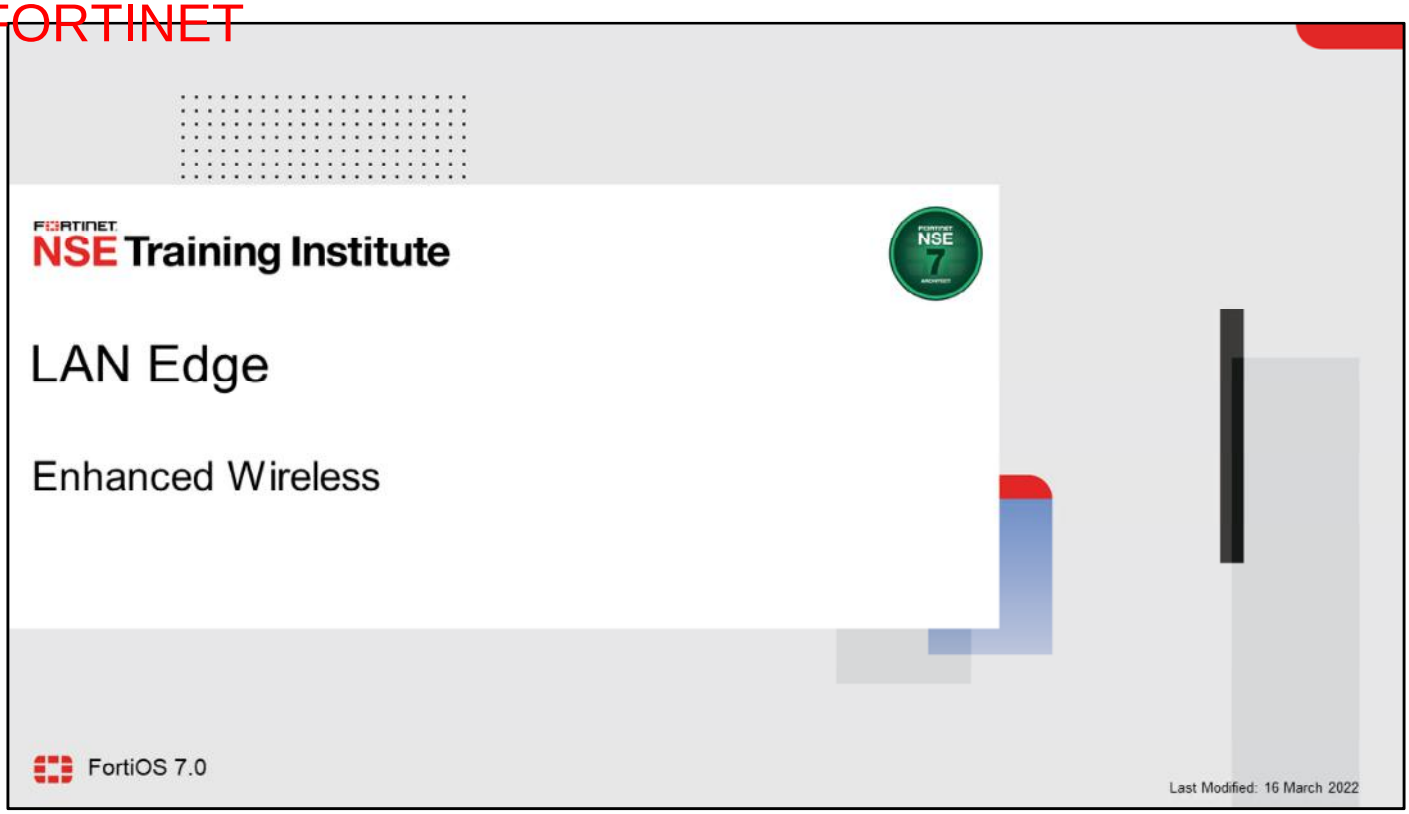
DO NOT REPRINT
© FORTINET
Brave-dumps.com



By mastering the objectives covered in this lesson, you learned how configure and use integrated wireless features on FortiOS and FortiAuthenticator to deploy a captive portal guest network.

Vouchers & Dumps are Available | WhatsApp +201224560923

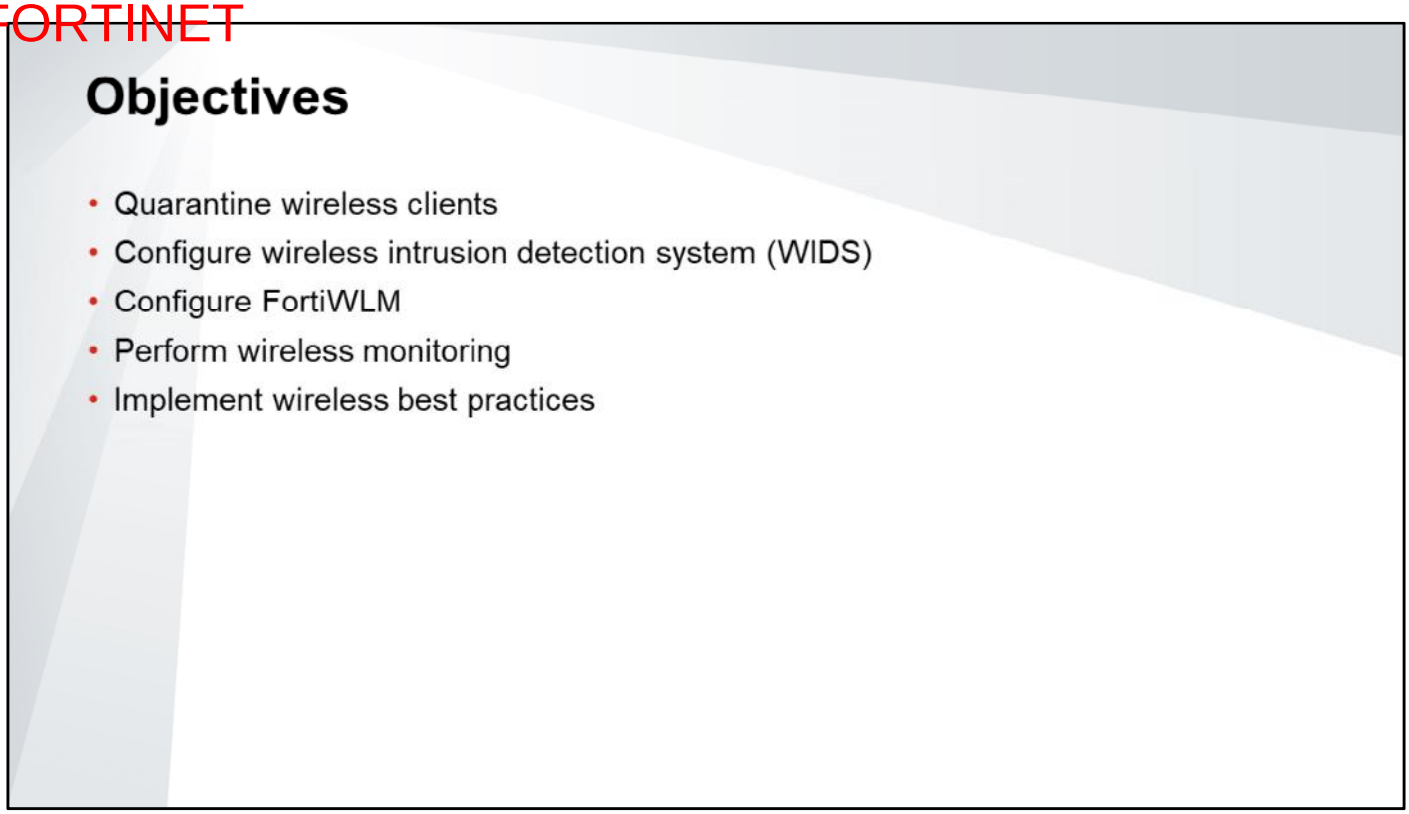
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this lesson, you will learn how to configure, use, and monitor integrated wireless features on FortiOS with FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

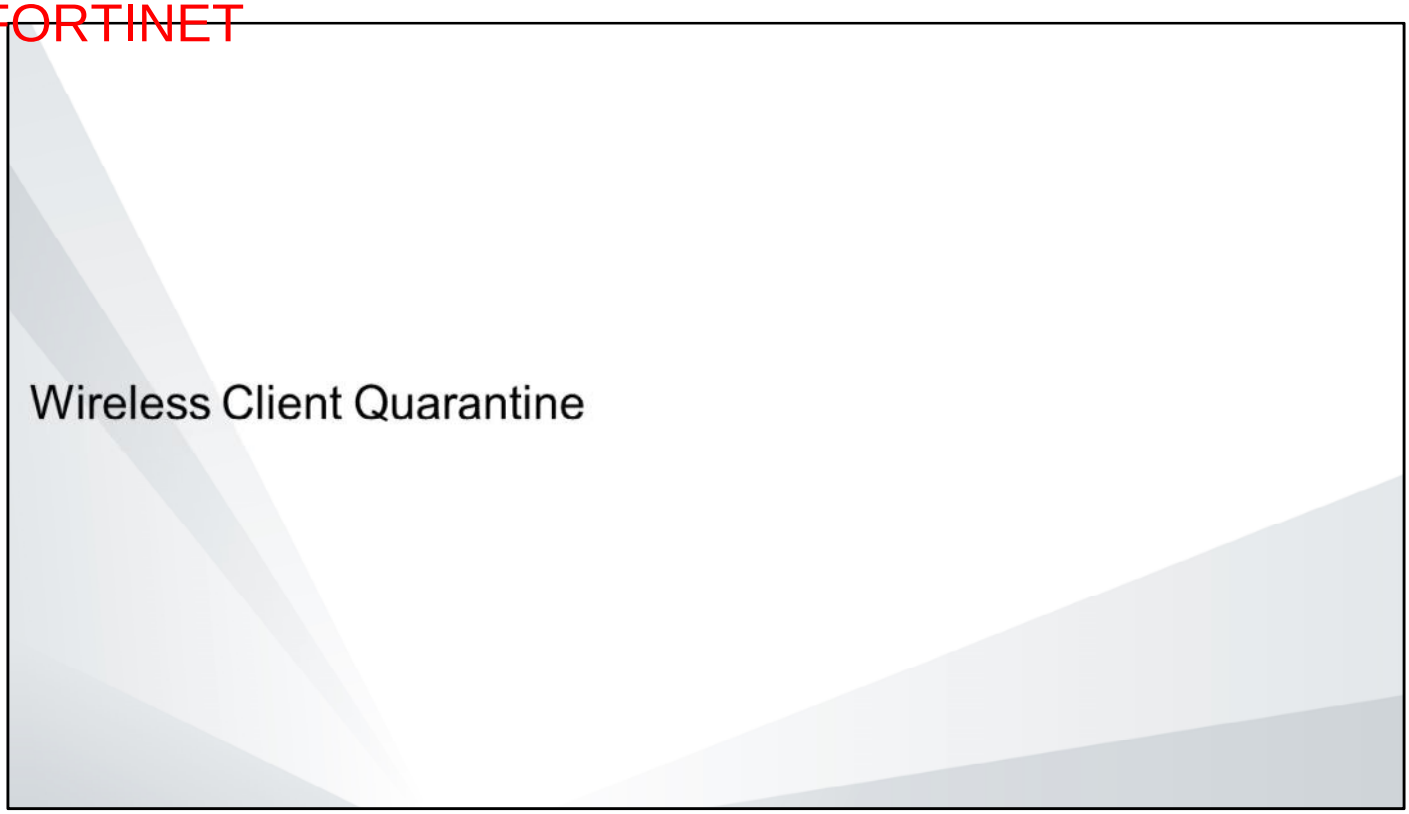


After completing this lesson, you should be able to achieve the objectives shown on this slide.

By demonstrating a competent understanding of enhanced wireless features, you will be able to configure, use, and monitor integrated wireless features on FortiOS with FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



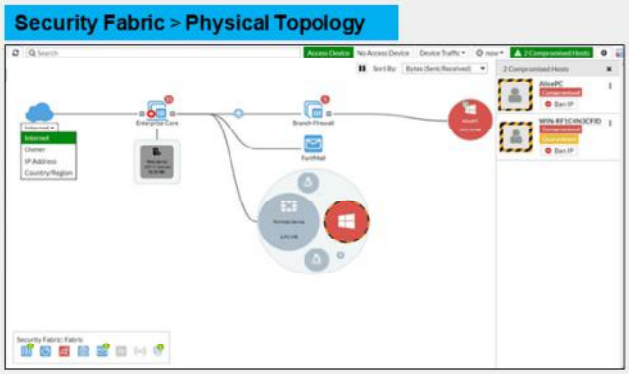
In this section, you will learn how wireless clients are quarantined on a FortiGate-controlled wireless network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Automated Response

- The Security Fabric allows multiple devices to share and leverage information
- If a device fails an IOC check, the entire fabric can react automatically
- How it works
  - A device is detected as compromised by one element of the Security Fabric
  - Switches and APs can automatically quarantine the device at the access layer
- Why it's important
  - Compromised IoT devices are no longer a threat to the wider network
  - Guest devices (if infected) will be dealt with automatically



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

4

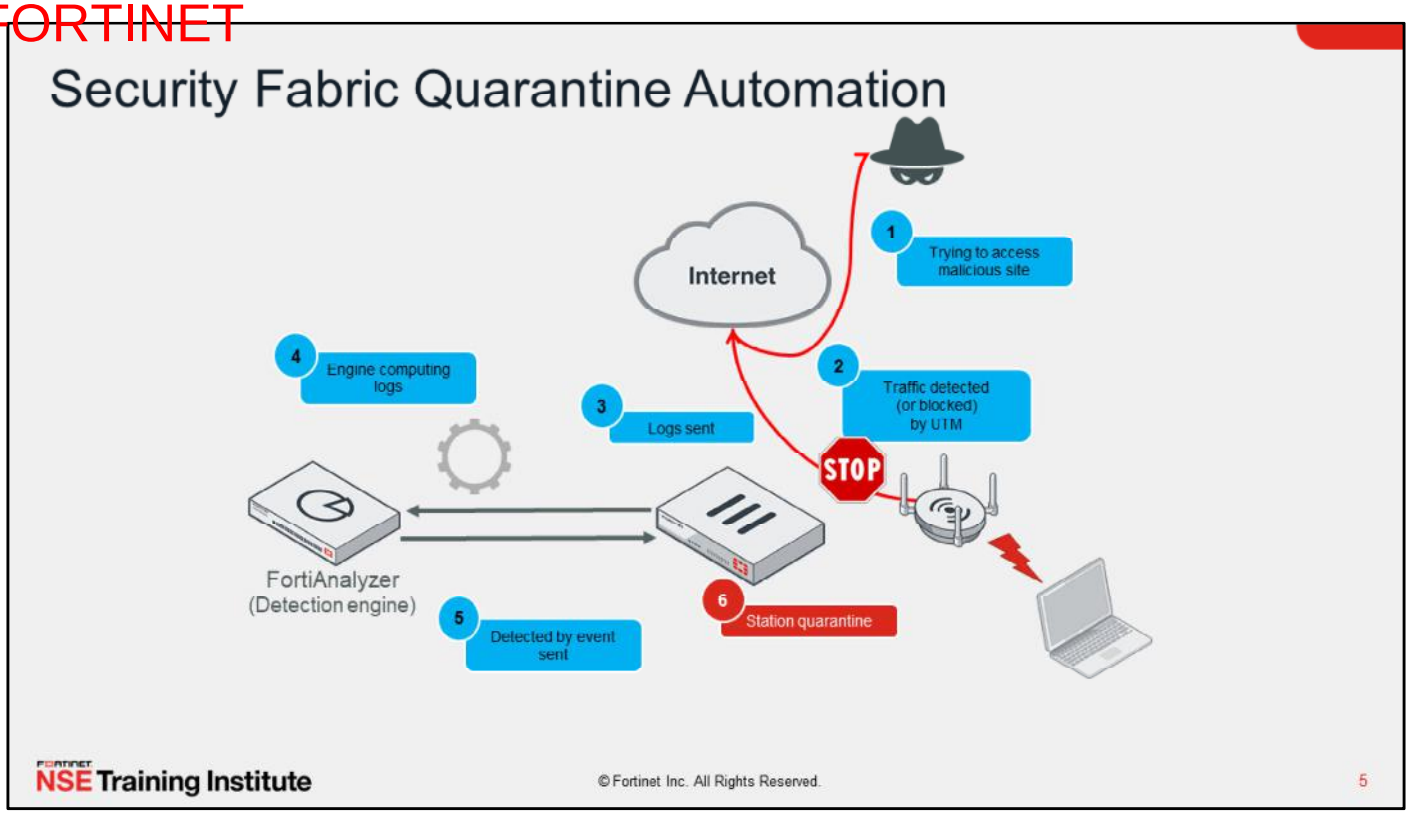
The Security Fabric allows you to detect and control compromised hosts, regardless of whether they are connected wirelessly or through a wired connection.

If a device fails an indicator of compromise (IOC) check, that device is considered as compromised and the entire fabric can respond by placing the device in quarantine. Quarantining the device it prevents it from becoming a threat to the wider network.

Compromised Internet of Things (IoT) devices will be isolated. Any other types of devices, such as a guest device, will also be isolated when they become compromised, but these devices will have the option to remediate themselves, if required.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



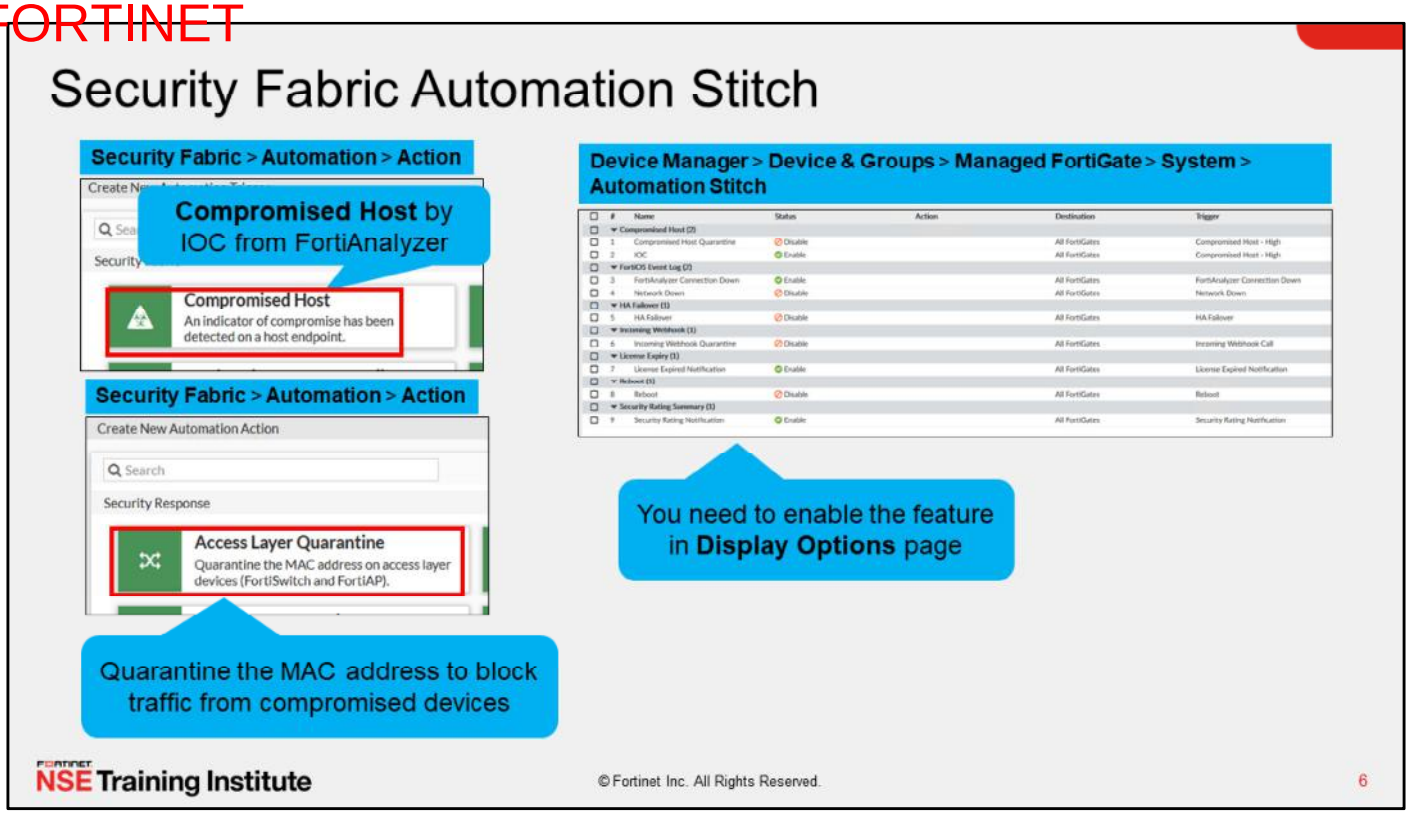
Just like it is with wired clients, known and unknown threat information is easily and efficiently shared among all elements and locations within the Security Fabric. User-defined automation on FortiGate can be used to quarantine compromised hosts; a process that can be strengthened by adding IOC services from FortiAnalyzer.

This slide shows the flow of events that occur when IOC and quarantine automation are combined to detect compromised workstations and place them in quarantine. The flow of events is as follows:

1. A workstation attempts to access content that is considered a security risk, such as a malicious website.
2. FortiGate blocks access to the site, based on the firewall policy defined with a web filter profile.
3. FortiGate sends a log record to FortiAnalyzer regarding the violation committed.
4. FortiAnalyzer processes the logs using information from the IOC services.
5. ForitAnalyzer determines a security risk verdict and sends that verdict back to FortiGate.
6. A user-defined automation quarantines the compromised workstation and places it in isolation.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Compromised wireless hosts are treated in the same way as compromised wired hosts; FortiAnalyzer identifies them using threat detection services, and then sends the IOC verdict to the root FortiGate of the Security Fabric group.

If an automation stitch is configured for compromised hosts, then that can be also be implemented.

The IOC verdict assigned to a compromised host triggers the actions specified in the automation stitch. **Access Layer Quarantine** is a Layer 2 action that places the host machine in isolation.

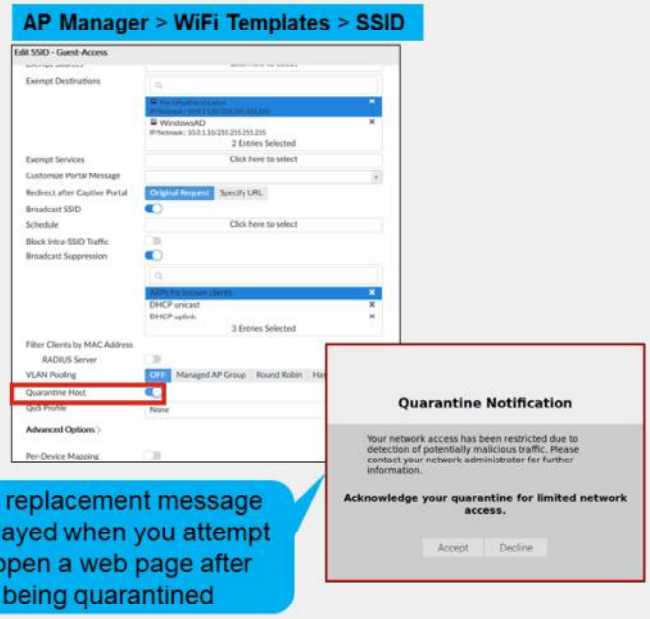
You can configure automation stitches at each FortiGate or apply a device configuration if a FortiManager manages FortiGate. You apply the setting on a per-device basis, it cannot be applied using a template.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Integrated Wireless Quarantine

- Wireless clients can be quarantined
  - Automatically using security automation
  - Manually
- Only works with tunnel mode SSIDs
- Mandatory to be in a Security Fabric
- When quarantine is enabled on an SSID, the required resources are automatically created
  - Quarantine soft switch
  - Quarantine interface
  - Default captive portal
- No quarantine firewall policy by default
- Can filter on a FortiGate level only



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

7

The quarantine process for wireless clients is very similar to wired clients; however the configuration is slightly different.

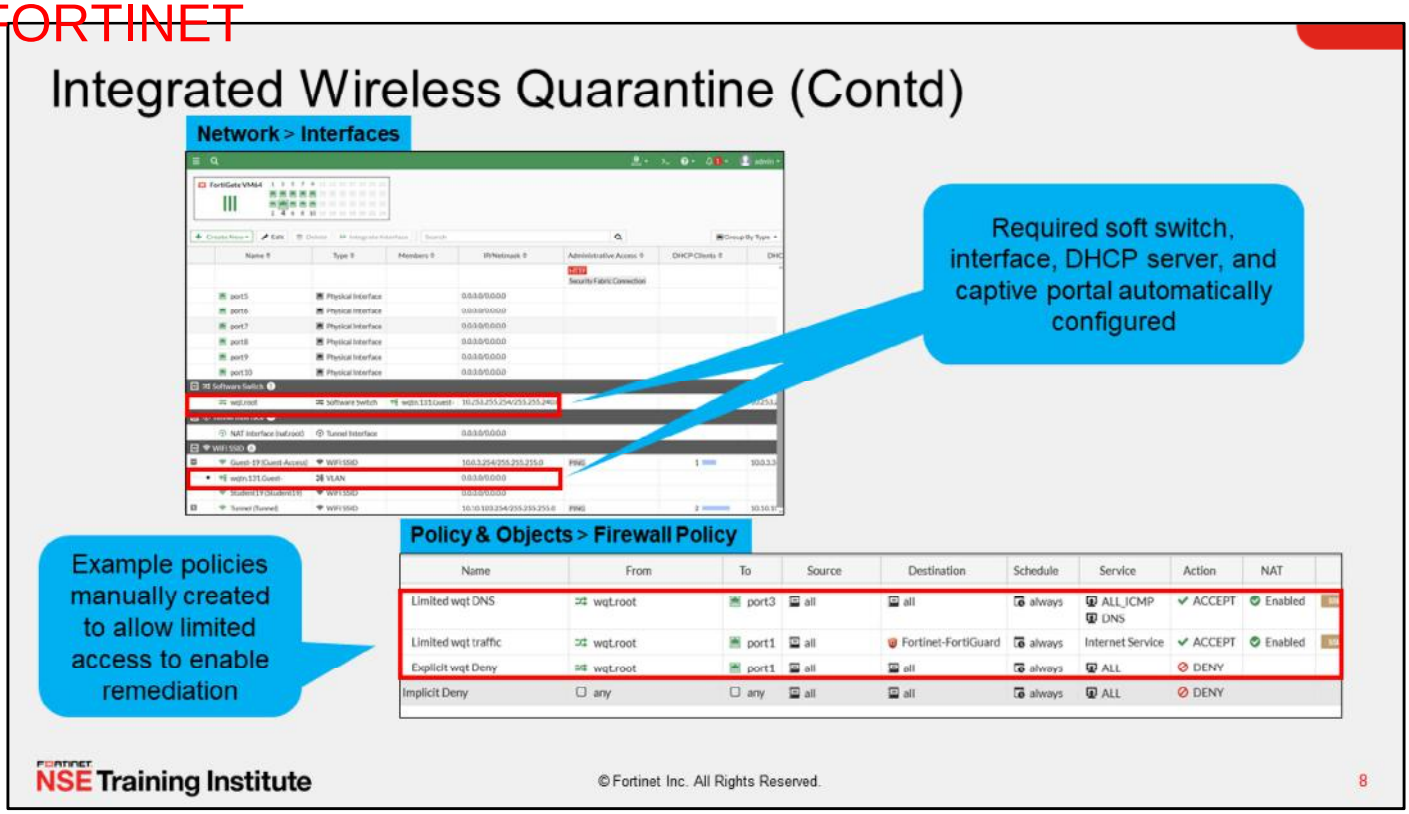
Note that it is currently possible to apply a quarantine to tunnel mode SSIDs only. For correct endpoint analysis, the APs and FortiGate have to be in the Security Fabric together with FortiAnalyzer.

You can enable quarantine on the SSID. When quarantine is enabled, FortiGate automatically creates a soft switch and interface, together with a captive portal. You create all of these features on FortiGate. FortiSwitch is not required. By default, there are no policies to allow quarantined devices access to the internet. Note that security automation can occur only at the FortiGate level, and not at the AP level.

After they are configured, wireless clients can be automatically quarantined using the same Security Fabric automation stitches as used for wired clients. Clients that are quarantined are placed in their own isolated VLAN and then presented with a captive portal informing them that they are now isolated. You can configure this captive portal in the same way as any other captive portal, to give users information on how to remediate their device.

Vouchers & Dumps are Available | WhatsApp +201224560923

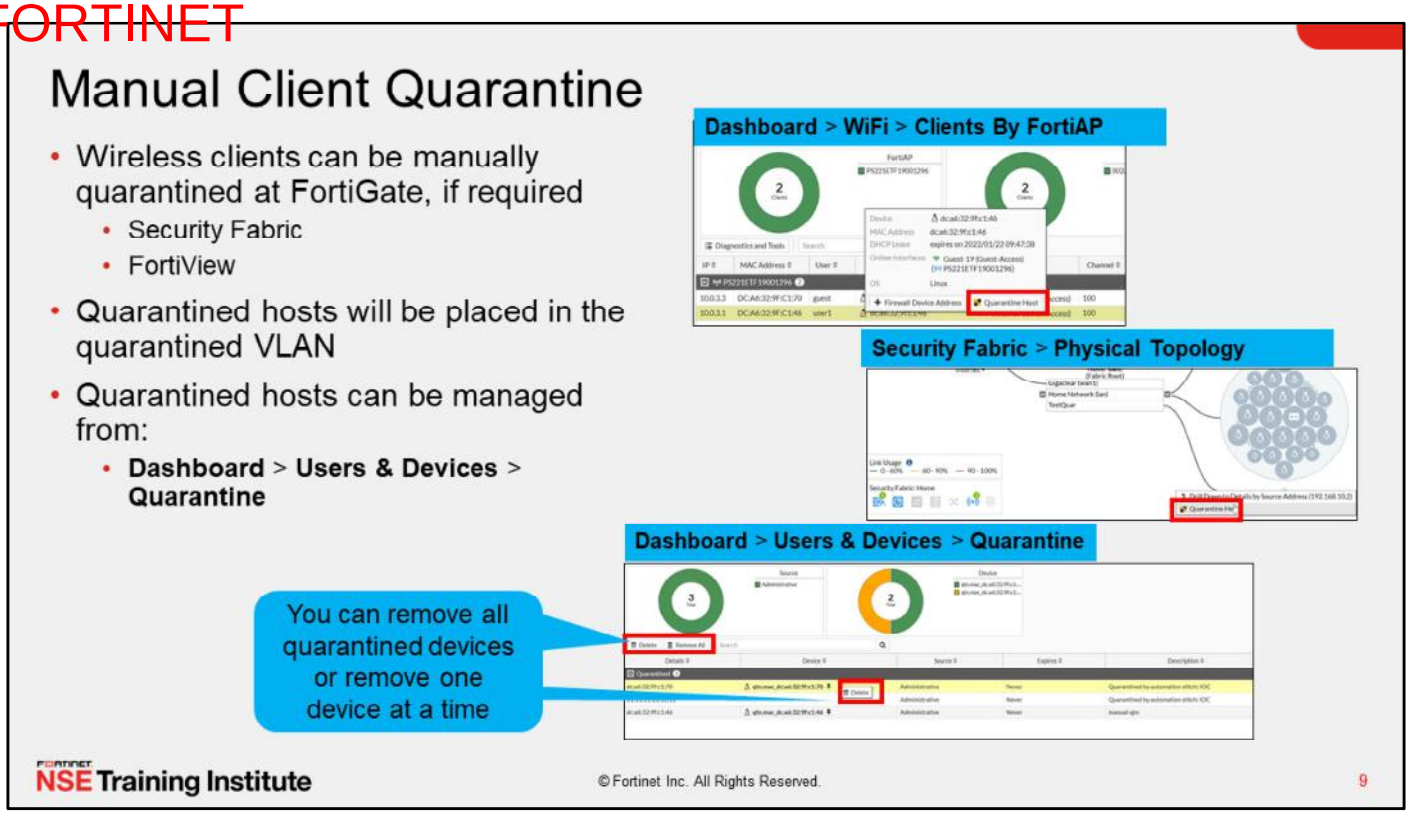
DO NOT REPRINT Brave-dumps.com
© FORTINET



Enabling a quarantine *automatically* creates a soft switch with a range of private IPs, together with a system DHCP server. It also creates a captive portal, and then creates a sub-interface under the quarantined wireless network. If you want wireless clients to have access to the internet to enable them to update themselves and/or install required software, you will need to configure a set of policies to allow limited access to the resources that are required. Typically, this requires DNS and specific HTTP/S access to resources that host the required remediation files.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

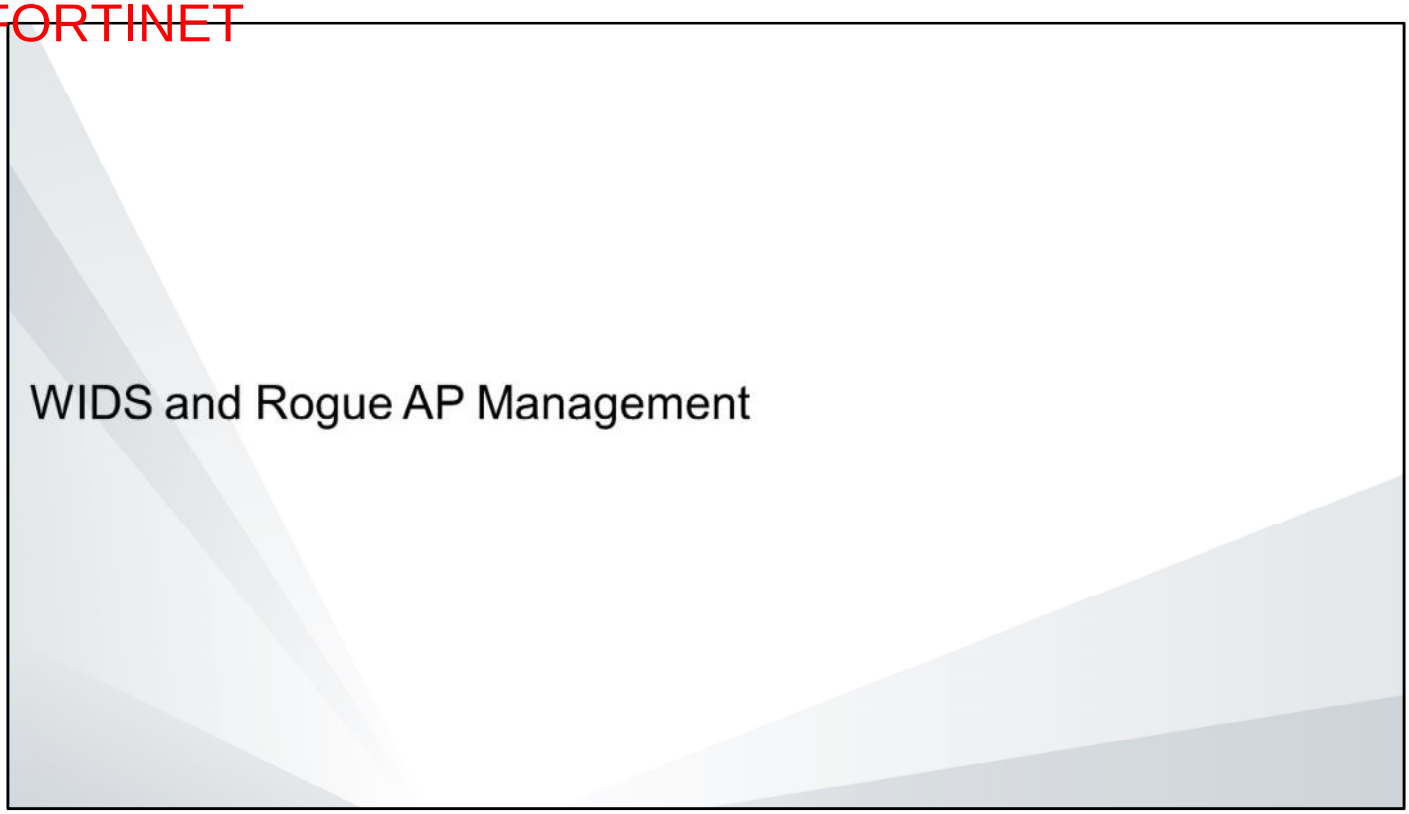


You can manually quarantine wireless clients on the Security Fabric or on FortiView.

You can manage any hosts that are currently quarantined, or release hosts from quarantine by using the **Quarantine** dashboard widget.

Vouchers & Dumps are Available | WhatsApp +201224560923

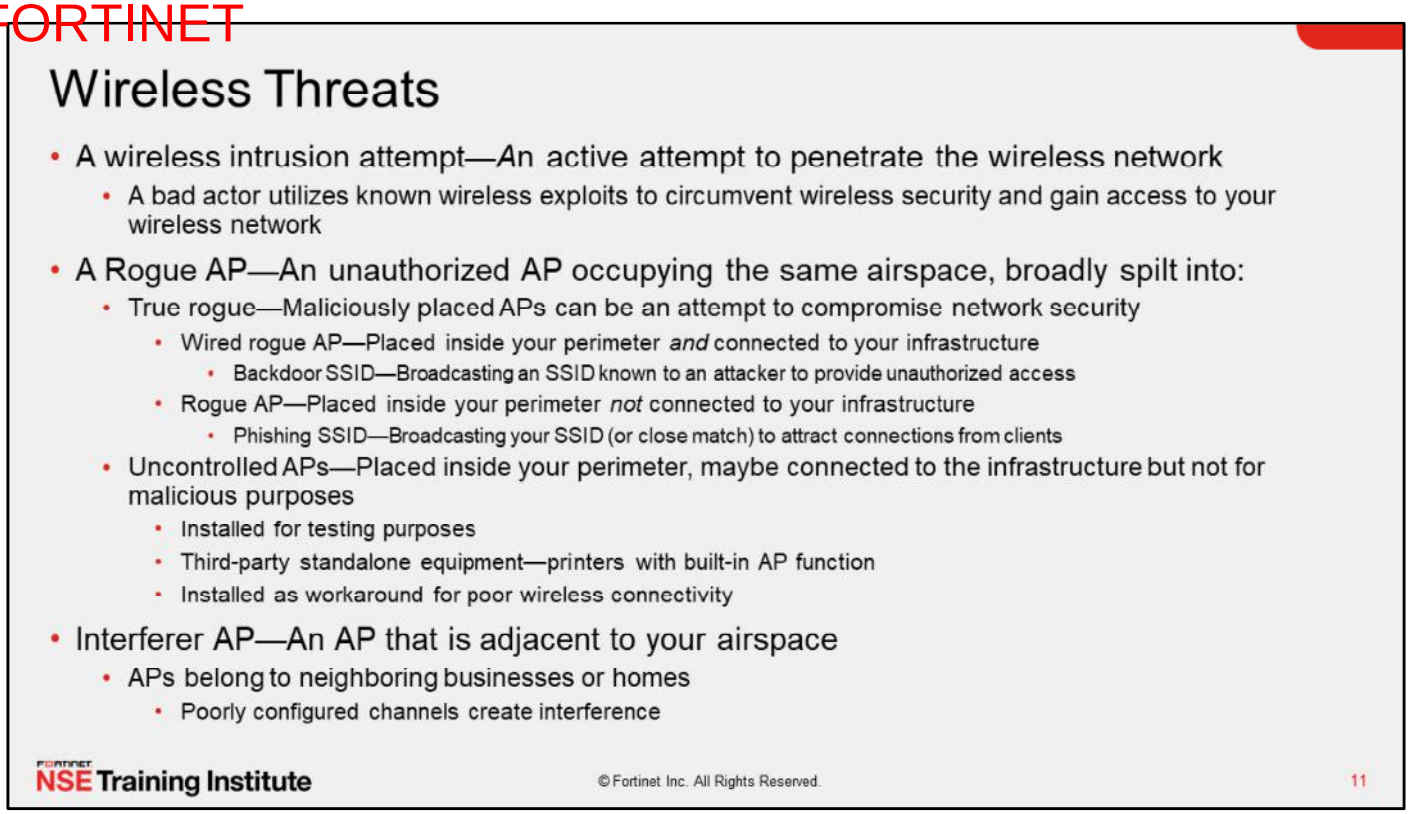
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn how to implement WIDS and configure it to detect and manage rogue APs and SSIDs.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Wireless networks are increasingly popular vectors for bad actors to gain access to the network. The inability to fully control where a wireless signal propagates makes it an attractive medium for hackers to use when attacking a network directly, or attacking it indirectly, by setting honeypots to trap unsuspecting end users.

Wireless threats can be characterized broadly as a security threat, where a bad actor is attempting to gain access to data on a network or end-user wireless devices (such as credentials or end-user data). Or, they can be characterized as a performance and reliability threat in which RF problems are generated in the airspace around your APs. There are three main types of threats:

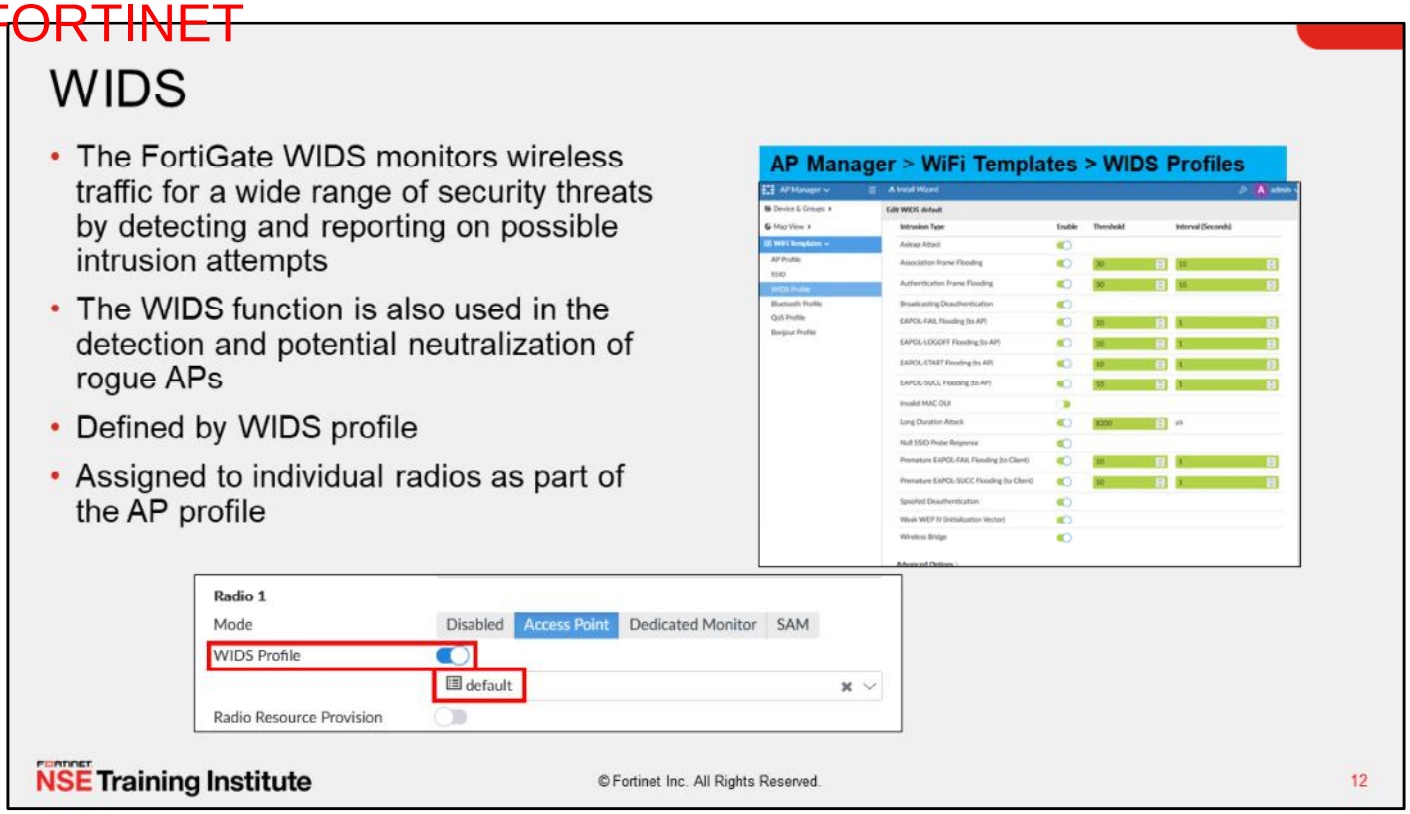
- A wireless intrusion attempt: A bad actor uses various methods and known exploits to defeat and bypass the security of a wireless network, or deny access to the wireless network. These types of intrusion attempts typically happen at the radio level, Layer 1, or Layer 2 of the OSI model.

- The rogue AP: An AP is placed either inside or adjacent to, your airspace. The ultimate classification depends on their purpose for being there. A true rogue AP is placed maliciously to provide either unauthorized access to your network using a backdoor SSID known to the attacker, or access to client data by attempting to attract legitimate clients to a phishing SSID.
  The second type of rogue AP, an uncontrolled device, is not placed for any particular malicious intent, but ultimately can provide another vector for bad actors to gain access to the network because of poor SSID security, or cause interference issues that lead to performance and reliability problems.

- The interferer AP: Because the wireless spectrum is not licensed, and is free for use by all, there is nothing to stop legitimate users from installing wireless APs to create their own network. While not a security threat, a badly configured neighboring wireless network can cause considerable problems for your own network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Wireless intrusion, rogue AP, and phishing SSID detection are configured using the WIDS profile. A WIDS profile is assigned to an AP radio through the AP profile. You can configure WIDS profiles centrally using FortiManager and deploy to multiple APs and FortiGate devices as part of the FortiAP profile.

You can configure the detection of specific threats in the profile. This allows for the detection of a wide range of Wi-Fi-specific security threats by monitoring for and reporting on possible intrusion attempts, such as:

- Weak WEP IV encryption used to crack WEP keys
- Null SSID probe responses that causes many wireless cards and devices to stop responding
- De-authentication broadcasts that are a denial of service (DoS) attack causing all clients to disconnect from the AP
- Invalid MAC organizationally unique identifiers (OUIs) (The OUI is the first three bytes of the MAC address.)
- Various management, EAP, authentication, and beacon floods

Some WIDS profile options have configurable thresholds and intervals. Usually, you will not need to alter the default values of these options.

You can also enable rogue AP detection in the FortiAP profile, and you can choose how to enable it.

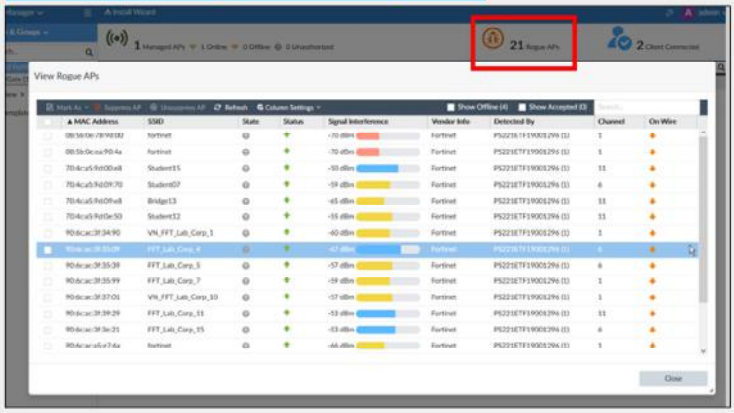
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Rogue AP Detection

- FortiAP can scan for other available APs in two ways:
  - In idle periods during AP operation
  - As a dedicated monitor
- If an attacker tries to use a rogue AP for unauthorized access
  - FortiOS can automatically detect it and list it in the Rogue APs monitor
  - Using a WIDS profile, you have the ability to suppress a rogue AP to avoid security threats (dedicated monitor mode)
- Rogue APs can monitored:
  - Centrally using **AP Manager** from FortiManager
  - At the FortiGate using the **Rogue APs** dashboard widget

AP Manager > Managed FortiGate > Rogue APs



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

13

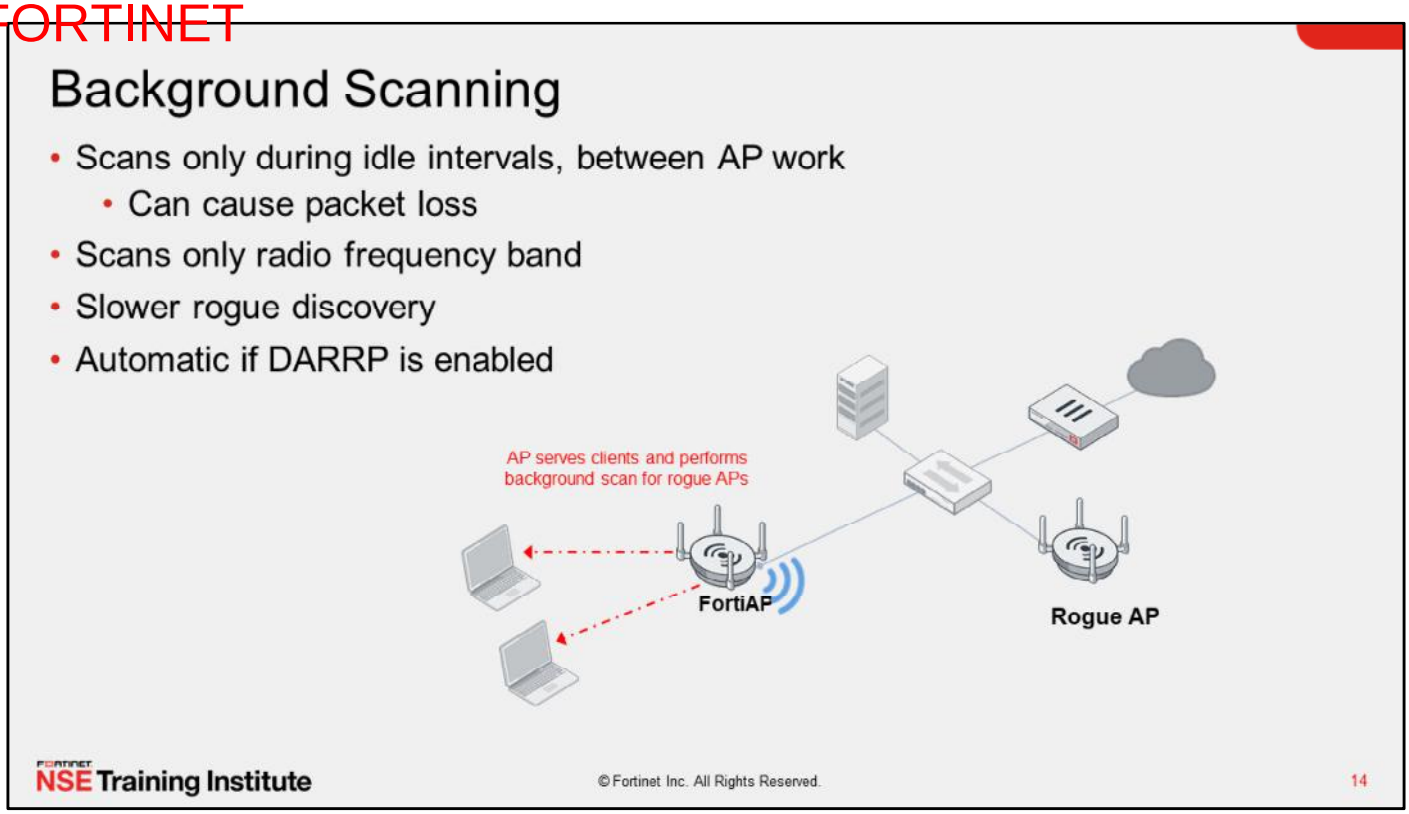
There are two ways to configure a FortiAP to detect rogue APs:

- As a dedicated monitor (can assign one or both radios)
- In idle periods during AP operation, referred to as a background scanning

You can also use one radio of an AP for scanning and reserve the other radio for normal AP use. However, this will limit you to using only one frequency—2.4 GHz or 5 GHz—because you can use only one band per radio. When a rogue AP is connected, an attacker tries to use it for unauthorized access. FortiOS automatically detects and lists the rouge AP in the **Rogue APs** widget. You can suppress it to avoid security threats.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



How does rogue AP detection on FortiOS work? It uses a radio to listen for and detect other APs. If your FortiAP is not using all of its radios, you can dedicate one of them to monitoring for rogue APs. Otherwise, you can configure the AP to run a background scan when a radio is idle.

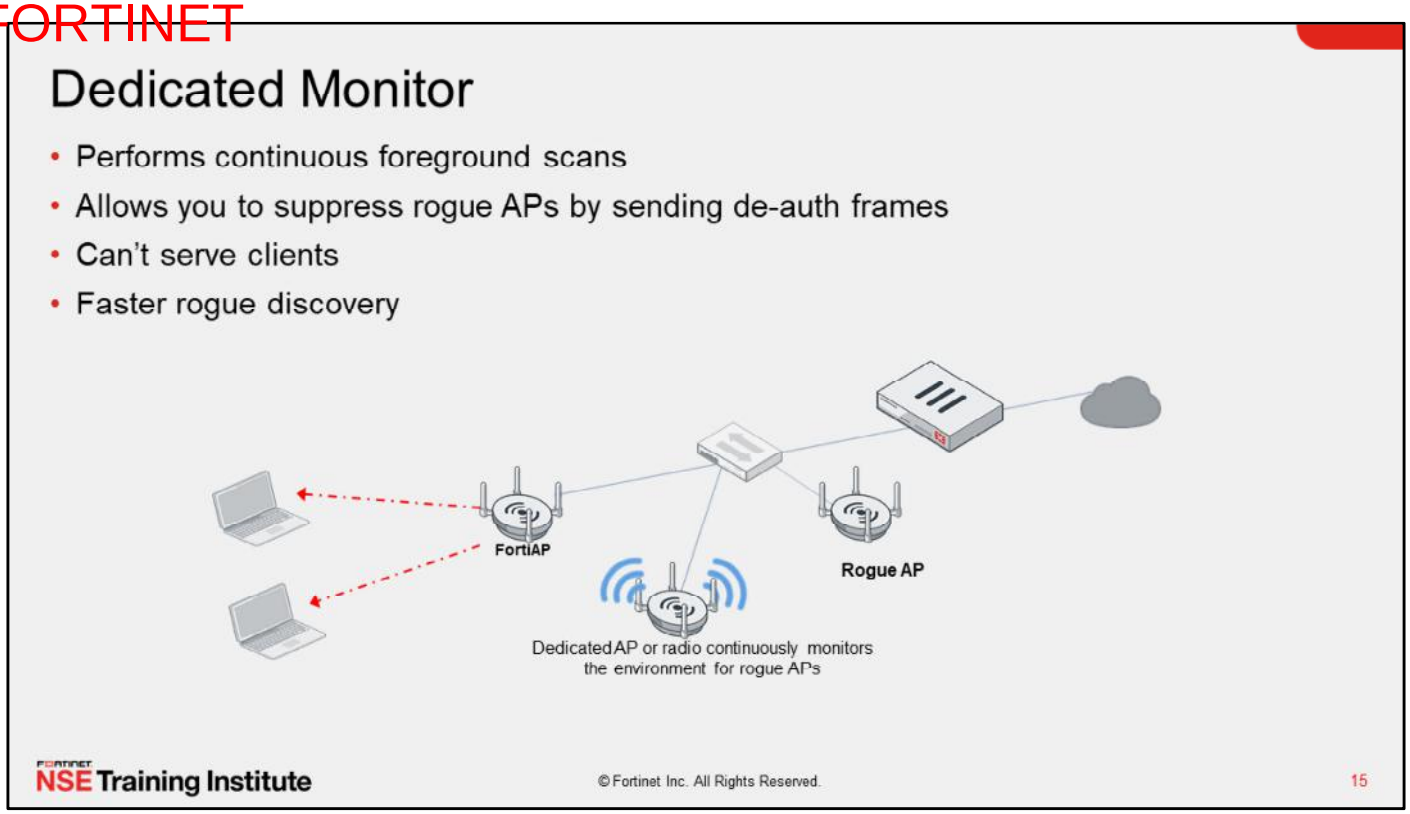
If you do not use a dedicated AP or a radio for scanning, you can configure the AP to run a background scan when a radio is idle or at a defined threshold.

A background scan is opportunistic. During idle periods, FortiAP briefly switches the radio from acting as an AP, to monitoring. By default, a scan period starts every 600 seconds, and each second a different channel is monitored for 20 ms until all channels in the radio frequency have been checked. If the radio is dual-band capable, it will *not* switch to the other frequency.

During heavy AP traffic, it is possible for background spectrum analysis scanning to cause lost packets when the radio switches to monitoring. This technique, which offers poor rogue AP detection, is enabled by default when using distributed automatic radio resource provisioning (DARRP).

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



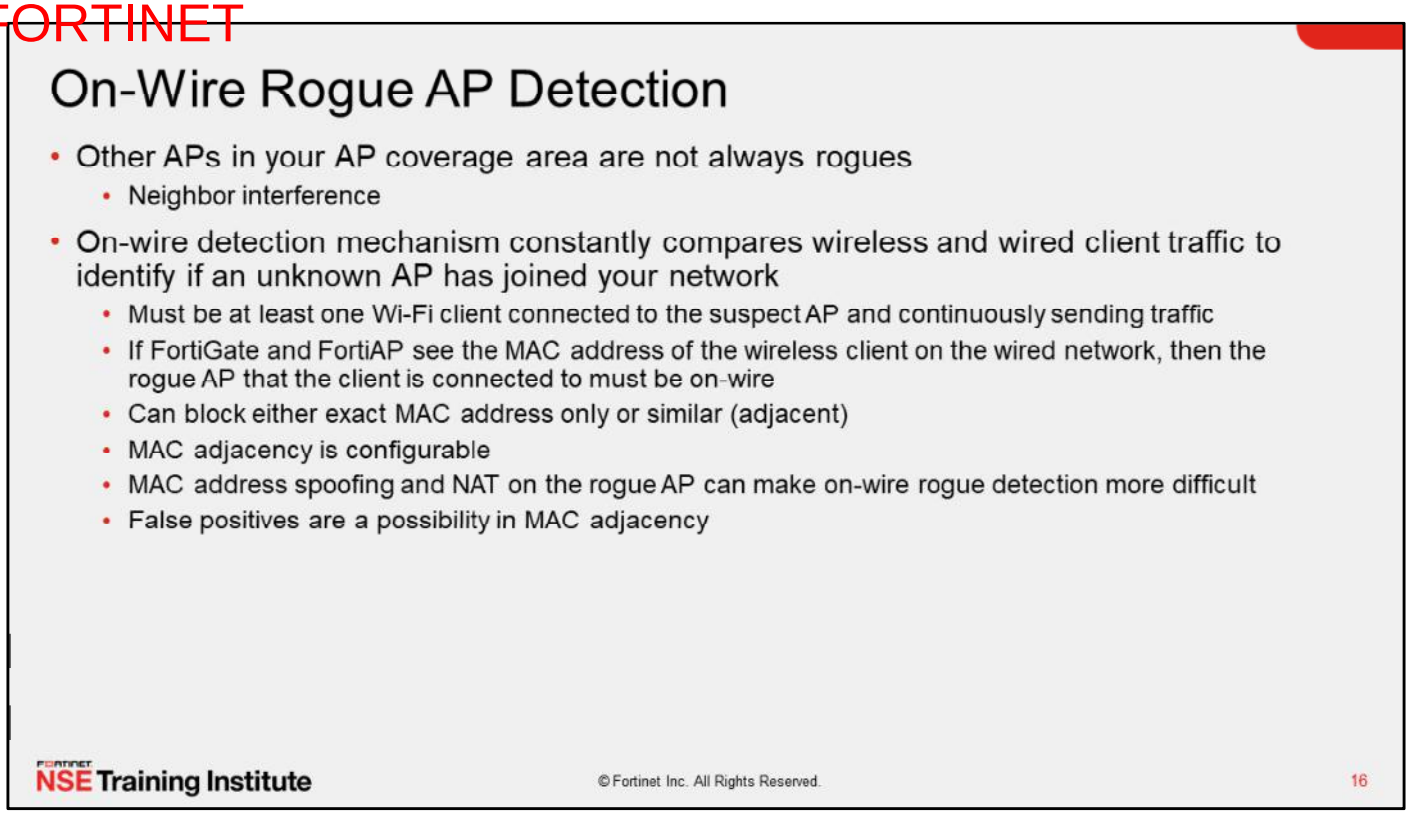
You should use one AP in your network as a dedicated monitor AP, because it can reduce the load on other APs, and saves them from switching to AP and monitoring mode.

Dedicated monitor radios are reserved for scanning and suppression, if enabled. They will not broadcast SSID, and will not allow any wireless clients to join them. This is the technique required to actively suppress rogue APs.

If you are going to use a dedicated monitor AP, for a normal coverage solution, you should allow for one dedicated monitor AP for four normal client connection APs. This allows for adequate rogue detection coverage because rogue detection requires detection of only the management frames of APs. Management frames are typically transmitted at lower link rates, which allows the signal of a potential rogue AP to propagate further, requiring fewer rogue detection APs to cover a network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



Another useful technique for rogue AP detection is on-wire detection. When you enable on-wire detection, FortiOS compares MAC addresses in wireless and wired traffic—in both Wi-Fi frames from clients, and from the APs. If FortiOS and FortiAP see the wireless client's MAC address on the wired network, then the rogue AP that the client is connected to must be on-wire. This normally requires the rogue AP to be a Layer 2 bridged AP, instead of a Layer 3 wireless router. Otherwise, the wireless controller will see only the wireless router's Ethernet MAC and not the wireless client's MAC. Two rogue detection methods are used by the on-wire scan:

- Exact MAC address match: If the same MAC address is seen in frames on the wired LAN and on the Wi-Fi network, this means that the wireless client is connected to the LAN. In your FortiOS configuration, if you did not authorize the AP that the client is using, then FortiOS will treat that AP as an on-wire rogue.
- MAC adjacency: If an AP is a wireless router, it applies NAT to Wi-Fi packets. This can make rogue detection more difficult, because the frames in wired and wireless traffic won't have the same MAC address. However, an AP's Wi-Fi interface MAC address is usually similar to its wired MAC address. So, the MAC adjacency rogue detection method matches LAN and Wi-Fi network MAC addresses that have close hexadecimal numbers. By default, the MAC adjacency value is 7.

You can change MAC adjacency value setting using this CLI command: `set rogue-scan-mac-adjacency {integer}`.The integer value 0 to 31 represents the maximum numerical difference between an AP's Ethernet and wireless MAC values, to match for rogue detection. The default value is 7.

If an AP is found through on-wire detection, it will appear on the AP monitor with a green check mark in its **On Wire** column.

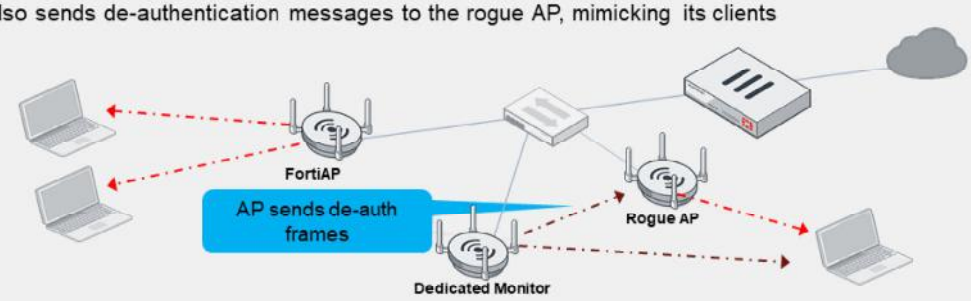
Note that because of the nature of the MAC adjacency method, there is a possibility of false positives.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Suppressing Rogue APs

- Check your regional laws and regulations before enabling suppression
- Uses monitoring radio
  - Requires dedicated monitor mode
  - Not possible with background scan
- Actively interferes with the connectivity of clients and rogue APs
  - Uses on-wire detection
  - When suppression is activated:
    - Wireless controller sends de-authentication messages to rogue APs clients, mimicking rogue AP
    - Also sends de-authentication messages to the rogue AP, mimicking its clients



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

17

After you detect a rogue AP, you will usually want to actively prevent your users from connecting to it. You can use your FortiAP radios to suppress rogue APs.

Before enabling the rogue suppression feature, verify that rogue suppression is compliant with the applicable laws and regulations of your region.

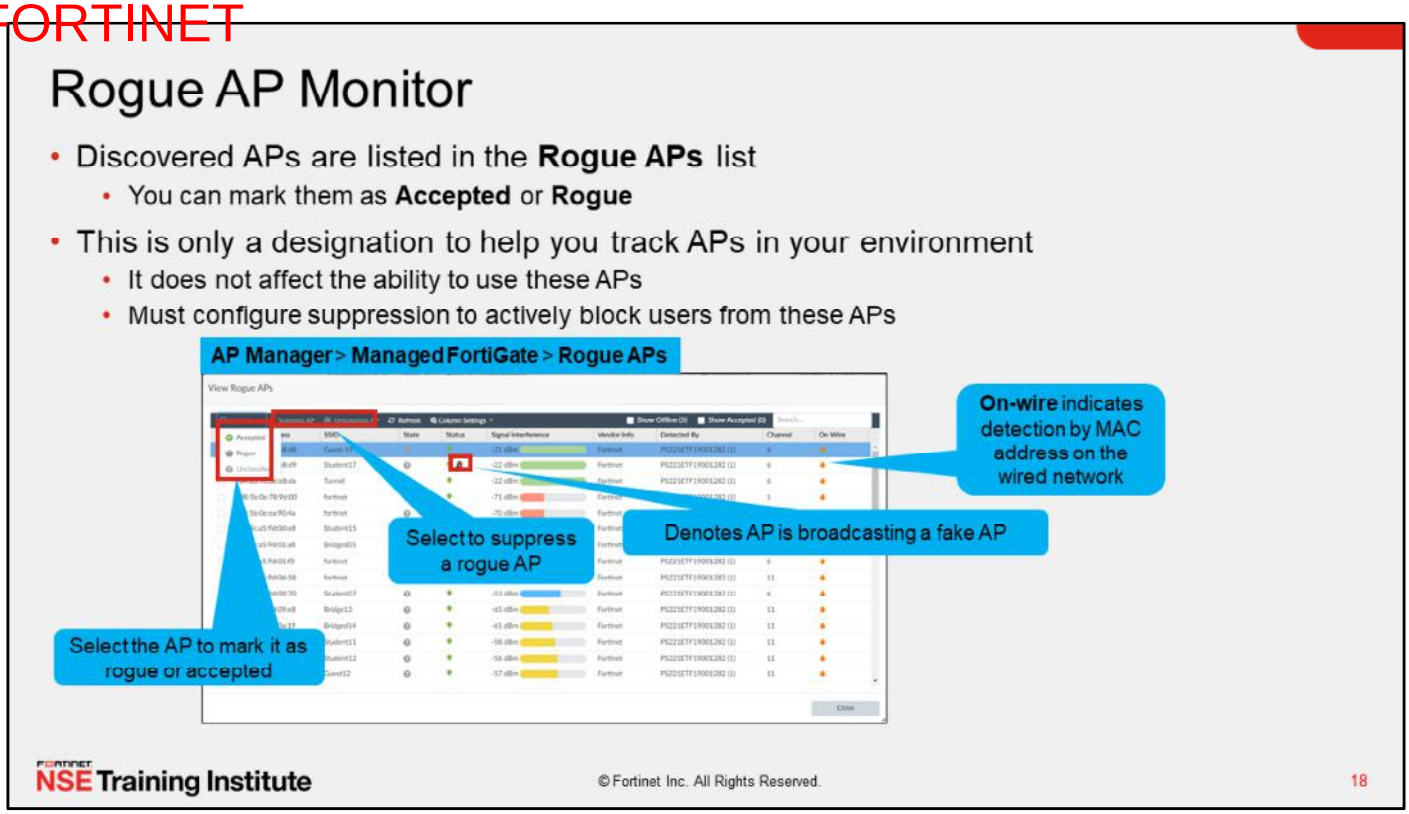
Because rogue suppression is an active process, it requires that you dedicate one FortiAP radio to the process it. You can't use rogue suppression with a background scan.

How does rogue suppression work? While pretending to be the rogue AP, the FortiGate Wi-Fi controller uses the dedicated monitoring radio on a nearby AP. It sends de-authentication messages to the rogue AP clients. This makes it difficult for the clients to maintain a connection with the rogue AP because FortiOS also mimics the rogue AP clients, sending de-authentication messages to the rogue AP.

Note that suppression of rogue APs is becoming increasingly more difficult, because new wireless security standards are beginning to mandate management frame protection (802.11w). This requires that clients authenticate management frames as being legitimate, preventing man-in-the-middle wireless attacks. Because rogue suppression is a form of man-in-the-middle attack, an AP that the client is not connected to is trying to send de-authentication frames and, as a result, 802.11w prevents the client from taking notice of the dedicated monitoring AP.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



When FortiGate detects a new AP that is not authorized, that AP is listed in the **Rogue APs** dashboard widget on FortiGate and the **Rogue APs** table.

You can sort and filter this list. Sorting by **Signal Interference** is especially useful because it sorts the APs with the strongest detected signal to the top of the list.

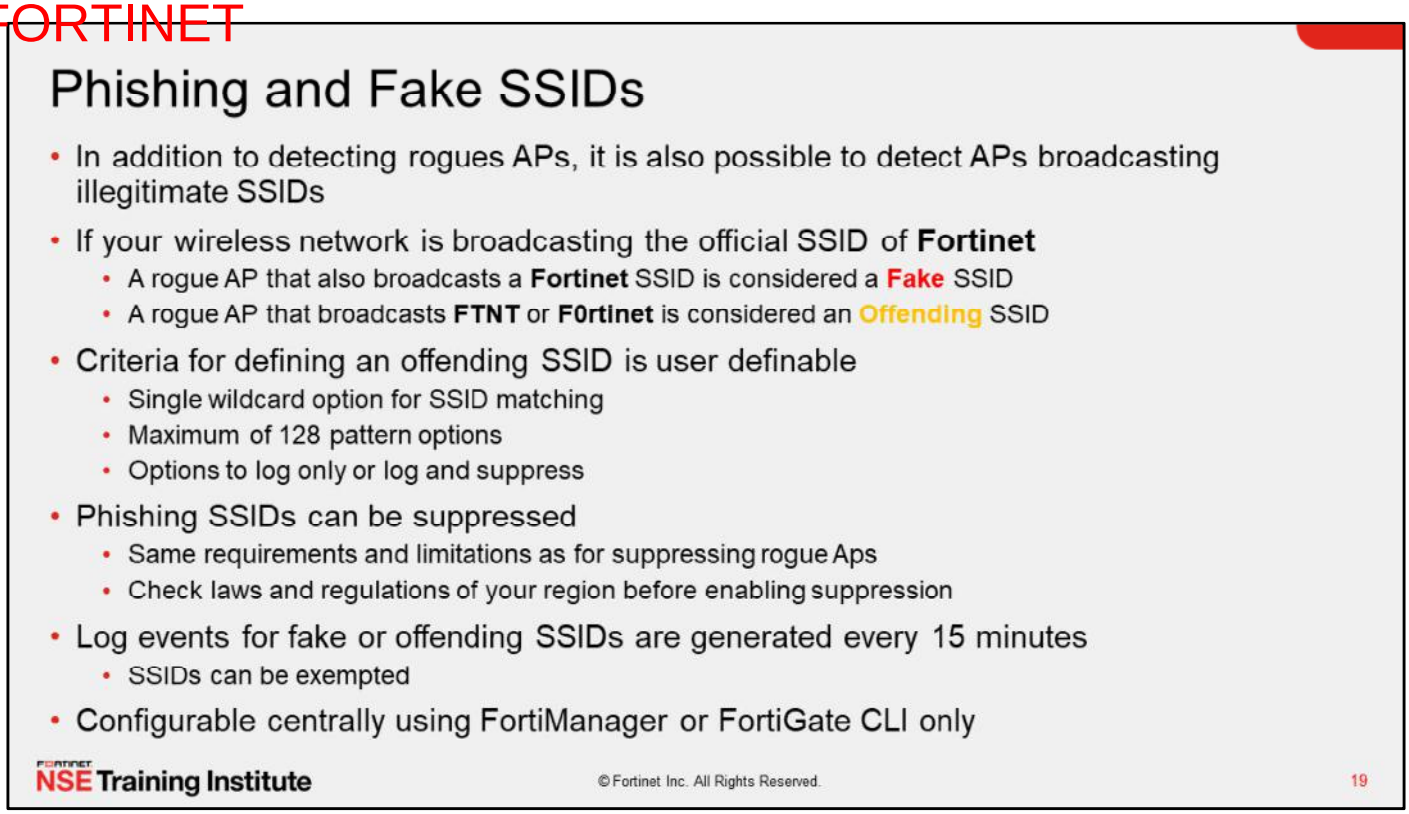
In the example shown on this slide, not only is the unauthorized AP in your air space, indicated by the signal strength being relatively strong, but it is also connected to your wired infrastructure, *and* it is also broadcasting a fake AP. You might be using equipment from different wireless vendors in your network to broadcast your corporate network, in which case, FortiGate will detect it as a rogue AP and fake SSID. If this is the case, then you may need to mark this equipment as accepted. On the other hand, the AP could also be a bad actor attempting to perform a man-in-the-middle attack. Either way, the suspect devices should be investigated and appropriately classified.

You can mark APs as either **Accepted** or **Rogue**, which helps you to track which APs are authorized by you, or not. By default, when you mark an AP as a rogue, it does not affect anyone's ability to use these APs. For that, you need to configure suppression.

When you mark an AP as **Accepted**, it removes that AP from the default rogue AP list. This usually indicates that the AP is not a threat to network security, *but* the presence of that AP will need to be considered as a source of interference. If that AP is on the same channel, co-channel interference (CCI) or adjacent channel interference could be a problem. You may need to alter your network channel configuration, if interference of high channel utilization becomes an issue.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



As well as detecting rogue APs, it is also possible to look for networks that might have been set up to perform phishing operations. Often bad actors will attempt to attract connections from legitimate clients, either by broadcasting an SSID that is the same as, or very *similar* to, the official network SSID.

You can configure the FortiAP devices to detect duplicate SSIDs and classify them as fake. You can then log, and optionally suppress, these fake SSIDs.

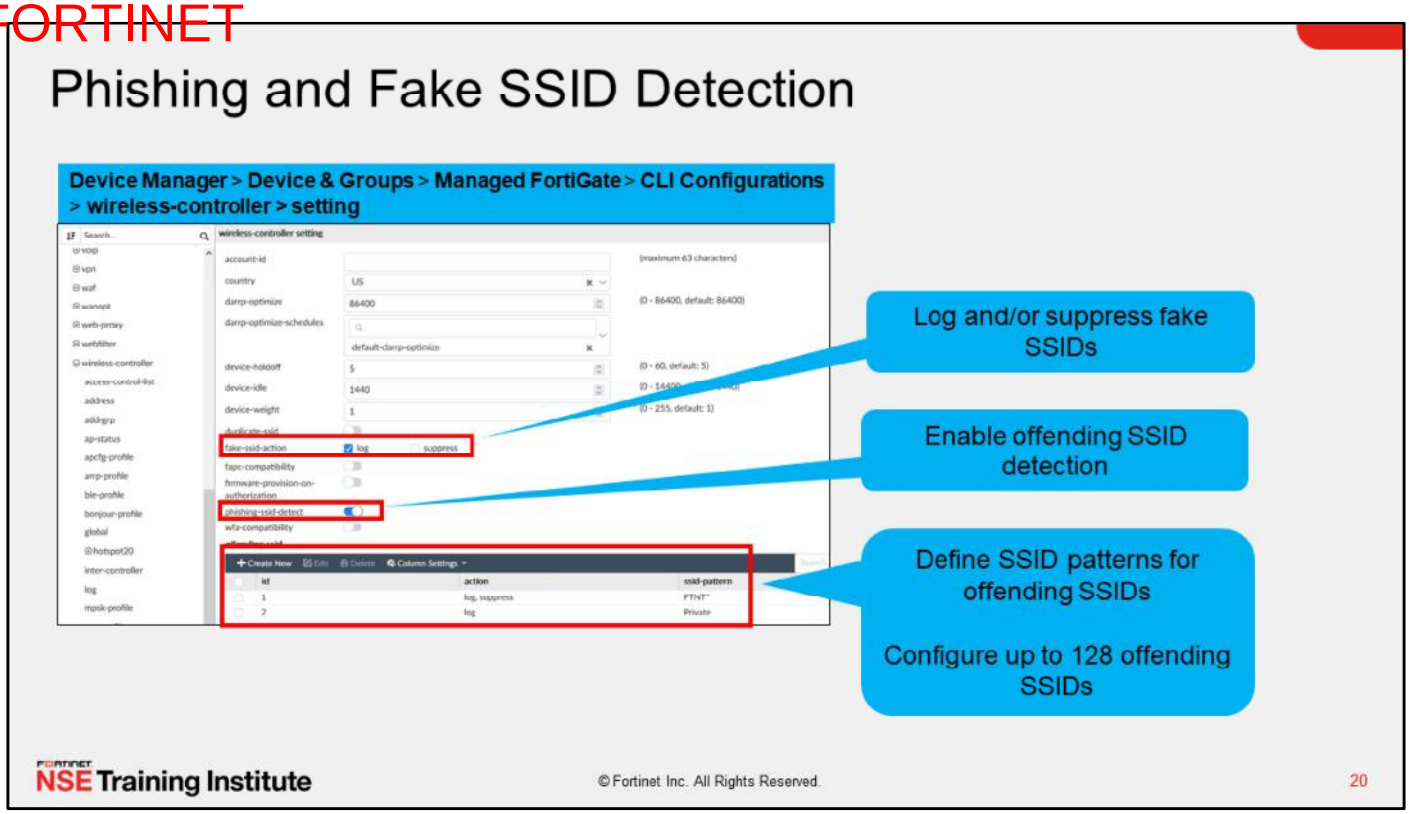
As well as looking for identical matches in the SSID, it is also possible to look for user-defined SSIDs. This can be useful to detect SSIDs that do not *quite* match the broadcast SSID, but may seek to look official enough for clients to attempt to connect. These SSIDs are classified as offending. You can choose to log and suppress them. Up to 128 offending SSIDs can be defined on all controller models, and it is possible to use a single wildcard match.

You can suppress phishing SSIDs in the same way as rogue APs; again, verify that the operation the suppression is compliant with the applicable laws and regulations of your region.

Any fake or offending SSIDs that are detected are logged every 15 minutes until they are classified.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



You can configure phishing SSID detection centrally on a per-controller basis using a **CLI Configuration**. By default, fake SSIDs are detected and logged only, and no offending SSIDs are defined.

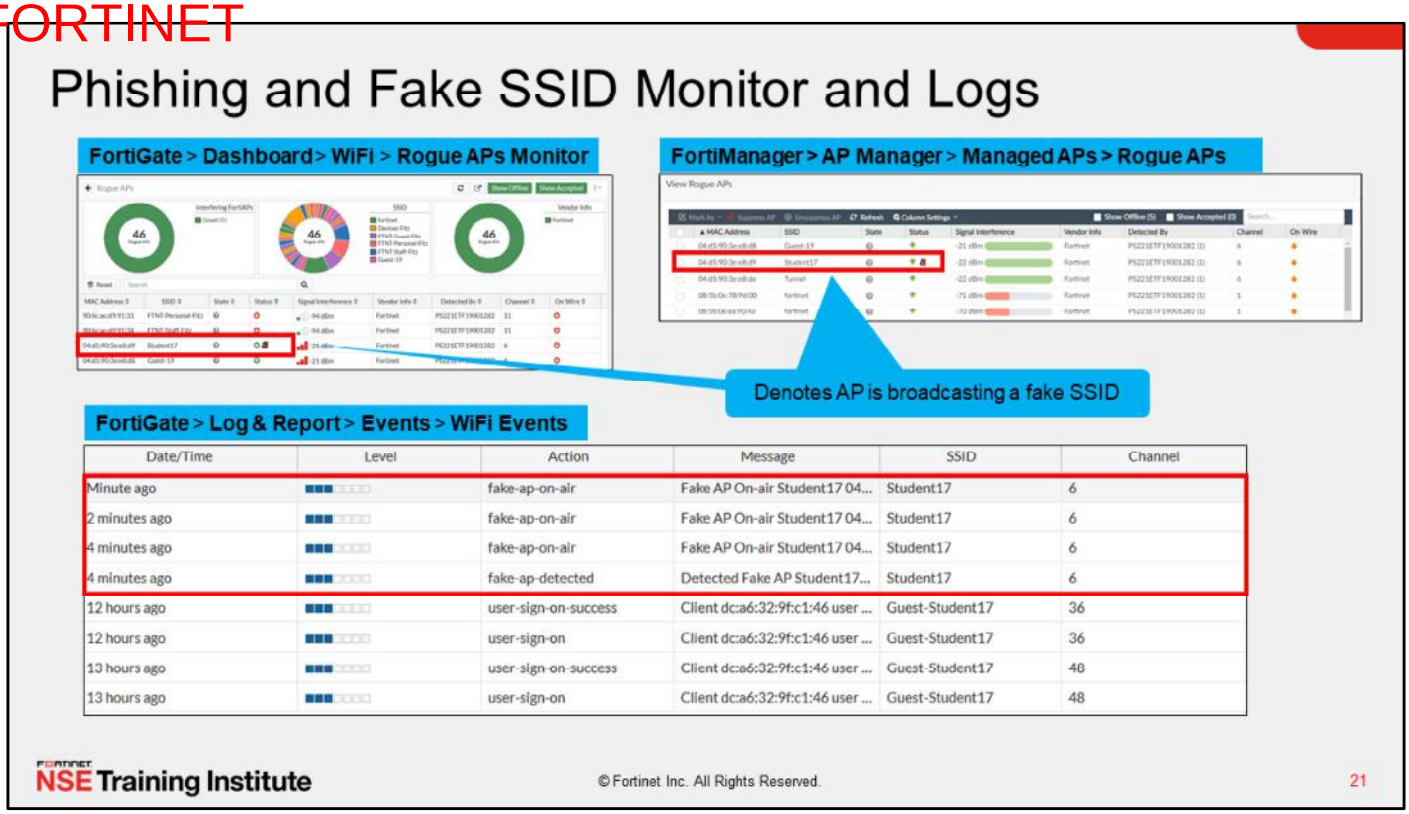
You can add offending SSIDs to the **offending-ssid** table with the option to log, or, to log and suppress. Wildcards are supported, in the example shown on this slide, a **ssid-pattern** of FTNT* is specified. Any SSIDs that broadcast a wireless network SSID beginning with FTNT are classified as an offending SSID.

You should then enable **Phishing-ssid-detect** to detect offending SSIDs.

The FortiGate GUI does not support the configuration of offending SSID detection. You can enable it using the CLI.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



After you enable phishing detection, it is possible to log entries in both the **Rogue APs Monitor** dashboard widget and the **WiFi Events** log located in **Log & Report** > **Events** on FortiGate.

FortiManager will also display the fake SSID in the **AP Manager** > **Managed FortiGate** > **Rogue APs** table.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



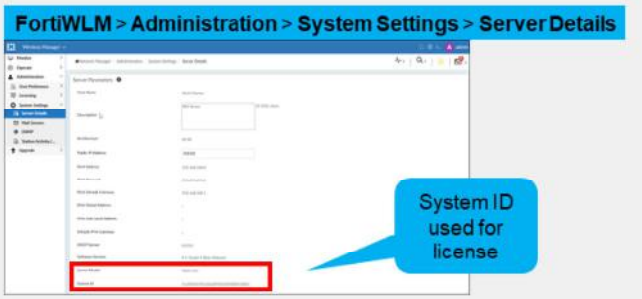
In this section, you will learn how to set up and configure the optional FortiWLM function.

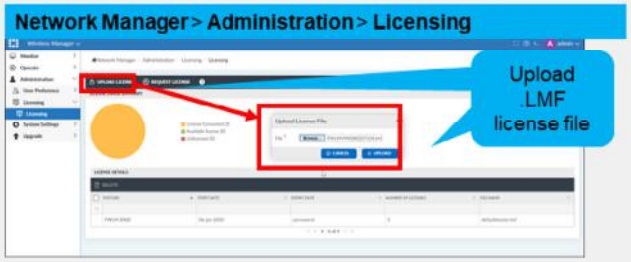
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiWLM Licensing

- By default, FortiWLM is supplied with licenses to support the monitoring of three APs
- Base license is required to support additional 50 APs and full functionality
  - Further APs added using AP licenses
- Licenses are keyed to FortiWLM system ID
  - The system ID is a unique identifier
    - Hardcoded in hardware appliances
    - Generated from configuration on virtual devices
  - Reboot of FortiManager may be required after initial FortiWLM configuration to generate ID
  - When licensing a virtual device, ensure the final configuration has been applied





NSE Training Institute

© Fortinet Inc. All Rights Reserved.

23

FortiWLM wireless manager is available in multiple platforms. It can be purchased as a dedicated hardware device, a virtual machine, or as a module for FortiManager. It is licensed by the number of APs that it can support, and the different appliances support different maximum numbers of APs. Refer to the datasheet for more information.

When first enabled, FortiWLM on FortiManager will support three APs for evaluation purposes. To add support for additional APs you will need to purchase and install an additional license.

Licenses are unique to each appliance and are keyed to the system ID. You can find the system ID under **Administration** > **System Settings** > **Server Details**. The system ID for hardware appliances is hardcoded at the factory. For virtual devices, it is generated using the system installation information. For this reason, you should ensure that any virtual appliances are configured in their final configuration before recording the system ID. Any change in configuration information could cause the system ID to change, and as a result, the license could become invalid and require regeneration.

If the system ID is not showing correctly, then a reboot of the appliance may be required.

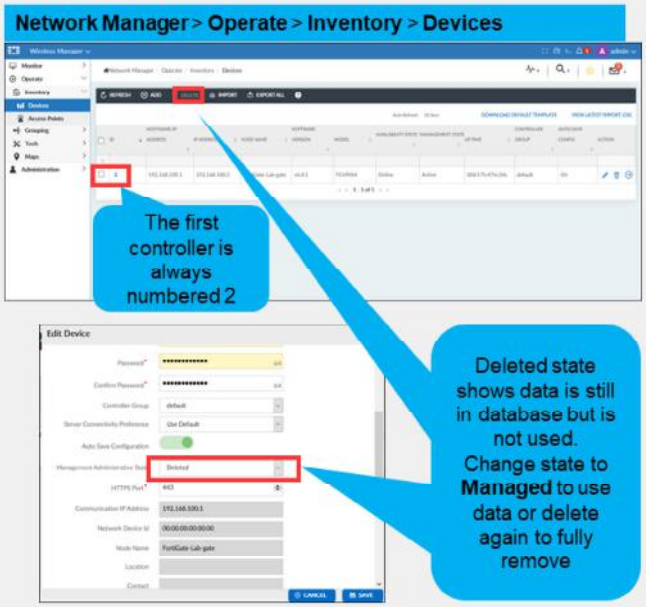
The system ID is applied at the Fortinet licensing portal together with the license code. This will result in an LMF license file being uploaded to FortiWLM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Controller Inventory

- FortiGate devices operating as wireless controllers need to be added to FortiWLM
- APs controlled by FortiGate are automatically added
  - Changes in AP configuration are automatically synchronized
- Controllers can be have multiple actions applied to them
  - **ADD**: Add an individual FortiGate
  - **IMPORT**: Add multiple controllers in the form of a CSV file. Template is downloadable from the **DOWNLOAD DEFAULT TEMPLATE** link
  - **DELETE**: Delete puts the controller in a temporary state. The data is still stored. Delete again and data is removed



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

24

The controller inventory contains all the FortiGate devices that are currently being monitored by FortiWLM. To enable monitoring of FortiGate, you can add them individually or by performing a CSV import. It is possible to download an example template for the CSV from the link. When you add the first FortiGate, you will notice that it is added with an ID of 2, which is by design.

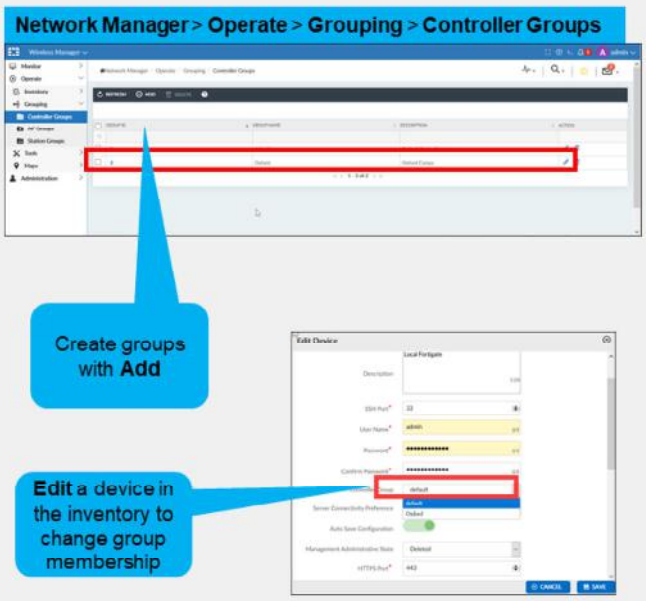
It is also possible to delete a FortiGate device. The deletion is a two-stage process. The first delete will move the controller into a deleted state, but not actually remove any data from FortiWLM. The deleted state will stop the data from being reported or used in any of the metrics. Deleting the controller again will fully remove the controller and data from the system. This two-stage process is to prevent accidental deletion.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Controller Grouping

- Controller groups allow the grouping of wireless controllers
  - Typically groups represent geographical locations
  - May contain multiple FortiGate devices of different models
  - Controllers may belong to only one group at a time
- Used for monitoring and administration purposes
- Non-hierarchical – no subgroups



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

25

After you import a FortiGate device into the inventory, you can add the FortiGate device into a controller group.
Controller groups allow the grouping of controllers together, typically based on geographical location. Where multiple controllers exist in a single location, it could make sense to organize them into a single group.
Controller groups are used for simple monitoring and administration purposes and are non-hierarchical; this means that there are no subgroups. There is no limitation to what type of controllers can be in a group, but a controller can belong to only one group.

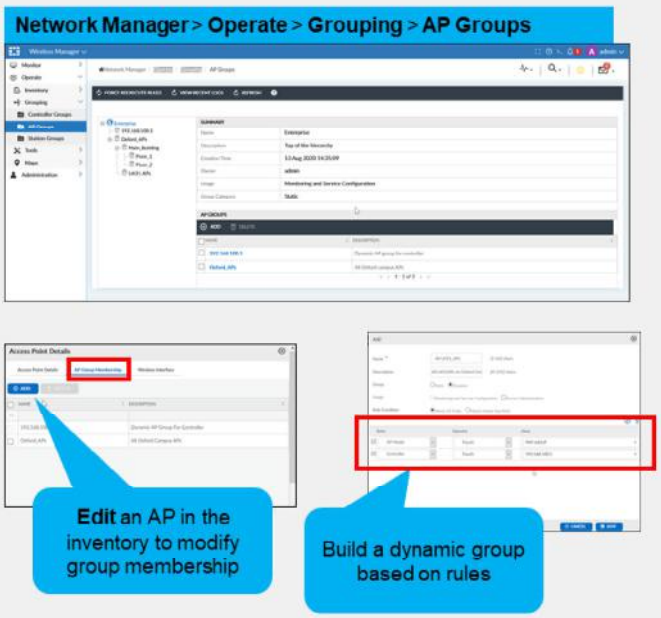
When you add a controller to a group, it is immediately taken out of any other group that it is a member of. To make a controller a member of a group, edit it in the device inventory where you will find the menu option allowing you to select an existing group.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

AP Grouping

- AP groups contain multiple APs
  - APs can be from any FortiGate controller
- An AP can belong to more than one group at a time
- AP groups are hierarchical
  - Groups can have multiple subgroups
  - Subgroups can have further subgroups
- Group membership can be static
- Group membership can be built dynamically
- Used for monitoring and notification purposes
  - Certain groups of APs can notify certain groups of users of issues



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

26

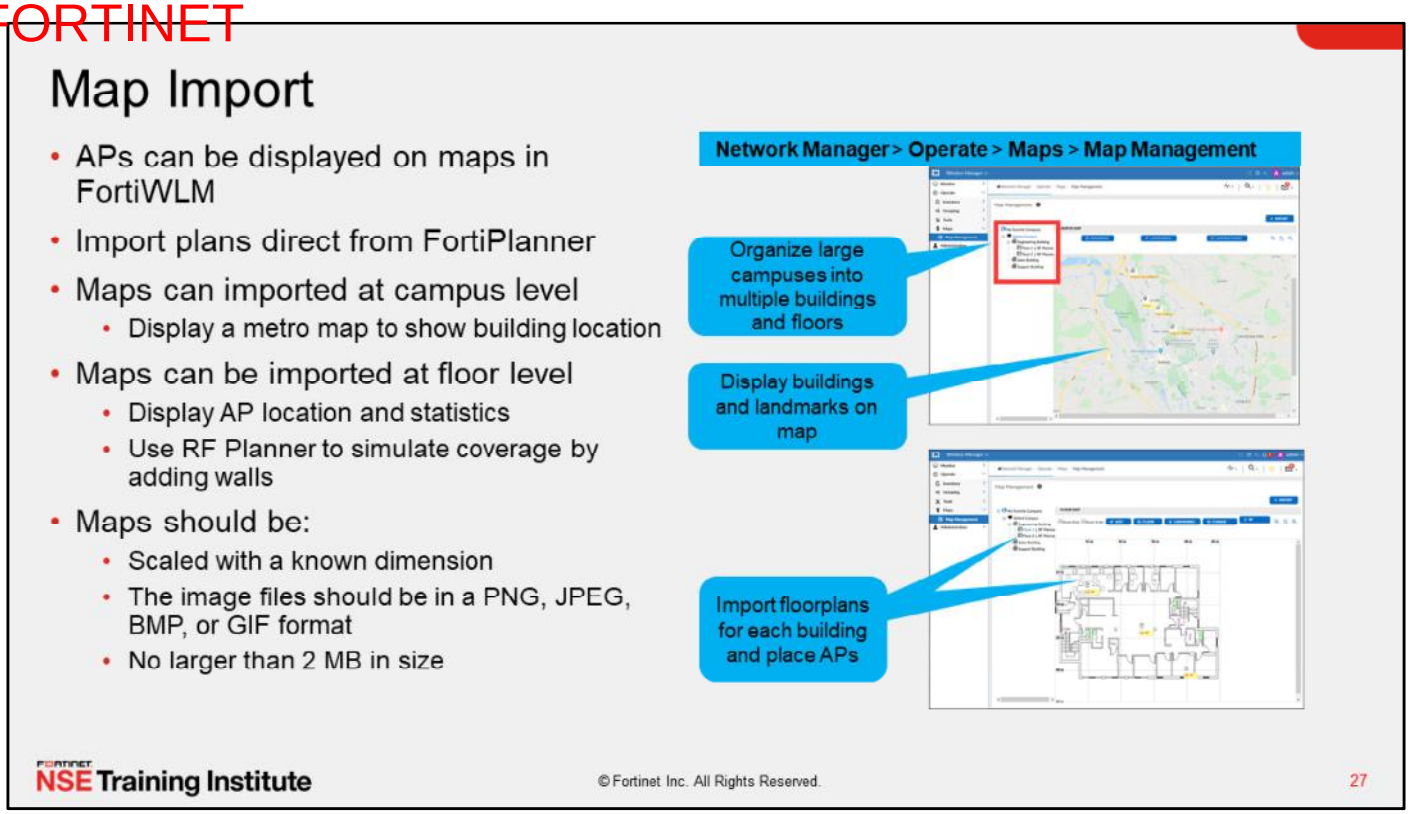
You can also group APs. APs groups are used for monitoring as well as for notification purposes. It is possible to use notifications to inform select administrators about problems with groups of APs. For example, all APs on a particular campus can be grouped together and then assigned to a notification profile. When a set of criteria is met, an email notification can be sent to a distribution group containing administrators responsible for the campus.

AP groups are hierarchical; each group can have multiple subgroups. Groups can be built dynamically based on a set of rules, for example, all APs of a particular type that are installed on a specific controller can be placed into a dynamic group. This avoids the need to maintain the group membership manually; any new APs that match the rules are automatically added to the group when installed. You can also build groups manually. Edit an AP in the inventory, and you'll see an option to make it a member of a group or groups. An AP can be a member of multiple groups; typically, groups also represent geographical locations. However, subgroups will give the ability to further organize APs, for instance, into floors and rooms of a building.

Currently, AP groups are used for monitoring and notification purposes only. Device administration groups are currently supported only on FortiWLC-based networks.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



One of the main benefits of using FortiWLM is the ability to visualize the wireless network. You can import maps and floor plans and then use them to display useful information about your network in the form of heat maps for monitoring purposes or RF planning using the RF Planner function.

You can import maps and plans at multiple levels. At the topmost level, it is possible to display groups of buildings on a campus. Organizations can have numerous campuses; each campus can have a metro map associated with it that shows the location of buildings and landmarks. Each building can then have multiple floors associated with it; each floor can have its own floor plan, which can be used to place APs on or for use with the RF Planner function.

Maps and plans should be in the PNG, JPEG, BMP, or GIF format and no more than 2 MB in size. Floor plans should be scaled and cropped to exclude as much white space around the plan as possible. When you import the file, you are asked for the dimensions. For instance, if the floor is 60 meters by 40 meters, you enter these dimensions. Network Manager will then scale the imported plan to 60 by 40 meters; however, if there is white space around the floorplan, this will cause the RF simulation to be incorrect because this white space is counted as part of the dimensions.

If you use FortiPlanner to plan your wireless networks, you can export the plans in a ZIP format and import directly into FortiWLM.

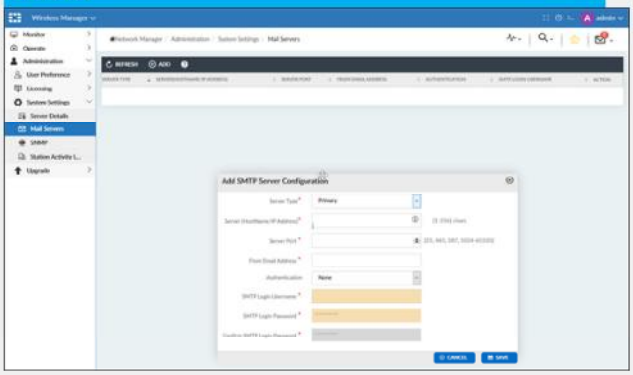
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Email Server Configuration

- To enable FortiWLM to send email notifications an email server is required
- SMTP with TLS, SSL, or none
- Multiple servers allowed

Network Manager > Administration > System Settings > Mail Servers



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

28

You can configure FortiWLM to send notification emails warning about issues with wireless network. To do this, you will need to define an email server.

You can define both primary and secondary servers. Servers are to support SMTP using TLS, SSL, or there is also the option to use no security.

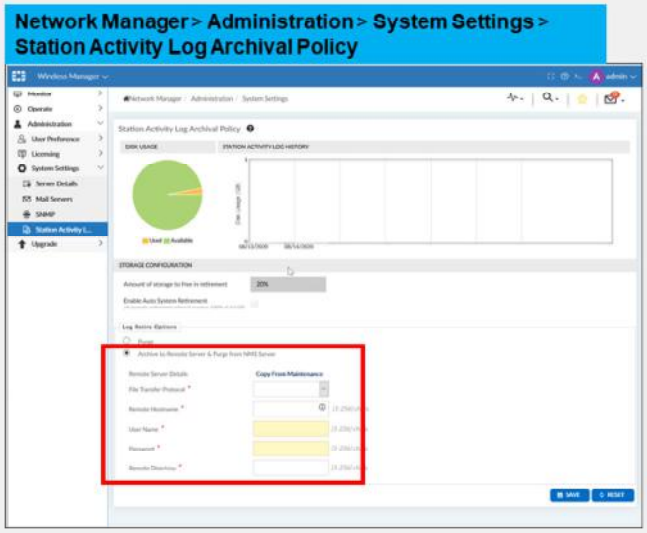
Once the email server is set up, it can be referenced in a notification profile.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Station Activity Log Maintenance

- The Station Activity Log is a log of events for all the stations that connect to the wireless network
- In large networks, this can generate a huge volume of information
- By default, 10 GB of data is stored
  - By default, FortiWLM will purge data when nearing capacity
- For compliance or security purposes, you may want retain data over an extended time
- Option to archive to a remote SCP or FTP server



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

29

The Station Activity Log is a function of the FortiWLM that collects detailed information about every station that connects to the wireless network. Detailed information about connection time, connection location, link rates, and data exchanged are all recorded.

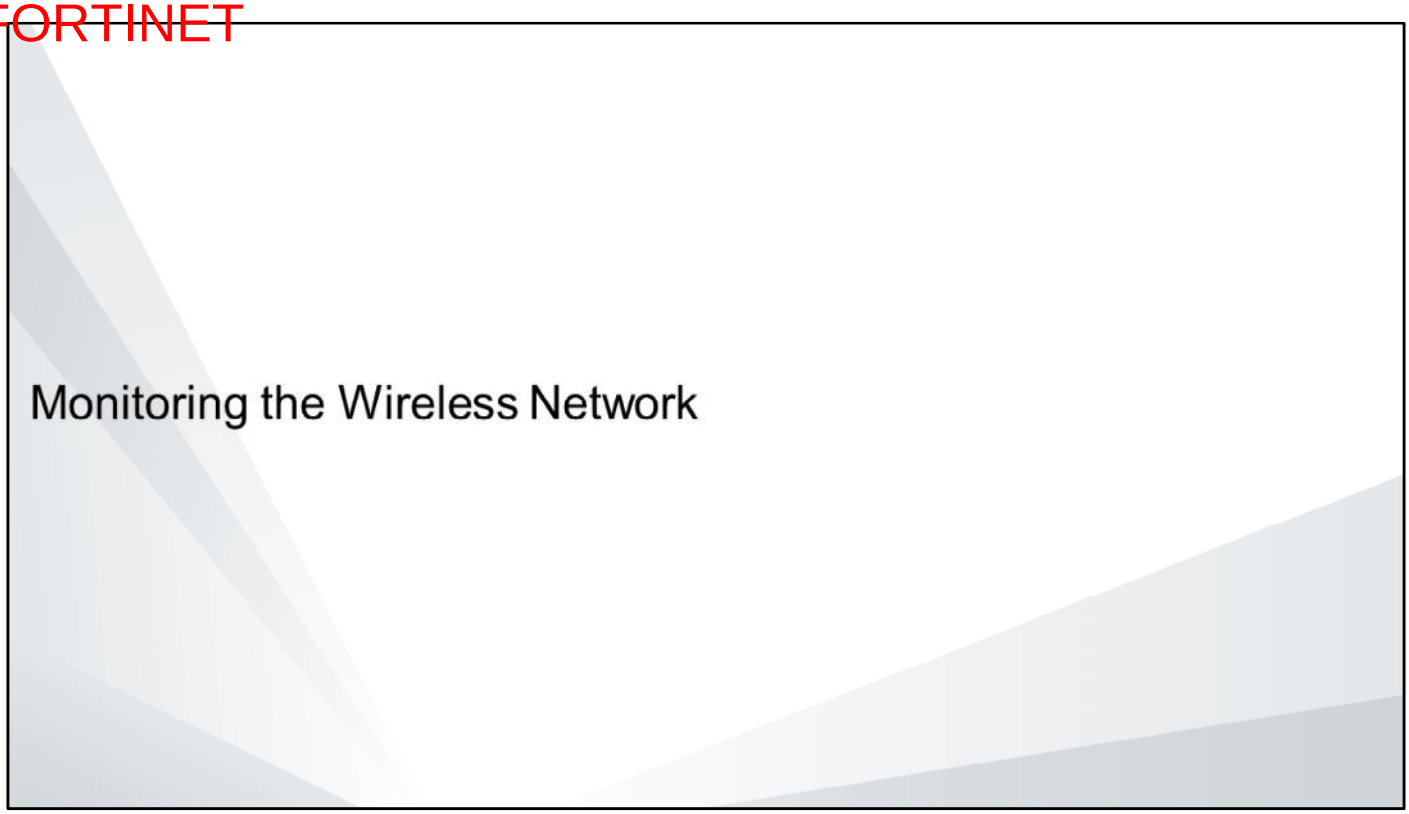
This information can be beneficial for extended monitoring purposes, but also for security and compliance, because it provides a forensic log of where and when clients connected to the network.

By its nature, this function generates huge amounts of data. FortiWLM has only a limited amount of space to store this information. As a result, by default, data is purged when the storage is nearly full.

If you wish to retain information for longer, you can specify an archive server that FortiWLM can archive data to, instead of deleting. The server can be an SCP or FTP server.

Vouchers & Dumps are Available | WhatsApp +201224560923

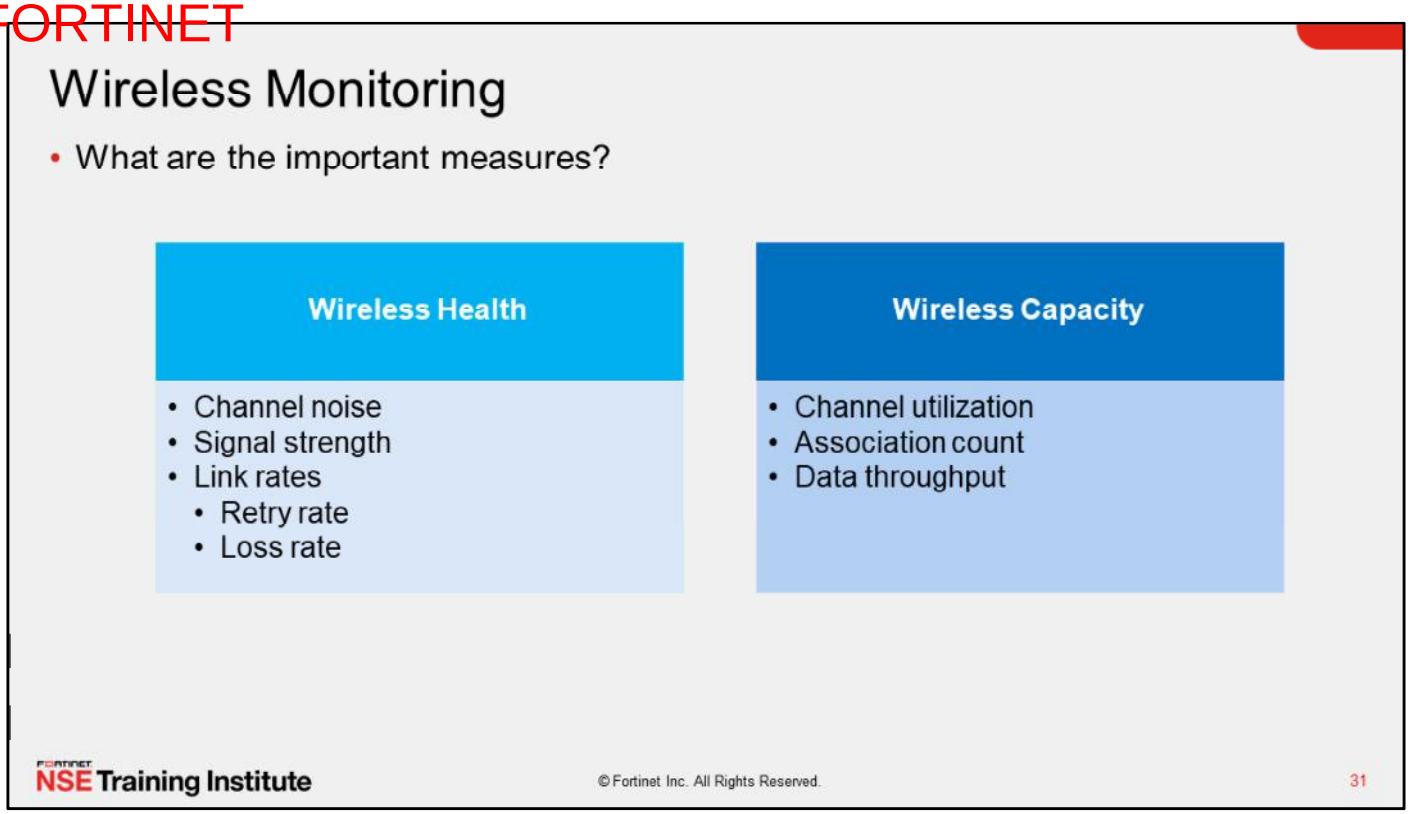
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn how to monitor the FortiGate managed wireless network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



A large proportion of wireless troubleshooting revolves around ensuring that a number of wirelesses metrics are within acceptable ranges.

The important measures belong to two broad categories—wireless health and wireless capacity.

Wireless health includes measures of factors that affect connection reliability, such as getting or staying connected to a wireless network. It is a measure of how healthy the RF is around a specific interface. Wireless health assesses how well wireless frames are being transmitted from the APs to the clients. You can check wireless health by looking at the channel noise measured by the interface in a specific area, the signal strength of the client, and the link rates that the client is using.

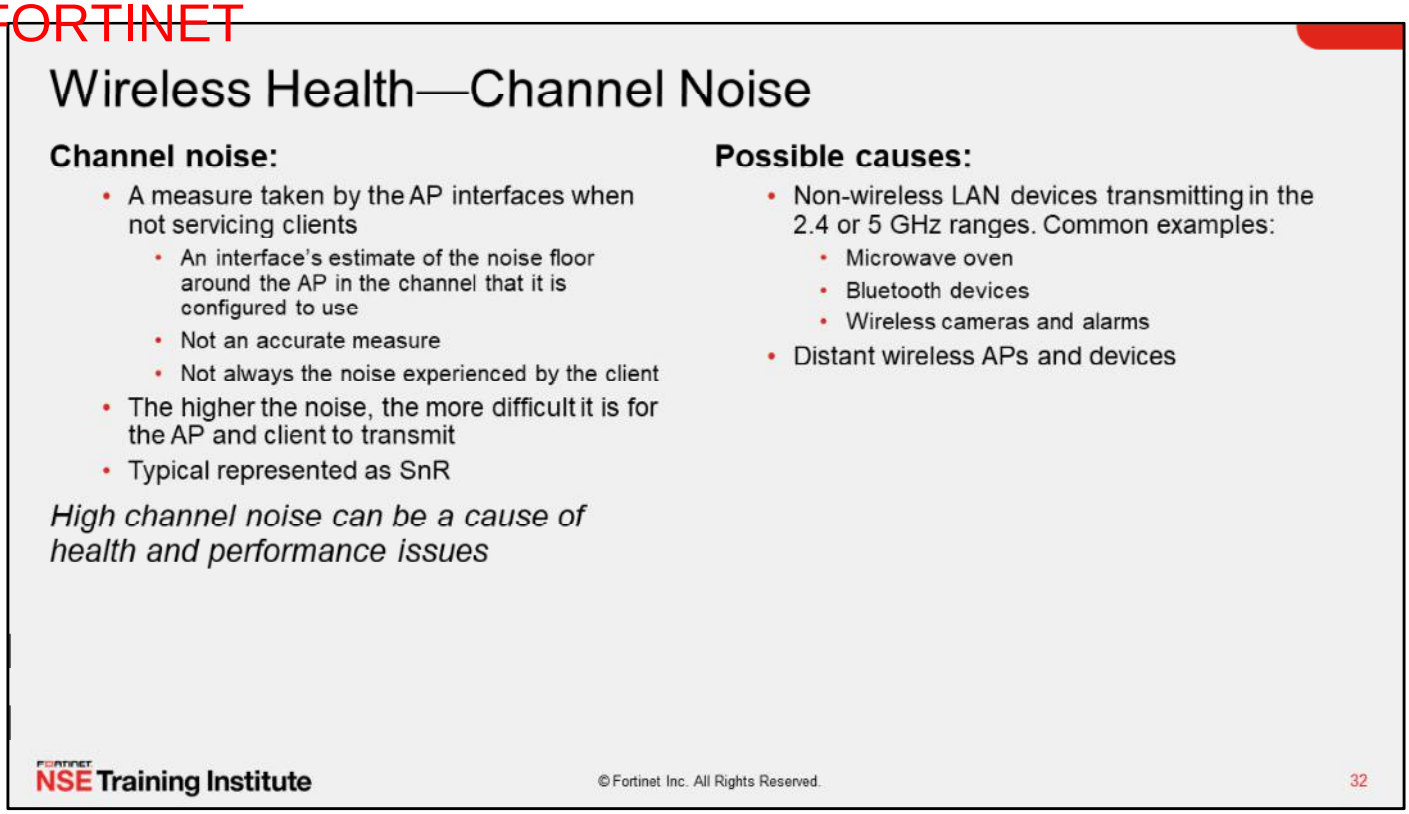
Wireless capacity measures factors that affect the capacity of the interface, and the channel capacity around the interface. It is a measure of channel utilization—how busy the interface and the spectrum is and the number of clients on an interface. The retry rate can be an indication that the collision rate is high, which can occur when there are large numbers of clients in the network. This is also a capacity measure.

A number of metrics are relevant to both categories; however, some are more important than others.

Some of these measures, such as retry and loss rates, are not easily measurable on FortiAPs; however, because these measures are important in the AP and client calculation of link rates, the link rate can be used as a prime indicator of connection quality.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



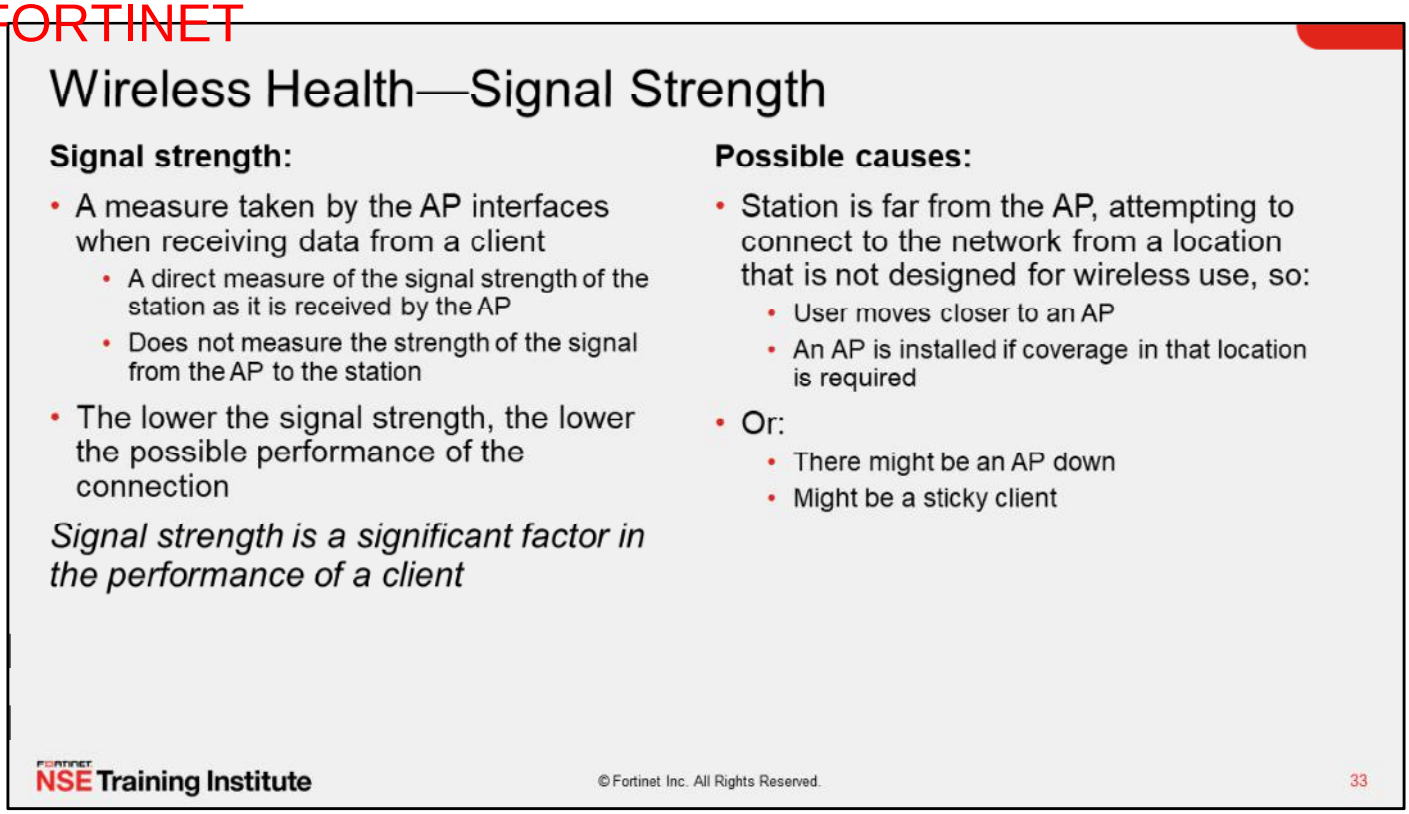
The AP interfaces are constantly monitoring the wireless channel they are tuned in to. One of the things an interface can do when it is not servicing clients is take a measurement of the noise floor. Channel noise is a measure of the background wireless signal that the radio cannot interpret as a wireless LAN signal. To a radio, any signal that comes from another non-Wi-Fi device sounds like radio static sounds to a human.

Ambient channel noise is generated by many different sources that can interfere with a network. The higher the level of noise, the lower the signal-to-noise ratio (SnR). This can affect both the APs and clients ability to send a frame. Often, both the client and AP radios will respond to the decrease in SnR by reducing the link rates of the connections. This can result in an acceptable signal strength, but a unusually low link rate, indicating that there is a potential noise issue.

Because the interface is not a dedicated spectrum analyzer, this measure is only an *estimate*. However, it is a very important indicator of potential interference in a specific area of the network. Such an interference would cause significant issues with the network if it was both powerful and frequent.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The controller maintains a list of the receive signal strength (RSSI), for all clients. RSSI is measured by the AP of each client as transmissions occur. It is *not* a measure taken by the *client* of the AP signal strength, which arguably is more important because the majority of data is downstream.

However, it is still possible to infer that the downstream signal strength is somewhat stronger than the upstream signal strength. In general, the transmission power of the AP is higher than the transmission power of the client, so it is reasonable to expect that the clients signal strength is somewhat less than the signal strength of the AP.

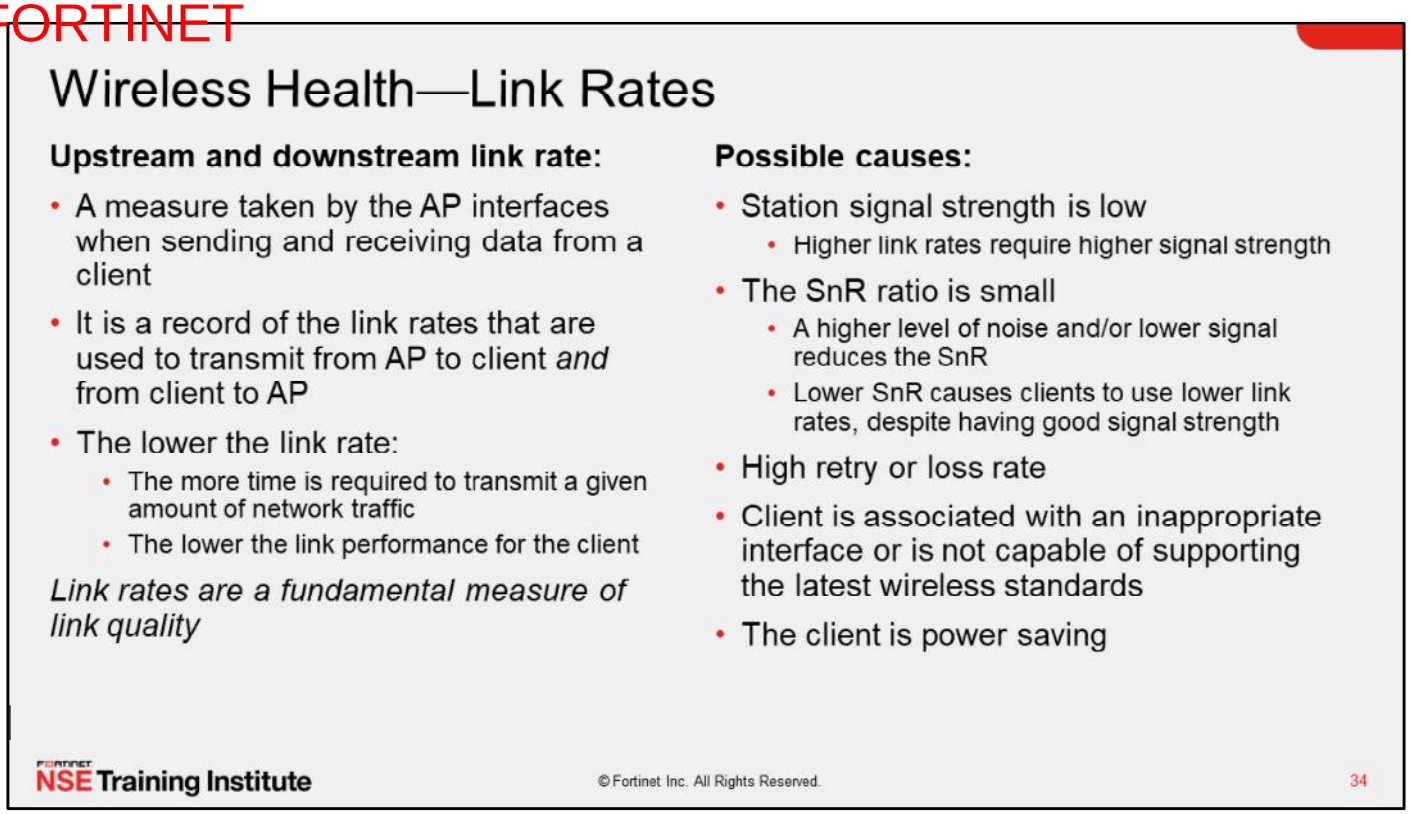
The lower the signal strength, the lower the ability of the radio to use higher modulation rates. The lower those rates, the lower the connection performance of the client. Low signal scenarios can occur for a number of reasons. Most commonly, someone is trying use the wireless network from a location that was never designed to support wireless devices. As a result, they are simply standing too far away from the AP. At that point, the user must choose to either move to a location that is designed to be supported by the wireless network or, if the location warrants it, install a new AP to improve the signal strength.

Low signal strength may also indicate that an AP has stopped running. The network is designed with overlap to allow for RF redundancy. In the event of an AP failure, there is usually another AP within range, even if it has a much lower signal strength. The result is that the client will associate with that other AP, but will appear as a low signal strength client.

In a more complex RF environment, a client might maintain a connection to the original AP. After the client moves to another location, they remain *stuck* to the original AP and are known as a sticky clients. In these types of design scenarios, low signal strength stations can be a fact of life. It may not be possible to eliminate low signal strength stations completely, but it is possible to monitor the number of devices that are poorly connected.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



The transmit and receive link rates show the data rates that are being used by the AP, which is the TX or transmit rate, and client, which is the RX or receive rate. Both are closely linked to signal strength—they often go hand in hand, but are also impacted by other factors. The AP keeps a record of the link rates used when transmitting to and from each associated client. The ultimate aim for all wireless implementations is to ensure that the link rates are as high as possible for clients. A high link rate means that both the signal strength and the signal quality are good. Because it is possible to measure the upstream link rate directly, this is a great way to check if the client is suffering from RF issues.

The higher the link rates, the faster data is transferred, and the less air time is used for transmissions. This not only ensures high performance for the client, but also allows maximum opportunity for other clients to transmit as well, improving their overall performance. The link rates are calculated by the wireless chipset, based on signal strength, the SnR, and the retry and loss rate of frames. A client might have very good signal strength but a low link rate, which could indicate that the noise floor is higher than is optimal because the SnR is potentially quite small. This prevents the client from using the upper link rates regardless of how strong the signal is. The frame retry and loss rates will also cause a lower connection rate. If either the client or the AP radio is struggling to send frames because, for example, there are a large number of collisions because of stations on neighboring APs, the radio can reduce its link rate to attempt to make transmissions more reliable.

Lower link rates may also indicate that the wireless client might be an older client and, as such, might only support older wireless standards where the link rates are a lot lower. For maximum efficiency, it is often worthwhile to ensure that these older clients are replaced as soon as possible with newer-standard clients that support more efficient link rates. Finally, upstream link rates can be reduced when a client enters power save mode. Many handheld devices will aggressively reduce link rates when they are not transmitting data because this can save significant amounts of battery power. However, this does make the client appear as if it is having a poor experience because the signal strength is often strong. Lower link rates are relevant in this scenario when you can see that the client is transmitting data. The radio should be trying to attain the highest link rates possible, and the fact that it isn't indicates that the client might have an RF issue.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Wireless Capacity—Channel Utilization

Channel utilization:

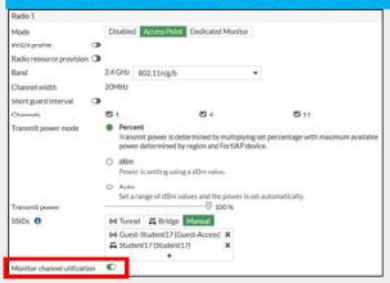
- A percentage count of used airtime on the interface channel
  - Around each AP for all interfaces
- It measures all wireless traffic in the channel
  - Controllers own AP and station traffic
  - Any other traffic from any other APs or station in the locality
- The higher the channel utilization the less capacity there is

Channel utilization is a primary indicator of capacity

Possible causes:

- Large number of station connections
- Poorly connected stations with low link rates
- High throughput applications
- High numbers of neighboring wireless networks on the same channel

FortiGate > WiFI & Switch Controller > FortiAP



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

35

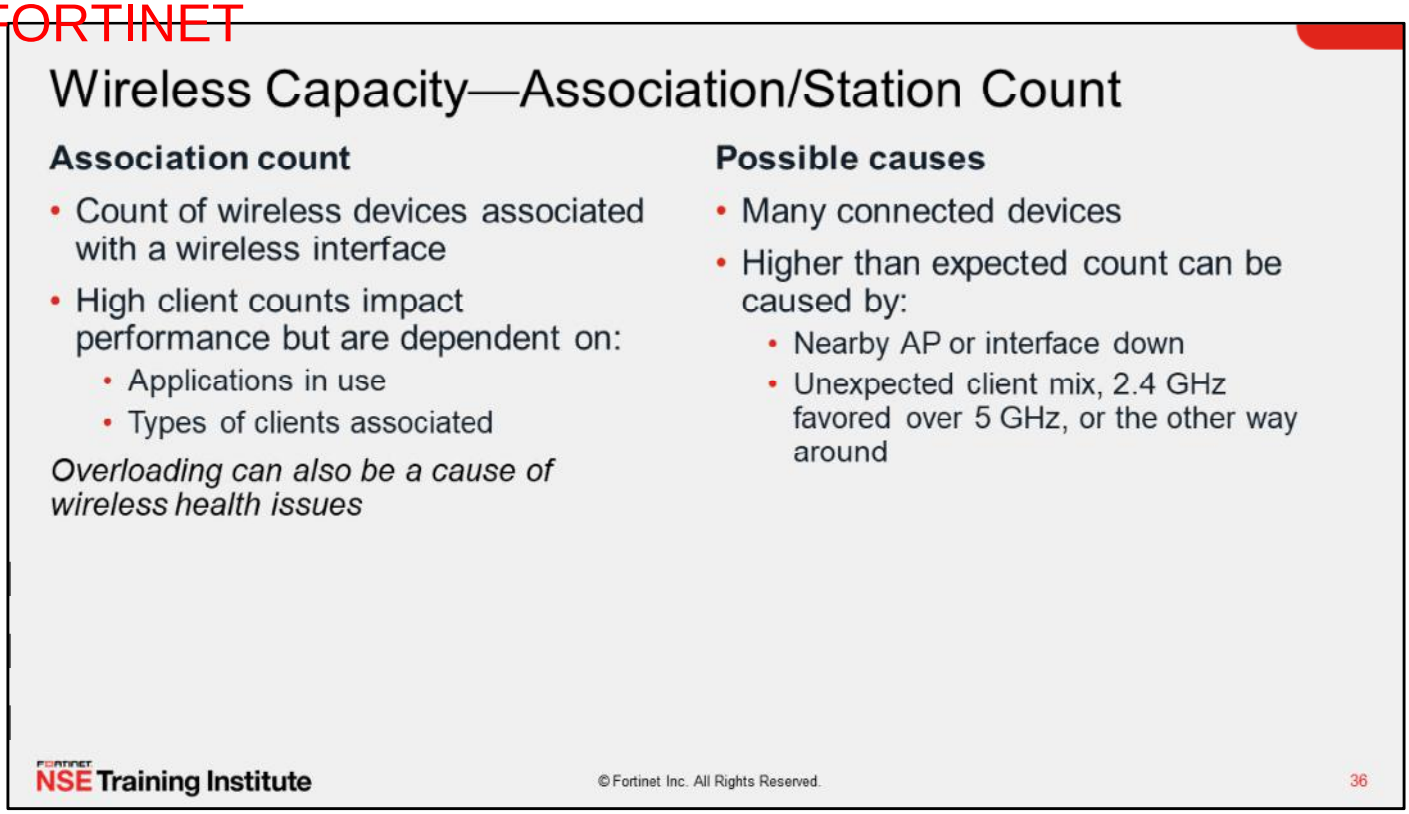
Channel utilization is the primary indicator of capacity around an interface. When enabled, the AP constantly monitors the amount of wireless traffic it can decode in the channel and provides a measure. It is not only accounting for traffic transmitted by its own clients, it is also is accounting for other wireless traffic on the channel, which could be coming from neighboring APs and wireless clients not associated with your wireless network. The neighboring APs and wireless clients still use capacity, even though they are not part of your network, and your network cannot transmit data while those other transmissions are occurring.

The higher the channel utilization, which is measured in percent, the less the spare airtime that is available. Channel utilization is the most important indicator of wireless capacity.

High channel utilization is usually caused by a high number of station connections, but can also be caused by a smaller number of stations transmitting a large amount traffic. It does not matter if the stations and APs are your own, or if they are neighboring devices.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

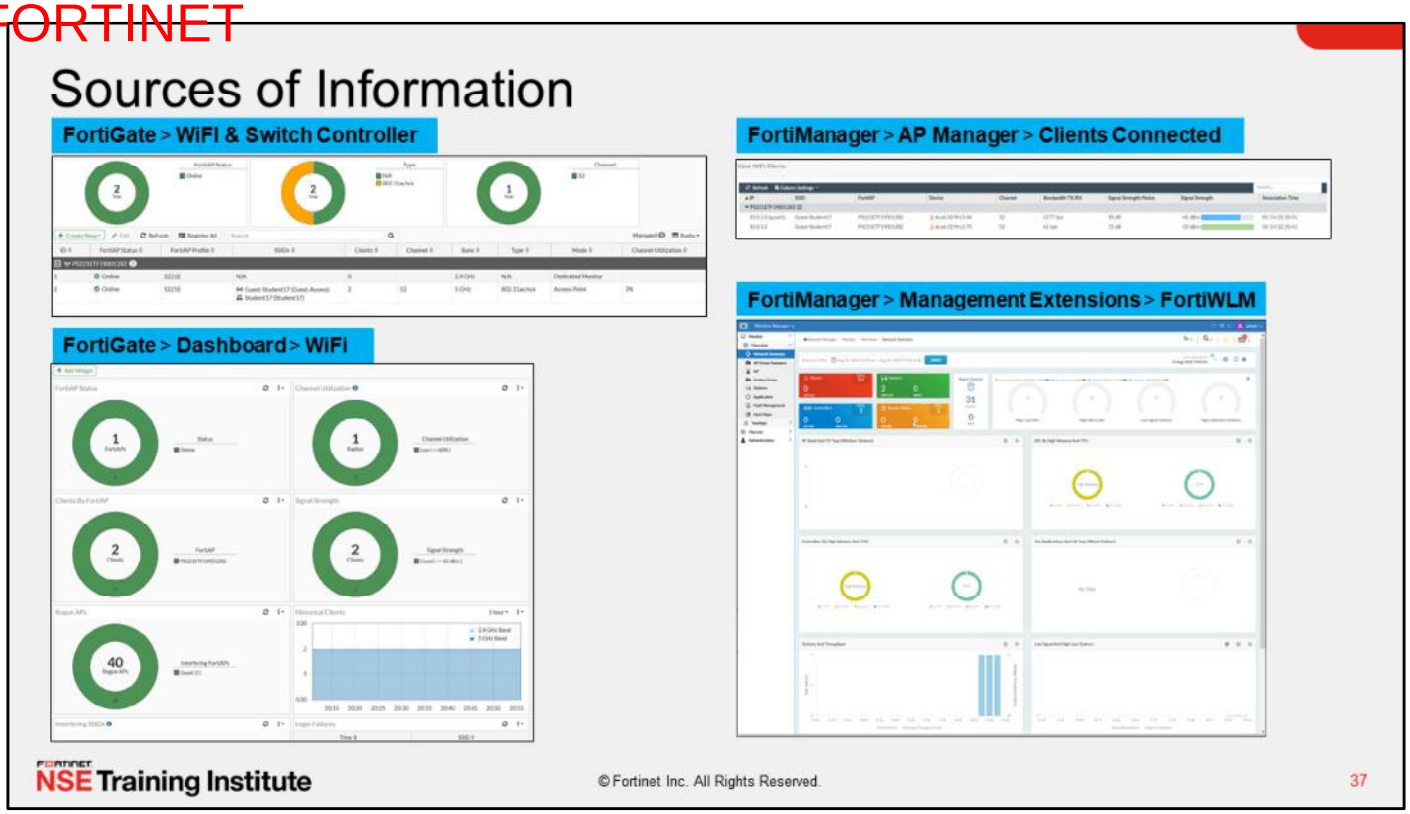


Another critical metric for your wireless interface is the associated client count. Association count is a measure of the number of clients associated with each interface. A high client count will always affect performance, but the applications in use and the types of clients also matter.

Many devices means many associations. A higher than expected count can be caused by a nearby AP that stops running, or an unexpected mix of clients that prefer one frequency range over another.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



So, where do you find information about these metrics?

There are multiple sources of information, dependant on the products that are available in the network.

Information that is available from FortiGate is generally related to the *current* status of the wireless network. The amount of historical wireless data that is available is generally less.

FortiManager and its optional FortiWLM management extension provide additional monitoring capabilities for the wireless network, in addition to the core monitoring functions available using FortiGate.

One of the key benefits of implementing the FortiWLM module in FortiManager is the ability to record metrics and events over time. FortiWLM will report on statistics about the wireless network going back days, weeks, or months.

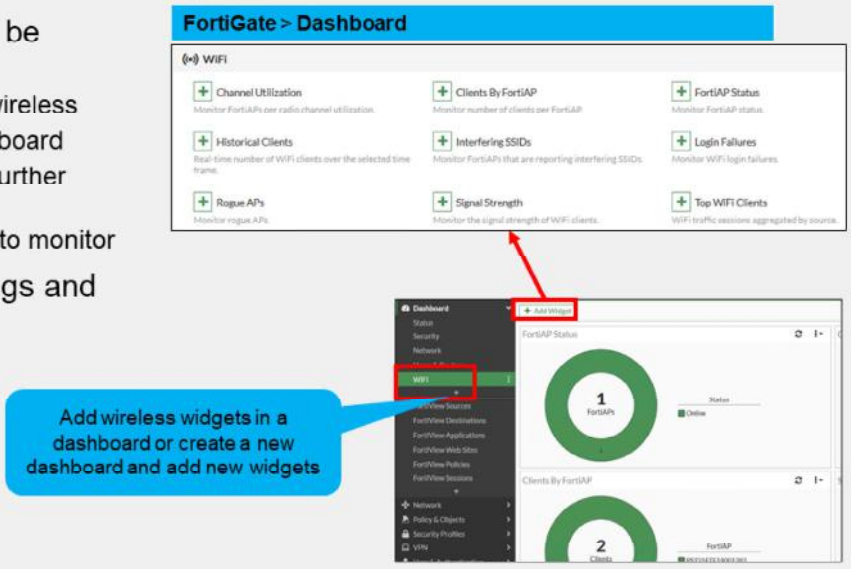
It is often an exercise to collate all the relevant information to form a picture of the wireless environment.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiGate—Wireless Widgets

- Optional widgets that can be added to a dashboard
  - No default dashboard for wireless
  - Can be added to any dashboard
  - Clickable as a shortcut to further information
  - Widgets can be converted to monitor
- Some widgets have settings and durations
- Key widgets to monitor:
  - **Channel Utilization**
  - **FortiAP Status**
  - **Signal Strength**



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

38

The wireless widgets are a great place to start. By default, wireless widgets are not added to any dashboard. If you are regularly monitoring wireless performance and capacity, it is a good idea to create a dedicated dashboard that consists of wireless widgets. The widgets will be color-coded to indicate their status.

Of particular interest will be the **Channel Utilization** and **Interfering SSIDs** widgets. These widgets highlight the radio interfaces that are potentially suffering issues from high channel utilization or excessive interference

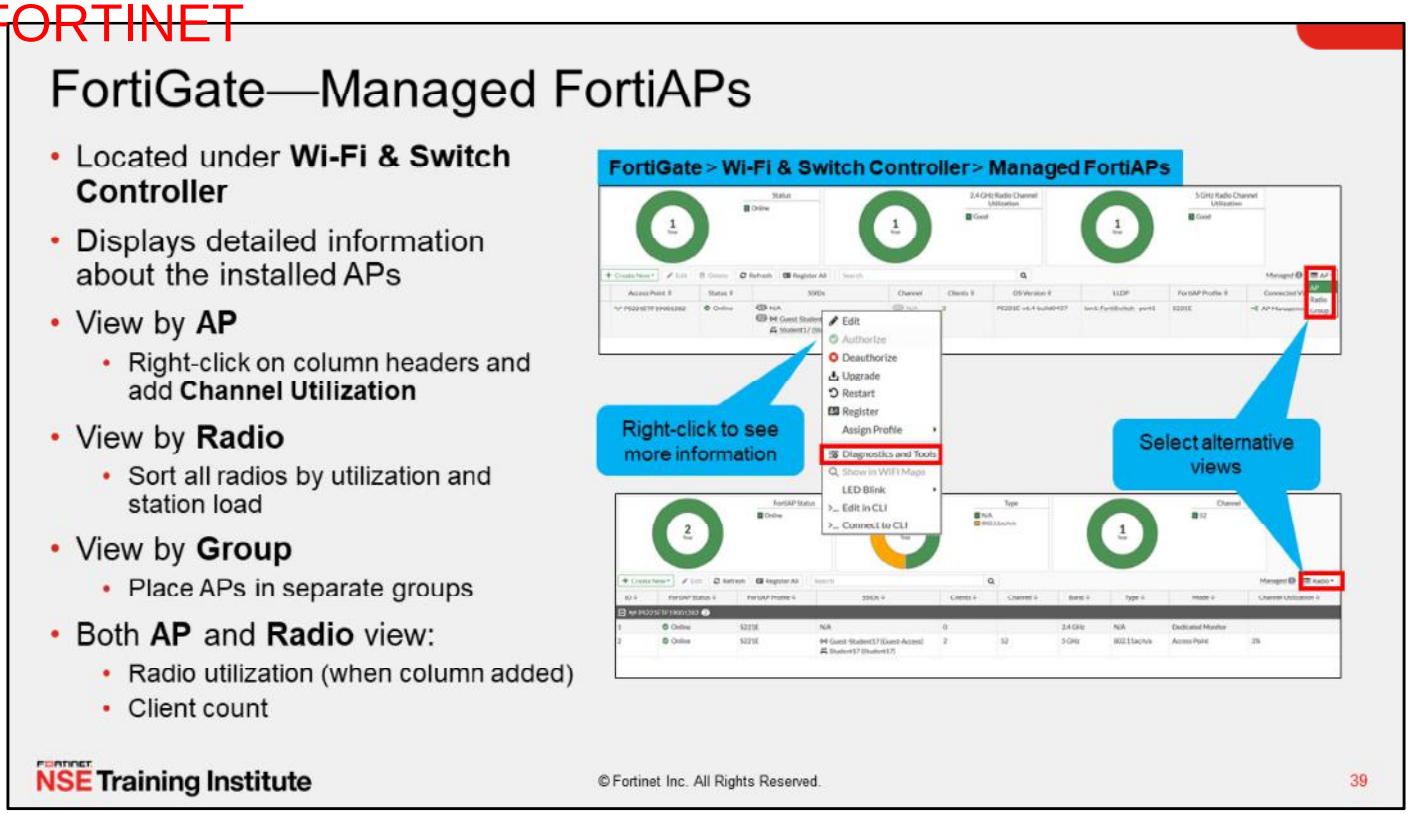
Clicking on the widget elements often reveals more information in the form of a table. Click the **Channel Utilization** widget, and you will see a complete list of all the wireless interfaces supported by FortiGate, together with the channel utilization.

In the **Interfering SSIDs** widget, you can click a radio to reveal a table of interfaces. You can sort these tables to highlight radios that are interfering the most.

The widgets can quickly show essential information that you can use to diagnose potential causes of poor performance and connection reliability. You can also convert them into monitors.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Starting at FortiGate, the **Managed FortiAPs** table also contains useful information about the status of connected APs.

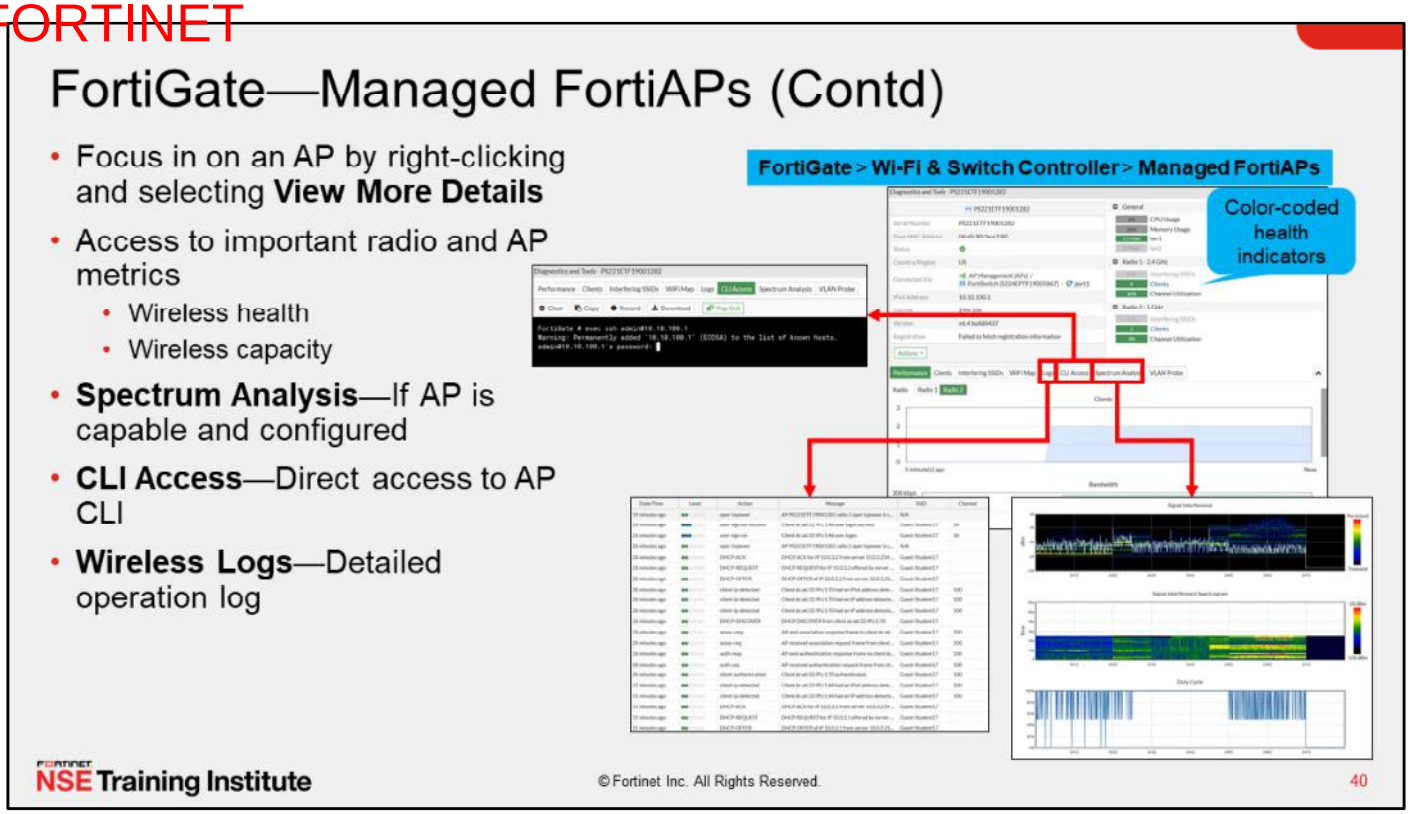
Found under **Wi-Fi & Switch Controller** > **Managed FortiAPs**, it provides three different views.

AP View is the default view and groups radio interfaces together under an AP.

The **Radio** option is more useful for assessing load because it allows you to easily sort the radios to highlight interfaces that are in trouble. Note that you can add useful columns, such as **Channel Utilization**, to a view.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



When you right-click an AP, you get the option to select **View More Details**. You can see a more detailed summary of the individual AP details and can perform basic actions on the AP, such as upgrade, restart, or de-authorize. It is also possible to edit the configuration directly, which will override the profile settings.

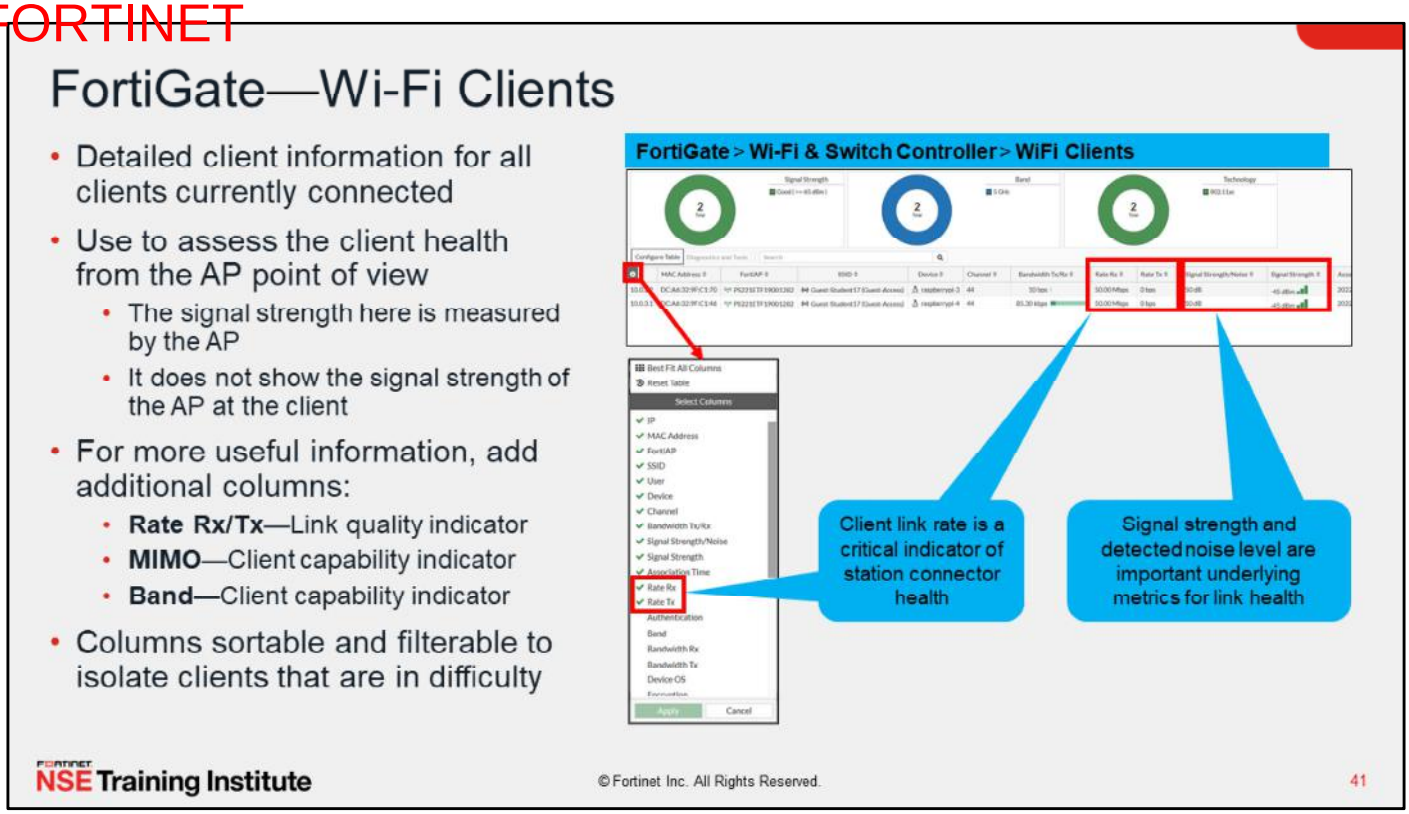
You will see color-coded health indicators in the upper-right corner, which will give you an immediate indication as to the status of the AP and its radios. The colors indicate the severity of the issue, using the colors red, green, and yellow to indicate the severity.

The table shows the configuration and the status of the radios by default. The **Clients** tab shows all the clients that are associated with the AP. You can also drill down into the individual clients, if required. The logs view filters the wireless events just for this AP. Double-clicking on each event will shows the event details.

The CLI access option allows direct access to the APs CLI, if required. If the AP is capable and is configured for dedicated operation, then you will be able to enable spectrum analysis. Not all APs are capable of spectrum analysis—refer to the release notes for more information. The spectrum analysis view shows the real-time view of the wireless spectrum, together with any detected interferers.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



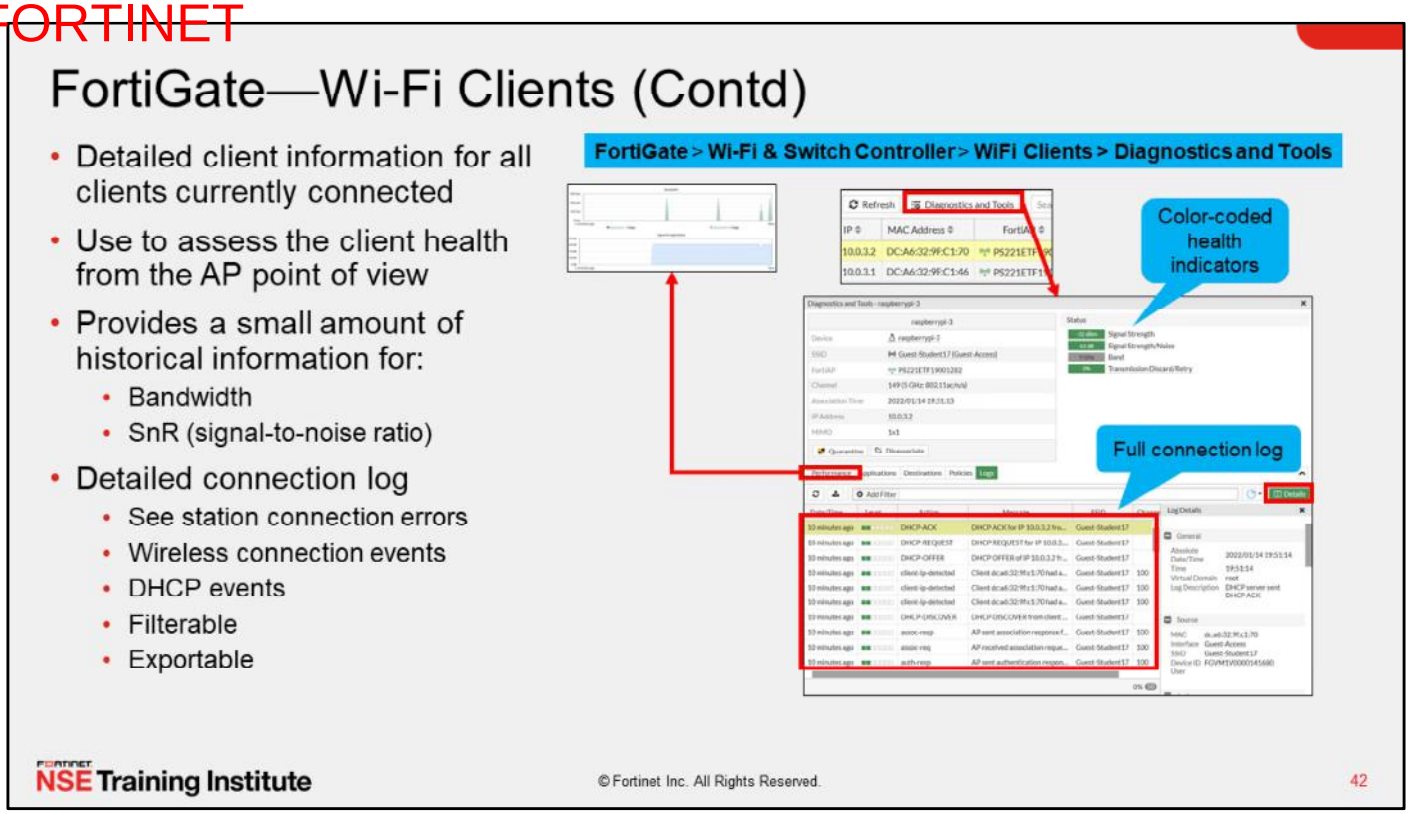
The **WiFi Clients** table provides detailed information about clients that are currently connected.

Again, you can add additional columns to provide useful information about a client's connection state, such as the signal strength the AP is receiving from the station, the downstream link rate, the channel configuration, and so on.

Again, you can sort and filter to highlight clients that are in trouble.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Select a station in the client list. Then, right-click and select **Diagnostics and Tools** to open diagnostics about a station.

From here, you can perform basic actions, such as quarantine or disassociate workstation. The health icons are color-coded and will give an immediate indication of any issues, such as poor signal strength or SnR.

There is an option to display a graph which, by default, will show bandwidth but can also show SnR. The graphing is limited to approximately 10 minutes of data.

If you select the **Logs** tab is possible to see a logical log of a station connection events. This log is useful for quickly diagnosing common connectivity issues, such as incorrect passwords or pre-shared keys, because the association and authentication steps the wireless client performs are listed in the log. You can see details of each log event by clicking the **Details** button. This can show further information about any failures.

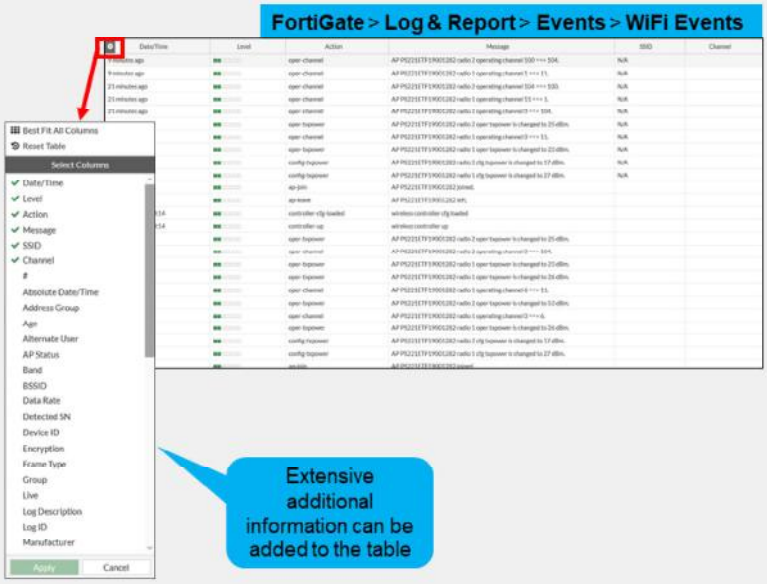
Filter the log and export its contents into a text file for a more detailed analysis.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiGate—Wi-Fi Events

- Provides a historical log of wireless-related events
- To view specific station information
  - Add the following columns:
    - **Band**
    - **Data Rate**
    - **Physical AP**
  - Add a filter for Station Mac
- To monitor a specific AP
  - Add the following columns
    - **Physical AP**
  - Add a filter for **Physical AP**



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

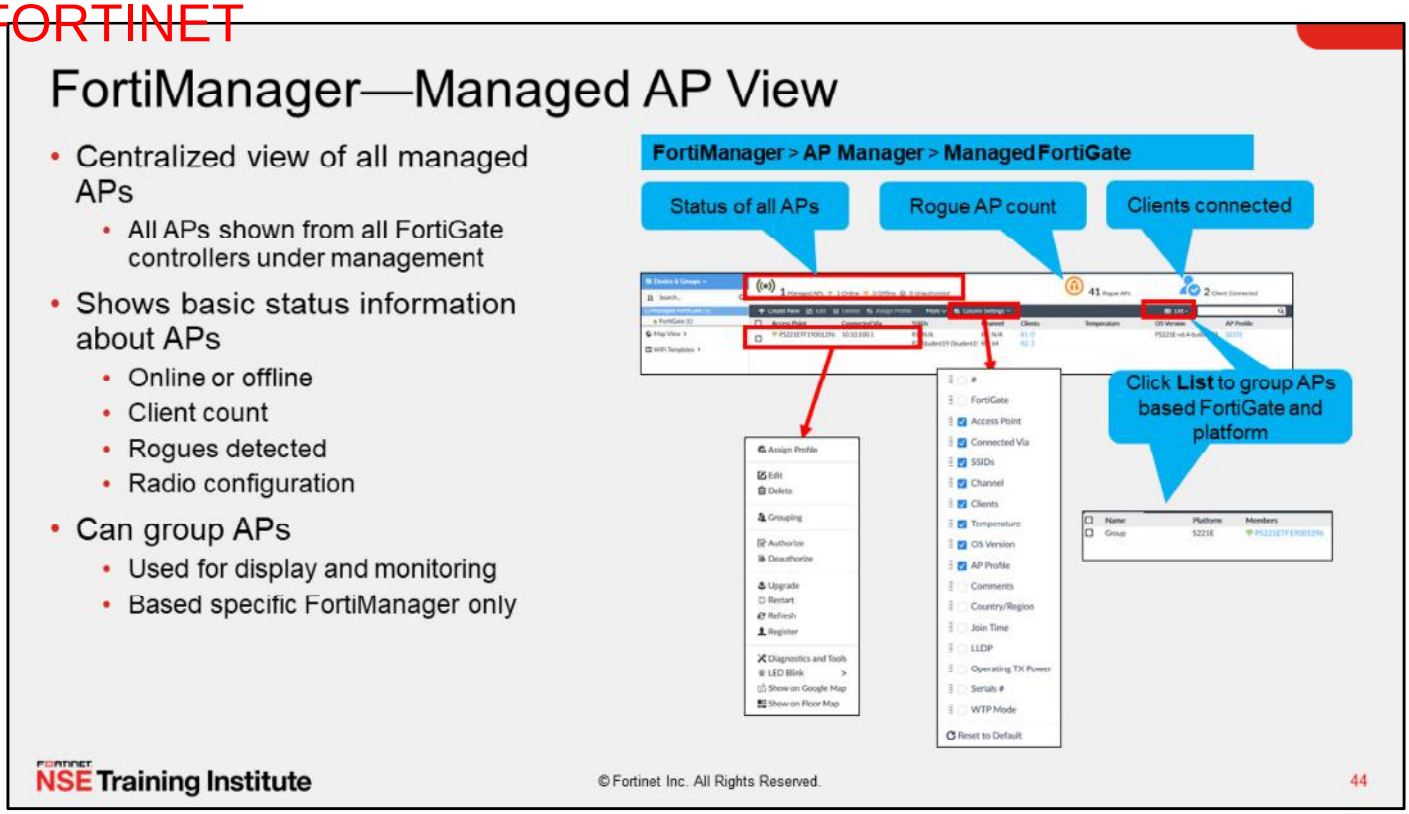
43

The **Events** table provides a whole-controller historical view of the wireless network. You can use this to identify events that affect both clients and APs over time.

Adding additional columns and filtering allows you to focus in on wireless clients or APs that are misbehaving.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



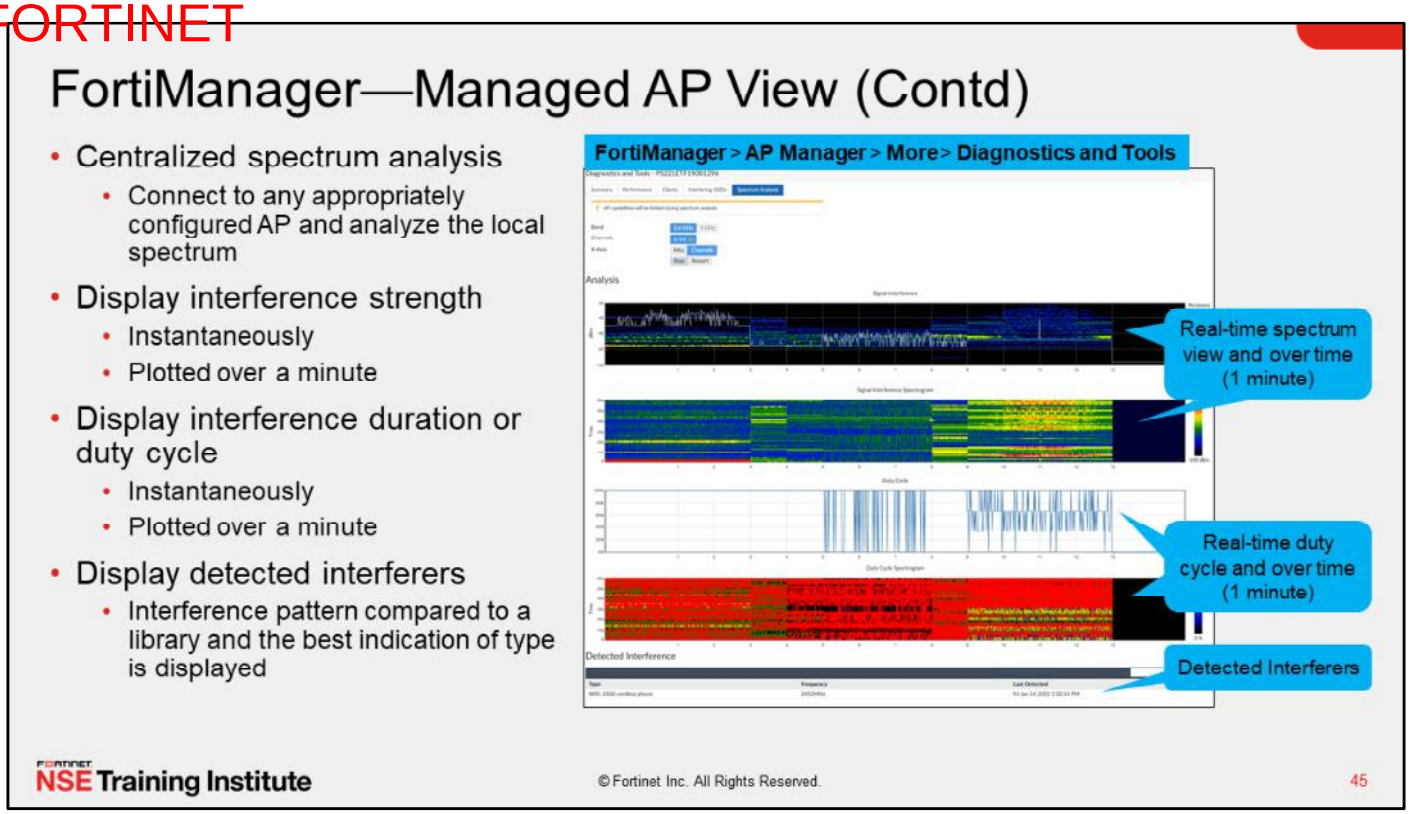
When FortiManager is installed in the network, you can use it to perform basic monitoring of the status of APs and clients. The main benefit of using FortiManager is that you can get an overall view of the APs installed on the network without having to go to each FortiGate in turn. However, the amount of information available on FortiManager, specifically about the status of radios, is less than what is being available on FortiGate.

The **Managed APs** view is mostly used for configuration, rebooting, upgrading, or assigning profiles. However, you can also see useful metrics here. The total number of managed APs is shown, together with a count of the APs that are offline and online. Clicking on the rogue AP count icon will take you to a complete list of the rogue APs detected by all of the APs on the network. Likewise, clicking the client's connected icon will take you to a table that shows all clients connected to all of the APs managed by FortiManager.

You can also group APs for display and monitoring purposes. These groups are used inside FortiManager only. Groups to organize the displays so you can drill down and monitor APs in a more organized way. APs can belong to multiple groups, but the groups are specific to a controller and an AP type.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



FortiManager also includes the ability to perform a centralized spectrum analysis. Some FortiAPs can operate their wireless chipset in two modes. The first mode is normal mode, which supports wireless client connectivity, and the second put the radio into spectrum analysis mode. Refer to the AP datasheet to see if an AP is capable of spectrum analysis. To put the radio into spectrum analysis mode, you will need to configure both radios of an AP as dedicated sensors. The best way to do this is to create and assign an AP profile. Once done, you will be able to right-click an AP and select **View Spectrum Analysis**.

By default, the 2.4 GHz range is selected for analysis, although you can choose 5 GHz as well. When selecting 5 GHz, you will need to choose a range of channels to scan. There are three useful pieces of information displayed.

The first two graphs cover signal interference—all the power of the interfering signal. This is usually a measure of how close the interference source is. The smaller the negative number, the more powerful the signal is. You can see the instantaneous value as well as a plot of the signal strength over the last 60 seconds.

The duty cycle is a measure of how constant the interference is. The longer the duty cycle, the more disruptive the potential issue.

The final table shows a list of detected interferers. FortiManager will compare the spectrum signature against an inbuilt library of known interference sources and display its best guess as to what the interferer is.

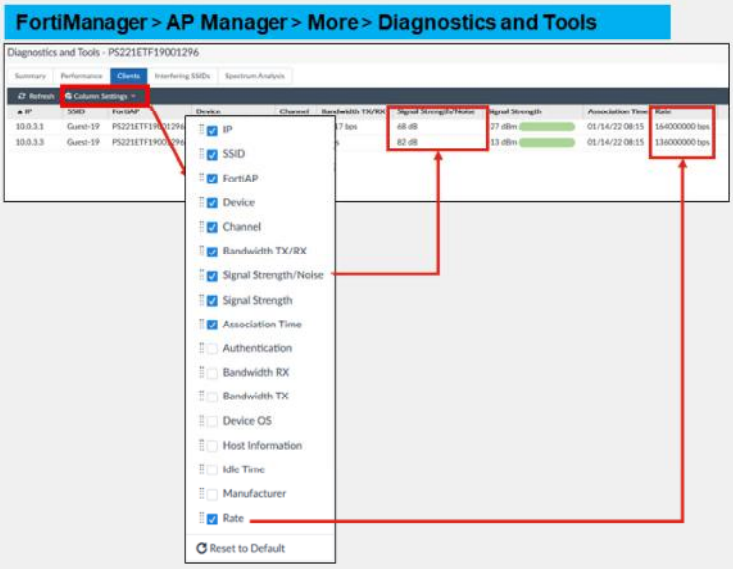
Interpreting the output of the spectrum analyzer requires experience and practice. Experimenting with, and viewing, the output of the spectrum analyzer is recommended. The more experience you get looking at different spectra, the easier it becomes to identify unusual events.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

FortiManager—Client Monitor

- Full list of all clients associated with the APs
- Add columns for more information
- Tables are sortable to highlight clients that are having issues
- The **Rate** and **Signal Strength** columns are recommended



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

46

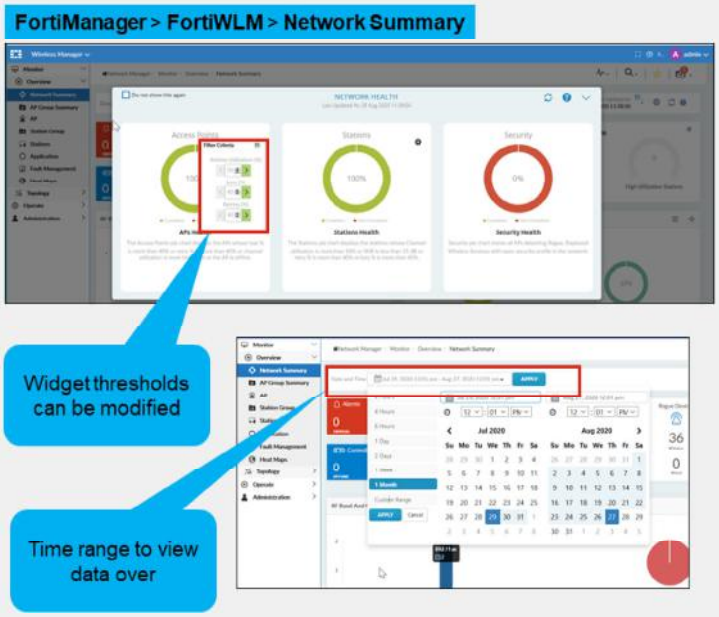
The **Client Monitor** shows a list of all the clients currently associated with the APs. If you have created different groups of APs, the list will be filtered depending on which AP the clients are connected to. You can add extra columns; the **Rate** measure displays the downstream link rate from the AP to the client. Together with the **Signal Strength** column, this is probably the quickest way to determine the health of a station's wireless connection. As with other tables, you can sort the columns to identify clients that are having issues.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiManager—FortiWLM Summary

- **FortiWLM** communicates *directly* with FortiGates that have been added
- **FortiWLM** does not import information from **AP Manager**
- **Network Summary** is the default screen
  - **Network Health** will give an immediate overview of network using three fixed widgets
- Almost all views have a time period
  - From two hours to one month
  - Or custom



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

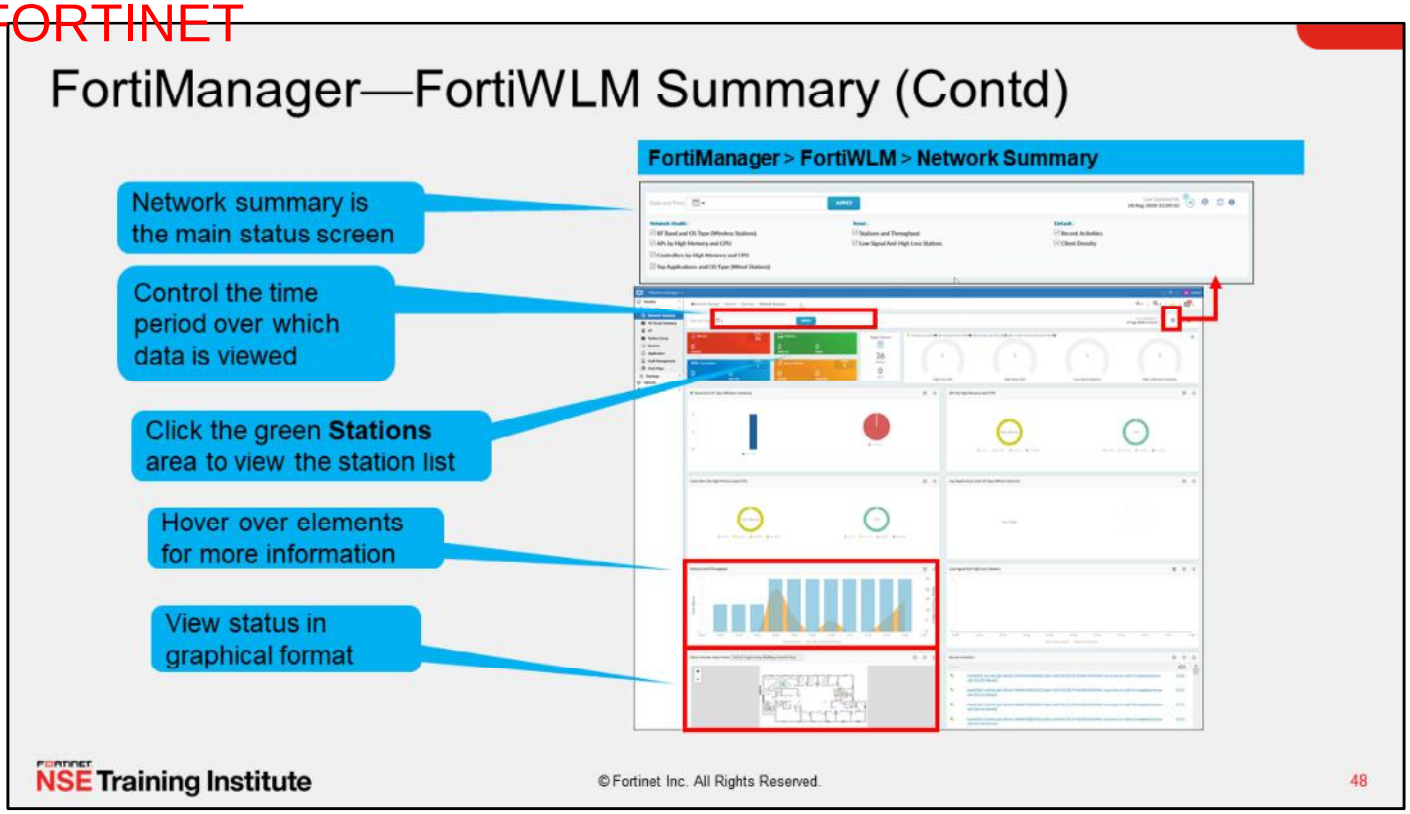
47

The FortiWLM module is the final source of monitoring information. This module operates alongside AP Manager as FortiManager as an optional management extension. It interfaces directly with the FortiGate device installed on the network. It is important to note that information is not imported from the AP Manager. You must add FortiGate devices separately to enable monitoring from FortiWLM. The **Network Summary** screen is the first screen displayed when you open Network Manager. By default, you will see a **Network Health** pop-up window. This shows three fixed widgets that give a quick status view of the APs stations and the health of the wireless network. The widgets are fixed. However, you can change the thresholds that govern the color codes. Each widget shows a color code that indicates status. The more green you see, the better the condition of your wireless network. Each widget will have a description for the thresholds. For instance, the **AP Health** widget will display APs that have greater than 40% loss or retry, or a channel utilization greater than 50% as non-compliant.

The **Network Health** widgets are in a media assessment of the network. You can refresh it by clicking the refresh icon, and a new assessment is made. Many more of FortiWLM displays are time related. This allows you to view of data over a flexible time range. This ability to view the detailed status of a wireless network over time is one of the main benefits of using FortiWLM.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



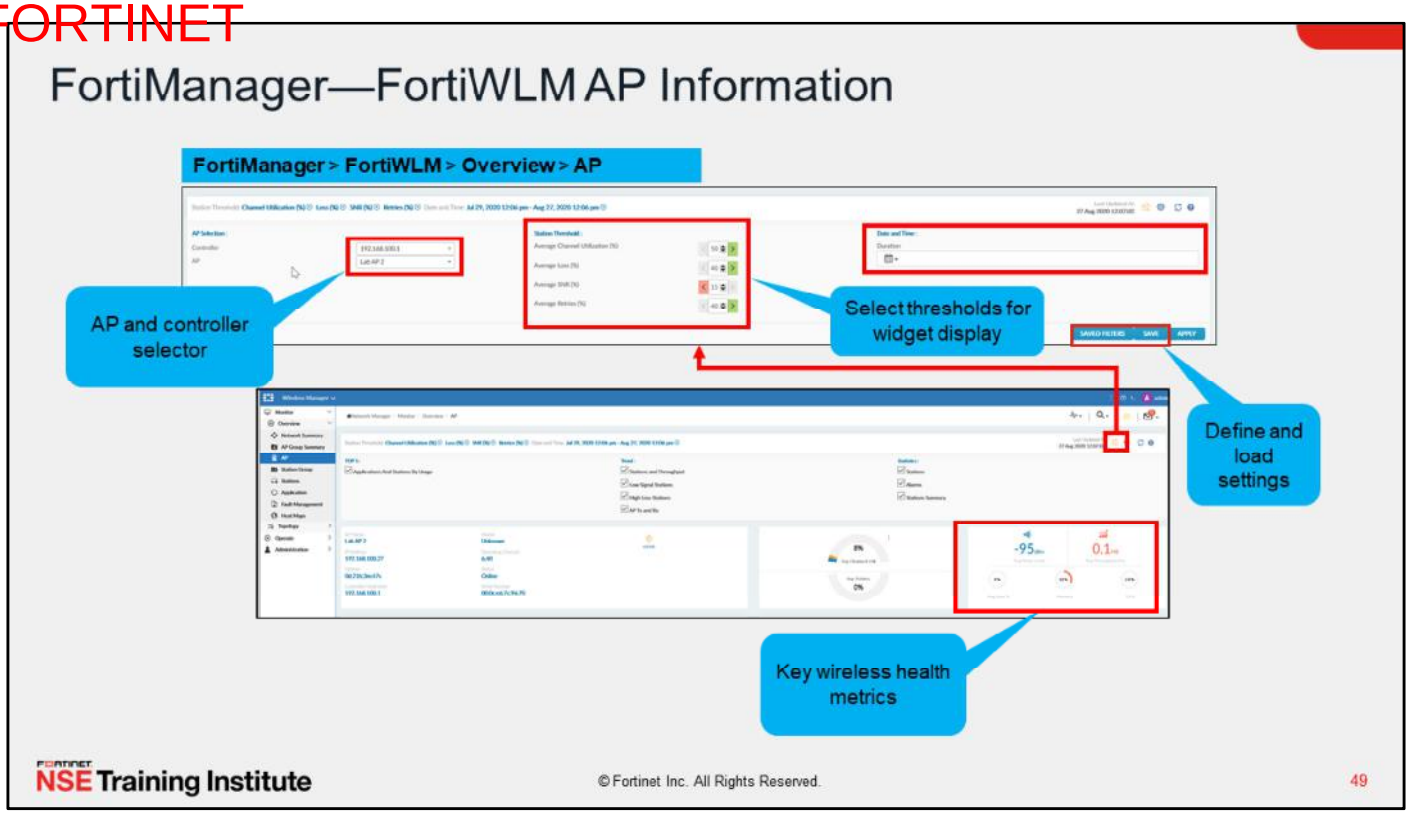
The **Network Summary** screen is the most complete source of information about the wireless network. If you were to display one screen in a network operations center (NOC), it would be this one, because it contains the most information in one view. You can add or remove widgets and information elements, and you can change the time range over which the data is displayed. The display itself will update every 60 seconds and will display the status of the network at that point.

Many of the widgets have thresholds that you can change. This causes widgets to display information after the underlying metric has crossed a specific threshold. This makes it easy to quickly identify things as high retry APs quickly.

It is also possible to display information in graph format, and APs on the floor plans (if they have been setup). Hovering over many of the information elements will show more information. For example, hovering over the columns in the **Stations and Throughput** table shares the number of stations contributing to that measure.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



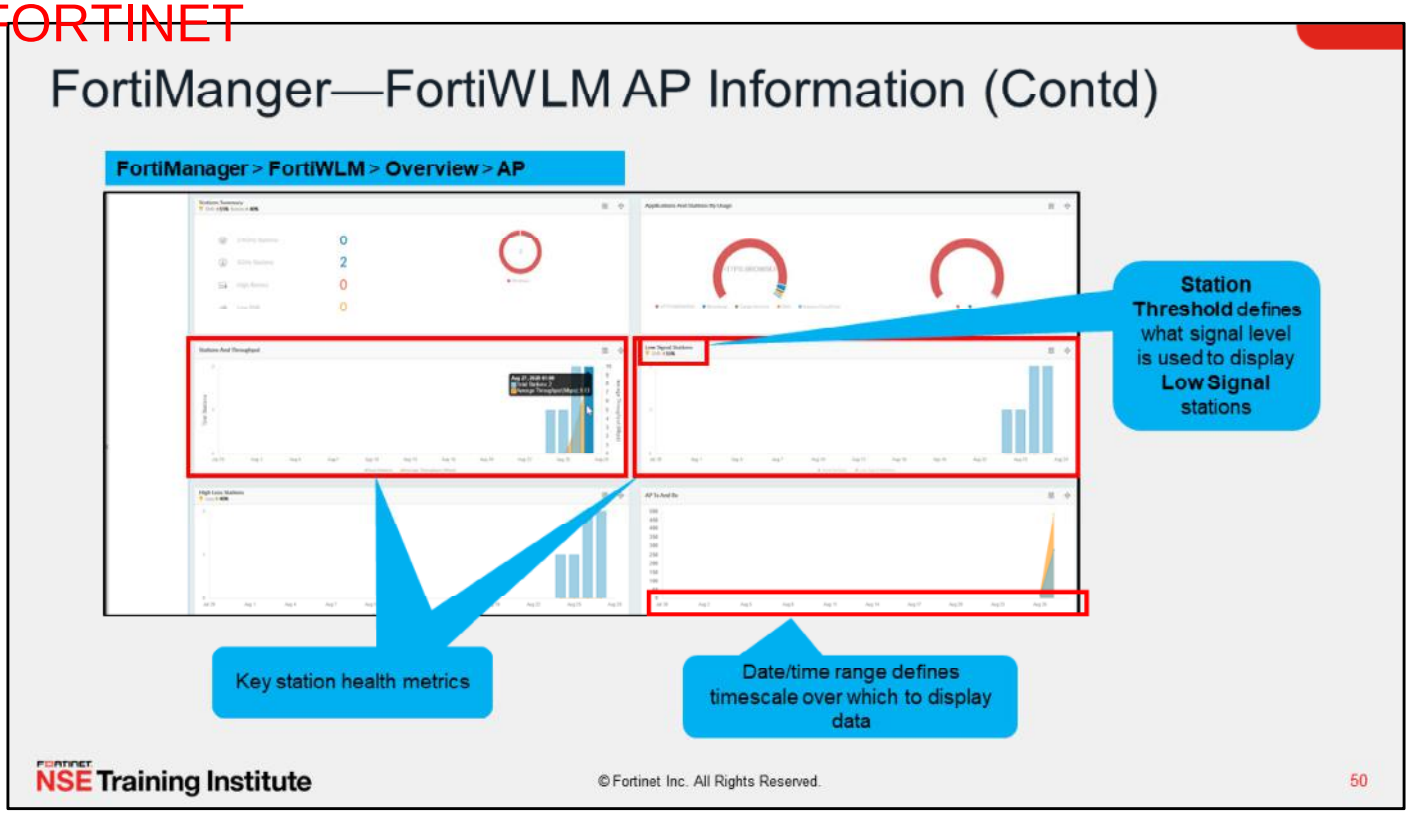
The AP option allows you to focus in on individual APs.

Use the **Filters** icon to select the AP and controller you want to view. You will see important information, such as noise level, average loss rate, average retries, and channel utilization. You can save and recall specific filter settings.

Alter the time period to see those metrics over an extended period of time. This is particularly useful when you are looking at the station loads and channel utilization, and can help identify APs on your network that are regularly overloaded. This dashboard is one of the few places you will see this information recorded and displayed over any length of time.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

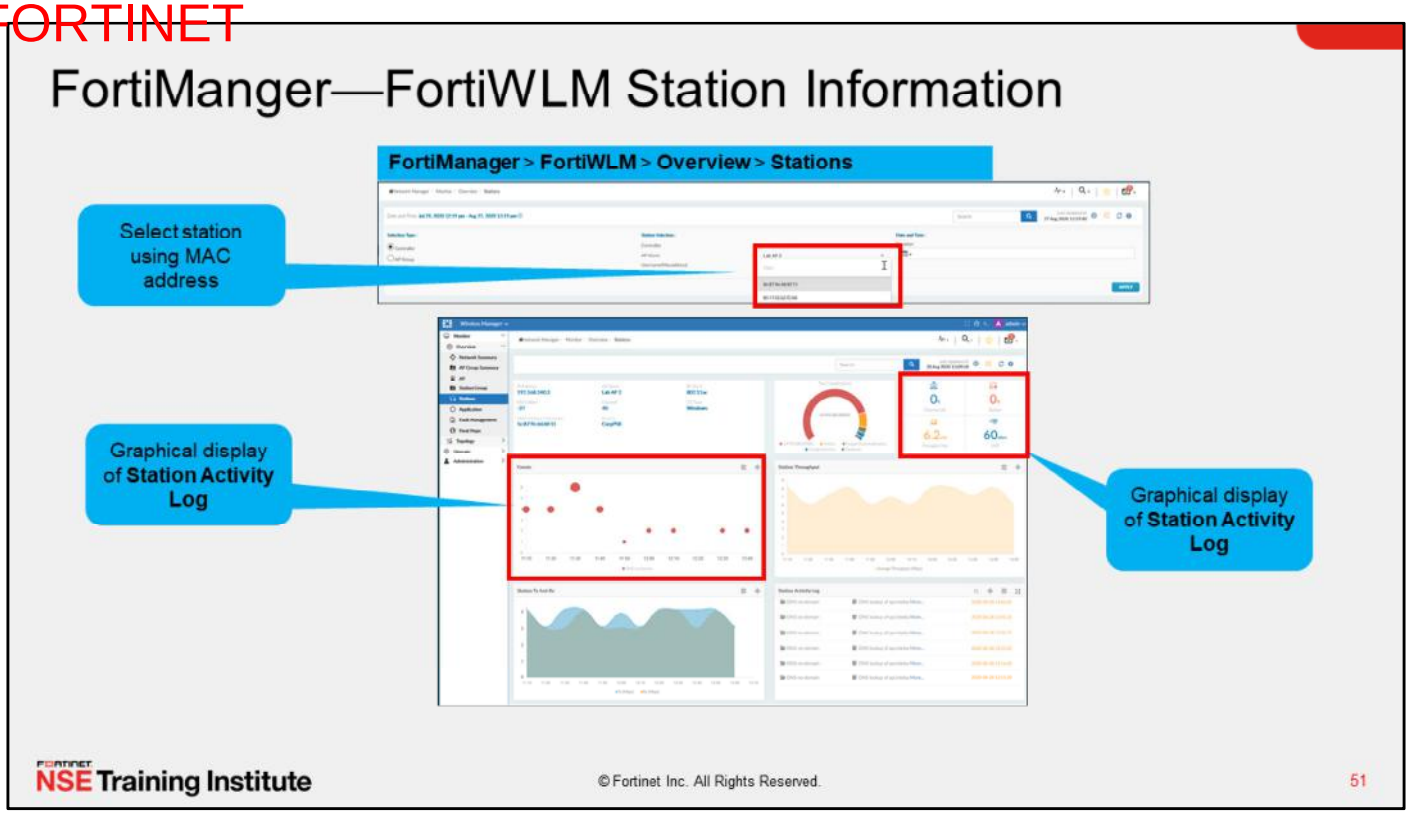


Of particular interest is the **Low Signal Stations** table. This table shows the number of stations that are connecting a low signal strength. This might indicate that you have APs in the wrong locations and would mean a poor experience for the end user.

The **AP Group Summary** works in the same way as this AP dashboard. The main difference is that you specify a group of APs to report on.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



To inspect an individual workstation, you have a choice as to how you select it. If you select **Monitor** > **Overview** > **Stations**, you must select the station's MAC address from the filter options. If you use the **Network Summary** and select the green station's panel, you'll get a full list of stations to choose from.

Again, after you select the station, you can see detailed information about each workstation. You will see an SnR listed together with the channel utilization and retries. This shows the health of our individual workstation's wireless connection.

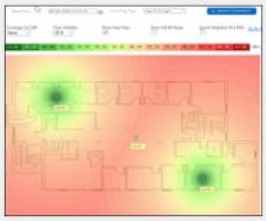
You also see two events-based tables. The **Station Activity Log** shows more events specific to that particular workstation, and **Events** shows the frequency of these events occurring over time. Large numbers of events occurring inside a particular time frame might indicate that the station is struggling with some element of connectivity. In other words, the more circles you have, the more issues there might be potentially. Like other views, it is possible to vary the time frame over which this data is displayed. This can be very useful when you are investigating historical issues, because you can review import historical metrics going.

Vouchers & Dumps are Available | WhatsApp +201224560923

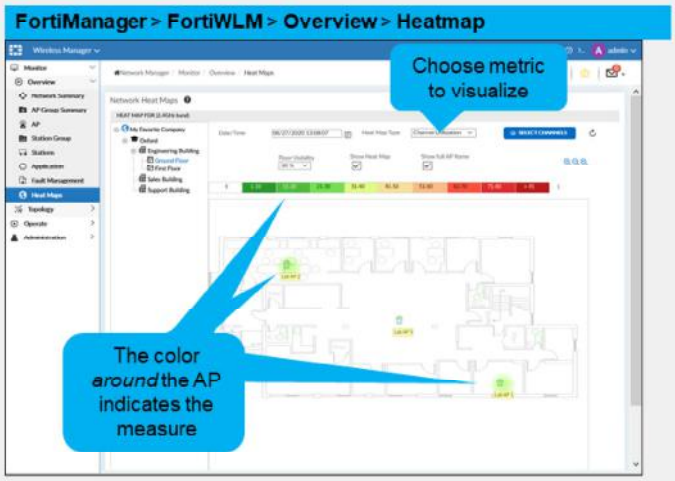
DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiManger—FortiWLM Heat Map

- Heatmaps graphically display measures in a geographical context
- They are *not* a heatmap in a traditional sense
  - The color simply indicates a status
  - This is the **Signal Strength** visualization:



  - Does not show *actual* signal strength across the floor
  - Simply a *basic* predication of signal strength in each location



NSE Training Institute © Fortinet Inc. All Rights Reserved. 52

On initial inspection, the heatmap function can be misleading. Many wireless professionals are familiar with predictive planning tools, such as FortiPlanner and Ekahau site survey. These tools allow the import of floor plans, the drawing of walls, and the prediction and display of signal strength based on complex algorithms. One of the measures that you can visualize using the FortiWLM heatmap, is signal strength. The FortiWLM heatmap will display the estimated receive signal strength of the associated workstations, and then plot it onto the floor plan. However, this is not a measure of the actual signal strength in different places on the floor. It is simply a color-coded estimate. The FortiWLM heatmap cannot perform any of the complex predictive signal planning that accounts for signal absorption by walls. It performs a basic calculation of radio power and distance, based on the floor plan's scale and size. It is possible to visualize the following heatmap types:

Number of Stations: This shows the relative number of stations across all the APs on the floor, which is very useful for identifying overloaded APs.

Channel Utilization: This shows the relative channel utilization across the APs on the floor, which is very useful for identifying overloaded APs, or potential channel conflict issues.

Loss: This is a visual indication of the loss rate for each of the APs.

Throughput: This is a visual indication of the throughput and at each AP, which is very useful for identifying areas of the network that are overloaded.

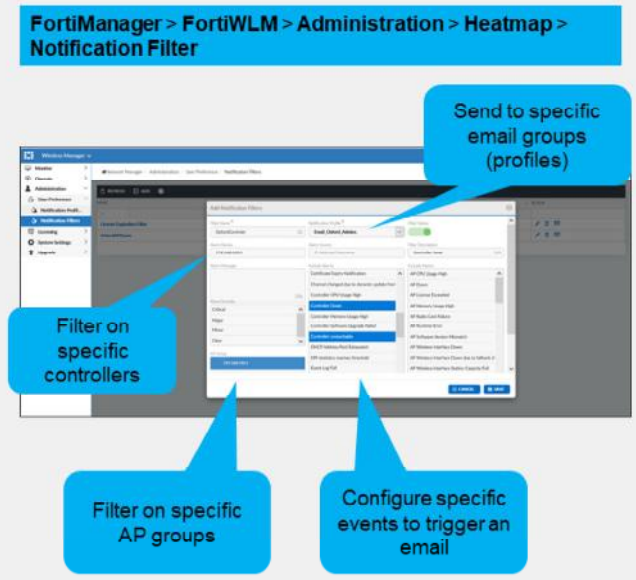
The benefit of heatmaps is realized when you import all of your building's floorplans. You can quickly review large numbers of APs by browsing each floor and looking for red colors. It makes the identification of problem areas quick and easy.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

FortiManger—FortiWLM Notifications

- Provides proactive notification using configured email server
- Create **Notification Profiles** to define groups of users
- Create **Notification Filters** to define what event emails are sent
- Filter on controller and AP group basis
- Filter on event type
- For example:
  - If an AP fails on the Oxford Campus, send an email to the Oxford technicians group
  - If a controller fails, send and email to the global admin group



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

53

FortiWLM can also send notifications. These notifications are entirely self-contained and unique to FortiWLM and require access to an email server.

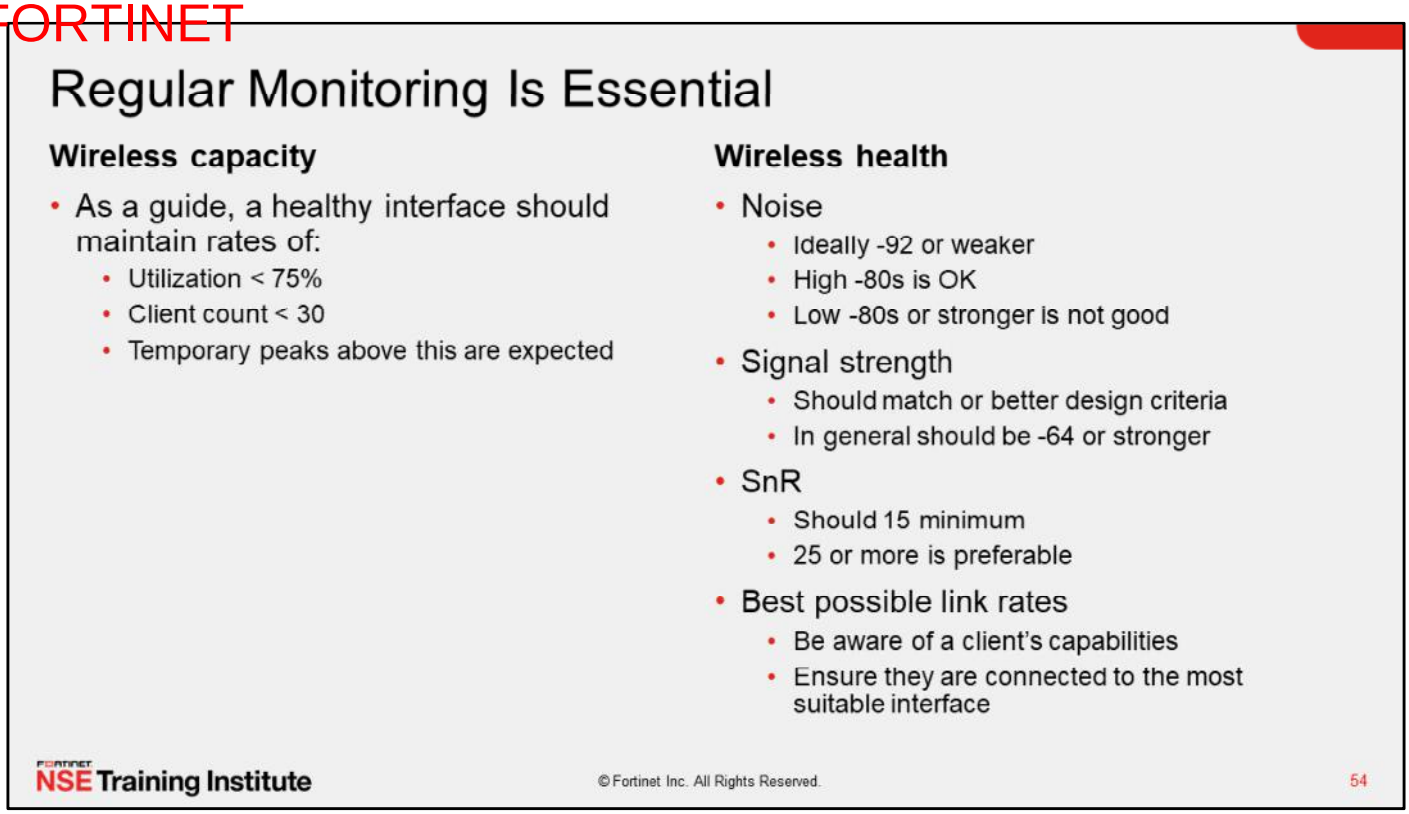
There are two elements to notifications. The Notification Profile is effectively an email group, a comma-separated list of the email addresses. These profiles define groups of users, usually with different responsibilities inside the network. The Notification Filter will define the events that trigger the email sent.

The notification filter is highly flexible. It is possible to send a notification based on alarm severity, or you can drill down and select individual alarms. It is possible to specify individual controllers, APs, or groups of APs.

When you have enterprise networks with large numbers of network administrators responsible for different campuses, it is possible to send relevant emails to the administrators who are managing the other parts of the system.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Finally, the key to using monitoring tools properly is understanding what a good and bad metrics are. You can then use the tools to identify parts of the network that are in trouble. Regular monitoring is essential, and you should aim to keep your wireless metrics within the ranges shown on this slide.

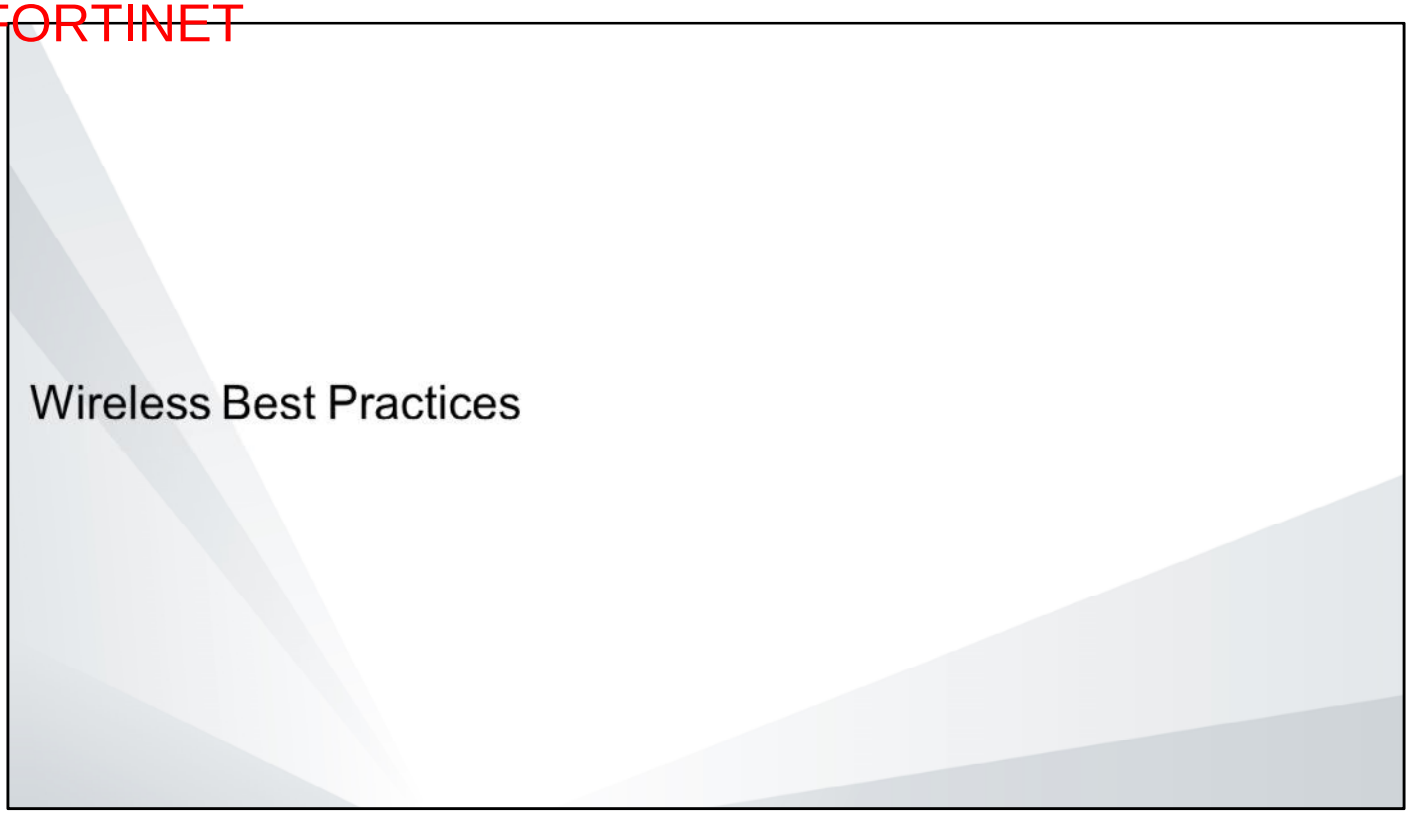
The lower the channel noise, the better. Signal strength is measured in negative decibels—the greater the negative number, the weaker the signal. For noise, a signal weaker than -92 is considered optimal. A signal in the high -80s is acceptable. A signal in the low -80s or -70s indicates significant interference that you should investigate using a spectrum analyzer.

The wireless network is designed and specified with a target signal strength for clients. You should make sure that the majority of your clients have that minimum signal strength or greater. It is not unusual to have a small number of weaker stations. For example, wireless devices enter and leave buildings, which can cause small numbers of low signal strength clients to appear and disappear. Generally, you should see signal strengths of -64 or stronger, with a good SnR of *at least 15*, but preferably 25 or more. Newer, higher speed standards generally require a higher signal strength *and* a greater SnR, but these numbers provide a good baseline and allow most wireless connections to work.

Finally, the ultimate indicator of health is the link rates that the client and AP use to communicate with each other. Before you can make a judgment on the link rate, you first need to understand the specifications of the wireless client to identify the maximum link rate you can use. Often, devices will be equipped with one or twop stream 2.4 GHz-capable and 5 GHz-capable clients. Analysis of the link rates being used may show that, rather than connecting near the theoretical maximums of 433 Mbps (for a one stream 802.11ac client) or 866 Mbps (for a two stream client), which you might expect, they are connecting closer to 65 Mbps. Often, this is simply a result of the clients connecting to the 2.4 GHz radio rather than a more suitable 5 GHz radio. Equally, link rates will be reduced if the underlying metrics (loss, retry, signal strength, and noise) are impacted.

Vouchers & Dumps are Available | WhatsApp +201224560923

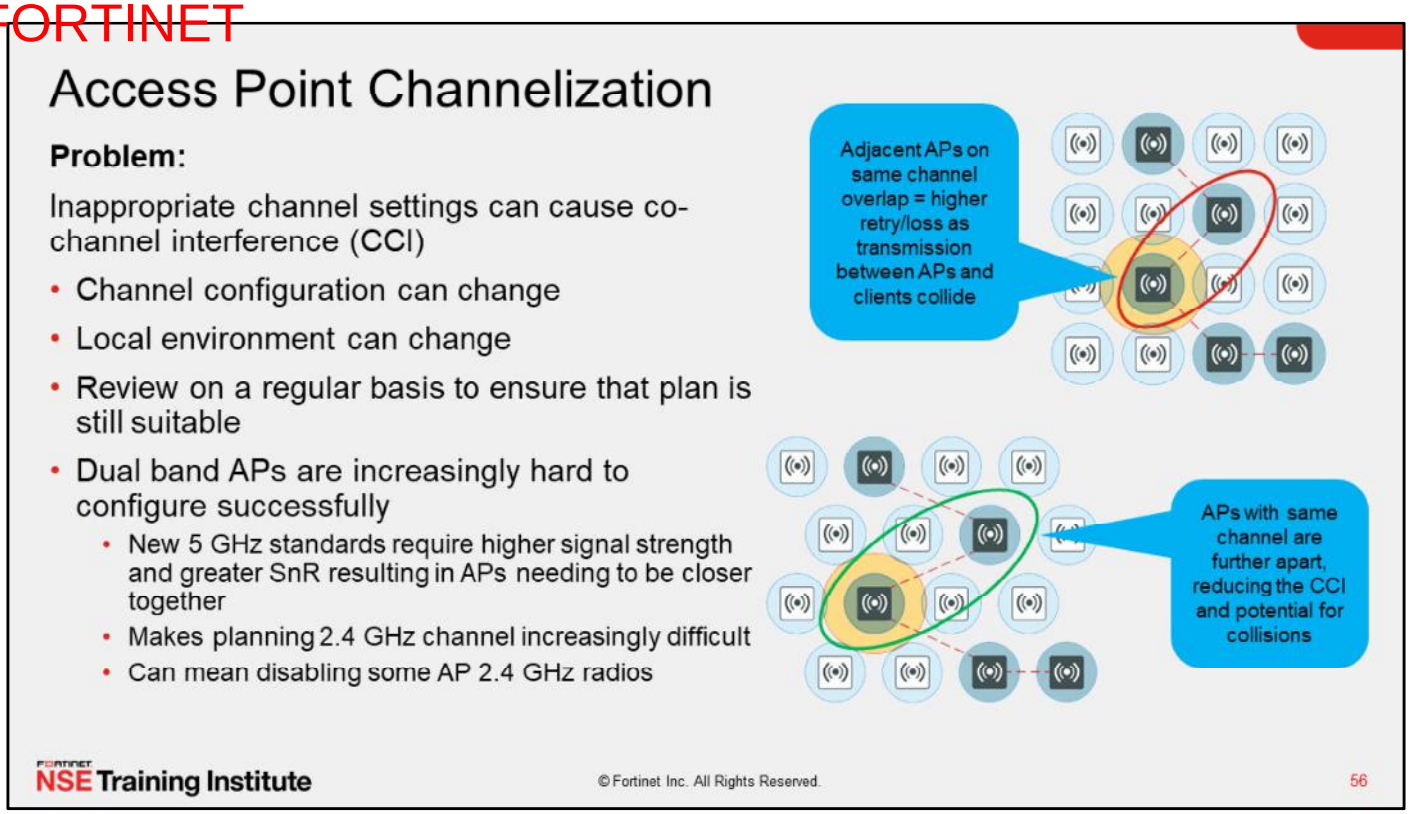
DO NOT REPRINT
© FORTINET
Brave-dumps.com



In this section, you will learn about some of the best practices that you can adopt when deploying a wireless network.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



A big source of issues with a wireless network can be incorrect channel settings.

Regardless of whether channels are set manually, or by an automated system such as Radio Resource Provisioning, it is possible to reach a scenario where AP radios have channel or power settings that cause CCI.

Automated systems can change channels to adapt to changes in local RF conditions, such as a new moving in and installing their own wireless network. This can cause your APs to attempt to recalculate their channel settings.

Or, in the case of 5 GHz dynamic frequency selection (DFS) channels, a radar signal is detected which can cause APs to change channels.

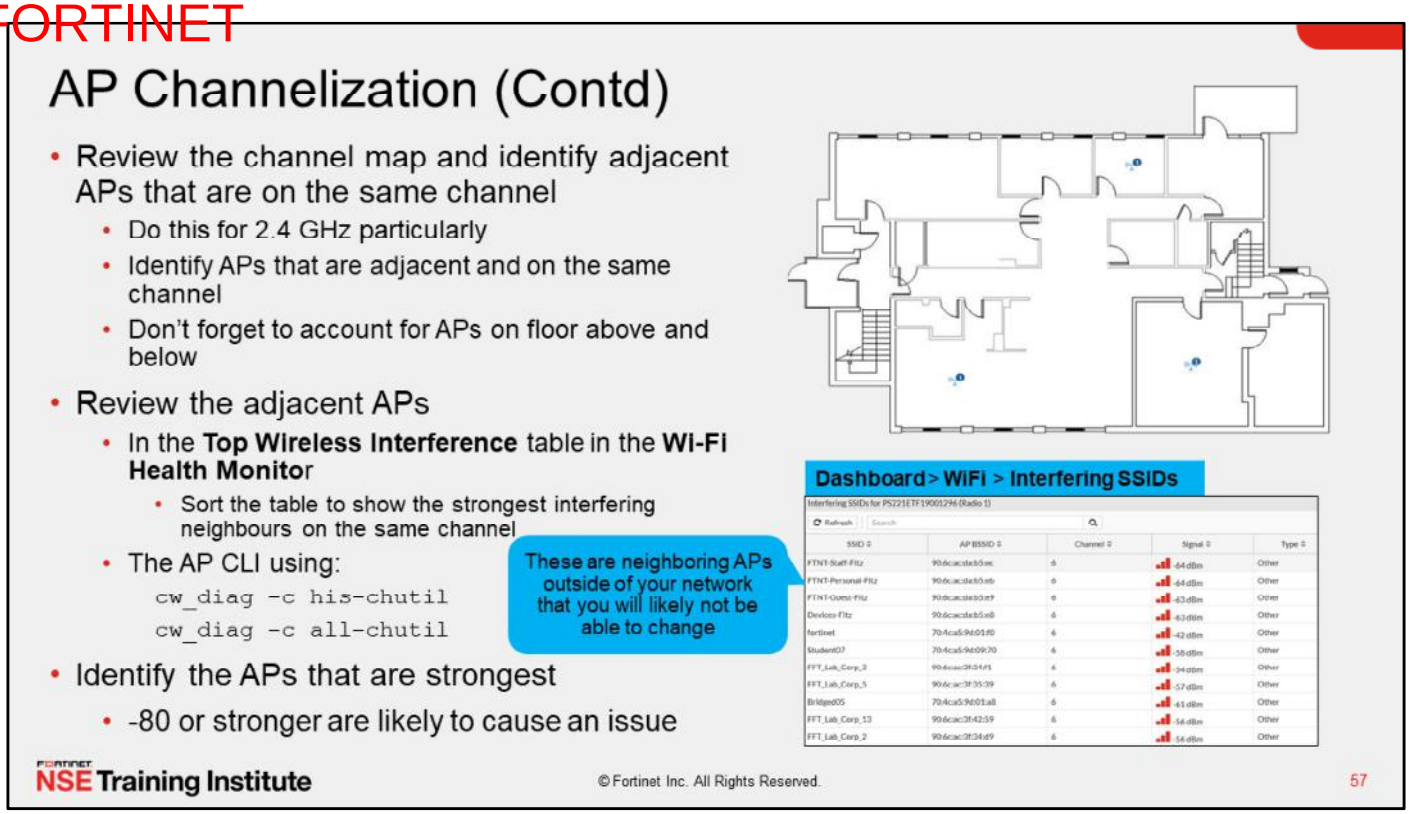
However it happens, APs that are close together should avoid being on the same channel. It is important to make sure that your AP population is configured in the best way possible, in accordance with conditions.

Note that it can be difficult in modern networks to balance the needs of 5 GHz clients with older 2.4 GHz clients. Newer 5 GHz standards can mean that APs need to be *much* close together to ensure the best performance. This can make 2.4 GHz clients very difficult to deploy from the same sets of APs, because 2.4 GHz signals tend to propagate farther.

This can be too difficult to accommodate by, for instance, turning down the transmission power. So, in many modern networks, it is now common practice to turn off select 2.4 GHz radios, or assign them to another task, such as dedicated rogue detection.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



When reviewing the AP channels, the Wi-Fi map is very useful. It allows you to view the channel settings for each AP, instantly seeing which AP interfaces could be interfering with each other. It is possible to view each frequency individually. You should pay particular attention to the 2.4 GHz interfaces, because these are the ones that usually experience issues.

The **Top Wireless Interference** table, when sorted, also shows the APs that are potentially interfering. You can sort to highlight the strongest interfering radios. Some of these radios may well be your own, in which case, you might be able to do something about them. However, it is also equally likely that there are radios from surrounding wireless networks that have a signal strength strong enough to cause a potential issue for you. You *may* have to consider changing *your* AP channels to avoid any highly used neighboring networks.

As a guideline, you should consider that radios in the same channel that are *stronger than -80* might cause issues.

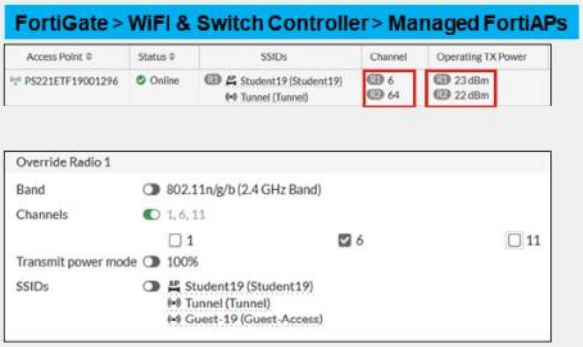
Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Access Point Channelization (Contd)

Solution:

- For own APs in your network:
  - Review the power settings for the interfering radios and, if required, reduce by overriding the radio
  - If already at a low setting (minimum of 10 dB), override the channel setting with a more suitable channel
  - If a more suitable channel cannot be selected, consider disabling the radio by adding the AP to a new profile with the interface disabled
- For APs outside your network:
  - Other third-party APs that are outside your control are difficult to deal with
  - Often the only solution is to configure your AP radio to avoid the interfering radio or accept the loss in performance



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

58

If you identify AP radios in your own network that are interfering with each other, then the first thing to do is review the power settings in use. By default, the automatic power management algorithm will automatically vary the power between 10 and 17 decibels. If the radio is already at the minimum 10 decibels, then it is inadvisable to reduce that further because it will begin to have a significant impact on any connected clients.

Rather than reduce the power any further, you should investigate setting the radio to another channel. In the 2.4 GHz range, this can be difficult because of the limited number of channels available (1,6,11).

Ultimately, if you cannot reduce the power or change the channel, one of the final things to consider is to disable the radio interface. This will allow other radio interfaces that were previously being interfered with to increase their power and provide service.

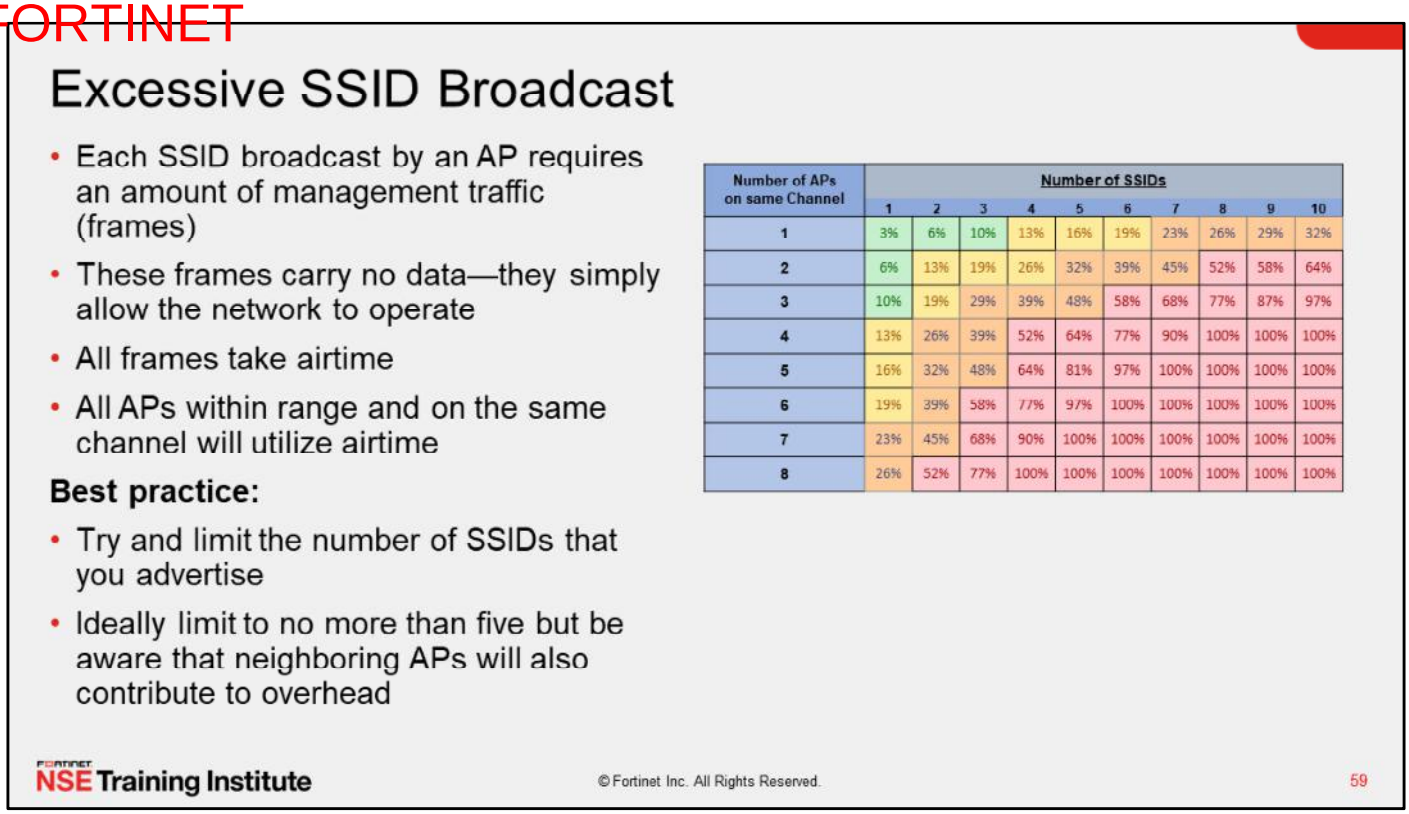
If you identify APs outside of the network, it is likely that they are outside of your control and, as such, it would be difficult to reduce their power or change the channel. As a result, the only potential option for your radios that are being interfered with is to change the channel to avoid CCI.

Note that the amount of CCI is very much dependent on the amount of wireless traffic being transmitted. If the neighboring network is small and under used, then the amount of disruption that it could potentially cause to your network may be acceptable.

To change individual radios, you can override them by configuring each AP in **Managed FortiAPs** or by overriding them in FortiManager.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



A key best practice that you should consider is the reduction or minimization of the number of wireless networks that your APs broadcast. This is applicable to all wireless network types and vendors.

The temptation is to broadcast many wireless networks to fulfil many purposes. However, each wireless network broadcast from an AP requires an amount of wireless management traffic. This traffic, or these management frames, carry no data and, as such, take up airtime or wireless capacity. By default, management frames also tend to be broadcast at low data rates. This means that not only could there be a lot of them, if many VAPS/SSIDs are being broadcast, but that they will use a substantial amount of airtime when being broadcast.

The table on this slide shows an *approximate* calculation of the amount of airtime used when the number of APs in a channel broadcast a number of SSIDs.

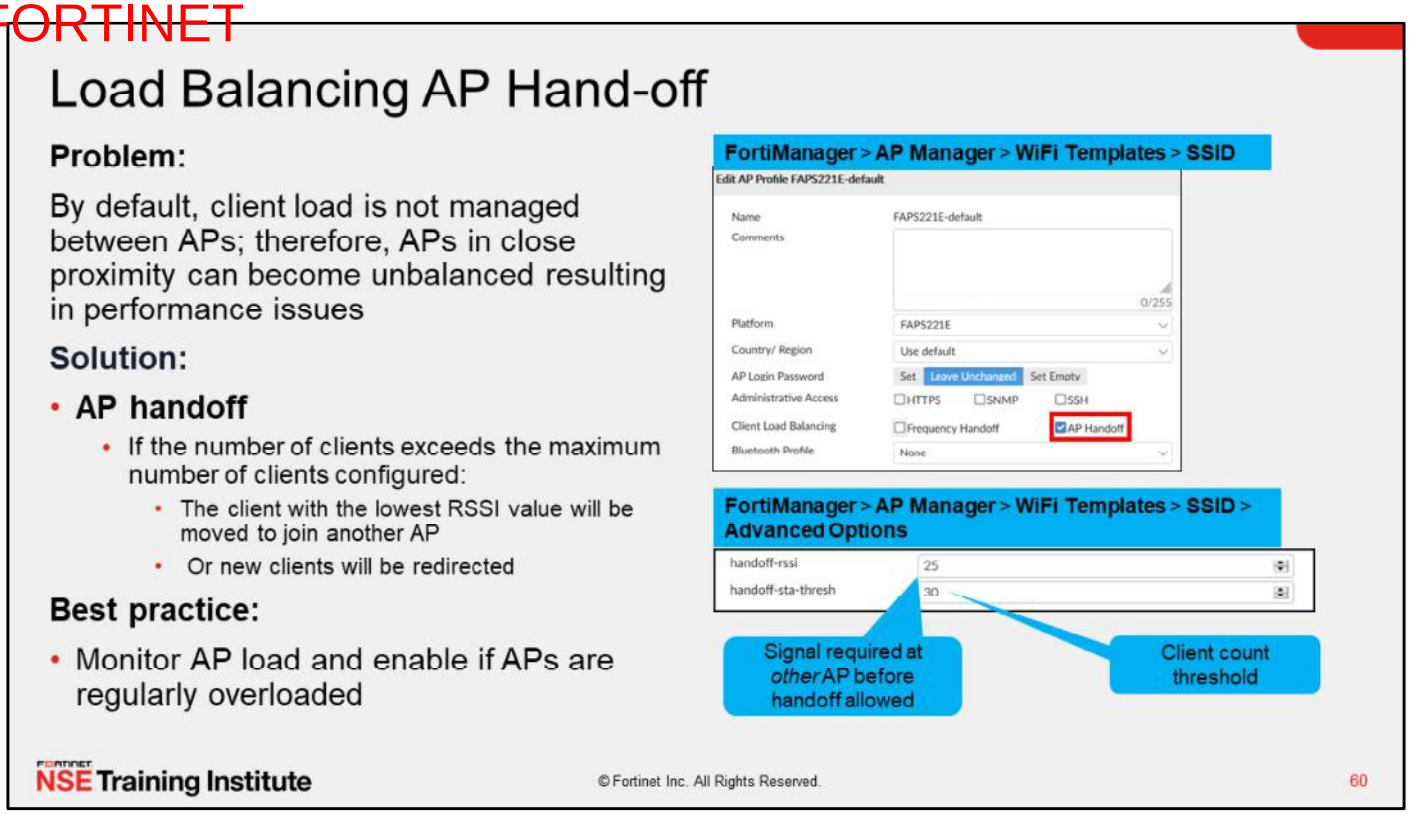
For example, if only one AP broadcasts ten networks or SSIDs, approximately 32% of the available airtime would be used sending and receiving management frames without actually exchanging any useful data. This calculation also assumes an ideal environment, with little or no interference. In the real world, it is likely that additional capacity could be lost to this as well.

Note that it makes no difference if it is your APs or a neighboring network's APs, the same overhead applies. Management frames take airtime wherever they come from.

To minimize the effects, it is a best practice to limit the number of broadcasting networks to five, but preferably fewer. Note that there are various mechanisms, such as dynamic VLANs, that you can use to help limit the need to have multiple wireless networks being broadcast.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



AP handoff is a load balancing method that is used by FortiGate to increase wireless performance and use the resources on APs more efficiently. AP handoff is a way of load balancing wireless clients among managed APs on FortiGate. AP handoff works in two ways:

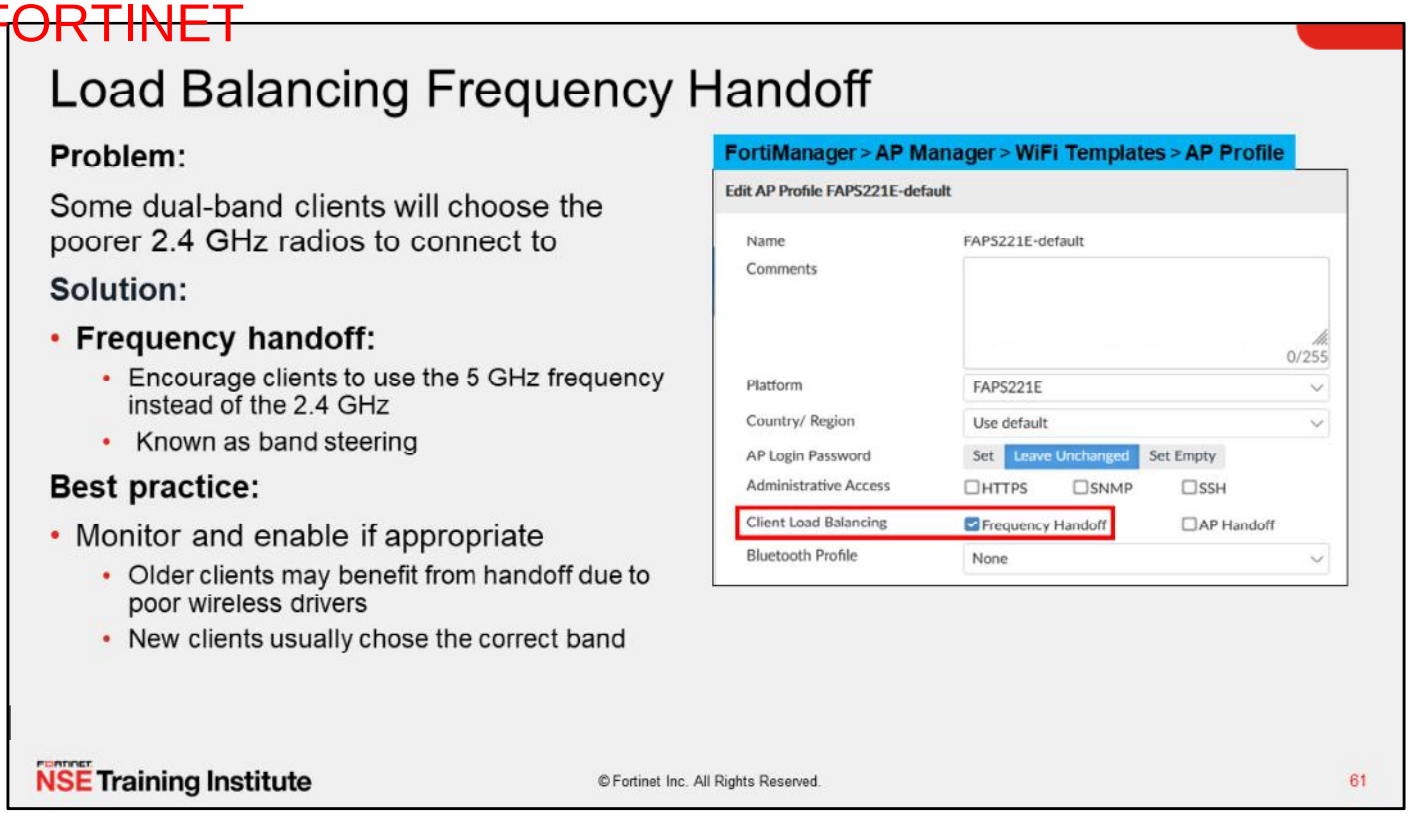
1. If the number of clients exceeds the maximum number of clients configured for an AP, the client with the lowest RSSI value will be forced to join another AP.
   - The RSSI value must meet the signal strength on the nearby AP.
2. If the number of clients is *already* at the defined threshold, new clients will be redirected to join the least busy nearby AP.
   - The least busy nearby AP will respond to the client's join request.

Handoff-sta-thresh defines the value after which the handoff protocol is initiated for new client. FortiGate will instruct the least busy nearby AP to respond to the join request for any new client that tried to connect to an overloaded AP, as long as the configured RSSI value condition is met. You must enable the AP handoff feature on all radios on an AP. The **handoff-rssi** value threshold defined in the AP profile is used when handed off client tries to connect to the second AP. The client`s signal strength must be equal to or more than the defined RSSI value on the AP. Signal strength is determined based on the RSSI value—a higher RSSI value means better signal strength.

The best practice is to monitor the client load across the APs. If you see a regular imbalance between APs relatively close together, enabling AP handoff can help balance the load between APs. It is typically a high-density environment that suffers imbalances because of the large numbers of clients and the necessary proximity of APs. Be aware that *some* clients, particularly low-cost and simple IoT type devices, do not respond well to being load balanced and refuse to be directed to another AP. This can cause a connectivity issue, and load balancing may need to be avoided for these types of clients.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET



Frequency handoff is a band steering technique that FortiGate uses to encourage clients to use the 5 GHz frequency instead of the 2.4 GHz.

Clients that support the 5 GHz frequency benefit from faster speeds and decreased interference. This also benefits clients that do not support 5 GHz, because there will be less interference on 2.4 GHz because of the reduced number of clients.

FortiGate continuously probes the clients to identify if they can operate on the 5 GHz frequency. FortiGate maintains a table to track which clients support both frequencies, and records the RSSI value, along with the other information for each frequency.

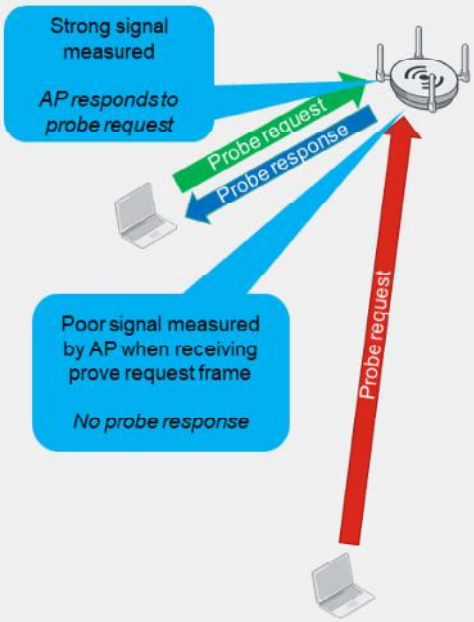
When a client tries to connect, FortiGate checks whether it can support 5 GHz and, if so, how good the signals are. If a client supports the 5 GHz frequency and the signal is strong enough to connect, FortiGate will ignore the client's requests to join the network on 2.4 GHz until the request times out. The client will then automatically try to join the same network using 5 GHz. FortiGate will instruct the AP to respond to the join request and allow the client to connect.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Probe Response Threshold

- The AP will respond to probe requests from clients that have a receive signal strength above a certain level
  - Known as the probe response threshold
  - AP measures the signal strength of client probing
- The default allows for a wide range of clients to connect
  - Can result in distant clients connecting inappropriately
  - Can result in excessive airtime usage because of low link rates



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

62

Signal strength is one of the major factors in wireless performance. Clients with poor signal strength to and from the AP will likely have poor performance. They will also cause poor performance for other clients connected to the same AP because of the excessive amount of airtime they will take to transmit and receive their data.

The wireless client is in control of the AP selection process in a Fortinet integrated and cloud network. Because of the quirks of RF, and the possible poor quality of the wireless client hardware or drivers, it is possible for wireless clients to make poor decisions when connecting to APs. A client may choose to connect to an AP farther away when there may be a closer, more suitable AP to connect to, for example. This results in a connection that has poor signal strength and poor link rates, resulting in performance issues. The AP/controller does have limited control in how a client connects. Part of the client's connection process involves a probe request and a probe response process that occurs during the initial association. This can give the AP the opportunity to not respond to a probe request from a client that is too far away. If the client does not get a probe response from an AP, it should carry on looking for other suitable APs to connect to. The AP can measure the signal strength of the client's probe request. If it decides the signal is too weak, then it can choose to not respond with a probe response frame. The signal strength the AP uses is defined by the probe response threshold and is measured in dBm.

The probe response threshold applies only when the client is attempting to connect to an AP. If the client is already connected and starts moving away from the AP, resulting in the signal strength dropping below the threshold, then it will *not* be forcibly disconnected by the AP/controller. However, if the connection drops for any other reason, the client will need to probe to reconnect. At that point, the client will be below the threshold and will not get a probe response.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Probe Response Threshold (Contd)

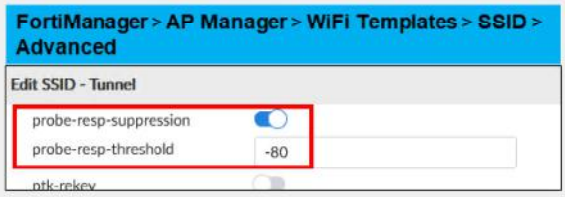
- Threshold is configurable
  - On a per-VAP/SSID basis
  - CLI only at the FortiGate or via SSID profile using FortiManager
  - Configurable from -20 to -95 with default value of -80.

Best practice:

- Monitor poorly or inappropriately connected clients
  - The Wi-Fi Client monitor displays all connected clients and is sortable/filterable by signal strength
- If high numbers of low signal strength clients are connecting
  - Investigate their physical location—are they supposed to have wireless access there?
  - If clients are connecting to an AP that is too far away, consider decreasing the threshold by 5 dB

```
config wireless-controller vap
edit <vap_name>
set probe-resp-suppression enable
set probe-resp-threshold
<level_int>
end
```

Setting –70 will require clients to be have a detected signal strength of -70 or stronger before the AP will respond to a probe



NSE Training Institute © Fortinet Inc. All Rights Reserved. 63

The probe response threshold is applicable to the VAP/SSID. You can configure it only on the CLI. By default, the threshold is -80 dBm. This requires that any probe request frame that comes *to* any of the wireless radios that are broadcasting the SSID should be measured at -80 or stronger, before the AP will respond. -80 allows for clients with a relatively weak signal strength to make the connection. While this may be acceptable for some networks, performance in high-density networks could suffer substantially if these slow clients are allowed to connect and exchange small amounts of data across low-speed links, using large amounts of airtime. Most wireless networks should be designed with a target signal strength in mind for their clients, which is usually around -64. It is a good practice to monitor clients that are connecting to the network, and monitor the signal strength. If you have large numbers of clients that are connecting with poor signal strength, it could indicate the following:

- Clients are trying to connect from an area that does not have wireless coverage. In this case, you will need to investigate whether additional coverage is required. Perhaps a new part the building has opened and now requires wireless service. In this case, you would need to consider deploying more APs.
- Clients are connecting to a suboptimal AP. Variations in radio frequency caused by multipath and reflections can make an AP *look* more attractive to the client than they should. Wireless client quality can also be a big factor in AP selection. Poorly designed, engineered, or tested drivers can make poor AP radio selection decisions in an enterprise environment.

If you find that large numbers of clients are connecting at poor signal strength without any other obvious issues, you can reduce the probe response threshold for the VAP/SSID. Reduce it in increments, and monitor the effect. Always remember that decibels are logarithmic. Small changes in decibel count can mean quite large changes in signal strength, so choose an increment of around 5 dB. After you change the probe response threshold, spend more time monitoring the client connections, and reduce the threshold, if required.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Multicast to Unicast Conversion

- Multicast data is sent at a lower data rates in Wi-Fi
  - This occupies considerable air time
- Multicast to unicast causes stream to be sent to each client at high data rate
  - It therefore reduces air time usage
- Configurable on a per SSID/VAP basis
- Configurable from CLI only at FortiGate or centrally using a FortiManager profile

Best practice:

- Enable by default

```
config wireless-controller vap
edit <vap_name>
set multicast-enhance enable
end
```

FortiManager > AP Manager > WiFi Templates > SSID > Advanced



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

64

By default, multicast traffic is sent at a lower wireless transmission rate. If a lot of multicast traffic is being passed by the network, then this can needlessly consume airtime.

Converting multicast traffic to unicast traffic might well increase the amount of traffic sent because each multicast message will be converted to a unicast message for *each* wireless client connected to the wireless SSID. However, because the unicast traffic is transmitted at a much higher wireless data rate, the net effect on wireless performance is positive because each frame will be consuming much less airtime.

The effect on the network will obviously be dependent on the amount of multicast traffic that is generated on your network; however, enabling conversion by default will likely have little negative effect.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Disable 802.11b Rates

- All wireless standards attempt to be backwards compatible
  - Original 802.11b protocol still supported on 2.4 GHz radios
  - Management frames at lowest link rate, consuming maximum airtime
- Disabling increases airtime, but:
  - Removes support for older clients
  - Reduces the effective range of the AP

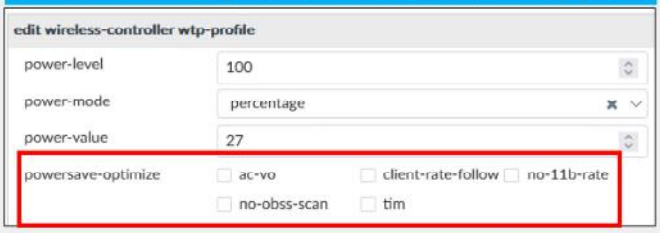
Best practice:

- Consider enabling in high-density environments where:
  - Support for legacy 802.11b clients is not required
  - AP density is high enough to support good connectivity in areas requiring coverage

Enabled on an AP profile basis and only required to be set on the 2.4 GHz radio:

```
config wireless-controller wtp-profile
edit <name_string>
config radio-1
set powersave-optimize no-11b-rate
end
```

FortiManager > Device Manager > Device & Groups > Managed FortiGate > CLI Configurations > wireless-controller > wtp-profile



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

65

All wireless standards are designed to be backwards compatible. This means that even the newest wireless standards have to accommodate the wireless connection that was originally specified as part of a standard that is a more than 20 years old.

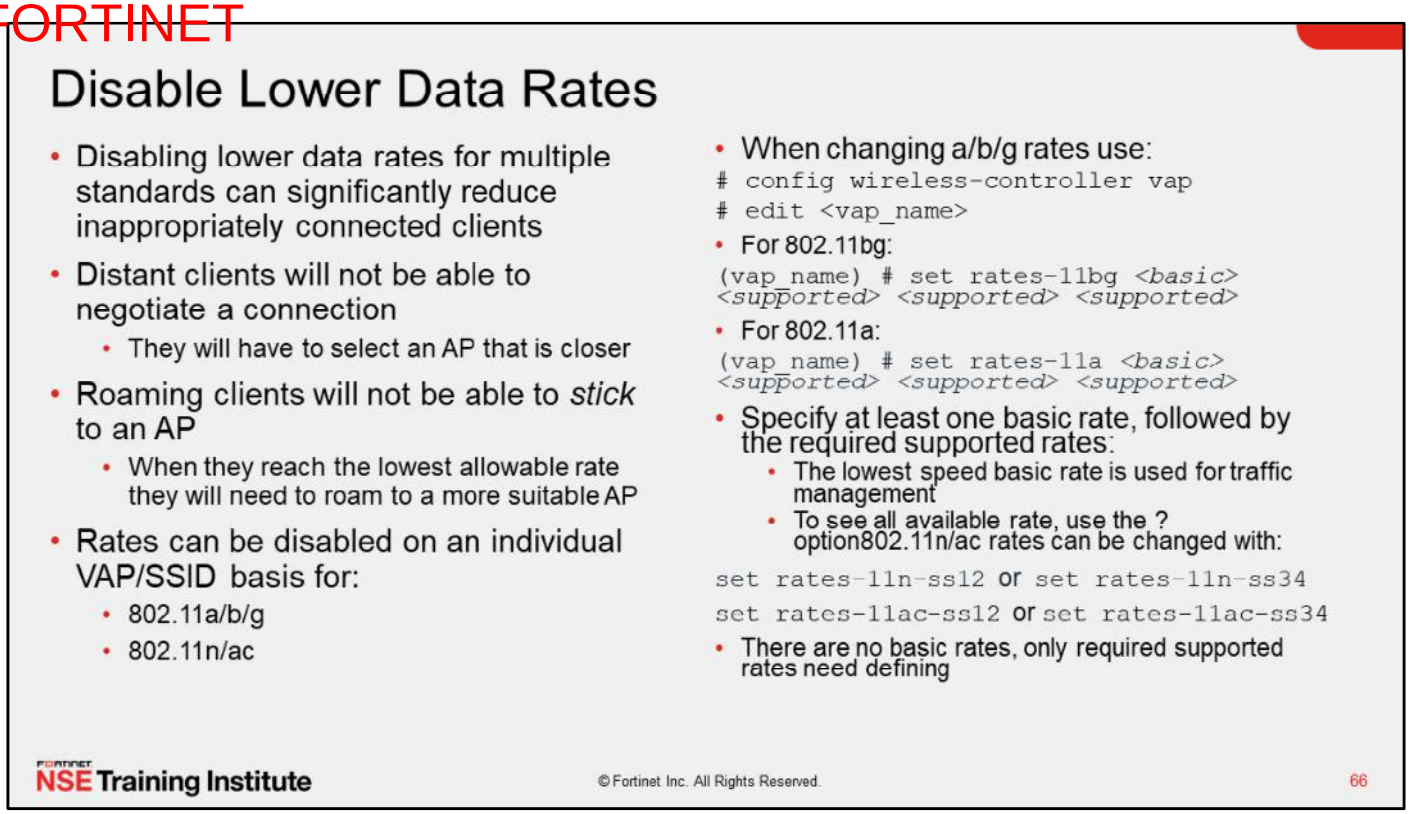
The original 802.11b standards mandated that management frames should be sent out at the lowest MCS connection rate, which, for 802.11b, was 1 Mbps. This means that modern networks have to also transmit management frames at this low MCS rate, even when the vast majority of, or perhaps all, clients support newer standards. This results in large amounts of wasted airtime.

Disabling 802.11b rates means that the management frames are now transmitted at a minimum of 6 Mbps, improving airtime efficiency. This comes at the cost of no longer supporting extremely old 802.11b clients, and removing those legacy rates from the network. This also has the side effect of preventing clients from connecting from an extreme range. Even the latest wireless clients will revert to the old 802.11b rates when trying to connect to an AP that is far away. Prohibiting these rates also stops excessive airtime use by clients that are too far away to make the best use of the wireless network.

If you choose to disable these rates, you should be aware that clients will no longer be able to connect, and the receive range of your APs will also be less. However, if your network is designed correctly, clients that require wireless coverage will have signal strength high enough to allow a good connection. So, it should not be necessary for your clients to revert to the legacy rates.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



It is also possible to support data rates in a more granular way. If required, it is possible to customize the individual rates for each SSID/VAP broadcast. For example, you can configure a corporate SSID/VAP that is used to support known client types can to support only higher data rates in both the 2.4 and 5 GHz frequency ranges. Because the client specification is known, it should be easy to select appropriate data rates to optimize wireless performance. A guest SSID/VAP may have a wide variety of different wireless clients connecting to it, therefore it may be better to leave the SSID supporting the default data rates.

Adjusting the data rates appropriately will prevent clients from *sticking* to an AP after the initial association; that is, when the client roams, the updated link rates will ensure that the client moves to a more suitable AP more quickly because of the increase in supported rates. It will also provide a significant barrier to clients that are connecting with poor signal strength during the association process. It will not be possible for clients with poor signal strength to meet the requirements for associating with APs that have a higher basic link rate requirement.

Rates are configurable on the CLI only, and on a per-VAP basis. It is possible to configure rates separately for 2.4 GHz 802.11bg, and 8021.11n. For 5 GHz it is possible to configure separately for 802/11a, 802.11n, and 802.11ac.

When specifying a/b/g rates, you must set at least one basic rate. The lowest basic rate that is advertised by an AP is the rate at which management traffic is broadcast. Once the basic rates have been defined, then you can also define the optional, or supported rates, the clients can use if they meet the signal strength requirements.

When configuring 802.11n and 802.11ac rates, you need to specify only the required supported rates.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT Brave-dumps.com
© FORTINET

Disable Lower Data Rates (Contd)

Best practice:

- Configurable using the CLI for FortiGate or deployable using FortiManager
- Leave 802.11n/ac rates set to default
- If sticky clients and channel utilization are a problem:
  - Disable lower rates in 802.11bg
    - Set the basic rate to be 6 Mbps or above
    - Allow rates above 6 Mbps as optional
  - Disable lower rates in 802.11a
    - Set the basic rate to 18 Mbps
    - Allow rates above as optional
- Repeat monitoring

```
# config wireless-controller vap
# edit <vap>
```

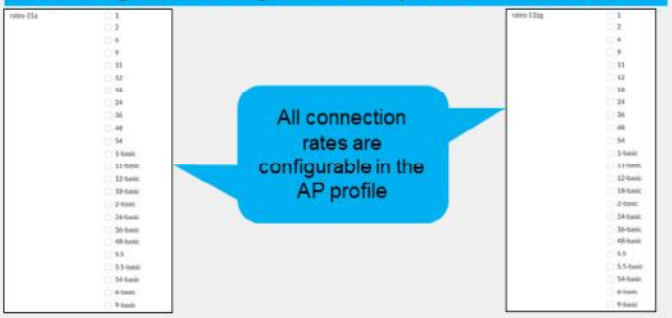
Set the 802.11bg rates

```
# set rates-11bg 6-basic 9 12 18 24 36 48 54
```

Set the 802.11a rates

```
# set rates-11a 18-basic 24 36 48 54
# end
```

FortiManager > AP Manager > WiFi Templates > SSID > Advanced



NSE Training Institute

© Fortinet Inc. All Rights Reserved.

67

While it is possible to alter the supported rates for 802.11n and 802.11ac, there is currently no best practice that suggests it is necessary to do so.

When using the legacy wireless standards in a congested or high-density environment, you can improve airtime efficiency by eliminating the low-rate connections. Allowing low rate connections also creates the possibility of clients *sticking*, or connecting inappropriately to APs.

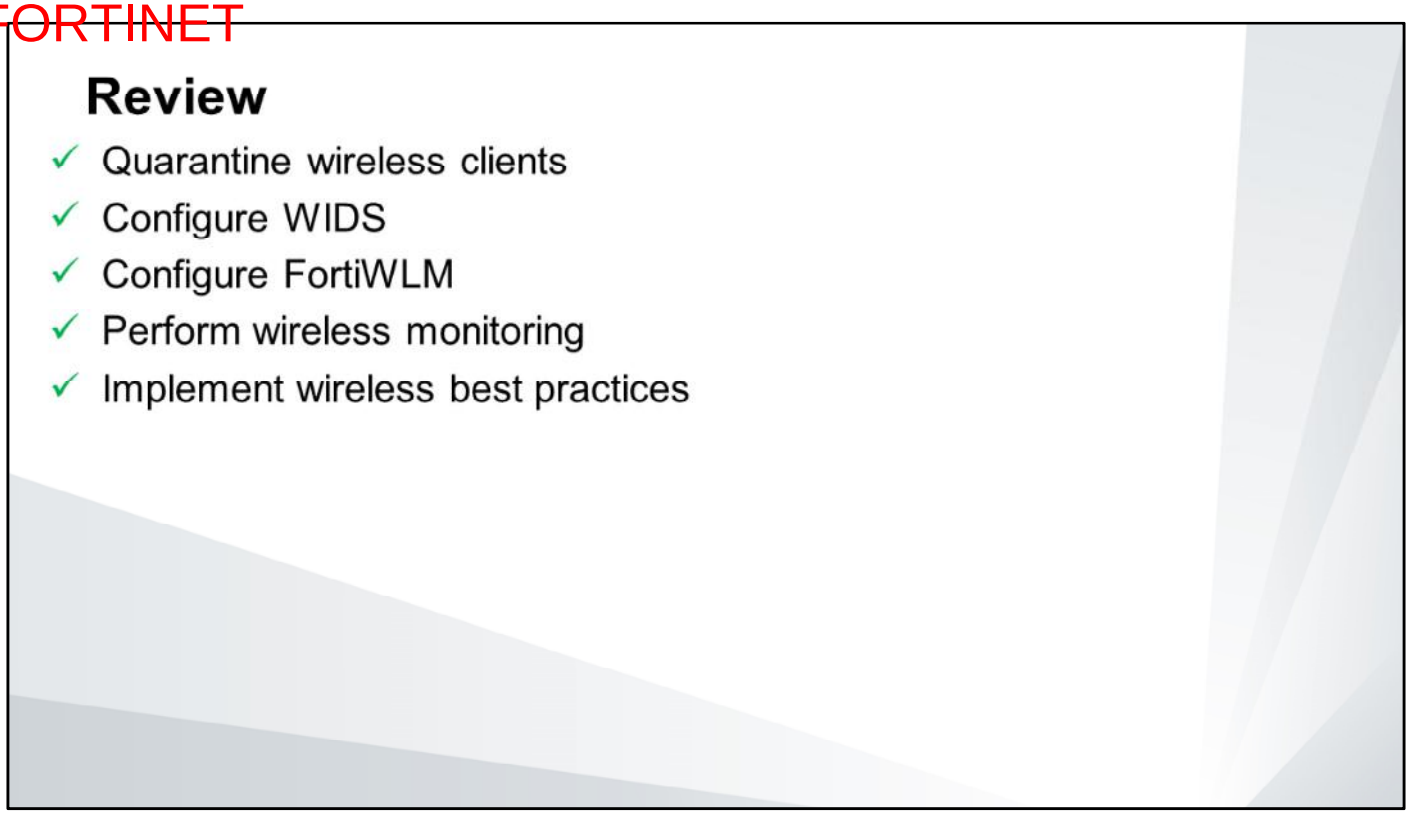
You can change the supported rates on the CLI only, on a per-VAP/SSID basis. This allows for different wireless networks to be broadcast from the same AP, but with different supported rates.

Disabling rates will restore the default settings on the VAP. To revert to default rates using the CLI, use the following commands:

```
# config wireless-controller vap
# edit <vap>
# unset rates-11bg
# unset rates-11a
# end
```


Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

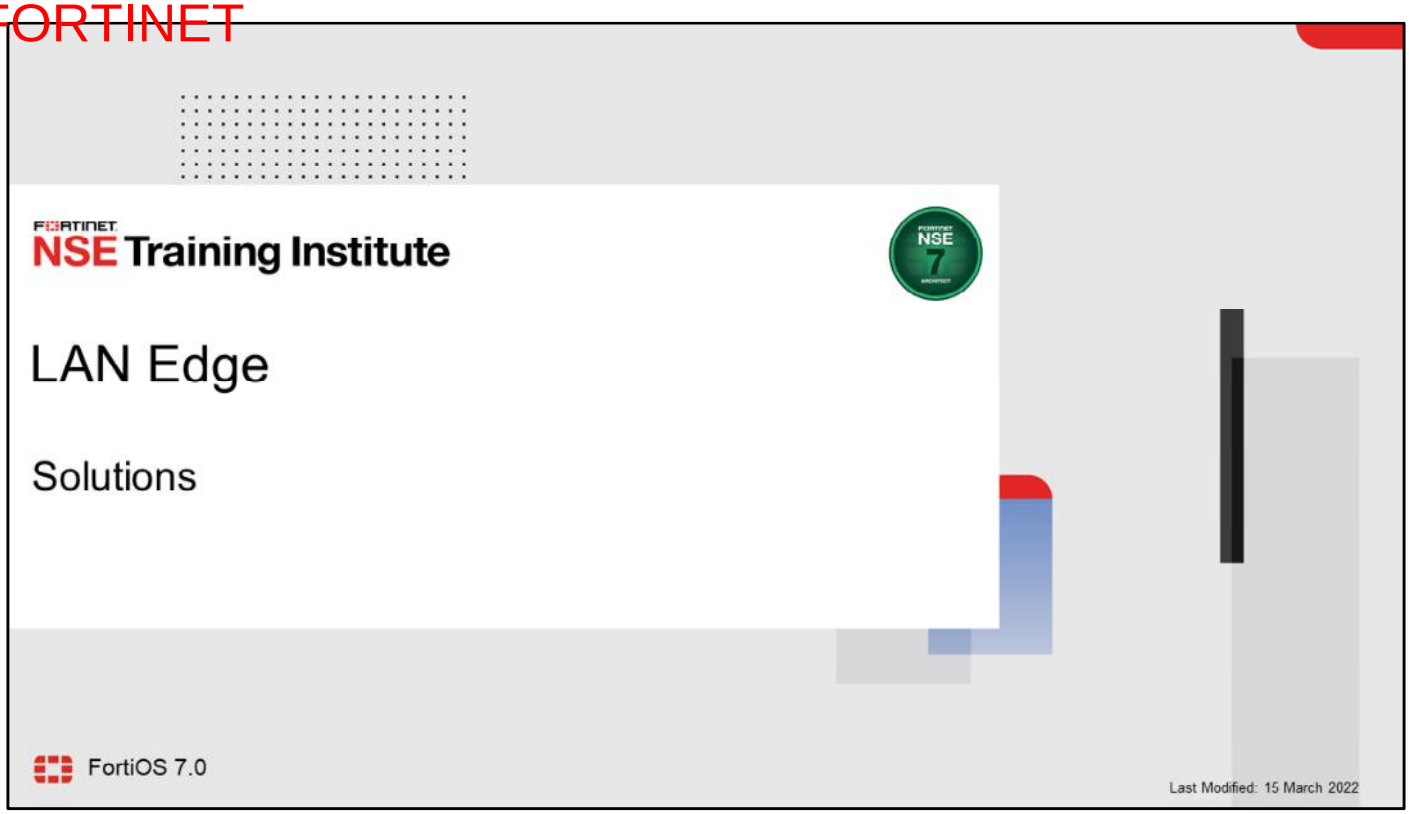


This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to secure, troubleshoot, and apply best practices for integrated wireless features in FortiOS.

Vouchers & Dumps are Available | WhatsApp +201224560923

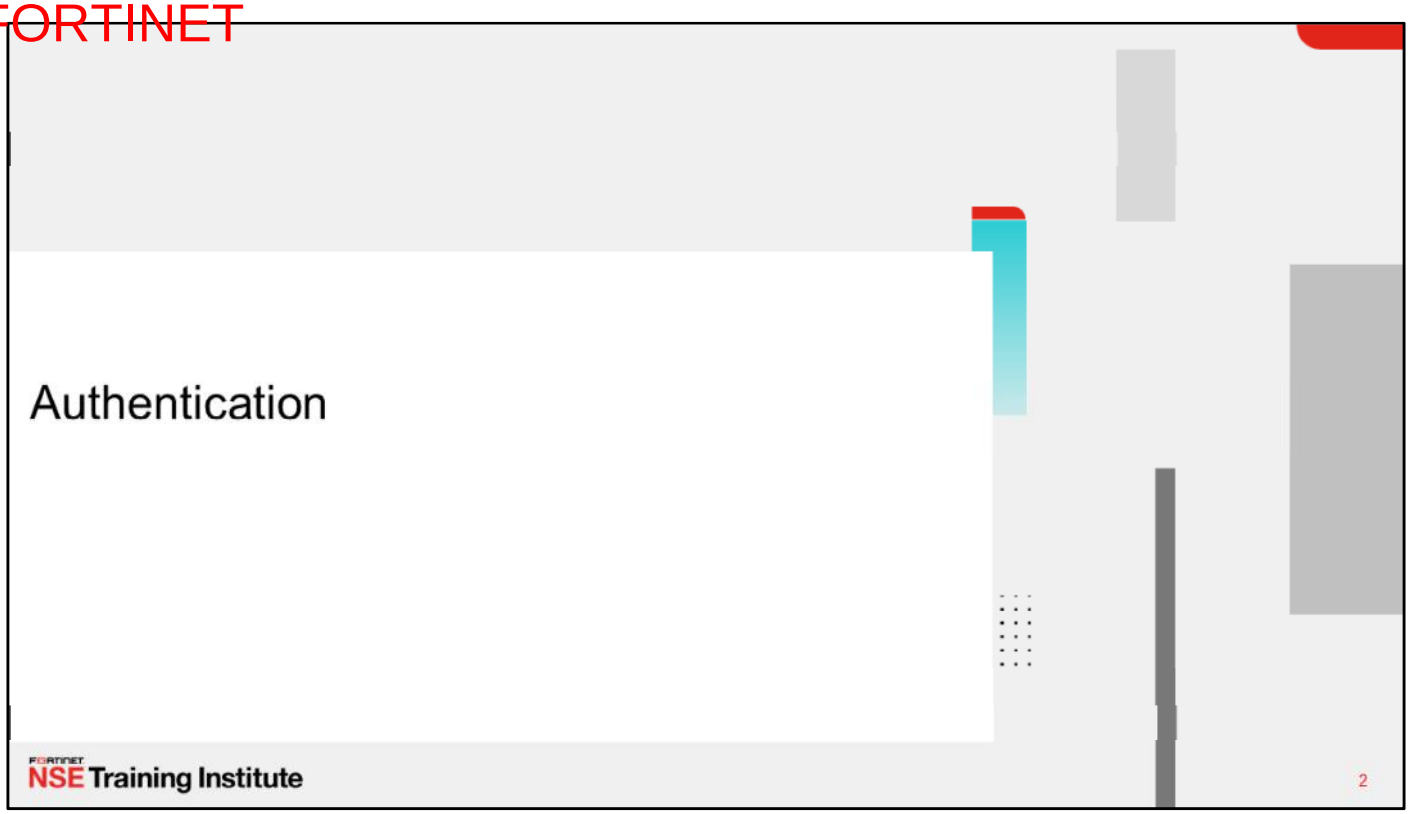
DO NOT REPRINT
© FORTINET
Brave-dumps.com



This lesson provides problem descriptions and solutions for the Secure Access troubleshooting labs.

Vouchers & Dumps are Available | WhatsApp +201224560923

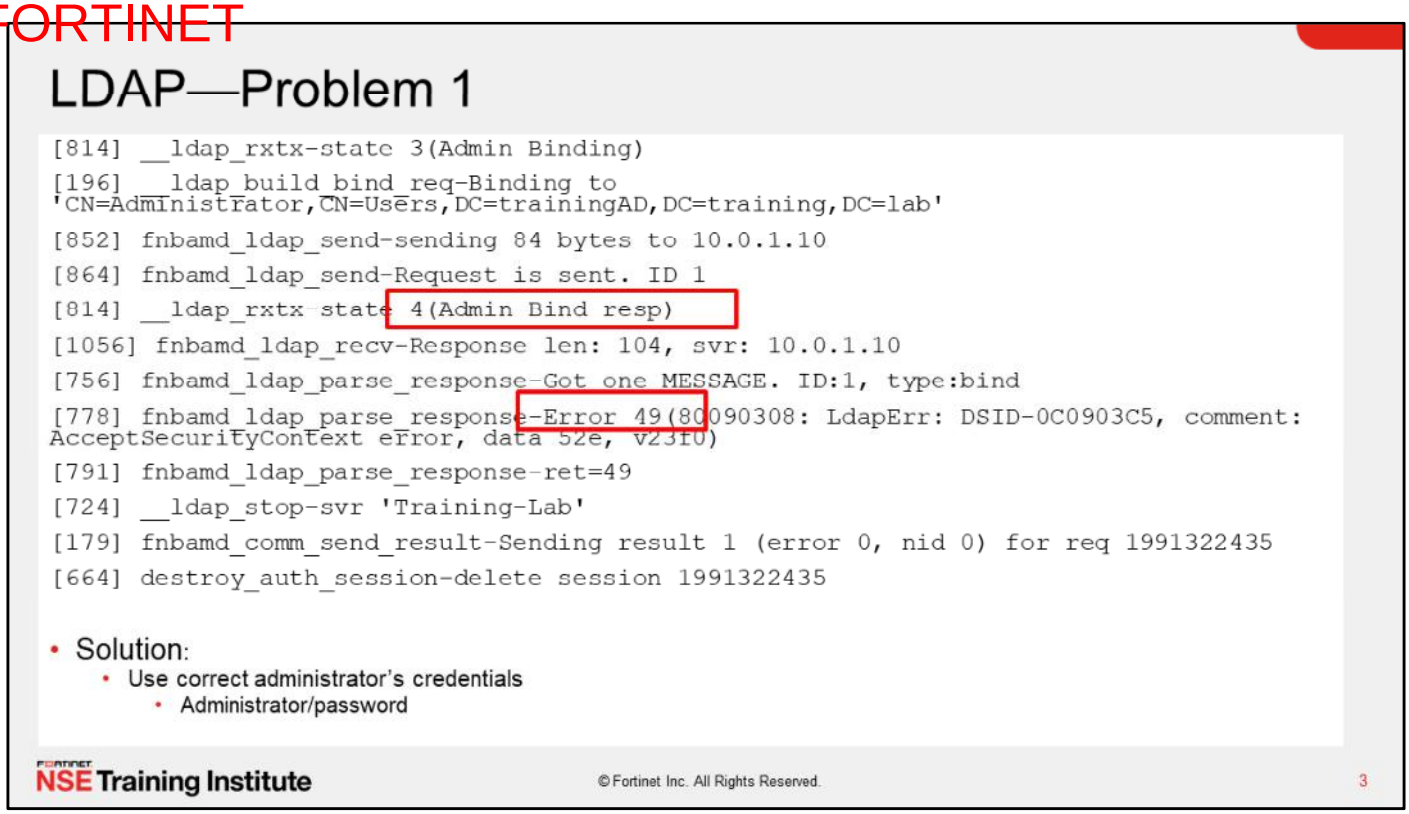
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Now, you will review Lab 1 problems and solutions.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



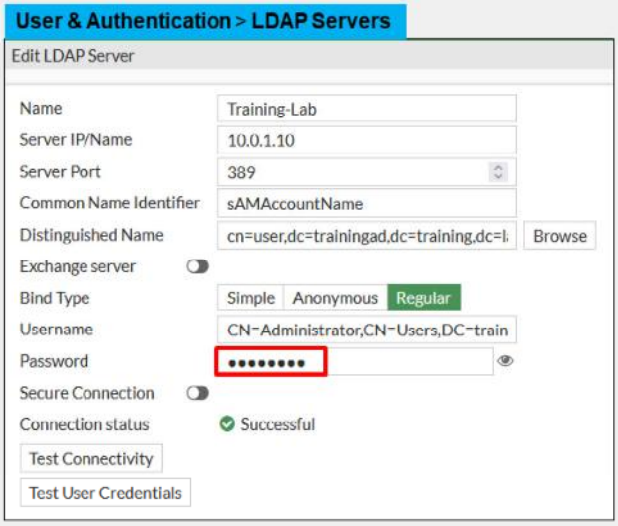
LDAP authentication failed at the admin binding state. Error 49 indicates that the administrator provided invalid credentials. Because LDAP authentication is failing at the admin binding state, it means there is an issue with the administrator credentials.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

LDAP—Solution to Problem 1

- Enter `password` as the password



NSE Training Institute

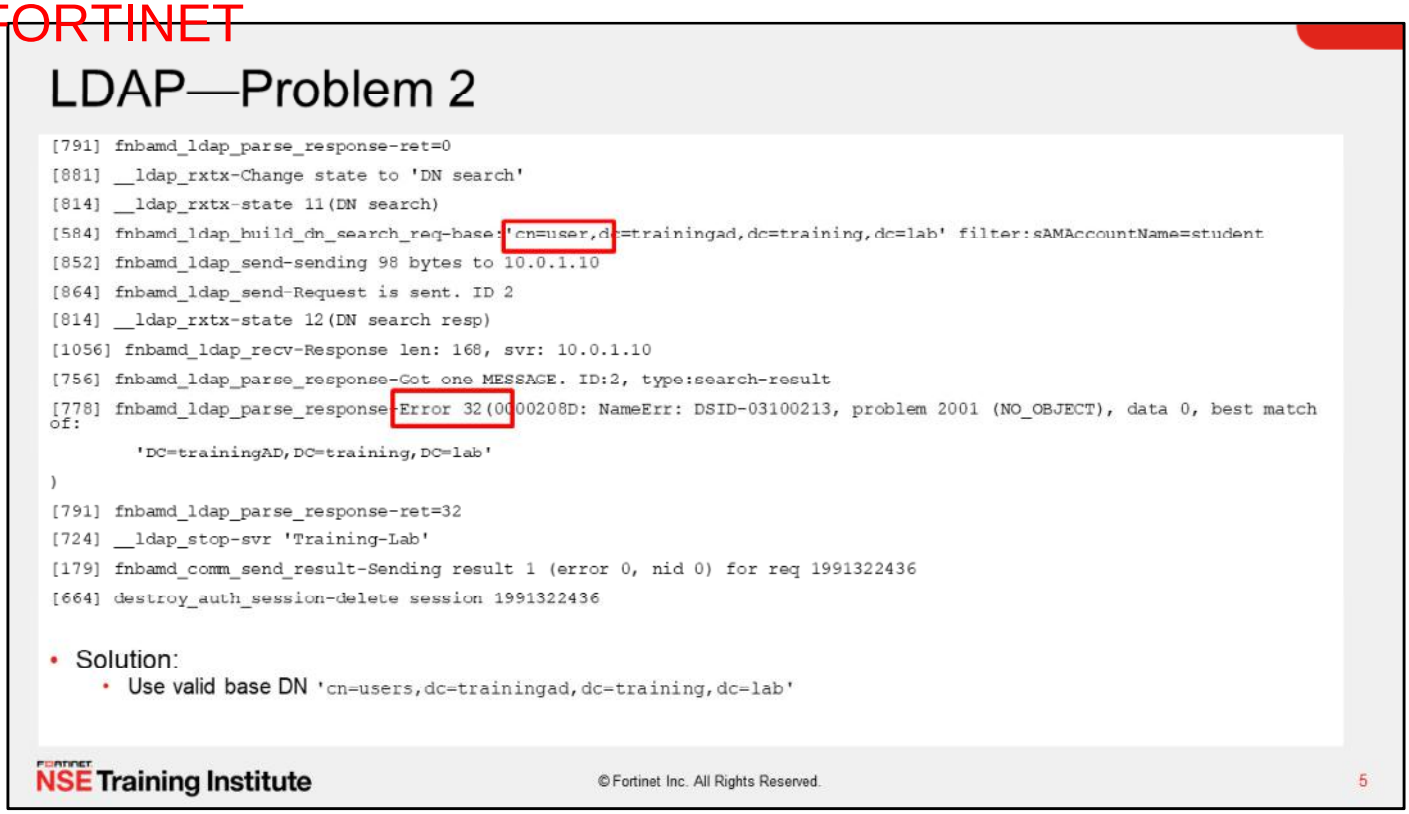
© Fortinet Inc. All Rights Reserved.

4

The cause of the first problem is an incorrect password. To resolve this issue, change the administrator password to `password` on FortiGate.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



This problem occurs at the user search state. The output shown on the slide indicates that admin binding was successful, but FortiOS is having trouble locating the user in the LDAP tree. Take a close look at the base DN; the CN user does not exist on the LDAP server. The correct LDAP tree DN should be `cn=users,dc=trainingad,dc=training,dc=ldap`.

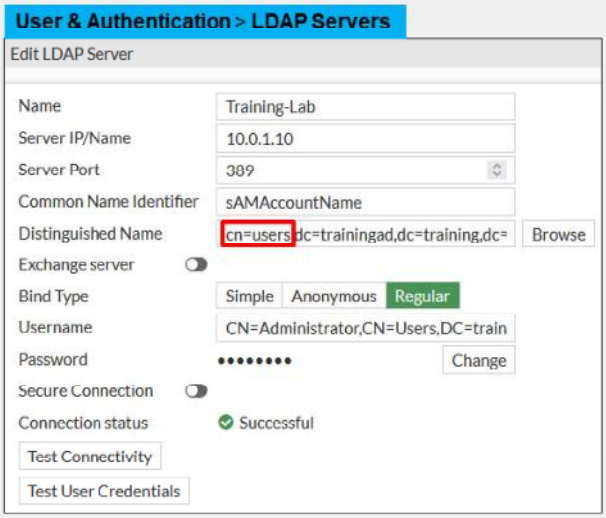
This type of problem is very common. A small typing error can cause the LDAP query search to fail.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

LDAP—Solution to Problem 2

- Fix the **Distinguished Name** field



NSE Training Institute

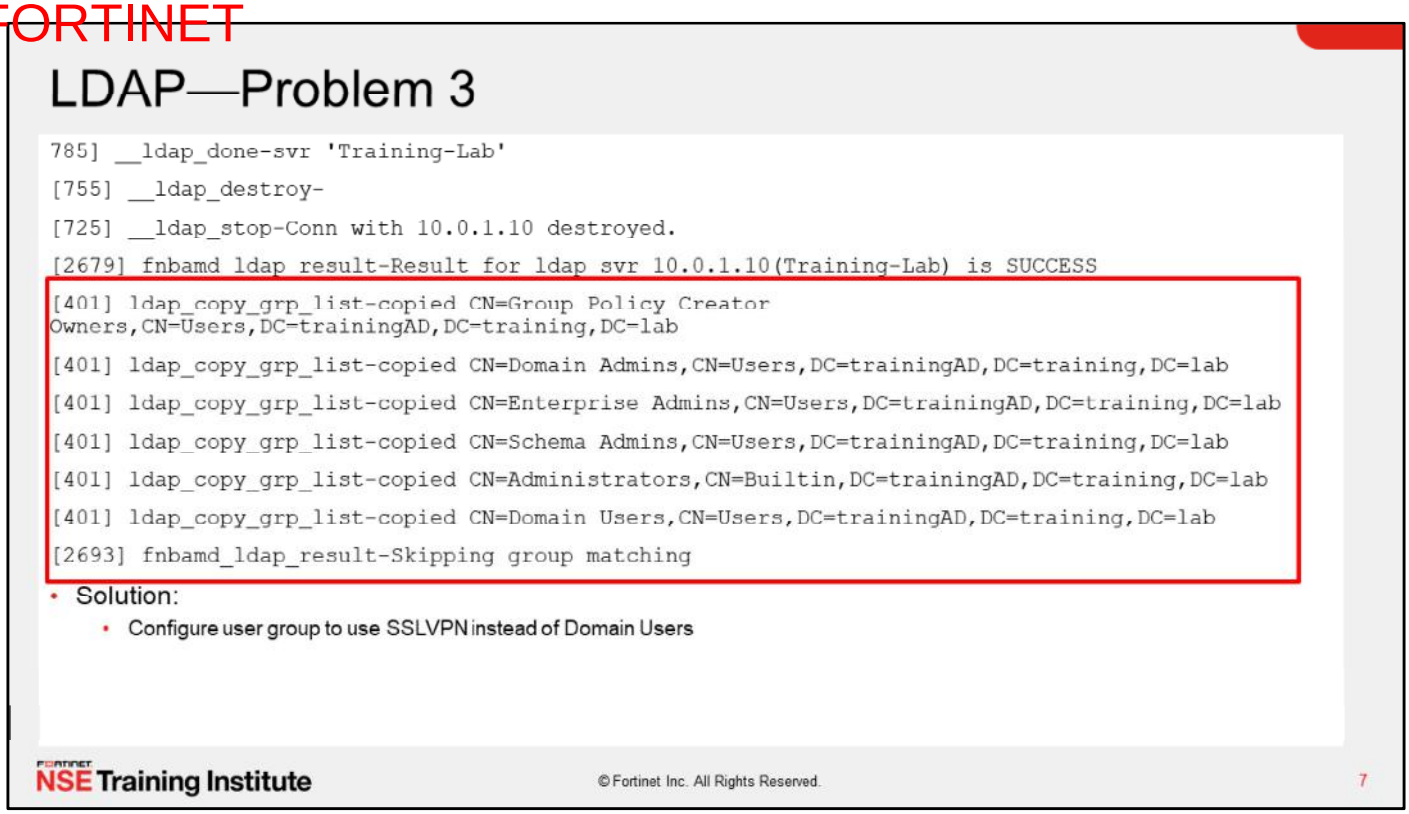
© Fortinet Inc. All Rights Reserved.

6

You can fix the second problem by fixing the typing error in the **Distinguished Name** field. It should be pointing to `cn=users`, not `cn=user`.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



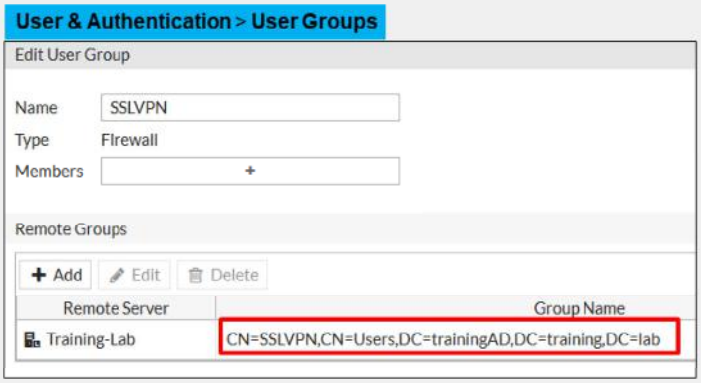
The last problem is with group matching. The VPN user group on FortiGate is configured to allow access to all users that belong to Domain Users. Remote group matching needs to be changed to SSLVPN instead of Domain Users. This will ensure that users who are member of the SSLVPN group on the LDAP server are allowed access to SSLVPN.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

LDAP—Solution to Problem 3

- Select the correct **Group Name** in the **SSLVPN** user group



NSE Training Institute

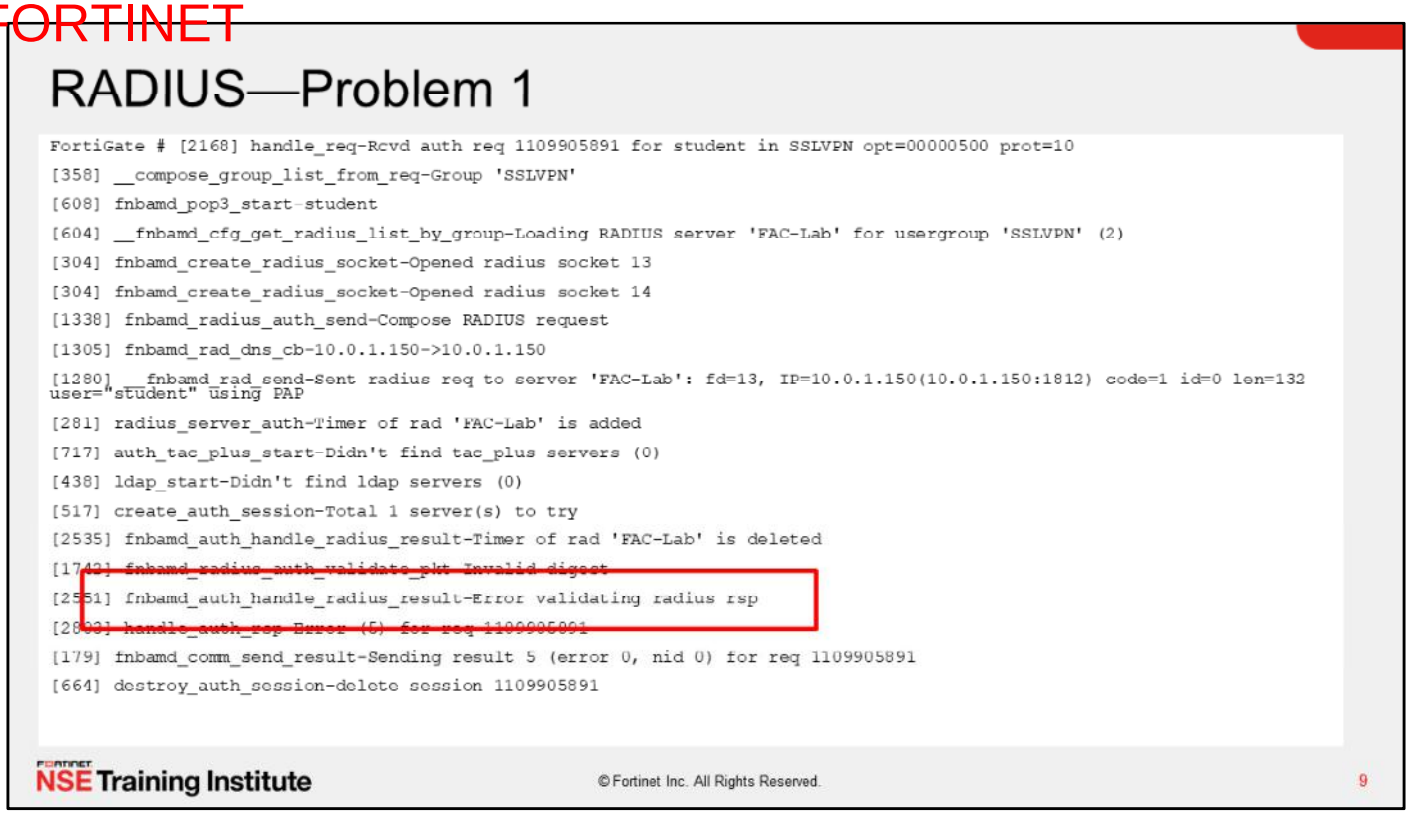
© Fortinet Inc. All Rights Reserved.

8

To fix the third problem with LDAP configuration, point the user group to SSLVPN instead of Domain Users.

Vouchers & Dumps are Available | WhatsApp +201224560923

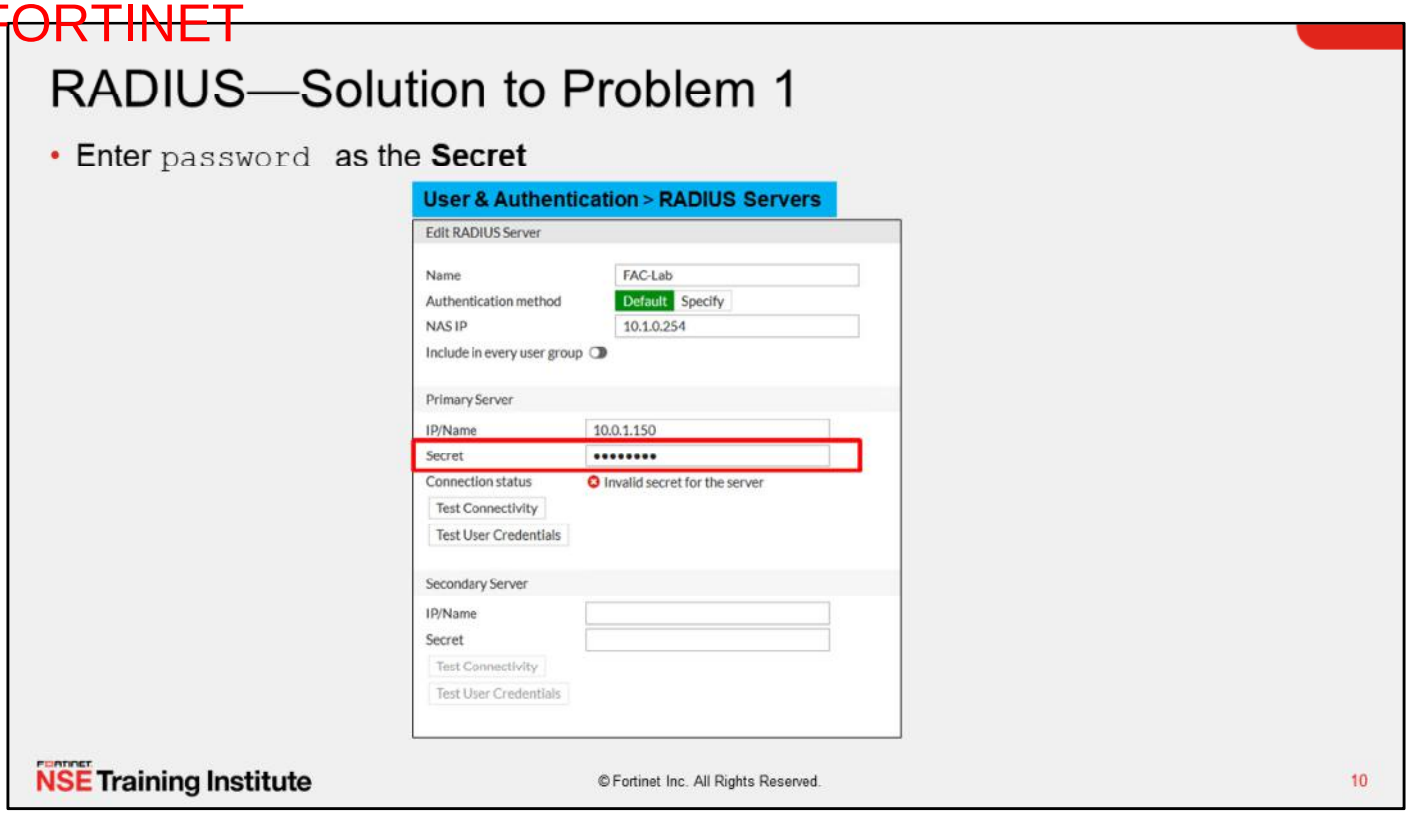
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The first problem in the RADIUS troubleshooting exercise is related to a preshared key mismatch between FortiGate and the RADIUS server (FortiAuthenticator). Update FortiGate with the correct preshared key and the communication between FortiGate and FortiAuthenticator will succeed.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



On the RADIUS server configuration page on FortiGate, update the secret to fix the first problem.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

RADIUS—Problem 2

```
[358] __compose_group_list_from_req-Group 'SSLVPN'
[608] fnbamd_pop3_start-student
[604] __fnbamd_cfg_get_radius_list_by_group-Loading RADIUS server 'FAC-Lab' for usergroup
'SSLVPN' (2)
[304] fnbamd_create_radius_socket-Opened radius socket 13
[304] fnbamd_create_radius_socket-Opened radius socket 14
[1338] fnbamd_radius_auth_send-Compose RADIUS request
...
[1280] __fnbamd_rad_send-Sent radius req to server 'FAC-Lab': fd=13,
IP=10.0.1.150(10.0.1.150:1812) code=1 id=1 len=132 user="student" using PAP
[62] handle_rad_timeout-Timer of rad 'FAC-Lab' is added
[2535] fnbamd_auth_handle_radius_result-Timer of rad 'FAC-Lab' is deleted
[1746] fnbamd_radius_auth_validate_pkt-RADIUS resp code 2
[305] extract_success_vsas-FORTINET attr, type 1, val SSLVPN
[2561] fnbamd_auth_handle_radius_result-->Result for radius svr 'FAC-Lab' 10.0.1.150(1) is 0
[2491] fnbamd_radius_group_match-Skipping group matching
[938] find_matched_usr_grps-Skipped group matching
[179] fnbamd_comm_send_result-Sending result 0 (error 0, nid 0) for req 1109905892
[664] destroy_auth_session-delete session 1109905892
```

NSE Training Institute

© Fortinet Inc. All Rights Reserved.

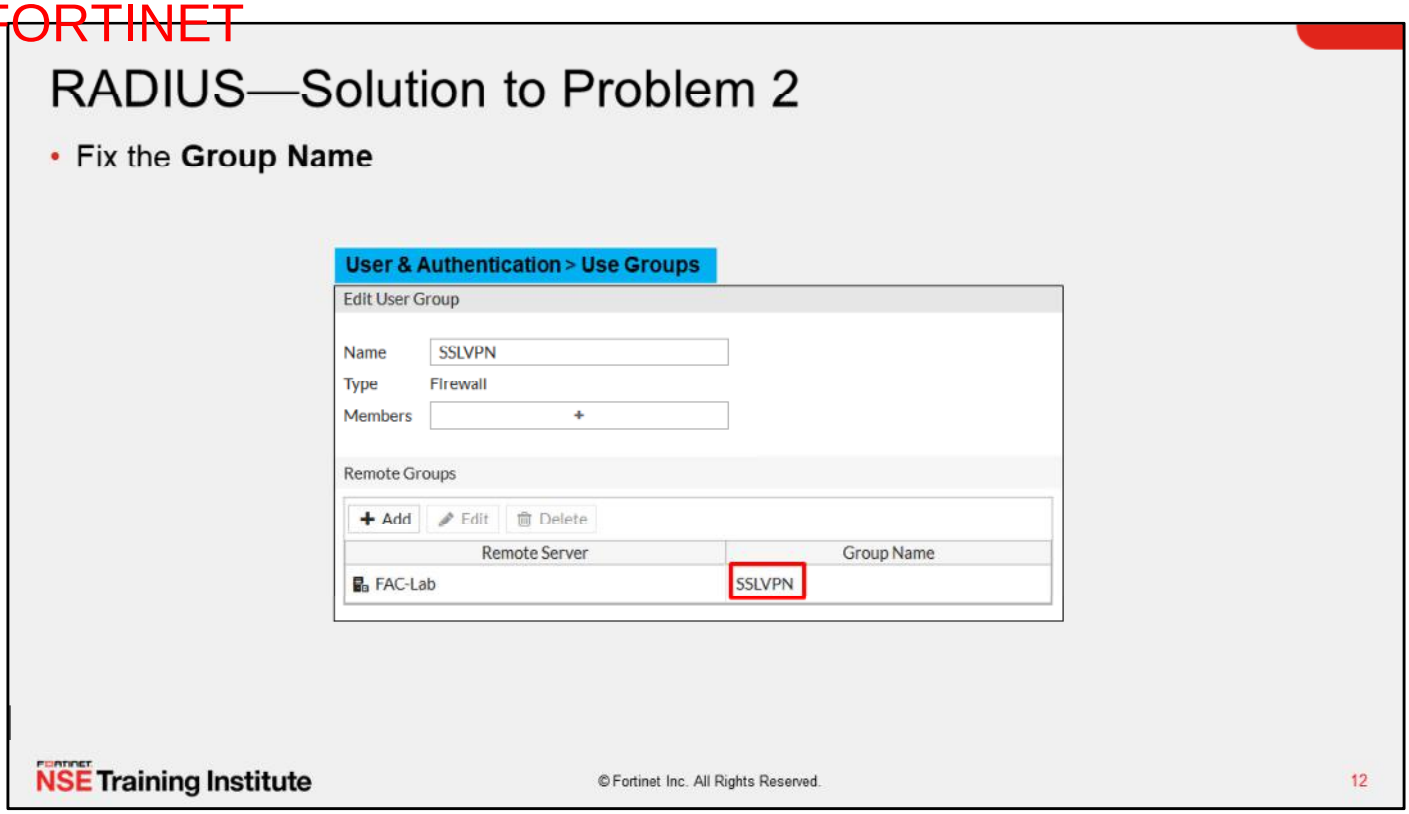
11

The second problem with the RADIUS server is related to the VSA. FortiGate is configured with `SSL-VPN`, which contains a hyphen. However, RADIUS is sending `SSLVPN`, without the hyphen. This causes the attributes to mismatch and FortiGate to reject the authentication for the user.

VSAs are case-sensitive and must match on both sides.

Vouchers & Dumps are Available | WhatsApp +201224560923

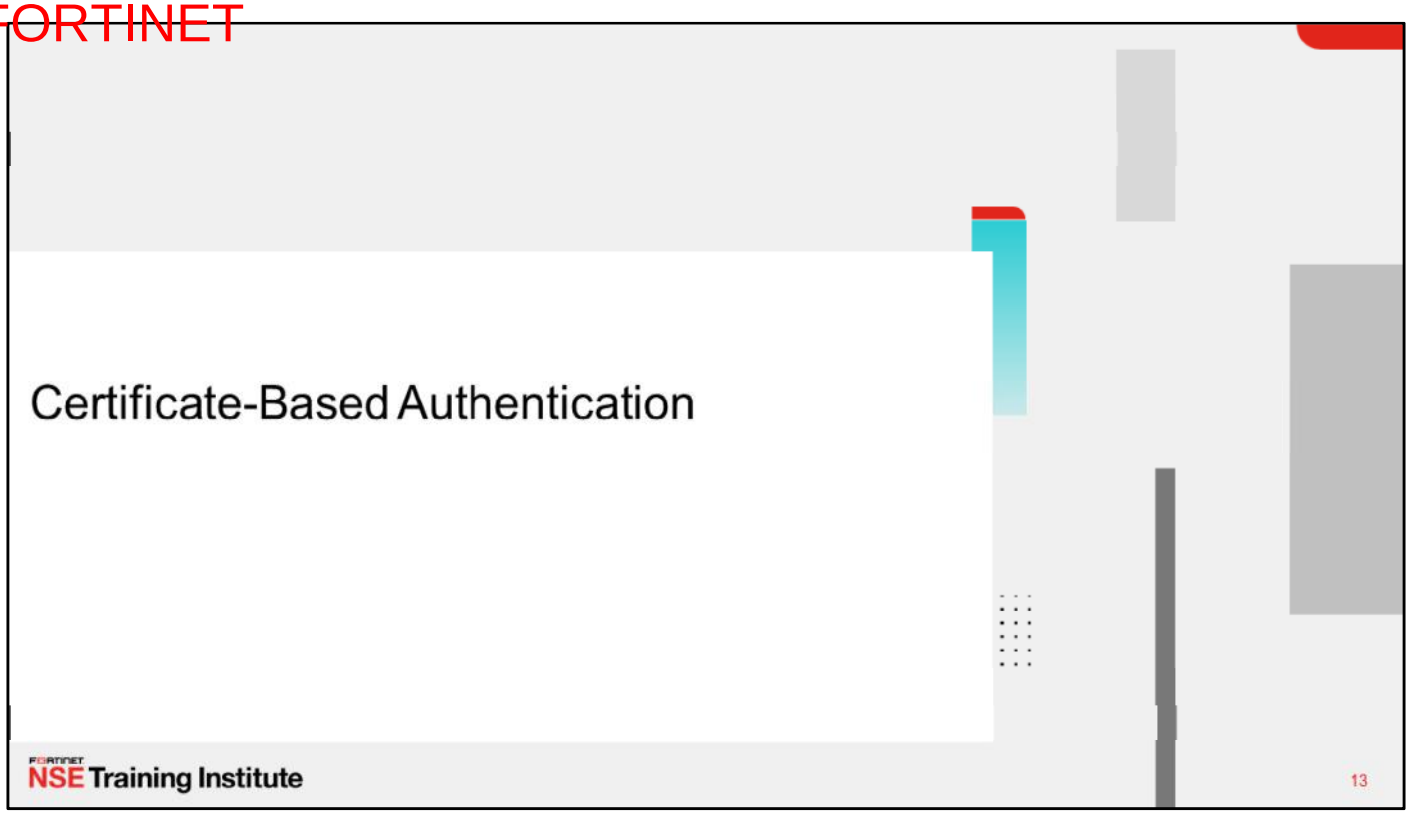
DO NOT REPRINT
© FORTINET
Brave-dumps.com



To fix the second problem, remove the hyphen from `SSL-VPN` to change it to `SSLVPN`.

Vouchers & Dumps are Available | WhatsApp +201224560923

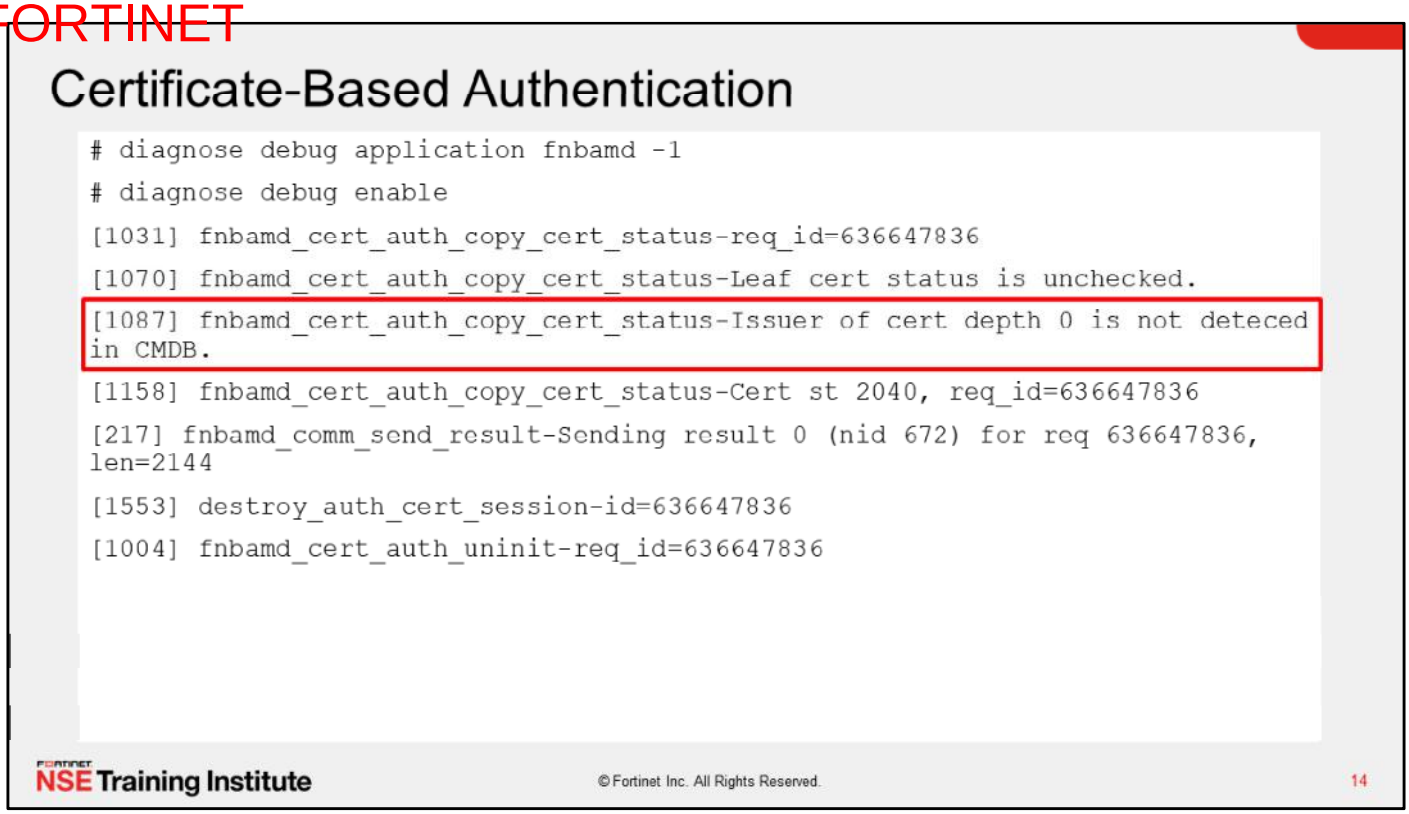
DO NOT REPRINT
© FORTINET
Brave-dumps.com



Now, you will review certificate lab problems and solutions.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



The certificate installed and used for the IPsec dialup VPN is not signed by a trusted CA. FortiGate is unable to validate the certificate and, therefore, authentication is failing.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

Certificate-Based Authentication

- Signed by an untrusted (incorrect) CA



- Solution:
  - Add the CA certificate of the authority that signed the user certificate
  - Generate a new user certificate signed by a trusted CA

NSE Training Institute

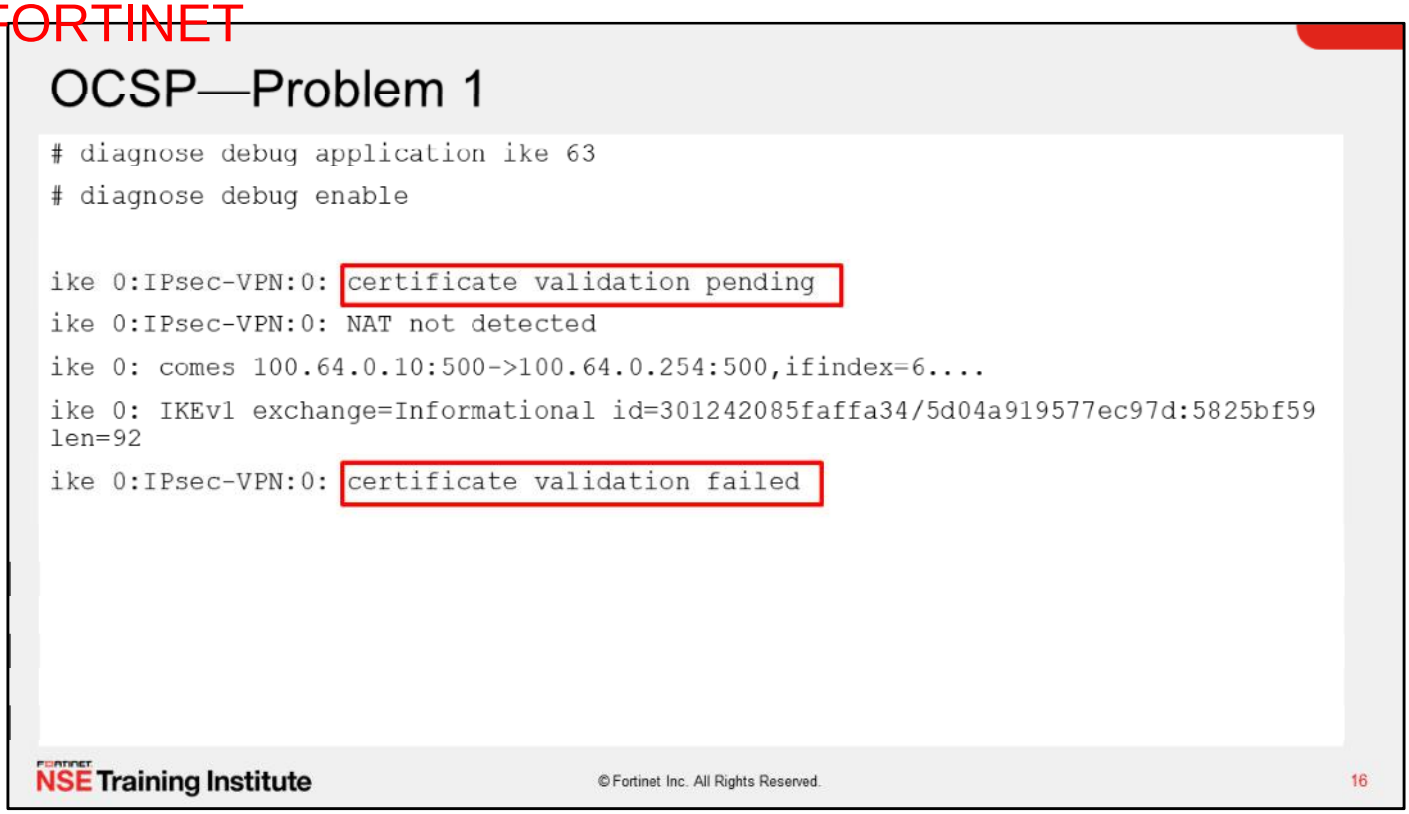
© Fortinet Inc. All Rights Reserved.

15

This slide shows that the certificate is signed by `Fortinet.lab`, which is not the CA you are using in the lab. The correct certificate should be signed by `trainingad.training.lab`. You will need to create a new user certificate that is signed by the correct CA.

Vouchers & Dumps are Available | WhatsApp +201224560923

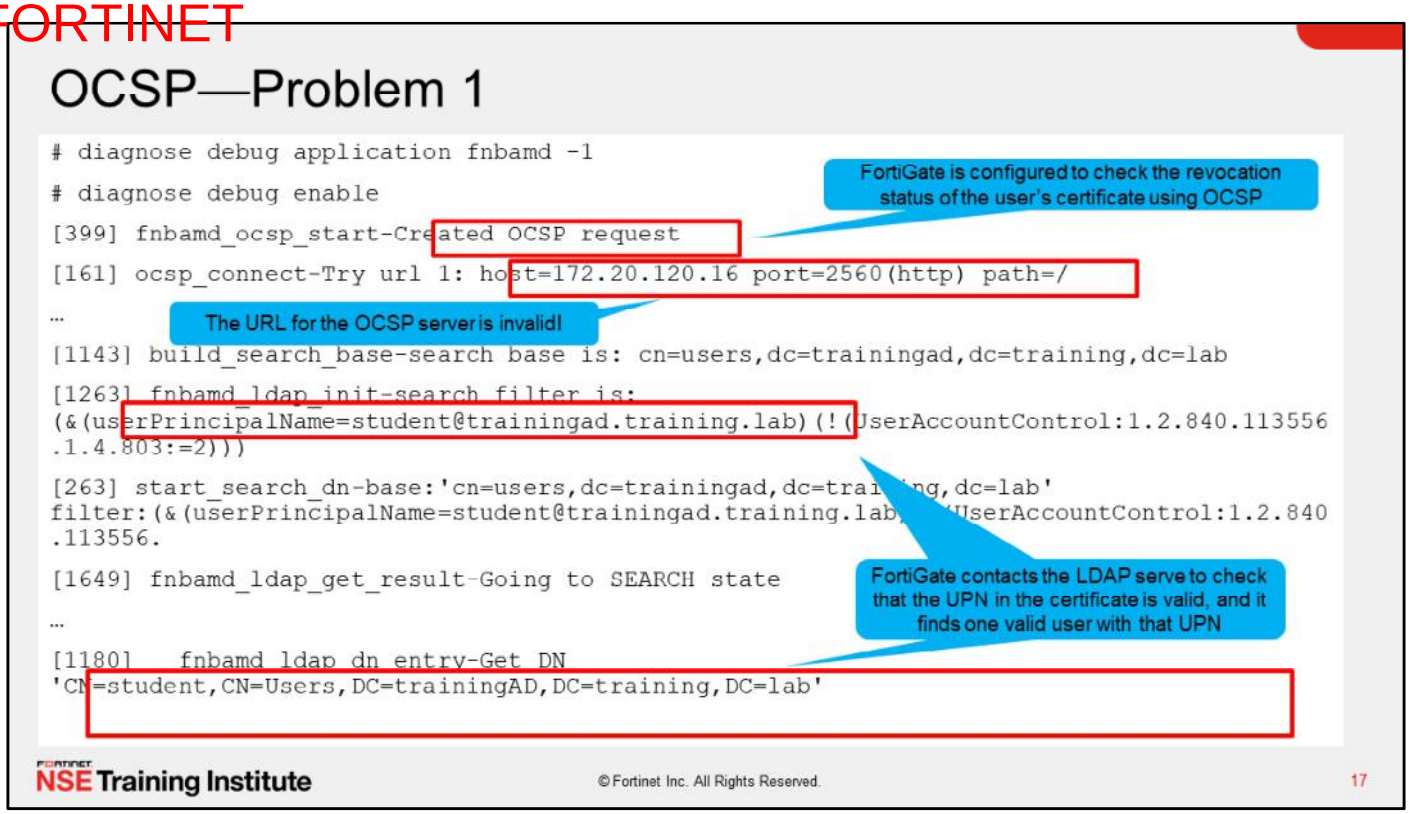
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The first issue with the lab is caused by a certification validation failure. The IKE real-time debug shows that the process is failing at the certificate validation stage.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com

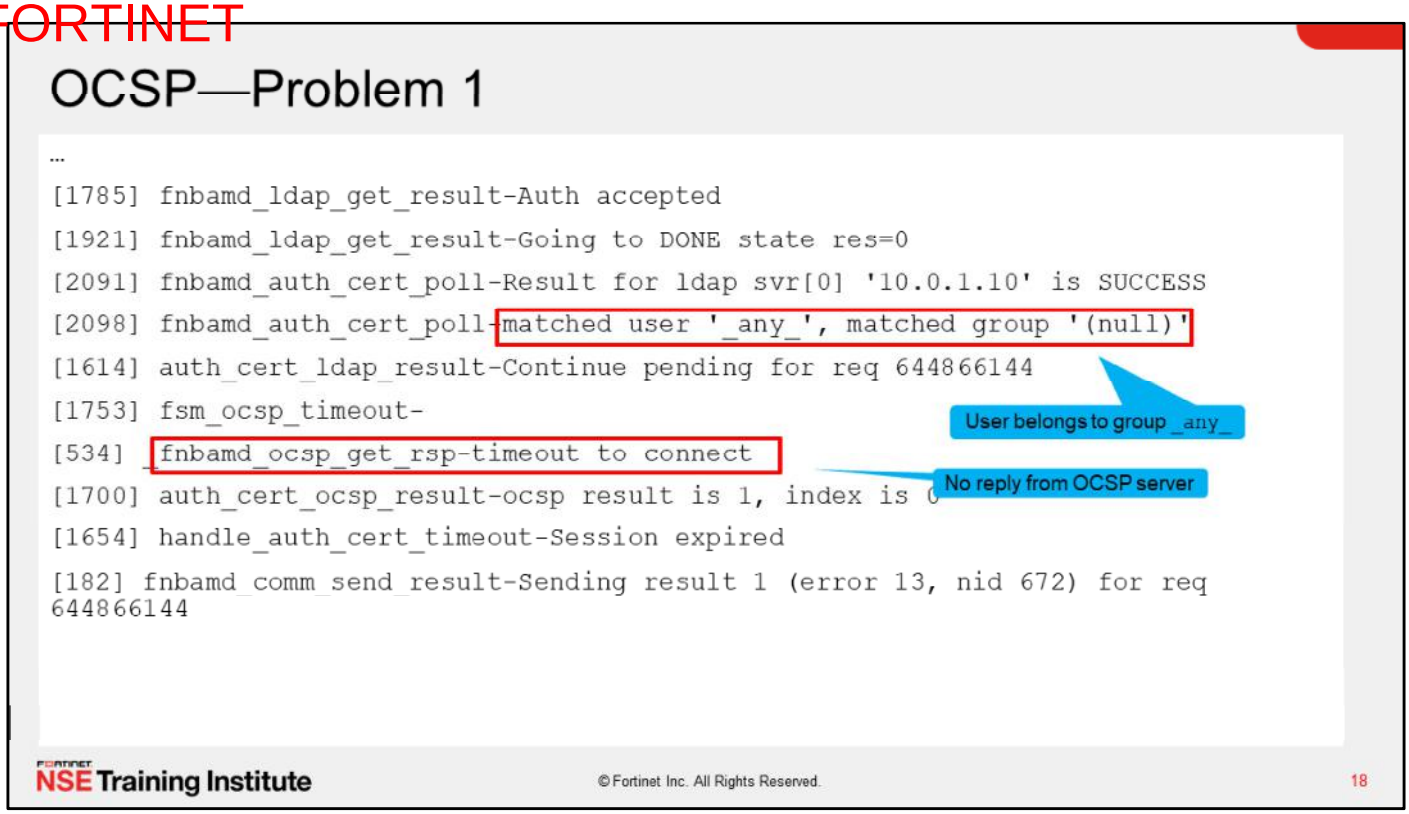


The `fnbamd` real-time debug shows that the issue is with OCSP request. The issue, in this case, is that FortiGate is configured with the wrong OCSP URL.

The LDAP lookup of the UPN string in the certificate is valid, and it finds one valid user with that UPN.

Vouchers & Dumps are Available | WhatsApp +201224560923

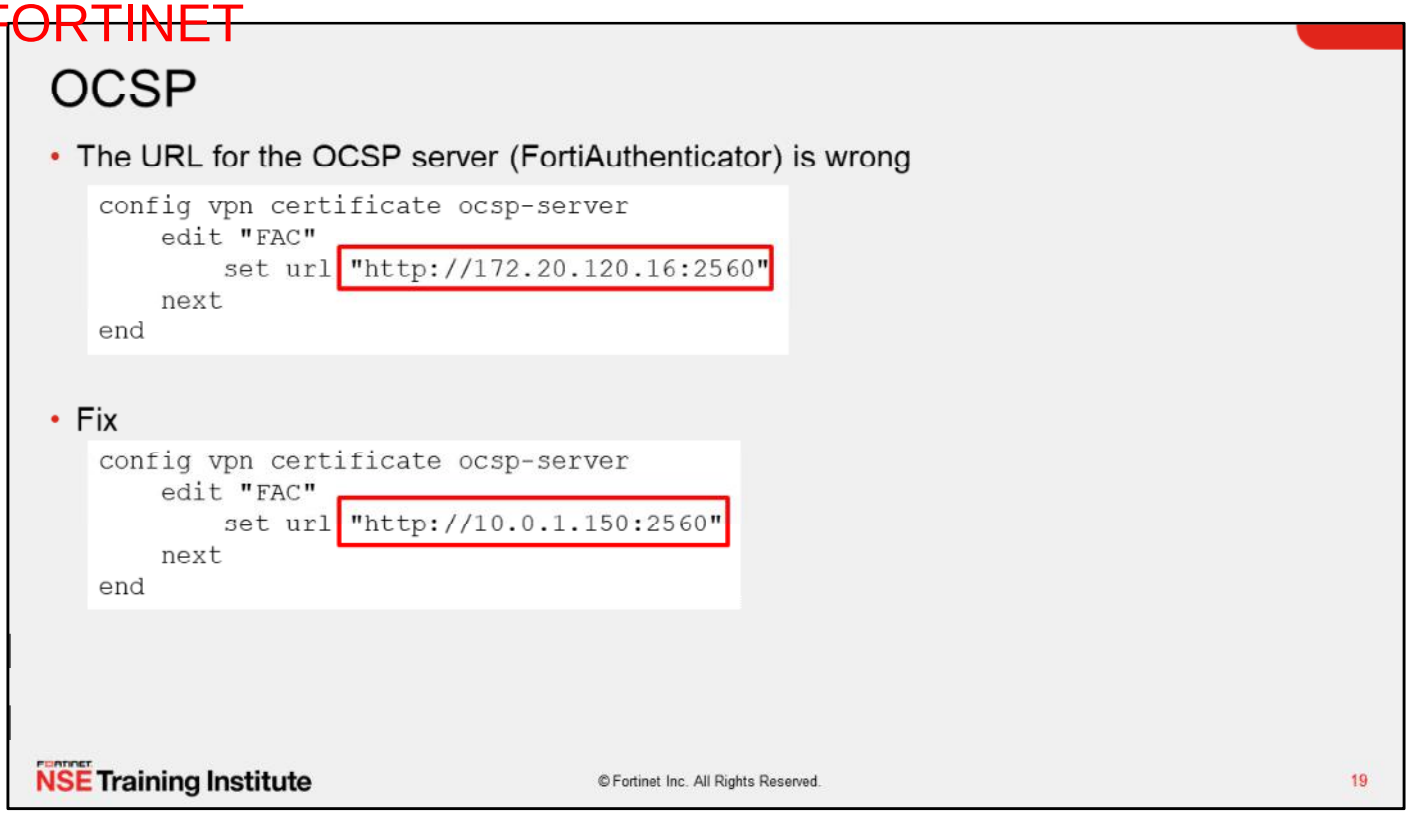
DO NOT REPRINT
© FORTINET
Brave-dumps.com



The `fnbamd` debug shows you that the OCSP response timed out, which basically means that FortiGate was unable to connect to OSCP, which is FortiAuthenticator.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



To fix the issue, change the OCSP server IP address to `10.0.1.150:2560`. You must also specify a port number for the configuration to work properly.

Vouchers & Dumps are Available | WhatsApp +201224560923

DO NOT REPRINT
© FORTINET
Brave-dumps.com



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.

Vouchers & Dumps are Available | WhatsApp +201224560923