FORTINET Network Security Expert 7

Secure Access Study Guide

for FortiGate 6.2

FORTINET NSE
NSE Certification Program

Fortinet Training

http://www.fortinet.com/training

Fortinet Document Library

http://docs.fortinet.com

Fortinet Knowledge Base

http://kb.fortinet.com

Fortinet Forums

https://forum.fortinet.com

Fortinet Support

https://support.fortinet.com

FortiGuard Labs

http://www.fortiguard.com

Fortinet Network Security Expert Program (NSE)

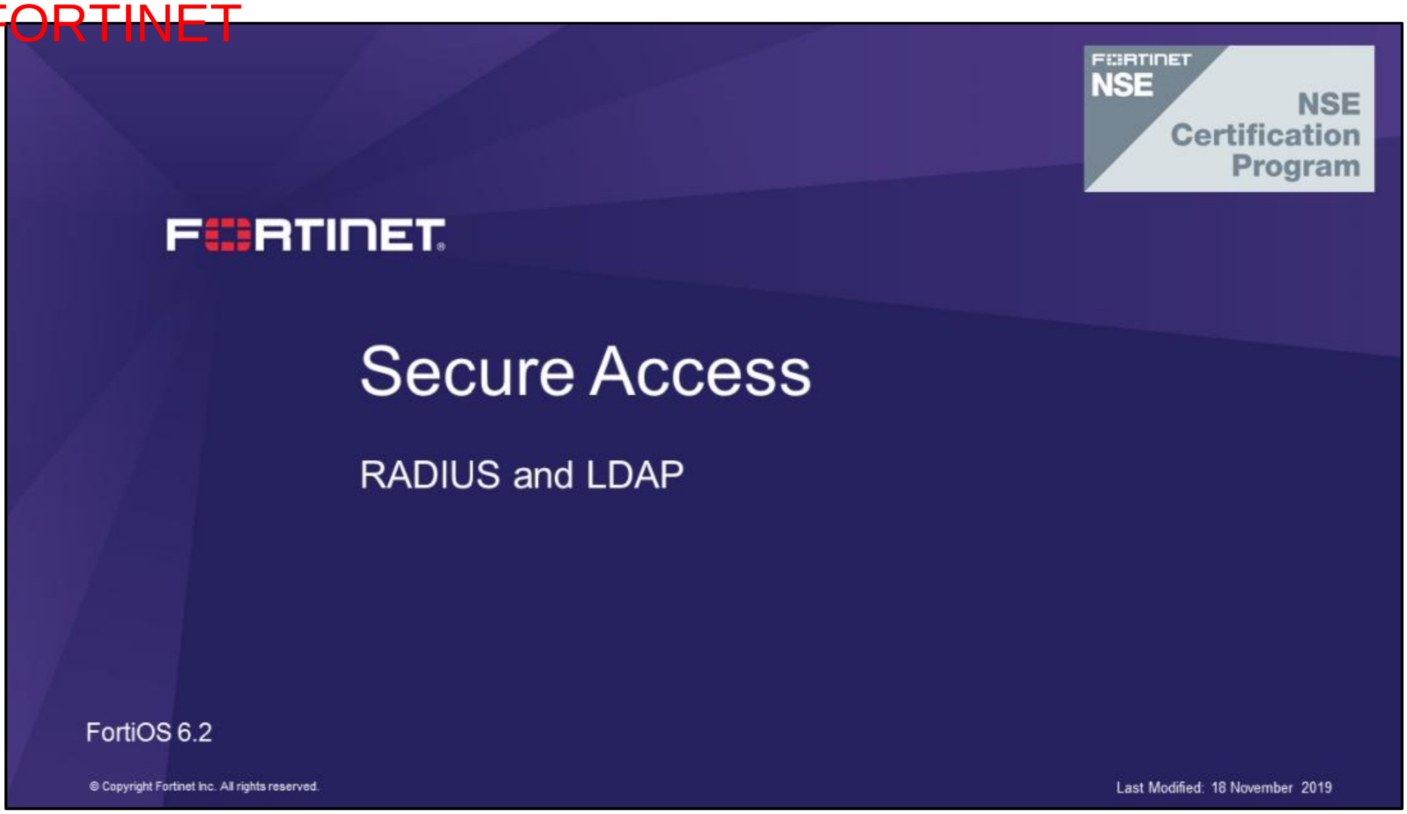
https://www.fortinet.com/support-and-training/training/network-security-expert-program.html

Feedback

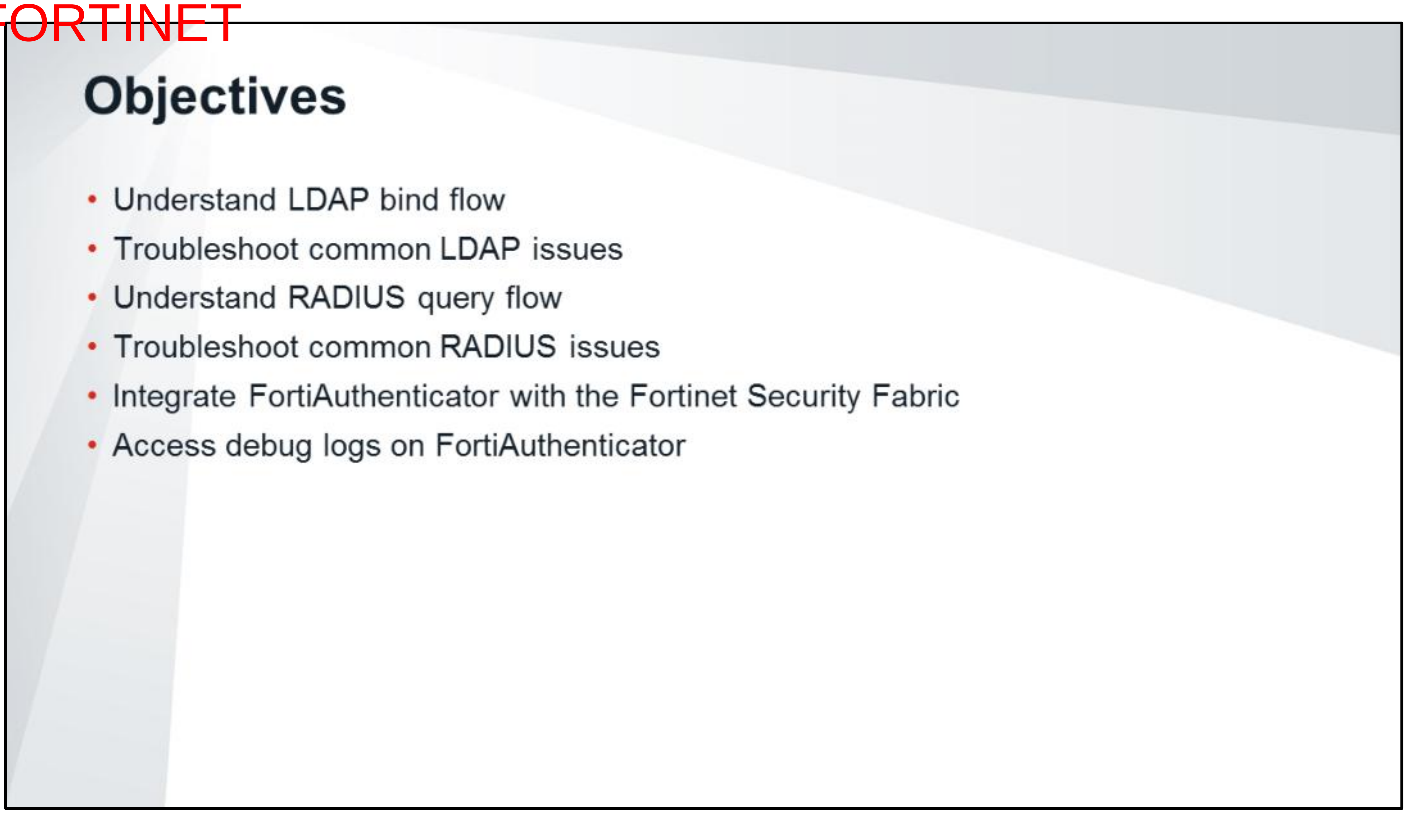
Email: courseware@fortinet.com

11/18/2019

TABLE OF CONTENTS



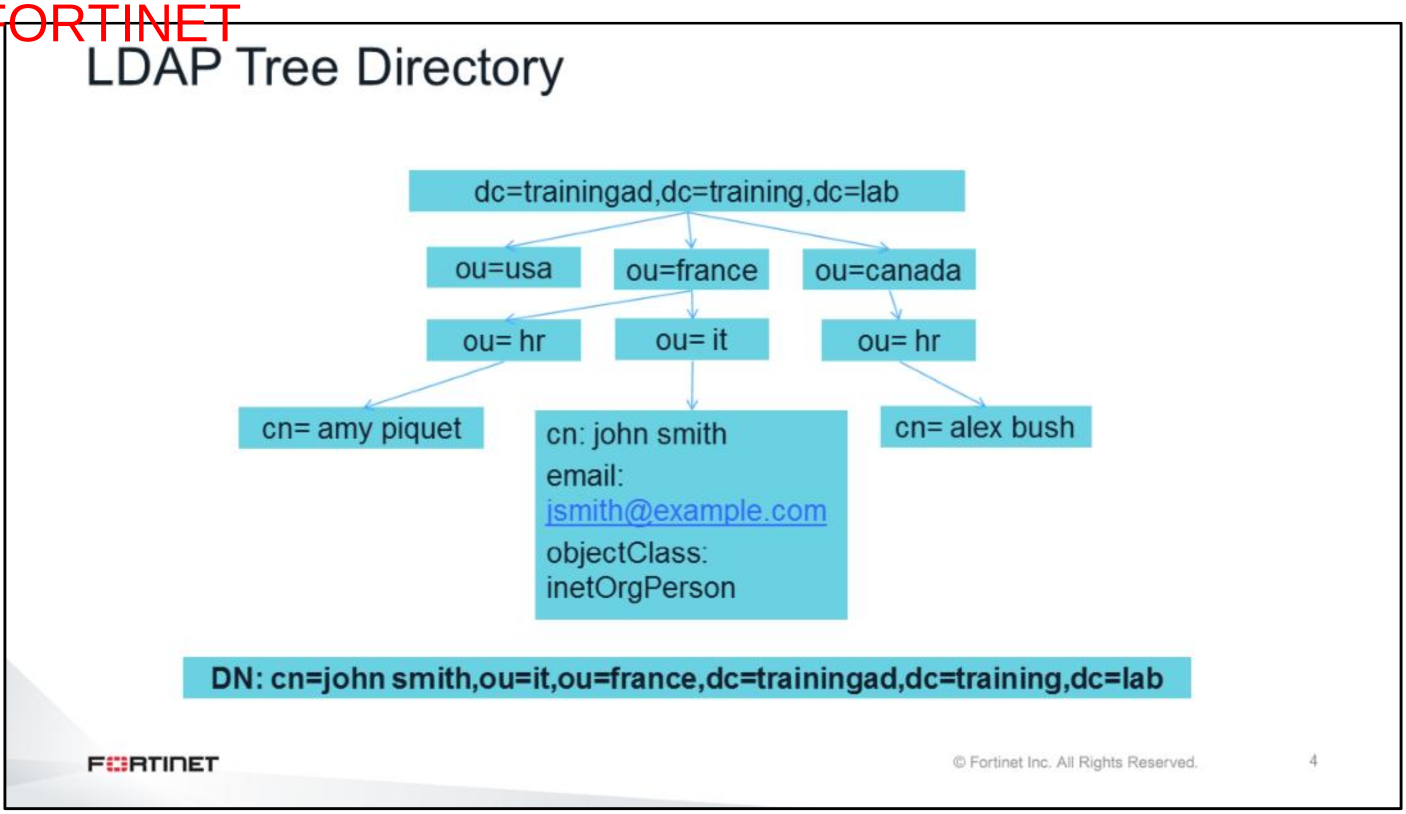
In this lesson, you will learn how to configure and troubleshoot RADIUS and LDAP authentication on FortiGate. You will also review some FortiAuthenticator basics.



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

LDAP

In this section, you will learn about Lightweight Directory Access Protocol (LDAP).



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.

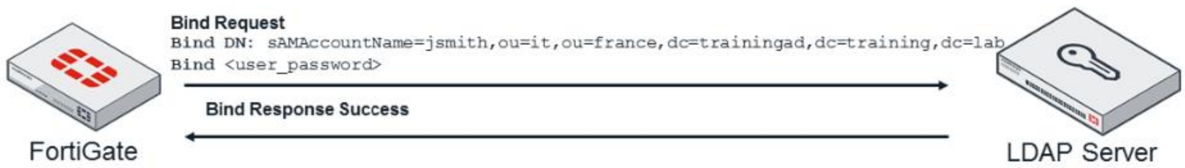
Simple Bind

- It works as long as all the users are in the same branch

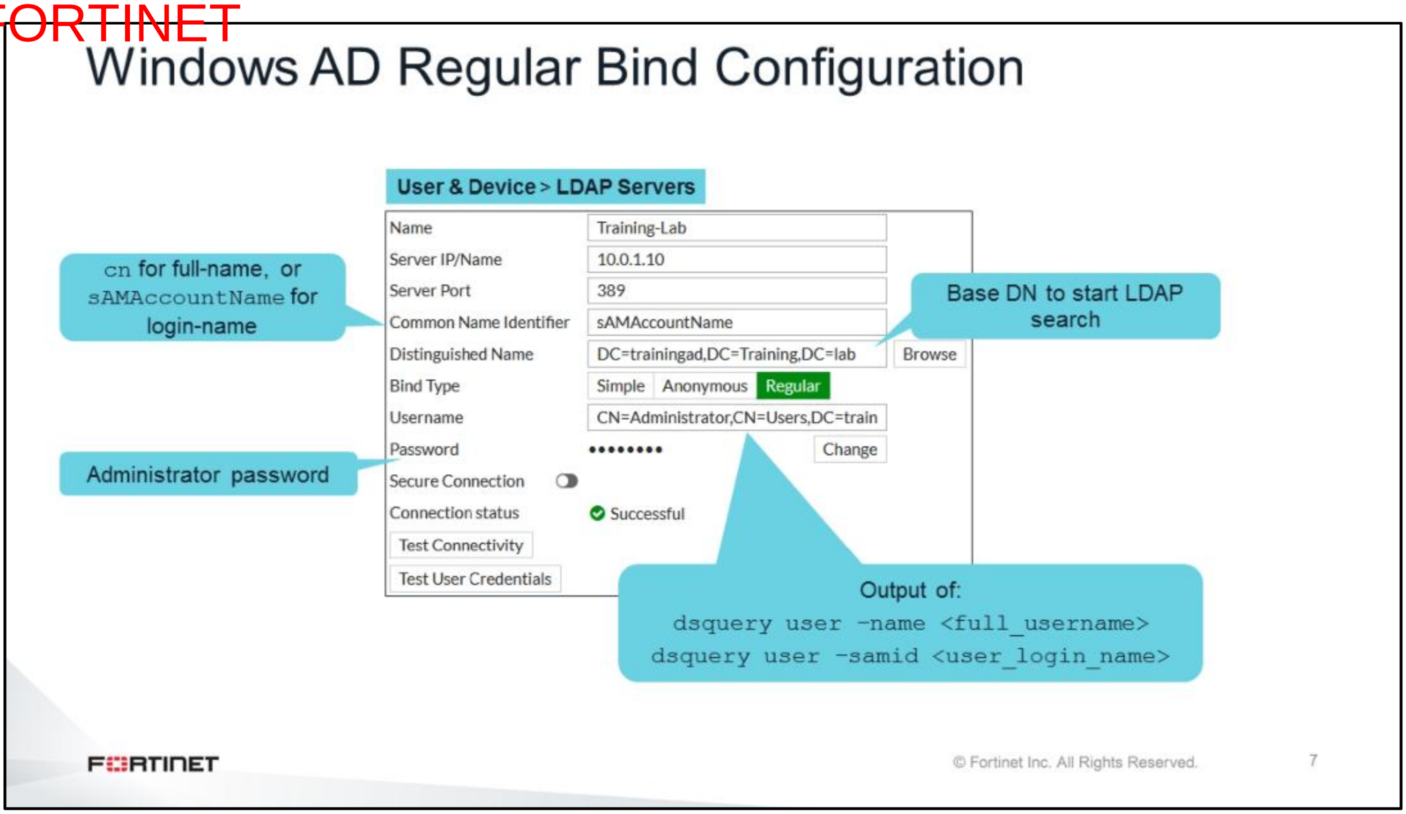
There are three different methods, or bind types, a FortiGate can use to access an LDAP server: simple, anonymous, and regular. During this lesson, you will learn about simple and regular binds.

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.

Simple Bind Flow



When simple bind flow is used, 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.



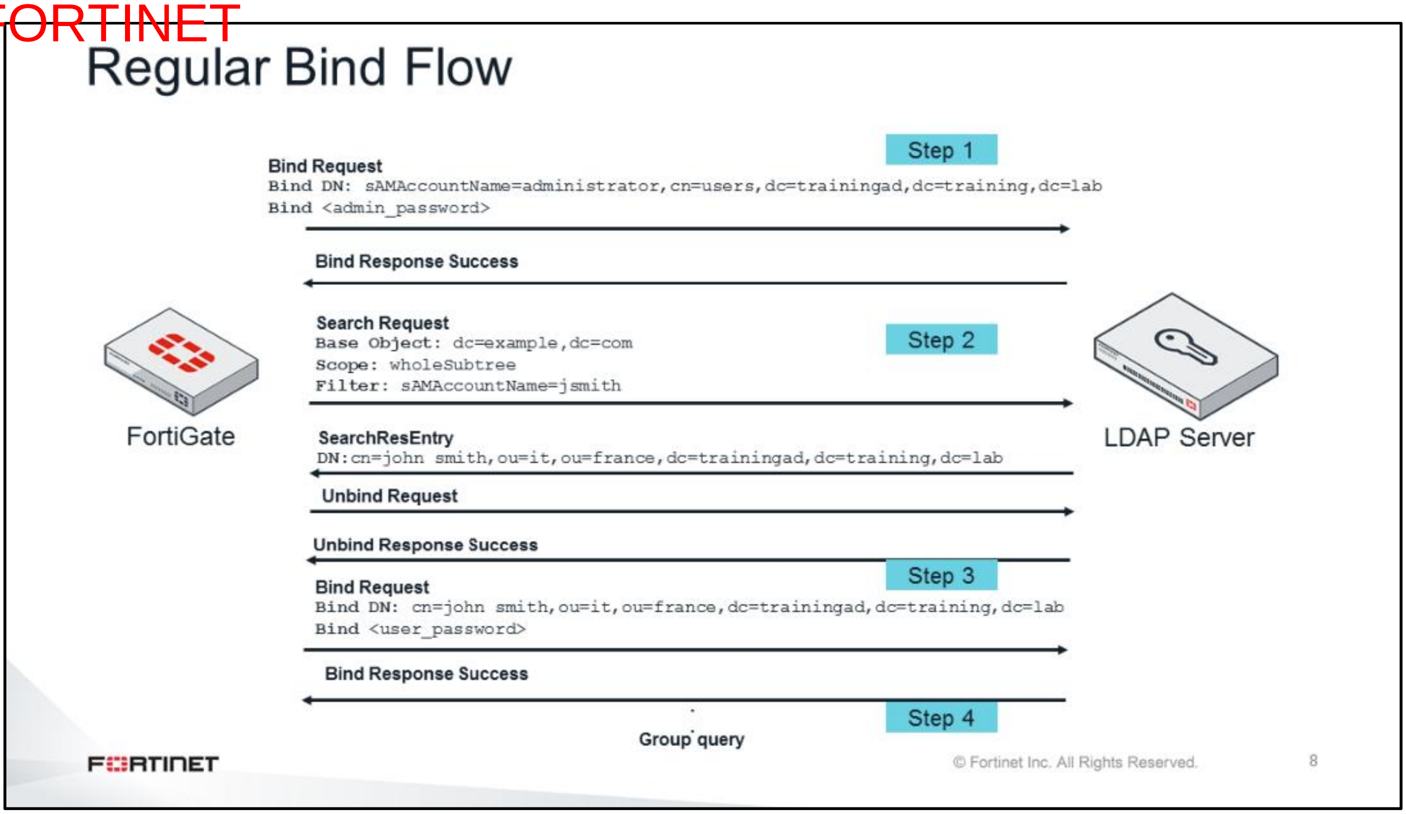
This slide shows a summary of how to properly configure regular bind for Windows AD. A different type of LDAP server might require a different approach.

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 **User DN** by querying the administrator DN with the same Windows AD command `dsquery`.

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



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

1. FortiGate logs to (binds to) the LDAP server, using an administrator account.

After this step, the 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's DN.

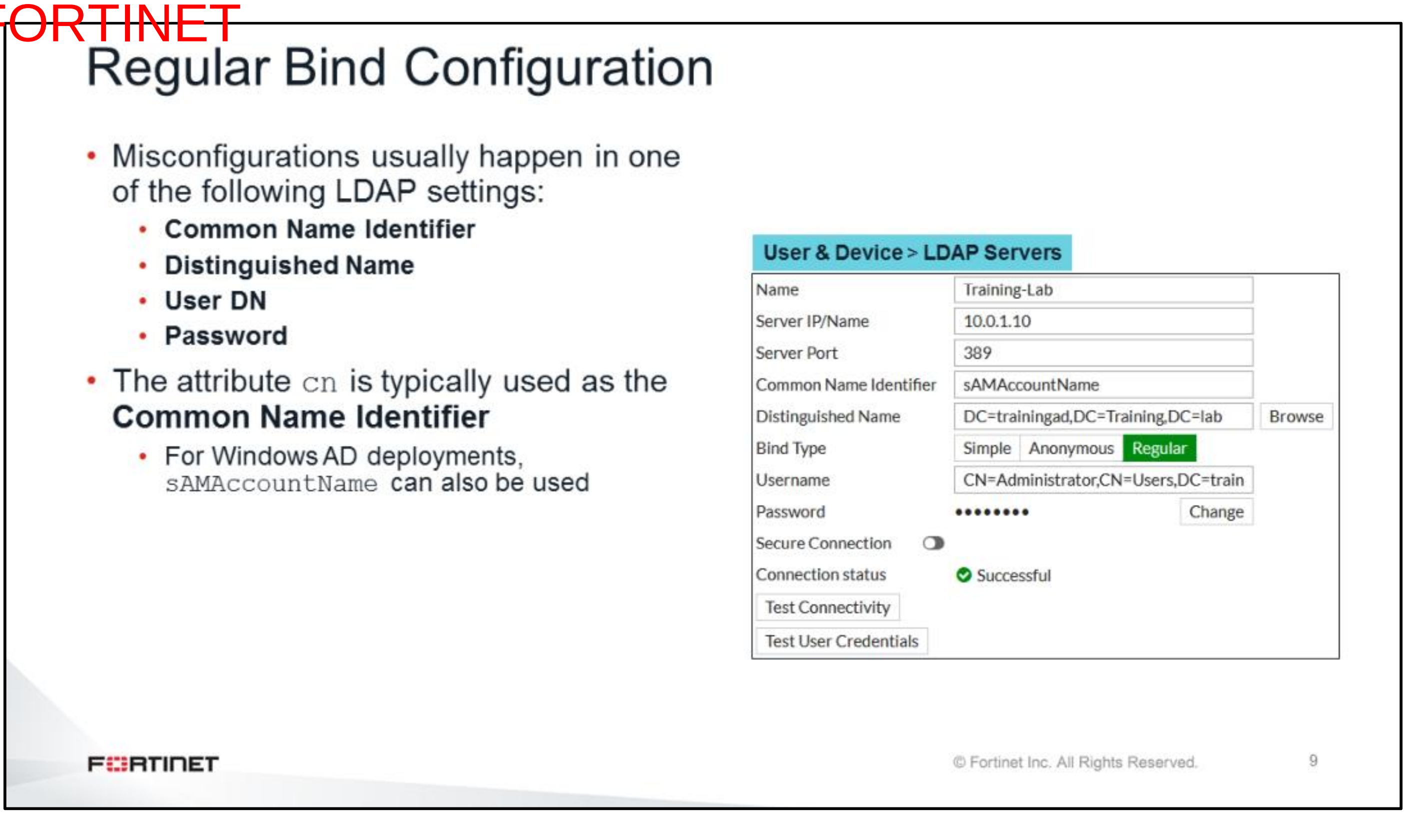
Then, FortiGate logs out of (unbinds from) the LDAP server.

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.

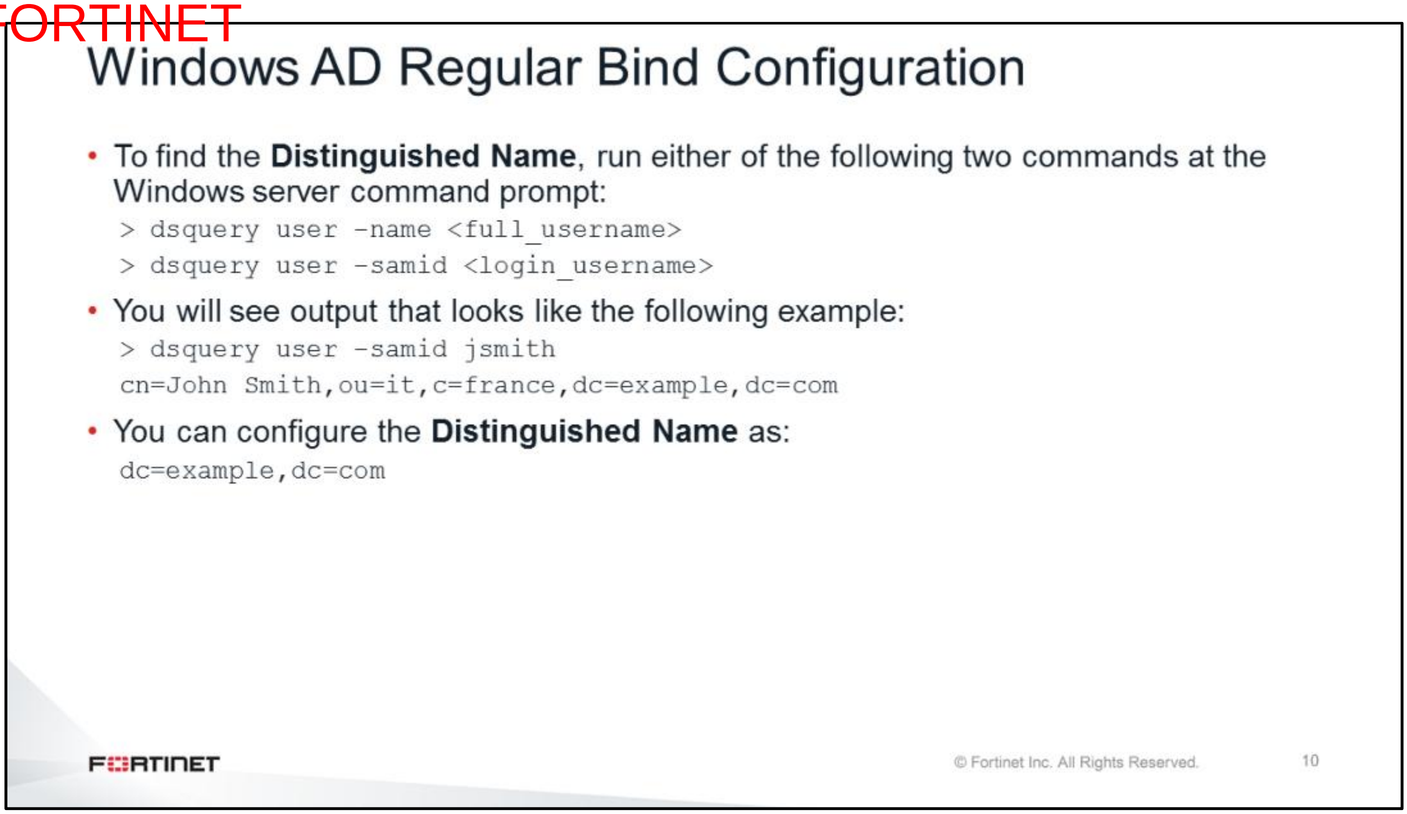
When isolating an LDAP problem, you must first identify which of these four steps is failing.



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

- Common Name Identifier
- Distinguished Name
- User DN
- 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.



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=example,dc=com
```

Windows AD Regular Bind Configuration

- For the **Bind DN**, use either of the following two commands at the server command prompt:

```
> dsquery user -name <admin_full_username>
> dsquery user -samid <admin_login_username>
```

- Copy and paste the full administrator DN
- For example, for the following output:

```
> dsquery user -samid administrator
cn=administrator,ou=it,c=france,dc=example,dc=com
```

- Configure the **Bind DN** as:

```
cn=administrator,ou=it,c=france,dc=example,dc=com
```

FORTINET

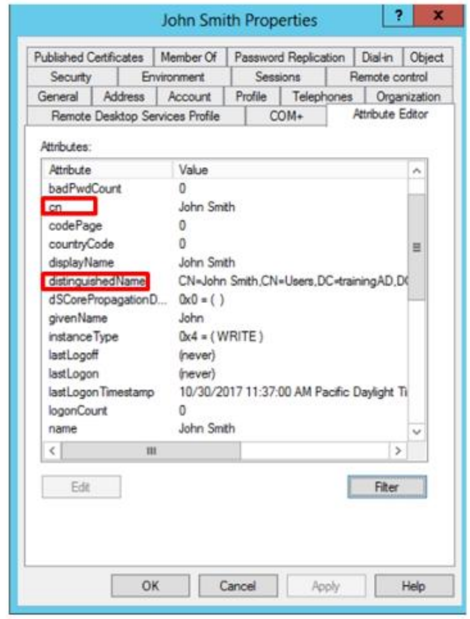
 11

The **User DN** (or **Bind DN**) setting is the full DN of the LDAP administrator account. We 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.

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 Common name identifier

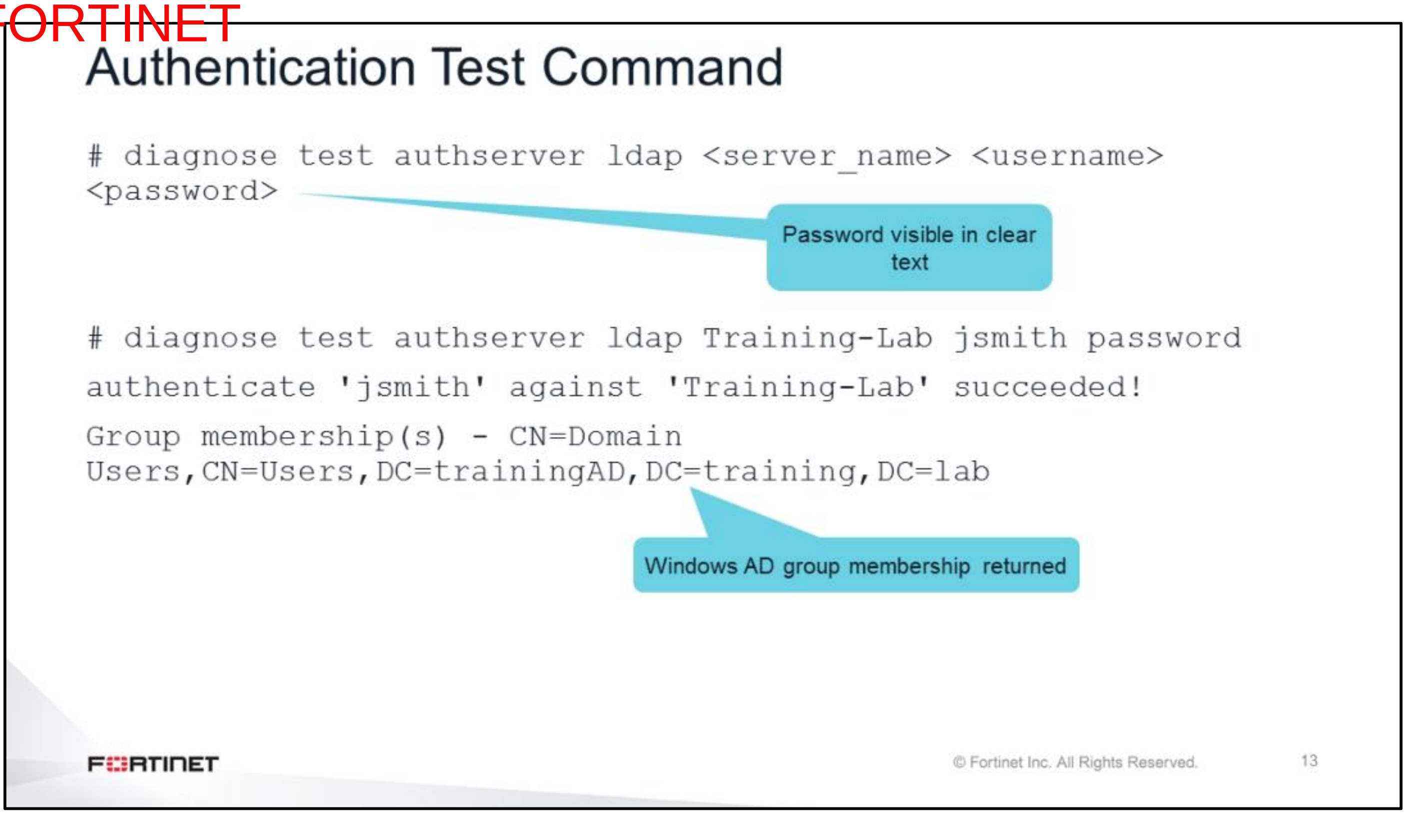


FERTINET

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.

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



The CLI includes an LDAP authentication test command. It is `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.

Real-Time Debug

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

FortiGate # [2168] handle_req-Rcvd auth req 1014692423 for jsmith in Training-Lab
opt=0000001b prot=0
[358] __compose_group_list_from_req-Group 'Training-Lab'
[608] fnbamd_pop3_start-jsmith
[1038] __fnbamd_cfg_get_ldap_list_by_server-Loading LDAP server 'Training-Lab'
[1544] fnbamd_ldap_init-search filter is: sAMAccountName=jsmith
[1553] fnbamd_ldap_init-search base is: DC=trainingad,DC=Training,DC=lab
[973] __fnbamd_ldap_dns_cb-Resolved Training-Lab(idx 0) to 10.0.1.10
[1021] __fnbamd_ldap_dns_cb-Still connecting.
[517] create_auth_session-Total 1 server(s) to try
[939] __ldap_connect-tcps_connect(10.0.1.10) is established.
```

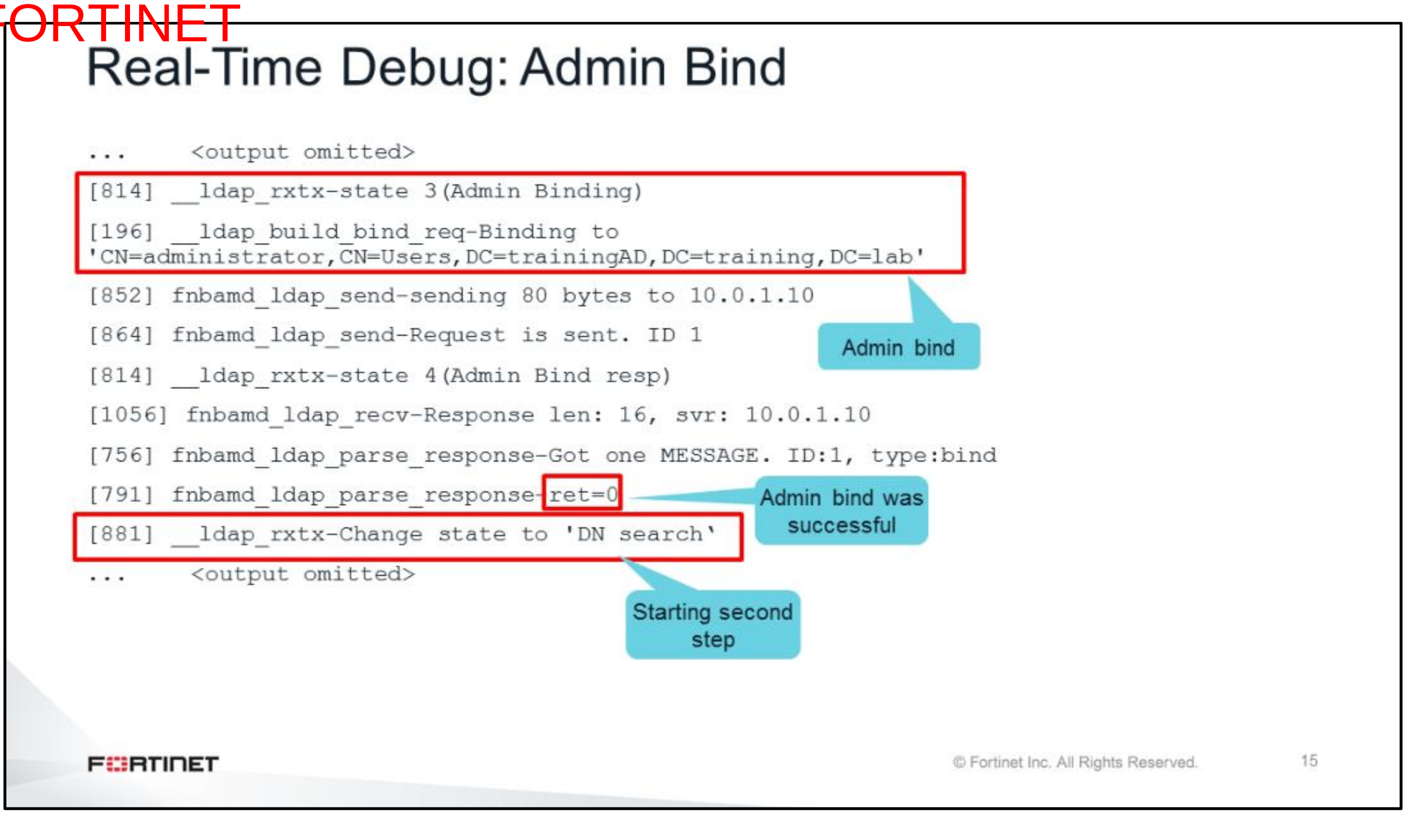
Username and base DN for LDAP search

FORTINET

 14

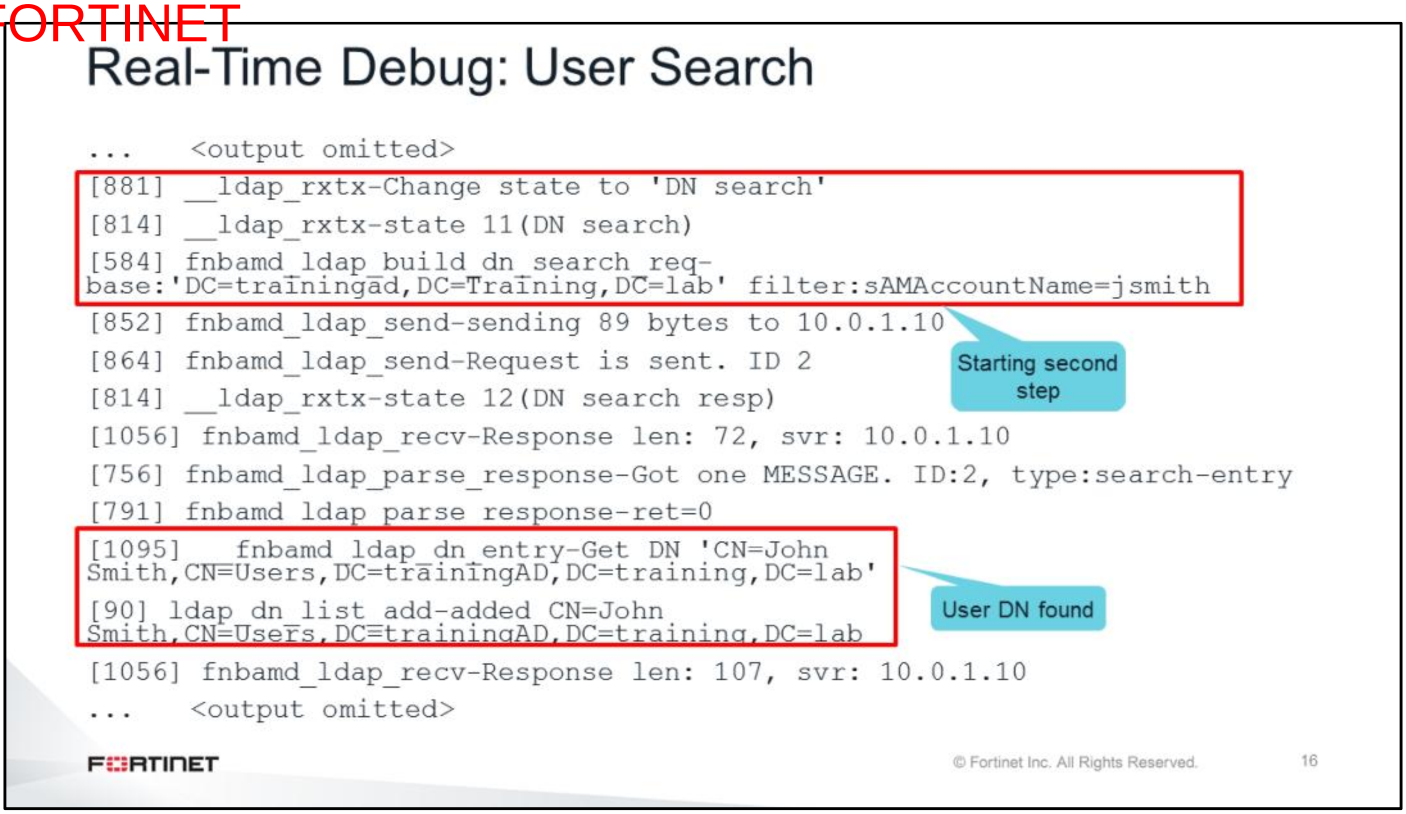
The Fortinet non-blocking authentication module daemon (`fnbamd`) is the process that handles LDAP and RADIUS authentication. This command enables the real-time debug for the `fnbamd` daemon.

In the example shown on this slide, the `handle_req-Rcvd auth` message indicates that the 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 will be used to search the user in the LDAP tree, base DN, and server name/IP address.



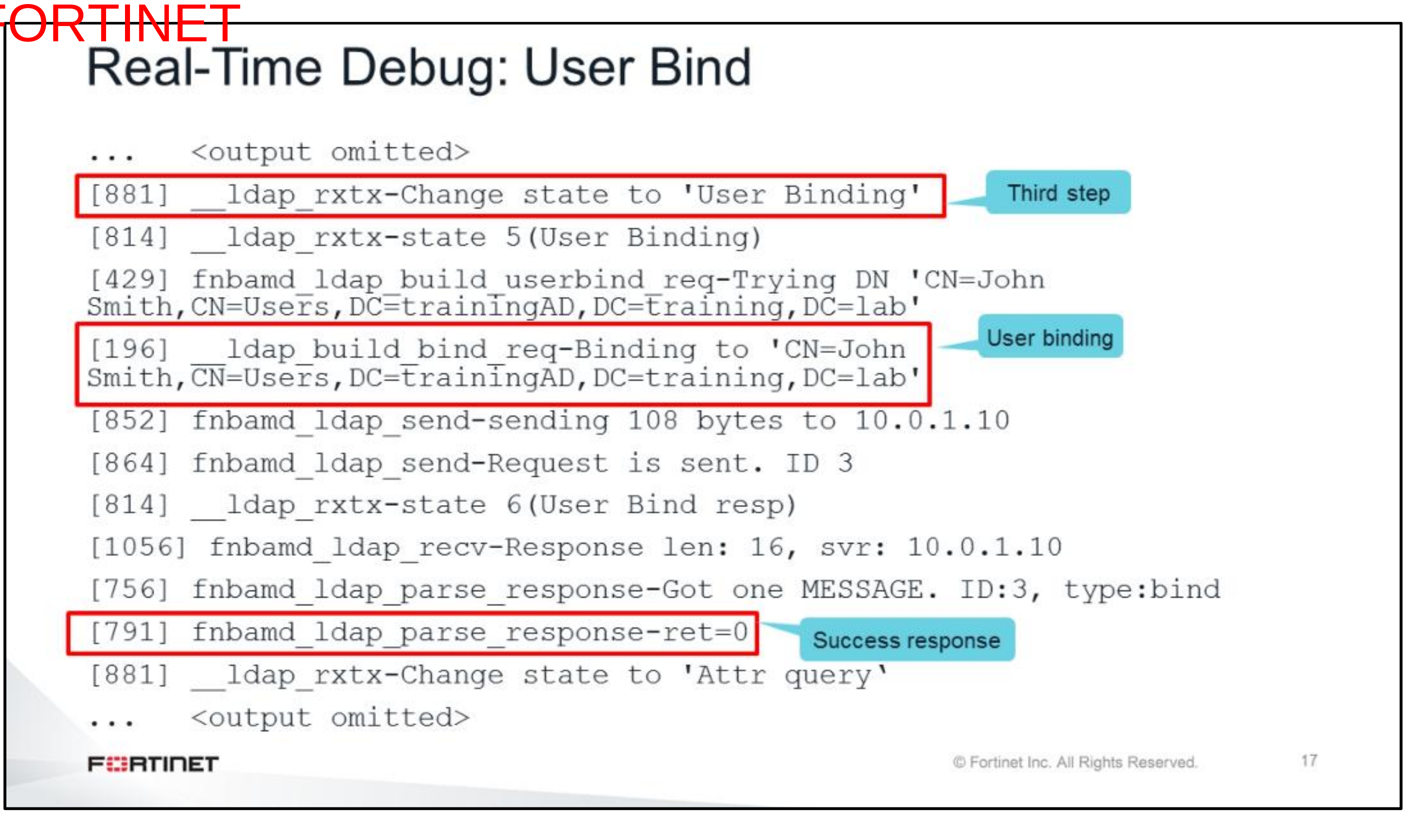
Continuing with the output, the next step for FortiOS is to perform an Admin Bind, since we are using regular bind flow for this example. This is the first step of the regular bind flow that starts with the `Admin Binding` heading. You can see that FortiOS is requesting authentication for the `administrator` 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.

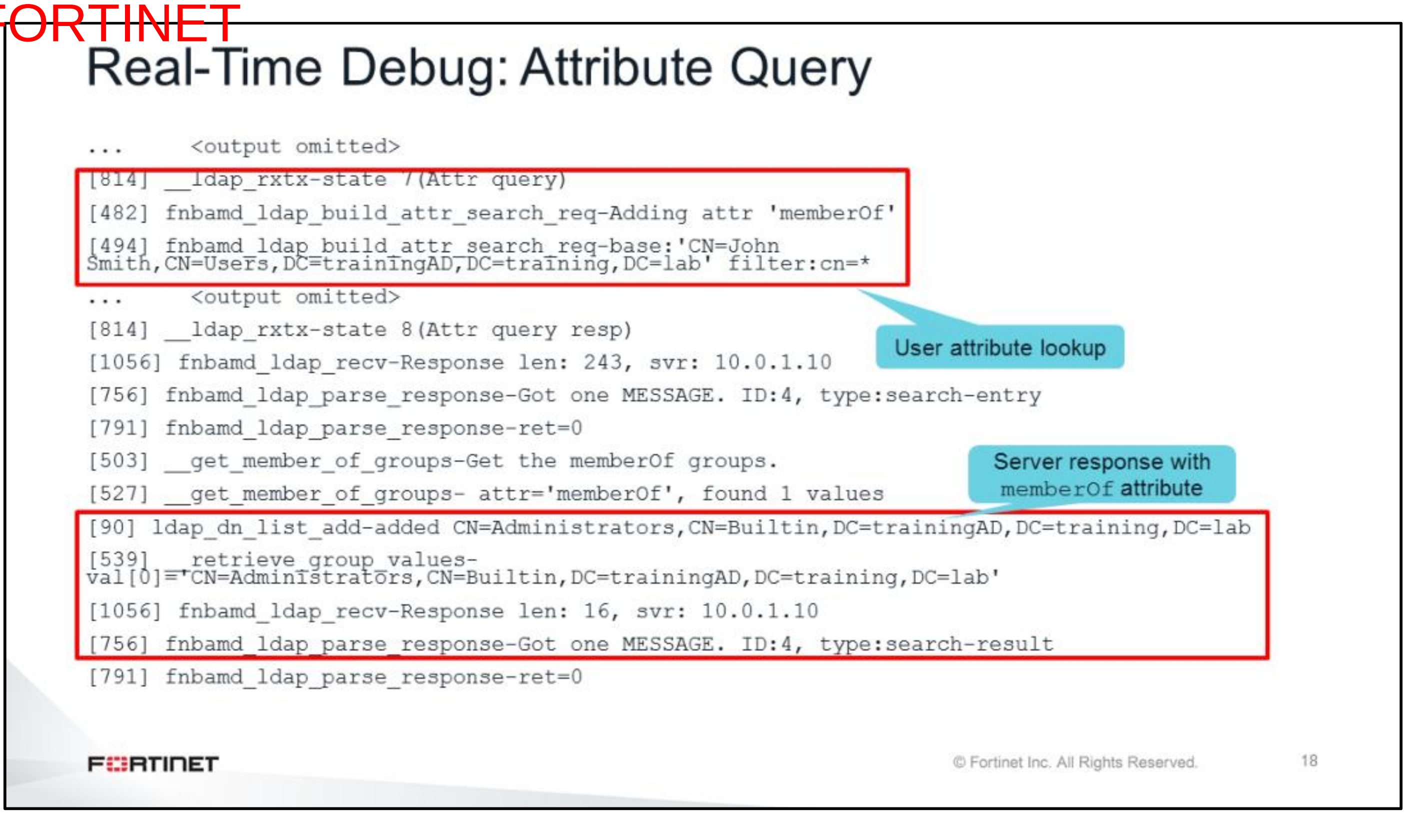


Continuing with the `fnbamd` output, this section indicates that the FortiGate is performing the second step mentioned earlier, which is searching for the user in the LDAP tree. The message includes the `base` branch (**Distinguished Name** setting) and the name of the attribute used to locate the user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

If a user is located on the LDAP server, in the `DN search resp` section the LDAP server responds back with the user DN.



`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.



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.

Real-Time Debug: Group Query

```
...      <output omitted>
[1170] __fnbamd_ldap_attr_next-Entering CHKPRIMARYGRP state
[881] __ldap_rxtx-Change state to 'Primary group query'
[814] __ldap_rxtx-state 13(Primary group query)
[518] fnbamd_ldap_build_primary_grp_search_req-starting primary group check...
...      <output omitted>
[814] __ldap_rxtx-state 14(Primary group query resp)
[1056] fnbamd_ldap_recv-Response len: 127, svr: 10.0.1.10
[756] fnbamd_ldap_parse_response-Got one MESSAGE. ID:5, type:search-entry
[791] fnbamd_ldap_parse_response-ret=0
[90] ldap_dn_list_add-added CN=Domain Users,CN=Users,DC=trainingAD,DC=training,DC=lab
[453] __get_one_group-group: CN=Domain Users,CN=Users,DC=trainingAD,DC=training,DC=lab
...      <output omitted>
[1288] __fnbamd_ldap_primary_grp_next-Auth accepted
[52] ldap_dn_list_del_all-Del CN=John Smith,CN=Users,DC=trainingAD,DC=training,DC=lab
[2859] fnbamd_ldap_result-Result for ldap svr 10.0.1.10 is SUCCESS
...      <output omitted>
```

Primary group matching

User authentication successful

 19

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 LDAP regular bind process. `SUCCESS` indicates that authentication was successful and FortiGate now has all of the required information for the authenticated user.

Sniffer for LDAP Traffic

```
# diagnose sniffer packet any "port 389" 3
```

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

FORTINET

 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.

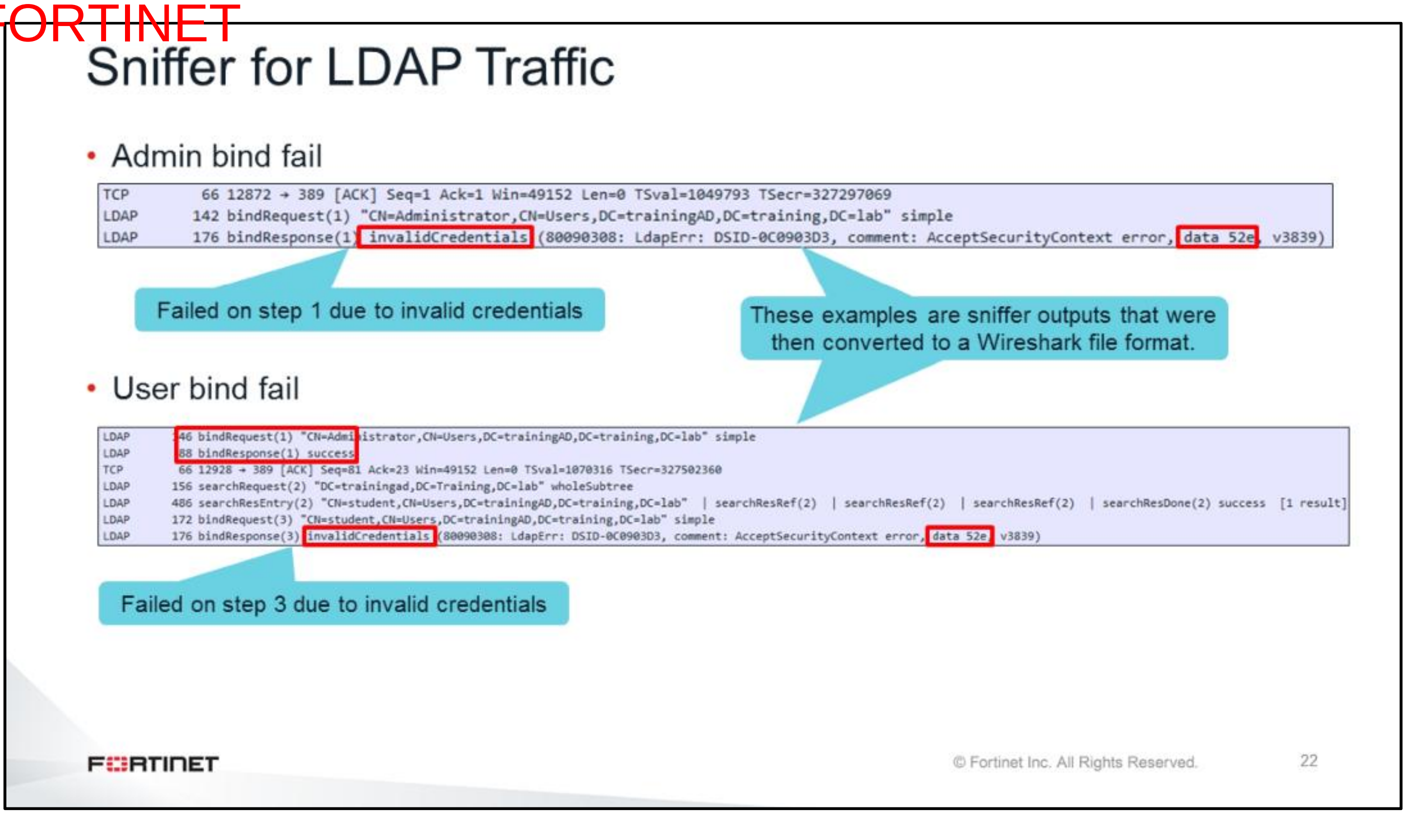
LDAP Result Codes

- Common industry-standard LDAP result codes

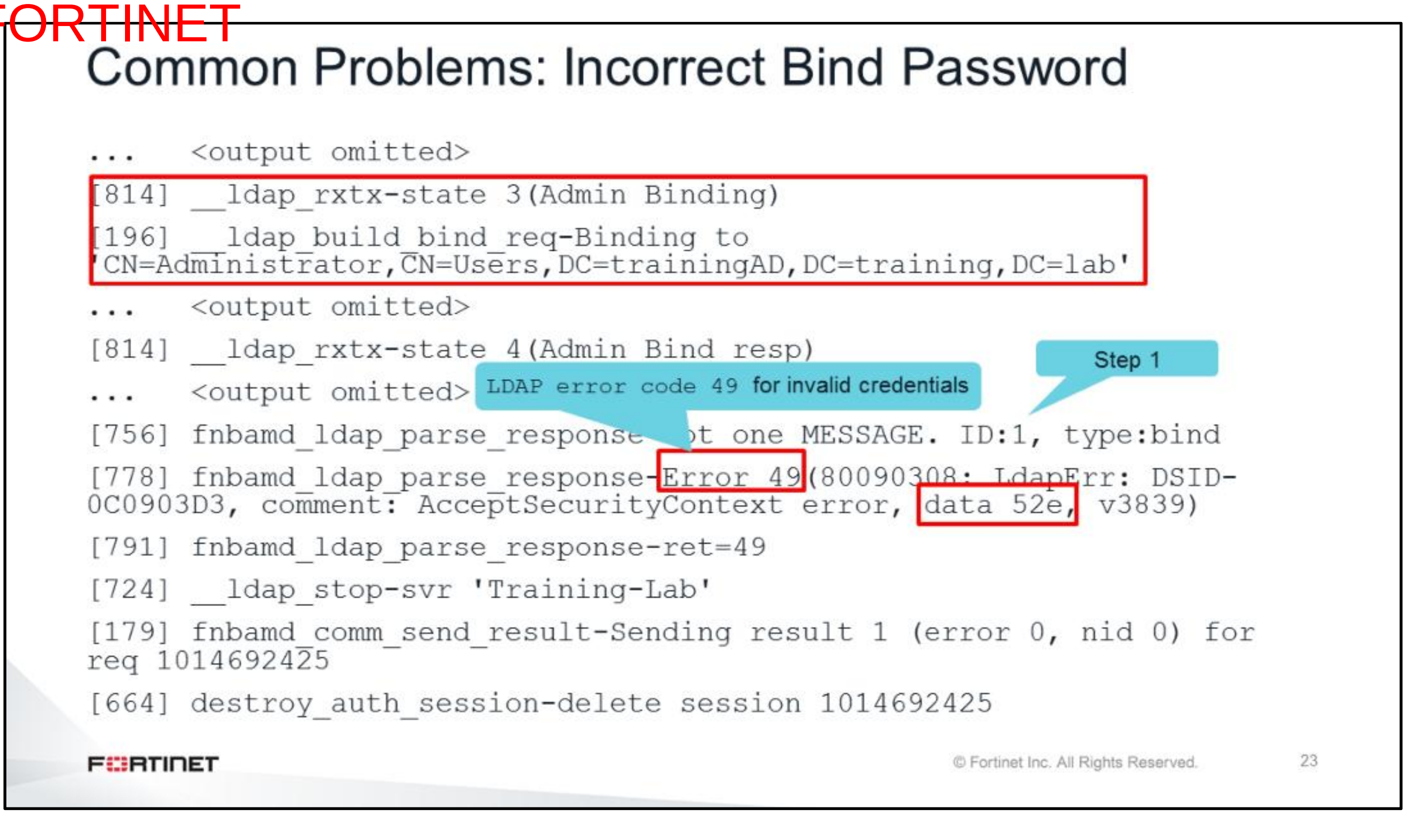
LDAP Error	Description
0	SUCCESS
2	PROTOCOL ERROR
7	AUTH METHOD NOT SUPPORTED
16	NO SUCH ATTRIBUTE
21	INVALID SYNTAX
32	NO SUCH OBJECT
34	INVALID DN SYNTAX
49	INVALID CREDENTIALS/ ACCOUNT DISABLED
50	LDAP INSUFFICIENT ACCESS

FORTINET 21

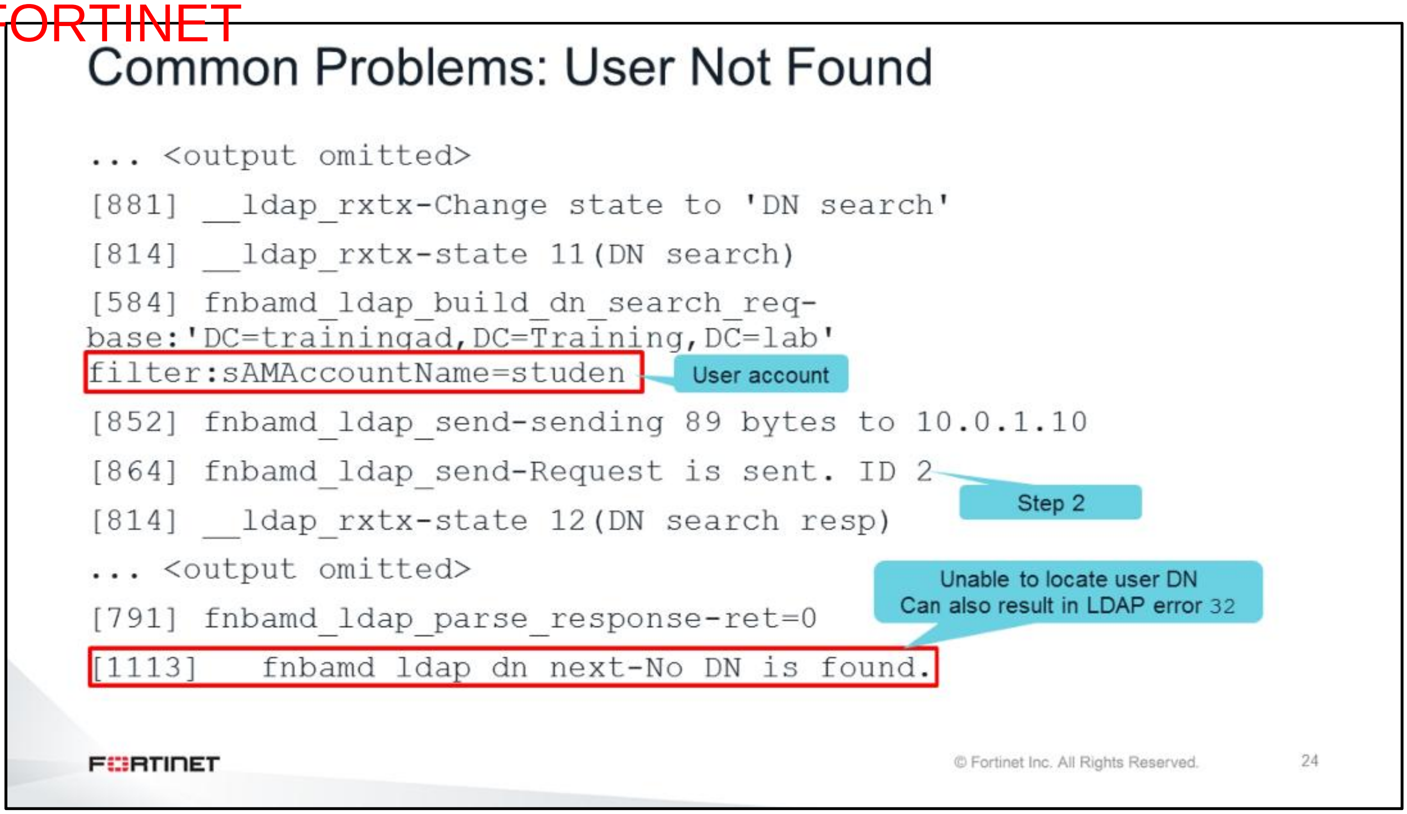
Here are a few industry-standard LDAP result codes. During LDAP authentication, the LDAP server returns a result code for both successful and unsuccessful authentication attempts, which can indicate why an authentication attempt was unsuccessful. For unsuccessful authentication requests, this error code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



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.



Real time debug for LDAP will display `error 49` for invalid credentials.



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 of the scope of the LDAP search path.

Common Problems: Incorrect User Password

```
[881] __ldap_rxtx-Change state to 'User Binding'
[814] __ldap_rxtx-state 5(User Binding)
[429] fnbamd_ldap_build_userbind_req-Trying DN
'CN=student,CN=Users,DC=trainingAD,DC=training,DC=lab'
[196] __ldap_build_bind_req-Binding to
'CN=student,CN=Users,DC=trainingAD,DC=training,DC=lab'
[852] fnbamd_ldap_send-sending 106 bytes to 10.0.1.10
[864] fnbamd_ldap_send-Request is sent. ID 3
[814] __ldap_rxtx-state 6(User Bind resp)
[1056] fnbamd_ldap_recv-Response len: 104, svr: 10.0.1.10
[756] fnbamd_ldap_parse_response-Got one MESSAGE. ID:3, type:bind
[778] fnbamd_ldap_parse_response-Error 49(80090308: LdapErr: DSID-
0C0903D3,
 comment: AcceptSecurityContext error, data 52e, v3839)
[791] fnbamd_ldap_parse_response-ret=49
```

User DN

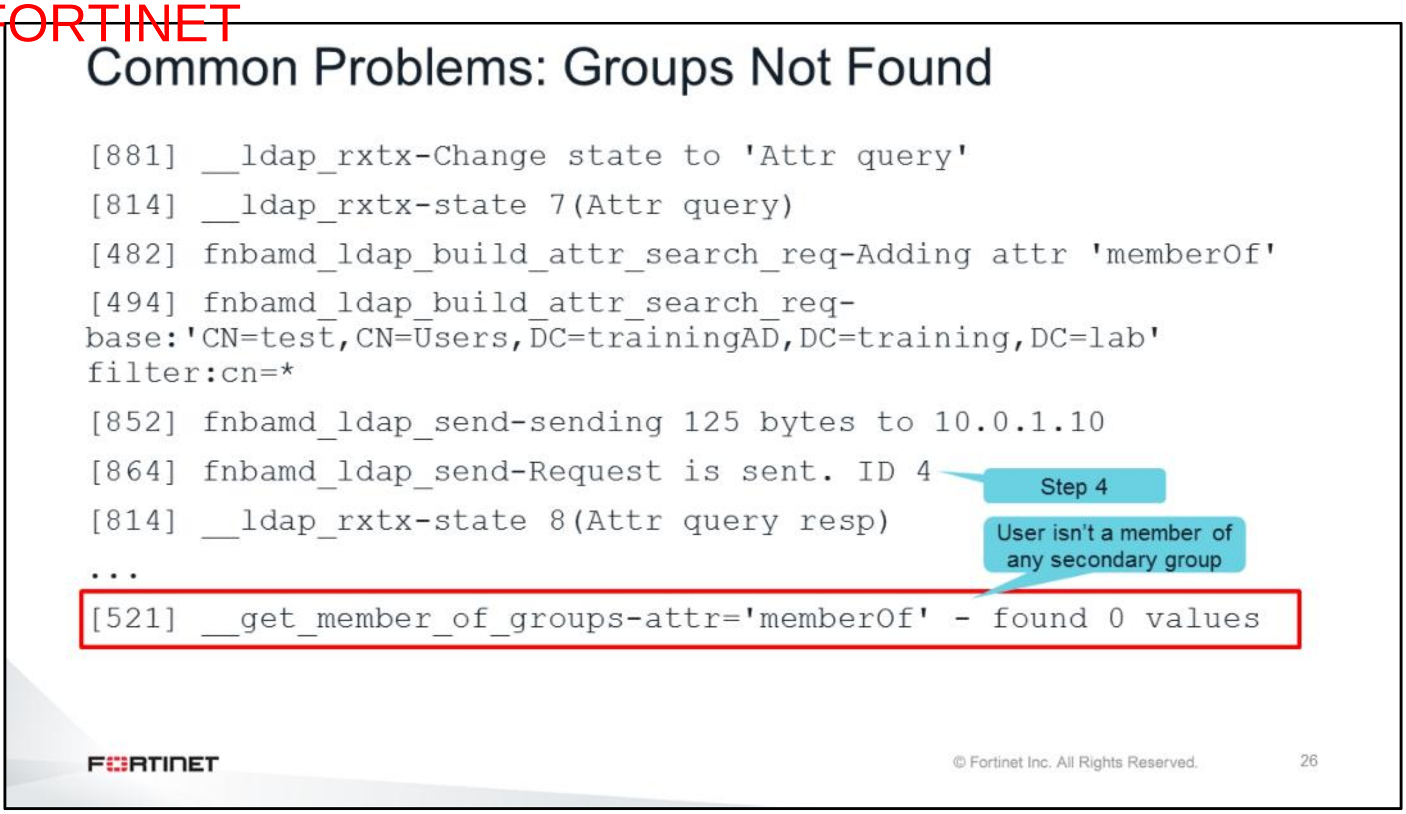
Step 3

Invalid credentials

FORTINET

 25

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

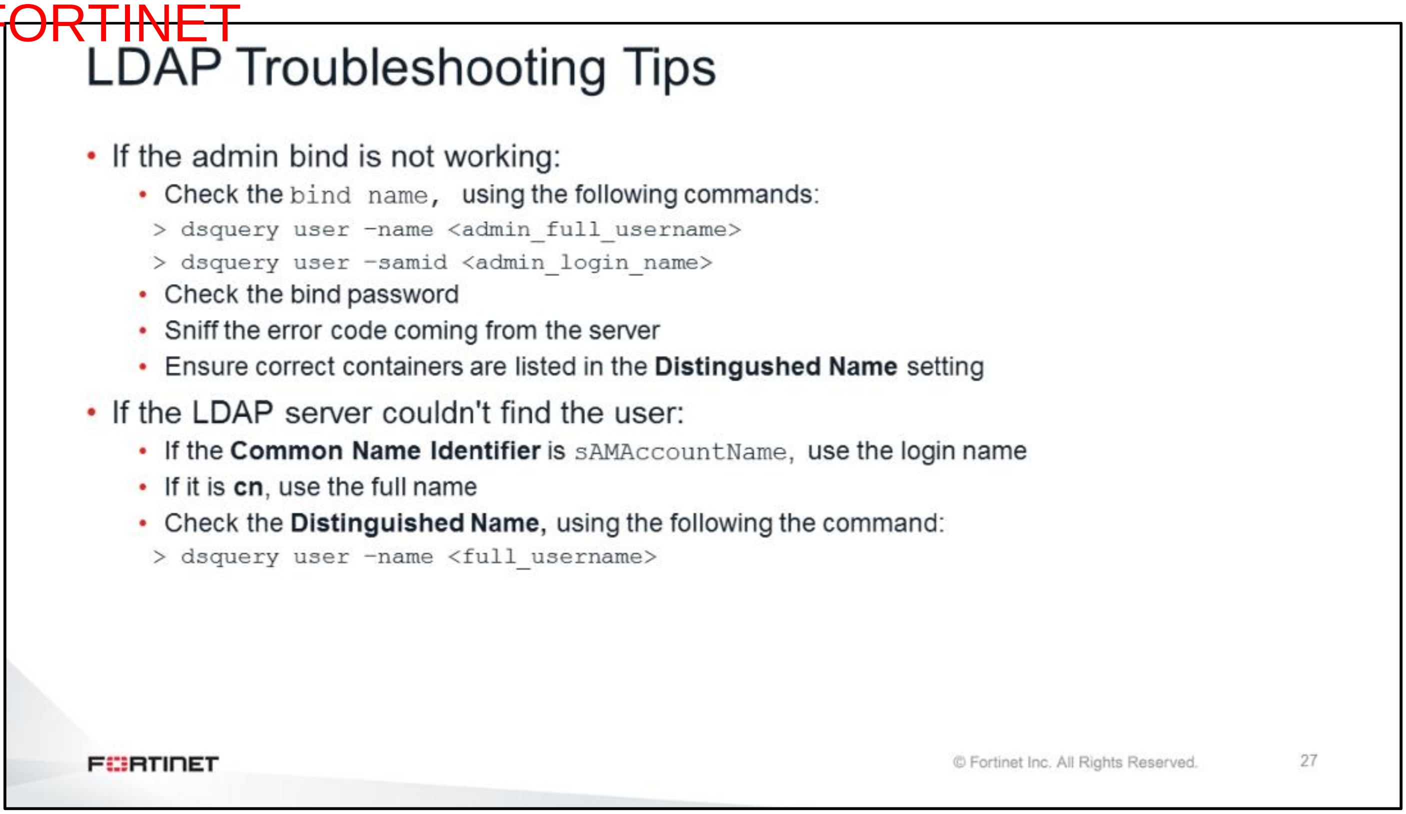


Finally, the following error indicates a problem in step 4:

```
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 about the user. There is additional configuration that will allow the FortiGate to work with these implementations, but the debug will not reflect this, in these cases. In these implementations, you can ignore this error.



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

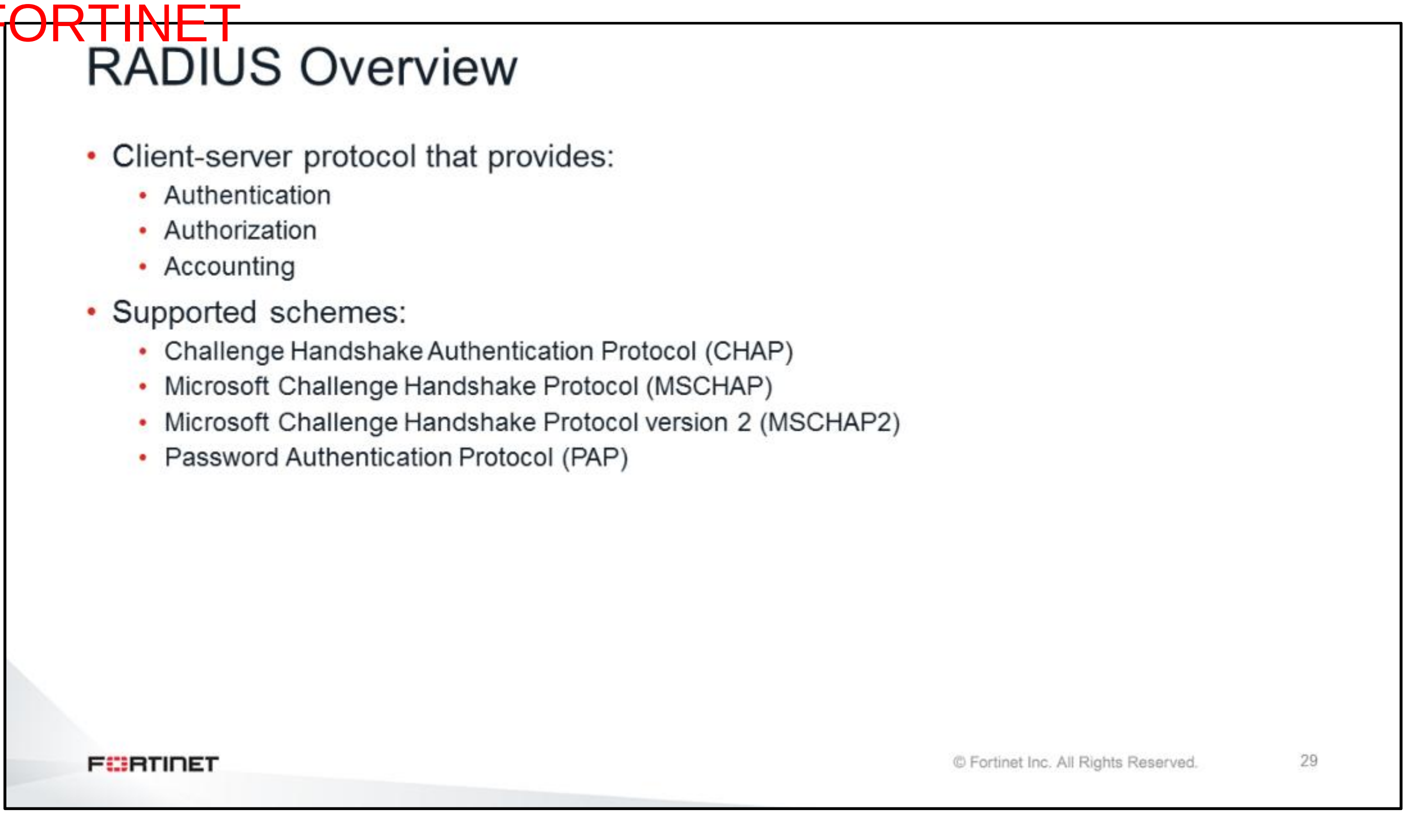
- Use the `dsquery` query to check the administrator DN
- Check the administrator password
- Sniff the error code coming from the server

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

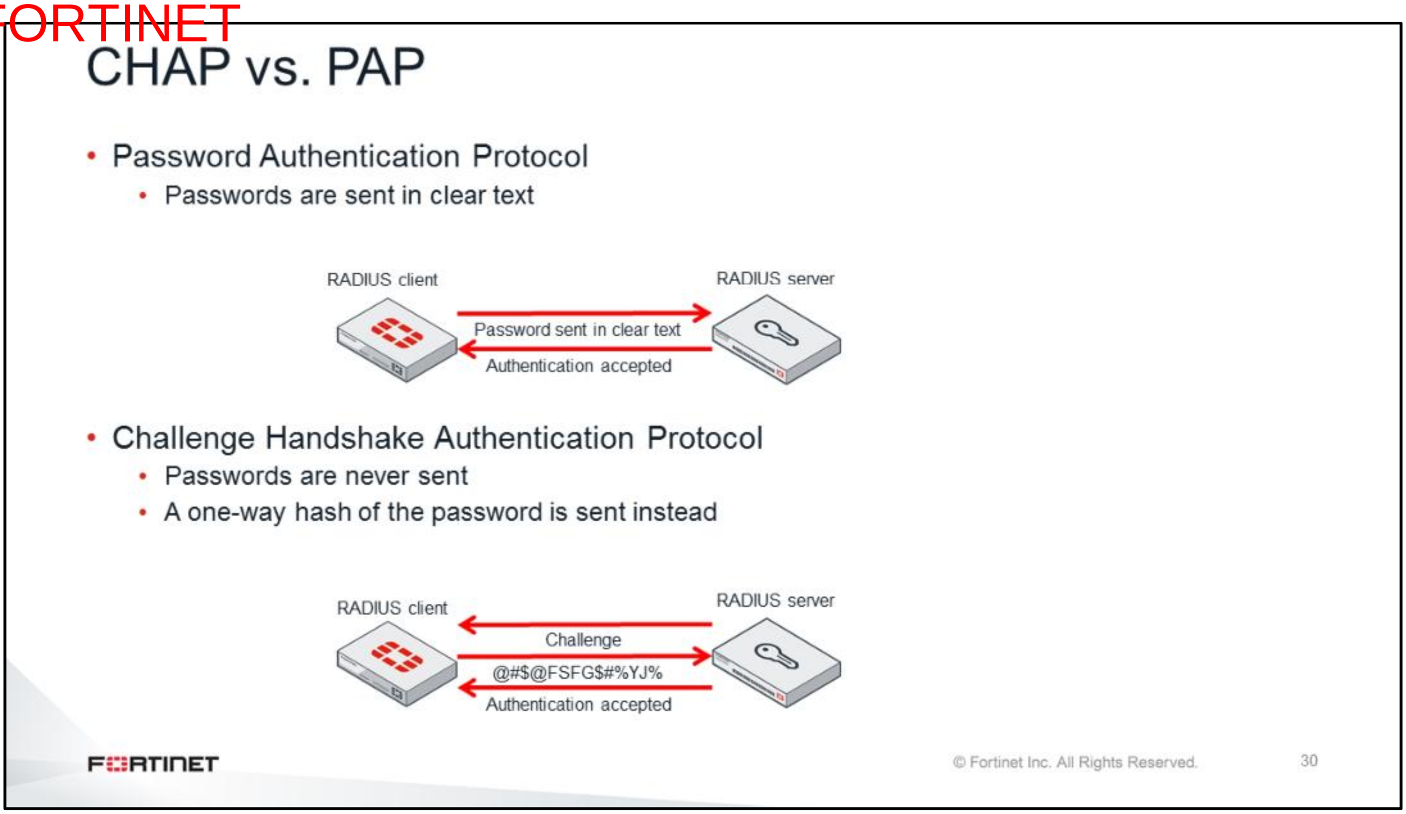
- If the **Common Name Identifier** is set to `sAMAccountName`, the user must use the login name. If it is set to `cn` instead, the user must use the full name.
- Check the **Distinguished Name** setting, using the `dsquery` command

RADIUS

In this section, you will learn about Remote Authentication Dial-In User Service (RADIUS).



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 access to the network, to 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.



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:

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

Attributes

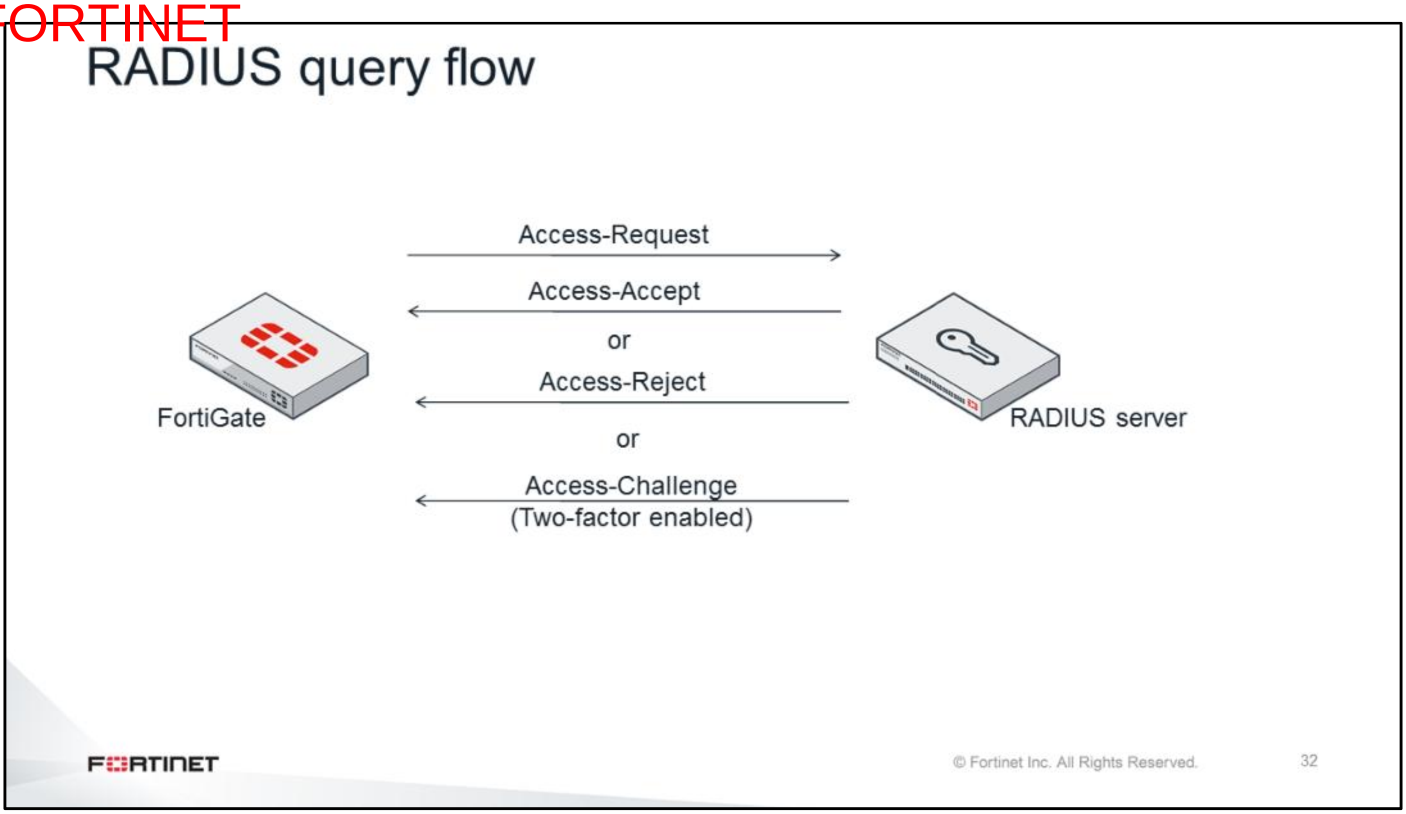
- RADIUS attributes are used to exchange information between the RADIUS server and the RADIUS client
  - RADIUS attributes in a user account provide user-related information
    - Can be used to assign an IP address to a user
  - RADIUS attributes in a user group can provide general information that will be applicable to the whole group
    - Can be used to apply a security profile to multiple users within a specified user group
- Vendor-specific attributes
  - Used by vendors to extend the basic functionality of RADIUS
  - Requires VSA dictionaries, which are supplied by the vendors
  - Fortinet RADIUS vendor ID is 12356

FORTINET

 31

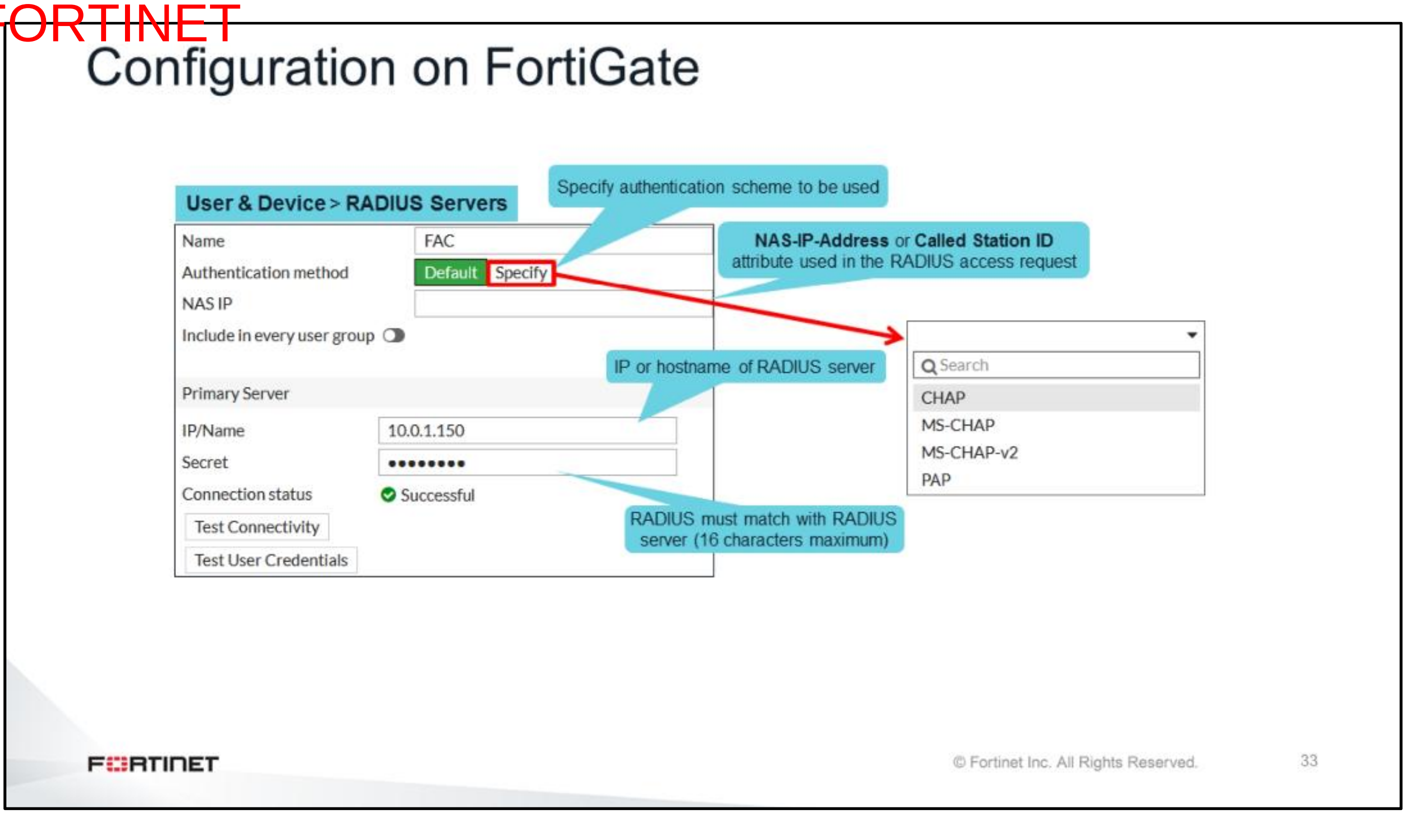
RADIUS attributes can be used to provide information about a user or a user group. RADIUS attributes configured at a user level can provide user-related information, such as IP addresses. Attributes configured at the user-group level are used to provide information that will be applied to the all users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

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



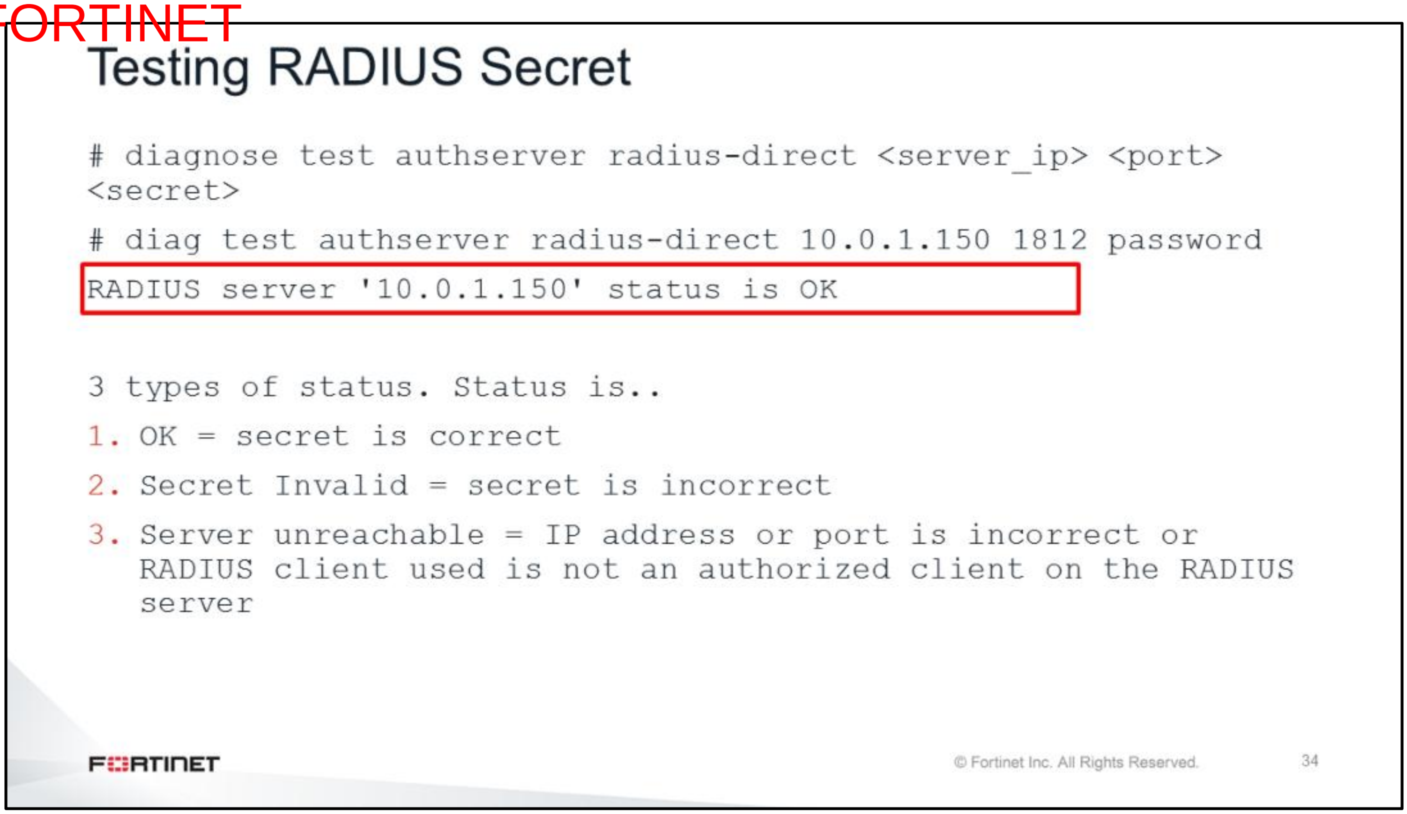
Normal authentication queries with the RADIUS protocol begin with an "Access-Request" being sent from the FortiGate to the RADIUS server. Valid responses to this are "Access-Accept" and "Access-Reject" (yes and no, respectively).

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



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 will try the different authentication schemes, starting with MSCHAP2, CHAP and 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.

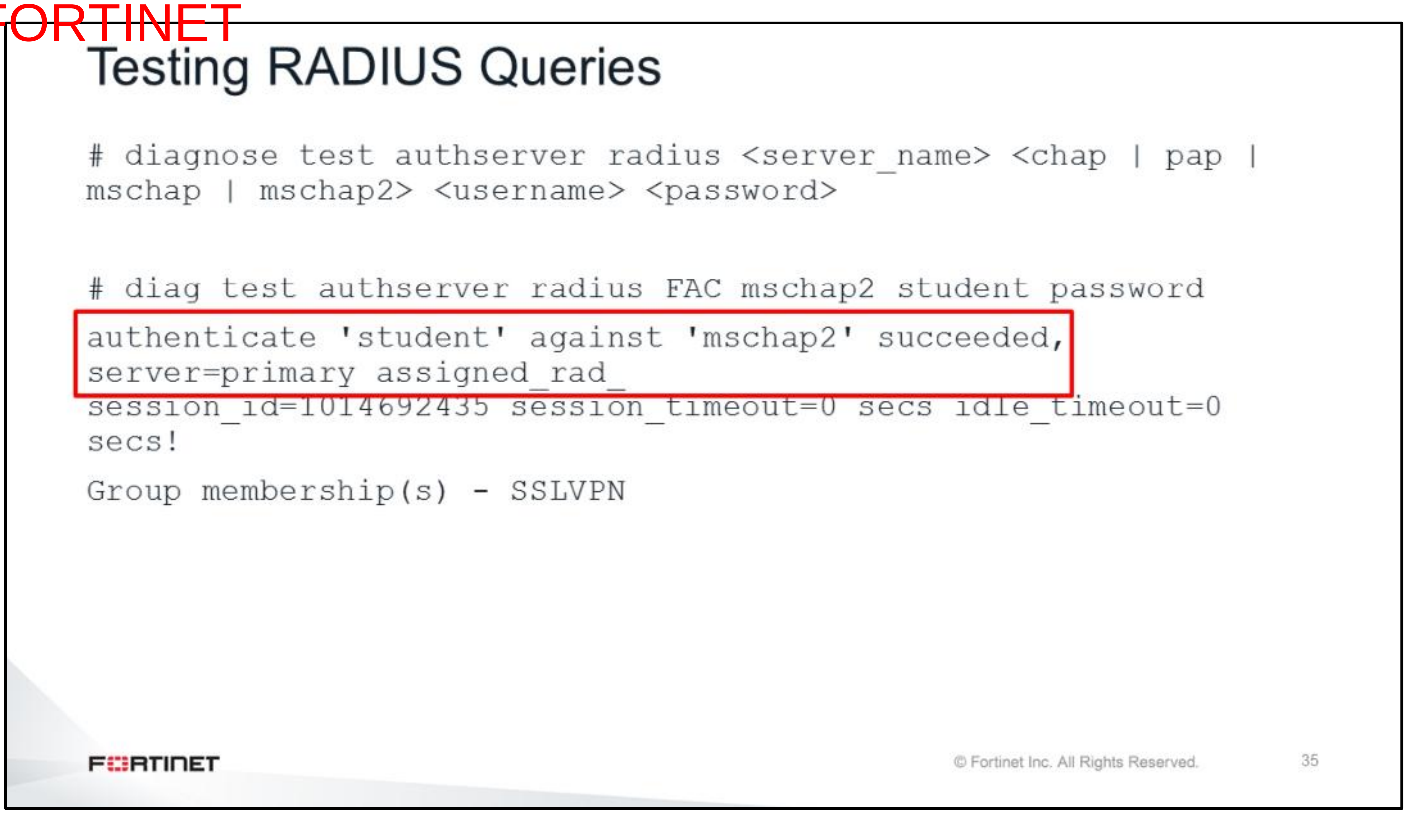
Note: MSCHAP is never used when the authentication method is set to **Default**. If you want to use only MSCHAP as the authentication method scheme, you must specify MSCHAP manually.



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

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

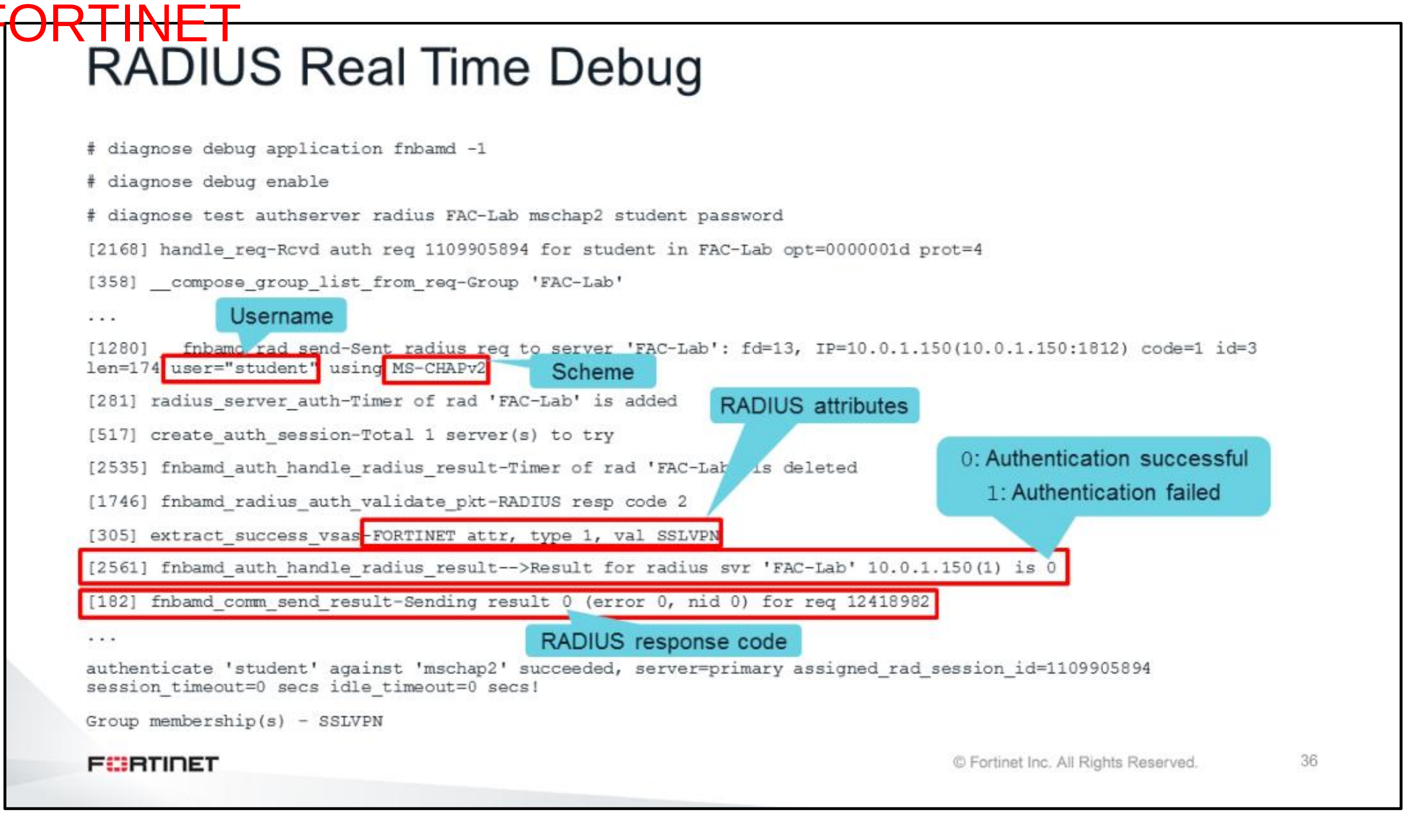
The RADIUS client is the FortiGate here. There are two possible replies that you can see in the output, as listed on the slide. It is important to note that `Secret Invalid` is only displayed if the RADIUS client is an authorized client on the RADIUS server. If the RADIUS client is not authorized on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



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

When you used 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.



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, as defined on FortiGate
- 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
- RADIUS response code provides more detail as to why the authentication was successful or unsuccessful

RADIUS Response Code

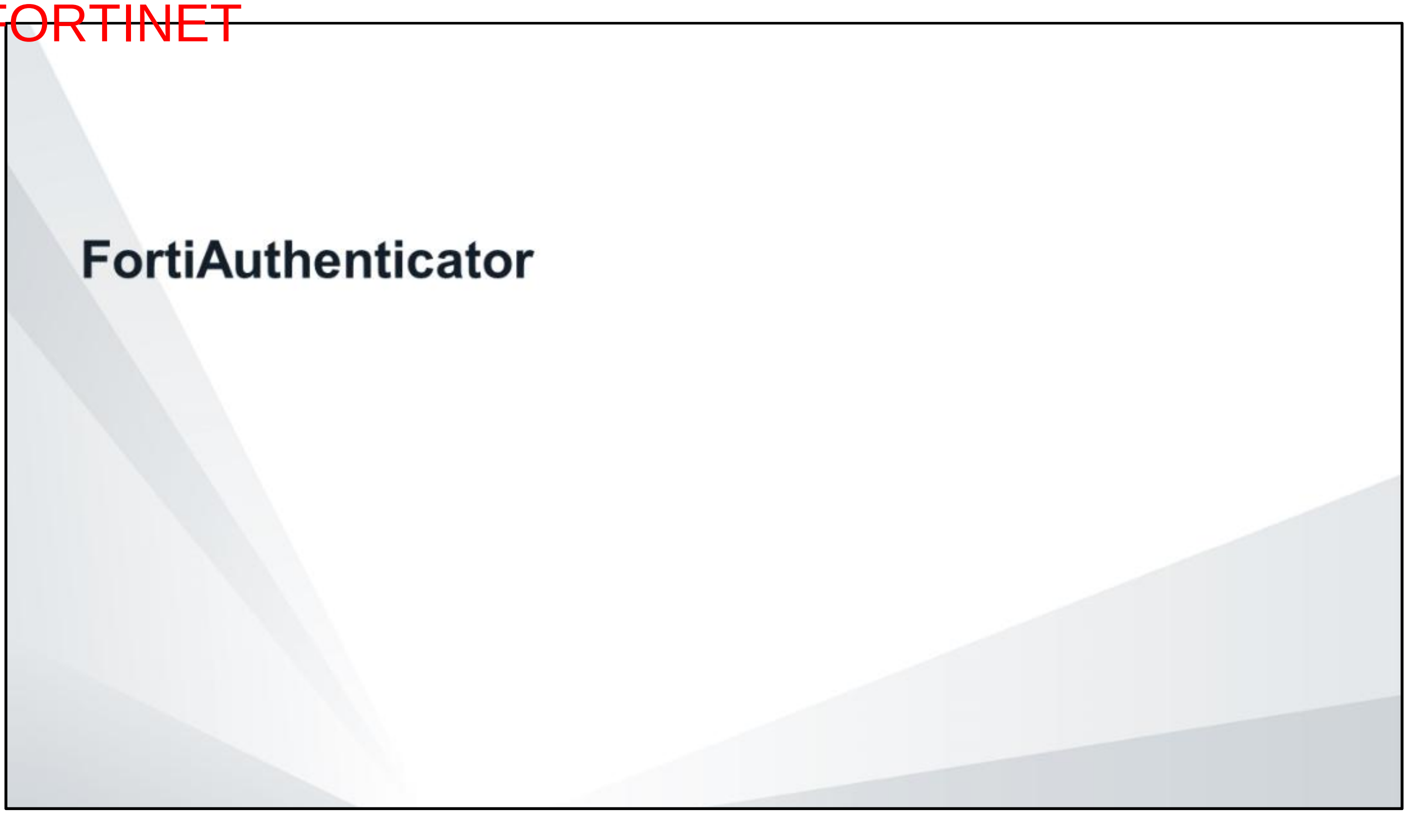
RADIUS response code	Description
0	Success
1	Deny
2	Challenged (for password renewal or remote token)
3	Unknown
4	Pending
5	Error
6	Framed IP Conflict
7	Token code is required
8	Need next token is required due to token out of sync
9	Response buffer is too small
10	Authentication times out
11	Max concurrent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

Most common ones

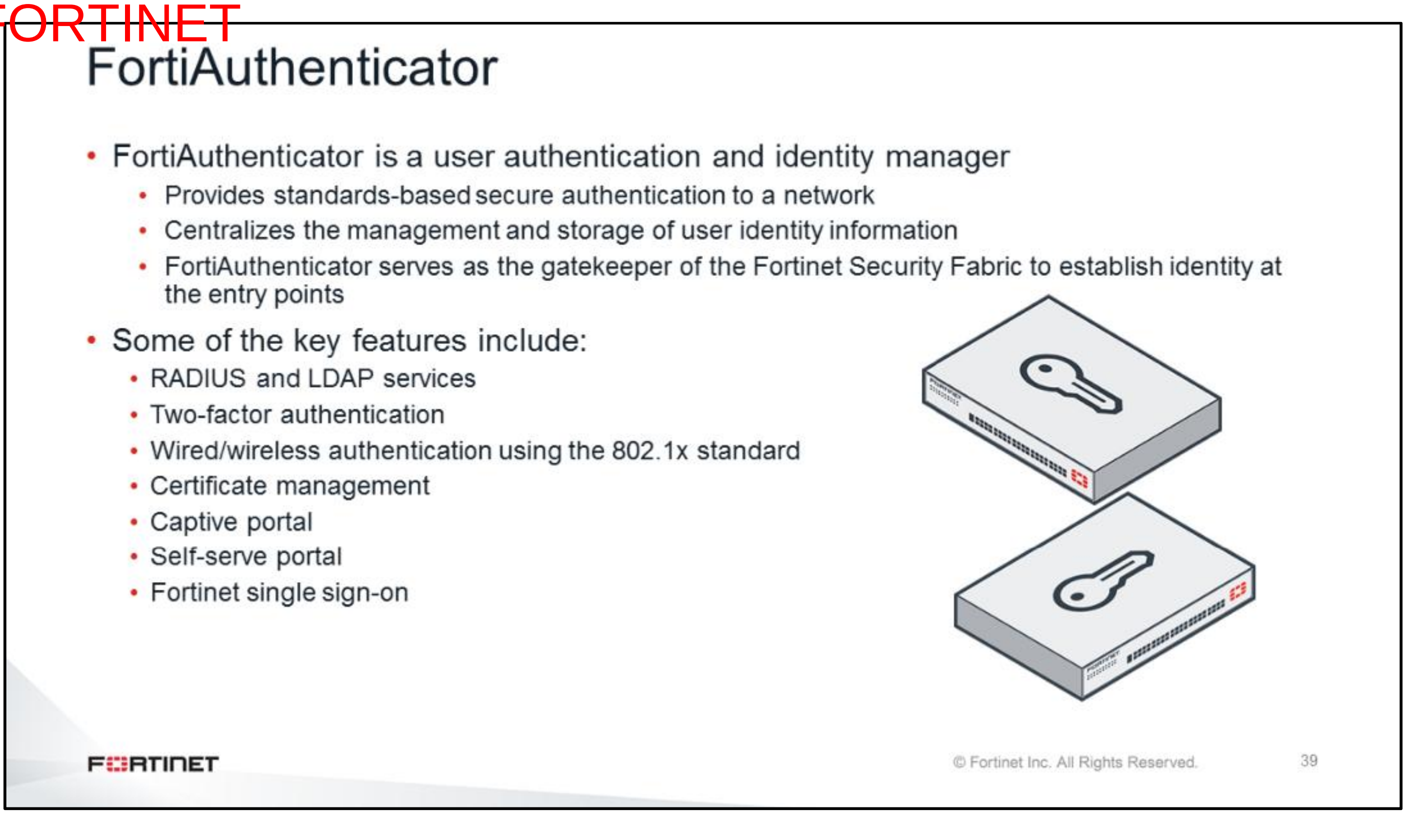
FORTINET

37

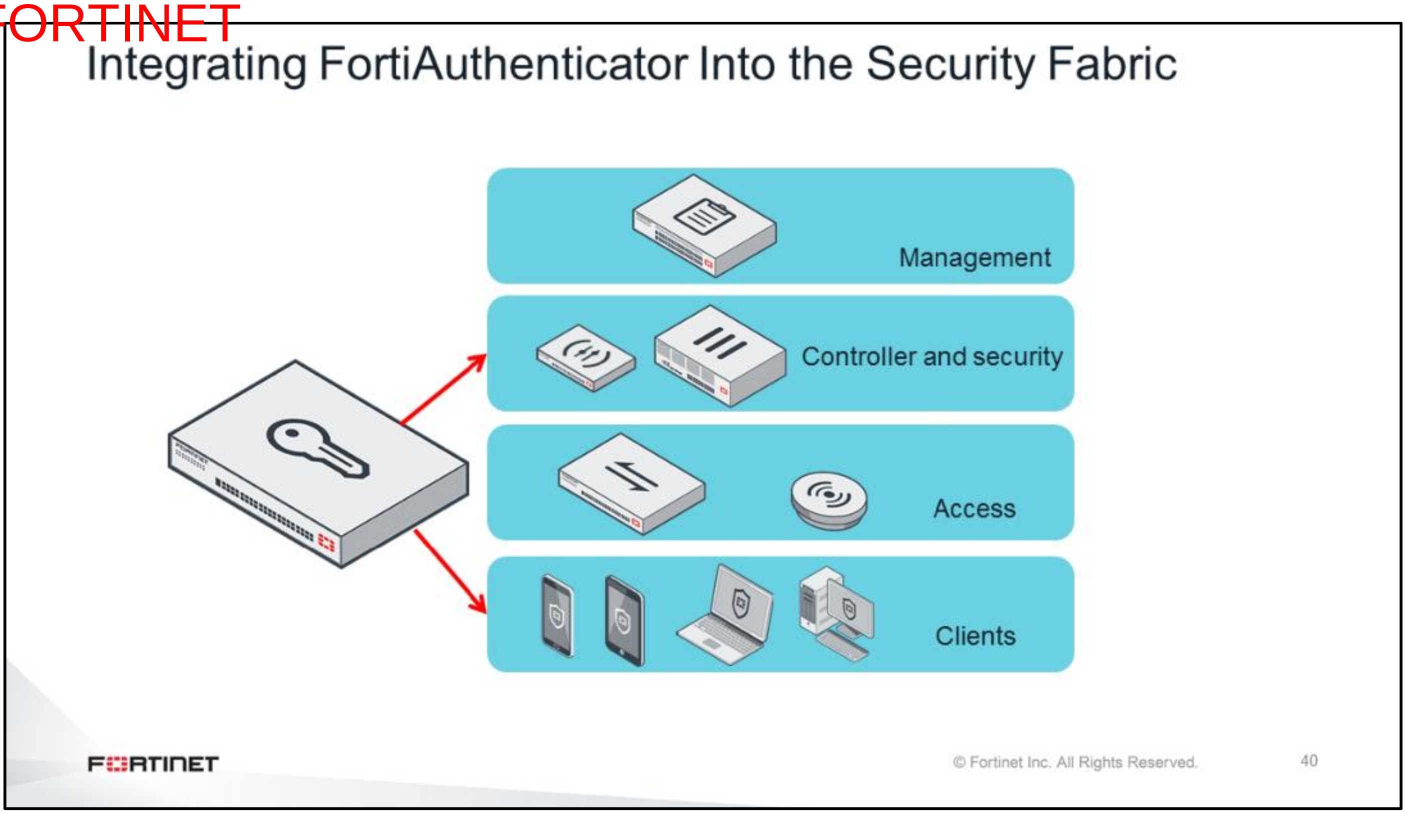
Here is the full list of RADIUS response codes that you can receive from the RADIUS server. These codes can help you find the root cause of authentication issues.



In this section, you will learn about FortiAuthenticator basics.



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 FortiGates and third-party devices. Together, FortiAuthenticator and FortiToken deliver cost-effective, scalable, secure authentication to your entire network infrastructure.



FortiAuthenticator is a key component in the Fortinet secure access 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.

FortiAuthenticator Key Differences

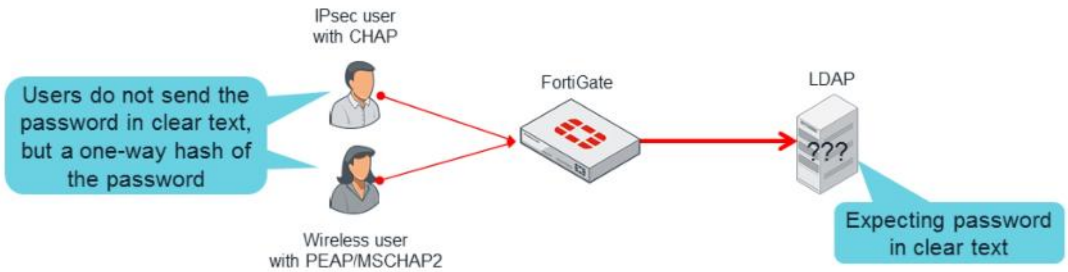
Features	Key differences compared to FortiGate
RADIUS	RADIUS authentication and authorization server RADIUS authentication and accounting proxy Rule-based rewrite of RADIUS accounting packets for FSSO
2FA	Centralized 2FA for users and tokens
FSSO	Restrict number of devices per FSSO user FSSO user/group/IP 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

 41

This list shown on the 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.

The CHAP and LDAP Dilemma

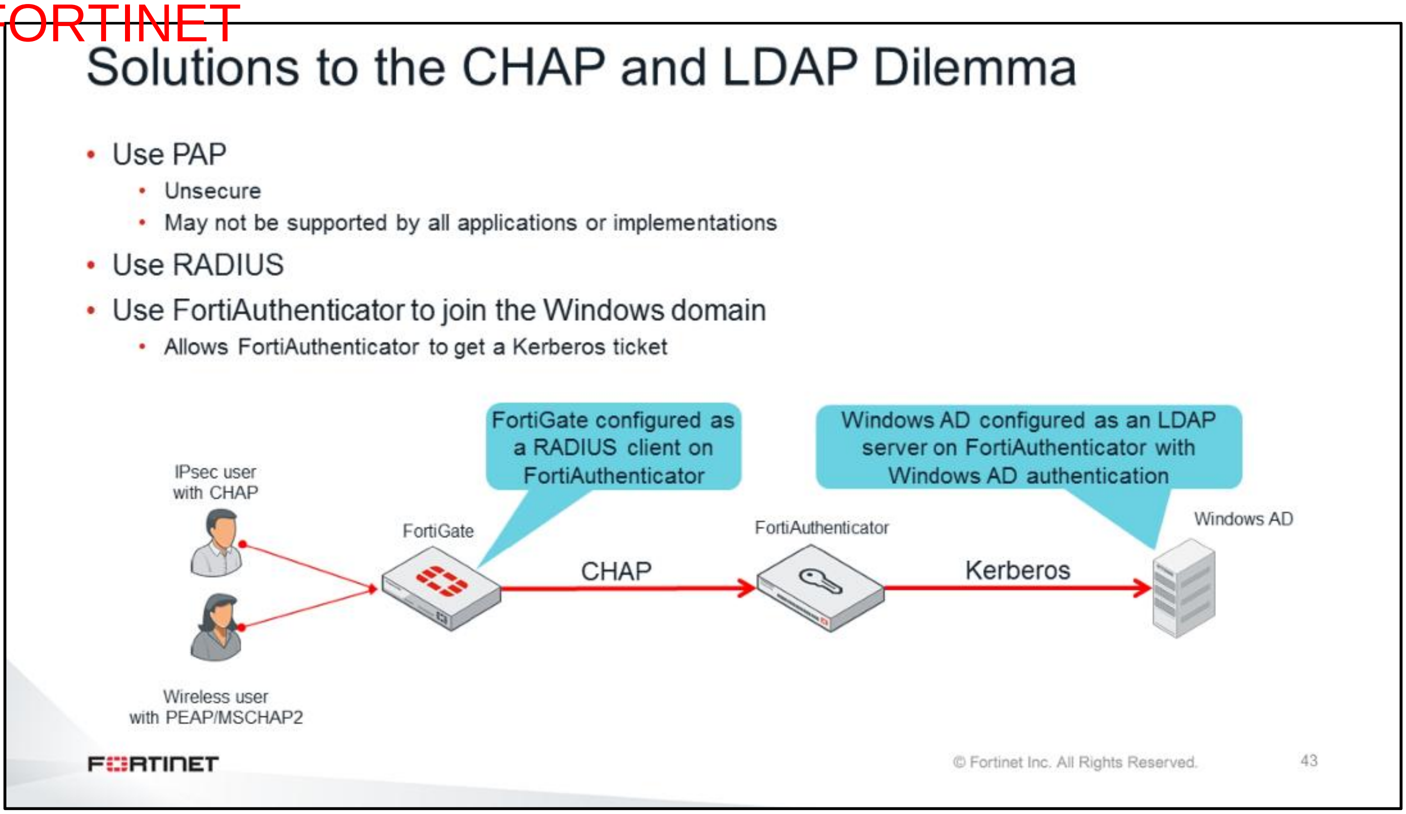
- If FortiGate uses LDAP for user authentication, neither CHAP, nor MSCHAP2 can be used
  - This might affect IPsec VPN and PEAP wireless users



Now, you will explore another benefit of adding FortiAuthenticator to your secure access solution.

If FortiGate is configured to authenticate clients using a remote LDAP server, VPN and wireless clients using CHAP schemas will not be able to authenticate. That is the case for wireless clients using PEAP/MSCHAP2 and IPsec VPN clients with extended authentication (XAuth) and CHAP.

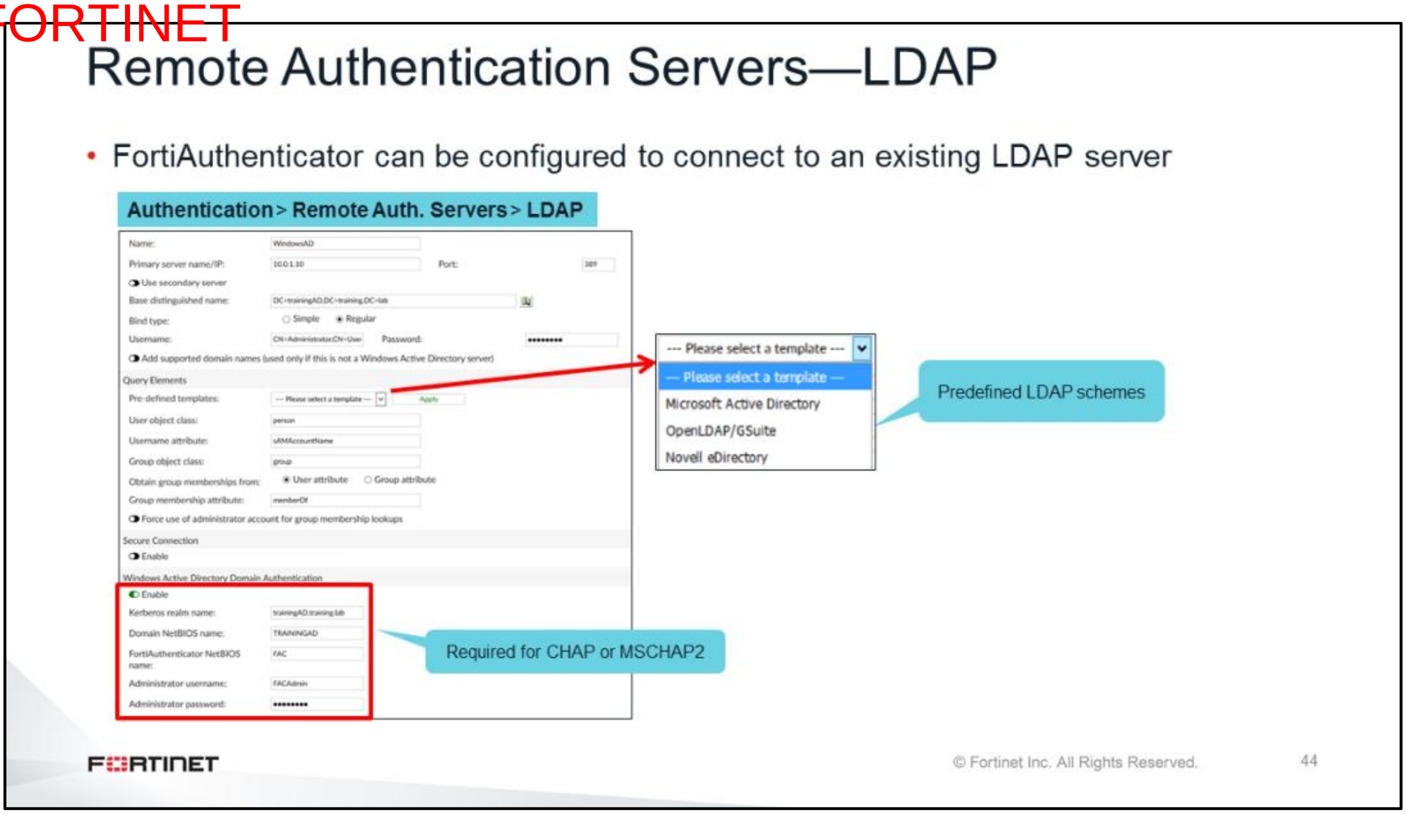
The reason is that during CHAP authentication, a client sends a one-way hash of the password. However, the LDAP server, which is on the backend, is expecting the password itself. The FortiGate, which is acting as the LDAP client, does not have the client passwords, and it also can't convert a hashed password to a clear text password.



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 due to the nature of the PAP protocol.
- Use RADIUS: Change your backend 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. The FortiAuthenticator would be located between FortiGate and the Windows server. You will also need to configure FortiAuthenticator to log in to the Windows domain using the credentials of a Windows administrator. This will add 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 Kerberos.



A FortiAuthenticator can store the user database locally. It can also proxy authentication requests from a client to a backend authentication server.

This is 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** will set the root node where LDAP will start searching for user accounts.

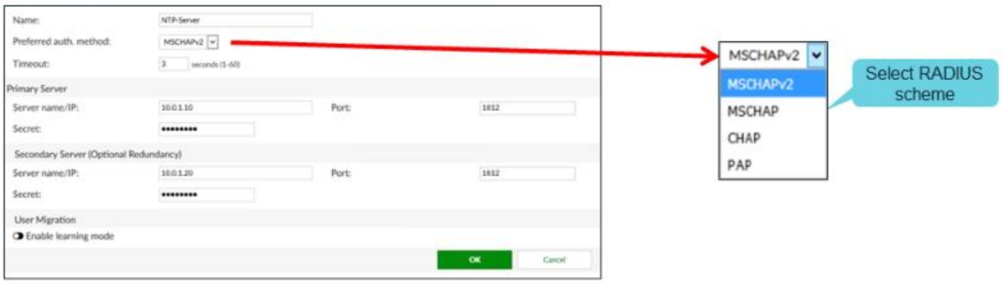
There are predefined LDAP templates. They include default attribute settings for well-known LDAP servers, such as Windows AD, OpenLDAP, and Novell eDirectory.

If you want FortiAuthenticator to relay CHAP authentication to a Windows AD server, you must enable **Windows Active Directory Domain Authentication**, and enter the credentials for a Windows administrator. The FortiAuthenticator will log in to the domain as a trusted device, allowing FortiAuthenticator to proxy CHAP authentications, using Kerberos.

RADIUS Remote Authentication Server

- FortiAuthenticator can be configured to connect to existing RADIUS servers
  - If the local user database is not used, FortiAuthenticator will proxy RADIUS authentication requests

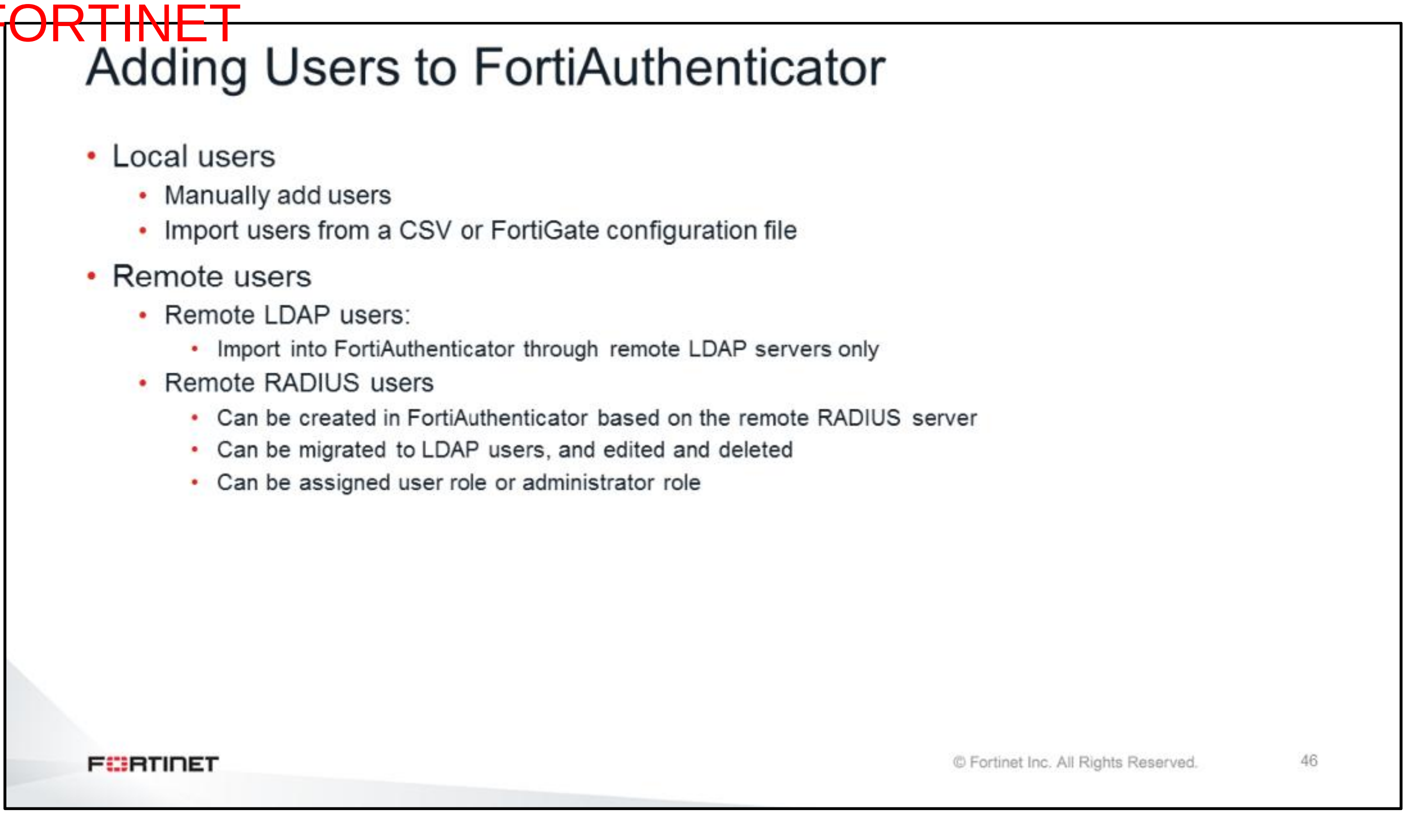
Authentication > Remote Auth. Servers > RADIUS



FORTINET

 45

This is a sample of the configuration required for FortiAuthenticator to proxy authentication requests to a remote RADIUS server.



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

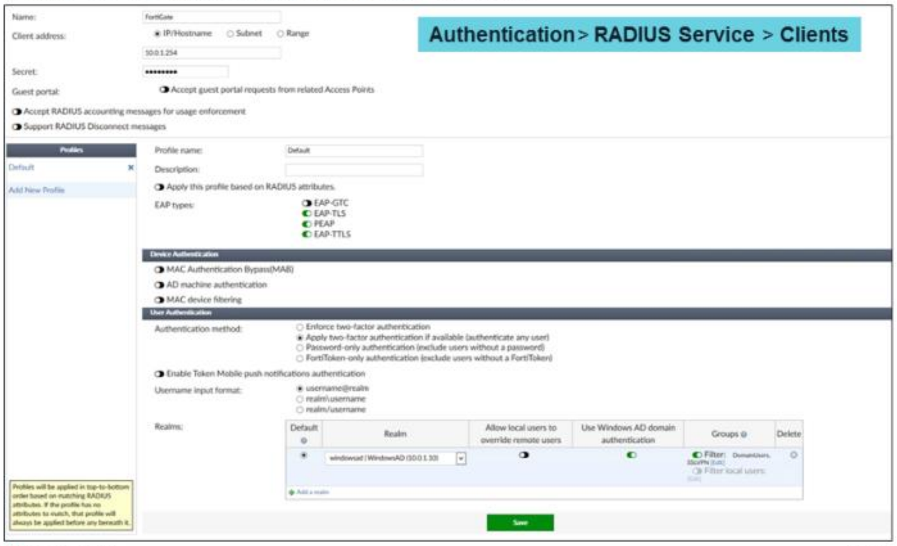
Note that FortiAuthenticator includes a self-service portal where users can register themselves.

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.

RADIUS Clients

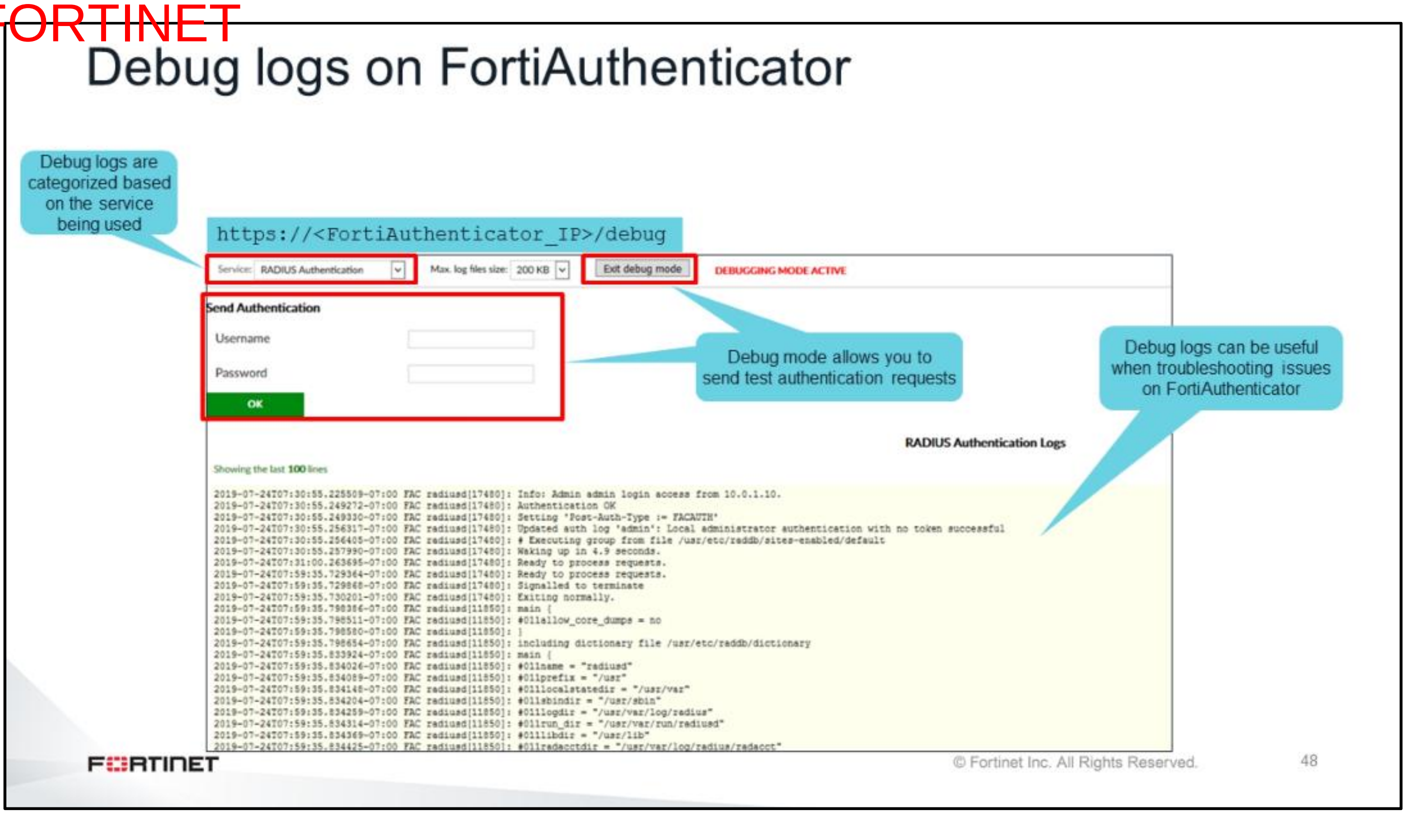
- FortiAuthenticator will accept RADIUS authentication requests only from clients that have been added as RADIUS clients



 47

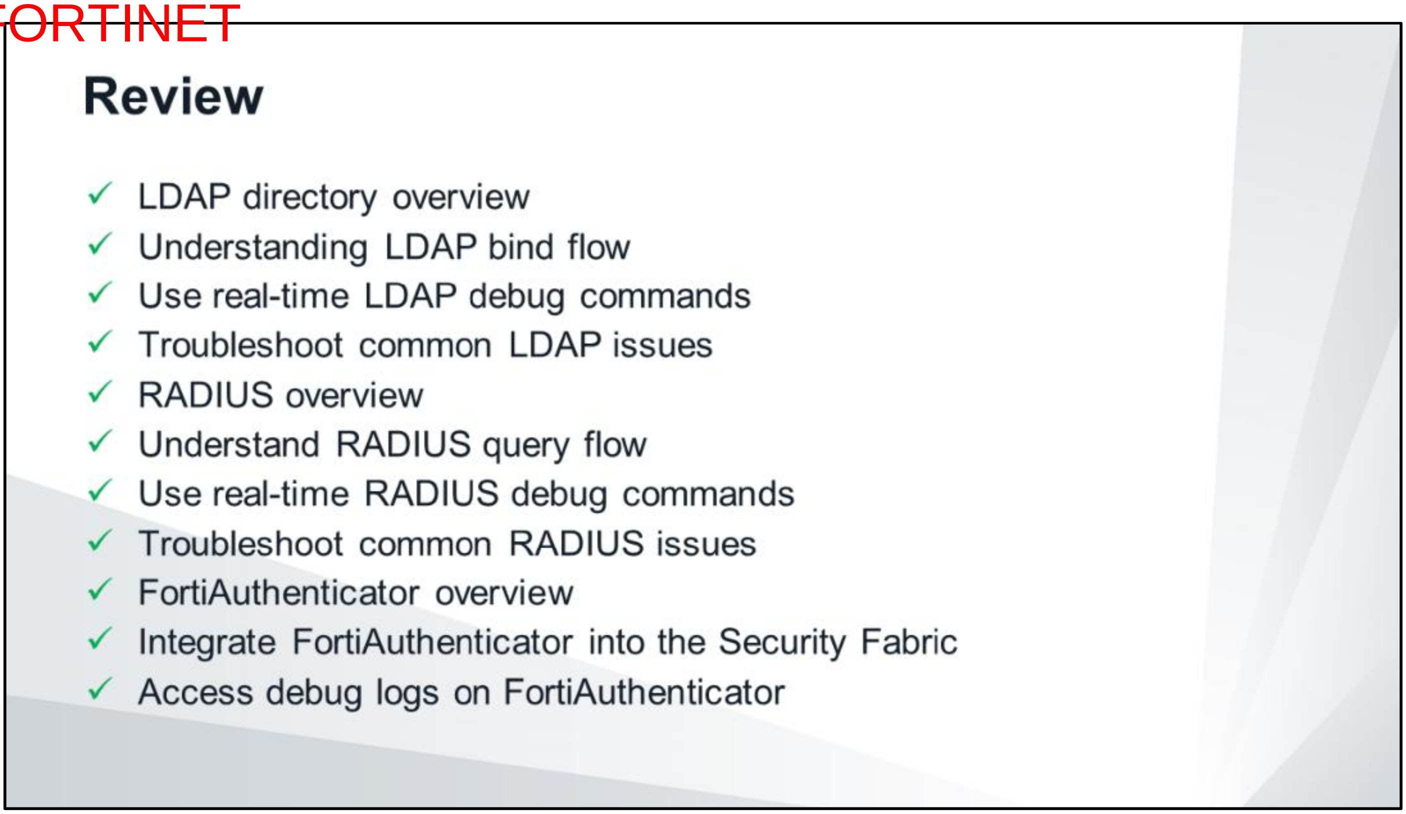
FortiAuthenticator will accept RADIUS authentication requests only from approved RADIUS clients. After you configure remote authentication servers or a local user database, you must allow FortiGate to make authentication requests to FortiAuthenticator. This is done under RADIUS clients on the FortiAuthenticator.

This is where you define the type of authentication requests that will be processed, and options that FortiAuthenticator would apply to the RADIUS client.

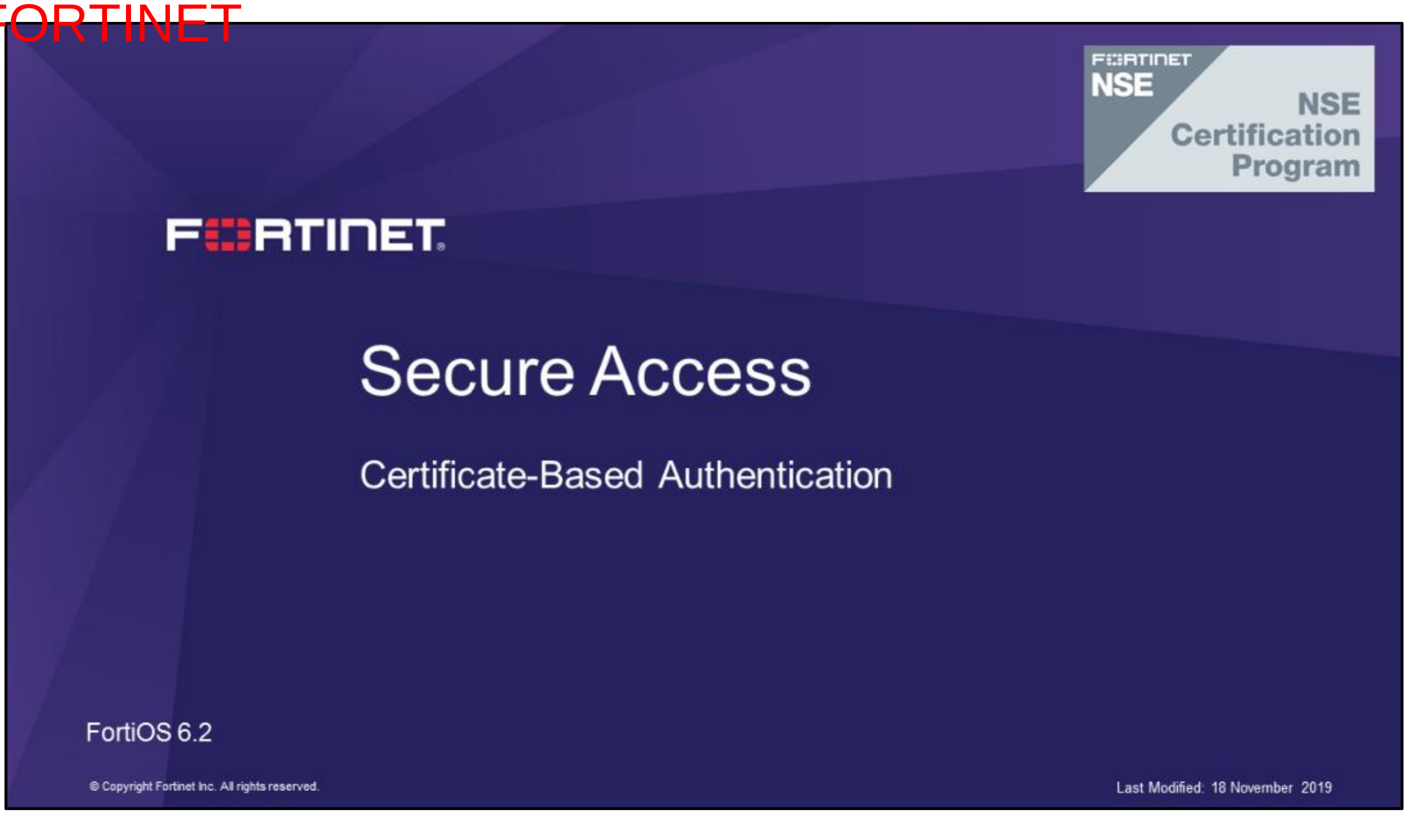


Unlike FortiGate, FortiAuthenticator does not have real-time debug commands. Instead, you can access extended logs for individual services. You can access the debug log page using the URL at `https://<FortiAuthenticator_IP>/debug`. These logs can be used to troubleshoot issues with services running on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

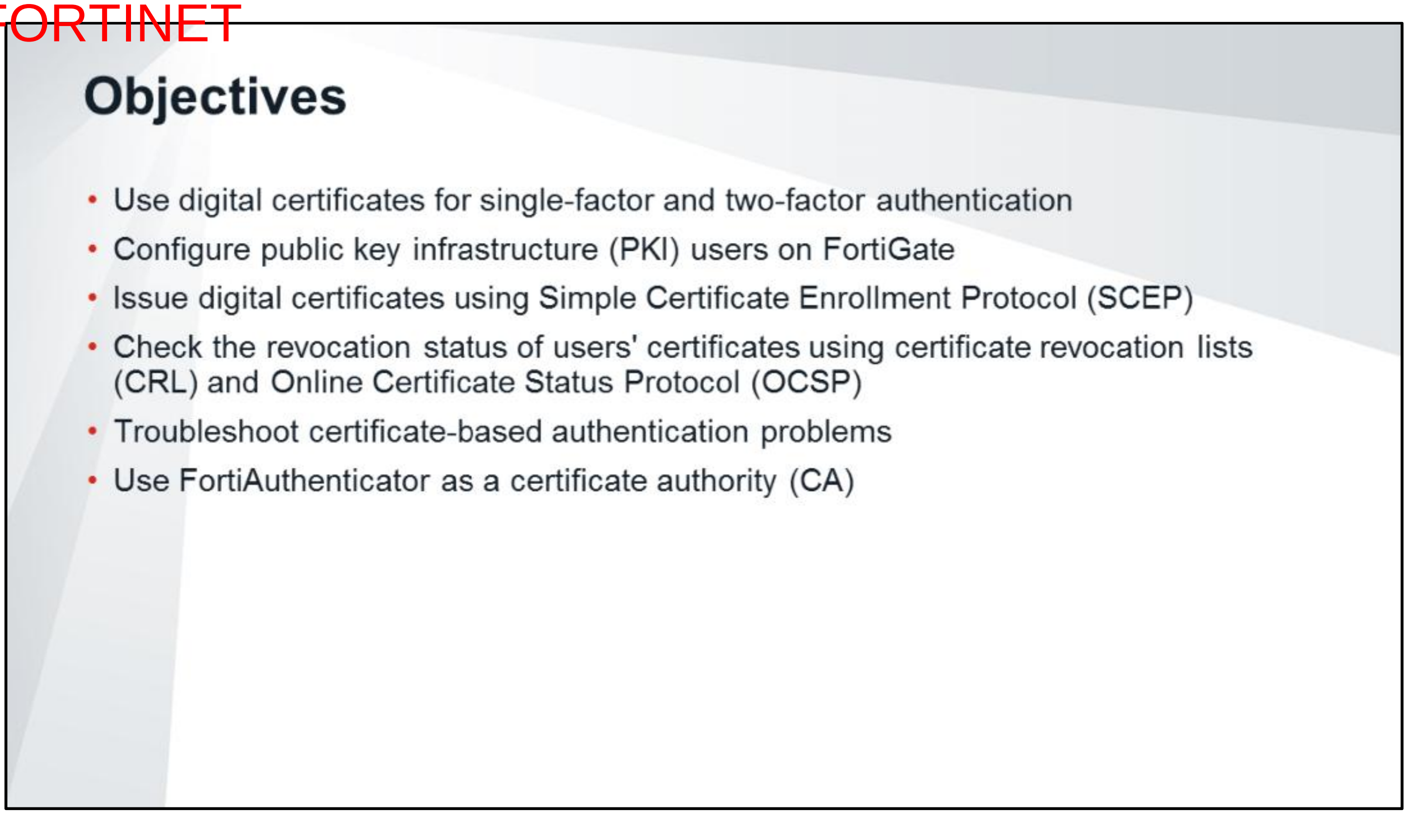
In the case of the debug logs for RADIUS authentication, there is the option of enabling **debug mode**, which allows administrators to test RADIUS authentication using the credentials of a test user from the debug logs window.



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



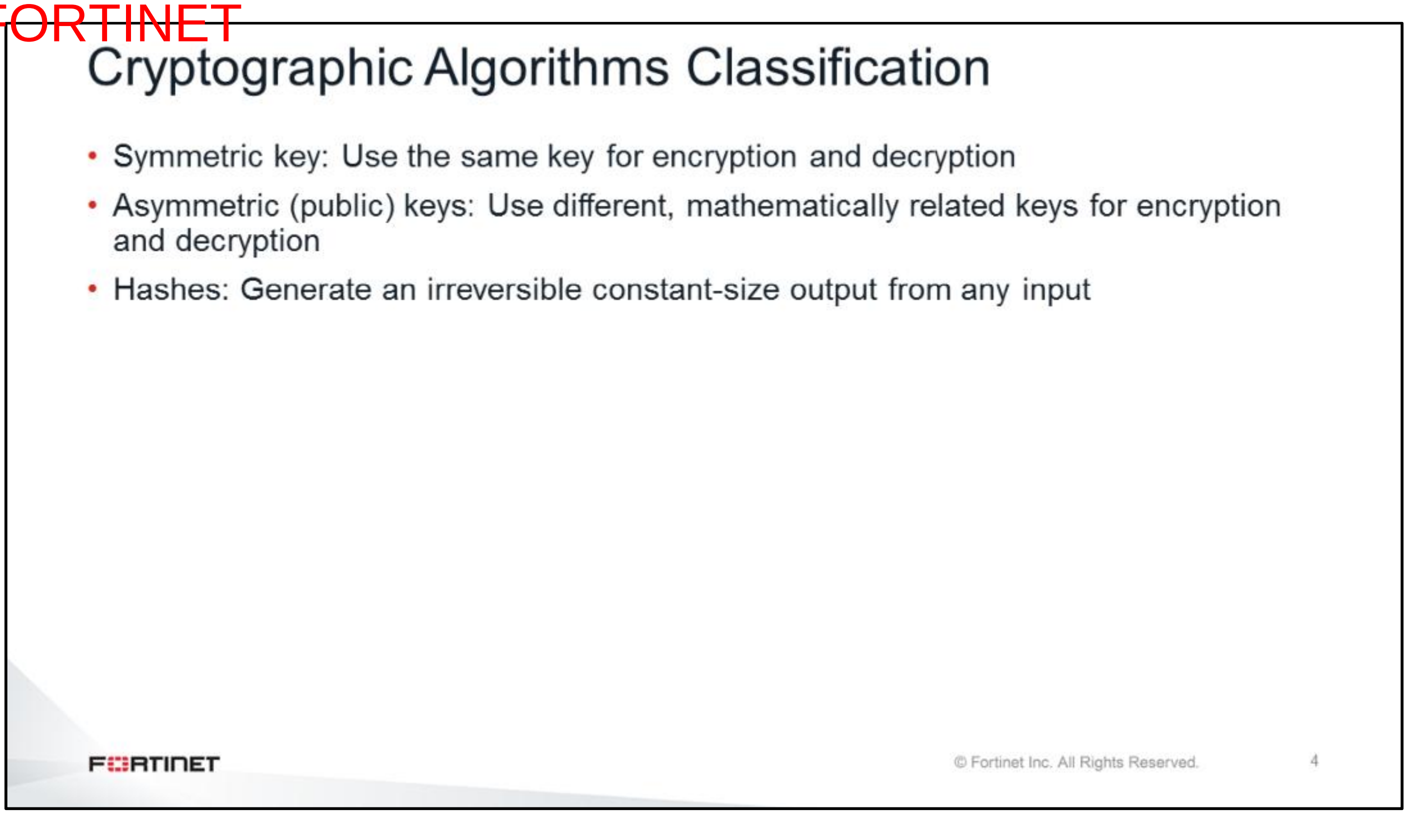
In this lesson, you will learn how to configure and troubleshoot certificate-based authentication.



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

Digital Certificates Review

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

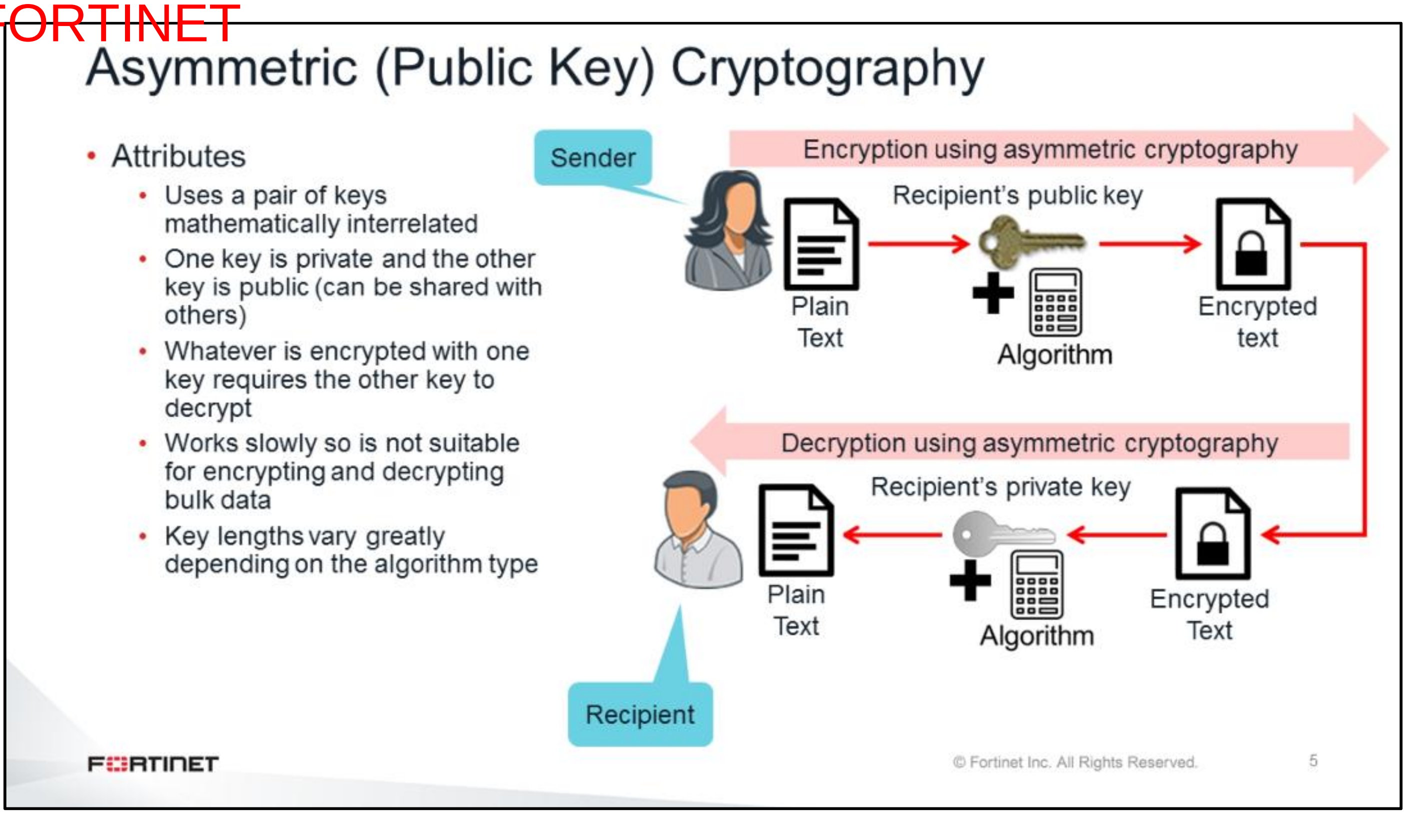


Now, you will review some terminology. There are two general types of encryption: symmetric and asymmetric.

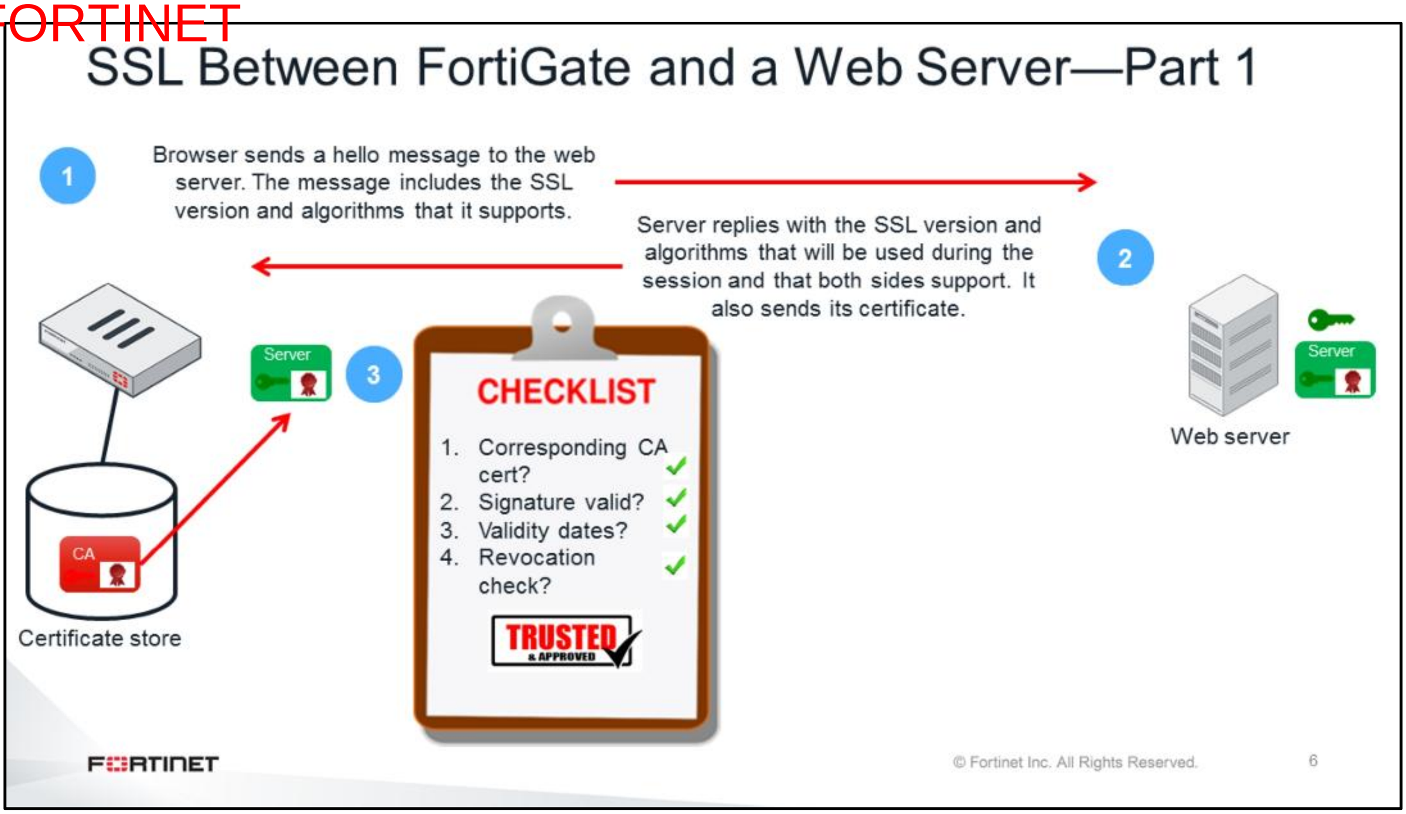
Symmetric encryption uses a single key for encrypting and decrypting. This key is shared by the parties that are interchanging encrypted information.

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 as they cannot be decrypted. A hash algorithm generates an irreversible output from any input.



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's public key. So, the sender uses the recipient's public key to encrypt the information that is intended for the recipient only. Because the information was encrypted using the recipient's public key, it can be decrypted using only the recipient's 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.

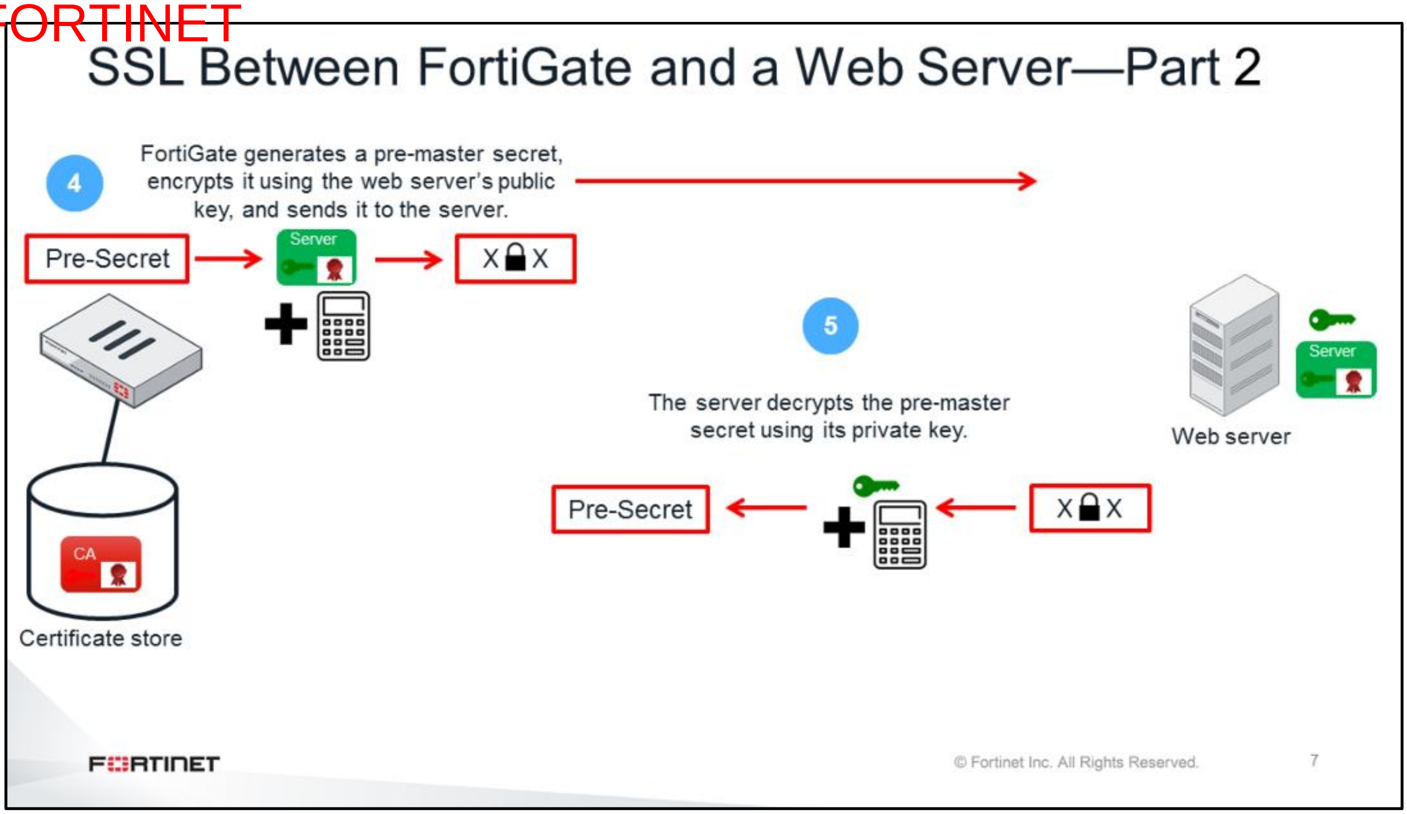


Now, you will learn more about the process of establishing an SSL session.

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 server's SSL version number and the names of the cryptographic algorithms that it supports.

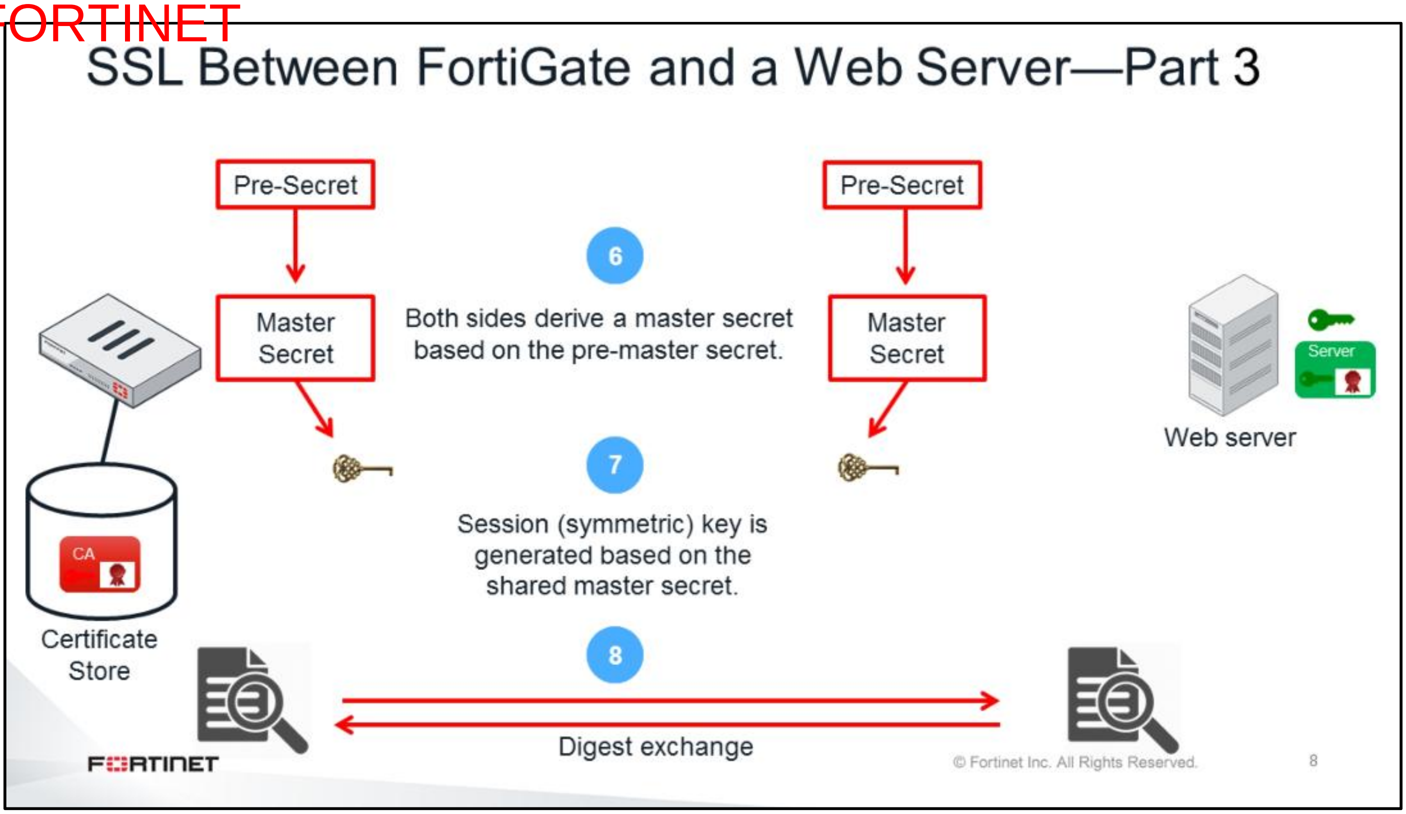
In the second step, the web server receives the message from FortiGate, and chooses the first suite of cryptographic algorithms that is in FortiGate's list and that it supports. The web server sends its certificate to FortiGate. Note that the certificate information is passed as clear text over the public 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's certificate. The checklist shown on the 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.



In the fourth step, FortiGate generates a value known as the pre-master secret. FortiGate uses the server's public key, which is in the certificate, to encrypt the pre-master secret. FortiGate then sends the encrypted pre-master secret to the web server. If a third-party intercepted the pre-master 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 pre-master secret. Now, both FortiGate and the web server share a secret value that is known by only these two devices.

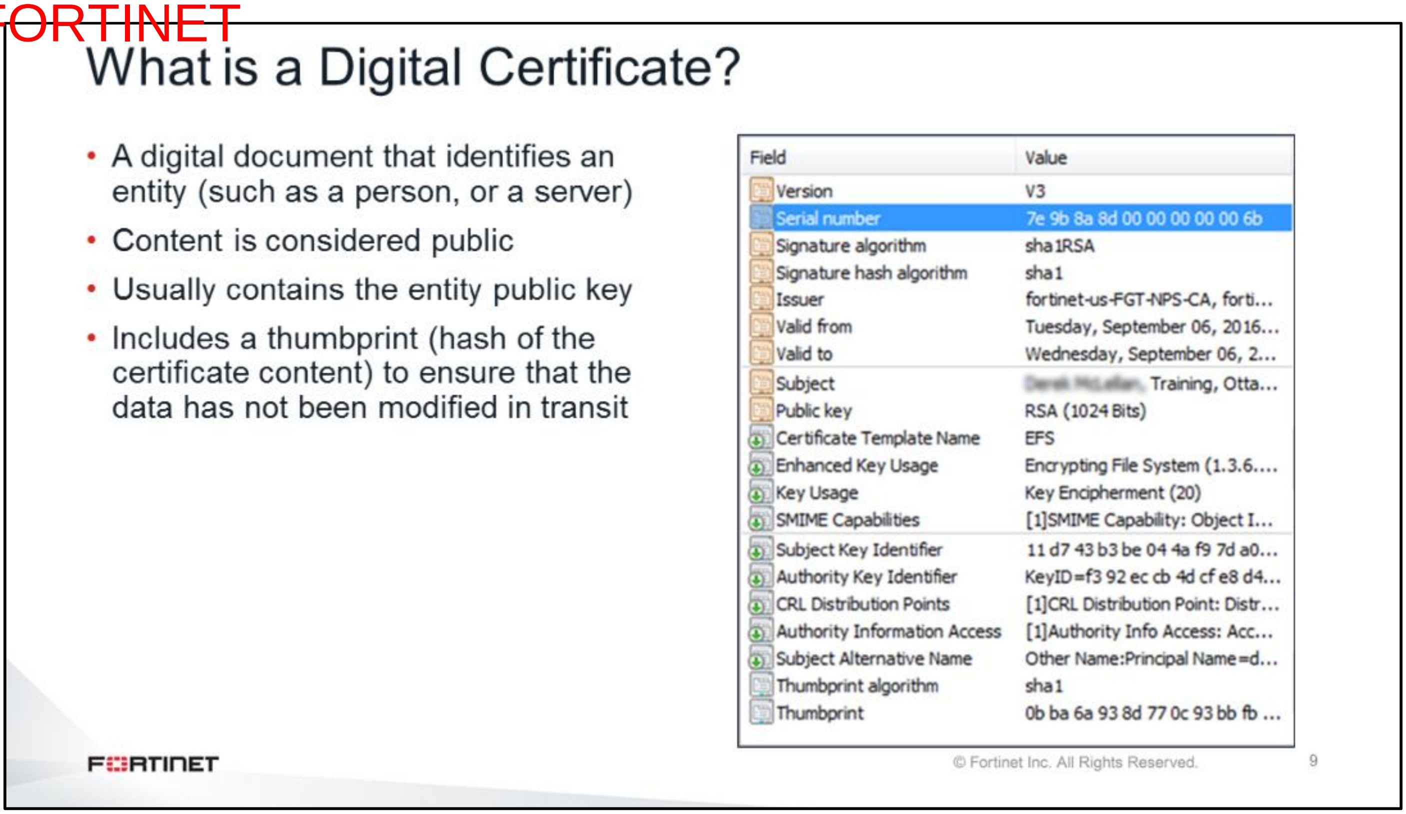


In the sixth step, both FortiGate and the web server derive the master secret based on the pre-master secret.

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.

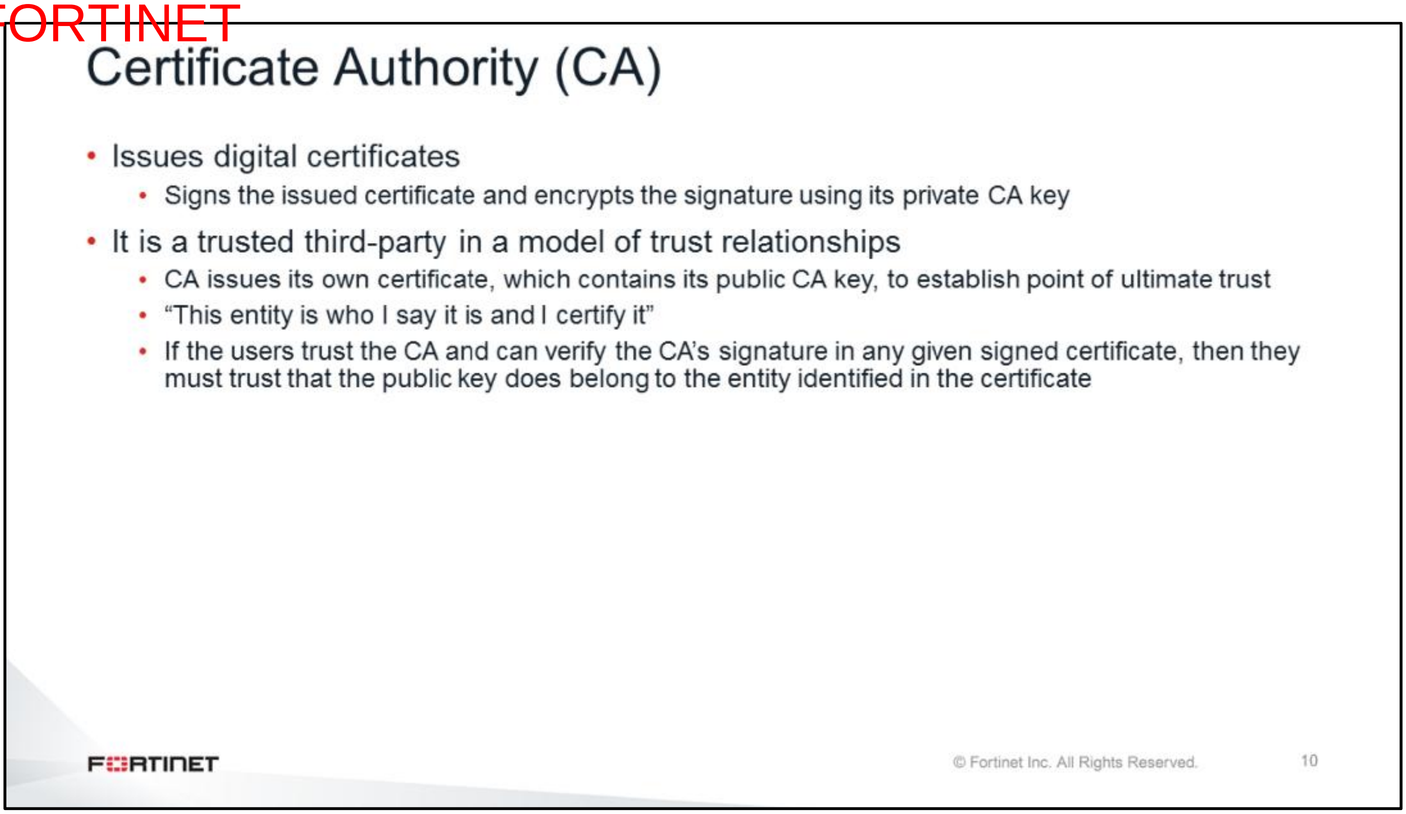
The SSL handshake is now complete. Both FortiGate and the web server are ready to communicate securely, using the session keys to encrypt and decrypt the data they send over the network or Internet.



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:

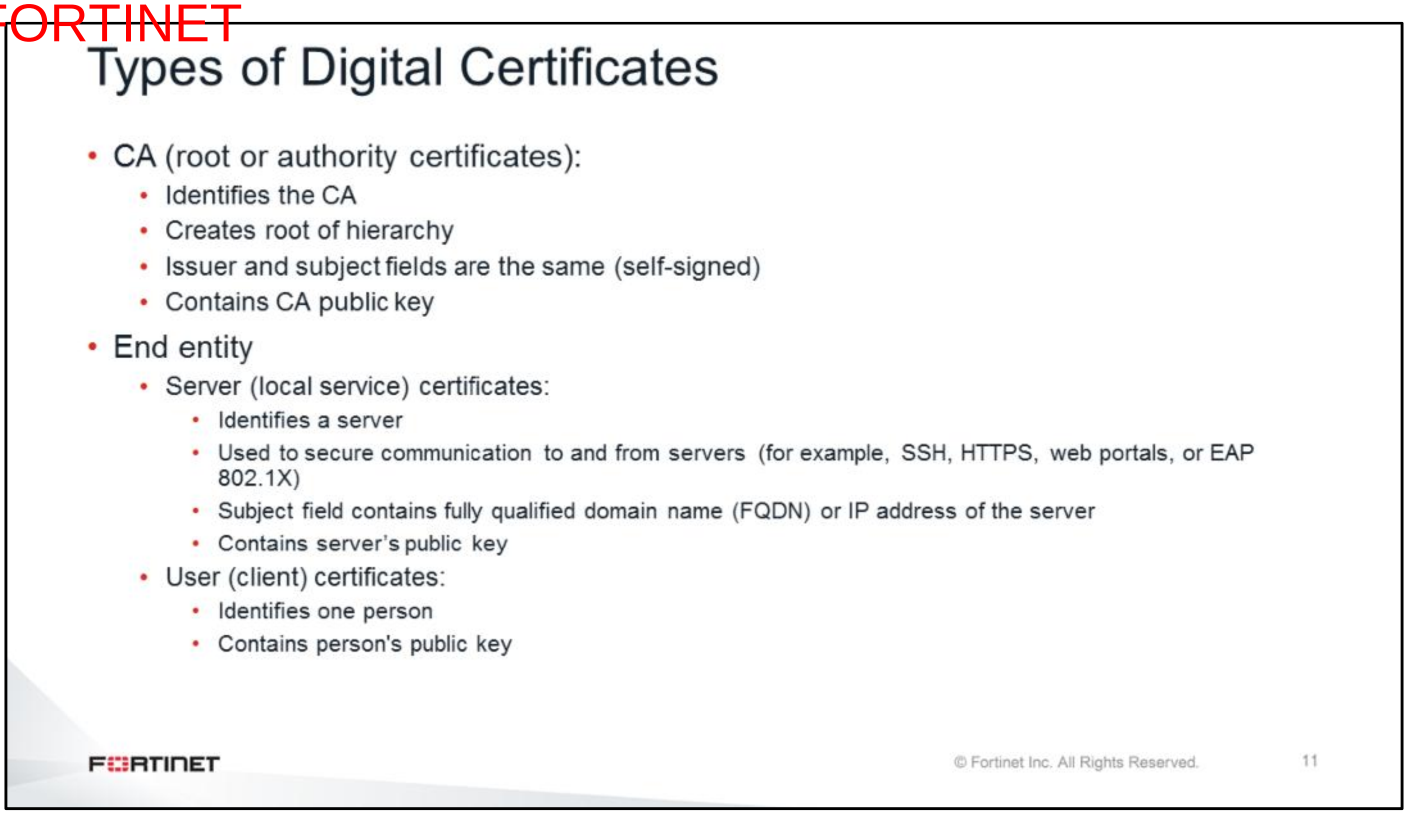
- **Serial number**: A unique number for the issuing CA that identifies the certificate.
- **Signature algorithm**: Identifies the hashing and asymmetric algorithms used to produce the digital signature that secures this certificate.
- **Issuer** and **Subject**: Identify the CA that produced the certificate 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.



Certificate authorities (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. Once 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.



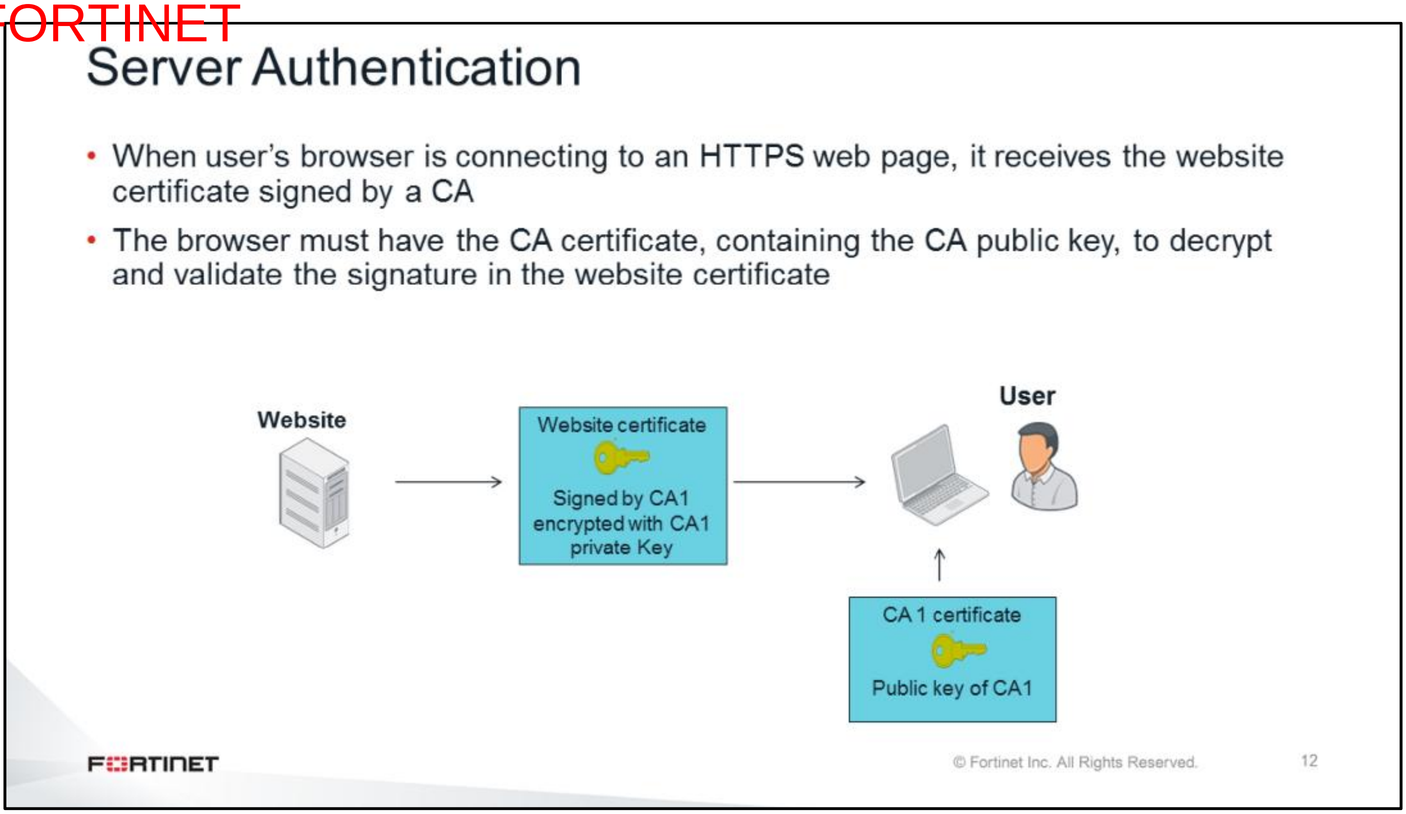
A CA can generate many different types of certificates, each with different functions (and sometimes, confusingly, with different names). A few common certificate types include:

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.

Web server certificates (also called local service certificates): These certificates identify services and are used to secure communication to and from servers, such as an Secure Shell (SSH) server, 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.

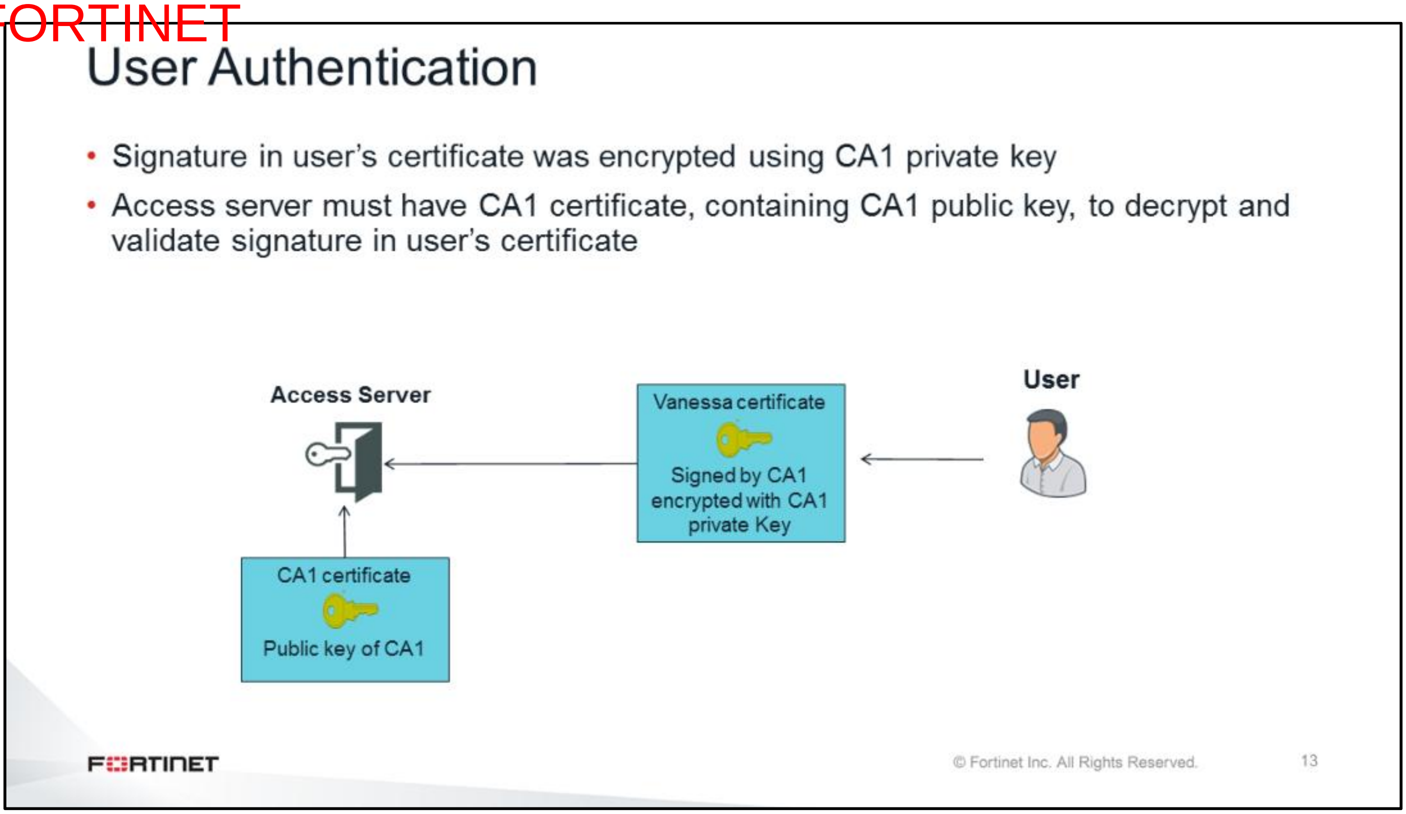
User certificates (also called client certificates): These certificates identify one person to another, a person to a device or gateway, or one device to another device. The certificate includes the public key associated with the identity.

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



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 CA1 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 CA digital certificate, which contains its public key.

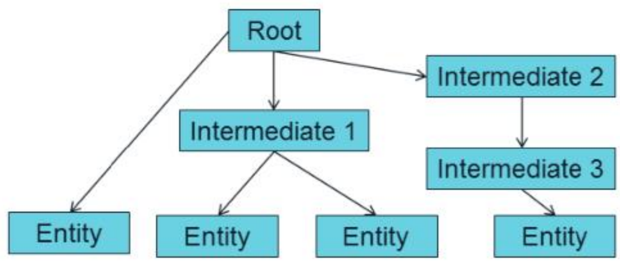
Most browsers already have preinstalled the CA certificates of the most well-known public CAs. However, if the server certificate is signed by a private CA, the public CA certificate must be installed in the browser. In this way, the browser *trusts* the private CA and can decrypt the digital certificates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



In a similar way, digital certificates can be used to authenticate users. It 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. The CA signature is encrypted with the CA private key. The access server must have the CA certificate installed (which contains the CA public key) for decrypting and validating the user's certificate.

Chain of Trust

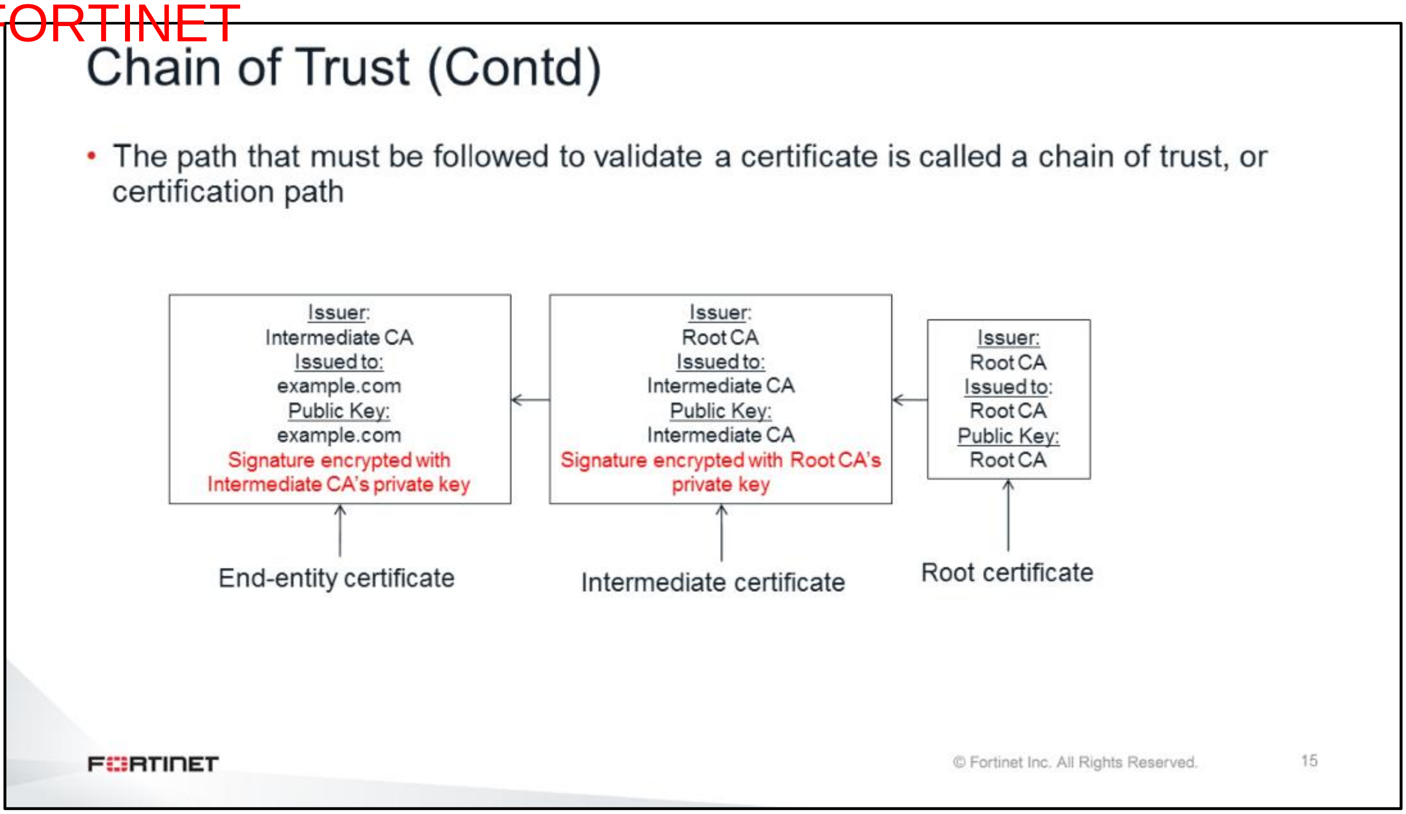
- **Root**: A self-signed certificate that identifies a CA
- **Intermediate**: A subordinate CA certificate signed by a root or by another intermediate CA
- Both can issue (sign) end-entity certificates



FORTINET

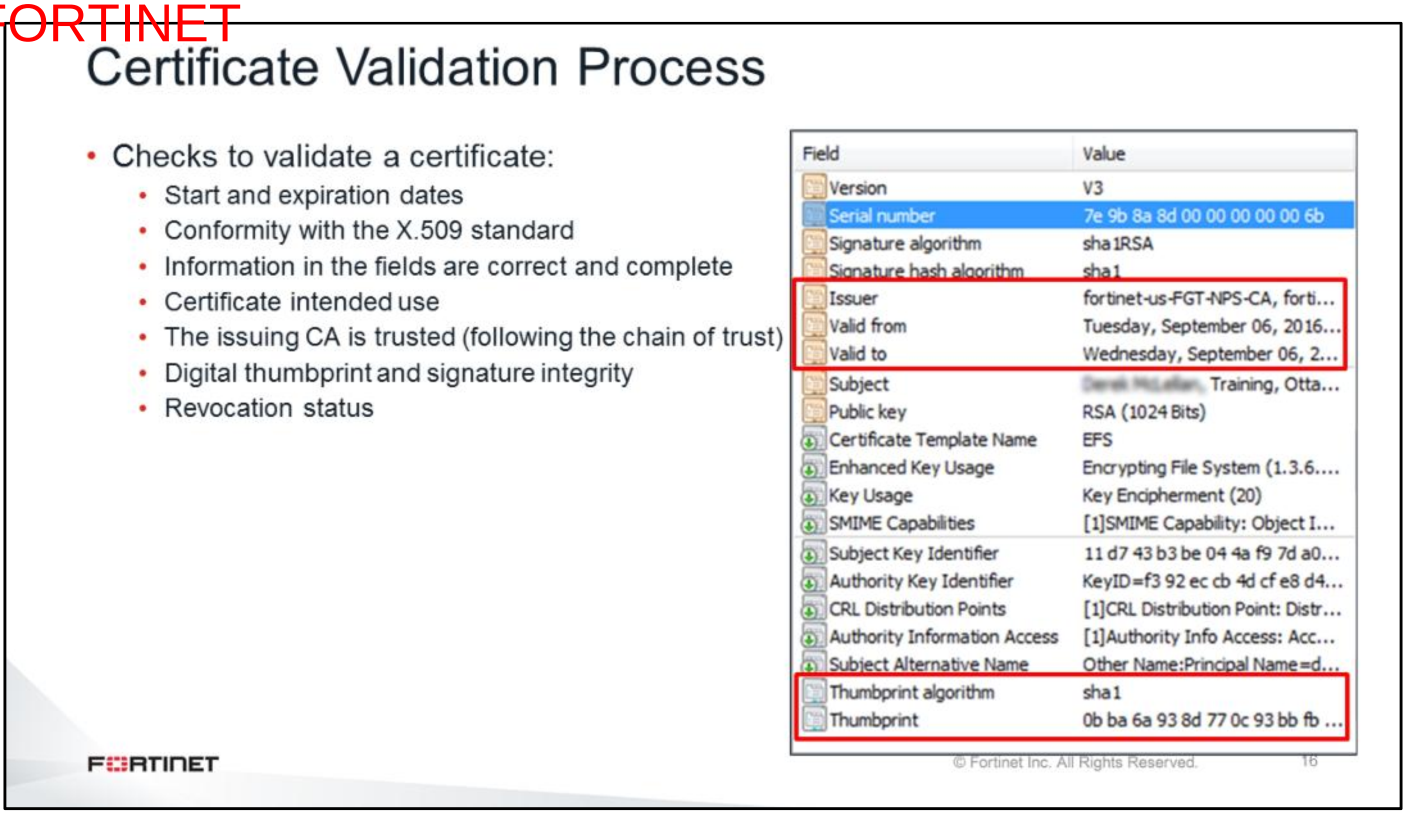
 14

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.



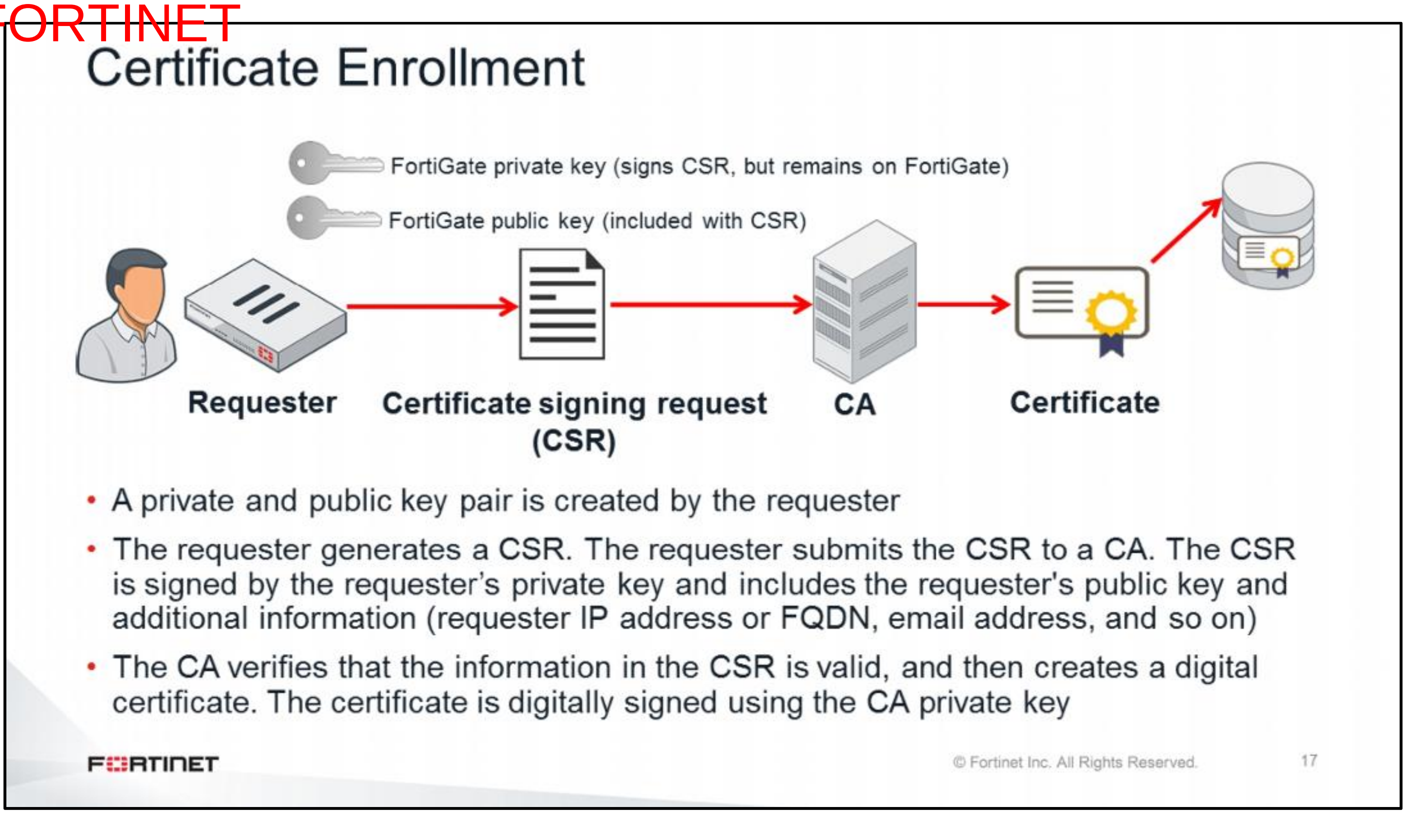
In the example shown on this slide, the end-entity certificate was signed by an intermediate CA. The intermediate CA certificate was signed by the root CA.

The process of validating the end-entity's certificate goes from bottom to top 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's certificate requires the certificates of both the root CA and the intermediate CA.



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

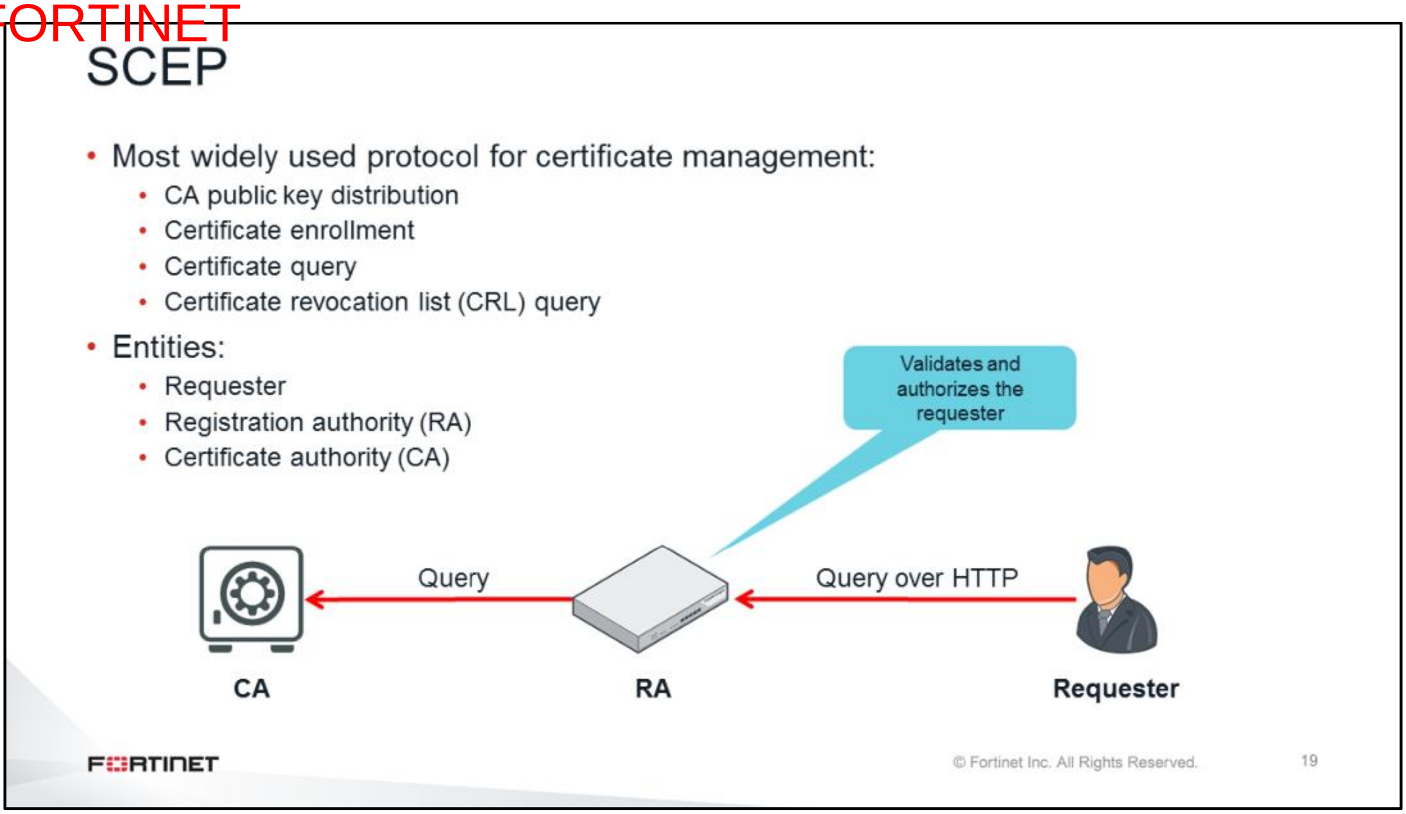
- Valid period (start and expiration dates)
- Conformity with the X.509 standard
- Information in the fields are proper and complete
- Certificate intended use
- The issuing CA is trusted (following the chain of trust)
- Digital thumbprint and signature integrity
- Revocation status



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

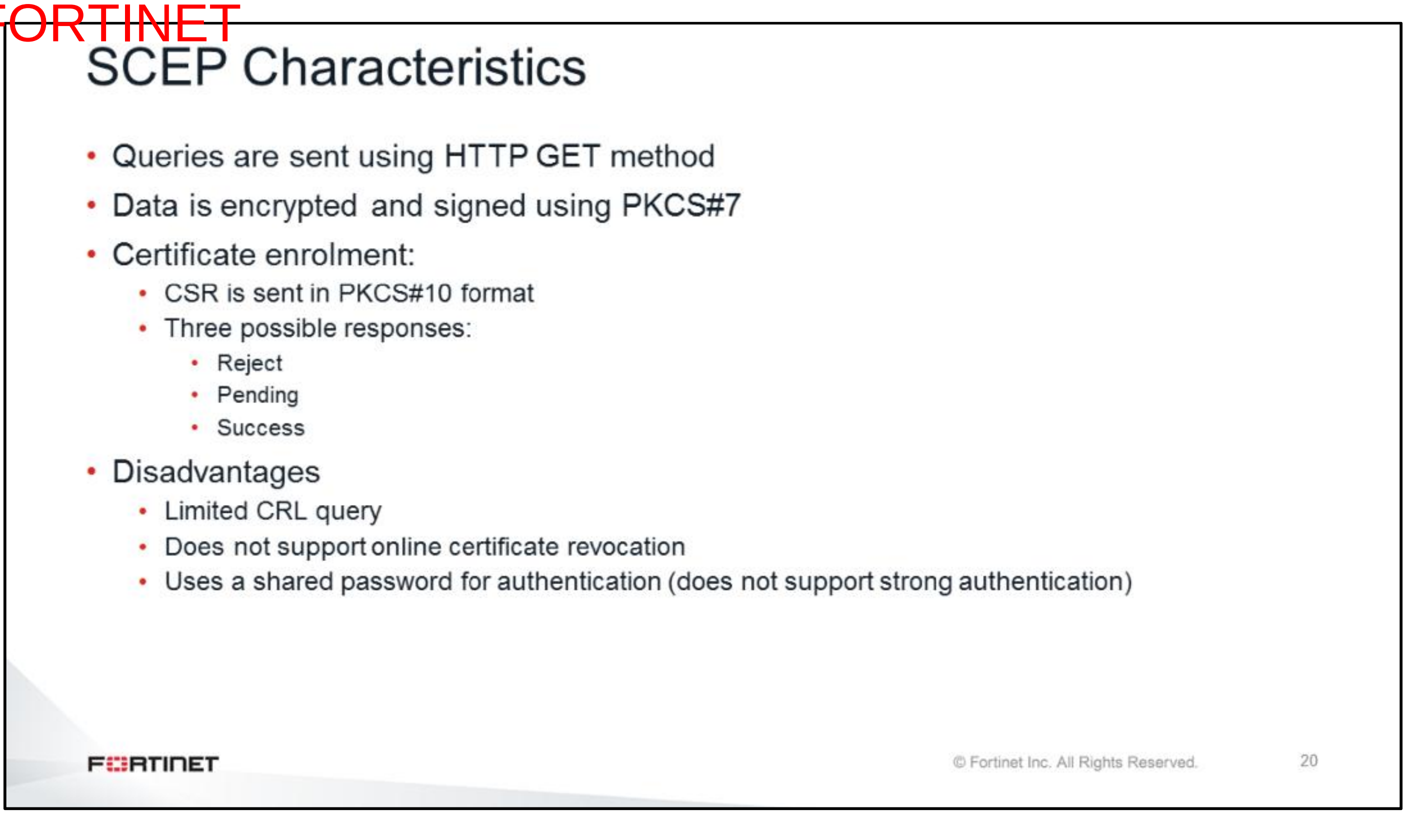
1. The requester generates a CSR. A private and public key pair is created. The CSR is signed by the requester's private key.
2. The requester submits the CSR to a CA. The CSR includes the requester's public key and specific information about the requester (IP address, distinguished name, email address, and so on). Note that the private key remains confidential.
3. 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.
4. The certificate is returned to the requester.

In this section, you will review SCEP.



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.



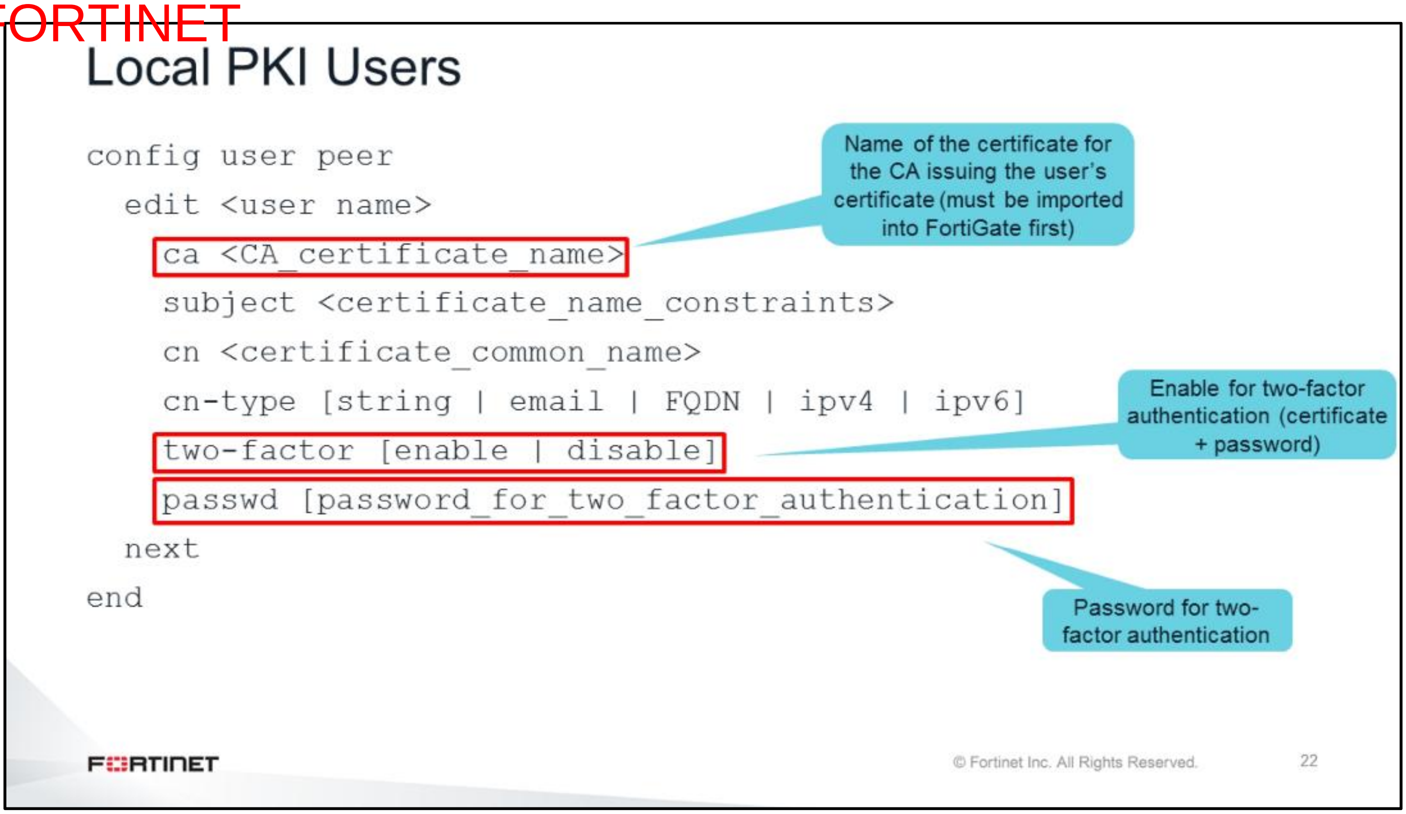
SCEP is based on HTTP. It uses the regular HTTP GET method to sends queries to the RA. Data, though, is encrypted and signed using the standard PKCS#7.

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, and 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's 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.

FortiGate PKI Users

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



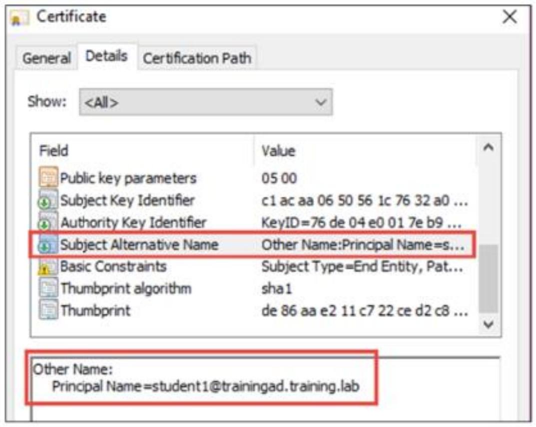
You must use the CLI to create the first PKI user. After you create the first PKI user, and as long as there is at least one PKI user, the menu option to create and administrate more PKI users will appear on the GUI.

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's password.

Authorizing PKI Users Using Principal Name

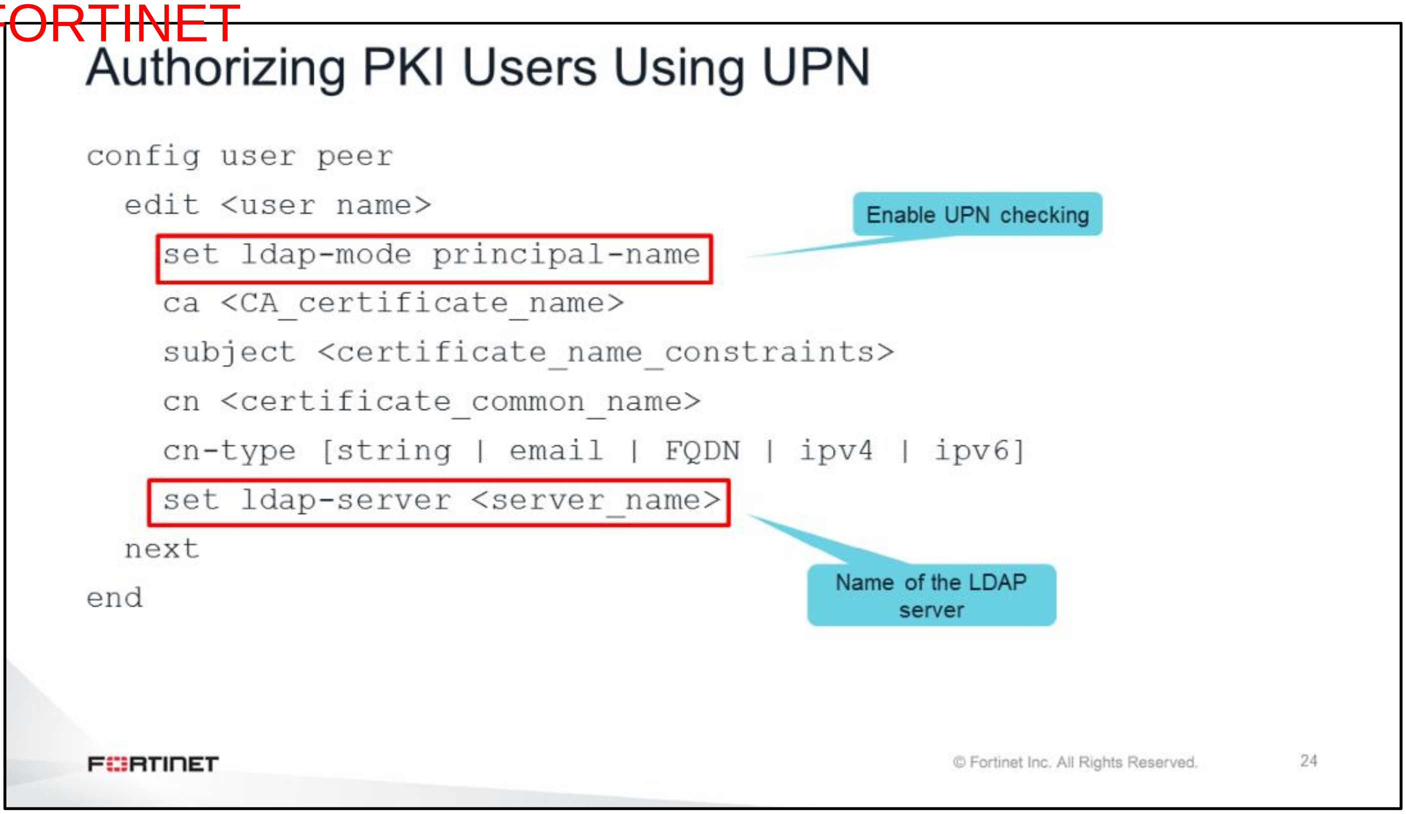
- FortiGate can use LDAP to validate the information in the certificate's user principal name (UPN) field
  - Authentication fails if there is no valid user with a UPN that matches the UPN in the certificate



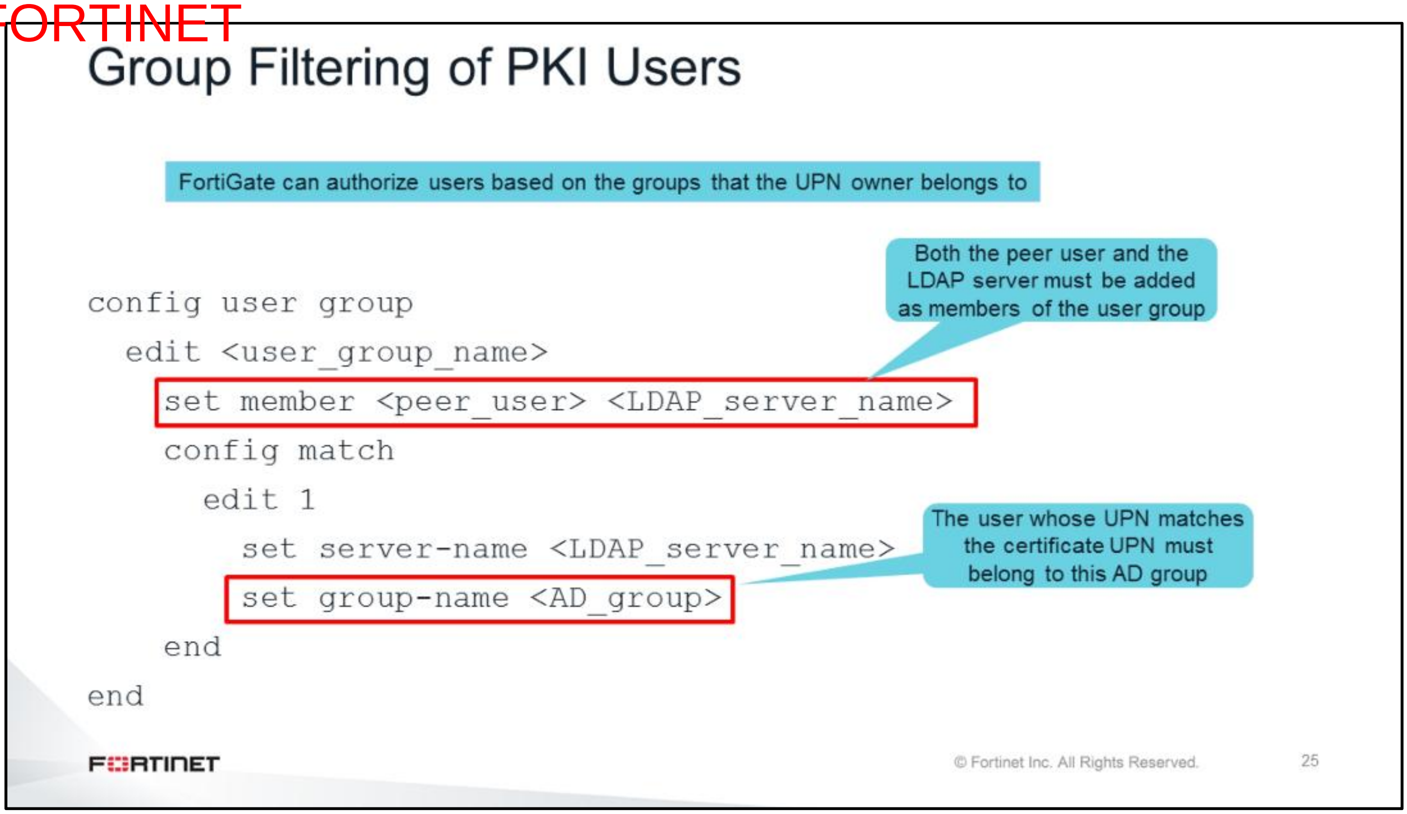
FORTINET

 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 will fail if is there is no valid user with a UPN that matches the UPN in the user's certificate.



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.

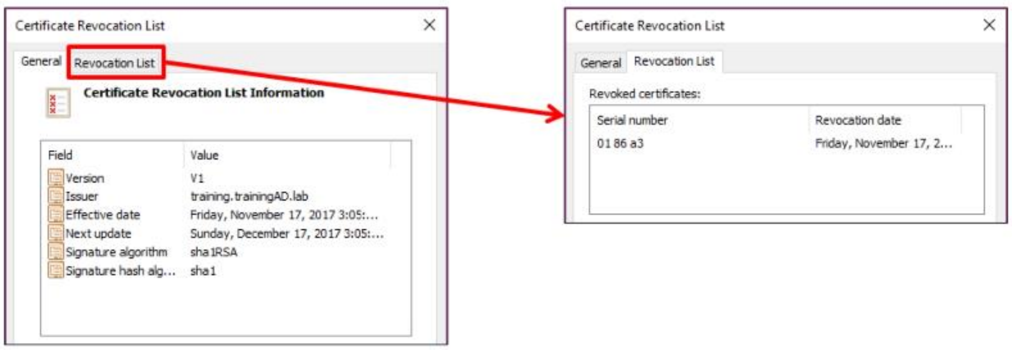


When you configure UPN validation for a PKI user, and the UPN belongs to a valid user, FortiGate will query the LDAP for the user groups. You can use that information to authorize access only to users that belong to specific groups.

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

Certificate Revocation List (CRL)

- A CRL contains serial numbers of certificates that have been revoked
- Revoked certificates are automatically placed on the CRL
- Administrator can manually export CRLs from CAs to network devices (such as FortiGate)

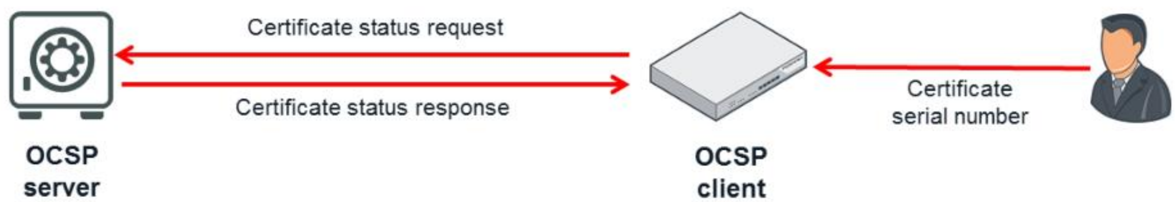


A certificate revocation list (CRL) contains the serial numbers of certificates that have been revoked. There is usually one CRL per root CA.

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

Online Certificate Status Protocol (OCSP)

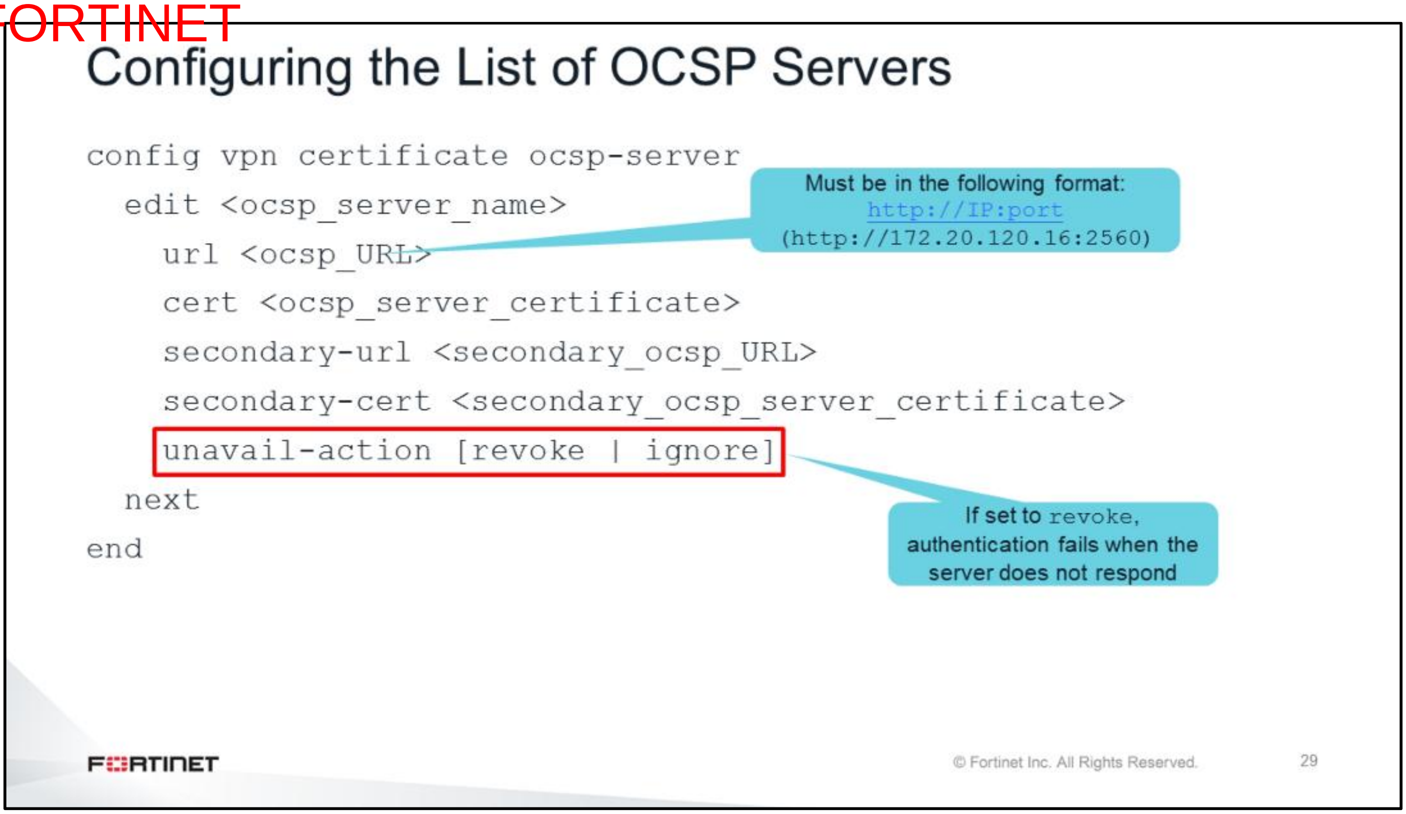
- Online service that provides the revocation status of digital certificates
- Possible responses:
  - Good
    - Certificate has not been revoked
  - Revoked
    - Certificate has been revoked
  - Unknown
    - The certificate was issued by a different (unknown) CA



 28

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's serial number to an OCSP server. The OCSP server replies with one of three possible answers:

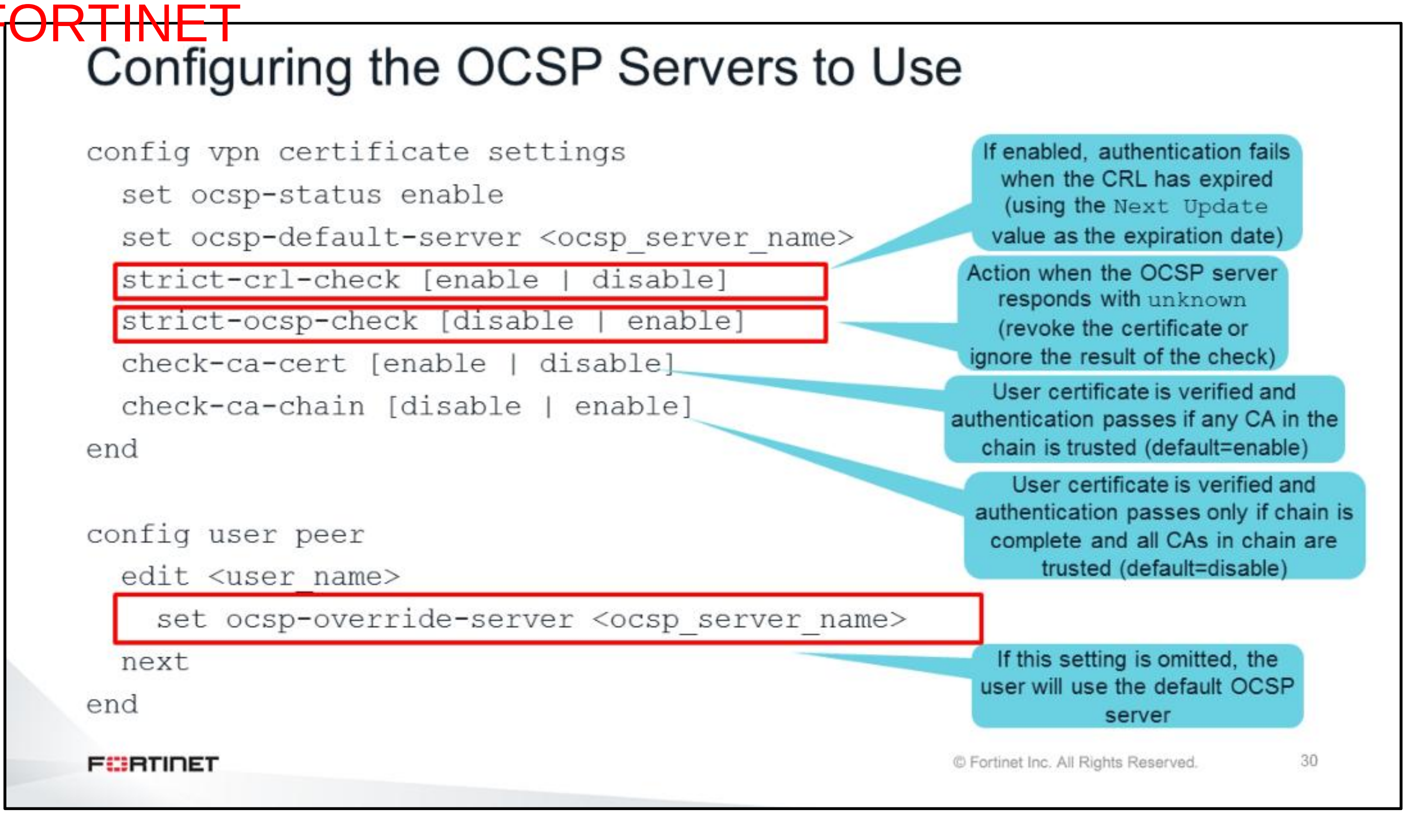
- **Good**: The certificate has not been revoked.
- **Revoked**: The certificate has been revoked.
- **Unknown**: The certificate was issued by another CA.



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 there is no reply from the primary server.

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

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



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 will be rejected if the OCSP server responds with `unknown` (or from the secondary OCSP server, if there is one).

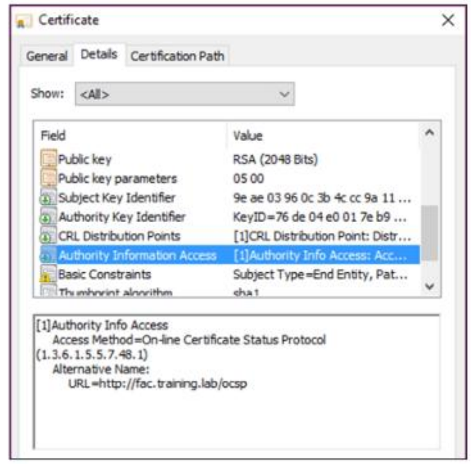
If you are using a CRL list instead of OCSP, the `strict-crl-check` setting defines what action to take when the CRL has expired.

OCSP URL Embedded in the Certificate

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

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

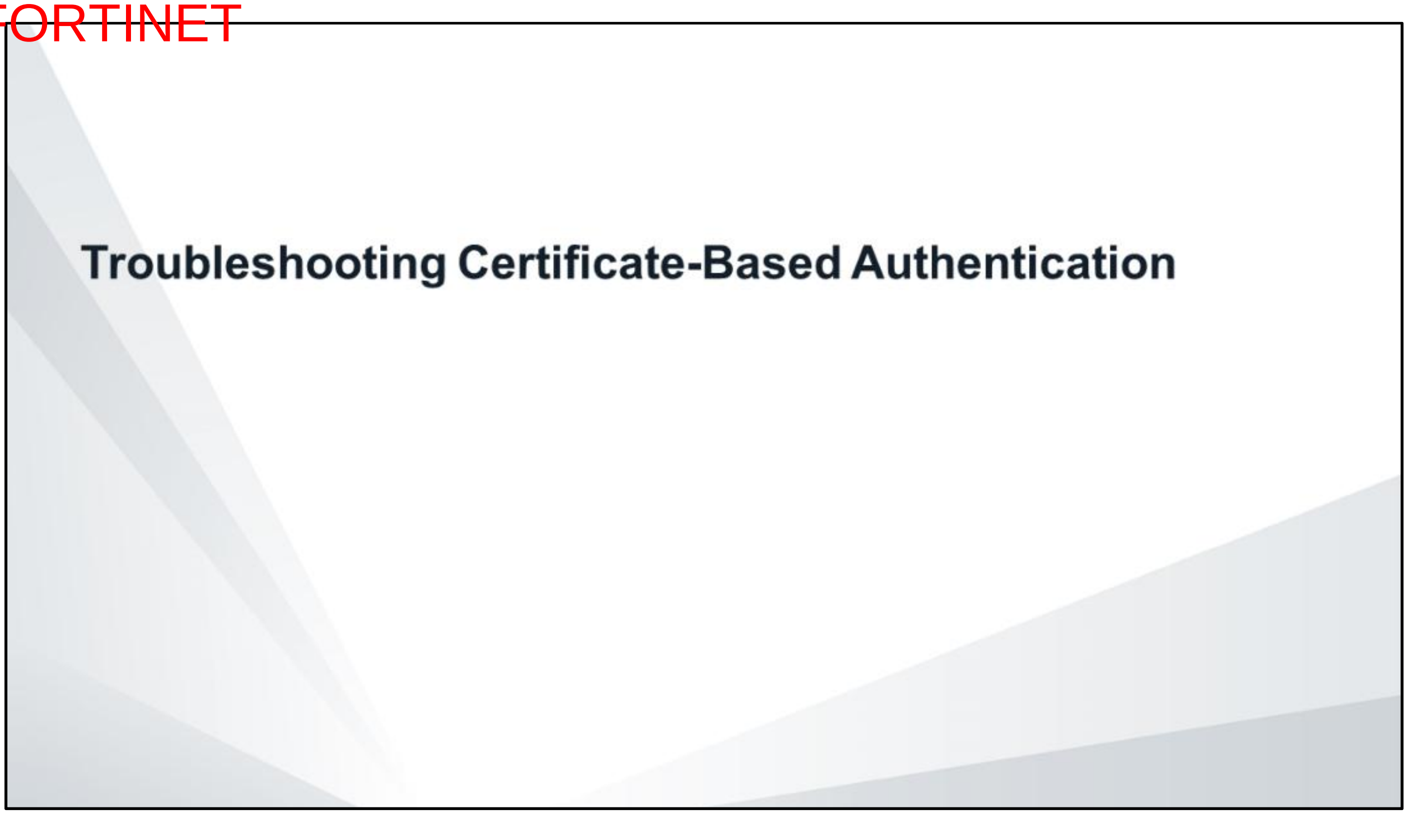
  - `certificate`: Use URL from certificate (if present)
  - `server`: Always use URL in FortiGate configuration



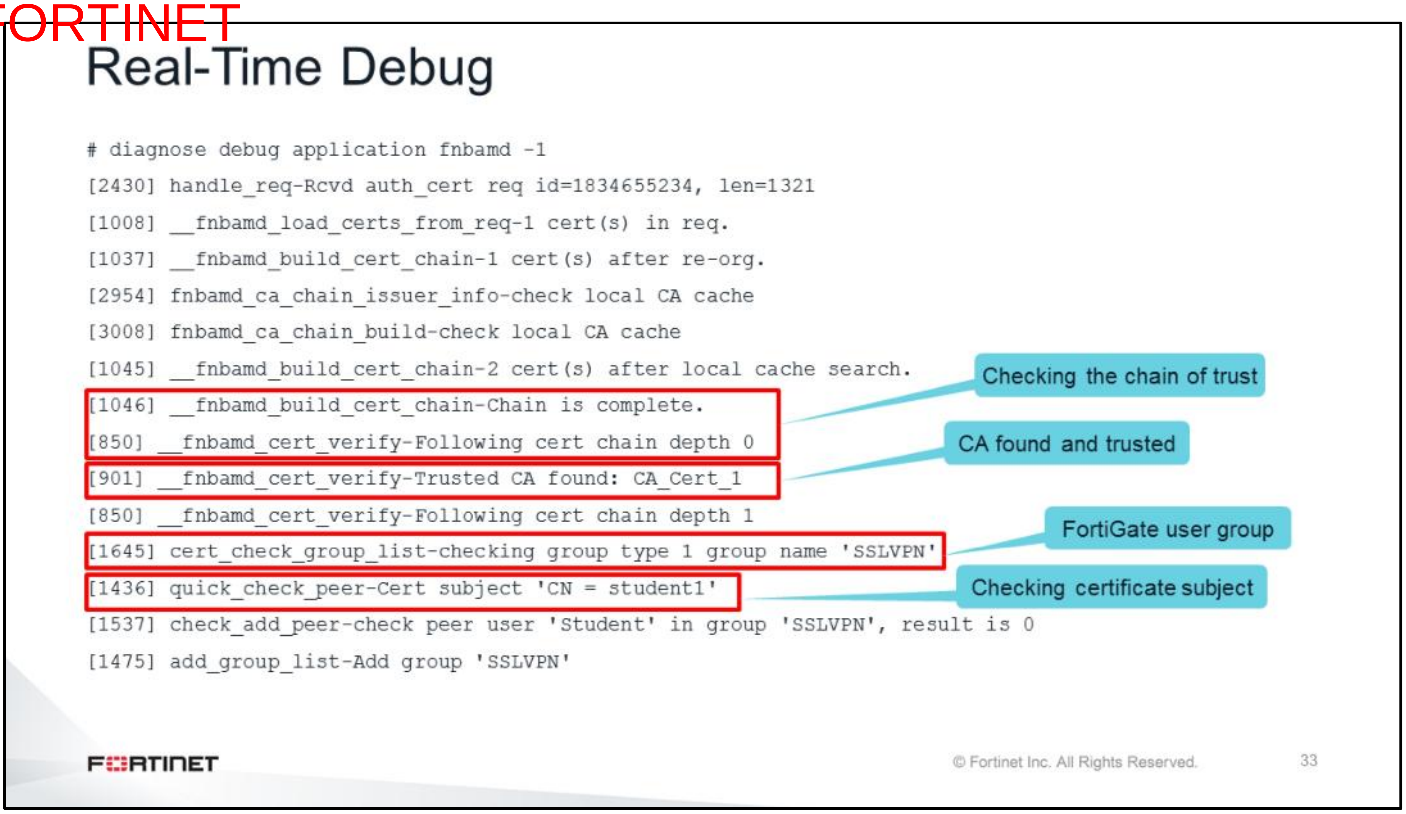
FERTINET

 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).

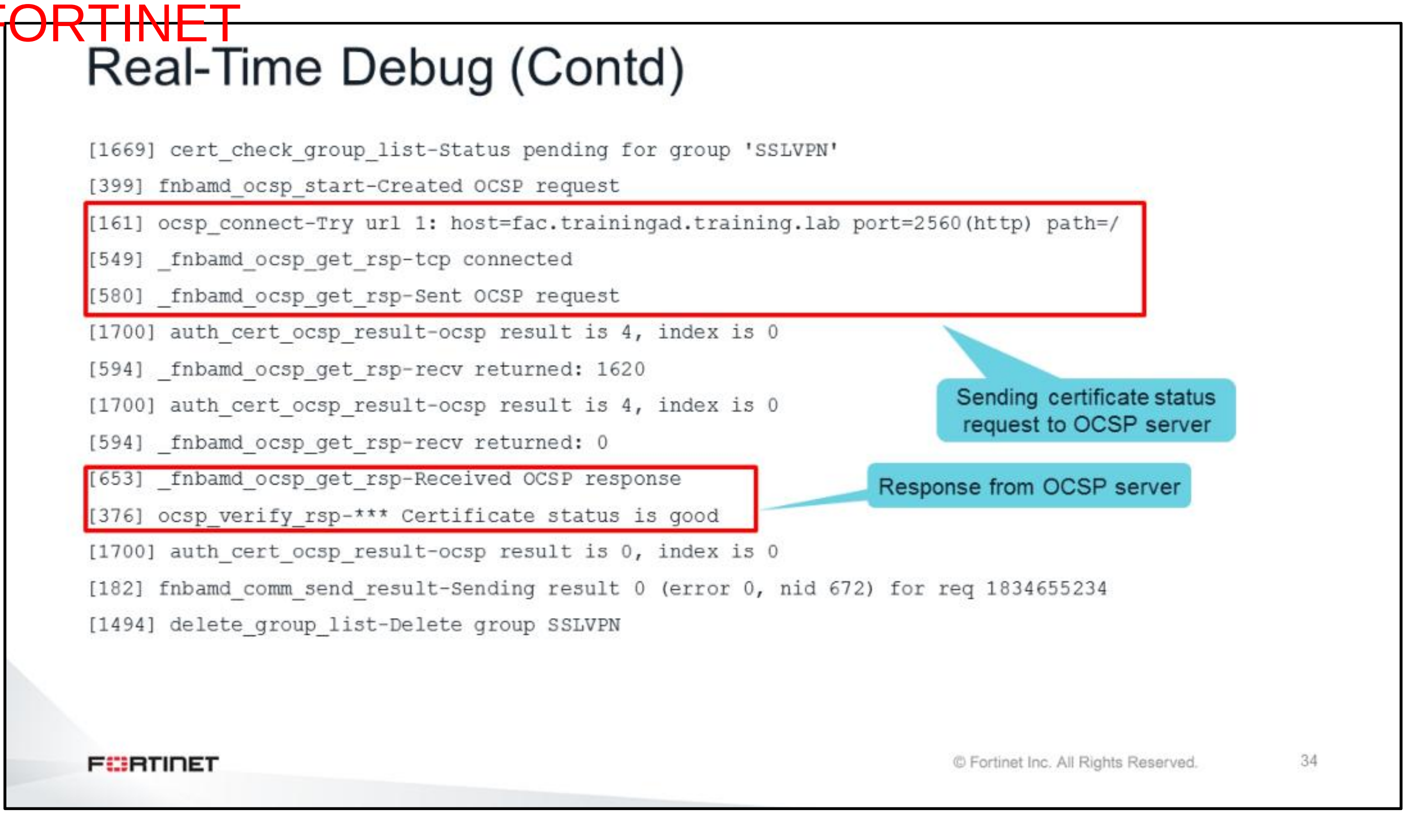


In this section, you will learn how to troubleshoot certificate-based authentication problems.



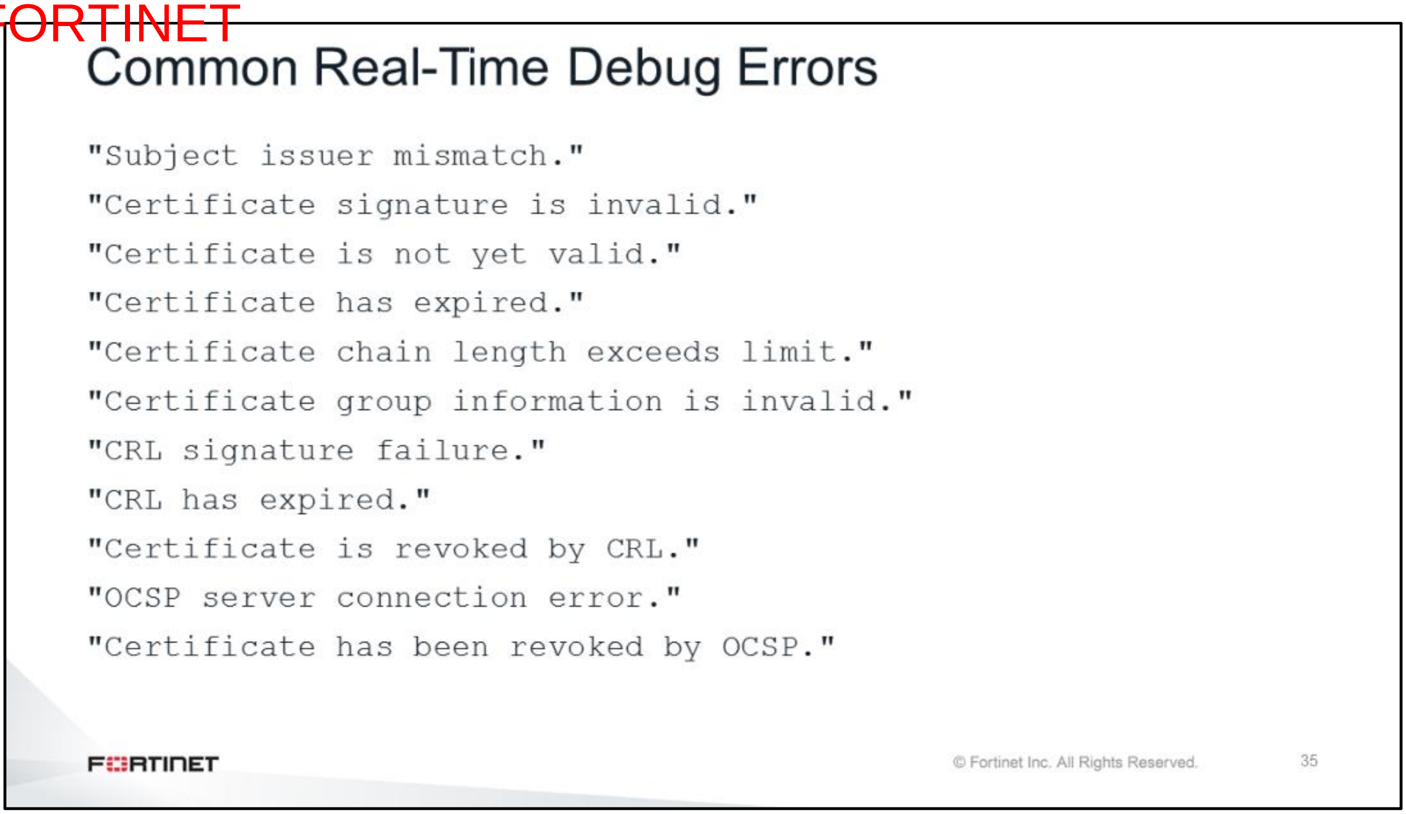
The Fortinet non-blocking authentication daemon (`fnbamd`) is the process that validates user certificates. The output of its real-time debug shows, step-by-step, what the non-blocking authentication daemon does when a user's certificate is received and must be validated.

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.



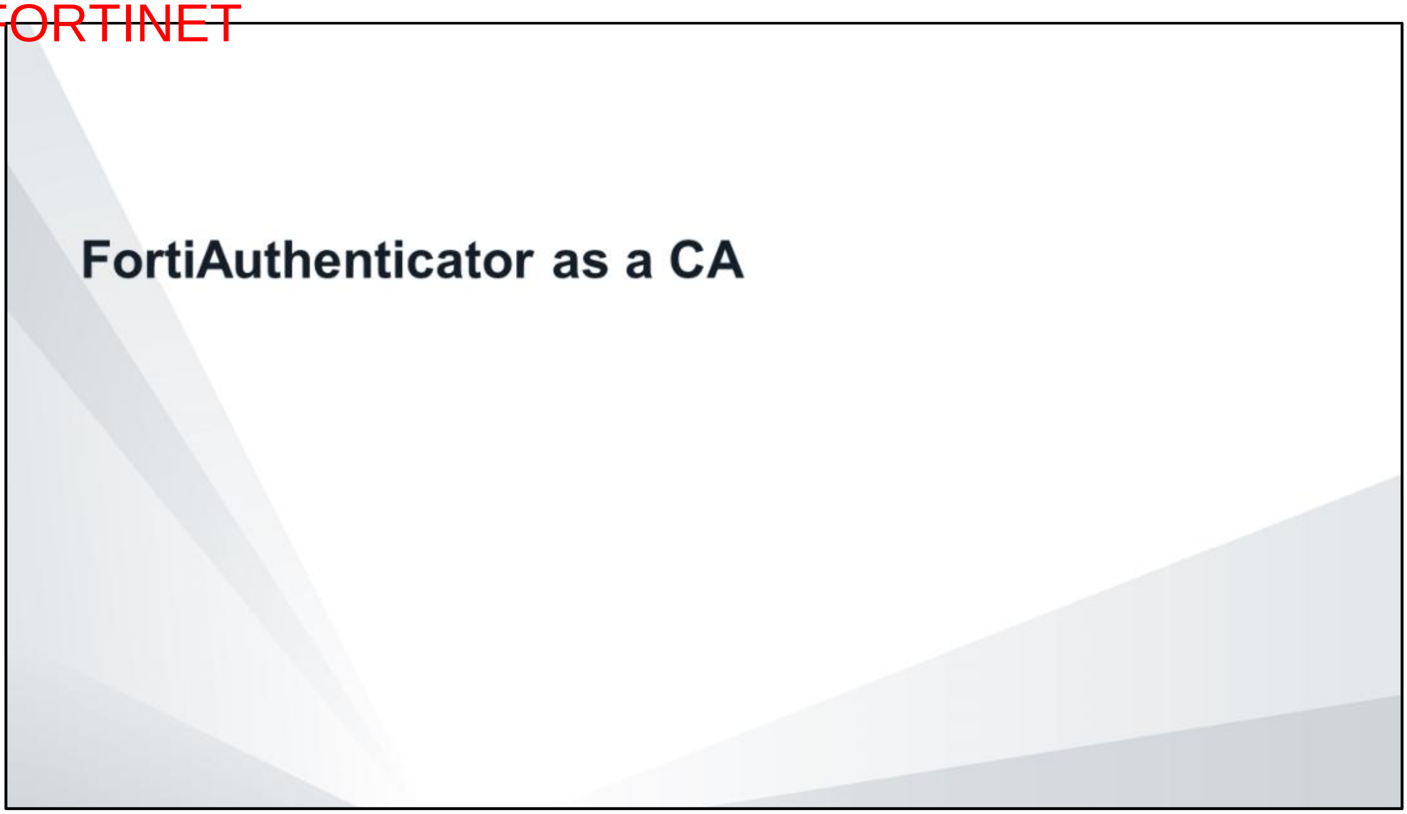
In the example shown on this slide, FortiGate is configured to validate the certificate revocation status using OCSP. The output of the real-time debug shows the OCSP URL and a log entry indicating that the OCSP request has been sent.

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.



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

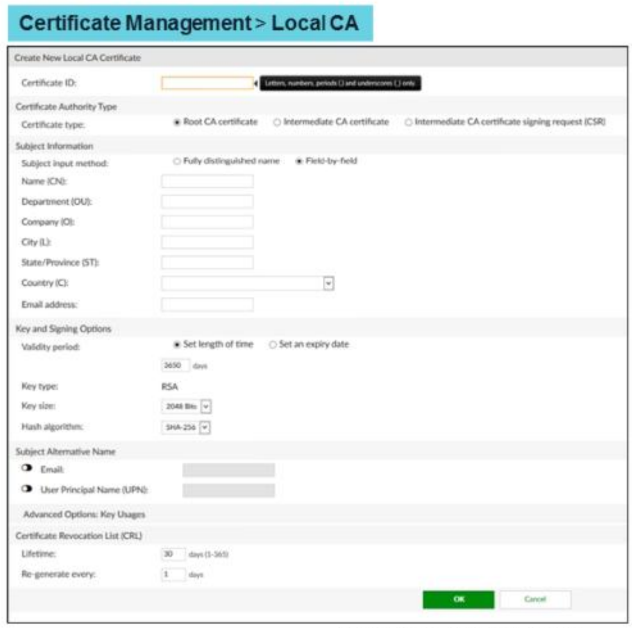
- The subject does not match the subject in the PKI user configuration
- The Certificate is not valid yet or has expired
- The CRL has expired
- The Certificate has been revoked
- And so on



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

FortiAuthenticator as a CA

- FortiAuthenticator can act as:
  - CA
    - Root and/or intermediate
    - CRL
  - SCEP RA
  - OCSP Server

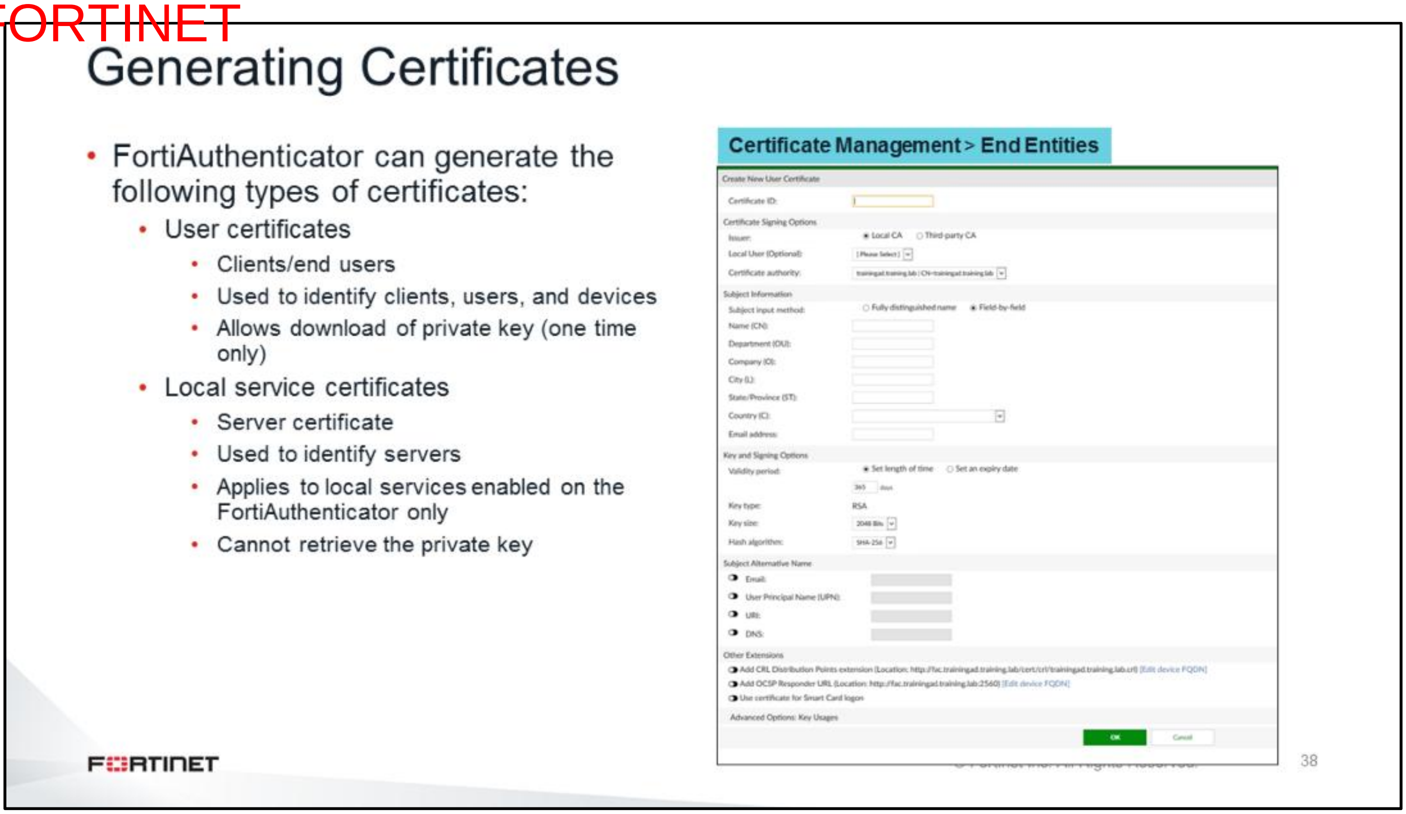


 37

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

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

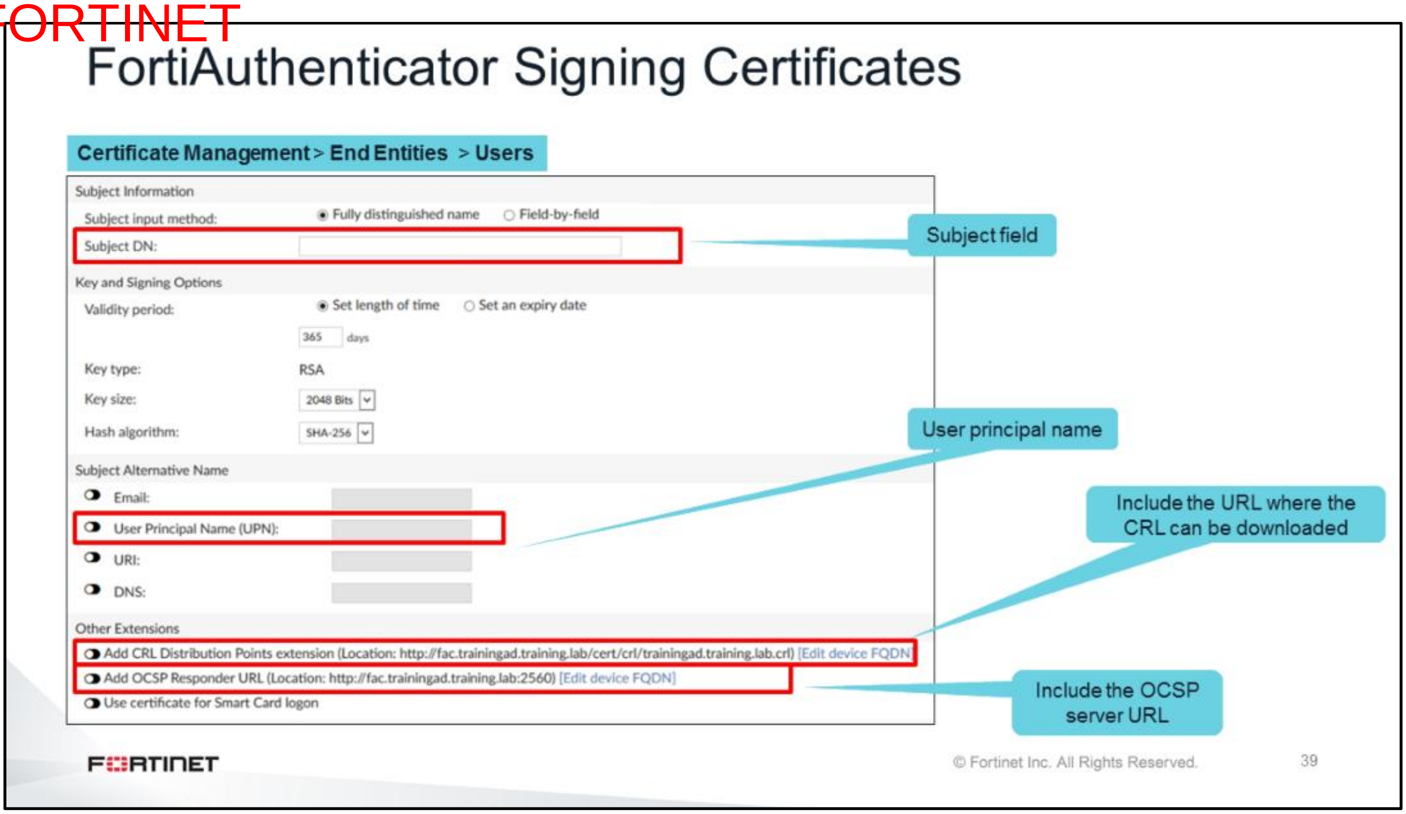
FortiAuthenticator can also act as an OCSP server (for certificate revocation checks) and a SCEP RA (for receiving CSRs and issuing certificates).



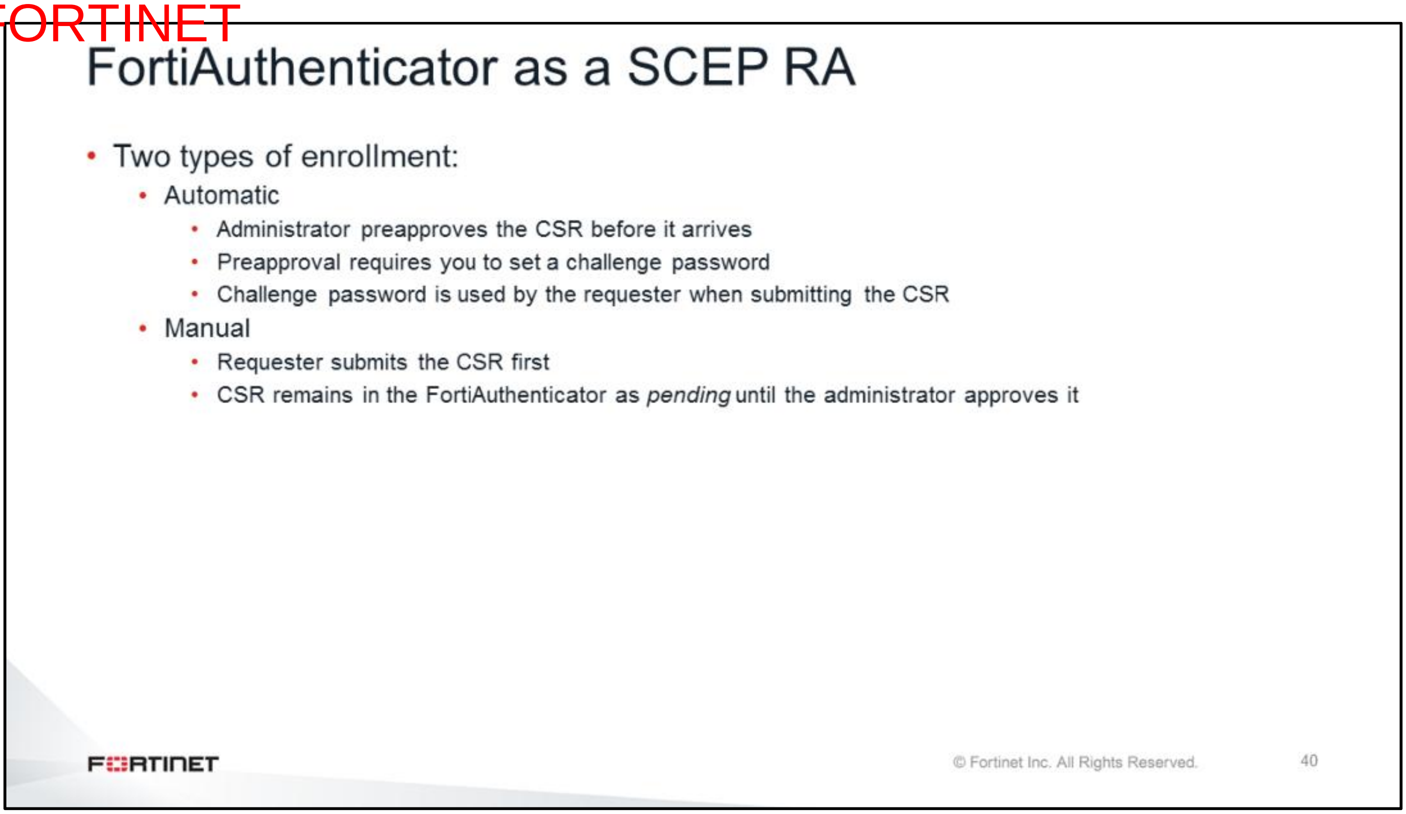
User and server certificates are required for mutual authentication on many HTTPS, SSL, and IPsec VPN network resources.

You can create a user certificate on FortiAuthenticator, or import and sign a CSR. User certificates, client certificates, or local computer 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.

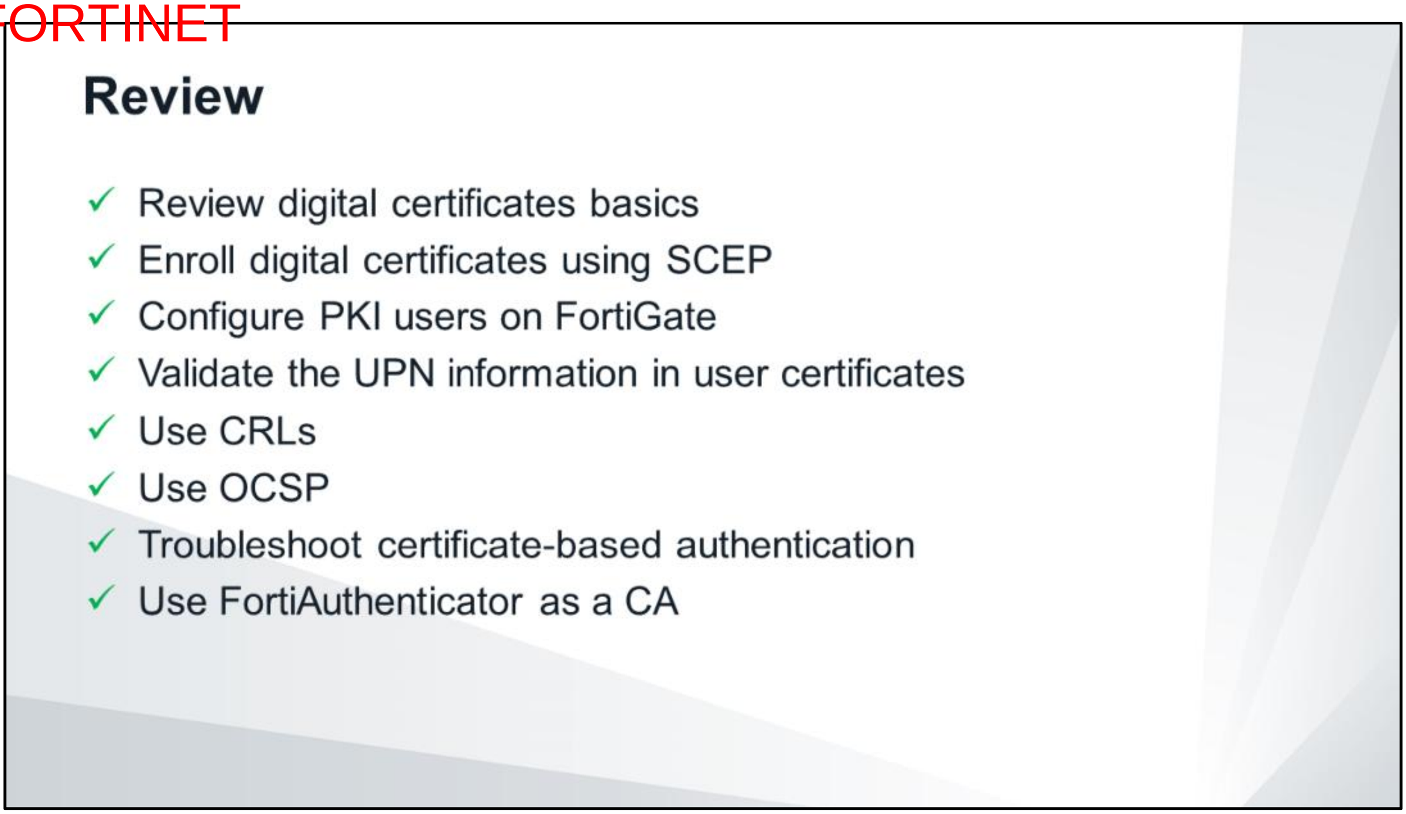


Once you have created a CA certificate, FortiAuthenticator can start issuing certificate to users. In each user certificate, you can define the subject field, expiration date, UPN, URL where the CRL can be downloaded, and the OCSP's URL.



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. Once 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.



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

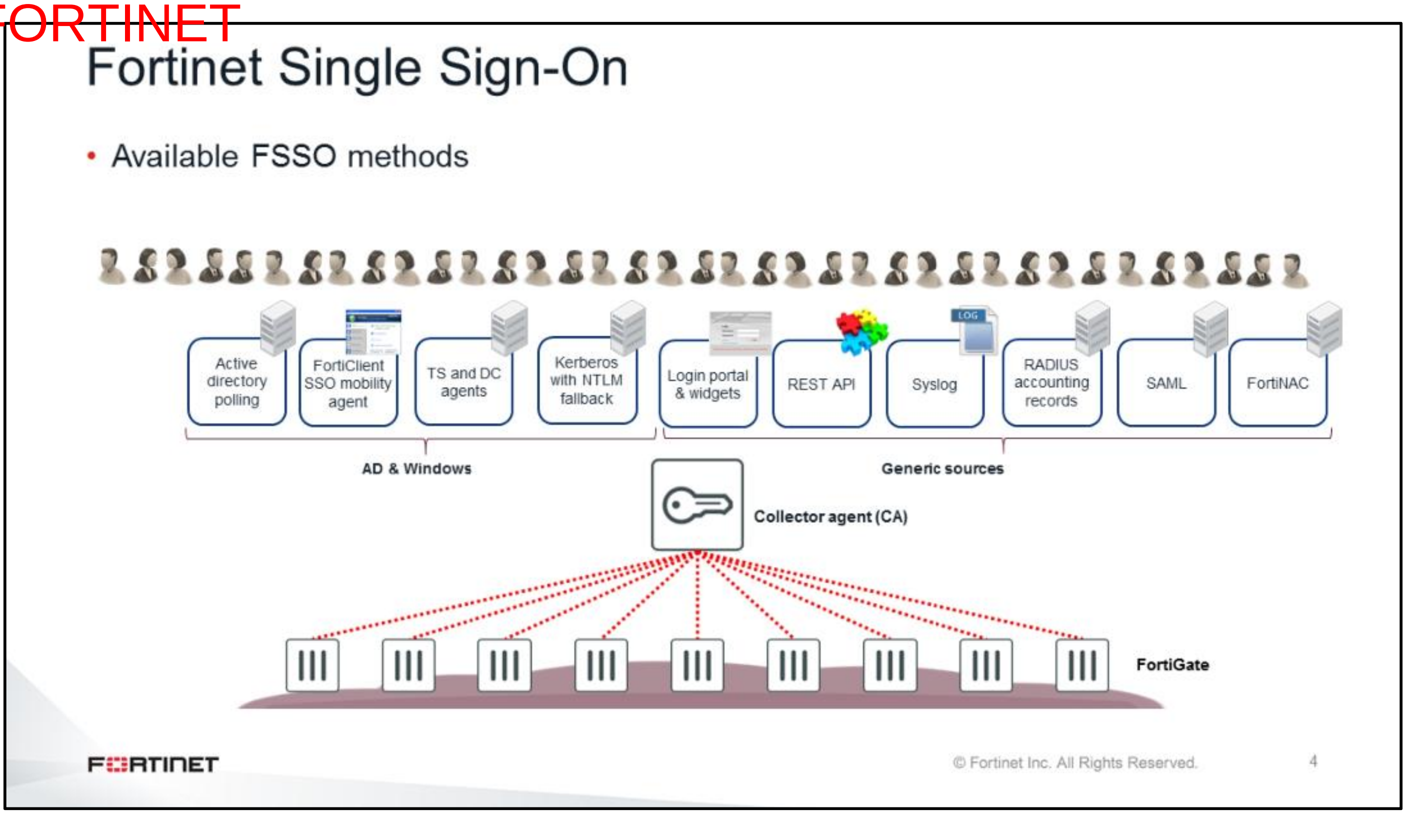
In this lesson, you will learn about different ways to collect logon events and convert them to Fortinet Single Sign-On (FSSO) events. You will focus on RADIUS and Syslog Single Sign-on and their relevant configurations.

Objectives

- Understand available FSSO methods on FortiAuthenticator
- Configure and monitor Syslog SSO
- Explore RADIUS Single Sign-On (RSSO) deployment scenarios
- Configure RSSO
- Troubleshoot RSSO
- Configure SSO sources on FortiAuthenticator
- Troubleshoot FSSO on FortiAuthenticator

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

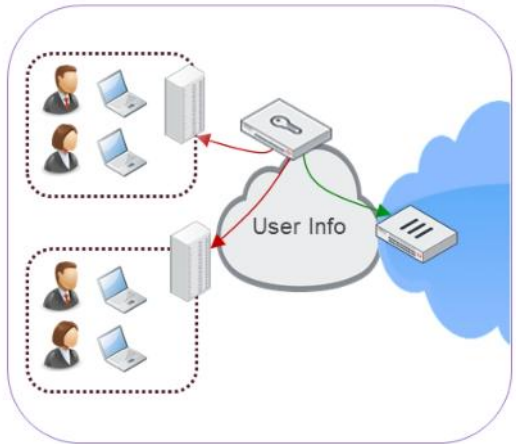
In this section, you will learn about FSSO collection methods.



This slide shows the methods you can use to collect sign-on 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 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.

Active Directory Polling

- WinSec logs polling
  - Available for FortiAuthenticator and software collector agent
- WMI log-based AD polling
  - Available for FortiAuthenticator and software collector agent
  - Five-second polling
- Net API-based AD polling
  - Software collector agent only
  - Five-second polling



FORTINET

 5

FortiAuthenticator and the software Collector Agent are able to poll Windows domain controllers to monitor the security event logs for login events. Polling of the Security Event log is configured to occur every five seconds so that any login event that has occurred since the previous poll is captured and entered into FSSO. The Collector Agent can be configured to use WMI logs to extract login and logout information. Event log polling may run a bit slower, but will not miss events. Event log polling is required if there are Mac OS users logging in to Windows AD.

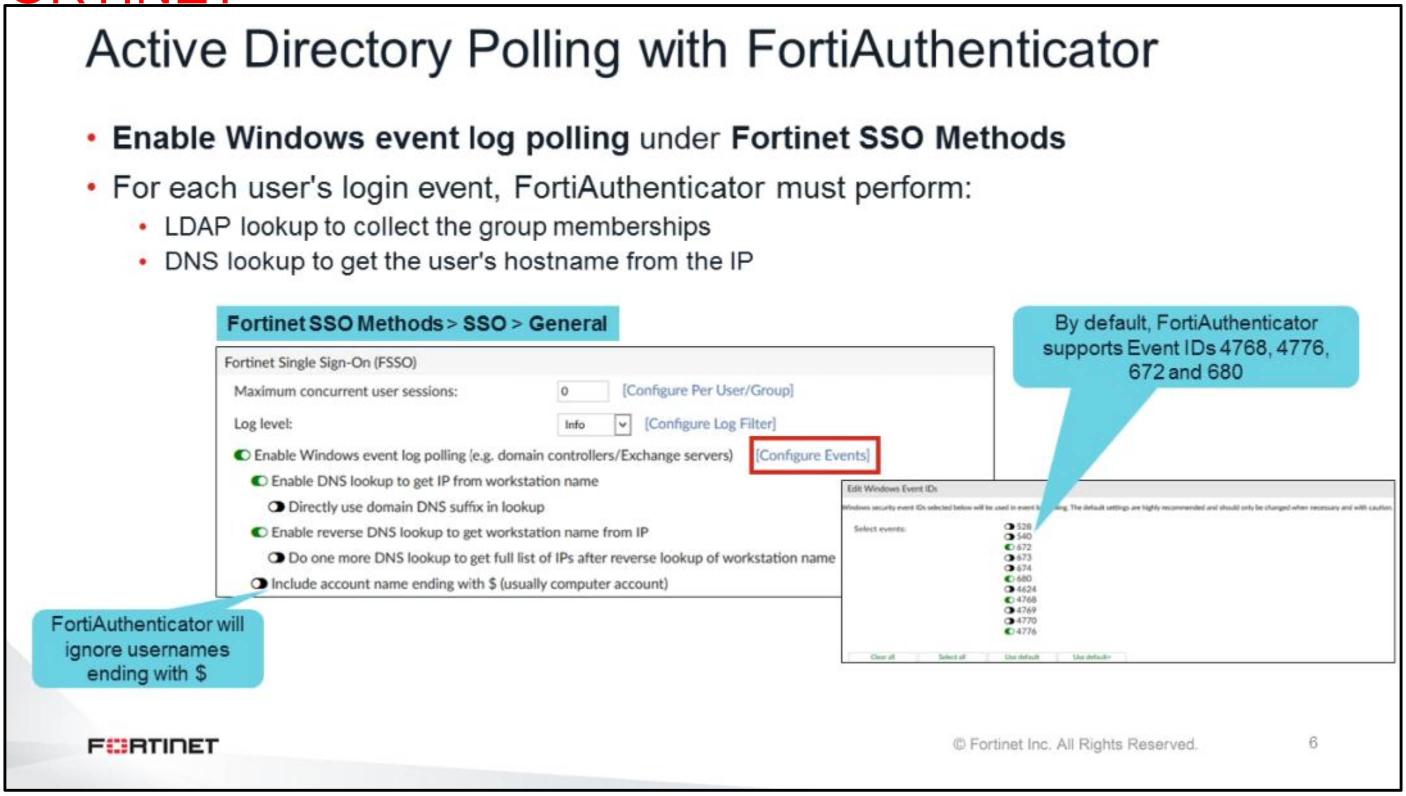
Windows Management Instrumentation (WMI) is a Windows API designed to get system information from a Windows server. Collector Agent is a WMI client and sends WMI queries for user logon events to the domain controller (DC), which, in this case, is a WMI server. The main advantage of this mode is the Collector 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 polling is used to retrieve server logon sessions. This includes the logon event information for the collector agent. NetAPI runs faster than Event log polling, but it may miss some user logon events under heavy system load. It requires a query round-trip time of less than 10 seconds. This method is available only on the software-based Collector Agent.

Note that while login events can be detected from the Security Event logs, you can’t detect logout events. This is because logout events can be triggered by many different processes, not just the logout process.

While some methods natively support logout detection (like the FortiClient SSO Mobility Agent), others, such as AD polling, do not. To enable logout detection, FortiAuthenticator supports Windows Management Instrumentation (WMI) polling to identify the current logged-in user state for a device and then log the user out. You can set a manual timeout period, to remove the user from the authorization table.

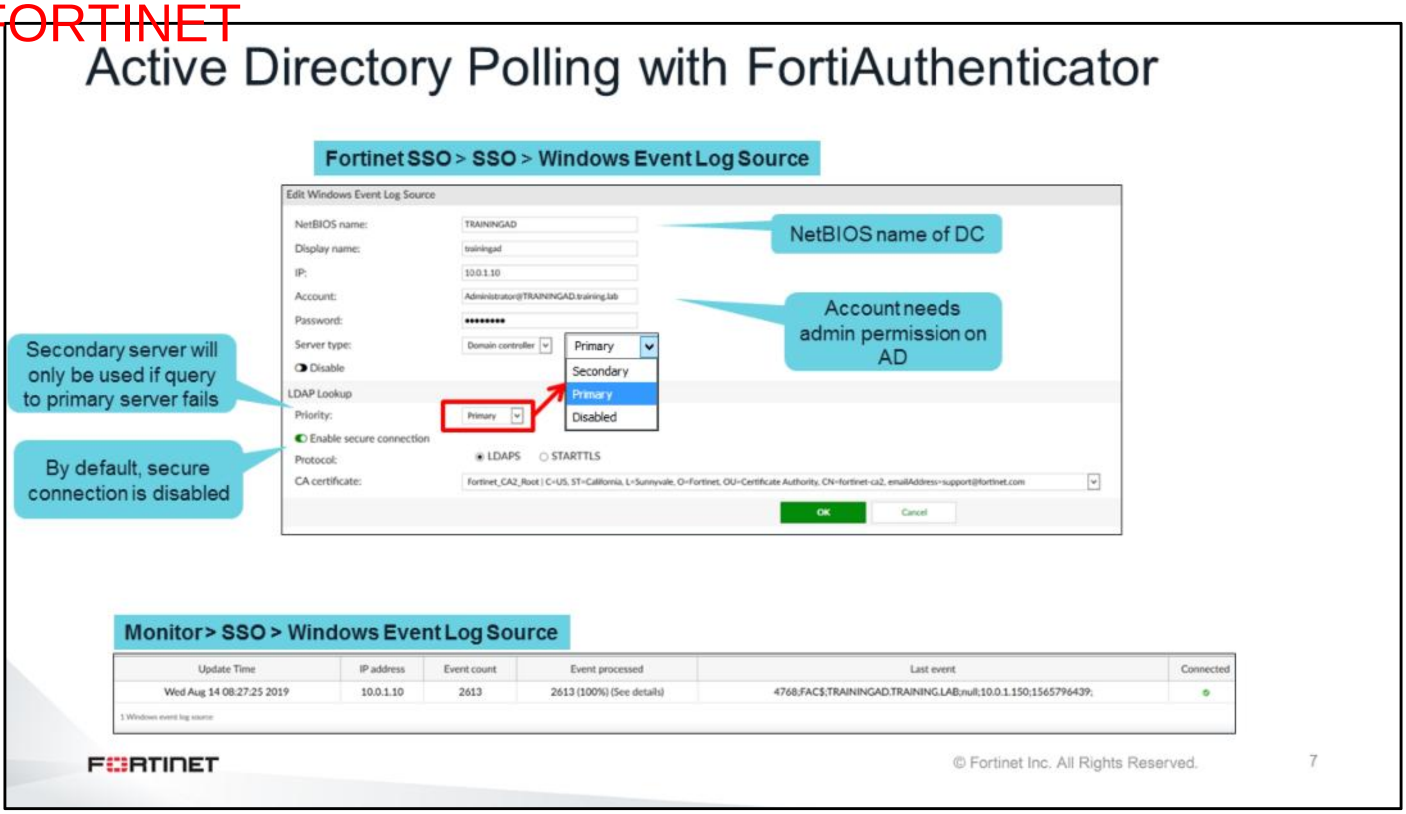
By default, FortiAuthenticator ignores events from usernames ending with a $ sign.



You can enable the Windows AD polling method on FortiAuthenticator by clicking **Fortinet SSO Methods** > **SSO** > **General**. FortiAuthenticator uses LDAP lookup to collect user group memberships, and DNS lookup to get the user's hostname from the IP. 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 will not be accurate or even valid.

By default, FortiAuthenticator supports event IDs 4768, 4776, 672, and 680, however, you can enable support for the following Event IDs by clicking on **Configure Events**:
528, 540, 673, 674, 4624, 4769, 4770

Note that FortiAuthenticator will ignore usernames ending with a $ sign.

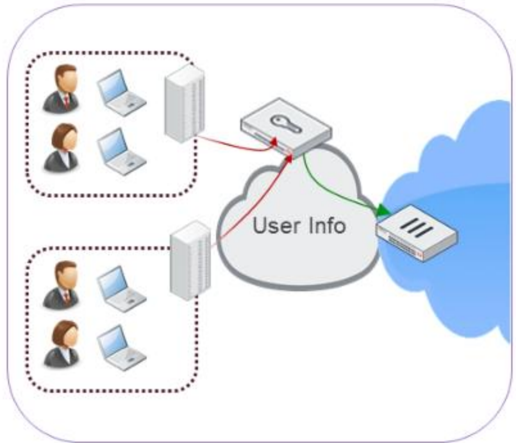


After you have enabled AD polling in the FSSO methods section, you must configure the FSSO source. You can configure FSSO source and then enable it in the FSSO methods or configure FSSO methods and then enable it in the the FSSO source section. You must enable **NetBIOS name**, **IP**, and **Account** with administrator privileges in the AD and on the password. There is an option that allows you to configure a secondary server for redundancy, and enable a secure connection using LDAPS or STARTTLS.

After you configure and enable the **Windows Event Log Source**, you can check the **Monitor SSO** section on FortiAuthenticator to verify that FortiAuthenticator can poll login events.

FSSO Agent

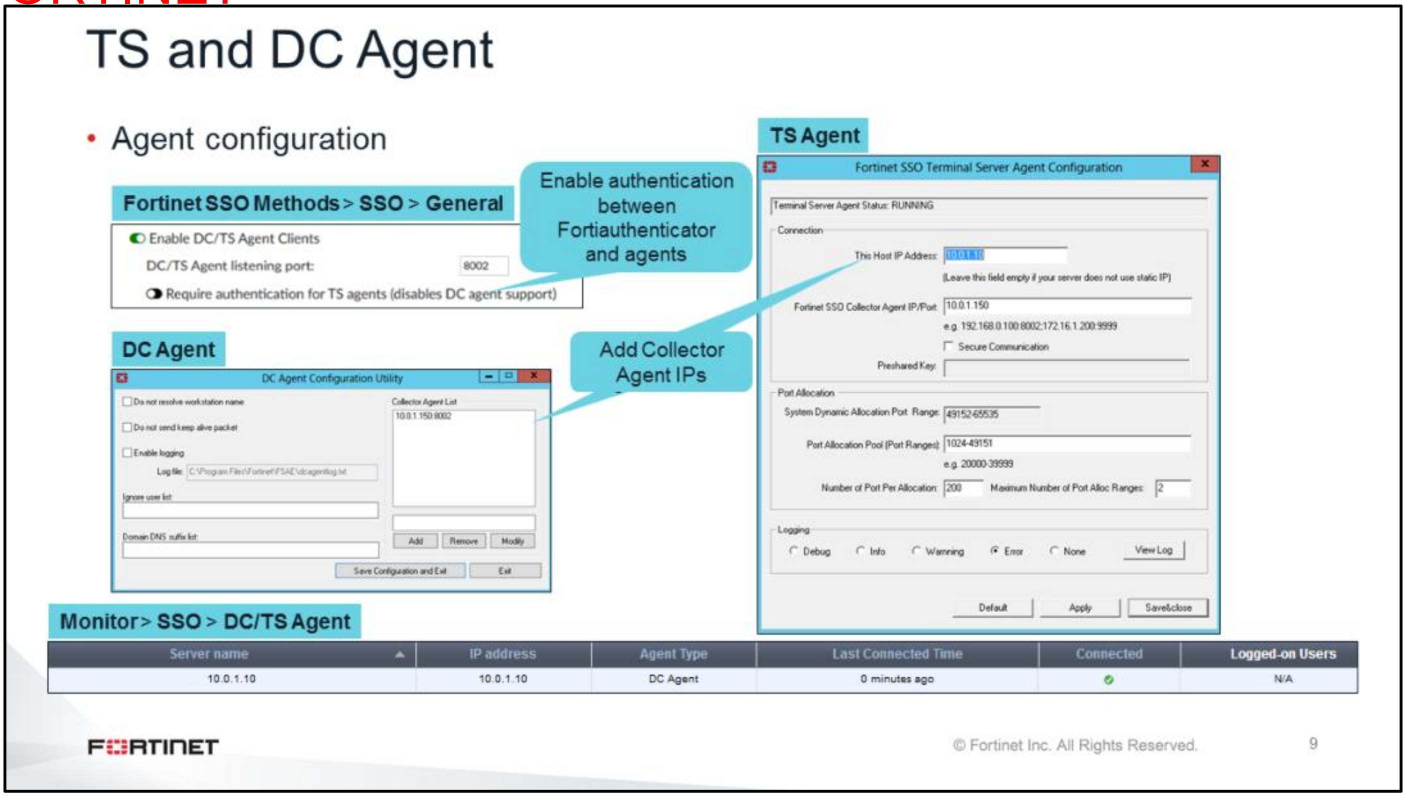
- DC agent
  - DC agent is installed on all DCs
  - Monitors user logons in real-time
  - Logon events pushed to the Collector Agent in real-time
- TS agent
  - Installed on Citrix terminal servers
  - Monitors user logons in real-time
  - Works just like DC agent on AD domain controller



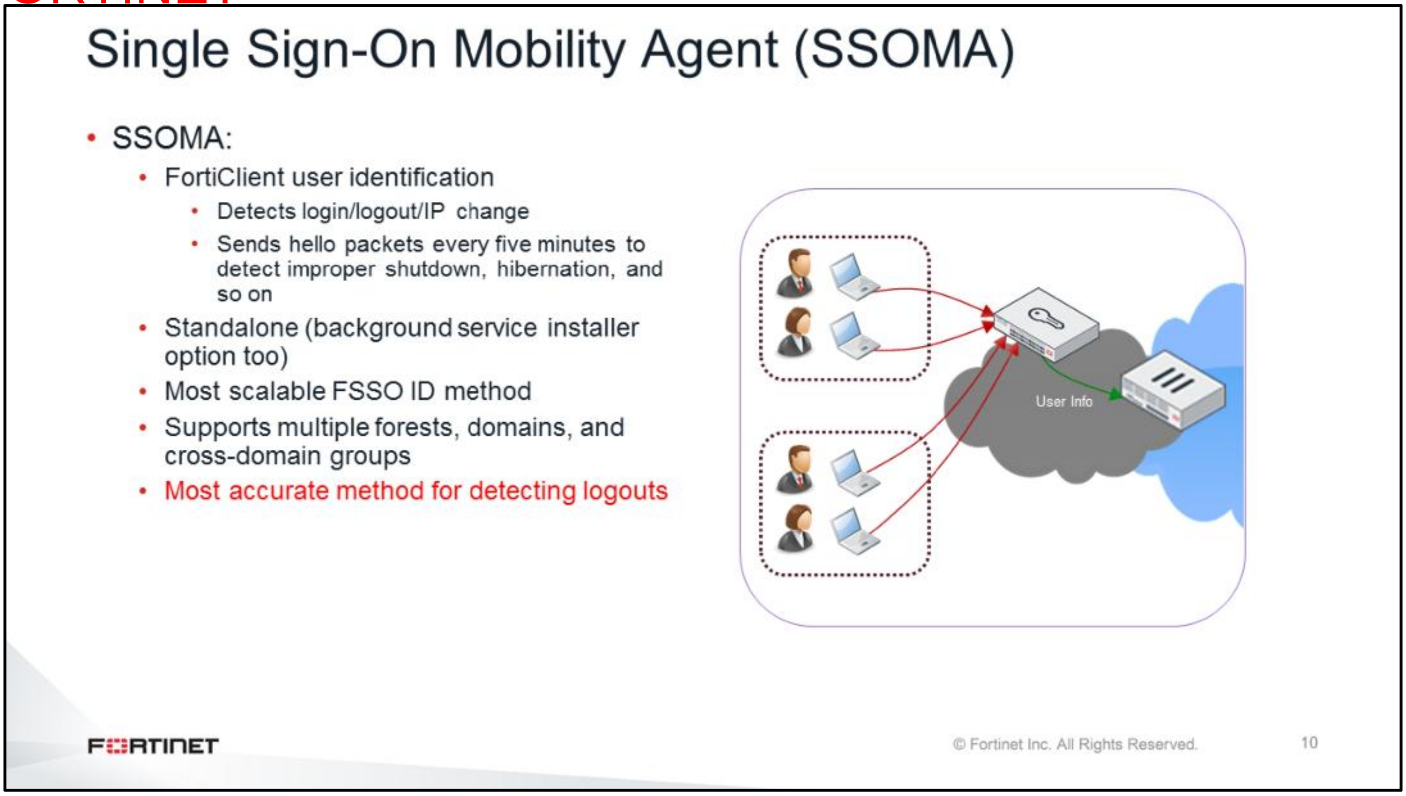
In DC agent mode, a Fortinet authentication agent is installed on each domain controller. These DC agents monitor user logon events and pass the information to FortiAuthenticator (which is a collector agent), which stores the information and sends it to FortiGate.

The DC agent installed on the DC is not a service like the collector agent—it is a DLL file called `dcagent.dll` that is installed in the Windows\system32 directory. It must be installed on all DCs of the domains that are being monitored. DC agent mode provides reliable user logon information, however, you must install a DC agent on every domain controller. A restart is needed after the agent is installed. Each installation requires some maintenance as well. For these reasons, it may not be possible to use DC agent mode.

The Citrix/Terminal Server (TS) agent is installed on a Citrix terminal server to monitor user logons in real time. It functions much like the DC agent on a Windows AD domain controller.



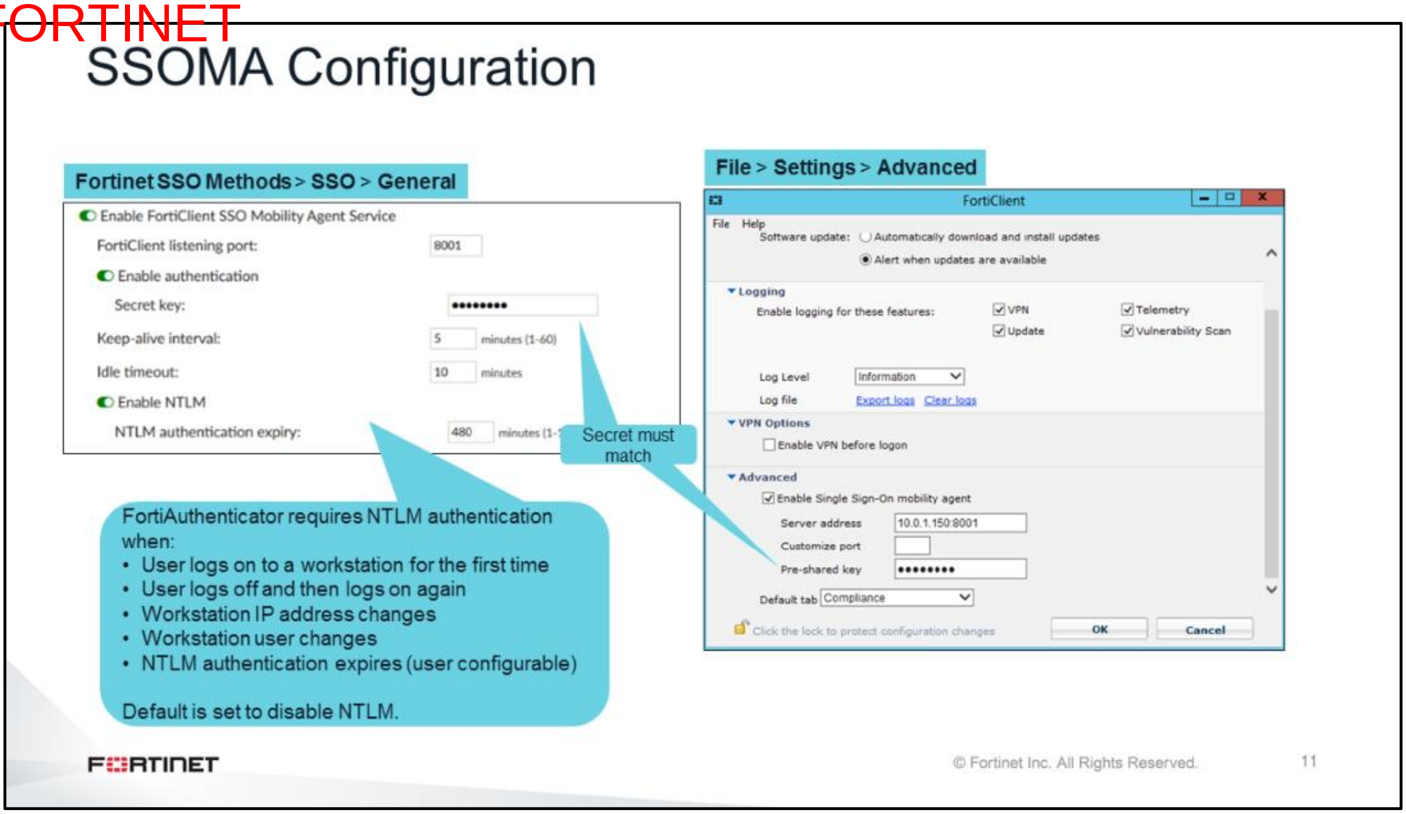
You must enable the DC/TS agent under in FSSO methods on FortiAuthenticator to allow communication between TS/DC agents and FortiAuthenticator. You can also enable optional authentication for added security. You must configure both the TS/DC agent and FortiAuthenticator with the same password.



SSOMA is a feature of FortiClient 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 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 de-authenticates the user



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 preshare keys, and configure keepalive and idle timeout intervals.

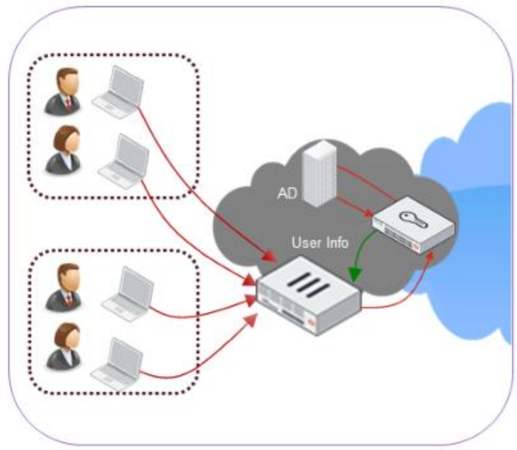
Optionally, you can enable NTLM within SSOMA settings that will work in conjunction with FSSO. When enabled, FortiAuthenticator requires NTLM authentication when:

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

By default, NTLM is disabled.

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



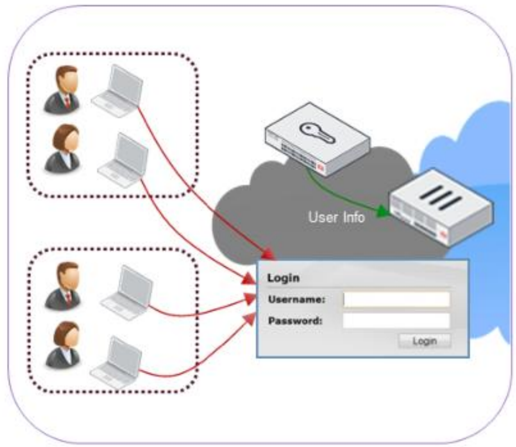
FORTINET

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.

FSSO Method—Portal Authentication and Widgets

- Portal authentication and widgets
  - Captive 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)

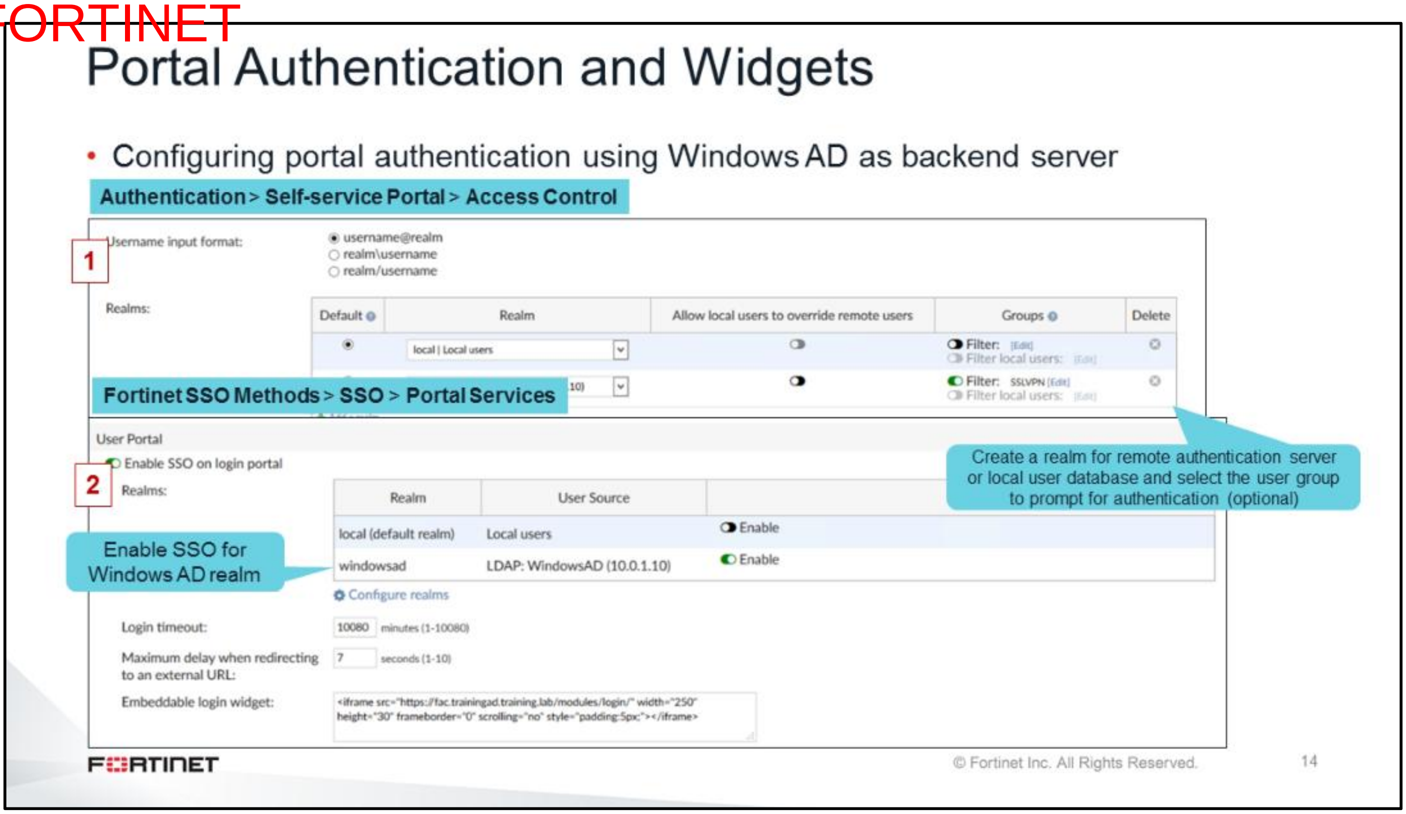


FORTINET

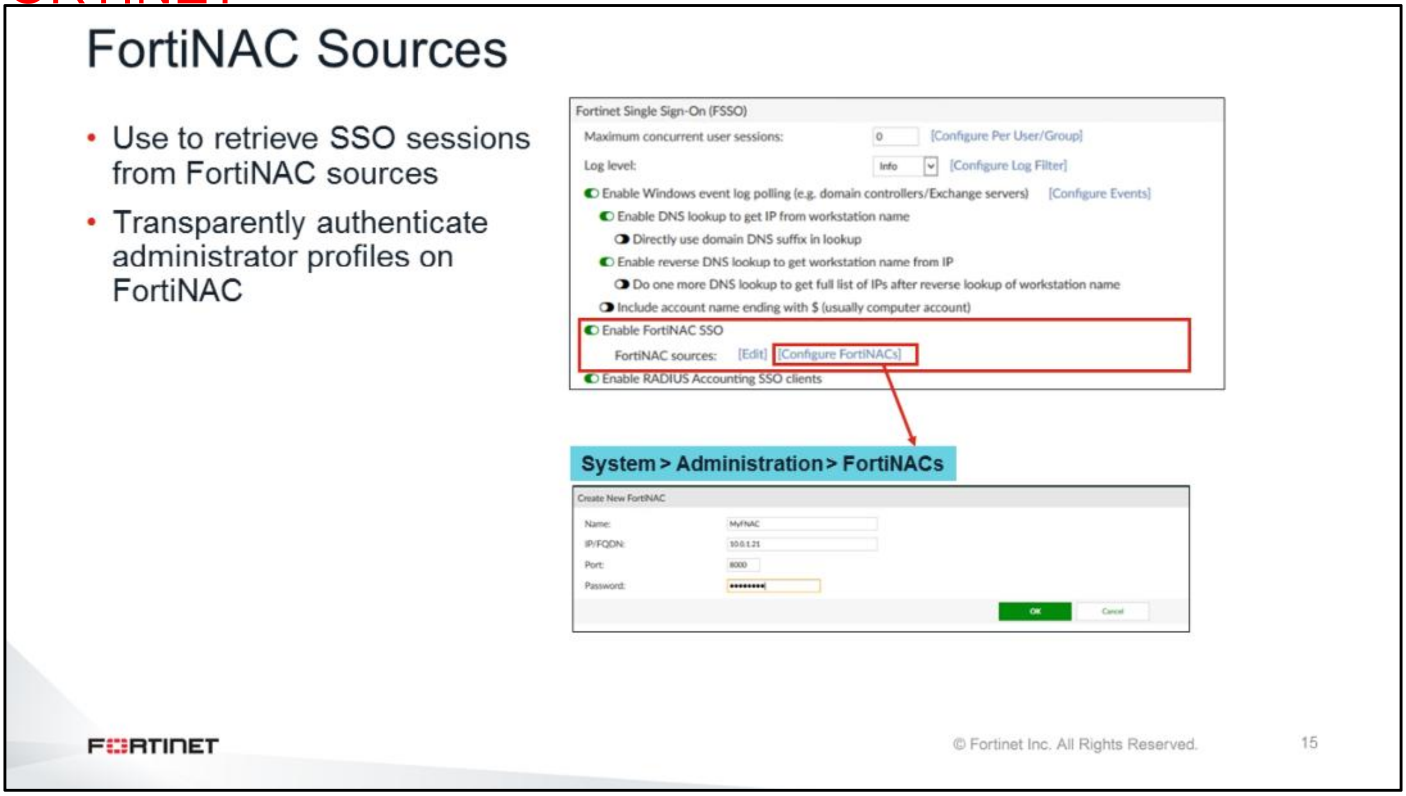
 13

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.



Portal authentication and widgets require you to configure a self-service portal 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 that for SSO will use.

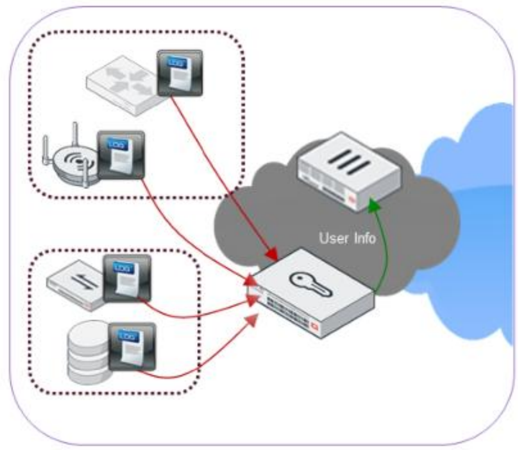


Select **Enable FortiNAC SSO** to enable the retrieval of SSO sessions from FortiNAC sources.

Similar to FortiOS, FortiAuthenticator can incorporate the use of administrator profiles. You can grant each administrator either full permissions, or a customized admin profile. Profiles are defined as aggregates of read-only or read/write permission sets. The most commonly used permission sets are predefined, but you can also create custom permission sets.

External Syslog

- Syslog SSO
  - Receive external syslog feeds to learn user feeds
    - 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

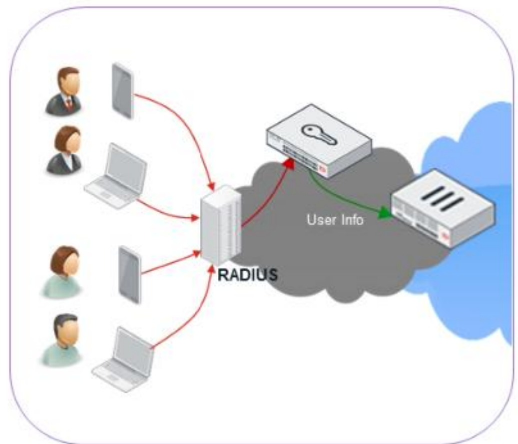


 16

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 logout 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.

RADIUS Accounting Packets SSO

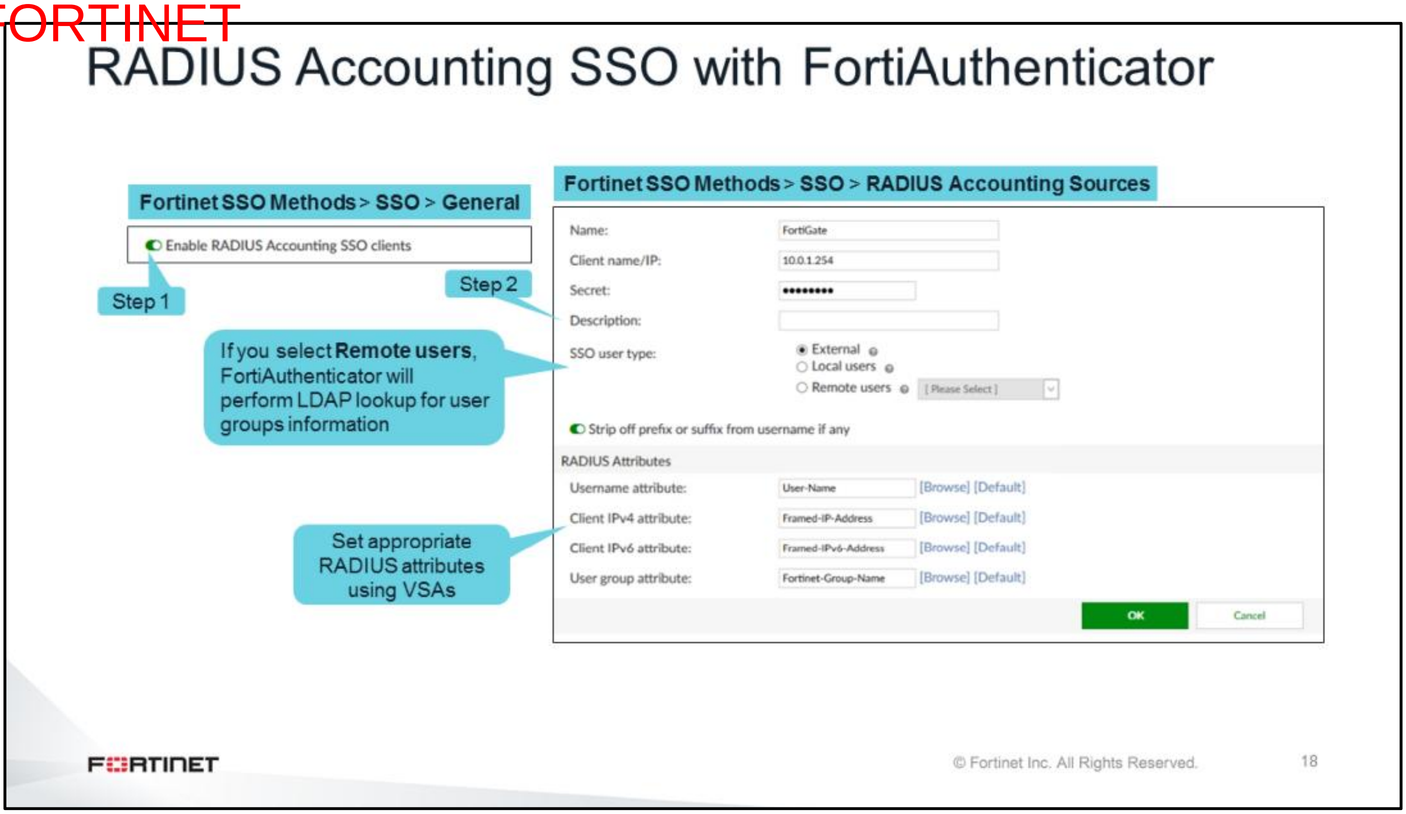
- RADIUS accounting
  - RADIUS accounting start, interim, and stop packets used as a source of user identification
  - Can come from any source that is capable of sending RADIUS accounting packets
    - VPN gateways
    - Wireless controller/APs
    - Switches



 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.

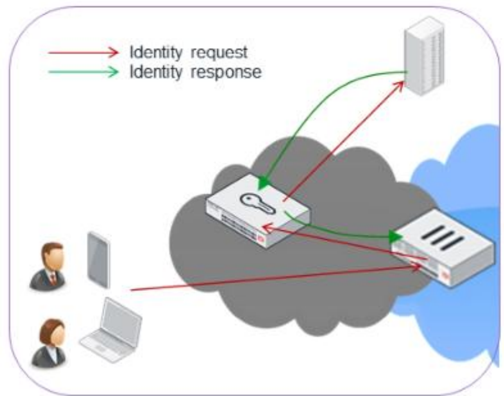
The benefit of using this method is that vendors who support sending such packets, do not require any direct support from FortiAuthenticator (they use standard RADIUS which is already supported), and require minimal change to enable the input of user authentication data into FSSO.



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 users' 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 can the **External** SSO user type, FortiAuthenticator will extract only the information that is included in the accounting message and will not validate the group membership.

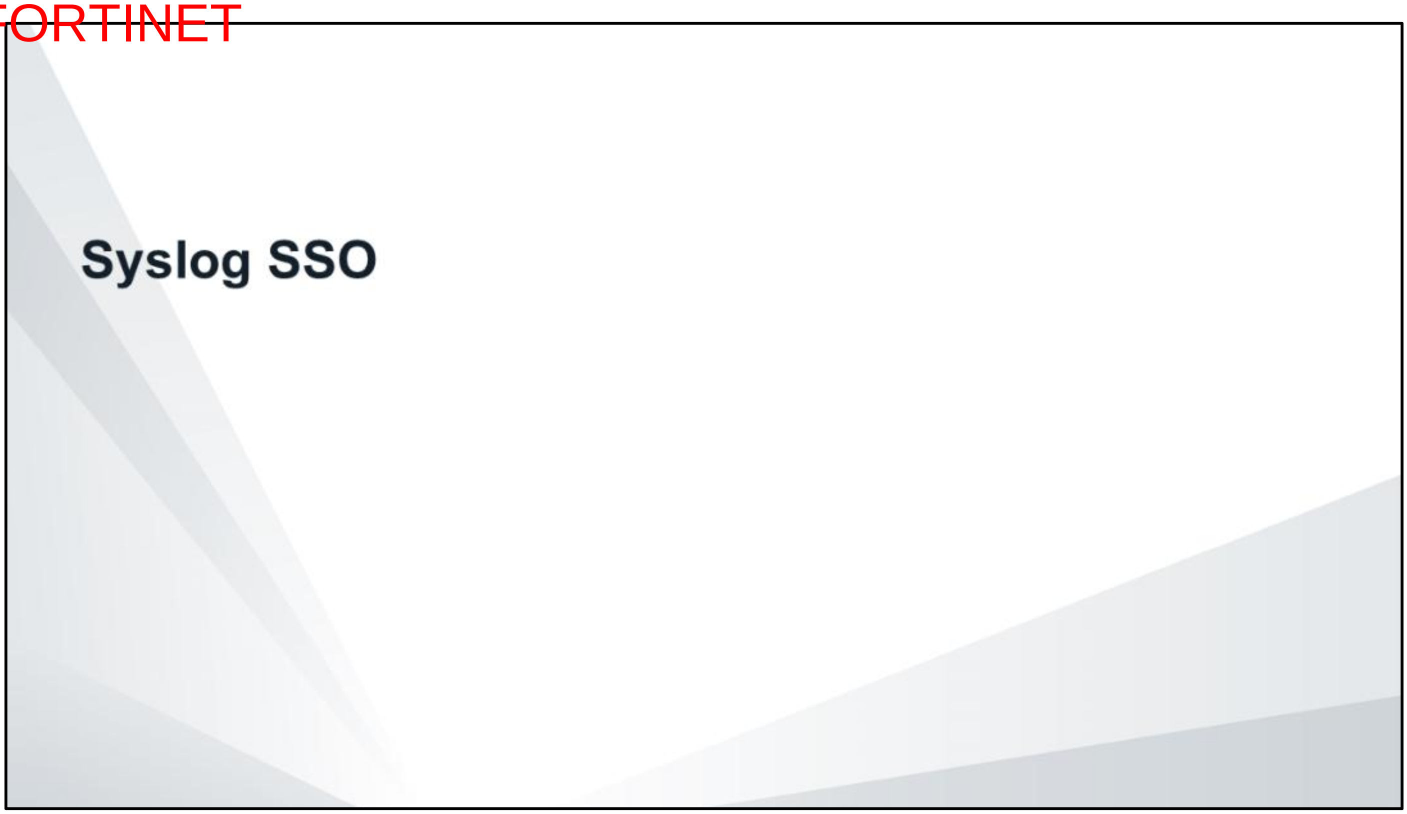
Security Assertion Markup Language (SAML)

- 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)
  - 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) checks with the existing third-party IDP to get the user's identity
  4. FortiAuthenticator pushes identity and group information to FSSO
  5. FortiAuthenticator redirects the user to the original URL
  6. FortiGate sees the user in FSSO and allows the user to pass

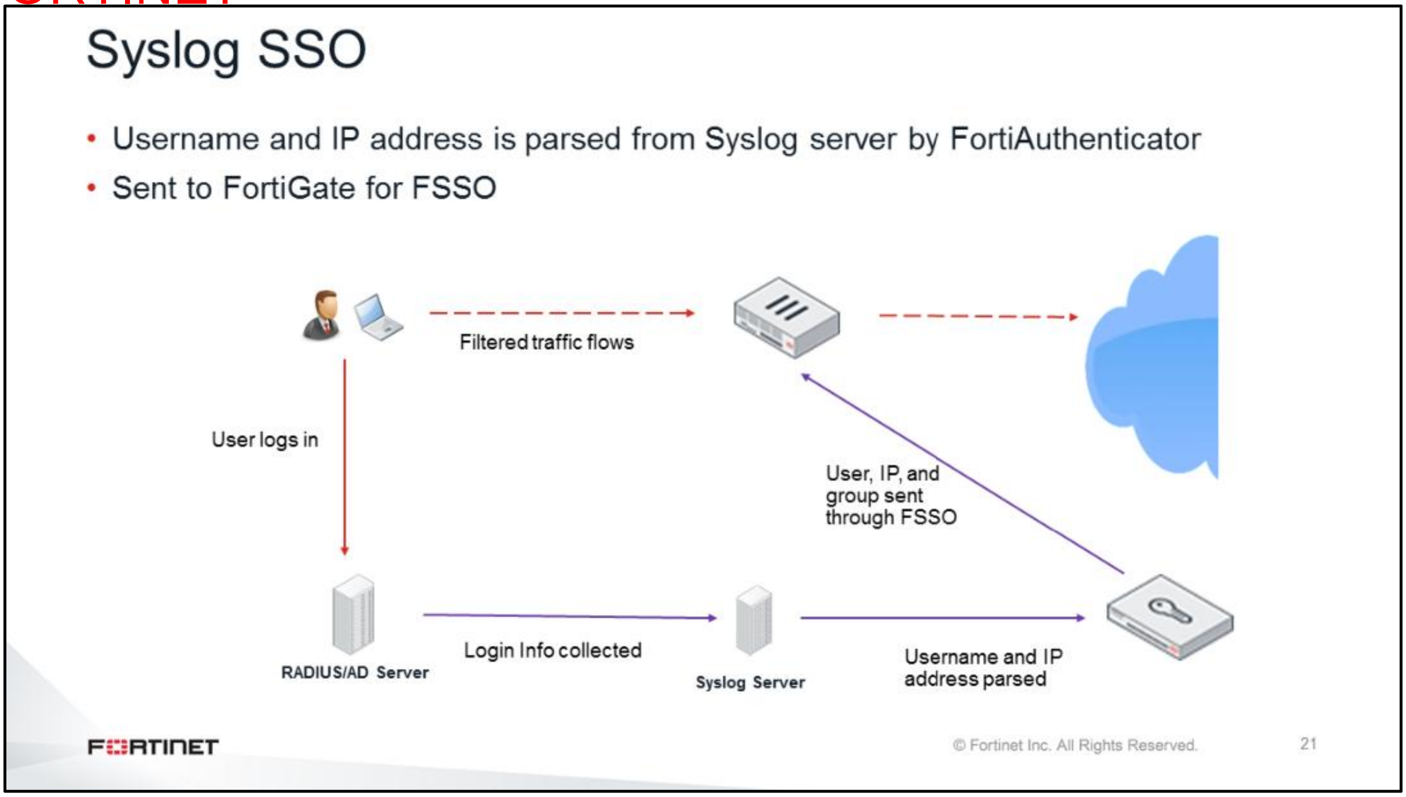


 19

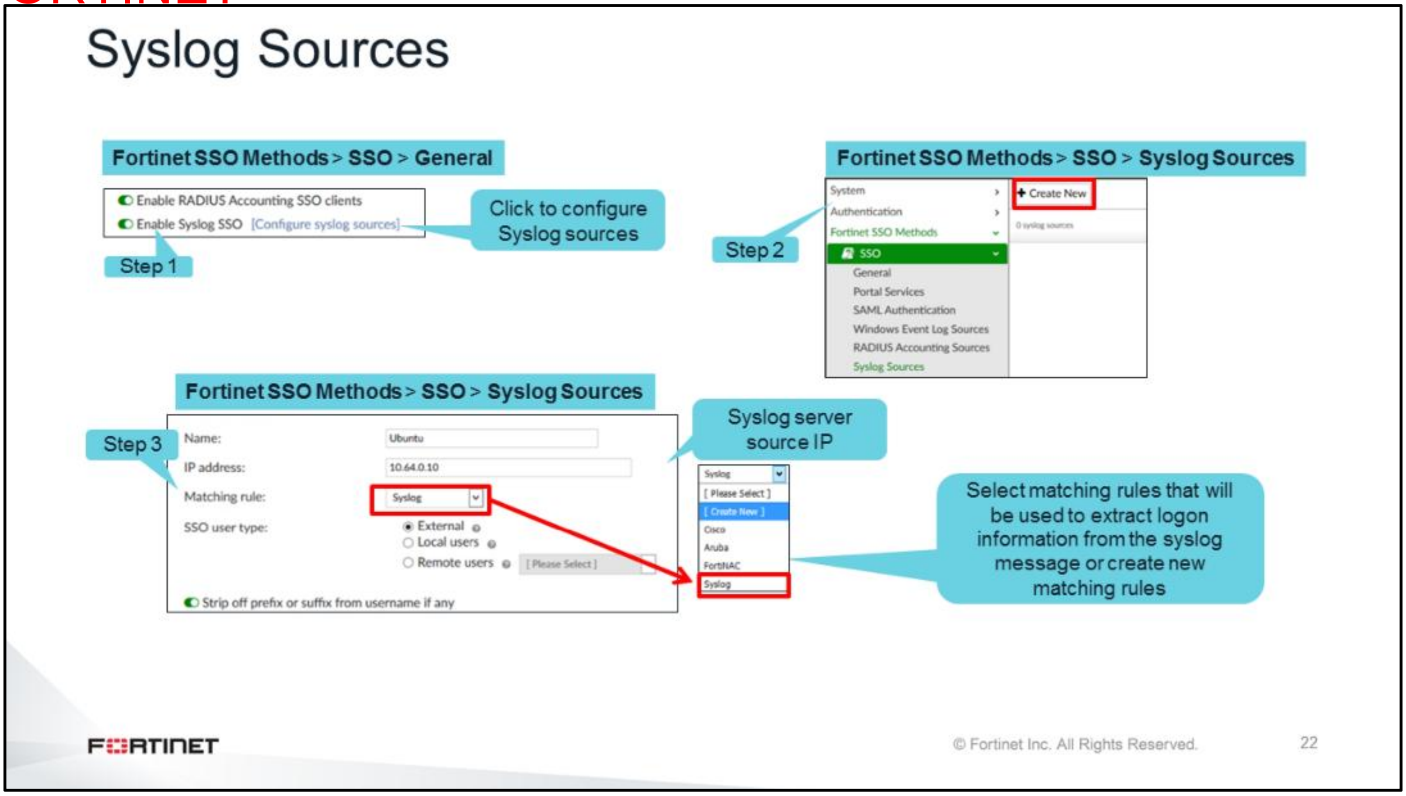
FortiAuthenticator can use SAML assertions to generate FSSO events when you use FortiAuthenticator as a SAML service provider. In service-provider mode, FortiAuthenticator can use SAML assertions to extract username, IP address, and other available SAML attributes to generate FSSO events. These events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



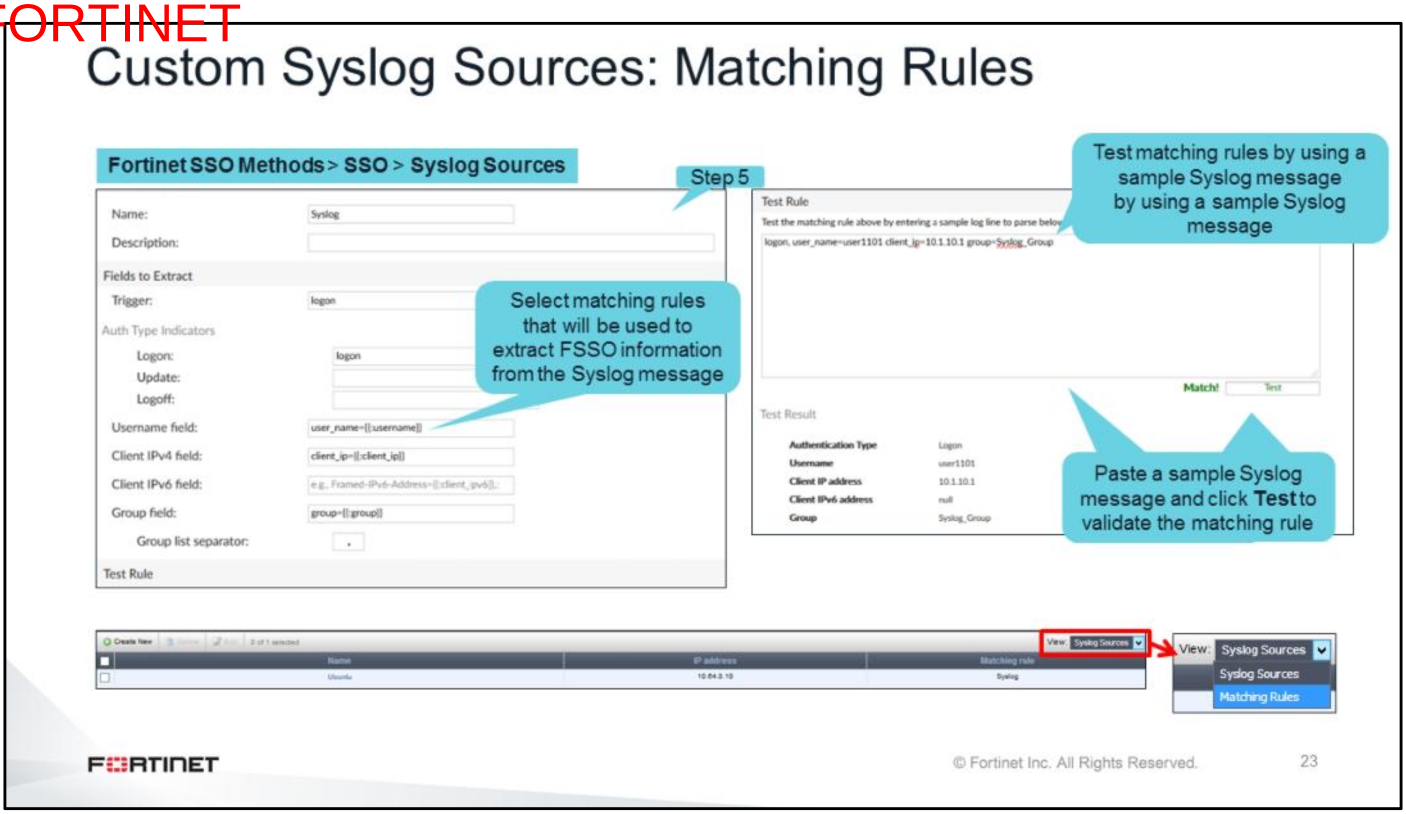
In this section, you will learn about Syslog SSO using FortiAuthenticator.



The 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.



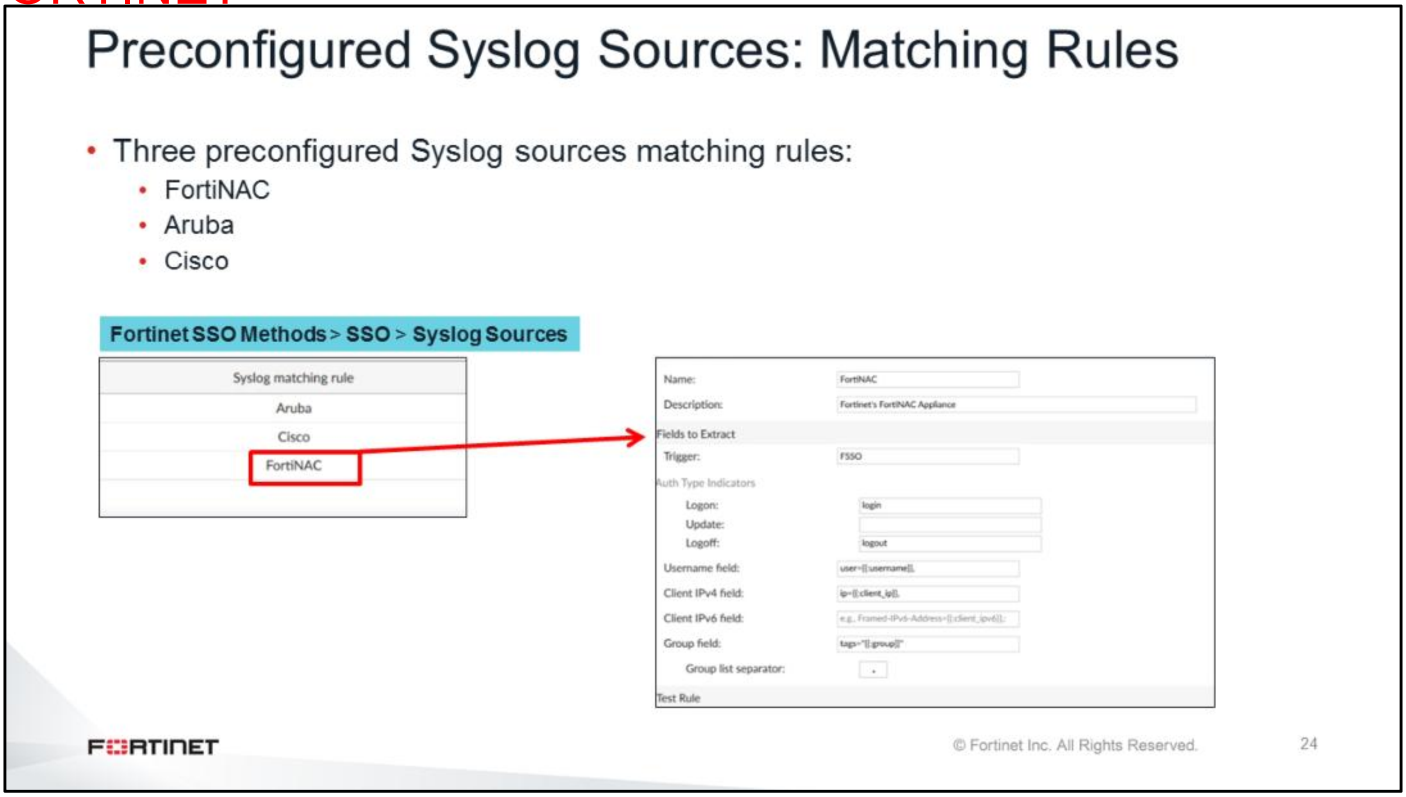
Syslog objects include sources and matching rules. Sources identify the entities sending the Syslog messages, and matching rules are used to extract the events from the Syslog messages. FortiAuthenticator ignores messages coming from non-configured sources.



Once you have specified a Syslog source, you must configure a matching rule. 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 key words to trigger logon, update, and logoff messages. FortiAuthenticator will use these fields to extract the username and IP address from the messages to convert them to FSSO events.

You can easily test custom matching rules by using the **Test Rule** section to verify that FortiAuthenticator can extract all the required information from the Syslog feed.



There are three preconfigured matching rules for some third-party Syslog server formats:

- FortiNAC
- Aruba
- Cisco

Syslog SSO Sessions

- Monitoring Syslog SSO Sessions on FortiAuthenticator

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
Tue Aug 20 10:19:35 2019	Tue Aug 20 10:19:35 2019	10.1.10.1	10.1.10.1	DEFAULT	SSO_EXT_USER	USER1101	Syslog	USER1101+SYSLOG_GROUP
Tue Aug 20 10:19:37 2019	Tue Aug 20 10:19:37 2019	10.1.10.2	10.1.10.2	DEFAULT	SSO_EXT_USER	USER1102	Syslog	USER1102+SYSLOG_GROUP
Tue Aug 20 10:19:39 2019	Tue Aug 20 10:19:39 2019	10.1.10.3	10.1.10.3	DEFAULT	SSO_EXT_USER	USER1103	Syslog	USER1103+SYSLOG_GROUP
Tue Aug 20 10:19:41 2019	Tue Aug 20 10:19:41 2019	10.1.10.4	10.1.10.4	DEFAULT	SSO_EXT_USER	USER1104	Syslog	USER1104+SYSLOG_GROUP
Tue Aug 20 10:19:43 2019	Tue Aug 20 10:19:43 2019	10.1.10.5	10.1.10.5	DEFAULT	SSO_EXT_USER	USER1105	Syslog	USER1105+SYSLOG_GROUP

5 SSO sessions

- Monitoring Syslog SSO Sessions on FortiGate

Monitor > Firewall User Monitor

Refresh | Deauthenticate | Show all FSSO Logons | Search

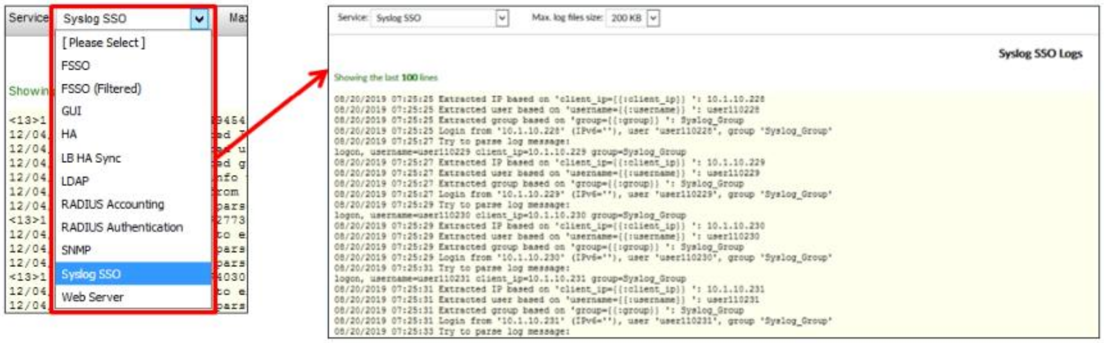
User Name	User Group	Duration	IP Address	Traffic Volume	Method
USER1101	SYSLOG_GROUP	1 minute(s) and 1 second(s)	10.1.10.1	0 B	Fortinet Single Sign-On
USER1102	SYSLOG_GROUP	1 minute(s) and 1 second(s)	10.1.10.2	0 B	Fortinet Single Sign-On
USER1103	SYSLOG_GROUP	56 second(s)	10.1.10.3	0 B	Fortinet Single Sign-On
USER1104	SYSLOG_GROUP	56 second(s)	10.1.10.4	0 B	Fortinet Single Sign-On
USER1105	SYSLOG_GROUP	56 second(s)	10.1.10.5	0 B	Fortinet Single Sign-On

 25

You can view Syslog SSO sessions on FortiAuthenticator by clicking **Monitor** > **SSO** > **SSO Sessions**. On FortiGate, you would click **Monitor** > **Firewall User Monitor,** to view the FSSO logs.

Debug Logs

- Viewing debug logs from a specific service



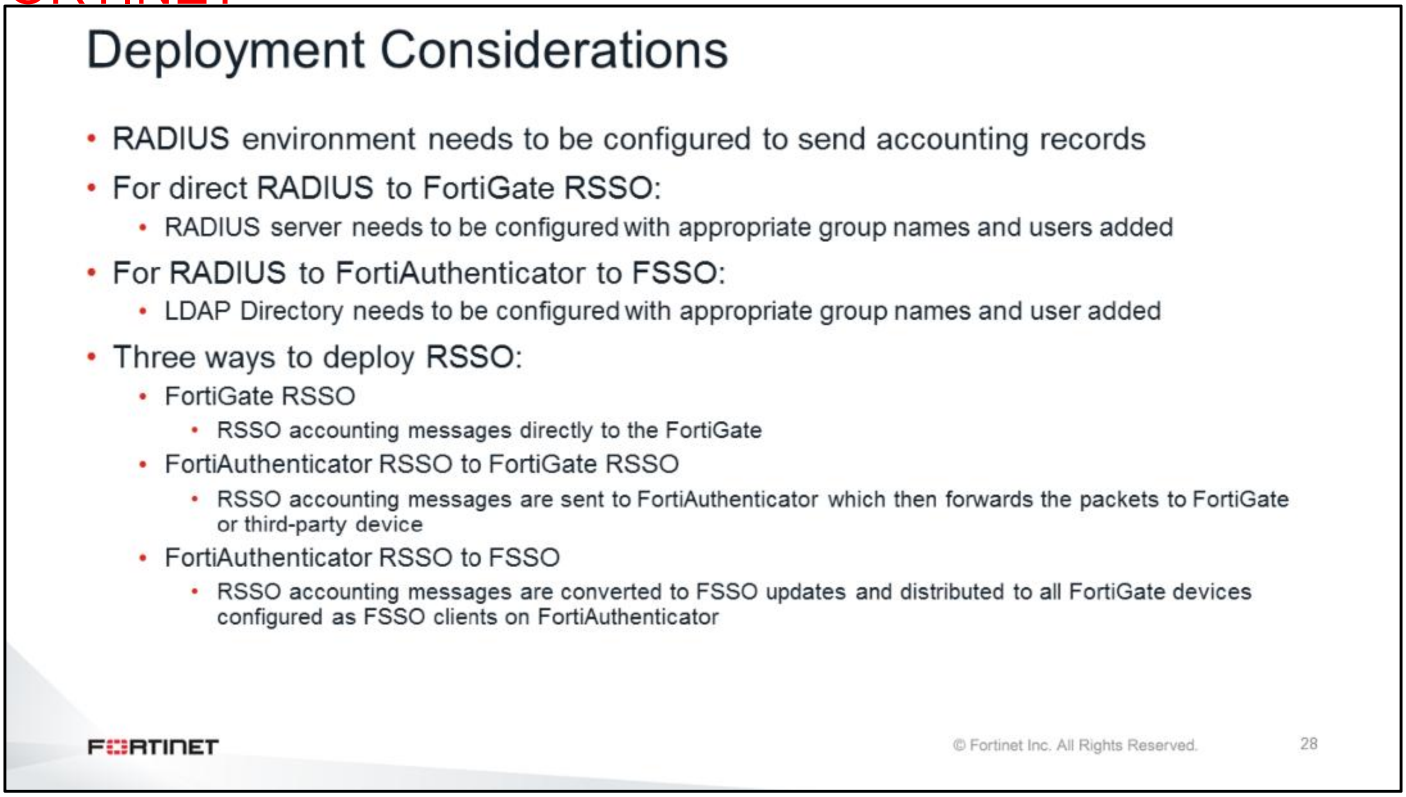
- Debug logs can be very handy when troubleshooting SSO-related issues
  - Display information-level logs from the selected service
  - View service logs that are relevant to the FSSO method that is encountering issues
  - Most recent logs are at the bottom

FURTINET

 26

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.

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



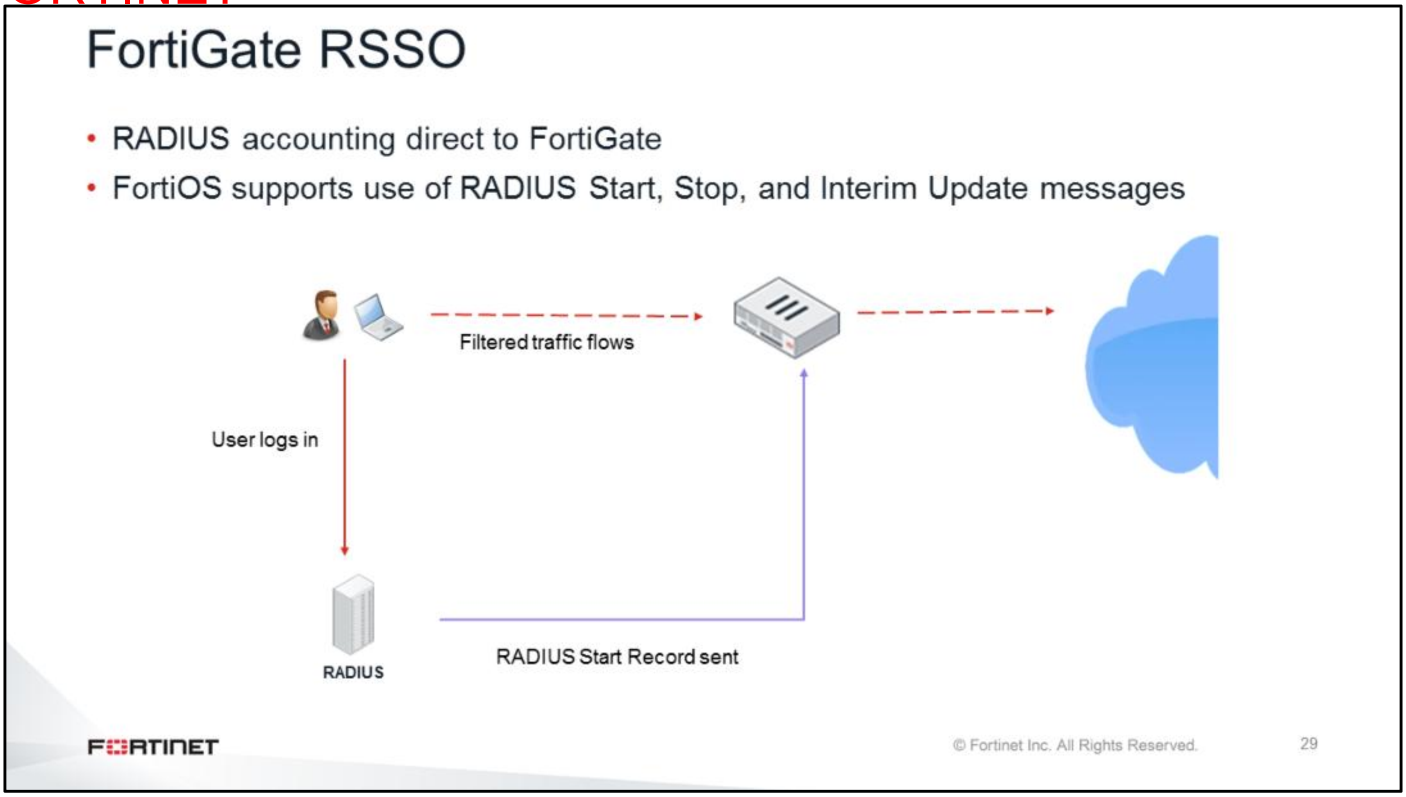
The following are important aspects that need to be considered before using RSSO:

- 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-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

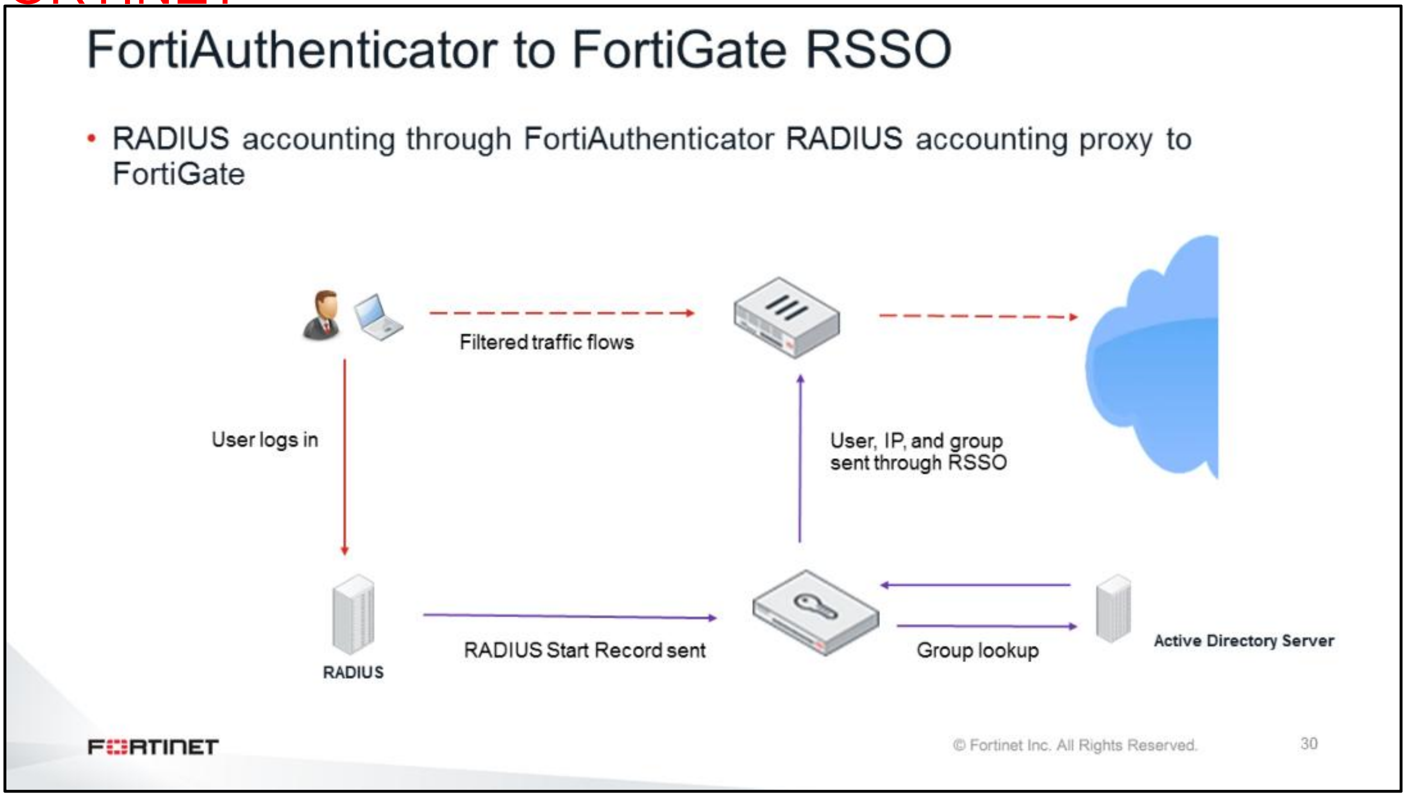
There are three different ways to deploy RSSO:

- FortiGate RSSO: RSSO accounting messages directly to the 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

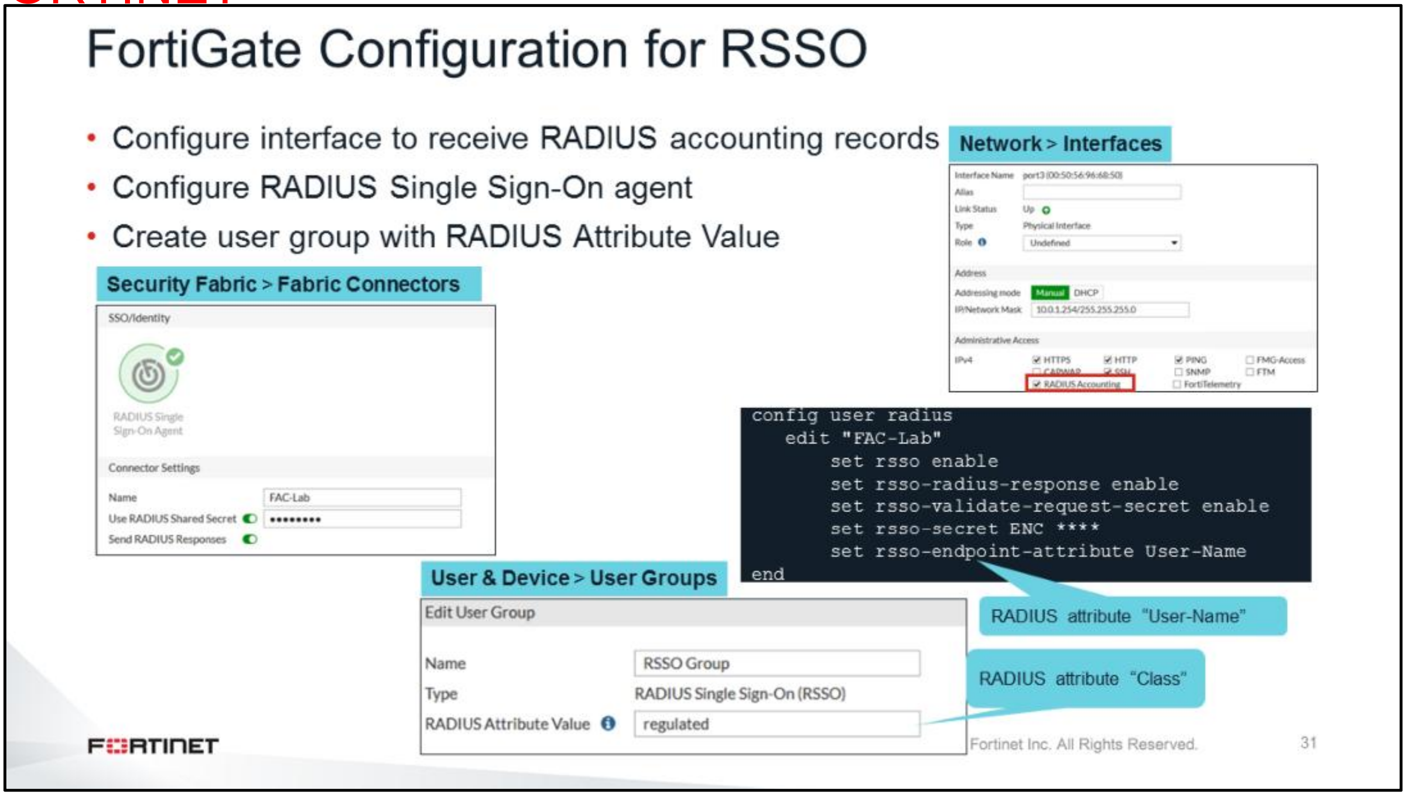
Now, you will look at each of the three methods in more detail.



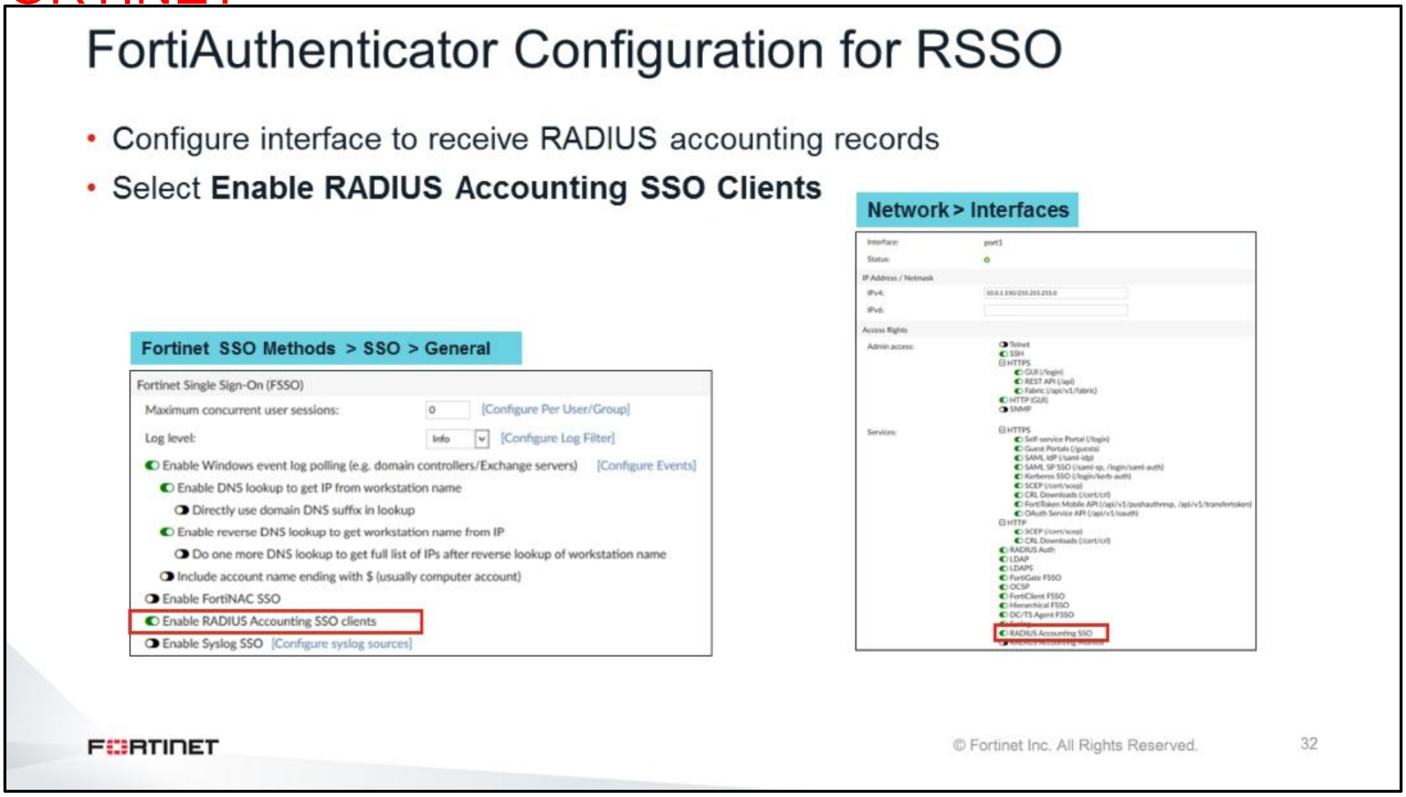
FortiOS supports the use of RADIUS Start, Stop, and Interim Update messages to authenticate and manage active users transparently. It is quite straightforward to configure FortiGate to receive and use these records is quite.



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 the RADIUS server is business-critical IT infrastructure, limiting the changes that can be made to the server configuration.



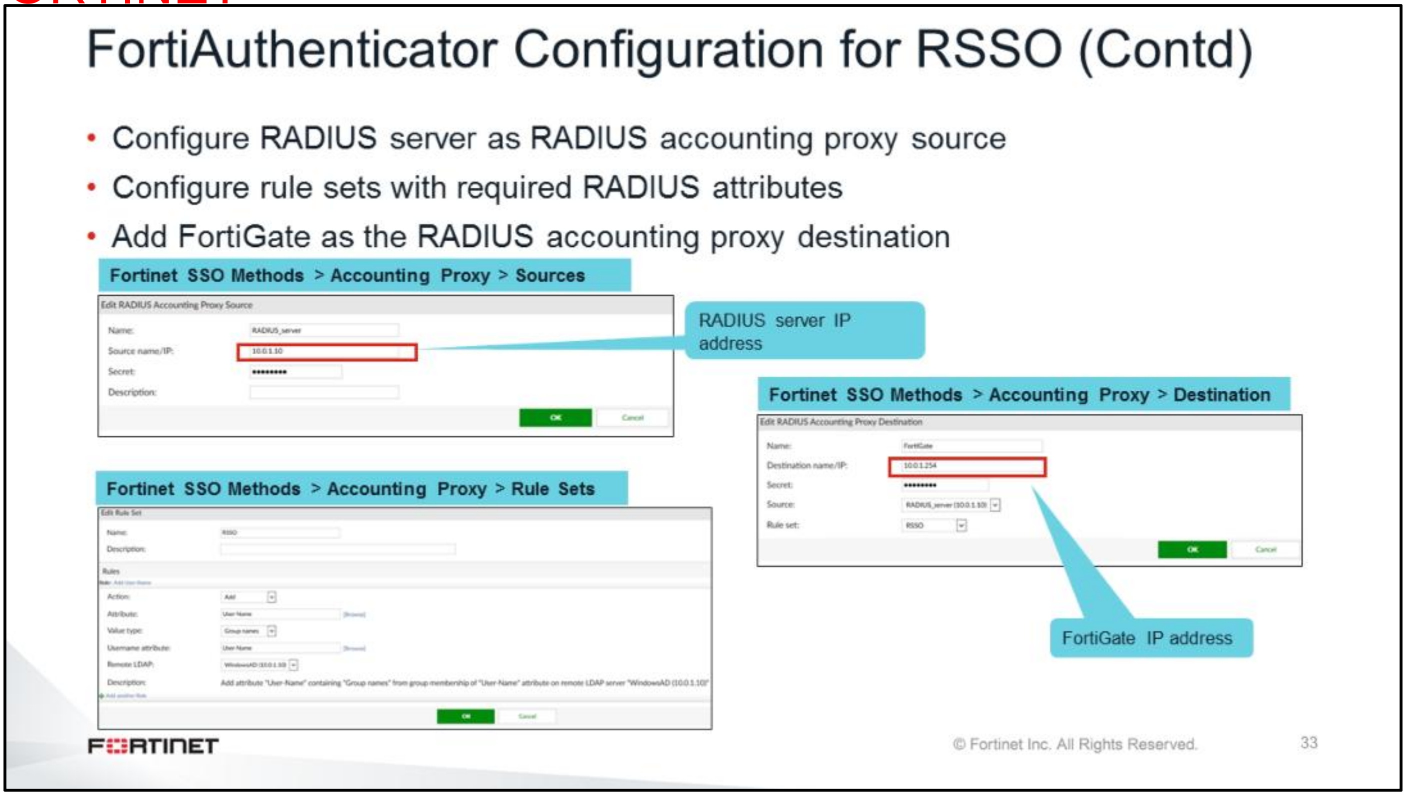
There are a few configuration steps that you must perform to enable RSSO on FortiGate. The FortiGate interface where you expect to receive the RSSO messages must have RADIUS Accounting enabled in the **Administrative Access**. Then, you must define an RSSO under **Fabric Connectors** and configure it with a unique name and RADIUS shared secret that must match those of the RADIUS accounting server. This enables a form of authentication between RSSO client (FortiGate) and the RSSO server. You will also need to create a user group locally on FortiGate, and assign the `rsso-endpoint-attribute` that will be used to match with the attribute that is sent by the RADIUS server. You can then use the user groups on a firewall policy to enable access for RSSO users.



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

Step 1 – Configure the interface to receive RADIUS accounting records.
Step 2 – Select **Enable RADIUS Accounting SSO Clients.**

Note that you can enable **RADIUS Accounting Monitor** to look for RADIUS Authentication Request messages, which uses port 1646.

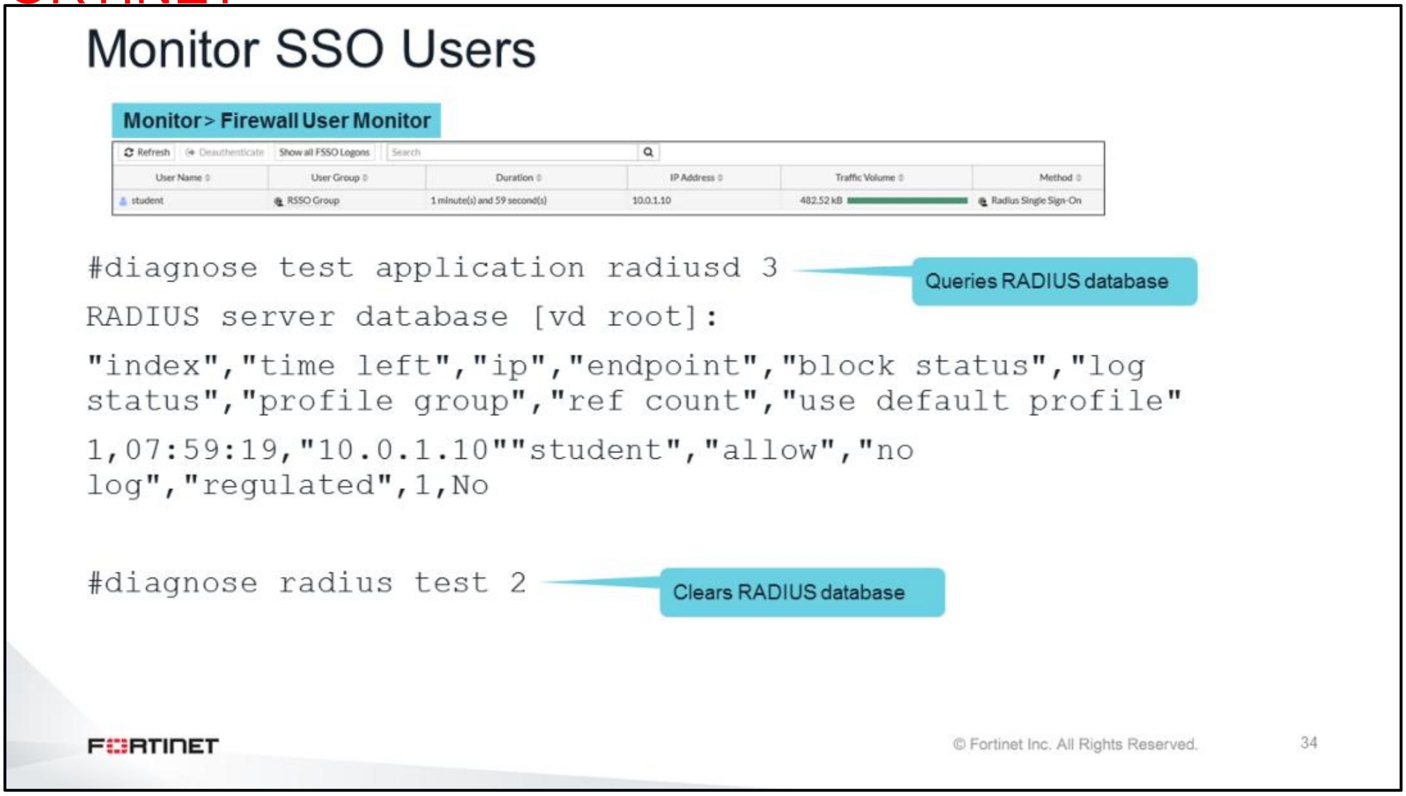


Step 3 – Configure the RADIUS server as a RADIUS accounting proxy source

Step 4 – Configure rule sets with the required RADIUS attributes
Select **Add** for a new attribute , and select **Modify** to translate an existing attribute FortiAutheticator uses the Username attribute to parse group membership information from the LDAP server. FortiAuthenticator add the Value type attribute to the accounting messages it forwards to FortiGate. To add the user's group membership information, select group names. Select the LDAP server that FortiAuthenticator will run the group membership query on.

Step 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 message 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**.



There are various commands available on FortiGate to view information regarding RSSO users.

The command `diagnose test application radiusd 3` queries the RADIUSD database for all RADIUS users currently logged in.

The command `diagnose radiusd test 2` clears the RADIUSD database of all RSSO users. To clear an individual user you must send an Accounting Stop record for that user.

Querying RADIUS Database

`#diagnose test application radius <code>`

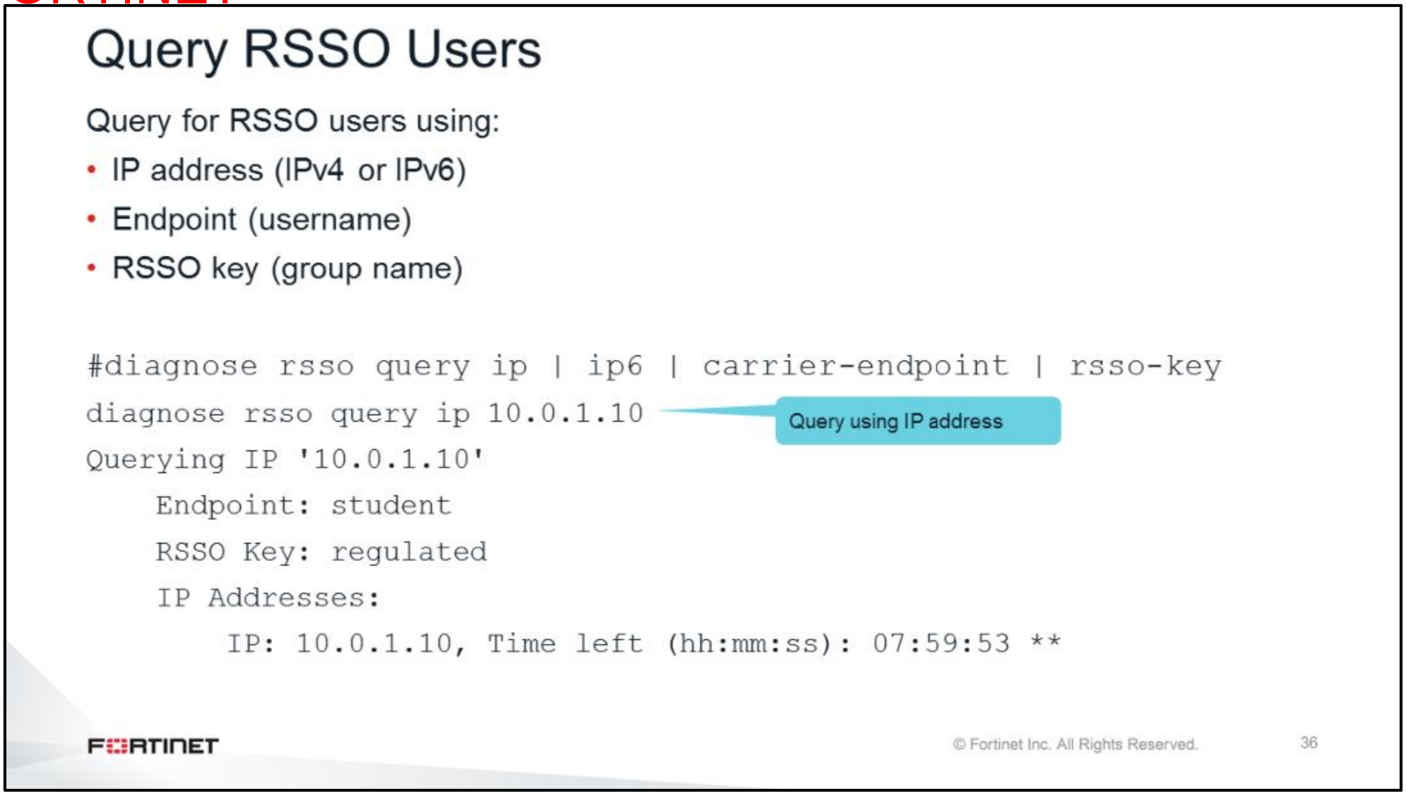
Queries or clears entire RADIUS database

<code>	Description
2	Clear RADIUS server database
3	Show RADIUS server database
33	Show RADIUS server database (with start time)
4	Show RADIUS server database info
9	Check HA context table checksums
11	Show HA sync connection status
20	Show RADIUS server configuration cache
21	Show RADIUS server interface configuration cache
99	Restart RADIUSD

FORTINET

35

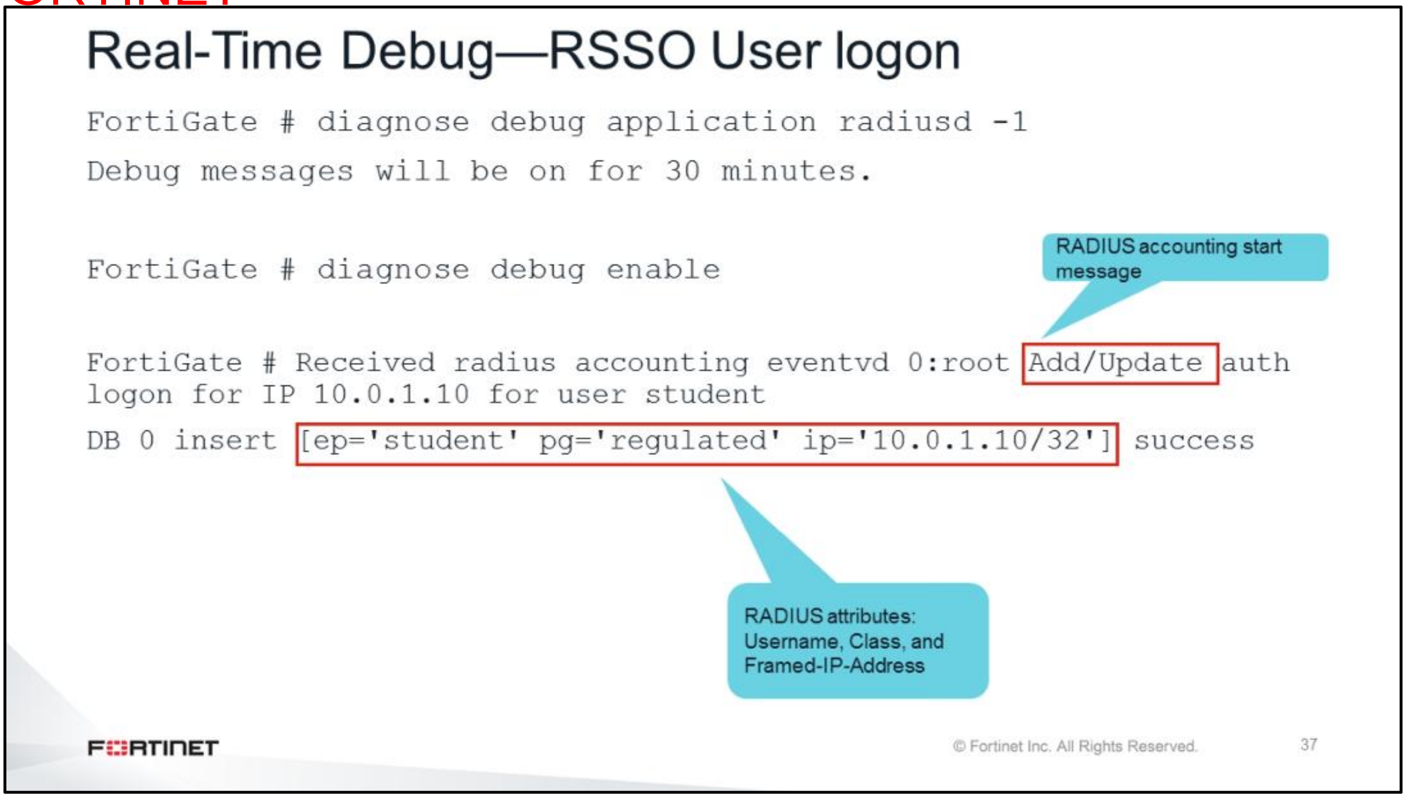
The command `diagnose test application radiusd` allows you to query, clear, or restart the RADIUSD database.



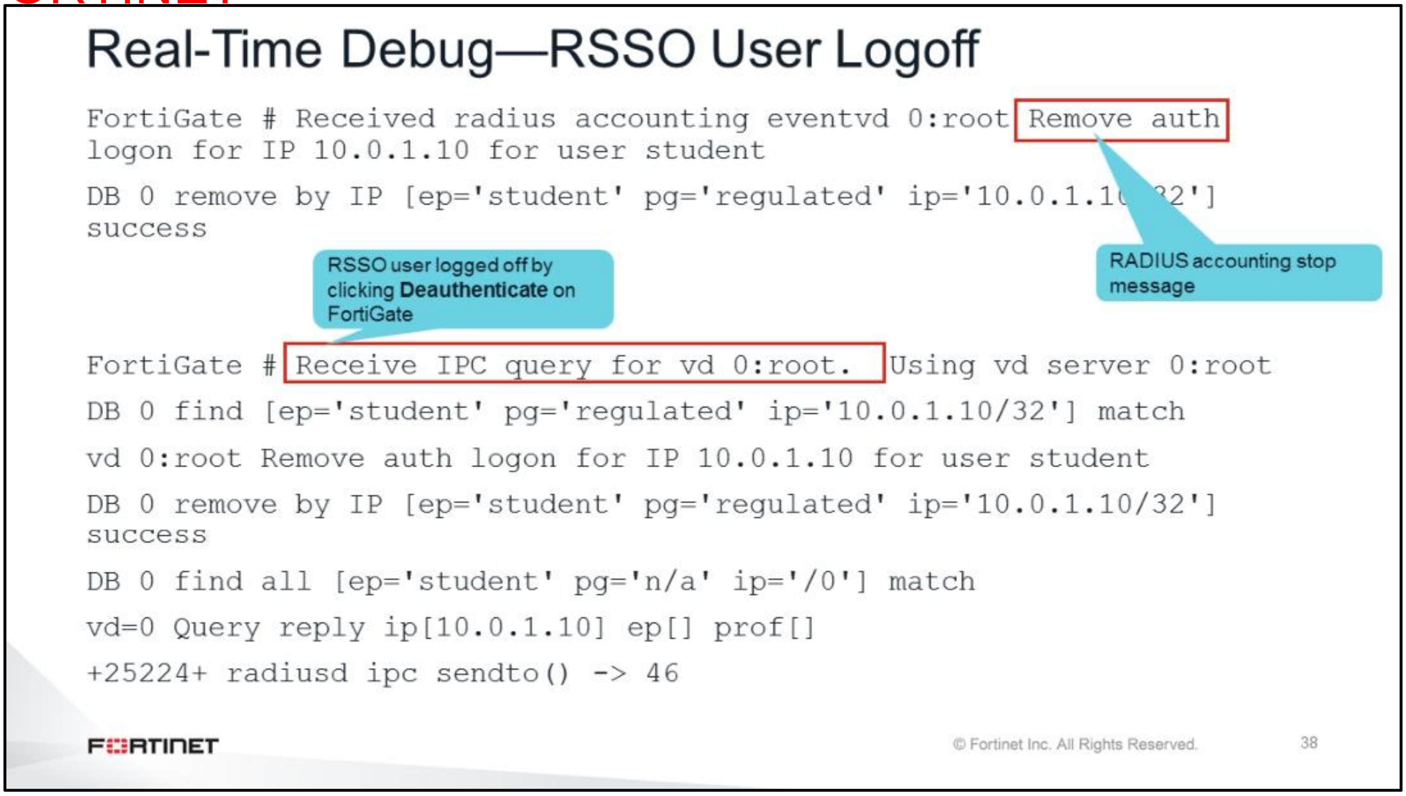
The command `diagnose rsso query` queries RSSO users on FortiGate.

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

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

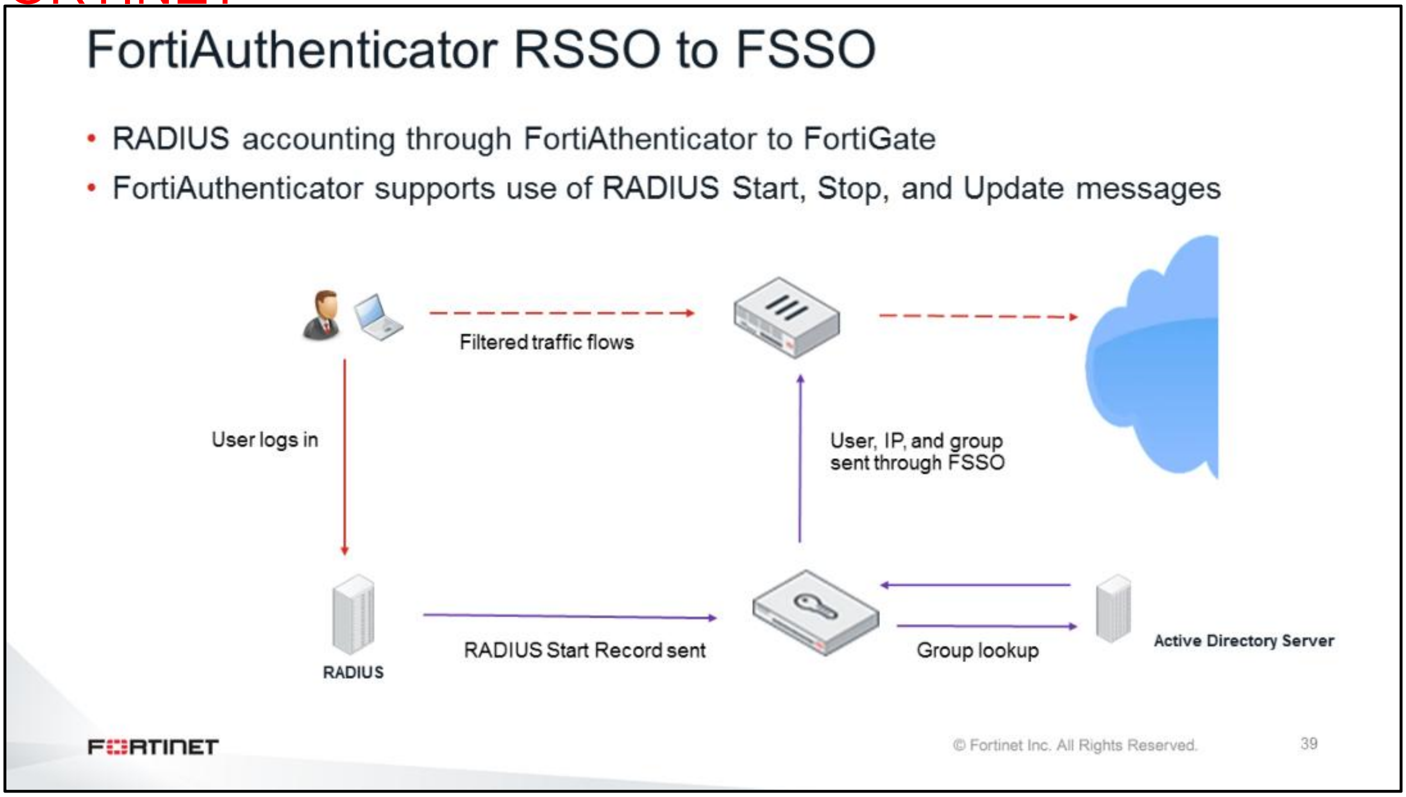


This slide shows real-time debugging when FortiGate receives a RADIUS accounting start message from the RADIUS server.

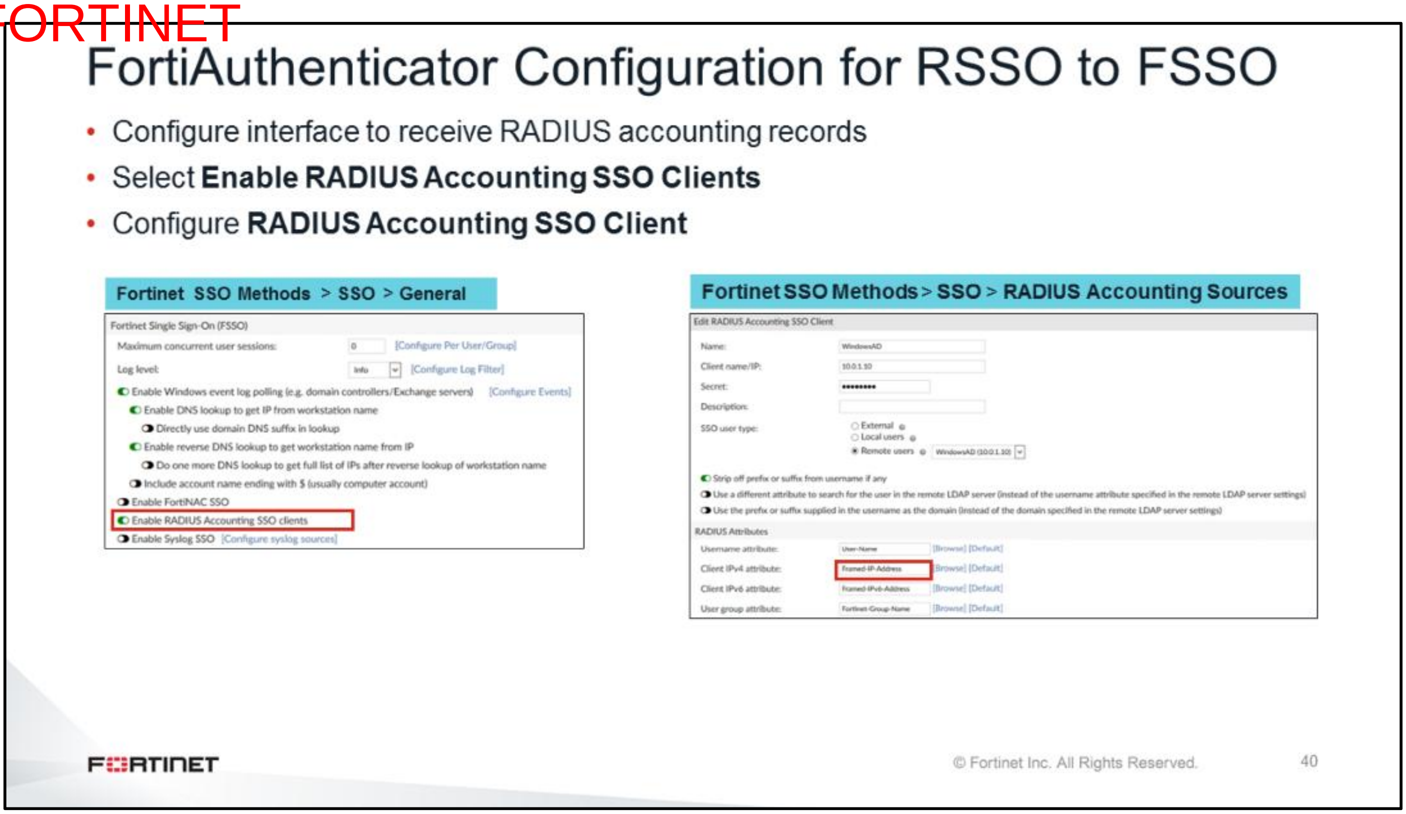


This slide shows two different debug outputs, both resulting in the RSSO user being logged off:

1. FortiGate receives a RADIUS accounting stop message from the RADIUS server.
2. The RSSO user is logged out of FortiGate using the **Deauthenticate** tab.



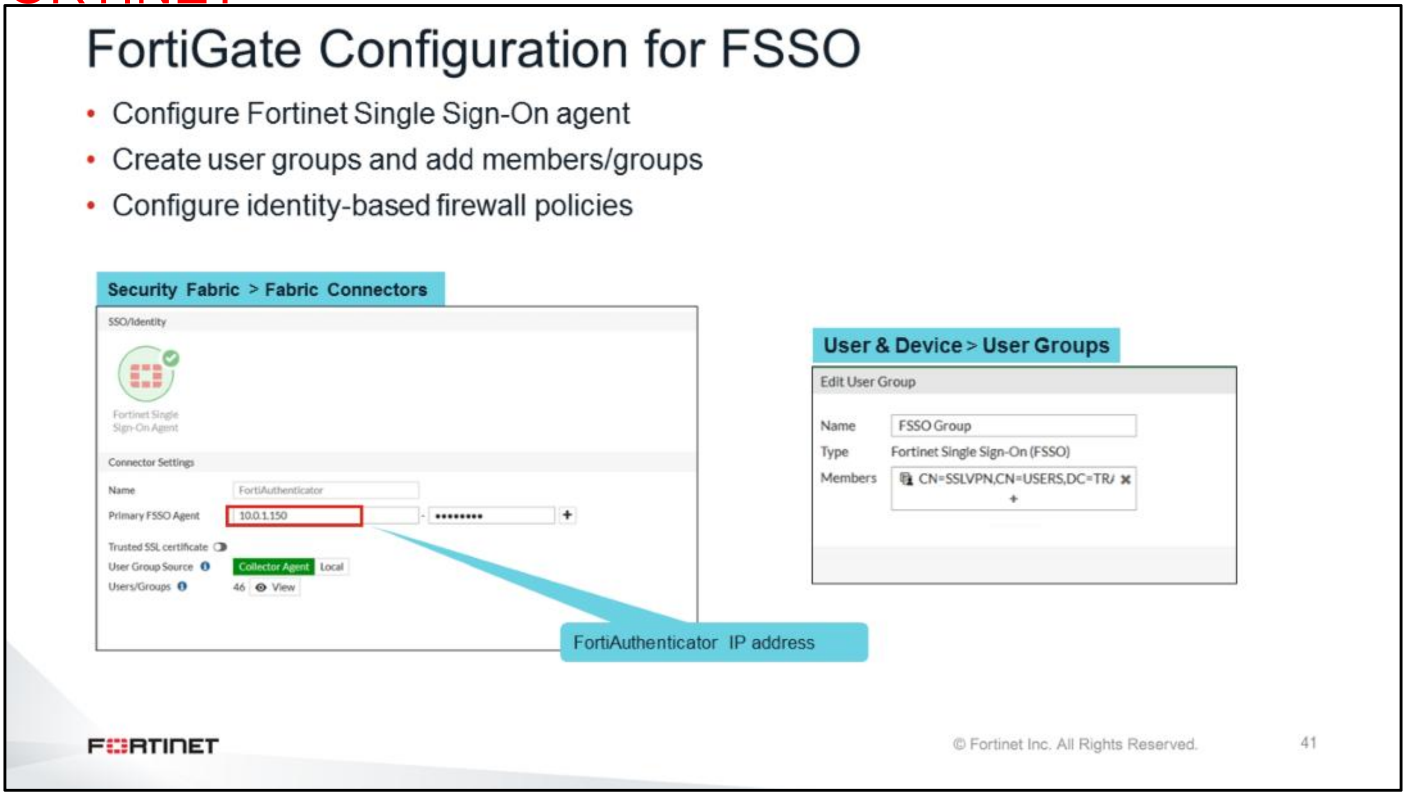
FortiAuthenticator supports the use of RADIUS Start, Stop, and Interim Update messages to authenticate and manage active users transparently. It receives RADIUS accounting messages, performs lookups against the LDAP server for group membership and then populates its FSSO cache with the correct information.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



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 be configured to receive FSSO updates in the network.

Use the following steps to configure FortiAuthenticator for FSSO:
Step 1 – Configure the interface to receive RADIUS Accounting Records.
Step 2 – Select **Enable RADIUS Accounting SSO Clients**.
Step 3 – Configure the RADIUS accounting SSO client.

You must select the LDAP server from the drop-down list if you want to validate the user using a backend the LDAP server. FortiAuthenticator can retrieve group memberships from 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 user account is not expected to be configured in the local or remote database. RADIUS attributes **Username** (default User-Name) **Client IP** attribute (default **Framed-IP-Address**) are required. You should use the default setting. **User group attribute** is not required. You must select the LDAP server from the drop-down list, because this is how FortiAuthenticator establishes group membership.



You must configure FortiGate with FSSO settings to be able to receive the FSSO updates from FortiAuthenticator. You must configure **Fortinet Single Sign-On Agent** in **Fabric Connectors**. After you configure the FSSO agent, you can pull or create a user group, and assign remote members to the group. You can then use the user group on a firewall policy to assign network access to FSSO users.

Monitor SSO Users

- FortiAuthenticator monitor shows user logged in through **Radius Accounting** source

Monitor > SSO > SSO Sessions

	Logon Time	Update Time	Workstation	IP address	Domain Grouping	Domain	Username	Source	
	Thu Aug 15 14:03:00 2019	Thu Aug 15 14:03:00 2019	10.0.1.10	10.0.1.10	DEFAULT	TRAININGAD.TRAINING.LAB	STUDENT	Radius Accounting	CN=STUDENT,CN=USERS,DC=TRAININGAD,DC=TRAINING,DC=LAB+CN=SSLV

1 SSO session

- FortiGate monitor confirms RSSO user has been authenticated as FSSO user on FortiGate

Monitor > Firewall User Monitor

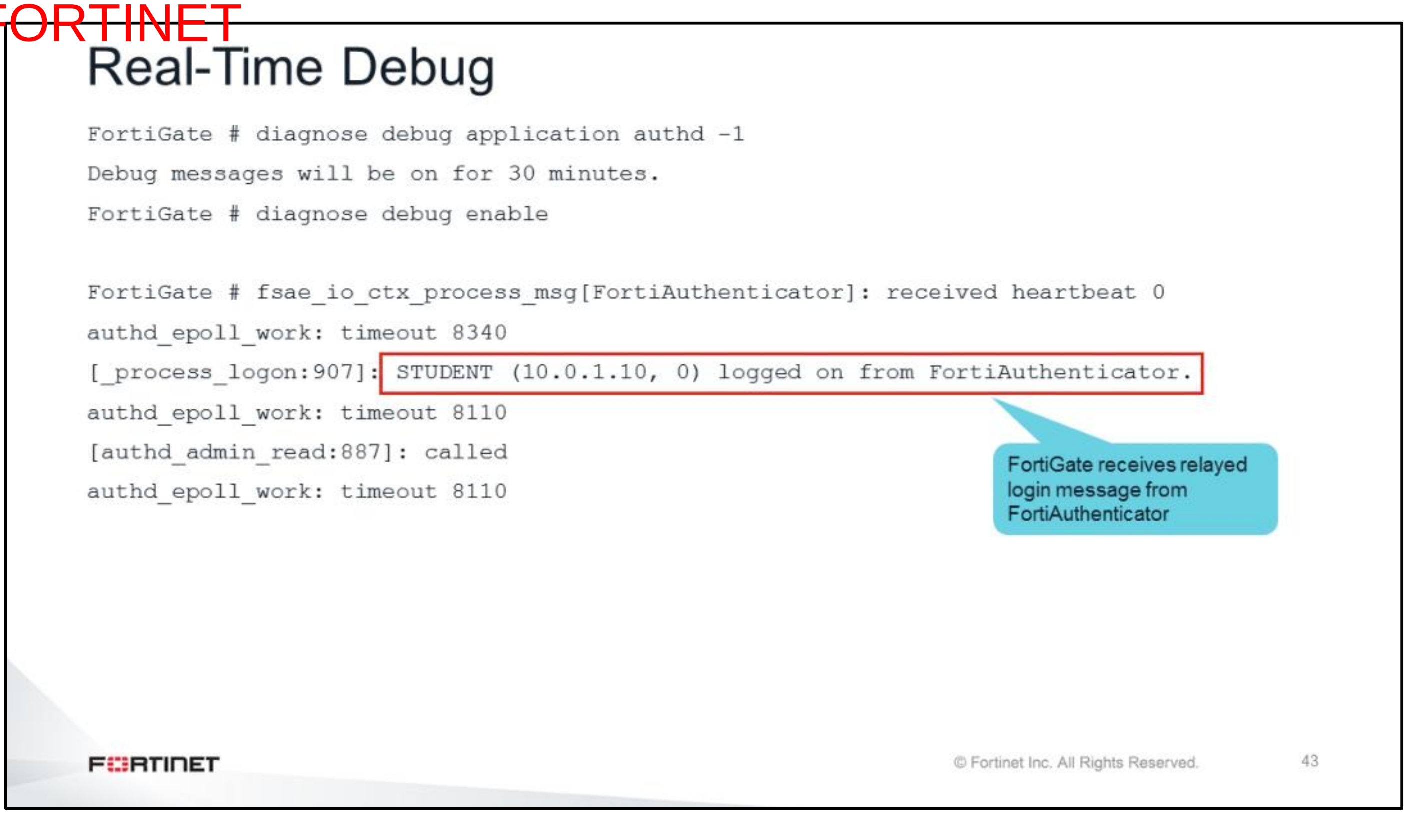
User Name	User Group	Duration	IP Address	Traffic Volume	Method
STUDENT	FSSO Group CN=SSLVPN,CN=USERS,DC=TRAININGAD,DC=TRAINING,DC=LAB CN=DOMAIN USERS,CN=USERS,DC=TRAININGAD,DC=TRAINING,DC=LAB	17 minute(s) and 59 second(s)	10.0.1.10	372.52 kB	Fortinet Single Sign-On

```
FortiGate # diagnose debug authd fsso list
----FSSO logons----
IP: 10.0.1.10  User: STUDENT  Groups:
CN=STUDENT,CN=USERS,DC=TRAININGAD,DC=TRAINING,DC=LAB+CN=SSLVPN,CN=USERS,DC=TRAININGAD,DC=TRAINING,DC
=LAB+CN=DOMAIN USERS,CN=USERS,DC=TRAININGAD,DC=TRAINING,DC=LAB  Workstation: 10.0.1.10 MemberOf:
FSSO Group CN=SSLVPN,CN=USERS,DC=TRAININGAD,DC=TRAINING,DC=LAB CN=DOMAIN
USERS,CN=USERS,DC=TRAININGAD,DC=TRAINING,DC=LAB
Total number of logons listed: 1, filtered: 0
----end of FSSO logons----
```

FORTINET 42

While the FortiAuthenticator monitor will record that the user logged in through a **Radius Accounting** source, you can confirm that the user was authenticated on FortiGate using the FSSO method by looking at the **Firewall User Monitor**.

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



This slide shows real-time debugging of the FortiGate receiving a RADIUS accounting start message from the RADIUS server, which has been relayed using FortiAuthenticator.

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

FortiAuthenticator Logs

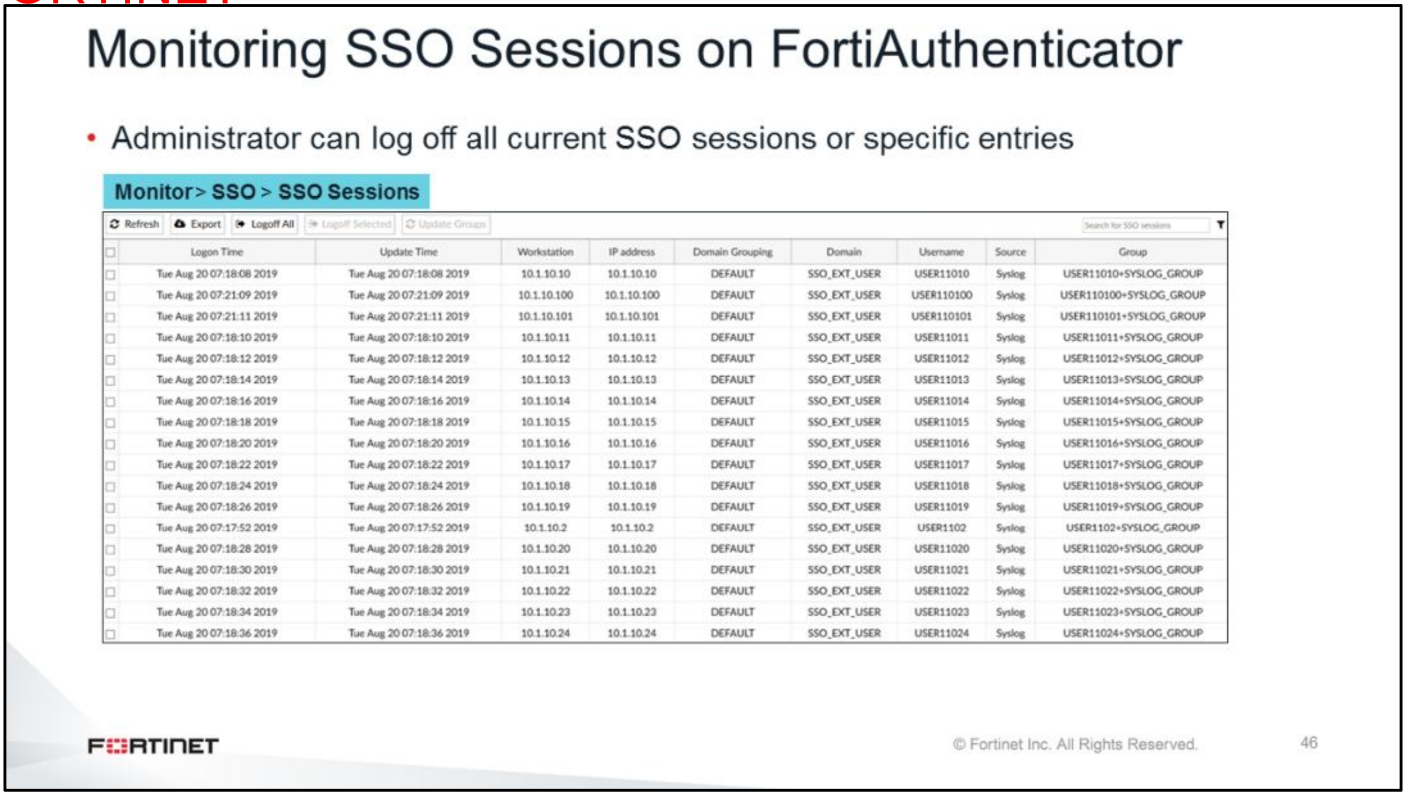
- FortiAuthenticator displays:
  - SSO domains
  - Active SSO sessions (logons that are still valid)
  - Windows event log sources
  - Active FortiGate devices connected to FortiAuthenticator as FSSO agents
  - DC/TS agents connection status

Monitor > SSO > SSO Sessions

 45

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 if the TS/DC agents are connected to FortiAuthenticator. If not, ensure that the correct IP, port, and secret are configured on both FortiAuthenticator and the DC/TS agents.

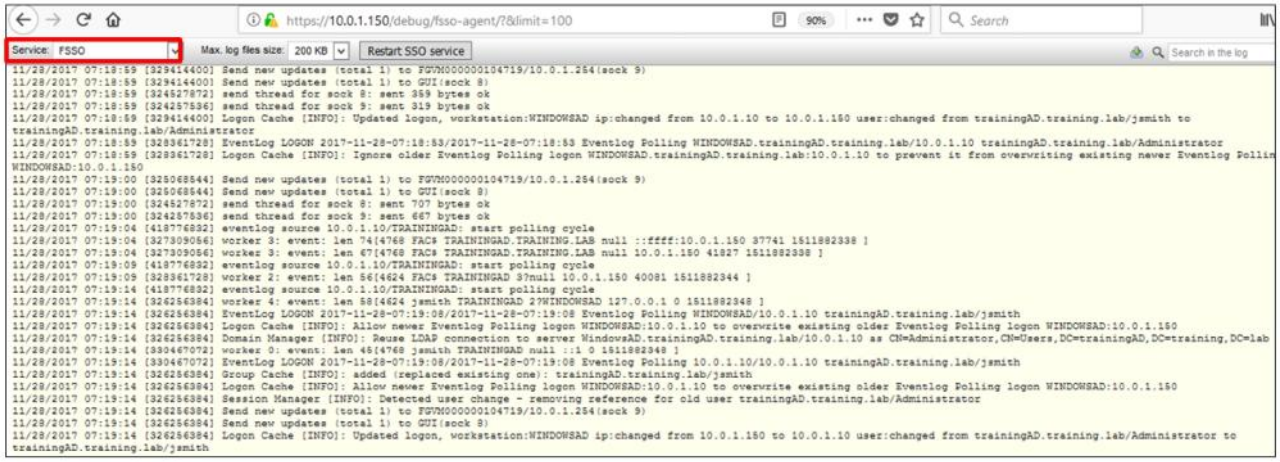


Logon Time	Update Time	Workstation	IP address	Domain Grouping	Domain	Username	Source	Group
Tue Aug 20 07:18:08 2019	Tue Aug 20 07:18:08 2019	10.1.10.10	10.1.10.10	DEFAULT	SSO_EXT_USER	USER11010	Syslog	USER11010+SYSLOG_GROUP
Tue Aug 20 07:21:09 2019	Tue Aug 20 07:21:09 2019	10.1.10.100	10.1.10.100	DEFAULT	SSO_EXT_USER	USER110100	Syslog	USER110100+SYSLOG_GROUP
Tue Aug 20 07:21:11 2019	Tue Aug 20 07:21:11 2019	10.1.10.101	10.1.10.101	DEFAULT	SSO_EXT_USER	USER110101	Syslog	USER110101+SYSLOG_GROUP
Tue Aug 20 07:18:10 2019	Tue Aug 20 07:18:10 2019	10.1.10.11	10.1.10.11	DEFAULT	SSO_EXT_USER	USER11011	Syslog	USER11011+SYSLOG_GROUP
Tue Aug 20 07:18:12 2019	Tue Aug 20 07:18:12 2019	10.1.10.12	10.1.10.12	DEFAULT	SSO_EXT_USER	USER11012	Syslog	USER11012+SYSLOG_GROUP
Tue Aug 20 07:18:14 2019	Tue Aug 20 07:18:14 2019	10.1.10.13	10.1.10.13	DEFAULT	SSO_EXT_USER	USER11013	Syslog	USER11013+SYSLOG_GROUP
Tue Aug 20 07:18:16 2019	Tue Aug 20 07:18:16 2019	10.1.10.14	10.1.10.14	DEFAULT	SSO_EXT_USER	USER11014	Syslog	USER11014+SYSLOG_GROUP
Tue Aug 20 07:18:18 2019	Tue Aug 20 07:18:18 2019	10.1.10.15	10.1.10.15	DEFAULT	SSO_EXT_USER	USER11015	Syslog	USER11015+SYSLOG_GROUP
Tue Aug 20 07:18:20 2019	Tue Aug 20 07:18:20 2019	10.1.10.16	10.1.10.16	DEFAULT	SSO_EXT_USER	USER11016	Syslog	USER11016+SYSLOG_GROUP
Tue Aug 20 07:18:22 2019	Tue Aug 20 07:18:22 2019	10.1.10.17	10.1.10.17	DEFAULT	SSO_EXT_USER	USER11017	Syslog	USER11017+SYSLOG_GROUP
Tue Aug 20 07:18:24 2019	Tue Aug 20 07:18:24 2019	10.1.10.18	10.1.10.18	DEFAULT	SSO_EXT_USER	USER11018	Syslog	USER11018+SYSLOG_GROUP
Tue Aug 20 07:18:26 2019	Tue Aug 20 07:18:26 2019	10.1.10.19	10.1.10.19	DEFAULT	SSO_EXT_USER	USER11019	Syslog	USER11019+SYSLOG_GROUP
Tue Aug 20 07:17:52 2019	Tue Aug 20 07:17:52 2019	10.1.10.2	10.1.10.2	DEFAULT	SSO_EXT_USER	USER1102	Syslog	USER1102+SYSLOG_GROUP
Tue Aug 20 07:18:28 2019	Tue Aug 20 07:18:28 2019	10.1.10.20	10.1.10.20	DEFAULT	SSO_EXT_USER	USER11020	Syslog	USER11020+SYSLOG_GROUP
Tue Aug 20 07:18:30 2019	Tue Aug 20 07:18:30 2019	10.1.10.21	10.1.10.21	DEFAULT	SSO_EXT_USER	USER11021	Syslog	USER11021+SYSLOG_GROUP
Tue Aug 20 07:18:32 2019	Tue Aug 20 07:18:32 2019	10.1.10.22	10.1.10.22	DEFAULT	SSO_EXT_USER	USER11022	Syslog	USER11022+SYSLOG_GROUP
Tue Aug 20 07:18:34 2019	Tue Aug 20 07:18:34 2019	10.1.10.23	10.1.10.23	DEFAULT	SSO_EXT_USER	USER11023	Syslog	USER11023+SYSLOG_GROUP
Tue Aug 20 07:18:36 2019	Tue Aug 20 07:18:36 2019	10.1.10.24	10.1.10.24	DEFAULT	SSO_EXT_USER	USER11024	Syslog	USER11024+SYSLOG_GROUP

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 logon 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.

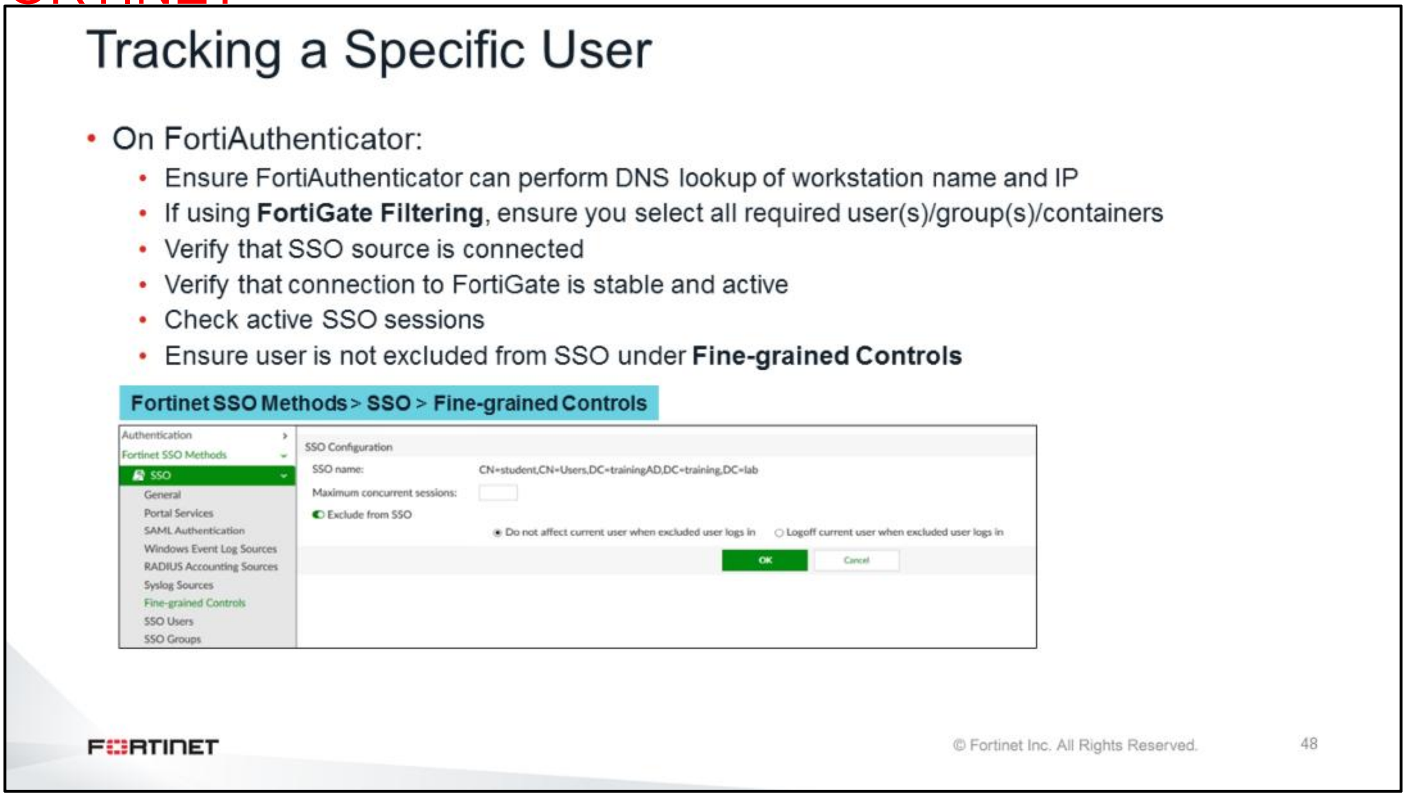
FortiAuthenticator Debug Logs

- `https://<FortiAuthenticator_IP>/debug`



 47

You can also view debug-level logs on FortiAuthenticator by connecting to `https://<FortiAuthenticator_IP>/debug` and selecting **FSSO service**. The debug log page allows 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.



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
- 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

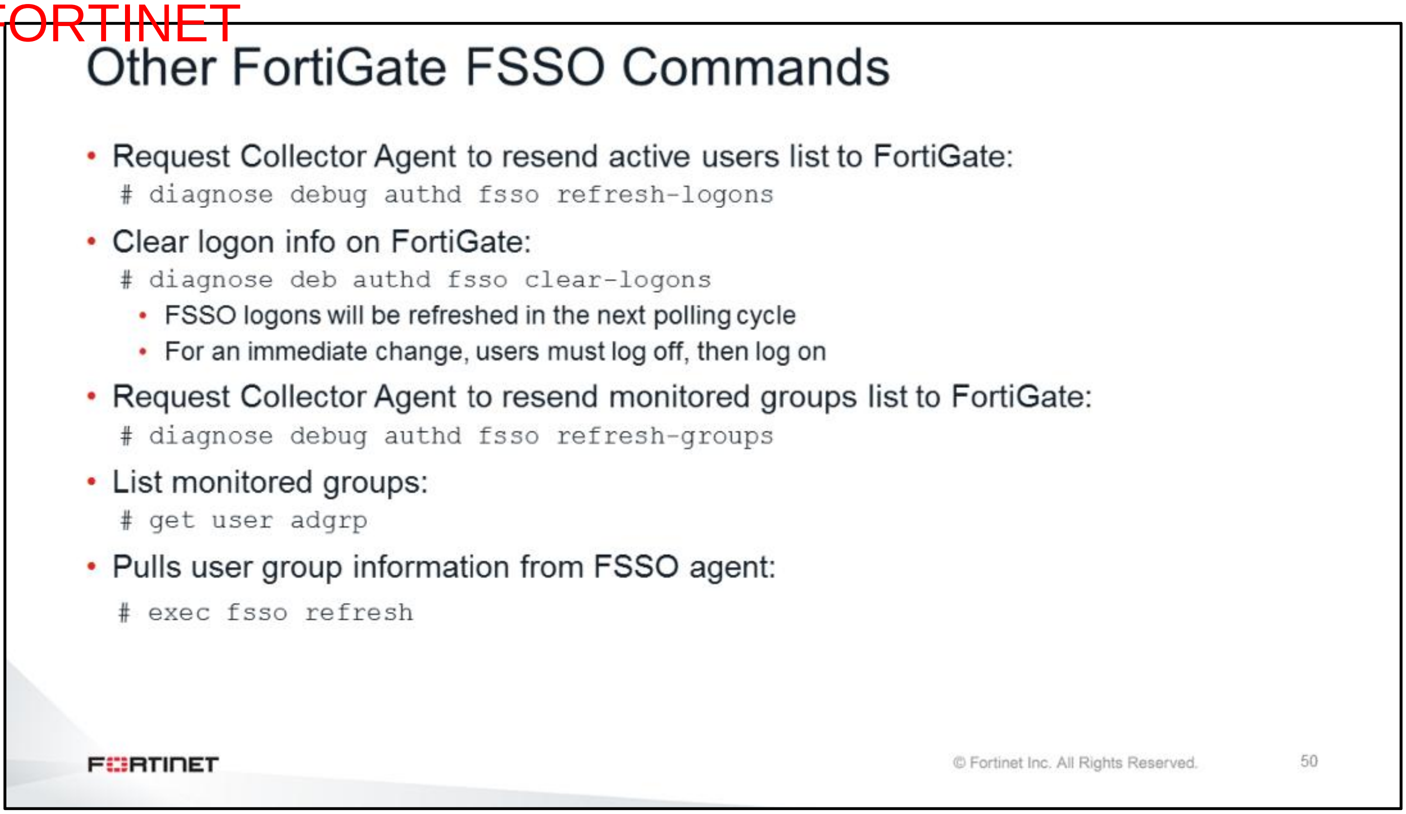
When troubleshooting FSSO issues related to the DC Agent mode (Windows AD) environment, the steps are the same for the software Collector Agent agent and FortiAuthenticator. The only difference between the two is that all the DC agents are pointing to FortiAuthenticator instead of to the software Collector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

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: 192.168.3.1  User: STUDENT  Groups: TRAININGAD/USERS
Workstation: WIN-INTERNAL.TRAININGAD.TRAINING.LA
IP: 10.0.1.10  User: STUDENT  Groups: TRAININGAD/USERS
Workstation: WIN-INTERNAL.TRAININGAD.TRAINING.LA
Total number of logons listed: 2, filtered: 0
```

FORTINET 49

To get the list of active 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`.



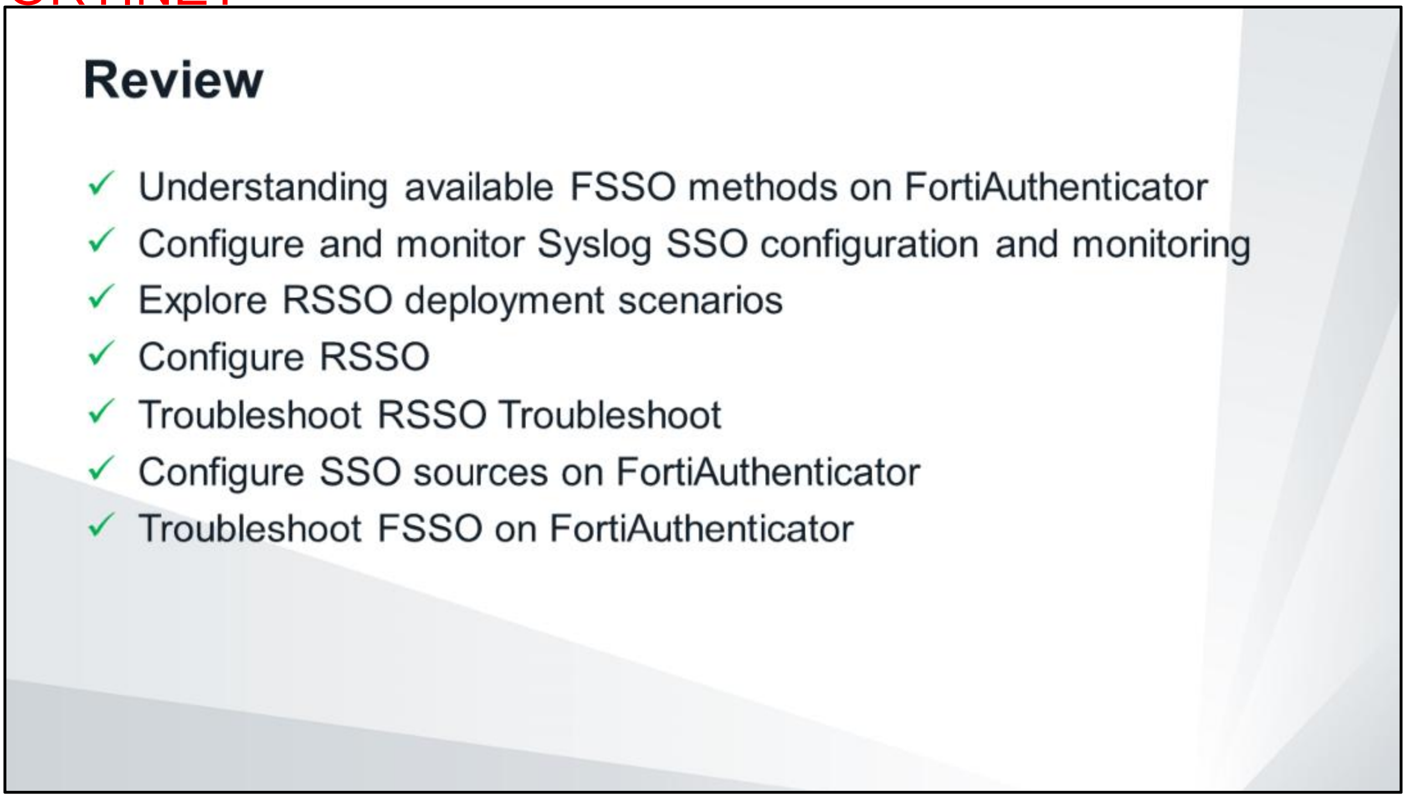
The CLI command `diagnose debug authd fsso refresh-logons` refreshes the active FSSO user list on FortiGate by getting this information again from the Collector Agent.

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

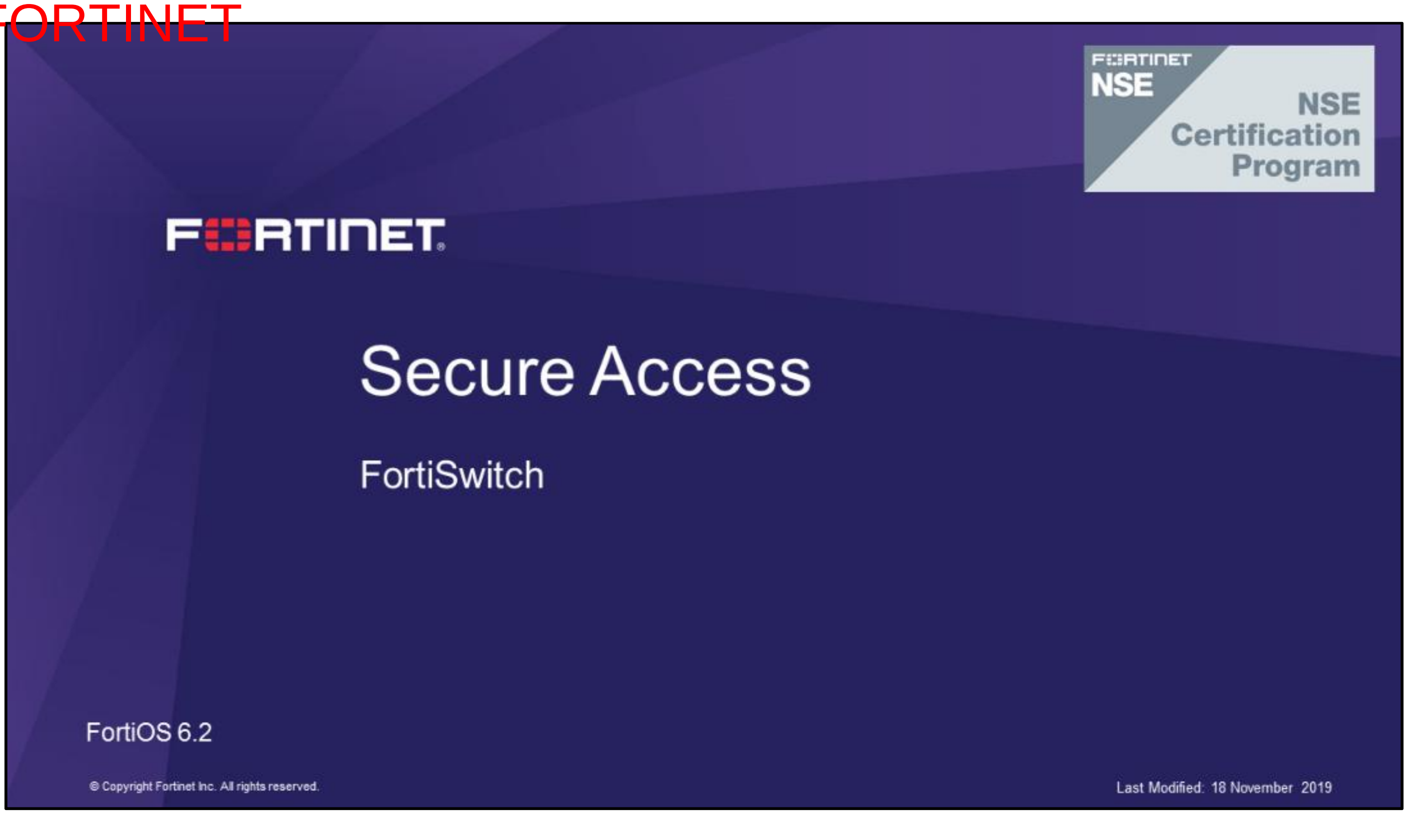
The CLI command `diagnose debug authd fsso refresh-groups` refreshes the user group information on FortiGate by getting this information again from the Collector Agent.

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

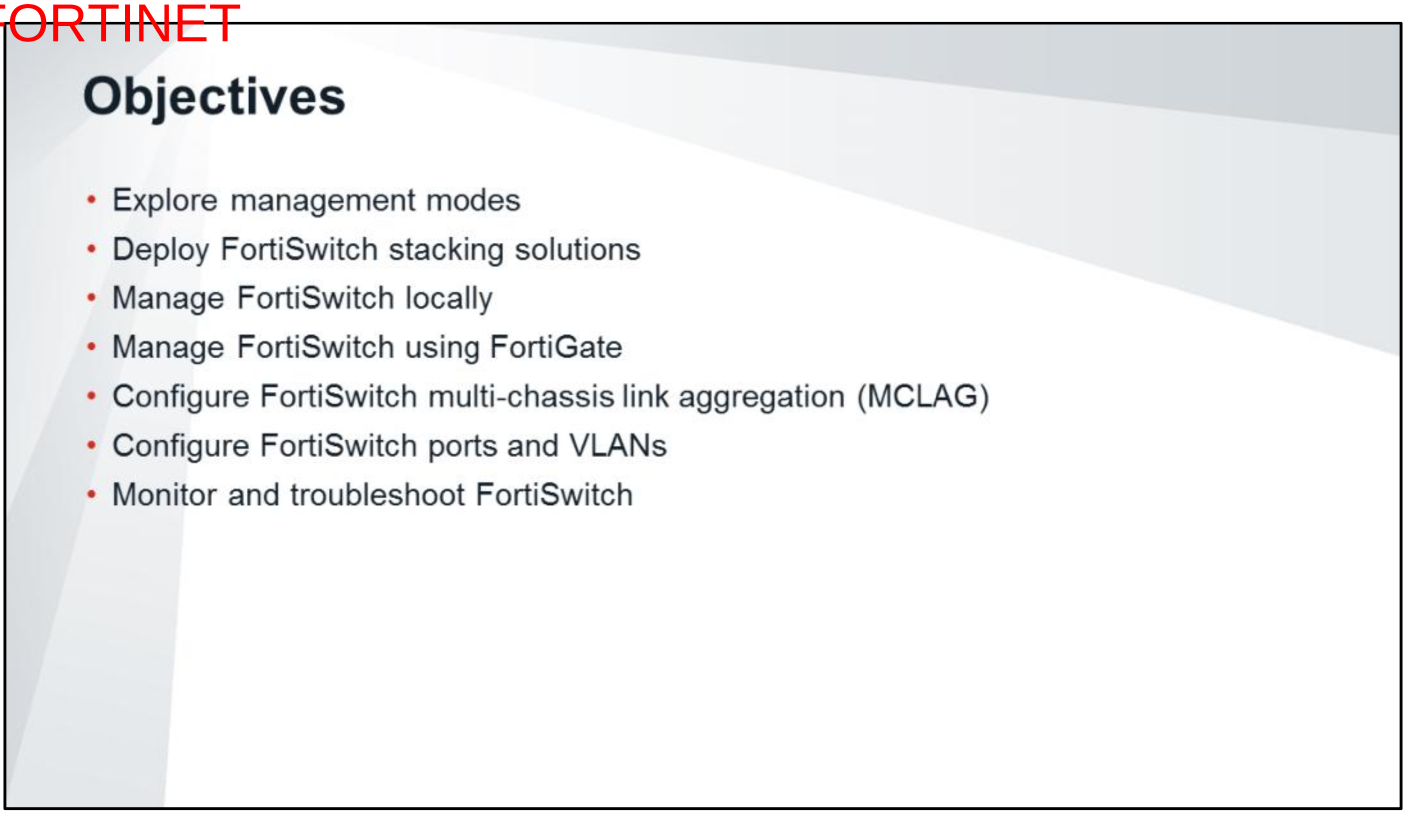
To list the monitored user groups, use the command `get user adgrp`.



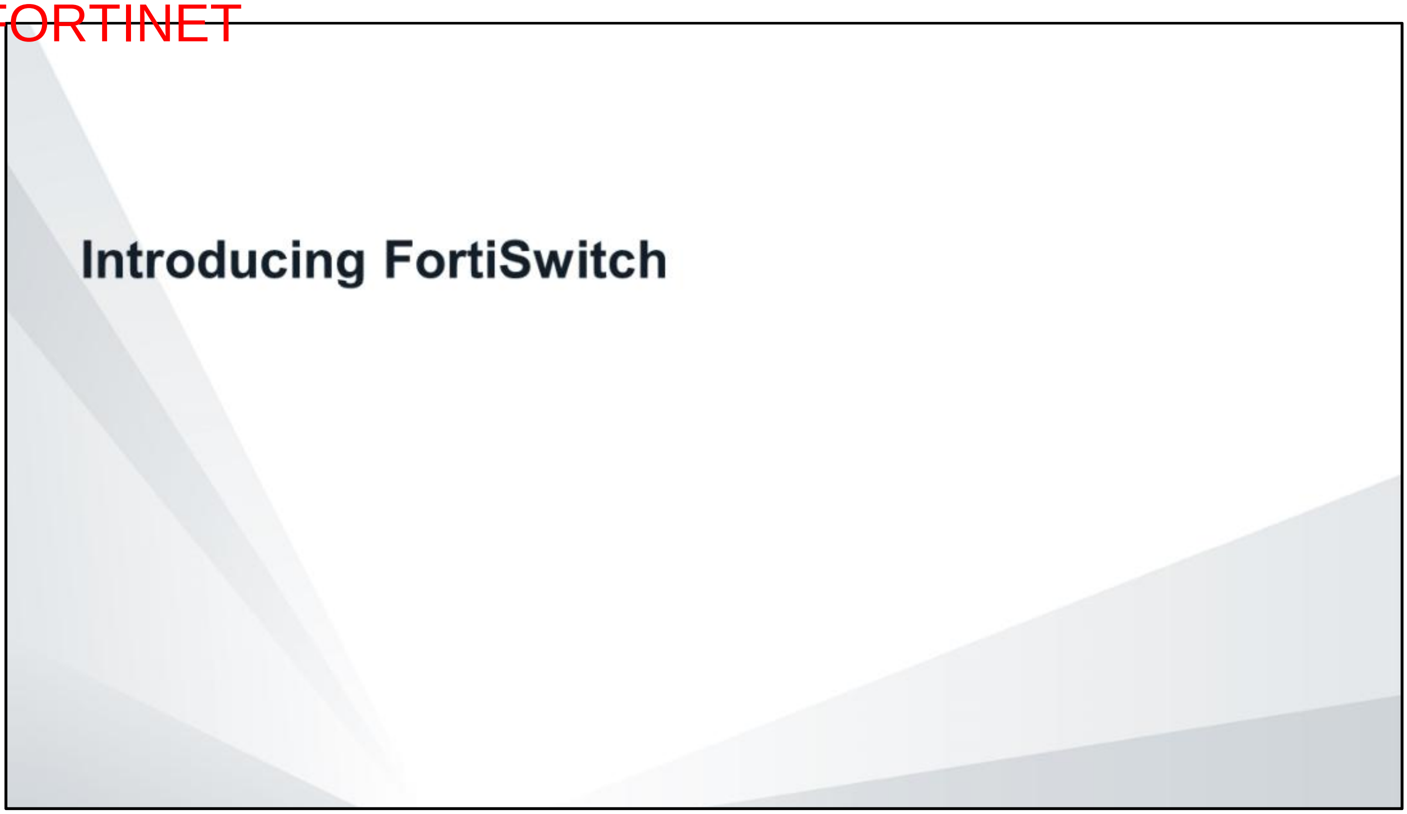
By mastering the objectives covered in this lesson, you learned how to collect logon events and convert them to Fortinet Single Sign-On (FSSO) events.



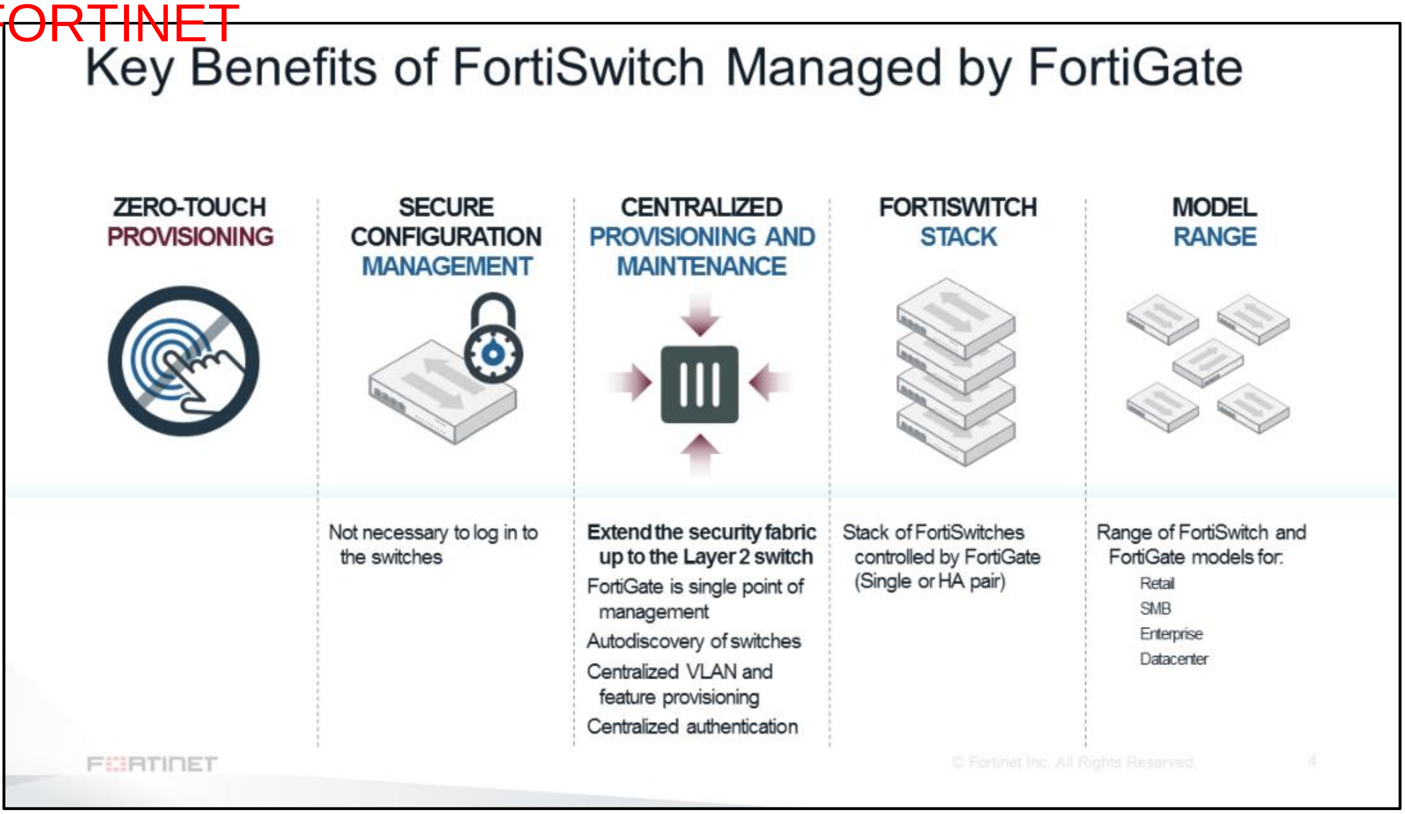
In this lesson, you will learn about FortiSwitch deployment, configuration, and troubleshooting.



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



In this section, you will learn how to deploy FortiSwitch.

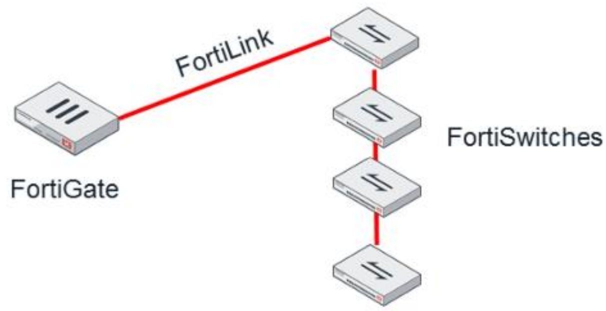


Managing FortiSwitch devices using FortiGate offers important key benefits:

- Zero-touch provisioning: Administrators only need to connect FortiSwitch to a FortiGate interface that has FortiLink enabled. FortiGate will automatically discover and provision FortiSwitch.
- Secure configuration management: All FortiSwitch management is done on the FortiGate CLI and GUI. Administrators are not required to log in to FortiSwitch.
- Centralized provisioning and maintenance: FortiSwitch becomes an extension of FortiGate. The way you configure firewall policies using FortiSwitch VLANs is the same as the way you do it for FortiGate VLANs. Authentication and authorization are also handled centrally on FortiGate.
- FortiSwitch stack: FortiGate can manage multiple FortiSwitch devices stacked in different ways to offer scalability and redundancy.
- Model range: There are different sizes of FortiGate and FortiSwitch devices to accommodate the needs of retail and SMB customers, up to data centers.

FortiSwitch Modes

- You can deploy FortiSwitch as a standalone switch (with its own GUI and CLI access)
- Or, you can manage FortiSwitch on FortiGate using FortiLink:
  - FortiLink is dependent on the internal switch fabric (ISF) of FortiGate
  - Specific FortiGate models currently support FortiLink



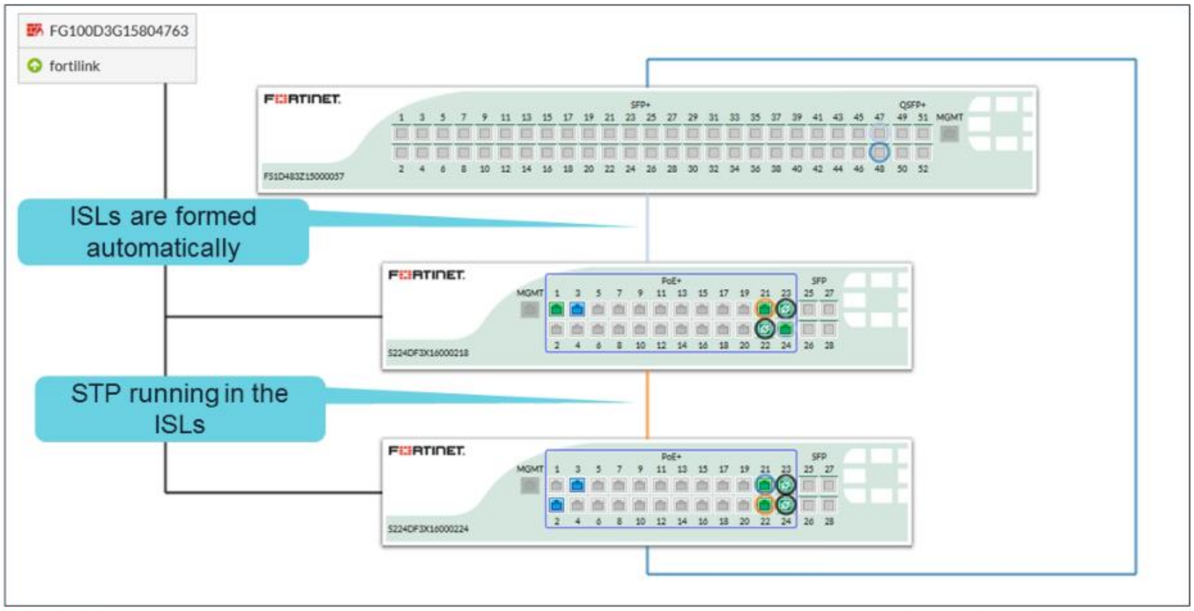
FORTINET

5

You can deploy FortiSwitch as a standalone switch, or as a switch that you can manage from FortiGate (FortiLink mode).

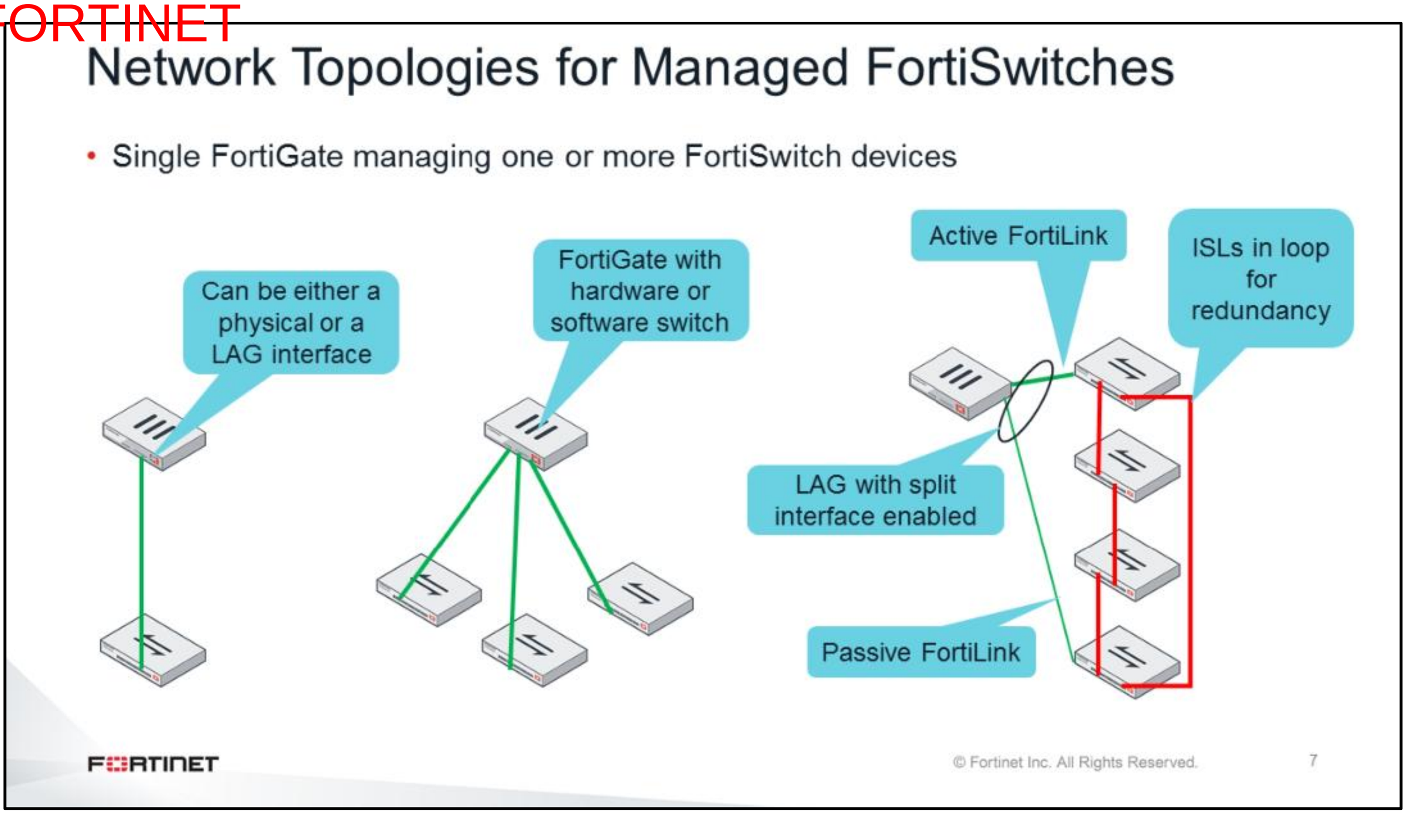
You can use FortiLink to manage FortiSwitch from FortiGate. FortiLink is supported by specific FortiGate models.

Stacking



 6

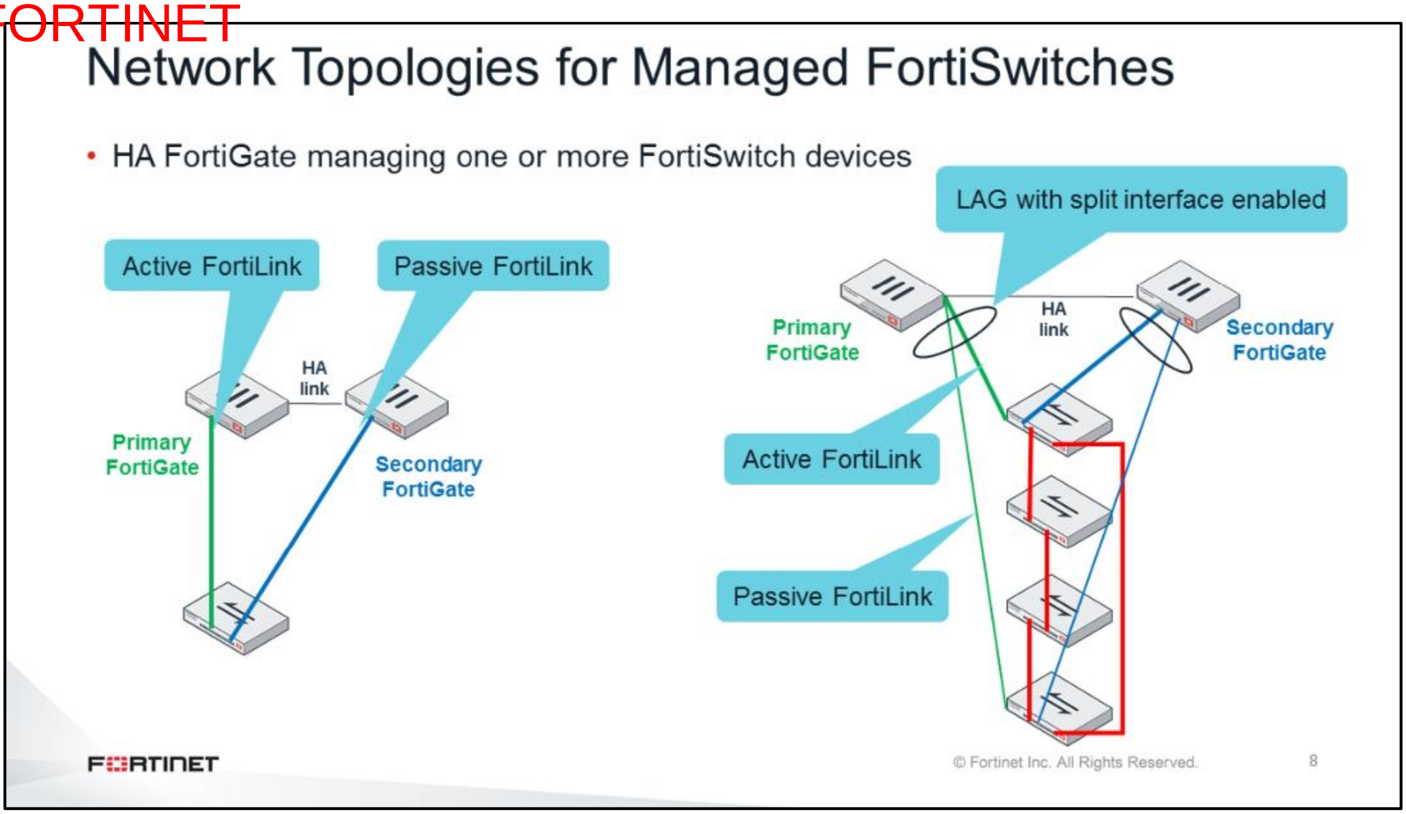
Using FortiLink, FortiGate automatically provisions stacked FortiSwitches, forms inter-switch link (ISL) between FortiSwitch devices, and enables the Spanning Tree Protocol on the ISLs. FortiGate autodiscovers all FortiSwitch devices in the stack, and manages them centrally.



Now, you will learn about the different ways you can deploy FortiSwitch using FortiGate. The simplest deployment is one FortiGate managing one FortiSwitch. The interface FortiGate uses to manage FortiSwitch could be either one single physical interface, or an aggregated interface with multiple physical interfaces.

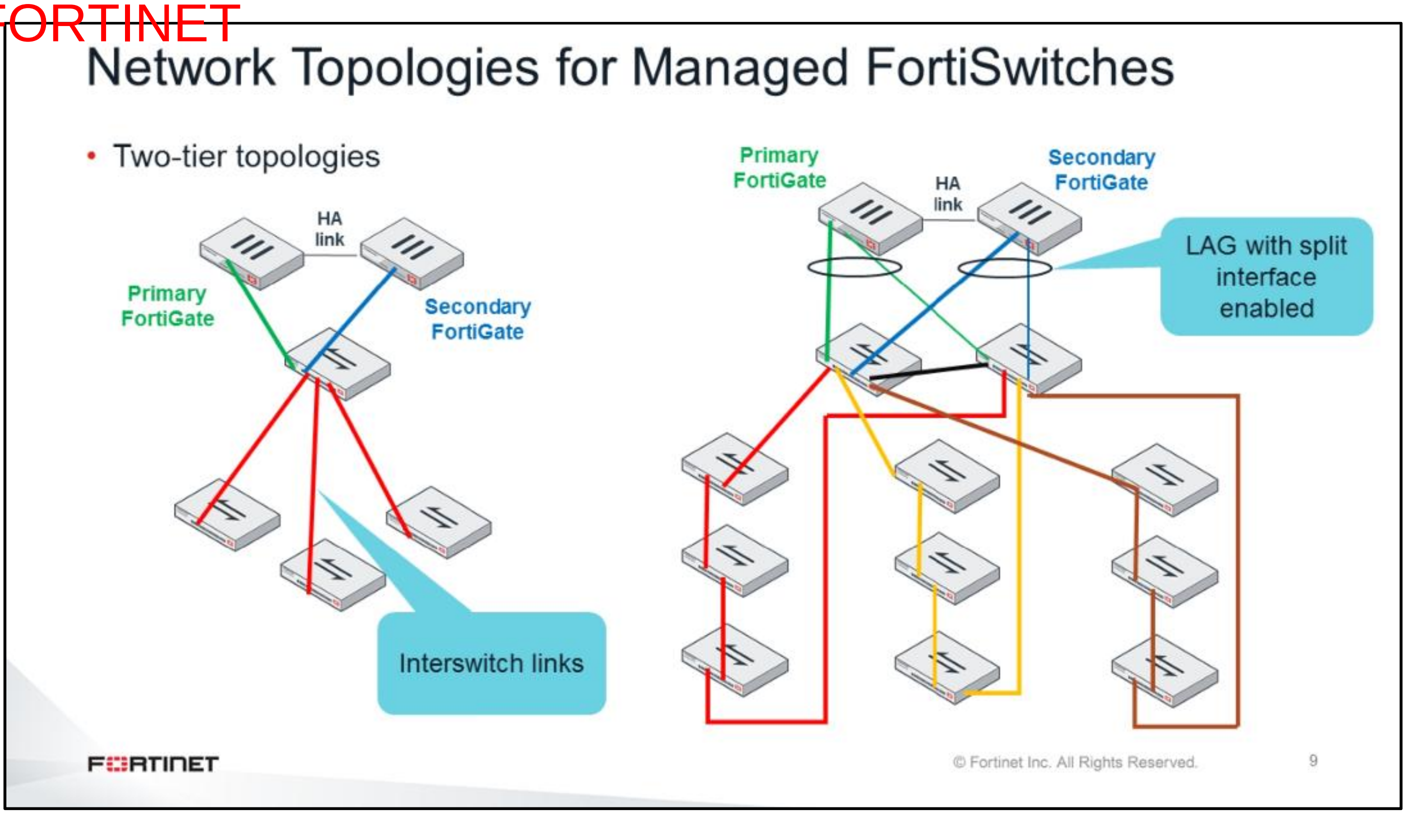
In the deployment example shown on the middle of this slide, multiple FortiSwitch devices are connected in parallel to FortiGate with either a hardware or a software switch.

You can also interconnect the FortiSwitch devices in a ring (or loop) topology using ISL trunks. One of the FortiSwitch devices is connected to one of the FortiGate interfaces through an active FortiLink. Optionally, you can use a FortiGate aggregated interface (LAG) with two physical interfaces. One physical interface is the active FortiLink, connected to one FortiSwitch; and the second physical interface is the passive FortiLink, connected to another FortiSwitch. This deployment mode is one way you can offer redundancy for FortiLink. You must enable the split interface in the settings on the aggregated interface.



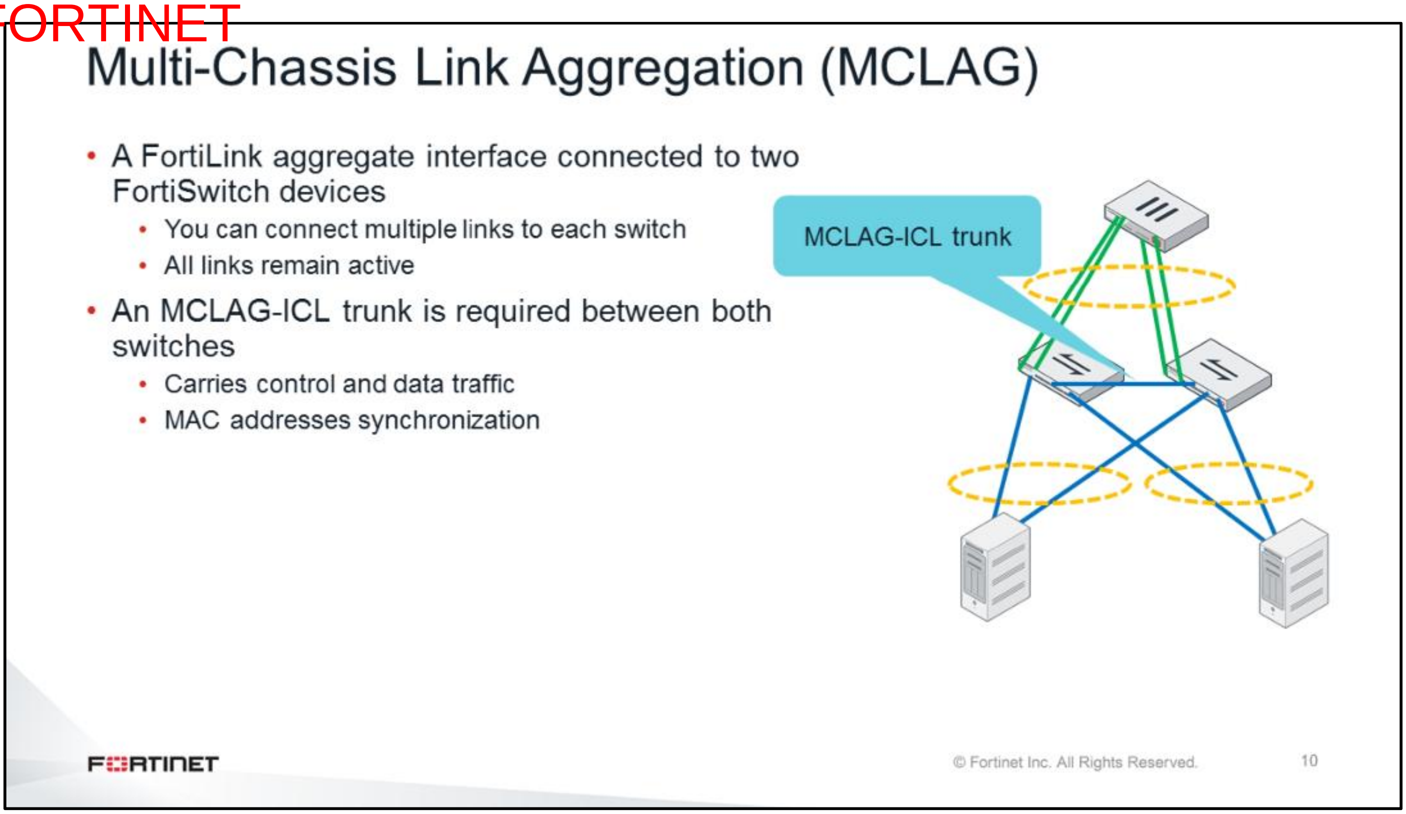
The example on the left side of this slide shows a deployment with two FortiGate devices in HA mode, and one FortiSwitch. The primary FortiGate has the active FortiLink. The secondary FortiGate has the passive FortiLink.

You can combine FortiGate devices in HA mode with FortiSwitch devices stacked in a ring topology. In this case, you can have up to two FortiLink interfaces (LAG) connected to each HA member. One FortiLink on the primary FortiGate is active, the other FortiLink on the primary is passive, and the two FortiLink devices on the secondary FortiGate are also passive. In the example shown this slide, you must enable split interfaces on the aggregated interfaces of both the primary and secondary FortiGate devices.



FortiLink supports multi-tier topologies. The example on the left side of this slide shows three FortiSwitch devices connected to one central FortiSwitch. The central FortiSwitch is connected to FortiGate devices in HA mode.

The right side of this slide shows a more complex and scalable example. Three sets of FortiSwitch devices in a ring topology are connected to two central FortiSwitch devices, which are then connected to two FortiGate devices in HA mode.



In all the previous examples, there is either one physical interface, or a LAG with two physical interfaces, connected to each FortiGate. A split interface is required when using a LAG with two interfaces, and only one of the interfaces can be active at any given time.

MCLAG allows you to have LAGs with more than two physical interfaces connected to each switch. Also, when you use MCLAG, all the interfaces in the LAG are active. In the example shown on this slide, two links from one FortiGate are connected to each of the two FortiSwitch devices. The two links are active.

This deployment mode requires you to disable the split interface. You must also configure an MCLAG-ICL trunk between the switches to carry control and data traffic, including the synchronization of the MAC address table.

Standalone FortiSwitch

In this section, you will learn how to manage FortiSwitch locally, as a standalone device.

Management Access

- Access the FortiSwitch configuration using the CLI
  - Use the device serial console port to configure initial settings
- Access the web console using the management IP
  - *mgmt* interface on devices with a dedicated management port
  - Or *internal* interface (data path) to use VLAN ID 1:

```
config system interface
  edit <mgmt-int>
    set ip 10.0.13.1/24
    set allowaccess https ssh ping
  end
end
```

FORTINET 12

A FortiSwitch device has a serial console port to initially configure the device to allow access through the web console and CLI using an IP address.

To enable access, you must configure an IP address on the management interface, whether it is the dedicated port or one of the internal interface physical ports, by creating VLAN ID 1.

Remote Management Access

- To allow out-of-band access, a default gateway is required
- Enable *allowaccess* on the management interface
- If the management interface IP is set manually
  - Configure a static route to the management default gateway:

```
config router static
  edit 1
    set device <mgmt-int>
    set gateway <mgmt-defaultgw>
```

- If DHCP server assigned IP to the management interface
  - Ensure *defaultgw* is enabled:

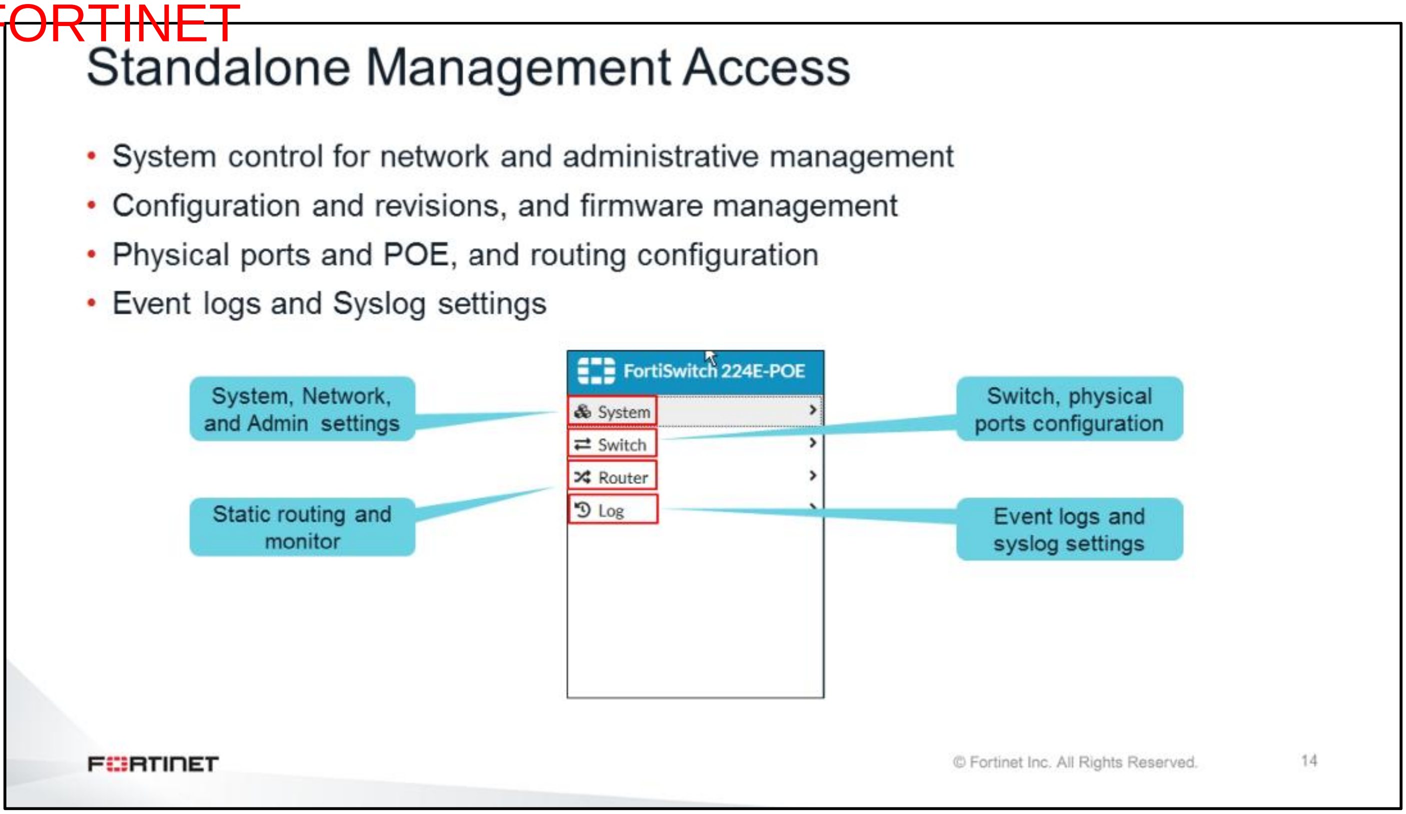
```
config system interface
  edit <mgmt-int>
    set defaultgw enable
```

FORTINET

 13

Out-of-band management allows remote access to FortiSwitch. The management interface must enable access using the available management protocol, such as HTTPS and SSH.

If the management interface IP address is configured statically, you will need to create a static route for the default gateway. If it is dynamically configured, enable `defaultgw` in the management interface configuration using the CLI.



Local management on ForitSwitch provides access to system control settings, including networking and administrative management control.

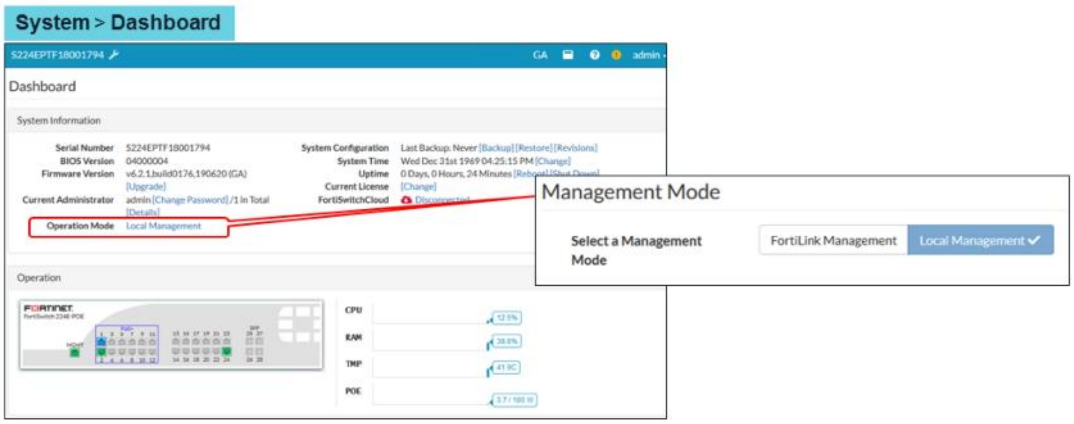
Standalone FortiSwitch devices provide switch configuration to manage physical ports, and advanced switching, such as Power Over Ethernet (PoE) and Quality of Service (QoS).

Router configuration and monitoring is also available when managing the FortiSwitch locally.

You can set up logging on FortiSwitch to view event logs and offload logs to a Syslog server.

Management Mode

- **Local Management** is configured by default
- **FortiLink Management**
  - Configuration is managed by a switch controller (FortiGate)
  - Uses CAPWAP—the same method used to manage wireless AP (FortiAP)



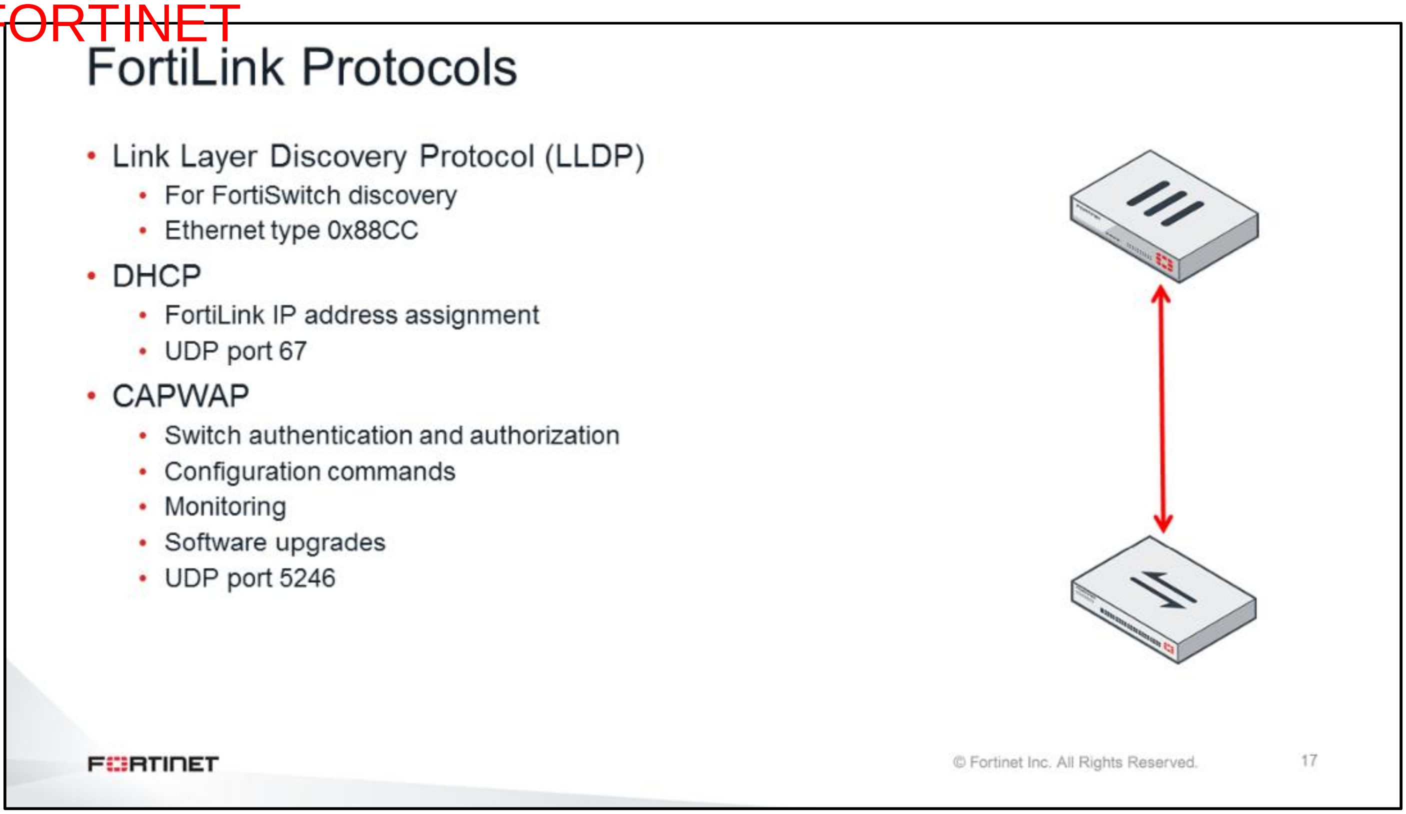
 15

Configuring FortiSwitch as a standalone device requires a direct connection to the management interface or console. You can select **FortiLink Management** to make FortiGate a switch controller that uses CAPWAP, along with other protocols, to communicate.

Standalone configuration requires the administrator to access and manage all FortiSwitch devices in a network manually. This process can add administrative overhead. You should use FortiLink to manage FortiSwitch devices to decrease administrator work and enable Layer 2 security fabric integration.

FortiLink

In this section, you will learn how the FortiLink protocol works.



FortiGate uses multiple protocols for discovering, provisioning, and administrating FortiSwitches. First, FortiGate uses the Link Layer Discovery Protocol (LLDP) to discover FortiSwitch. After that, and after FortiSwitch is authorized, DHCP assigns the FortiSwitch IP address. After IP connectivity is up, CAPWAP authenticates and authorizes the switch. FortiGate also uses CAPWAP to carry configuration commands, monitoring, and software updates.

FortiLink Protocols (Contd)

- FortiLink Heartbeat
  - Includes switch identifier, number of ports, and port attributes
  - Ethernet type 0x88FF
- NTP
  - Time synchronization
  - UDP port 123
- HTTPS
  - Configuration and diagnostics using REST API
  - TCP port 443
- User data
  - Ethernet-tagged traffic using 802.1q frames

FORTINET 18

Once FortiGate is managing FortiSwitch, the two devices interchange FortiLink heartbeat packets. These packets include the switch identifier, number of ports, and port attributes.

FortiLink uses NTP for clock synchronization, and HTTPS for configuration and diagnostics using the FortiSwitch REST API.

Finally, FortiLink transports user traffic using 802.1q VLAN tagging. So, the FortiLink interface between FortiGate and FortiSwitch is a trunk interface, where all control traffic uses the native (untagged) VLAN, and user traffic uses the tagged VLAN.

Enabling the Switch Controller

- To enable the switch controller on FortiGate:

```
config system global
  set switch-controller enable
end
```

- To enable the switch controller GUI on FortiGate:

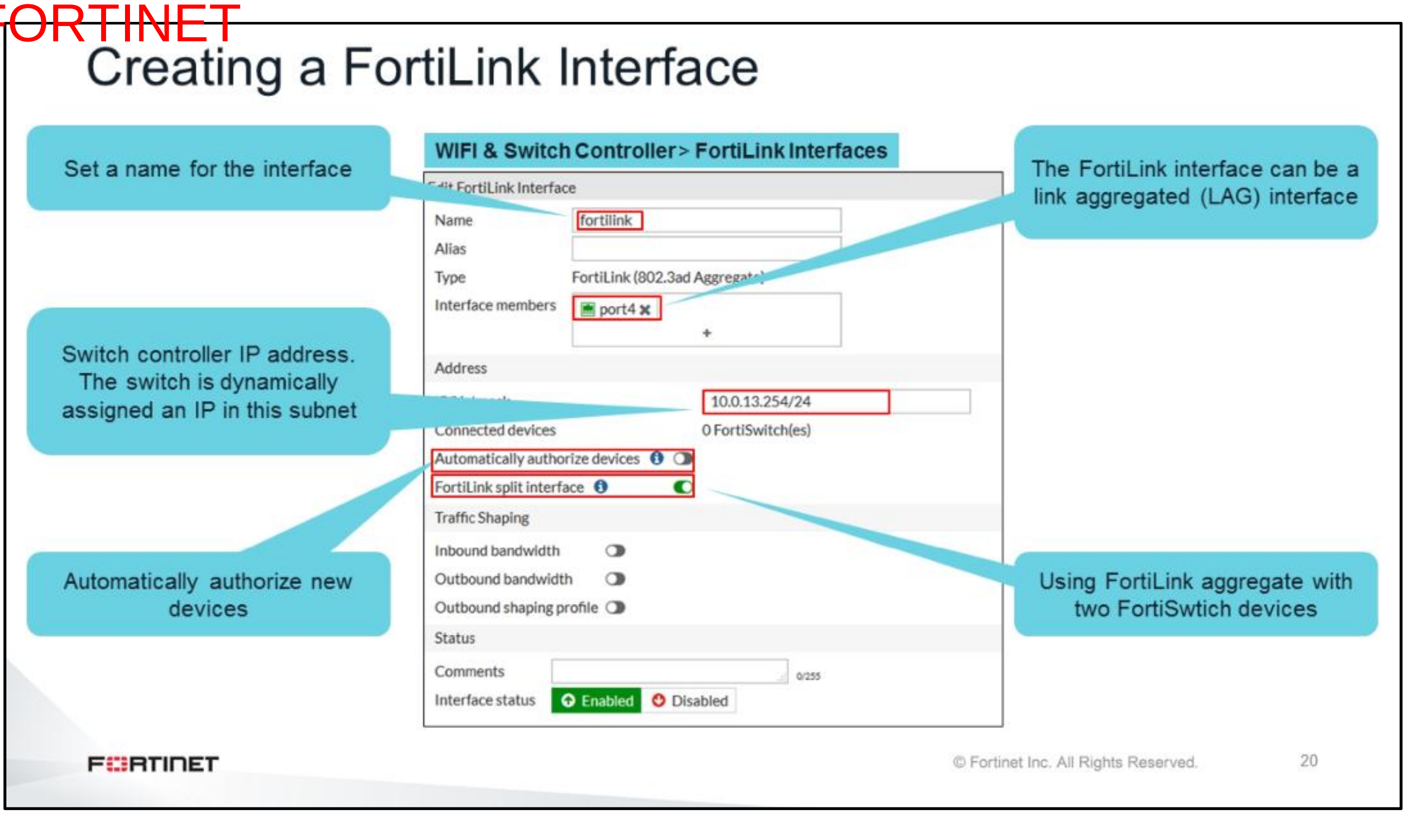
```
config system settings
  set gui-switch-controller enable
end
```

FORTINET

 19

By default, the FortiSwitch controller is disabled. You must enter the `config system global` command followed by the `set switch-controller enable` command.

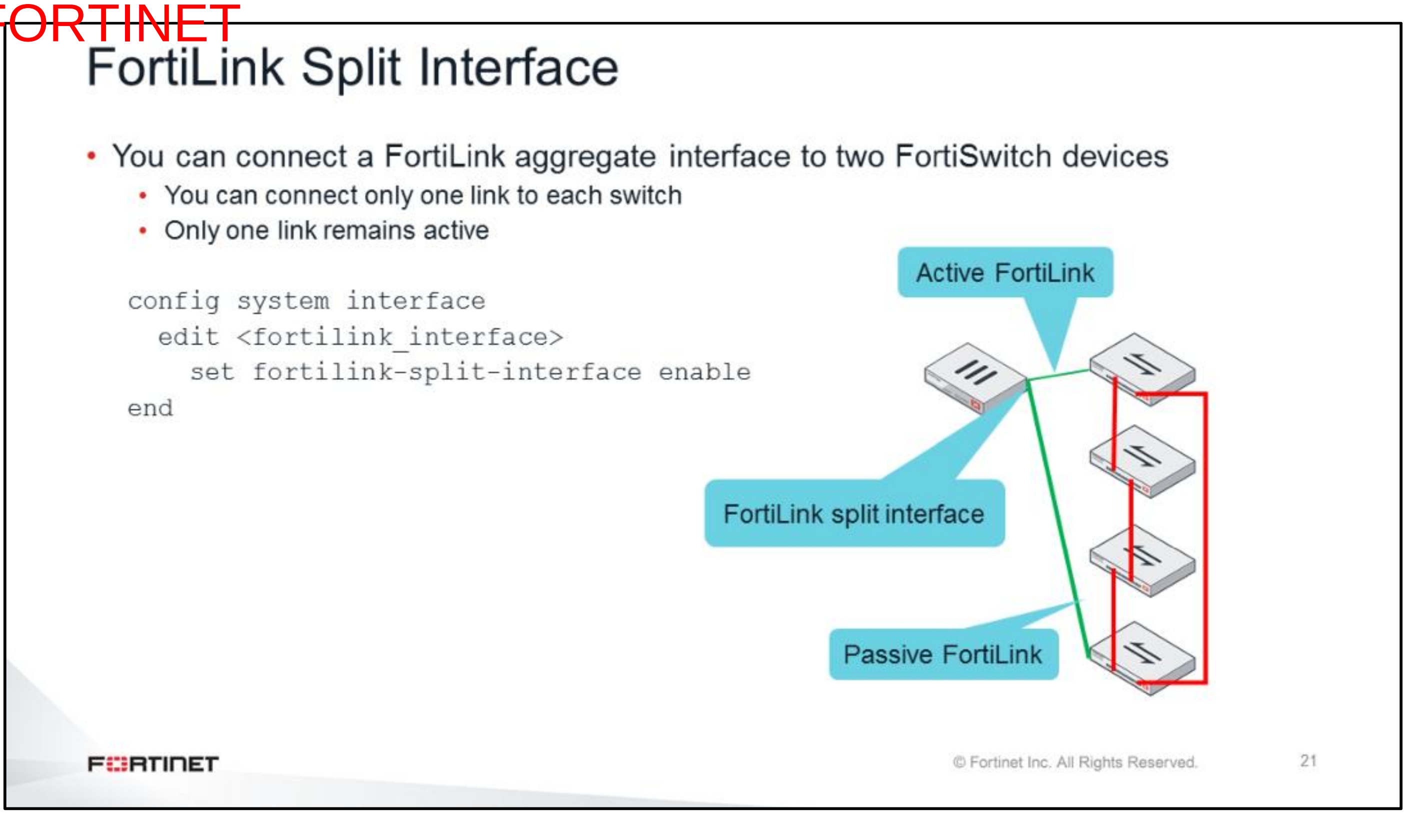
If you want to make the switch controller settings available on the GUI, you must also enter the `config system settings` command followed by the `set gui-switch-controller enable` command.



Once you enable the switch controller globally, you have the option to create a FortiLink and dedicate one of the FortiGate interfaces to FortiSwitch. The interface can be either a physical or an aggregated interface.

You must assign an IP address to the new FortiLink interface, and all the FortiSwitch devices will get IP addresses in this subnet through DHCP.

To allow two links to be connected to two different FortiSwitch devices, the FortiLink split interface must be enabled in the case of an aggregated interface. By default, this option is enabled.



As you learned earlier, you must enable a split interface on a FortiGate aggregated interface to allow two links to be connected to different FortiSwitch devices. One link will be active, the other one will be inactive. This is required in some deployment modes, like the example shown on this slide, which shows multiple FortiSwitch devices connected in a ring topology.

Default Auto-FortiLink Ports

- FortiLink is enabled on all switches
- Previous releases have some FortiSwitch ports (depending on each model) with FortiLink enabled by default
- To enable or disable FortiLink on ports:

```
config switch interface
   edit <port>
      set auto-discovery-fortilink enable
   end
end
```

 22

By default, FortiLink is enabled on all switch ports, beginning in FortiSwitchOS version 3.3.0. In previous releases, depending on the model, only specific ports had FortiLink enabled by default. Please check the model-specific documents to see which ports had FortiLink enabled, or, upgrade the firmware on FortiSwitch to version 3.3.0 or higher.

You can use the command `auto-discovery-fortilink` to enable or disable FortiLink on each FortiSwitch port.

MCLAG Configuration

- FortiSwitch configuration on FortiGate:

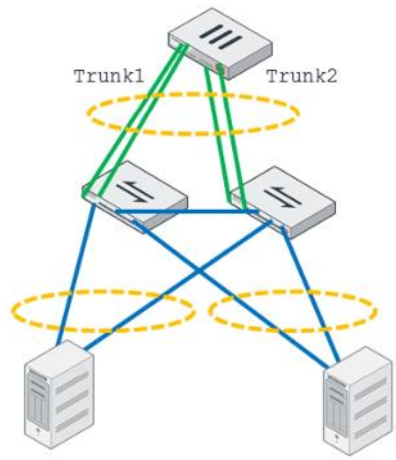
```
config switch-controller managed-switch
    edit <switch_id>
           config ports
                  edit <trunk_name>
                         set mclag enable
    end
```

- Disable split interface:

```
FortiGate# config system interface
  edit <fortilink_interface>
    set fortilink-split-interface disable
end
```

- MCLAG-ICL trunk configuration on FortiSwitch:

```
FortiSwitch# config switch trunk
 edit <trunk_name>
  set mode lacp-active
  set mclag-icl enable
  set members <port1> <port2>
end
```



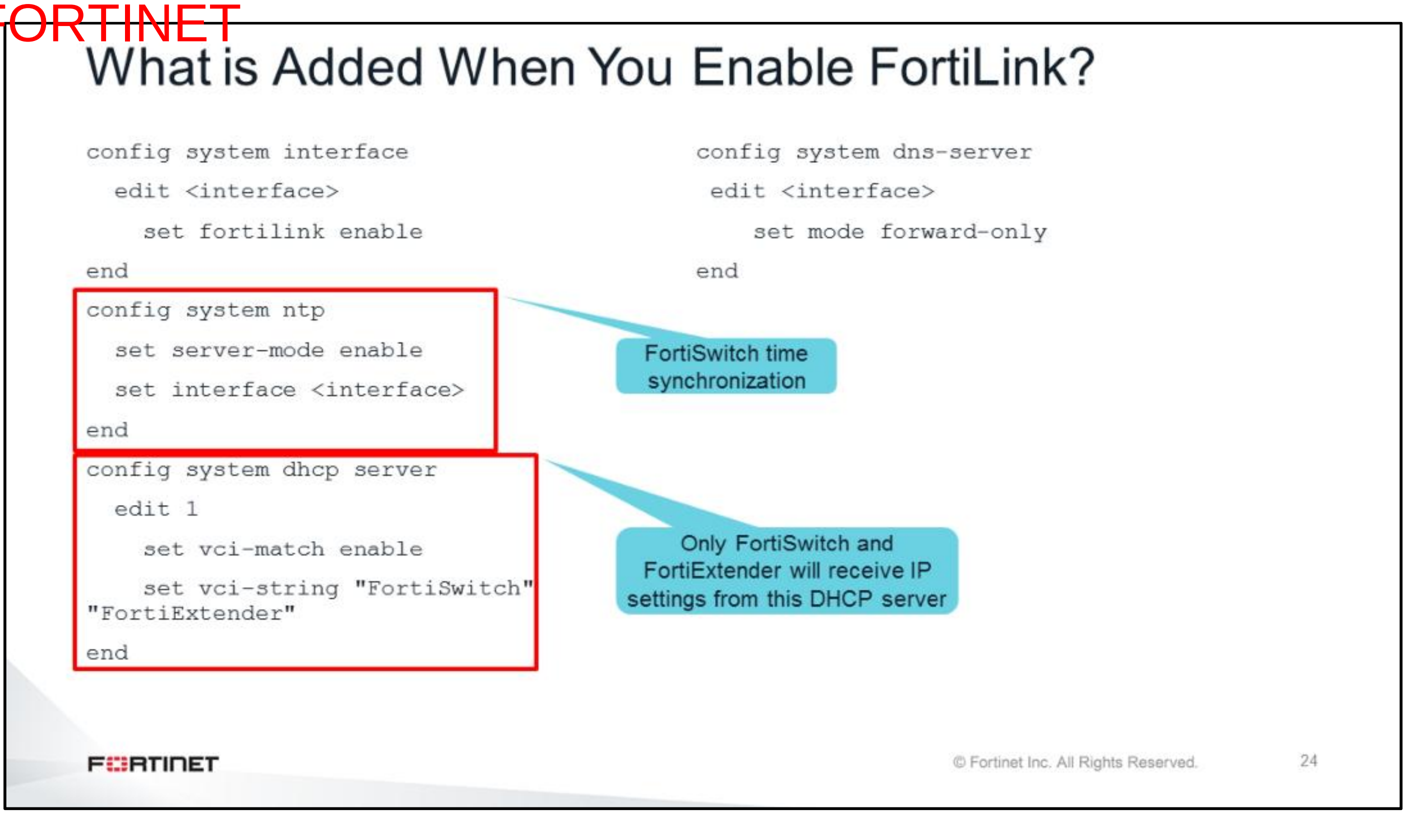
FORTINET

23

As you learned earlier, if it is required to have two or more active FortiLink interfaces from the same FortiGate LAG connected to two FortiSwitches, you must use MCLAG.

You must perform the following three steps to configure MCLAG:

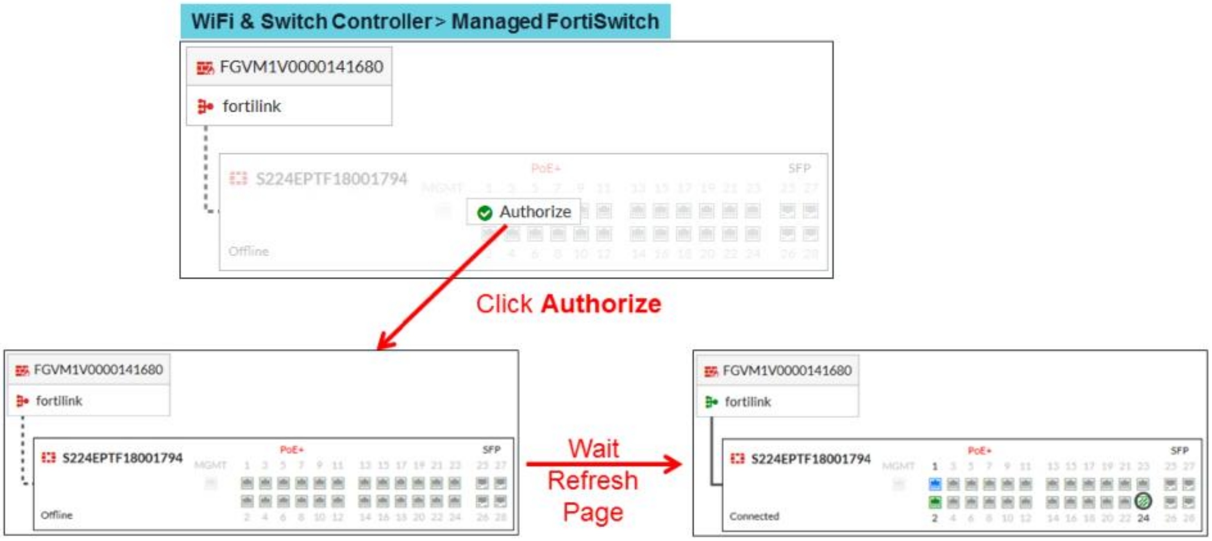
1. Enter the `config switch-controller managed-switch` command followed by the `set mclag enable` command.
2. Disable the split interface.
3. Configure an MCLAG-ICL link between both FortiSwitch devices.



When you dedicate a FortiGate interface to FortiLink, the system automatically applies the following configuration changes to the FortiGate configuration:

- Enables FortiLink on the interface
- Configures FortiGate as an NTP server
- Adds a DHCP server to the FortiLink interface

FortiSwitch Authorization



 25

After you enable FortiLink on the FortiGate interface, FortiLink uses LLDP to discover FortiGate. If you have not configured the FortiGate interface to authorize FortiSwitch automatically, you must manually do it. A few minutes after FortiGate authorizes FortiSwitch, the FortiGate GUI will display a solid line connected to FortiSwitch, indicating that the management is up.

IP Address Assignment

- DHCP monitor shows the IP address assigned to FortiSwitch

Interface	Device	MAC	Reserved	IP	Host Information	Expires	Status
fortilink		70:4c:a5:e0:55:33	Not Reserved	10.0.13.1	VCI: FortiSwitch-224E-POE Hostname: S224EPTF18001794	2019/08/27 14:26:20	Leased out
snf.fortilink		70:4c:a5:e0:55:33	Not Reserved	10.254.252.208	VCI: FortiSwitch-224E-POE Hostname: S224EPTF18001794	2019/08/27 14:25:35	Leased out

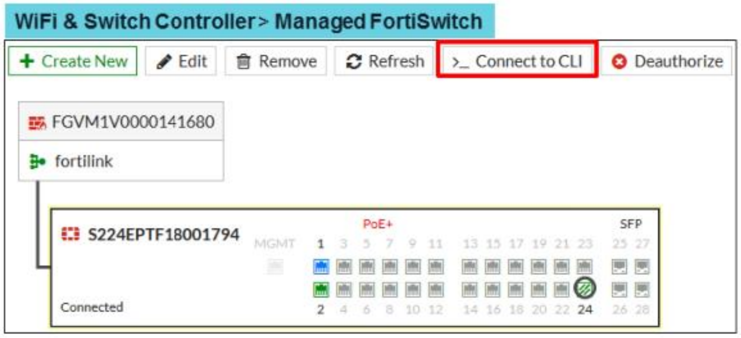
 26

FortiGate assigns an IP address to FortiSwitch through DHCP. The DHCP monitor on the FortiGate GUI displays the FortiSwitch serial number, FortiSwitch hostname, MAC address, and assigned IP address.

It also assigns an IP on the sniffer VLAN, which you will learn about later in this lesson.

Connecting to the FortiSwitch CLI

- On the FortiGate GUI:



- On the FortiGate CLI:

```
# execute telnet <fortiswitch_ip>
# execute ssh <fortiswitch_ip>
```

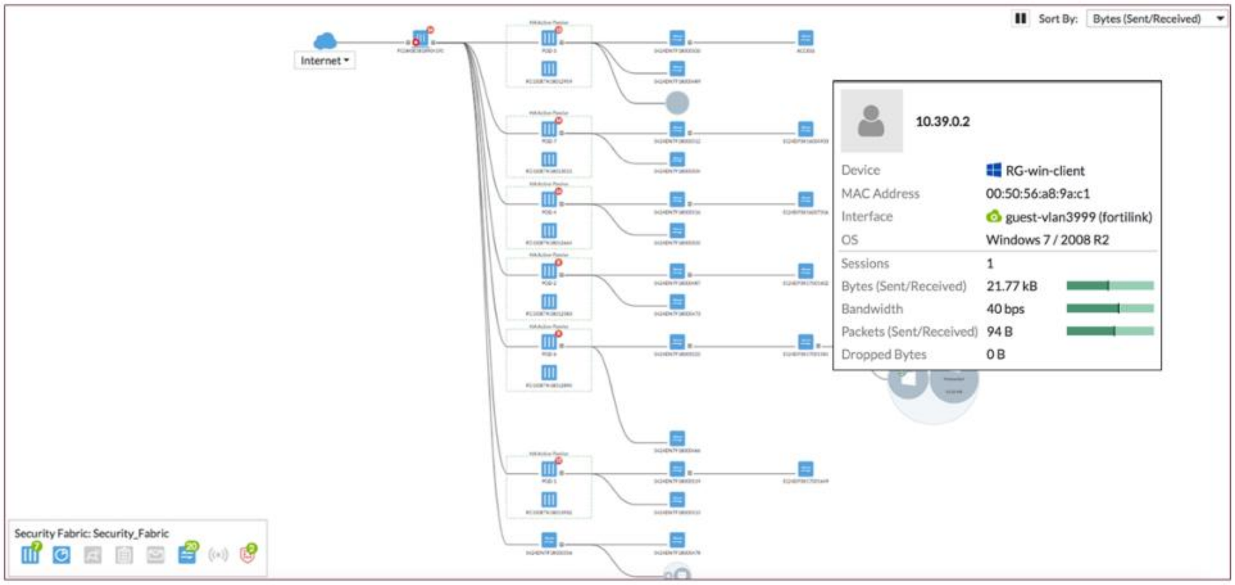
FERTINET

 27

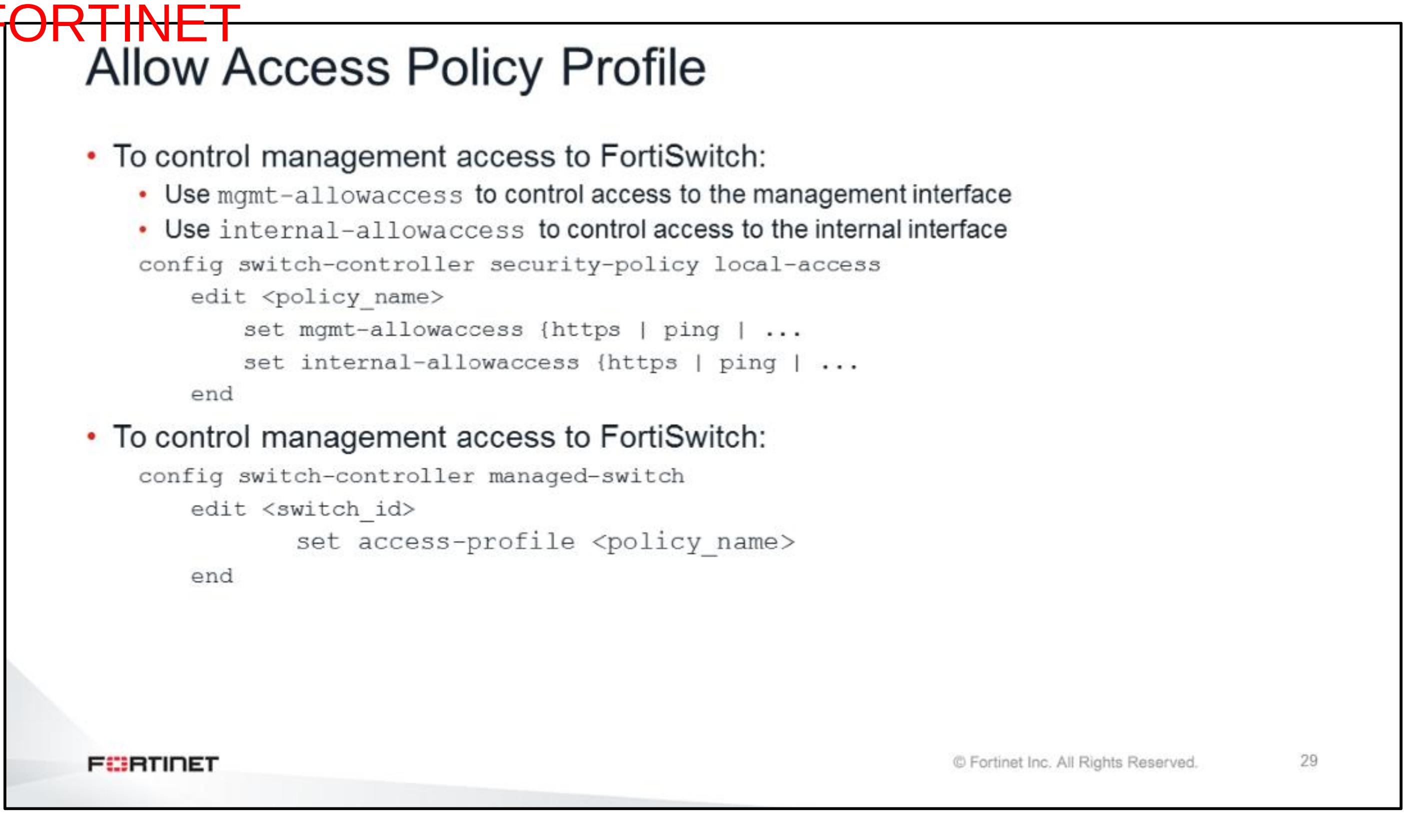
Once FortiSwitch is managed by FortiGate, you usually do not need to connect to the FortiSwitch GUI or CLI. All the administration is done on FortiGate. However, if access to a managed FortiSwitch CLI is required, you can connect to the FortiSwitch CLI by running a telnet or SSH on the FortiGate CLI.

You can also connect to the FortiSwitch CLI using the FortiGate GUI.

FortiSwitch Extends the Security Fabric



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 topology views, you can visualize different security segments, together with all the stacked FortiSwitch and end devices connected.



When a FortiSwitch becomes managed by FortiGate, it is assigned a local-access policy that controls levels of access to the FortiSwitch interfaces.

The profile defines two separate access policies:

1. The management interface
2. The internal interfaces

Change Admin Password on All FortiSwitch Devices

- To override the default configuration and set a password:

```
config switch-controller switch-profile
   edit <profile_name>
         set login-passwd-override {enable | disable}
         set login-passwd <password>
   end
```

- To assign the override password switch policy:

```
config switch-controller managed-switch
   edit <switch_id>
         set switch-profile <profile_name>
   end
```

 30

Switch profiles allow administrators to change the password on multiple FortiSwitch devices managed by the same FortiGate. You assign the FortiSwitch devices to a switch profile by entering the `set switch-profile` command. Then, you set the password by entering the `set login-passwd-override` and `set login-passwd` commands.

Switch Groups

- The following commands group multiple FortiSwitch devices
  - You can perform operations on the entire group instead of one switch at a time:

```
config switch-controller switch-group
  edit <group_name>
    set members <switch_id_1> <switch_id_2> ...
    set description <group_description>
end
```

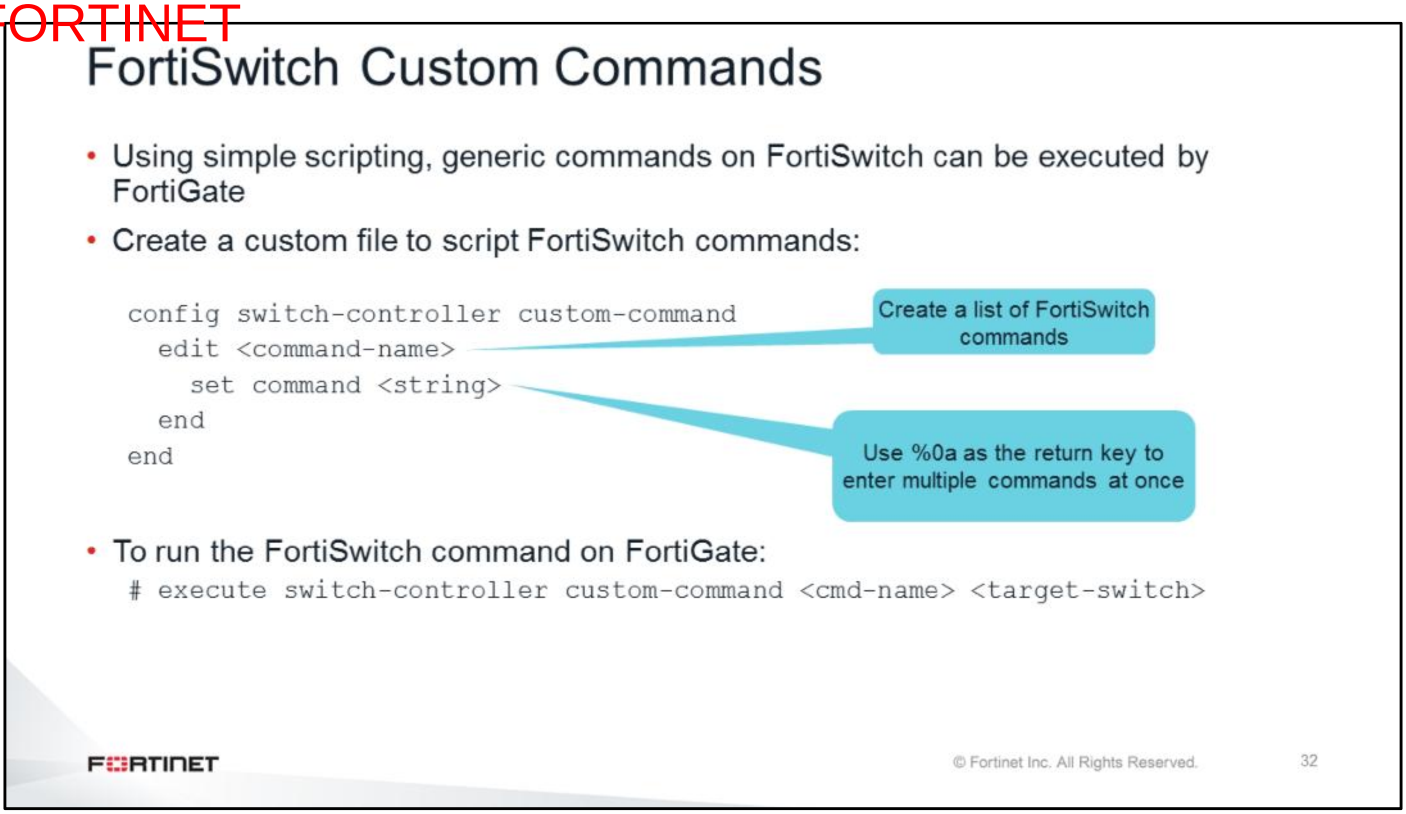
  - For example, to restart all the FortiSwitch devices in a group:

```
# execute switch-controller switch-action restart swtp switch-group
<switch-group ID>
```

FORTINET

31

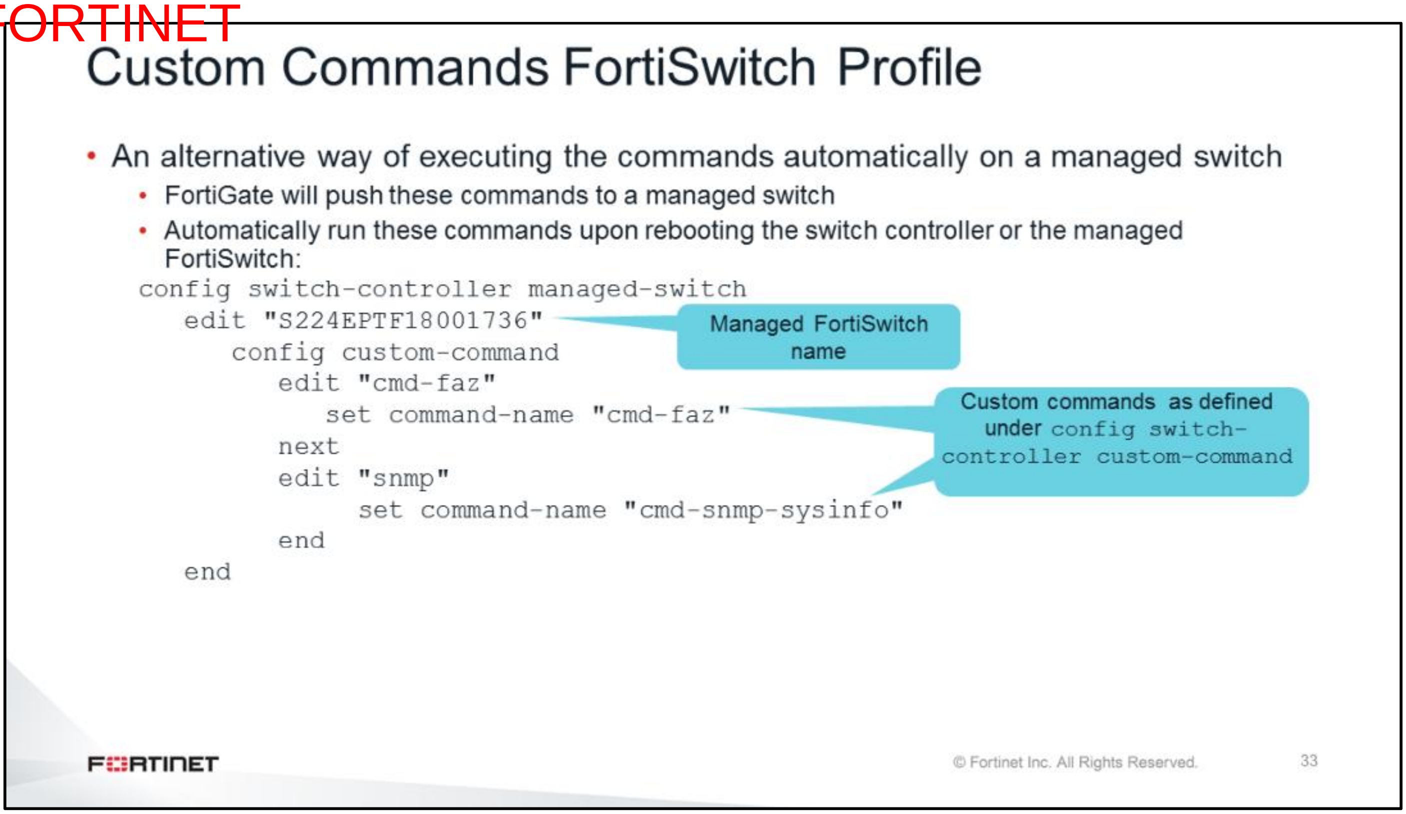
Switch groups, on the other hand, allow you to execute actions over multiple managed FortiSwitch devices. For example, the command `execute switch-controller switch-action restart swtp switch-group` restarts all the FortiSwitch devices that belong to the same switch group.



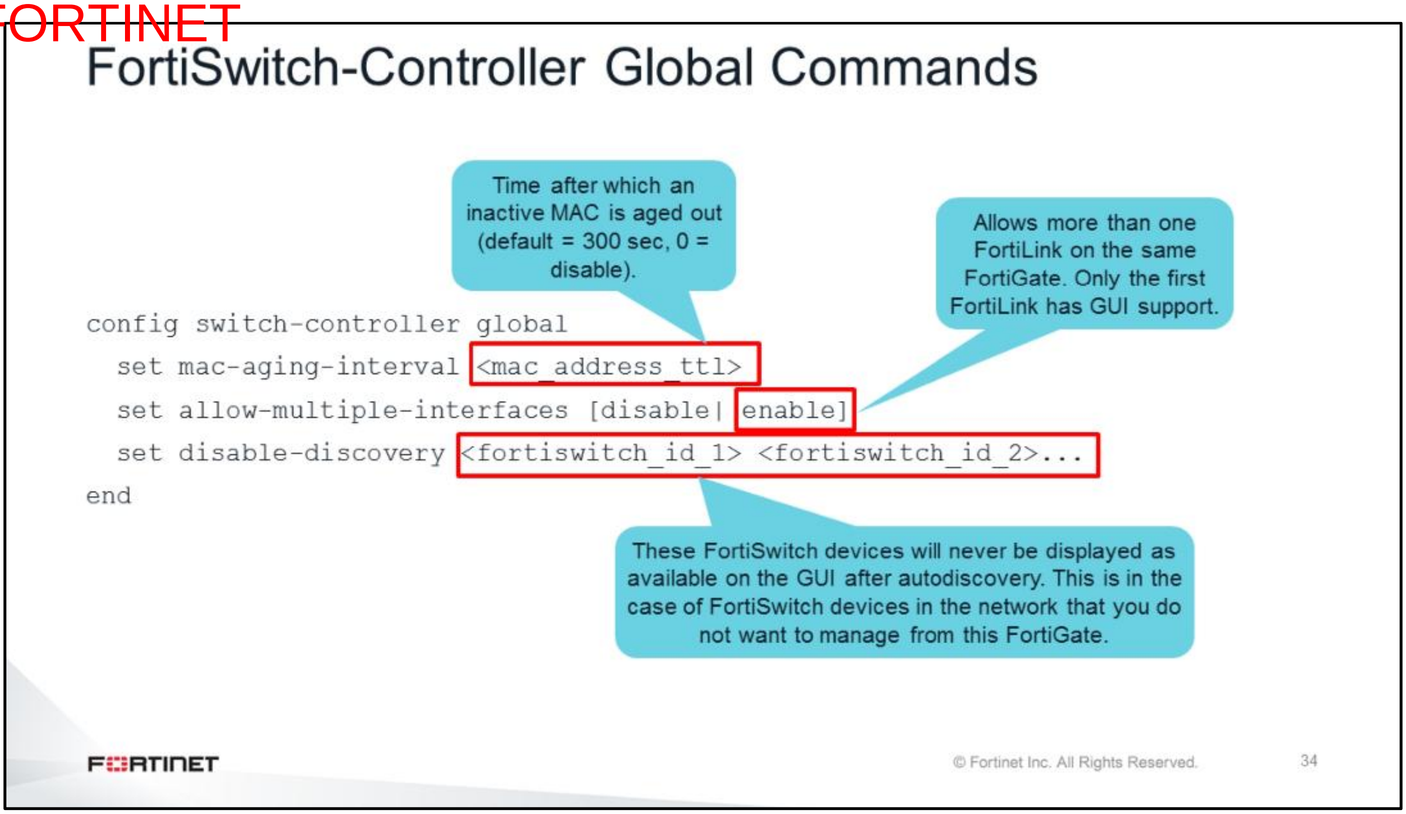
The FortiSwitch managed by FortiGate has limited access to perform commands locally on FortiSwitch.

You can create a simple generic script file to include the commands to run. To separate between commands, you can use the special character %0a as a return key on the CLI.

Run another command on FortiGate to execute the script by specifying the name of the script file and the managed FortiSwitch.



You can configured defined custom commands on the managed FortiSwitch so it can be run once the switch controller or the managed FortiSwitch reboots.



There are three switch controller settings that are applied globally to FortiGate and all managed FortiSwitch devices:

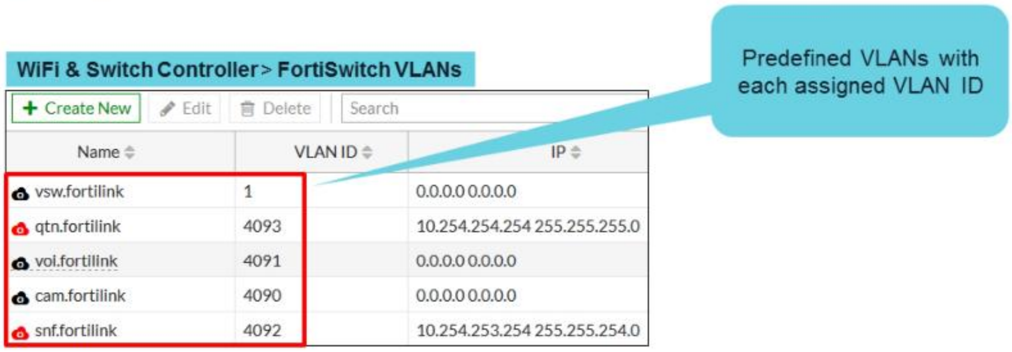
- `mac-aging-interval`: The time after which an inactive MAC address is aged out
- `allow-multiple-interfaces`: By default, you can dedicate one FortiGate interface per VDOM to FortiLink. When you enable this setting, you can dedicate multiple FortiGate interfaces to FortiLink
- `disable-discovery`: A list of FortiSwitch devices connected to FortiGate that you do not want to be discovered. Use this command is cases of FortiSwitch devices that you do not want to manage on FortiGate

Ports and VLANs

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

Preconfigured VLANs

- FortiLink creates additional VLANs, each for specific traffic
  - Default, quarantine, voice, camera, and sniffer
  - Further settings configured, for example, DHCP servers for some VLANs
  - Can be deleted



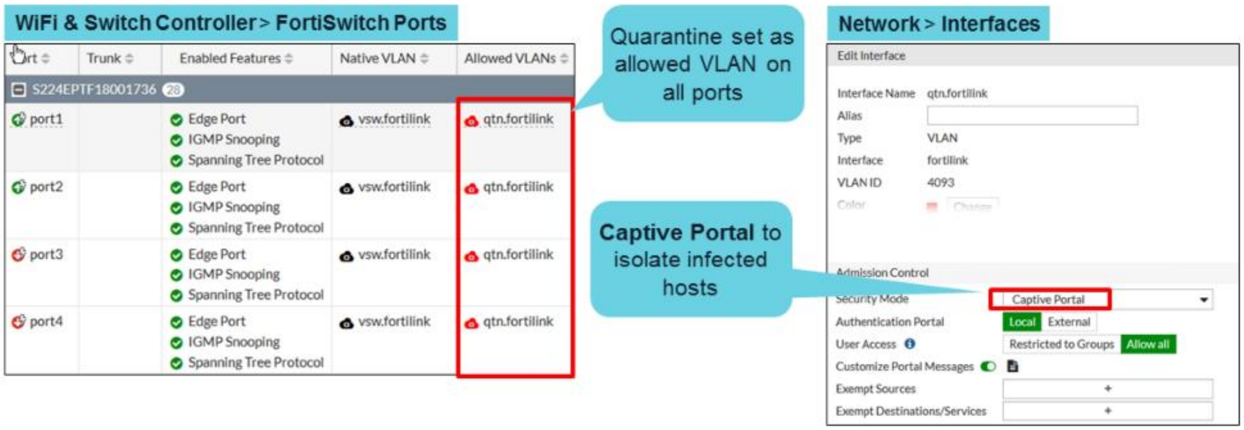
 36

Each FortiLink interface that you create comes with additional defined VLANs. Each VLAN has a VLAN ID preassigned to handle a different type of traffic, such as camera, voice, and packet sniffer.

Some of the VLANs have a preconfigured DHCP server to assign a host IP address, and others are associated with security profiles, such the FortiVoice profile on a voice VLAN.

Quarantine VLAN

- Configured as an allowed VLAN on all ports by default
- Requires firewall policy defined for quarantine and captive portal
- Move infected host MAC to the quarantine VLAN

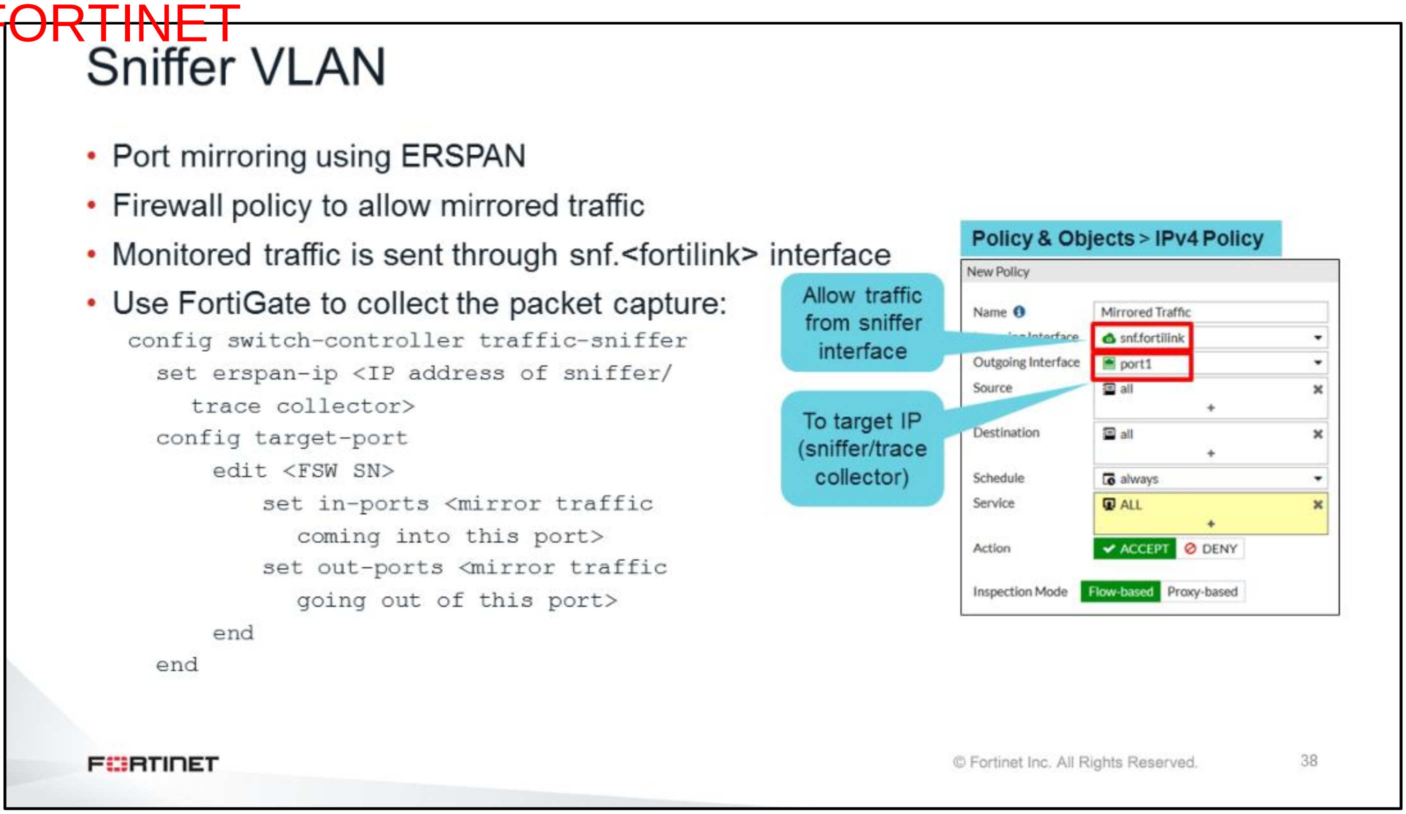


FORTINET

 37

By default, a Quarantine VLAN is set as the allowed VLAN on all ports. The VLAN is used to quarantine hosts using actions such as automation stitch in the Security Fabric, that is, to isolate malicious traffic and avoid spread of attacks from infected hosts.

The infected host MAC address is moved to the quarantine VLAN and continues to be in full isolation. The captive portal is used for remedial actions and has a firewall policy with the action set to **Deny**.



The network traffic sniffer can easily provide monitoring on data traffic passing through FortiSwitch. You can use the predefined sniffer VLAN to use the Encapsulated Remote Switched Port Analyzer (ERSPAN) to monitor traffic sent through the FortiLink sniffer interface.

By creating a firewall policy to allow mirror traffic and define sniffer parameters using the CLI on FortiGate, you can use MAC, IP, and ports to mirror traffic ingress and egress, and specify the packet capture collector IP, which, in this case, is FortiGate.

Power Over Ethernet (PoE) Configuration

- PoE uses a single Ethernet cable to provide data and electrical power
  - Power devices like Wi-Fi AP, cameras, and phones
- PoE power mode
  - Priority based: Lower ports gets power first–high number may get disabled if more power needed
  - First come, first served (FCFS): Existing powered devices receive power first
- Maximum power and threshold settings
- Settings can be global or per port
- Configuration on the FortiSwitch CLI

```
config switch global
  set poe-power-mode <mode>
  set poe-alarm-threshold <integer>
  set poe-guard-band <integer>
end
```

FEURTINET

 39

PoE uses a single Ethernet cable to provide both a data connection and electrical power to devices such as wireless access points (AP), IP cameras, and VoIP phones.

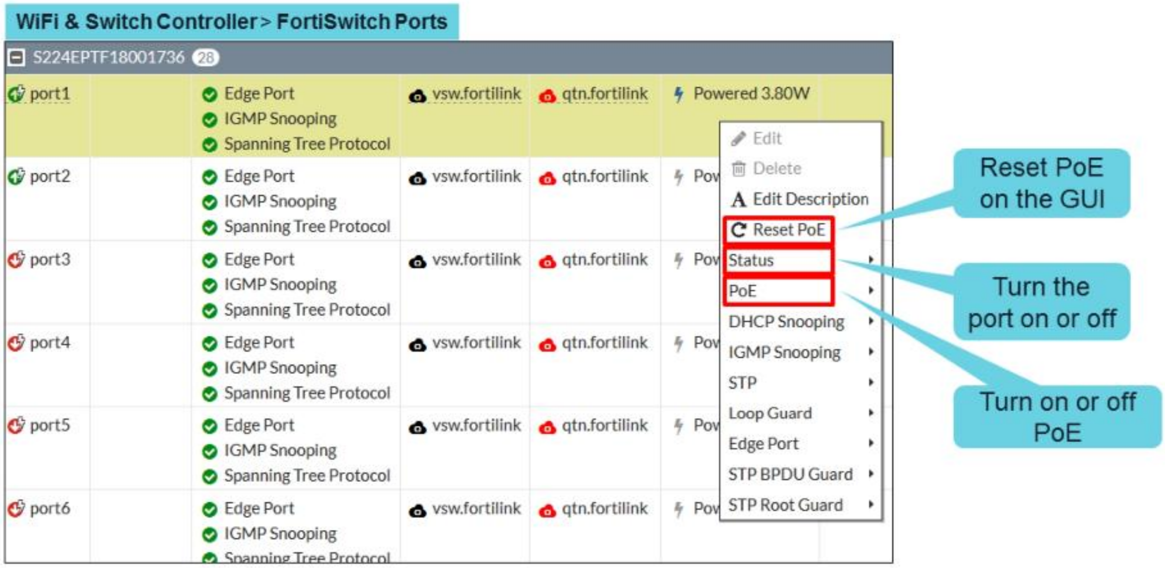
Power mode is based on priority, and the FCFS process.

Priority mode gives lower numbered ports higher priority, that is, port1 has the highest priority. Higher numbered ports are disabled first when more power is needed.

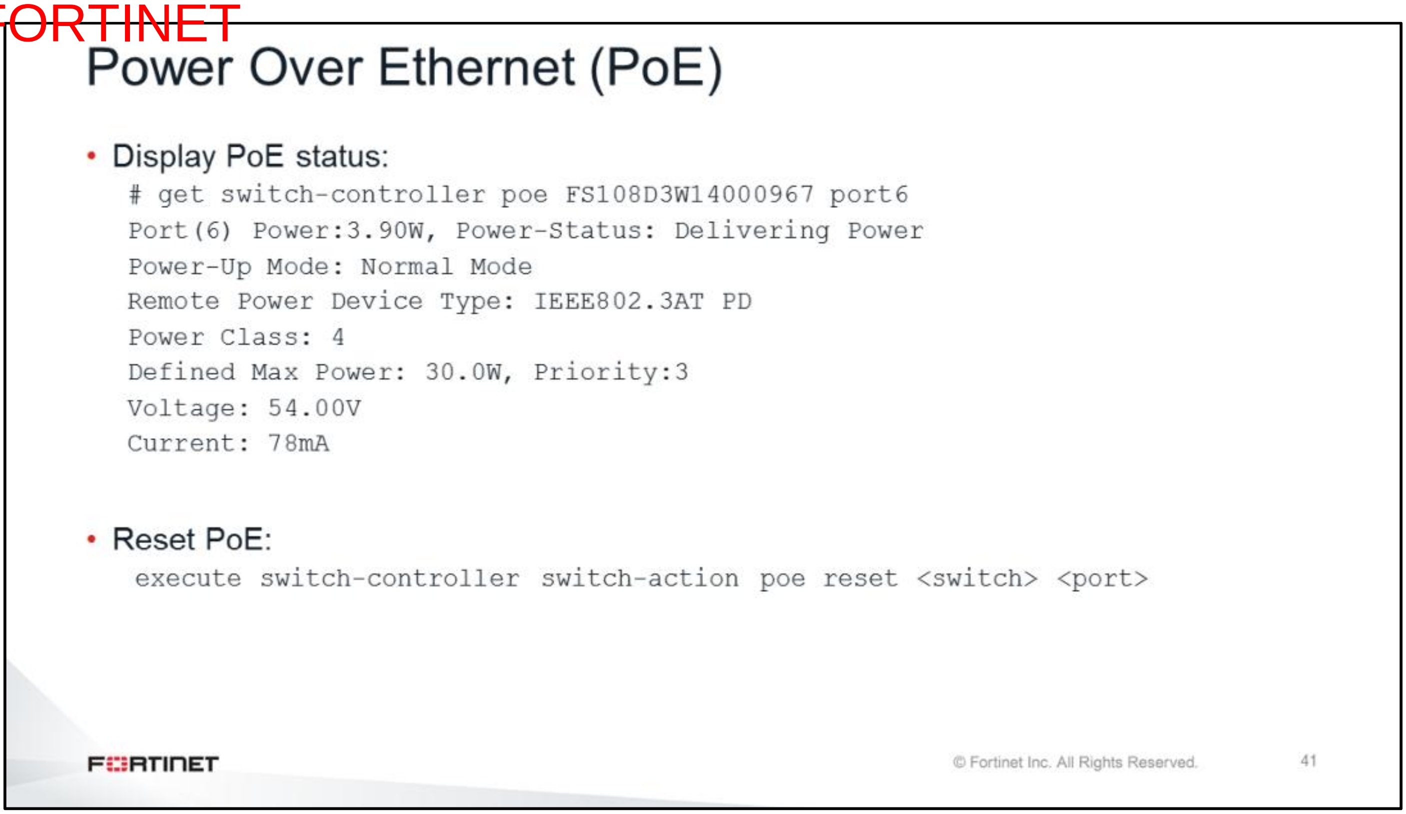
FCFS mode will continue to provide power to connected PoE devices. New devices do not connect if there is not enough power.

In addition to PoE mode, you can set maximum power and threshold levels. Depending on the FortiSwitch model, you can configure the settings globally or per physical port.

Configuring Ports

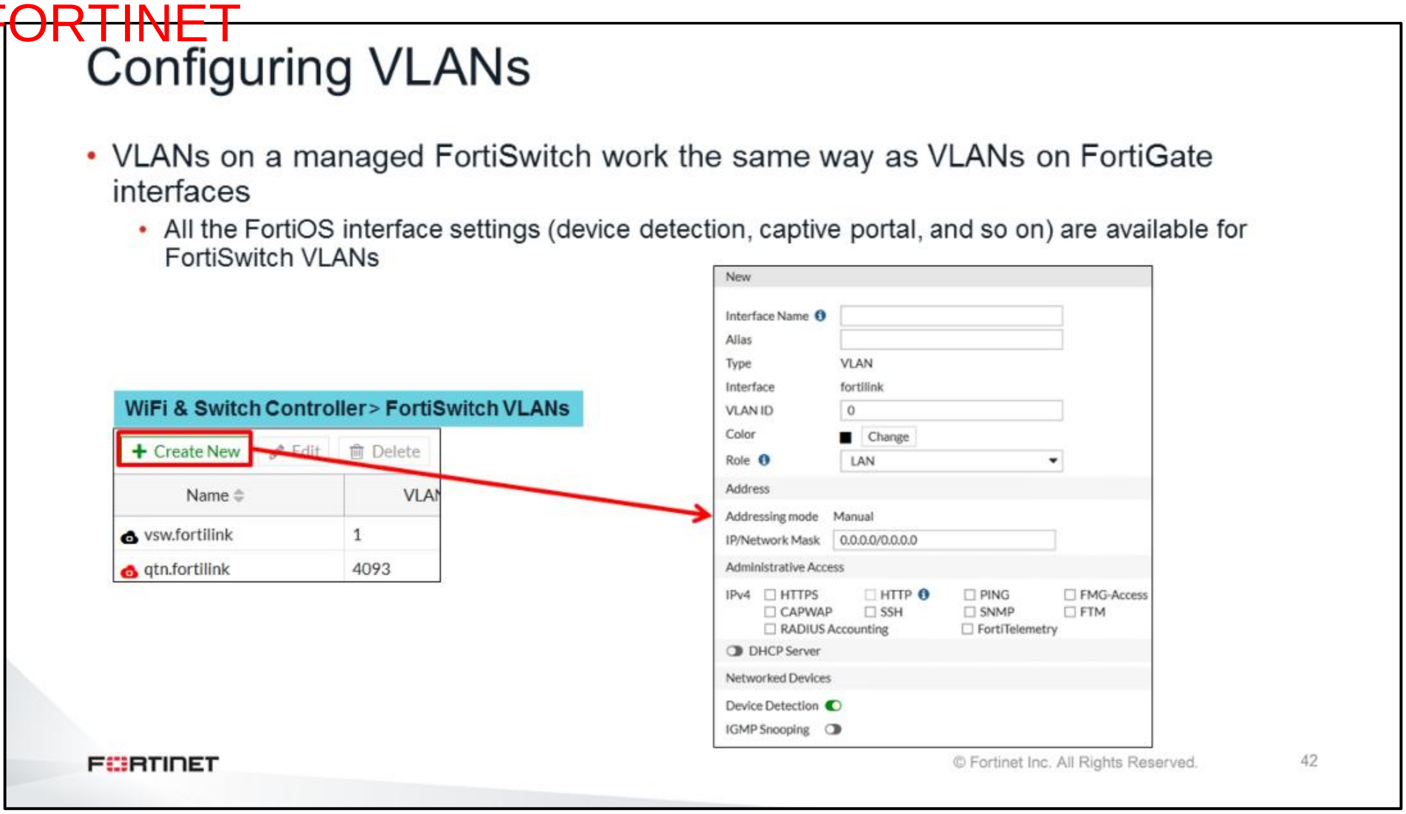


On the FortiGate GUI, you can change the status of a port, or the port PoE.

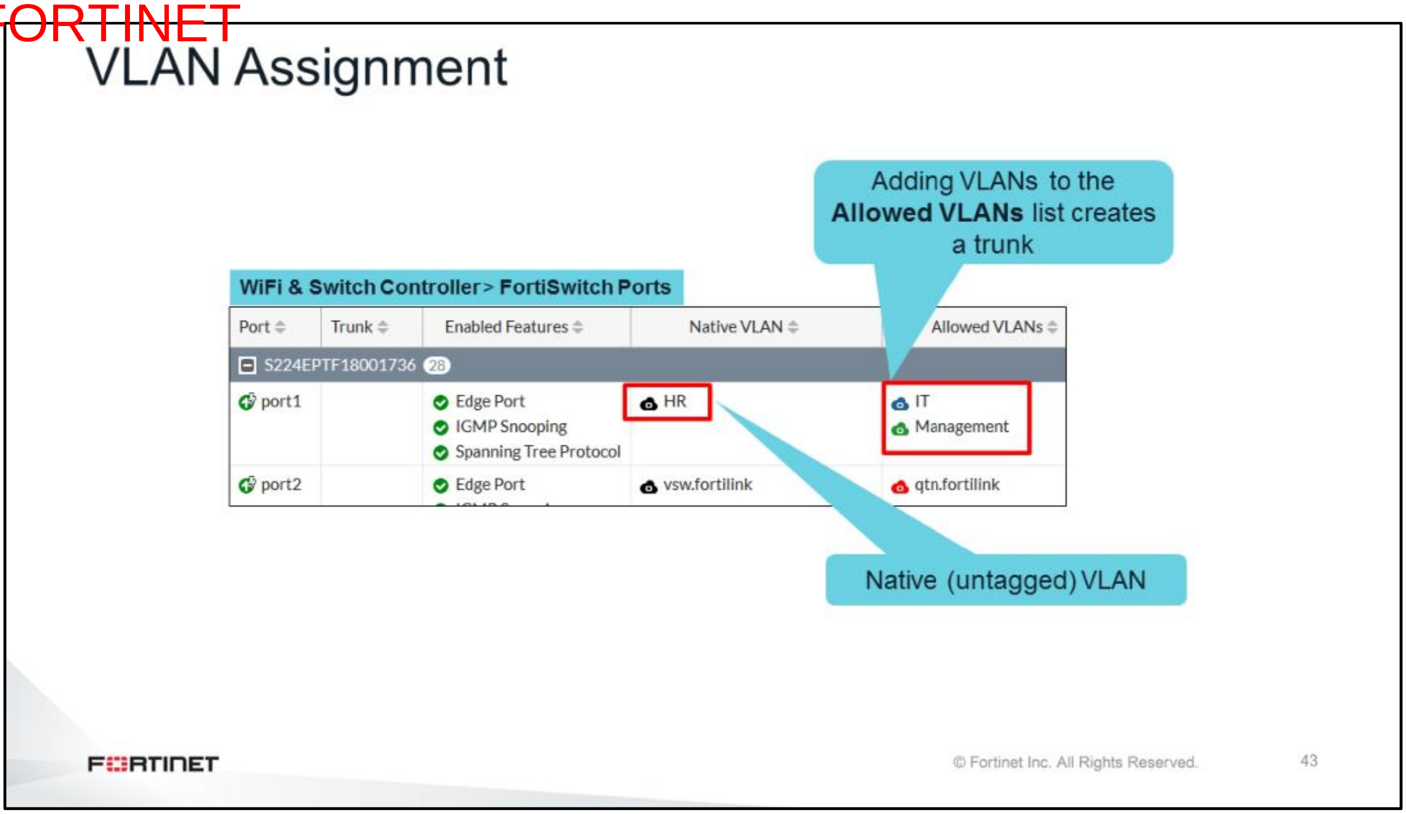


You can also restart the port PoE on the CLI, using the command `execute switch-controller poe-reset`.

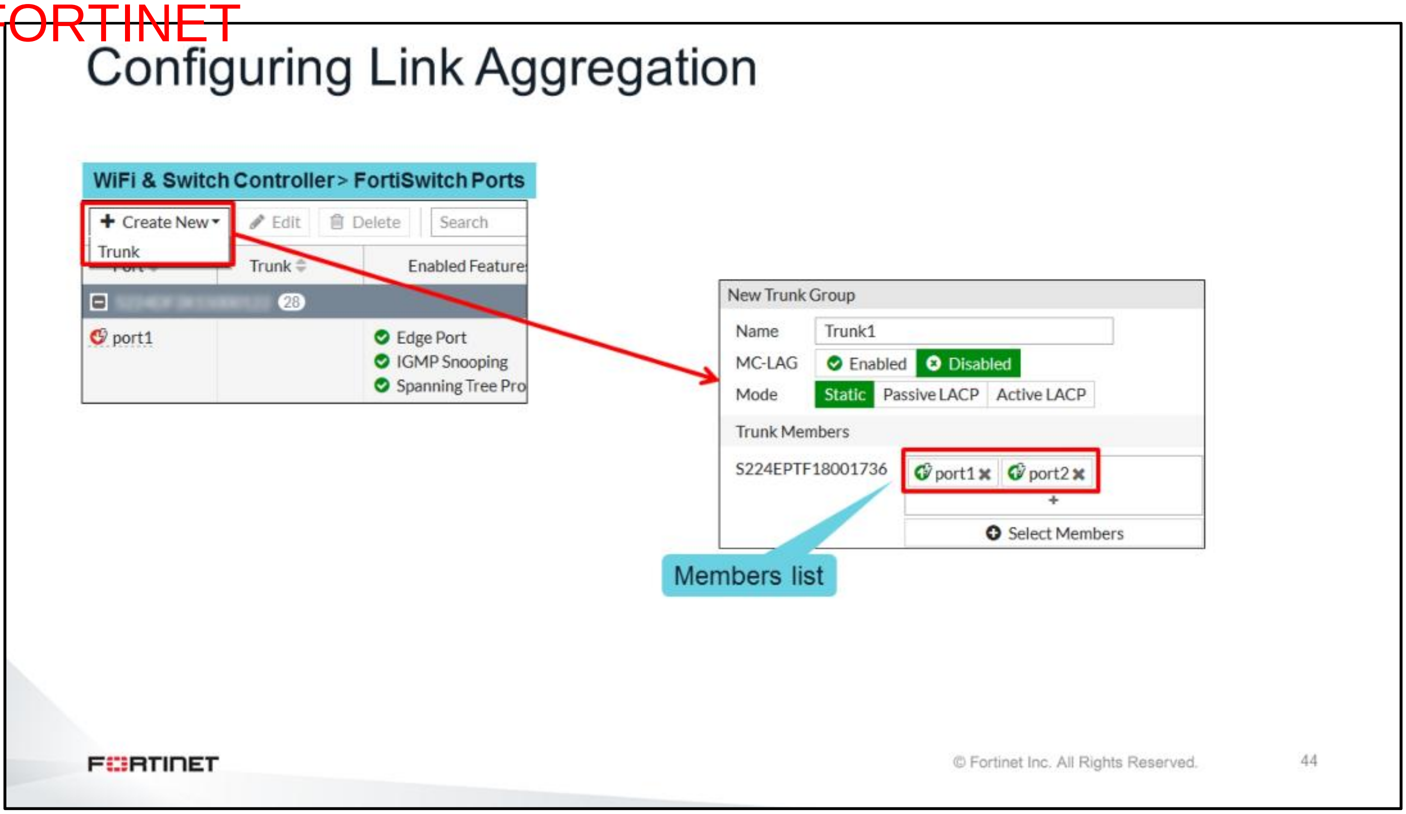
The command `get switch-controller poe` shows information about the port PoE, such as power class, voltage, current, and maximum power.



When you use FortiLink, managed FortiSwitch devices become an extension of FortiGate. You configure and use FortiSwitch VLANs in the same way as FortiGate VLANs. All interface settings usually available on FortiGate VLANs, are available on FortiSwitch VLANs, such as device detection, captive portal, and so on.



Once you create the VLANs, you define which FortiSwitch ports are assigned to each VLAN by selecting the respective VLAN as the **Native VLAN** for the port. In the same GUI section, you can convert one FortiSwitch port to a trunk by selecting one or more additional VLANs under **Allowed VLANs**.



You can create link aggregation interfaces on the FortiGate GUI by clicking **WiFi & Switch Controller** > **FortiSwitch Ports**.

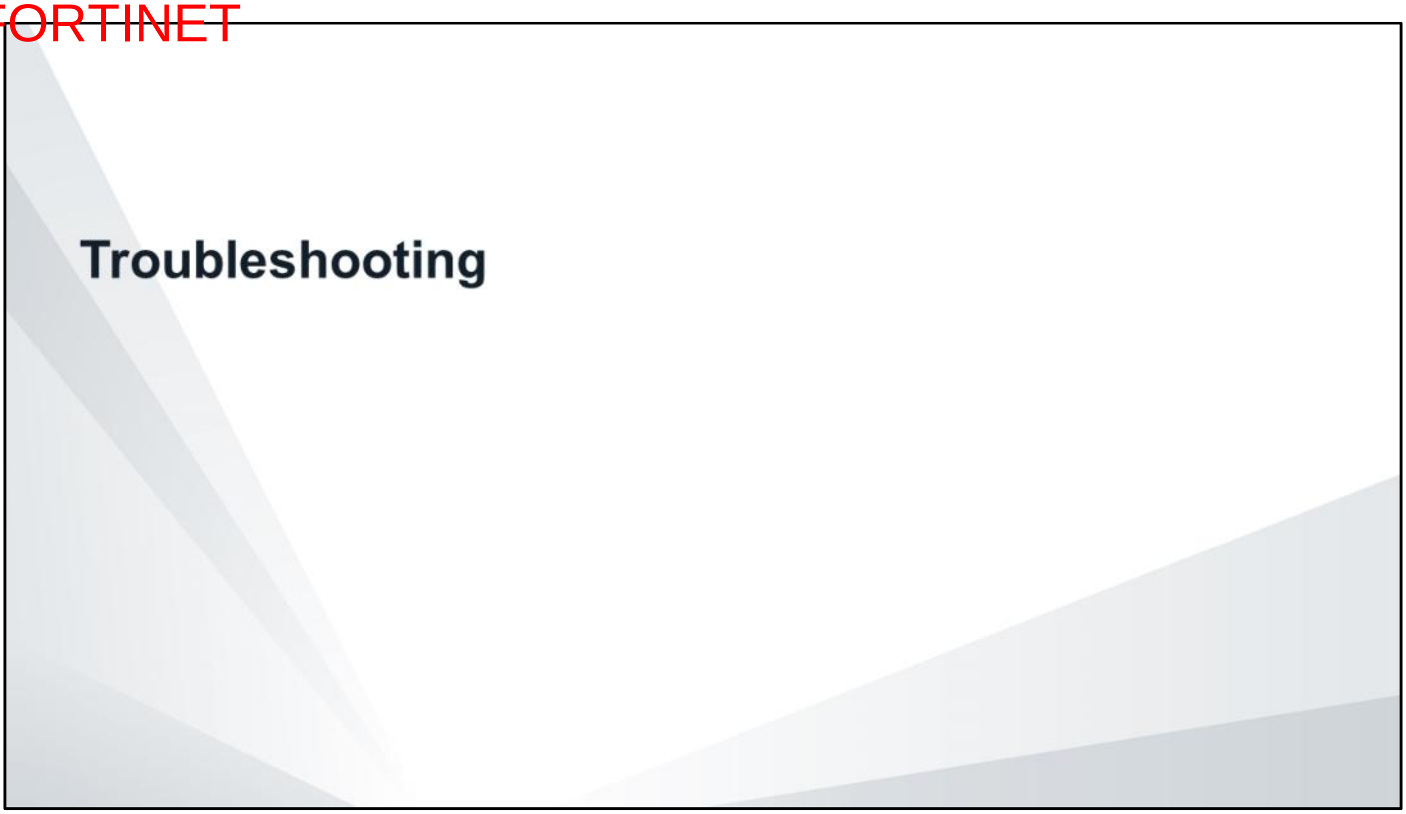
Creating Firewall policies

- Firewall policies can include FortiSwitch VLANs as incoming and/or outgoing interfaces
  - All the security inspection profiles, NAT settings, and so on, are available

F::RTINET

45

You can select the FortiSwitch VLANs as incoming and outgoing interfaces in the FortiGate firewall policies in the same way that you can select FortiGate VLANs. All the regular firewall policy settings, such as security inspection profiles, NAT settings, and so on, are available in policies coming from, or going to, FortiSwitch VLANs.



In this section, you will learn about CLI commands to use for FortiSwitch troubleshooting and diagnostics.

FortiSwitch Status

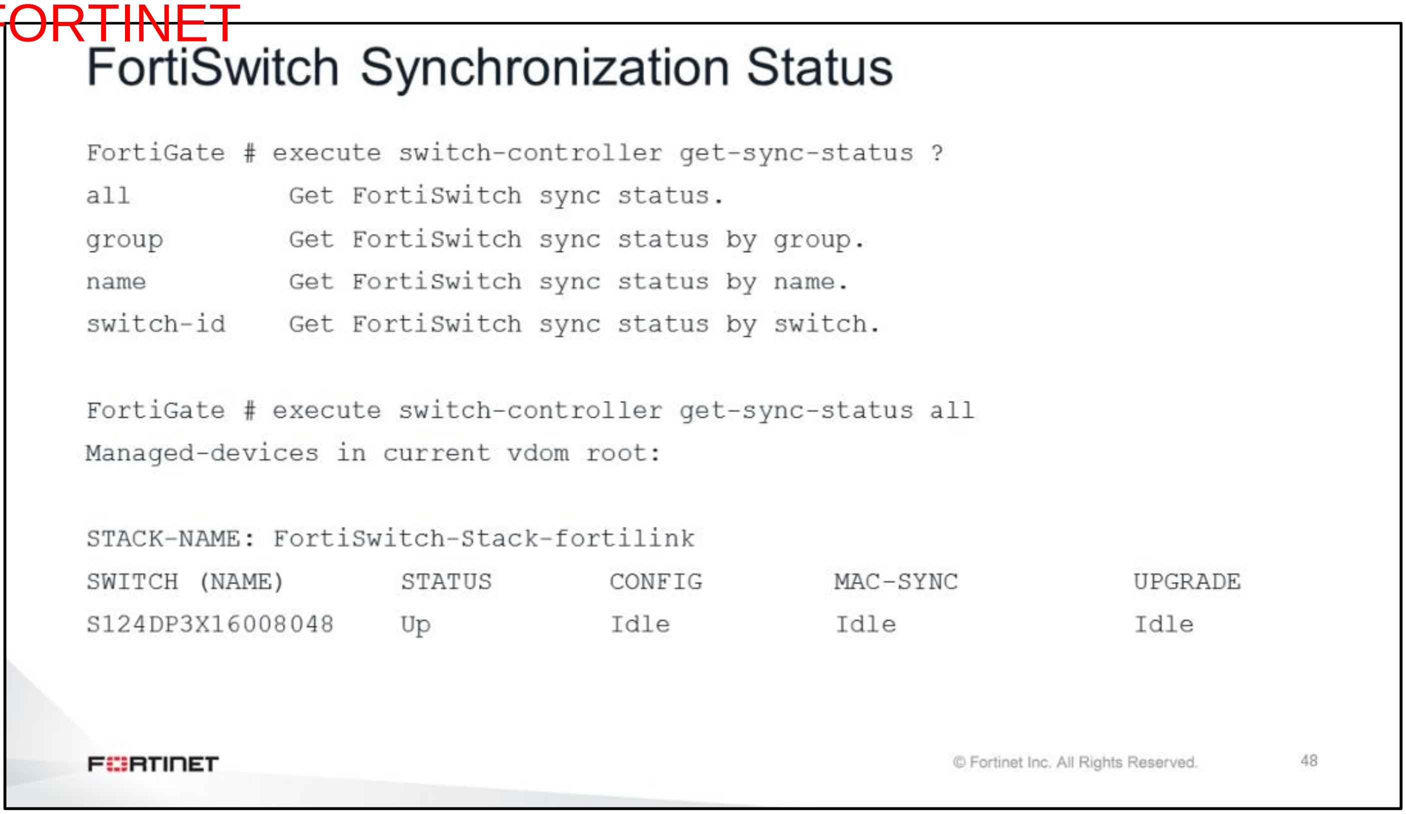
```
# get switch-controller managed-switch
== [ FS108D3W17002387 ]
switch-id: FS108D3W17002387
# execute switch-controller get-conn-status
Managed-devices in current vdom root:

STACK-NAME: FortiSwitch-Stack-fortilink
SWITCH-ID         VERSION    STATUS          FLAG  ADDRESS        JOIN-TIME                 NAME
FS108D3W17002387 v6.2.1     Authorized/Up    -    10.1.1.2       Thu Aug  22 04:39:13 2019    -

        Flags: U=upgrading, S=staged, D=delayed reboot pending, E=configuration sync error
        Managed-Switches: 1 UP: 1 DOWN: 0
```

FORTINET

 47

The command `get switch-controller managed-switch` shows the ID of all FortiSwitch devices managed by FortiGate.

The command `execute switch-controller get-conn-status` shows more information about each managed FortiSwitch, such as the FortiSwitch OS version, status, IP address, and time that FortiSwitch joined FortiGate management.



Each time you change the FortiSwitch configuration on FortiGate, the change is saved in the FortiGate configuration first. Then, FortiGate pushes the configuration change to FortiSwitch, and FortiSwitch saves it in its configuration.

The command `execute switch-controller get-sync-status` shows the configuration synchronization status between FortiGate and FortiSwitch.

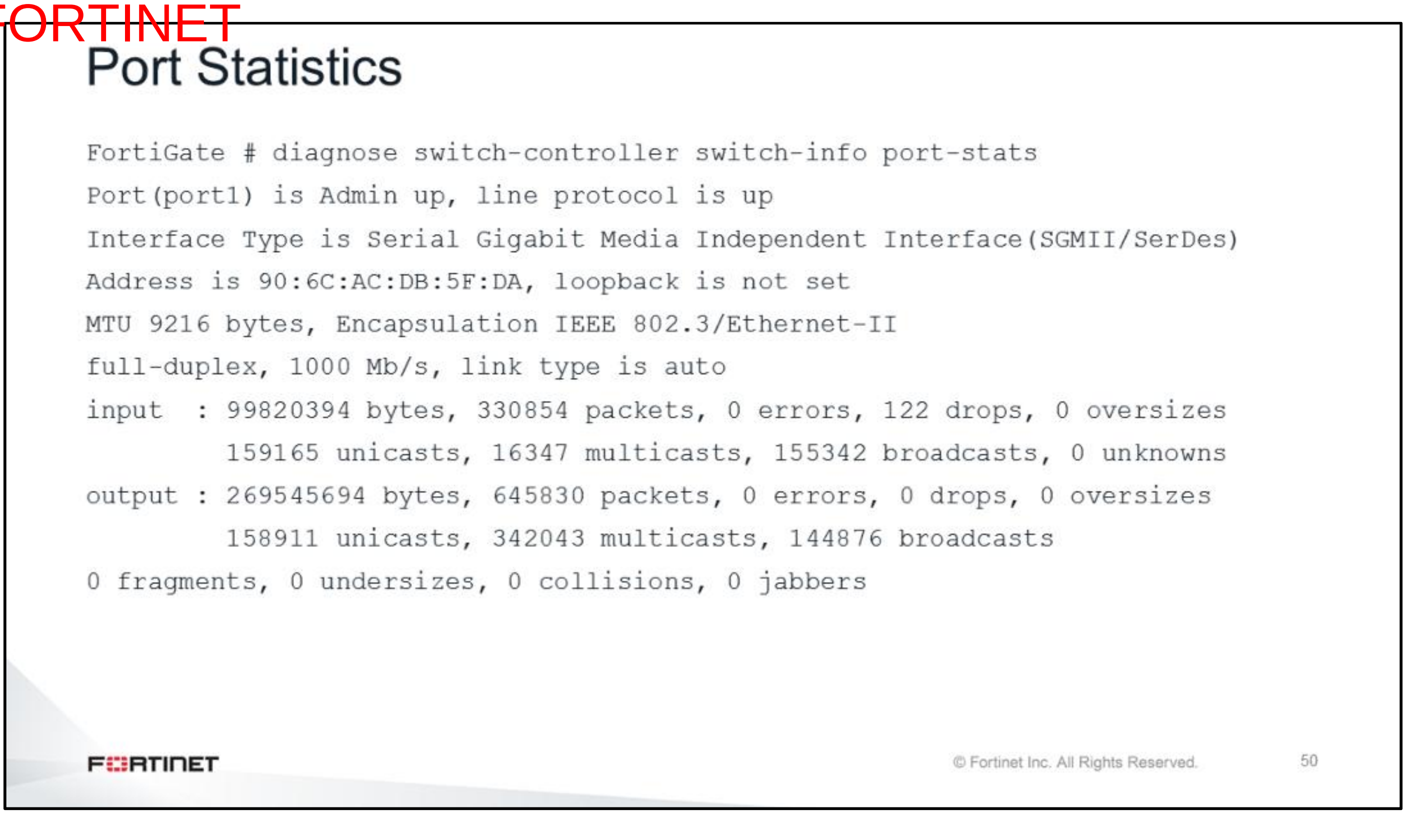
Port Status

```
# execute switch-controller get-conn-status S224EPTF18001736
Get managed-switch S224EPTF18001736 connection status:
Admin Status: Authorized
Connection: Connected
Image Version: S224EP-v6.2.1-build176,190620 (GA)
Remote Address: 10.0.13.1
Join Time: Thu Aug 22 07:57:52 2019
   interface    status   duplex  speed     fortilink   stacking    poe status
    port2        up        full   1000Mbps  yes          no         Delivering Power
    port3      down        N/A    0          no          no         Searching
Aggregate Interfaces:
    Interface                Status   Duplex    Speed          Type
    GVM1V0000141680 *)       up       full      1000Mbps        FL
ISL: Inter-Switch-Link trunk.
FL: Fortilink Trunk connected to FGT.
(*): System auto generated trunk
```

FURTINET

49

The command on this slide shows details about a managed FortiSwitch. The details include information about each port, such as link status, duplex mode, speed, and PoE status.



The command shown on this slide lists the counters, such as packets sent and received, and errors, for each FortiSwitch port.

MAC Table

```
# diagnose switch-controller switch-info mac-table
Vdom: root
S224EPTF18001736        0 :

 MAC address           Interface          vlan
======================================================
70:4c:a5:e0:4e:67       internal           4094
00:50:56:96:37:cd       GVM1V0000141680    4094
70:4c:a5:9d:0a:e8       port1              100
70:4c:a5:e0:4e:67       internal           4092
```


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

Other switch-info Commands

```
FortiGate # diagnose switch-controller switch-info ?
lldp                    LLDP-related information.
mclag                   Dumps MCLAG related information from FortiSwitch.
trunk                   Trunk information.
port-stats              Managed FortiSwitch port statistics.
qos-stats               Managed FortiSwitch QoS statistics.
modules                 Dumps modules related information from FortiSwitch.
stp                     Managed FortiSwitch STP instance status.
bpdu-guard-status       Managed FortiSwitch STP BPDU guard status.
mac-table               Managed FortiSwitch MAC address list.
igmp-snooping           IGMP snooping information.
loop-guard              Managed FortiSwitch loop-guard status.
dhcp-snooping           Managed FortiSwitch DHCP snooping interface list.
arp-inspection          Managed FortiSwitch ARP inspection interface list.
802.1X                  Managed FortiSwitch port 802.1X status.
mac-limit-violations    Managed FortiSwitch violated MACs.
flow-tracking           Managed FortiSwitch flow information.
mirror                  Managed FortiSwitch mirror information.
```

 52

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

FortiGate and FortiSwitch Processes

- You can enable real-time debugs for any of these processes (on both FortiGate and FortiSwitch)

Function	FortiGate Process Name	FortiSwitch Process Name
FortiLink discovery and heartbeat	`fortilinkd`	`fortilinkd / flcmdd`
CAPWAP	`cu_acd`	`cu_swtpd`
Configuration changes	`flcfgd / cu_acd`	`cu_swtpd`

- To enable a real-time debug on FortiSwitch (and FortiGate):

```
# diagnose debug application <process_name> <debug_level>
```

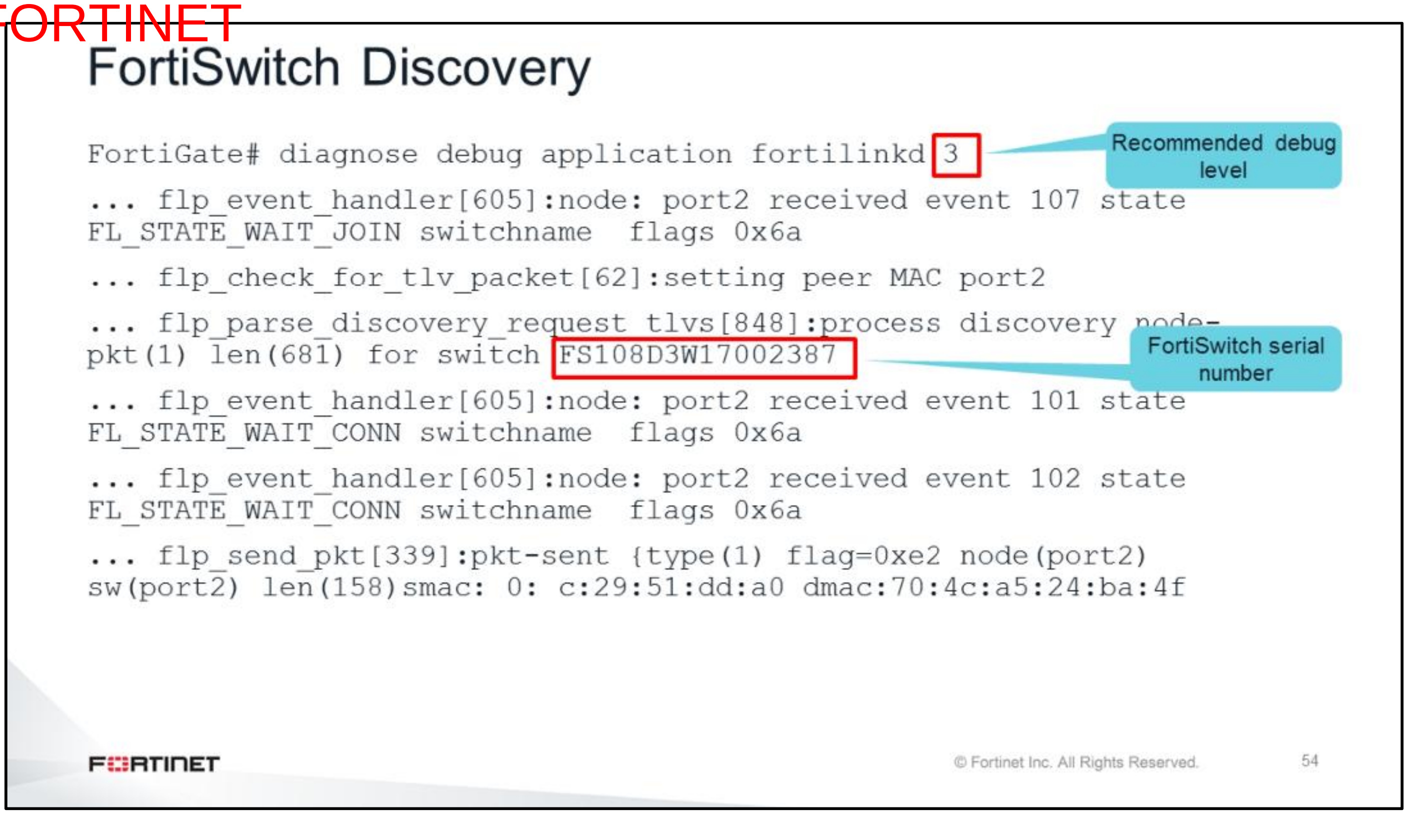
FORTINET

53

The table on this slide shows the processes that handle the communication between FortiGate and FortiSwitch. On the FortiGate side, the `fortilinkd` process handles the FortiSwitch discovery and FortiLink heartbeat. The CAPWAP communication is handled by the `cu_acd` process. Configuration changes are handled by the `flcfgd` and `cu_acd` processes.

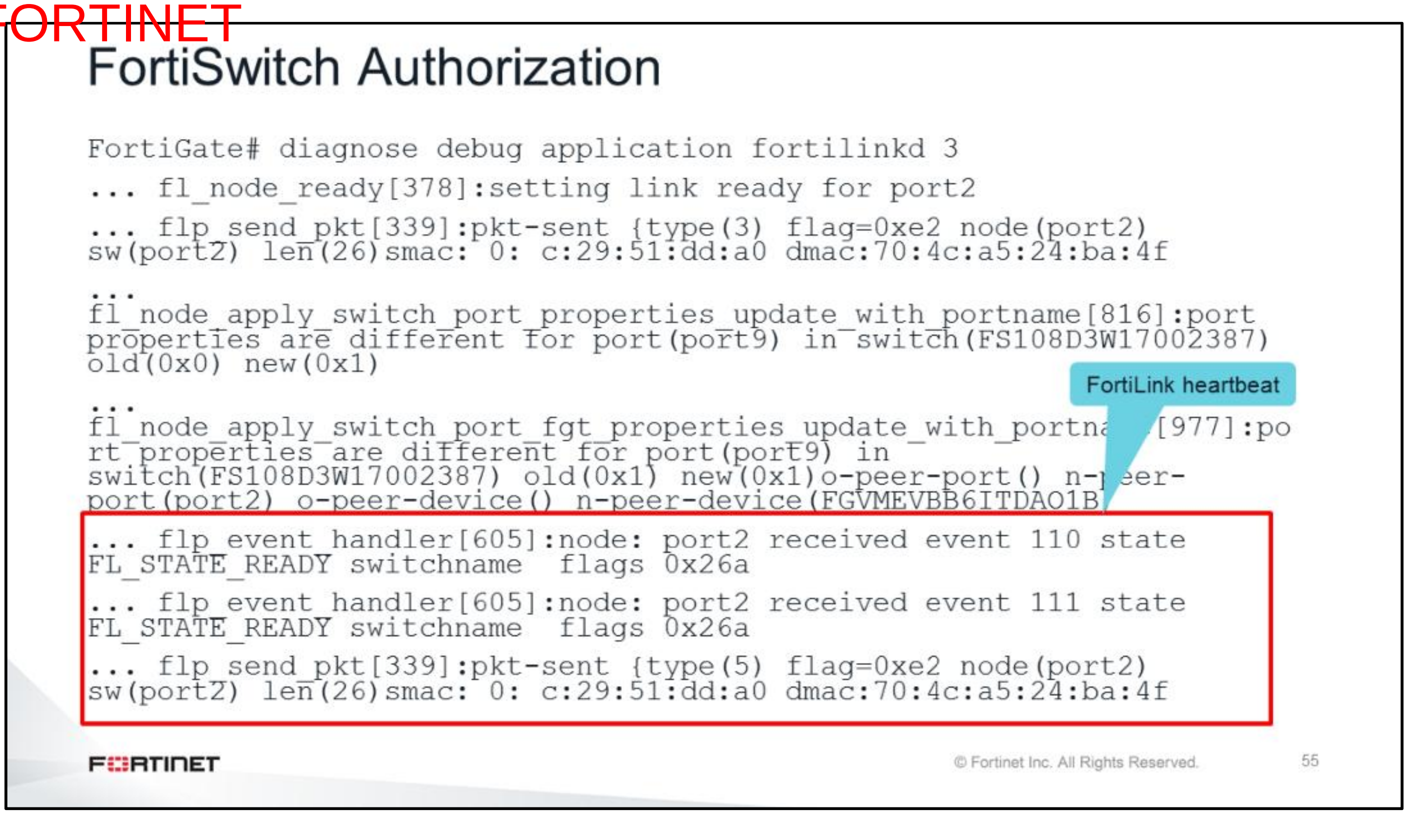
On the FortiSwitch side, there are three processes: `fortilinkd, flcmdd, and cu_swpd`.

There is a real-time debug available for each of these processes, on both FortiGate and FortiSwitch.

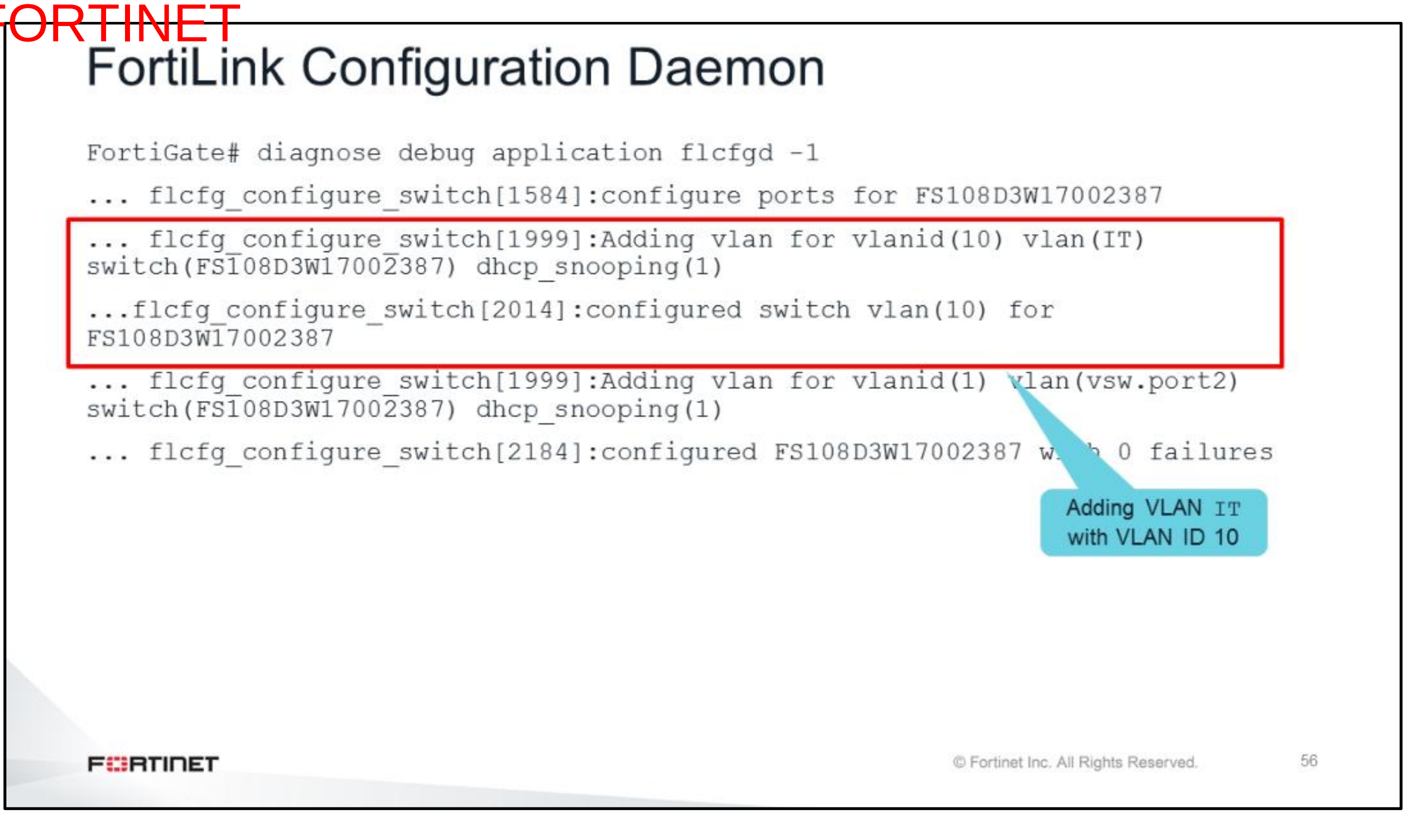


You can use the real-time debug for the `fortilinkd` process for monitoring and troubleshooting the discovery of FortiSwitch devices and the FortiLink heartbeat.

When a new FortiSwitch is discovered, the output shows the FortiSwitch serial number.



After FortiSwitch is authorized, the FortiLink real-time debug shows the heartbeat packets being interchanged between FortiGate and FortiSwitch.



The output of the real-time debug for the `flcfgf` process provides information about configuration changes pushed from FortiGate to FortiSwitch. In the example output shown on this slide, an administrator has created a new VLAN named `IT`, with tag ID 10. The output shows the moment when FortiGate pushed this new VLAN configuration to FortiSwitch.

FortiSwitch Logs

- By default, FortiSwitch exports the logs to FortiGate

```
config switch-controller switch-log
  set status [enable | disable]
  set severity [emergency | alert | critical | error | warning |
      notification | information | debug]
end
```

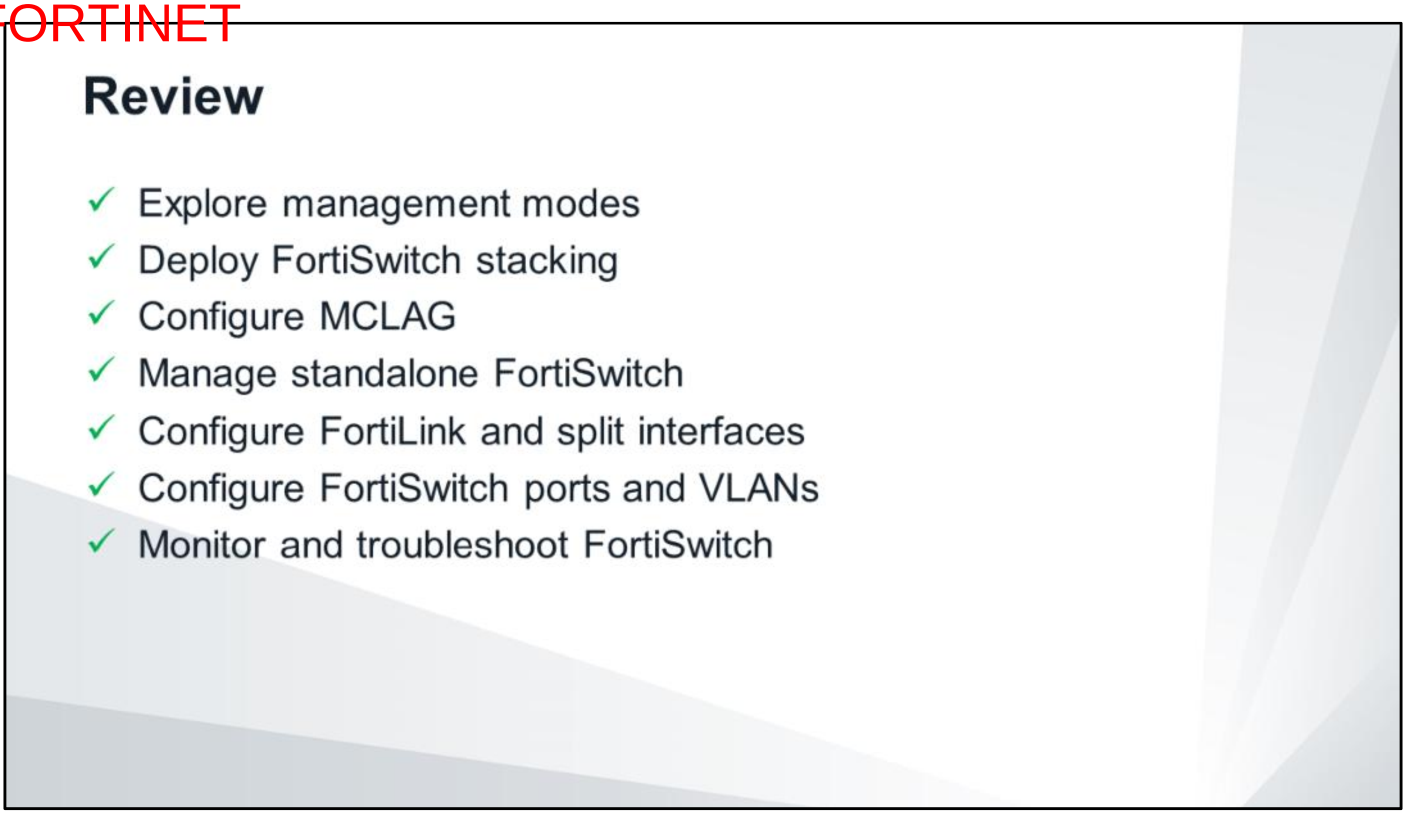
- You can override the global logging settings per FortiSwitch

```
config switch-controller managed-switch
  edit <switch_id>
    config switch-log
      set local-override enable
      set status [enable | disable]
      set severity <severity>
end
```

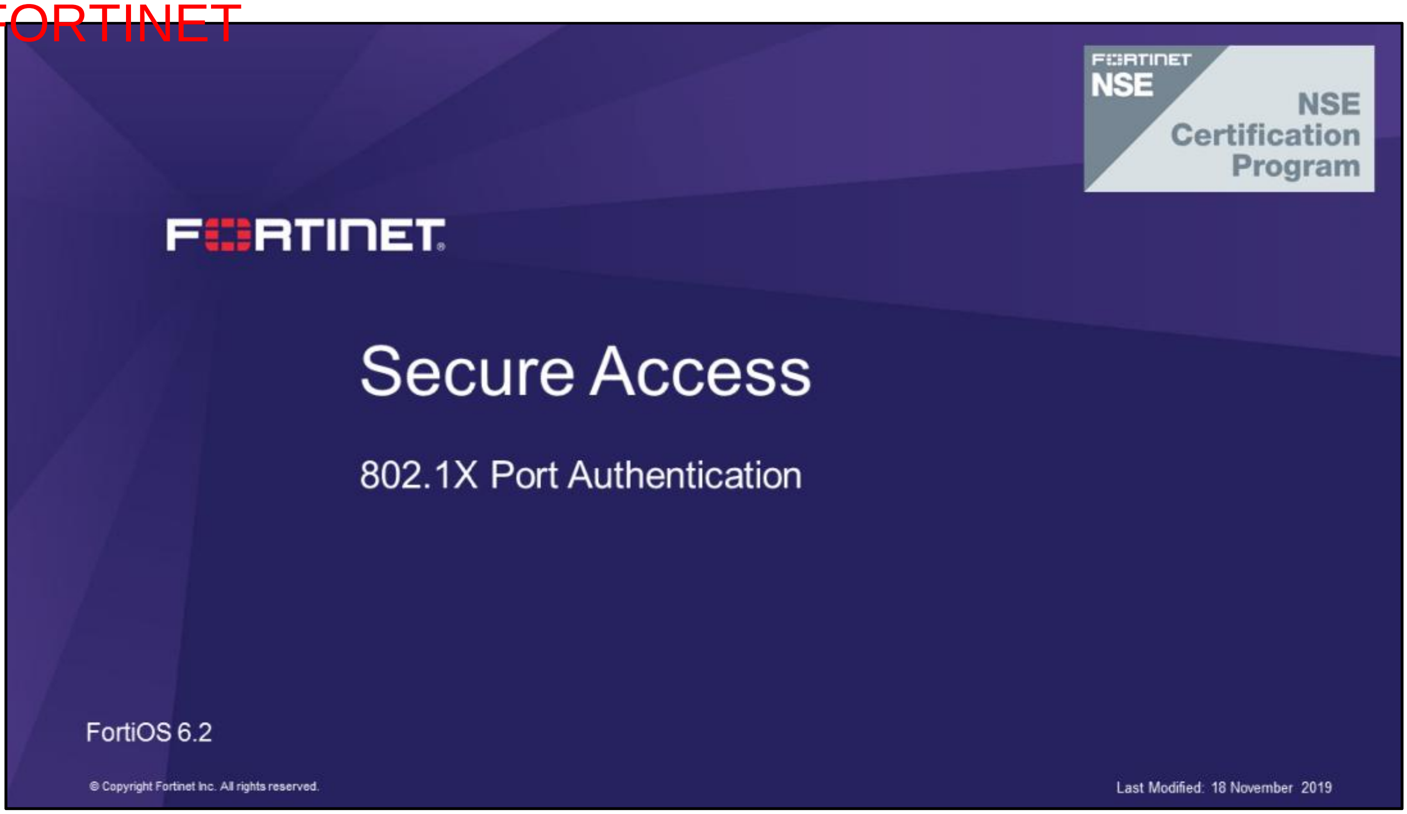
FORTINET

 57

By default, FortiSwitch logs are sent to FortiGate so they can be displayed on the FortiGate GUI. You can set the minimum severity level that generates logs either globally or per FortiSwitch.



By mastering the objectives covered in this lesson, you learned how to deploy, configure, and troubleshoot FortiSwitch.



In this lesson, you will learn how to configure 802.1X port authentication on FortiSwitch and FortiAuthenticator devices.

Objectives

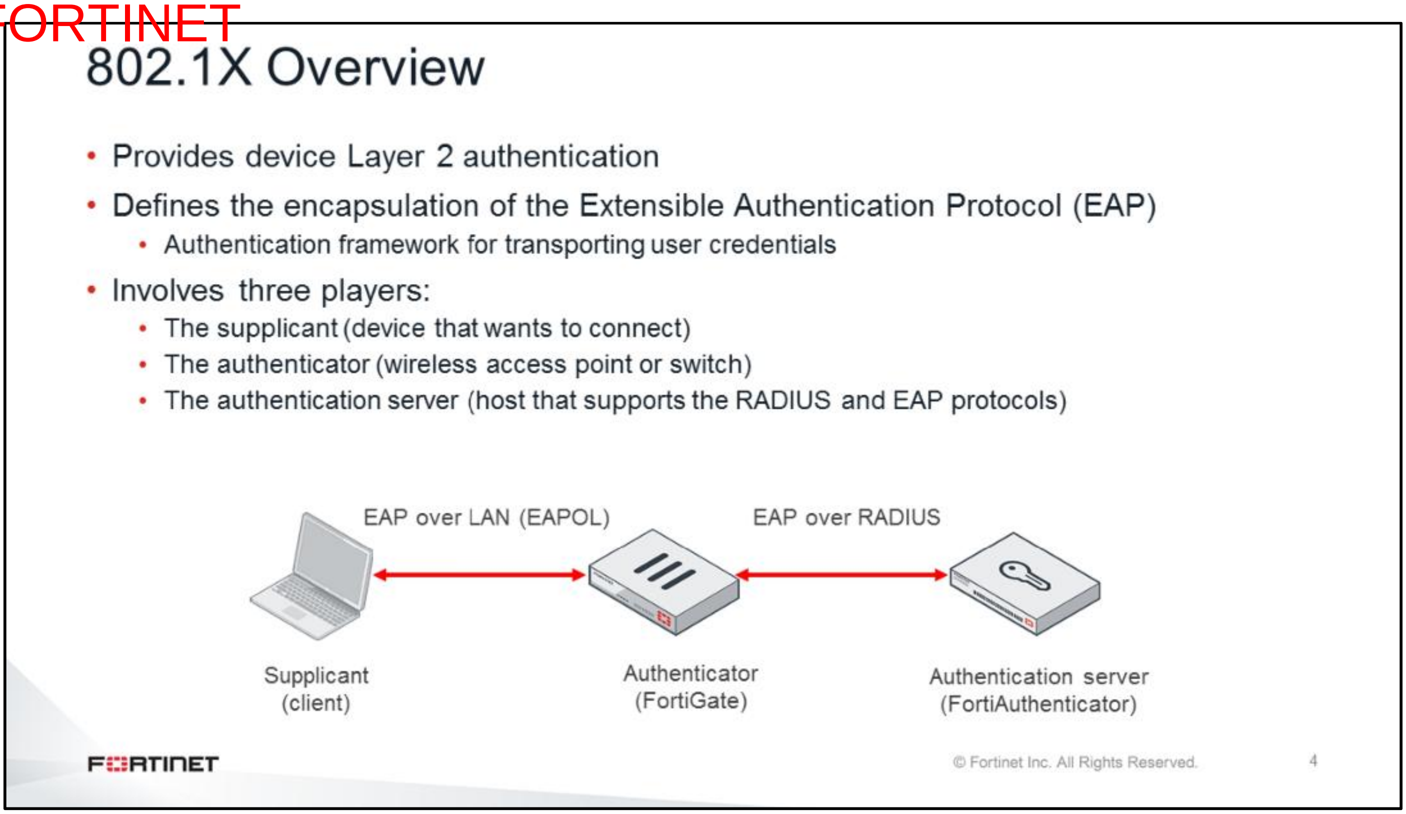
- Configure Layer 2 authentication using 802.1X
- Monitor 802.1X clients
- Configure machine authentication
- Configure MAC address bypass for clients that do not support 802.1X

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

By demonstrating competence in configuring 802.1X, you will be able to use port authentication on FortiSwitch and FortiAuthenticator devices.

802.1x Overview

In this section, you will learn about 802.1X.



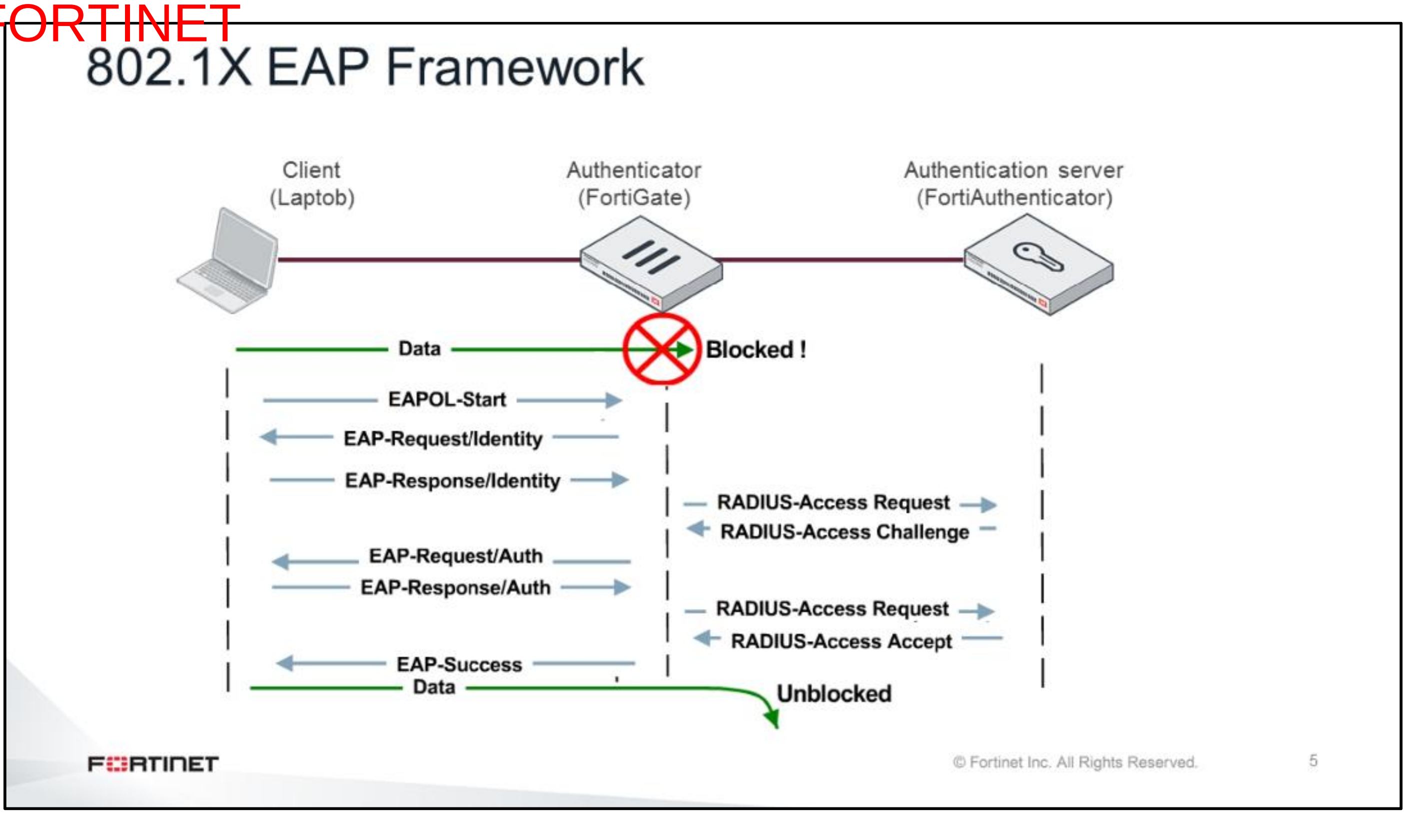
802.1X is a standard that is designed to provide authentication services to network devices that want to join a local wired or wireless network. The 802.1X standard defines an authentication protocol called EAP. It also defines how EAP is encapsulated over the LAN (the EAPOL protocol) and over RADIUS.

802.1X involves the following three parties:

- The client (also known as the supplicant) is the device that wants to join the network
- The authenticator is a network device, such as a wireless access point or switch
- The authentication server is a host that supports the RADIUS and EAP protocols, such as FortiAuthenticator

The client is not allowed to access the Layer 2 network until the client's identity is validated and authorized. Using 802.1X authentication, the client provides credentials to the authenticator, which the authenticator forwards to the authentication server for verification. If the authentication server determines that the credentials are valid, the client device is allowed to access the network.

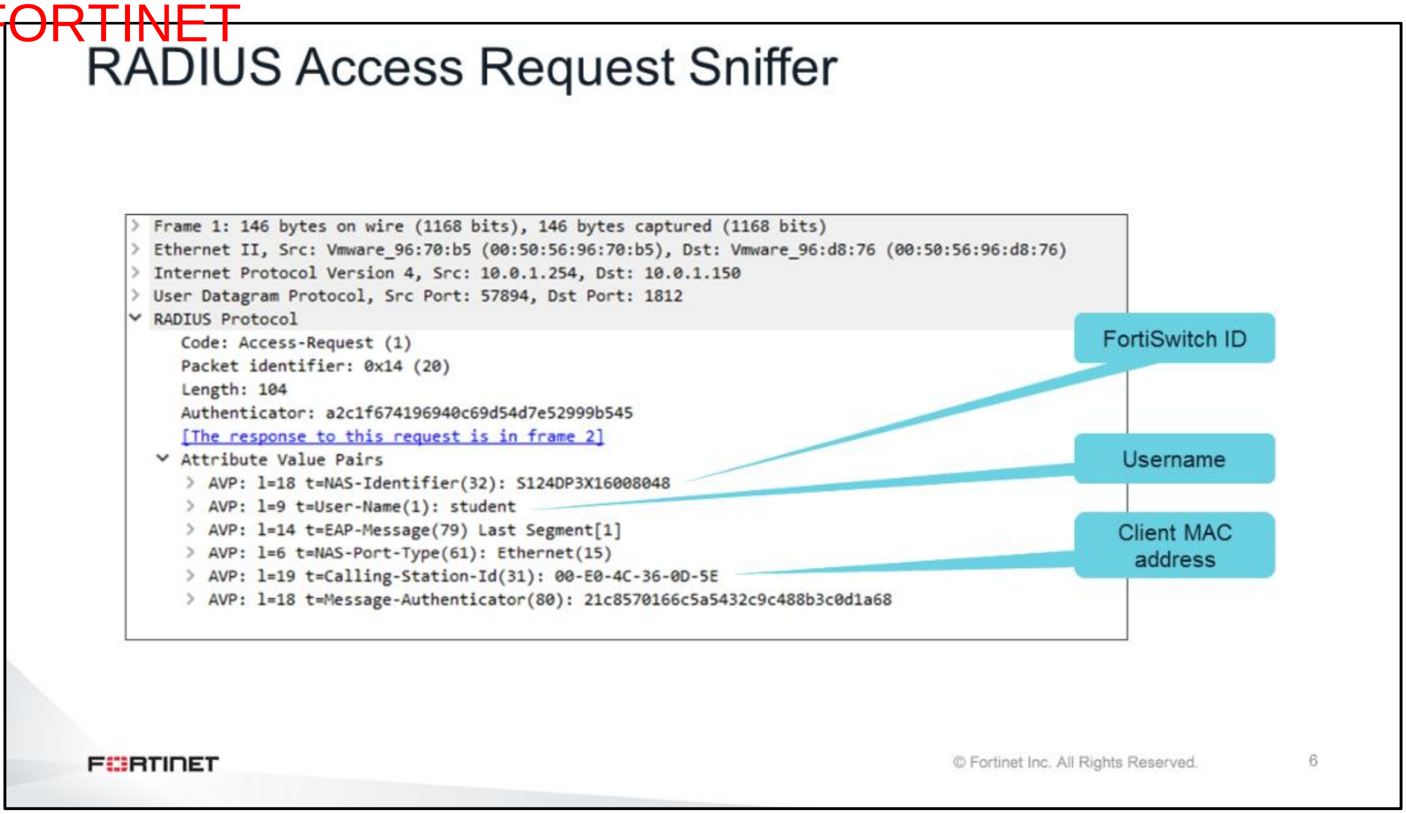
Note that the authenticator does not need to have a certificate or have knowledge of the authentication method (for example, PEAP or TLS). The authentication is tunneled from the client to the authentication server over the RADIUS protocol.



When a supplicant client (laptop) connects to a LAN switch that requires 802.1X authentication, the client credentials are sent to the authenticator (FortiGate), using EAP over LAN (or EAPOL). The authenticator (FortiGate) then forwards the EAP traffic to the authentication server (FortiAuthenticator), which is an EAP over RADIUS server.

If the client tries to send user data before authenticating, the traffic will be blocked by the authenticator. The client must authenticate first, using the following process:

1. The client sends an EAPOL-Start packet to initiate the EAP authentication.
2. The authenticator replies with an EAP-Request/Identity packet to request identification.
3. The client sends its identity (usually the username).
4. The information is forwarded to the RADIUS server in a RADIUS-Access request packet.
5. The RADIUS replies with an Access Challenge packet requesting the password.
6. The authenticator requests the password from the client.
7. The client replies with a Response/Auth packet, which contains the password.
8. The password is forwarded to the RADIUS server, which then replies with an Access-Accept packet to grant the access.
9. The authenticator sends an EAP-Success packet to the client with a confirmation that the credentials are okay.
10. The client can now send the user data.



This packet capture 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.

Native EAP Methods

- EAP-MD5
  - Sends MD5 hash of the user credentials
  - Offers client authentication, but not server authentication
  - Not recommended, and not supported by FortiAuthenticator
- EAP-TLS
  - Uses TLS and X.509 certificates to support client and server authentication
  - One of the most secure EAP methods

FORTINET

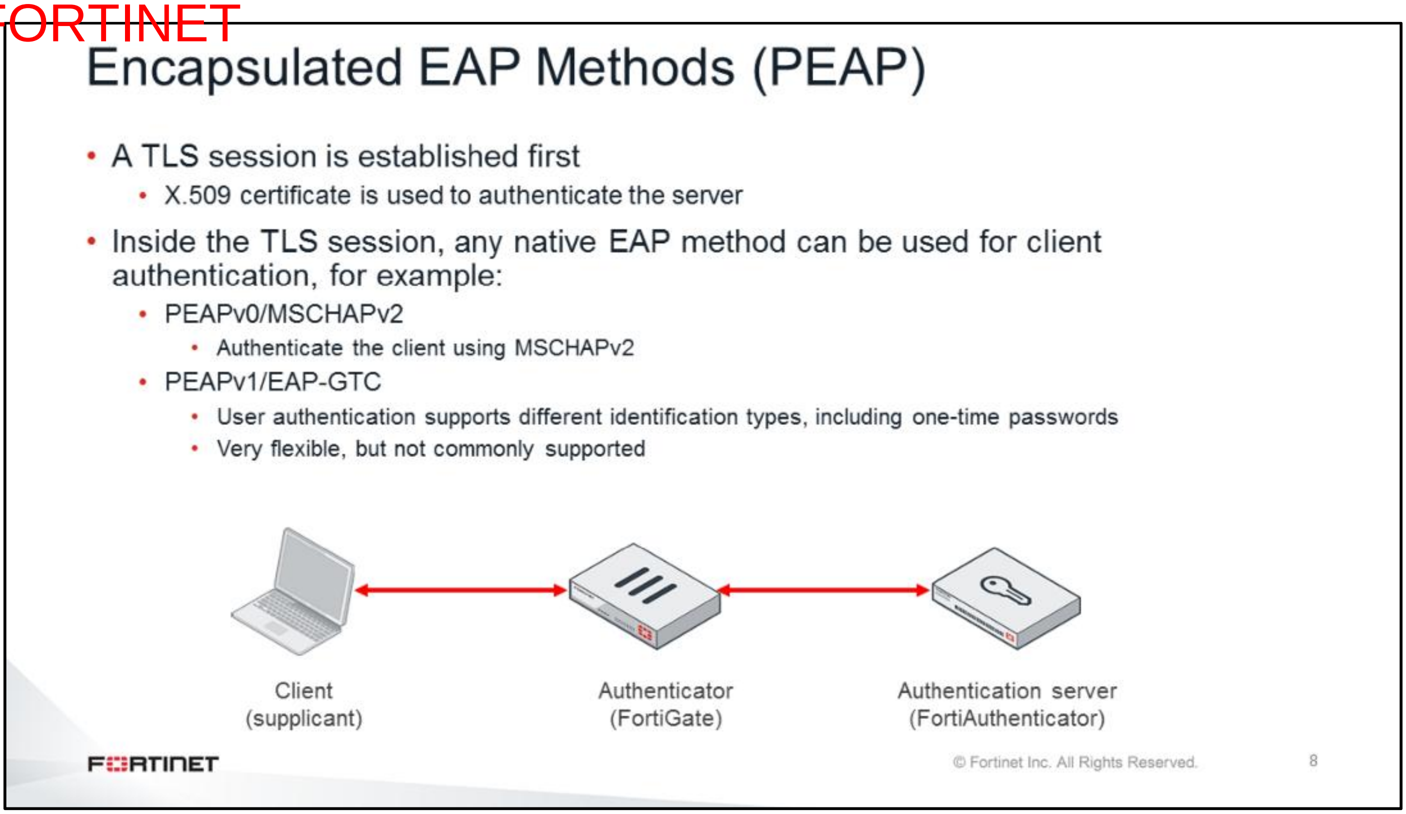
 7

EAP supports multiple methods. There are two types of EAP methods: native and encapsulated.

The two most common native methods are EAP-MD5 and EAP-TLS.

EAP-MD5 sends a hash of the user credentials. It can authenticate clients, but does not offer a mechanism for authenticating the server. This method is not recommended and is not supported by FortiAuthenticator.

EAP-TLS uses TLS and digital certificates to authenticate both the client and the server. It is one of the most secure EAP methods.



With encapsulated EAP methods, a TLS session is established first. At this point, a digital certificate is used to authenticate the server. Encapsulated inside the TLS session, any native EAP method is used for client authentication. Two examples of encapsulated EAP methods are:

- PEAPv0/MSCHAPv2: Authenticates the client using MSCHAPv2
- PEAPv1/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.

Encapsulated EAP Methods (EAP-TLS)

- Standard, original authentication protocol
- Client and server require a certificate
- RADIUS authentication server support
  - By default, EAP-TLS on FortiSwitch is enabled
  - If not supported, EAP pass-through needs to be disabled

```
config switch-controller security-policy 802-1X
    edit <policy_name>
        set eap-passthru disable
    end
end
```

 9

EAP-TLS It is one of the common native methods that uses TLS and digital certificates on both clients and servers to authenticate.

If the RADIUS authentication server does not support EAP-TLS, the FortiSwitch must disable the default setting to use EAP-TLS, by setting EAP pass-through to disable.

Encapsulated EAP Methods (EAP-TTLS)

- A TLS session is established first
  - X.509 certificate is used to authenticate the server
- Inside the TLS session, attribute-value pairs (AVPs) are interchanged
- These AVPs authenticate the client using:
  - A native EAP method
  - A legacy authentication protocol, such as PAP or CHAP

FORTINET

 10

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

EAP Methods Supported by FortiAuthenticator

	EAP-TLS	TTLS	PEAP	EAP-GTC
Protocol	TLS session that validates server and client certificates	Establish a TLS session, and exchange attribute-value pairs	Establish a TLS session, and run MS-CHAPv2	Establish a TLS session
Server certificate	Required	Required	Required	Required
Client certificate	Required	Optional	Optional	Optional
Server authentication	X.509 certificate	X.509 certificate	X.509 certificate	X.509 certificate
Client authentication	X.509 certificate	Various identification types over attribute-value pairs	MS-CHAPv2	Various identification types over GTC

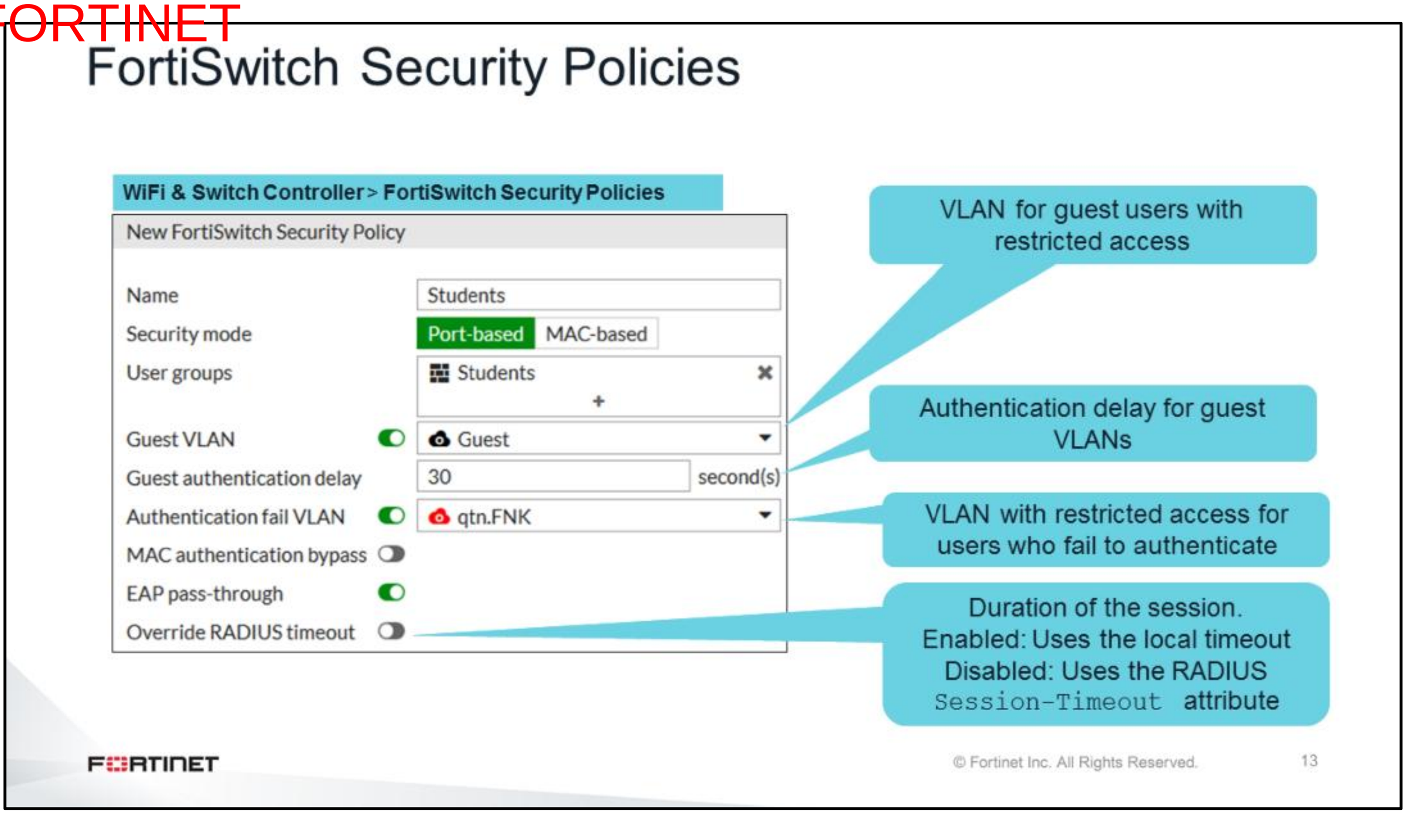
FORTINET

 11

FortiAuthenticator supports EAP-TLS, TTLS, PEAP, and EAP-GTC. In all of these four methods, a TLS session is established first, and a digital certificate is used for authenticating the server. How clients are authenticated varies from one method to another.

802.1x Authentication on FortiSwitch

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



To configure 802.1X port authentication on FortiSwitch, you must create a security policy. The security policy includes the user groups that are authorized.

Optionally, you can configure two VLANs for:

- Guest access: VLAN assigned to users who did not try authenticating using 802.1X
- Authentication failures: VLAN assigned to users who failed their 802.1X authentication attempt

If you need to override the session timeout in the RADIUS attribute received, you can enable the option in the security policy profile and use the local timeout.

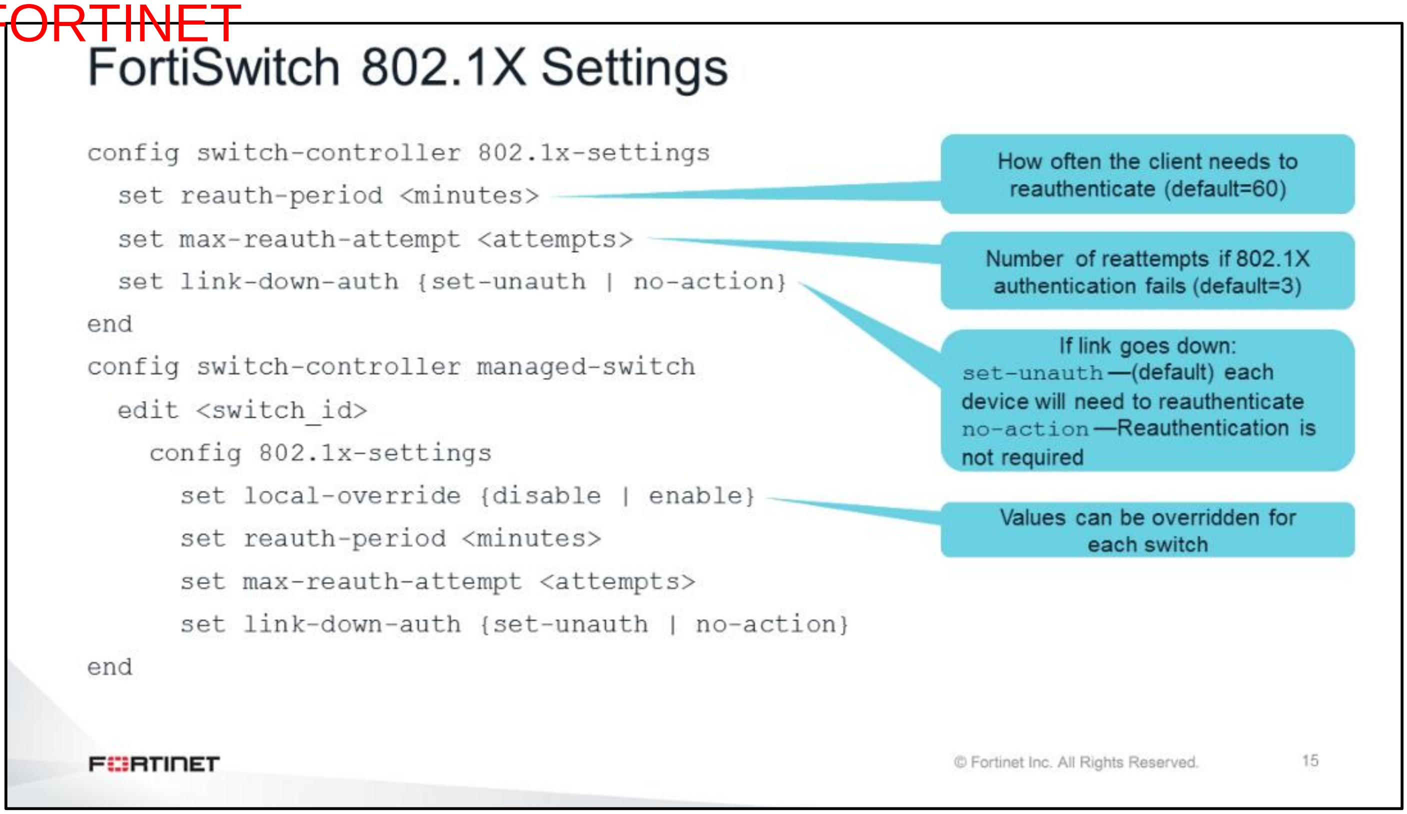
Assigning a Security Policy to a Port

WiFi & Switch Controller> FortiSwitch Ports

Port	Trunk	Enabled Features	Native VLAN	Allowed VLANs	Security Policy
S224EPTF18001736 28					
port1		Edge Port IGMP Snooping Spanning Tree Protocol	vsw.port4	All	802.1X Students
port3		Edge Port IGMP Snooping Spanning Tree Protocol	vsw.port4		

 14

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.



There are three 802.1X settings that can be configured either globally or for each switch. You can configure these settings on the CLI:

- `reauth-period`: Defines how often clients need to reauthenticate
- `max-reauth-attempt`: Defines how many times a FortiSwitch reattempts the authentication if it fails the first time
- `link-down-auth`: Defines if FortiSwitch requests a device to authenticate again after the link status of a port goes down and then comes back up.

Monitoring 802.1X Clients

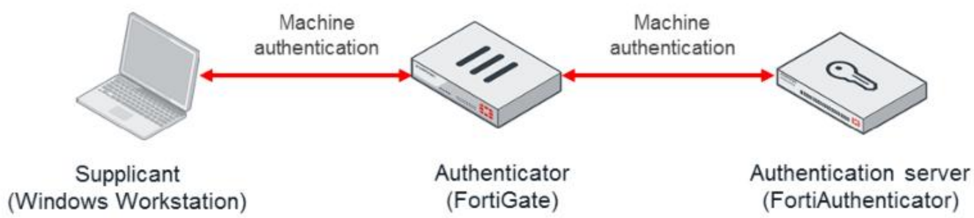
```
FortiSwitch# diagnose switch-controller switch-info 802-1X-status
Managed Switch : S124DP3X16008048 0

port2 : Mode: port-based (mac-by-pass enable)
  Link: Link up
  Port State: authorized (  )
  Dynamic Authorized Vlan : 0
  EAP pass-through mode : Enable
  Quarantine VLAN (4093) detection : Enable
  Native Vlan : 100
  Allowed Vlan list: 100
  Untagged Vlan list:
  Guest VLAN :
  Auth-Fail Vlan :

  Sessions info:
  00:e0:4c:36:0d:5e Type=802.1x,PEAP,state=AUTHENTICATED,etime=9,eap_cnt=11 params:reAuth= 3600
```

 16

This `diagnose` command displays 802.1X information about each port. The `Port State` indicates if the device has been authorized or not. This command also shows the device MAC address, quarantine VLAN, native VLAN, allowed VLANs, guest VLAN, and authentication-fail VLAN.

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

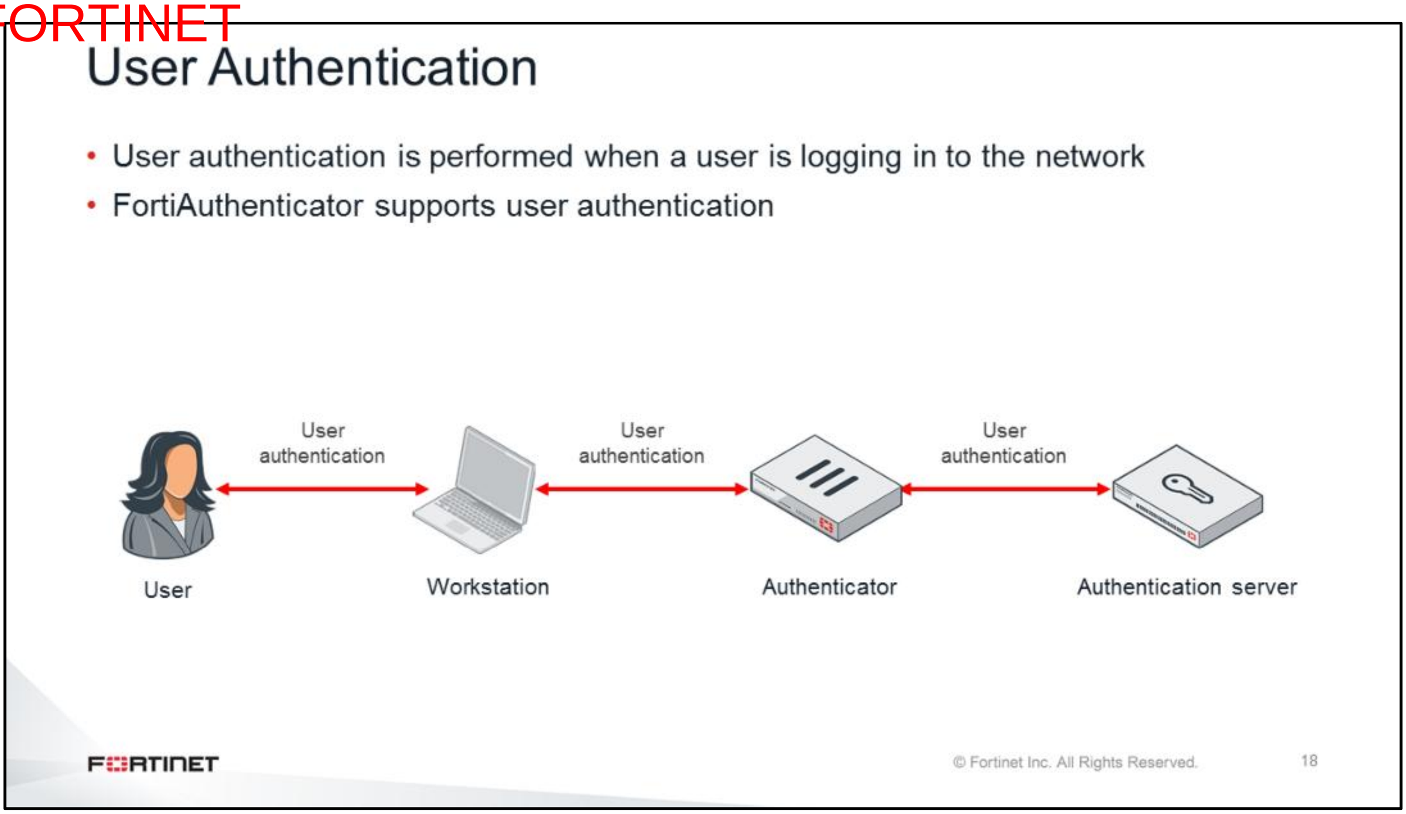


 17

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. 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.

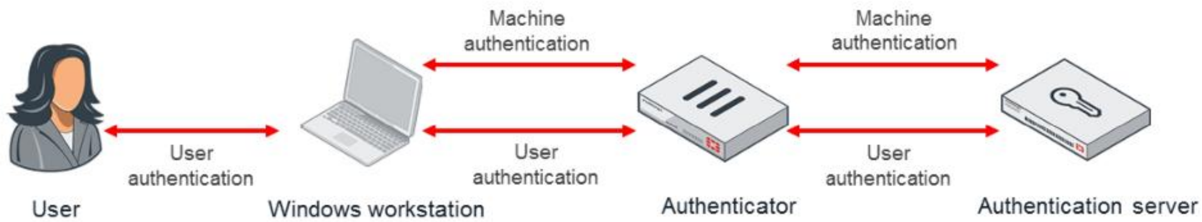


User authentication is performed by a user when that user is logging in to the network.

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

Machine and User Authentication

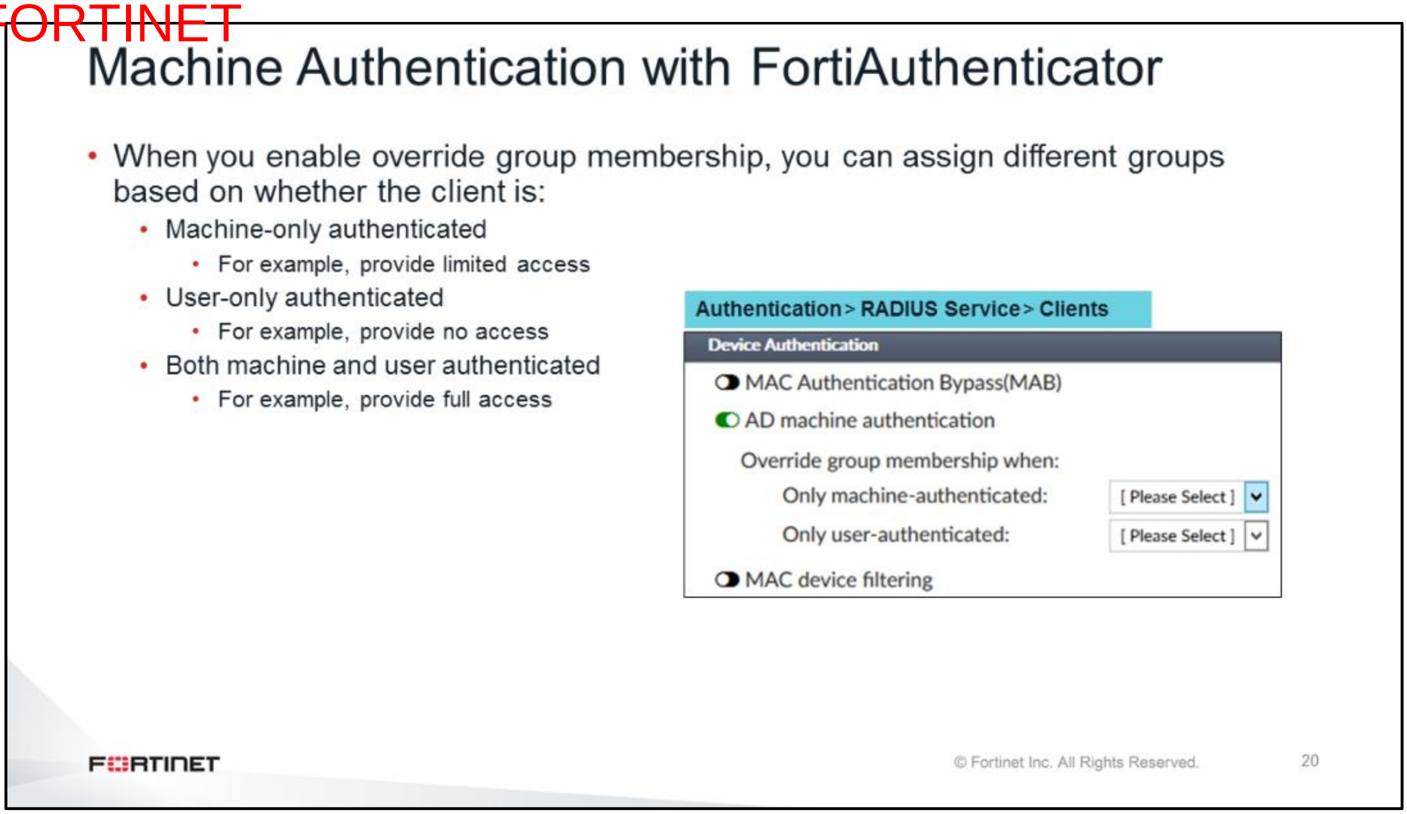
- FortiAuthenticator also supports the use of both machine and user authentication
  - You can limit access to the network based on machine credentials
  - User authentication can occur after machine authentication
  - You can grant further access to the network based on user credentials



19

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

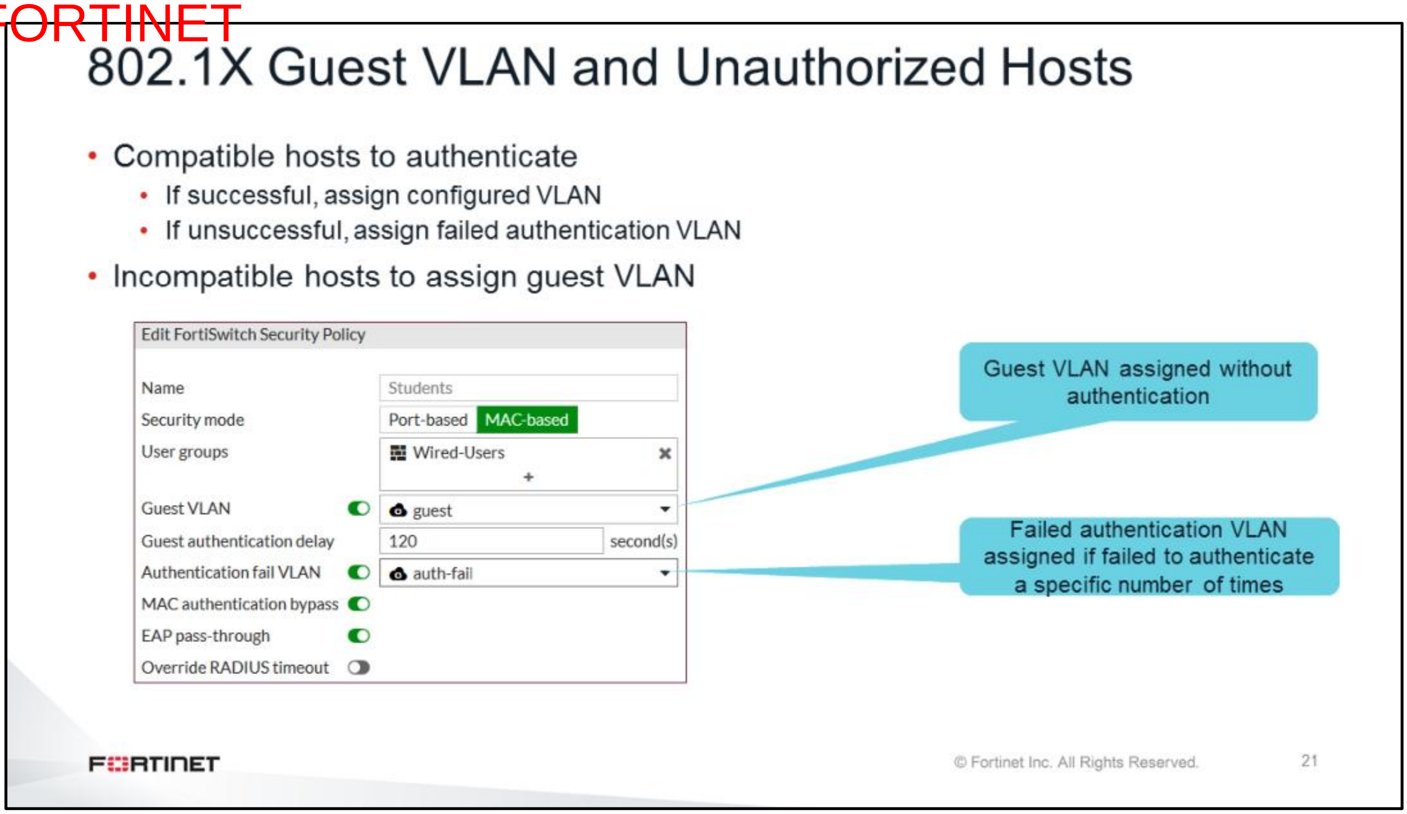
For example, you can provide limited network access to clients (for example, only Active Directory servers) that have done machine authentication, but have not done user authentication yet. After user authentication is successful, you can then grant further access to the network, based on user credentials. 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).



On FortiAuthenticator, you enable AD machine authentication by clicking **Authentication** > **RADIUS Service** > **Clients**. Once you enable AD machine authentication, you can override the user group for clients that have done either machine-only or user-only authentication.

The following are examples of enabling AD machine authentication cases:

- Devices that do only machine authentication can be placed in a group that is given permission to access only a limited number of resources
- Devices that do only user authentication can be placed in a group that is given permission to access only a limited number of resources rather than the normal group for that user
- Devices that do both machine and user authentication would place the user in their normal group



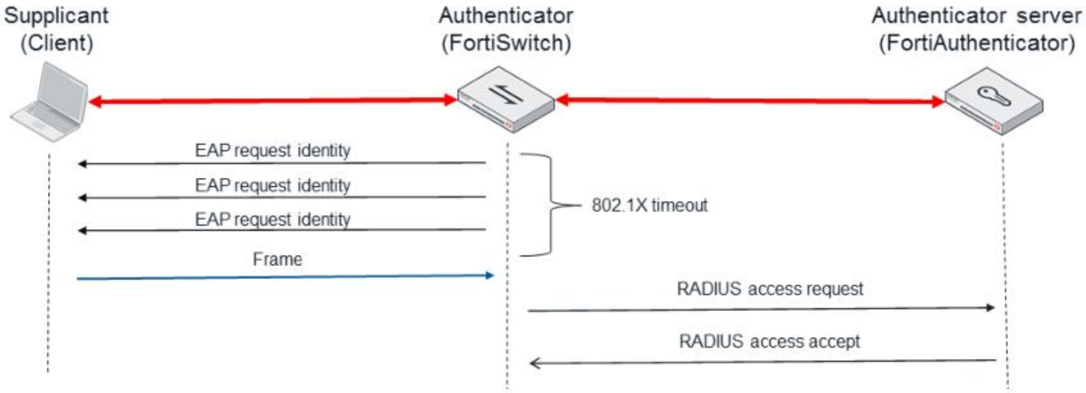
Create a guest VLAN and a failed authorization VLAN to dynamically assign them to hosts when they attempt to access the network.

Unauthenticated hosts will be assigned the guest VLAN. Hosts that fail to authenticate (for example, compatible host with incorrect credentials), will be assigned the failed authentication VLAN.

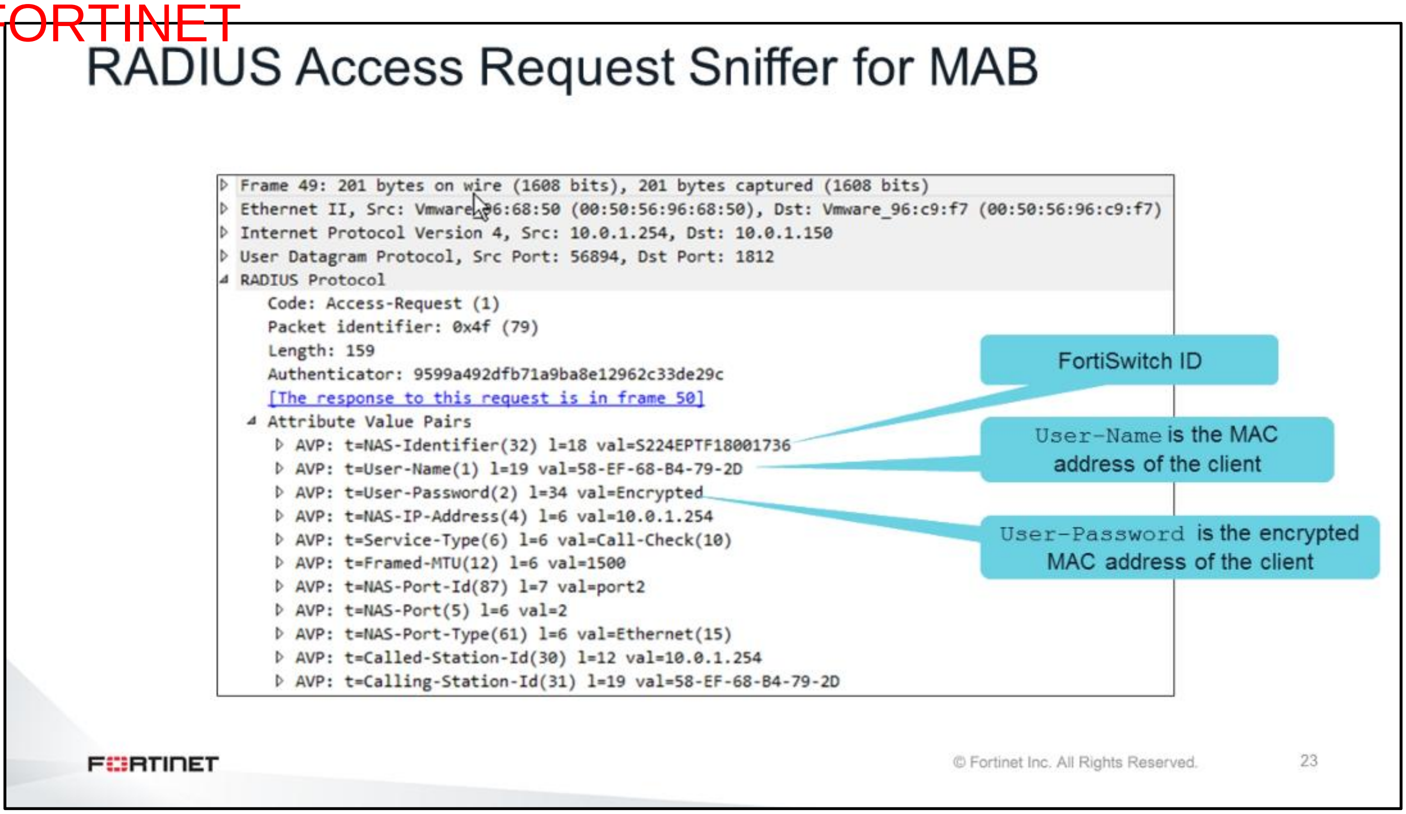
Each VLAN may provide DHCP service to allocate IP addresses to hosts.

MAC Address Bypass (MAB)

- FortiSwitch conducts the authentication for devices that do not support 802.1X
  - Supplicant MAC address is used for the username and password

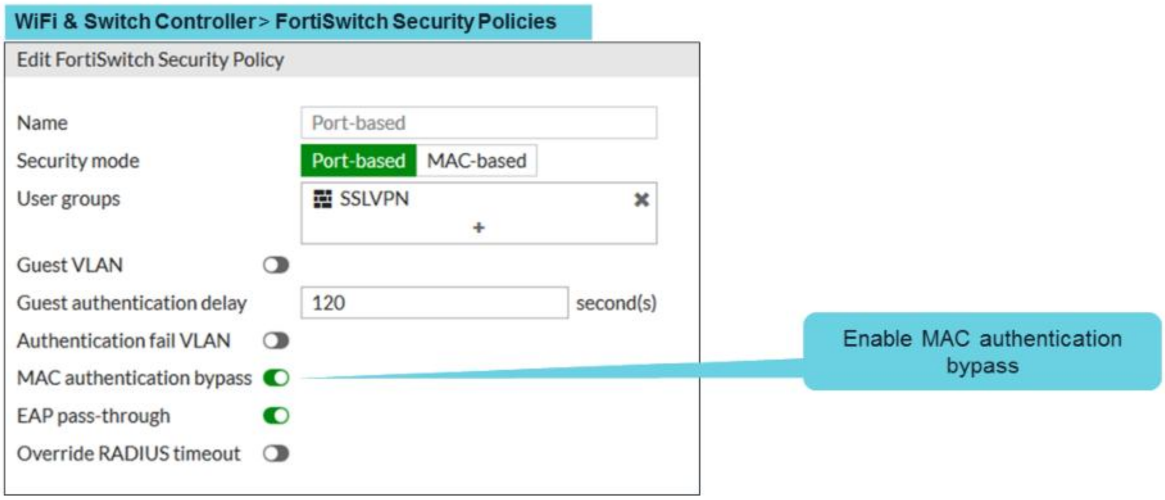


MAC address bypass allows access to devices that do not support 802.1X authentication. When MAB is enabled in the security policy, and the 802.1X authentication times out, FortiSwitch conducts the authentication on behalf of the connected device. For this purpose, FortiSwitch sends a RADIUS access request, using the MAC address of the device as the username, and the encrypted MAC address of the device as the password. FortiAuthenticator contains 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.



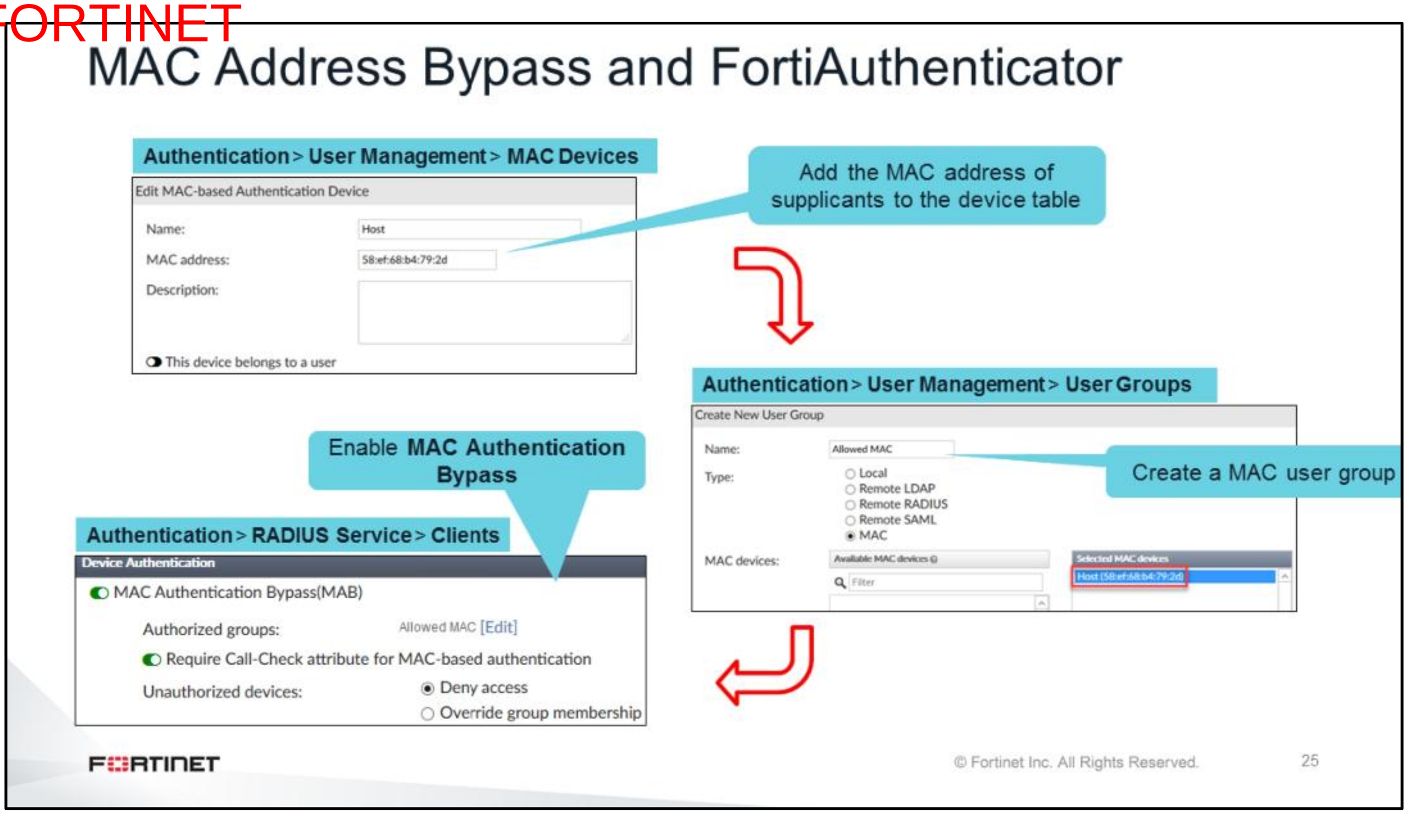
This packet capture shows the RADIUS access request when MAB is used. It includes the FortiSwitch ID, client MAC address (as the username), encrypted client MAC address (as the password), and the client MAC address (as the `Calling-Station-ID`).

MAC Address Bypass and FortiSwitch



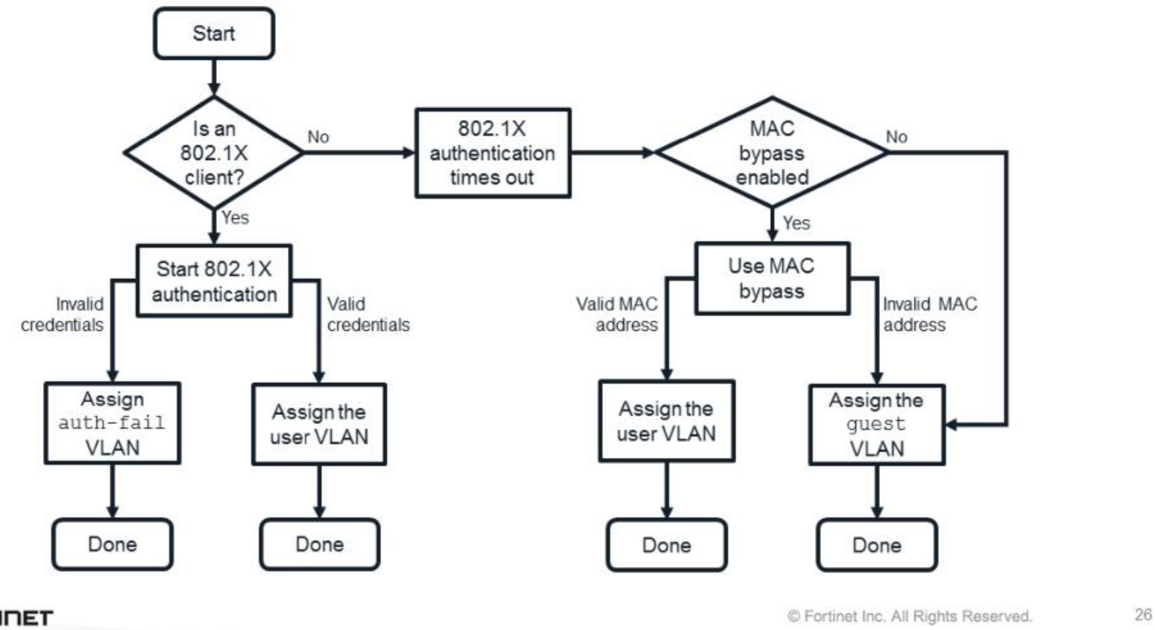
 24

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



In FortiAuthenticator, once MAC-based authentication is enabled, you must create a list of allowed MAC addresses on the **MAC Devices** page. After that, you must create a MAC address user group and assign it to the RADIUS client.

802.1X Port-Based Authentication



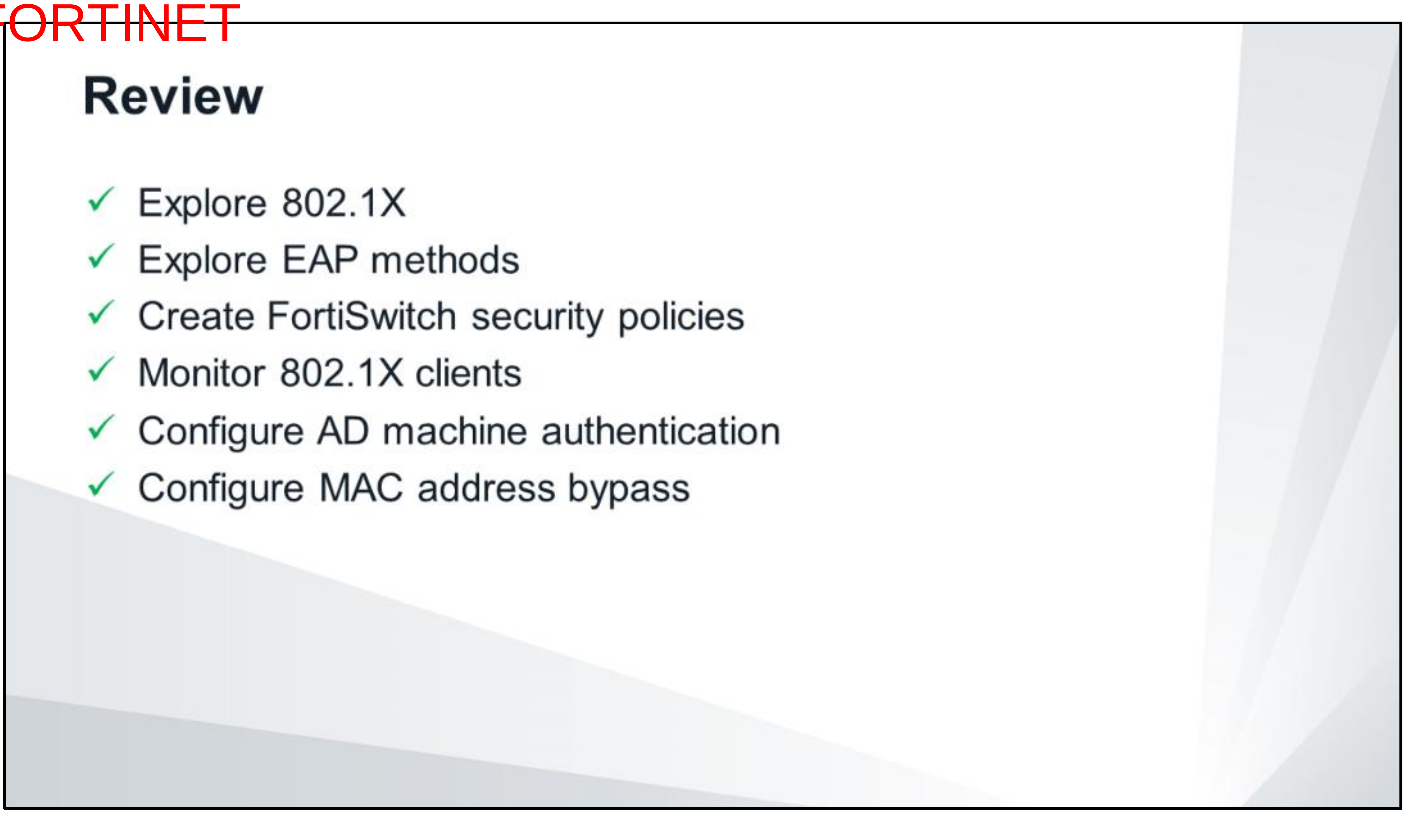
This slide shows the authentication process when 802.1X is combined with MAC address bypass. When a physical device is connected to an 802.1X port, FortiSwitch waits for the EAPOL-Start packet.

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 and the source MAC address of the device is checked, with the following results:

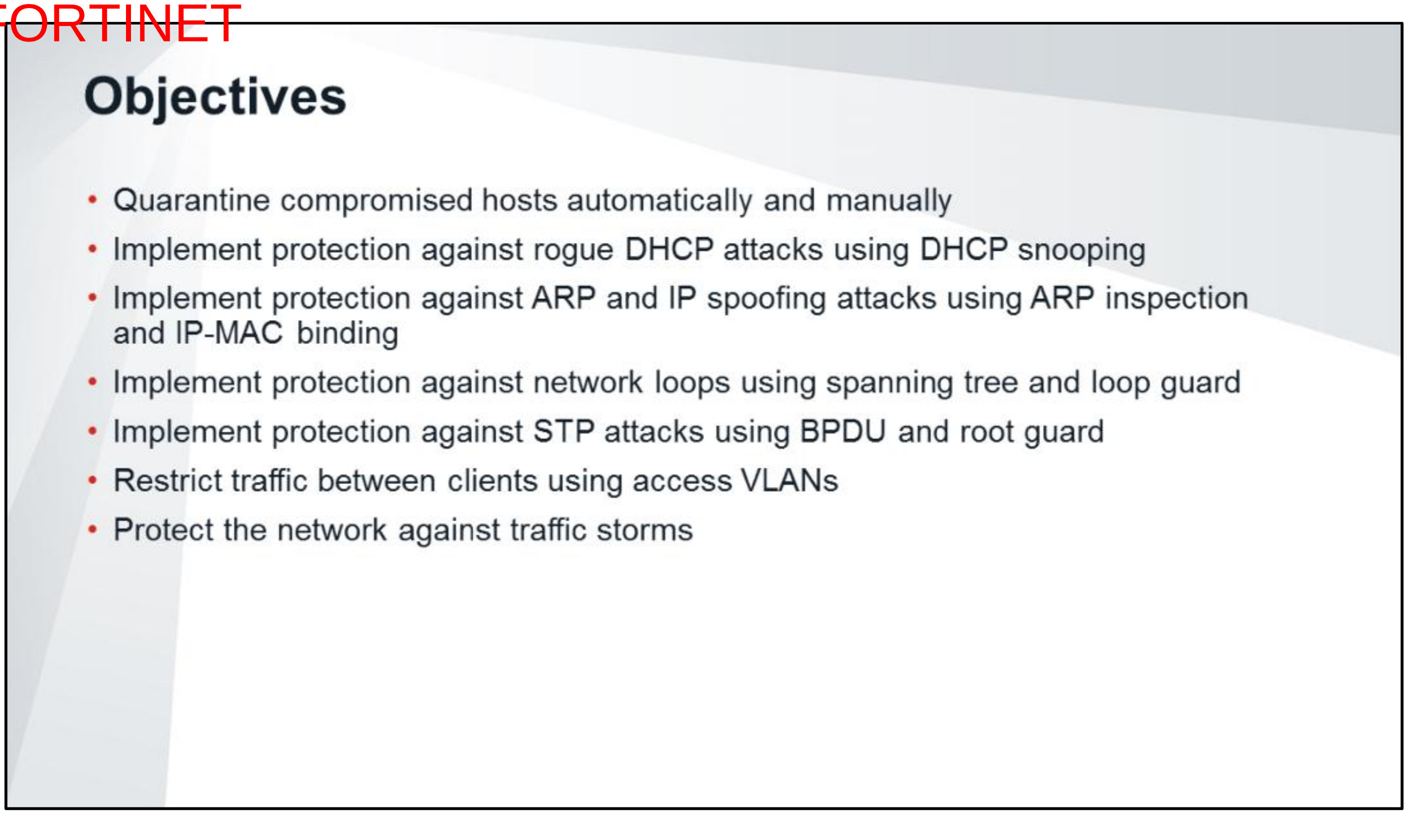
- If MAC bypass is disabled, the traffic is assigned to the guest VLAN (or blocked, if **Guest VLAN** is disabled).
- If MAC bypass is enabled, but the source MAC address is not in the MAB table, the traffic is assigned to the guest VLAN (or blocked, if **Guest VLAN** is disabled).
- If MAC bypass is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



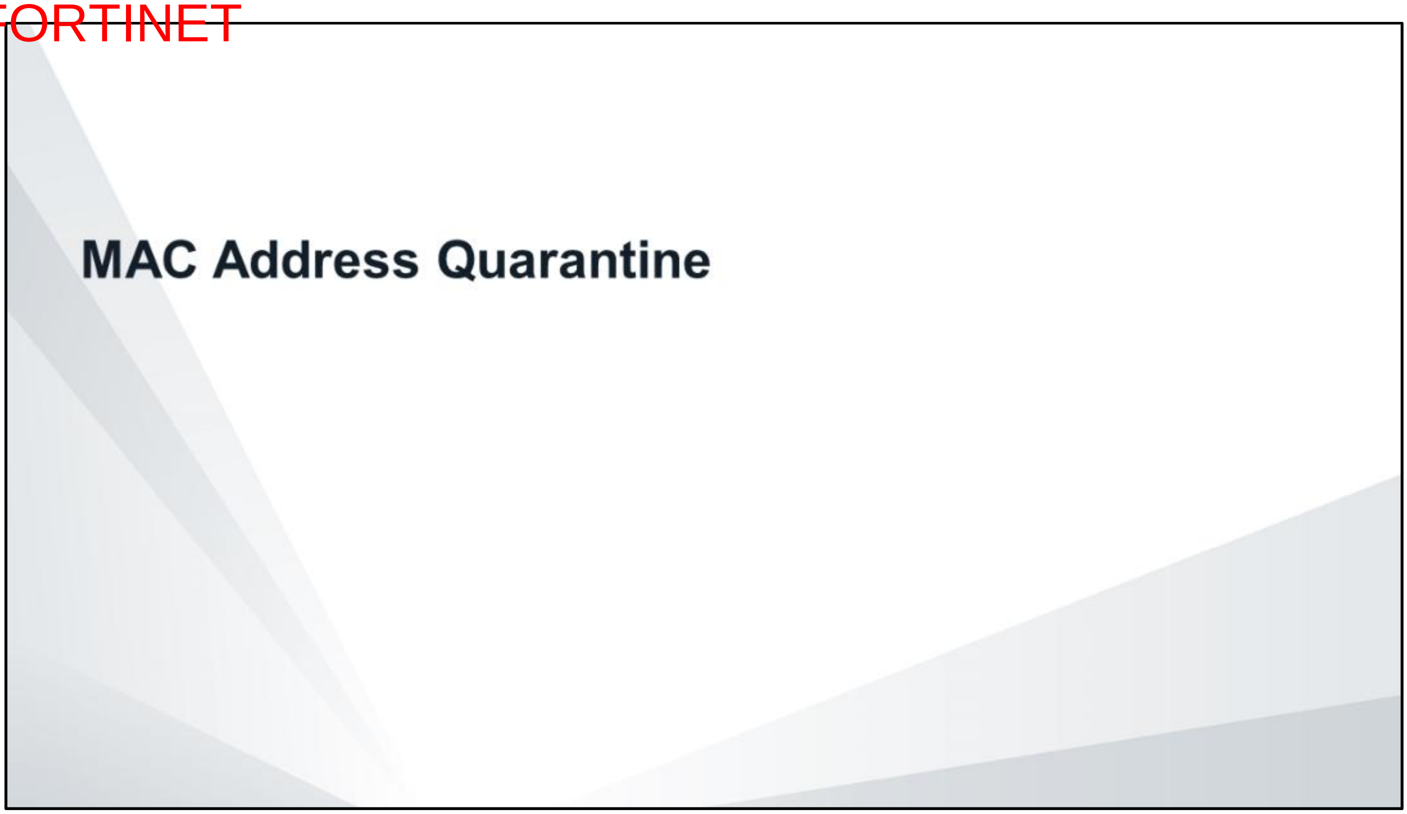
This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to configure 802.1X port authentication on FortiSwitch and FortiAuthenticator devices.

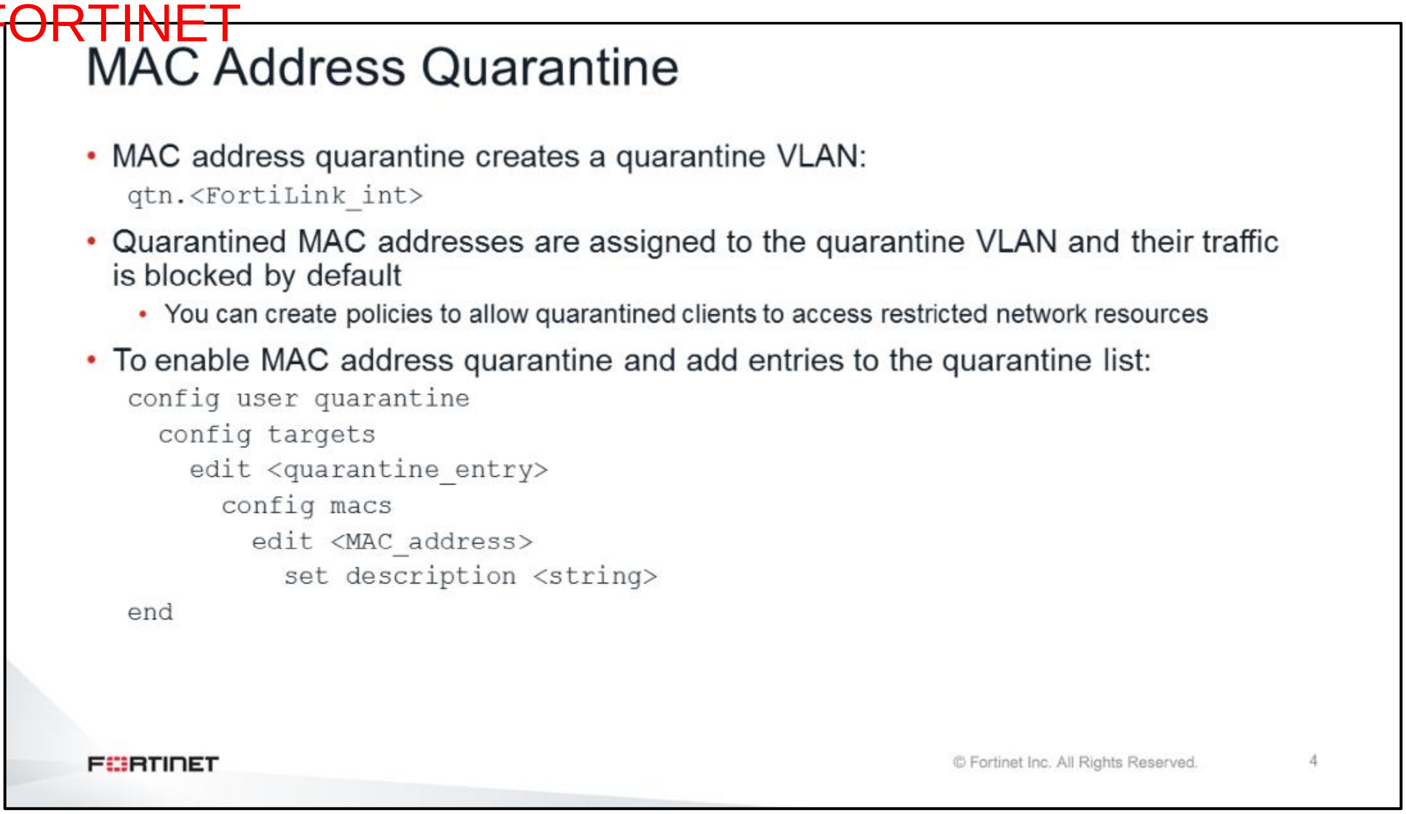
In this lesson, you will learn how to configure some additional FortiSwitch features to secure Layer 2.



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



In this section, you will learn how to quarantine MAC addresses on FortiSwitch.



You can enable MAC address quarantine on FortiSwitch using the `config switch-controller quarantine` command.

When you enable MAC address quarantine, FortiOS automatically adds a quarantine VLAN to the virtual domain. FortiOS assigns all quarantined devices to the quarantine VLAN. By default, the implicit deny-all policy blocks all traffic from the quarantine VLAN. However, you can add explicit policies to allow quarantined devices to access some network resources, such as servers with Windows and other software updates.

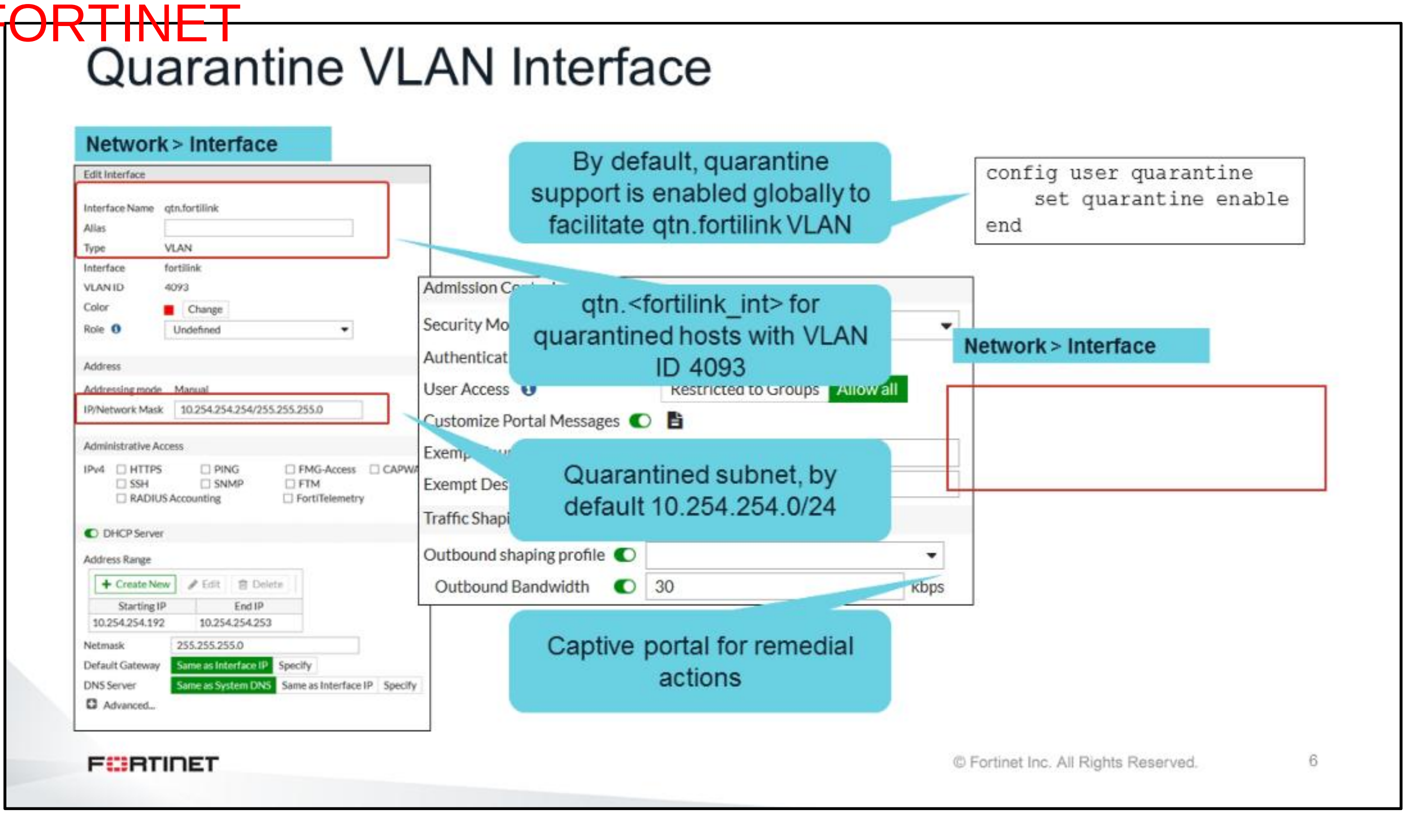
Host Quarantine With Security Fabric

- Uses Automation Stitch
- IP Ban L3 traffic
- Uses Layer Isolation
  - Move MAC address to quarantine VLAN
  - Captive Portal for remedial actions
- Uses malicious traffic to avoid spread of attacks from infected hosts
- Uses Security Fabric
- Threat Detection Services
  - Indicators of Compromise Services
  - FortiAnalyzer License

FORTINET

 5

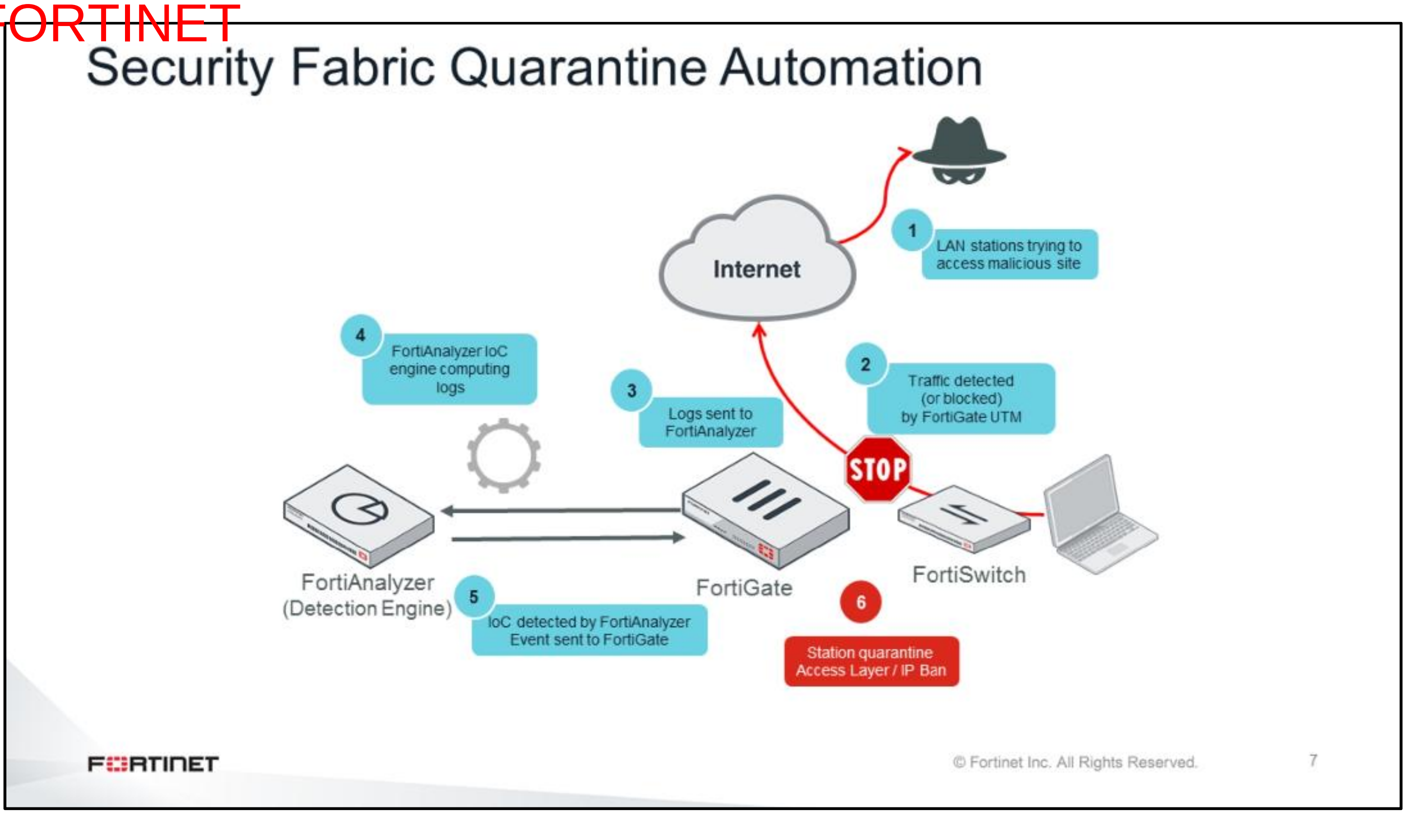
When a FortiGate is a member of a Security Fabric group, the Security Fabric an quarantine hosts automatically using Security Fabric automation stitches. If you are using IP ban and access layer isolation, then place the host into a quarantine subnet, which is created by default when you create a FortiLink interface.



By default, the quarantine VLAN gets created during the FortiLink interface creation process as long as the global setting under the command `config user quarantine` is enabled on the CLI.

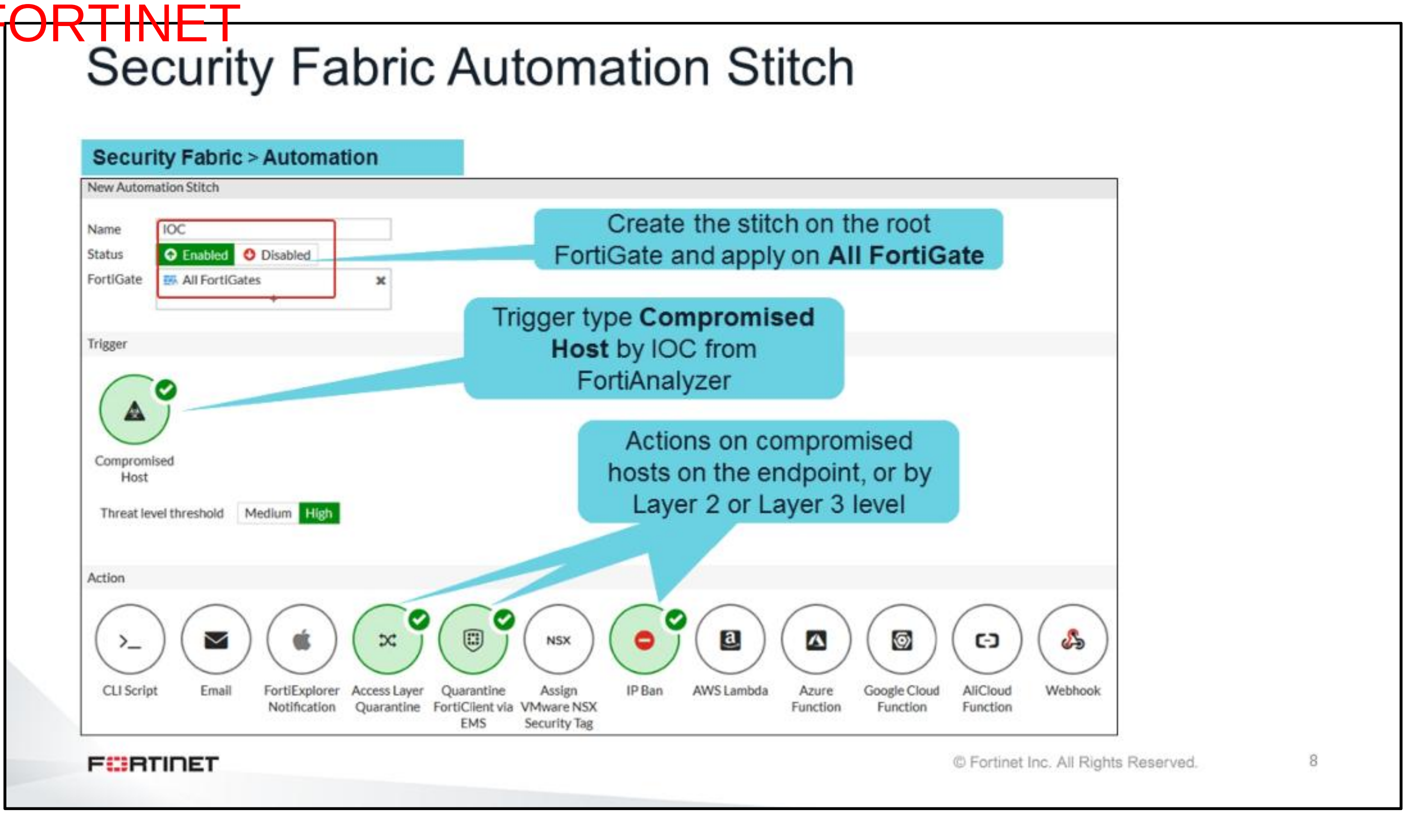
The interface VLAN of ID 4093 is configured with the default IP subnet of 10.254.254.0/24, and the DHCP server is enabled to assign IP addresses to quarantined hosts. By default, this VLAN is part of the allowed VLANs on a managed FortiSwitch.

Part of the role of the quarantining hosts is to challenge connectivity with the captive portal, which can be customized to present messaging appropriate to the organization.



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 hosts can be strengthened with Indicators of compromise (IoC) services on FortiAnalyzer. This slide shows the process of IoC and quarantine automation blocking and isolating stations that are compromised:

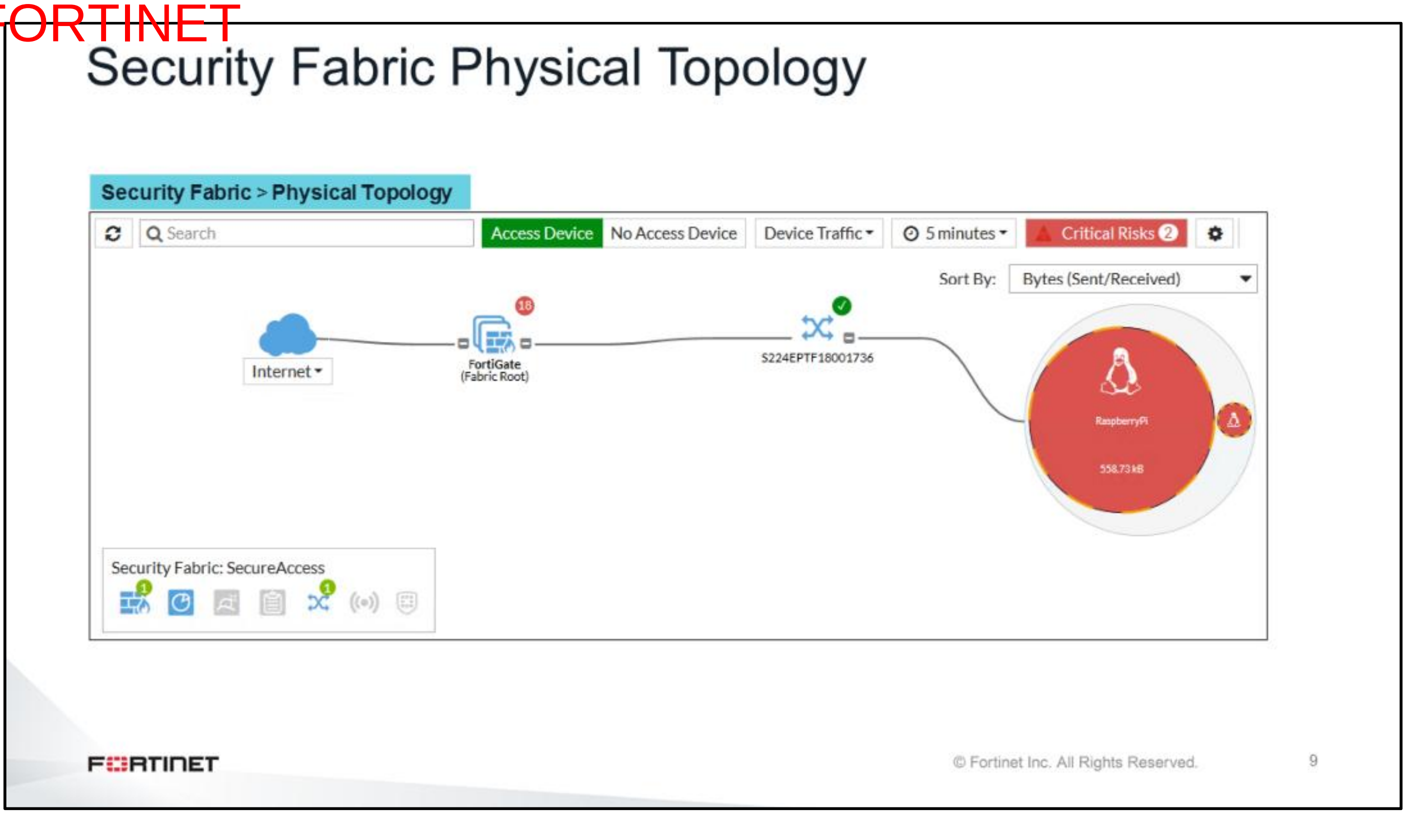
1. A rogue station attempts to access content that is a security risk, such as malicious websites.
2. FortiGate blocks access to the site as per the firewall policy defined with the web filter profile.
3. A log record is sent to FortiAnalyzer regarding the violation committed.
4. FortiAnalyzer then processes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



Compromised hosts are identified by FortiAnalyzer using Threat Detection Services. IoC verdicts get sent to the root FortiGate of the Security Fabric group in order provide the required information in case there is an Automation Stitch configured for compromised hosts.

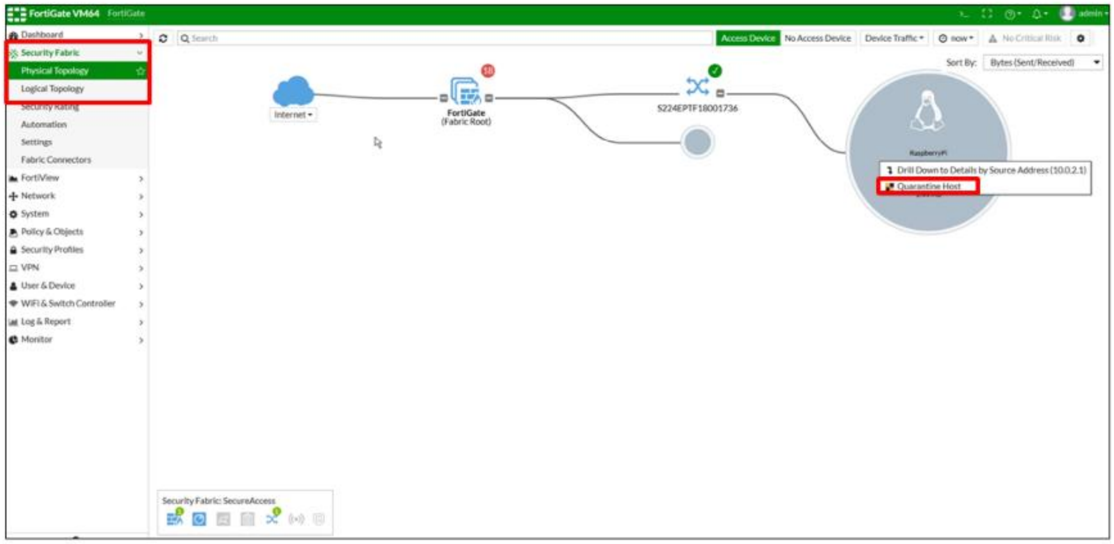
You can create the automation stitch only on the root FortiGate and select which of the Security Fabric FortiGate devices to apply the stitch when triggered.

The trigger required to specify the actions available to handle this risk in the Layer 2 quarantine uses the access layer quarantine action, or Layer 3 of the TCP/IP stack, to block the host machine from using its IP address.



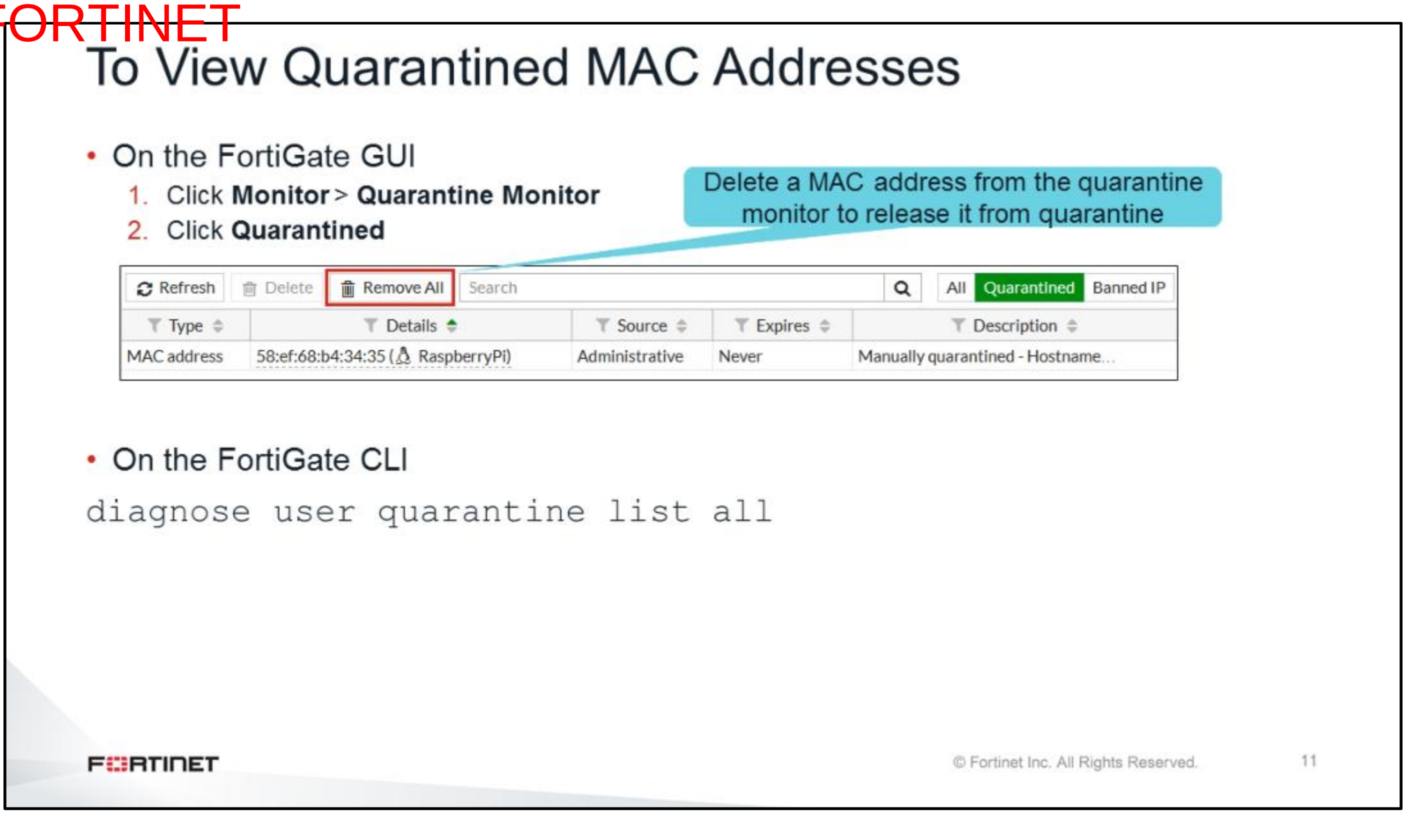
You can view compromised hosts that are quarantined within Security Fabric Physical and Logical Topologies. Quarantined hosts are displayed with a compromised label and quarantine mark on the border of the compromised host.

Quarantine a MAC Address Manually



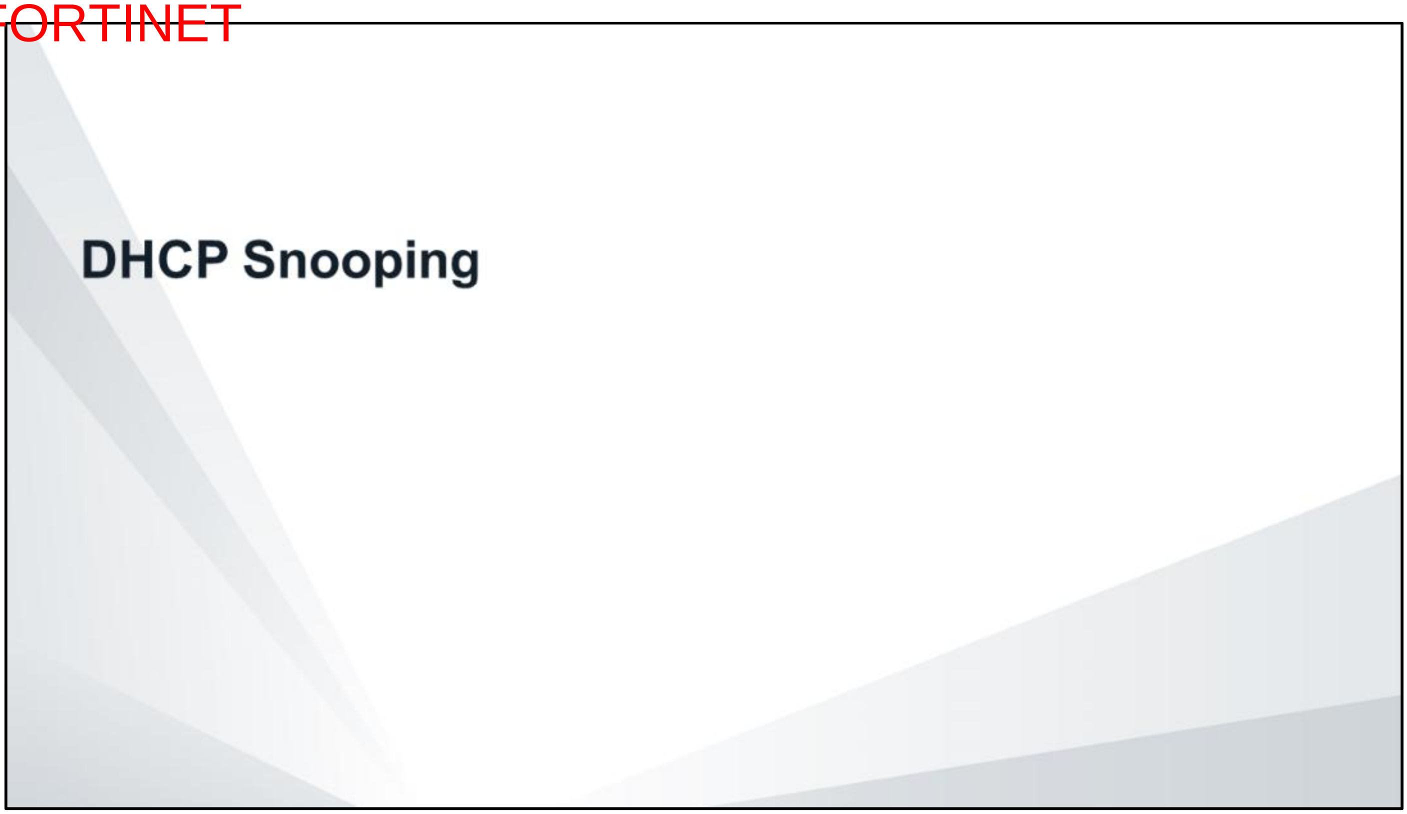
  10

Along with Security Fabric Automation, you can add any device manually to the quarantine list within the physical and logical topologies.

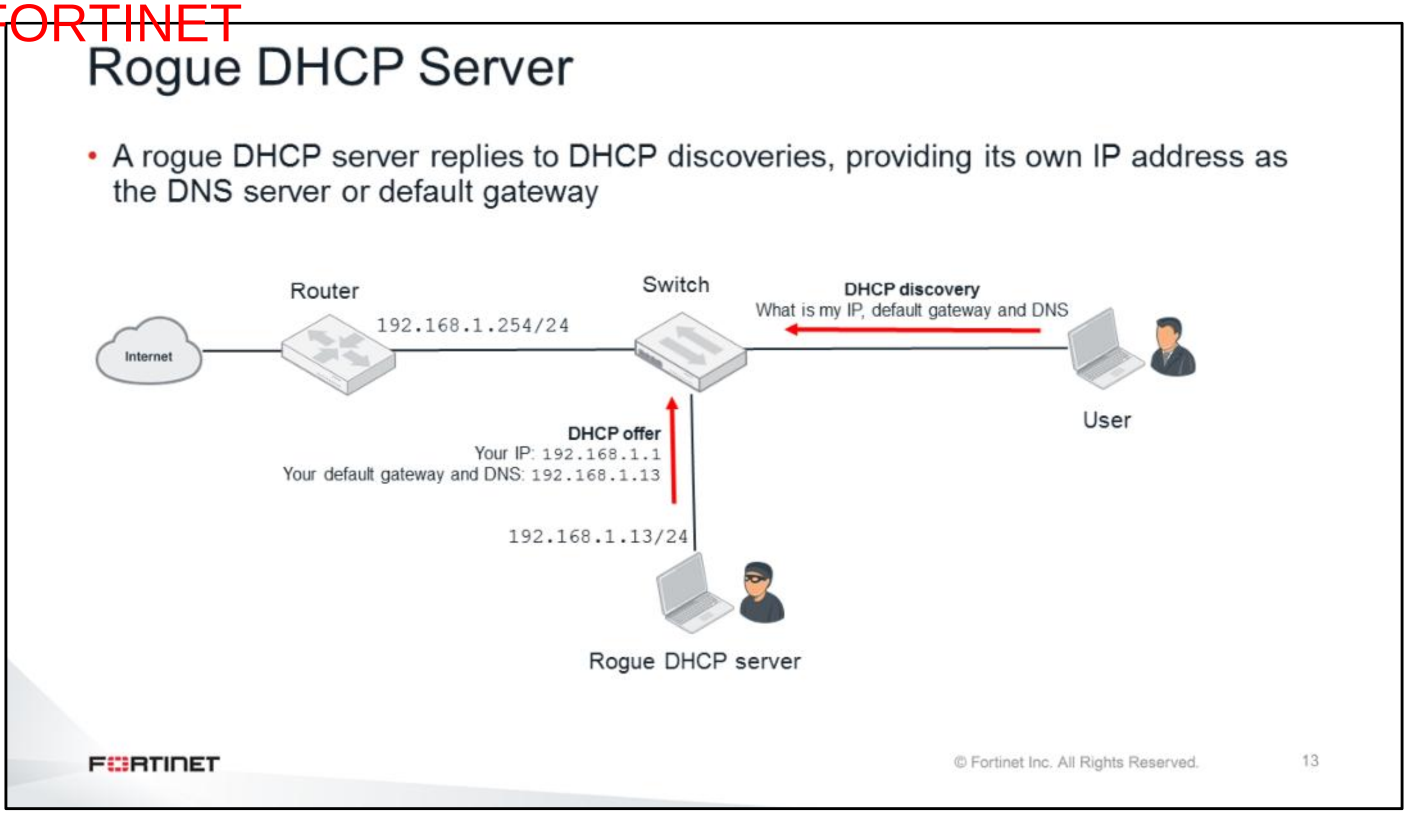


There are two ways to check the list of MAC addresses that have been quarantined:

- Through the GUI under **Monitor** > **Quarantine Monitor**
- Through the CLI with the command `diagnose user quarantine list all`

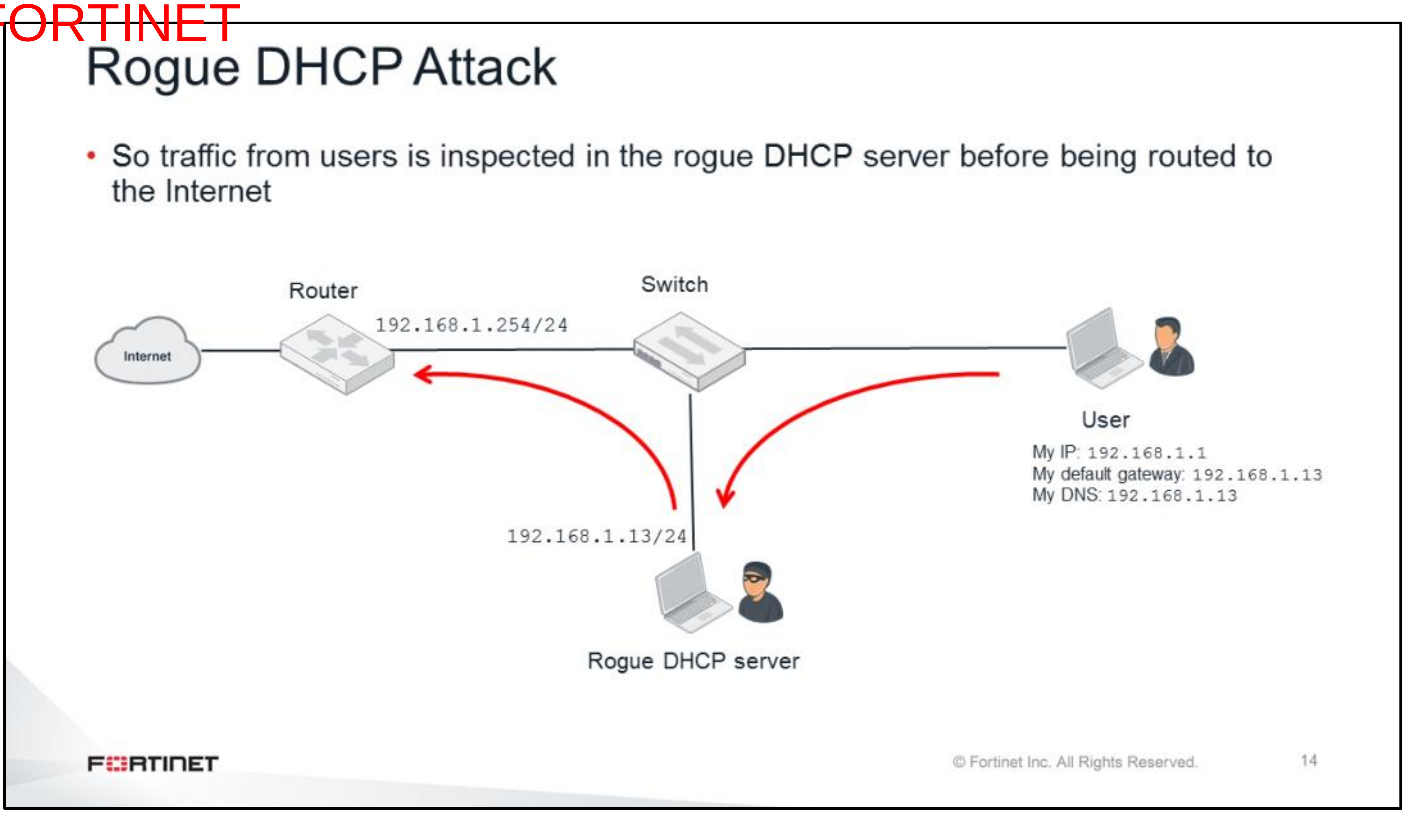


In this section, you will learn how to configure DHCP inspection.



One of the objectives of DHCP inspection is to protect your network against rogue DHCP servers.

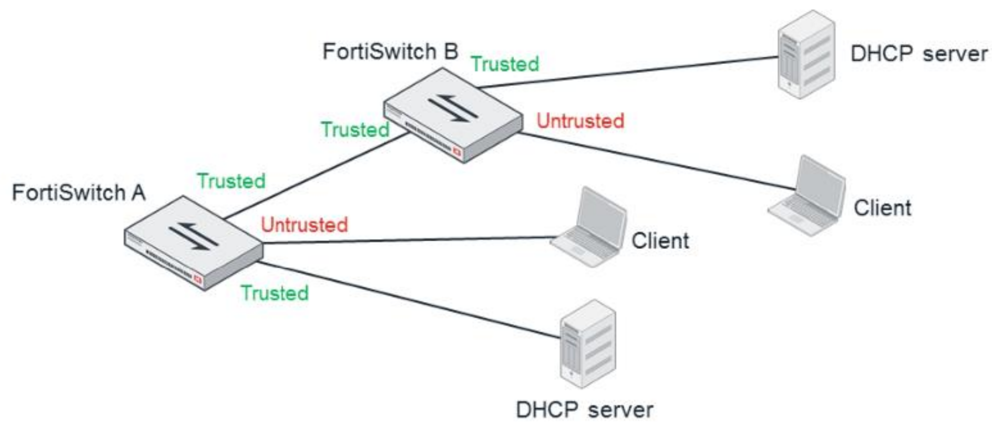
Attackers install rogue DHCP servers in your network with the purpose of replying to DHCP discoveries. The rogue DHCP server assigns to DHCP clients its own IP address as the DNS server and default gateway.



After the rogue DHCP server assigns the malicious default gateway and DNS, attackers start receiving clients' traffic. Attackers can also manipulate the DNS replies to redirect client traffic to malicious external destinations.

DHCP Trusted and Untrusted Ports

- Trusted ports are the ports on which DHCP offer packets are expected to be received
- Untrusted ports are the ports on which DHCP offer packets should not be received



FURTINET

 15

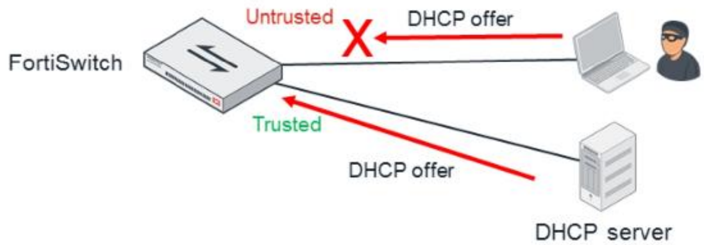
DHCP snooping is a FortiSwitch feature that prevents rogue DHCP attacks.

All ports are configured with DHCP snooping untrusted. When configuring DHCP snooping, you must define which FortiSwitch ports are trusted and which one are untrusted.

- Trusted ports are the ports on which DHCP offer packets are expected to be received, such as the ports where legitimate DHCP servers are connected
- Untrusted ports are the ports on which DHCP offer packets should never be received, such as the ports where user workstations are connected

DHCP Snooping

- Creates an IP-to-MAC binding database, with MAC addresses, ports, and leased IP addresses
- On untrusted ports, blocks invalid DHCP messages, such as:
  - DHCP offers
  - Requests to decline a DHCP offer if it is from a different port than the one that created the entry
  - DHCP release if it is from a different port than the one that created the entry



FORTINET

16

DHCP snooping inspects DHCP traffic in order to build a table that contains the MAC address, assigned IP address, and port number for each DHCP client.

On untrusted ports, DHCP snooping blocks the following types of DHCP messages:

- DHCP offers
- Requests to decline a DHCP offer, if it is from a different port than the one that created the entry
- A DHCP release, if it is from a different port than the one that created the entry

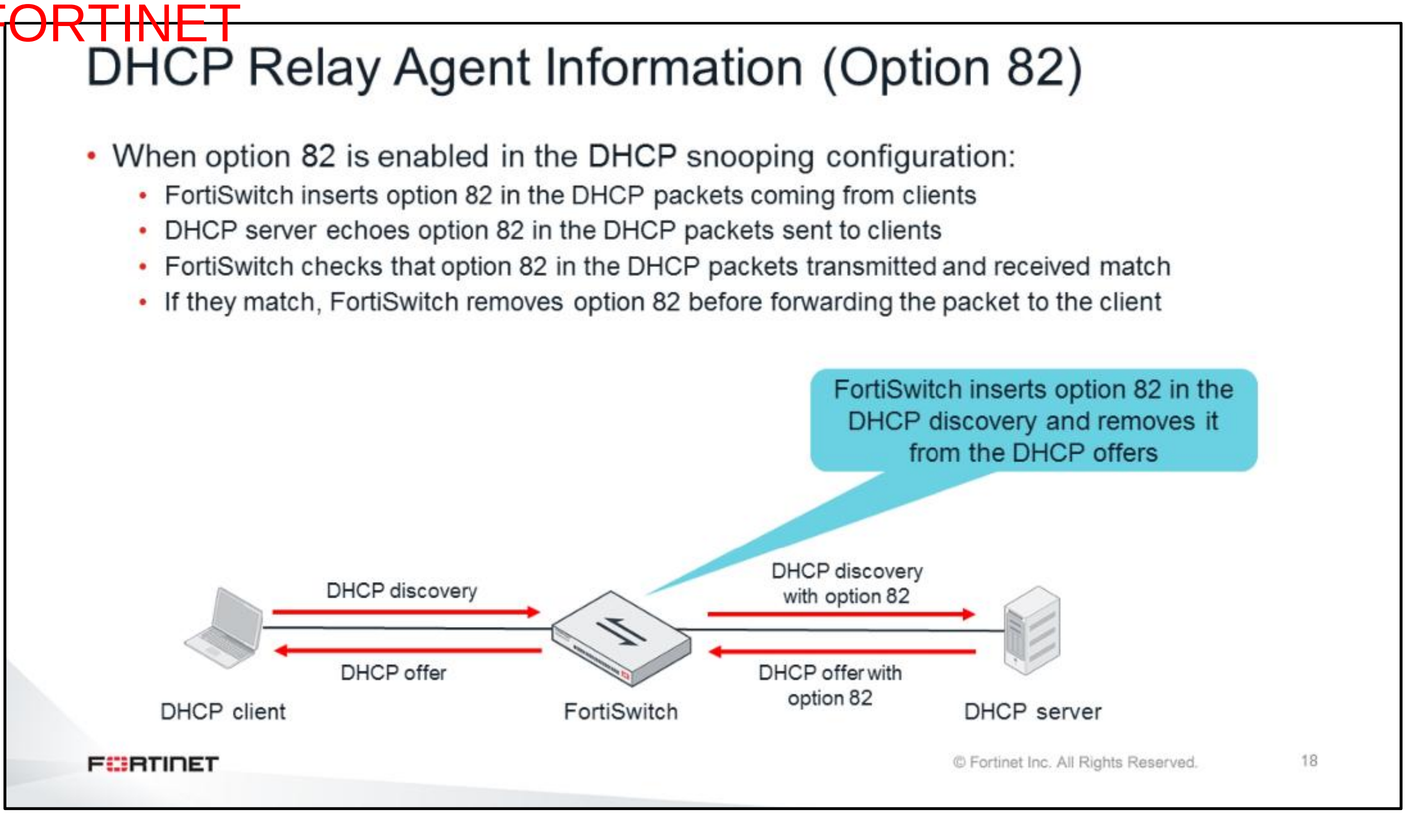
On trusted ports, all DHCP packets are accepted.

DHCP Relay Agent Information (Option 82)

- Option 82 provides information about the DHCP client
  - The DHCP server can use it to assign IP addresses and other parameters
  - Facilitates the identification of an assigned IP address
- Option 82 fields:
  - Circuit ID: `vlan-mod-port`
    - `vlan`: 2 bytes with the VLAN ID
    - `mod`: 1 byte with value 1 (meaning DHCP snooping)
    - `port`: 1 byte with the port ID
  - Remote ID: 6 bytes with the FortiSwitch MAC address

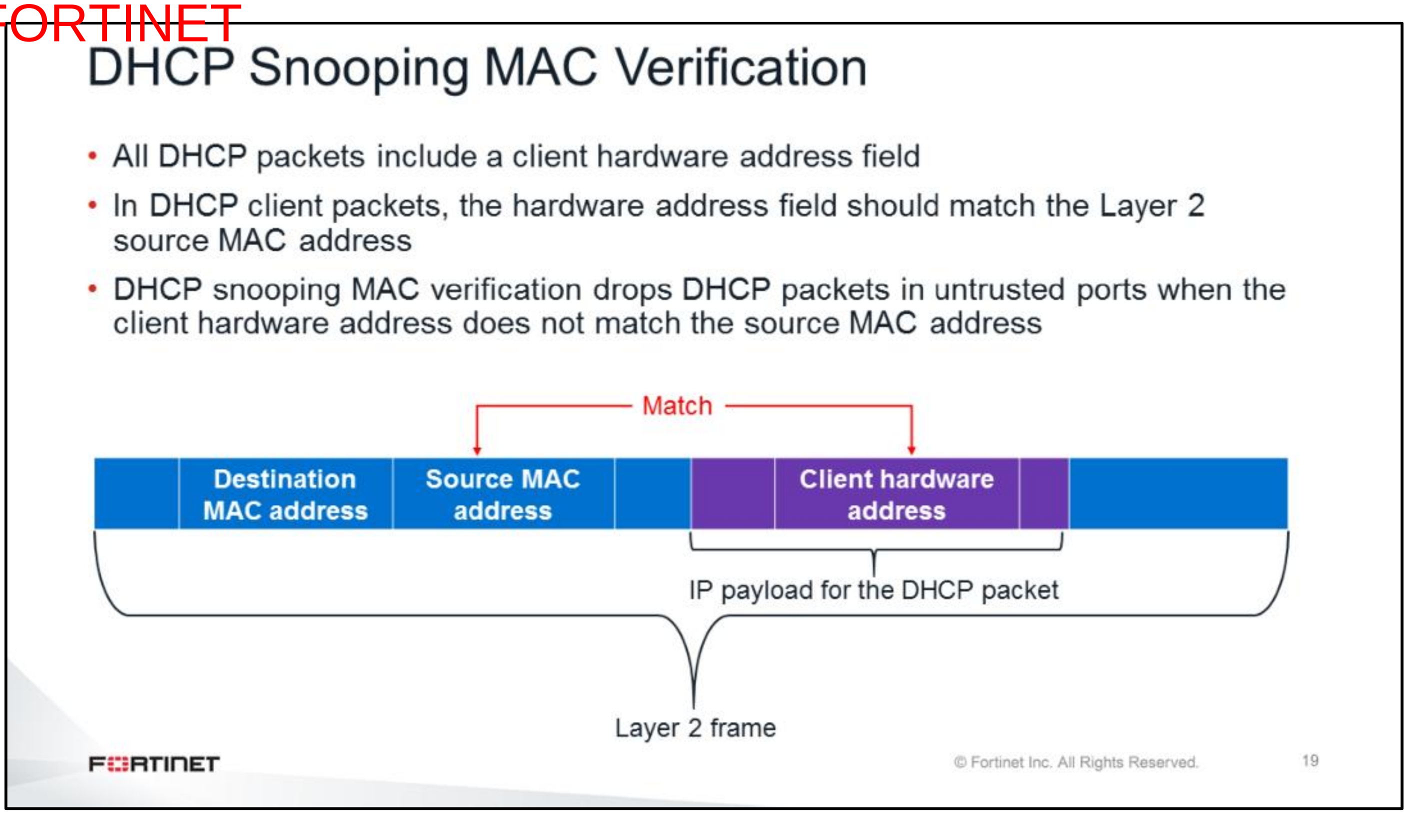
FORTINET 17

DHCP snooping can optionally insert the DHCP option 82 field into the DHCP packets coming from the clients. The option 82 field contains the VLAN ID, port ID, and FortiSwitch MAC address. This information can help administrators to locate the devices in the network. Additionally, the DHCP server can use this information to make assignment decisions based on the location of the device.



FortiSwitch inserts the option 82 field in any DHCP packets coming from a client. A DHCP server adds the same option 82 field to the DHCP offer.

When the DHCP offer with the option 82 field arrives, FortiSwitch compares the received field with the one sent. If they match, FortiSwitch removes the option 82 field before forwarding the DHCP offer to the client.



All DHCP packets include a client hardware address field. In the case of packets coming from DHCP clients, the hardware address field should match the Layer 2 source MAC address.

MAC verification is an optional DHCP snooping setting that drops DHCP packets in untrusted ports when the client hardware address does not match the source MAC address.

DHCP Snooping Configuration

```
config system interface
  edit <vlan-name>
    set switch-controller-dhcp-snooping enable
    set switch-controller-dhcp-snooping-option82 [enable | disable]
    set switch-controller-dhcp-snooping-verify-mac [enable | disable]
end
```

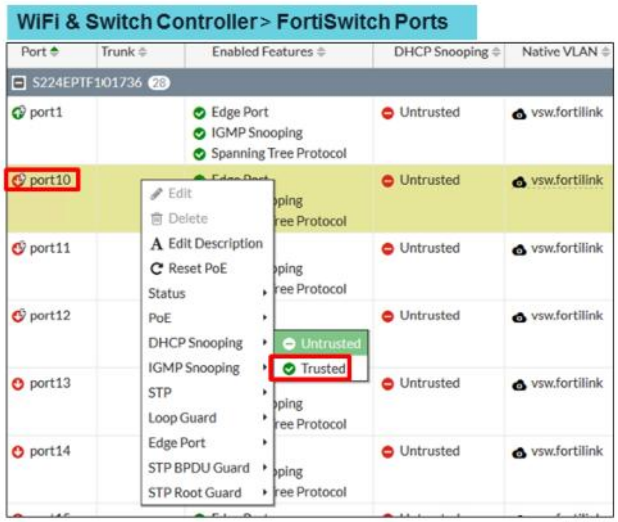
FERTINET

20

You enable DHCP snooping under the interface configuration. After enabling DHCP snooping, you have the option to enable DHCP option 82, and MAC address verification.

DHCP Snooping Configuration

- By default, all FortiSwitch ports are untrusted
- To trust the port, set **DHCP Snooping** to **Trusted**:



 21

By default, all FortiSwitch ports are untrusted. Untrusted ports are displayed in the GUI as having the **DHCP Snooping** set to **Untrusted**. To change a port to trusted, change the **DHCP Snooping** setting to **Trusted**.

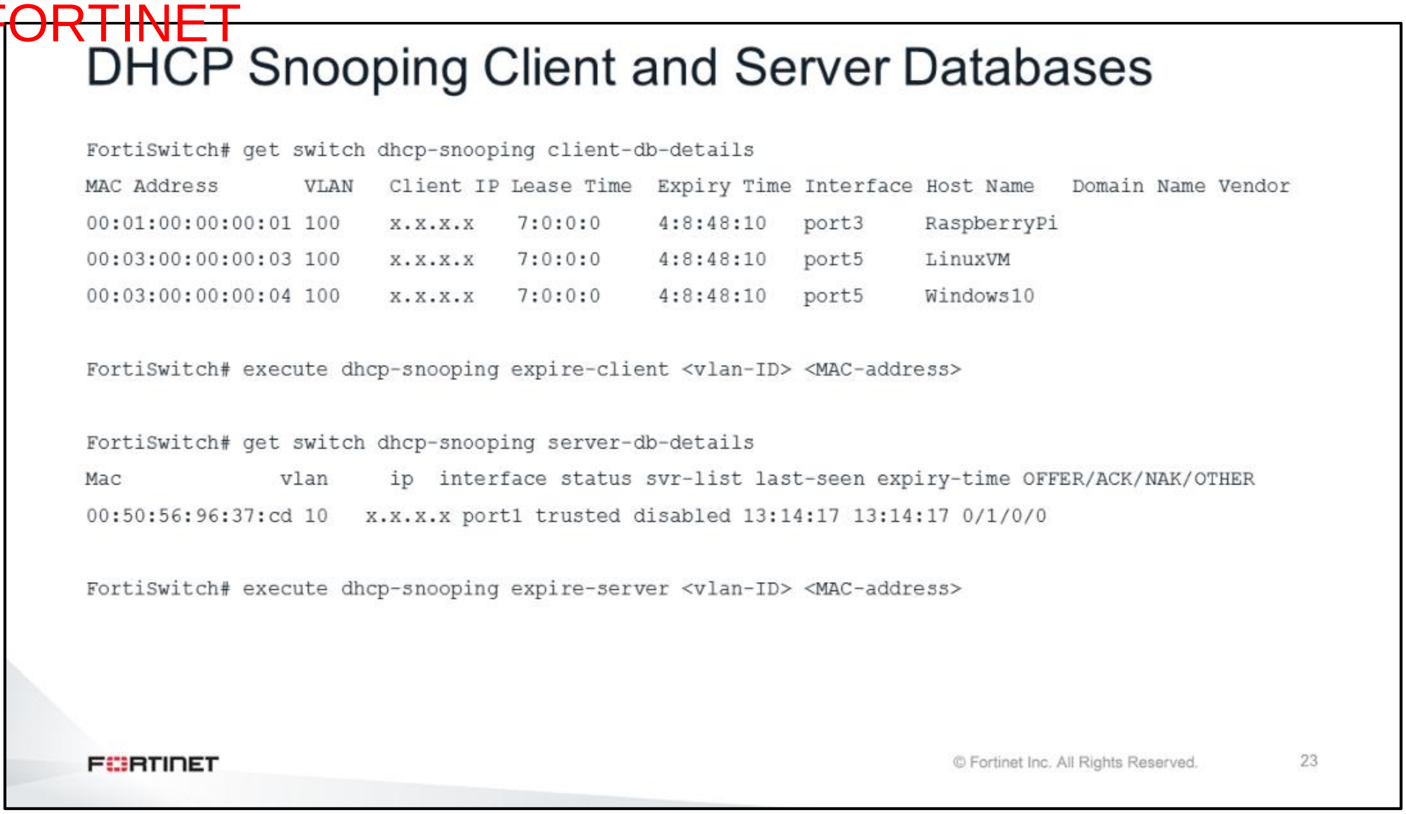
Monitoring DHCP Snooping

```
FortiGate# diagnose switch-controller switch-info dhcp-snooping database
Vdom: root

S224EPTF18001736:
snoop-enabled-vlans            : 10
verifysrcmac-enabled-vlans     :
option82-enabled-vlans         :
option82-trust-enabled-intfs   :
trusted ports    : GVM1V0000141680
untrusted ports  : port1 port2 port3 port4 port5 port6 port7 port8 port9 port10

Client Database          : 1 / 2000
Server Database          : 0 / 256
Limit Database           : 1 / 256

DHCP Global Configuration:
==========================
DHCP Tracking Mode              : Tracking
DHCP Broadcast Mode             : All
DHCP Allowed Server List        : Disable
Add hostname in Option82        : Disable
```

FORTINET 22

The output of the command `diagnose switch-controller switch-info dhcp-snooping database` shows some general information about DHCP snooping, such as:

- A list of VLANs with DHCP snooping enabled
- A list of trusted ports
- A list of untrusted ports
- The number of DHCP clients detected
- The number of DHCP servers detected



The command `get switch dhcp-snooping` displays the list of DHCP clients (using the `client-db-details` option) and the list of DHCP servers (using the `server-db-details` option).

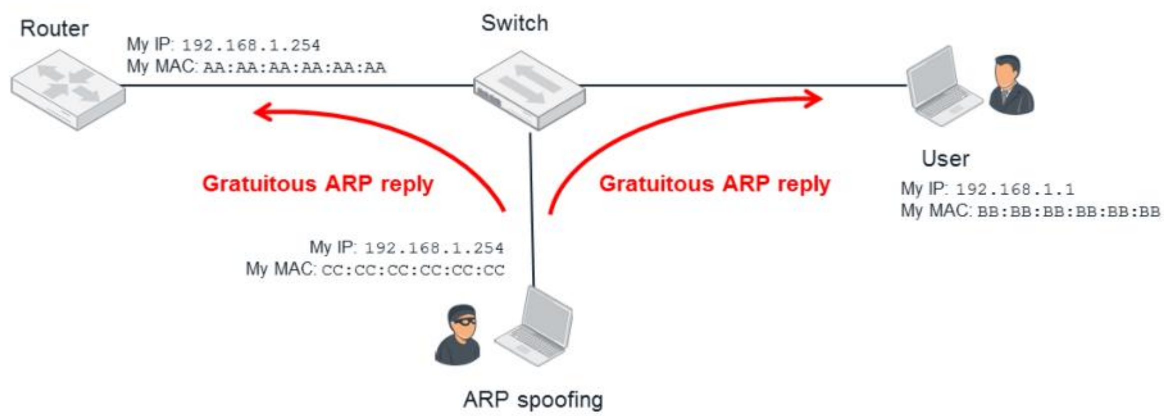
The command `execute dhcp-snooping` removes either a DHCP client (with the `expire-client` option), or a server (with the `expire-server` option), from the DHCP snooping database.

ARP Inspection

In this section, you will learn how to work with ARP inspection.

ARP Spoofing Attacks

- ARP protocol allows ARP gratuitous replies without any ARP request
- An attacker sends forged ARP replies using its MAC address and spoofing a target's IP address

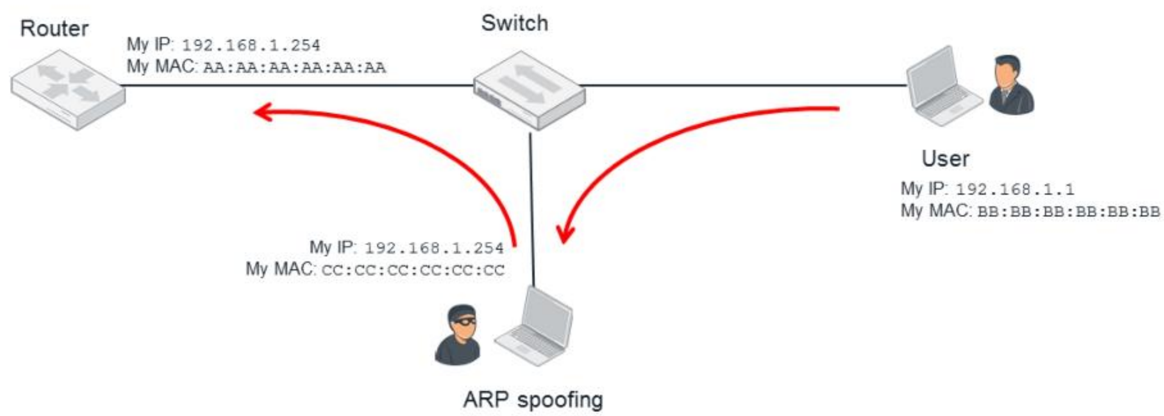


A security weakness in the ARP protocol is that it allows devices to send ARP replies without any ARP request. These packets are called gratuitous ARPs. This weakness can be exploited to execute an ARP spoofing attack (also called an ARP poison attack).

During ARP spoofing attacks, attackers send gratuitous ARP packets using their MAC addresses, but spoofing someone else's IP address. These gratuitous ARPs are broadcast throughout all of the switch's ports, causing all devices in the Layer 2 network to update their ARP tables.

ARP Spoofing Attacks

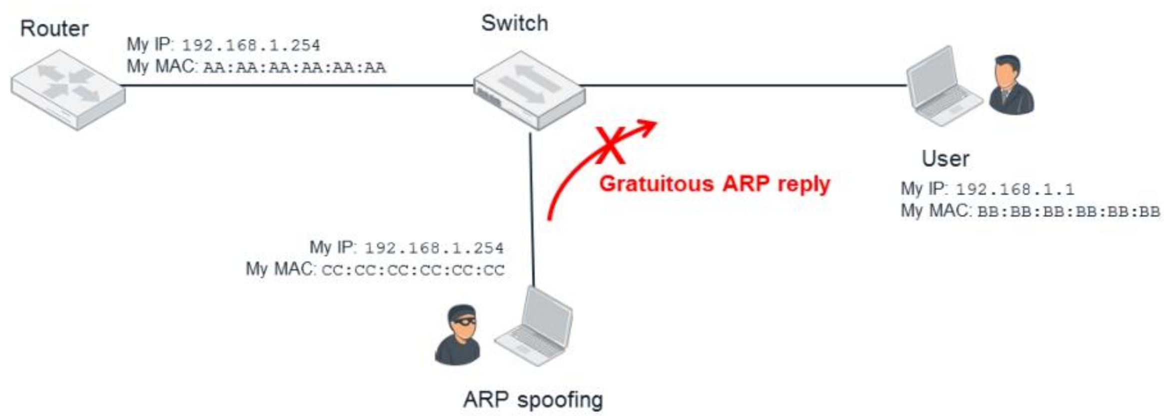
- User sends traffic to attacker's MAC address
- Attacker inspects the traffic and forwards it to router's MAC address



As a consequence of an ARP spoofing attack, all devices start sending traffic destined to the spoofed IP address to the attacker's machine. The attacker can then inspect and potentially modify the traffic before forwarding it to the device that legitimately owns the spoofed IP address.

ARP Inspection

- Uses the IP-to-MAC information collected by DHCP snooping
- Drops ARP packets with an invalid IP-to-MAC address binding

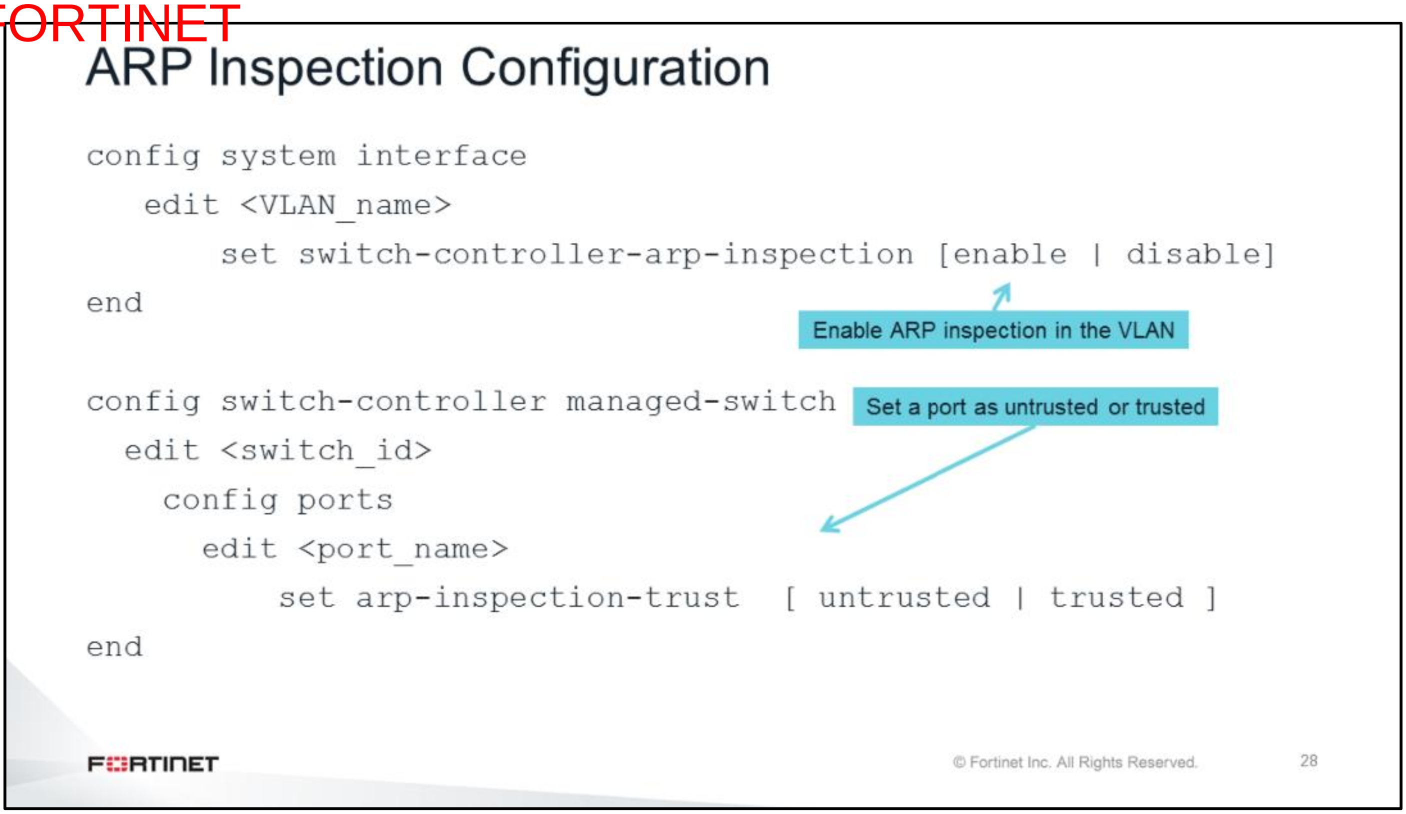


ARP inspection can prevent ARP spoofing attacks. ARP inspection uses the IP-to-MAC binding table populated by the DHCP snooping feature, to drop invalid ARP packets. An ARP packet is categorized as invalid when the IP and MAC address pair does not match the information in the IP-to-MAC binding table.

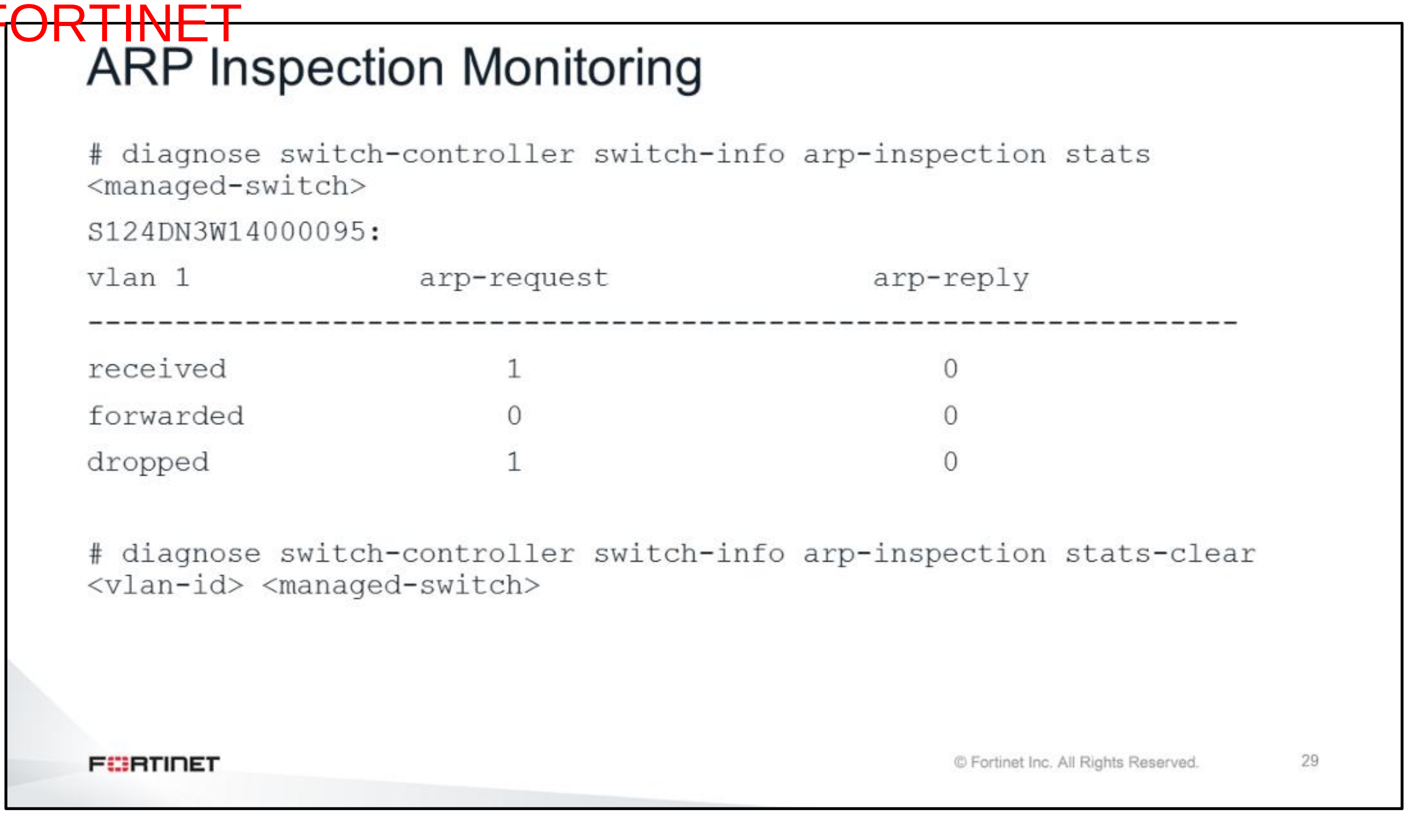
For ARP request packets, ARP inspection examines the source IP and MAC addresses. For ARP replies, ARP inspection examines both the source and destination MAC and IP addresses. The checking is done only on packets incoming to untrusted ports.

With this feature, gratuitous ARP reply packets with spoofed IP addresses are blocked, because they do not match the information in the IP-to-MAC binding table.

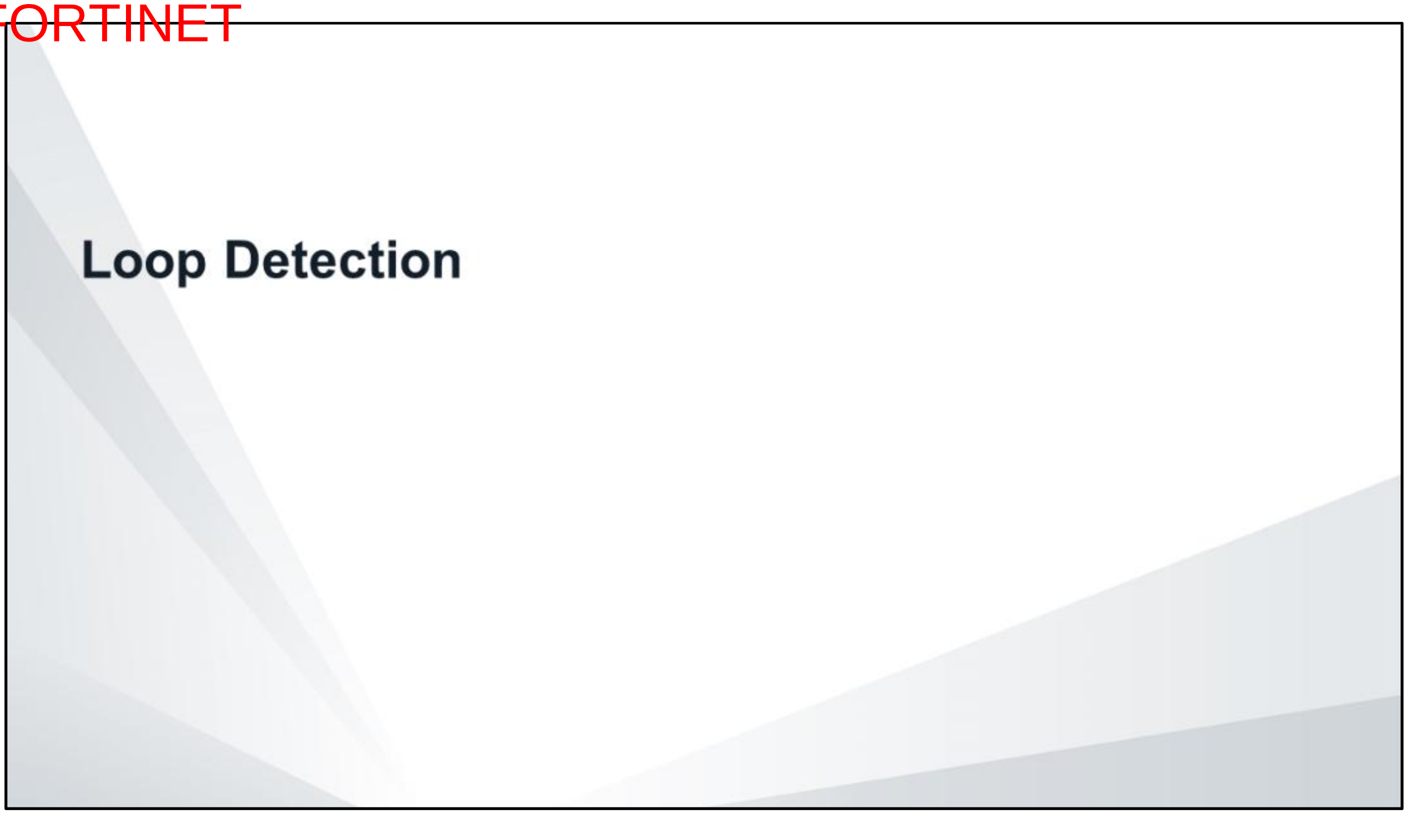
Because ARP inspection relies on the use of the IP-to-MAC binding table, it must work in conjunction with the DHCP snooping feature.



ARP inspection is enabled at the VLAN level. Each port is then configured as trusted or untrusted.



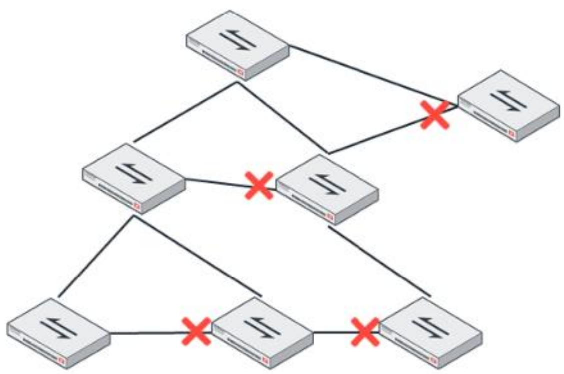
The output of the command `diagnose switch arp-inspection stats` shows general statistics about the ARP inspection feature, including the number of ARP requests and replies that have been received, forwarded, and dropped. You can clear these statistics using the command `diagnose switch arp-inspection stats clear`.

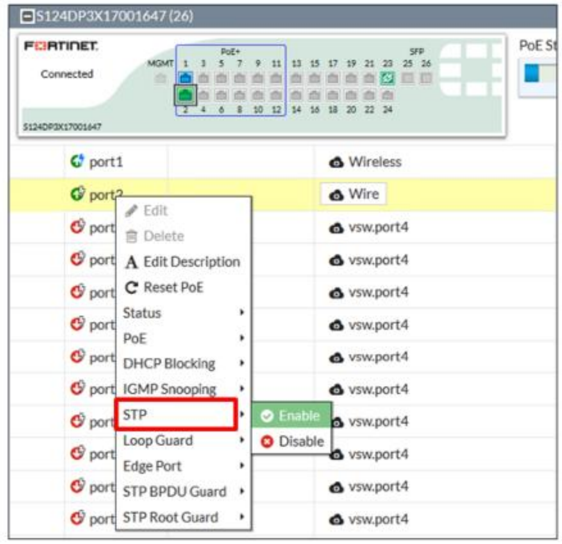


In this section, you will learn about the different mechanisms that FortiSwitch has to detect and avoid network loops that could create broadcast storms.

Spanning Tree Protocol (STP) 802.1d

- Builds a Layer 2 loop-free logical topology by blocking redundant ports





 31

The spanning tree protocol (STP) detects and disables switch ports that create network loops. It automatically builds a network topology free of loops by blocking redundant ports. Switches running STP build this loop-free topology by interchanging bridge protocol data unit (BPDU) frames.

There are different types of STP protocols. FortiSwitch managed by FortiGate supports the common STP, which is described in the 802.1d IEEE standard. FortiSwitches operating in standalone mode also supports multiple spanning tree protocol (802.s).

Port States in STP

Port State	Included in the active topology?	Send/receive BPDUs?	MAC address learning?	Forward user traffic?
Disable	No	No	No	No
Blocking	Yes	Receive only	No	No
Listening	Yes	Send and receive	No	No
Learning	Yes	Send and receive	Yes	No
Forwarding	Yes	Send and receive	Yes	Yes

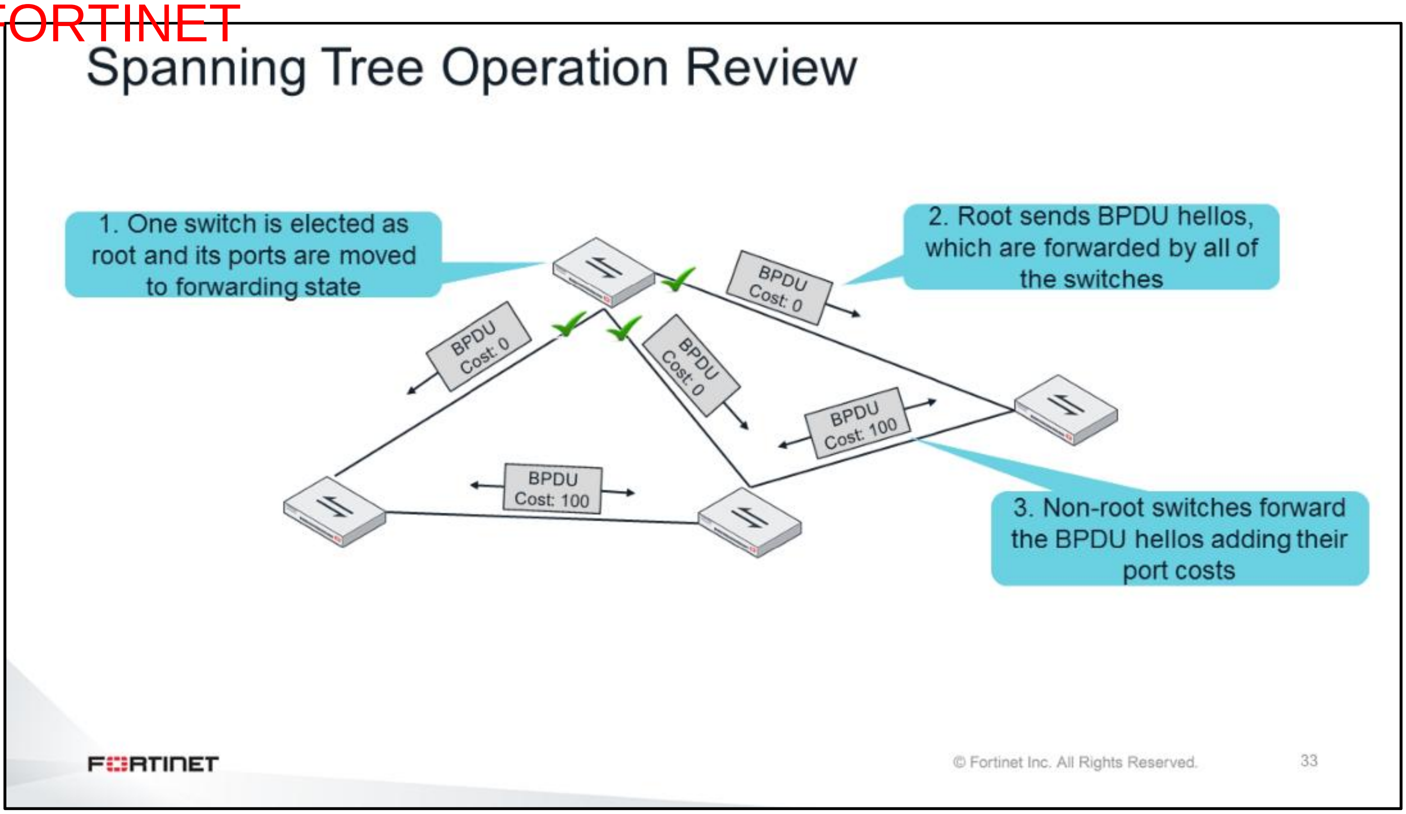
FORTINET

32

In STP 802.1d, any switch port can be in one of the following five states:

Disable: The port is not sending or receiving BPDU frames. The port is also not forwarding user traffic.
Blocking: The port is listening to incoming BPDU frames, but does not send any BPDU frames. The port is not learning MAC addresses, or forwarding user traffic.
Listening: Similar to the blocking state, but the port is both receiving and transmitting BPDU frames.
Learning: The port interchanges BPDU frames and learns MAC addresses, but does not forward user traffic yet.
Forwarding: The port interchanges BPDU frames, learns MAC addresses, and forwards user traffic. This is the normal state for an active port.

A port in blocking state must go through listening and learning states, before ending in forwarding state.

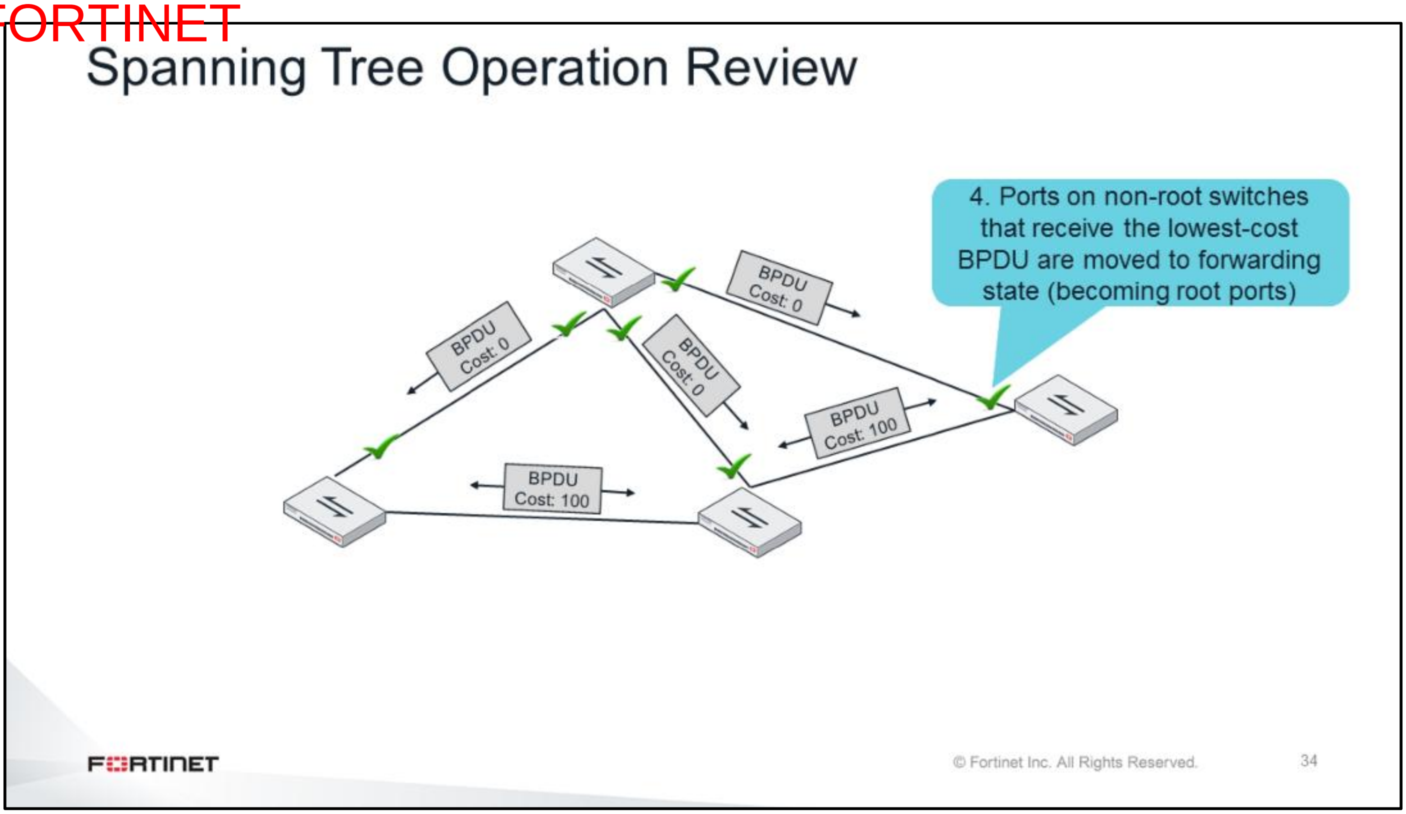


These are the steps that STP follows to build the loop-free topology:

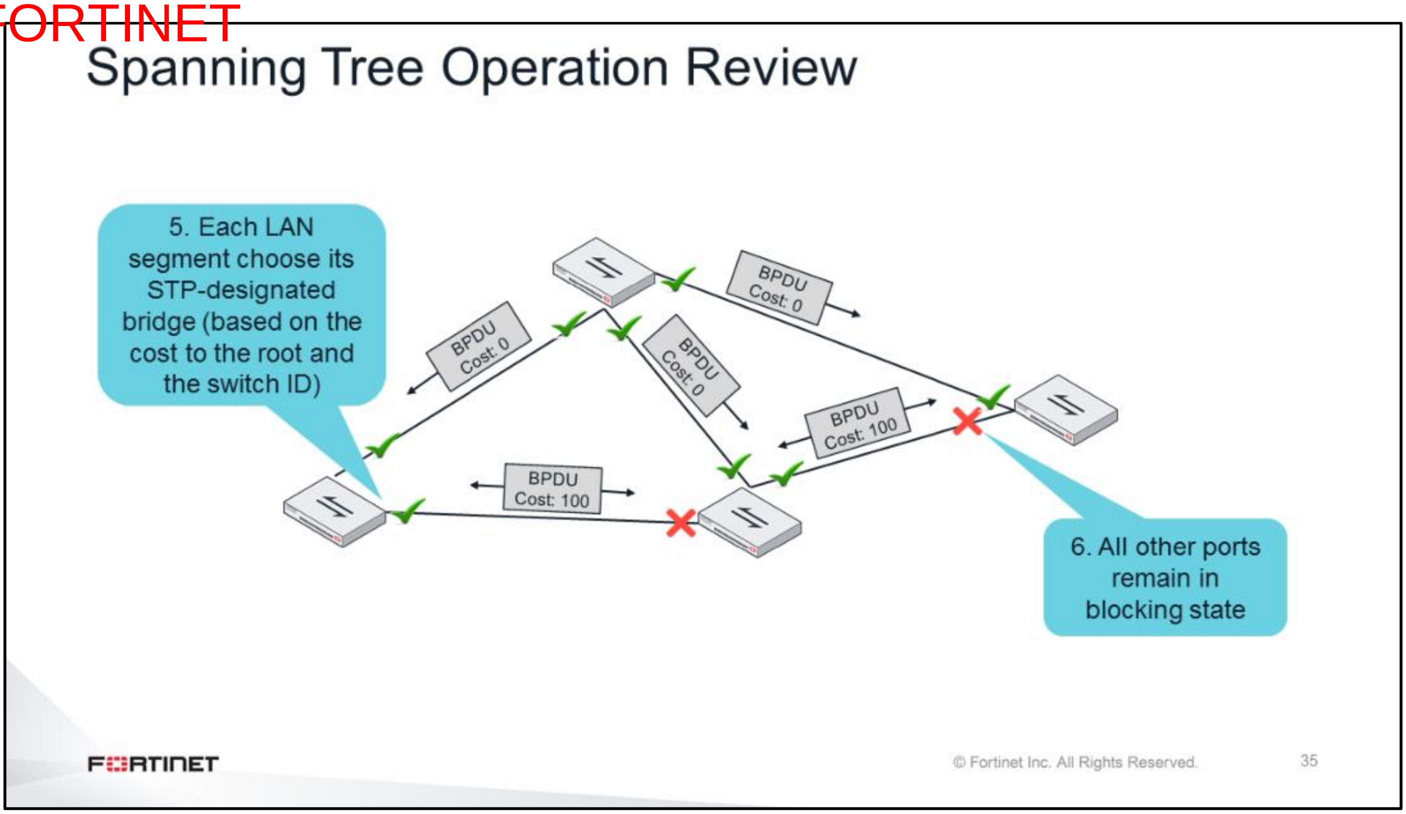
1. Each switch is assigned an STP priority. When STP starts, all switches start sending BPDU frames containing their priorities. The switch with the lowest priority is elected the root switch. All the ports in the root switch are moved to forwarding state.

2. After the root switch is elected, all the other switches stop generating BPDU frames. Only the root switch keeps generating BPDU frames.

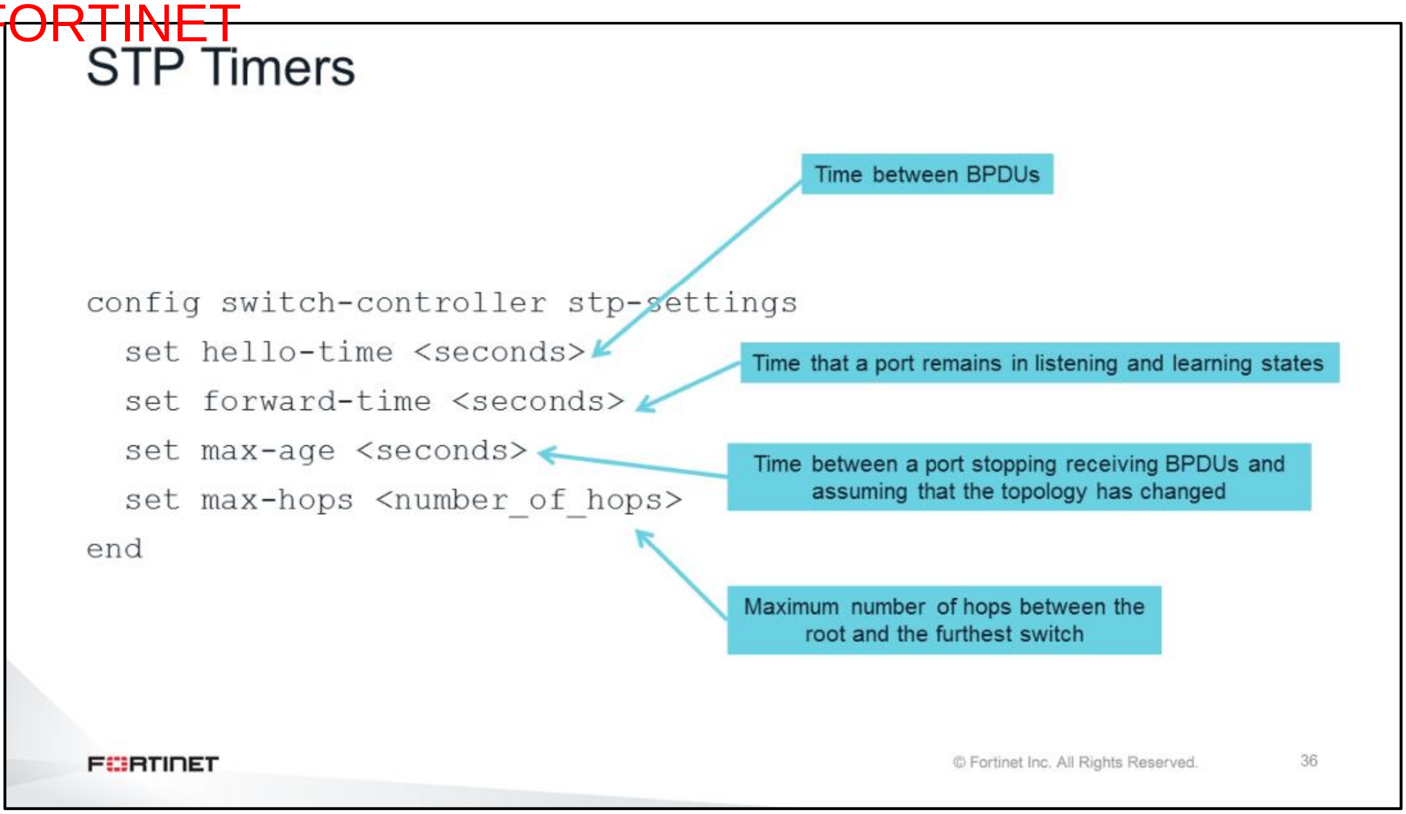
3. All the non-root switches receive the BPDUs coming from the root, and add their port's cost to the total-cost-to-the-root field, before forwarding the BPDUs to other switches.



4. Ports in non-root switches that receive the BPDUs with the lowest total-cost-to-the-root value are moved to forwarding state. They become root ports.



5. In each LAN segment, a designated port is elected, based on the cost to the root, the switch priority, and the port priority. The designated port for each LAN segment is moved to forwarding state.
6. All the other ports remain in blocking state.

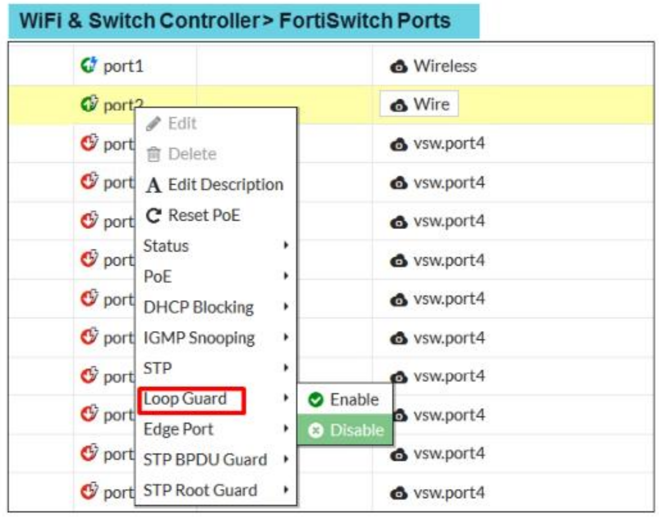


There are four switch-controller settings related to STP:

`hello-time`: Determines how frequently the root switch sends the BPDUs. The default is 2 seconds.
`forward-time`: Determines the time that a port remains in listening state before moving to learning state. It is also the time that a port remains in learning state before moving to forwarding state. The default is 15 seconds.
`max-age`: Determines that if a port has not received any BPDU during this time, the switch assumes that the network topology has changed and STP recalculation is required. Usually, if the port was in blocking state, it is moved to listening, learning, and forwarding state. If the port is a root port, a new root port is elected.
`max-hops`: Determines the maximum number of switches between the root switch and the furthest switch. This parameter sets a limit to the size of your Layer 2 network.

Loop Guard

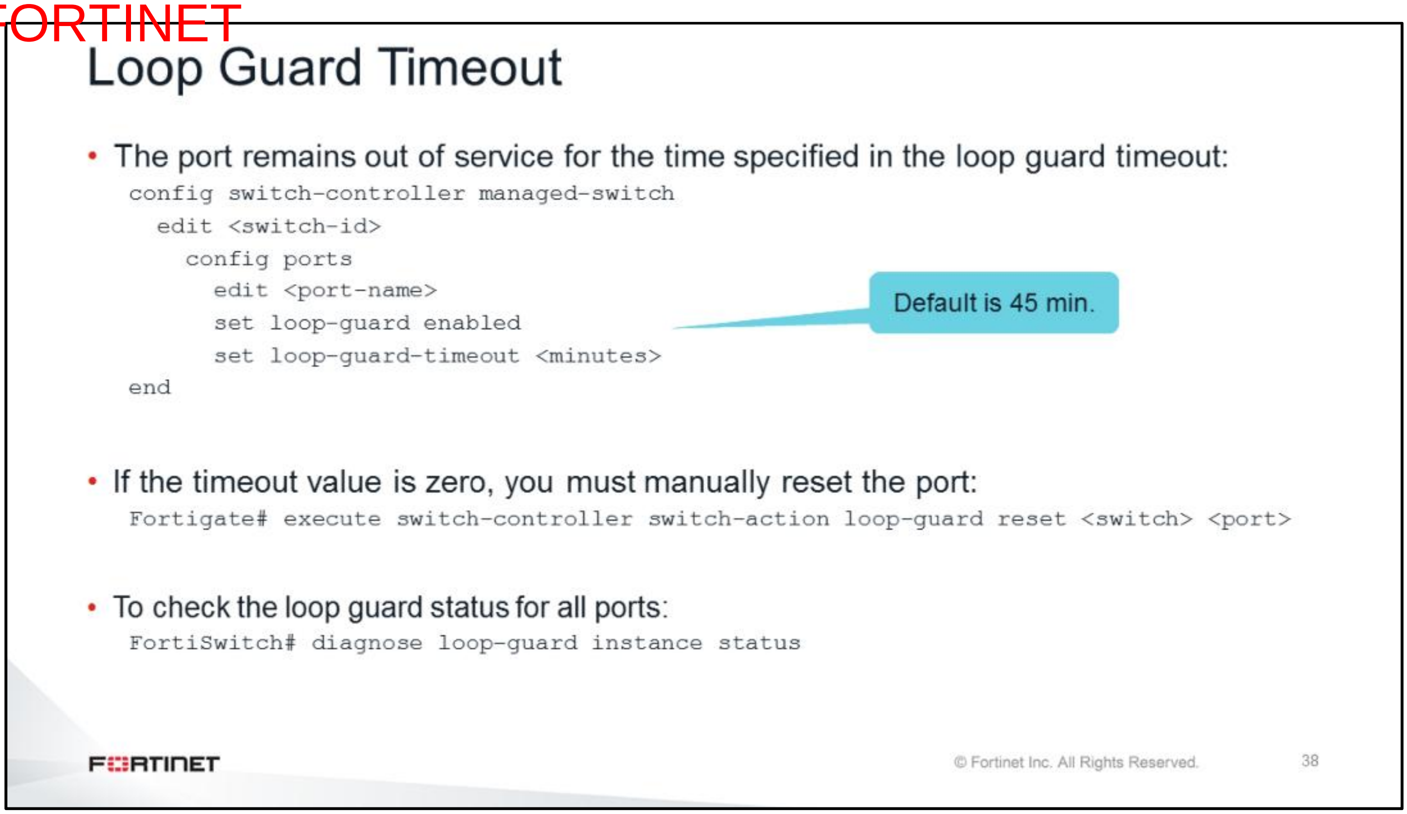
- Broadcasts loop guard data packets (LGDPs)
- If an LGDP packet is subsequently received by the sending switch, a loop exists and the sending port is shut down
  - This feature is not meant to be a replacement of spanning tree, but to work in concert with it



 37

Loop guard is another loop-detection mechanism available in FortiSwitch. This feature is not meant to be a replacement of spanning tree, but to complement it.

With loop guard, FortiSwitch periodically sends loop guard data packets (LGDPs). If the sending switch subsequently receives an LGDP packet, a loop exists and the sending port is shut down.



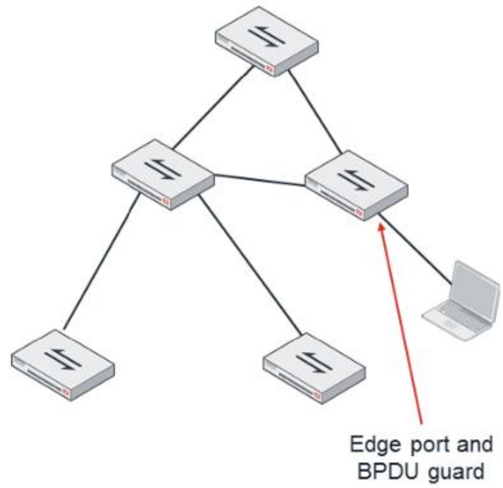
When loop guard detects a loop, the loop guard timeout defines the time the port will remain shut down.

If the loop guard timeout is set to zero and a loop is detected, the port remains shut down until you manually reset its loop-guard status, with the command `execute switch-controller loop-guard-reset`.

You can use the command `diagnose loop-guard instance status` to check the loop guard status for all ports.

Edge Port and BPDU Guard

- Edge ports:
  - Forward user traffic and learn MAC addresses
  - Do not send BPDUs
  - Are not part of the STP topology
  - Port flapping does not cause STP recalculations
- With BPDU guard, edge ports go down if any BPDU is received

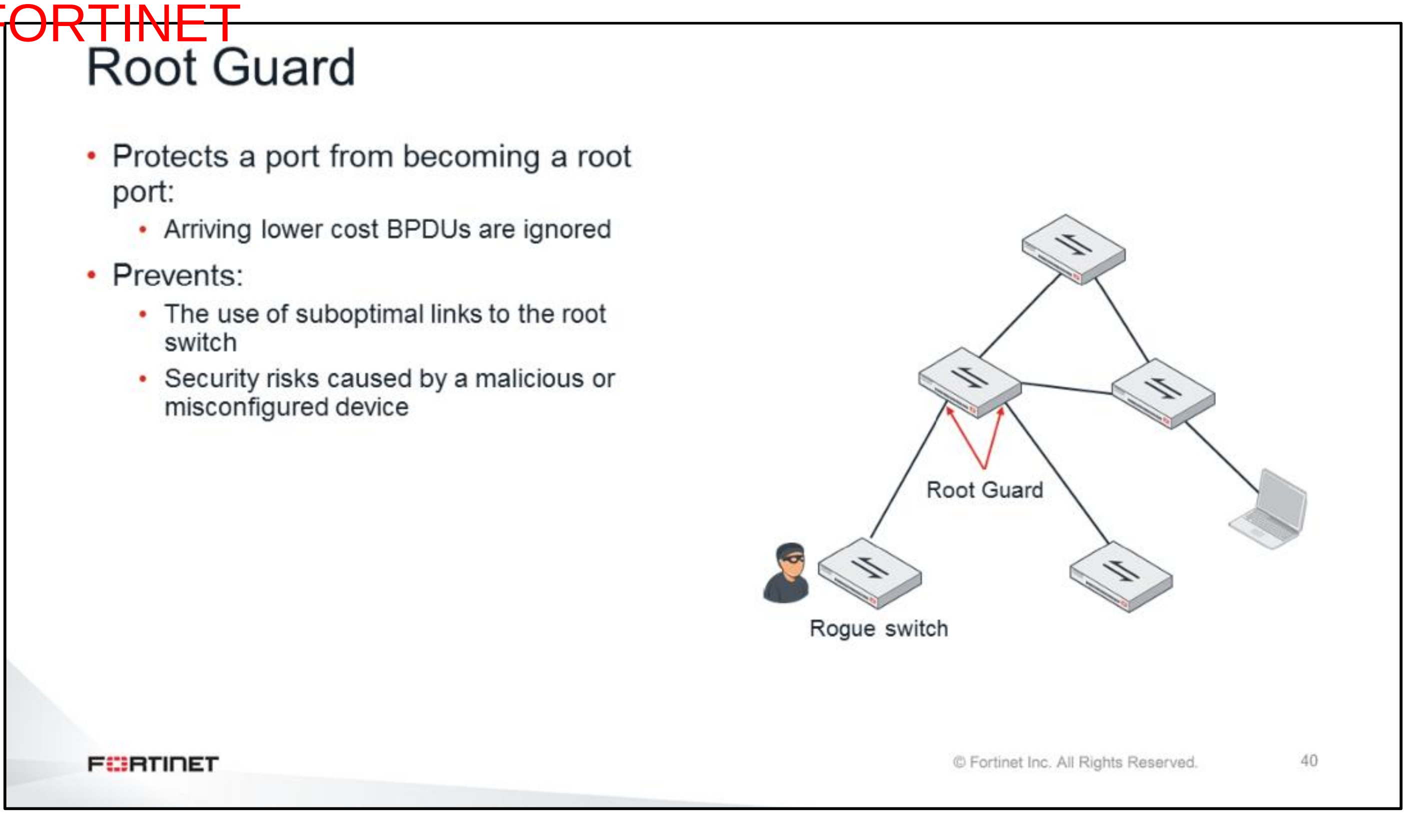


If you know that only end devices (and not other switches) will always be connected to a FortiSwitch port, you can set it as an edge port. This has the following advantages:

- The port can go directly from blocking state to forwarding state, avoiding the 30-seconds delay caused by the listening and learning states
- Port flapping does not cause STP recalculations

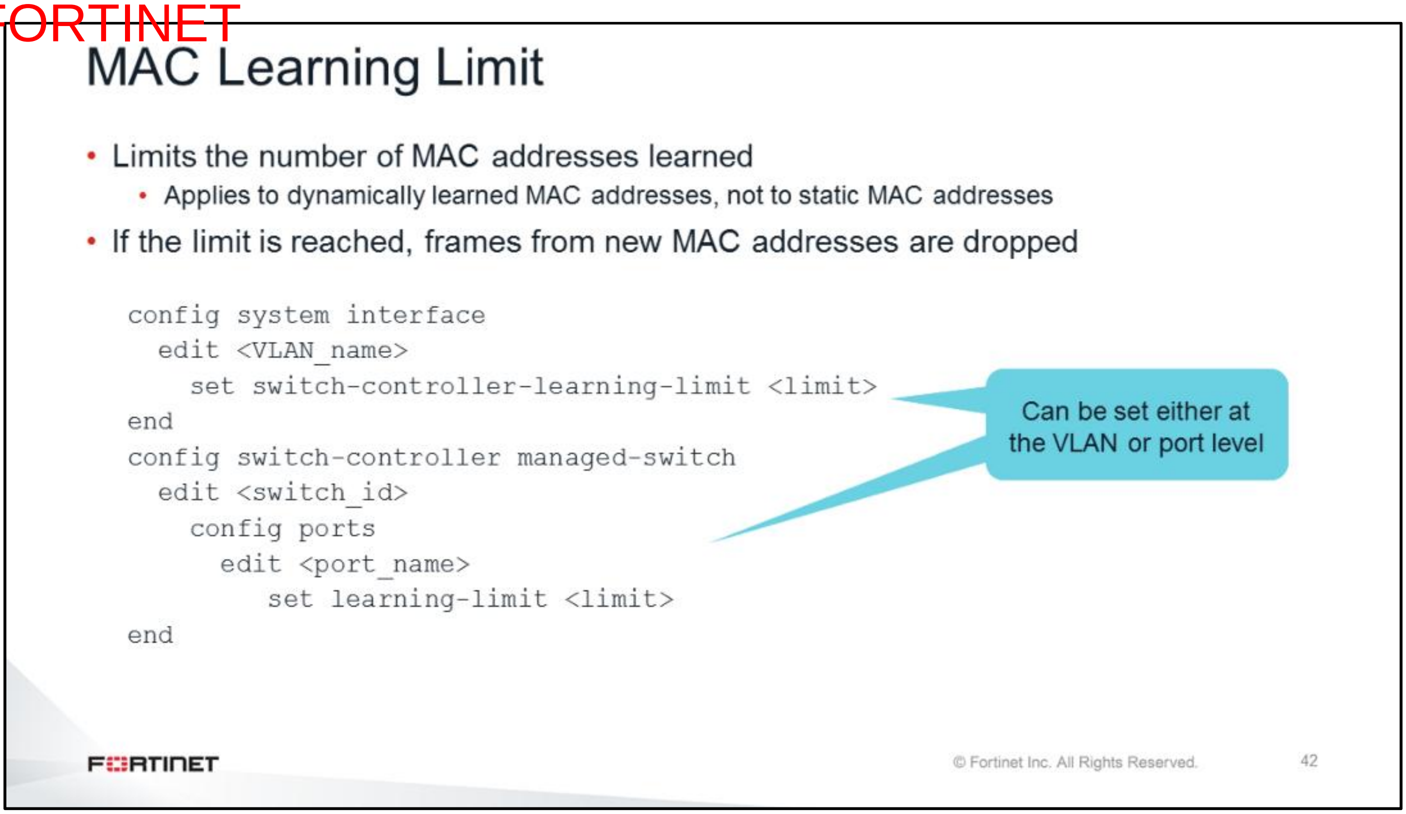
An edge port learns MAC addresses and forwards user traffic. An edge port does not send BPUDs and is not part of the STP topology.

You can use BPDU guard to protect edge ports from forming accidental loops. BPDU guard shuts down an edge port if it receives a BPDU, because it means that a switch was connected by mistake, and there is the potential of creating a network loop.



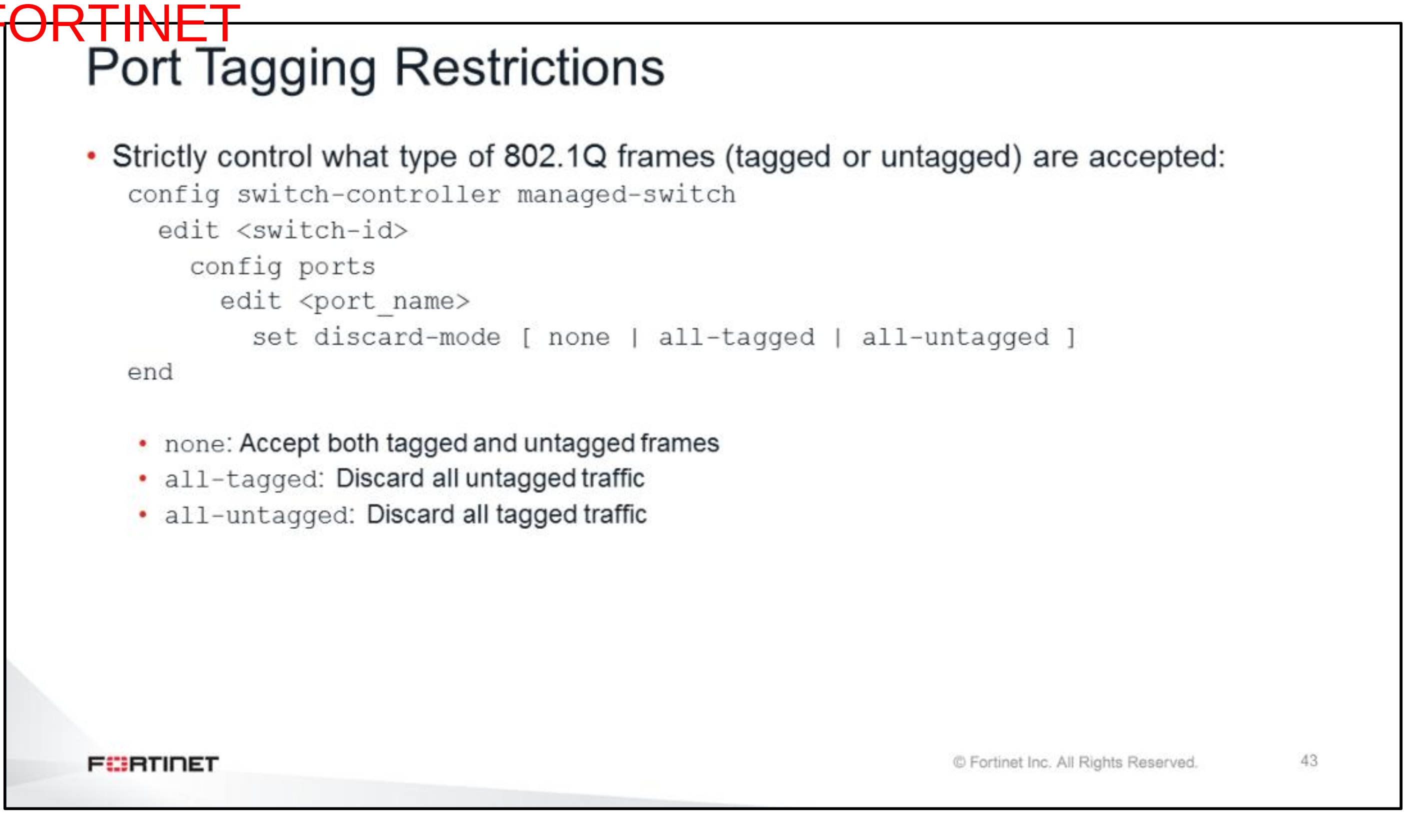
In an STP network, an attacker could potentially connect a rogue switch with a very low priority value to your network. This will trigger an STP recalculation and the rogue switch might become the root switch. Root guard offers a mechanism to protect your network against rogue or misconfigured switches. Root guard is enabled in ports that will never be used to reach the root switch. In other words, administrators usually enable root guard in ports where downstream switches are connected. With root guard, a port ignores any BPDU with a cost-to-root lower than the one received by the existing root port. So, ports where root guard is enabled can never become root ports.

In this section, you will learn about other FortiSwitch features for protecting your Layer 2 network.



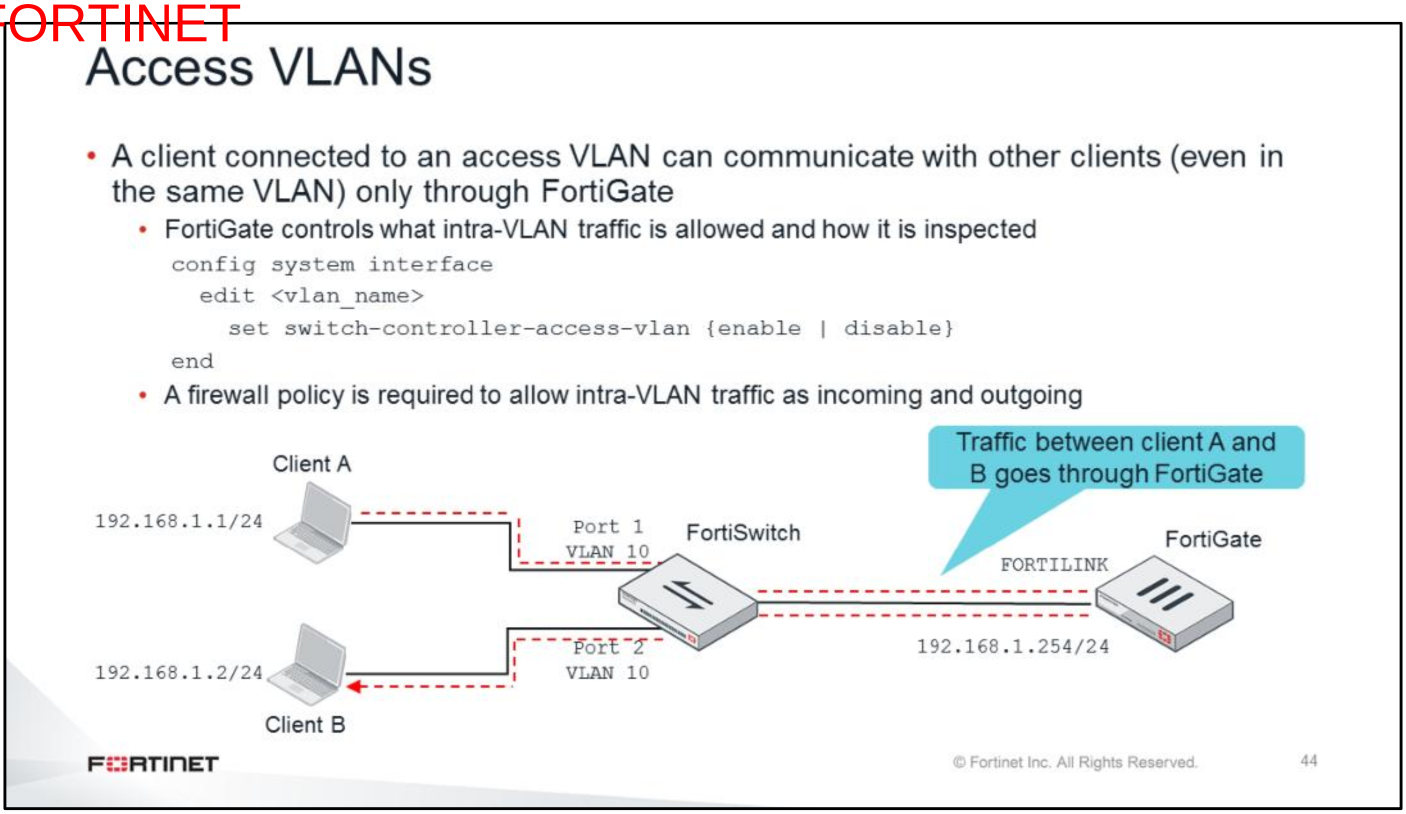
The MAC learning limit sets controls on the maximum number of MAC addresses that a port or VLAN can learn. It applies to dynamically learned MAC addresses, not to static MAC addresses.

If the limit is reached, frames from new MAC addresses are dropped.



The discard mode parameter, at the port level, sets restrictions regarding the type of 802.1q frames that FortiSwitch accepts:

`none`: Accepts both tagged and untagged frames
`all-tagged`: Discards all untagged traffic
`all-untagged`: Discards all tagged traffic



By default, traffic between clients connected to the same VLAN and the same FortiSwitch does not go through FortiGate. This traffic is locally handled by FortiSwitch.

With access VLANs, all traffic between clients (even traffic between clients in the same VLAN and switch) goes through FortiGate. This allows you to inspect and control intra-VLAN traffic. Firewall policies are required to allow the intra-VLAN traffic, which can now be inspected by FortiGate.

Static IP-MAC Binding

- FortiGate drops the packet if the source IP and MAC addresses do not match the static IP-to-MAC binding table
  - It is a FortiOS feature (not exclusive to FortiSwitch VLANs)

```
config firewall ipmacbinding setting
  set bindthroughfw [enable | disable]
  set bindtofw [enable | disable]
end
config system interface
  edit <port-name>
    set ipmac enable
end
config firewall ipmacbinding table
    edit <sequence-number>
        set ip <ip-address>
        set mac <mac-address>
        set name <name>
        set status enable
    next
end
```

Enable for inspecting traffic crossing FortiGate

Enable for inspecting traffic terminating or originating at FortiGate

Must also be enabled in the physical or VLAN interface

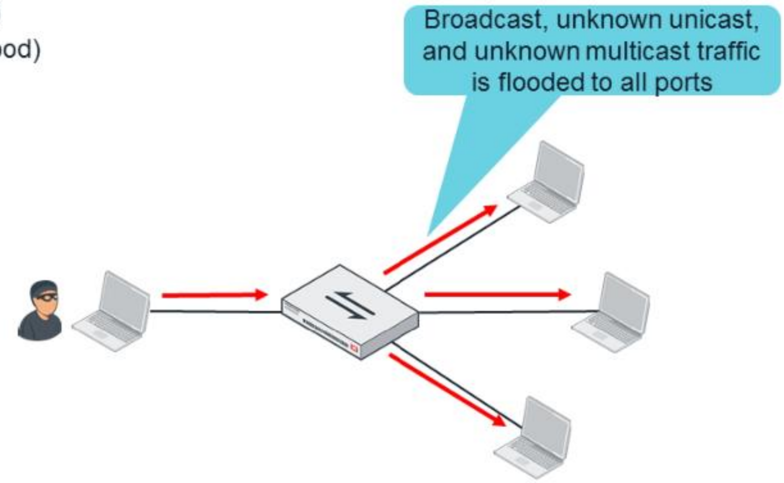
FURTINET

 45

DHCP snooping dynamically creates an IP-to-MAC binding table. You can also create a static IP-to-MAC binding table with these commands. This is a FortiOS feature that you can use with or without FortiSwitch. FortiGate drops the packet if the source IP and MAC addresses do not match the information in the static IP-to-MAC binding table.

Storm Control

- Unusually high levels of some types of traffic can disrupt user traffic:
  - Broadcast (broadcast flood)
  - Unknown unicast (unicast flood)
  - Unknown multicast (multicast flood)
- This could be caused by:
  - Spanning tree misconfiguration
  - Network loops
  - Faulty network cards
  - Attacks

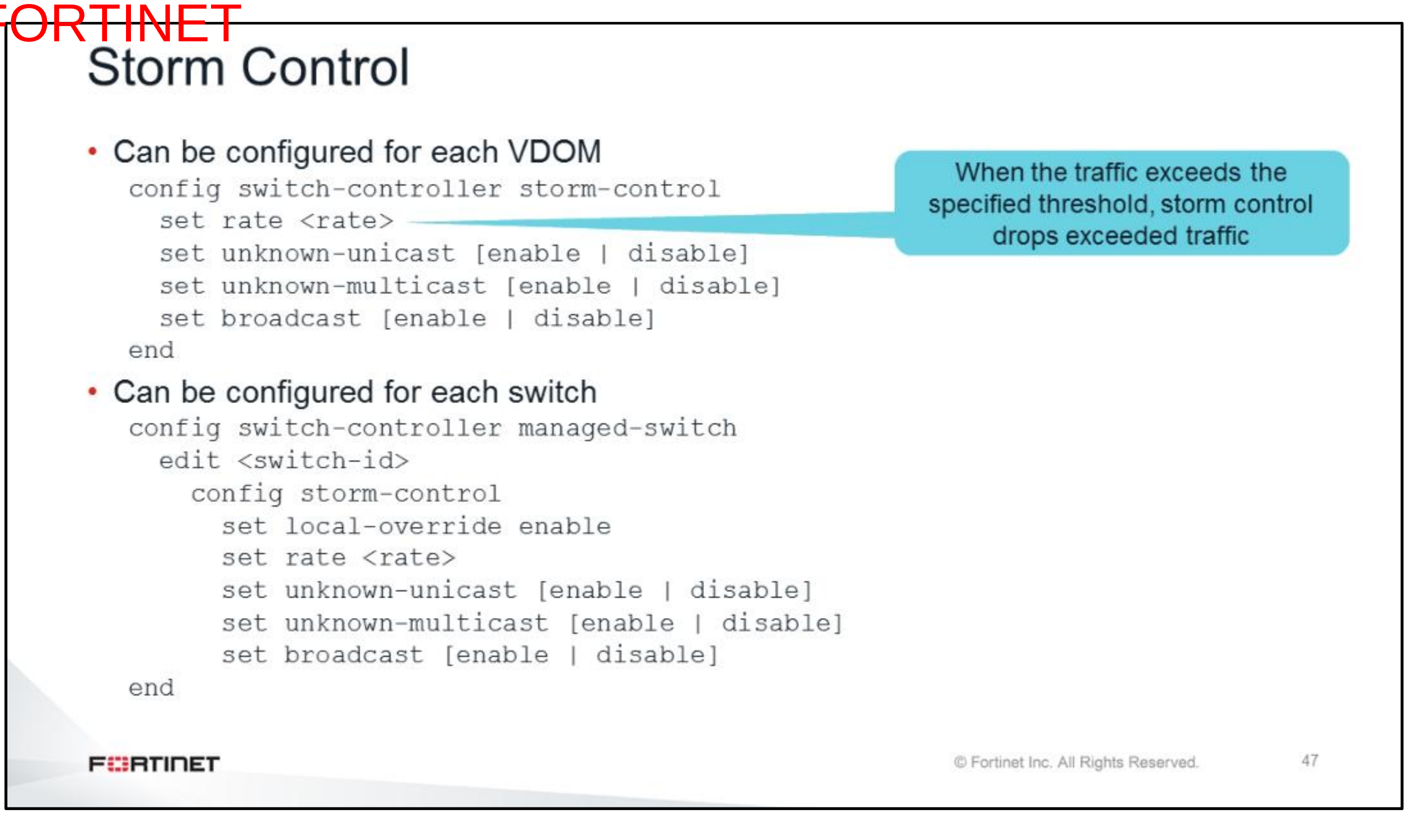


FERTINET

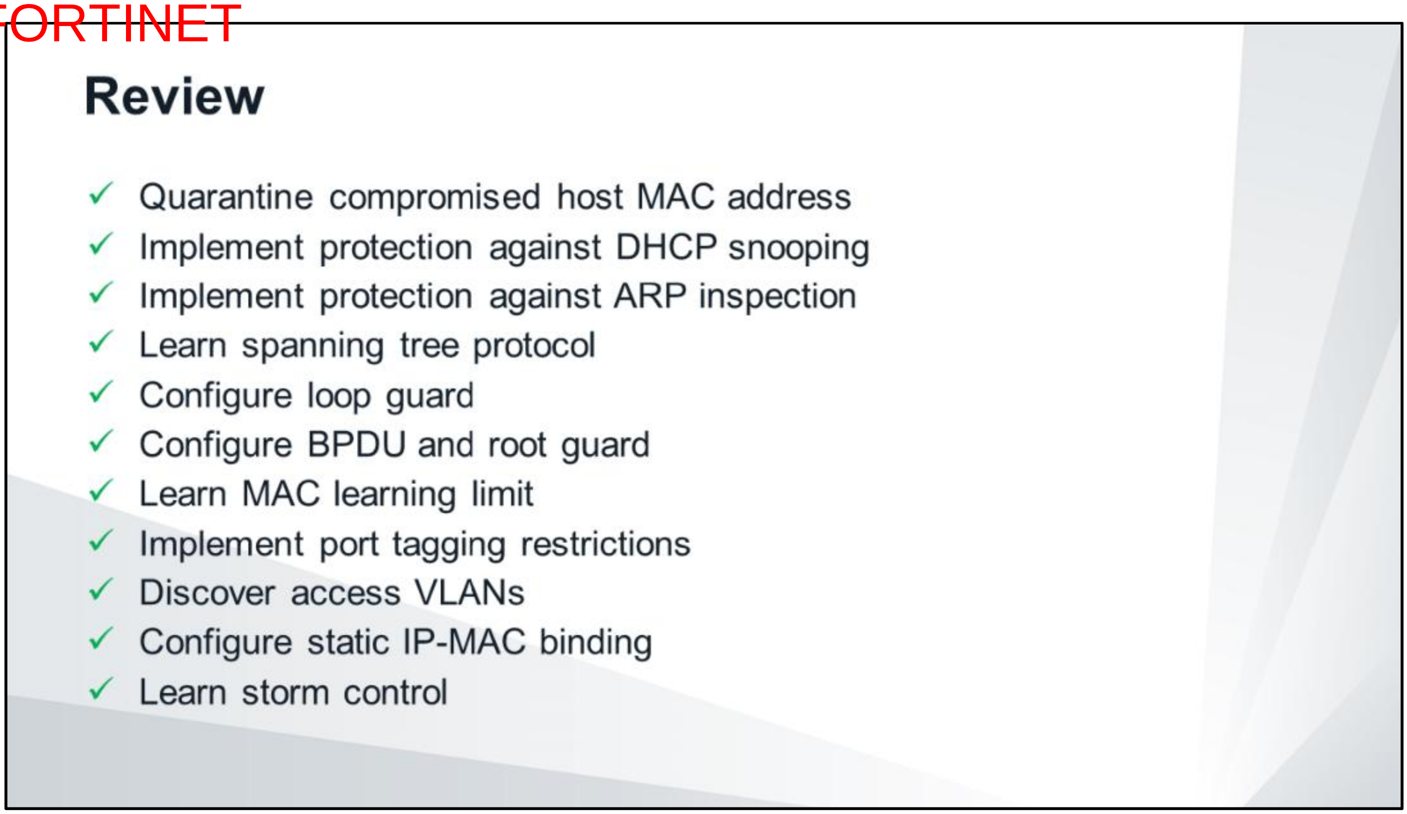
 46

A Layer 2 storm is an usually high level of some type of traffic that can disrupt user traffic. The types of traffic that could potentially create storms are broadcast, unicast to invalid destinations (unknown unicast), and multicast to invalid destinations (unknown multicast).

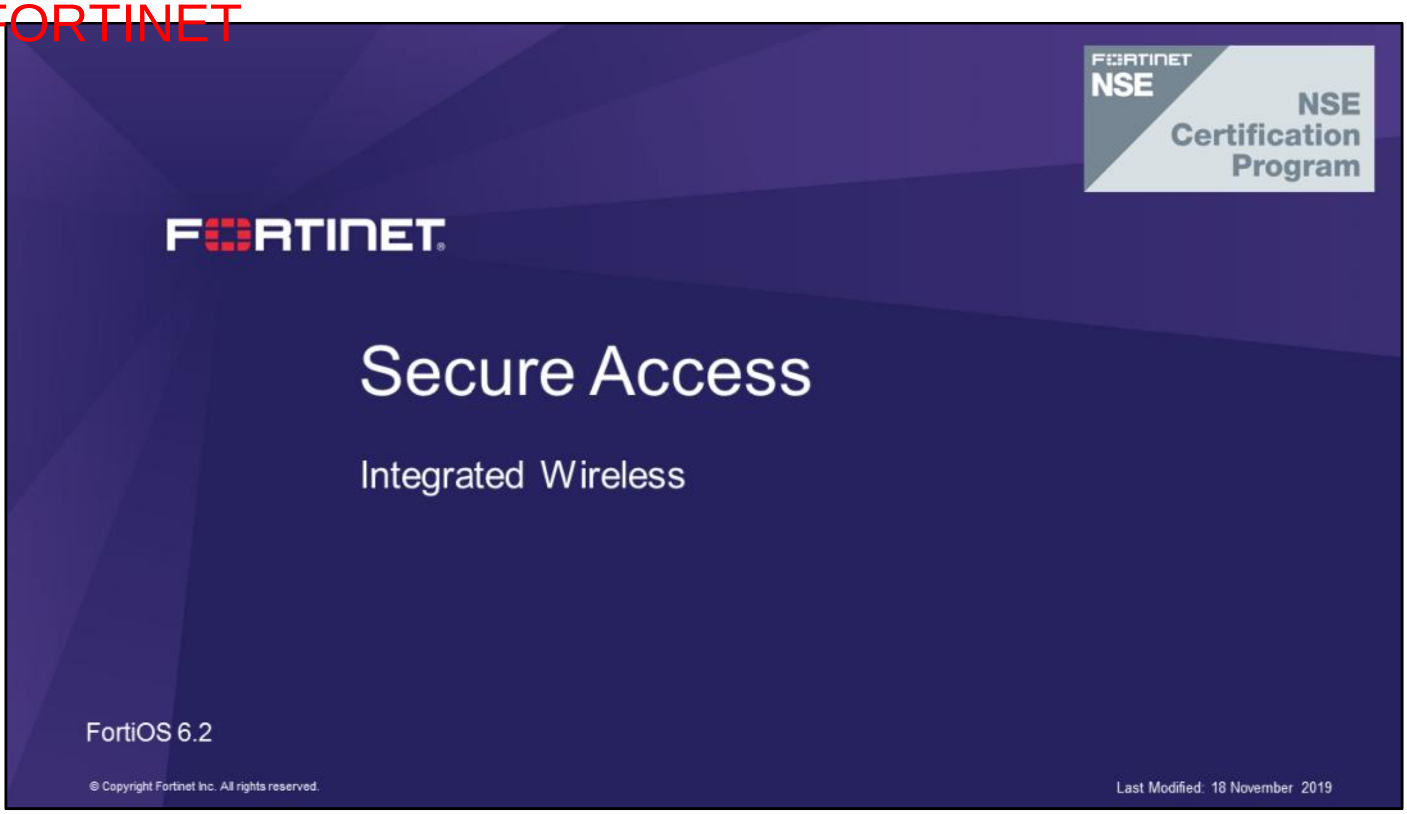
STP misconfiguration, network loops, faulty network cards, and attacks can cause Layer 2 storms.



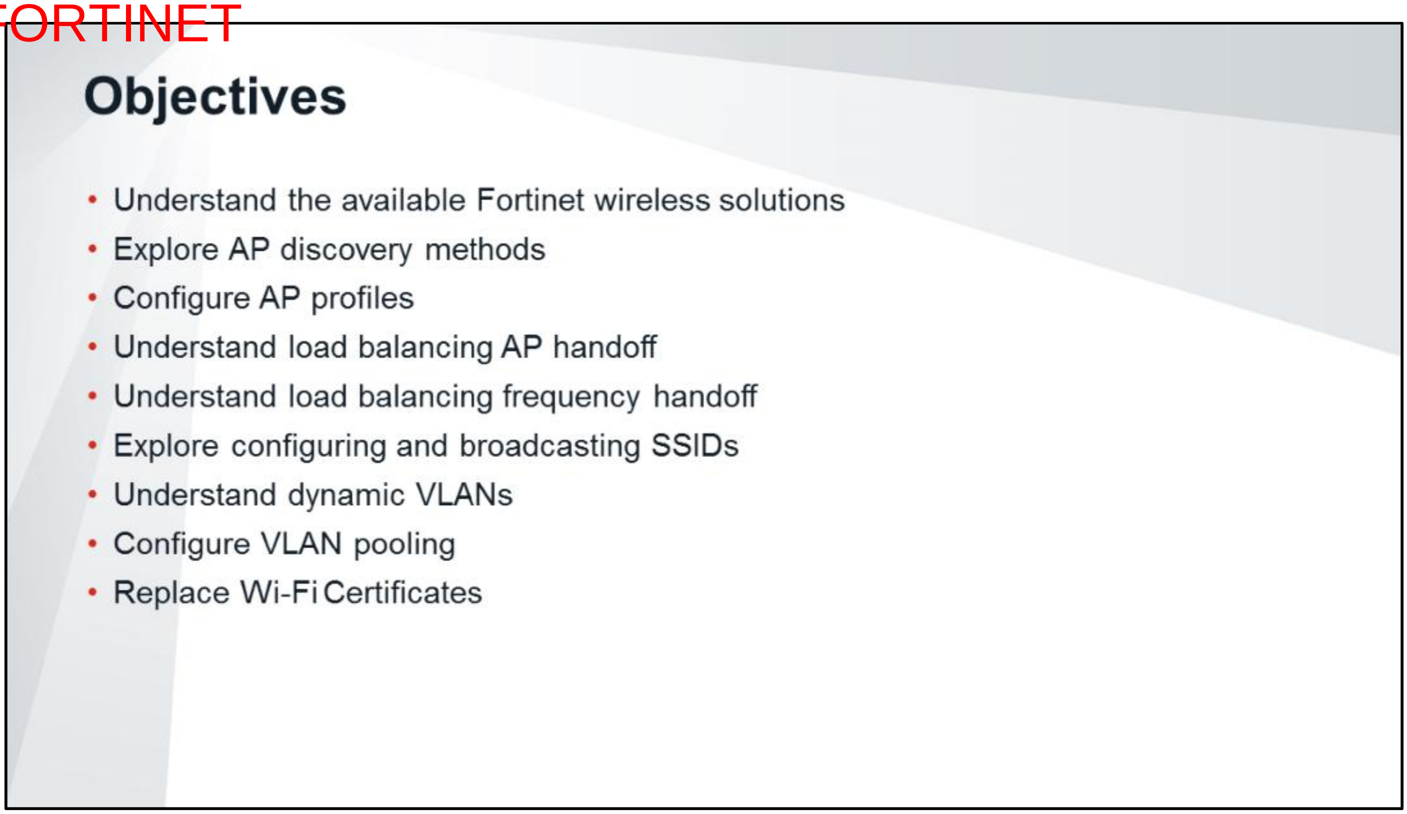
FortiSwitch has a mechanism, called storm control, for detecting and blocking Layer 2 storms. You enable storm control by configuring a maximum rate at either the global or switch level. You can apply this rate to unknown unicast, unknown multicast, and broadcast traffic. When the traffic exceeds the specified threshold, storm control drops the exceeded traffic



This slide shows the objectives that you covered in this lesson. By mastering the objectives covered in this lesson, you learned how to configure the additional features that secure Layer 2.



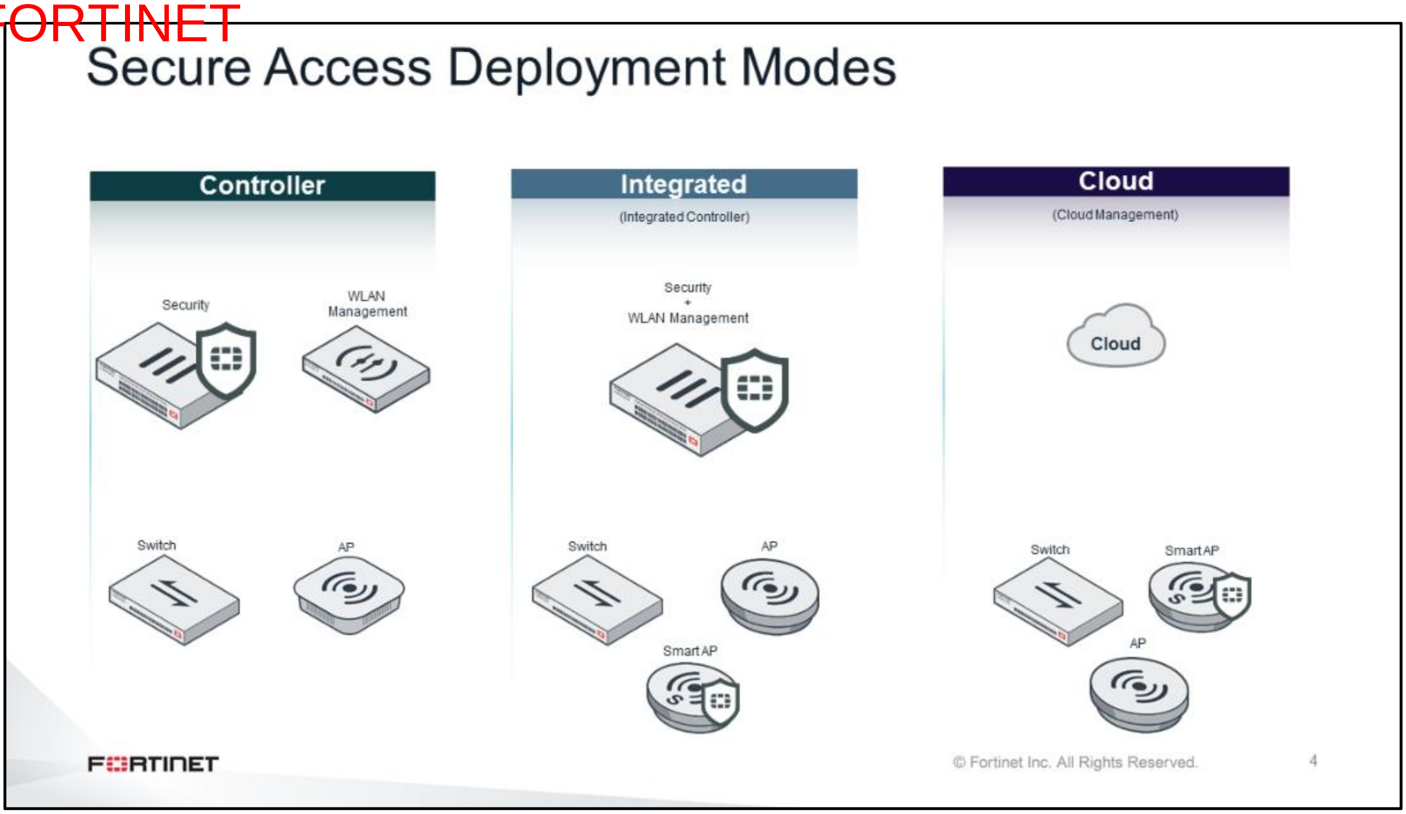
In this lesson, you will learn how to configure and use integrated wireless features on FortiOS.



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

Wireless Solutions

In this section, you will learn about Fortinet's secure access wireless offering.



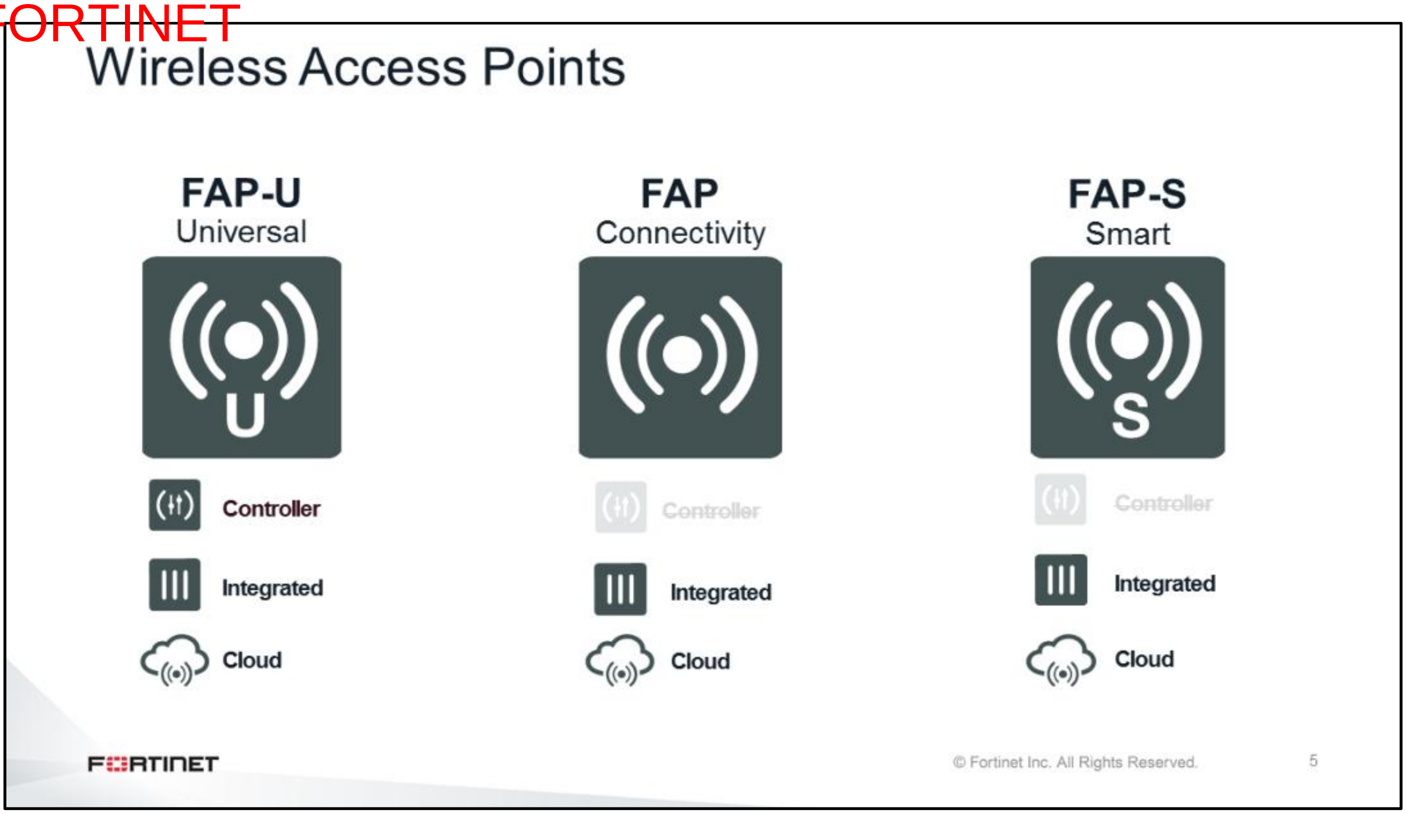
Fortinet offers multiple deployment solutions for secure wireless.

Controller solutions consist of FortiWireless Controllers (FortiWLCs) FortiWLCs are dedicated devices used only as the wireless controller for universal series APs.

The integrated solution uses the FortiOS integrated wireless controller, which is available on all FortiGate devices, including VMs.

Fortinet devices can also manage FortiAPs using the FortiCloud management features. In this deployment mode, you use Fortinet's cloud-based service for management and configuration.

In this lesson, you will learn about the integrated wireless solution only.

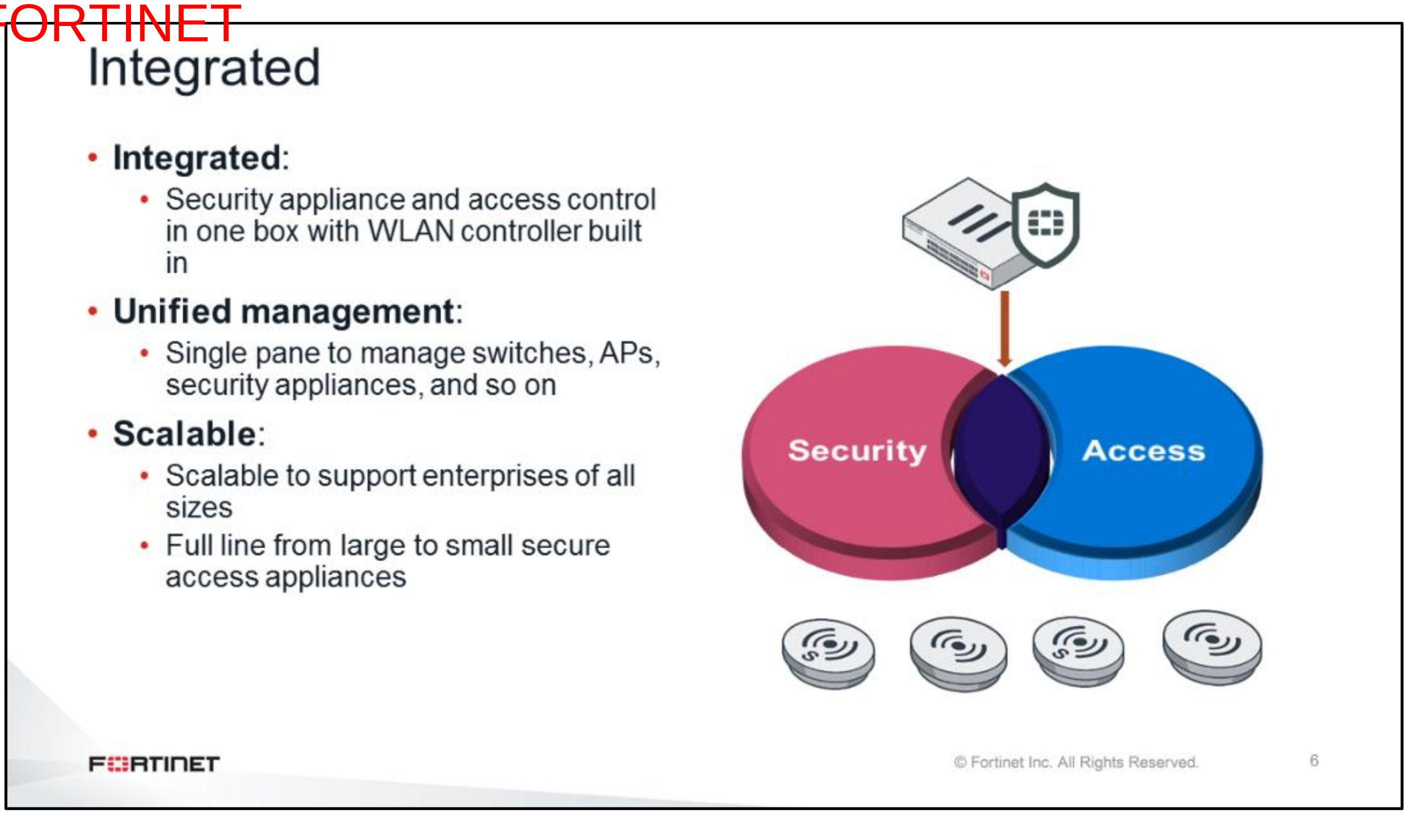


It is important to note that not all FortiAP models support all wireless deployment modes. When choosing a FortiAP for your deployment, make sure to select the model that works well for your network.

FortiAP-U (Universal) models work with all types of deployment modes, including FortiWLC. FortiAP-U models provide the flexibility to automatically and manually connect to all Fortinet management platforms. You can choose to redeploy an access point (AP) to any Fortinet wireless deployment.

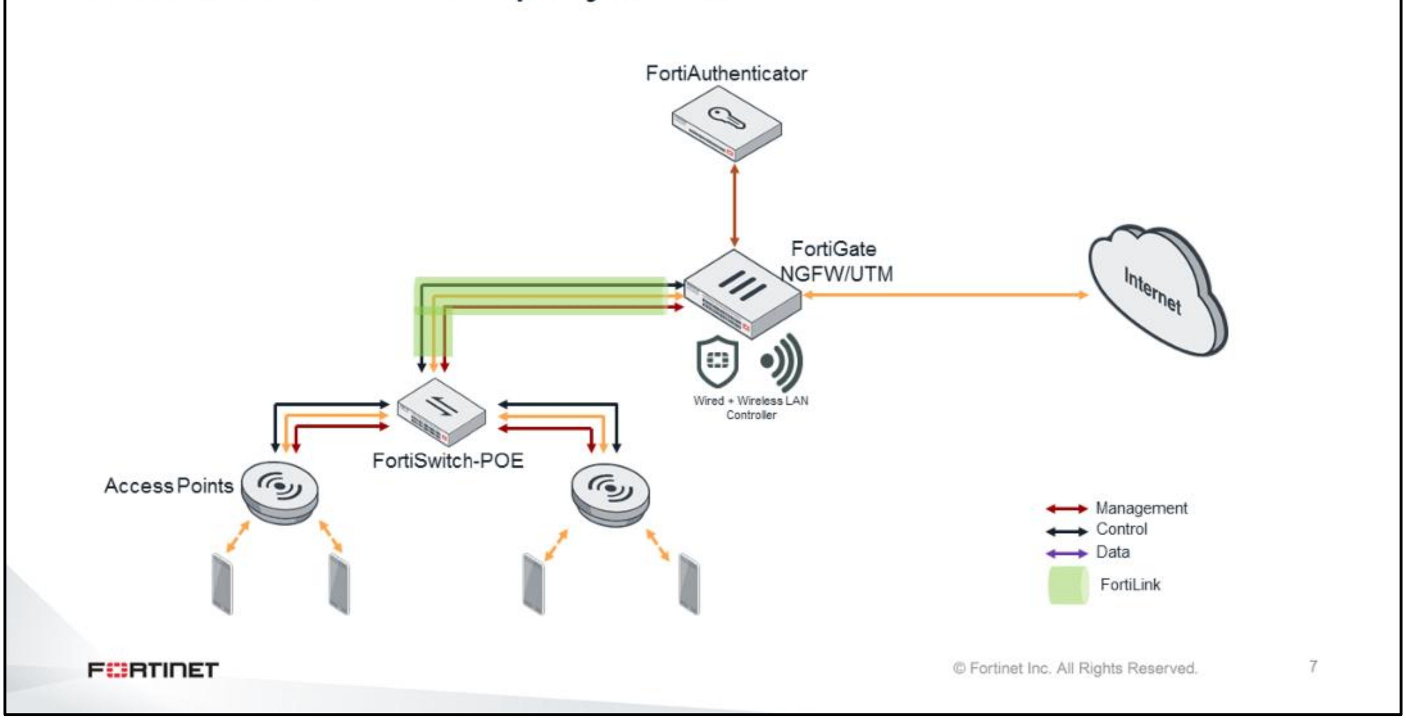
The FortiAP-C (Connectivity) series are cloud-managed and FortiGate-managed APs offering zero-touch provisioning to support enterprises with remote sites requiring basic wireless LAN connectivity. FortiAP series models support two types of deployment modes: integrated (FortiGate) and FortiCloud deployments.

The FortiAP-S (Smart) series is a family of single and dual-radio 802.11ac APs designed for deployment in small and medium business (SMBs) and distributed enterprise sites. They contain advanced security functions embedded in the AP hardware. Equipped with extra memory and twice the processing power of typical thin APs, they can perform real-time security processing at the network edge, not in the cloud or on the corporate LAN.



Fortinet's Integrated Wireless solution provides single-pane-of-glass management for security and access. The Integrated Wireless solution includes the FortiGate network security platform, FortiAP access points, and centralized management. FortiGate consolidates WLAN control, firewall, VPN gateway, network IPS, DLP, malware protection, web filtering, application control, and endpoint control in a single device.

Secure Access Deployment



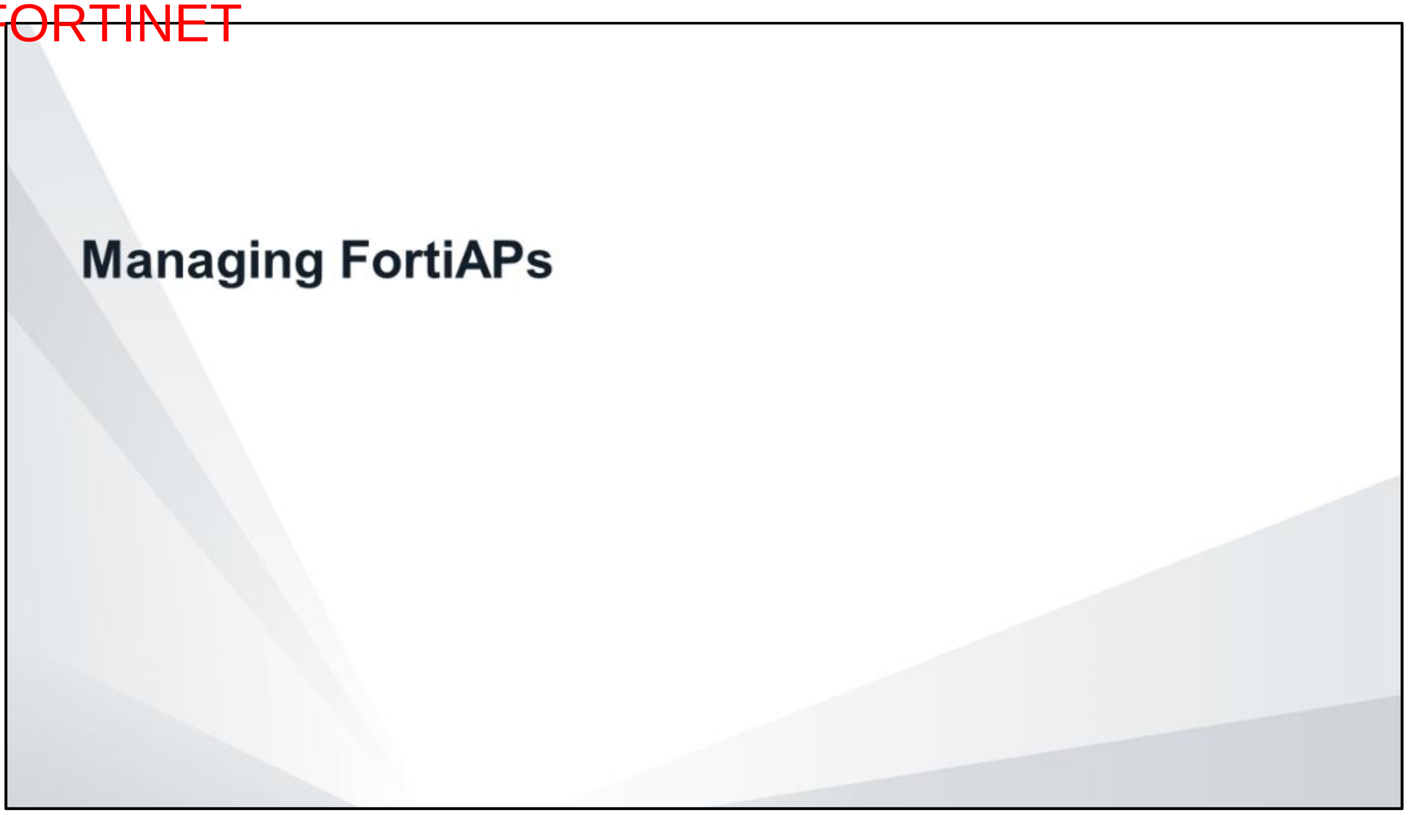
Fortinet's Secure Access solution includes APs, switches, and a firewall. This slide shows a high-level deployment diagram.

In the example shown on this slide, the FortiAPs are connected to a power over Ethernet (PoE) FortiSwitch. That switch then connects to a FortiGate firewall, using a FortiLink connection, which effectively integrates all switch management and configuration functions into the FortiGate management interface.

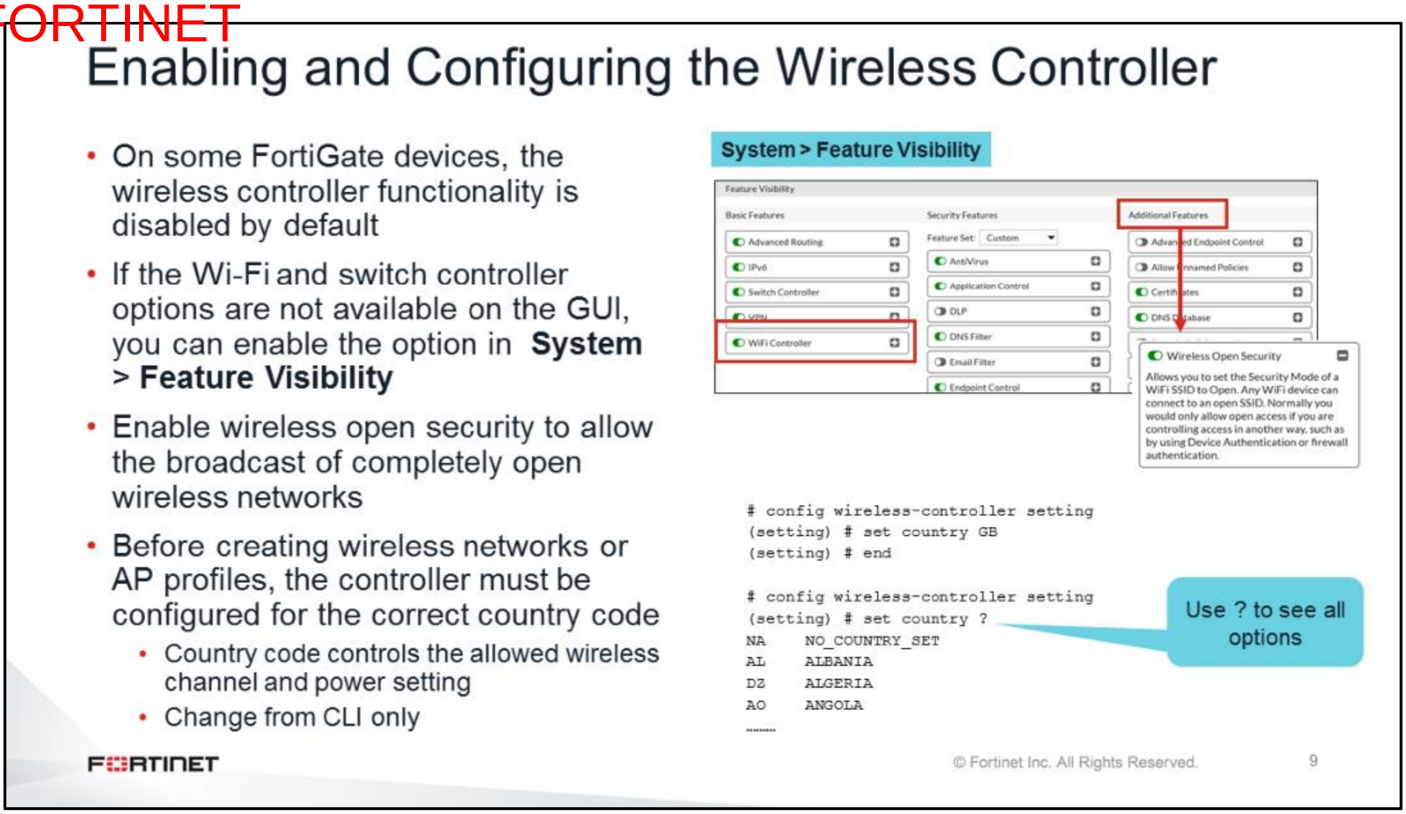
The traffic flow is straightforward. The AP management traffic goes directly to FortiGate. The user or device access path goes to the switch and then to FortiGate. User traffic is monitored and secured on the AP, sent through the switch, through the firewall, and out to the Internet or other destination.

The following is a list of traffic types and their purpose:

- Management=HTTP, SSH and so on. This is used when directly managing the AP.
- Control=CAPWAP control. This is used by the controller to configure, manage and update the AP.
- Data=user traffic. This is the traffic that is sent by the wireless clients to the rest of the network.



In this section, you will learn how to provision and manage FortiAPs using the FortiGate Integrated Wireless Controller.



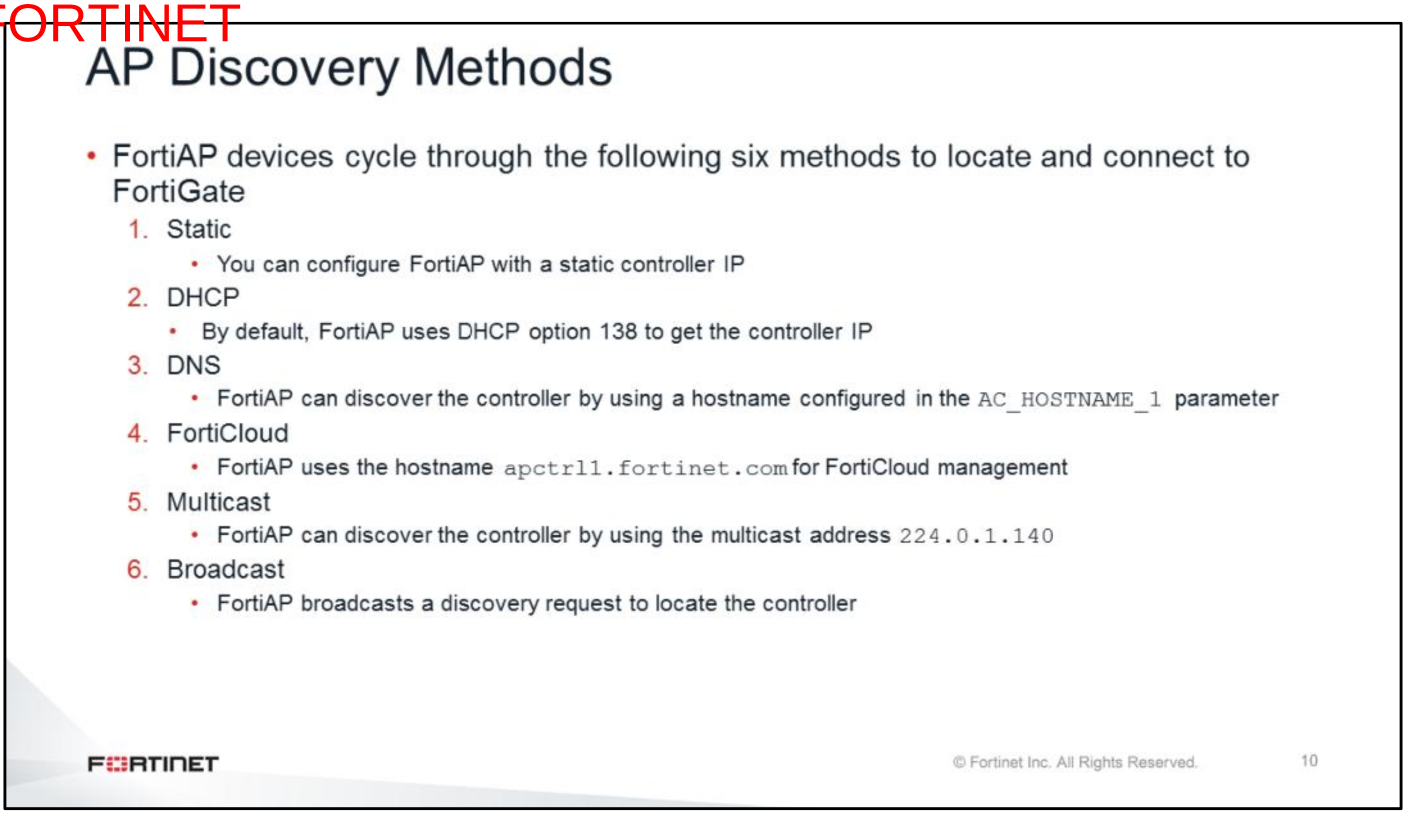
Before starting to install and configure APs, you may need to perform some prerequisite configuration.

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.

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 option will not be shown.

When configuring wireless AP radio settings, 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 control assessing *before* creating any AP profiles or adding any APs.

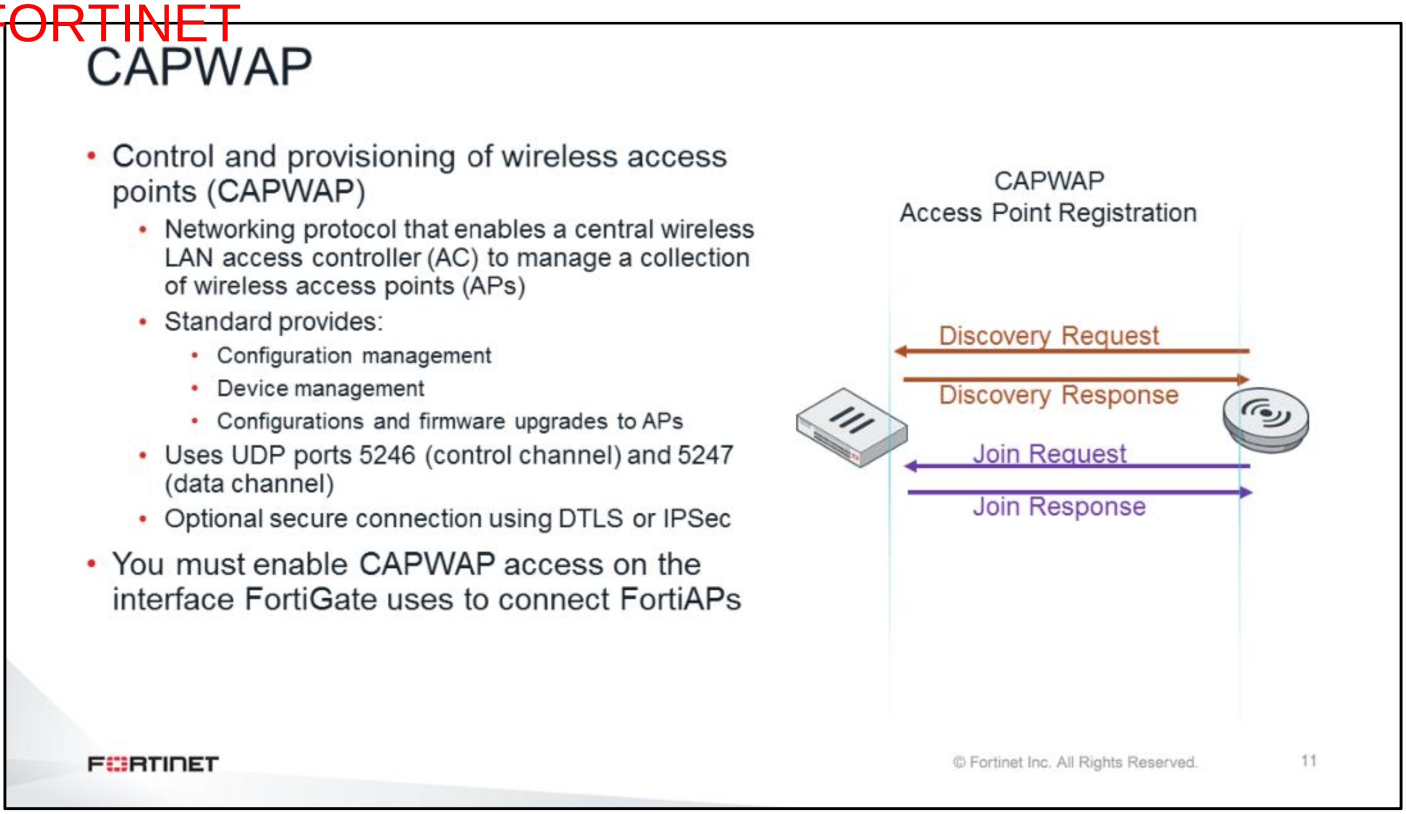
You can configure the regulatory domain in the CLI using the `set country` command followed by a country code. If you're not sure of the country code, you can use the ? Option to view the full list of country codes.



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 startup 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 properly 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 to the AP.



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 , and manage the device, and push firmware upgrades to FortiAPs.

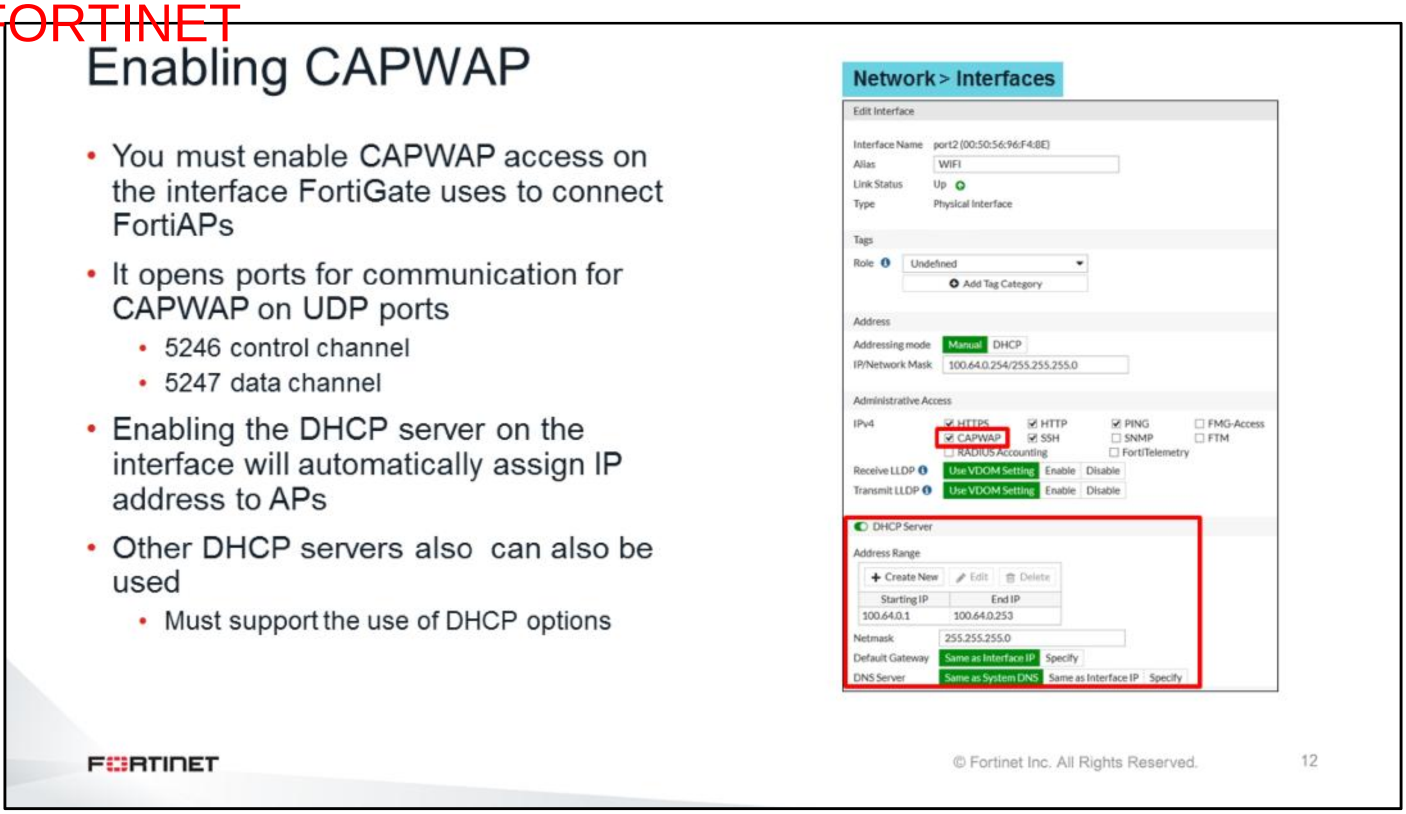
CAPWAP uses UDP port 5246 as the control channel and 5247 as the data channel.

CAPWAP enabled devices can optionally create a secure data channel to controller using DTLS encryption or IPSEC. Using IPSEC will benefit FortiGates that can offload CAPWAP to hardware resulting an greatly increased performance. DTLS encrypted CAPWAP *cannot* be offloaded. Where APs are located in a LAN, data plane 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 CPU. IPSec performance can be far greater if the 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. FortiAPs send a discovery request. FortiGate responds with a discovery response.
2. Both devices establish a secure DTLS session.
3. After FortiGate authorizes the FortiAP, the CAPWAP discovery and join phase takes place.
4. After the CAPWAP tunnel is established, FortiGate sends all required management and WLAN-related configuration to FortiAP.



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.

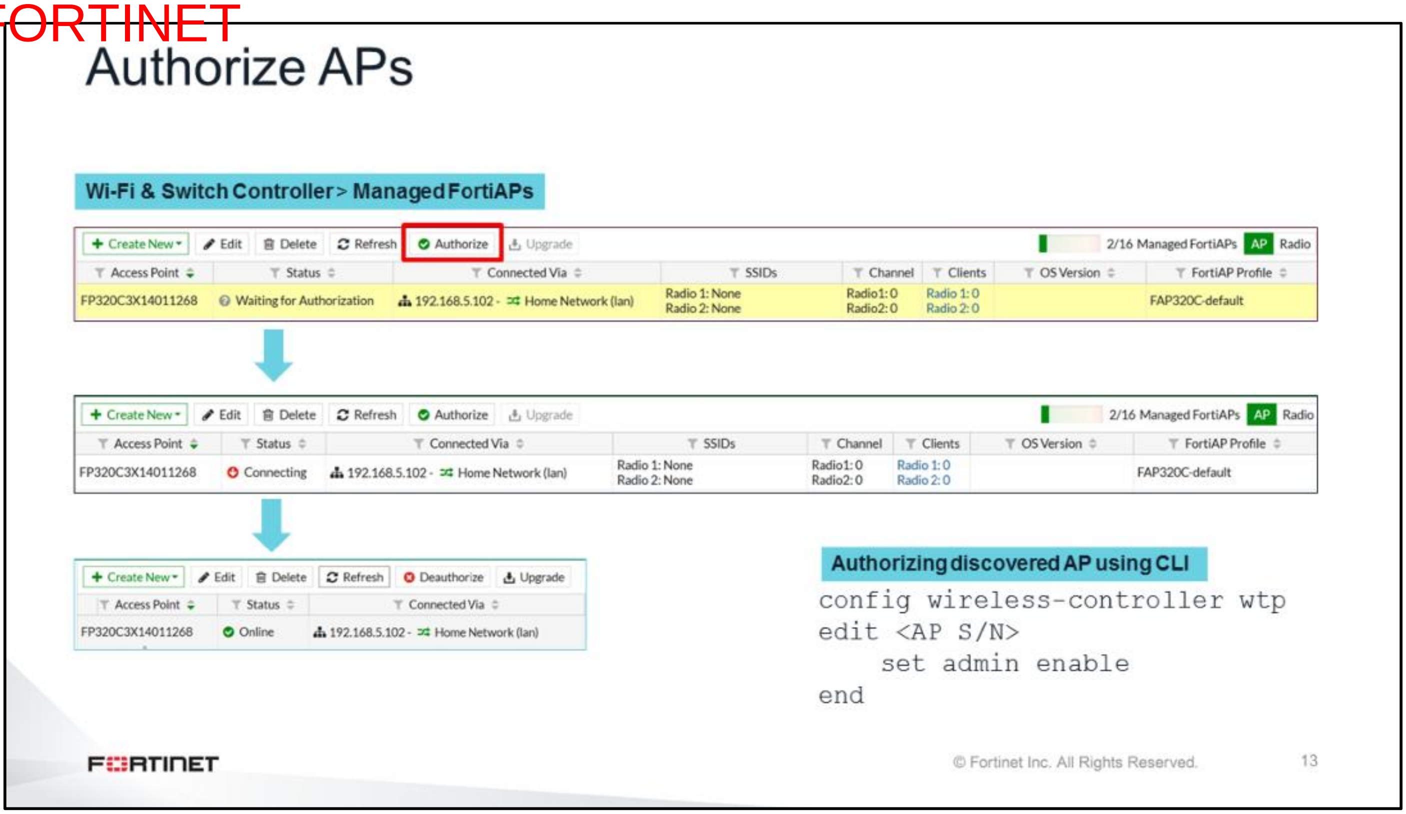
If required, enable the DHCP server option to allow the FortiGate to assign IP addresses to FortiAPs.

On the CLI, you can limit the IP assignment to *only* FortiAPs by matching the `FortiAP` VCI string, as follows:

```
config system dhcp server
  set vci-match enable
  set vci-string "FortiAP"
end
```

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.

This will save you from manually configuring the IP address on each AP.



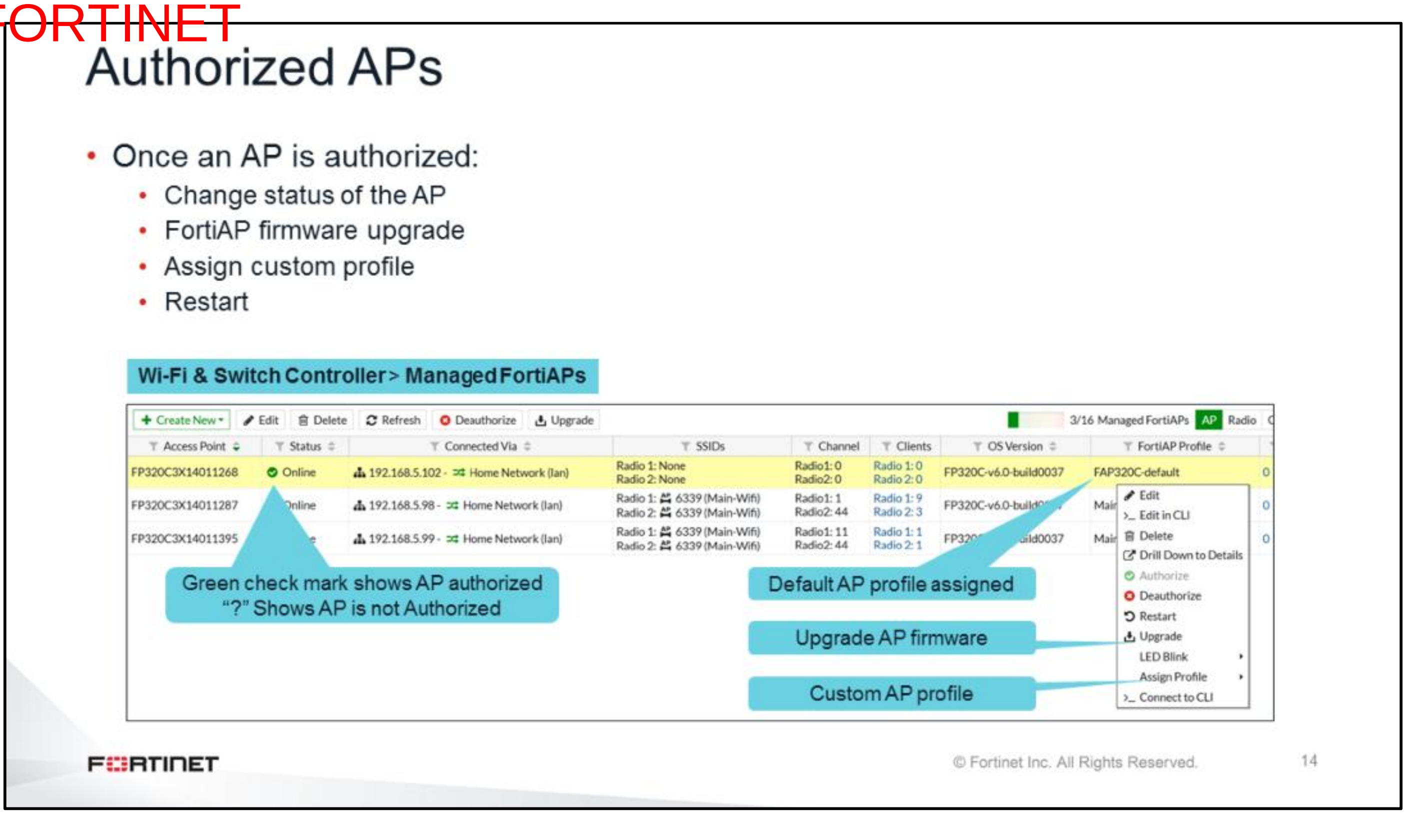
After you have configured the appropriate discovery method (if configuration is required), and you have enabled CAPWAP, you can turn the AP and it will begin trying to discover the controller. To view the new AP, click the **Wi-Fi and Switch Controller** > **Managed FortiAPs**. If the newly added AP is not visible, click the **Refresh**.

After the 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.

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

You can also authorize discovered APs using the FortiGate CLI. However, you must authorize the APs one-by-one, using the following commands:

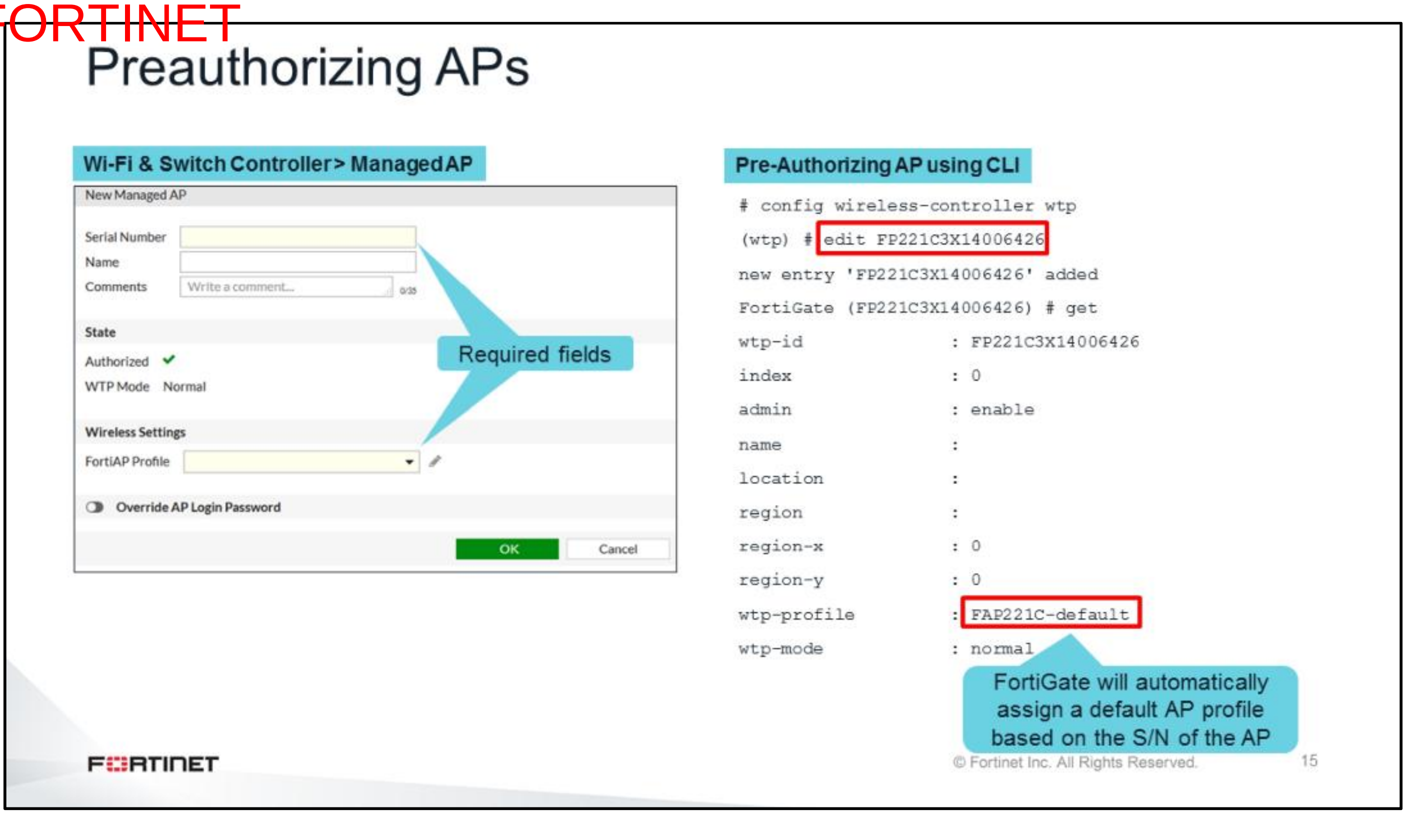
```
config wireless-controller wtp
edit <AP S/N>
    set admin enable
end
```



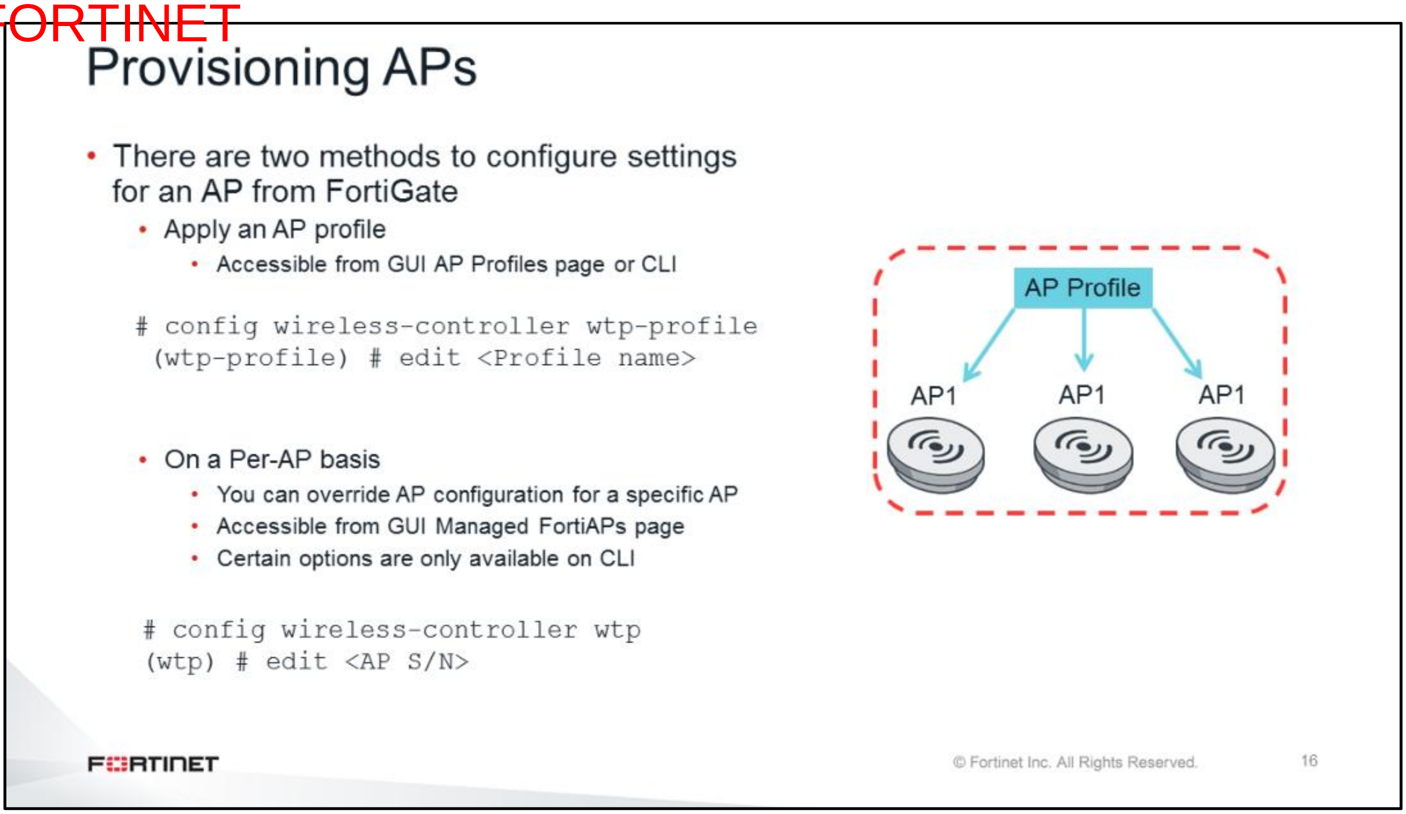
Once an AP is authorized, you can perform various tasks using the FortiGate GUI. On the **Managed FortiAPs** page, you can:

- Change the status of an AP (authorized to deauthorized)
- Perform AP firmware upgrade
- Change assigned AP profile
- Restart FortiAP
- Telnet to FortiAP CLI to execute commands directly on the AP

You might also see the message "**A new Firmware version is available**". This indicates that the FortiAP version can be upgraded. You can right-click the FortiAP unit in the list and select **Upgrade Firmware.** FortiOS will automatically find the appropriate firmware for the AP and upgrade it. This option requires you to register FortiAP on the Fortinet support site and have a valid support contract.



FortiGate allows you to preauthorize FortiAPs that will be added to your network. You must add all FortiAPs manually, one-by-one, to FortiGate using the AP`s serial number. After the preauthorized FortiAPs come online and are discovered by FortiGate, FortiGate authorizes the FortiAPs automatically. FortiGate will establish a CAPWAP tunnel to the FortiAPs and push the configuration to them, based on the assigned AP profile.

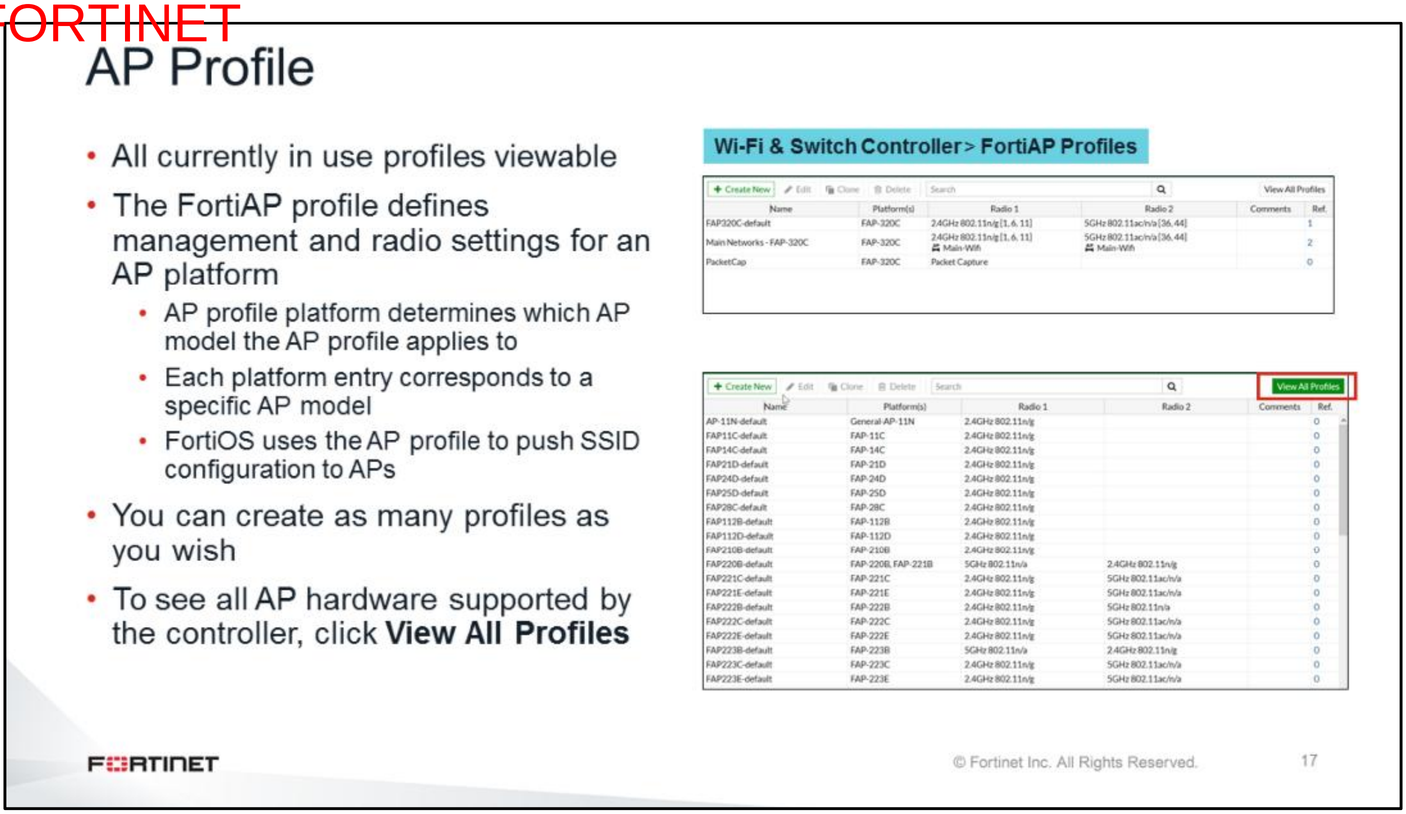


FortiGate automatically assigns a *default* AP profile to an AP when it is discovered and manually authorized. Once a CAPWAP tunnel is established between a FortiGate and an AP, the FortiGate uses the CAPWAP control channel to push all AP profile parameters to the AP.

You will likely want to assign an AP profile that is different to the assigned default, as 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 on a single AP. All APs that use the same AP profile will all receive the same set of configurations from the FortiGate.

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



To view and manage FortiAP profiles, click **Wi-Fi & Switch Controller** > **FortiAP Profiles.**

Only profiles are in use are shown. This includes the default profiles of any APs and profiles that have been created.

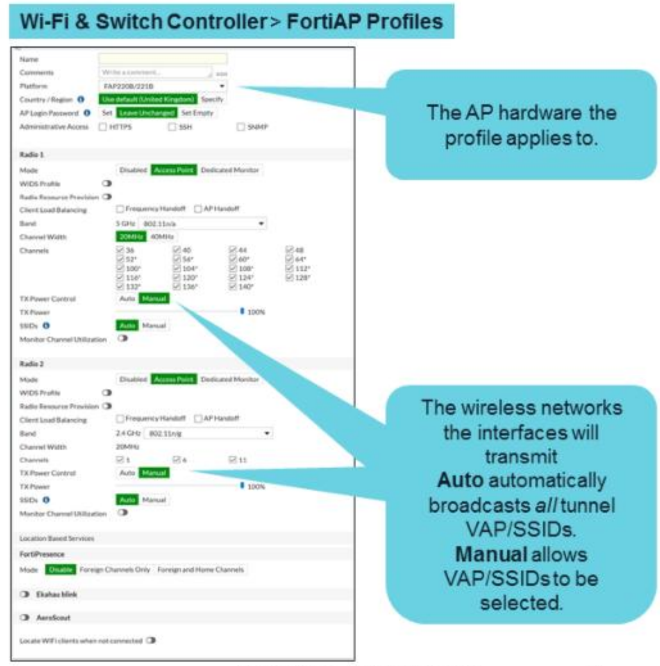
When an AP is assigned a profile, that profile controls the management and radio settings used for the channel setting, channel widths, transmission power level’s, and, wireless networks broadcast.

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. By default, you will not see all of the available default profiles, to see a complete list of profiles supported by the controller, click **View All Profile**. You will see default profiles for all currently supported AP types.

You can create multiple profiles by creating new ones or cloning existing. You can have multiple profiles for the same AP type, but each profile may specify slightly different configurations settings. When APs are no longer using a profile, you can delete the unused profile. Default system profiles cannot be deleted.

AP Profile

- Profiles allow the configuration of:
  - AP password
  - Administrative access to AP
- For each wireless interface
  - Allowed radio channels
  - Allowed radio power
  - SSIDs that will be broadcast
- The number and types of settings will generally vary depending on the AP platform
  - Some APs will only have a single radio
  - Some APs will have different channels available, depending on the country setting



FORTINET

 18

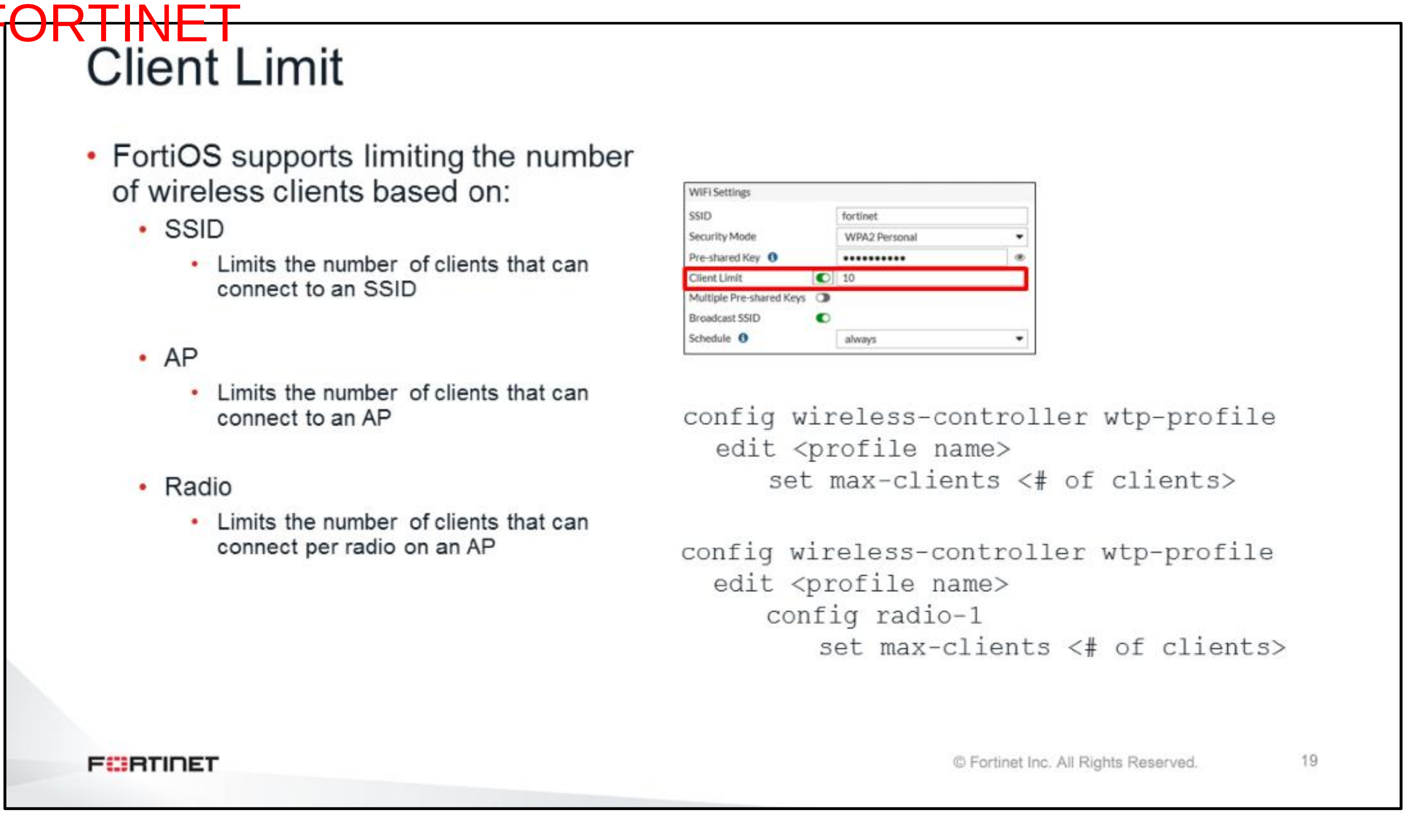
AP profiles control the various configuration options for access points and their radios.

Because the different AP models have different capabilities, one profile type can not control all of the different AP models. Each profile will have different options depending on the capability, type and numbers of the radios.

The AP profile is where you will decide which channels and power levels the AP will use when it is assigned the AP profile. It also controls which wireless networks are broadcast on which wireless interfaces. For instance, it will be possible to broadcast a network *only* on the 5 GHz interface by configuring it only on the radio interface 2.

When the default **Auto** setting is selected, any *existing* tunnel mode VAPs/SSIDs are automatically broadcast by this profile and any tunnel mode VAPs/SSIDs created *after* the AP profile is created will also be broadcast. **Manual** gives full control over which precise VAPs/SSIDs are broadcast. The manual option is the only way to broadcast a bridge mode VAP/SSID.

Changes to a profile will apply to all APs that are assigned that profile, and be applied immediately.

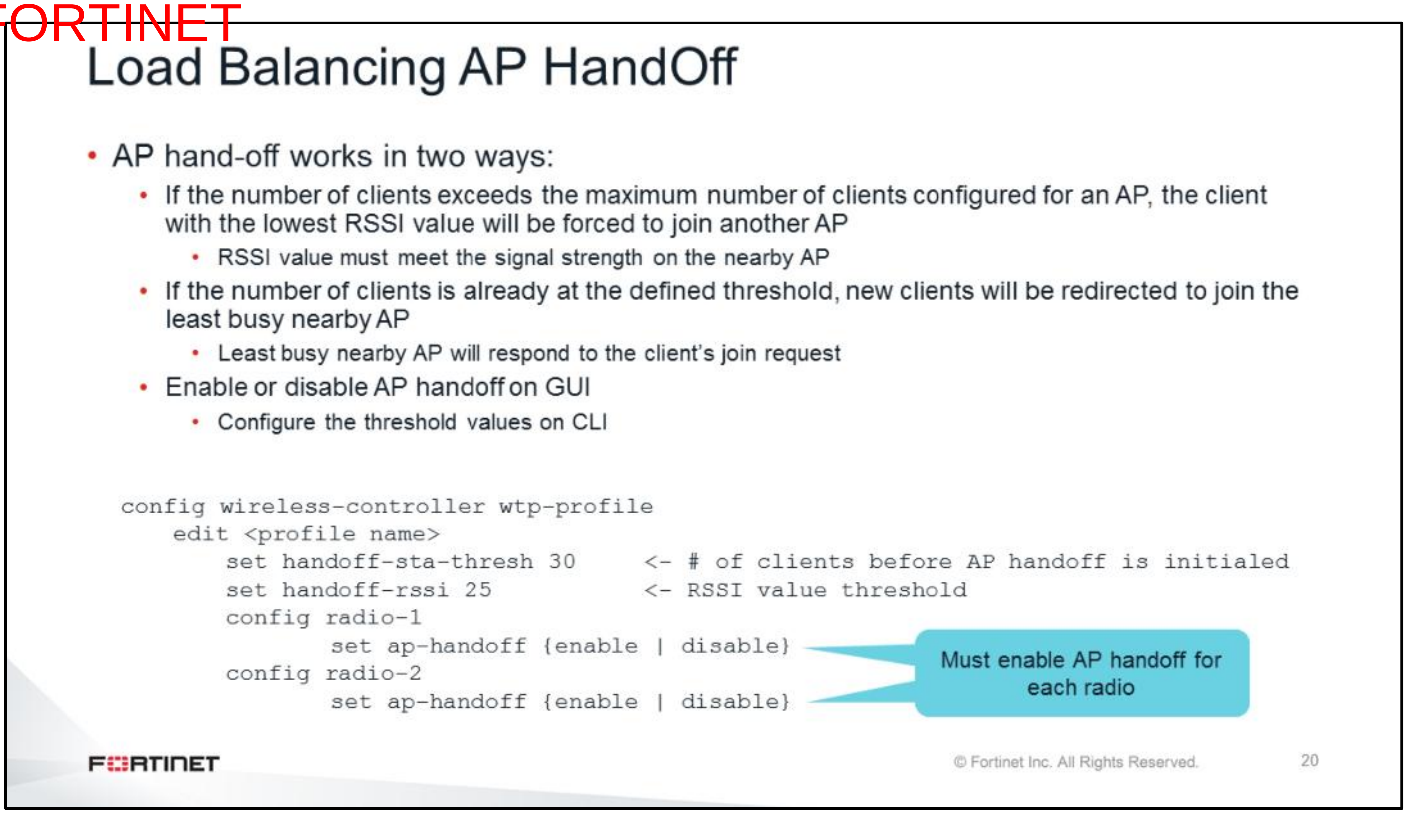


There are three ways to limit the number of clients that can connect to a wireless network. You can limit the number of clients that can connect to an SSID, or to an AP, or to a radio on an AP. Limiting the number of clients that are associated on a radio or an AP can help increase the performance and more efficiently load-balance wireless clients.

An SSID limits the number of clients that can connect to a wireless network, regardless of which AP they are on. The limit applies this to all APs that are broadcasting the SSID. You can apply the client limit for an SSID on the SSID configuration page on the GUI, or on the CLI in the `config wireless-controller vap` settings.

Limiting the number of clients that can associate with an AP or radio will affect all SSIDs that are being broadcast by the AP. It is important to note that some AP models have more radios than others and can handle more traffic. When limiting the number of clients for an AP keep that in mind and make the adjustments accordingly.

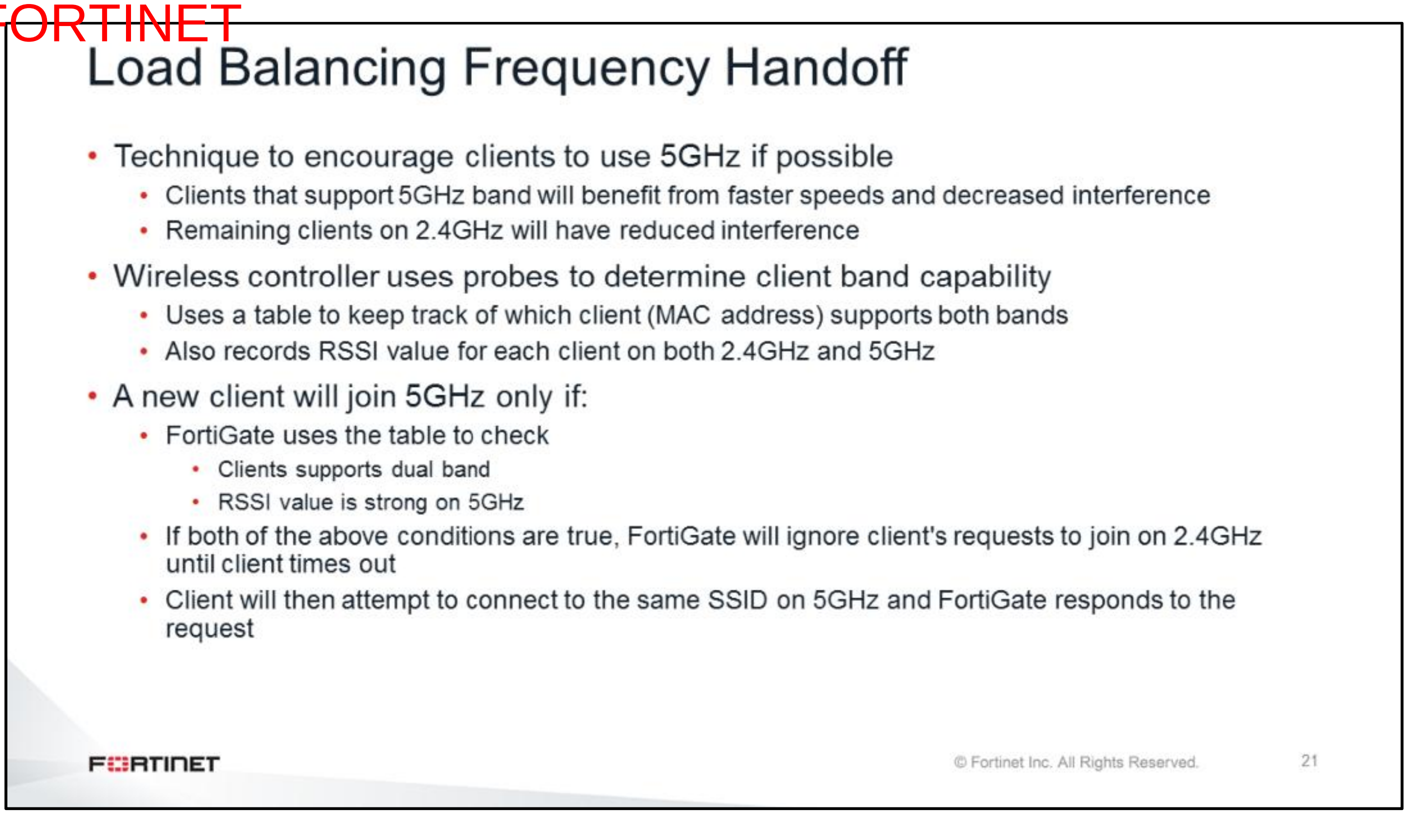
If an AP has more than one radio, you must make the changes on all radios. Otherwise, the AP will enforce only the settings for a single radio and, as a result, you may see more clients associating with an AP. You must make this change in the AP profile configuration using the CLI on FortiGate.



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 hand off is a way of load balancing wireless clients among managed APs on FortiGate. If an AP is overloaded and the maximum number of clients is configured for an AP or radio, FortiGate will drop the client that has weakest signals and connect the client to a nearby AP.

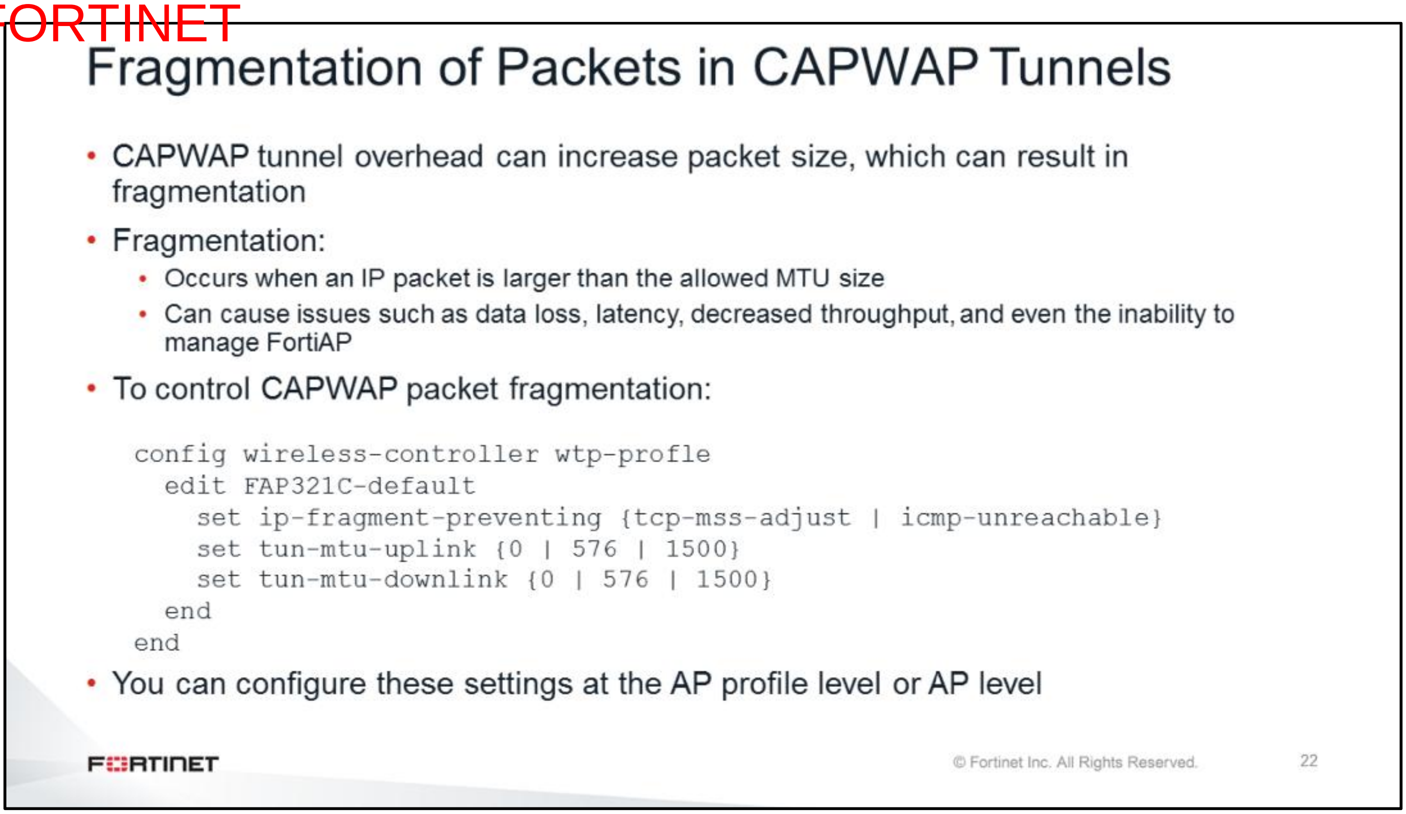
The RSSI value threshold defined in the AP profile is used when client tries to connect to the second AP. The client`s signal strength must be equal to or more than the defined RSSI value on the AP. Signal strength is determined based on the RSSI value–a higher RSSI value means better signal strength.

`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.



Frequency hand off is a band steering technique that FortiGate uses to encourage clients to use the 5GHz frequency instead of the 2.4GHz. Clients that support the 5GHz frequency benefit from faster speeds and decreased interference. This also benefits clients that do not support 5GHz, because there will be less interference on 2.4GHz because of the reduced number of clients. FortiGate continuously probes the clients to identify if they can operate on the 5GHz 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 5GHz and, if so, how good the signals are. If a client supports the 5GHz frequency and the signal is strong enough to connect, FortiGate will ignore the client’s requests to join the network on 2.4GHz until the request times out. The client will then automatically try to join the same network using 5GHz. FortiGate will instruct the AP to respond to the join request and allow the client to connect.



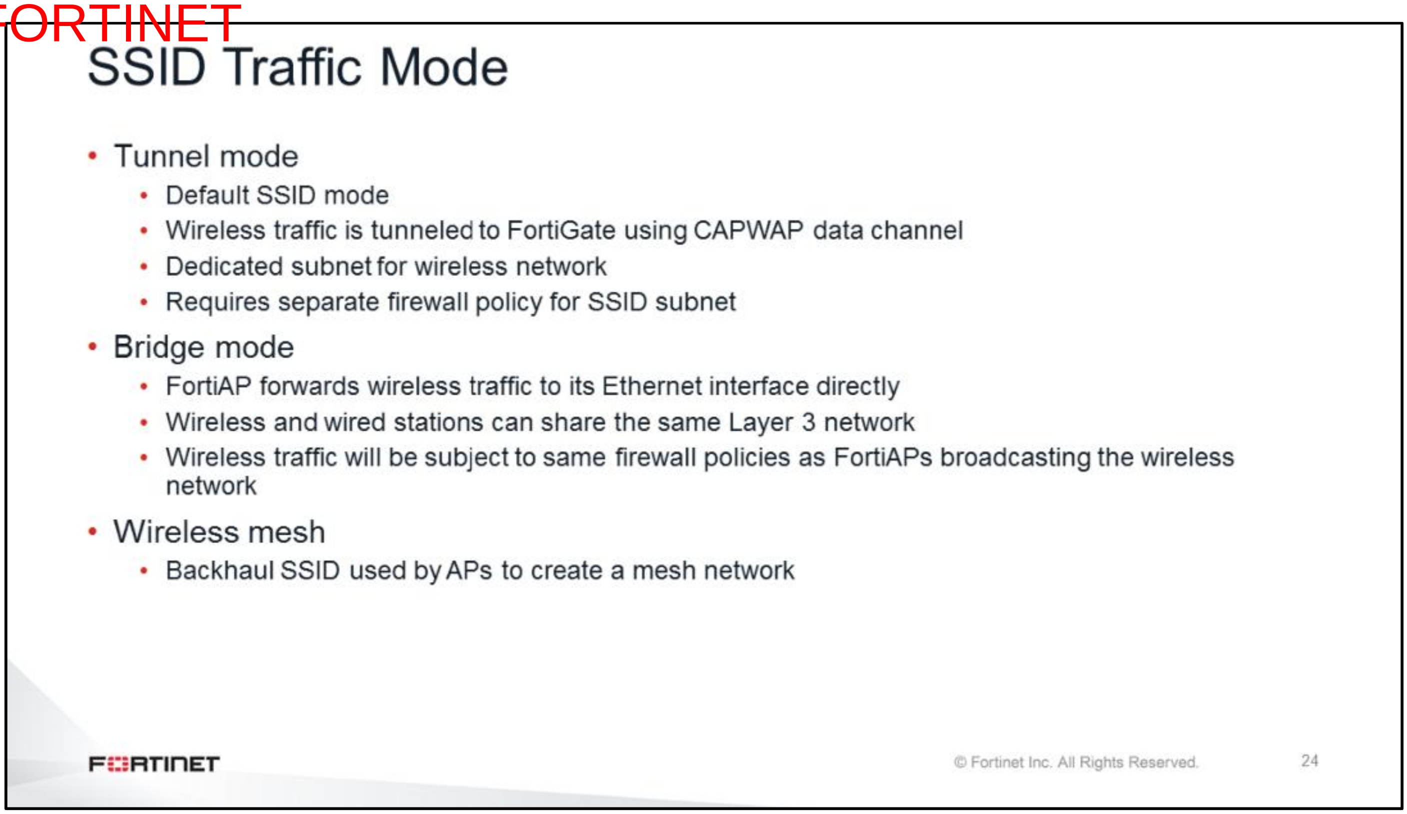
CAPWAP tunnel overhead can increase packet, size which can result in fragmentation. Fragmentation occurs when an IP packet is larger than the allowed MTU size. Fragmentation can cause issues such as data loss, latency, decreased throughput, and, in some cases the inability to manage FortiAPs.

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, instead of modifying it, using the AP profile.

In a LAN environment, fragmentation is not likely to be an issue due to the nature of the infrastructure. However, remote based APs could suffer fragmentation where different WAN link configurations are used in between the AP and the FortiGate.

SSIDs

In this section, you will learn how to configure and broadcast SSID on FortiOS.



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 the Internet.

There are two main advantages to using this mode:

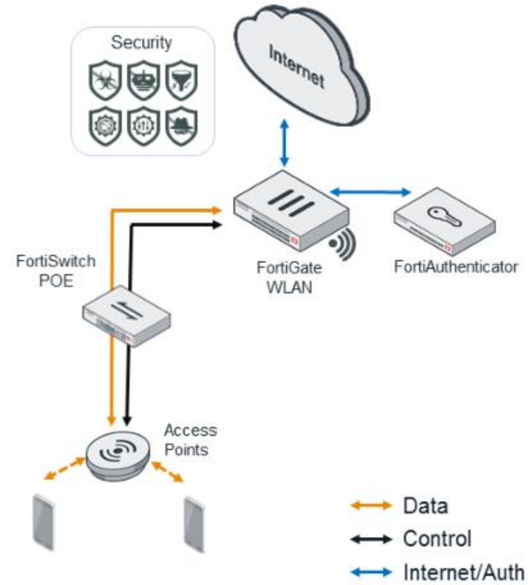
- Traffic is subject to firewall policies and security threat scanning. Traffic must go through a security profiles inspection and firewall policies examination before it is placed on the egress interface. This ensures that all security threats are addressed before a device is given access to internal 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 smart-series 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.

Tunnel Mode

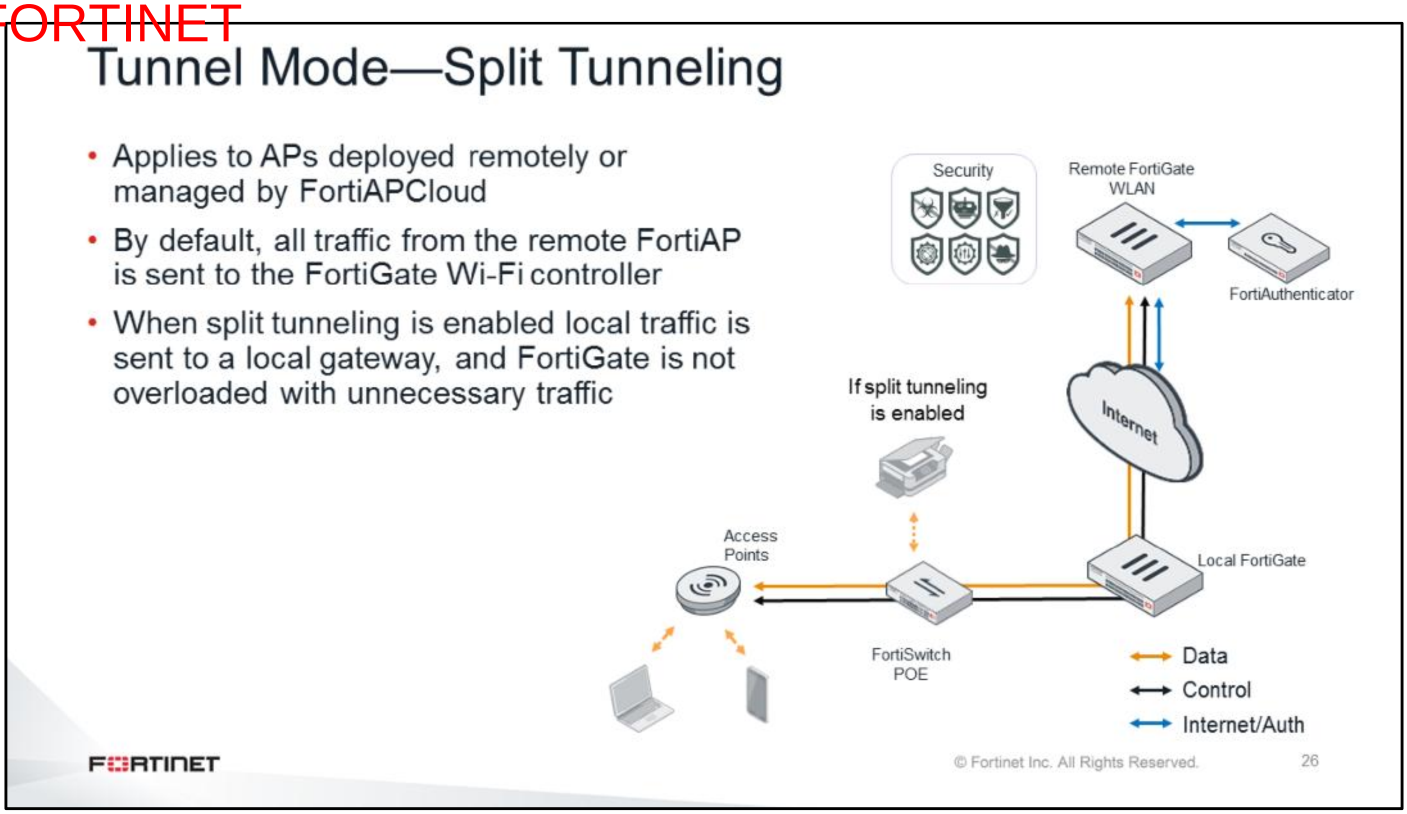
- **Pros**
  - Central place to enforce security
  - L3 traffic segmentation
- **Cons**
  - FortiGate must be sized according to traffic
  - If controller goes down, wireless network goes down



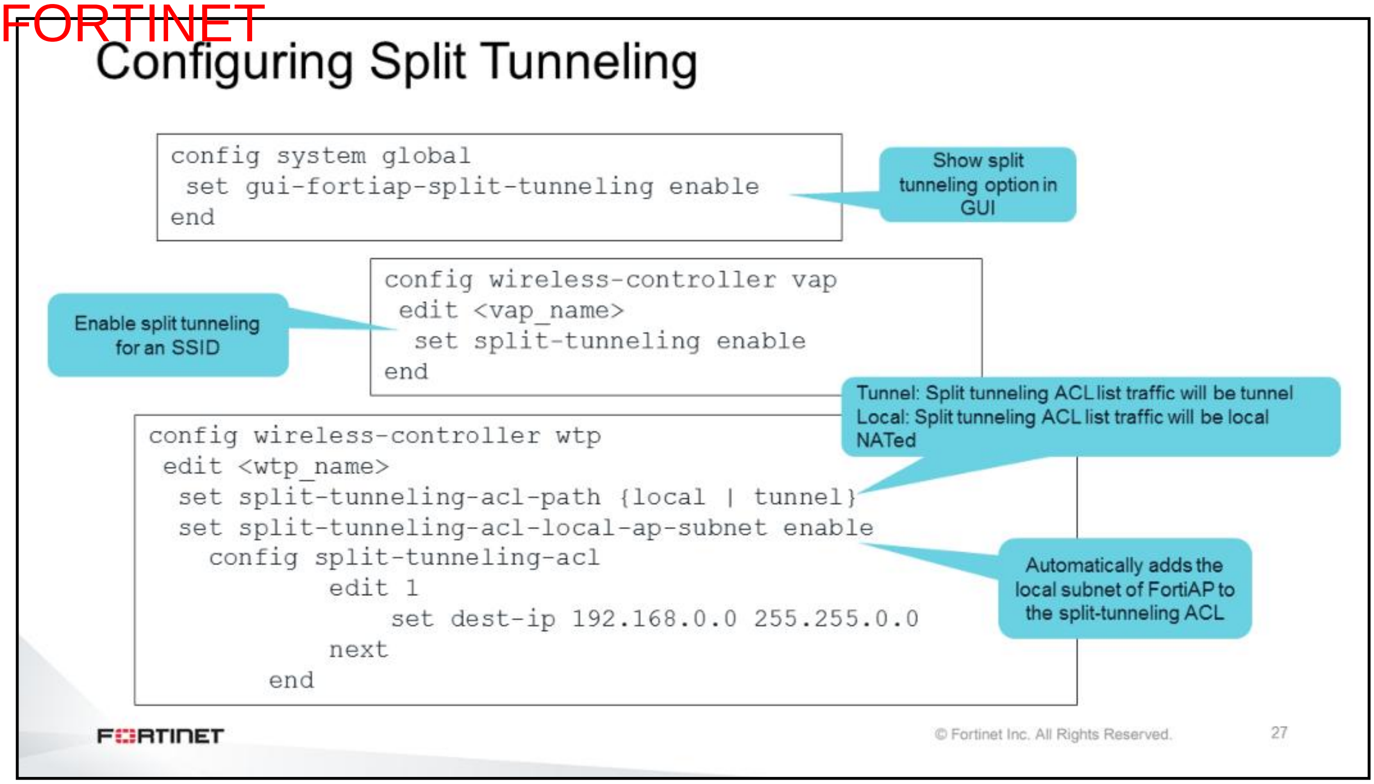
 25

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:

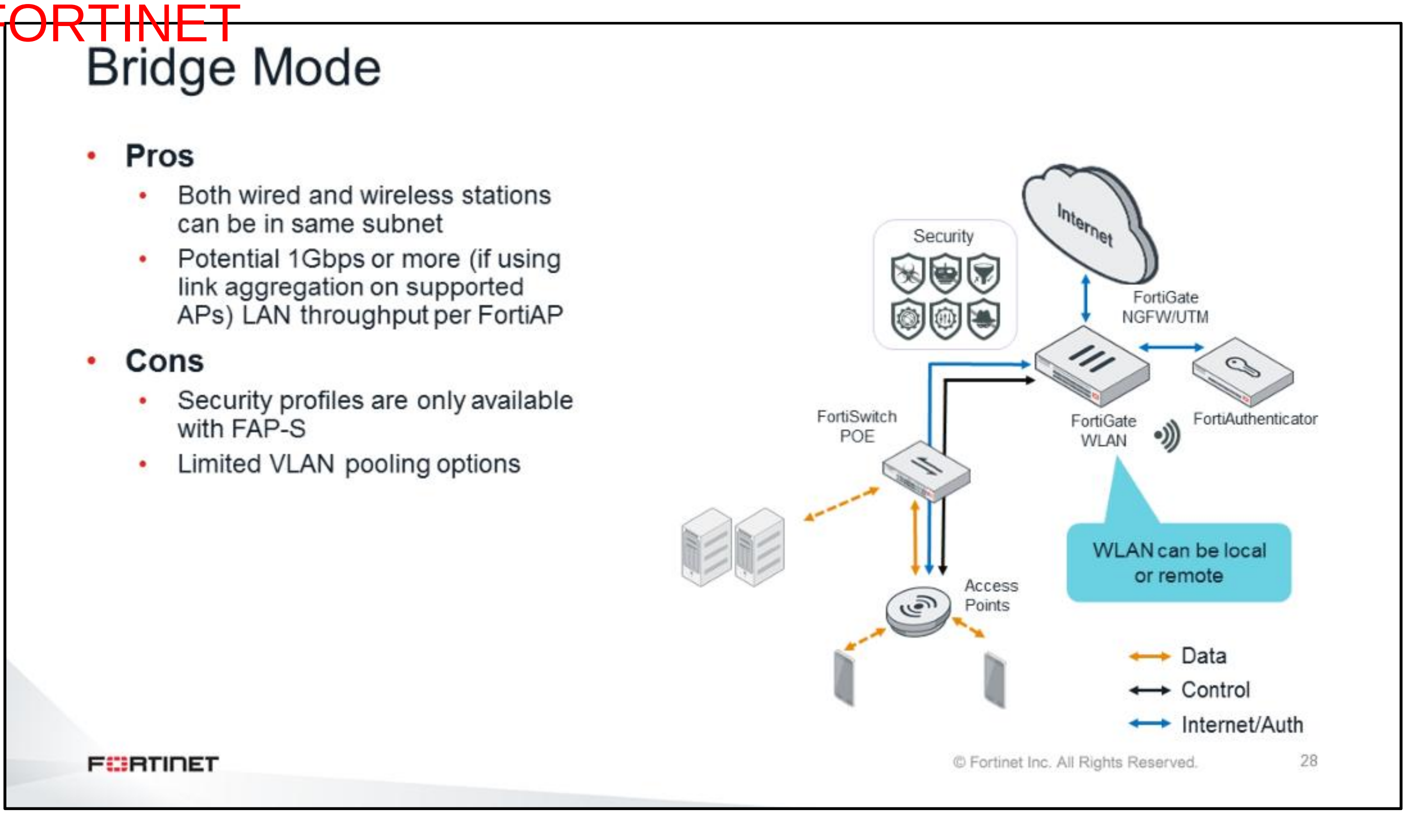
- Traffic is subject to firewall policies and security threat scanning. Traffic must go through a security profiles inspection and firewall policy examination before it is placed on the egress interface. This ensures that all security threats are addressed before a device is given access to internal 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.



By default, all traffic from the remote FortiAP is sent to the FortiGate Wi-Fi controller. If split tunneling is configured, only traffic destined for the corporate office networks is routed to FortiGate. Other general Internet traffic is routed, unencrypted, through the local gateway. Split tunneling eliminates loading the 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.



To enable split tunneling, you can use the CLI command shown on this slide. You can enable the option to show split tunneling on the GUI. 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. When `split-tunneling-acl-path` is set to `local`, you can define subnet(s) where traffic will remain 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.

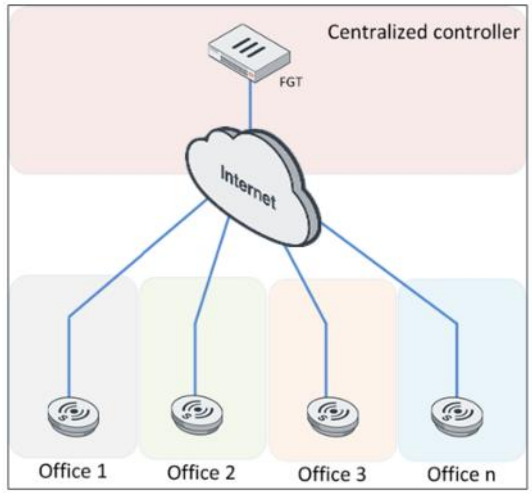


In local bridge mode SSID, wireless traffic is bridged directly to the local LAN that the AP is connected to. This mode is useful when deploying APs, at remote locations, that connect to a wireless controller over a WAN link. To ensure all traffic is scanned for security threats, consider deploying smart-series APs in this type of deployment.

Local traffic is switched at FortiSwitch, but CAPWAP control traffic still goes to the wireless controller.

Bridge Mode—Security Profile Support

- Only available in bridge mode deployments
- Available on FAP-S series APs
- Ideal for remote deployments
  - Can also be used in complex networks
- Supports FortiGate and FortiCloud deployments
- Supported profiles:
  - AV
  - IPS
  - Web filtering
  - App control
- Requires a separate FortiGuard subscription per AP



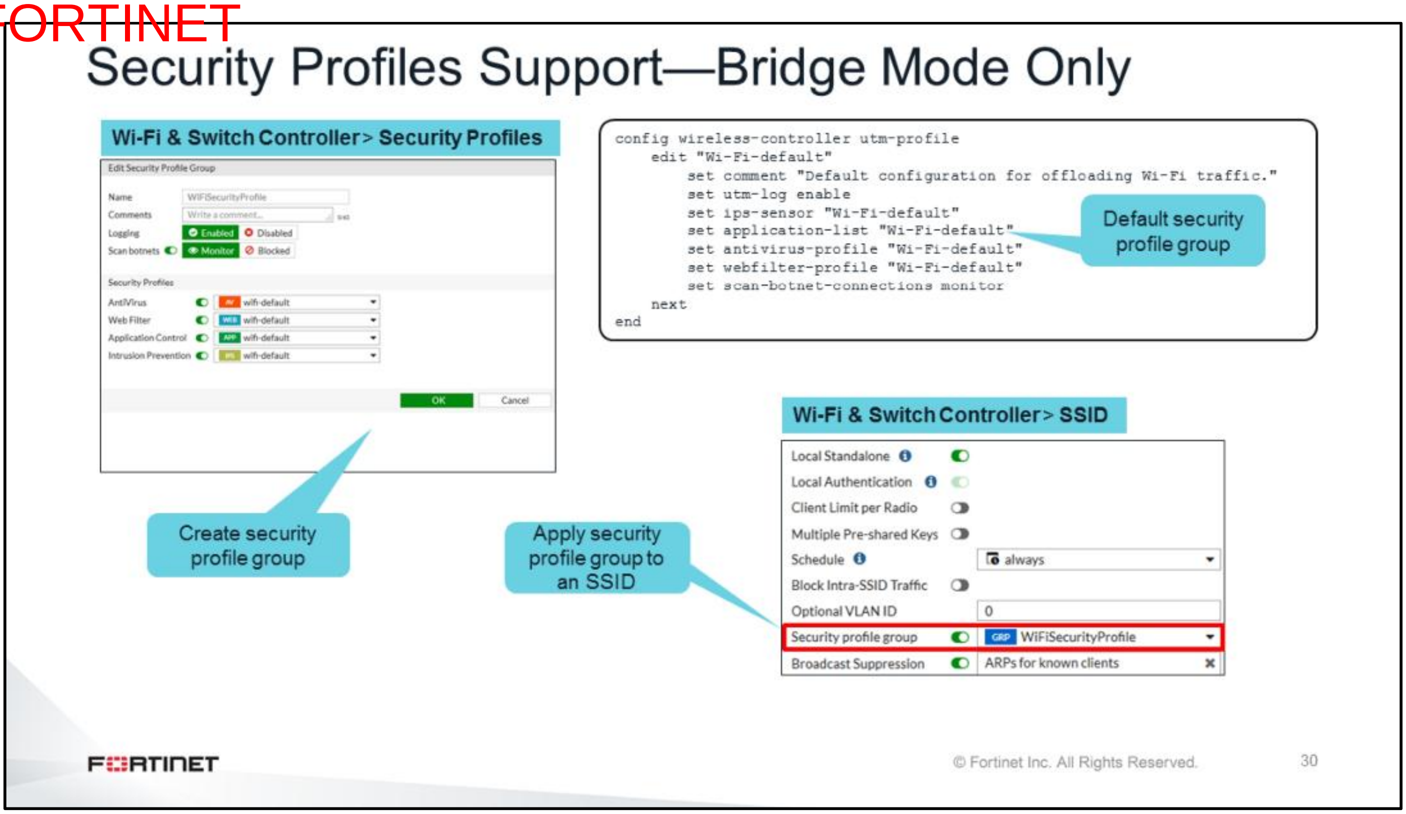
FORTINET

 29

If a bridge mode SSID is configured for a managed FortiAP-S (or smart FortiAP), 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:

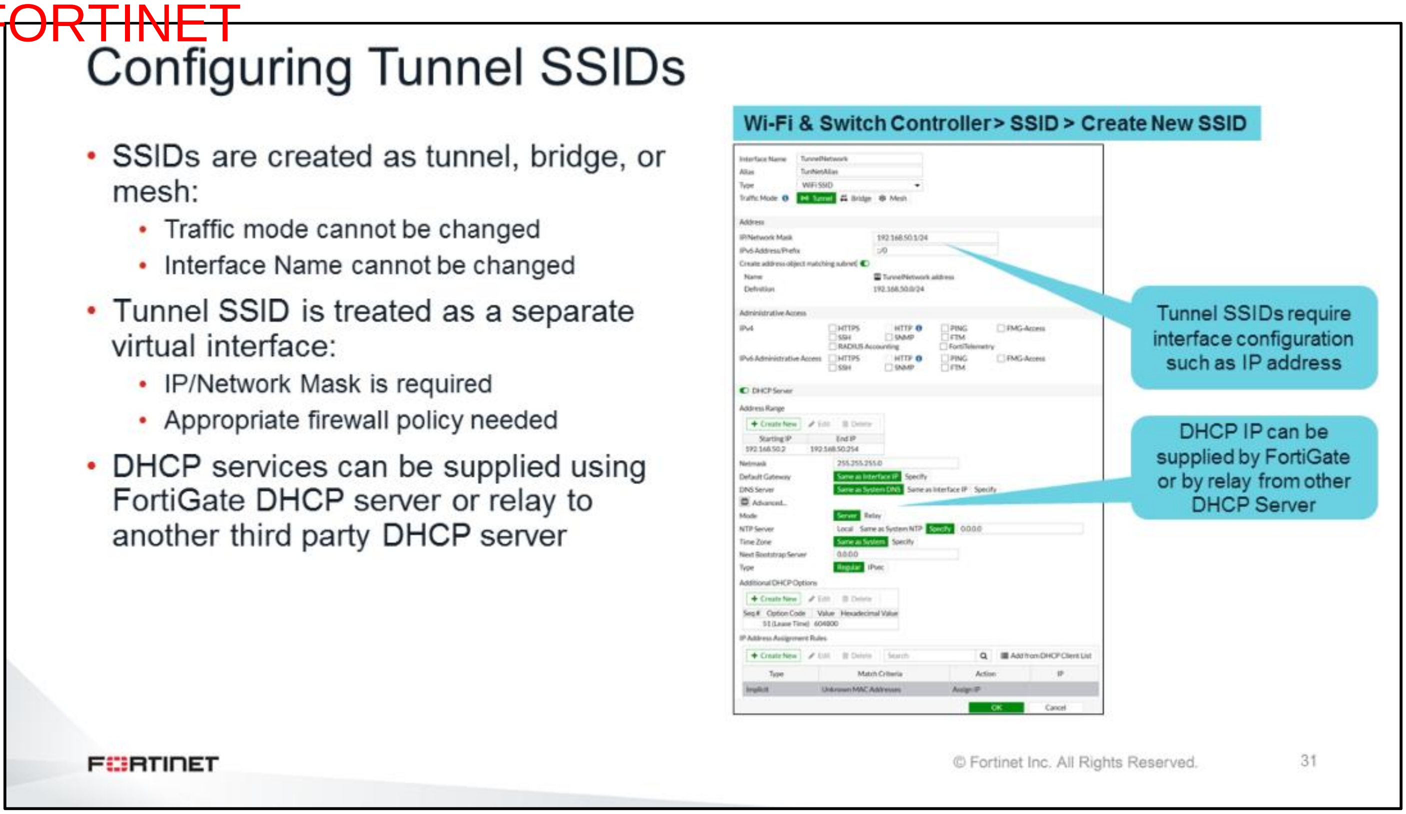
- Antivirus (including botnet protection)
- Intrusion prevention
- Application control
- Web filter

This is supported only in bridge mode. A tunneled SSID's traffic will be inspected by FortiGate, as usual.



You can create a security profile group and the apply it to an SSID. You cannot apply individual security profiles to an SSID, like you can with firewall policies.

FAP-S gets security profile updates from FortiGuard by a FortiGuard subscription.

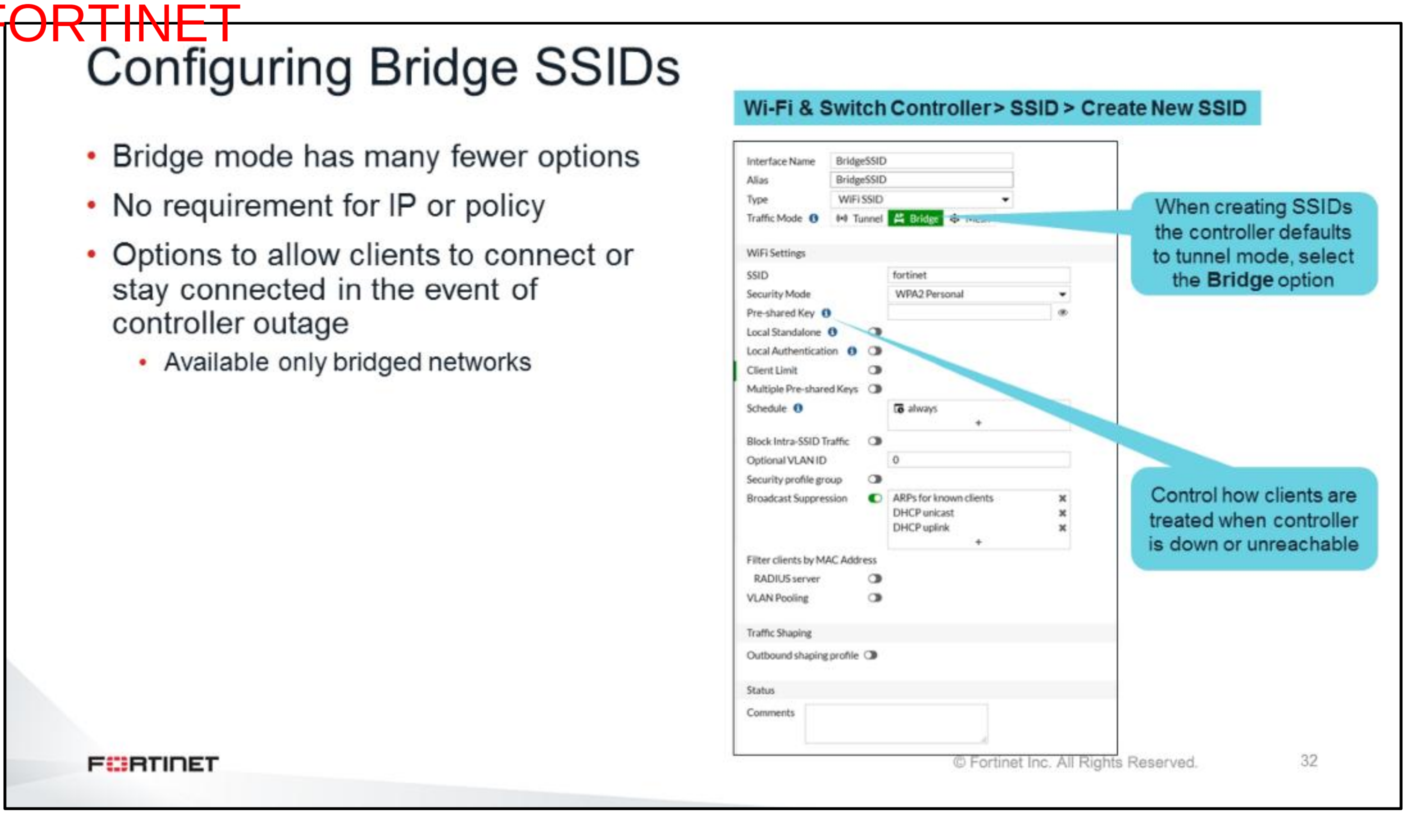


After you create the SSID, you *cannot* change the mode or interface name.

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.

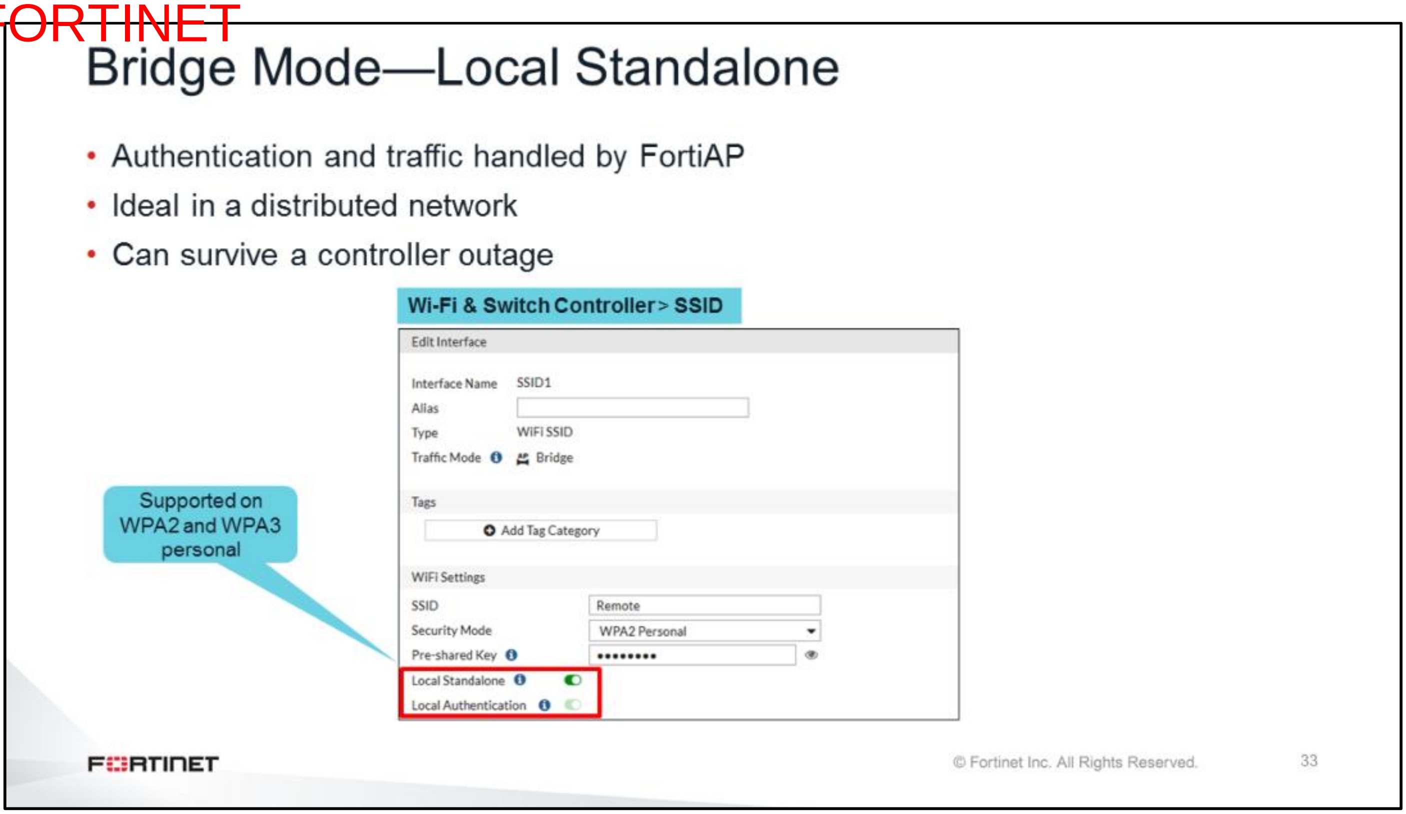
You may want consider adding administrative access services, depending on your requirements.

Clients attaching to 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.



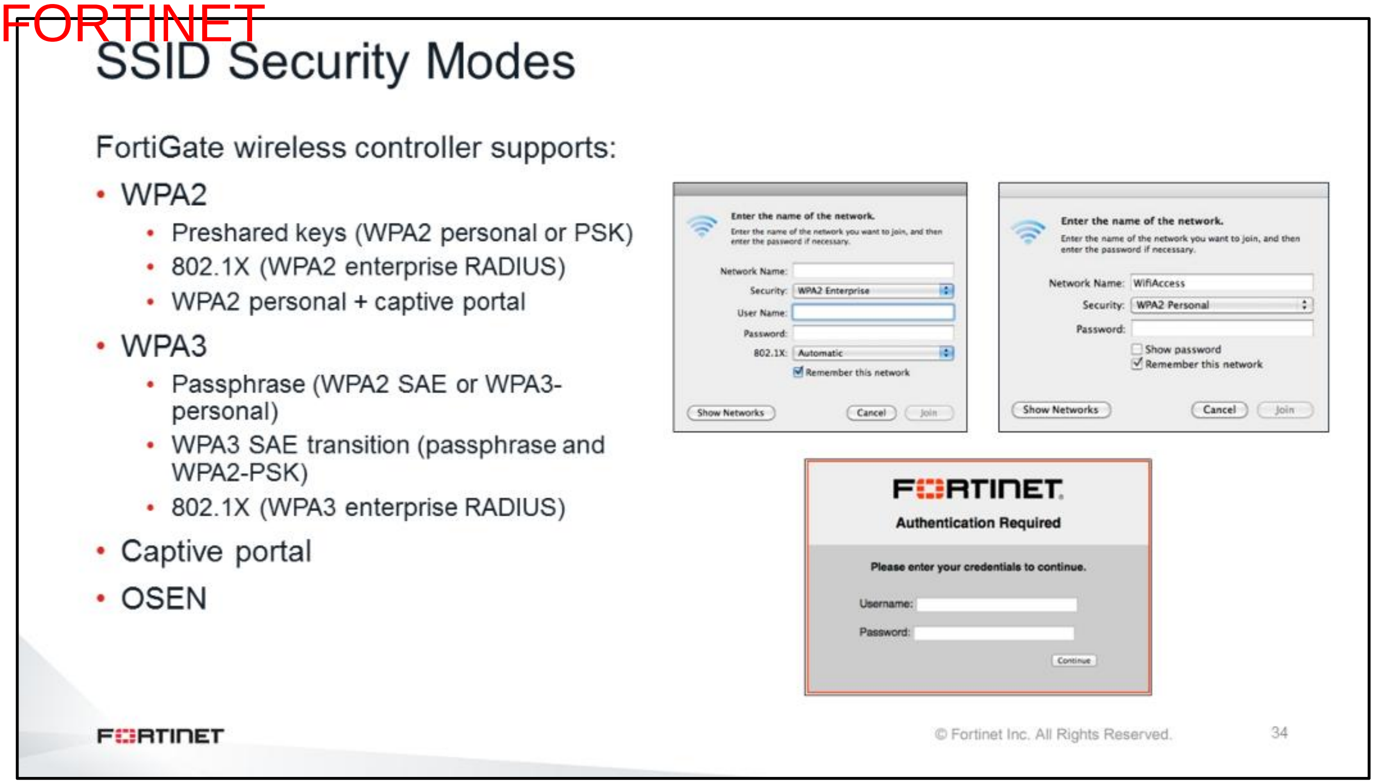
Bridge modes SSIDs are significantly easier to configure because they simply bridge the wireless traffic to the local Ethernet interface.

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.



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, the FortiAP device 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.



Configuring the 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)
- Preshared keys (WPA2 personal)
- Simultaneous Authentication of Equals (SAE)

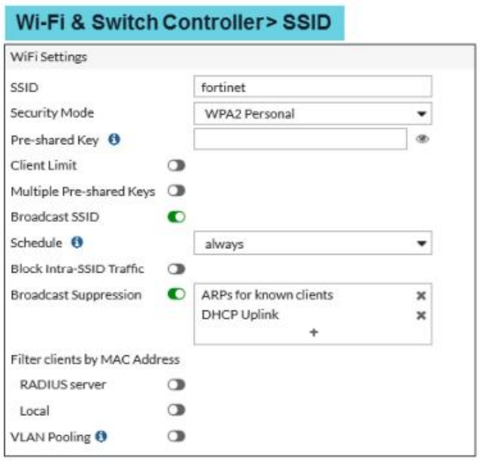
Alternatively, if you need to provide guest access without authentication, you can use captive portal as the security mode and disclaimer only as the portal type. Here is a complete list of supported formats:

- Captive portal – user authentication only, no encryption.
- WPA2 personal
- WPA2 personal with captive portal
- WPA2 enterprise - RADIUS based user authentication
- WPA3 enterprise - RADIUS based user authentication
- WPA3 SAE or officially referred to as WPA3 personal
- WPA3 SAE transition
- Completely unencrypted and unauthenticated
- OSEN

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 only be available if enabled in feature visibility.

Wireless Settings

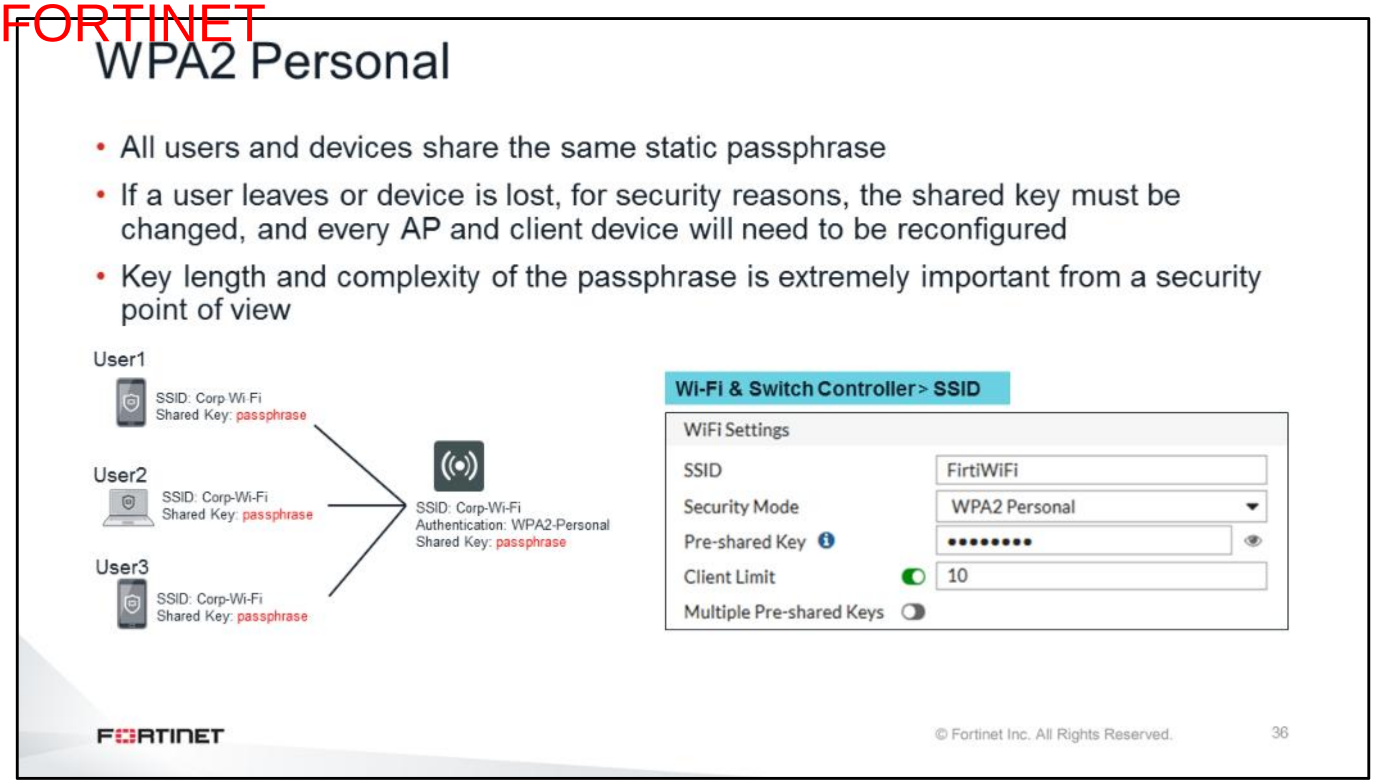
- Some options in wireless settings apply only to certain security modes
- Depending on which security mode is enabled, FortiGate will enable or disable GUI options



FERTINET

 35

It is important to note that, depending on the settings configured, FortiGate 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. This also applies to options such as local authentication, multiple preshared keys, and so on, that are available only for the WPA2 personal option.



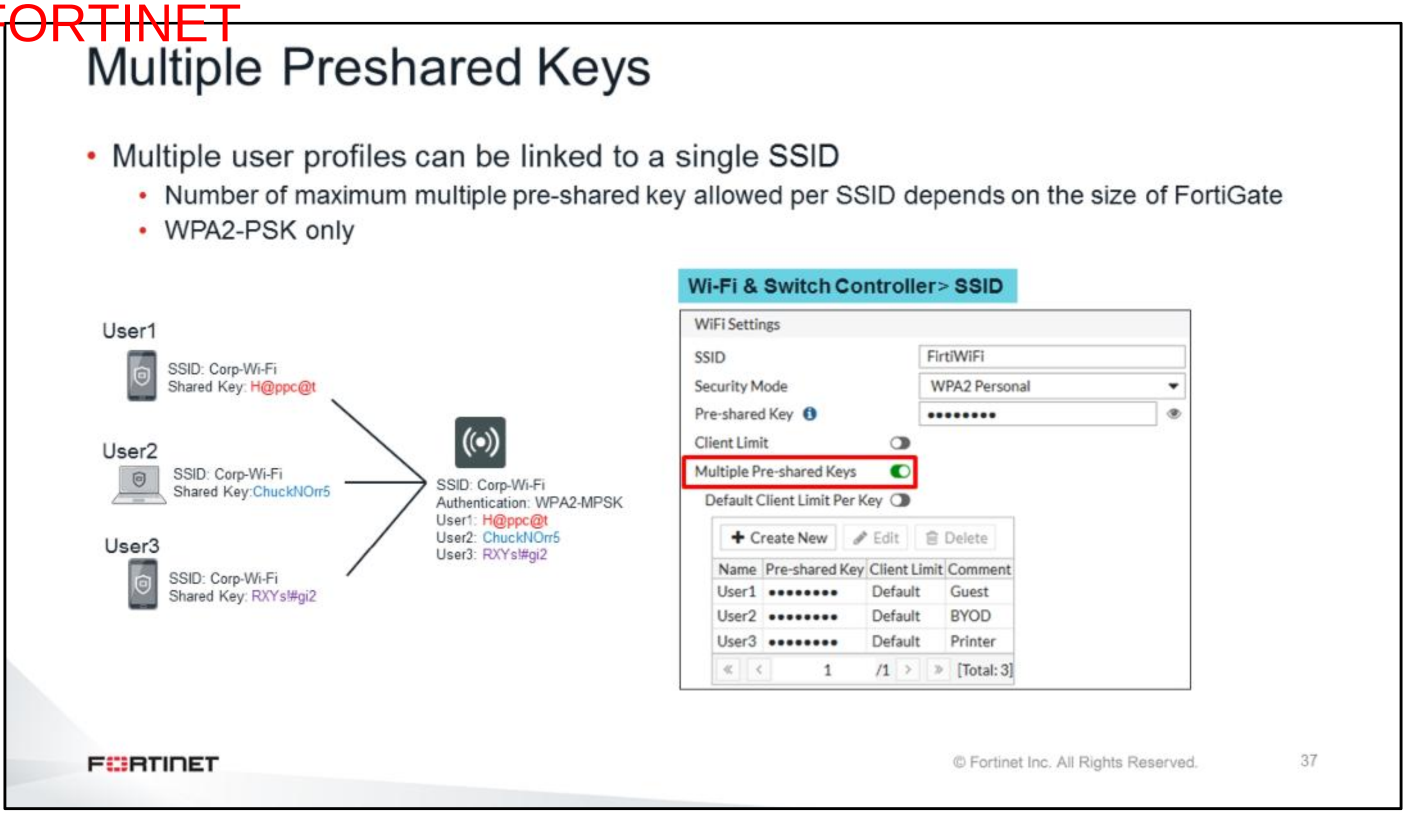
WPA2 security with a preshared key (or passphrase) for authentication is called WPA2 personal, but is also refereed to as WPA2 PSK. This key is static and common to all clients that connect to this SSID and utilizes the AES 256bit encryption to secure data in-flight.

WPA2 and particularly WPA2 PSK, have been the mainstay of wireless encryption for over 10 years and have proven to be effective; however, it is not without limitations.

WPA2 personal can work well for home use or a small group of trusted people in a small business. But, as the number of users increases, it is difficult to distribute new keys securely and there is increased risk that the key could fall into the wrong hands. Even if keys are preinstalled on devices it is often possible to recover the key, allowing end users to simply hand out the key to other people.

Key complexity is also a critical component of PSK security. WPA2 wireless traffic can be captured and analyzed offline. During offline analysis, traffic can be subjected to brute force attacks and dictionary based attacks in which the key can be derived. How easily the key can be derived depends on the complexity and length of the key or passphrase and the computational power available to the attackers. Simple, short keys are more easily compromised.

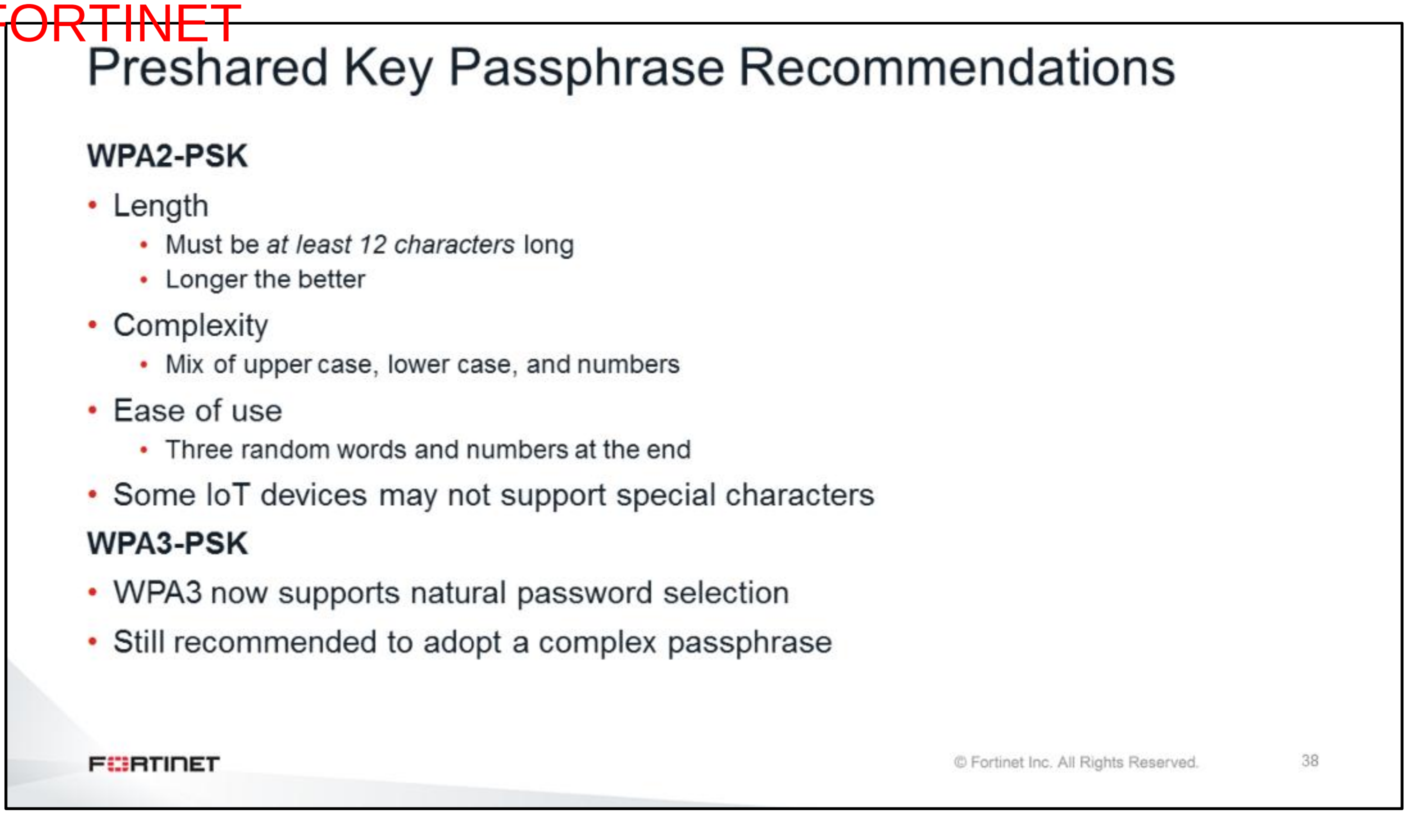
Once a key is compromised, it is time consuming and disruptive to change that key across the many devices that might have it.



As an extension to the original PSK standard, it is possible to enable multiple PSKs for a wireless network. This allows multiple keys to be used to allow access to the network, making key management easier, because all users and devices have unique credentials. If a user leaves or a device is lost, the multiple preshared keys credential is simply changed for that one user or device.

The number of PSKs allowed depends on the specification of FortiGate. It is also possible to limit the number of devices that use any MPSK.

Currently, MPSK is available on only wireless networks that allow WPA2-PSK authentication.

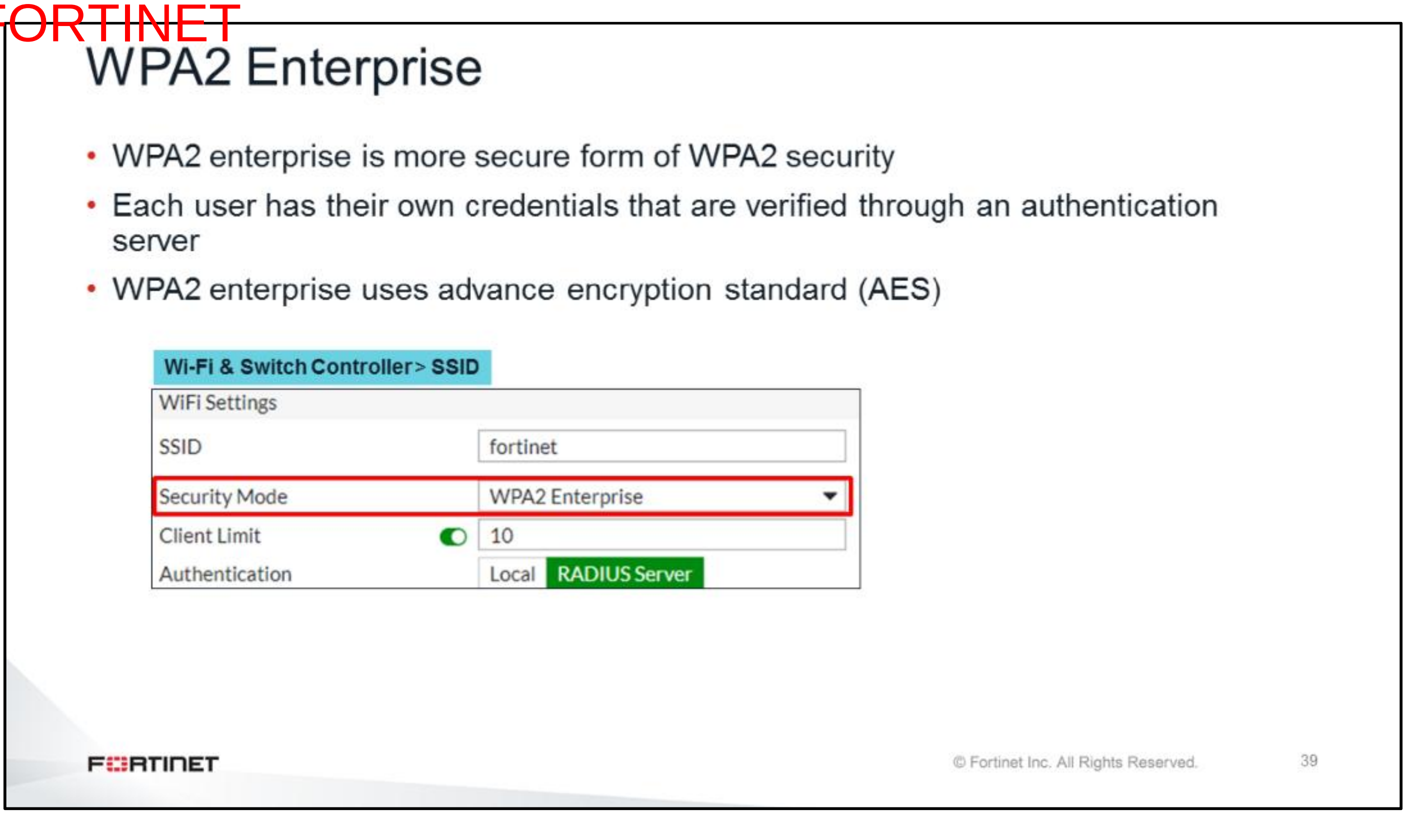


WPA2 preshared key is still widely used when it comes to deploying wireless networks. Due to its ease of use, preshared keys can be easily distributed to the wireless users. However, it is important to note that length and complexity of preshared keys can greatly increase the security of a wireless network

WPA3 has improved the security, however, it is still best practice to adopt a complex passphrase with the same recommendations as WPA2.

Here are some of the things to keep in mind when creating a preshared key or passphrase:

- Length
  - For WPA2: the pre-shared key length is enforced in FortiOS 6.2.1 to be at least 12 characters long
  - Longer is better
- Complexity
  - Use a mix of upper case letters, lower case letters and numbers. Some IoT devices do not support the use of special characters
- Ease of use
  - It is easier to remember three random familiar words and numbers than a complex randomly generated key, for example:
    WhiteCloudSky2# is easier to remember and type than **zndn9xgduygm6Rf**
  - Both passphrases consist of 15 characters and both would take millions of years to calculate using a brute force approach. A dictionary attack would potentially make the first password marginally more insecure, but still take an inordinate amount of time to find as using three or more chained words rapidly increases the complexity.

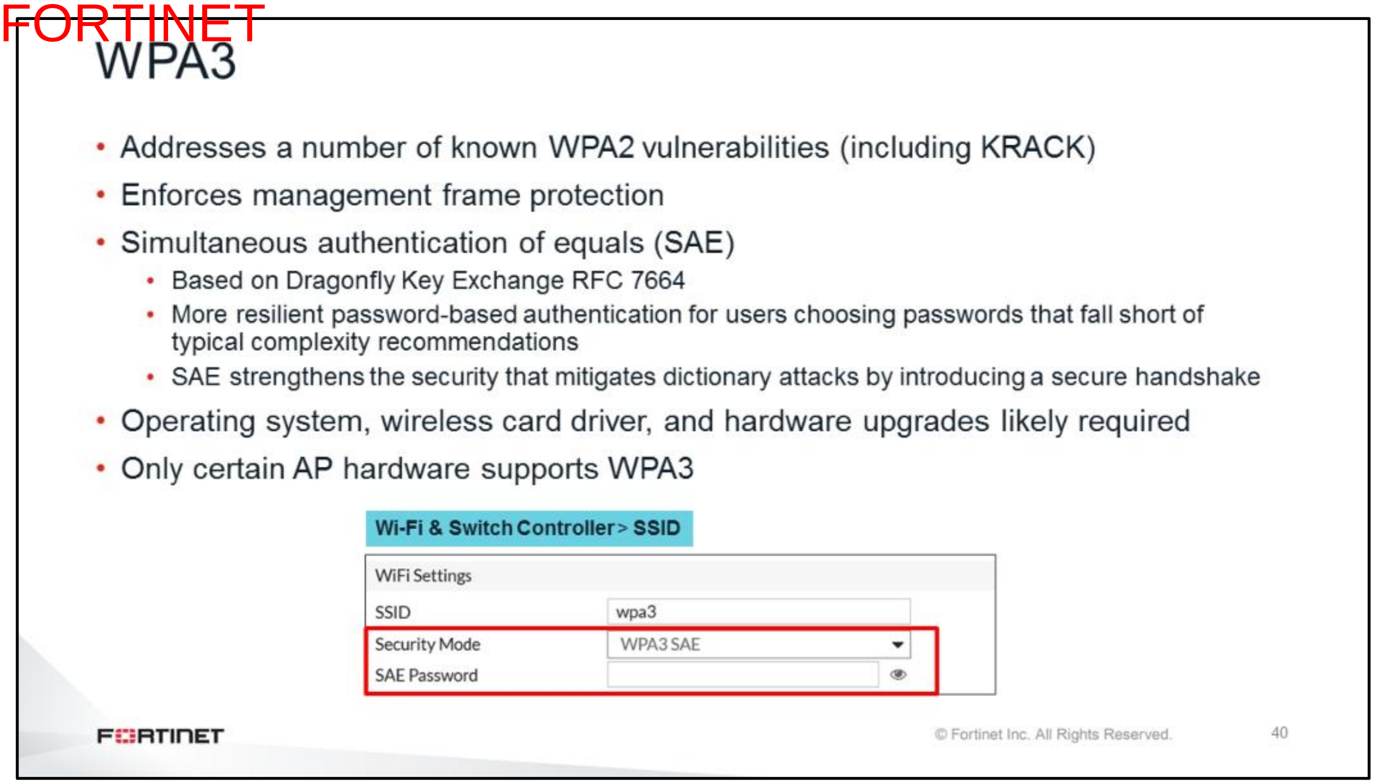


WPA2 enterprise is a more secure form of WPA2 security, but it can require additional infrastructure in the form of an AAA server. Each user has its own authentication credentials, verified through an authentication server, usually RADIUS. This allows access control on a *per user* basis, unlike PSK which allows anyone with the key to connect.

A benefit of using a FortiGate is that FortiOS can also authenticate WPA2 enterprise connections through its built-in user group functionality without the need of an external RADIUS server. This makes an excellent alternative to PSK, alleviating the limitations of PSK networks while adding little additional complexity, outside of adding users to the internal database. One downside to this approach is that many IoT and home use devices do not support, or perhaps do not properly work with, WPA2 enterprise networks, because support for WPA2 enterprise is not mandated in any wireless standard.

FortiGate user groups can include RADIUS servers and can select users by RADIUS user group. This makes role-based access control (RBAC).

As with WPA2-PSK, WPA2 enterprise encrypts in flight communication using Advanced Encryption Standard (AES). As there is no static key to attack, it is harder to penetrate an enterprise encrypted network. However, as the years have gone by, there are more and more potential vectors of attack appearing, making the move to the new WPA3 standards an increasing priority.



FortiOS 6.2 supports WPA3. WPA2 is the first major update in wireless security since WPA2, 14 years before. WPA3 addresses multiple vulnerabilities that affected previous version of WPA.

WPA3 features SAE, which provides more resilient password-based authentication for passwords that fall short of typical complexity recommendation. SAE strengthens the security of the wireless network against dictionary attacks, since it features a secure handshake method.

WPA3 also supports management protection that now identifies that frames coming from APs. This allows the clients to continuedly verify the identity of the frames that are used to connect and roam around a wireless network, making historical man-in-the-middle attacks substantially harder.

WPA3 is the future of wireless security; however, any new standard can take time to be adopted. It is *very* likely that significant client upgrades will be required to support the new standard, including operating systems, drivers and, potentially hardware. Some hardware may never support WPA3. It should be noted that not all FortiAPs will support WPA3. Refer to the AP datasheets for WPA3 compatibility.

Advertising a WPA3 *only* network could mean that a large number of clients may not be able to connect. For PSK/passphrase networks it is possible to advertise as a wpa3-sae-transition network. This allows both WPA2 and WPA3 keys/phrases to be used at the same time, make the support and migration of clients substantially more straightforward. Obviously, the network will only be as secure as its weakest link, in this case, WPA2 security.

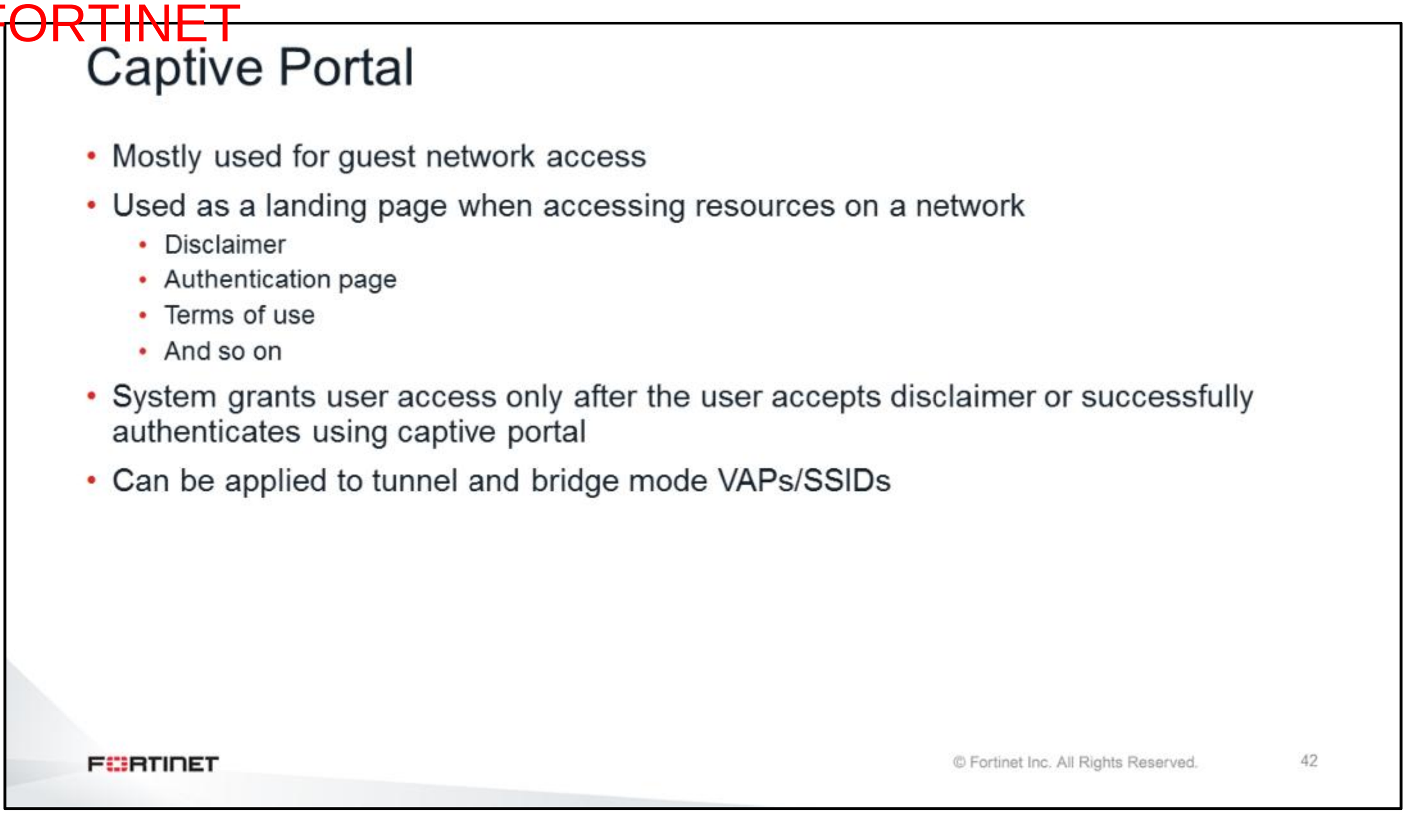
How is WPA3 Different?

Features	WPA2	WPA3
Released	2004	2018
Encryption	Advanced Encryption Standard (AES) With CCMP standard	AES-GCM encryption & Elliptical Curve Cryptography of CNSA Suite B.
Session Key Size	128-bit	192-bit
Handshake Protocol	Pre-Shared Key (PSK) exchange protocol	Uses Simultaneous Authentication of Equals (SAE), also known as Dragonfly Key Exchange, with Forwards Secrecy feature
Security Modes	WPA2 Personal: Pre-Shared Key (PSK) WPA2 Enterprise: IEEE 802.1X (RADIUS)	WPA3 Personal: 128-bit SAE WPA3 Enterprise: 192-bit SAE
Data Integrity	CBC-MAC having 64-bit Message Integrity Code (MIC)	Secure Hash Algorthm-2 for each input
Protected Management Frames	Available since 2018 BIP-CMAC-AES-128	Mandatory BIG-CMAC-256
Vulnerable to Krack	Yes	No, due to SAE exchange
Vulnerable to offline Dictionary attacks	Yes	Blocks authentication after a certain number of failed login-in attempts

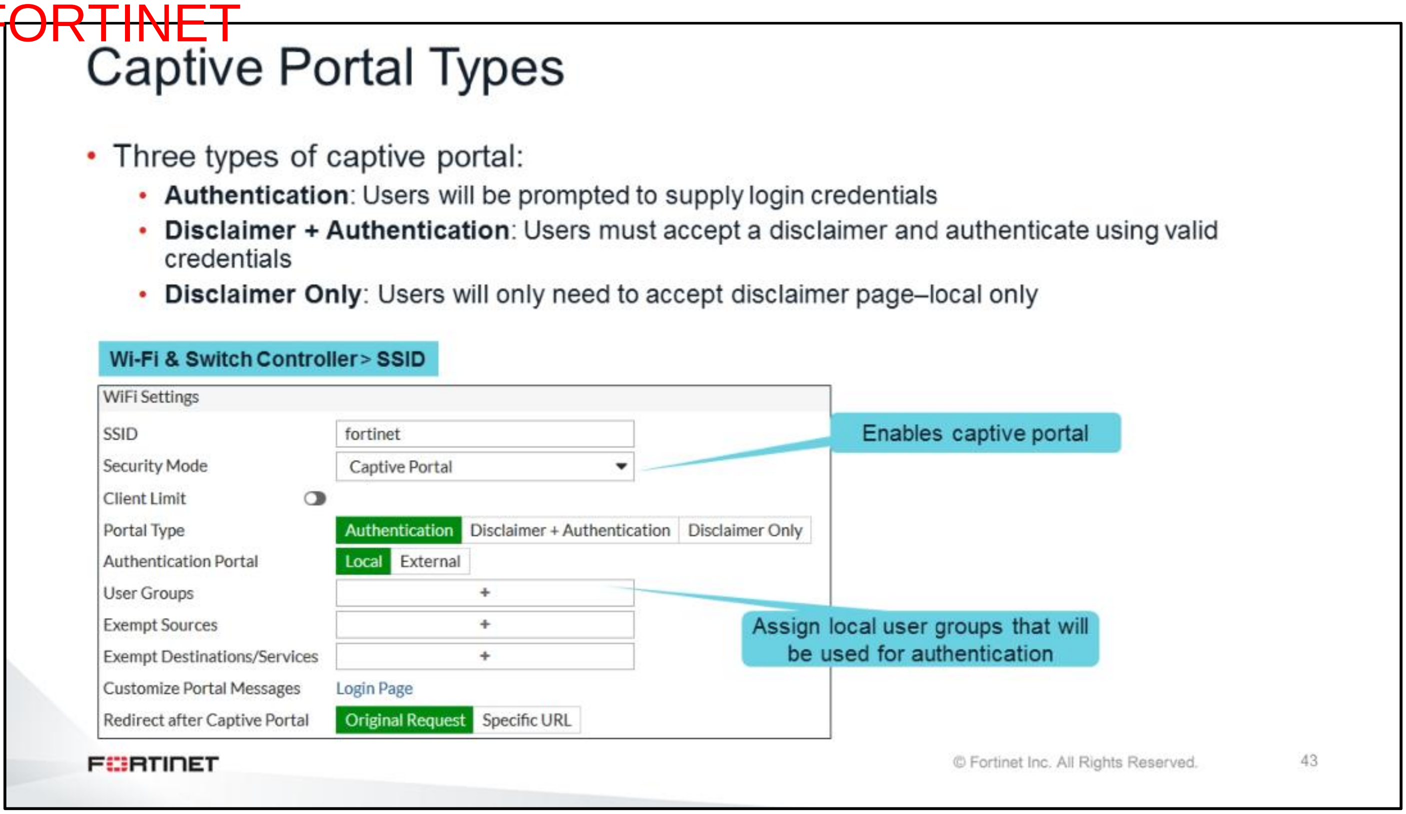
FORTINET

 41

This chart shows differences between WPA2 security mode and WPA3 security mode.

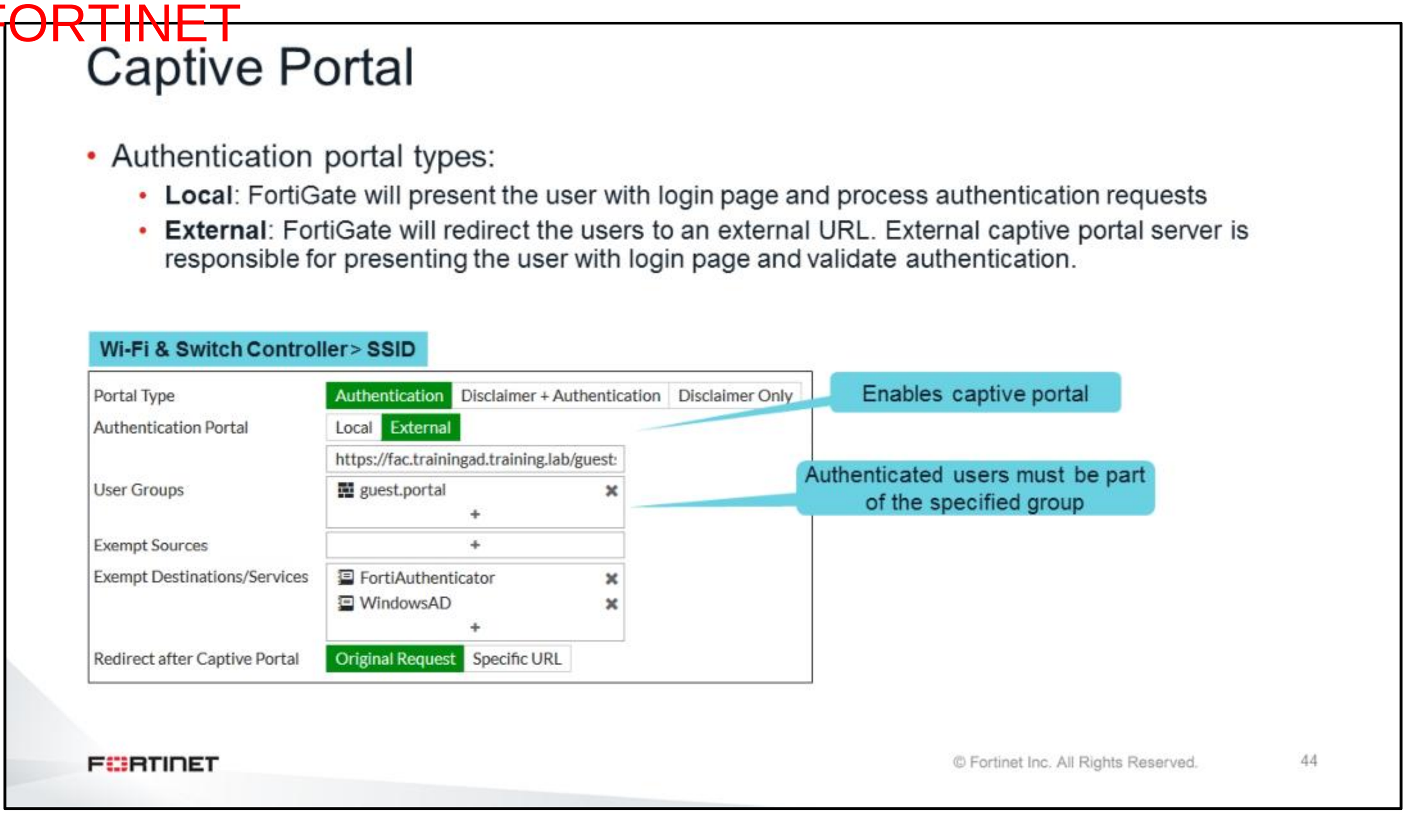


The captive portal is used as a landing page after a user connects to a network. This is mostly used for guest access and networks that require a disclaimer. You can also authenticate your users on a captive portal page that requests the user’s name and password. Until the user authenticates successfully, 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.



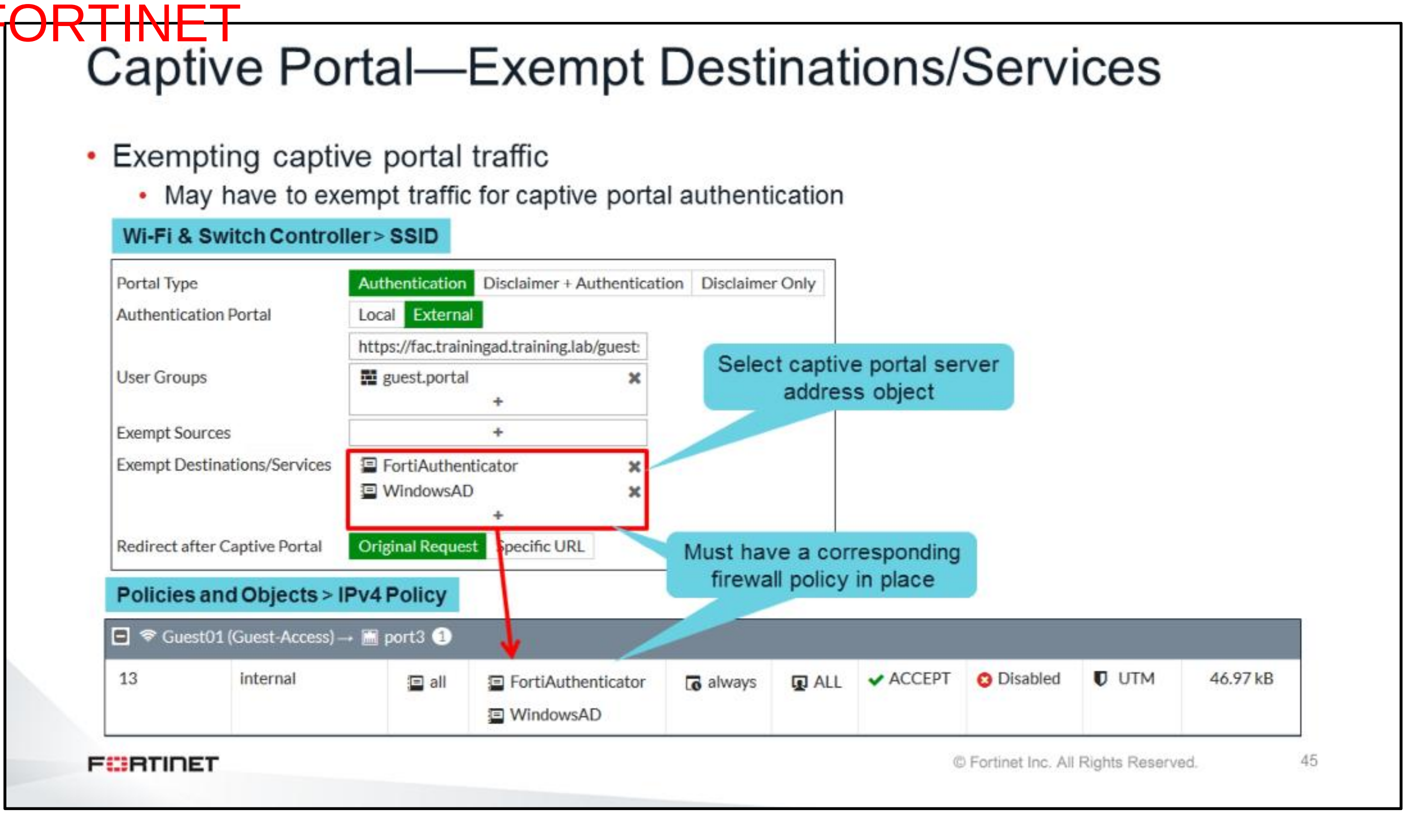
There are three types of captive portals that you can enable on an interface: authentication, disclaimer with authentication, and disclaimer only.

- **Authentication:** Request users to authenticate before they are allowed access to network.
- **Disclaimer with Authentication:** Presents 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:** Presents users with a disclaimer page. In this case, users do not have to authenticate using a username and password. They will be allowed to access the network after they accept a disclaimer page.



After you select **Authentication** in the **Portal Type**, select **Local** or **External** in the **Authentication Portal** field. If you select **Local** 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.

To use external captive portals, select **External** in the **Authentication Type** field and enter the FQDN or IP of the external captive portal server. In this case, FortiGate will redirect the users to the specified server address. Once the user meets the requirements of the external captive portal server, FortiGate will allow user access based on the firewall policy configurations.



By default, FortiGate blocks all traffic from users behind an interface that has the security mode set to captive portal. All HTTP traffic is redirected to the captive portal page and other traffic is blocked. However, there is an option to exempt certain traffic 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's ip address. You can exempt destination IP addresses and services on the SSID or interface configuration page. Add the address objects of the destination(s) that you want to exempt in the **Exempt Destinations/Services** section. 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 to allow the pinhole traffic to pass the through FortiGate.

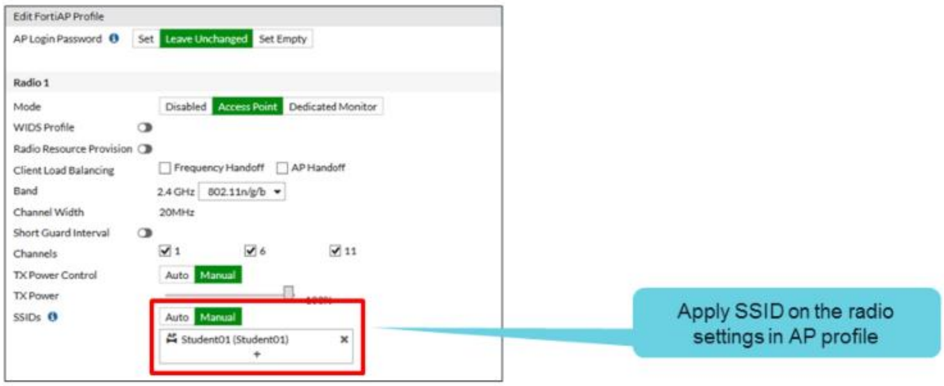
Therefore, this is a two-step process:

1. In the **Exempt Destinations/Services** section, select the destination and services on the SSID or interface configuration page.
2. On the captive portal interface, create a firewall policy to 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 the source the 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 require an Internet connection. For example, a printer might need to access the Internet for firmware upgrades, and so on.

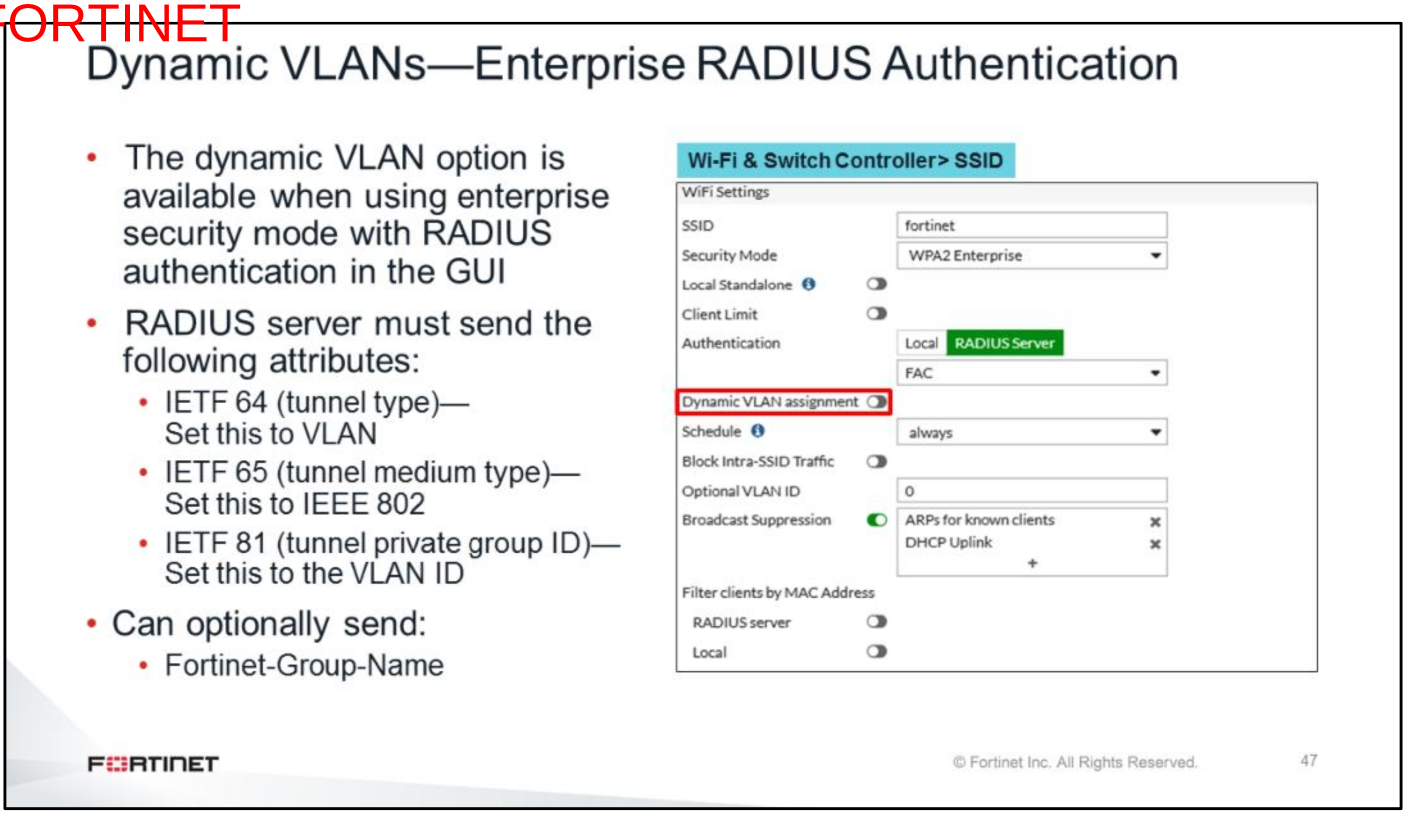
Applying SSID

- An AP profile will broadcast *all* tunnel SSIDs configured at a FortiGate automatically when set to **Auto**
- To broadcast *only* select tunnel SSIDs or *any* bridge mode SSIDs, use the **Manual** option in the AP profile or at the AP level



 46

Before an SSID is used, you must apply it to an AP profile so that APs can broadcast information for clients to connect to. If you do not apply the SSID to an AP profile, it will remain as a configuration on FortiGate, but FortiGate will not push it will not push to APs. APs must receive the SSID configuration from FortiGate before they can broadcast it. By default, AP profiles are configured to automatically inherit all SSIDs in a tunnel mode configuration and push them to APs. However, you must manually select SSIDs in bridge mode in the AP profile.



The option to add dynamic VLANs to SSID is available on FortiGate in both tunnel and bridge mode. You can apply 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.

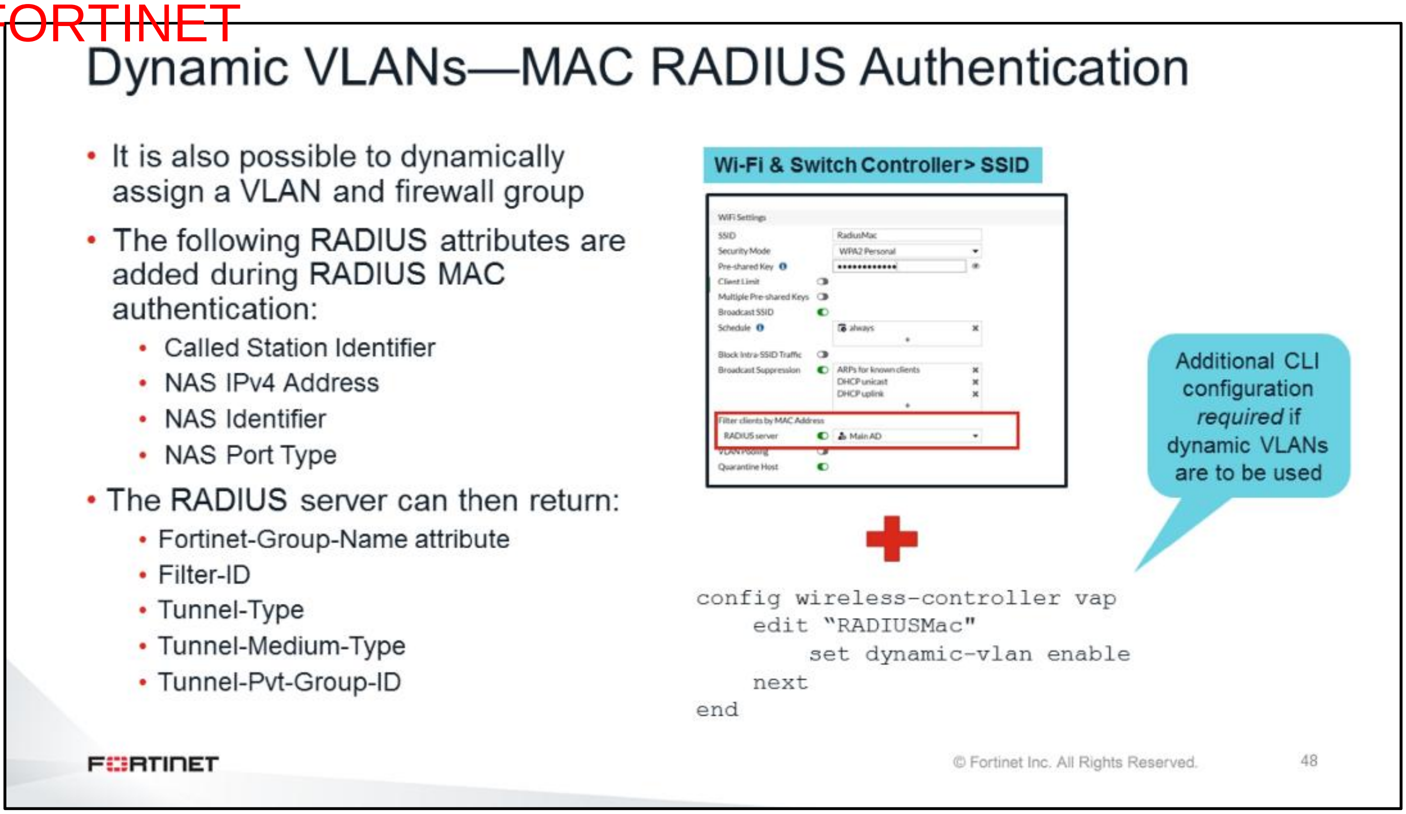
The RADIUS server is responsible for sending all the required attributes after a successful authentication. The RADIUS server must send the following attributes to the FortiGate:

- 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.



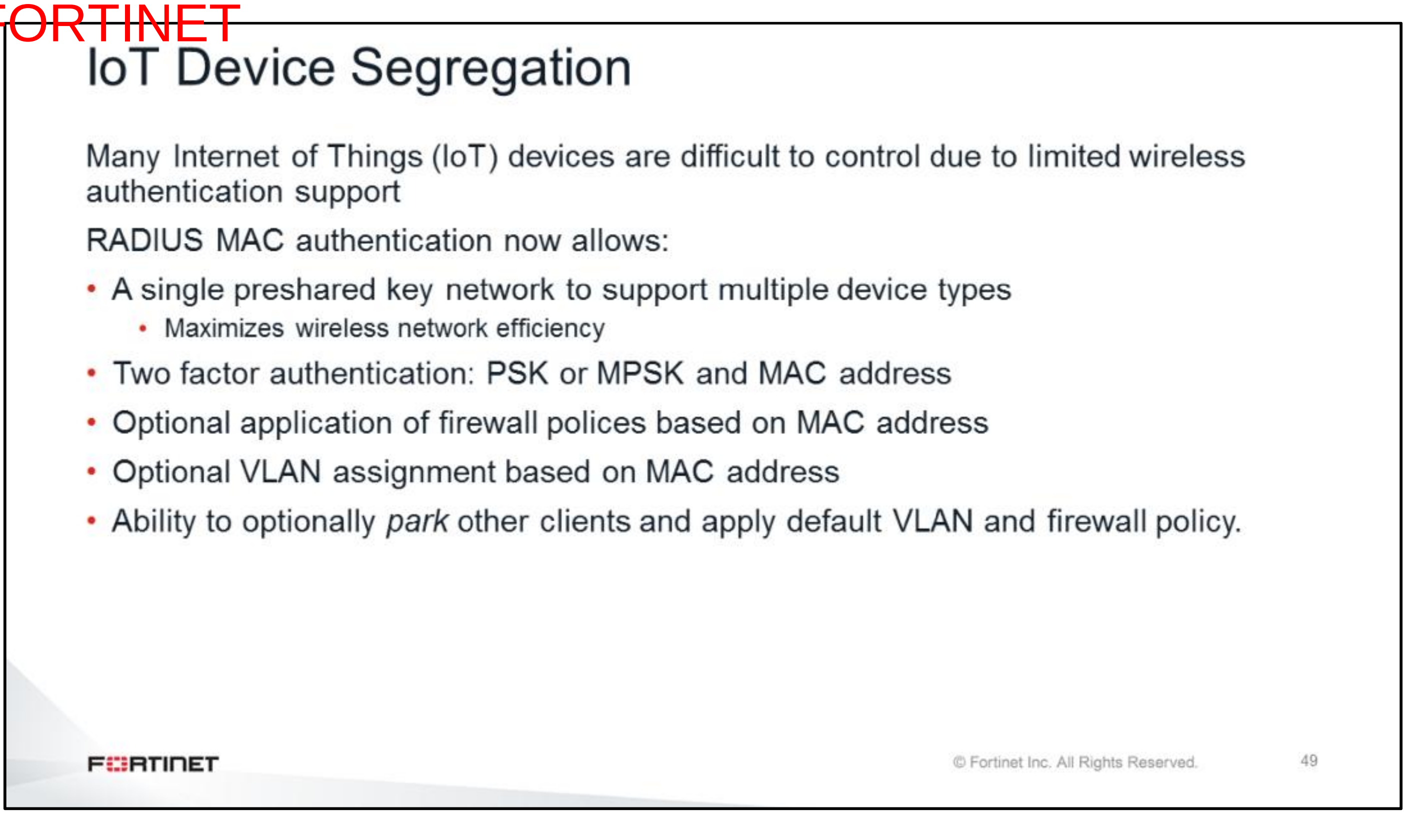
It is also possible to add dynamic VLANs to a non-enterprise network. Traditionally, open or preshared key networks did not allow for the dynamic allocation of VLANs. But, MAC filtering using RADIUS, it is now makes it possible to pass back the following attributes to the RADIUS server when authenticating 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 assigned a VLAN and a Fortinet group name attribute to allow dynamic VLANs and dynamic firewall policies.

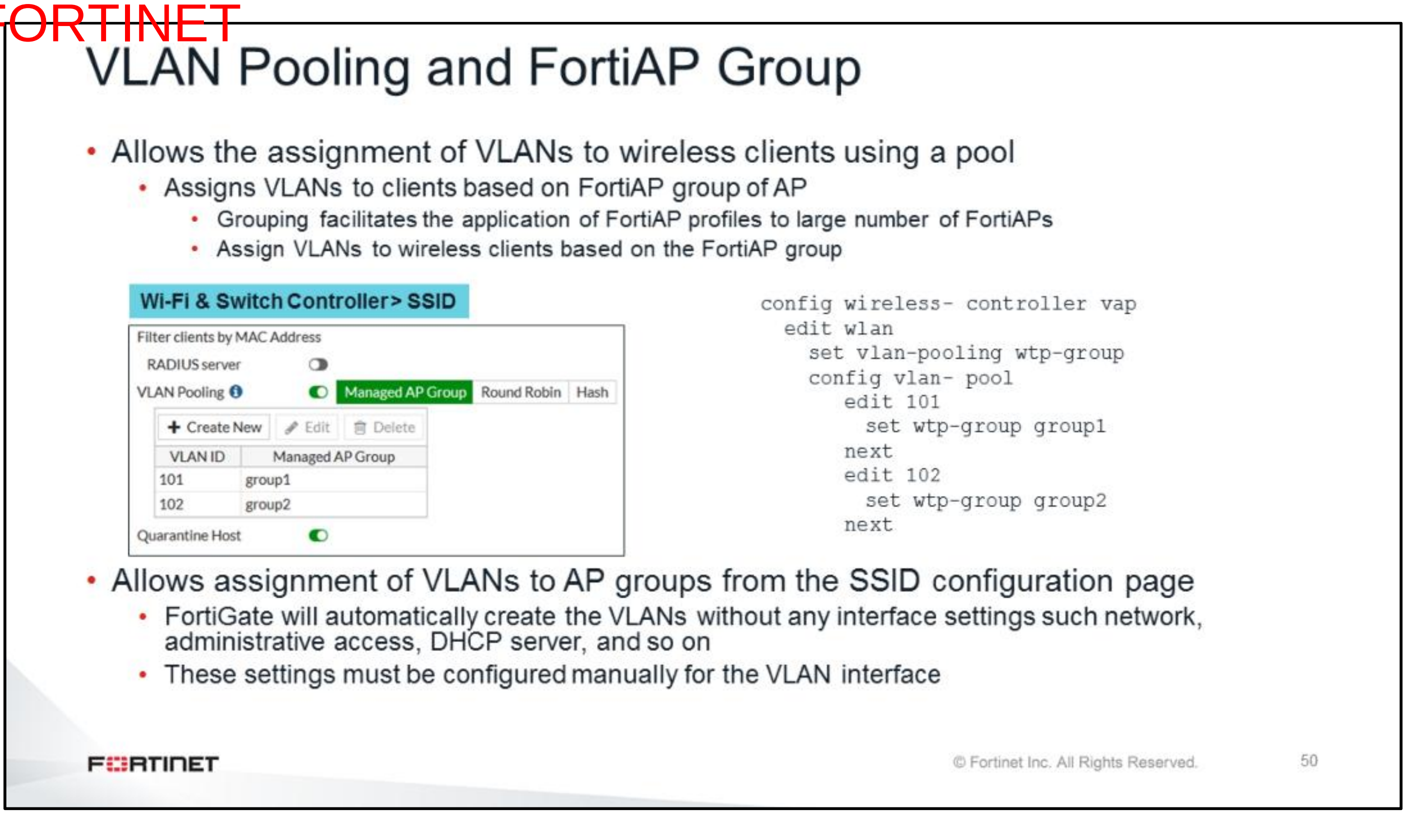


Many simple IOT devices are not capable of supporting a full WPA2-Entrprise supplicant. Many smart plugs, thermostats and other wirelessly connected devices support connection to a wireless network using a preshared key. While this level of security may be sufficient for small home-based networks, in enterprise environments with many devices, using only a single preshared key can be a significant.

In an attempt to control IoT devices, enterprises will often publish multiple preshared key wireless networks, assigning each of them their own VLAN. Doing this can cause significant management overhead and potential wireless performance issues, due to 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 preshared key, or if multiple preshared keys are enabled, a choice of key. This enables connection encryption and a second factor of identity.

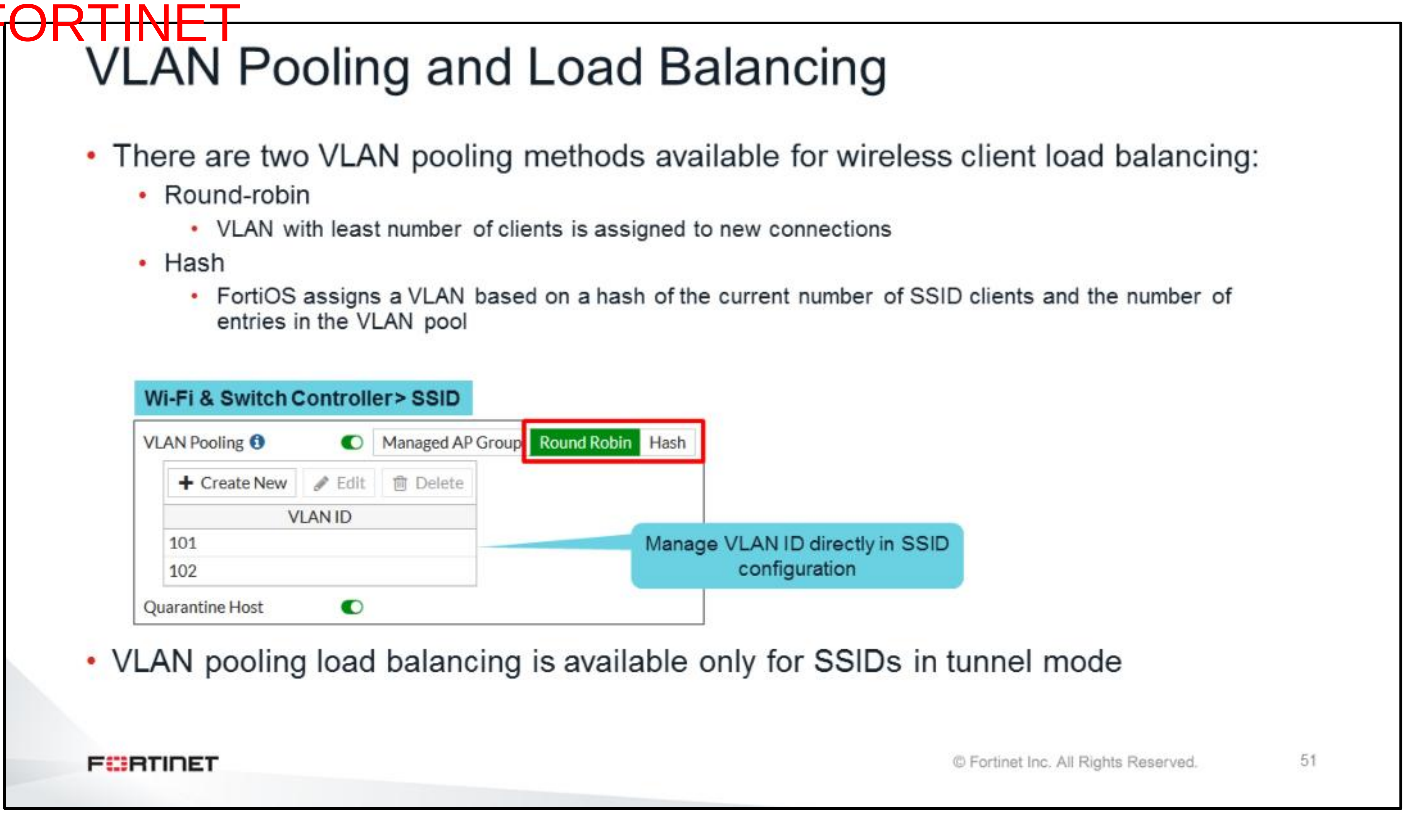
It is now possible to publish a single, preshared key-based network that serves multiple purposes. It could allow printers and IoT devices to be connected and controlled, assigning them to their own VLANs and firewall policies, while still allowing normal preshared clients such as guests to connect and gain access.



For the ease of management, you can put FortiAPs in a group of two or more APs. For example, you can group APs based on the floor of the office they are installed on. You must configure managed AP groups before you can use them in the VLAN pooling configuration.

You can then use FortiAP groups to dynamically assign VLANs to wireless clients based on the APs that the wireless clients connect to. This feature is useful in large deployments and can break down the broadcast domain, rather than putting all wireless clients into a single subnet. Another reason to assign VLANs based on APs is to apply security inspections and firewall rules based on the location of wireless clients. Doing this provides you with more granular control over wireless traffic.

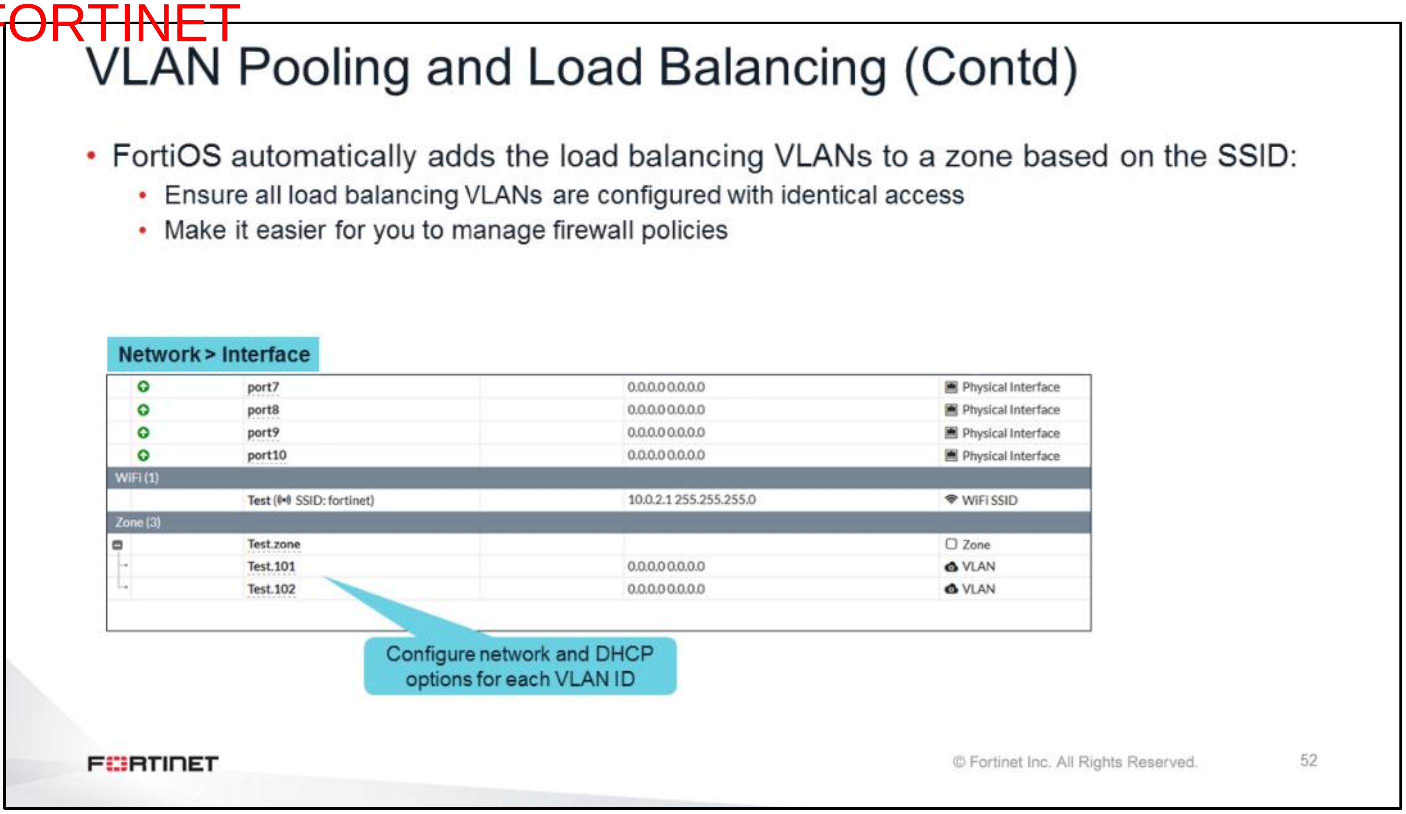
You can define VLANs and assign them to AP groups on the SSID configuration page on the GUI. However, you will still need to manually configure interface settings such as network, administrative access, DHCP server configuration, and so on.



There are two more options available in the VLAN pooling configuration that provide load balancing options for wireless clients: Round Robin and Hash. Once you enable VLAN pooling on SSID, you can enable **Managed AP Groups**, **Round Robin**, or **Hash**.

Similar to managed ap group configuration, you can define VLANs directly on the SSID configuration page for both the round robin and hash options. 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 only available for SSIDs operating in tunnel mode.

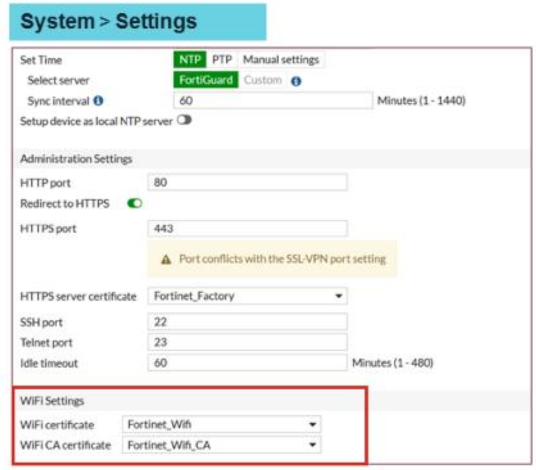


You can define VLAN pooling and load balancing VLANs on the SSID configuration page. FortiGate will automatically put all load balancing VLANs in a zone based on the SSID they were defined in. VLANs are tied to the SSID interface. The zone name includes the SSID interface name followed by `.zone`. For example, if you name your SSID interface Fortinet, then the zone will be named `Fortinet.zone`.

You must configure each VLAN with its own interface option, such as subnet, DHCP, and so on.

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 the CLI



 53

FortiGate uses certificates when connecting wireless clients. Click **System** > **Settings** to view or change the certificate that is in use.

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.

When using an external RADIUS server, the clients will use the certificate installed the RADIUS server instead.

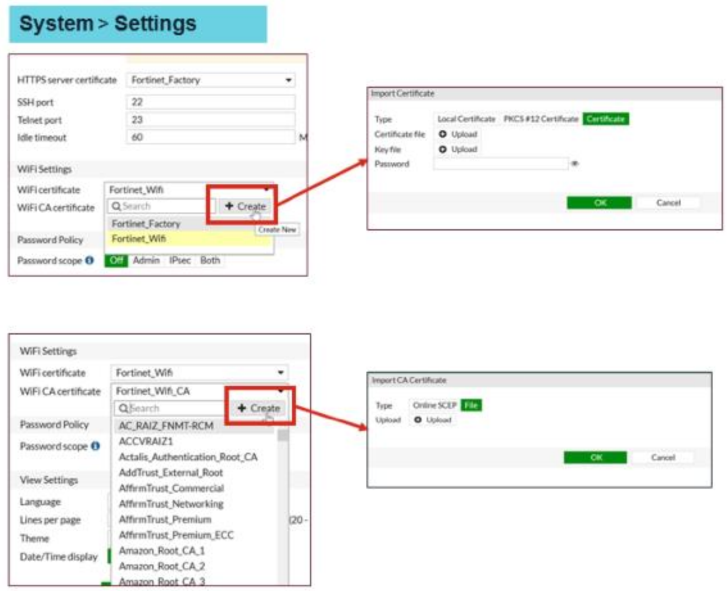
The Fortinet_Wi-Fi certificate is issued to Fortinet Inc. by DigiCert with common name (CN) `auth-cert.fortinet.com`. The Fortinet_Wi-Fi certificate can be updated automatically through the FortiGuard service certificate bundle update, but requires manual replacement if FortiGuard is not available.

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.

Replacing Wi-Fi Certificates (Contd)

- You can replace the certificate on the **Settings** window
- Create and import the certificate as required
- Create and import the CA certificate to be used
- Click **System > Certificates** to view imported certificates



FORTINET

 54

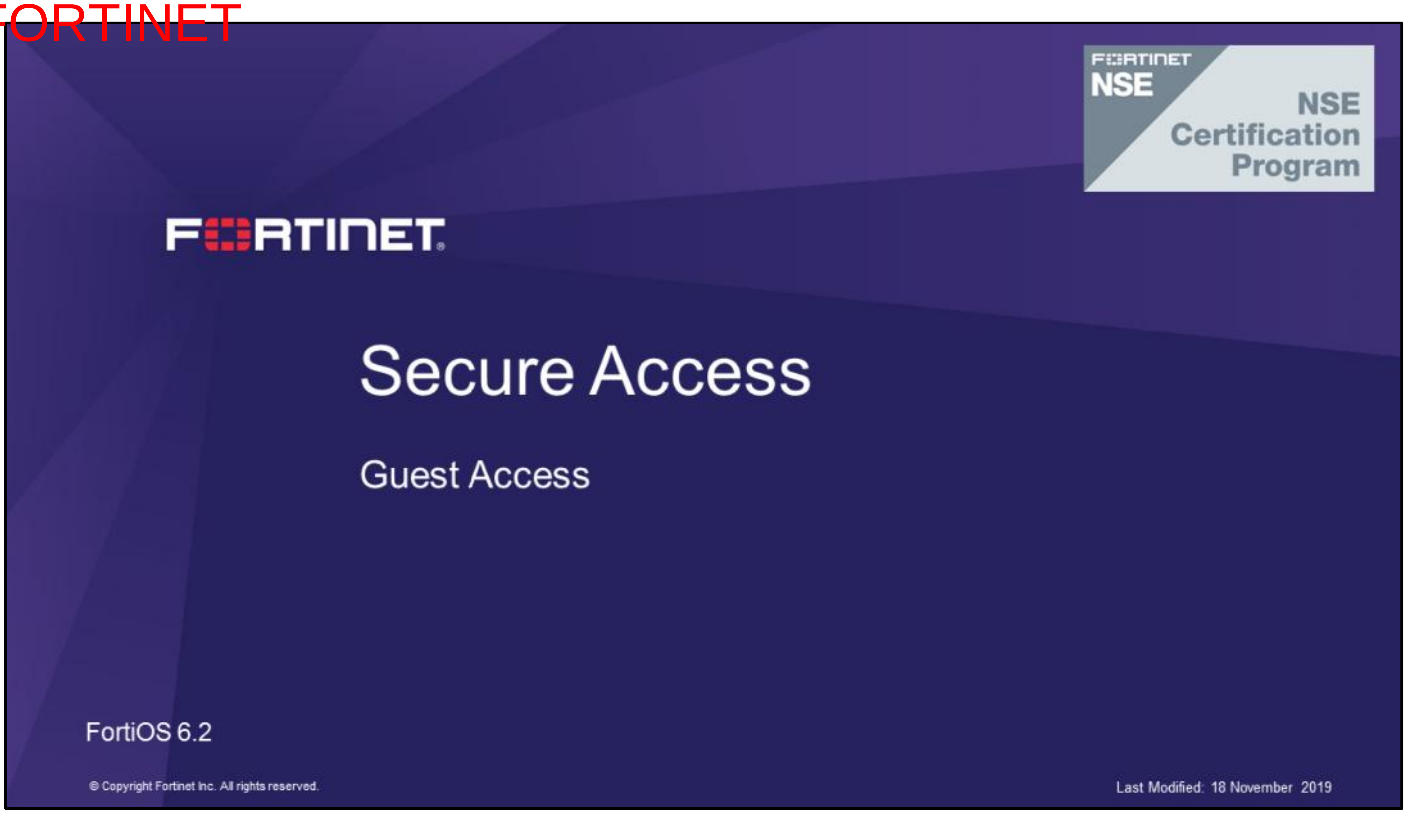
You can update certificates in the GUI and the CLI.

When using the GUI, you can import certificates from the **Setting** menu.

Review

- ✓ Understand the available Fortinet wireless solutions
- ✓ Explore AP discovery methods
- ✓ Configure AP profiles
- ✓ Understand load balancing AP handoff
- ✓ Understand load balancing frequency handoff
- ✓ Explore configuring and broadcasting SSIDs
- ✓ Understand dynamic VLANs
- ✓ Configure VLAN pooling
- ✓ Replace Wi-Fi Certificates

By mastering the objectives covered in this lesson, you learned how to configure and use FortiOS integrated wireless features.



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

Objectives

- Deploy a wireless network to guests
- Understand external captive portal packet flow
- Provision a guest portal on FortiAuthenticator
- Understand the guest portal workflow
- Monitor guest users

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

In this section, you will learn about managing guest access using FortiGate.

Guest Access Overview

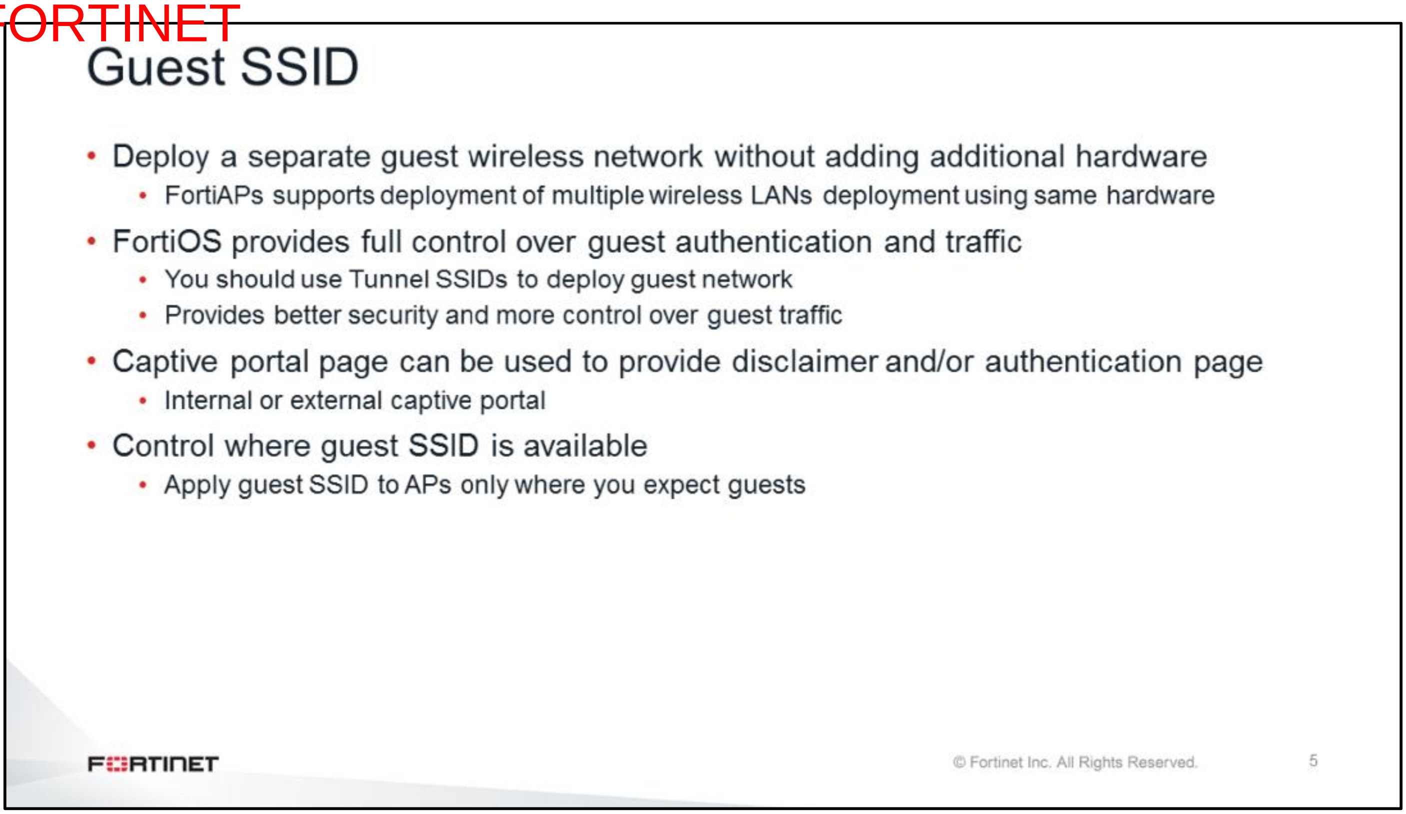
- FortiOS provides multiple ways to securely manage guest access for wireless networks
  - Guest SSID
    - Allows configuration of separate guest network, security profiles, firewall policies, and user authentication
  - Internal captive portal
    - Provides a landing page before access is allowed to the network
  - Guest management
    - Allows configuration of temporary guest accounts
  - External captive portal
    - Redirects guests to an external URL for authentication, disclaimer, and so on

FORTINET

4

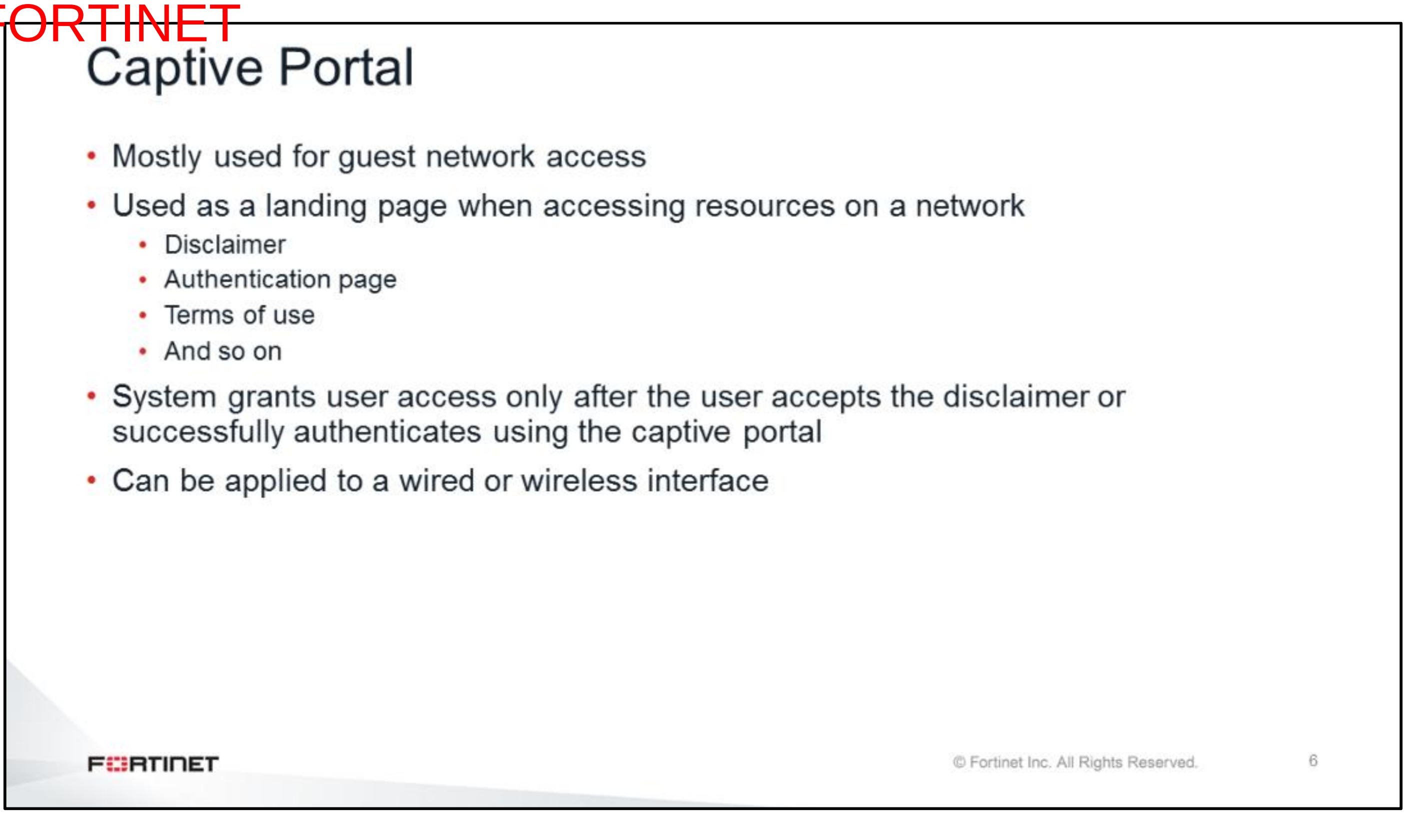
FortiGate provides multiple ways to securely manage guest access for wireless networks. You can deploy a completely separate wireless network using the existing hardware. FortiGate uses virtual AP (VAP) to deploy multiple SSIDs that are completely isolated from each other. This allows you to have complete 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.



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.

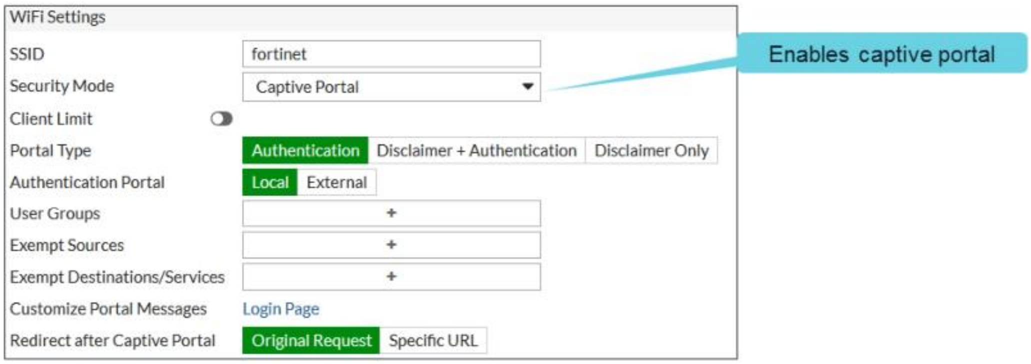
You can use a local or external captive portal to provide guests with a landing page. You can also use a captive portal to display a disclaimer, or authenticate guest users using guest accounts, or both. Because you will be using a separate wireless network for guest access, you can choose to broadcast the network on APs that are installed in locations where you expect guest users to be.



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 to only the members of a specified user group.

Captive Portal Types

- Three types of captive portal:
  - **Authentication**: Users are prompted to supply login credentials
  - **Disclaimer + Authentication**: Users must accept a disclaimer and authenticate using valid credentials
  - **Disclaimer Only**: Users need to accept the disclaimer page–local only.



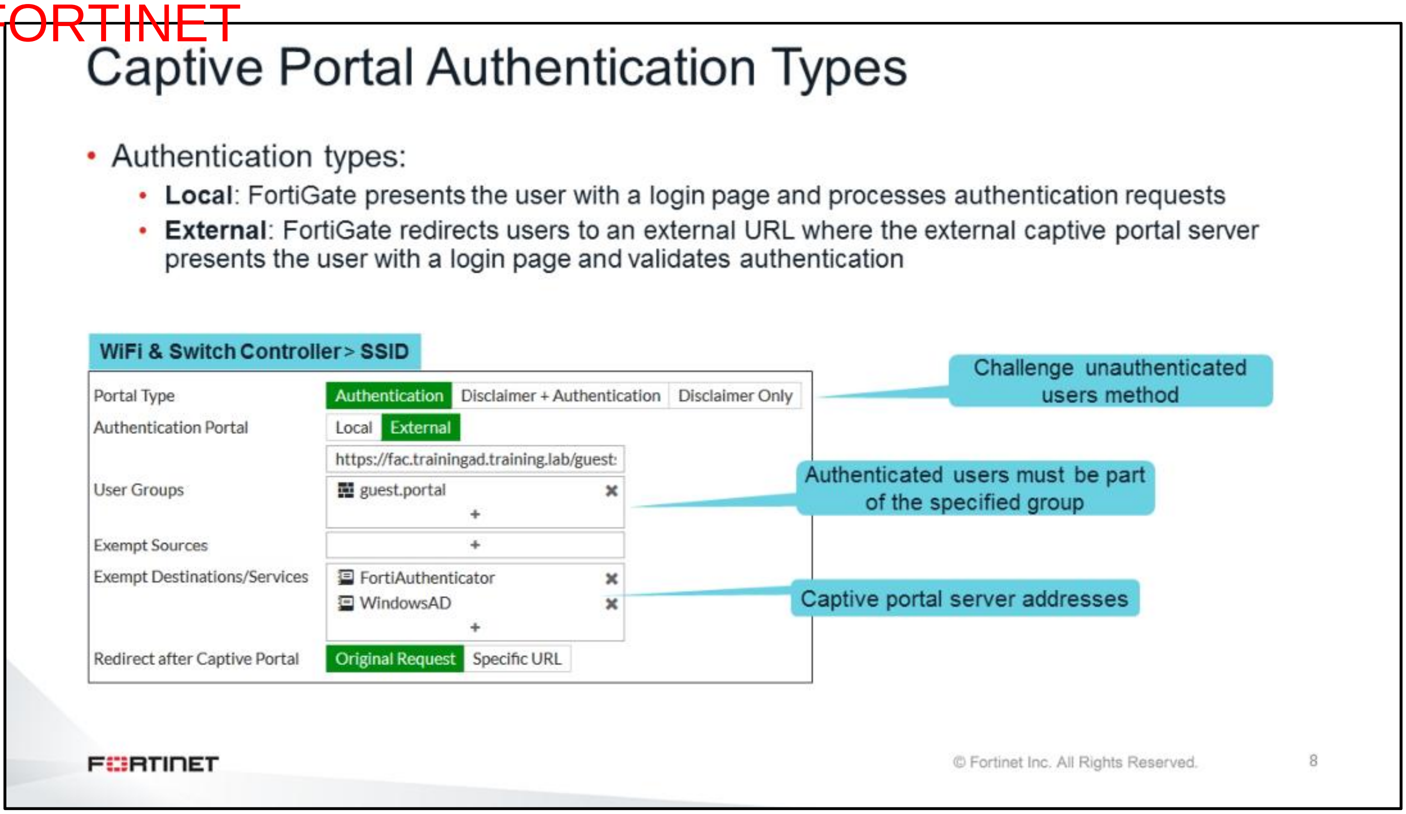
 7

There are three types of captive portals that you can enable on an interface: authentication, disclaimer with authentication, and disclaimer only.

Authentication type captive portals request users to authenticate before they are allowed access to network.

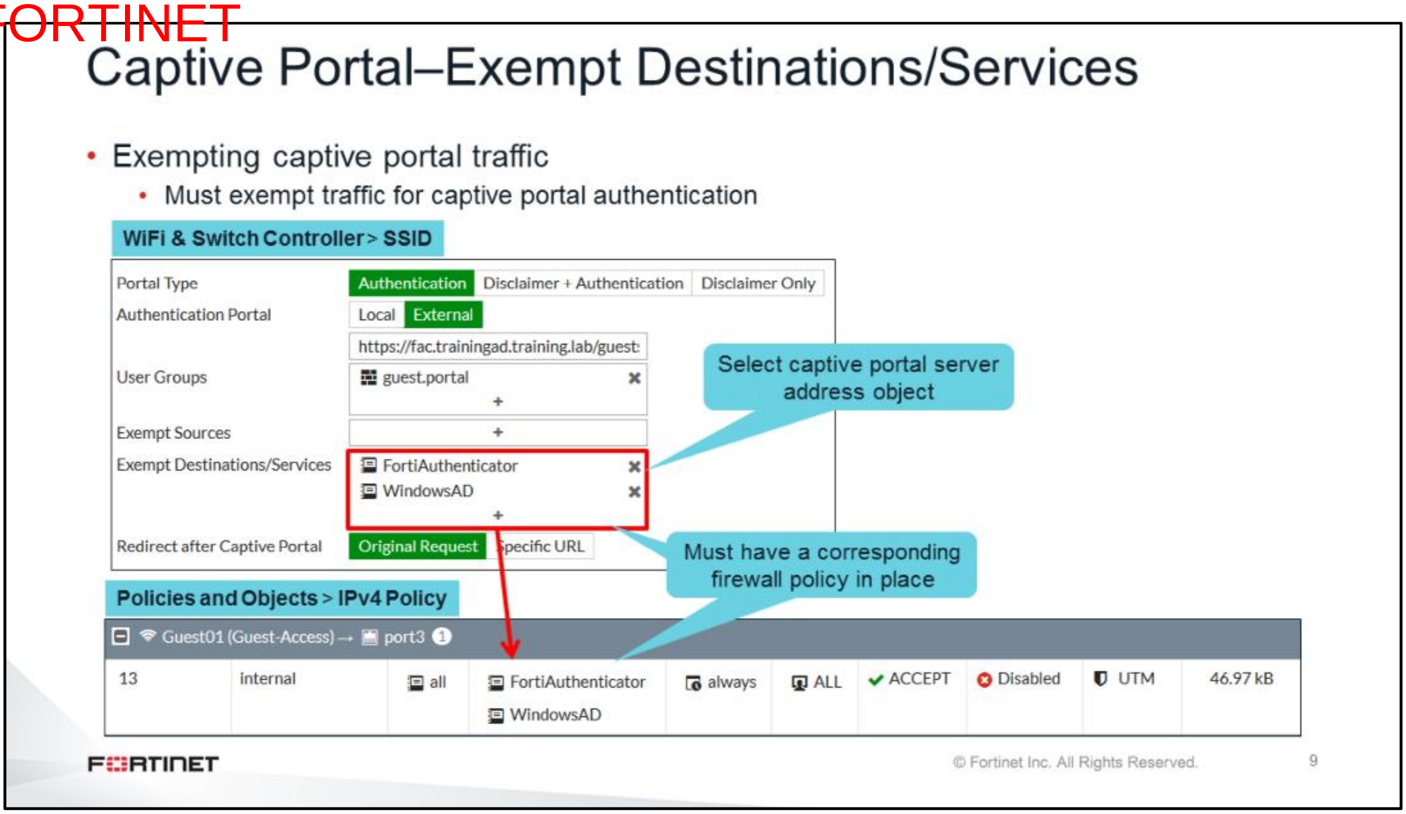
Disclaimer plus authentication type captive portals present users with a disclaimer page and an authentication page. The user must accept a disclaimer and authenticate successfully in order to get network access.

Disclaimer only type captive portals present users with a disclaimer page. Users do *not* have to authenticate using a username and password; they will be allowed to access the network after they accept the disclaimer.



After you select **Authentication** in the **Portal Type** field, you will have the option to select **Local** or **External** in the **Authentication Portal** field. If you select **Local** in the **Authentication Portal** field**,** 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 Type** field, 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.



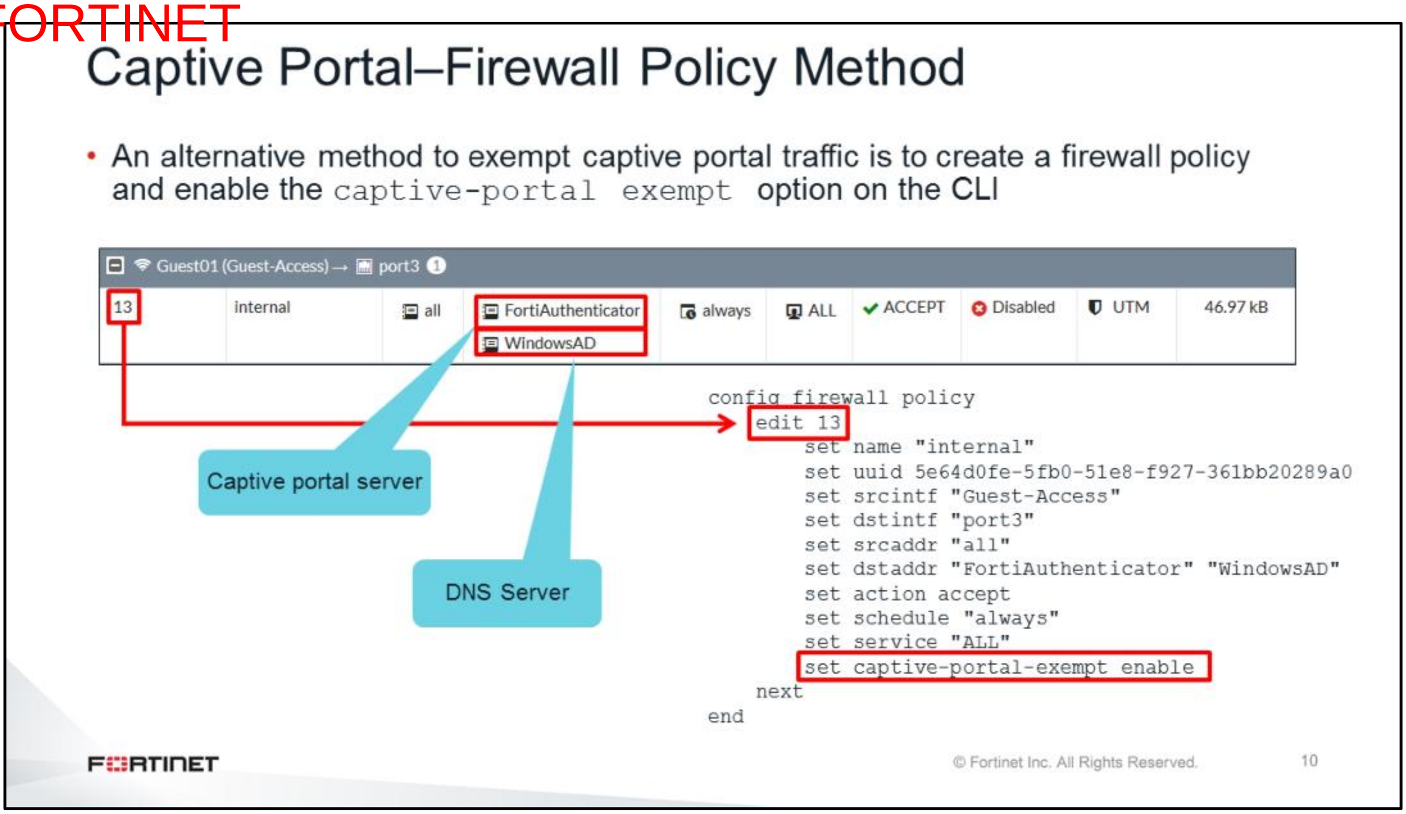
By default, FortiGate blocks all user traffic behind an interface that has the security mode set to captive portal. All HTTP traffic is redirected to the captive portal page and all other traffic is blocked. However, there is an option to exempt certain traffic, allowing it to flow through FortiGate 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 or interface configuration page. Add the address objects of the destination(s) that you want to exempt in the **Exempt Destinations/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 the through FortiGate.

Therefore, this is a two step process:

1. Select the destination and services on the SSID or interface configuration page in the **Exempt Destinations/Services** section.
2. Create 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.



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 firewall policy and set the destination to your captive portal server, and DNS server. On the CLI, edit the firewall policy rule and enable the `captive-portal-exempt` option. 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.

Firewall Policy

- Create a firewall policy for authenticated users only
  - Apply the user group that guests will be part of
  - FortiGate authorizes only users who are part of the specified groups to access the Internet
  - Do not enable the `captive-portal-exempt` option for this policy

Policies and Objects > IPv4 Policy

Create New | Edit | Delete | Policy Lookup | Search | Interface Pair View | By Sequence

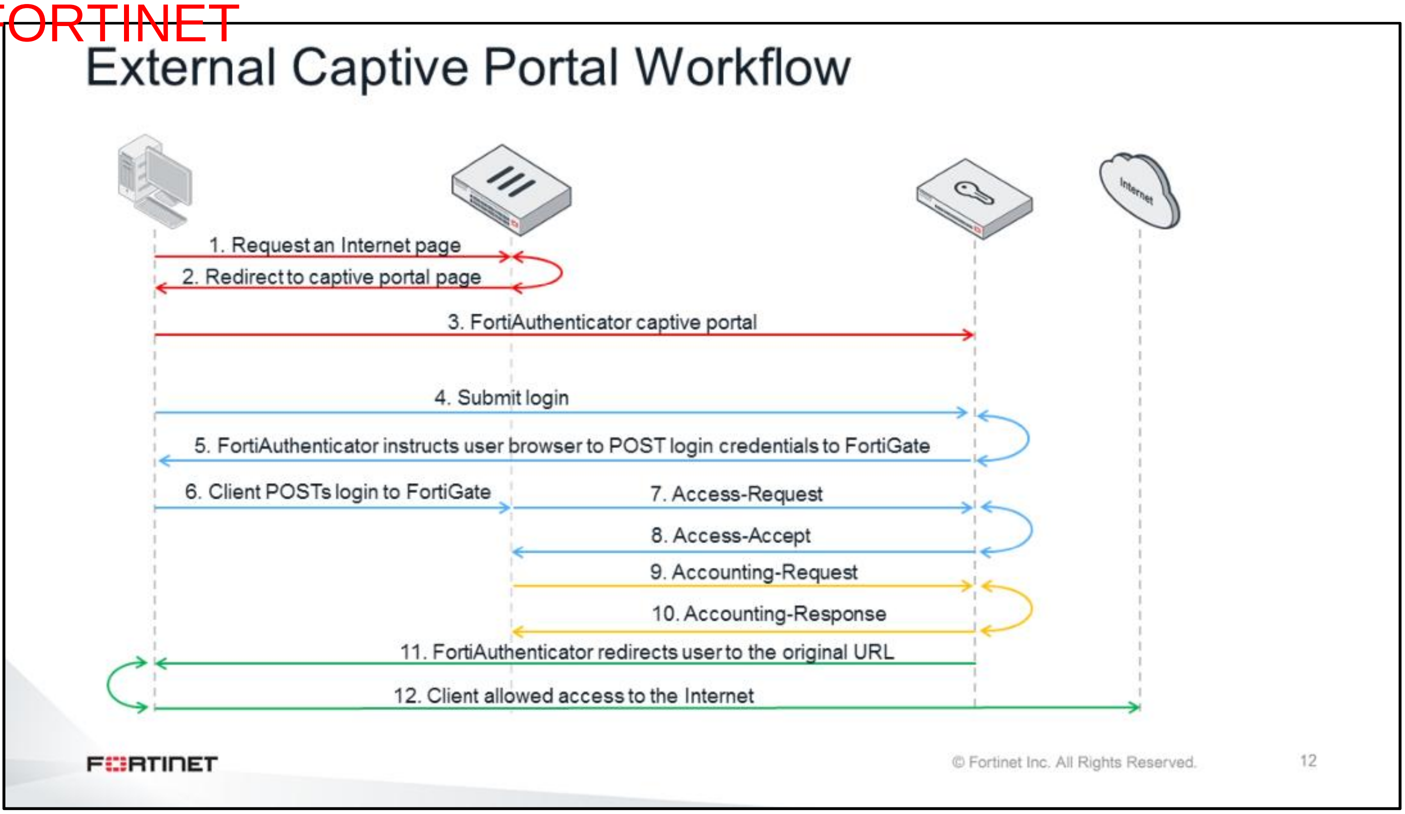
ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Byt
fortilink → port3 1										
Guest02 (Guest-Access) → port1 1										
13	Internet Access	all guest.portal	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	All	43.83 MB
Guest02 (Guest-Access) → port3 1										
12	DNS and Authentication traffic	all	LOCAL	always	ALL	ACCEPT	Disabled	SSL no-inspection	All	3.69 MB

FURTINET

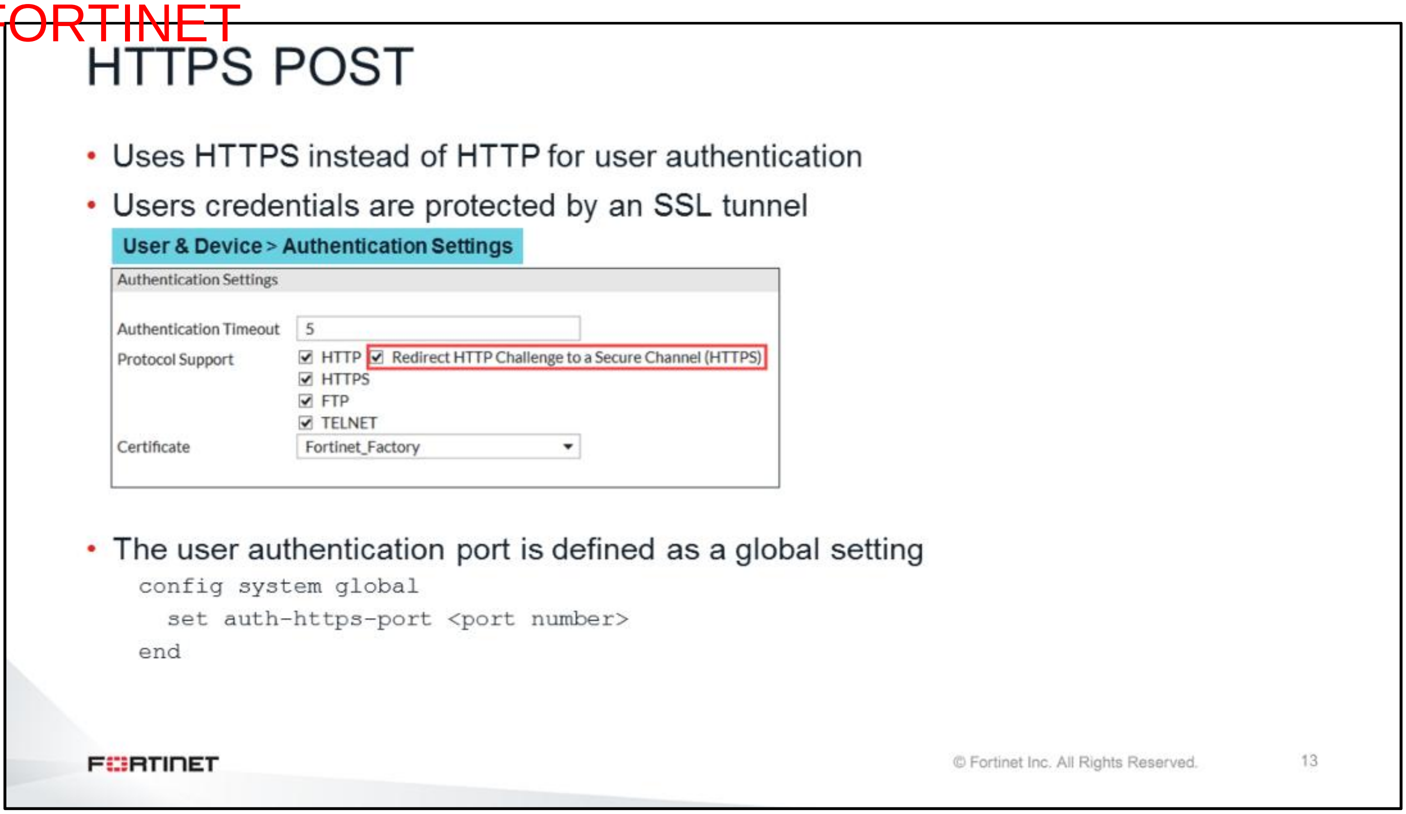
 11

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. When you do this, FortiGate allows access to the Internet for only authenticated users who are part of that group.

Do not enable the `captive-portal-exempt` 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.



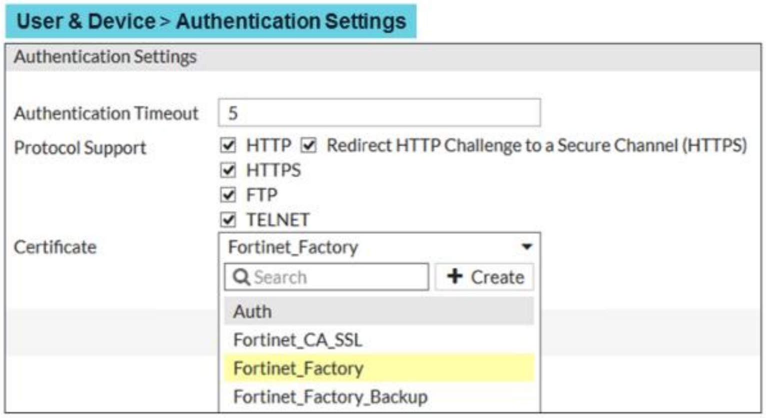
1. The client tries to access a website.
2. The initial HTTP traffic is intercepted by the FortiGate wireless controller and redirected to the FortiAuthenticator web login page defined in the FortiGate captive portal profile.
3. FortiAuthenticator presents the user with a login page.
4. The client enters 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.



During the redirection process, user credentials can be communicated, secured and encrypted, to the captive portal server. In the global user settings, you can configure authentication to use HTTP over SSL. In the system global settings, you can specify ports. The default setting is 1003.

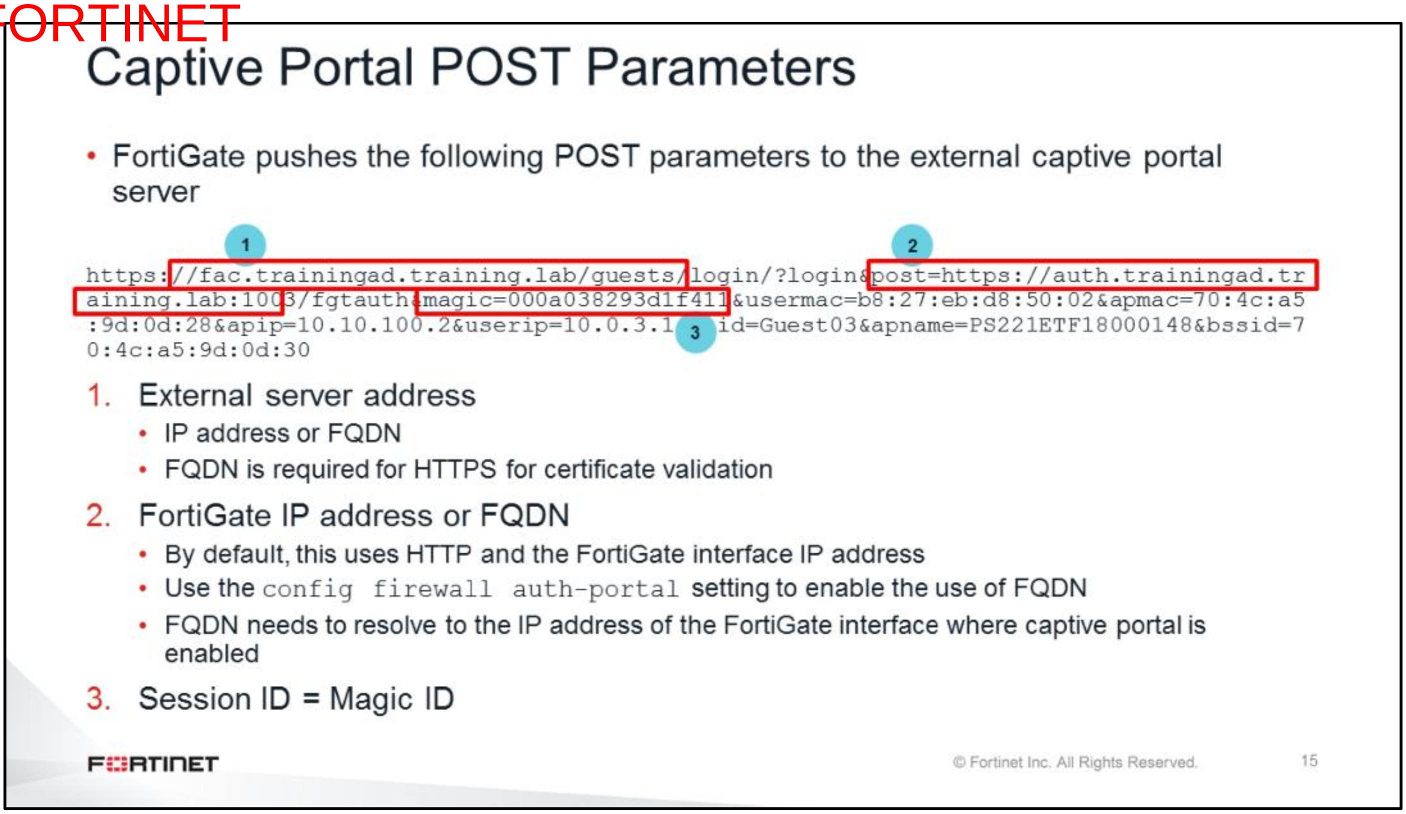
Authentication Certificate

- By default, FortiGate presents users with a factory default certificate on the authentication page
- You can upload your own certificate to use for the user authentication page

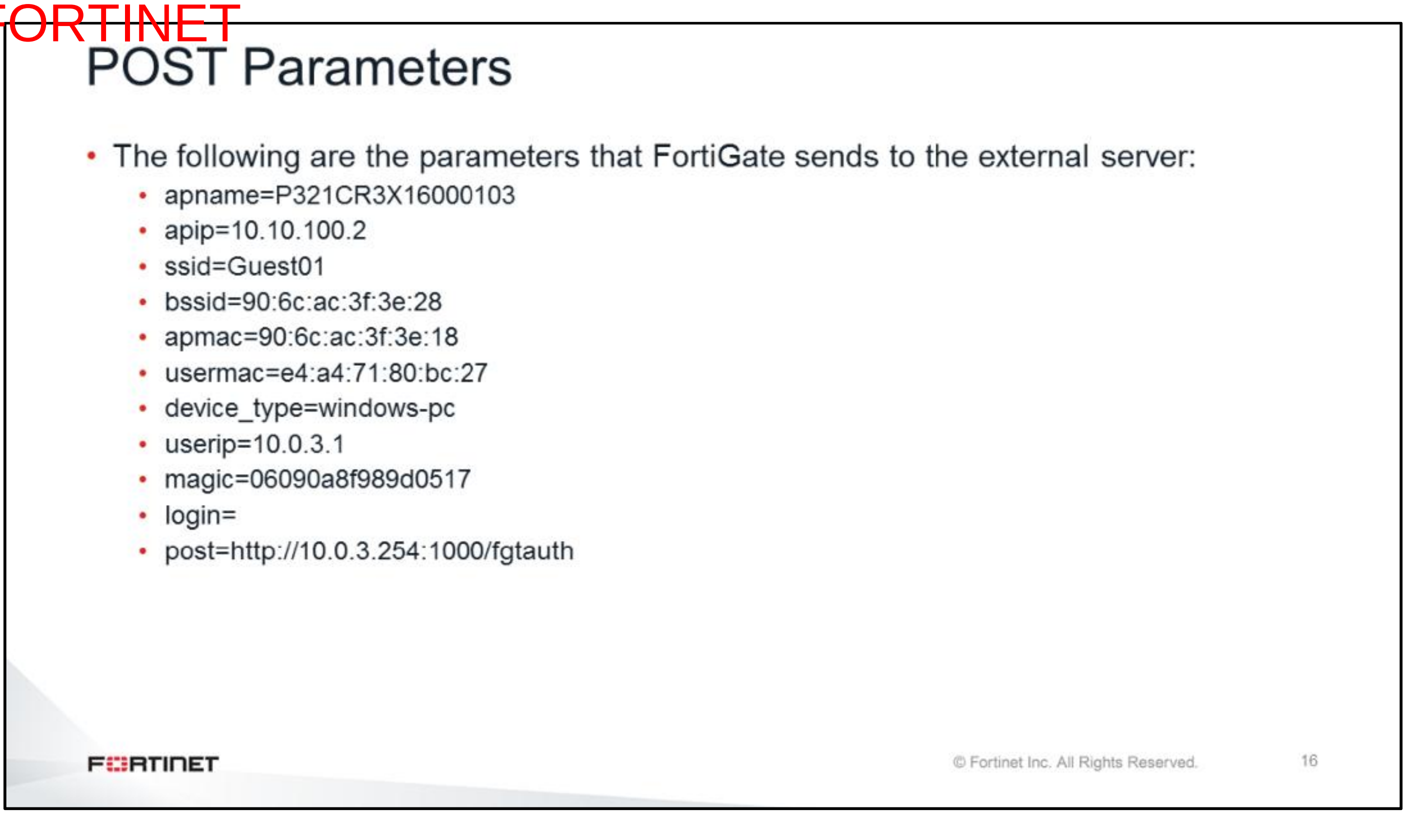


 14

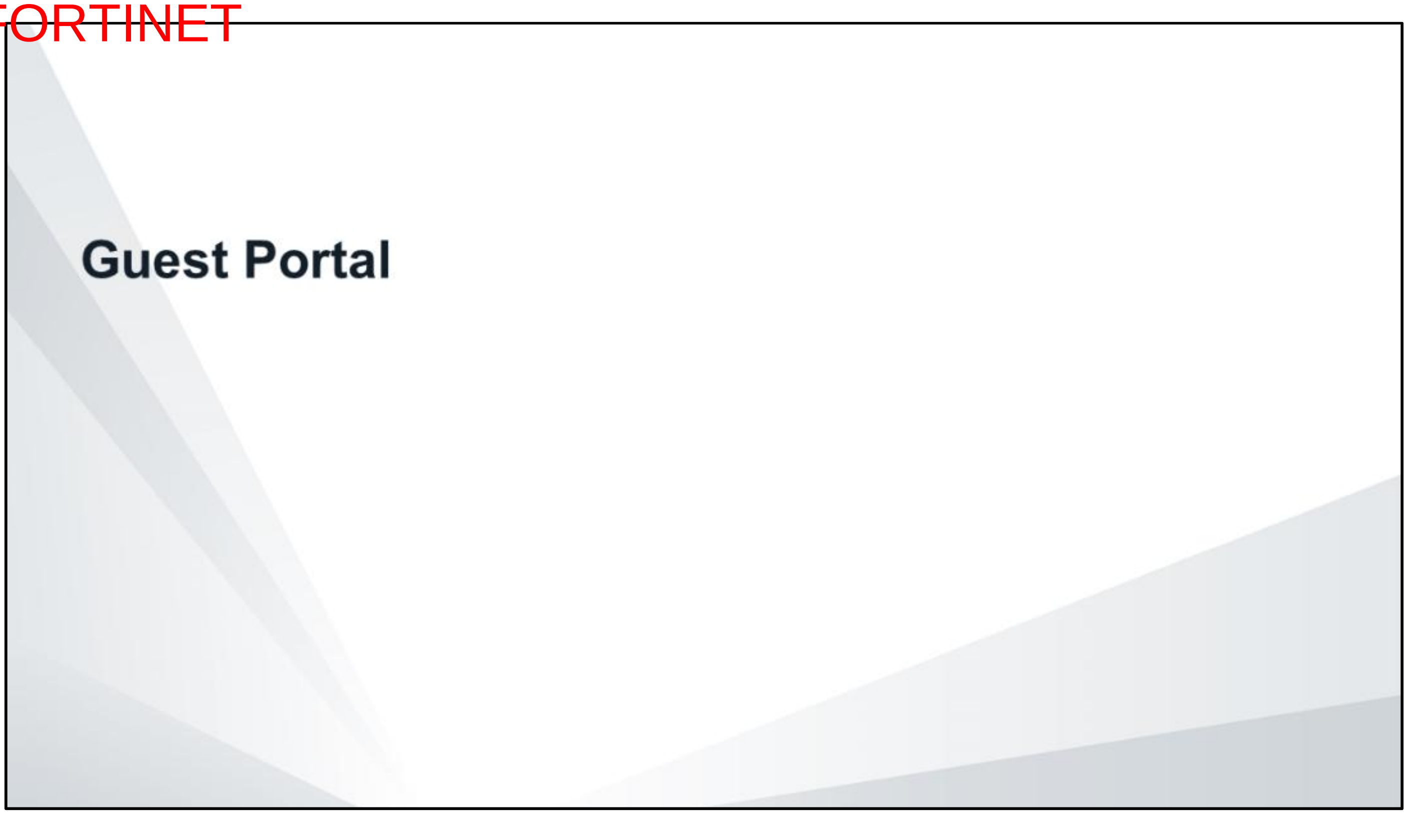
If you redirect the authentication page to an HTTPS page, the configured server certificate is presented. By default, the FortiGate factory certificate is the certificate that is presented. However, you can use another certificate (other than the default) as long as it is generated locally or can be publicly purchased.



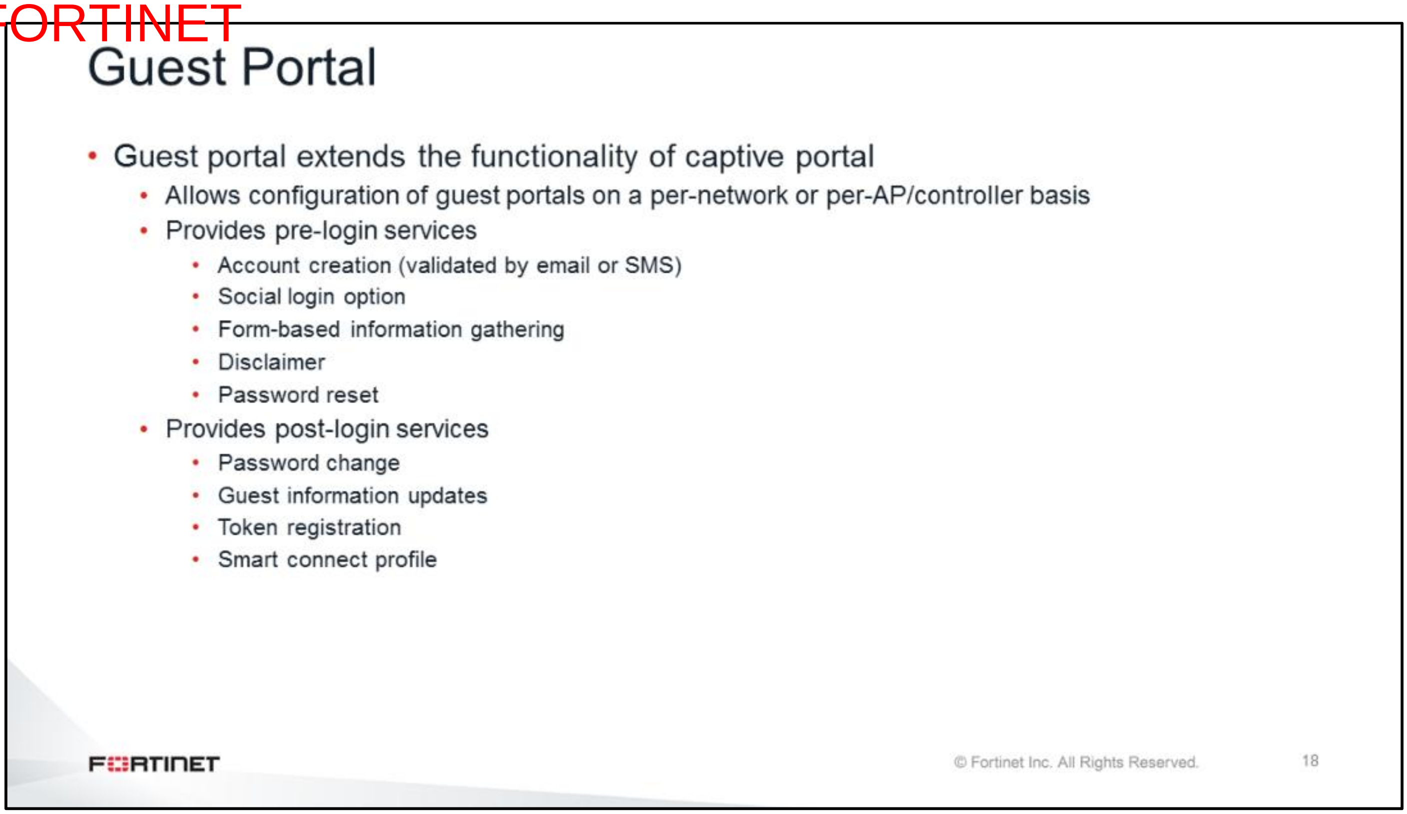
When FortiGate redirects a user to the external captive server, it adds the parameters shown on this slide to the HTTPS request. You can easily decode the information that FortiGate provides to the external captive portal server. The first part of the redirected URL includes the external server's address, 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.



This slide contains a list of all the parameters that are sent to the external captive portal from a wireless network on FortiGate.



In this section, you will learn about guest portal options available on FortiAuthenticator.



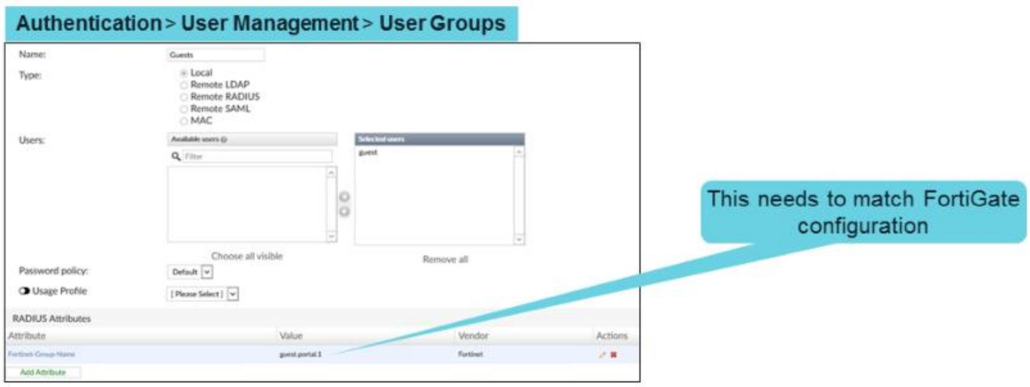
The guest portal on FortiAuthenticator extends the functionality of the captive portal available on FortiGate. The FortiAuthenticator captive portal is available through only one URL. However, but portal match is based on the mapping rules and RADIUS client profile, which makes this type of configuration 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.

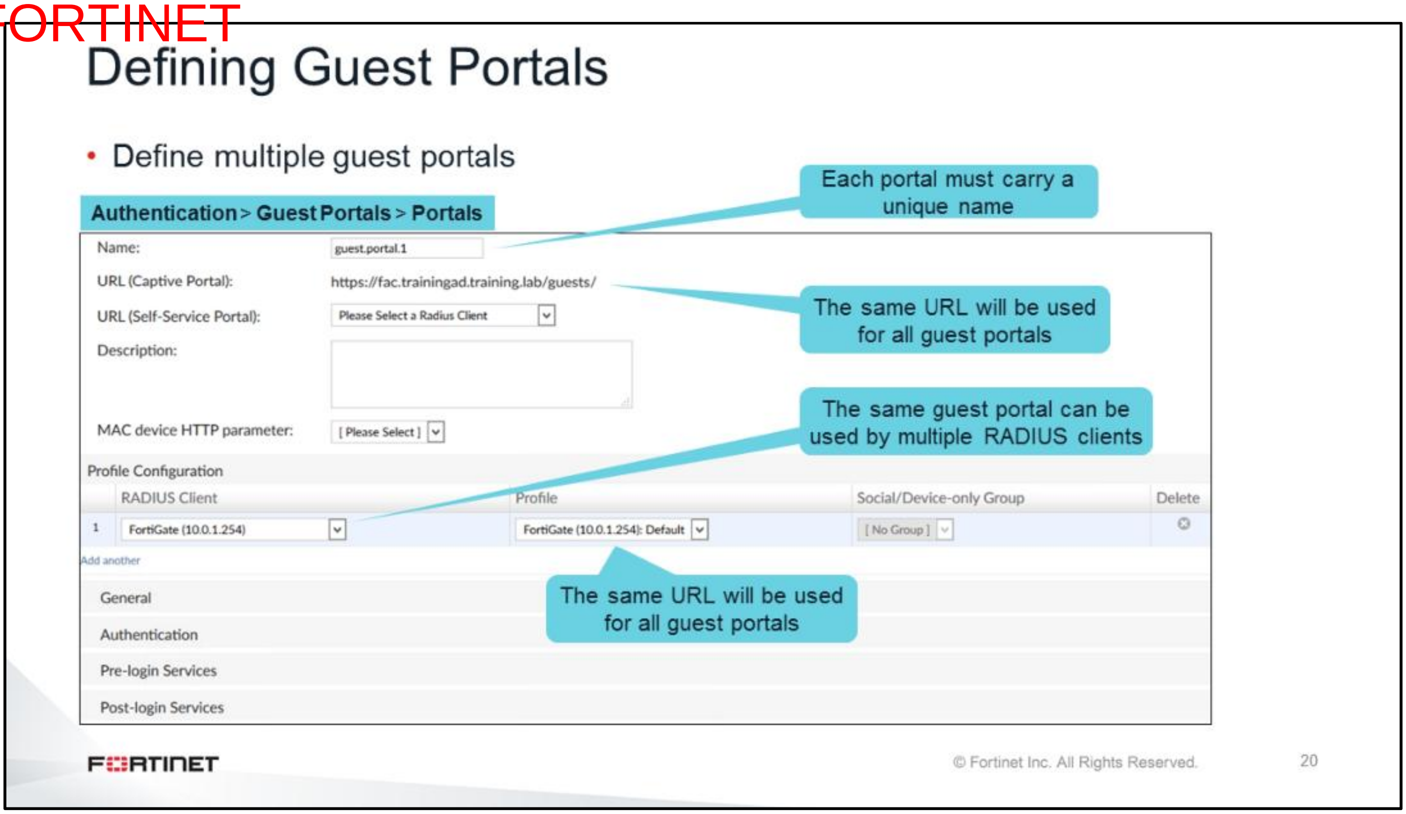
After the user logs in successfully, they can access the post-login services page by visiting FortiAuthenticator’s login page. On that page, users can make changes to their account, such as updating their information, changing their password, downloading a smart connect profile, and performing token registration.

Guest Group

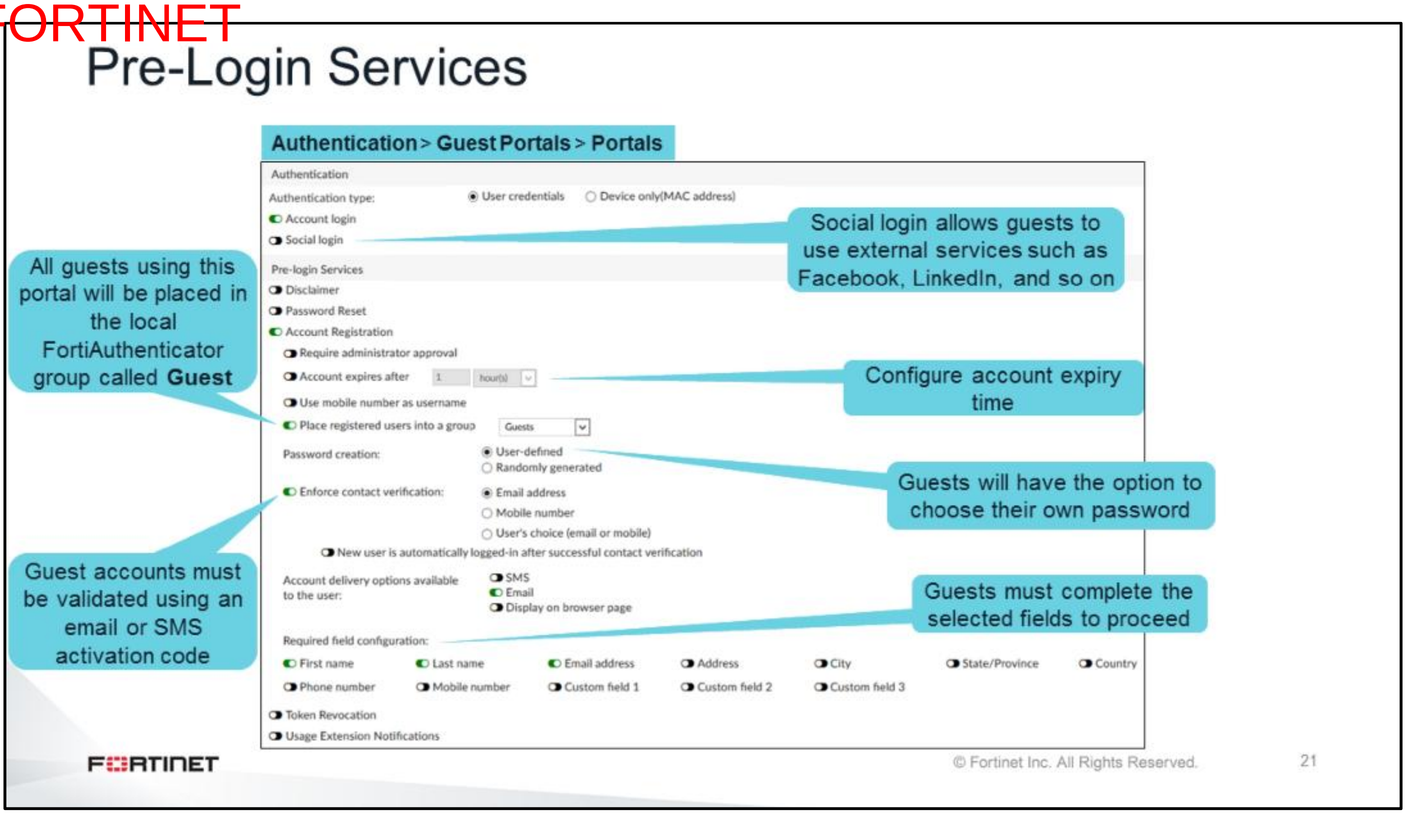
- Create a guest user group
  - Reference this group in the guest portal for automatic mapping of new users
- Configure the RADIUS attribute that is sent to FortiGate after a successful authentication
  - FortiGate uses the group name sent to assign authorization to users



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 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.



You can define guest portals on the **Portals** configuration page using the FortiAuthenticator GUI. All portals will be accessible on the same URL, but the mapping of the portals will depend on the mapping rules defined. Each portal must be configured with a unique name. You can reference multiple RADIUS clients or profiles within the same guest portal. This allows you to accept authentication requests for the same guest portal from multiple devices.

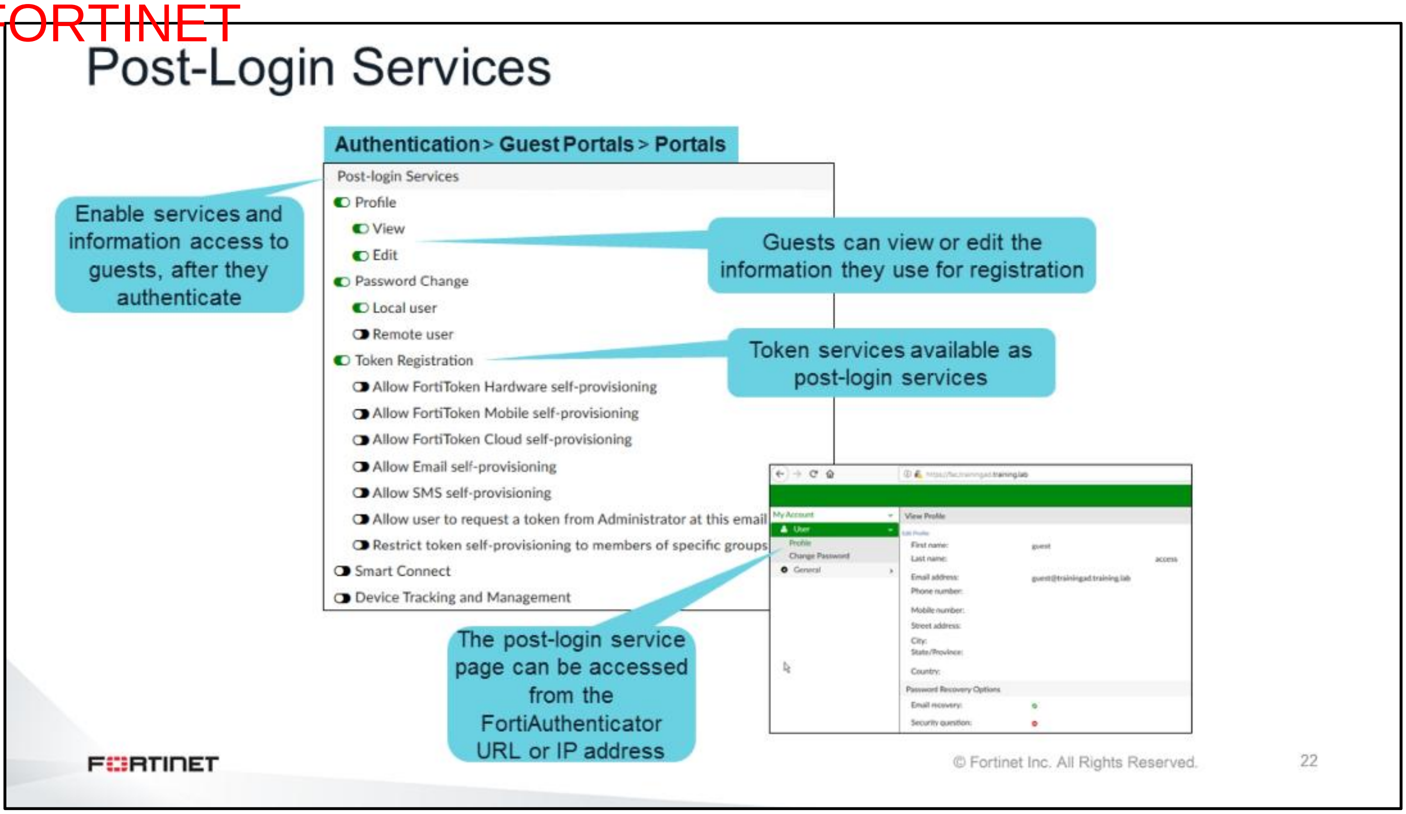


Within the guest portal configuration, you can also define the type of authentication (user or device) as well as whether you want to use it for account login and/or social login. The Social login option allows users to authenticate using third-party SSO services such as Facebook, LinkedIn, and so on. 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.

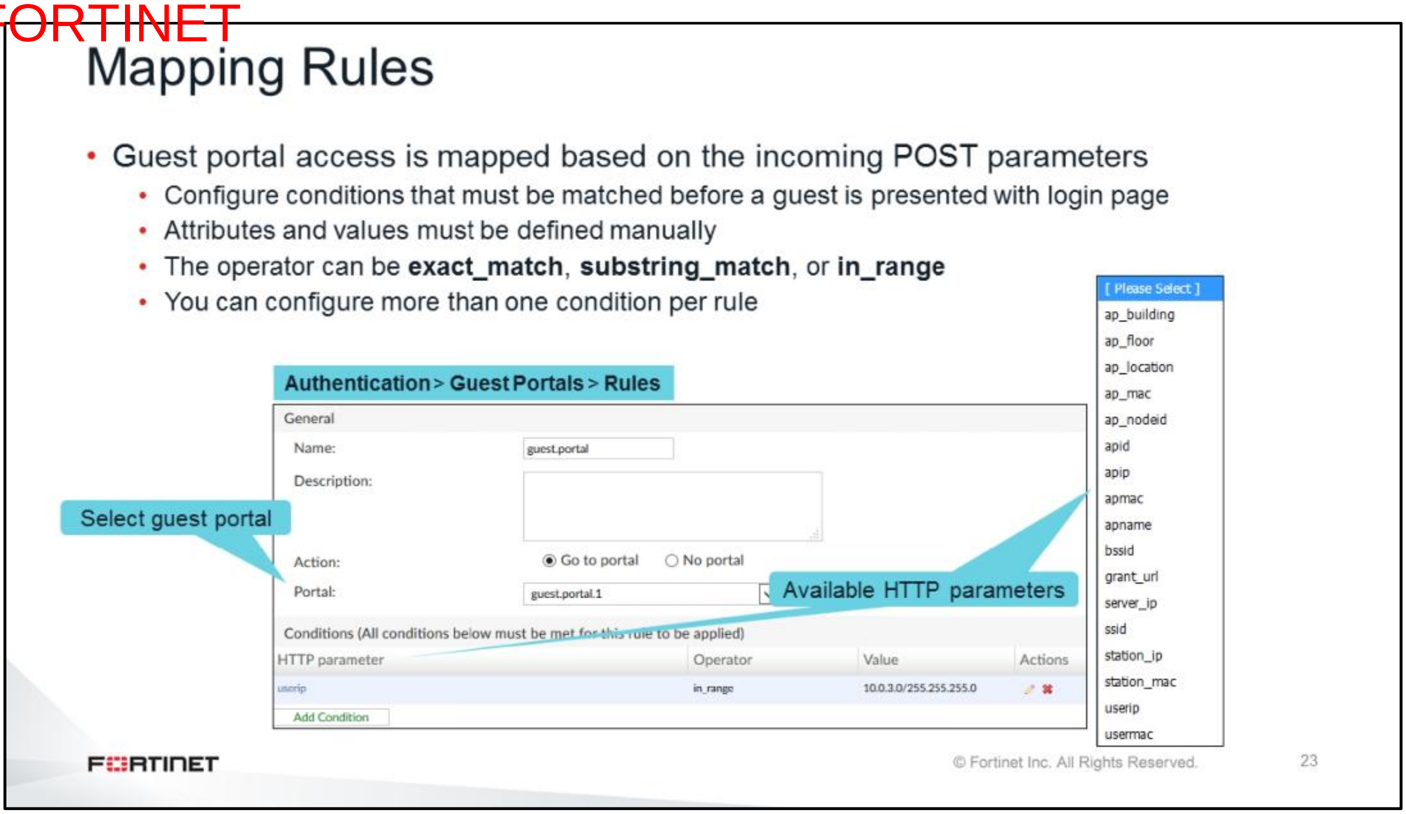
After you complete configuration in the **Authentication** section, you can enable the pre-login services that you would like to use for this guest portal. The **Account Registration** option enables guest users to create and validate their account using a form-based web page. The **Account expires after** option allows you to configure the account validity period. This setting will be applied to all self-registered accounts. You can also enable the administrator approval option, which would require an administrator to manually enable all self-registered accounts.

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. FortiAuthentication 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 are 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.

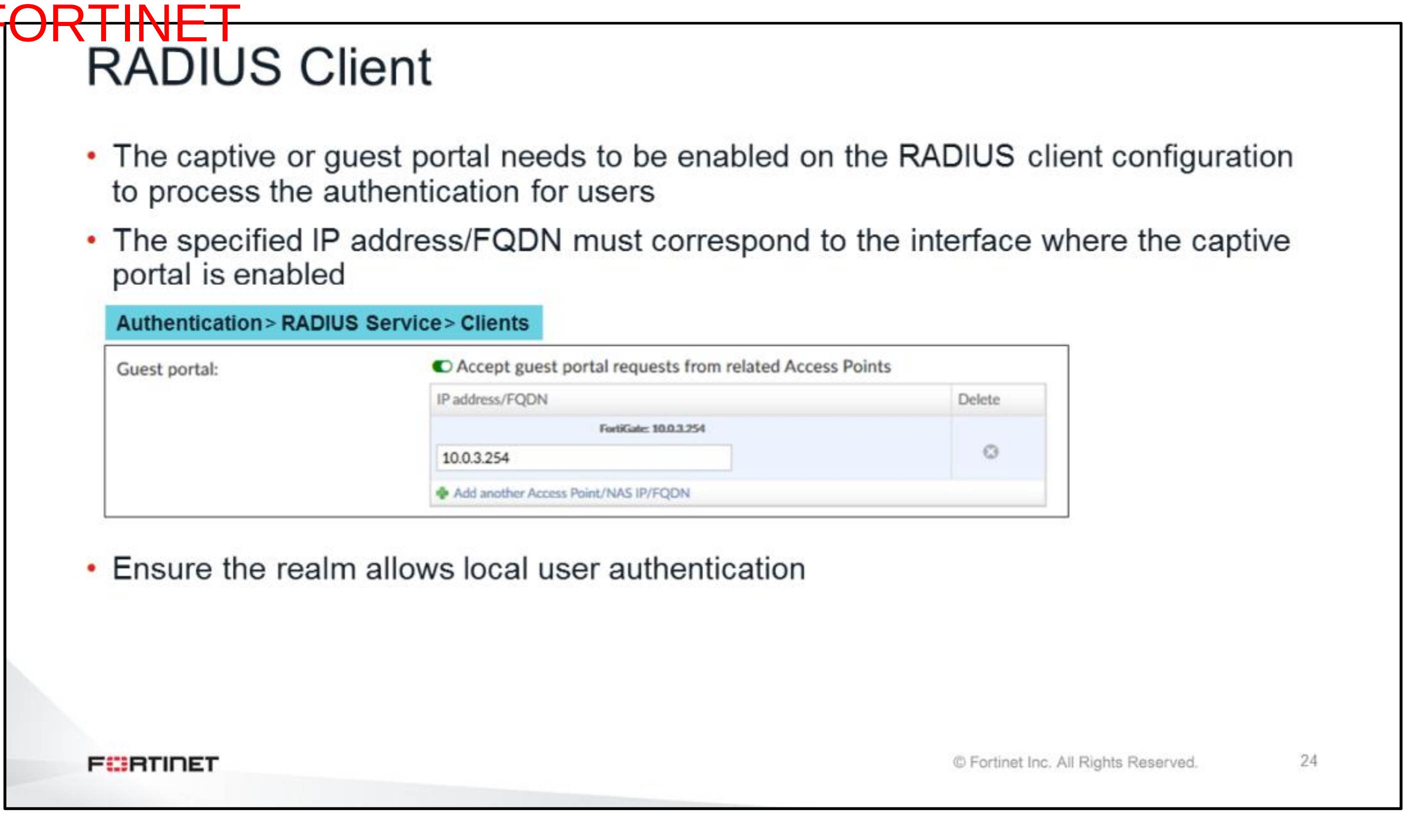
You can select the mandatory field that a user must fill out at the time of account registration. The selected field can not be left empty. The **Token Revocation** option adds a **"Lost my token"** link to the guest portal token verification page. Users can click this link if they need to request that their existing mobile token be reprovisioned, switch to an email token, or disable their account.



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.

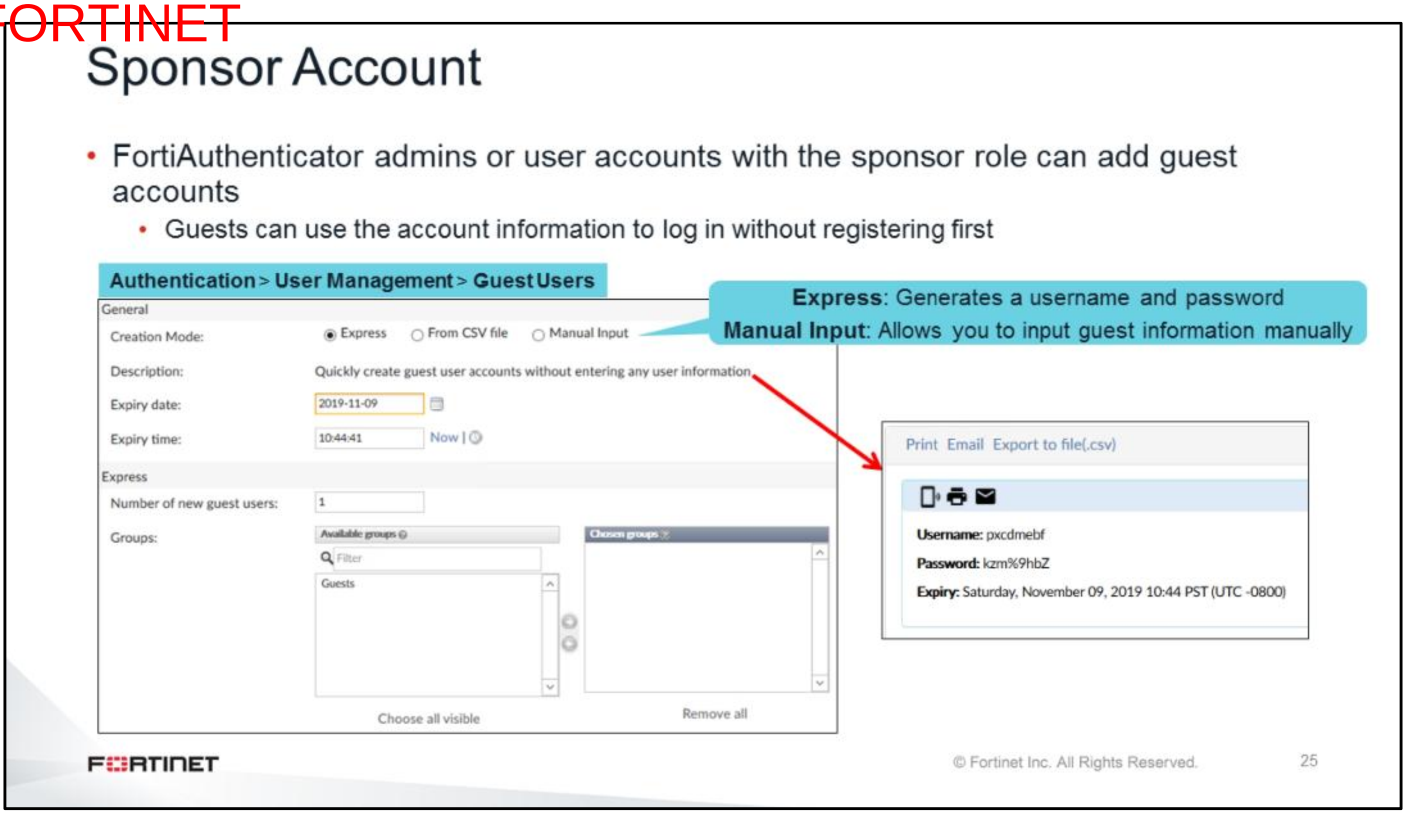


Guest portal rules use the incoming POST parameters and conditions defined within the rules to map the request to guest portals. You can define one or multiple conditions that must be matched to the POST parameter before a captive portal request is mapped to a guest portal login. You can select an HTTP 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.



RADIUS clients must be configured to accept the **Captive/Guest portal** authentication service. This allows RADIUS clients to send authentication requests to FortiAuthenticator from the IP/FQDN specified. If you disable this option, the RADIUS client will not be able to authenticate users using captive or guest portals.

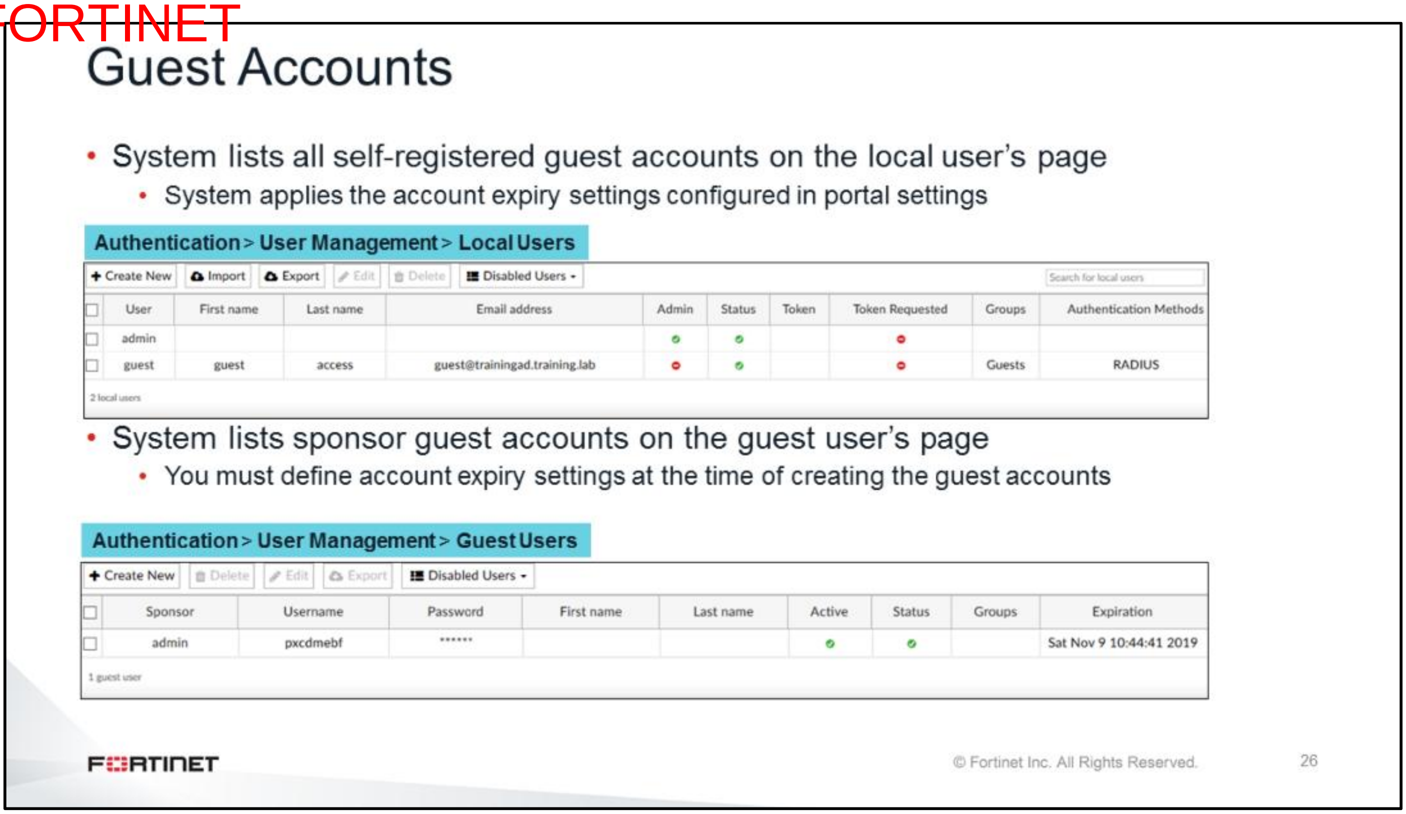
Note that self-registered guest users will be added to the local FortiAuthenticator database. Make sure that the RADIUS profile is configured to use a realm that allows the processing of local user authentication.



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 creates the 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 or guest accounts that you want to sponsor and groups that are assigned to it. After an account is created, FortiAuthenticator will display the login information. You can choose to send this information to guests directly using SMS or email. Alternatively, you can print the login information.

From CSV file creation mode allows administrators to create one or more guest accounts using parameters from a CSV file. **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.

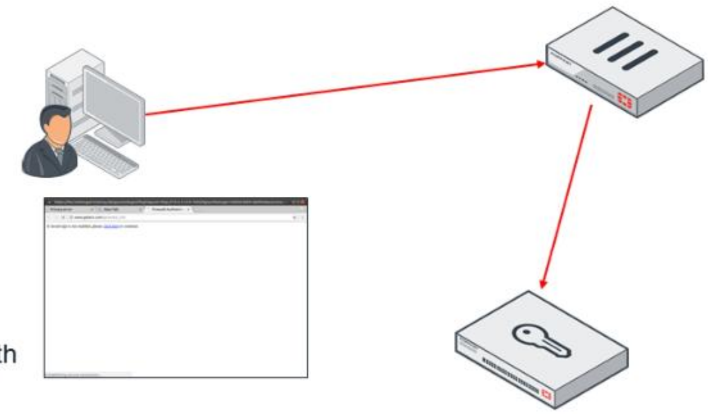


It is important to note that all the self-registered guest accounts will be listed on the **Local Users** page on the FortiAuthenticator GUI. The system will automatically assign an expiry date to all self-registered users as defined in the guest portal settings.

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.

Guest Portal Workflow

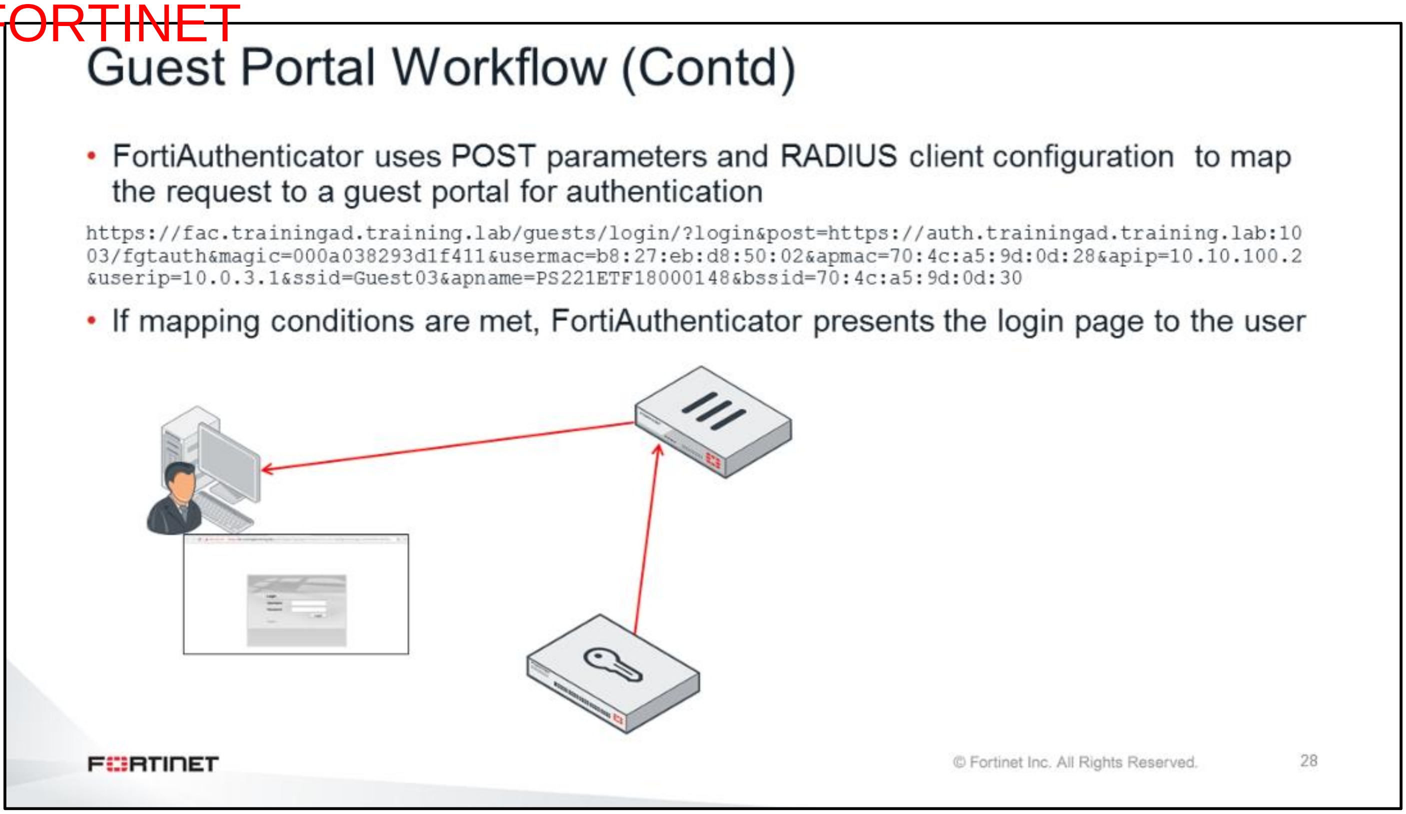
- FortiGate receives HTTP GET requests from users
- Redirects them to FortiAuthenticator
- FortiGate collects and sends the following POST parameters to FortiAuthenticator:
  - apname=P321CR3X16000103
  - apip=10.10.100.2
  - ssid=Guest01
  - bssid=90:6c:ac:3f:3e:28
  - apmac=90:6c:ac:3f:3e:18
  - usermac=e4:a4:71:80:bc:27
  - device_type=windows-pc
  - userip=10.0.3.1
  - magic=06090a8f989d0517
  - login=
  - post=http://10.0.3.254:1000/fgtauth



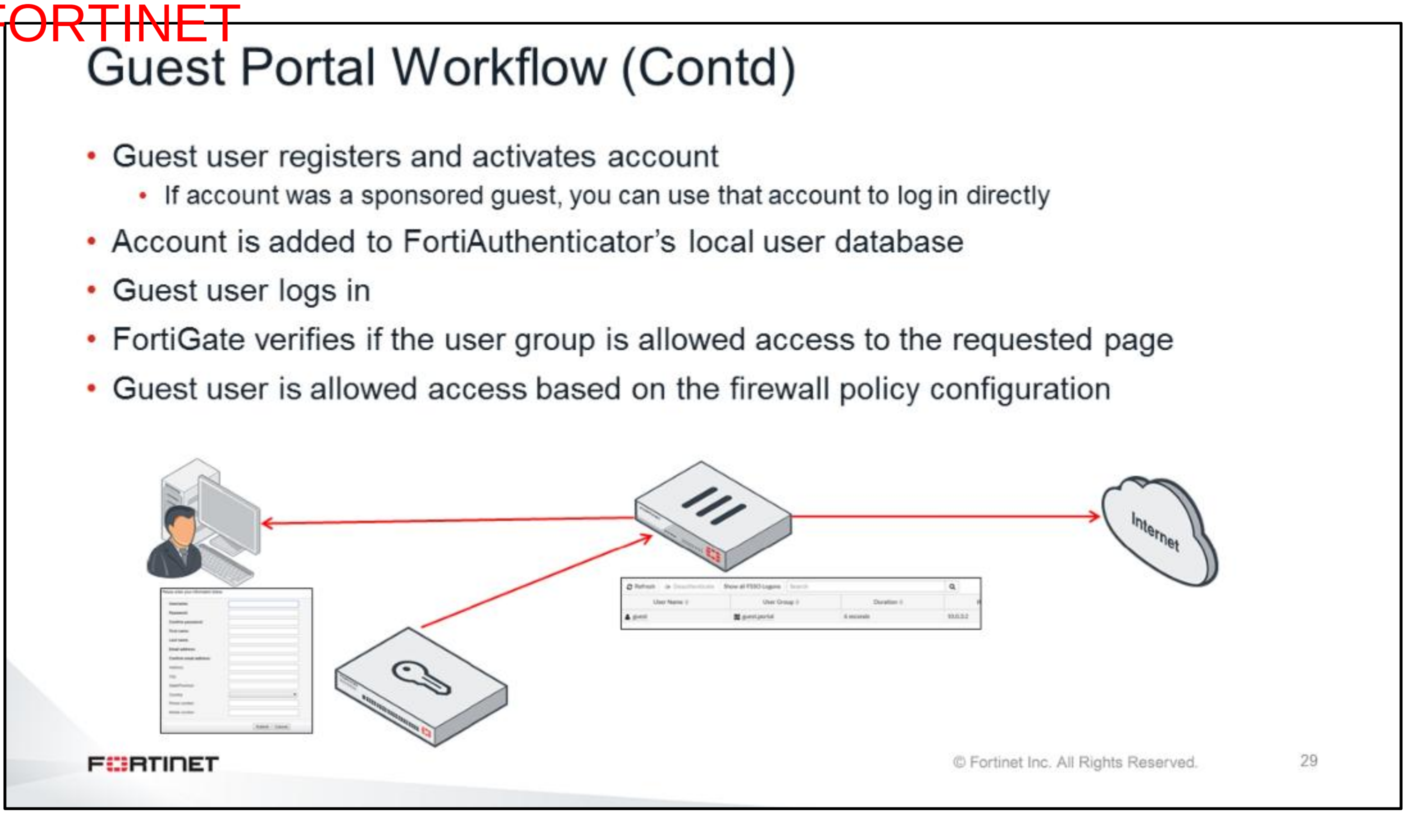
FORTINET

27

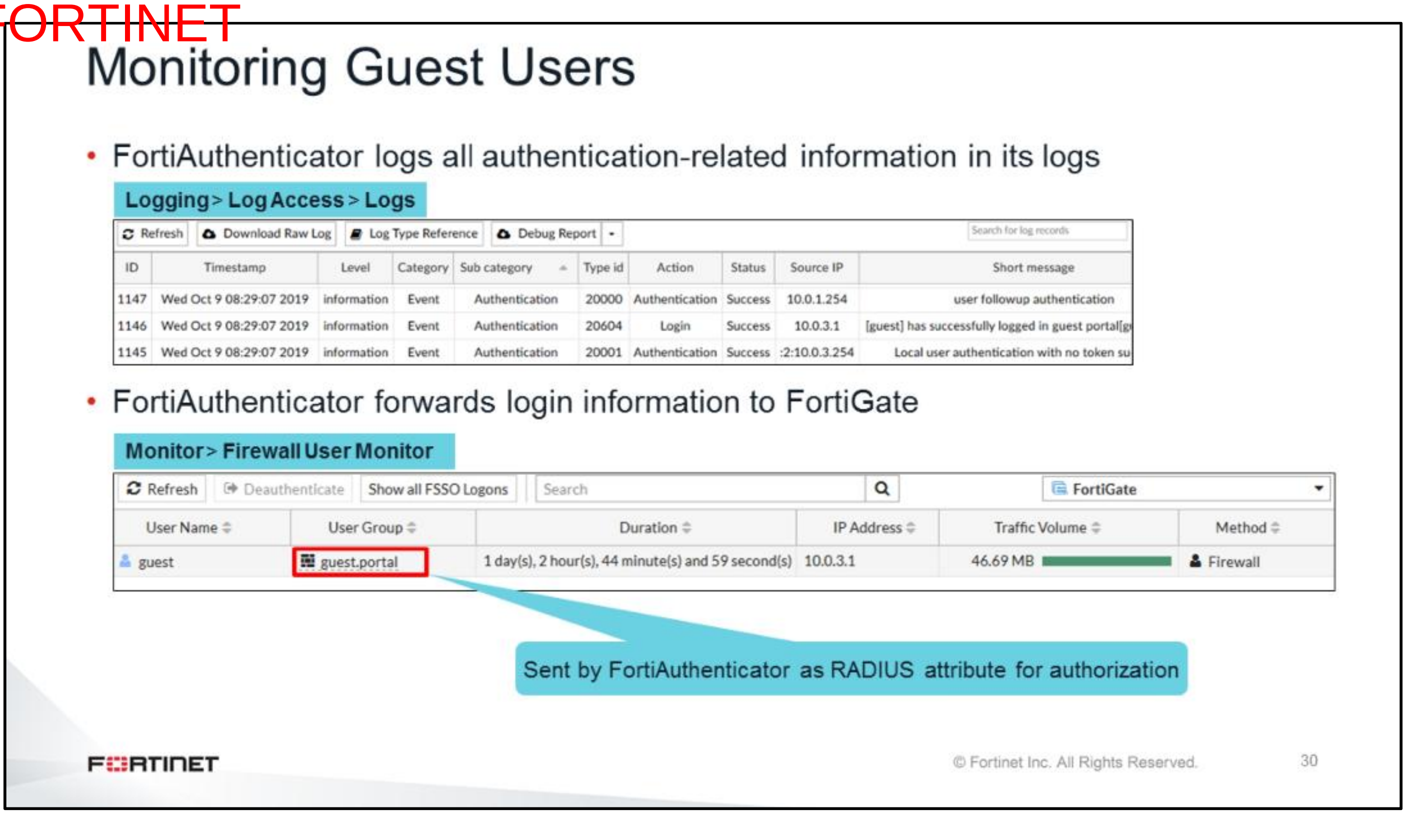
Now, you'll review the guest portal workflow. A client connects to a captive portal network on FortiGate. The client tries to visit a website. FortiGate receives an HTTP GET request from an unauthenticated user. It redirects the user to the captive portal URL along with the POST parameters.



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.



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 and/or phone number, FortiAuthenticator will send them an activation code. This activation code is a request to finish the self-registered account creation process. Once 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. Once 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.

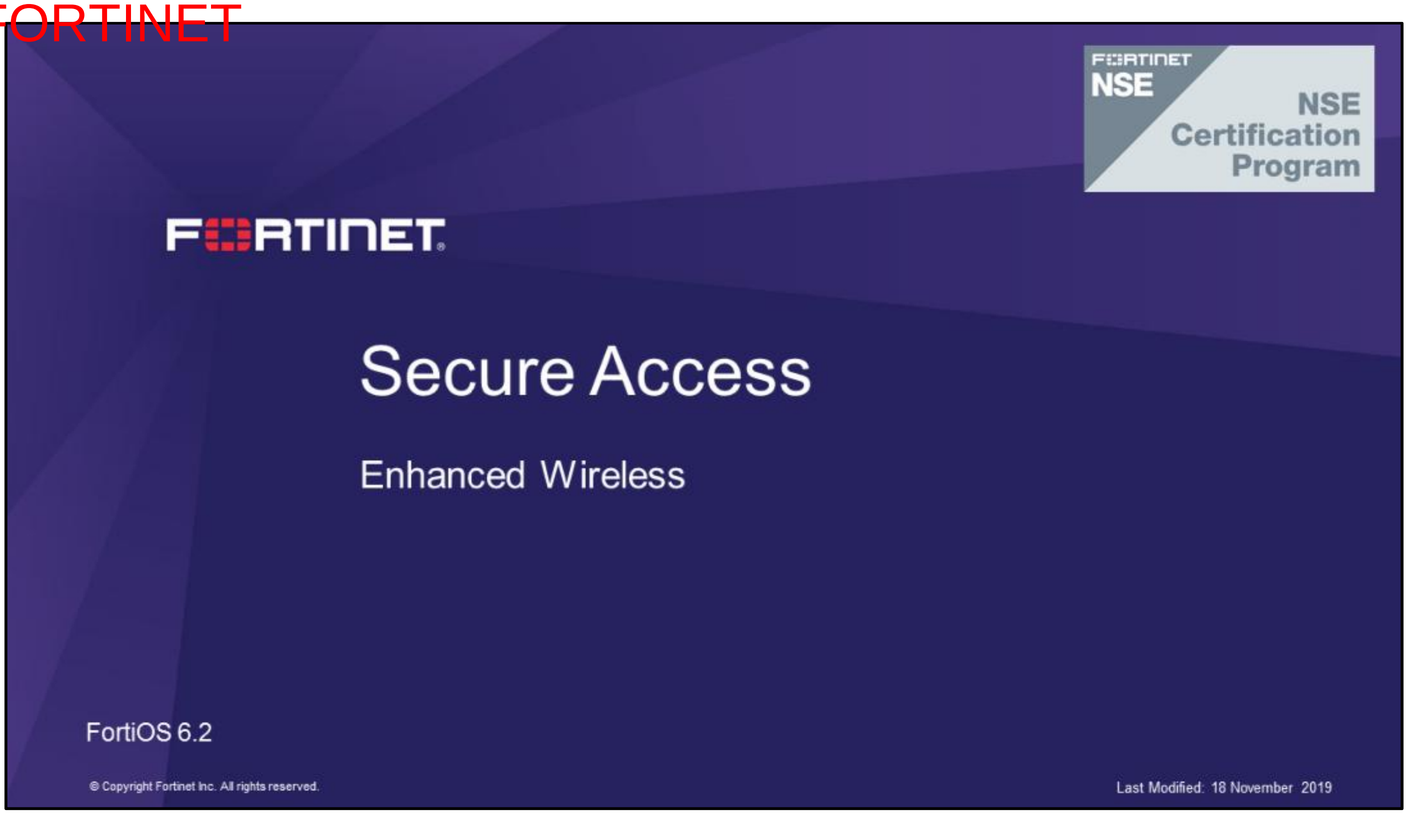


FortiAuthenticator logs all authentication-related information. This information includes username, time of authentication, status, IP address, guest portal used to authenticate, and so on. You can view active user sessions on FortiGate on the **Firewall User Monitor**, which lists the username, user group, duration of the session, and IP address.

Review

- ✓ Configure guest access SSID
- ✓ Configure captive portal
- ✓ Understand the captive portal packet flow
- ✓ Provision the guest portal
- ✓ Understand the guest portal workflow
- ✓ Monitor guest accounts

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

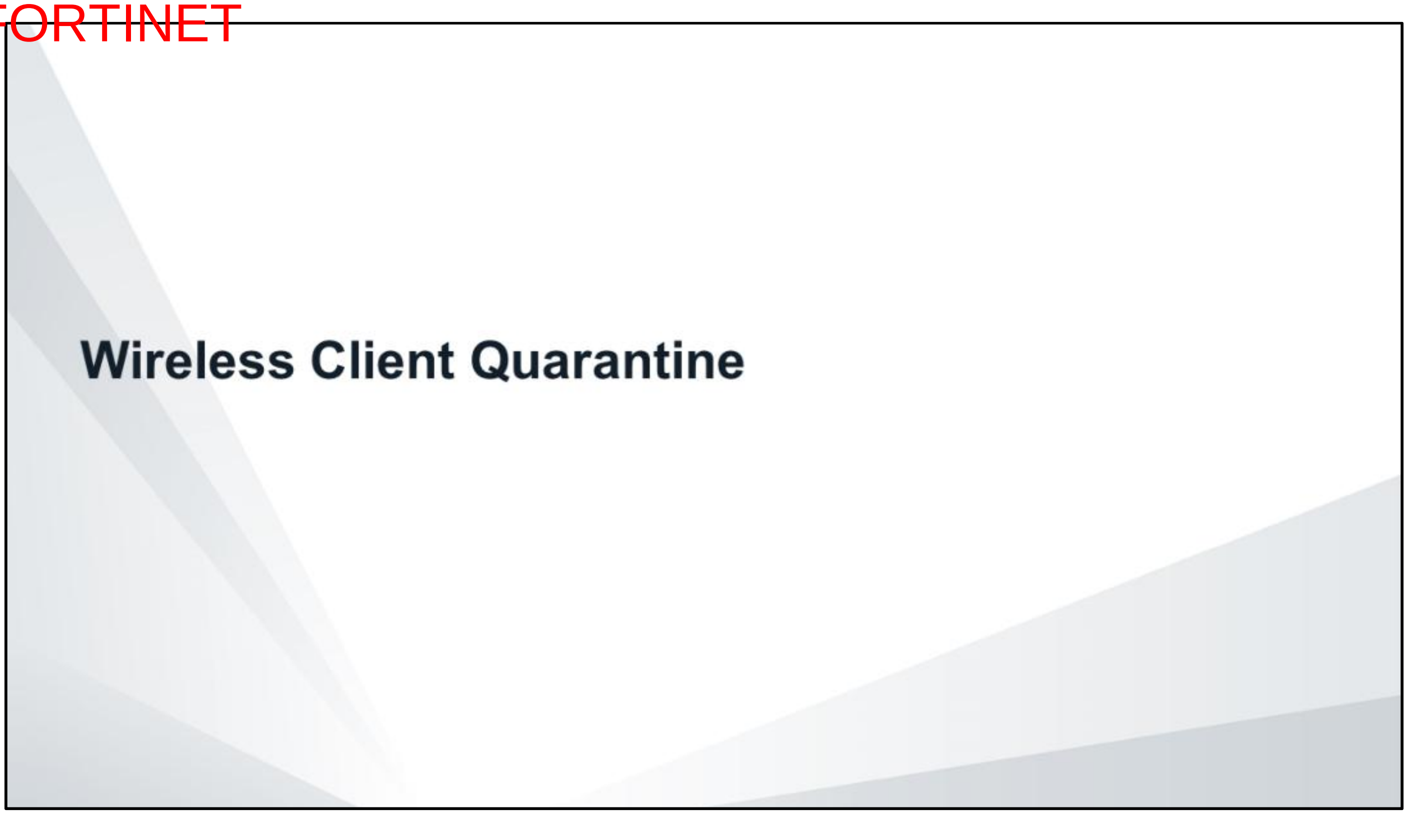


In this lesson, you will learn more about securing, troubleshooting, and, best practices for integrated wireless features in FortiOS.

Objectives

- Quarantine wireless clients
- Configure wireless intrusion detection system (WIDS)
- Perform wireless monitoring
- Perform wireless troubleshooting
- Implement wireless best practices

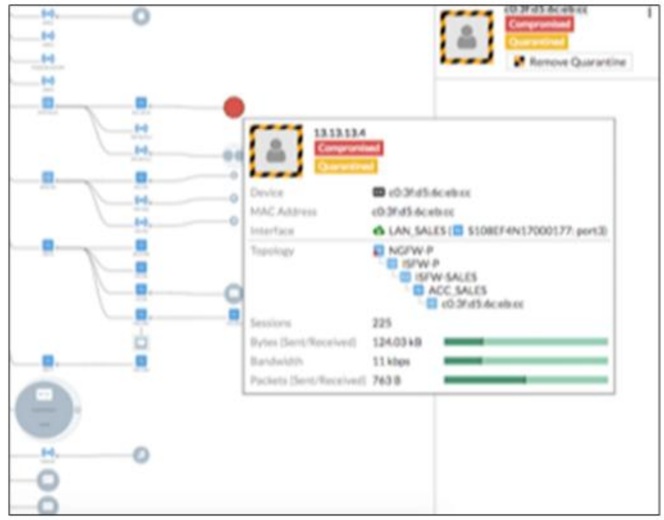
After completing this lesson, you should be able to achieve the objectives shown on this slide.



In this section, you will learn how wireless clients are quarantined on a FortiGate controlled wireless network.

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



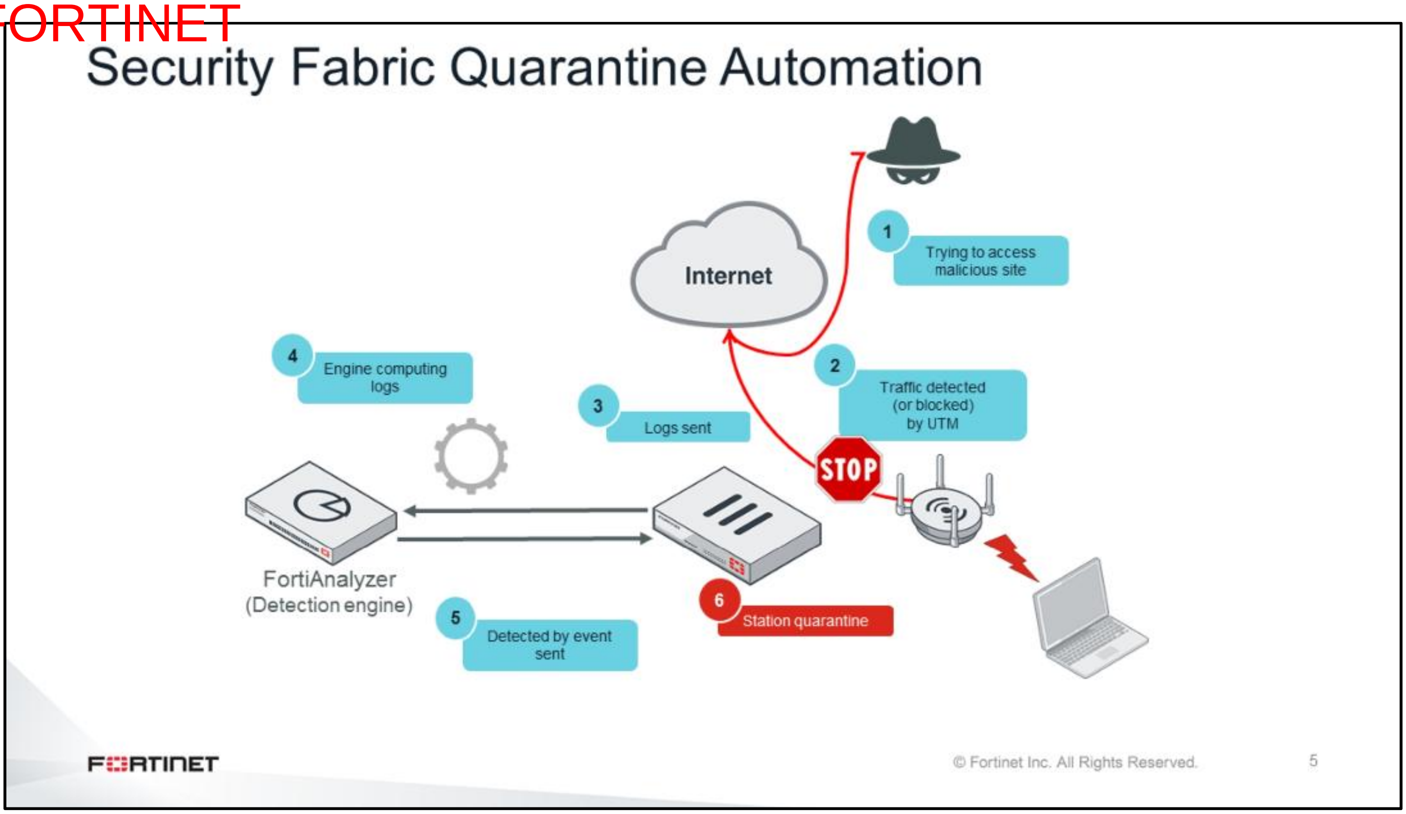
FORTINET

 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.

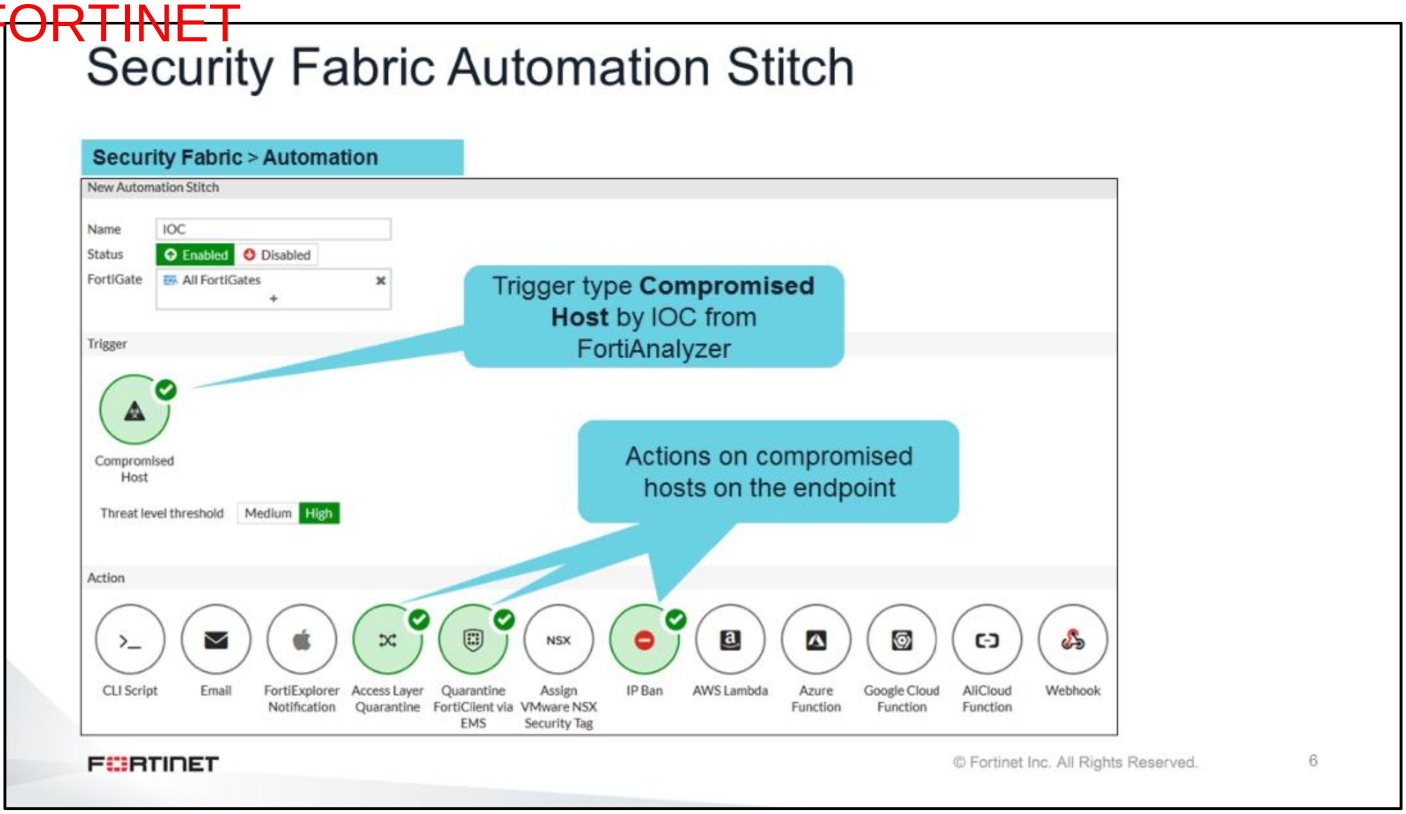
Compromised IOT type devices will be isolated. Any other types of devices, such as a guest device, will also be isolated when they become compromised, but these devices will have the option to remediate themselves, if required.



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 stations and place them in quarantine. The flow of events is as follows:

1. A station 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 station and places it in isolation.



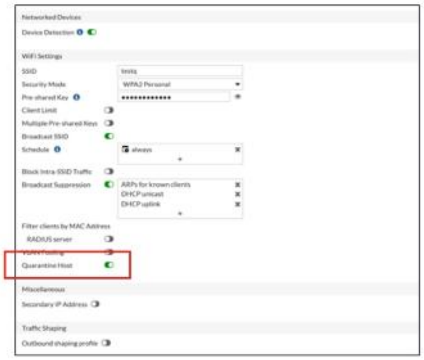
Compromised wireless hosts are treated in the same way as compromised wired hosts; FortiAnalyzer identifies them using threat detection services, and then sends the IOC verdict to the root FortiGate of the Security Fabric group.

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. IP Ban is a Layer 3 action that bans the host machine based on its IP address.

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 only filter on a FortiGate level



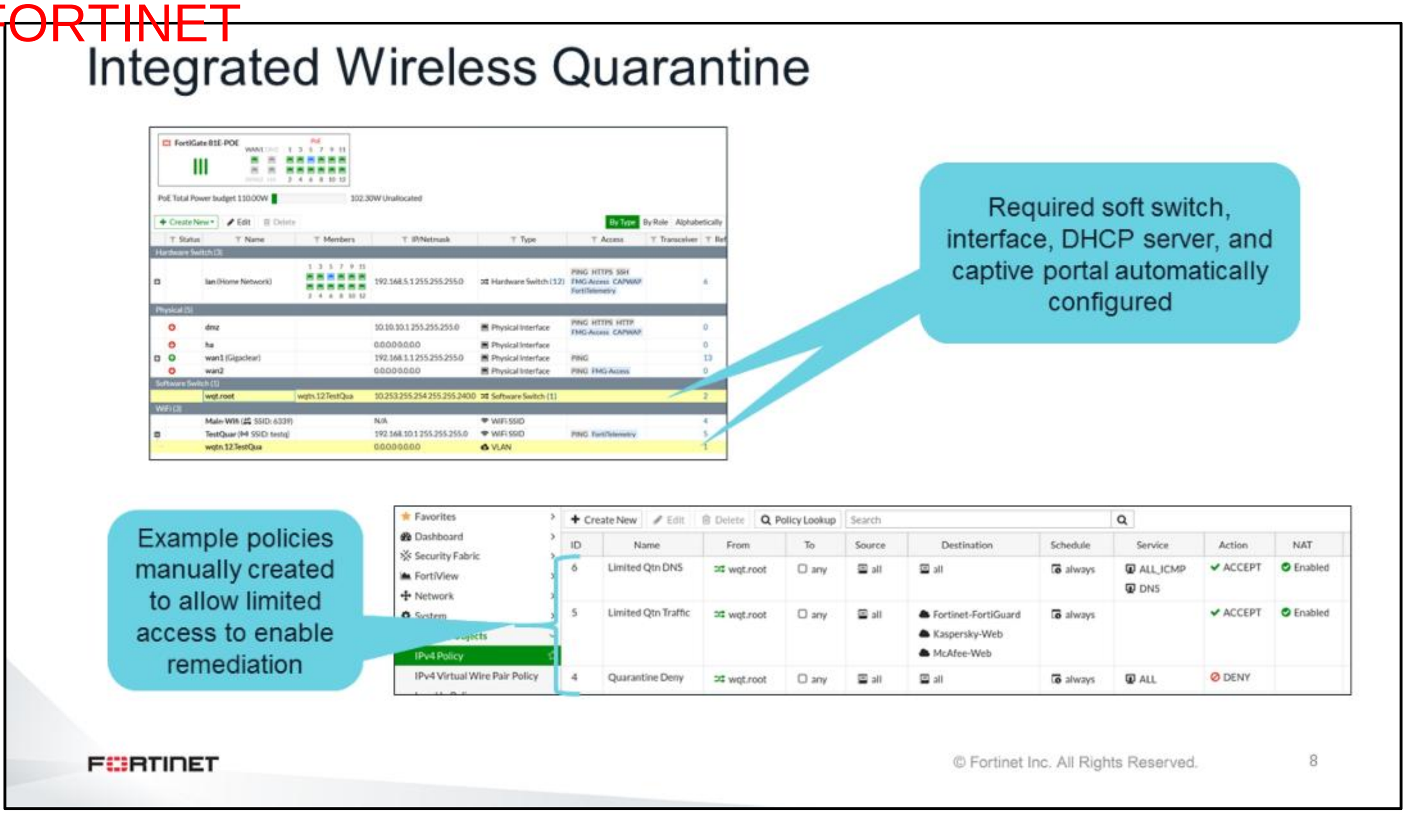
 7

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 a 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.

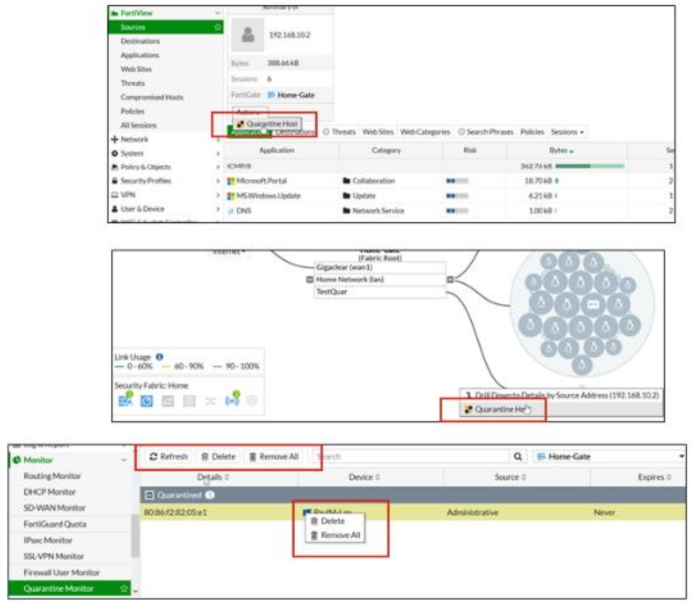
Once configured, wireless clients can be automatically quarantined using the same Security Fabric automation stitches as used for wired clients. Clients that are quarantined, are placed in their own isolated VLAN and then presented with a captive portal informing them that they are now isolated. You can configure this captive portal in the same way as any other captive portal, to give them information on how to remediate their device.



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.

Manual Client Quarantine

- Wireless clients can be manually quarantined, if required
  - Security Fabric
  - FortiView
- Quarantined hosts will be placed in the quarantined VLAN
- Quarantined hosts can be managed from:
  - **Monitor** > **Quarantine Monitor**



FORTINET

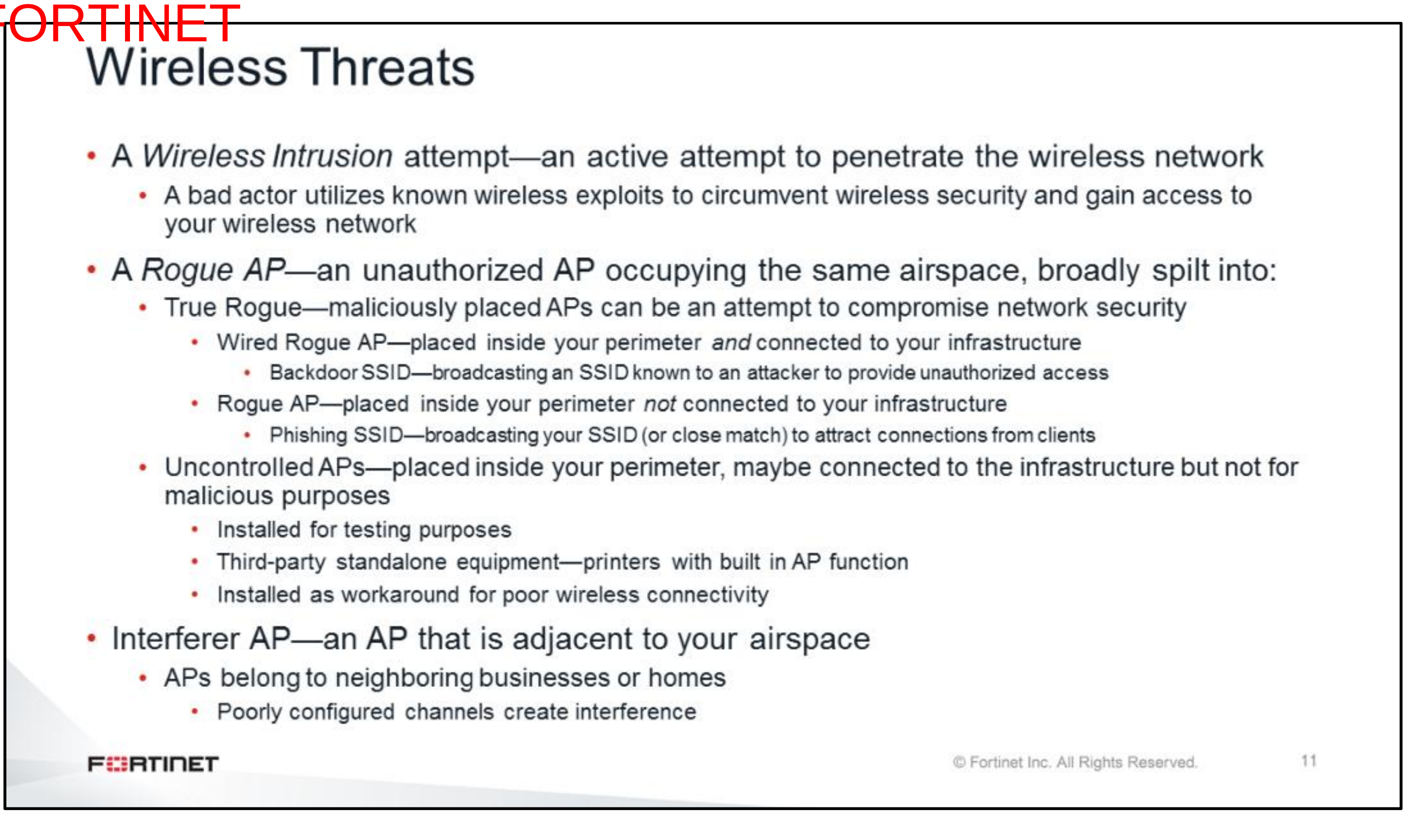
 9

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 Monitor**.

WIDS and Rogue AP Management

In this section, you will learn how to implement WIDS and configure it to detect and manage rogue APs and SSIDs.



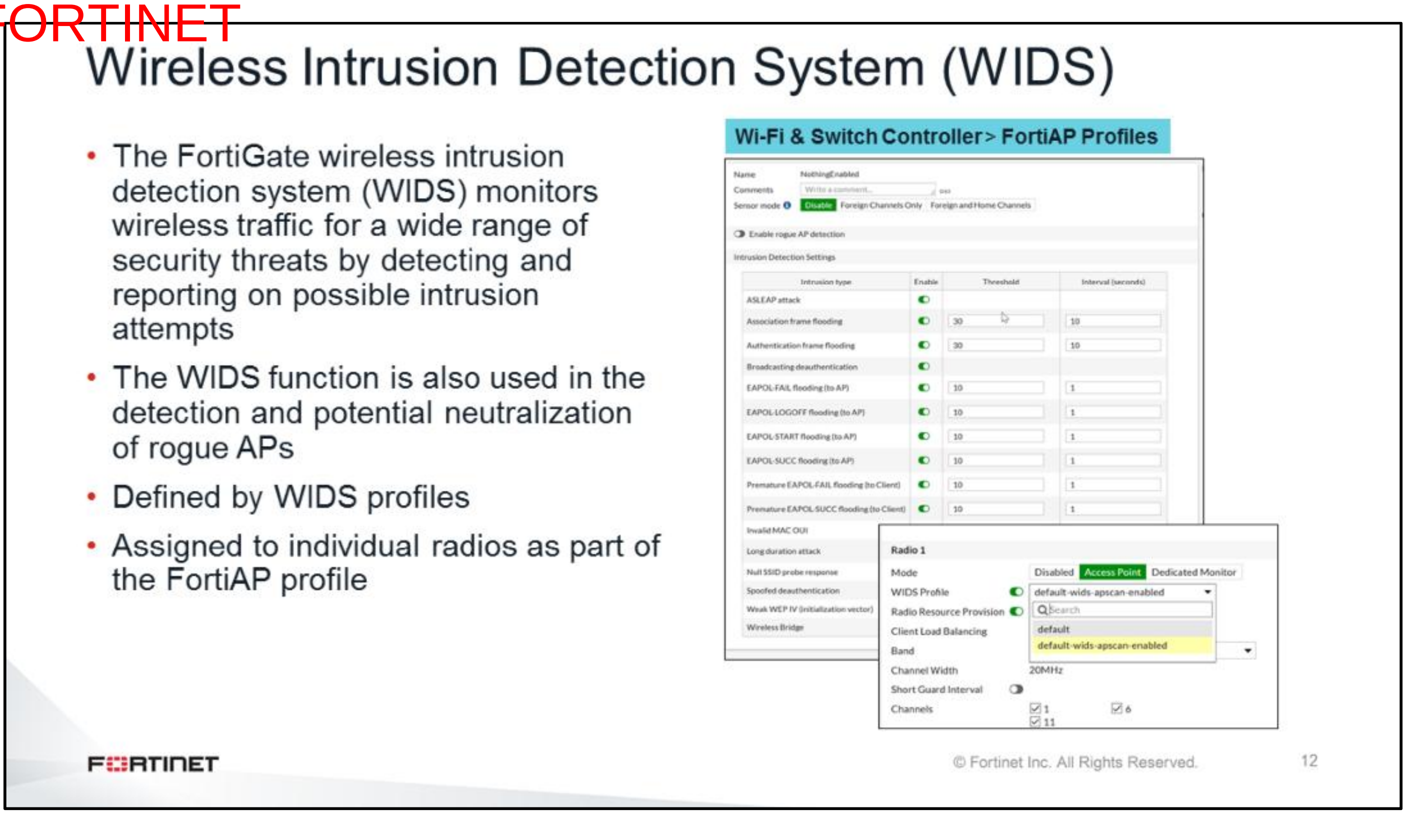
Wireless networks are increasingly popular as vectors for bad actors to gain access to the network. The inability to fully control where a wireless signal will propagate make it an attractive medium to use when either attacking a network directly, or, indirectly by setting honeypots to trap unsuspecting 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, 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 the purpose for being there; a true rogue AP is placed maliciously to either provide unauthorised access to your network using a backdoor SSID known to the attacker, or access to clients 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.



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.

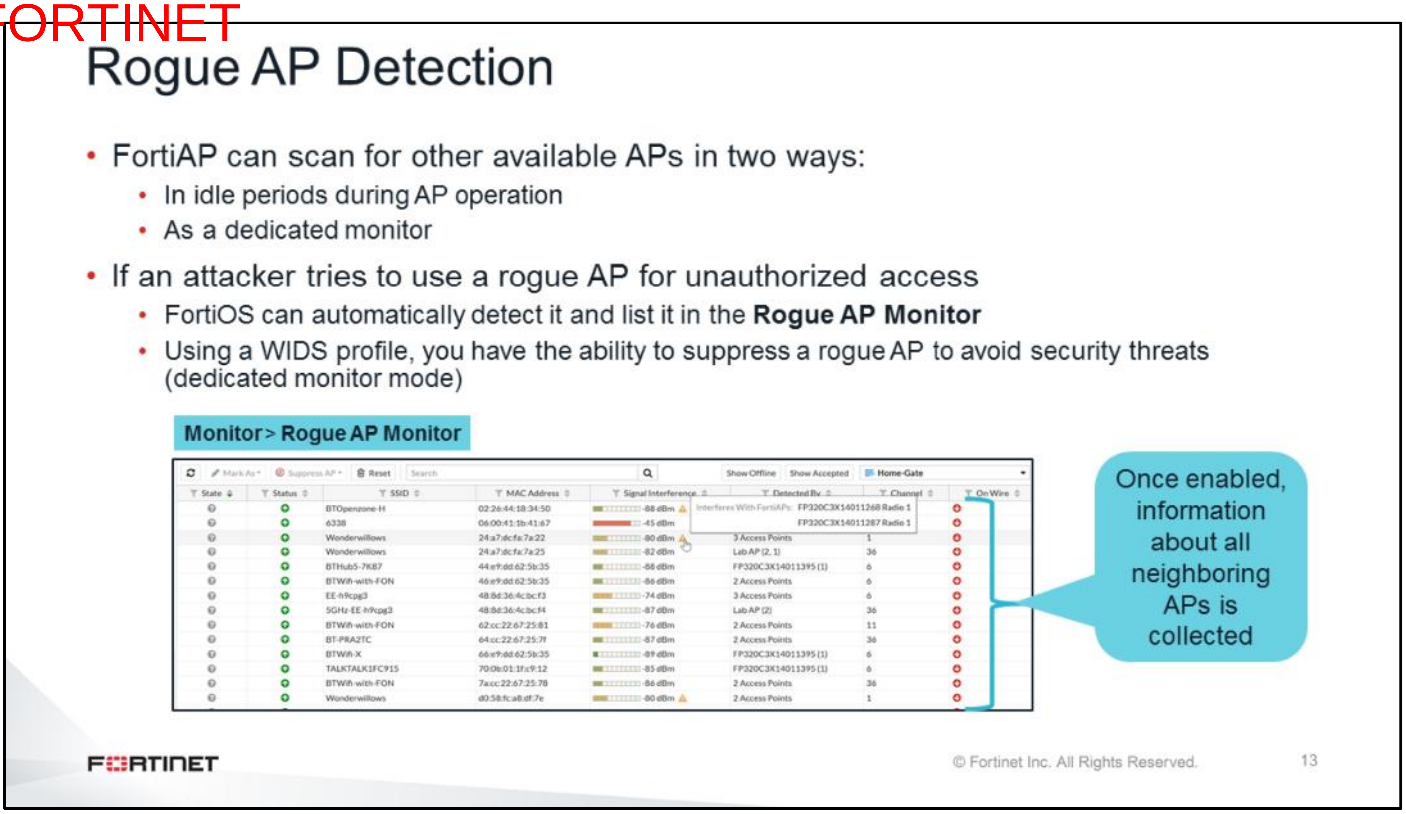
You can configure WIDS in the profile, which allows the detection of a wide range of Wi-Fi-specific security threats by detecting and reporting on possible intrusion attempts, such as:

- Weak WEP IV encryption used to crack WEP keys
- Null SSID probe response that causes many wireless cards and devices to stop responding
- De-authentication broadcasts are a denial of service (DoS) attack causing all clients to disconnect from the AP
- Invalid MAC OUI—The first three bytes of the MAC address are the Organizationally Unique Identifier (OUI), administered by IEEE
- Various management, EAP, authentication, and beacon floods

When enabling the different options, some will be found to have configurable thresholds and intervals. Alteration of these options is not normally required.

You can also enable rogue AP detection in the FortiAP profile, and you can choose how to enable it.

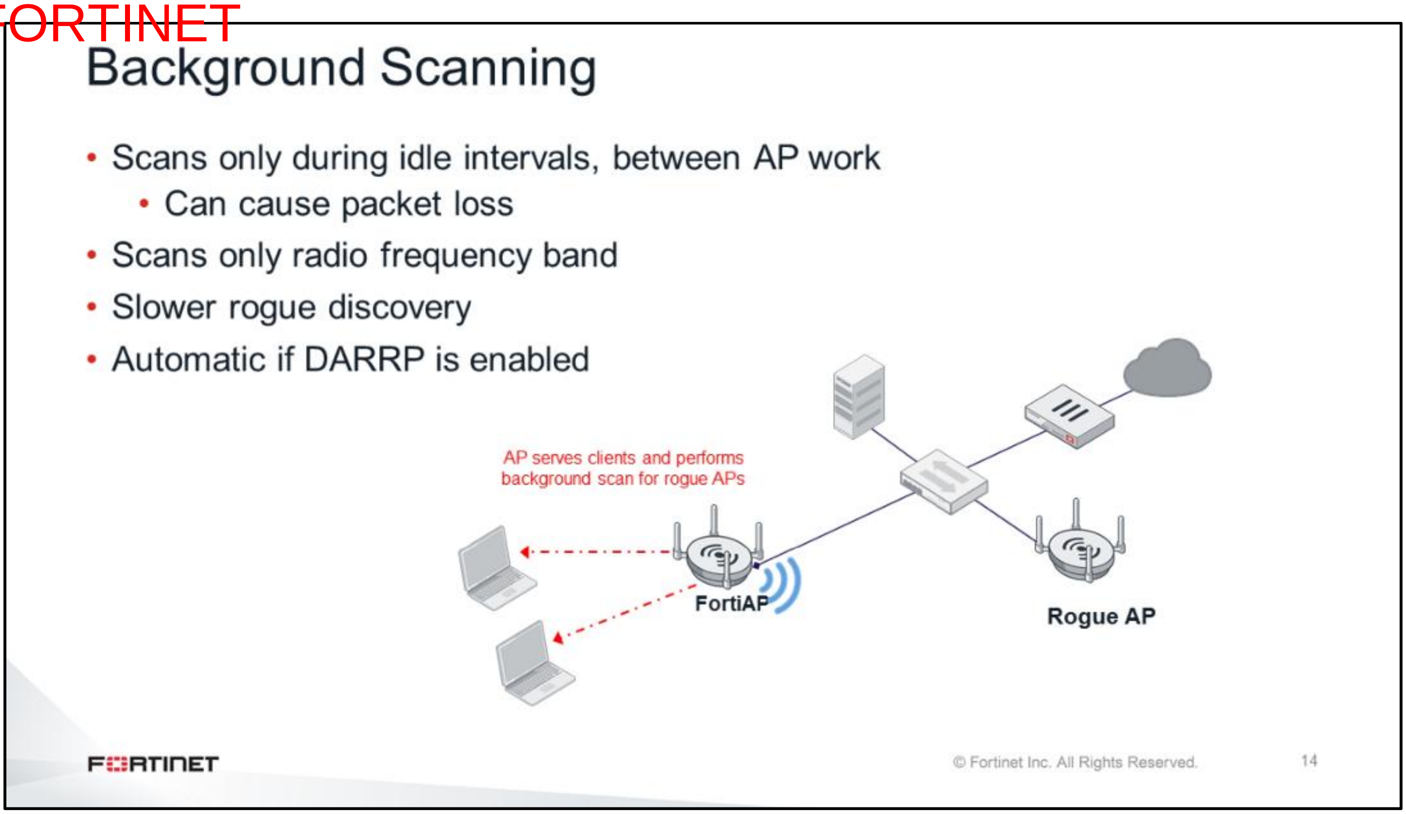
Configuration of rogue detection is covered later in this lesson.



There are two ways to configure 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, but 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 it in the **Rogue AP Monitor**, and you can suppress it to avoid security threats.



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.

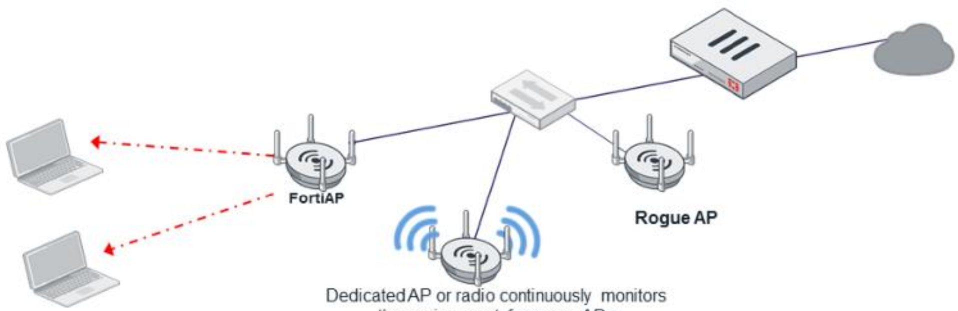
If you do not use a dedicated AP or a radio for scanning, you can configure the AP to run a background scan when a radio is idle or at a defined threshold.

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 when using Distributed Automatic Radio Resource Provisioning (DARRP).

Dedicated Monitor

- Performs continuous foreground scans
- Allows you to suppress rogue APs by sending de-auth frames
- Can't serve clients
- Faster rogue discovery



FORTINET 15

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 only of 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.

On-Wire Rogue AP Detection

- Other APs in your AP coverage area are not always rogues
  - Neighbor interference
- On-Wire detection mechanism constantly compares wireless and wired client traffic to identify if an unknown AP has joined your network
  - Must be at least one Wi-Fi client connected to the suspect AP and continuously sending traffic
  - If FortiGate and FortiAP see the MAC address of the wireless client on the wired network, then the rogue AP that the client is connected to must be on-wire
  - Can block either exact MAC address only, or similar (adjacent)
  - MAC adjacency is configurable
  - MAC address spoofing and NAT on the rogue AP can make on-wire rogue detection more difficult
  - False positives is a possibility in MAC adjacency

FORTINET

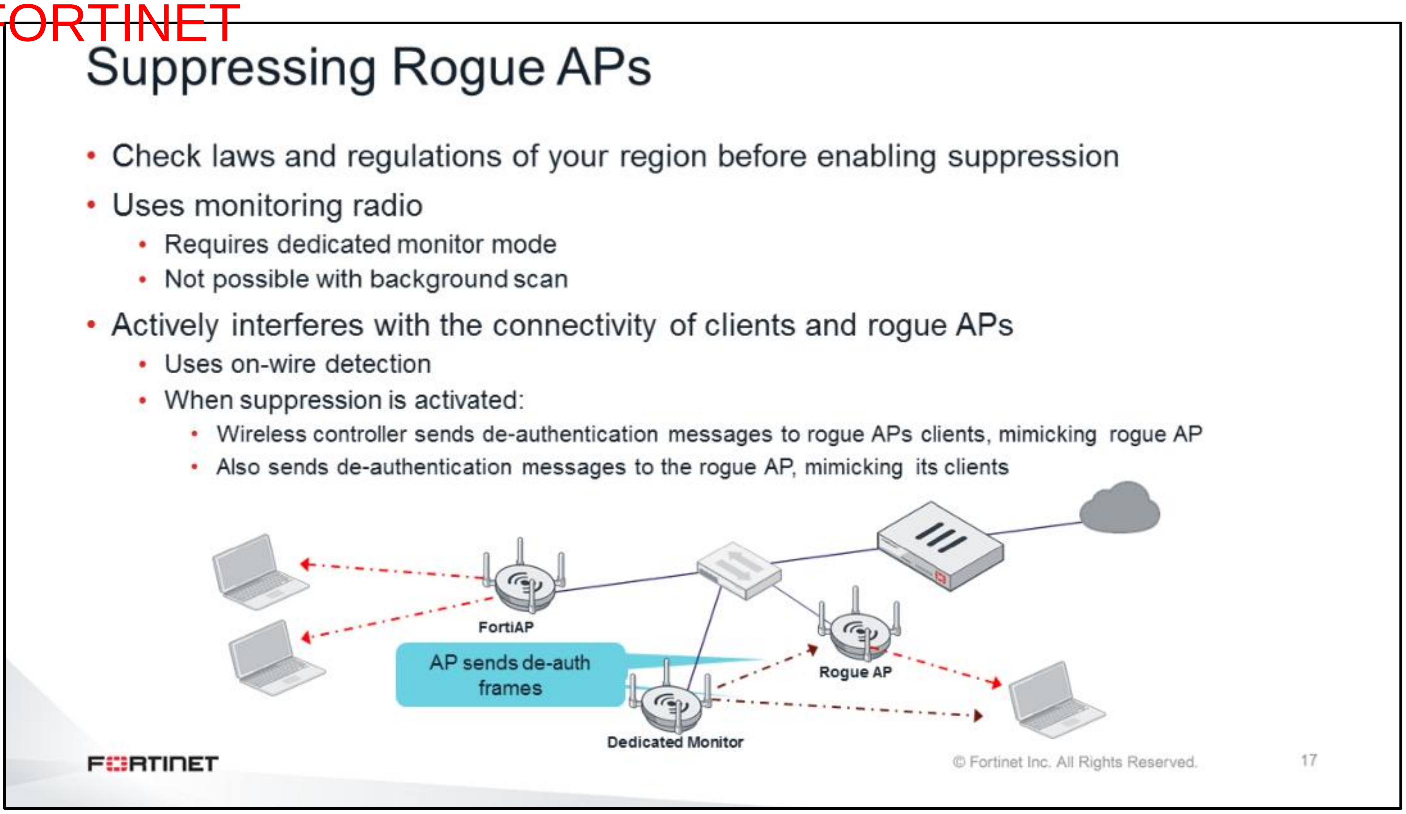
 16

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 either. Usually, however, an AP's Wi-Fi interface MAC address is 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 this setting using the following 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 by on-wire detection, it will appear on the AP monitor, and a green check mark will appear in its **On Wire** column.

Note that because of the nature of the MAC adjacency method, there is a possibility of false positives.



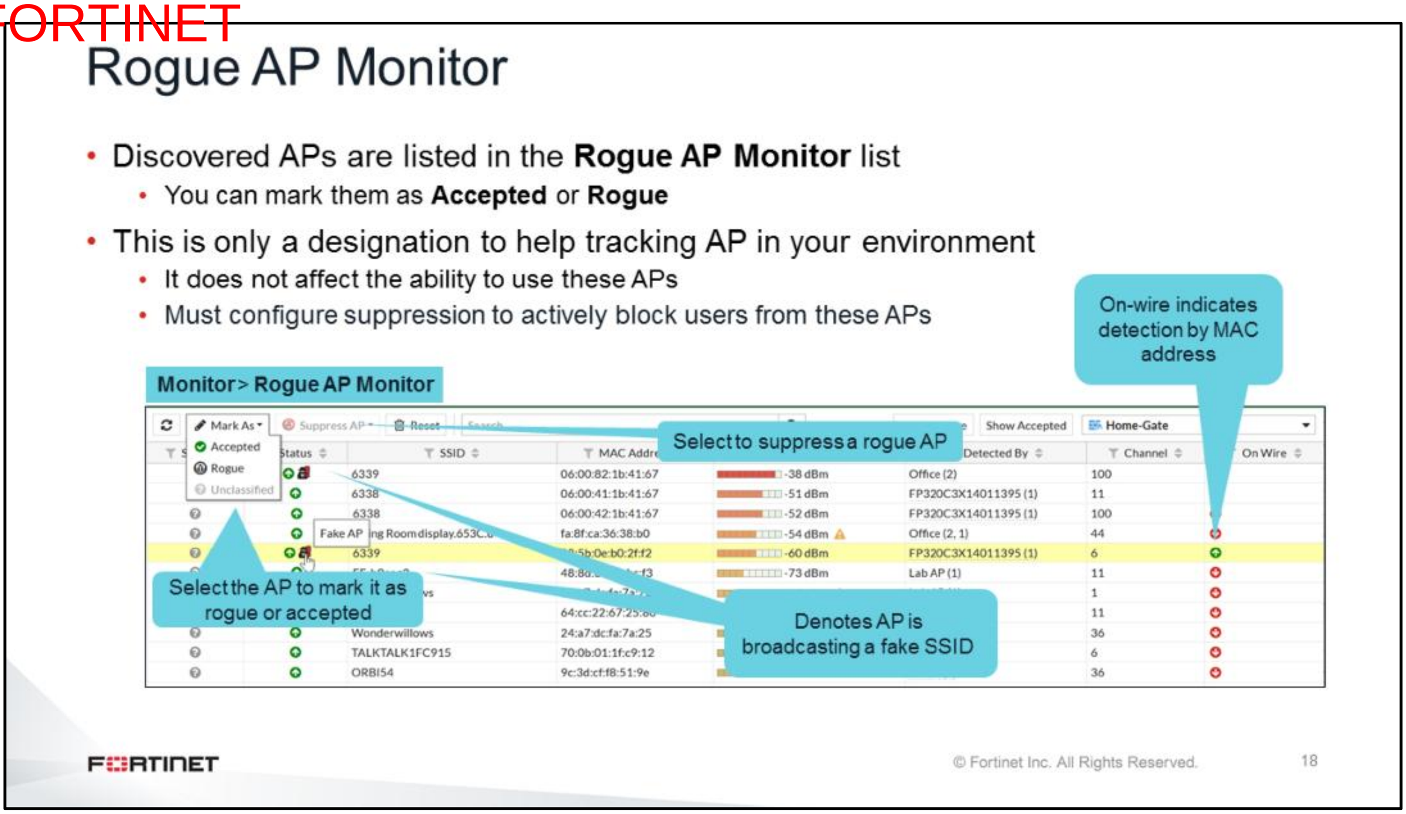
Once you've detected a rogue AP, usually you will want to actively prevent your users from connecting to it. You can use the radios of your FortiAPs to suppress them.

Before enabling this feature, verify that the operation of 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 of the radios of the FortiAP to it. You can't use it 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's clients. This makes it difficult for them to maintain a connection with it. FortiOS also mimics the rogue AP's clients, sending de-authentication messages to the rogue AP.

Note that suppression of rogue APs is becoming increasingly more difficult as 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 will prevent the client from taking notice of the dedicated monitoring AP.



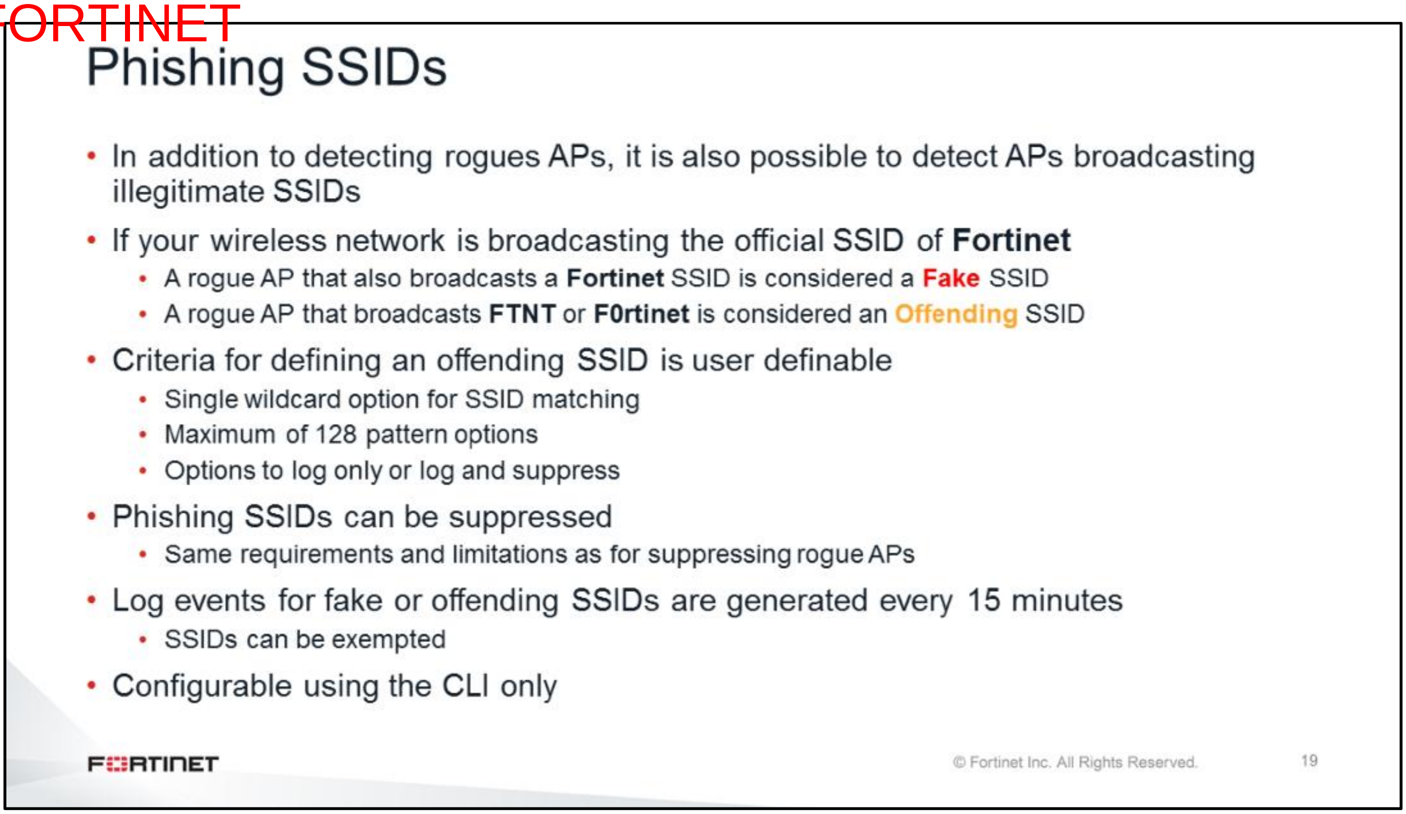
When FortiGate detects a new AP that is not authorized, the AP appears in the **Rogue AP Monitor** list. You can sort and filter this list. Sorting be by **Signal Interference** is especially useful because it sorts the APs with the strongest detected signal to the top of the list.

In the example shown on the slide, not only is the 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**. This helps you to track which APs are authorized by you or not.

By default, marking an AP as rogue does not affect anyone's ability to use these access points. For that, you need to configure suppression.

Marking an AP as **Accepted** removes that AP from the default rogue AP list. This usually indicates that the AP is not a threat in terms of 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.



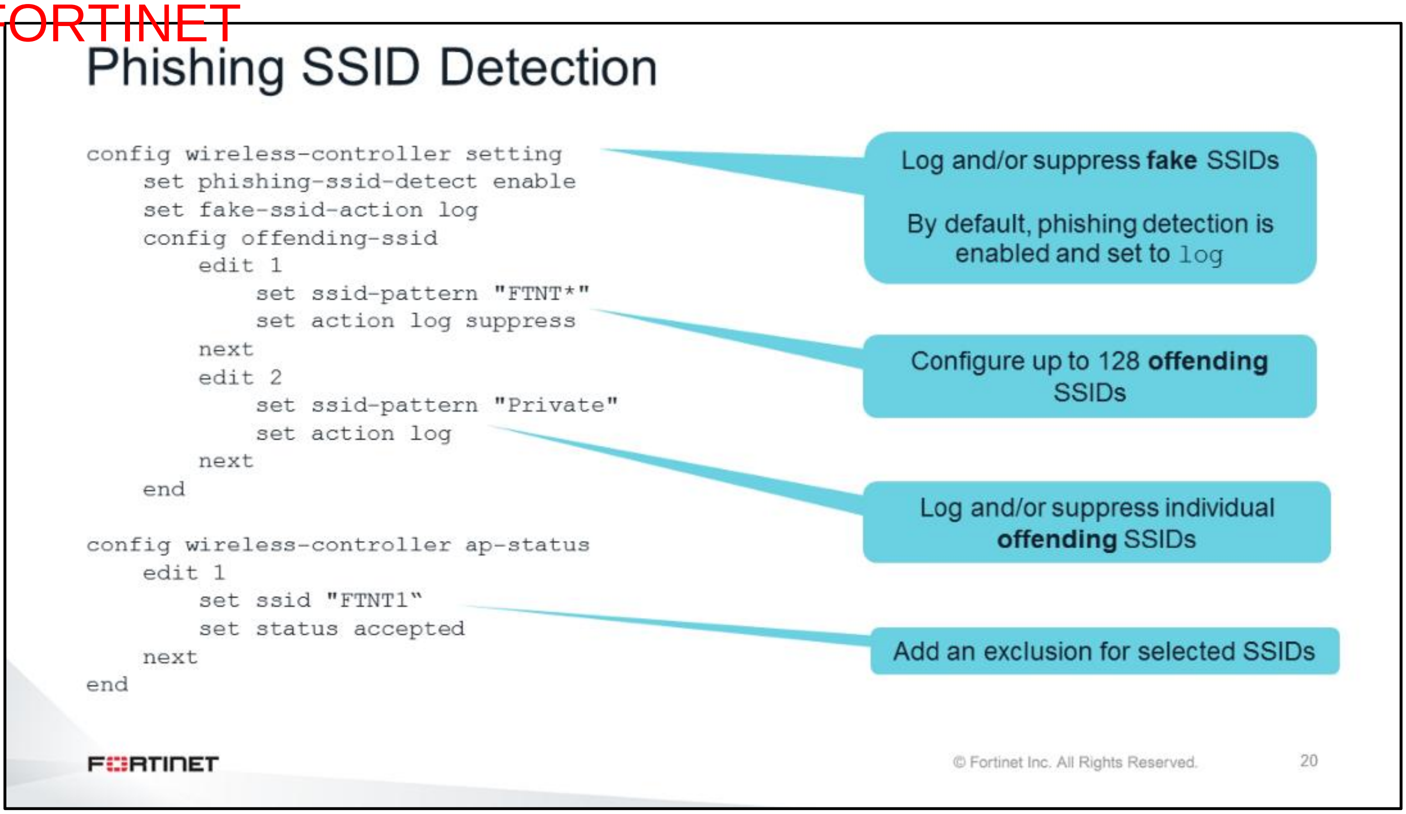
As well as detecting rogue APs, it is also possible to look for networks that might have been set up to perform phishing operations. Often bad actors will attempt to attract connections from legitimate clients, either by broadcasting an SSID that is the same as, or very similar to, the official network 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 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, however the same prerequisites are required.

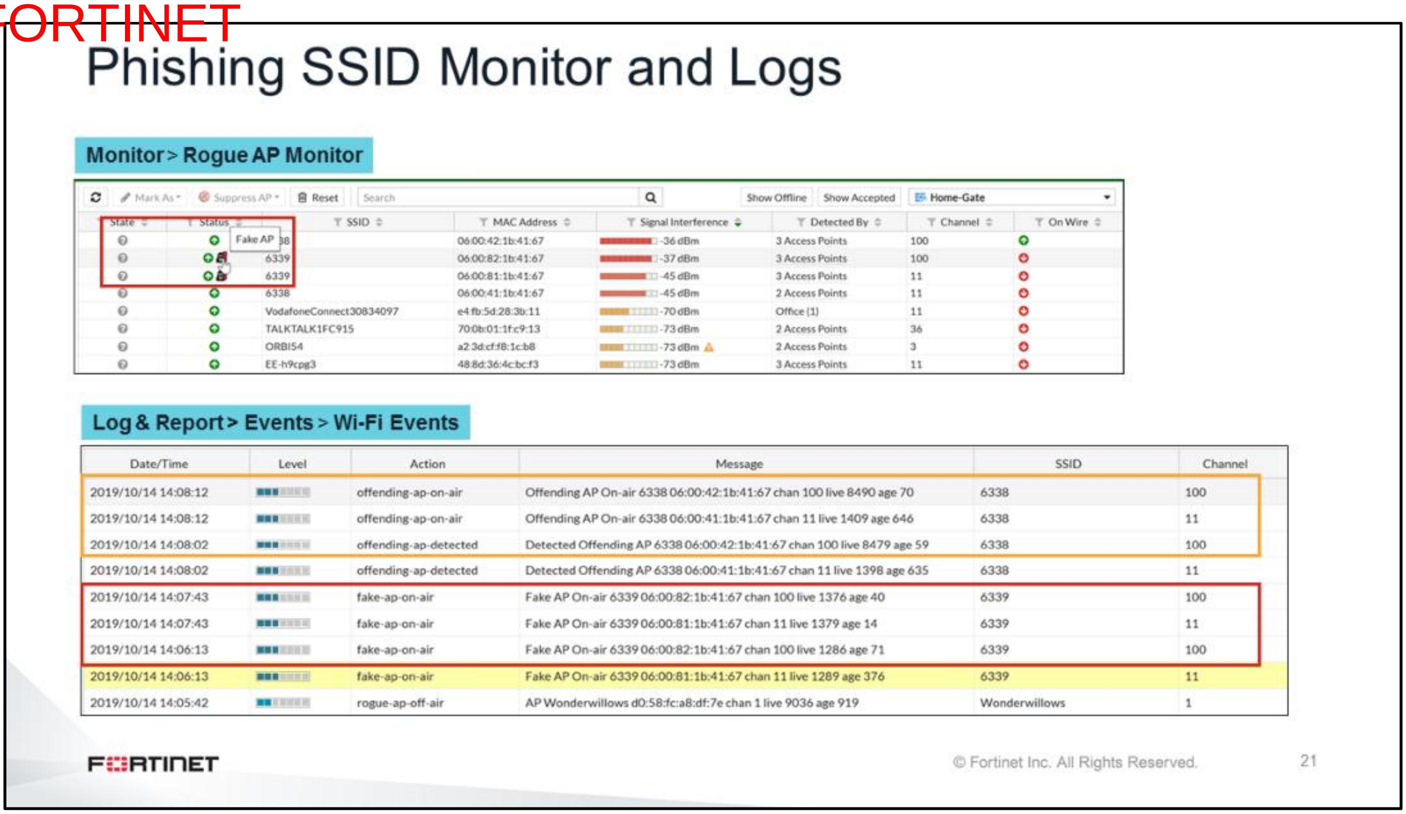
Any fake or offending SSIDs that are detected are logged every 15 minutes until they are classified.



Currently, you can configure phishing SSID detection only using the CLI. By default, fake SSIDs are only detected and logged.

By default, no offending SSIDs are defined. Offending SSIDs are added using the **`config offending-ssid`** command with the option to log, or, to log and suppress.

You can also add an exclusion for selected SSIDs, if required. In the example shown on this slide, a wildcard match for any SSID beginning with FTNT has been configured, however an exclusion for FTNT1 has been explicitly excluded from the offending SSID match.

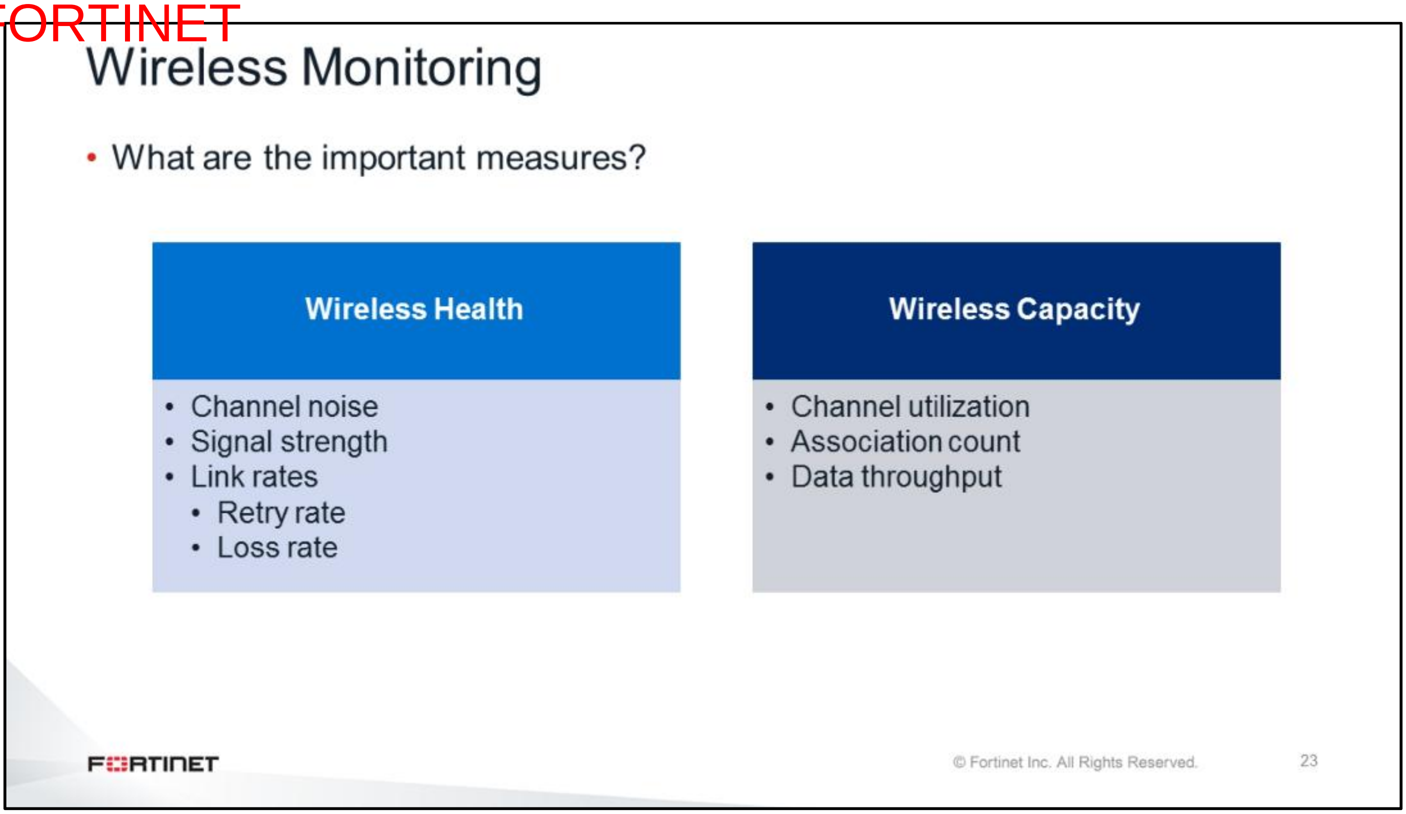


Once you enable phishing detection, it is possible to log entries in both the **Rogue AP Monitor** and the **Wi-Fi Events** log.

On the Rogue AP monitor, you can classify SSIDs in the same way as rogues, and optionally suppress them.

Monitoring the Wireless Network

In this section, you will learn how to monitor the FortiGate managed wireless network.



A large proportion of wireless troubleshooting revolves around ensuring that a number of wirelesses metrics are within acceptable ranges.

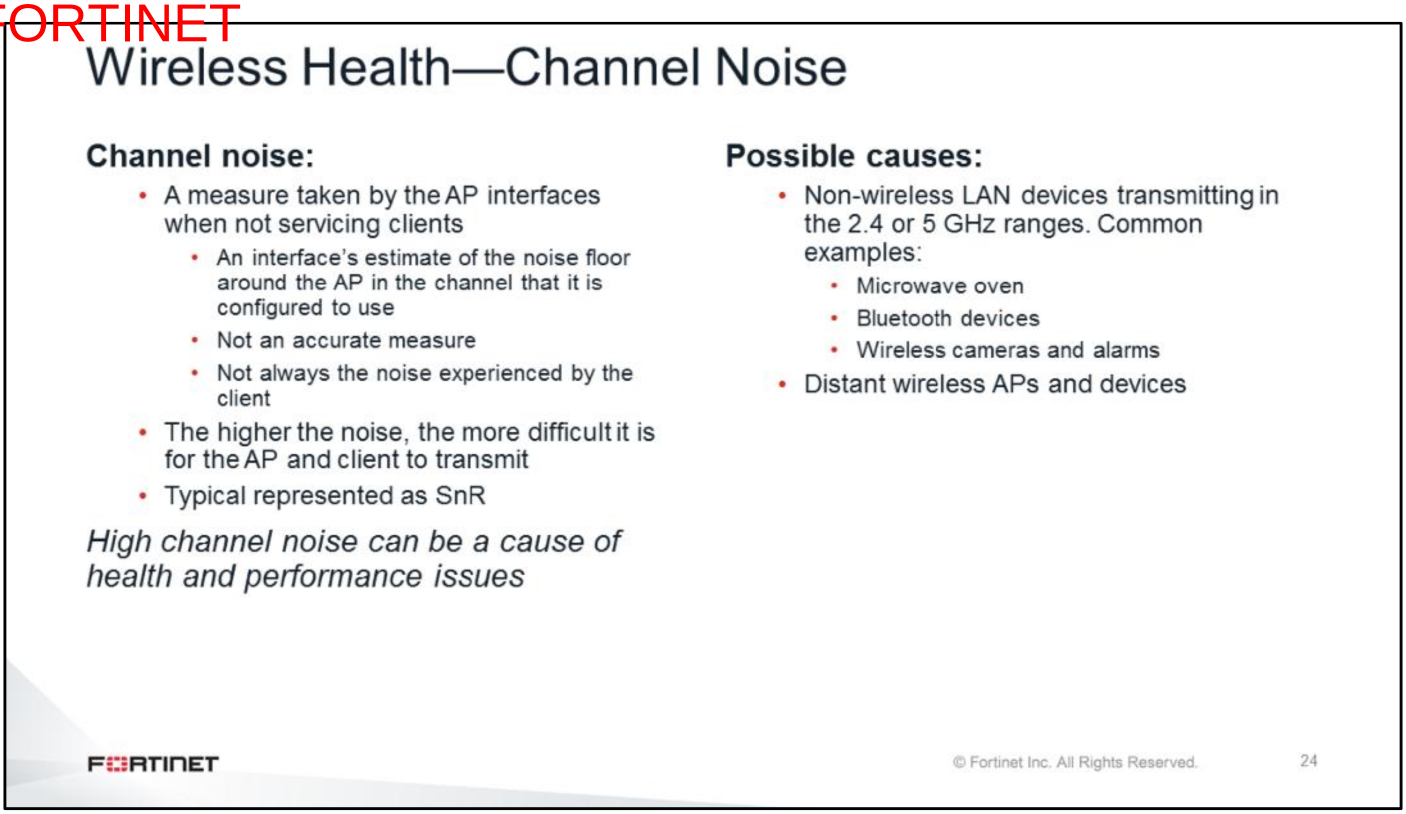
The important measures belong to two broad categories—wireless health, and wireless capacity.

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, again, a capacity measure.

A number of metrics are relevant to both categories, however, some are more important than others.

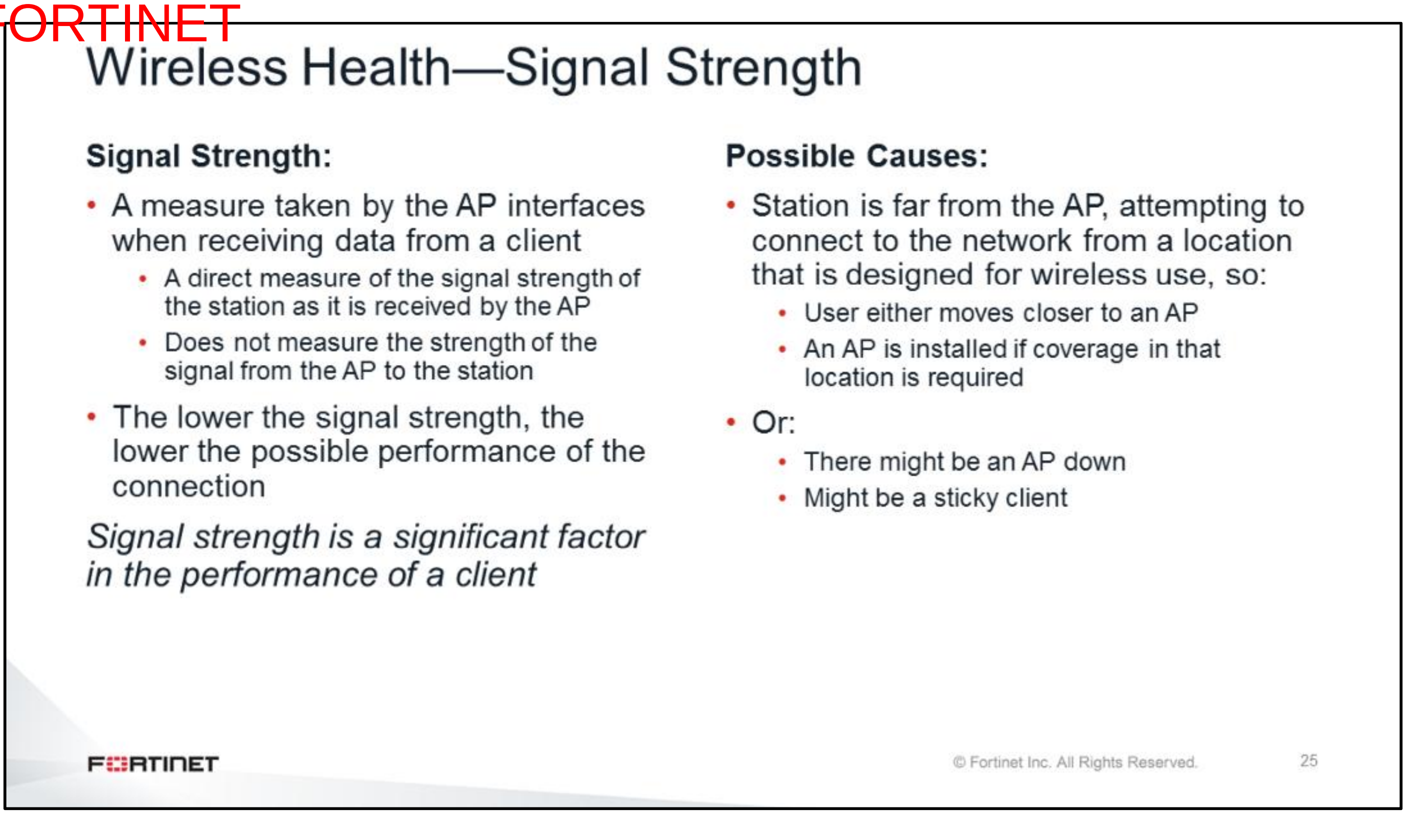
Some of these measures, such as retry and loss rates, are not easily measurable in a FortiWi-Fi system, however, because these measures are important in the AP and client calculation of link rates, the link rate can be used as a prime indicator of connection quality.



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 AP's and client's 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 interference would cause significant issues with the network if it was both powerful and frequent.



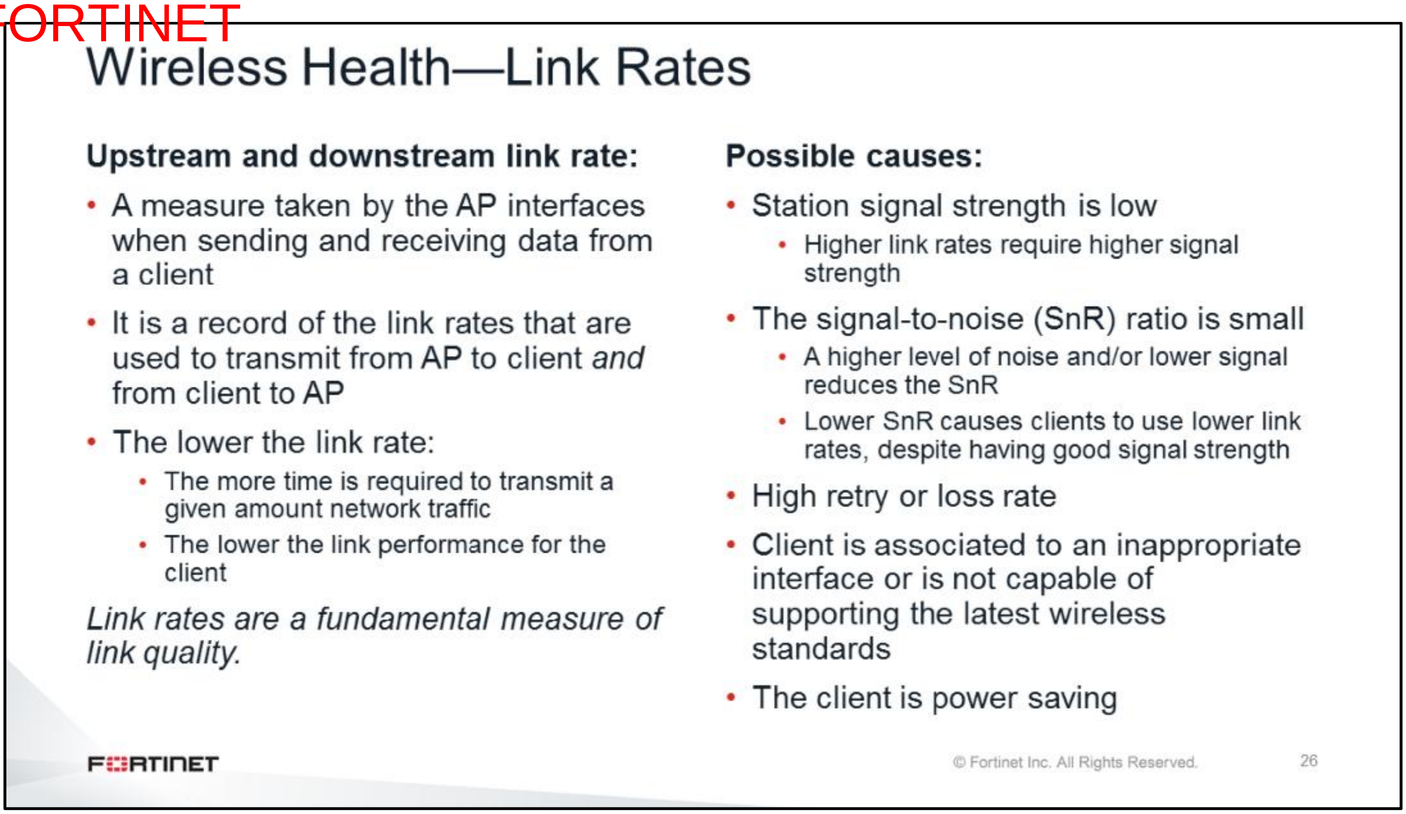
The controller maintains a list of the receive signal strength (RSSI), for all clients. RSSI is measured by the AP of each client as transmissions occur. It is *not* a measure taken by the *client* of the AP signal strength, which arguably is more important because the majority of data is downstream.

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 client's signal strength is somewhat less than the signal 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 environments, 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.



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, 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.

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

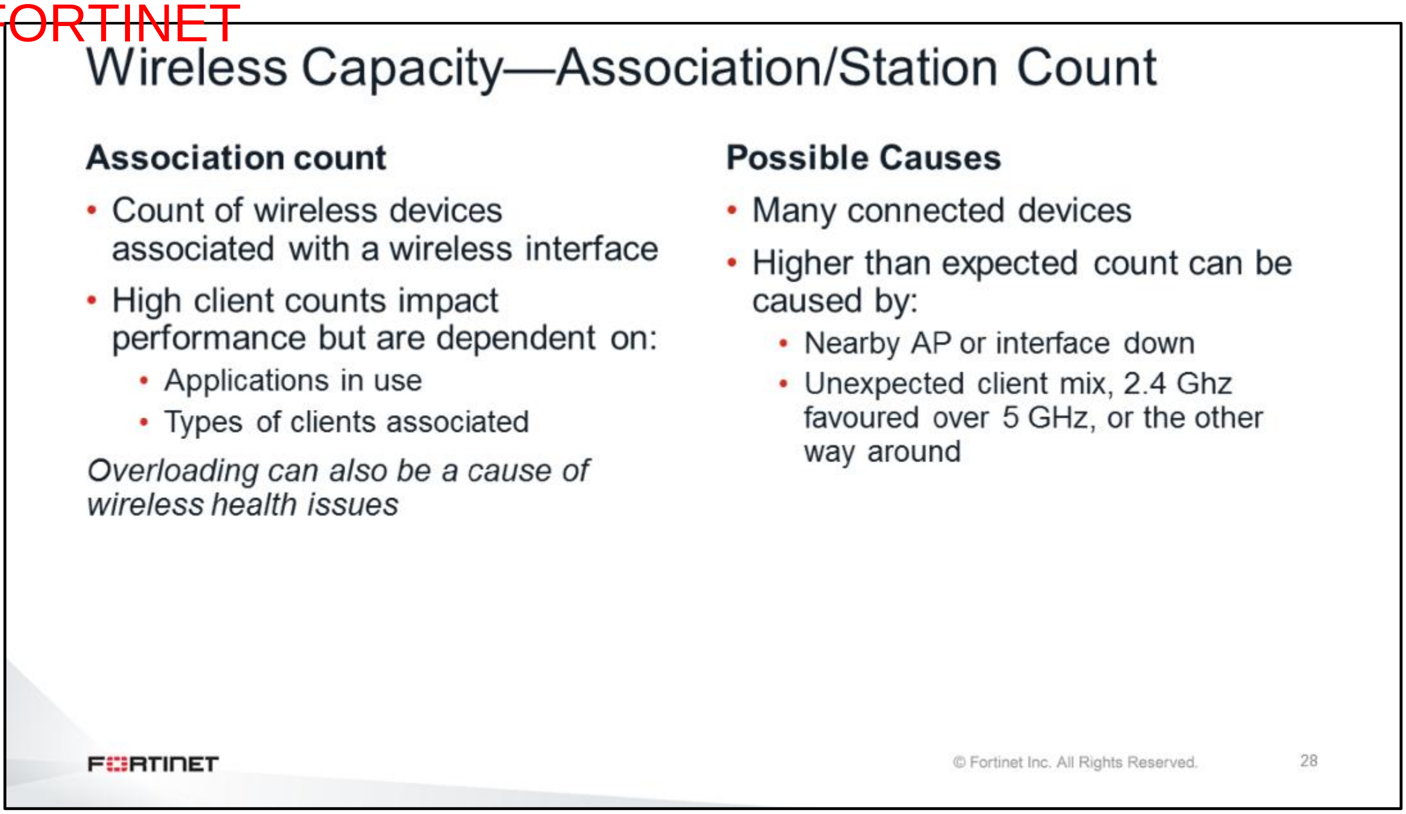
FORTINET

 27

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, but 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.

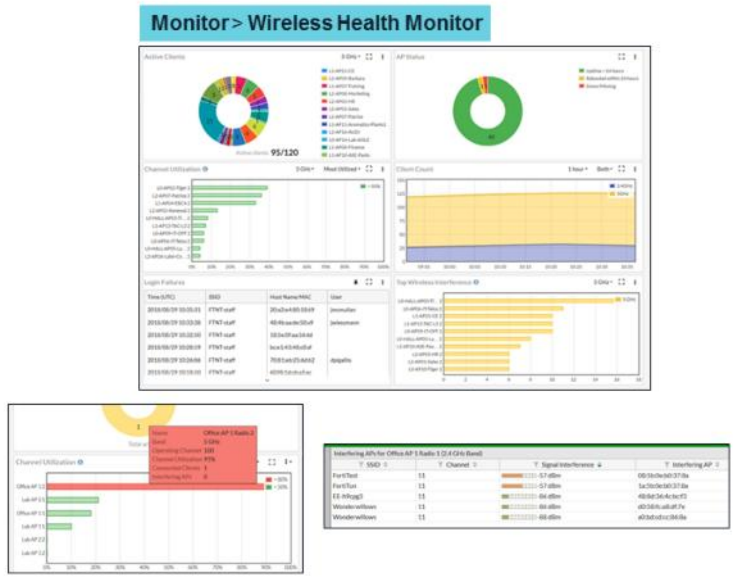


Another critical metric for your wireless interface is the associated client count. Association count is a measure of the number of clients associated with each interface. A high client count will always affect performance, but the applications in use and the types of clients also a matter.

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.

Sources of Information—Wi-Fi Health Monitor

- Located under **Monitor**
- AP status and client counts
- **Channel Utilization**
  - See the most utilised wireless interfaces
  - Interfaces must be enabled to monitor channel utilization in the AP
  - Hover over for more detail
- **Top Wireless Interference**
  - See the interfaces with the most RF issues
  - APs must be have WIDS profile or Radio Resource Provision enabled
  - Click through to see more information



FORTINET

 29

So where do you find information about these metrics?

There are multiple sources of information, both on the GUI and the CLI. Often, it is an exercise to collate all the relevant information to form a picture of the wireless environment.

The **Wireless Health Monitor** is a great place to start. Located under **Monitor**, it gives a dashboard view of the status of the network. A series of widgets provide an overview of the AP status and client counts across the entire controller.

Of particular interest will be the **Channel Utilization** and **Top Wireless Interference** widgets. These widgets highlight the radio interfaces that are potentially suffering issues from high channel utilization or excessive interference.

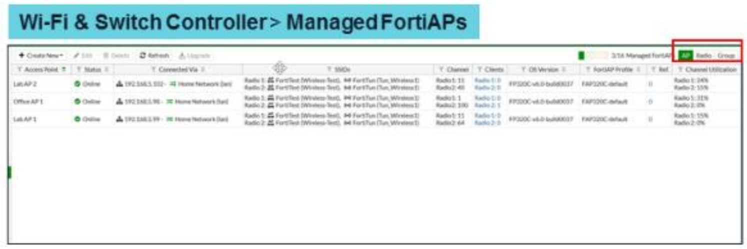
You can hover the cursor over the widget elements, which often reveals more information about a specific event. You can click many elements to reveal further information.

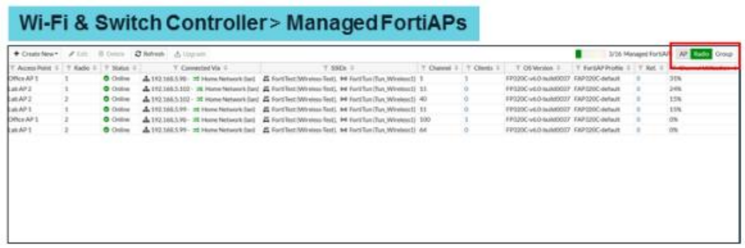
In the **Top Wireless Interference** widget, you can click a radio to reveal a table of the neighboring access point that the radio can detect, and its received signal strength. You can sort these tables to highlight radios that are interfering the most.

This is key information that you can use to diagnose potential causes of poor performance and connection reliability.

Sources of Information—Managed FortiAPs

- Located under **Wi-Fi & Switch Controller**
- Displays detailed information about the installed APs
- **View by AP**
  - Right-click on column headers and add **Channel Utilization**
- **View by Radio**
  - Sort all radios by utilization and station load
- Both views allow the view of:
  - Radio utilization
  - Client count





FORTINET

 30

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.

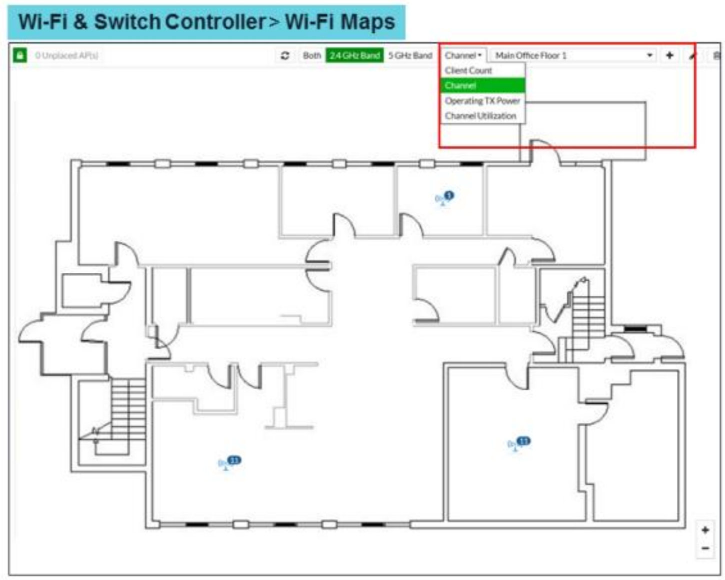
AP View is the default view and groups radio interfaces together under an AP.

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 **Utilization,** to a view.

Sources of Information—Wi-Fi Maps

- Provides graphical representation of the location of APs
- Useful for visualizing the state of the wireless network
  - Channel configuration
  - Channel utilization
  - Station load
- Allows easy identification of APs that might have inappropriate channel settings or are overloaded
- Requires setup
  - Floorplan import
  - AP placement



 31

It is often difficult to work out from a static table how an AP location will relate to another. The location of an AP is particularly important when assessing the channel setting, and using the Wi-Fi map will allow you to identify adjacent APs that might, for instance, have the same channel number, potentially causing an issue.

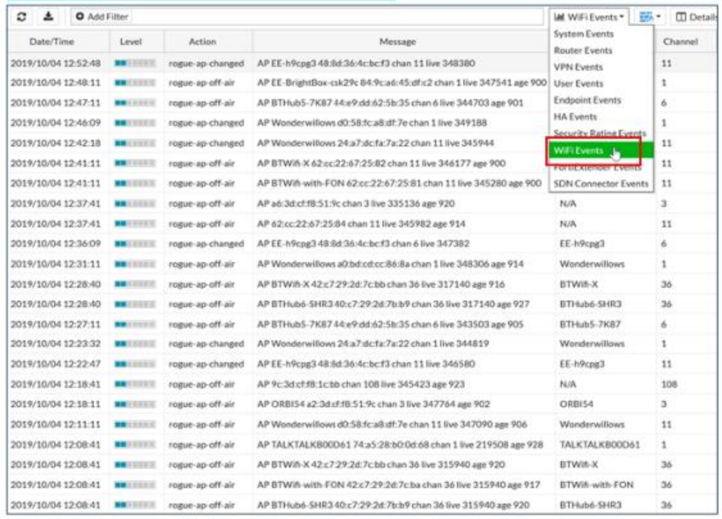
You can also change the view to identify APs that are overloaded, or are reporting high channel utilization.

You must import the maps, and place the APs on them. Also remember that buildings tend to have multiple floors, so when assessing APs, bear in mind that there may also be APs on floors above and below, so you would need to consider multiple floor maps.

Sources of Information—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**

Log & Report > Events > Wi-Fi Events



FORTINET

 32

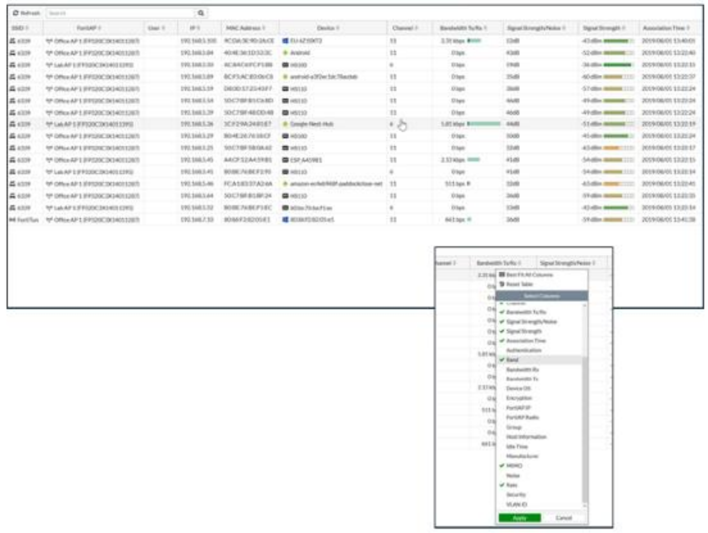
The events table provides a historical view of the wireless network. You can use this to identify events that affect both clients and APs over time.

Adding additional columns and filtering allows you to focus in on wireless clients or APs that are misbehaving.

Sources of Information—Wi-Fi Client Monitor

- Detailed client information for all clients currently connected
- Use to assess the client health from the APs point of view
  - The signal strength here is measured by the AP
  - It does not show the signal strength of the AP at the client
- For more useful information, add additional columns:
  - **Rate**—link quality indicator
  - **MIMO**—client capability indicator
  - **Band**—client capability indicator
- Columns sortable and filterable to isolate clients that are in difficulty

Monitor > Wi-Fi Client Monitor > Wi-Fi Events



 33

The **Wi-Fi Client Monitor** 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.

Sources of Information—Controller CLI

- List all stations connected to the APs

```
diag wireless-controller wlac -d sta | grep -v 0.0.0.0
```

```
vf=0 wtp=2 rId=1 wlan=Main-Wi-fi vlan_id=0 ip=192.168.5.50 mac=ac:84:c6:fc:f1:b8 vci= host=
user= group= signal=-37 noise=-95 idle=12 bw=0 use=5 chan=1 radio_type=11N
security=wpa2_only_personal mpsk=default encrypt=aes cp_authed=no online=yes mimo=1
```

- List all discovered neighboring APs

```
get wireless-controller scan
```

```
CMWF VF  SSID              BSSID              CHAN RATE SIGNAL NOISE  INT CAPS ACT LIVE   AGE WIRED
                                                        (dBm)  (dBm)
UNNN 0   BTHomeHub2-...    00:26:44:18:34:4f   1  130M  -88    -95    100 EPs  N  50435 50435   ?    RSN CCMP TKIP VEN WPA WME
UNNN 0   BTOpenzone-H      02:26:44:18:34:50   1  130M  -92    -95    100 Es   Y  103115  515   ?    VEN WME
UNNN 0   BTFON             02:26:44:18:34:51   1  130M  -90    -95    100 Es   N  104075 103003  ?    VEN WME
UNNN 0   EXT2-BTHub6...    1c:a5:32:f1:3b:eb  11  144M  -76    -95    100 EPs  Y  156386   22   ?    RSN CCMP WME VEN VEN VEN
```

- Show RF conditions around all AP radios

```
get wireless-controller rf-analysis
```

  - Shows a list of neighboring APs together with their signal strength, channel and RF score

- Show client load over time

```
get wireless-controller status
```

  - Shows a breakdown of total client load over multiple hours and days

FURTINET 34

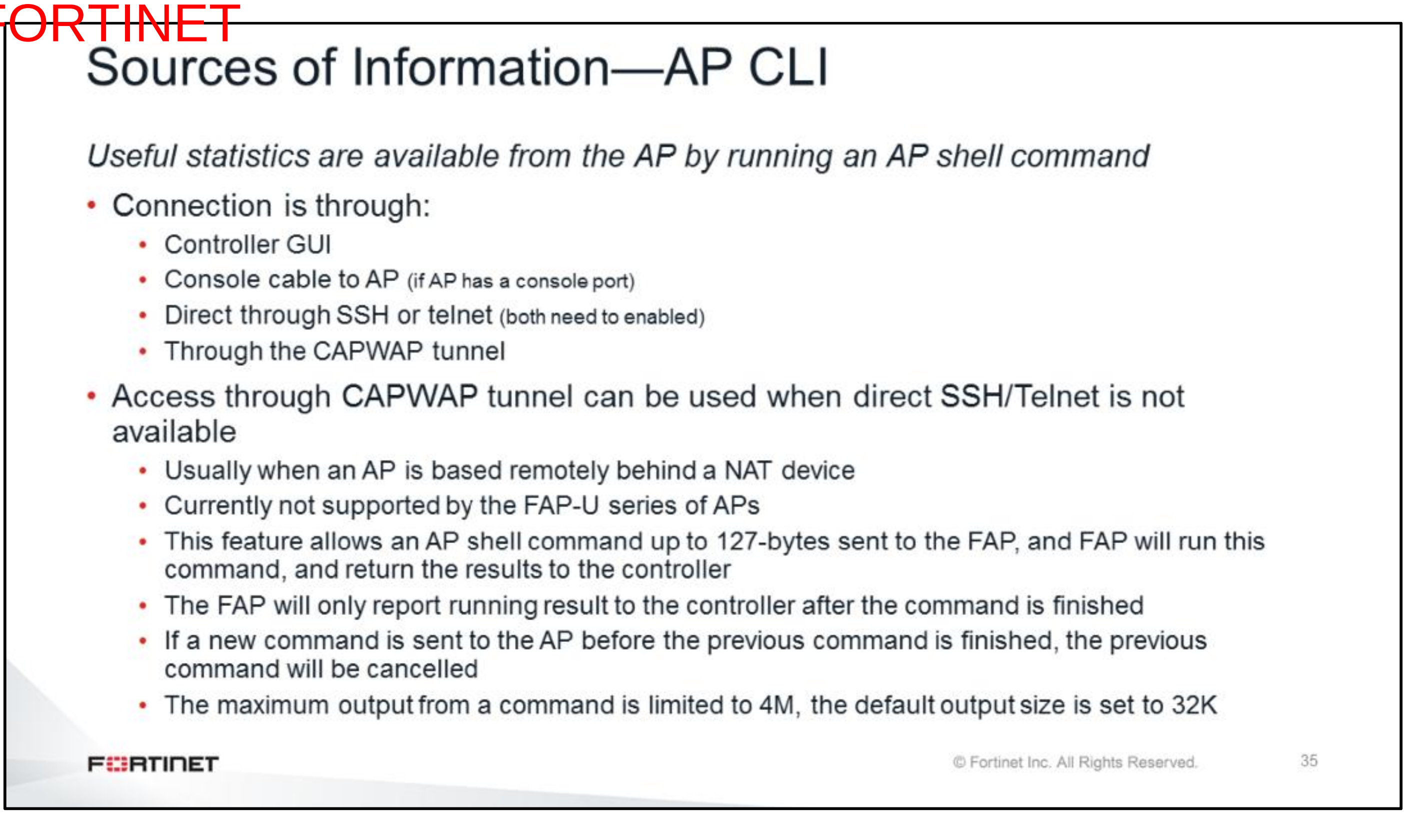
As well as the GUI on the controller, you can also gather information from the controller CLI.

You can list connected stations and APs as you would see them on the GUI.

It is also possible to get a better view of the RF status of all the radios by using the `get wireless-controller rf-analysis` command. Unlike the GUI, which only lists the top-most interfered with, you can list all of the interfaces.

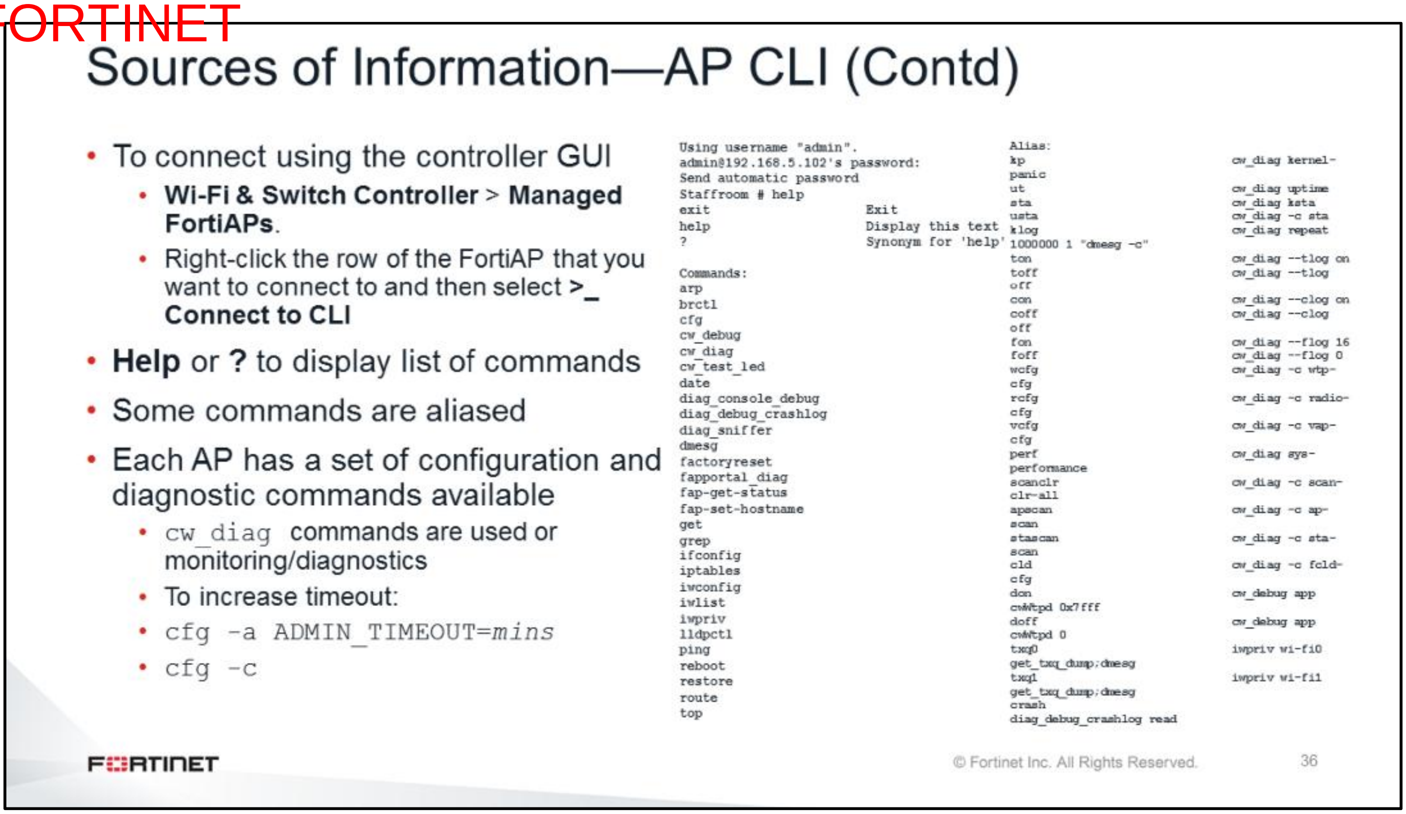
Or, you can focus on one AP by specifying the WTP ID, also known as the AP serial number.

There is little historical information available on the GUI, so `get wireless-controller status` is a useful command for monitoring client load over time.



The AP CLI can provide specific information about AP and client connectivity. Access to the AP can be achieved in multiple ways. Connections can be direct to the AP over a console cable, or over the network if the appropriate protocols are enabled on the AP.

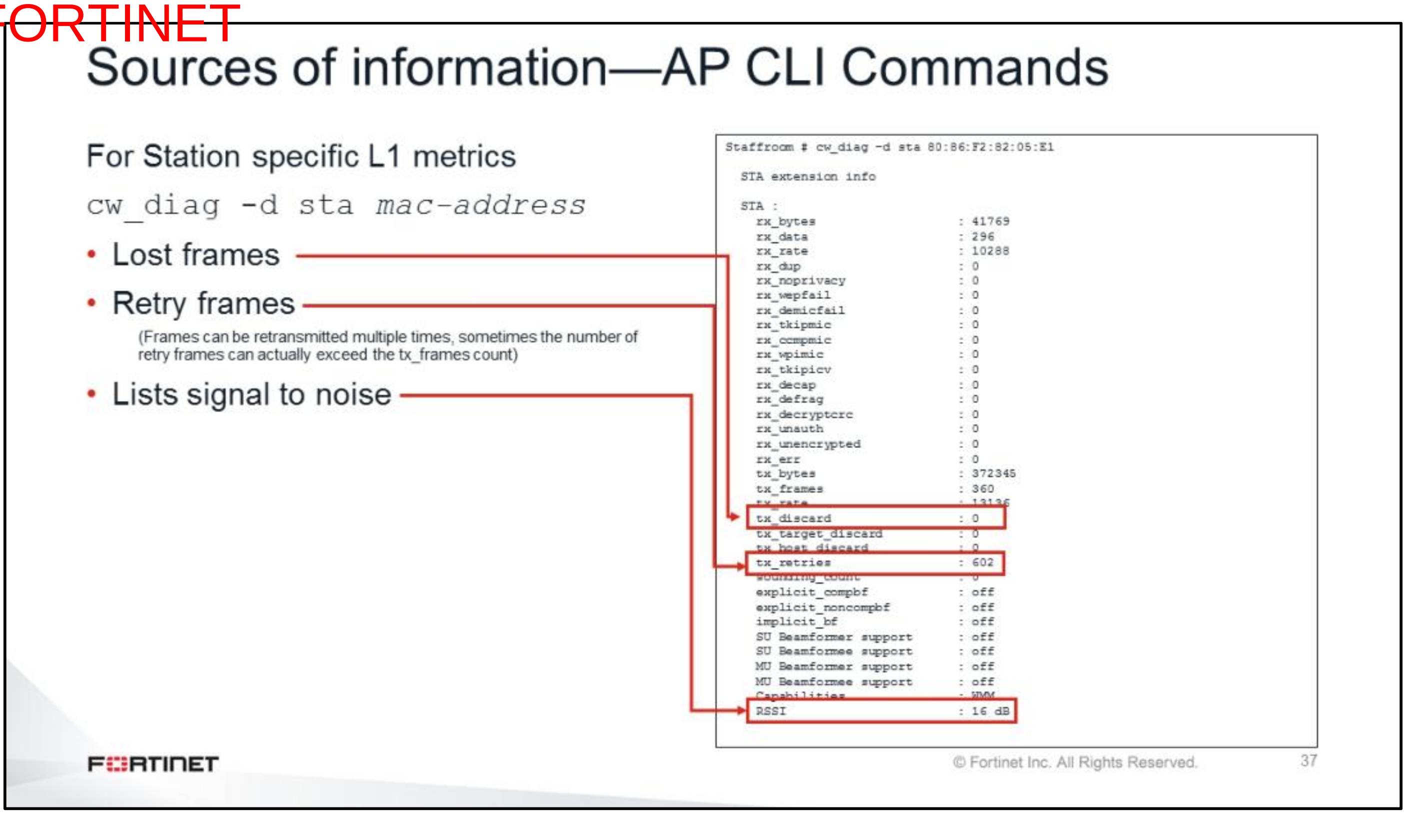
One new way of connecting is through the CAPWAP tunnel. This is useful when an AP is remotely based and cannot be reached by any other method. It bypasses the need to open ports because it allows commands through the CAPWAP tunnel. Commands are sent as a package, the AP executes the command, and then returns the result. If you send another command *before* the previous is completed, the first command is cancelled.



The easiest way to connect to a FortiAP using the controller GUI is to highlight an AP on the **Managed FortiAPs** table, and then click **Connect to CLI**. However, it is possible to connect directly to the AP if it has a console port, or by using one of the other listed methods.

As with other Fortigate CLI commands, you can use context-sensitive help.

By default, the CLI will timeout after approximately 5 minutes, which can be an issue if you are trying to troubleshoot. You can extend the timeout period by using the `cfg` command.

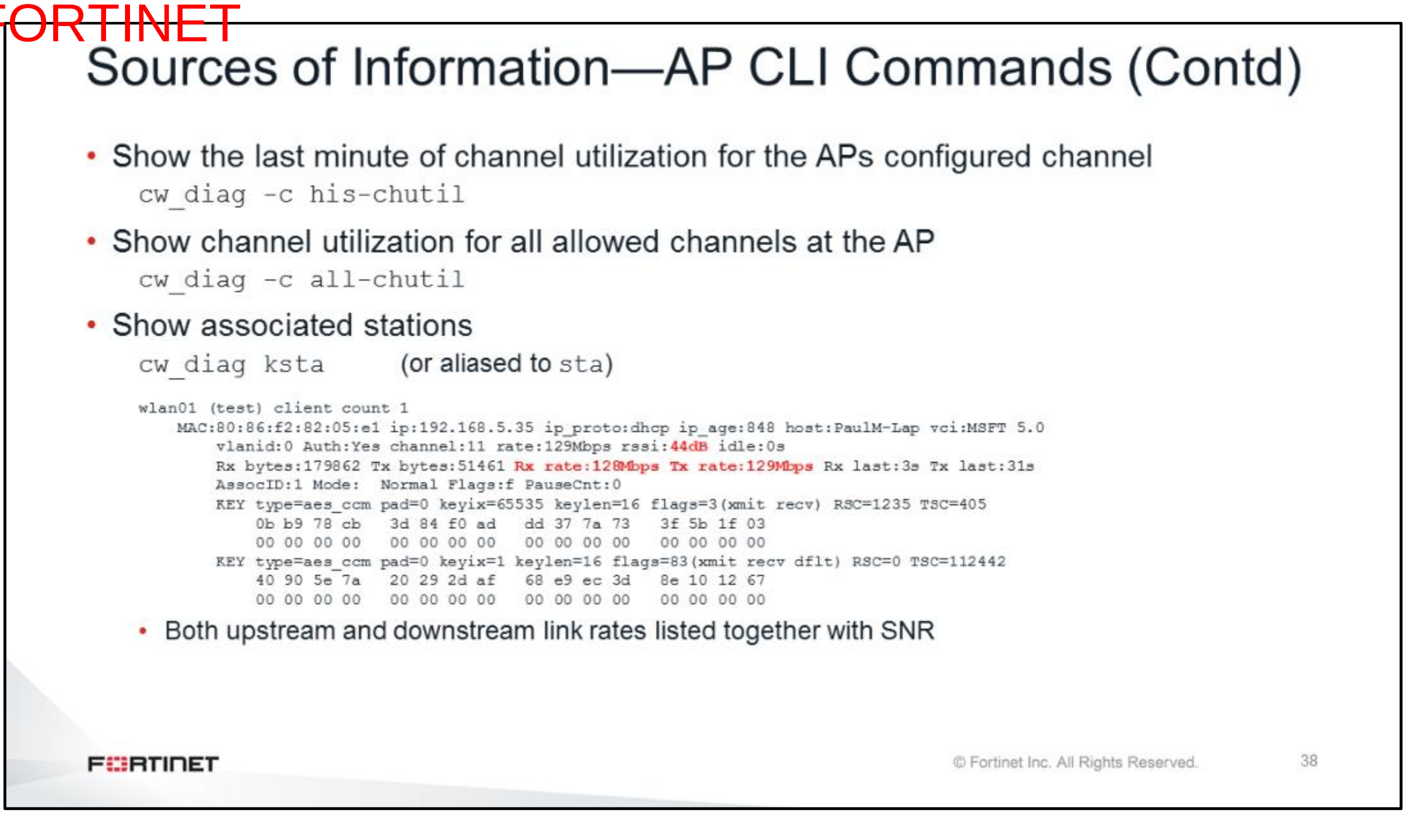


For stations, you can list more detailed RF information by using the `cw_diag -d sta` command for a specific station MAC address.

This command can reveal the frames that that were lost when the AP failed to send them to a client, together with frames that have been retried.

It is not unusual to see very low number of loss frames (in relation to the TX frame count), but an increasingly large number show that the AP has been unable to successfully send a data frame after numerous retries. This can indicate that the station is unable to clearly receive or decode frames from the AP, with the result that it is not sending an acknowledgement frame. This can indicate poor signal strength at the client, or a high noise floor

Retry frames are not unusual. Retries are part of normal wireless LAN network operation, but high numbers indicate an issue.

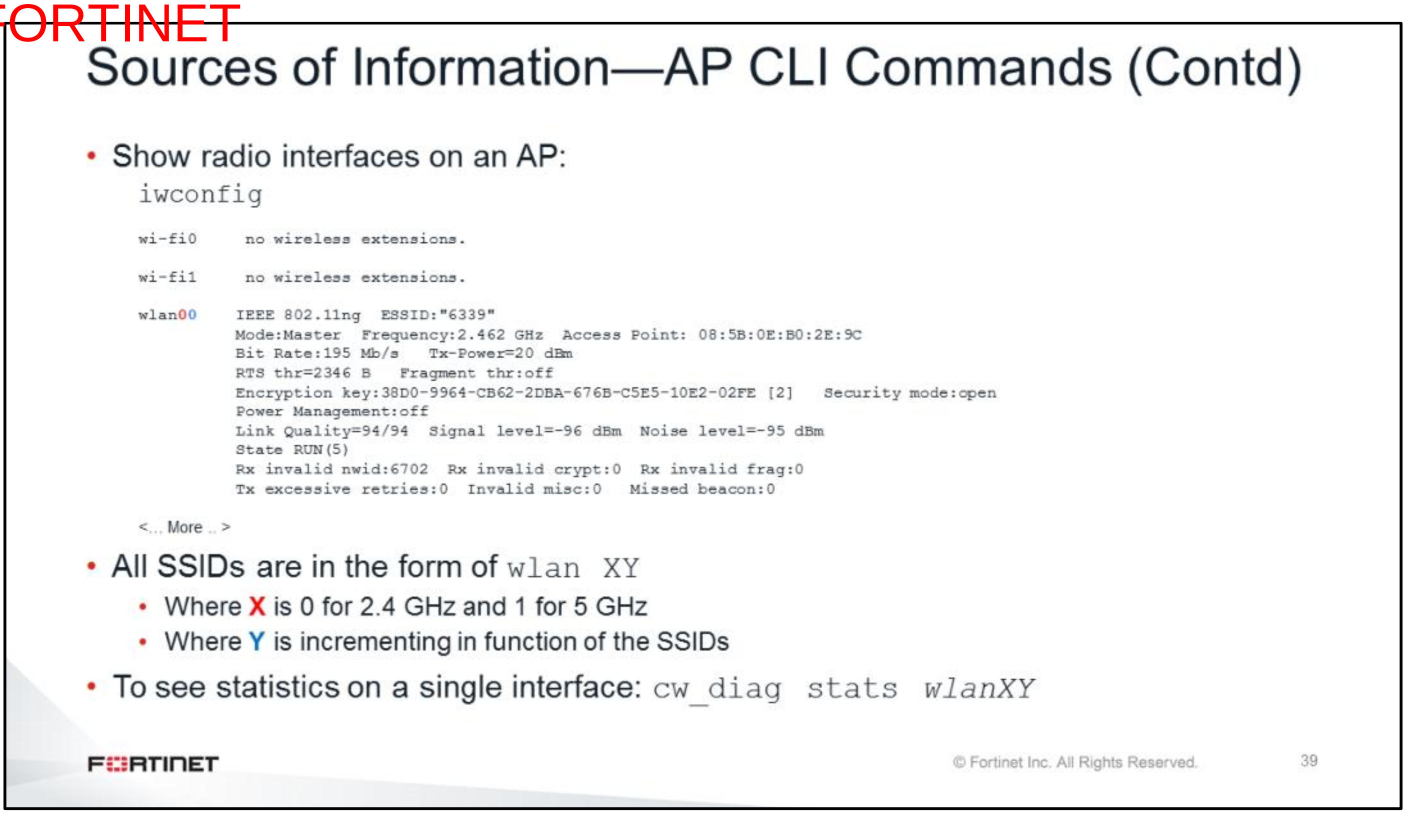


The `cw_diag -c his-chutel` command provide a short history of an AP's channel utilization for the AP's radios. So, rather than taking a one-time measure, which could be a peak, you can see over the span of one minute, a plot of the channel utilization.

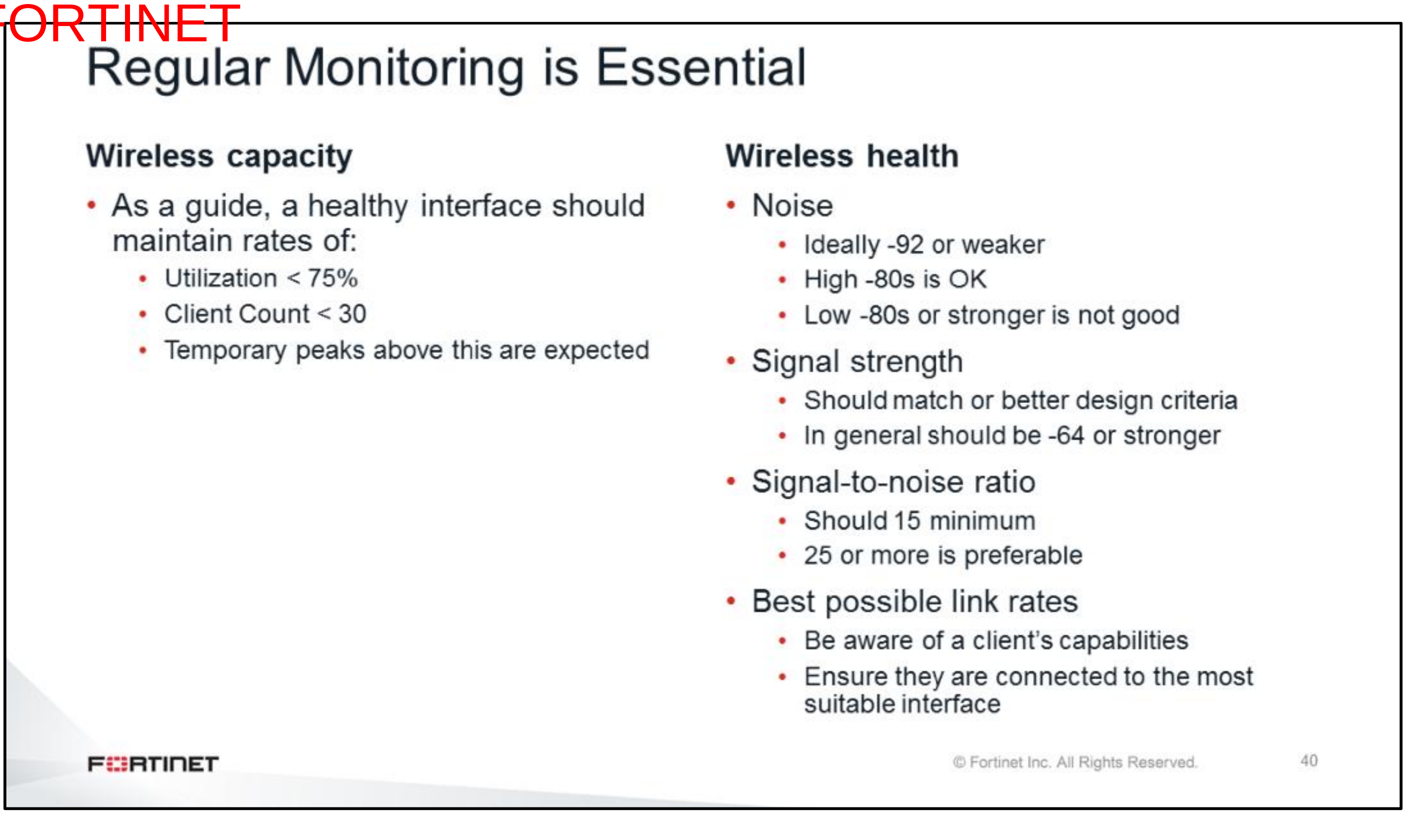
`cw_diag ksta` is an aliased command. The key information that is not available anywhere else is the downstream (AP to client) *and* upstream link rate. Both are great measures of connection quality, but assumes that you understand the range of connection rates the AP and clients are capable of.

For instance, handheld clients will likely have only a single or dual-stream radio and, as such, would never achieve the same link rates as an Apple MacBook Pro for example. Reviewing the specifications of the client will indicate the maximum rate it is capable of. Reviewing its connection using the `cw_diag ksta` command, will show how close it is to the maximum connection speed and, as a result, how healthy the connection is.

Note that many devices save battery power by reducing link rate when the connection is idle. Often, to get a good representation of the link rates, some data needs to be transmitted and received.



You can view more detailed interface information by using the `iwconfig` command.



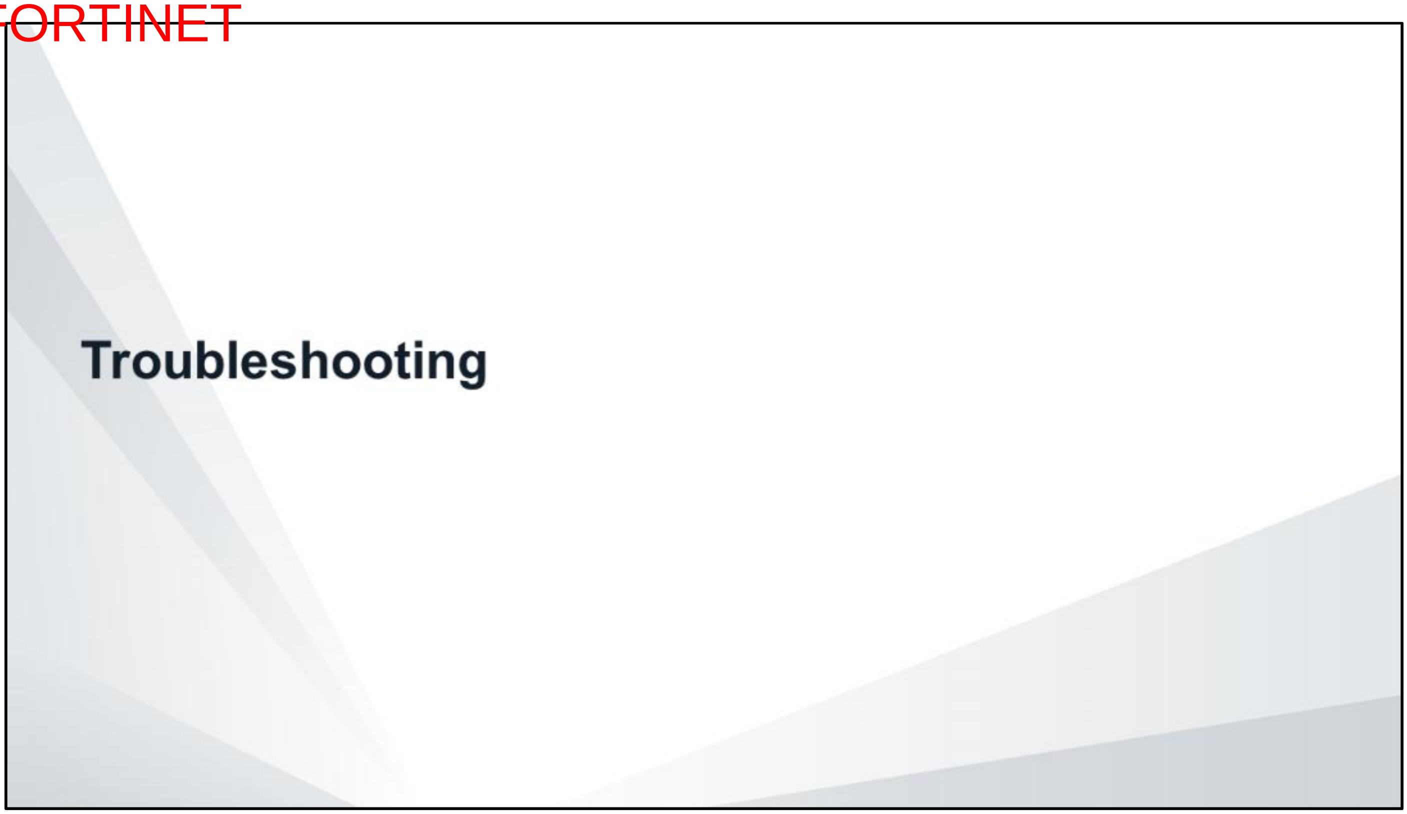
The lower the channel noise, the better. Signal strength is measured in negative decibels—the greater the negative number the weaker the signal.

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.

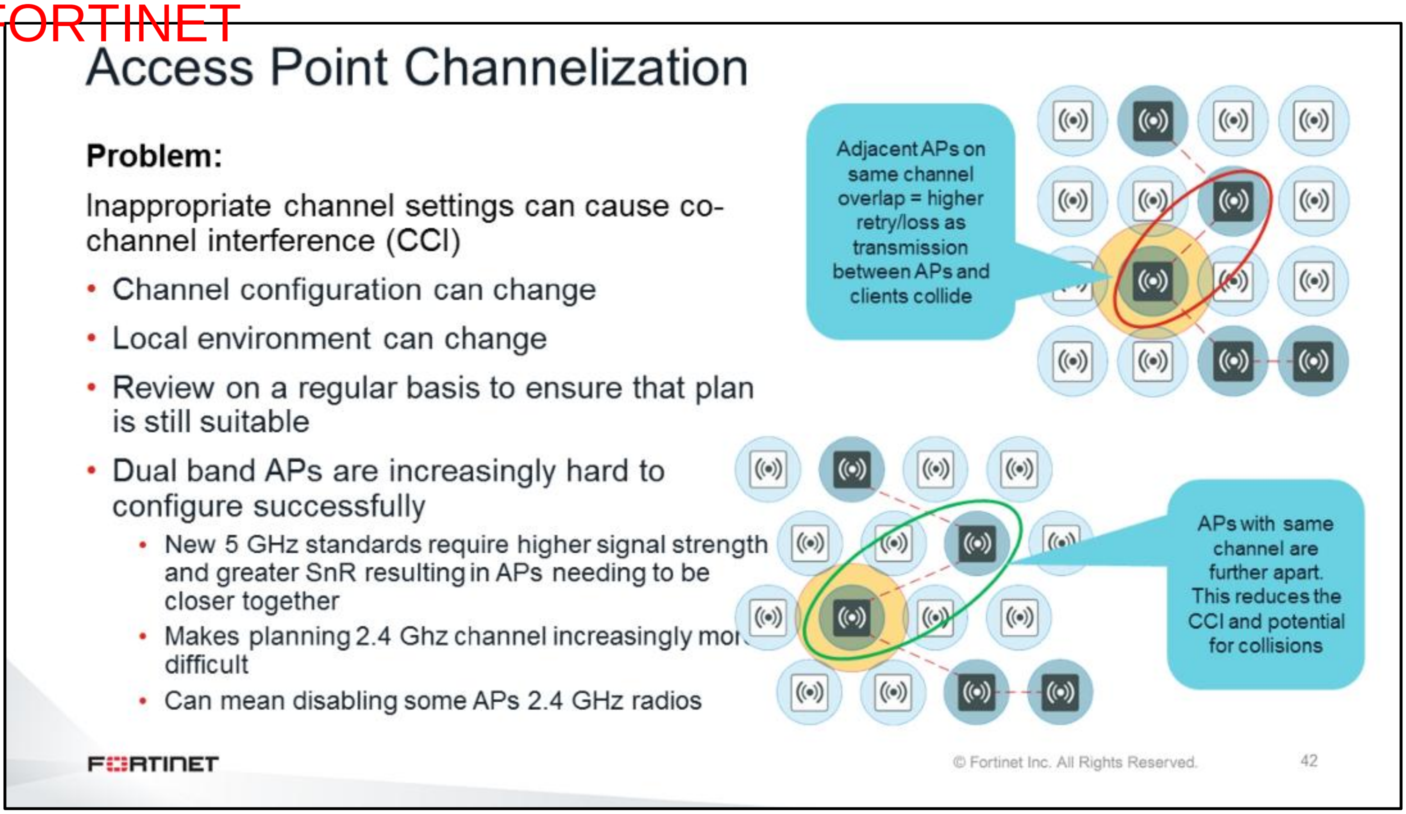
The wireless network would have been designed and specified with a target signal strength for clients. You should make sure that the majority of your clients have that minimum signal strength or greater. Is not unusual to have a small number of stations that are weaker. For example, wireless devices 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 will 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 are 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 1 or 2 stream 2.4 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 1 stream 802.11ac client) or 866 Mbps (for a 2 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.



In this section, you will learn about some of the key areas where wireless networks can experience issues.



A big source of issues with a wireless network can be incorrect channel setting.

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 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 clinets. 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.

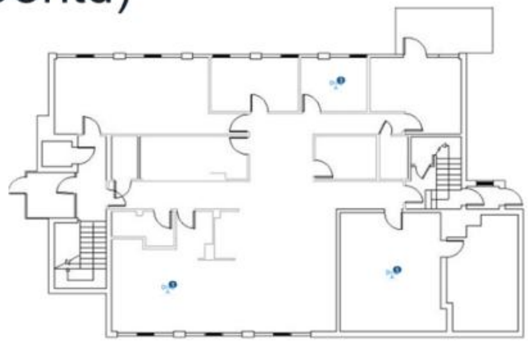
This can be too difficult to accommodate by, for instance, turning down the transmission power. So, in many modern networks, it is now common practice to turn off select 2.4 GHz radios, or at least assign them to another task, such as dedicated rogue detection.

Access Point Channelization (Contd)

- Review the channel map and identify adjacent APs that are on the same channel
  - Do this for 2.4 GHz particularly
  - Identify APs that are adjacent and on the same channel
  - Don't forget to account for APs on floor above and below
- Review the adjacent APs
  - In the **Top Wireless Interference** table in the **Wi-Fi Health Monitor**
    - Sort the table to show the strongest interfering neighbours on the same channel
  - The AP CLI using:

```
cw_diag -c his-chutil
cw_diag -c all-chutil
```

- Identify the APs that are strongest
  - -80 or stronger are likely to cause an issue



These are APs on our network. We may be able to change these

A neighboring AP outside of our network. Unlikely we could change these

Interfering APs for Office AP 1 Radio 1 (2.4 GHz Band)

Interfering AP	SSID	Channel	Signal Interference
08:5b:0e:b0:37:8a	6339	1	-51 dBm
08:5b:0e:b0:2e:9c	6339	1	-72 dBm
e4:f6:5d:28:3b:11	VodafoneConnect30834097	1	-78 dBm
70:0b:01:1f:c9:12	TALKTALK1FC915	1	-81 dBm
d0:58:fc:a8:df:7e	Wonderwillows	1	-86 dBm
94:0b:19:b8:ee:e8	VodafoneConnect87082708	1	-86 dBm
24:a7:dc:fa:7a:22	Wonderwillows	1	-88 dBm
ec:08:6b:c1:16:fe	TP-LINK_C116FE	1	-88 dBm
a0:bd:cd:cc:86:8a	Wonderwillows	1	-89 dBm
74:a5:28:b0:0d:68	TALKTALKB00D61	1	-90 dBm

FORTINET

 43

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.

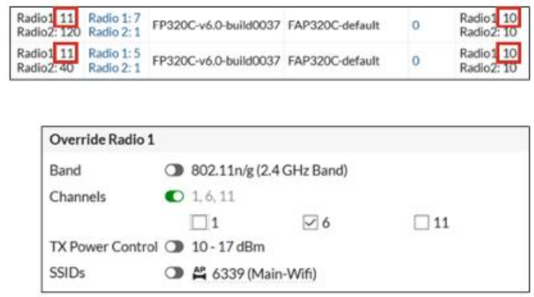
The **Top Wireless Interference** table, when sorted, also shows the APs that are potentially interfering. You can sort to highlight the strongest interfering radios. Some of these radios may well be your own, in which case, you might be able to do something about them. However, is equally likely that 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.

Access Point Channelization (Contd)

Solution:

- For own APs in 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 10dB), 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 a new profile with the interface disabled
- For APs outside of 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.



FORTINET

 44

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.

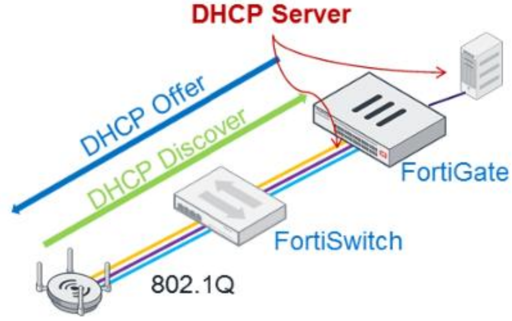
If you identify APs outside of the network, it is likely that they are outside of your control and, as such, it would be difficult to reduce their power or change the channel. As a result, the only potential option for your radios that are being interfered with is to change the channel to avoid CCI.

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**.

VPN Probe Tool

- New feature for FortiOS 6.2 (AP and FortiGate)
- Verification of VLAN availability to a FortiAP or FortiAP-S
  - Display VLANs tagged to AP port
  - Verifies DHCP availability
- Allows easy identification of AP the have missing or incorrect VLANs available at the port
- Identifies missing, misconfigured DHCP servers or relays
- Identifies DHCP server that are failing to issue IP's



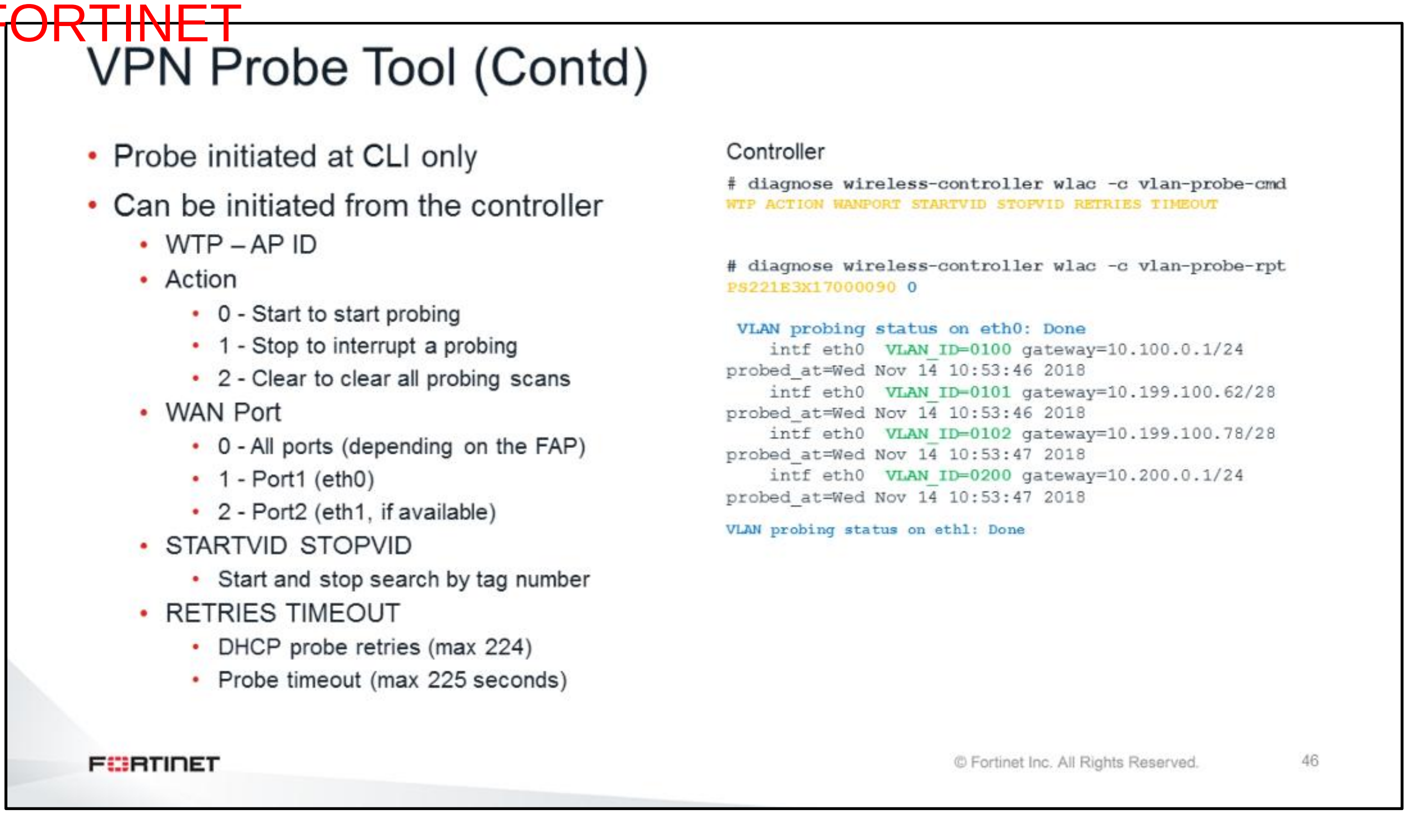
FORTINET

 45

A common cause of wireless connectivity issues is often not related to wireless connectivity at all. Wireless networks, as with all types of networks, rely on services such as DNS and DHCP to provide connectivity. Often the flexibility and the ability of a wireless network to connect clients can mean that these supporting services can suffer from overloading. The VPN Probe tool is a new feature that allows network administrators to identify issues with the DHCP and VLAN configuration on an AP wired port.

You can run the probe tool from either FortiGate or the AP itself. It displays information about VLANs that are tagged to the AP port. It will also perform DHCP availability checks, ensuring that a DHCP server is configured, and that is able to assign IP addresses.

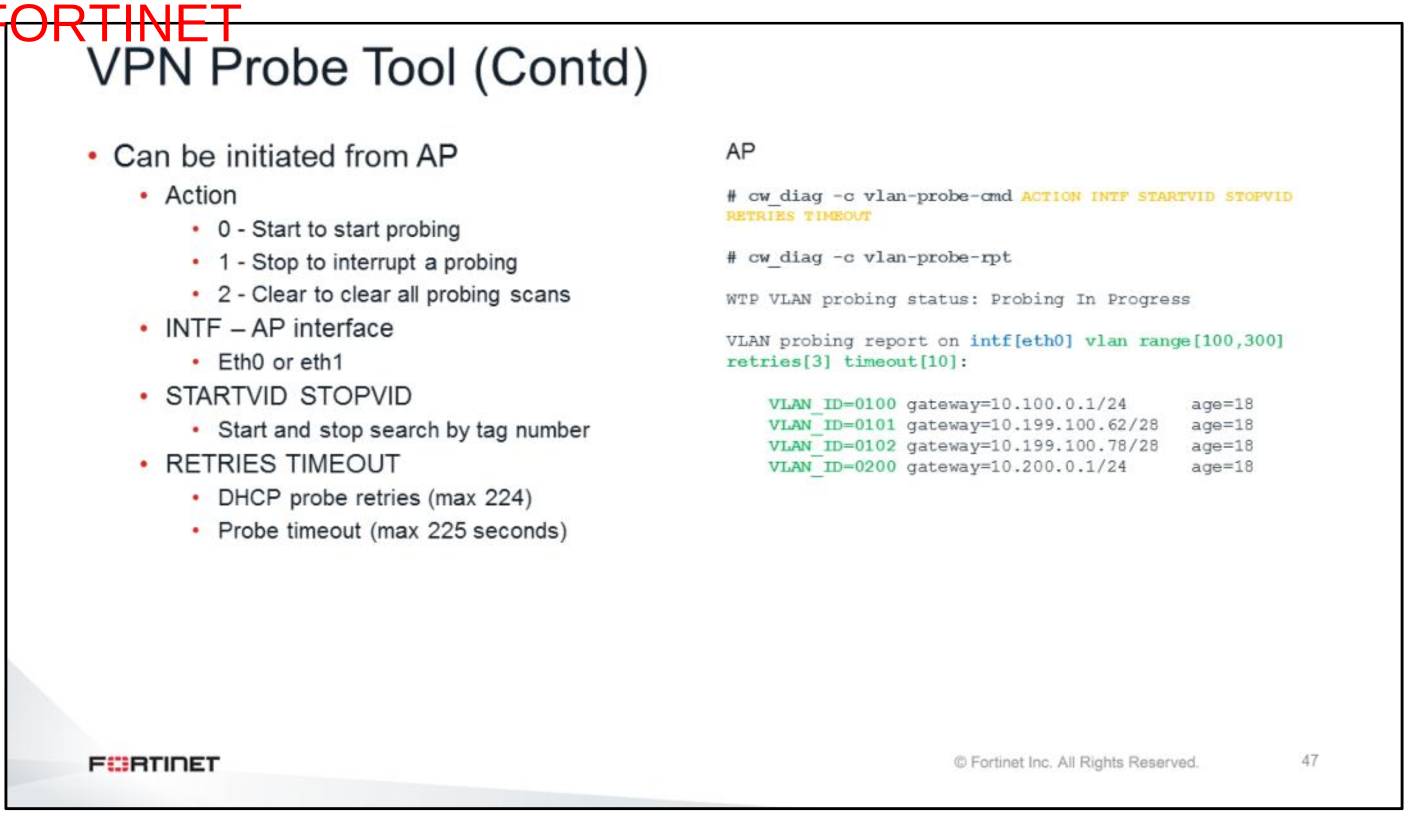
VPN Probe is a new feature in FortiOS 6.2 and requires that the AP is also updated to version 6.2 firmware.



You can run the probe tool using the CLI only, however, you can view the results in the logs using the FortiGate GUI.

When you run the probe tool using the CLI, the absolute minimum that you must specify is the access point ID, together with an appropriate command, such as zero, to start a probe. Optionally, you can specify the range of VLAN tag numbers, together with a specific AP wired interface (if the AP has multiple wide ports). You can also change the DHCP probe retries and time-out, if required.

Running the probe tool will return information about the VLANs found, together with any DHCP information gathered during the probe.



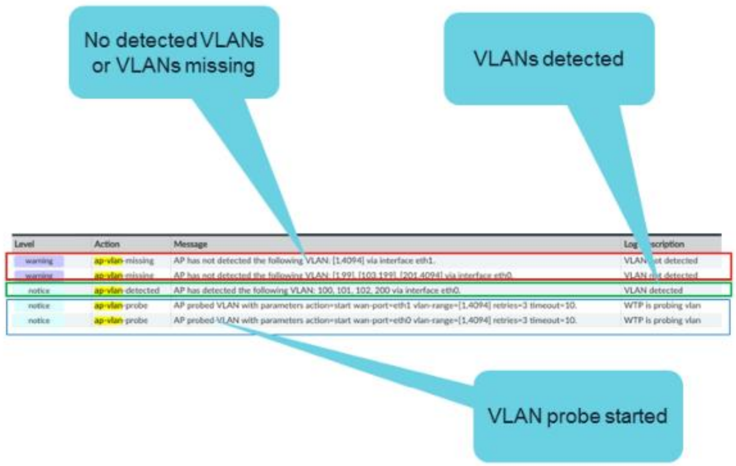
You can also run the probe tool using the AP CLI.

The CLI options are similar to running the probe tool using the FortiGate CLI, and so is the information the probe tool retrieves.

VPN Probe Tool—GUI Logs

- The FortiAP will send out a DHCP Discover on each VLAN specified in the range passed in the command option
  - If DHCP Offer is received, VLAN will be marked as Discovered
  - No DHCP Offer, VLAN will be Missing
- Immediate probe results displayed in the CLI
- Also displayed in the Wi-Fi events log

  Log & Report > **Events** > **Wi-Fi Events**



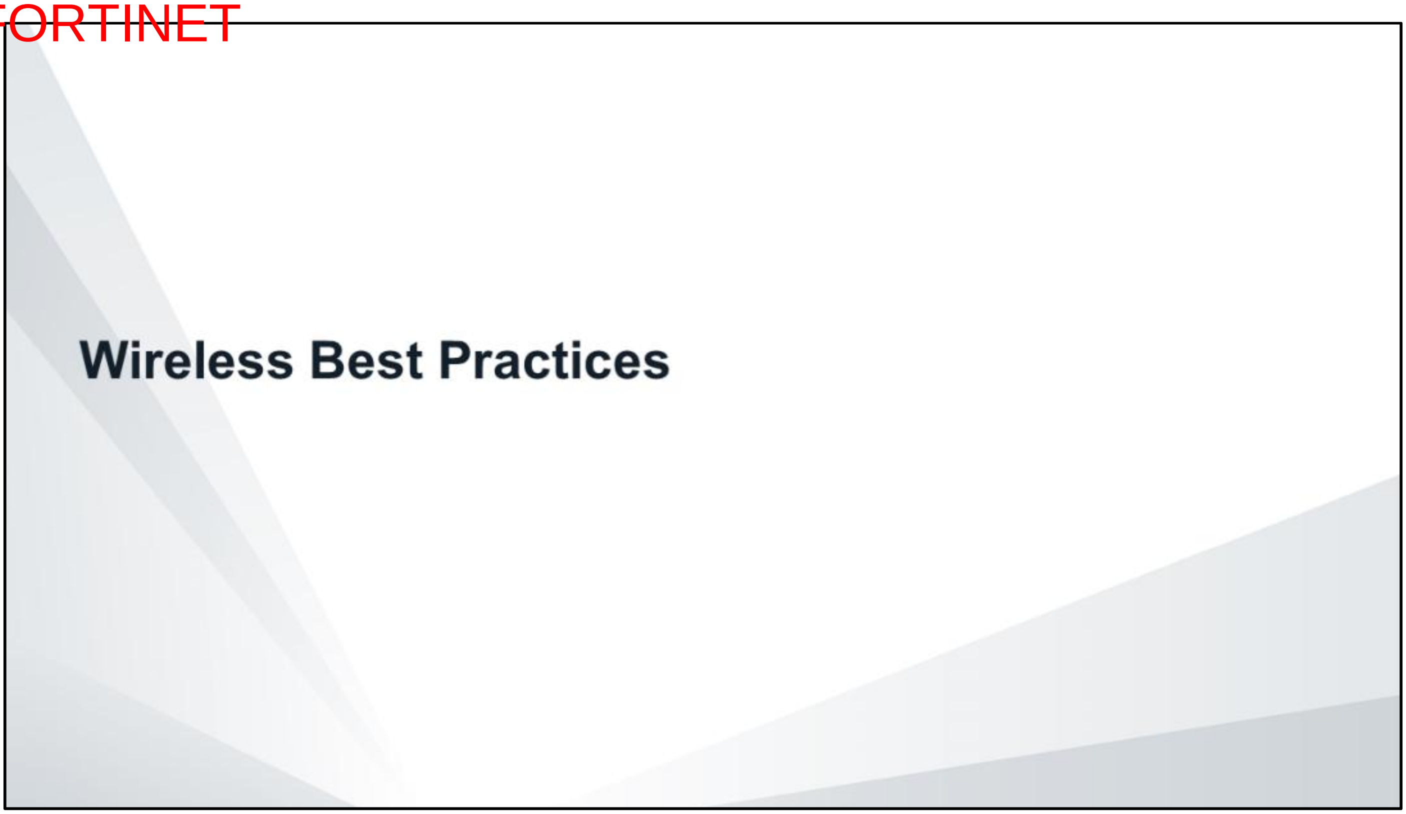
 48

The output from the commands on the CLI are immediate. The results are also displayed on the GUI in **Log & Report** > **Events** > **Wi-Fi Events**.

If you supply a range of VLANs on the CLI, the AP will attempt to discover each VLAN in the range and perform a DHCP discover.

If **DHCP Offer** is received, the VLAN will be marked as **discovered**.

If no **DHCP Offer** is received, the VLAN will be marked as **missing**.



In this section, you will learn about some of the best practices that you can adopt when deploying a wireless network.

Excessive SSID Broadcast

- Each SSID broadcast by an AP requires an amount of management traffic (frames)
- These frames carry no data. They purely allow the network to operate
- All frames take airtime
- All APs within range and on the same channel will utilize airtime

Best Practice:

- Try and limit the number of SSIDs that you advertise
- Ideally limit to no more than **5** but be aware that neighboring APs will also contribute to overhead

Number of APs on same Channel	Number of SSIDs									
	1	2	3	4	5	6	7	8	9	10
1	3%	6%	10%	13%	16%	19%	23%	26%	29%	32%
2	6%	13%	19%	26%	32%	39%	45%	52%	58%	64%
3	10%	19%	29%	39%	48%	58%	68%	77%	87%	97%
4	13%	26%	39%	52%	64%	77%	90%	100%	100%	100%
5	16%	32%	48%	64%	81%	97%	100%	100%	100%	100%
6	19%	39%	58%	77%	97%	100%	100%	100%	100%	100%
7	23%	45%	68%	90%	100%	100%	100%	100%	100%	100%
8	26%	52%	77%	100%	100%	100%	100%	100%	100%	100%

FURTINET

50

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, which 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 the slide shows an approximate calculation of the amount of airtime used when the number of APs in a channel broadcast a number of SSIDs.

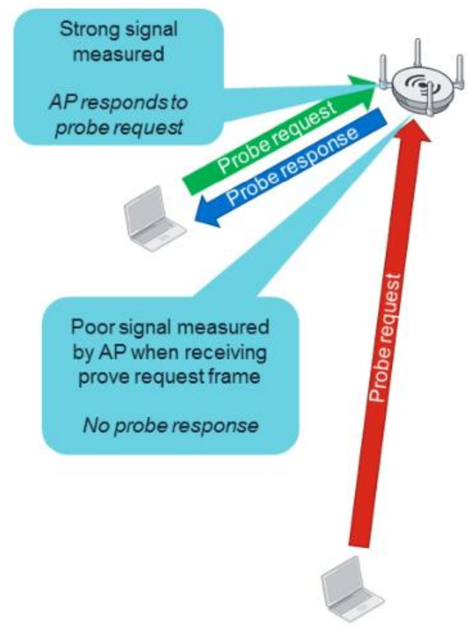
For example, if only one AP broadcasts ten networks or SSIDs, approximately 32% of the available airtime would be used sending and receiving management frames without actually exchanging any useful data. This calculation also assumes an ideal environment, with little or no interference. In the real world, 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.

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

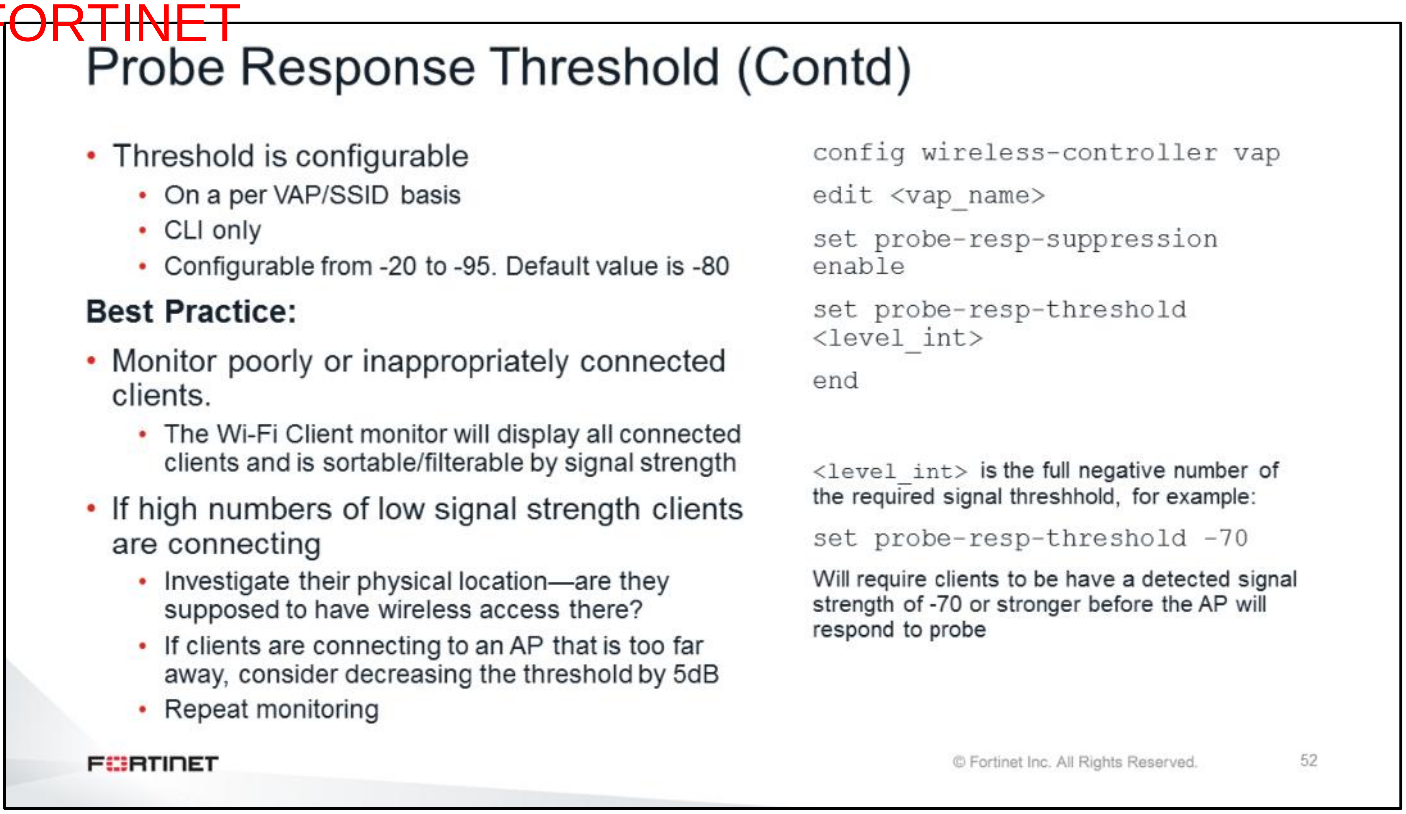


 51

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 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 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.



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 a 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:

- The 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.
- It could also mean that the 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 that 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 obvious other 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 to start with. Once the probe response threshold has changed, spend more time monitoring the client connections, and reduce the threshold, if required.

Multicast to Unicast Conversion

- Multicast data (streaming, ..) are sent at a low data rate 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

Best Practice:

- Enable by default

```
config wireless-controller vap
edit <vap_name>
set multicast-enhance enable
end
```

FERTINET

 53

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.

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 a 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
```

FORTINET

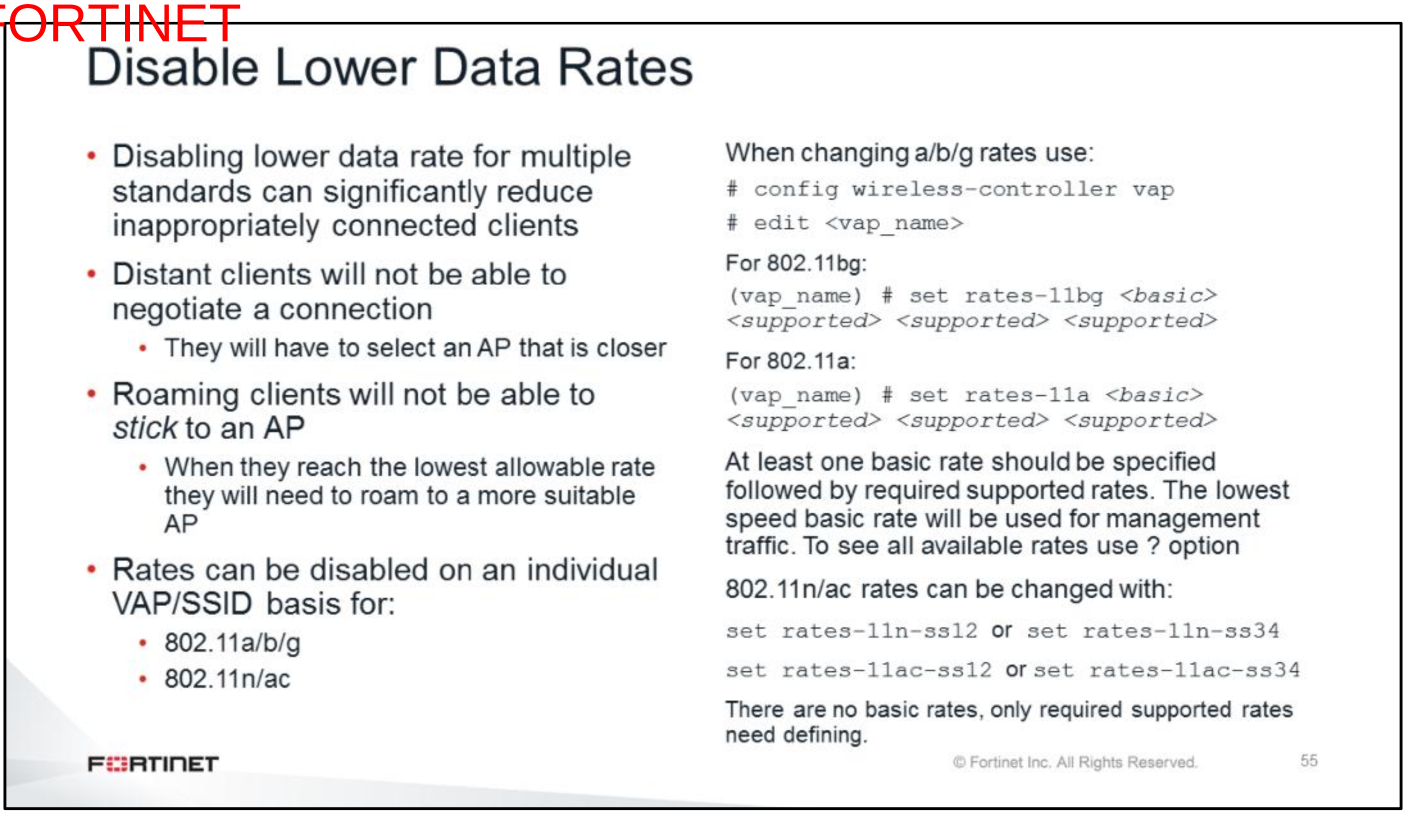
 54

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 rates, 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.



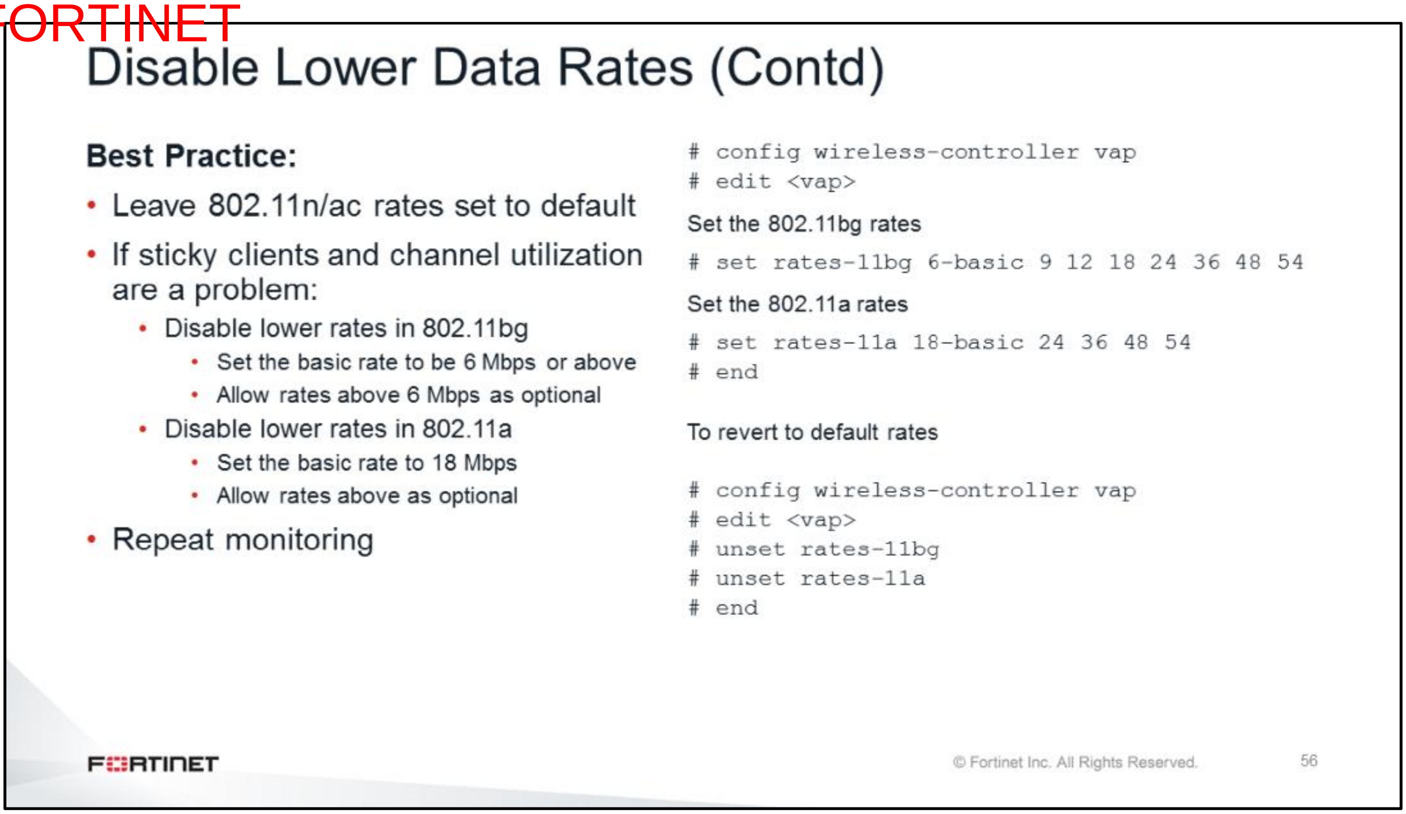
It is also possible to support data rates in a more granular way. If required, it is possible to customize the individual rates for each SSID/VAP broadcast. For example, a corporate SSID/VAP that is used to support known client types can be configured to support only higher data rates in both the 2.4 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 ac rates, you need to specify only the required supported rates.

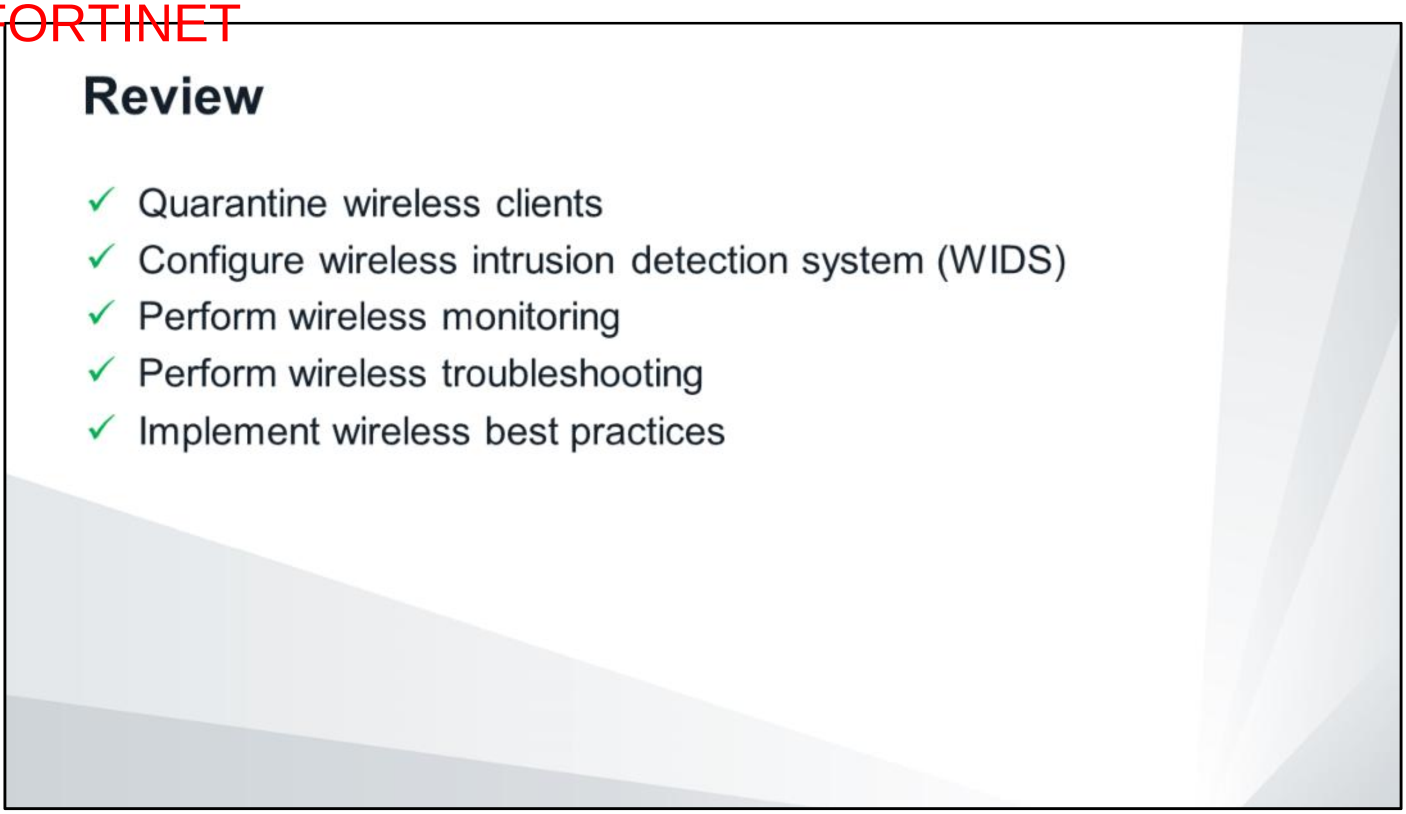


While it is possible to alter the supported rates for 802.11n and 802.11ac, there is currently no best practice that suggest it is necessary to do so.

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.



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.