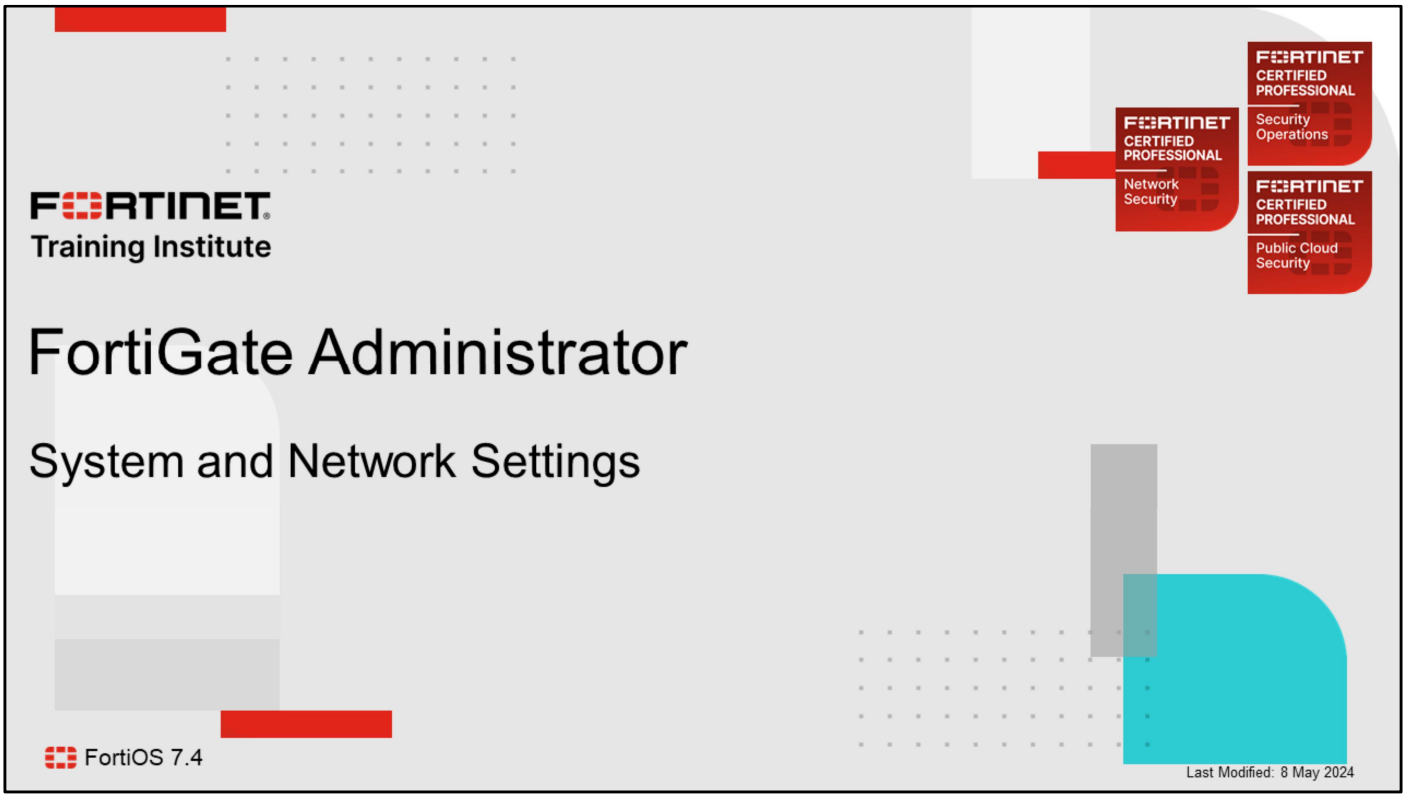



In this lesson, you will learn about system and network settings on FortiGate.

# Objectives

- Configure FortiGate on factory default settings
- Configure FortiGate as the DHCP server
- Configure and control administrator access to FortiGate
- Back up and restore system configuration files
- Upgrade FortiGate firmware
- Check and verify FortiGuard licenses

FORTINET Training Institute

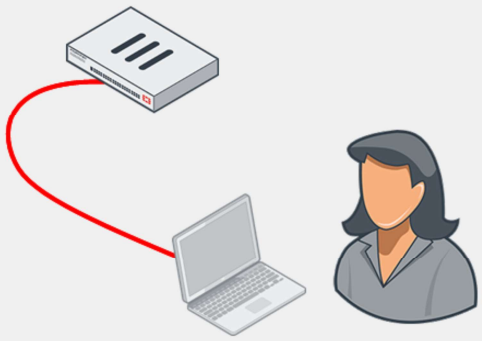
 

After completing this lesson, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in basic system and network administration, you will be able to install FortiGate into your network and configure basic networking settings. You will also be able to better manage administrative users to implement stronger security practices around administrative access.

# Factory Default Settings

- IP: `192.168.1.99/24`
  - Management interface on high-end and mid-range models
  - Port1 or internal interface on entry-level models
- PING, HTTPS, and SSH protocol management enabled
- Built-in DHCP server is enabled on port1 or internal interface
  - Only on entry-level models that support DHCP server
- Default login:
  User: `admin`
  Password: (blank)
  - Both are case sensitive
  - Modify the default (blank) password
- Can access FortiGate on the CLI
  - Console: without network
  - CLI console widget and terminal emulator, such as PuTTY or Tera Term



FORTINET Training Institute

Network address translation (NAT) mode is the default operation mode. What are the other factory default settings? After you have removed FortiGate from its box, what do you do next?

Now, you will take a look at how you set up FortiGate.

Attach your computer network cable to port1 or the internal switch ports (on the entry-level model). For high-end and mid-range models, connect to the management interface. In most entry-level models, there is a DHCP server on that interface. So, if your computer's network settings have DHCP enabled, your computer should automatically get an IP, and you can begin setup.

To access the GUI on FortiGate or FortiWiFi, open a web browser and visit `https://192.168.1.99`.

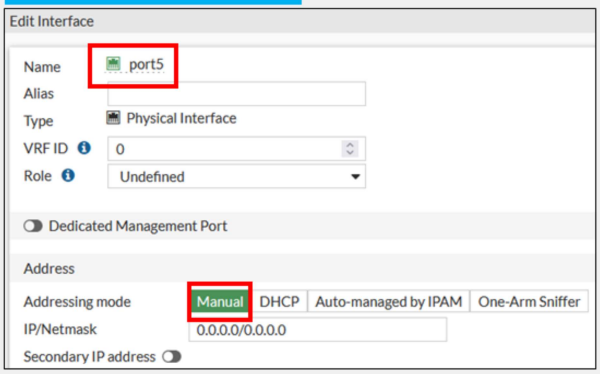
The default login information is public knowledge. Never leave the default password blank. Your network is only as secure as your FortiGate admin account. Once you logged in with default login details, you'll see a message to change the default blank password for the admin user password. Before you connect FortiGate to your network, you should set a complex password. You'll also be asked to apply additional configuration such as hostname, dashboard setup, register with FortiCare, and so on.

All FortiGate models have a console port and/or USB management port. The port provides CLI access without a network. You can access the CLI using the CLI console widget on the GUI, or from a terminal emulator, such as PuTTY or Tera Term.

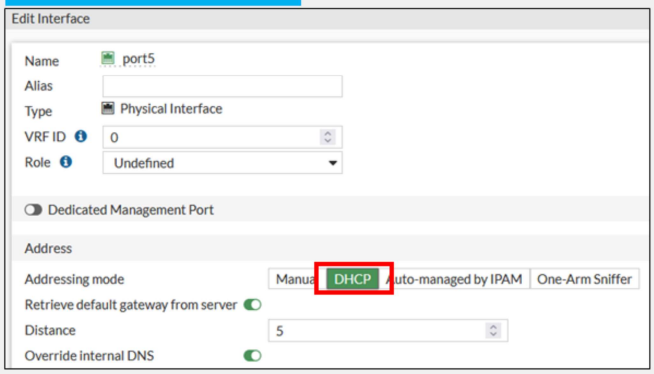
# Interface IPs

- In NAT mode, you can't use interfaces until they have an IP address:
  - Manually assigned
  - Automatic
    - DHCP
    - PPPoE

**Network > Interfaces**




**Network > Interfaces**

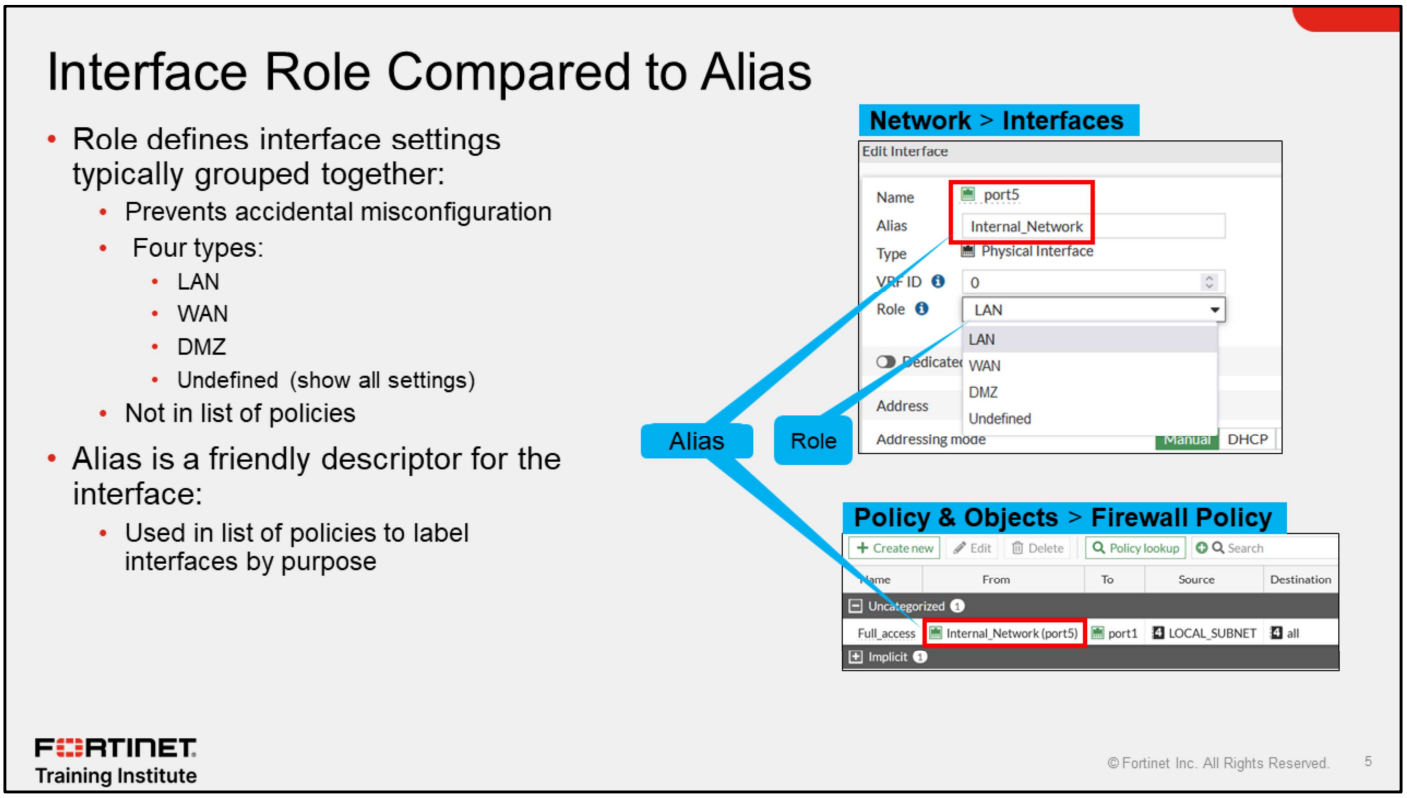



FORTINET Training Institute

When FortiGate is operating in network address translation (NAT) mode, every interface that handles traffic must have an IP address. When in NAT mode, FortiGate can use the IP address to source the traffic, if it needs to start or reply to a session, and as a destination address for devices trying to contact FortiGate or route traffic through it. There are multiple ways to get an IP address:

- Manually
- Automatically, using either DHCP or Point-to-Point Protocol over Ethernet (PPPoE) (available on the CLI)



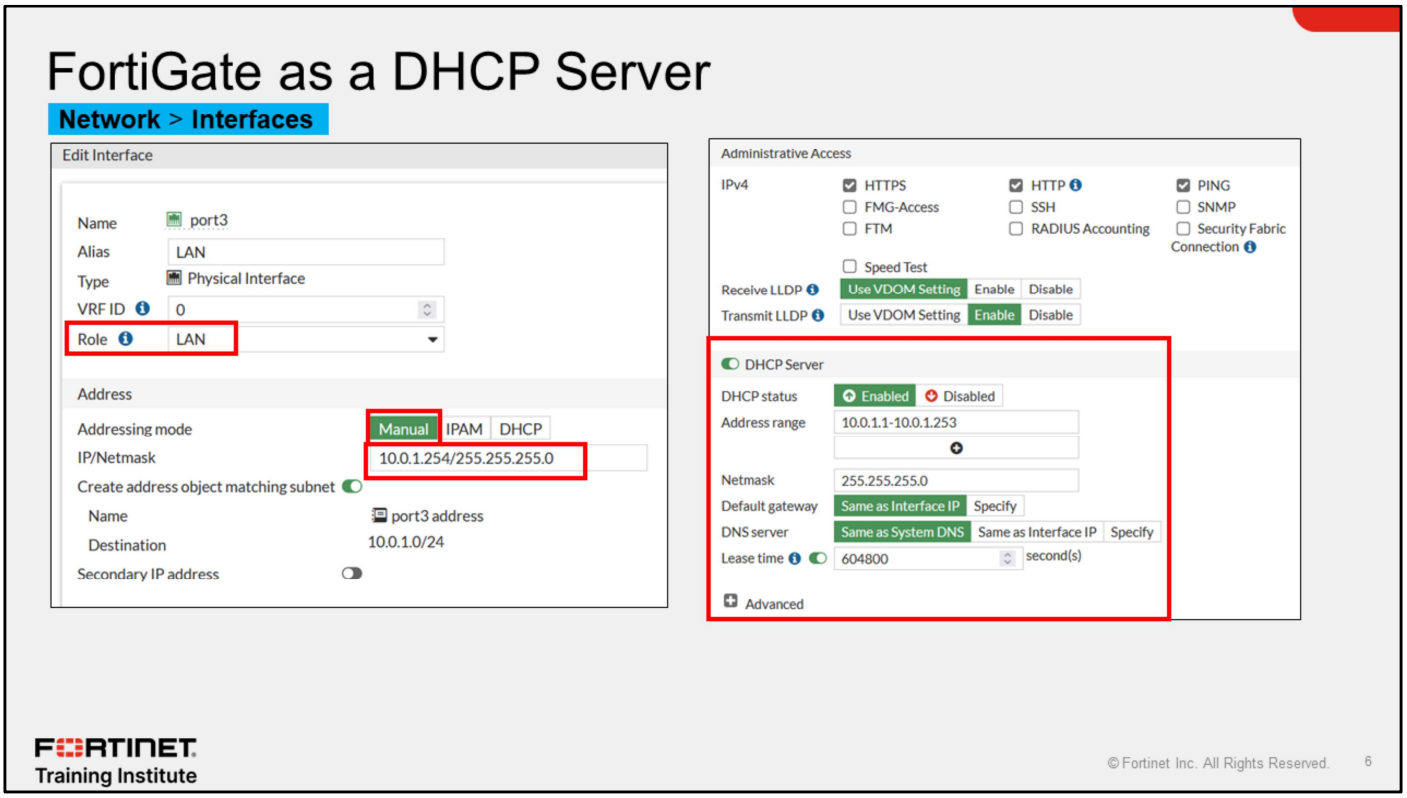

How many times have you seen network issues caused by a DHCP server—not client—enabled on the WAN interface?

You can configure the interface role. The roles shown on the GUI are the usual interface settings for that part of a topology. Settings that do not apply to the current role are hidden on the GUI. (All settings are always available on the CLI, regardless of the role.) This prevents accidental misconfiguration.

For example, when the role is configured as **WAN**, there is no DHCP server and device detection configuration available. Device detection is usually used to detect devices internally on your LAN.

If there is an unusual case, and you need to use an option that's hidden by the current role, you can always switch the role to **Undefined**. This displays all options.

To help you remember the use of each interface, you can give them aliases. For example, you could call port3 `internal_network`. This can help to make your list of policies easier to comprehend.




Wireless clients are not the only ones that can use FortiGate as their DHCP server.

For an interface (such as port3), select the **Manual** option, enter a static IP, and then enable the **DHCP Server** option. Options for the built-in DHCP server appear, including provisioning features, such as DHCP options and IP address assignment rules.

# VLANs

Physical interfaces

VLANs

- *Logically* subdivide your physical layer 2 network into smaller segments
  - Each segment forms a separate broadcast domain
  - VLAN tags added to frames to identify their network segments

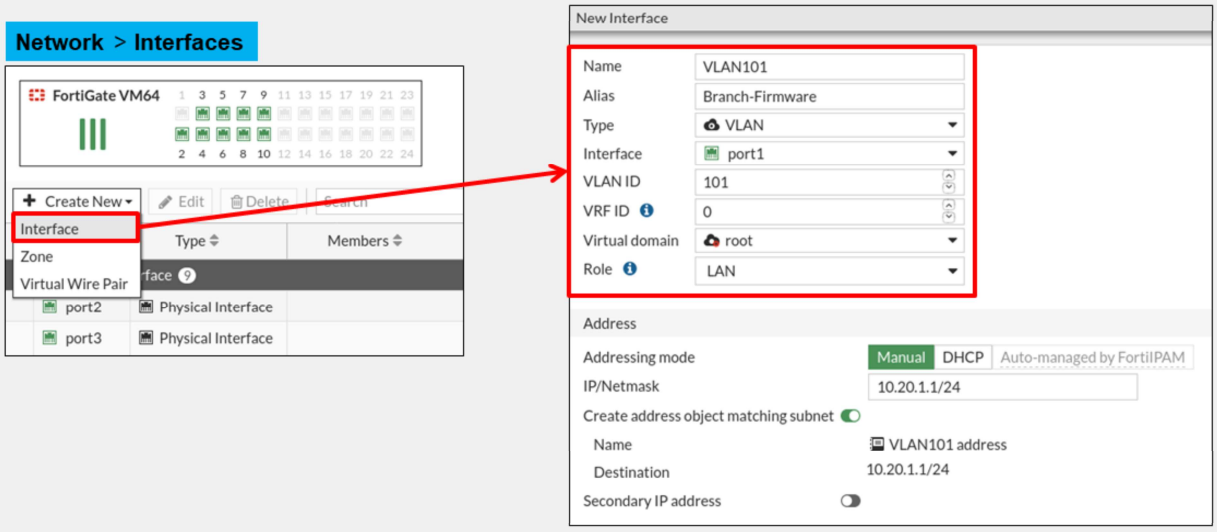
FORTINET Training Institute

VLANs split your physical LAN into multiple, logical LANs. In NAT operation mode, each VLAN forms a separate broadcast domain. Multiple VLANs can coexist in the same physical interface, provided they have different VLAN IDs. In this way, a physical interface is split into two or more logical interfaces. A tag is added to each Ethernet frame to identify the VLAN to which it belongs.

# Creating VLANs

- Frames sent or received by the physical interface segment are never tagged; they belong to the *native* VLAN

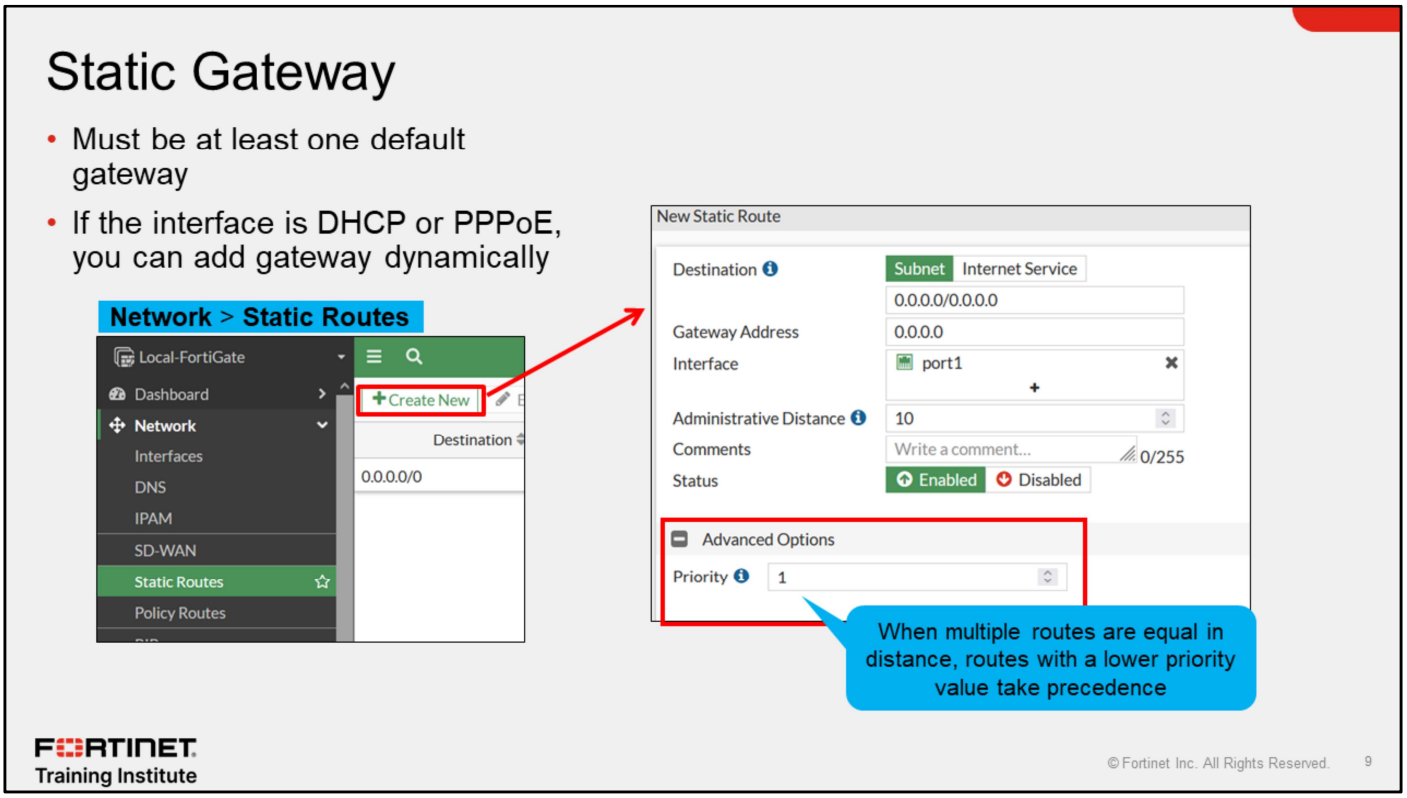



FORTINET Training Institute

To create a VLAN using the GUI, click **Create New**, select **Interface**, and then, in the **Type** field, select **VLAN**. You must specify the VLAN ID and the physical interface to which the VLAN will be bound. Frames that belong to interfaces of that type are always tagged. On the other hand, frames sent or received by the physical interface segment are never tagged. They belong to what is called the *native* VLAN (VLAN ID 0).

Note that in a multi-VDOM environment, the physical interface and its VLAN subinterface can be in separate VDOMs.




Before you integrate FortiGate into your network, you should configure a default gateway.

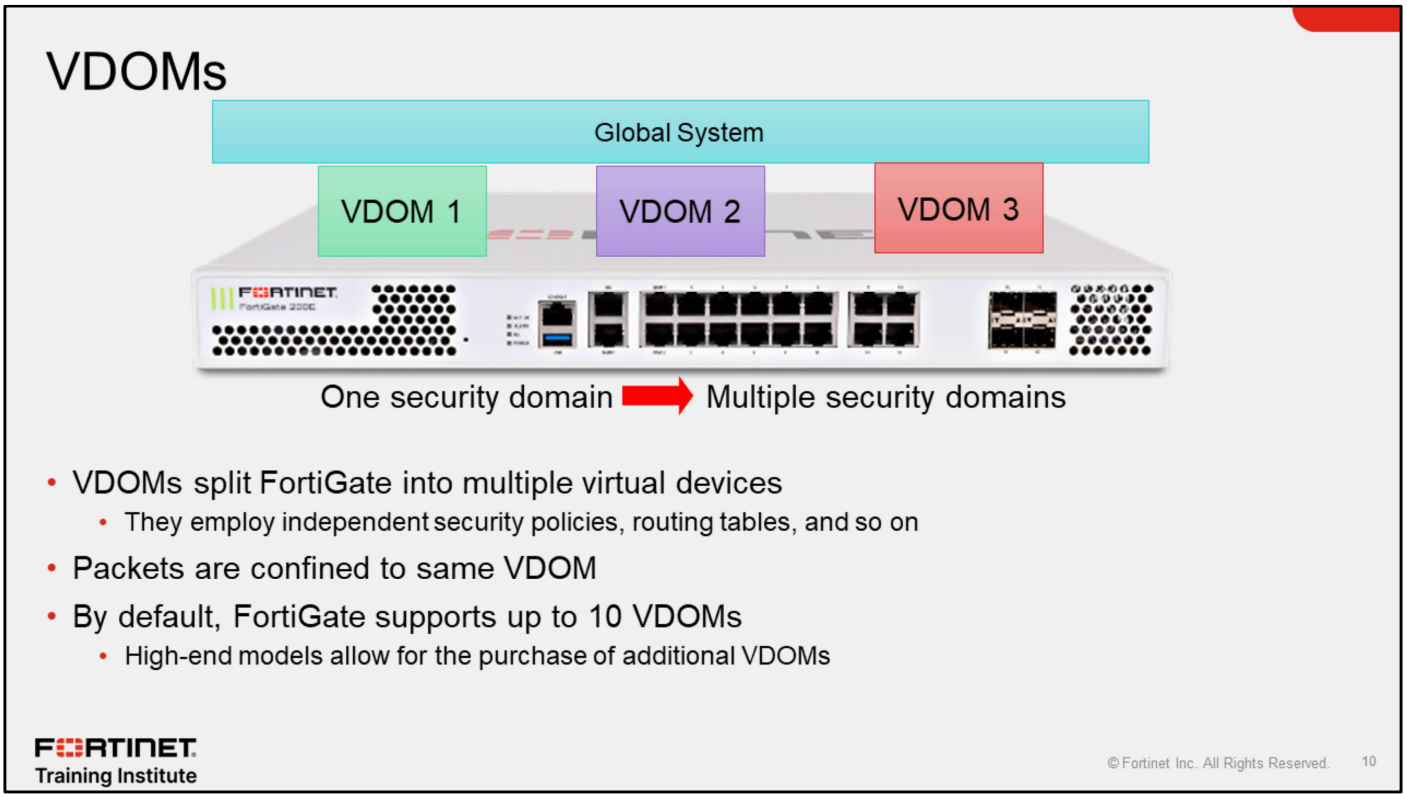
If FortiGate gets its IP address through a dynamic method, such as DHCP or PPPoE, then it should also retrieve the default gateway.

Otherwise, you must configure a static route. Without this, FortiGate will not be able to respond to packets outside the subnets directly attached to its own interfaces. It probably also will not be able to connect to FortiGuard—important for FortiGate to access—for updates, and may not correctly route traffic.

You should make sure that FortiGate has a route that matches all packets (destination is `0.0.0.0/0`), known as a default route, and forwards them through the network interface that is connected to the internet, to the IP address of the next router.

Routing completes the basic network settings that are required before you can configure firewall policies.

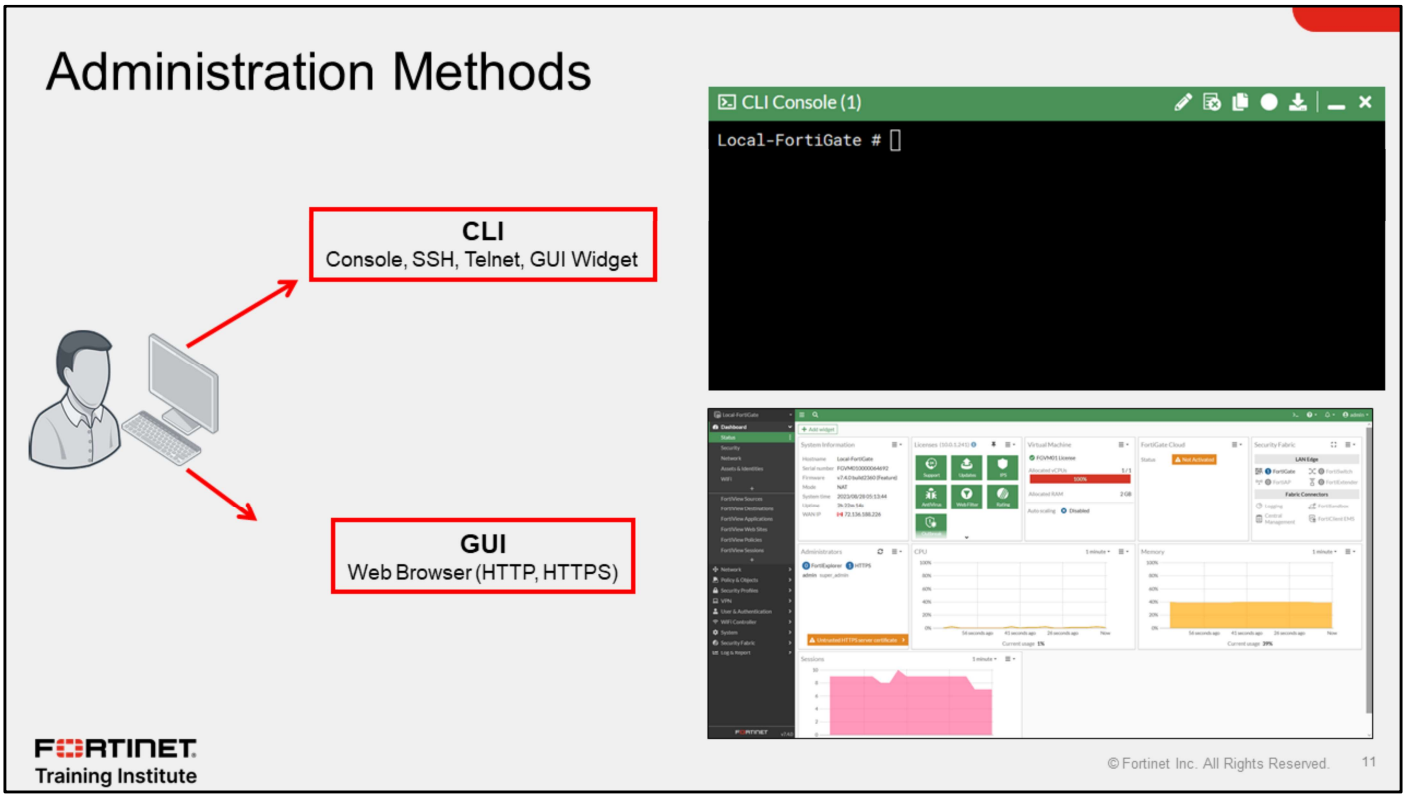
You can expand **Advanced Options** and enter a priority value. When two routes have an equal distance, the route with a lower priority value takes precedence.




What if, more than segmenting your network, you want to subdivide policies and administrators into multiple security domains?

In that case, you can enable FortiGate VDOMs, which split your FortiGate into multiple logical devices. Each VDOM has independent security policies and routing tables. Also, and by default, traffic from one VDOM cannot go to a different VDOM. This means that two interfaces in different VDOMs can share the same IP address, without any overlapping subnet problems.

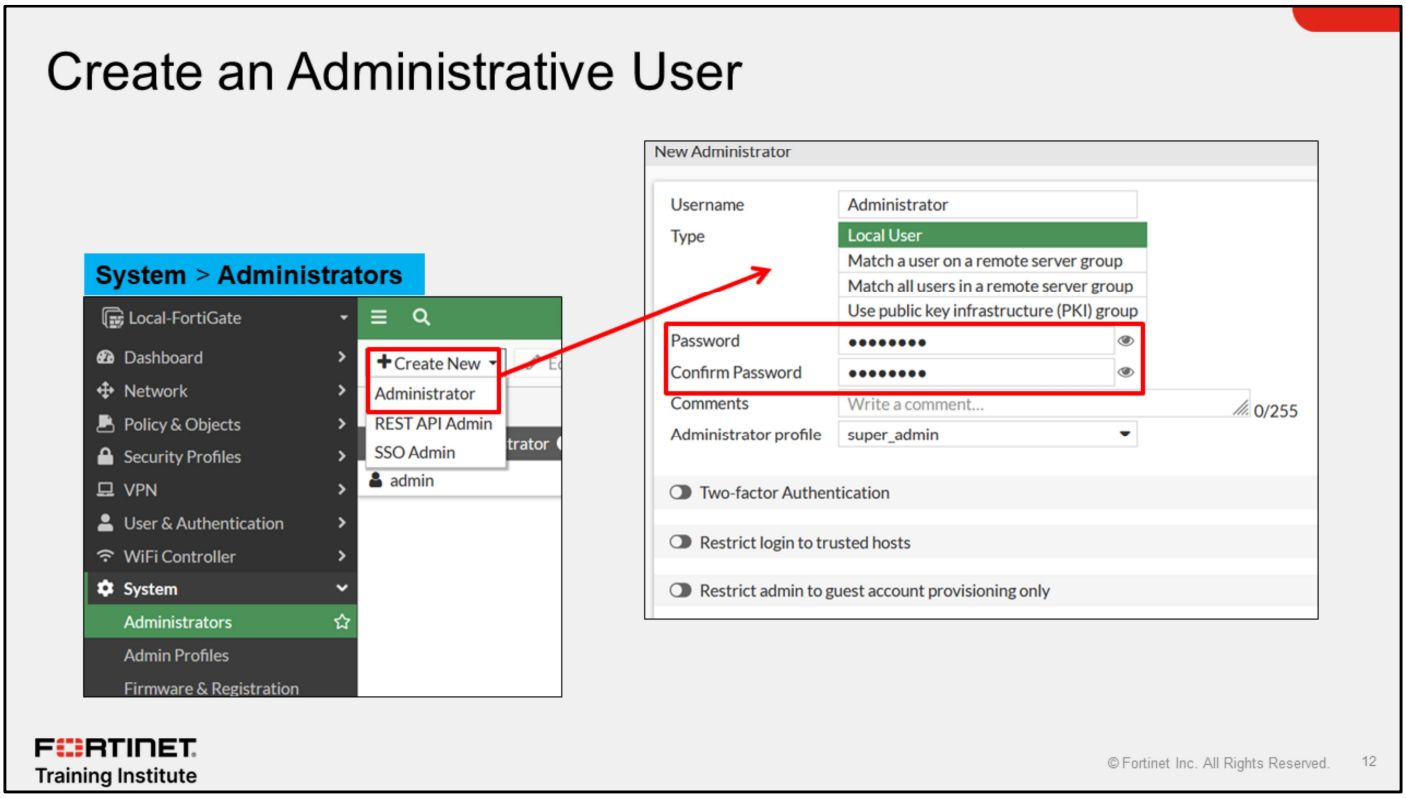
When you use VDOMs, a single FortiGate device becomes a virtual data center of network security, unified threat management (UTM) inspection, and secure communication devices.




Most features are available on both the GUI and CLI, but there are a few exceptions. You can't view reports on the CLI. Also, advanced settings and diagnostic commands for super users are usually not available on the GUI.

As you become more familiar with FortiGate, and especially if you want to script its configuration, you might want to use the CLI in addition to the GUI. You can access the CLI through either the JavaScript widget on the GUI named **CLI Console**, or through a terminal emulator such as Tera Term or PuTTY. Your terminal emulator can connect through the network—SSH or Telnet—or the local console port.

SNMP and some other administrative protocols are also supported, but they are read-only. You can't use them for basic setup.




Whichever method you use, start by logging in as admin. Begin by creating separate accounts for other administrators. For security and tracking purposes, it is a best practice for each administrator to have their own account.

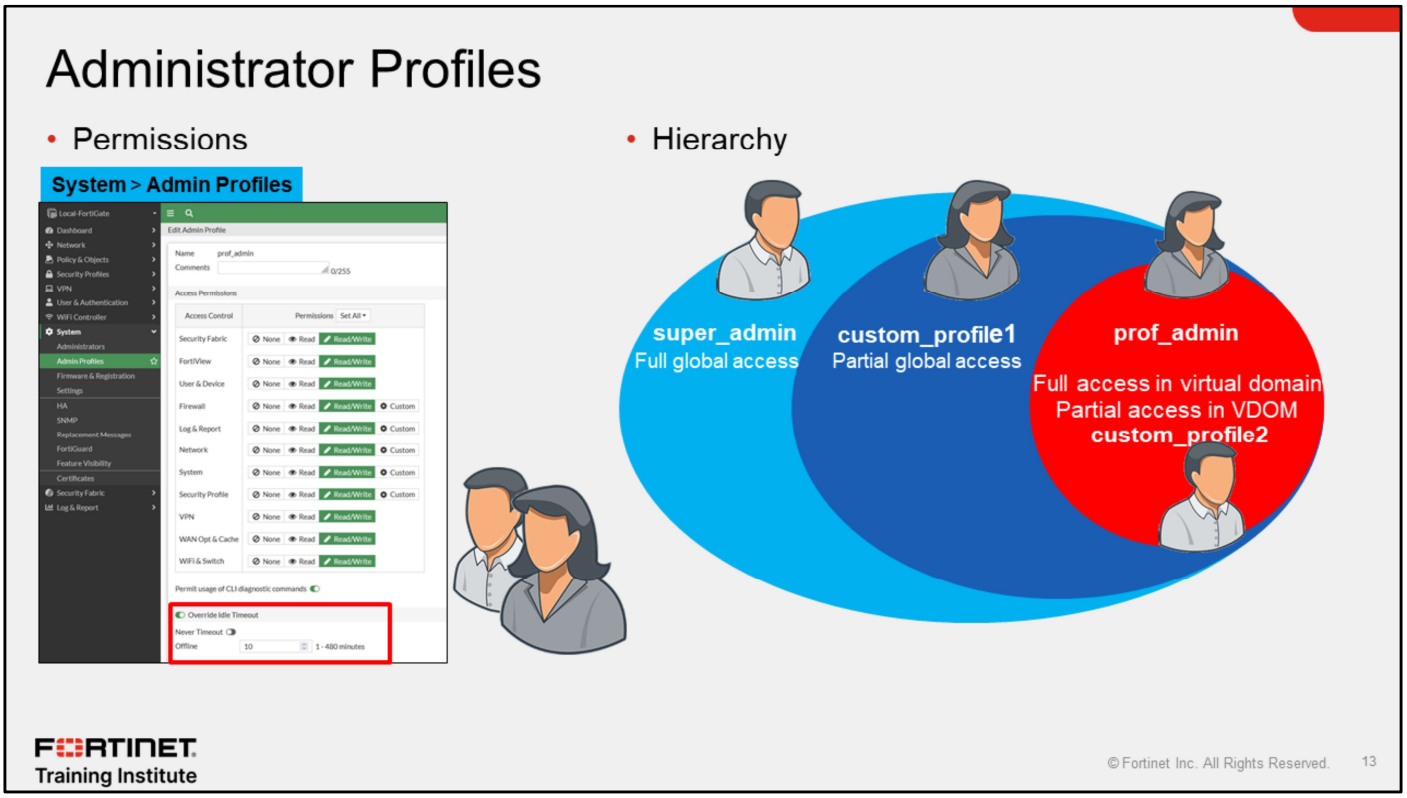
In the **Create New** field, you can select either **Administrator** or **REST API Admin**. Typically, you will select **Administrator** and then assign an **Administrator Profile**, which specifies that user's administrative permissions. You could select **REST API Admin** to add an administrative user who would use a custom application to access FortiGate with a REST API. The application would allow you to log in to FortiGate and perform any task that your assigned **Administrator Profile** permits.

Other options, not shown here, include:

- Instead of creating accounts on FortiGate, you could configure FortiGate to query a remote authentication server.
- In place of passwords, your administrators could authenticate using digital certificates that are issued by your internal certification authority server.

If you do use passwords, ensure that they are strong and complex. For example, you could use multiple interleaved words with varying capitalization, and randomly insert numbers and punctuation. Do not use short passwords, or passwords that contain names, dates, or words that exist in any dictionary. These are susceptible to brute force attack. To audit the strength of your passwords, use tools such as L0phtcrack (http://www.l0phtcrack.com/) or John the Ripper (http://www.openwall.com/john/). Risk of a brute force attack is increased if you connect the management port to the internet.

In order to restrict access to specific features, you can assign permissions.



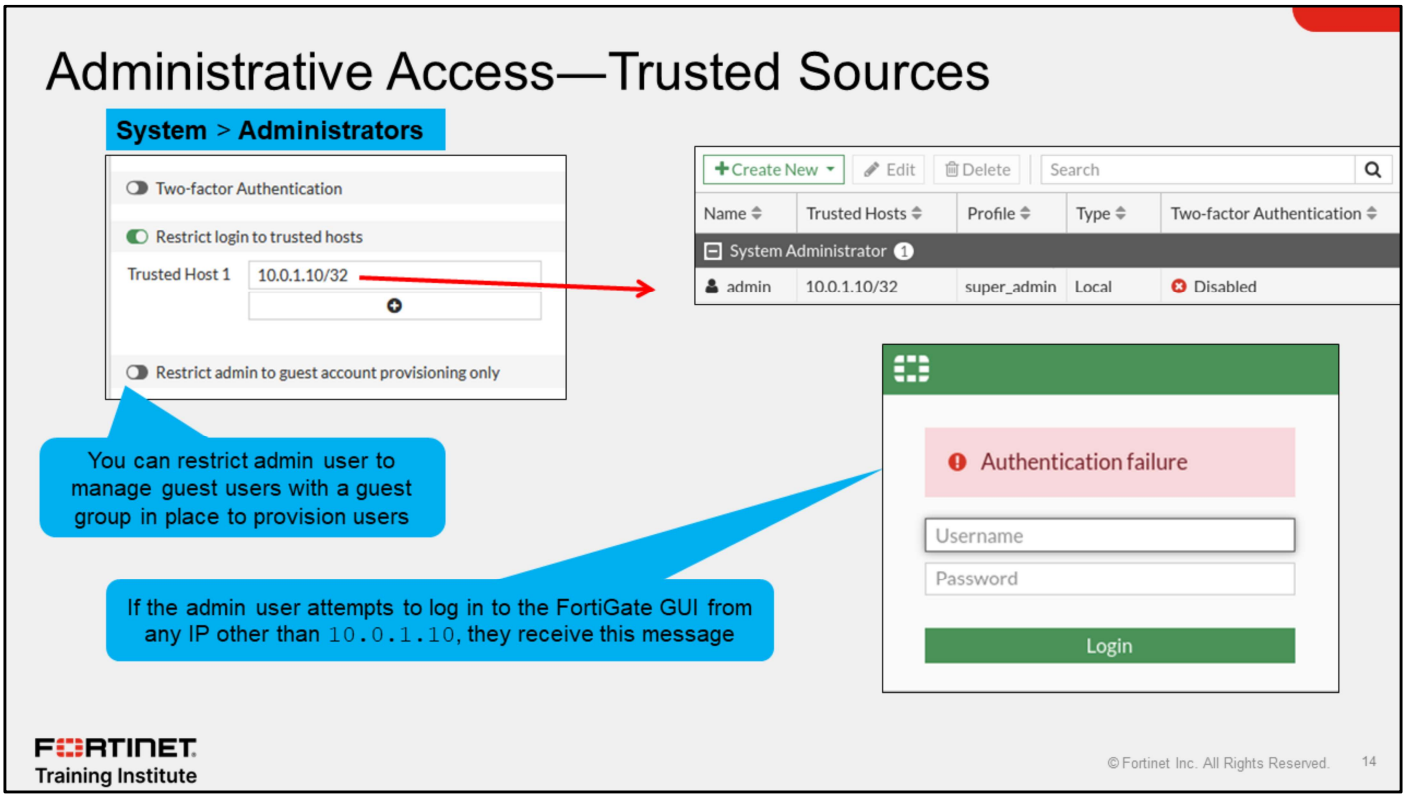

When assigning permissions to an administrator profile, you can specify read-and-write, read-only, or none to each area.

By default, there is a special profile named super_admin, which is used by the account named admin. You can't change it. It provides full access to everything, making the *admin* account similar to a root superuser account. The prof_admin is another default profile. It also provides full access, but unlike super_admin, it applies only to its virtual domain—not the global settings of FortiGate you can change its permissions.

You aren't required to use a default profile. You could create a profile named auditor_access with read-only permissions. Restricting a person's permissions to those necessary for his or her job is a best practice, because even if that account is compromised, the compromise to your FortiGate device (or network) is not total. To do this, create administrator profiles, then select the appropriate profile when configuring an account.

The **Override Idle Timeout** option allows the `admintimeout` value, under `config system accprofile`, to be overridden per access profile. You can configure administrator profiles to increase inactivity timeout and facilitate use of the GUI for central monitoring. Note that you can do this on a per-profile basis, to prevent the option from being unintentionally set globally. So, what are the effects of administrator profiles?

It's actually more than just read or write access. Depending on the type of administrator profile that you assign, an administrator may not be able to access the entire FortiGate device. For example, you could configure an account that can view only log messages. Administrators may not be able to access global settings outside their assigned virtual domain either. Virtual domains (VDOMs) are a way of subdividing the resources and configurations on a single FortiGate. Administrators with a smaller scope of permissions cannot create, or even view, accounts with more permissions.




Another way to secure FortiGate is to define the hosts or subnets that are trusted sources from which to log in.

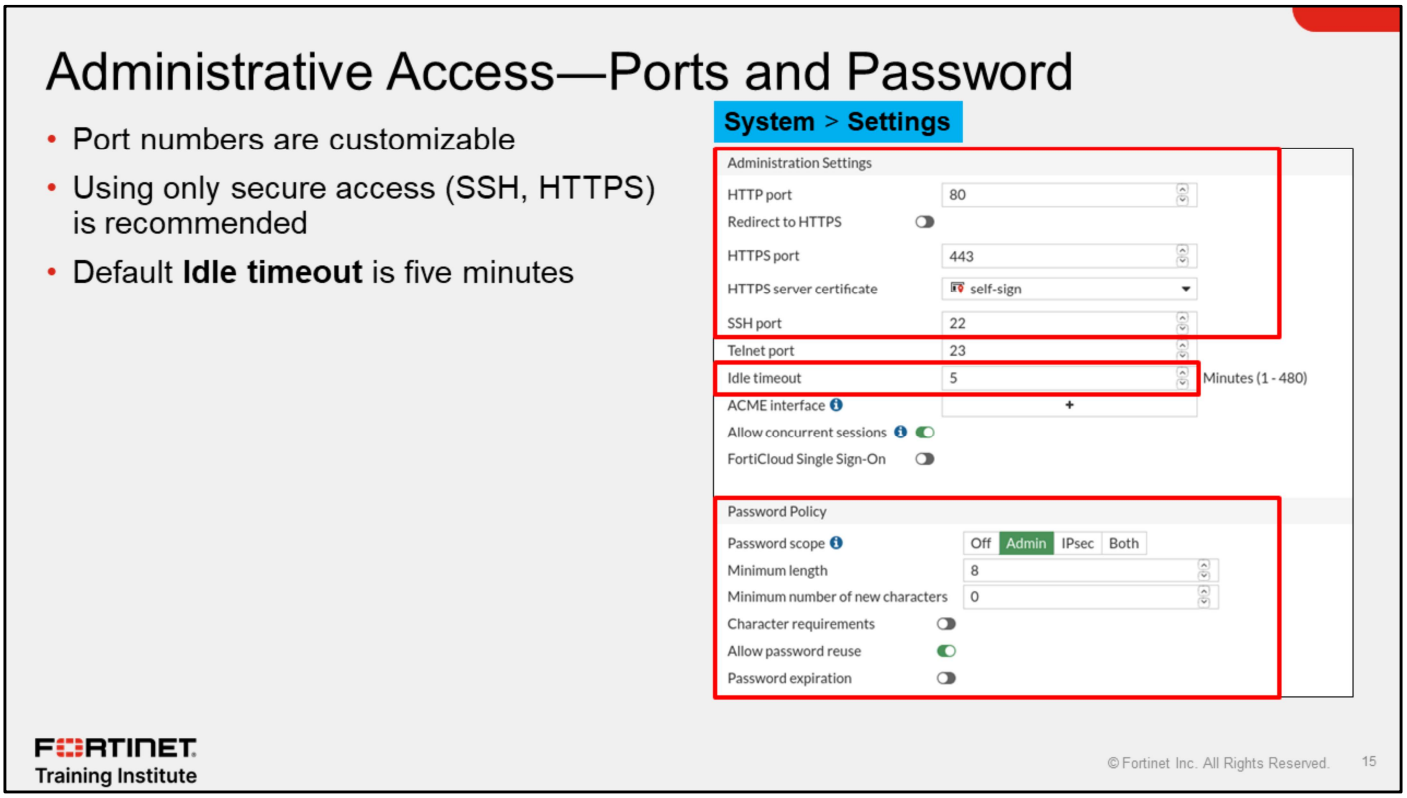
In this example, `10.0.1.10` is configured as the only trusted IP for admin from which admin logs in. If admin attempts to log in from a machine with any other IP, they will receive an authentication failure message.

Note that if trusted hosts are configured on all administrators and an administrator is trying to log in from an IP address that is not set on any of the trusted hosts for any administrators, then the administrator will not get the login page. Instead, the administrator will receive this message: “Unable to contact server”.

If you leave any IPv4 address as `0.0.0.0/0`, it means that connections from any source IP will be allowed. By default, `0.0.0.0/0` is the configuration for the administrator, although you may want to change this.

Notice that each account can define its management host or subnet differently. Be aware of any NAT that occurs between the desired device and FortiGate. You can easily prevent an administrator from logging in from the desired IP address if it is later NATed to another address before reaching FortiGate, thus defeating the purpose of the trusted hosts.

Another option to configure an administrator account to restrict access to only provision guest user accounts. By enabling this option, the administrator account will be able to provision guest user account given the fact a guest user group is available to provision guest users.




You may also want to customize the administrative protocols port numbers.

You can choose whether to allow concurrent sessions. You can use concurrent sessions to avoid accidentally overwriting settings, if you usually keep multiple browser tabs open, or accidentally leave a CLI session open without saving the settings, then begin a GUI session and accidentally edit the same settings differently.

For better security, use only secure protocols, and enforce password complexity and changes.

The **Idle timeout** settings specifies the number of minutes before an inactive administrator session times out (default is five minutes). A shorter idle timeout is more secure, but increasing the timer can help reduce the chance of administrators being logged out while testing changes.

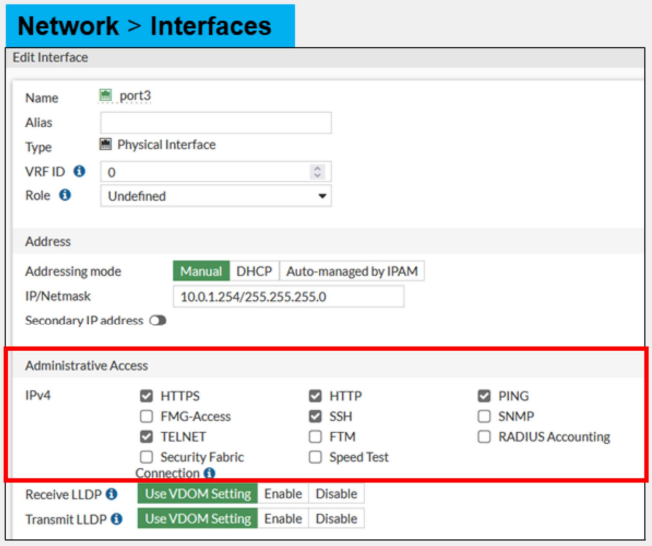
You can override the idle timeout setting per administrator profile using the **Override Idle Timeout** setting.

You can configure an administrator profile to increase inactivity timeout and facilitate use of the GUI for central monitoring. The **Override Idle Timeout** setting allows the **admintimeout** value, under **config system accprofile**, to be overridden per access profile.

Note that you can do this on a per profile basis, to avoid the option from being unintentionally set globally.

# Administrative Access—Protocols

- Enable acceptable management protocols on each interface independently:
  - Separate IPv4 and IPv6
  - IPv6 options hidden by default
- Also protocols where FortiGate is the destination IP:
  - Security Fabric Connection:
    - CAPWAP
    - FortiTelemetry
  - FMG-Access
  - FTM
  - RADIUS Accounting
- LLDP support
  - Detecting an upstream Security Fabric FortiGate through LLDP



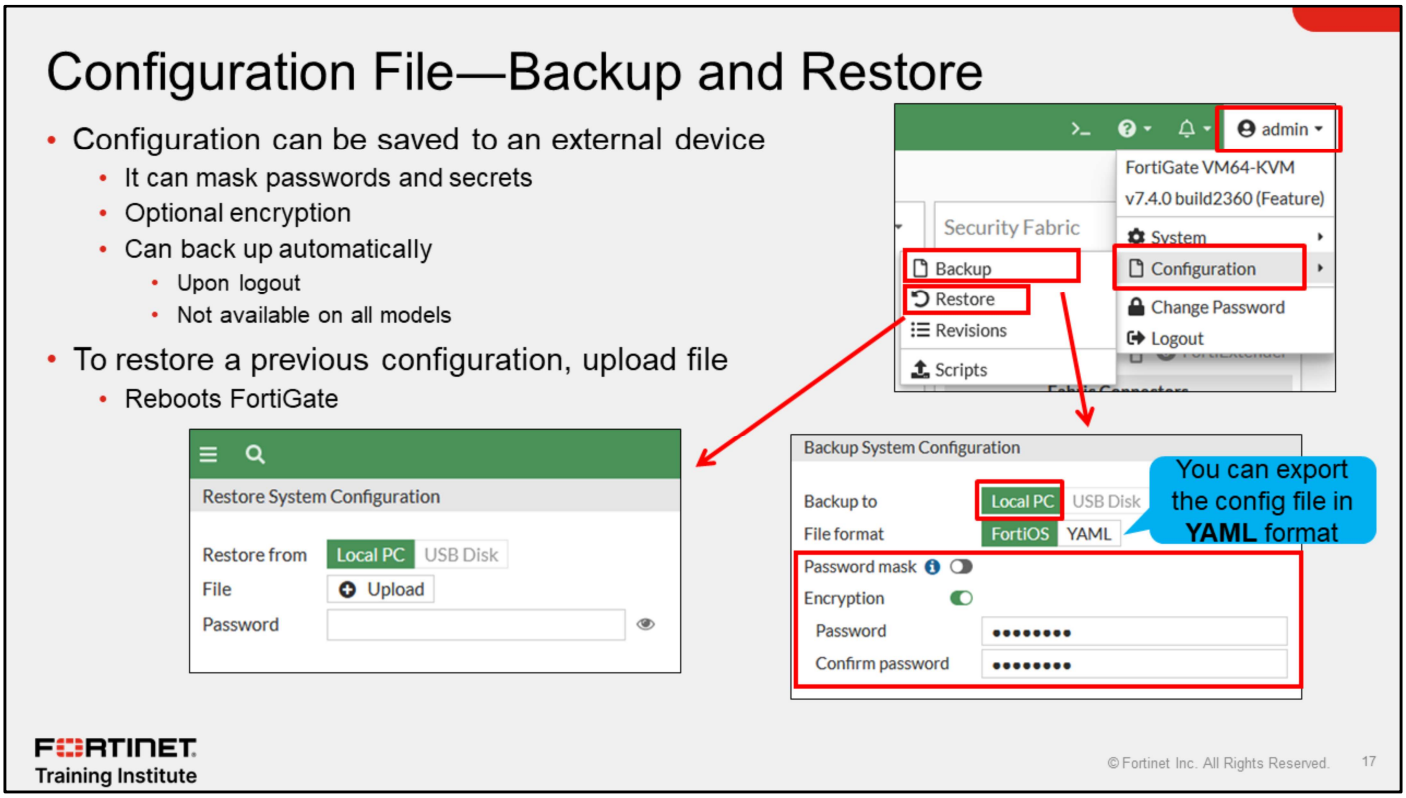

FORTINET Training Institute

You've defined the management subnet—that is, the trusted hosts—for each administrator account. How do you enable or disable management protocols?
This is specific to each interface. For example, if your administrators connect to FortiGate only from port3, then you should disable administrative access on all other ports. This prevents brute force attempts and also insecure access. Your management protocols are HTTPS, HTTP, PING, and SSH. By default, the HTTP and TELNET option is not visible on the GUI.

Consider the location of the interface on your network. Enabling PING on an internal interface is useful for troubleshooting. However, if it's an external interface (in other words, exposed to the internet), then the PING protocol could expose FortiGate to a DoS attack. You should disable protocols that do not encrypt data flow, such as HTTP and TELNET. IPv4 and IPv6 protocols are separate. It's possible to have both IPv4 and IPv6 addresses on an interface, but only respond to pings on IPv6.

Security Fabric connection includes CAPWAP and FortiTelemetry. Protocols like FortiTelemetry are *not* for administrative access, but, like GUI and CLI access, they are protocols where the packets have FortiGate as a destination IP. Use the FortiTelemetry protocol specifically for managing FortiClient and the Security Fabric. Use the CAPWAP protocol for FortiAP, FortiSwitch, and FortiExtender when they are managed by FortiGate. Use the FMG-Access protocol specifically for communicating with FortiManager when that server is managing multiple FortiGate devices. Use the RADIUS accounting protocol when FortiGate needs to listen for and process RADIUS accounting packets for single sign-on authentication. FTM, or FortiToken Mobile push, supports second-factor authentication requests from a FortiToken mobile app.
When you assign the interface roles LAN or WAN to the appropriate interfaces, your FortiGate uses the Link Layer Discovery Protocol (LLDP) to detect if there's an upstream FortiGate in your network. If FortiGate discovers an upstream FortiGate, you're prompted to configure the upstream FortiGate device to join the Security Fabric.



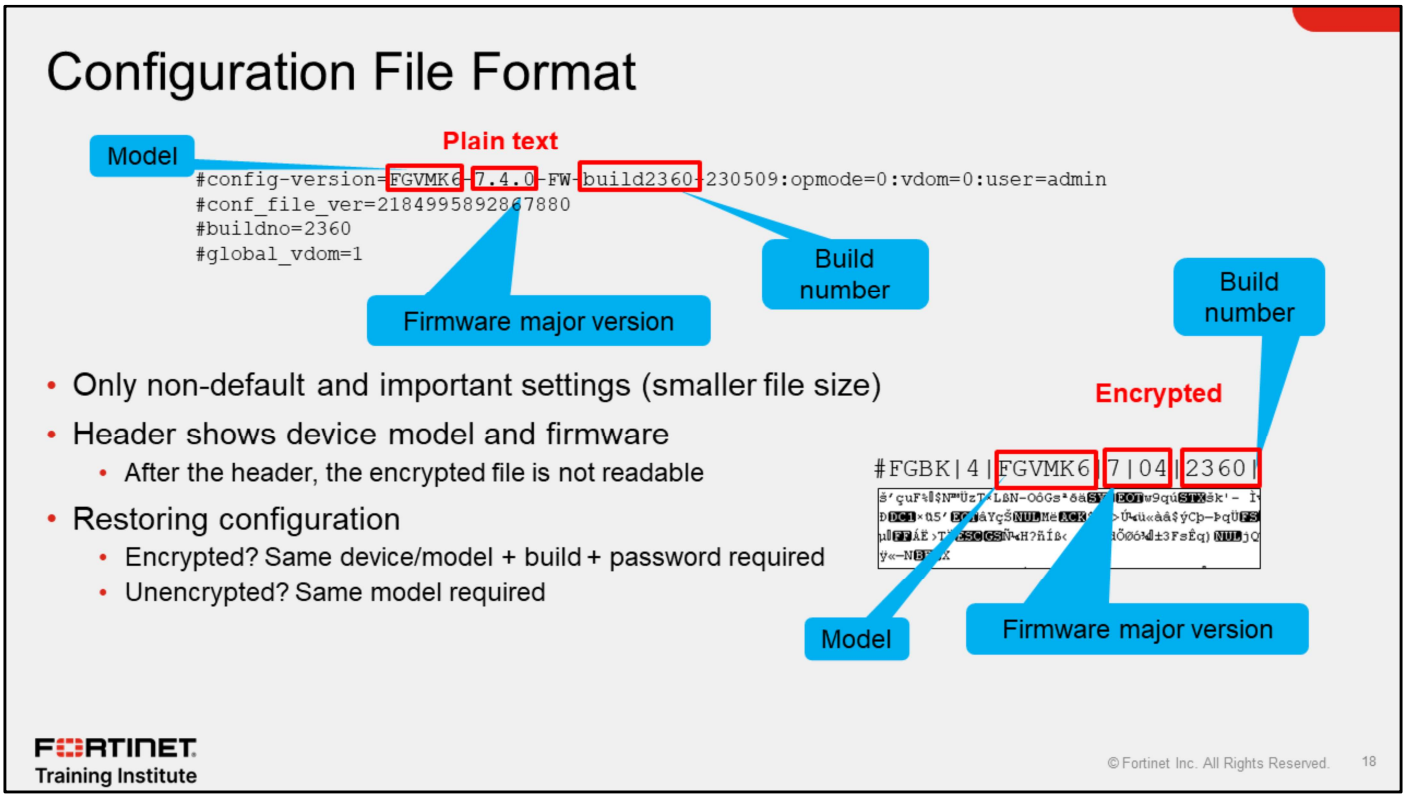

Now that FortiGate has basic network settings and administrative accounts, you will learn how to back up the configuration. In addition to selecting the destination of the backup file, you can choose to encrypt or not to encrypt the backup file. Even if you choose not to encrypt the file, which is the default, the passwords stored in the file are hashed, and, therefore, obfuscated. The passwords that are stored in the configuration file would include passwords for the administrative users and local users, and preshared keys for your IPSec VPNs. It may also include passwords for the FSSO and LDAP servers.

The other option is to encrypt the configuration file with a password. Besides securing the privacy of your configuration, it also has some effects you may not expect. After encryption, the configuration file cannot be decrypted without the password and a FortiGate of the same model and firmware. This means that if you send an encrypted configuration file to Fortinet technical support, even if you give them the password, they cannot load your configuration until they get access to the same model of FortiGate. This can cause unnecessary delays when resolving your ticket. Instead, you can enable password masking option when creating a new backup file to replace all passwords and secrets in the config file and prevent unintentional data leak when sharing the backup file with a third-party.

If you enable virtual domains (VDOMs), subdividing the resources and configuration of your FortiGate device, each VDOM administrator can back up and restore their own configurations. You don't have to back up the entire FortiGate configuration, however, it is still recommended.

Backups are needed to help speed up the return to production in the event of an unforeseen disaster that damages FortiGate. Having to recreate hundreds of policies and objects from scratch takes a significant amount of time, while loading a configuration file on a new device takes much less.

Restoring a configuration file is very similar to backing one up and restarts FortiGate.




If you open the configuration file in a text editor, you'll see that both encrypted and unencrypted configuration files contain a cleartext header that contains some basic information about the device. The example on this slide shows what information is included. To restore an encrypted configuration, you must upload it to a FortiGate device of the same model and firmware, then provide the password.

To restore an unencrypted configuration file, you are required to match only the FortiGate model. If the firmware is different, FortiGate will attempt to upgrade the configuration. This is similar to how it uses upgrade scripts on the existing configuration when upgrading firmware. However, it is still recommended to match the firmware on FortiGate to the firmware listed in the configuration file.

Usually, the configuration file contains only non-default settings, plus few default, yet crucial, settings. This minimizes the size of the backup, which could otherwise be several megabytes in size.

# Configuration File Format—YAML Format

- Support YAML and can be backedup and restored by GUI and CLI

YAML Format

```
config_system_global:
    admintimeout:480
    alias:FortiGate-100F
config_system_settings:
    default-voip-alg-mode: kernel-helper-based
    gui-dynamic-routing: enable
config_system_interface:
    - port1:
        vdom: root
        ip: "204.126.10.3 255.255.254.0"
        allowaccess: ping
        secondaryip:
            - 0:
                ip: "204.126.10.2 255.255.255.0"
                allowaccess: ping
```

Default Format

```
config system global
  set admintimeout 480
  set alias "FortiGate-100F"
end
config system settings
  set default-voip-alg-mode kernel-helper-based
  set gui-dynamic-routing enable
end
config system interface
     edit "port1"
          set vdom "root"
          set ip 204.126.10.3 255.255.254.0
          set allowaccess ping
          config secondaryip
              edit 1
                set ip 204.126.10.2 255.255.255.0
                set allowaccess ping
              end
      end
```

FORTINET Training Institute

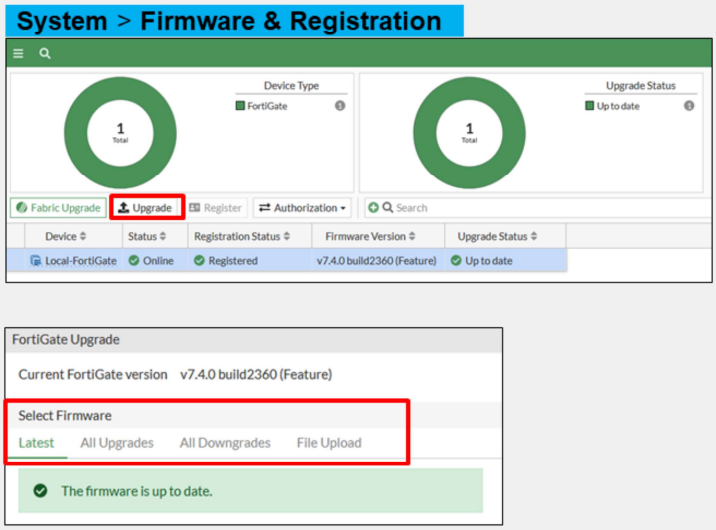
 

YAML format becomes more and more popular often use to create configuration files. FortiOS now supports YAML format, you can take a backup as well as restore YAML configuration file using GUI.

This slide shows the sample configuration to understand the difference between the default file format and YAML format.

# Upgrade Firmware

- You can view the current firmware version on the dashboard or in **System** > **Firmware & Registration** (or on the CLI: `get system status`)
- If there is an updated firmware version, you are notified
- You can update the firmware by clicking **Upgrade** and then selecting the **All Upgrades** or **File Upload** option
- Make sure you read the *Release Notes* to verify the upgrade path and other details




FORTINET Training Institute

You can view the current firmware version in multiple places on the FortiGate GUI. When you first log in to FortiGate, the landing page is the dashboard. You can see the firmware version in the **System** widget. This information is also found at **System** > **Firmware & Registration**. And, of course, you can retrieve the information on the CLI using the command `get system status`.

If a new version of the firmware is available, you are notified on the dashboard and on the **Firmware & Registration** page. The **Firmware & Registration** page allows administrators to manage the firmware running on each FortiGate, FortiAP, and FortiSwitch in the Security Fabric, and to authorize and register these Fabric devices.

You can use **Upgrade** option to upgrade firmware of the selected device. The **Fabric Upgrade** option upgrades firmware for the root FortiGate as well as Fabric devices. You can also use this option to upgrade firmware for a non-Security Fabric FortiGate with managed FortiSwitch and FortiAP devices.
The **Fabric Upgrade** option uses released firmware images from FortiGuard.

You can also use the **Register** option to register a selected device to FortiCare and an **Authorize** option to authorize a selected device for use in security fabric.

Remember to read the *Release Notes* to make sure that you understand the supported upgrade path. The *Release Notes* also provide pertinent information that may affect the upgrade.

# FortiGuard Subscription Services

- Internet connection and contract required
- Provided by FortiGuard Distribution Network (FDN)
  - Major data centers in North America, Asia, and Europe
    - Or, from FDN through your FortiManager
  - FortiGate prefers the data center in nearest time zone, but will adjust by server load
- Package updates: FortiGuard antivirus and IPS
  - `update.fortiguard.net`
  - TCP port 443 (SSL)
- Live queries: FortiGuard web filtering, DNS filtering, and antispam
  - service.fortiguard.net for proprietary protocol on UDP port 53 or 8888
  - securewf.fortiguard.net for HTTPS over port 443, 53 or, 8888
- FortiOS uses FortiGuard server for DNS request
  - By default, uses DNS over TLS (DoT) to secure dns traffic


FORTINET Training Institute

Some FortiGate services connect to other servers, such as FortiGuard, in order to work. FortiGuard Subscription Services provide FortiGate with up-to-date threat intelligence. FortiGate uses FortiGuard by:

- Periodically requesting packages that contain a new engine and signatures
- Querying the FDN on an individual URL or host name

By default, the FortiGuard server location is set to anywhere FortiGate selects a server based on server load, from any part of the world. However, you have the option to change the FortiGuard server location to USA. In this case, FortiGate selects a USA-based FortiGuard server.

Queries are real-time; that is, FortiGate asks the FDN every time it scans for spam or filtered websites. FortiGate queries, instead of downloading the database, because of the size and frequency of changes that occur to the database. Also, you can select queries to use UDP or HTTPs for transport; the protocols are not designed for fault tolerance, but for speed. So, queries require that your FortiGate device has a reliable internet connection.

Packages, like antivirus and IPS, are smaller and don't change as frequently, so they are downloaded (in many cases) only once a day. They are downloaded using TCP for reliable transport. After the database is downloaded, their associated FortiGate features continue to function, even if FortiGate does not have reliable internet connectivity. However, you should still try to avoid interruptions during downloads—if your FortiGate device must try repeatedly to download updates, it can’t detect new threats during that time.

When using FortiGuard servers for DNS, FortiOS uses DNS over TLS (DoT) by default to secure the DNS traffic. New FortiGuard DNS servers have been added as primary and secondary servers.


Now, third-party SSL certificate verification and OCSP stapling check has been implemented for all FortiGuard servers. By default, the FortiGuard access mode is *anycast* on FortiGate, to optimize the routing performance to the FortiGuard servers. The FortiGuard server has one IP address to match its domain name. FortiGate connects with a single server address, regardless of where the FortiGate device is located.

The domain name of each FortiGuard service is the common name in the certificate of that service. The certificate is signed by a third-party intermediate CA. The FortiGuard server uses the Online Certificate Status Protocol (OCSP) stapling technique, so that FortiGate can always validate the FortiGuard server certificate efficiently. FortiGate will complete the TLS handshake only with a FortiGuard server that provides a *good* OCSP status for its certificate. Any other status results in a failed SSL connection.

The FortiGuard servers query the OCSP responder of the CA every four hours and update its OCSP status. If FortiGuard is unable to reach the OCSP responder, it keeps the last known OCSP status for seven days.

FortiGate aborts the connection to the FortiGuard server if:
- The CN in the server certificate does not match the domain name resolved from the DNS.
- The OCSP status is not good.
- The issuer-CA is revoked by the root-CA.

The FortiGuard access mode *anycast* setting forces the rating process to use protocol HTTPS, and port 443.

# FortiGuard Subscription Services (Contd)

- Some of the FortiGuard domain name and their IP addresses:

| Server | Domain name and IP address |
|---|---|
| Object download | globalupdate.fortinet.net - 173.243.140.6 |
| Querying service (webfiltering, antispam) | globalguardservice.fortinet.net - 173.243.140.16 |
| FortiGate Cloud logging | globallogctrl.fortinet.net - 173.243.132.25 |
| FortiGate Cloud management | globalmgrctrl.fortinet.net - 173.243.132.26 |
| FortiGate Cloud messaging | globalmsgctrl.fortinet.net - 173.243.132.27 |
| FortiGate Cloud sandbox | globalaptctrl.fortinet.net - 184.94.112.22 |
| The productapi used by OCVPN registration and GUI icon download | globalproductapi.fortinet.net - 66.35.17.252 |

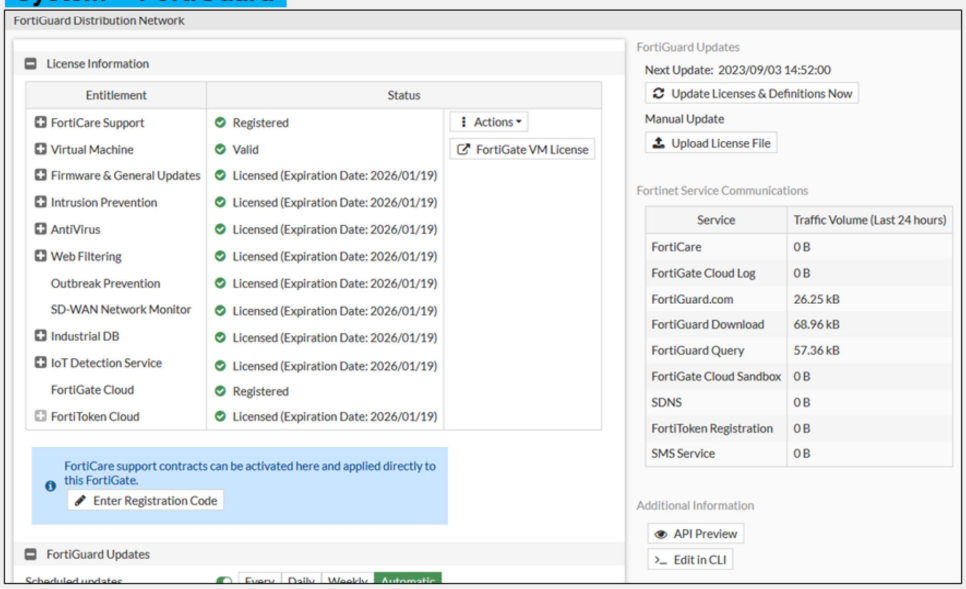
FORTINET Training Institute




The table on this slide shows a list of some of the FortiGuard servers and their domain names and IP addresses.

# FortiGuard Licenses

**System > FortiGuard**




FORTINET Training Institute

You can check the status of FortiGuard licenses and the communication to FortiGuard on the FortiGate GUI. You can also check the versions of the locally installed databases for each of the FortiGuard services.

# FortiGuard Licenses (Contd)

```
Local-FortiGate # diagnose autoupdate versions
AV Engine
---------
Version: 7.00015 signed
Contract Expiry Date: Mon Jan 19 2026
Last Updated using manual update on Thu Jul 13 02:54:00 2023
Last Update Attempt: Mon Aug 25 13:52:18 2023
Result: No Updates

Virus Definitions
---------
Version: 90.01635 signed
Contract Expiry Date: Mon Jan 19 2026
Last Updated using manual update on Mon Jul 25 13:52:18 2023
Last Update Attempt: Mon Aug 25 13:52:18 2023
Result: Updates Installed
```

FORTINET Training Institute

The command shown on this slide lists all the FortiGuard databases and engines installed. The information includes the version, contract expiration date, time it was updated, and what happened during the last update.

The list includes but is not limited to antivirus, IPS, application, mobile malware definitions, and other security services FortiGate is licensed and updated using FortiGuard services.

# Knowledge Check

1. How do you restrict logins to FortiGate from only specific IP addresses?
   - A. Change the FortiGate management interface IP address.
   - ✓ B. Configure a trusted host.

2. When restoring an encrypted system configuration file, in addition to the FortiGate model and firmware version from the time the configuration file was produced, what else must you provide?
   - ✓ A. The password to decrypt the file
   - B. The private decryption key to decrypt the file

3. To increase the chances of success, what document should you consult before upgrading or downgrading firmware?
   - A. *CLI Reference Guide*
   - ✓ B. *FortiOS Release Notes*

## Review

- ✓ Configure FortiGate on factory default settings
- ✓ Configure FortiGate as the DHCP server
- ✓ Configure and control administrator access to FortiGate
- ✓ Back up and restore system configuration files
- ✓ Upgrade FortiGate firmware
- ✓ Check and verify FortiGuard licenses

FORTINET Training Institute

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

By mastering the objectives covered in this lesson, you learned how and where FortiGate fits into your network and how to perform basic FortiGate administration.