Administration Guide

FortiZTP 25.4

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

March 5, 2025
FortiZTP 25.4 Administration Guide
73-254-1151540-20250305

TABLE OF CONTENTS

Change log

Date	Change description
2025-11-13	Initial release of 25.4.

Introduction

FortiZTP is a cloud service to manage zero touch provisioning of devices or virtual machines (VM) to cloud or on-premise management solutions from a centralized console. FortiZTP provides the following features:

- Bulk provisioning of devices and VMs to a desired cloud service or on-premise management solution
- Visibility of where devices are provisioned
- Deprovisioning devices

FortiZTP automatically loads devices that are registered to Asset Management under the same FortiCloud account and Cloud or FortiDeploy key verification. You must perform the Cloud or FortiDeploy key verification during Asset Management registration. If Asset Management does not prompt for the verification step, the Cloud key or FortiDeploy key is invalid in FortiCare. Contact Fortinet Support to inquire on the key status. The centralized FortiZTP service integrates with various FortiCloud services to view the provisioning status and perform actions to provision, deprovision, hide, or change provisioning targets.

FortiZTP supports the following devices and provisioning targets:

Device	Provisioning target
• FortiGate • FortiGate-VM • FortiWiFi	• FortiGate Cloud • FortiManager • FortiManager Cloud
FortiAP	• FortiGate • FortiEdge Cloud
FortiSwitch	FortiEdge Cloud
FortiExtender	• FortiExtender Cloud • FortiSASE

You must register or import devices to the Asset Management portal in the same FortiCloud account.

Functions

Function	Description
Provisioning status summary	Displays the number of provisioned and unprovisioned devices for supported products.
Provision devices (zero touch)	Provision product to the supported target on-premise or cloud service.
Deprovision devices	Deprovision products from the cloud service.
Hide devices	Hide unprovisioned products from the list if they are managed locally.

Function	Description

Regions	• Global (North America)
	• Europe (EU)
	• Japan (APAC)
	FortiZTP supports FortiGate Cloud, FortiEdge Cloud, and FortiManager Cloud. For information on region support for these products, see the following:
	• **FortiGate Cloud**: see Functions.
	• **FortiEdge Cloud**: includes the Global, Europe, and Japan regions:
	  • The data center in Canada serves the GL and JP domains.
	  • The data center located in Germany serves the EU domain.
	• **FortiManager Cloud**: when logged in to the FortiManager Cloud instance, see the region list from the dropdown list in the top right corner. See Deploying a FortiManager Cloud instance.
	• FortiSASE
	• FortiExtender Cloud

Languages	English

Requirements

The following items are required to use FortiZTP:

Requirement	Description
FortiCloud account	Create a FortiCloud account if you do not have one. Using FortiZTP requires a FortiCloud account. You must register or import devices to the Asset Management portal in the same FortiCloud account for them to be available for provisioning in FortiZTP.
Cloud service licensing	You must ensure that you have the license for the cloud services that you are using as provisioning targets, such as FortiGate Cloud, FortiEdge Cloud, or FortiManager Cloud. Refer to the specific cloud service documentation in the Fortinet Document Library for detailed licensing information.
FortiGate-VM licensing	To provision a FortiGate-VM using the FortiZTP portal, it must have a valid license applied.

Requirement	Description

	FortiZTP requires a FortiGate model that supports the zero-touch provisioning (autojoin) feature. FortiGate/FortiWiFi/POE desktop and 1U models up to 100F support the zero touch provisioning feature. For other models, FortiZTP supports one-touch provisioning. For these models, you must configure DHCP on the port of choice. The FortiZTP server can push FortiManager settings to devices that fulfill this requirement. Having trained personnel handle larger deployments is recommended. FortiZTP is available for devices running FortiOS 5.2.2 and later.
	A FG-VM01 or FG-VM01V license is recommended, as the autojoin feature is enabled by default.
	
	To enable autojoining FortiGate Cloud:
	
	From FortiOS 5.2.3 and later, the `auto-join-forticloud` option is enabled by default. You must enable it for FortiZTP to function correctly. You can ensure that the option is enabled by running the following commands:
	
	`config system fortiguard`
	`  set auto-join-forticloud enable`
	`end`
	
	You must also set:
	
	`config system central-management`
	`  set type fortiguard`
	`end`
	
	After changing the settings, restart the device and ensure that the device is sending traffic to FortiGate Cloud to verify that you have configured it correctly.
	For a non-U.S. government FortiGate-VM, you must unset the FortiGuard location:
	
	`config system fortiguard`
	`  unset update-server-location`
	`end`

Browsers	• Microsoft Edge 41 and later versions • Microsoft Internet Explorer 11 and later versions • Mozilla Firefox 59 and later versions • Google Chrome 65 and later versions
FortiGate certificate	FortiGate devices must possess a valid certificate with serial number as CN signed by Fortinet to ensure proper functionality of FortiZTP.

Getting started with the FortiZTP portal

To access the FortiZTP portal, log in with your FortiCloud credentials.

FortiZTP provides region-specific portals. Each regional portal retains the data within the specified region. You can switch between regions from the top banner.

The top of the GUI displays how many devices are unprovisioned and hidden. It also displays how many devices are in the following states:

State	Description
Incomplete	Provisioning did not complete within 30 minutes due to one of the following reasons: • Device is offline. • Device cannot access the Internet. • Device cannot connect to destination service. • Device does not have required license.
Unprovisioned	Registered to Asset Management with same FortiCloud account used to access FortiZTP and available for provisioning to a Fortinet service.
Provisioned	Provisioned to a Fortinet service.
Hidden	Hidden from view in FortiZTP.

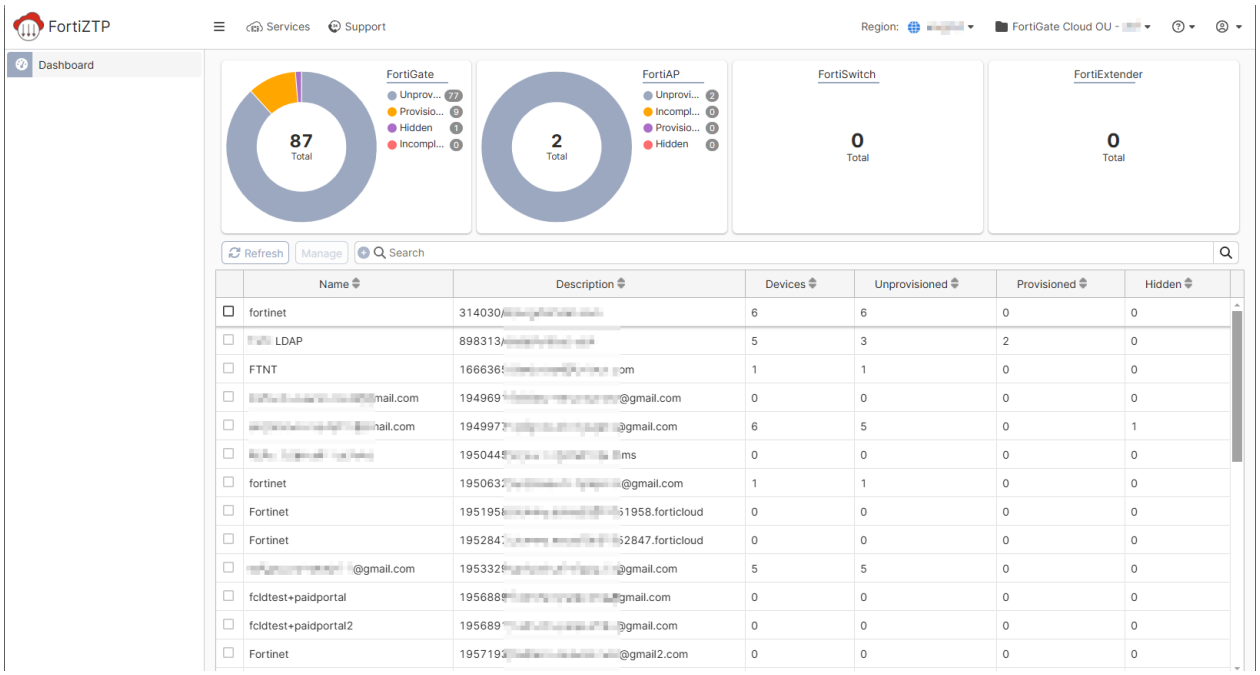
You can filter which devices display in the list. The list displays the following information for each device:

- Device type
- Model
- Serial number
- Name
- Provisioning status
- Provisioning target
- Provisioning start date
- Provisioning completion date

You can also search for the desired device.

If the device needs additional setup after provisioning, the *Provisioning Status* indicates that the device is *(Not Setup)*. You can click *(Not Setup)* to go to the respective service to complete the setup.

If you are logged in to an organizational unit (OU), you can use the central pane to navigate to an account. The pane also displays the accounts in this OU and the number of devices in each account.



If you are logged in as an Identity & Access Management (IAM) user with read-only permissions, you can view the portal, but cannot provision or update any FortiZTP settings. Options are grayed out. You also only see devices that are registered in FortiCloud Asset Management, while non-IAM users can see FortiCloud-registered devices and FortiGate Cloud local inventory devices.

FortiZTP supports role-based access control using FortiCloud permission profiles. See Creating a permission profile.

User permissions

IAM users

FortiCloud Identity & Access Management (IAM) supports creating IAM users and allowing access to FortiZTP using the admin or read-only access role. The admin role allows the same permissions as a full admin email account user. The read-only role allows read-only access to all FortiZTP pages.

FortiZTP supports specifying IAM user folder permissions. For example, if a local IAM user has been specified with permissions to a folder, FortiZTP only shows devices within that folder.

See Adding IAM users for details on configuring IAM users.

FortiCloud organizations

FortiZTP supports organizational unit (OU) account selection and switching. OU support is available to external customers with FortiCloud Premium license accounts. See Organization Portal for details on creating an OU.

To create an IAM user with OU scope, see User permissions.

OU

FortiZTP supports organizational unit (OU) account selection and switching. OU support is available to external customers with FortiCloud Premium license accounts. See Organization Portal for details on creating an OU.

FortiZTP supports logging in via an external identity provider with OUs.

Logging in to FortiZTP and accessing OU accounts

To log in to FortiZTP and access OU accounts:

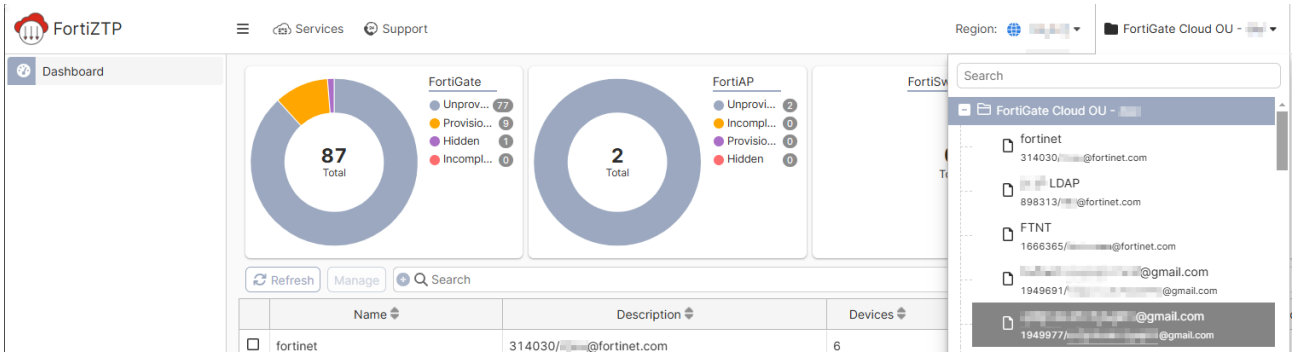
1. In the FortiZTP landing page, select *IAM Login*.
2. Enter your account ID/alias, username, and password, then click *Log In*.
3. Select the desired account or OU to log into.

Returning to the OU tree

To return to the OU tree, select the dropdown list in the upper right corner of the GUI, which displays the OU that you are currently logged in to. Select the desired OU or account from the dropdown list. You can also select your username in the upper right corner of the GUI, then select *Switch Accounts*.

Switching OUs or accounts

To switch the OU or account that you are using to access FortiZTP, select your account in the upper right corner of the GUI, then select the desired OU or account from the dropdown list.



Provisioning devices

FortiZTP automatically loads devices that are registered to Asset Management with same FortiCloud account. You can view these devices in *Assets* in FortiZTP and provision them to various Fortinet services as desired.

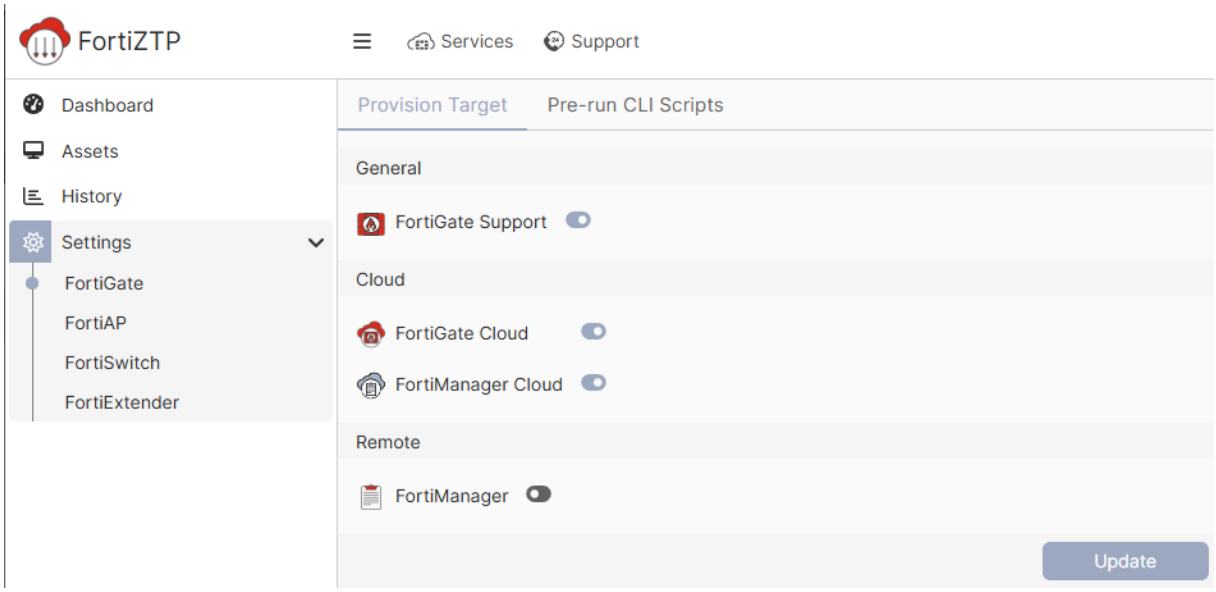
FortiZTP automatically deletes provisioning history older than one year.

Provisioning a FortiGate

The following describes provisioning a FortiGate. After FortiZTP provisions devices, they appear as *Provisioned*.

To provision a FortiGate to FortiGate Cloud:

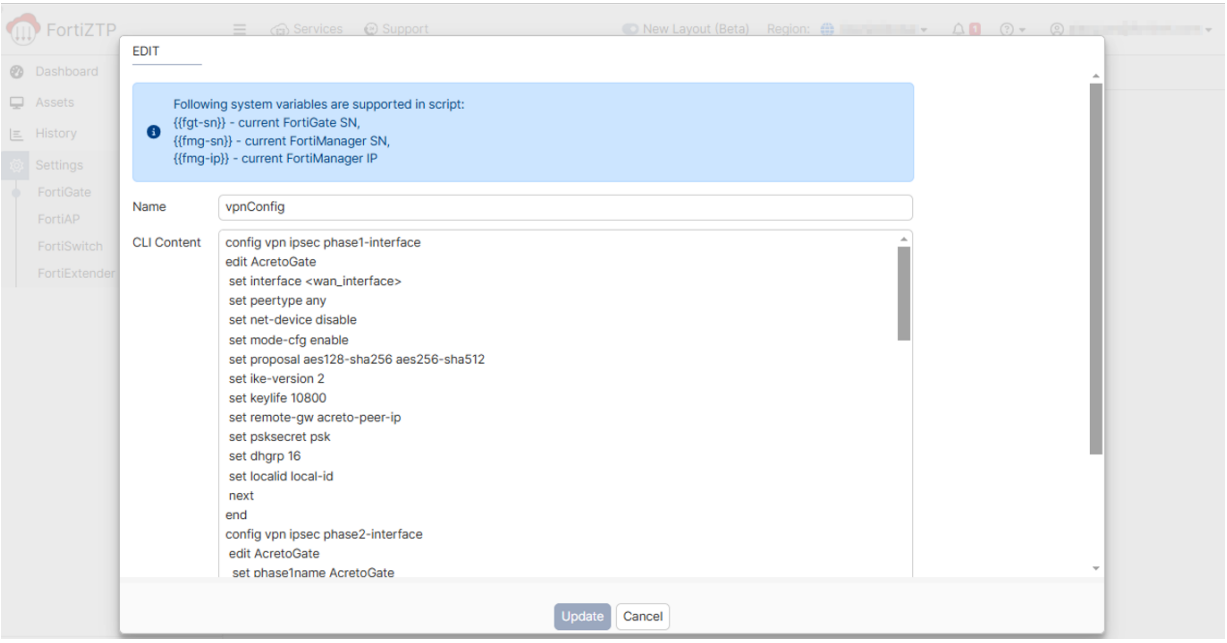
1. Go to *Settings* > *FortiGate*.
2. Ensure that *FortiGate Cloud* is enabled.
3. Click *Update*.



4. In *Assets*, select the checkboxes for the desired FortiGates, then click *Provision*.
5. Under *Target Location* in the *Provision* dialog, select the desired target location for the FortiGate(s). Only options that you have configured in *Settings* appear in this dialog.
6. From the *Please select a firmware profile* dropdown list, select the desired firmware profile. See Firmware Profile.
7. Click *Provision*.

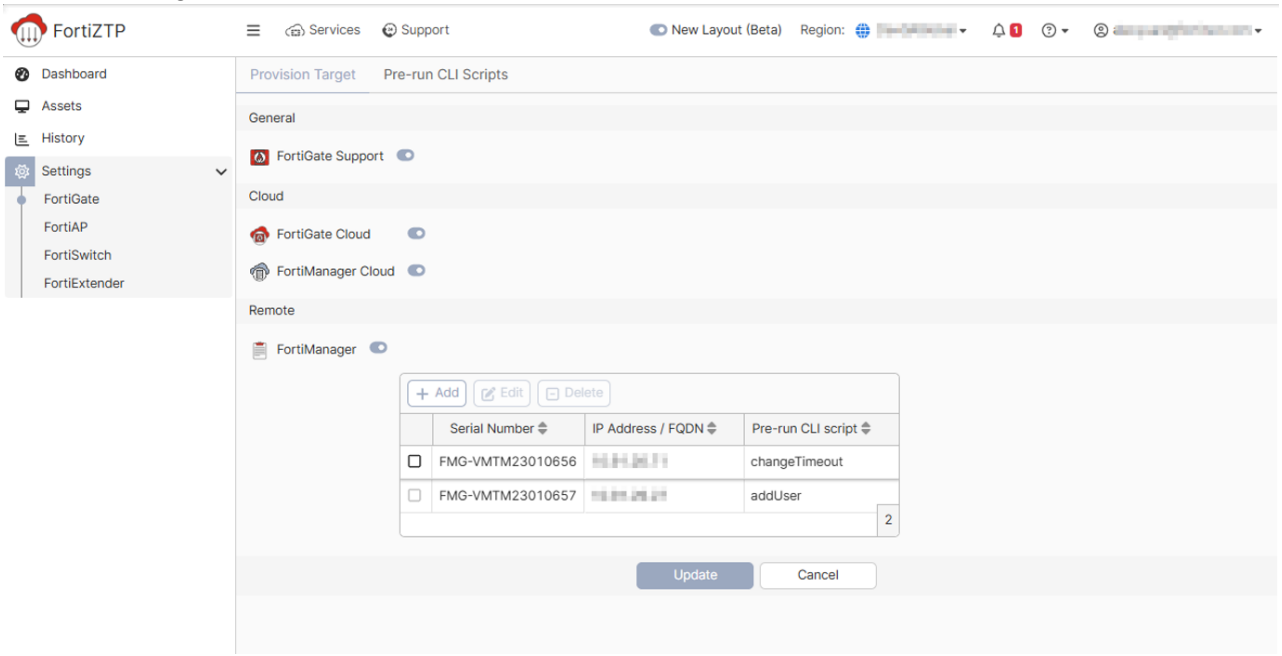
To provision a FortiGate to FortiManager:

1. Go to *Settings* > *FortiGate*.
2. Optionally, configure a pre-run CLI template. Pre-run CLI scripts will be pushed to FortiGate before it connects with FortiManager.
   a. Select the *Pre-run CLI Scripts* tab.
   b. Click *Add* to create a new script.
   c. Enter a *Name* for the script, and provide the *CLI Content*.

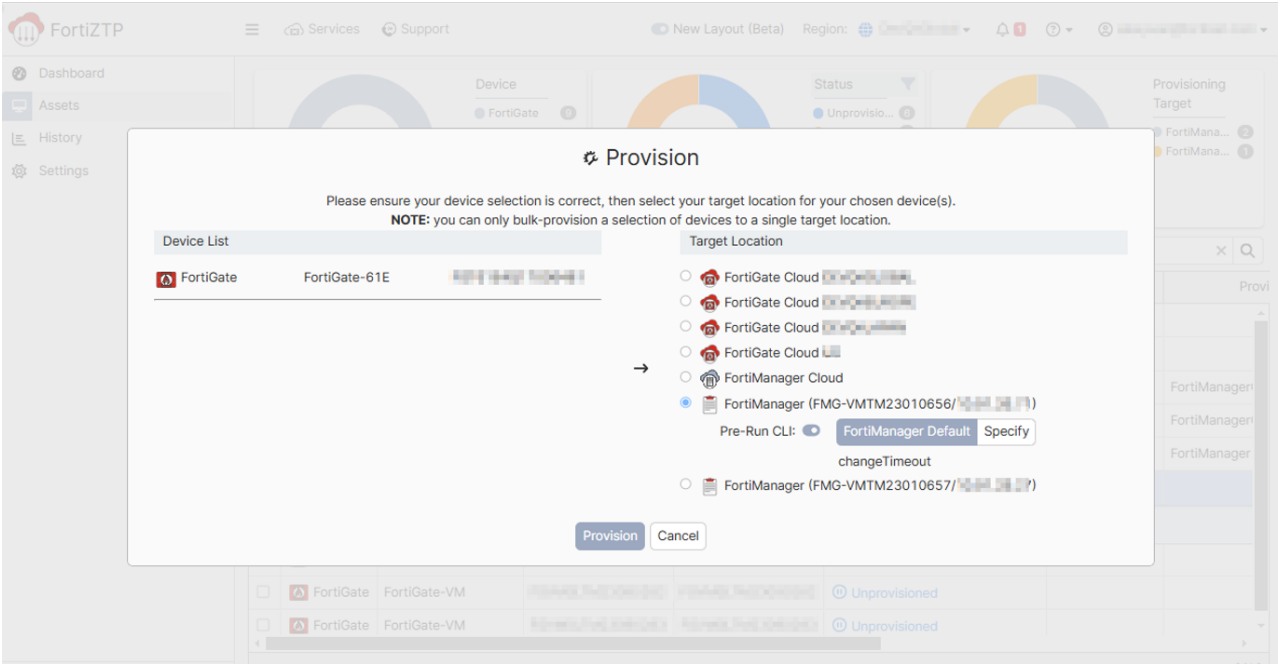


   d. Click *Update* to save the script.
   This script can now be specified as the default pre-run CLI script for a target FortiManager, or selected during the provisioning process. You can edit or delete an existing script by clicking the *Edit* or *Delete* options.
3. Select the *Provision Target* tab.
4. Enable *FortiManager*.
5. Click *Add*.
6. In the *Serial Number* and *IP Address/FQDN* fields, enter the FortiManager details. If you are provisioning FortiGate to FortiManagers in a high availability (HA) pair, enter both nodes' serial numbers separated by a comma in the *Serial Number* field and one IP address (the virtual IP address or hostname) in the *IP Address/FQDN* field. FortiZTP supports provisioning for FortiManager 7.2 HA.

7. Optionally, enable *Pre-run CLI Script* to choose a previously configured pre-run CLI script as the default for this FortiManager.



8. By default, FortiGate Cloud is enabled. If desired, you can disable FortiGate Cloud.
9. Click *Update*.
10. In *Assets*, select the checkboxes for the desired FortiGates, then click the *Provision* button.
11. Under *Target Location* in the *Provision* dialog, select the desired target location for the FortiGate(s). Only options that you have configured in *Settings* appear in this dialog.
12. Optionally, enable *Pre-Run CLI* to provision the FortiGate with a pre-run CLI script. You can choose the *FortiManager Default* script or select *Specify* to choose another script configured under the *Pre-run CLI Scripts* tab.



13. Click *Provision*.

To provision a FortiGate to FortiManager Cloud:

1. Go to *Settings* > *FortiGate*.
2. Enable *FortiManager Cloud*.
3. In *Assets*, select the checkboxes for the desired FortiGates, then click the *Provision* button.
4. Under *Target Location* in the *Provision* dialog, select the desired target location for the FortiGate(s). Only options that you have configured in *Settings* appear in this dialog.
5. Click *Provision*.

See Using FortiZTP with FortiManager Cloud for FortiManager Cloud-side instructions.

In previous versions, provisioning a device to FortiManager Cloud using FortiZTP automatically created a model device in FortiManager Cloud. This no longer occurs. You can manually create a model device or perform the provisioning without a model device, then authorize it in the unregistered list in FortiManager Cloud. Performing preconfiguration requires creating a model device manually in FortiManager Cloud before provisioning.

Troubleshooting provisioning FortiGate to FortiManager Cloud

Issue	Possible cause	How to debug/resolve
FortiManager Cloud (FMGC) grayed out on FortiZTP portal	FMGC instance not ready	Login to FMGC to check status
	FortiZTP connection to FMGC network issue	Contact CS
Provision failure by public API	FMGC instance not ready	Login to FortiManager Cloud to check status
	FortiZTP connection to FMGC network issue	Contact CS
Incomplete – Provision too log	FortiGate unable to connect to internet	Check that FortiGate has an internet connection `execute ping 8.8.8.8`

	FortiGate unable to connect to FortiZTP	`exec ping logctrl1.fortinet.com`
		`exec telnet <IP resolved from last step> 443`
		`exec ping globallogctrl.fortinet.net`
		`exec telnet <IP resolved from last step> 443`
		`exec ping mgrctrl1.fortinet.com`
		`exec telnet <IP resolved from last step> 443`
		`exec fortiguard-log domain`

Issue	Possible cause	How to debug/resolve
		exec ping fortideploy-gl.fortigate.forticloud.com exec telnet fortideploy-gl.fortigate.forticloud.com 541 diag debug app forticldd -1 diag debug enable exec fortiguard-log login <email> <password> <domain> diag fdsm log-controller-update diag fdsm contract-controller-update
	FortiGate central management not set a FortiGuard	Factory reset for FortiGate, or config system central-management set type fortiguard end
	FortiGate does not have valid FMGC license	Apply valid FMGC contract for FortiGate
	FortiZTP unable to get provision status from FMGC	CLI script pushed to FortiGate but still show provision too long – contact CS

Provisioning a FortiAP

The following describes provisioning a FortiAP.

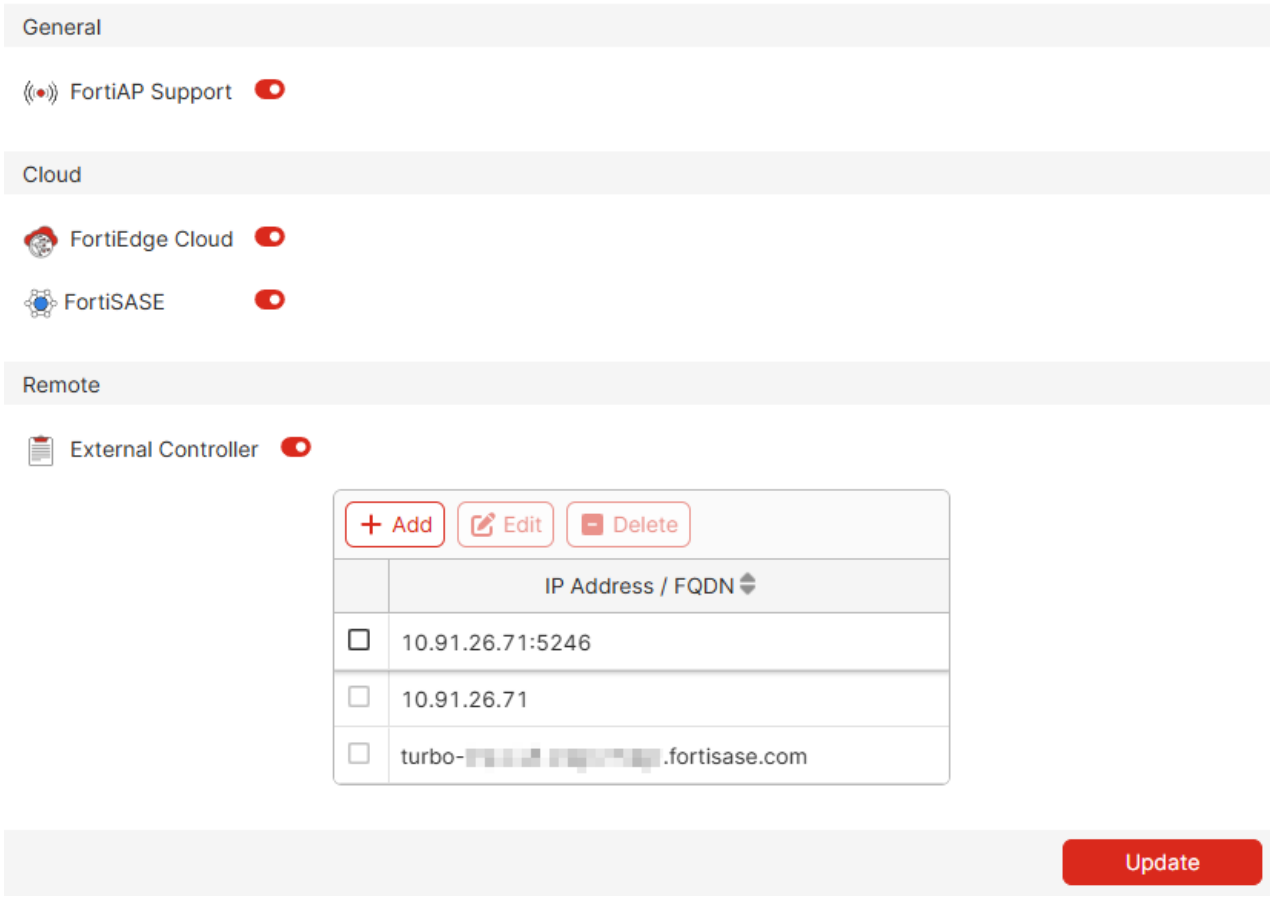
To provision a FortiAP to FortiGate:

1. Go to *Settings* > *FortiAP*.
2. Enable *External Controller*.
3. Click *Add*.
4. In the *IP Address / FQDN* field, enter the desired FortiGate IP address or FQDN.
5. Click *Add*.
6. Click *Update*.
7. In *Assets*, select the checkboxes for the desired FortiAPs, then click the *Provision* button.
8. Under *Target Location* in the *Provision* dialog, select the desired target location for the FortiAP(s). Only options that you have configured in *Settings* appear in this dialog.
9. Click *Provision*.

To provision a FortiAP to FortiEdge Cloud:

1. Go to *Settings* > *FortiAP*.
2. Ensure that *FortiEdge Cloud* is enabled.

3. Click *Update*.

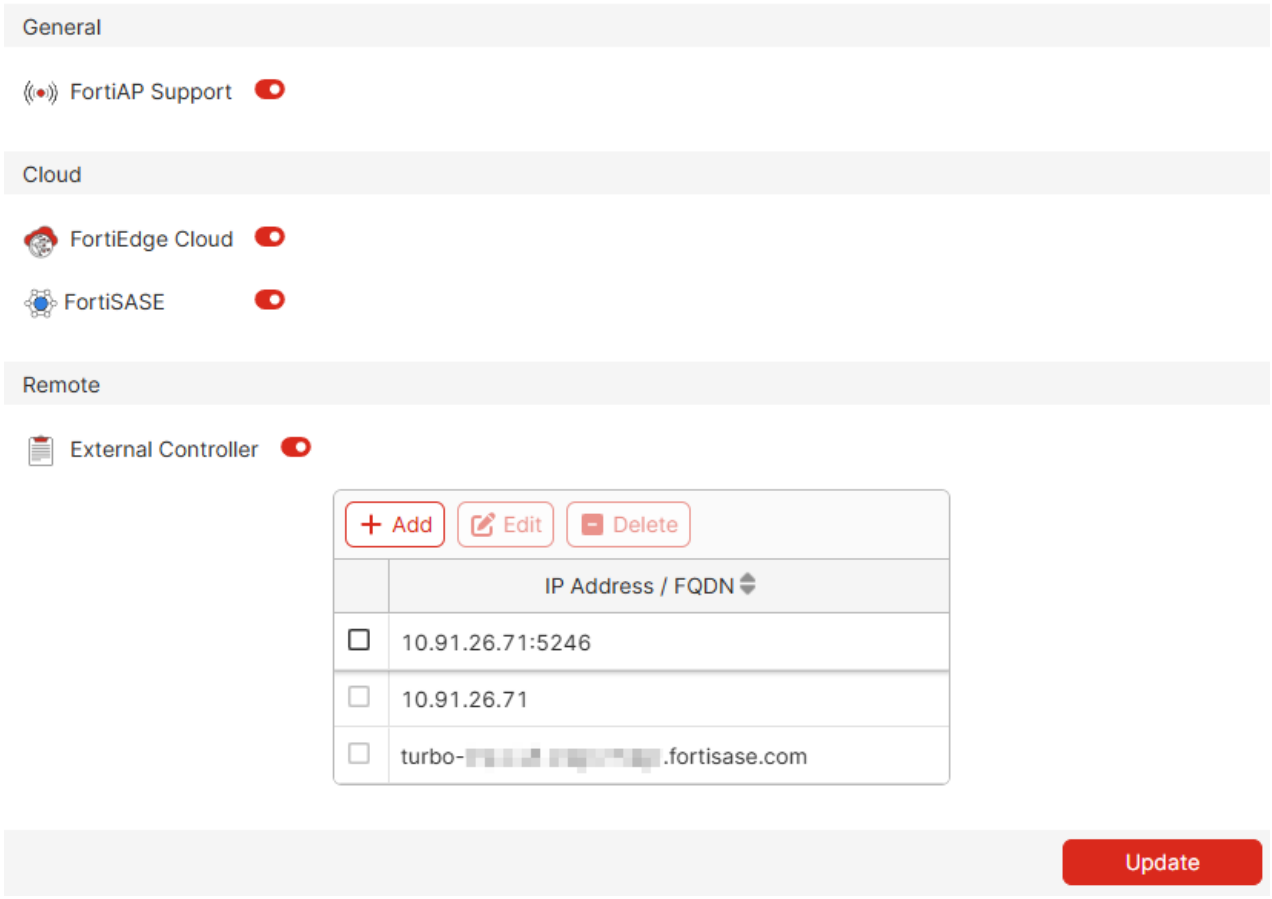


4. In *Assets*, select the checkboxes for the desired FortiAPs, then click the *Provision* button.
5. Under *Target Location* in the *Provision* dialog, select the desired target location for the FortiAP(s). Only options that you have configured in *Settings* appear in this dialog.
6. Click *Provision*.

To provision a FortiAP to FortiSASE:

1. Go to *Settings* > *FortiAP*.
2. Ensure that *FortiSASE* is enabled.

3. Click *Update*.



4. In *Assets*, select the checkboxes for the desired FortiAPs, then click the *Provision* button.
5. Under *Target Location* in the *Provision* dialog, select the desired target location for the FortiAP(s). Only options that you have configured in *Settings* appear in this dialog.
6. Click *Provision*.

Provisioning a FortiSwitch

The following describes provisioning a FortiSwitch.

To provision a FortiSwitch to FortiEdge Cloud:

1. Go to *Settings* > *FortiSwitch*.
2. Ensure that *FortiEdge Cloud* is enabled.
3. Click *Update*.
4. In *Assets*, select the checkboxes for the desired FortiSwitches, then click the *Provision* button.
5. Under *Target Location* in the *Provision* dialog, select the desired target location for the FortiSwitch(es). Only options that you have configured in *Settings* appear in this dialog.

6. Click *Provision*.

Provisioning a FortiExtender

The following describes provisioning a FortiExtender. FortiZTP only supports provisioning a FortiExtender to FortiSASE for FortiExtenders running FortiOS 7.2.3 or a later version.

You must set `discovery-type` to `cloud` on the FortiExtender before you can provision it to FortiExtender Cloud or FortiSASE. Use the following commands:

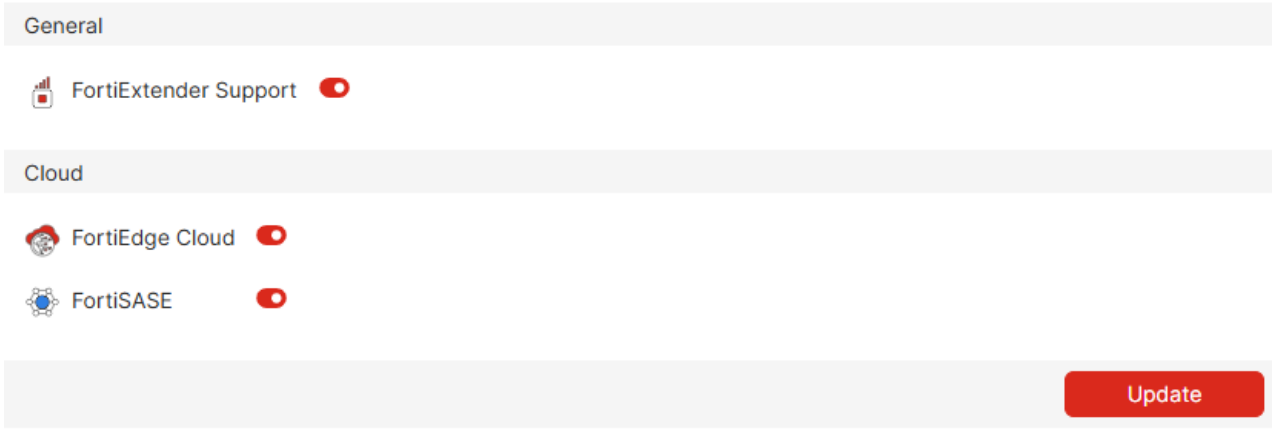
```
config management
   set discovery-type cloud
end
```

To provision a FortiExtender to FortiExtender Cloud:

1. Go to *Settings* > *FortiExtender*.
2. Ensure that *FortiExtender Cloud* is enabled.
3. Click *Update*.
4. In *Assets*, select the checkboxes for the desired FortiExtenders, then click the *Provision* button.
5. Under *Target Location* in the *Provision* dialog, select the desired target location for the FortiExtender(s). Only options that you have configured in *Settings* appear in this dialog.
6. Click *Provision*.

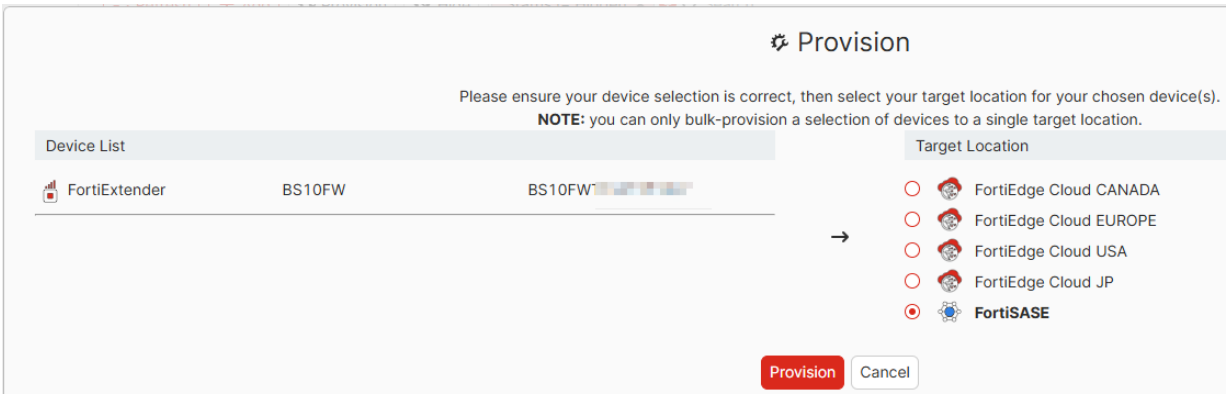
To provision a FortiExtender or FortiBranchSASE to FortiSASE:

1. Go to *Settings* > *FortiExtender*.
2. Ensure that *FortiSASE* is enabled.
3. Click *Update*.



4. In *Assets*, select the checkboxes for the desired FortiExtender and/or FortiBranchSASE devices, then click the *Provision* button.
5. Under *Target Location* in the *Provision* dialog, select the desired target location for the FortiExtender and/or FortiBranchSASE devices. Only options that you have configured in *Settings* appear in this dialog.

6. Click *Provision*.



Deprovisioning a device

To deprovision a device:

1. Go to the *Assets*.
2. Do one of the following:
   - To deprovision a single device, click the device, then click *Deprovision* for the desired device. The *Deprovision* button appears below the entry for the device.
   - To deprovision multiple devices, select the checkboxes for the desired devices. Click the *Deprovision* button.
3. In the dialog, click *Deprovision*.

Deprovisioned devices now display as *Unprovisioned*. You can reprovision them as desired.

After deprovisioning a FortiGate from FortiManager or FortiManager Cloud, you must do one of the following to ensure that you can successfully reprovision the FortiGates:

- Factory reset the FortiGate.
- Execute the following CLI commands on the FortiGate, then reboot it:

```
config system central-management
   set type fortiguard
end
```

Self-diagnosis

Provisioning FortiGate to FortiGate Cloud self-diagnosis

The following provides self-diagnosis instructions for a scenario where you have provisioned a FortiGate to FortiGate Cloud, FortiZTP shows that the provisioning succeeded, but the FortiGate displays that FortiGate Cloud is not activated.

To self-diagnose this scenario:

1. Check the Anycast status:

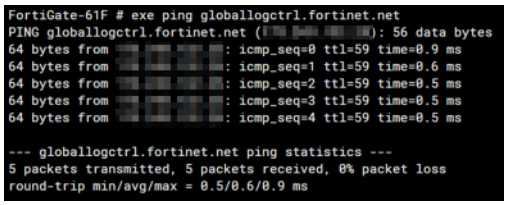
   ```
   config system fortiguard
   show
   end
   ```

   The following shows example output for this command:

   ```
   config system fortiguard
      set fortiguard-anycast disable
   end
   ```

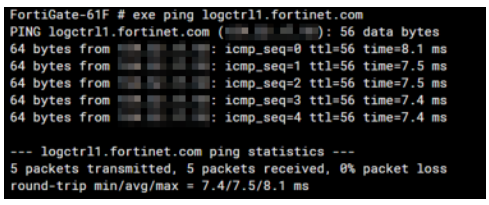
2. Check the network connection. Do one of the following:
   - If Anycast is enabled, enter the following:

     ```
     execute ping globallogctrl.fortinet.net
     ```

   - If Anycast is disabled, enter the following:

     ```
     execute ping logctrl1.fortinet.com
     ```

   If ping succeeds, enter the following:

```
execute telnet <IP address resolved above> 443
```

The following shows example output for this command:

```
Trying ...
Connected to...
```

If telnet succeeds, go to the next step.

3. Attempt connection to FortiGate Cloud:

```
execute fortiguard-log domain
```

```
FortiGate-61F # exe fortiguard-log domain
EUROPE
US
GLOBAL
```

```
diagnose debug application forticldd -1
diagnose debug enable
execute fortiguard-log join
```

```
FortiGate-61F # exe fortiguard-log join
Request sent.
```

```
diagnose fdsm log-controller-update
```

```
FortiGate-61F # diag fdsm log-controller-update
Protocol=2.0|Response=202|Firmware=FAZ-4K-FW-2.50-100|SerialNumber=FAMS000000000000|Persistent=false|ResponseItem=HomeServer:[redacted]*AlterServer:[redacted]
[redacted]*APTServer:[redacted]*APTAlterServer:[redacted]*AccountType:regular*Contract:20241029*ContractType:Purchased*NextRequest:86400*Disk:500000000*Used:0.0*Volume:1000000*Archive:True*Domain:GLOBAL

Result=Success
```

```
diagnose fdsm contract-controller-update
```

```
FortiGate-61F # di fdsm contract-controller-update
Protocol=2.0|Response=202|Firmware=FAZ-4K-FW-2.50-100|SerialNumber=FAMS000000000000|Persistent=false|ResponseItem=HomeServer:[redacted]*AlterServer:[redacted]
[redacted]*AccountType:regular*Contract:20241029*NextRequest:86400*UploadConfig:False*ManagementMode:Local*ManagementID:[redacted]

Result=Success
```

Provisioning FortiGate to FortiManager self-diagnosis

The following provides self-diagnosis instructions for a scenario where you have provisioned a FortiGate to FortiManager, FortiZTP shows that the provisioning succeeded, but the FortiGate does not appear on FortiManager.

To self-diagnose this scenario:

1. In the FortiOS CLI, check that the central management type is set to FortiGuard:

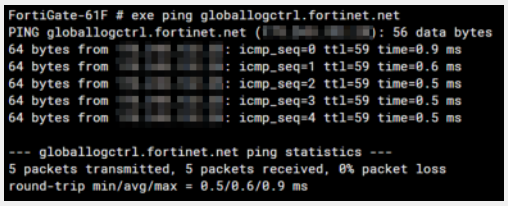
```
config system central-management
show
end
```

2. Check the Anycast status:

```
config system fortiguard
show
end
```

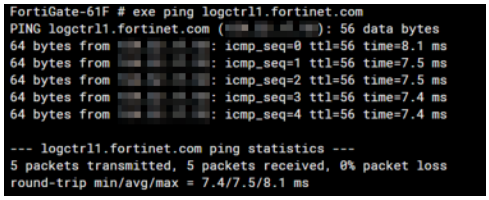
3. Check the network connection. Do one of the following:
   a. If Anycast is enabled, enter the following:

```
execute ping globallogctrl.fortinet.net
```



   b. If Anycast is disabled, enter the following:

```
execute ping logctrl1.fortinet.com
```



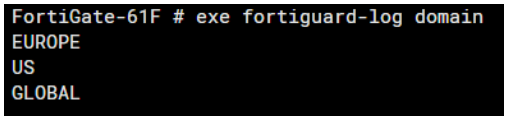
   If ping succeeds, enter the following:

```
telnet <IP address resolved above> 443
```

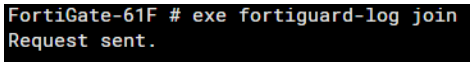
   If telnet succeeds, go to the next step.

4. Attempt connection to FortiGate Cloud:

```
execute fortiguard-log domain
```




```
diagnose debug application forticldd -1
diagnose debug enable
execute fortiguard-log join
```




```
diagnose fdsm contract-controller-update
```

```
FortiGate-61F # di fdsm contract-controller-update
Protocol=2.0|Response=202|Firmware=FAZ-4K-FW-2.50-100|SerialNumber=FAMS000000000000|Persistent=false|ResponseItem=HomeServer:[redacted]*AlterServer:[redacted]
[redacted]*AccountType:regular*Contract:20241029*NextRequest:86400*UploadConfig:False*ManagementMode:Local*ManagementID:[redacted]

Result=Success
```

Ensure that 'HomeServer' returned is a valid FortiDeploy server IP address. If it is 192.168.0.1, that means the device is not properly connected to FortiGate Cloud, and you must rerun the join request or run a login request in CLI:

```
execute fortiguard-log login <email> <password>
```

5. Check the network connection to the FortiDeploy server:

```
execute telnet <FortiDeploy server IP address> 541
```

```
FortiGate-61F # exe telnet [redacted] 541
Trying [redacted]...
Connected to [redacted].
```

6. Ensure that the management tunnel is established:

```
diagnose debug application fgfmd -1
diagnose debug enable
fnsysctl killall fgfmd
```

7. Check that FortiManager Cloud pushed a setting script to FortiGate. After FortiManager Cloud pushes the script to FortiGate, central management should be set to FortiManager:

```
config system central-management
show
end
```

```
FortiGate-61F # config system central-management

FortiGate-61F (central-management) # show
config system central-management
    set type fortimanager
end

FortiGate-61F (central-management) # end
```

8. Check the network connection to FortiManager:

```
execute ping <FortiManager IP address>
```

If the results of all steps are as expected but the FortiGate still does not show up on FortiManager, contact the FortiManager team for further investigation.

Provisioning FortiGate to FortiManager Cloud self-diagnosis

The following provides self-diagnosis instructions for a scenario where you have provisioned a FortiGate to FortiManager Cloud, FortiZTP shows that the provisioning succeeded, but the FortiGate does not appear on FortiManager Cloud.

To self-diagnose this scenario:

1. In the FortiOS CLI, check that the central management type is set to FortiGuard:

```
config system central-management
show
end
```

```
FortiGate-61F # config system central-management

FortiGate-61F (central-management) # show
config system central-management
    set type fortiguard
end

FortiGate-61F (central-management) # end
```

2. Check the Anycast status:

```
config system fortiguard
show
end
```

3. Check the network connection. Do one of the following:
   - If Anycast is enabled, enter the following:

```
execute ping globallogctrl.fortinet.net
```

```
FortiGate-61F # exe ping globallogctrl.fortinet.net
PING globallogctrl.fortinet.net (                ): 56 data bytes
64 bytes from                : icmp_seq=0 ttl=59 time=0.9 ms
64 bytes from                : icmp_seq=1 ttl=59 time=0.6 ms
64 bytes from                : icmp_seq=2 ttl=59 time=0.5 ms
64 bytes from                : icmp_seq=3 ttl=59 time=0.5 ms
64 bytes from                : icmp_seq=4 ttl=59 time=0.5 ms

--- globallogctrl.fortinet.net ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.5/0.6/0.9 ms
```

   - If Anycast is disabled, enter the following:

```
execute ping logctrl1.fortinet.com
```

```
FortiGate-61F # exe ping logctrl1.fortinet.com
PING logctrl1.fortinet.com (                ): 56 data bytes
64 bytes from                : icmp_seq=0 ttl=56 time=8.1 ms
64 bytes from                : icmp_seq=1 ttl=56 time=7.5 ms
64 bytes from                : icmp_seq=2 ttl=56 time=7.5 ms
64 bytes from                : icmp_seq=3 ttl=56 time=7.4 ms
64 bytes from                : icmp_seq=4 ttl=56 time=7.4 ms

--- logctrl1.fortinet.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 7.4/7.5/8.1 ms
```

   If ping succeeds, enter the following:

```
telnet <IP address resolved above> 443
```

```
FortiGate-61F # exe telnet                443
Trying                ...
Connected to                .
```

   If telnet succeeds, go to the next step.

4. Attempt connection to FortiGate Cloud:

```
execute fortiguard-log domain
```

```
FortiGate-61F # exe fortiguard-log domain
EUROPE
US
GLOBAL
```

```
diagnose debug application forticldd -1
diagnose debug enable
execute fortiguard-log join
```

```
FortiGate-61F # exe fortiguard-log join
Request sent.
```

```
diagnose fdsm contract-controller-update
```

```
FortiGate-61F # di fdsm contract-controller-update
Protocol=2.0|Response=202|Firmware=FAZ-4K-FW-2.50-100|SerialNumber=FAMS000000000000|Persistent=false|ResponseItem=HomeServer:[redacted]*AlterServer:[redacted]
[redacted]*AccountType:regular*Contract:20241029*NextRequest:86400*UploadConfig:False*ManagementMode:Local*ManagementID:[redacted]

Result=Success
```

Ensure that 'HomeServer' returned is a valid FortiDeploy server IP address. If it is 192.168.0.1, that means the device is not properly connected to FortiGate Cloud and you must rerun the join request or run a login request in CLI:

```
execute fortiguard-log login <email> <password>
```

5. Check the network connection to the FortiDeploy server:

```
execute telnet <FortiDeploy server IP address> 541
```

```
FortiGate-61F # exe telnet [redacted] 541
Trying [redacted]...
Connected to [redacted].
```

6. Ensure that the management tunnel is established:

```
diagnose debug application fgfmd -1
diagnose debug enable
fnsysctl killall fgfmd
```

7. Check that FortiManager Cloud pushed a setting script to FortiGate. After FortiManager Cloud pushes the script to FortiGate, central management should be set to FortiManager:

```
config system central-management
```

```
show
```

```
end
```

```
FortiGate-61F # config system central-management

FortiGate-61F (central-management) # show
config system central-management
    set type fortimanager
end

FortiGate-61F (central-management) # end
```

8. Check the network connection to FortiManager Cloud:

```
execute ping fortimanager.forticloud.com
```

If the results of all steps are as expected but the FortiGate still does not show up on FortiManager Cloud, contact the FortiManager Cloud team for further investigation.

Frequently asked questions

Question	Answer
How do I access the FortiZTP portal?	You can access the FortiZTP portal via https://fortiztp.forticloud.com. You can use your FortiCloud account credentials to log in.
Why is the account I would like to access not listed after login?	Ensure that your login email has full administrator rights over all of that account's cloud service regions.
How do I find the device I want to provision?	The FortiZTP portal automatically loads devices that are registered to Asset Management with your FortiCloud account, so ensure that you log in to the same account when accessing the FortiZTP portal. After login, you can search the device by its serial number on the *Unprovisioned* tab.
How do I find a recently provisioned device?	You can search for a device by its serial number or sort the provisioned device list by provisioning date.
Why does the *Unprovisioned* tab of the FortiZTP portal not list my device?	Ensure that the device has been registered to the same account in FortiCloud Asset Management.
How do I go to the cloud service portal of a particular device after provisioning?	Click the device serial number and the GUI redirects you to its cloud service portal.
How do I change a device's provisioning location?	Deprovision the device, then reprovision it with the preferred provisioning location.
What steps should I take when Zero-Touch Provisioning is halted by a certificate error?	FortiGate devices running some older FortiOS versions may encounter a certificate error during the first boot because the built-in CA bundle has not yet been updated from FortiGuard. After the initial boot, allow 10–15 minutes for the FortiGate to automatically download the updated CA bundle from FortiGuard. If the automatic download does not occur, you can manually trigger the update from the CLI: `execute update-now`

API

There is an API available for FortiZTP. You can find information on supported API calls at the FortiZTP REST API documentation.

The API usage limit is 2 000 calls per hour. If the usage goes over 2 000 calls per hour, API calls fail and a message displays that you are over the limit.

You can do a single API call on multiple devices by entering multiple device serial numbers.

The FortiZTP v2.0 API is available. For API changes and documentation, see the FortiZTP API docs.

www.fortinet.com