FORTINET

Administration Guide

FortiZTP 23.1

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

FORTINET VIDEO GUIDE
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

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

February 03, 2023
FortiZTP 23.1 Administration Guide
73-231-878107-20230203

TABLE OF CONTENTS

Change log **4**
Introduction **5**
Functions 5
Requirements 6
What's new **8**
Getting started with the FortiZTP portal **9**
Provisioning devices **10**
Provisioning a FortiGate 10
Provisioning a FortiAP 12
Provisioning a FortiSwitch 13
Provisioning a FortiExtender 13
Deprovisioning a device **15**
Frequently asked questions **16**

Change log

Date	Change Description
2023-02-03	Initial release of 23.1.

Introduction

FortiZTP is a centralized zero-touch provisioning platform for FortiCloud cloud product services. Powered by FortiDeploy, the service supports individual or bulk device provisioning to the target on-premise or cloud services. The centralized 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 • FortiLAN Cloud
FortiSwitch	FortiLAN 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.
Regions	• Global (North America) • Europe (EU) • Japan (APAC) FortiZTP supports FortiGate Cloud, FortiLAN Cloud, and FortiManager Cloud. For information on region support for these products, see the following: • **FortiGate Cloud**: see Functions. • **FortiLAN Cloud**: FortiLAN Cloud includes the Global, Europe, and Japan regions: • The data center in Canada serves the GL and JP domains.

Function	Description
	• 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.
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, FortiLAN 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.
	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`
	After changing this setting, restart the device and ensure that the device is sending traffic to FortiGate Cloud to verify that you have configured it correctly.

Requirement	Description

	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

What's new

- Support for organizations:
  - Allow portal access for Identity & Access Management (IAM) user and identity provider user with organization unit (OU) scope and portal permissions
  - OU account selection and switching
  - OU dashboard
  - Support OU/account switching within portal after login
- Provision history support
- IAM user support enhancements
- Default landing page automatically set to provisioned list if there are no unprovisioned devices
- Provisioning FortiExtender to FortiSASE

Getting started with the FortiZTP portal

You can access FortiZTP by going to fortiztp.forticloud.com.

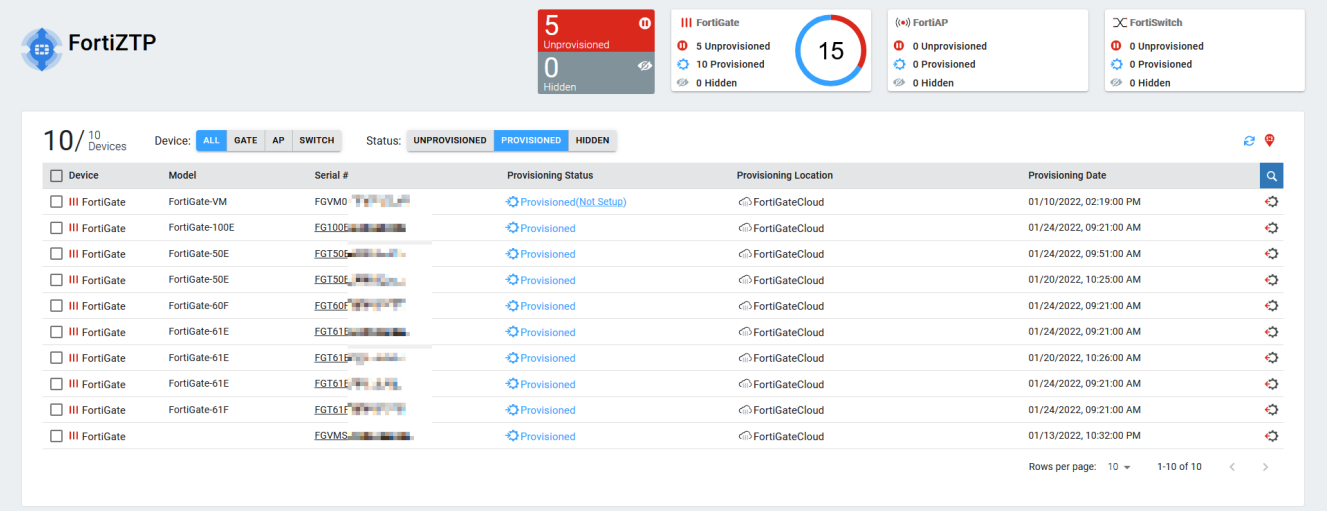
The top of the GUI displays how many devices are unprovisioned and hidden. It also displays how many FortiGates are unprovisioned, provisioned, or hidden, as well as the total number of FortiGates that are available for configuration. It displays the same information for FortiAPs and FortiSwitches.

You can use the *Device* and *Status* tabs to filter which devices display in the list. The list displays the following information for each device:

- Device type
- Model
- Serial number
- Provisioning status

If viewing provisioned devices, the list also displays the provisioning location and date for each 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.



Provisioning devices

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

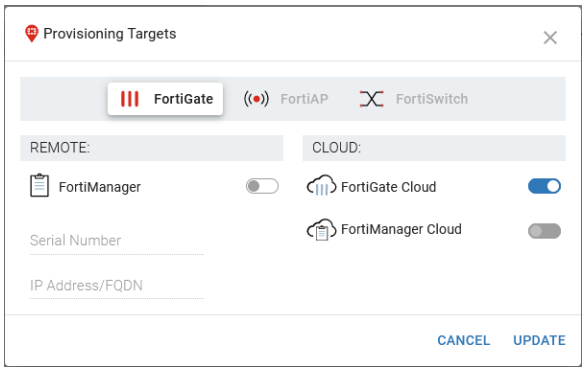
FortiZTP automatically deletes provisioning history older than one year.

Provisioning a FortiGate

The following describes provisioning a FortiGate.

To provision a FortiGate to FortiGate Cloud:

1. Click the *Provisioning Settings* button on the right. On the *FortiGate* tab, ensure that *FortiGate Cloud* is enabled.
2. Click *UPDATE*.



3. On the *UNPROVISIONED* tab, do the following:
   a. To provision a single FortiGate, click the *Provision* icon.
   b. To provision multiple FortiGates, select the checkboxes for the desired FortiGates, then click the *PROVISION* button.
4. Under *TARGET LOCATION* in the *Provision devices* dialog, select the desired target location for the FortiGate(s). Only options that you have configured in *Provisioning Settings* appear in this dialog.
5. Click *PROVISION NOW*.

After devices are provisioned, they appear on the *PROVISIONED* tab.

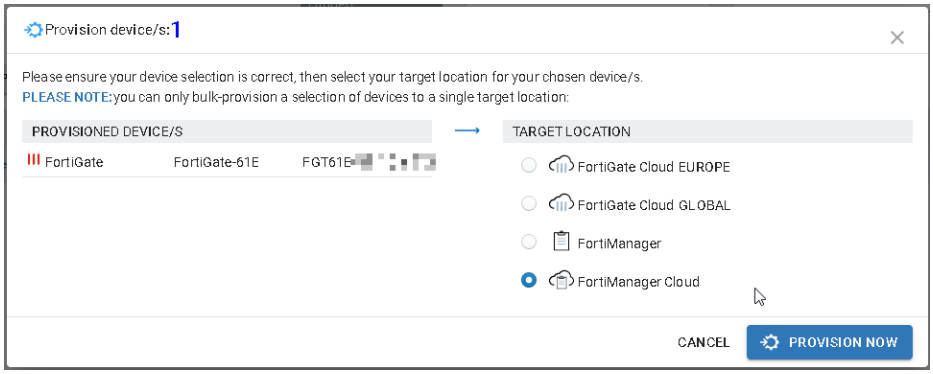
To provision a FortiGate to FortiManager:

1. Click the *Provisioning Settings* button on the right.
2. In the *Provisioning Targets* dialog, on the *FortiGate* tab, enable *FortiManager*.
3. In the *Serial Number* and *IP Address* fields, enter the FortiManager details.
4. By default, FortiGate Cloud is enabled. If desired, you can disable FortiGate Cloud.
5. Click *UPDATE*.

6. On the *UNPROVISIONED* tab, do the following:
   a. To provision a single FortiGate, click the *Provision* icon.
   b. To provision multiple FortiGates, select the checkboxes for the desired FortiGates, then click the *PROVISION* button.
7. Under *TARGET LOCATION* in the *Provision devices* dialog, select the desired target location for the FortiGate(s). Only options that you have configured in *Provisioning Settings* appear in this dialog.
8. Click *PROVISION NOW*.

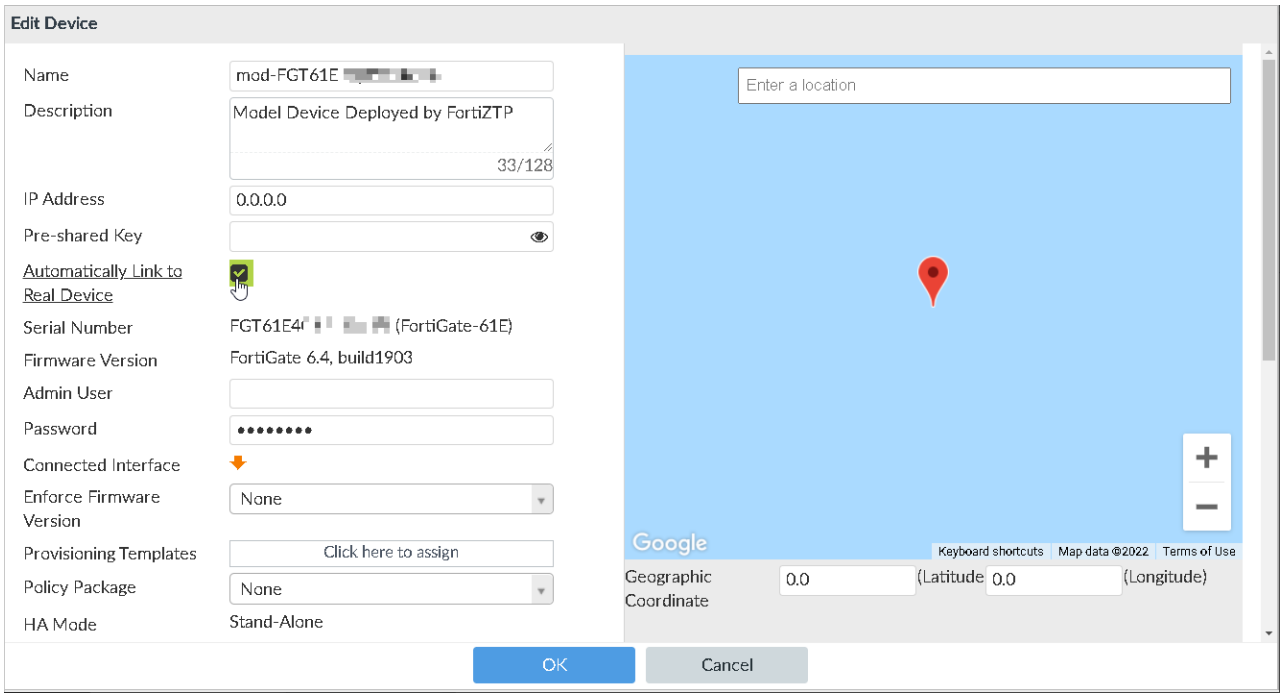
To provision a FortiGate to FortiManager Cloud:

1. Click the *Provisioning Settings* button on the right.
2. On the *FortiGate* tab, enable *FortiManager Cloud*.
3. Click *UPDATE*.
4. On the *UNPROVISIONED* tab, do the following:
   a. To provision a single FortiGate, click the *Provision* icon.
   b. To provision multiple FortiGates, select the checkboxes for the desired FortiGates, then click the *PROVISION* button.
5. Under *TARGET LOCATION* in the *Provision devices* dialog, select *FortiManager Cloud*.
6. Click *PROVISION NOW*.



7. Power on or factory reset the FortiGate.
8. In FortiManager Cloud, go to Device Manager. Right-click the FortiGate, then select *Edit*.

9. Enable *Automatically Link to Real Device*, then click *OK*.



After devices are provisioned, they appear on the *PROVISIONED* tab.

Provisioning a FortiAP

The following describes provisioning a FortiAP.

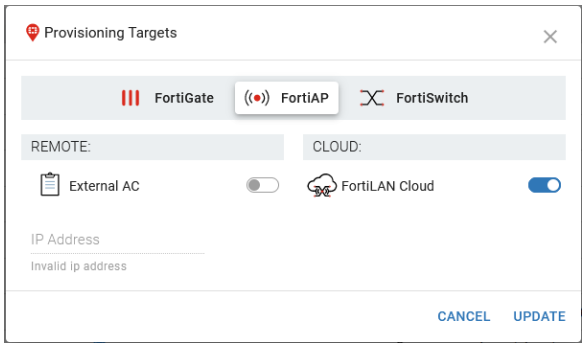
To provision a FortiAP to FortiGate:

1. Click the *Provisioning Settings* button on the right.
2. On the *FortiAP* tab, enable *External AC*.
3. In the *IP Address* field, enter the desired FortiGate IP address.
4. Click *UPDATE*.
5. On the *UNPROVISIONED* tab, do the following:
   a. To provision a single FortiAP, click the *Provision* icon.
   b. To provision multiple FortiAPs, select the checkboxes for the desired FortiAPs, then click the *PROVISION* button.
6. Under *TARGET LOCATION* in the *Provision devices* dialog, select *External AC*. Only options that you have configured in *Provisioning Settings* appear in this dialog.
7. Click *PROVISION NOW*.

To provision a FortiAP to FortiLAN Cloud:

1. Click the *Provisioning Settings* button on the right.
2. On the *FortiAP* tab, ensure that *FortiLAN Cloud* is enabled.

3. Click *UPDATE*.



4. On the *UNPROVISIONED* tab, do the following:
   a. To provision a single FortiAP, click the *Provision* icon.
   b. To provision multiple FortiAPs, select the checkboxes for the desired FortiAPs, then click the *PROVISION* button.
5. Under *TARGET LOCATION* in the *Provision devices* dialog, select the desired target FortiLAN Cloud for the FortiAP (s). Only options that you have configured in *Provisioning Settings* appear in this dialog.
6. Click *PROVISION NOW*.

Provisioning a FortiSwitch

The following describes provisioning a FortiSwitch.

To provision a FortiSwitch to FortiLAN Cloud:

1. Click the *Provisioning Settings* button on the right.
2. On the *FortiSwitch* tab, ensure that *FortiLAN Cloud* is enabled.
3. Click *UPDATE*.
4. On the *UNPROVISIONED* tab, do the following:
   a. To provision a single FortiSwitch, click the *Provision* icon.
   b. To provision multiple FortiSwitches, select the checkboxes for the desired FortiSwitches, then click the *PROVISION* button.
5. Under *TARGET LOCATION* in the *Provision devices* dialog, select the desired target location for the FortiSwitche (s). Only options that you have configured in *Provisioning Settings* appear in this dialog.
6. Click *PROVISION NOW*.

Provisioning a FortiExtender

The following describes provisioning a FortiExtender. Provisioning a FortiExtender to FortiSASE is only supported 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. Click the *Provisioning Settings* button on the right.
2. On the *FortiExtender* tab, ensure that *FortiExtender Cloud* is enabled.
3. Click *UPDATE*.
4. On the *UNPROVISIONED* tab, do the following:
   a. To provision a single FortiExtender, click the *Provision* icon.
   b. To provision multiple FortiExtenders, select the checkboxes for the desired FortiExtenders, then click the *PROVISION* button.
5. Under *TARGET LOCATION* in the *Provision devices* dialog, select FortiExtender Cloud. Only options that you have configured in *Provisioning Settings* appear in this dialog.
6. Do one of the following:
   a. Click *NEXT*. You can choose to associate the FortiExtender with a profile. Select the desired profile, then click *PROVISION NOW*.
   b. Click *PROVISION NOW*.

To provision a FortiExtender to FortiSASE:

1. Click the *Provisioning Settings* button on the right.
2. On the *FortiExtender* tab, ensure that *FortiSASE* is enabled.
3. Click *UPDATE*.
4. On the *UNPROVISIONED* tab, do the following:
   a. To provision a single FortiExtender, click the *Provision* icon.
   b. To provision multiple FortiExtenders, select the checkboxes for the desired FortiExtenders, then click the *PROVISION* button.
5. Under *TARGET LOCATION* in the *Provision devices* dialog, select FortiSASE. Only options that you have configured in *Provisioning Settings* appear in this dialog.
6. Do one of the following:
   a. Click *NEXT*. You can choose to associate the FortiExtender with a profile. Select the desired profile, then click *PROVISION NOW*.
   b. Click *PROVISION NOW*.

Deprovisioning a device

To deprovision a device:

1. Go to the *PROVISIONED* tab.
2. Do one of the following:
   a. To deprovision a single device, click the *Deprovision* icon for the desired device. The *Deprovision* icon is on the right side of the GUI.
   b. To deprovision multiple devices, select the checkboxes for the desired devices. Click the *Deprovision* button.
3. In the dialog, click *Deprovision Now*.

Deprovisioned devices now display on the *UNPROVISIONED* tab. 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 FortiGates can successfully be reprovisioned:

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

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

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.

www.fortinet.com

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.