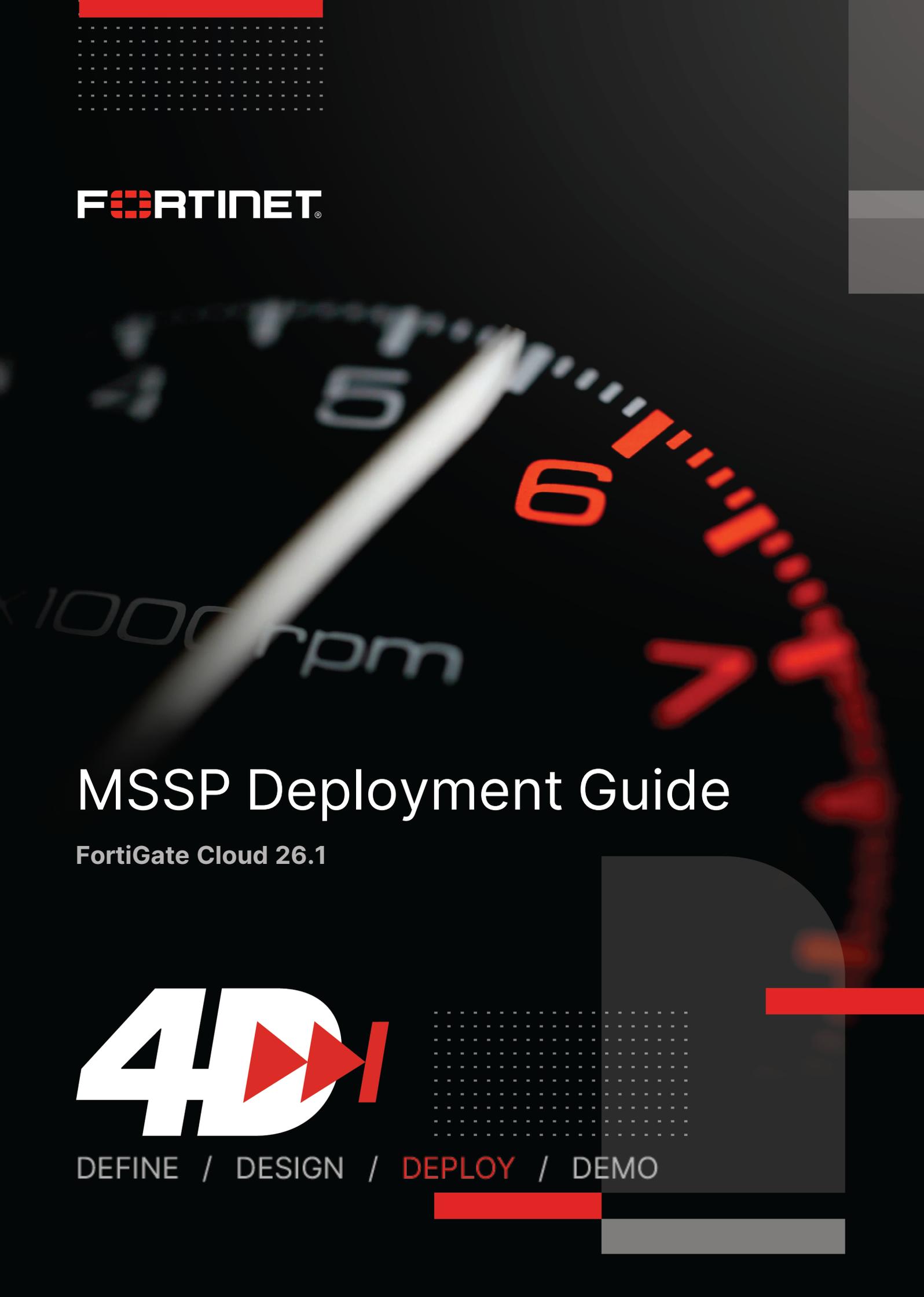




FORTINET®



MSSP Deployment Guide

FortiGate Cloud 26.1



DEFINE / DESIGN / **DEPLOY** / DEMO



Table of Contents

Change log	3
Introduction	4
Executive summary	4
Multitenancy licensing	4
Intended audience	5
About this guide	6
Deployment procedures	7
Creating the primary account	7
Registering the primary FortiCloud account with FortiCare support	7
FortiCloud navigation and account ID	8
Multitenancy	9
Multitenancy and subaccounts	9
Multitenancy with FortiCloud Organizations	11
Deploying FortiGates to subaccounts	14
Deploying FortiGates using FortiCloud keys	14
Adding a FortiGate with a FortiCloud key	14
Adding a FortiGate to Inventory with a FortiCloud key	15
Adding multiple FortiGates to Inventory with a FortiCloud bulk key	16
Moving a FortiGate between subaccounts	16
Undeploying and redeploying a FortiGate	17
Moving a FortiGate from an old account	17
Configuration complete	18
Appendix A - Products used in this guide	19
Appendix B - Documentation references	20

Change log

Date	Change description
2026-02-04	Initial release.

Introduction

Executive summary

FortiGate Cloud is a cloud-based software-as-a-service offering with multitenant functionality for managed security service providers (MSSP). MSSPs can leverage Fortinet's FortiCloud infrastructure, including Fortinet-managed 24/7 datacenters and cloud presence. MSSPs can focus on configuration, management, and customer service without having to go into the data center business. FortiGate Cloud offers zero touch deployment, configuration management, reporting, and analytics. FortiGate Cloud can grow with your and your customer's requirements, from a single FortiGate to a complete management solution for thousands of devices across multiple customers.

This deployment guide is intended to cover the key multicustomer configuration needs for using Fortinet's FortiGate Cloud portal in an MSSP context with multiple customers, administrators, and subaccounts. As a cloud management service that Fortinet hosts in Fortinet datacenters, FortiGate Cloud has an enormous scalability range, and is well-suited for MSSPs of all sizes, from a single FortiGate at a single customer site to thousands of FortiGates and thousands of customer sites.

This guide is specifically about multitenancy and managing administrators and subaccounts and not about detailed configuration of individual FortiGates. See the [FortiGate Cloud Administration Guide](#) for detailed FortiGate administration.

Multitenancy licensing

The multitenancy account option in FortiGate Cloud is designed for MSSPs. A multitenancy account is a one- or five-year service for an administrator to create and manage multiple subaccounts. It also allows you to move devices between these accounts. You can allocate administrators to each subaccount with full or read-only access, allowing more control over a managed service's provisioning.

To obtain a multitenancy license, contact your Fortinet partner or reseller, requesting the following SKU: FCLD-10-FCLD0-161-02-DD. You receive a multitenancy activation code via email.

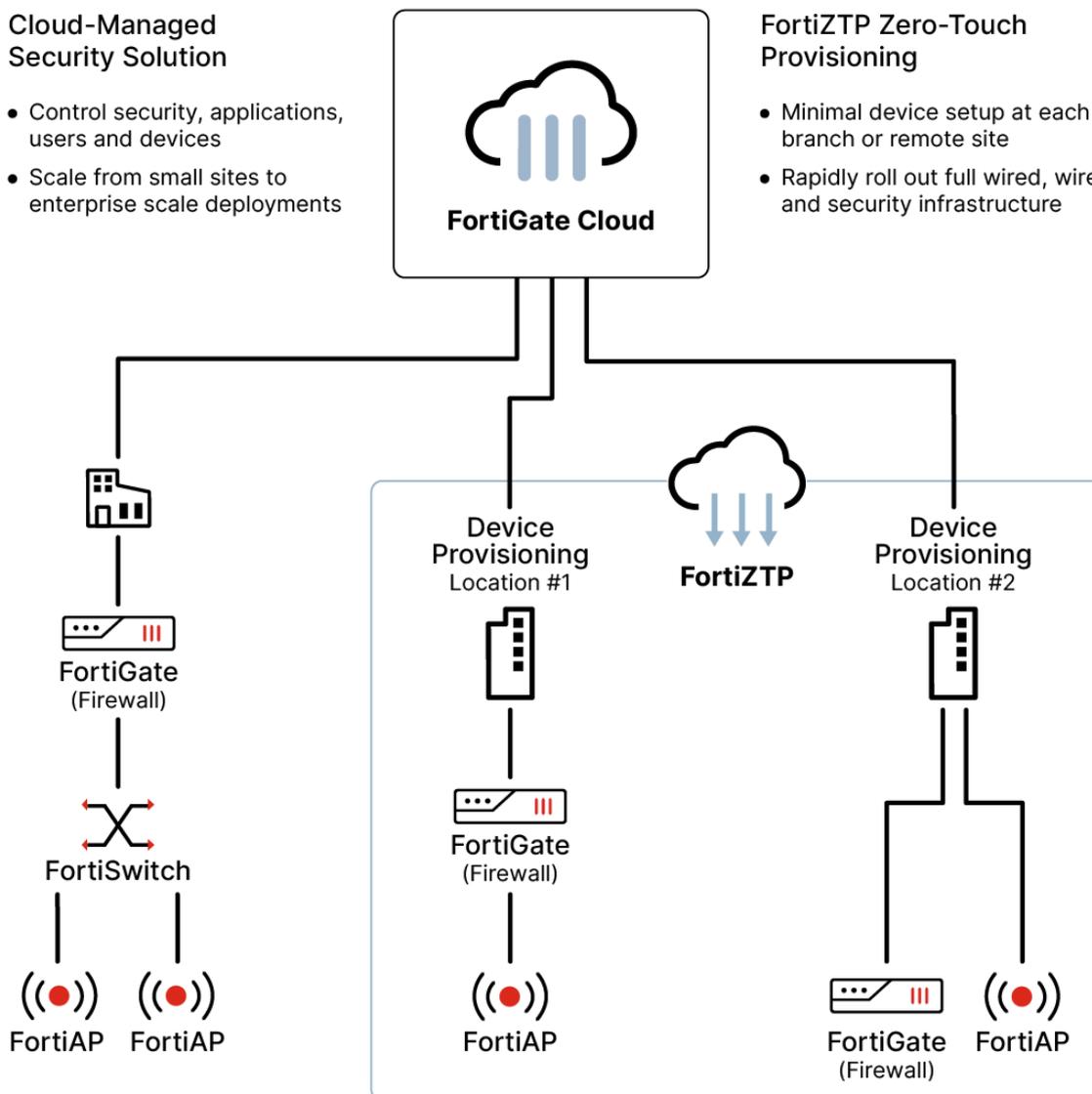
FortiGate Cloud with FortiDeploy

Cloud-Managed Security Solution

- Control security, applications, users and devices
- Scale from small sites to enterprise scale deployments

FortiZTP Zero-Touch Provisioning

- Minimal device setup at each branch or remote site
- Rapidly roll out full wired, wireless and security infrastructure



Intended audience

This guide is intended for an MSSP interested in deploying a multitenant FortiGate Cloud-based offering for their customers. Readers should have a basic understanding of cloud solutions, networking, and security concepts before they begin. Interested audiences may include:

- MSSP network, wireless, and security architects
- MSSP network, wireless, and security engineers

About this guide

This guide gathers the relevant material to setup FortiGate Cloud for an MSSP. FortiGate Cloud is only one of a suite of cloud portals for multiple Fortinet products. Exploring the suite of Fortinet products is recommended for MSSPs. You can find more information at the following links:

- [Fortinet MSSP services](#)
- [4D resources – best practices](#)
- [FortiCloud](#)
- [FortiGate Cloud Administration Guide](#)

This deployment guide presents one of many possible ways to deploy the Fortinet solutions. It may also omit specific steps where readers must make design decisions to further configure their devices. It is recommended that readers also review supplementary material found in product admin guides, example guides, cookbooks, release notes, and other documents where appropriate.

Deployment procedures

You can use the following procedures for a FortiGate Cloud deployment as a managed security service provider.

Creating the primary account

This account controls all subaccounts. Take appropriate measures to ensure it is secure and accessible as the business undergoes changes. It is best this not be a personal account and that the credentials be transferable. You should also anticipate growth.

Registering the primary FortiCloud account with FortiCare support

To register the primary FortiCloud account with FortiCare support:

1. Register an account:
 - a. In a browser, go to the [FortiGate Cloud portal](#).
 - b. Click *Register*.
 - c. In the *Account Email* field, enter the main account email address, then click *Register*.
 - d. A CAPTCHA code displays. Enter the code, then click *Get Verification Code*. The configured account email address receives a verification code.
 - e. In the *Verification Code* field, enter the received verification code, then click *Next*.
 - f. Create and reenter a password following the displayed password rules. Click *Next*.
 - g. Enter your user and company information, then click *Submit*.
 - h. Read and agree to the Fortinet service terms and conditions, then click *Register*.
 - i. Click *Complete*. The portal displays a login screen. If desired, you can log in. The login screen allows you to select Identity & Access Management (IAM) login, which is a different account type than the account that you just created, which is an email login account. See [IAM users](#).
2. To return to the login screen, go to the [FortiGate Cloud portal](#) in a browser. Click *Login*, select *Email Login*, and

enter the account credentials.



FortiGate Cloud

Login

Register

FortiGate Cloud simplifies network operations for Fortinet FortiGates and the connected devices, FortiSwitch, FortiAP, and FortiExtender for initial deployment, setup and ongoing maintenance.

FortiGate Cloud brings enterprise-grade analytics and reporting for small to medium



FortiCloud navigation and account ID

In a web browser, go to the [FortiGate Cloud portal](#) and log in to FortiCloud. In addition to FortiGate Cloud, you can use the upper menu ribbon to go to FortiCloud's other specialized portals. In the upper right corner, click your account email address. You can use these menu items to modify account settings.

For example, you can click *My Account* to change passwords and account settings. In addition to an account name, the account has a unique account ID number.

From a FortiCloud screen, click *Services* to view FortiCloud administrative portals. This menu consists of the following sections:

Section	Description
Assets & Accounts	Asset and user administration.
Cloud Management	FortiCloud's cloud management portals. This guide focuses on the FortiGate Cloud portal.
Cloud Services	Portals for Fortinet's cloud-based security products.

The *Support* menu contains support options. FortiCloud is fully integrated with FortiCare support. FortiCloud's most basic function is FortiCare support.

Multitenancy

FortiGate Cloud supports the following options for multitenancy:

- **Multitenancy with subaccounts:** see [Multitenancy and subaccounts on page 9](#).
- **Multitenancy with FortiCloud Organizations:** see [Multitenancy with FortiCloud Organizations on page 11](#).

Multitenancy and subaccounts

Activating a FortiGate Cloud multitenancy license

You need a multitenancy account activation code, delivered via email. If you do not already have a multitenancy activation code, contact your Fortinet partner or reseller to purchase a license, and request the following SKU: FCLE-10-FCLD0-161-02-DD. They will email you a multitenancy activation code.

To apply the activation code:

1. Log in to the [FortiGate Cloud portal](#).
2. Go to *Account Setting > Activate multi-tenancy feature*.
3. In the *Activation Code* field, enter the code. Click *Submit*.
4. An *Activation successful* dialog displays. Click *OK*.
5. Log out and relog in. Confirm that subaccounts are enabled. The following screenshots show the difference in the upper banner when multitenancy is not activated and activated.



Adding a subaccount

You can use subaccounts for any administrative purpose that fits your business. However, they are most frequently aligned with customer accounts.

To add a subaccount:

1. Go to *Settings > Account Setting*. You can view all accounts associated with this FortiGate Cloud. You can see that users have different roles. For role descriptions, see [User roles](#).
2. Click *Manage Subaccounts*.

3. If desired, in the *Search* field, enter the name of the desired parent subaccount for your new subaccount.
4. Select desired subaccount to see the gear icon. Click the gear icon and select *Add*.
5. In the *Name* field, enter the desired name for the new subaccount, then click *OK*.

A subaccount can have its own subaccount in a typical tree structure, allowing a hierarchical build out of subaccounts. You can select one of the other options in the menu to move, edit, and delete subaccounts.

When you move a subaccount, FortiGate Cloud deletes all scheduled reports and tasks associated with that subaccount's devices. This warning displays in the GUI when you move a subaccount.

Activating a subaccount user account

The subaccount user must acknowledge their FortiCloud account activation. The following instructions are from the subaccount user's perspective.

To activate a subaccount user account:

1. Open the registration confirmation email from FortiCloud. Click the link in the email to complete signup.



2. The browser prompts for password reset. Enter the desired password, then click *Submit*.
3. The browser displays a success message. Click the link to go to the login screen. You now have an email login account to FortiCloud. Log in using your credentials.
4. The portal may display the account access screen. Click *Access*. You have read-only access to the subaccounts.



Modifying subaccount user access

The primary account user can modify subaccount user settings.

To modify subaccount user access:

1. Log in to the primary account as the primary account user.
2. Go to *Account Setting*.
3. Use the *Users* dropdown list or the search bar to find the desired user. Click the pencil icon for the user.
4. From the *Role* dropdown list, select the desired role.

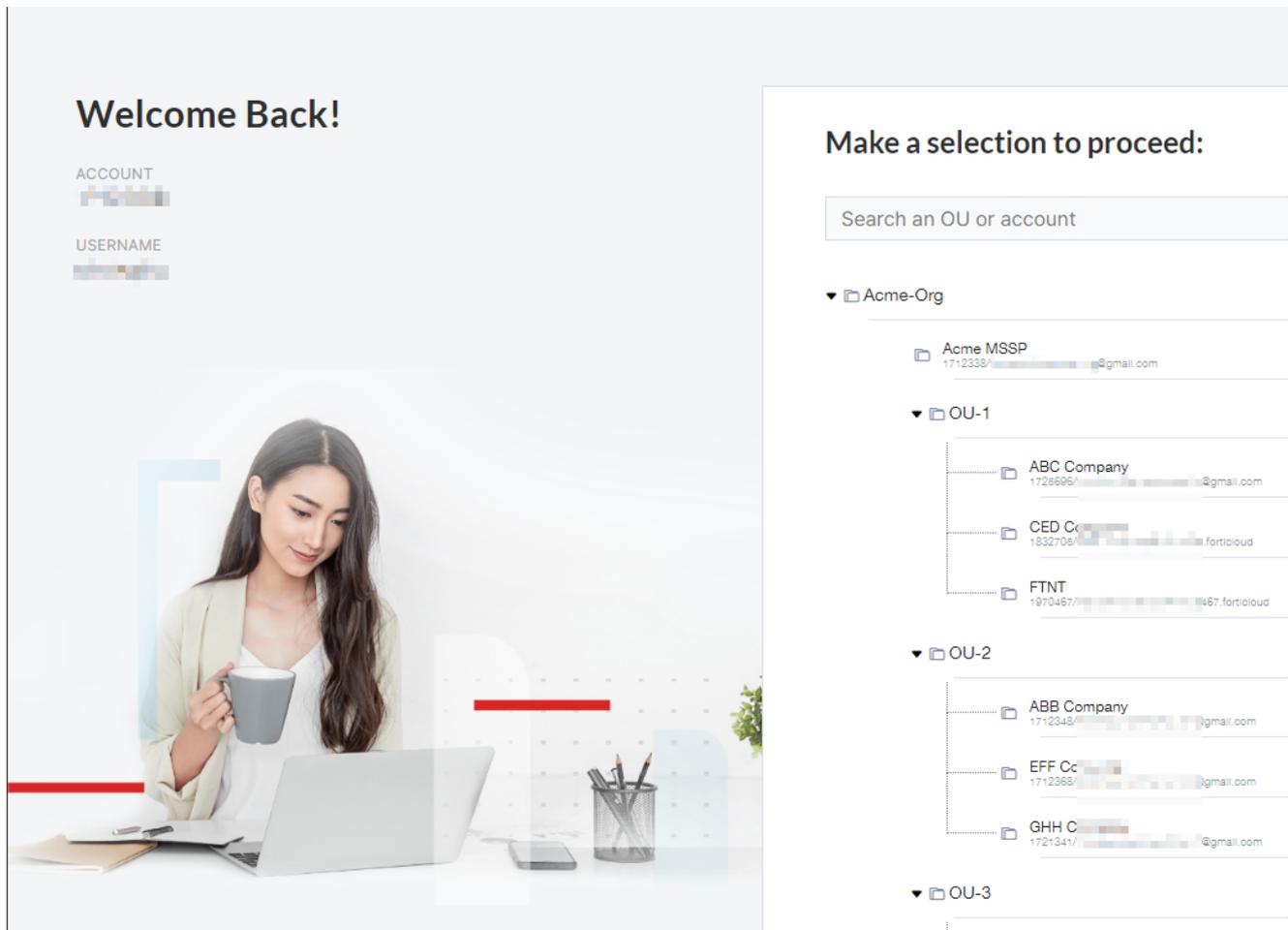
5. To modify subaccount access, click *Selected* for *Manage Sub Account*. Select the desired subaccounts for the user to have access to.
6. Click *Submit*. The modified settings activate at the subaccount user's next login.

Multitenancy with FortiCloud Organizations

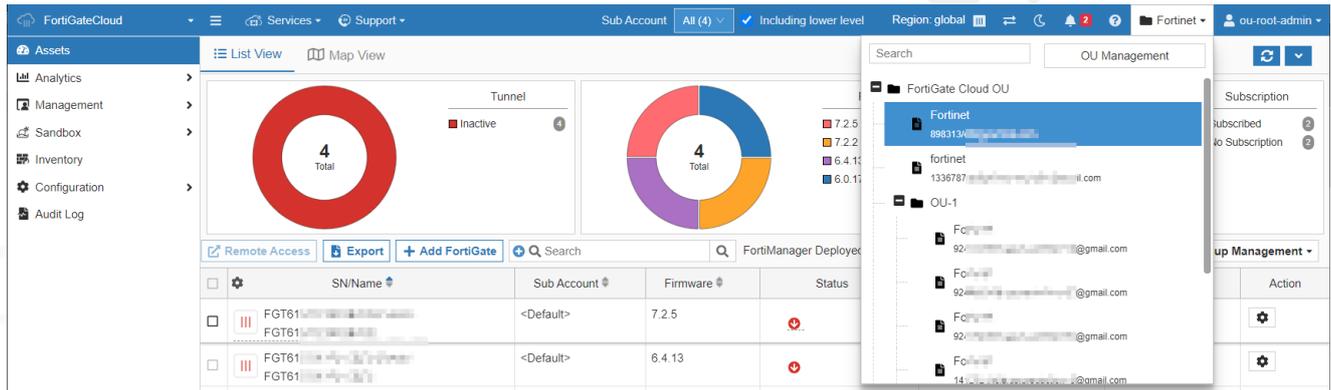
FortiGate Cloud supports FortiCloud Organizations for seamless multitenant features designed for managed security service providers across multiple FortiCloud accounts. With Organizations, Identity & Access Management (IAM) users can view an organizational unit (OU) Dashboard for a single pane of glass view of assets across the entire Organization or OUs. Administrators can add additional users with a fine grained permission model (IAM permission profile) and manage the visibility and access to full Organization or specific OU or OU member accounts. See the following for details on various OU tasks:

Task	Instructions
Creating an OU	Adding and deleting OUs
Creating an OU IAM user	Organization user management When creating a permission profile in the IAM portal, you must add the FortiGate Cloud portal to the profile, and configure the desired permissions.
Log in as an OU IAM user	Logging into an OU account

When you log in to FortiGate Cloud, if OUs are enabled on the account, an OU or account selection screen displays. You can select an OU or account to access from this tree.



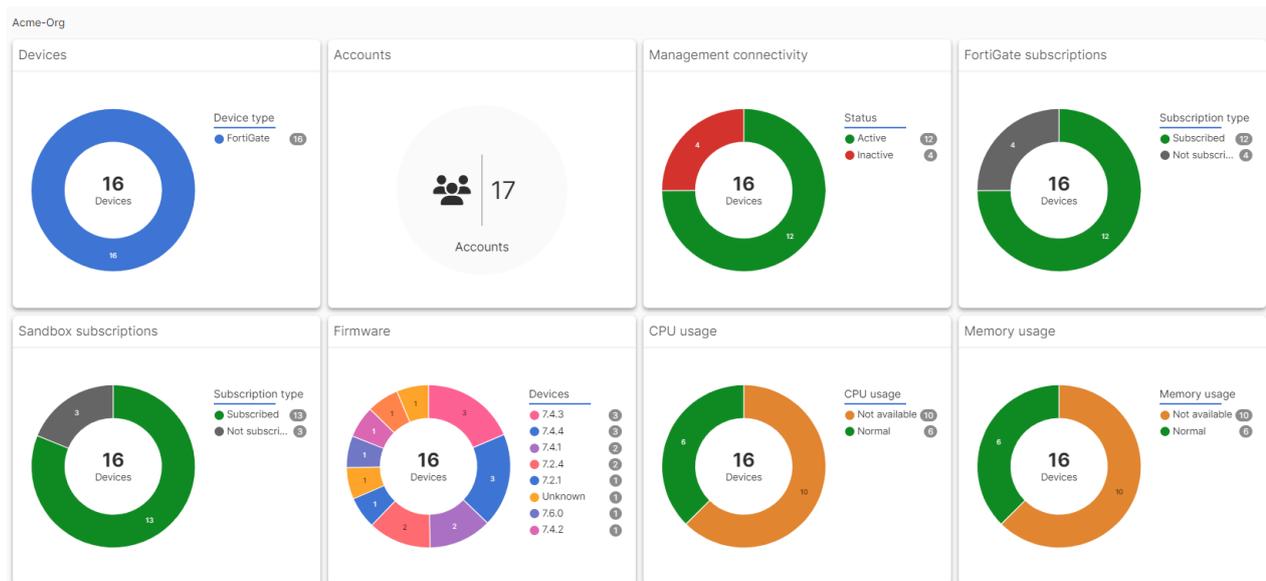
To move to another OU or account, select the desired OU from the dropdown list in the upper right corner.



OU Dashboard

The OU Dashboard provides a consolidated view of accounts and assets in the given scope of the Organization. The dashboard is available for Organization type IAM users and the visibility of accounts and assets depends on the OU scope selected for the IAM user.

When you access an OU from the OU tree, FortiGate Cloud displays an OU dashboard. The following lists OU dashboard widgets:



Widget	Description
Devices	Displays a donut chart that details the device type breakdown and total number of devices in this OU.
Accounts	Displays a donut chart that details the total number of accounts in this OU.
Management connectivity	Displays a donut chart that details the management connectivity status breakdown and total number of devices in this OU.
FortiGate subscriptions	Displays a donut chart that details the FortiGate Cloud subscription type breakdown and total number of devices in this OU.
Sandbox subscriptions	Displays a donut chart that details the Sandbox subscription type and total

Widget	Description
	number of devices in this OU.
Firmware	Displays a donut chart that details the firmware versions on devices in this OU.
CPU usage	Displays a donut chart that details the CPU usage data on devices in this OU.
Memory usage	Displays a donut chart that details the memory usage data on devices in this OU.

To transfer a device between accounts:

1. Go to *Assets > Asset list*.
2. Go to the desired account.
3. Select the desired device(s).
4. Click *Transfer FortiGates*.
5. From the *To* dropdown list, select the desired account to transfer the device to.
6. Select the desired data transfer option. If you select *Migrate data to new account*, the device's configuration backups, existing logs, report instances, and report configs are migrated to the new account.

7. Confirm the acknowledgment, then click *OK*.

TRANSFER FORTIGATES
✕

From: [redacted]@gmail.com

To: CED.Company@1832705.forticloud

Data transfer options:

- Remove all data
Permanently delete all log data associated with the FortiGate after transfer.
- Migrate data to new account**
Update log data ownership from the source account to the new account.
- Keep data in original account
Retain ownership of the log data associated with the FortiGate in the original account.

+ Q Search
Q

FortiGate

FortiGate-91G

FGT91G [redacted]

1

I acknowledge and understand that upon transferring, all scheduled reports, firmware upgrades, CLI script tasks, and any existing logs and reports associated with the FortiGate will be lost. I further acknowledge that if all FortiGates with FortiGate Cloud subscriptions are transferred out of an account that is using the Premium Portal, the portal will be downgraded to the Standard Portal after one month.

OK
Cancel

Deploying FortiGates to subaccounts

Deploying FortiGates using FortiCloud keys

You can use one of the following options to deploy a FortiGate using a FortiCloud key:

Adding a FortiGate with a FortiCloud key

You can find the FortiCloud key on a sticker on the FortiGate.

To add a FortiGate with a FortiCloud key:

1. Go to *Inventory*.
2. Click *Import FortiCloud Key*.
3. Enter the FortiCloud key.
4. From the dropdown list, select the desired timezone.
5. Select the desired subaccount.
6. Click *Submit*.

FortiGate Cloud

Add FortiGate

Please input the FortiGate Cloud Key to add a FortiGate:

AAAABBBB

Select Display Timezone for Device

(GMT-07:00) Pacific Time (US & Canada)

Select Sub Account

<Default>

Chicago

San Francisco

Seattle

Redmond

Submit

Adding a FortiGate to Inventory with a FortiCloud key

You can find the FortiCloud key on a sticker on the FortiGate.

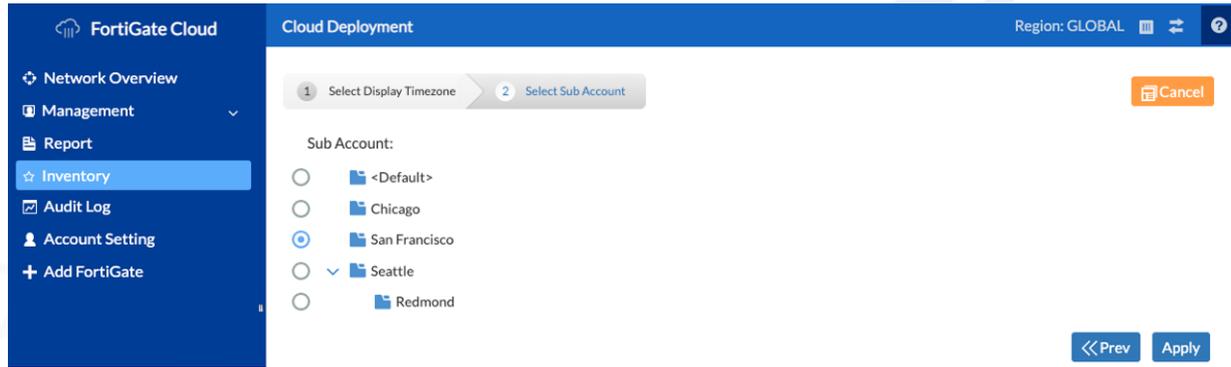
To add a FortiGate to Inventory with a FortiCloud key:

1. Go to *Inventory*.
2. Click *Import FortiCloud Key*.
3. Enter the FortiCloud key.
4. Click *Submit*.

To deploy an inventory FortiGate to a subaccount:

1. Go to *Inventory*.
2. Select the desired FortiGate.
3. Click *Deploy* to FortiGate Cloud.
4. From the dropdown list, select the desired timezone. Click *Next*.

5. Select the desired subaccount. Click *Apply*.



Adding multiple FortiGates to Inventory with a FortiCloud bulk key

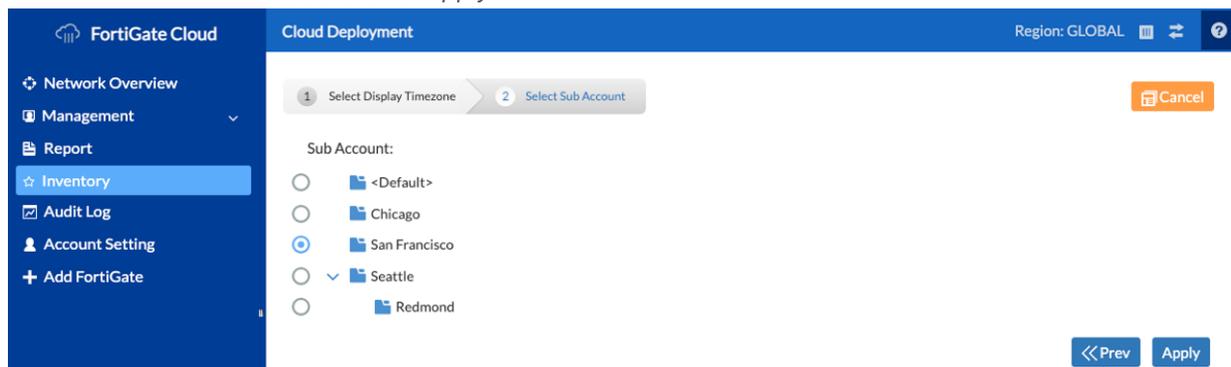
You can find the FortiCloud bulk key on the purchase order for multiple FortiGates.

To add multiple FortiGates to inventory with a FortiCloud bulk key:

1. Go to *Inventory*.
2. Click *Import Bulk Key*.
3. Enter the FortiCloud key.
4. Click *Submit*.

To deploy an inventory FortiGate to a subaccount:

1. Go to *Inventory*.
2. Select the desired FortiGate.
3. Click *Deploy* to FortiGate Cloud.
4. From the dropdown list, select the desired timezone. Click *Next*.
5. Select the desired subaccount. Click *Apply*.



Moving a FortiGate between subaccounts

Assigning a FortiGate to a new subaccount moves its historical data to the new subaccount. If you do not want to keep data, undeploy your device, then assign it to another subaccount.

To move a FortiGate between subaccounts:

1. Log in to the FortiCloud account.
2. Go to *Assets*.
3. Click the management icon for the desired FortiGate.
4. Click *Assign To*.
5. Select the desired subaccount, then click *Submit*.
6. A warning message appears. If there is no issue, click *Yes*. The FortiGate is assigned to the new subaccount.

Undeploying and redeploying a FortiGate

Undeploying returns a FortiGate to Inventory. You can redeploy it from there. The current version of FortiGate Cloud includes the option of preserving the FortiGate's logs or deleting them from FortiGate Cloud.

To undeploy and redeploy a FortiGate:

1. Go to *Assets*.
2. Click the management icon for the desired FortiGate.
3. Click *Undeploy*.
4. Enable or disable *Keep Data* as desired.
5. Click *YES*. The FortiGate is undeployed. You can redeploy it from Inventory in the future.

Moving a FortiGate from an old account

Migrations are sometimes necessary, particularly taking over the management of an existing FortiGate.

To move a FortiGate from an old account:

1. Log in using the old account to migrate the FortiGate from.
2. Go to *Assets*.
3. Click the gear icon for the desired FortiGate.
4. Click *Migrate Existing Data*.
5. In the *Account ID* field, enter the new primary account email address. Click *OK*.
6. An authorization message displays. However, you must log in to the new account from the FortiGate. Click *OK*.

Ultimately, you must have access other than via the FortiCloud to attach a FortiGate to a new account. However, remote access from the original FortiGate is NOT removed until the FortiGate logs out from the original account, so the disconnect process CAN be done entirely remotely. Typically, someone will have to have local access to the FortiGate to join the new account.

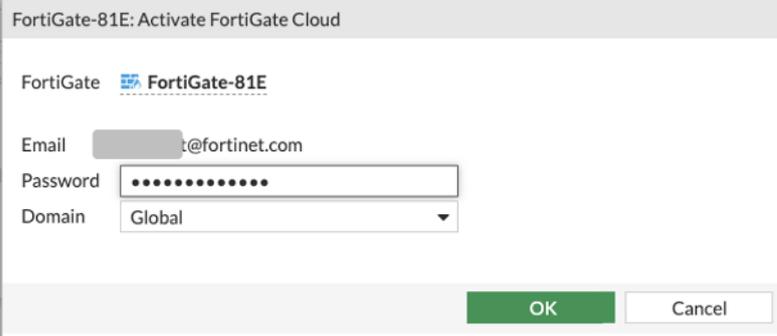
To remotely access the FortiGate from the original account:

1. Go to *Assets*.
2. Click *Remote Access* for the desired FortiGate.
3. In the *Remote Access* dialog, change the FortiGate web GUI port if necessary. Click *OK*.
4. The browser presents the FortiOS login page identically as for a local connection.

To transfer the FortiGate to another FortiCare account:

You can perform this remotely or with any standard network connection to the FortiGate.

1. Log in to the FortiGate.
2. Go to *Dashboard > Status*.
3. In the *Licenses* widget, click *FortiCare Support*, then *Transfer FortiGate to Another Account*.
4. In the *Password* field, enter the old account's password.
5. Under *Target FortiCloud Account*, enter the primary FortiCloud account email address and password. Click *Next*.
6. Click *Transfer*.
7. Dissociate this FortiGate with the old FortiGate Cloud account:
 - a. Go to *Dashboard > Status*.
 - b. In the *FortiGate Cloud* widget, click *Activated*, then *Logout*.
 - c. Click *OK*.
8. At this point, if you are using FortiCloud to remotely access the FortiGate, you lose access. Completing the transfer requires another method of network access to the FortiGate. Activate the new FortiGate Cloud account on the FortiGate:
 - a. Log in to the FortiGate.
 - b. In the FortiGate Cloud widget, click *Not Activated*, then *Activate*.
 - c. The email address is autopopulated from the FortiCare settings. Enter the password, then click *OK*. In a few moments, the FortiGate shows up in the FortiCloud account and you can deploy it as desired.



FortiGate-81E: Activate FortiGate Cloud

FortiGate  FortiGate-81E

Email

Password

Domain

Configuration complete

This configuration is scalable from a small MSSP with a few elite customers to a large organization with many customers. However, in many ways, this design can be considered a start. It only scratches the surface of possibilities available with Fortinet's full suite of cloud solutions. As your needs, design goals, and customer services evolve, please see other Fortinet documentation found in the Appendix.

Appendix A - Products used in this guide

This guide uses the following product models and firmware:

Product	Model	Firmware
FortiGate Cloud	N/A	26.1

Appendix B - Documentation references

- [Fortinet MSSP offerings](#)
- [FortiCloud documentation](#)
- [FortiGate Cloud Administration Guide](#)



www.fortinet.com

Copyright © 2026 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 SVP Legal and above, 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.