

Partner Administration Guide

FortiCloud Services 26.2



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



May 02, 2026

FortiCloud Services 26.2 Partner Administration Guide

57-262-1280848-20260502

TABLE OF CONTENTS

Change Log	4
Introduction	5
Getting started	6
Logging into the account	6
Switching between connected accounts	7
Asset Management	9
Partner aggregated view in the Asset Management portal	9
Selecting accounts	10
Identity & Access Management (IAM)	11
Partner roles	11
Partner role capabilities	11
Connecting with your Customer as a Fortinet Partner using Partner roles	12
Interacting with a Partner role as a Customer	15
Special case: Self-connecting a Partner role in the Fortinet Partner account	20
Partner role FAQ	22
FortiCare	25
Partner aggregated view in the FortiCare portal	25
Bug Tracker	27

Change Log

Date	Change Description
2026-05-02	Initial release.

Introduction

Being a Fortinet Partner allows you to collaborate with Fortinet Inc. to deliver our cybersecurity solutions and services. Partners leverage the [Fortinet Engage](#) program and the [Partner portal](#) to build a profitable and highly differentiated security practice that leverages the industry's best security solutions to drive customer success.

This guide outlines the specialized capabilities of a Partner within the FortiCloud Services suite, including the following portals:

- [Identity & Access Management \(IAM\) on page 11](#)
- [Asset Management on page 9](#)
- [FortiCare on page 25](#)

For common capabilities of the FortiCloud Services suite, see the [FortiCloud Services documentation](#).

Getting started

The following demonstrates the general requirements to get started as a Fortinet Partner:

1. Apply to become a Fortinet Partner and register as a new user. See the documentation included in the Partner portal (<https://partnerportal.fortinet.com>).
2. For connecting and managing your customer accounts, create a FortiCloud account. See the [FortiCloud Account guide](#).
3. Log into your account. See [Logging into the account on page 6](#).
4. Instruct your customer to create a FortiCloud account and create a Partner role for you. When connected through a Partner role, you can get access to a customer's Asset Management, FortiCare, and IAM portals. See [Creating a Partner role as a Customer on page 16](#).
5. Instruct your customer to share an invitation token to connect your accounts with their accounts. See [Connecting a Partner role using a token on page 17](#).
6. Use the token to connect your FortiCloud account to that of your customer. See [Connecting to the Customer using a token-based invitation in Partner roles on page 13](#).
7. Manage a customer's account:
 - Log into your Partner account by visiting forticloud.com to manage your customer's assets, tickets, or users depending upon the permission provided by the customer.
 - Using the Partner role created for you, access your customer's account through the connected account.

See [Logging into the account on page 6](#).

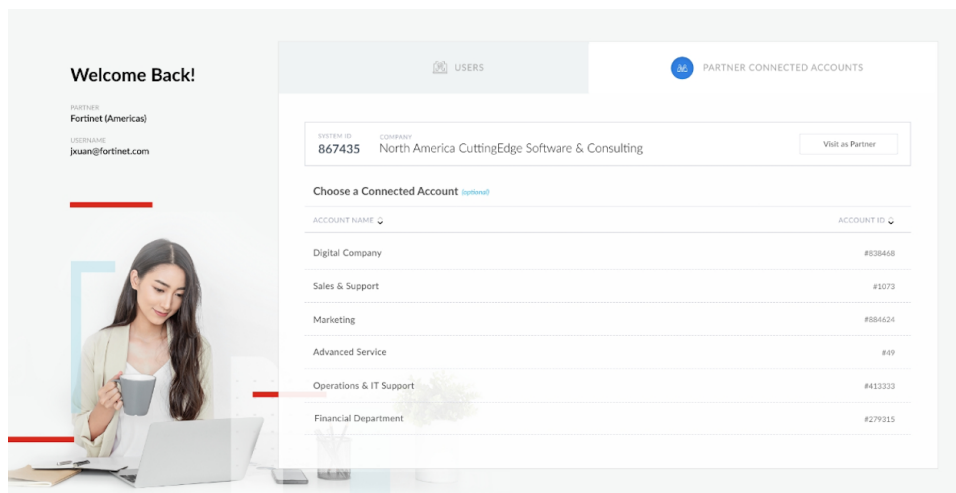
Logging into the account

As a Partner, you can log into your FortiCloud account and access your customer's accounts that you are connected to:

- Visiting as a Partner allows you to access your Partner account to perform management and review purposes, such as the Partner aggregated view. See [Partner aggregated view in the Asset Management portal on page 9](#).
- Selecting any connected accounts lets you access the customer's account through your Partner role. To select other customer's account, you can switch accounts from the account menu in the top right corner.

To access Partner connected accounts:

1. Go to support.fortinet.com.
2. Select *Login Now*. The log in portal opens.
3. Select *Email Login*.
4. Enter your FortiCloud email and password in the *Email* and *Password* fields.
5. Click *Log In*. Accounts linked to your credentials are displayed.
6. Select *Partner Connected Accounts*. Accounts linked to the Partner account are displayed.



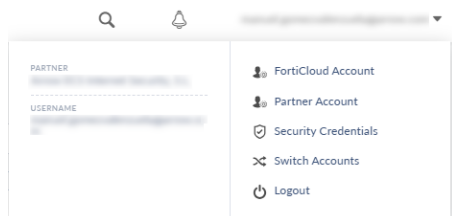
7. Select the account access method:
 - Select *Visit as Partner* to access the Partner account. This allows you to review and overview of your customers' aggregated assets, tickets, accounts, and so on.
 - Hover over an *Account Name* and click *Select* to access a customer connected account. Depending on the permission provided through the Partner role, you may have access to Asset Management, FortiCare, or IAM portals.The portal will open to the *Dashboard*.

Switching between connected accounts

After logging into FortiCloud Services, you can switch between accounts, as needed, using the account dropdown menu. This allows you to easily navigate between the Partner account and the various connected accounts.

To switch to a Partner connected account:

1. Select the profile menu in the top right.



2. Select *Switch Accounts*. The *Switch Accounts* dialog is displayed.

ACCOUNT NAME*	ACCOUNT ID*
Company 1192709	1192709
Fortinet	78997
Fortinet	190932
Fortinet	244020
Fortinet	275858
Fortinet	767418
Fortinet	821230
Fortinet	826665

3. Select the *Partner Connected Accounts* tab. A list of Partner and connected accounts is displayed.
4. Select the account you want to change to:
 - Select *Visit as a Partner* to access the Partner account.
 - Hover over an *Account Name* and click *Select* to access a connected account.
5. A message may display confirming the change between accounts. Click *Continue*. You will be redirected to the *Dashboard* of the selected account.

Asset Management

Asset Management is an easy-to-use portal to register, organize and view all Fortinet products and services in FortiCloud.

New products, licenses, or contracts can be registered and managed using the Asset Management portal. Registered products are displayed in the *Product List* as well as a customizable folder structure called *My Assets*. The *Product List* provides a complete view of all products and services. For each product, the Asset Management portal provides a drill-down view of all the asset-related information including entitlements, support tickets, license and keys, renewals, statistics, and cloud services.

As a Partner, you can access the Asset Management portal to review the assets registered to your customer accounts.

This section includes the following:

- [Partner aggregated view in the Asset Management portal on page 9](#)

For more information on the portal, see the [Asset Management](#) guide.

Partner aggregated view in the Asset Management portal

When accessing the Asset Management portal as a Partner, the *My Products > Product List* is displayed in an aggregated view to include the assets of connected customer accounts.

SERIAL NUMBER #	PRODUCT MODEL #	DESCRIPTION #	COMPANY #	DAYS TO EXPIRATION #	REGISTRATION DATE #
FADVM	FortiADC VMS	FortiADC VMS	company 8	Expired	2021-07-01
FAZ-VMTM	FortiAnalyzer VM	FortiAnalyzer VM	company 8	Expired	2021-06-22
FPENT	FortiPenTest	FortiPenTest	company 8	Expired	2021-07-02
FMG-VM	FortiManager VM	FortiManager VM	company 8	No coverage	2021-06-23
FPVULTM	FortiPAM VM	FortiPAM VM	company 8	Expired	2023-06-02
FAZ-VMTM	FortiAnalyzer VM	FortiAnalyzer VM	company 7	No coverage	2020-11-20
FCTEMS	FortiClient EMS / FortiSASE	FortiClient EMS / FortiSASE	company 7	72 days	2020-09-04
FCTEMS	FortiClient EMS / FortiSASE	FortiClient EMS / FortiSASE	company 7	Expired	2021-01-29
FCTEMS	FortiClient EMS / FortiSASE	FortiClient EMS / FortiSASE	company 7	Expired	2021-02-02

The assets displayed in the aggregated view are dependent on the access permissions of the Partner roles. If a Partner role created by a customer does not provide access to the Asset management portal, then the assets linked to that account will be excluded from the aggregated view.

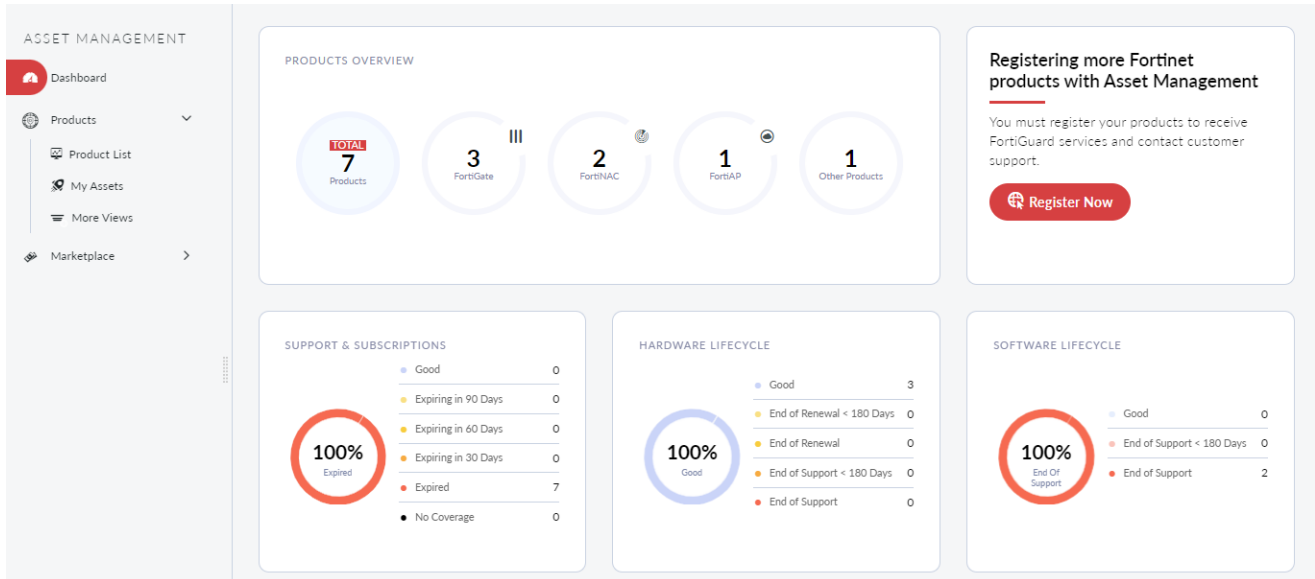


Partner aggregated view is also available for the FortiCare portal's tickets. See [Partner aggregated view in the FortiCare portal on page 25](#).

For more information on Partner roles, see [Partner roles](#) in the Identity & Access Management guide.

Selecting accounts

The navigation menu only displays the *Product List* and *Decommissioned Units* until you select an account from the *Switch Accounts* option.



The options available in the navigation menu will vary depending on your Asset Management resource permissions for the selected account and connected roles. For more information, see [Portals with resource-based permission](#) in the IAM guide.

Asset Management			
Resources			
Entitlement Management	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Asset Maintenance	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Renewal Notice	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Vulnerability List	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Account Services	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Identity & Access Management (IAM)

Identity & Access Management (IAM) is a service to help you control access to FortiCloud Services portals and assets. You can use the portal to manage users, authentication credentials, and asset permissions. Partner roles can be leveraged to connect customer and Partner accounts, and control access permissions.

A Partner role refers to the specific function that a partner assumes within a business relationship or collaborative venture. It provides a standardized and secure way for customers to collaborate with partners, replacing legacy mechanisms with a more scalable and manageable model.

This section includes:

- [Partner roles on page 11](#)

For more information on the portal, see the [IAM guide](#).

Partner roles

A Partner role refers to the specific function that a partner assumes within a business relationship or collaborative venture. It provides a standardized and secure way for customers to collaborate with partners, replacing legacy mechanisms with a more scalable and manageable model.

Partner role capabilities

The Partner roles feature enhances how partners connect with customers, leveraging FortiCloud's IAM user model and permission profiles for fine-grained, secure access management. One Partner account can link to multiple FortiCloud accounts however a FortiCloud account can only link to one Partner account.

Partner roles:

- Are built on the IAM model. See [IAM User Model](#) in the IAM guide.
- Use permission profiles. See [Permission profiles](#) in the IAM guide.
- Replaces the legacy sub-user model with a token-based invitation system.

Each Customer account can have only one Partner role connection at a time. Customers manage these connections from the *Users* page.

Partner role and account details are visible in different sections depending on the login context:

- Customer View: In the *Users* page, Customers can view *Username*, *Type*, *Permission Profile*, *Status*, and so on.

USERNAME/ROLE/ID	DESCRIPTION	TYPE	PERMISSION PROFILE	PERMISSION SCOPE	STATUS	ACTION
test1	test1	IAM User	Full Access	test1	Active	
test2	test2	IAM User	No AM Access	test2	Active	
test3	test3	IAM User	elite_test	MyAssets	Active	
test4	test4	IAM User	SysAdmin	test4	Active	
test5	test5	External IDP Role	Full Access	test5	Active	
test2	test2	Partner Role	SysAdmin	MyAssets	Active	

- **Partner View:** In the Partner *Connected Accounts* page (which is only available to Partners), Partners can view the *Customer Account*, *Partner Role*, *Customer Company*, connection status, and so on.

Account	Partner Role	Company	User Name	Email	Action
test1	PARTNER ROLE	test1	test1	test1@test1.com	
test2	PARTNER ROLE	test2	test2	test2@test2.com	

This section includes the following:

- [Connecting with your Customer as a Fortinet Partner using Partner roles on page 12](#)
 - [Connecting to the Customer using a token-based invitation in Partner roles on page 13](#)
 - [Managing Partner roles as a Partner on page 14](#)
- [Interacting with a Partner role as a Customer on page 15](#)
 - [Creating a Partner role as a Customer on page 16](#)
 - [Connecting a Partner role using a token on page 17](#)
 - [Managing a Partner role as a Customer on page 18](#)



For additional information on Partner roles, see [Partner role FAQ on page 22](#).

Connecting with your Customer as a Fortinet Partner using Partner roles

The following content is intended for Fortinet Partner accounts. Partners may migrate existing connected accounts to new Partner roles, connect new accounts, disconnect existing accounts, and so on.

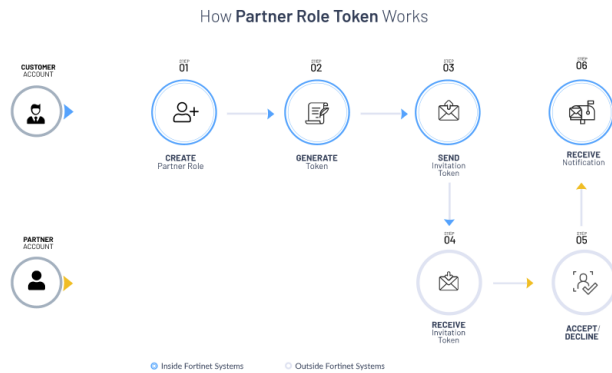
This section includes the following:

- [Connecting to the Customer using a token-based invitation in Partner roles on page 13](#)
- [Managing Partner roles as a Partner on page 14](#)

Connecting to the Customer using a token-based invitation in Partner roles

A new Partner role can be connected to a Partner in combination with the IAM portal and the Partner *Connected Accounts* page. To connect a Partner role, actions must be taken by both the Customer and the Fortinet Partner.

Once the Partner role has been created by the Customer, a token is generated that can be used to connect it to the Partner. The Customer must share the token with the Partner. Then, the Partner can add the token to their account to connect the new role.

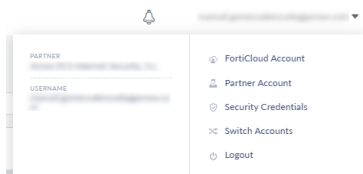


For information on the Customer-side actions, see [Connecting a Partner role using a token on page 17](#).

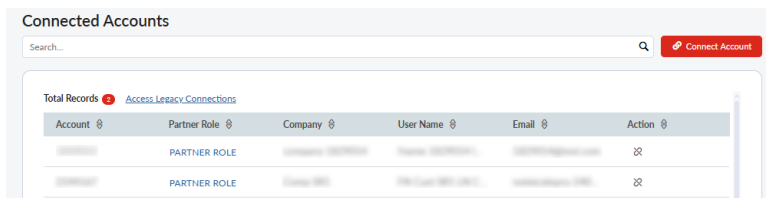
For a video demo, see [Connecting to a Customer using a Token](#).

To connect a Partner role as a Fortinet Partner:

1. Log in as the Partner.
2. In the account menu, select *Partner Account*.



3. Select *Connected Accounts*.



4. Click *Connect Account*.



5. Paste the token that was shared with you and click *Go*.
6. Enter the *Notification Email*.



The *Notification Email* address will be used for renewal notification emails pertaining to this Partner role.

7. Select the acknowledgment.
8. Click *Accept*.

Managing Partner roles as a Partner

Partners can remove the connection with the Customer connected through Partner role by disconnecting them from the Partner *Connected Accounts* page. Furthermore, inactive connected Partner accounts can be disabled from the IAM portal.

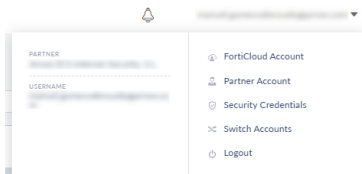
For a video demo, see [Disconnecting from a Customer Account](#).



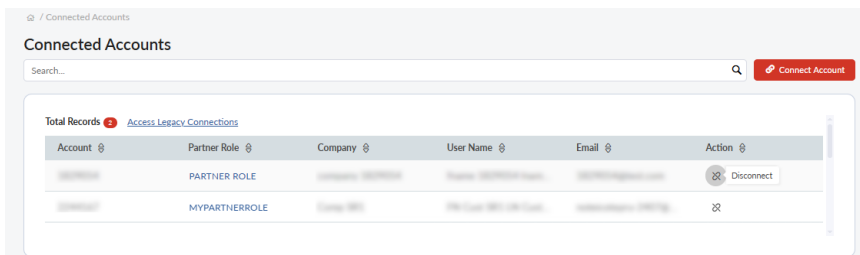
If you have performed the self-connection case of adding a Partner role within your Partner account, the role can also be edited, disabled, and deleted in the *Users* page. See [Special case: Self-connecting a Partner role in the Fortinet Partner account on page 20](#) and [Managing a Partner role as a Customer on page 18](#).

To disconnect a Partner role as the Partner:

1. Log in as the Partner.
2. In the account menu, select *Partner Account*.



3. Click *Connected Accounts*.
4. Select *Disconnect* for the role you want to disconnect.



5. Click *Confirm*.



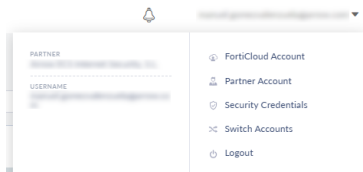
When a Partner role is disconnected, the notification email address will be removed.

Notification renewal email

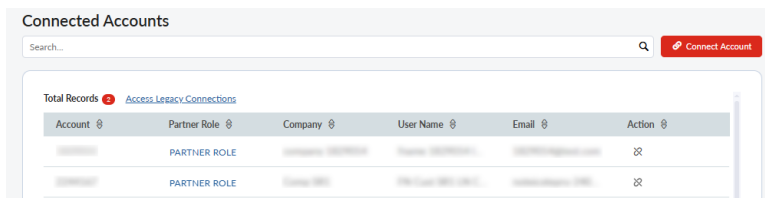
Partners can designate an email address for a Partner role that will receive renewal notification emails. The notification email address can be added to existing Partner roles when viewing the role details.

To edit the Partner role notification email:

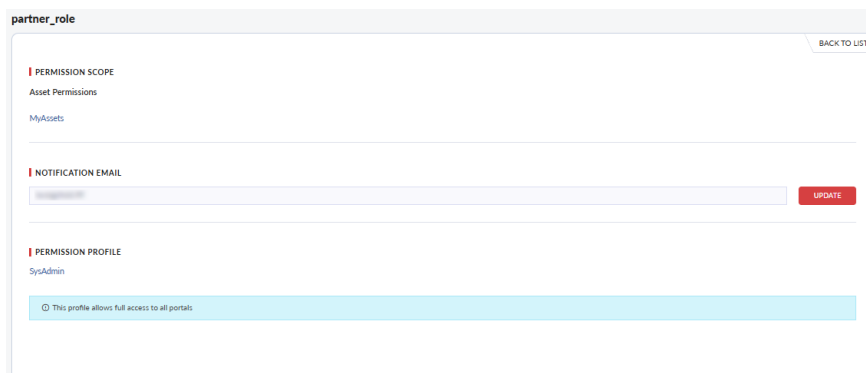
1. Log in as the Partner.
2. In the account menu, select *Partner Account*.



3. Click *Connected Accounts*.



4. Select the Partner role to view the role details.



5. Enter the email address in the *Notification Email* field.
6. Click *Update*.

Interacting with a Partner role as a Customer

The following content is intended for Fortinet Customers. Customers may create new Partner roles, manage existing Partner roles, and so on.

This section includes the following:

- [Creating a Partner role as a Customer on page 16](#)
- [Connecting a Partner role using a token on page 17](#)
- [Managing a Partner role as a Customer on page 18](#)

Creating a Partner role as a Customer

The partner role can be created in the *Users* page. If your account is already connected to a Fortinet Partner through the legacy sub-user method, the legacy sub user connection will be disconnected once the new Partner role has been created. Likewise, if a legacy connection with an inactive Partner is detected, the connection will be disconnected as well when the Partner role has been created.

For a video demo, see [Creating a Partner Role \(Customer View\)](#).



In certain instances, a Partner account or connection may need to be disconnected:

- You can manually disconnect inactive Partners by selecting the role in the *Users* page.
- If a legacy Partner connection using the sub user model with limited permissions is detected, the Partner must first disconnect the connection before you can proceed with creating a Partner role.

See [Managing a Partner role as a Customer](#) on page 18.



Partner roles cannot be added to or configured based on a user group.

To create a Partner role as a Customer:

1. Go to *Permission Profiles*.
2. Create a permission profile with permissions to Asset Management and FortiCare. Alternatively, you can use the default *SysAdmin* permission profile which provides access to the Asset Management, FortiCare, and IAM portals by default. See [Creating a permission profile](#) in the IAM guide.
3. Go to *Users*.
4. Click *Add New > Partner Role*.

New Partner Role

The Partner role enables you to connect a Fortinet Partner to your account with the required access permissions. [Learn more in our help documentation](#).

[BACK TO USERS LIST](#)

ROLE DETAILS

PARTNER ROLE NAME *	DESCRIPTION
Enter Partner Role Name	Enter Description

SELECT A TYPE *

Choose the profile type as Local for limiting the profile to current account and Organization for OU accounts

Local

PERMISSION SCOPE

Select an Asset Folder *

None

PERMISSION PROFILE

Select a Permission Profile *

None

Cancel
Add Role



Only one Partner role is allowed per account.

5. Enter the *Partner Role Name*.
6. Enter a *Description*.

7. Select the *Permission Scope*.
8. Select the *Permission Profile* created in Step 2 or use the *SysAdmin* permission profile.



If the permission profile selected includes portals that do not support Partner roles, the portals will be marked as *Not Supported*.



If the *SysAdmin* profile is selected, the Partner role will have full access to the Asset Management, IAM, and FortiCare portals. By granting IAM permissions to the Partner role, the Fortinet Partner will have access to the IAM portal and will therefore be able to manage users.

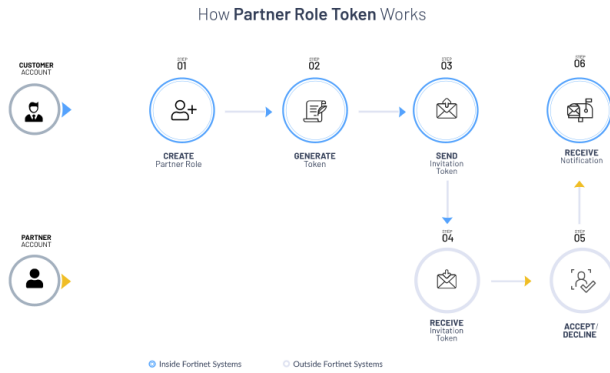
9. Click *Add Role*.

A token is displayed which can be shared with the account to be connected. The token will expire after five days but can be regenerated if needed. See [Connecting a Partner role using a token on page 17](#).

Connecting a Partner role using a token

A new Partner role can be connected to a Partner in combination with the IAM portal and the Partner *Connected Accounts* page. To connect a Partner role, actions must be taken by both the Customer and the Fortinet Partner.

Once the Partner role has been created by the Customer, a token is generated that can be used to connect it to the Partner. The Customer must share the token with the Partner. Then, the Partner can add the token to their account to connect the new role.

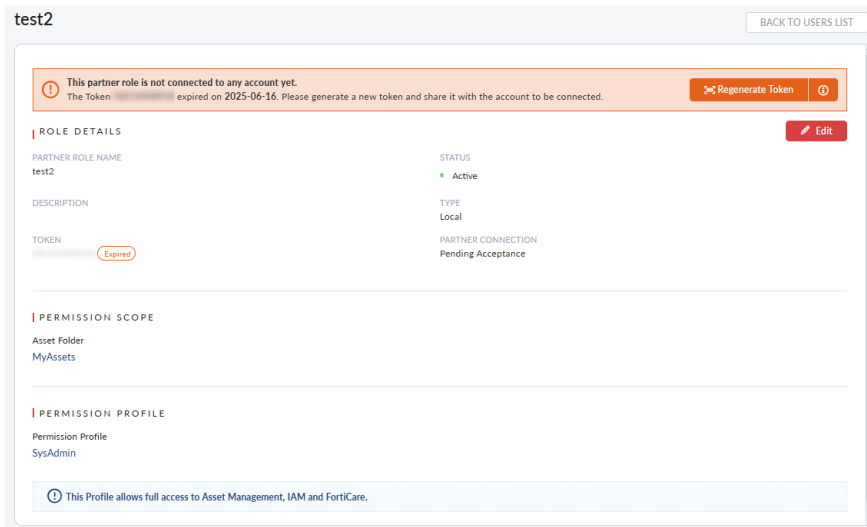


For a video demo, see [Overview of Sharing Token \(Customer View\)](#).

For information on the Partner-side actions, see [Connecting to the Customer using a token-based invitation in Partner roles on page 13](#).

To share a partner role token as the Customer:

1. Go to *Users* and find the Partner role you want to connect.
2. If the token has expired, click *Regenerate Token*.



3. Copy the new token and share it with the account you want to connect with. You may choose to share the token with the Fortinet Partner verbally, through email, and so on.

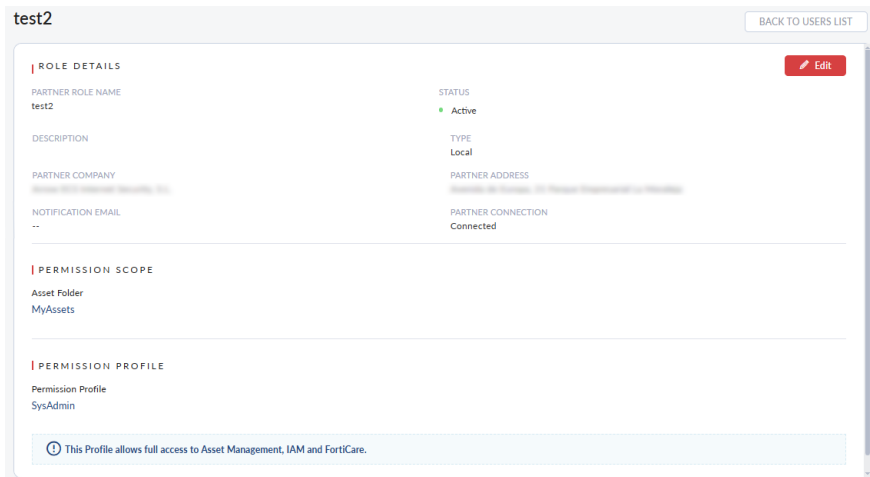
Managing a Partner role as a Customer

The Partner role can be viewed, edited, disabled, and deleted in the *Users* page.

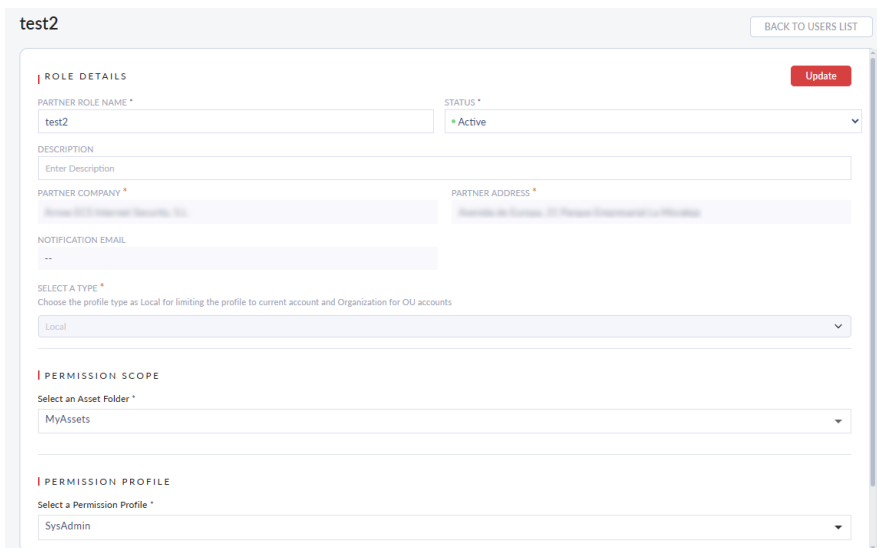
For a video demo, see [Disabling a Partner Role \(Customer View\)](#) and [Deleting a Partner Role \(Customer View\)](#).

To edit a Partner role:

1. Go to *Users*.
2. Select the Partner role.



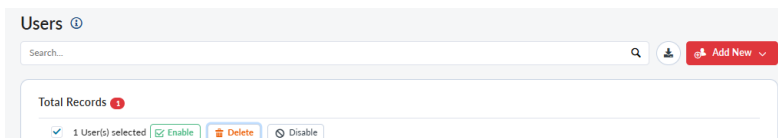
3. Click *Edit*.



4. Edit the fields as required.
5. Click *Update*.

To disable a Partner role in the IAM portal:

1. Go to *Users*.
2. Select a role in the list.



3. Click *Disable*.



Confirm To Disable User

You are about to disable this user. This action will deny the user access to the system. Are you sure you want to continue?

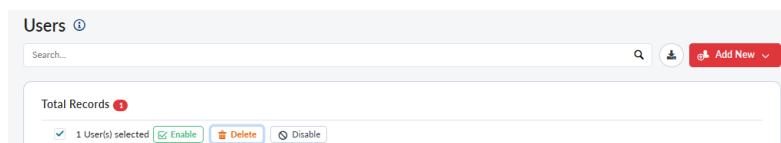
Yes, I Want to Continue.

Cancel

4. Click *Yes, I Want to Continue*.

To delete a partner role:

1. Go to *Users* and find the Partner role you want to delete.
2. Select the role.



3. Click *Delete*. A confirmation dialog is displayed.



Confirm to Delete User

You are about to delete this user. This action cannot be reverted. Are you sure you want to continue?

Yes, I Want to Continue.

Cancel

4. Click *Yes, I Want to Continue*.

Special case: Self-connecting a Partner role in the Fortinet Partner account

If you would like to allow Fortinet Partner users to access your personal Partner account, you can create Partner roles within your Fortinet Partner account.




This self-connection case of adding a role within a Partner account is not related to connecting to a Fortinet Customer and requires a FortiCloud account.

To create a Partner role as a Fortinet Partner:


1. Go to *Permission Profiles*.
2. Create a permission profile with permissions to Asset Management and FortiCare. Alternatively, you can use the default *SysAdmin* permission profile which provides access to the Asset Management, FortiCare,

and IAM portals by default. See [Creating a permission profile](#) in the IAM guide.

3. Go to *Users*.
4. Click *Add New > Partner Role*.

 Only one Partner role is allowed per account. If the account already has a partner role, a dialog is displayed noting that you must contact customer service. You must inform customer service which Partner roles to disconnect and which one you would like to keep.

5. Enter the *Partner Role Name*.
6. Enter a *Description*.
7. Select the *Permission Scope*.
8. Select the *Permission Profile* created in Step 2 or use the *SysAdmin* permission profile.

 If the permission profile selected includes portals that do not support Partner roles, the portals will be marked as *Not Supported*.



If the *SysAdmin* profile is selected, the Partner role will have full access to the Asset Management, IAM, and FortiCare portals. By granting IAM permissions to the Partner role, the Fortinet Partner will have access to the IAM portal and will therefore be able to manage users.

9. Click *Add Role*.
10. If the current Master account is recognized as a Fortinet Inc. Partner, a dialog is displayed. Select whether you want to link the new Partner role to the Fortinet Inc. Partner account. This dialog is not displayed if the Master user has been connected to the Partner through the legacy portal.
If the current account is not the Master account or you decided not to link the new role, a token is displayed which can be shared with the account to be connected. The token will expire after five days but can be regenerated if needed. See [Connecting a Partner role using a token on page 17](#).

Partner role FAQ

This topic discusses frequently asked questions related to the external Partner roles:

- [General questions on page 22](#)
- [Fortinet Partner-specific questions on page 23](#)
- [Customer-specific questions on page 23](#)

General questions

1. What is a Partner role?

A Partner role refers to the specific function that a Partner assumes within a business relationship or collaborative venture. A Partner role allows a Fortinet Partner to securely access and manage a Customer's FortiCloud account through a standardized token-based connection. It replaces the legacy sub-user model and aligns with FortiCloud's Identity and Access Management (IAM) framework. Only one Partner role can exist per Customer account. See [Partner roles on page 11](#).

2. Why was this change introduced?

The Partner role feature replaced the outdated legacy connected accounts model, which required Customers to create sub-users and share credentials manually.

This new model:

- Enables secure, token-based connections.
- Supports fine-grained permission control through permission profiles.
- Improves manageability and transparency of Partner-Customer relationships.

See [Partner roles on page 11](#).

3. What are the key benefits of using the Partner Role?

Key benefits include:

- Stronger Security: No shared credentials
- Simplified Management: One unified IAM-based model
- Granular Permissions: Easily assign or limit access through permission profiles
- Streamlined Migration: Legacy connections can be migrated easily

See [Partner roles on page 11](#).

4. Can Partner roles be assigned to user groups?

No. Partner roles cannot be added to user groups. Each role is created and managed individually.

5. Is the Partner Role connection bidirectional?

No. Partner Role connections are unidirectional. The Partner gains access to the Customer account as per the assigned permission profile. The Customer does not gain access to the Partner's account.

6. Where can I learn more about Partner roles and how to use them?

See the following resources:

- [Partner roles on page 11](#)
 - [Connecting with your Customer as a Fortinet Partner using Partner roles on page 12](#)
 - [Interacting with a Partner role as a Customer on page 15](#)
- [Partner roles overview video](#)

Fortinet Partner-specific questions

1. Can a Partner initiate the connection to a Customer?

No. Only Customers can initiate a Partner role by creating it and sharing the token. The Partner must paste the token into the Partner *Connected Accounts* page to complete the connection.

See [Connecting to the Customer using a token-based invitation in Partner roles on page 13](#).

2. Is this applicable to self-managed Partner accounts?

Yes. Fortinet Partners can use this feature to create self-connected roles within their own accounts for internal team access. See [Special case: Self-connecting a Partner role in the Fortinet Partner account on page 20](#).

3. What happens if my Fortinet Partner account is inactive or terminated?

If a connected Partner account becomes inactive or is deleted, the associated Partner role will be automatically disabled on the Customer's side. The Customer may then choose to connect to a different Partner.

4. Can a Partner have multiple Customer accounts connected through Partner roles?

Yes. A Partner can connect to multiple Customer accounts, each using a unique token-based Partner role setup initiated by the respective Customer.

Customer-specific questions

1. Do I need to take any action as a Customer?

Yes, action is recommended. Customers can perform self-migration starting immediately. Auto-migration occurred on November 15th, 2025 for **Partners linked to master and sub-users with administrative permissions** that were not migrated manually through the legacy connection.

See [Creating a Partner role as a Customer on page 16](#).

2. Can Customers manage the Partner role?

Yes. Customers can:

- View, edit, disable, or delete the Partner role.
- Regenerate and share tokens.
- Disconnect inactive or unwanted Partner connections.

All management is done through the *Users* page in the IAM portal.

See [Connecting a Partner role using a token on page 17](#) and [Managing a Partner role as a Customer on page 18](#).

3. Can I create multiple Partner roles for different Partners?

No. Only one Partner role is allowed per Customer account at a time. To switch Partners, the Customer must first delete the existing Partner role. See [Managing a Partner role as a Customer on page 18](#).

4. Can Customers customize what a Partner can or cannot see?

Yes. Customer can use Permission Profiles to assign role-specific access levels. Customer can restrict access to specific services like Asset Management, IAM, or FortiCare, or limit access to read-only if desired.

See [Creating a Partner role as a Customer on page 16](#) and [Permission profiles](#) in the IAM guide.

5. What happens if the token expires before the Partner uses it?

Tokens are valid for 5 days. If expired, the Customer can regenerate the token from the *Users* page in the IAM Portal and resend it to the Partner.

See [Creating a Partner role as a Customer on page 16](#).

6. Can a Customer revoke Partner access at any time?

Yes. Customers can disable or delete a Partner role at any time from the *Users* page. This will immediately terminate the Partner's access to the account.

See [Managing a Partner role as a Customer on page 18](#).

FortiCare

FortiCare is a user-friendly ticketing system, designed to streamline your ticket management process. The new comprehensive ticketing web interface supports various workflows based on the ticket types to efficiently submit, track, prioritize, and resolve tickets with ease.

As a Fortinet Partner, the FortiCare portal can be used to track customer tickets in an aggregated or account-focused view. Likewise, you can use the Bug Tracker to view active bugs being tracked by the Global Technical Support organization.

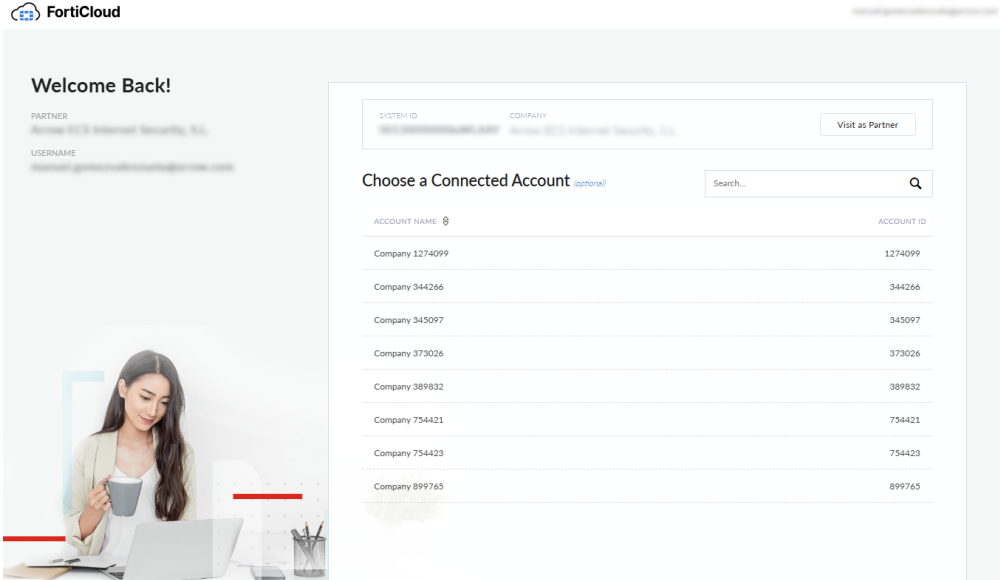
This section includes:

- [Partner aggregated view in the FortiCare portal on page 25](#)
- [Bug Tracker on page 27](#)

For more information on the portal, see the [FortiCare](#) guide.

Partner aggregated view in the FortiCare portal

When a Partner logs in, they must select a connected account to access the registered assets for that account. See [Logging into the account on page 6](#).



The screenshot shows the FortiCare portal interface. On the left, there is a 'Welcome Back!' message with fields for PARTNER (Aruba 123 Internet Security, S.), USERNAME, and a profile picture of a woman. On the right, there is a 'Choose a Connected Account' section. At the top, there are fields for SYSTEM ID and COMPANY, with a 'Visit as Partner' button. Below this is a search bar and a table of connected accounts.

ACCOUNT NAME	ACCOUNT ID
Company 1274099	1274099
Company 344266	344266
Company 345097	345097
Company 373026	373026
Company 389832	389832
Company 754421	754421
Company 754423	754423
Company 899765	899765

These assets are reflected in the FortiCare portal. The FortiCare portal will only display tickets and allow ticket creation for the assets connected to the current connected account being accessed by the Partner. If you want to create or view tickets for assets related to other connected accounts, you can switch using the profile menu. See [Switching between connected accounts on page 7](#).

When creating a ticket, the *Ticket Visibility* pane is displayed for Partner users to select who can view, update, and close the ticket. See [Creating tickets](#) in the FortiCare guide.

When accessing the FortiCare portal as a Partner, the *Tickets > All Tickets* list is displayed in an aggregated view to include the connected Partner roles' assets.

Ticket ID	Subject	Request Type	Creation Date	Close Date	Ticket Type	Account
12345678	Issue with network connectivity	Customer Service	2024-11-20 04:00	2024-11-20	Customer	company 75
87654321	Issue	RMA	2025-05-22 09:16	2025-06-04	Partner	company 345
23456789	Issue with network connectivity	Customer Service	2024-10-24 02:44	2024-11-03	Customer	company 345
34567890	Issue	Customer Service	2025-05-22 01:31	2025-06-01	Customer	company 344
45678901	Issue with network connectivity	Customer Service	2025-05-14 00:40	2025-05-20	Customer	company 344
56789012	Issue with network connectivity	Customer Service	2025-05-13 02:30	2025-05-19	Customer	company 344
67890123	Issue with network connectivity	Customer Service	2025-04-15 02:08	2025-04-24	Customer	company 344

The tickets displayed in the aggregated view is dependent on the access permissions of the Partner roles. If a Partner role does not have access to the FortiCare portal, then the tickets linked to that account will be excluded from the aggregated view.

For example, there are three Partner roles connected to Partner X with the following permissions:

- Role A has access to the FortiCare portal, the IAM portal, and the Asset Management portal.
- Role B has access to the Asset Management portal and has been denied access to the FortiCare portal.
- Role C has access to the FortiCare and the ELA portal.

When Partner X logs into the FortiCare portal and chooses *Visit as Partner*, they will see an aggregated list of Role A and Role C's tickets only.

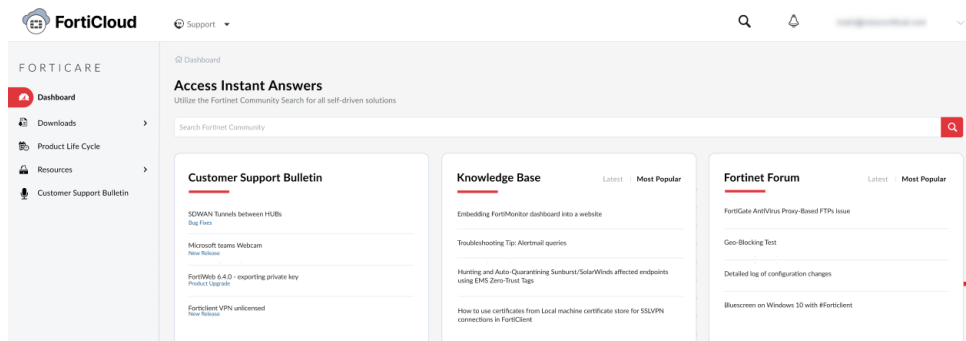


Partner aggregated view is also available for the Asset Management portal's assets. See [Partner aggregated view](#) in the Asset Management portal on page 9.

For more information on Partner roles, see [Partner roles](#) in the Identity & Access Management guide.

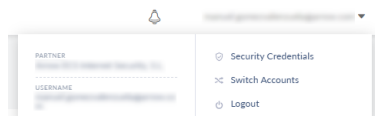
Partners without a FortiCloud account and connected accounts

If a Fortinet Partner account that does not have a FortiCloud account or any connected accounts, the Partner will be directed to the FortiCare portal upon logging in. The *Services* dropdown menu will be unavailable for switching to other portals.



💡 If the Fortinet Partner account does not have a FortiCloud account but does have connected accounts, the *Services* menu is available for navigating to the general sections of the FortiCare portal, such as *Resources*, *Product Lifecycle*, *Downloads*, and *Customer Support Bulletin*. You also get access to the Knowledge Base, CSBs, and Fortinet forums. See *Partner aggregated view* in the *Asset Management* portal on page 9.

Furthermore, the *FortiCloud Account* and *Partner Account* options are not included in the account dropdown menu.



Bug Tracker

The FortiCare bug tracker provides an overview of active bugs being tracked by the Global Technical Support organization. The *Bug Tracker* page is only available to Partners.

The bug tracker lists high level information in the *Bug Tracker* list, such as the *Category*, *Known Fixed Release*, *Status*, and a brief *Summary*. The column selector icon can be used to select which columns to make visible.

Bug Tracker

Bug tracker is aimed to facilitate your work by providing an overview of active bugs being tracked by the Global Technical Support organization [More Info](#)

Search: Export

Total Records **425**

BUG#	CATEGORY	PROJECT	KNOWN FIXED RELEASE	STATUS	SUMMARY
1164092	All	FortiOS	7.2.12-1753	acknowledged	B1740: On NF7 platforms, a change in the destination MAC address or fib change may cause traffic to stop on certain interfaces
1161023		FortiOS	7.6.4-3564, 8.0.0-0026 0027	resolved	B2794: Groups of Wi-Fi clients are not retained after roaming to a different FAP
1160819		FortiManager	7.4.8-2696, 7.6.4-3527	resolved	B3524 - command 'system.local-in-policy' is not permitted if no valid license
1154383		FortiManager	7.6.4-3528	resolved	B3516 - Unable move policy package & move/delete folders. Error "cannot get pkg path"
1153119		FortiManager	7.4.7-2674, 7.6.4-3520	resolved	B3515: FortiManager (workspace mode) unable to Add FGT HA-Model device via API if included commit script
1152640		FortiManager	7.4.8-2698, 7.6.4-3527	resolved	Fail to install due to "Must set at least one port (default port=443) or enable ssl inspect-all" error
1151713		FortiOS	7.4.8-2793, 7.6.4-3543, 8.0.0-0010	acknowledged	B2726: FortiAP offline due to ERR: NO MEM for USER_LOCAL_MSG
.....					R2776: Annihilation newelf crash on FG-120G

Select a bug *Summary* or *Bug#* to view more detailed information.

947237 | Multiple Issues Observed with Fortiportal 7.0.5

STATUS: KNOWN FIXED RELEASE
resolved 7.0.7.0221, 7.2.1.1061, 7.2.2.1063

DESCRIPTION
1. Looks like the portal is sending all web traffic via the proxy, including the API calls to FAZ/FMG. This would not work as those proxies are Internet proxies for customer. They dont expect the FMG/FAZ out go via web Proxy and they are bring to use it for Internet out only. Dont find a way in CLI to change that behaviour. 2. License update failed sometimes 3. CLI does not allow a host route (or even a route with /31 mask) to be added 4. It was not possible to add a second or third NTP server.

To export the bug tracker list:

1. Go to *Bug Tracker*.
2. Select the file format you want to export from the dropdown menu:
 - *Excel File*
 - *CSV File*

The file is saved to your device.



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 Chief Legal Officer, 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.