

FortiMail Cloud: User Import from Microsoft 365 Deployment Guide

Version 7.4



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 COOKBOOK

<https://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<https://www.fortinet.com/training>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



TABLE OF CONTENTS

Change Log.....	4
Introduction	5
Configuring MS365 accounts	5
Configuring FortiMail Cloud with Tenant ID, Application ID, and Application Secret.....	11

Change Log

Date	Change Description
2024-03-01	Initial release

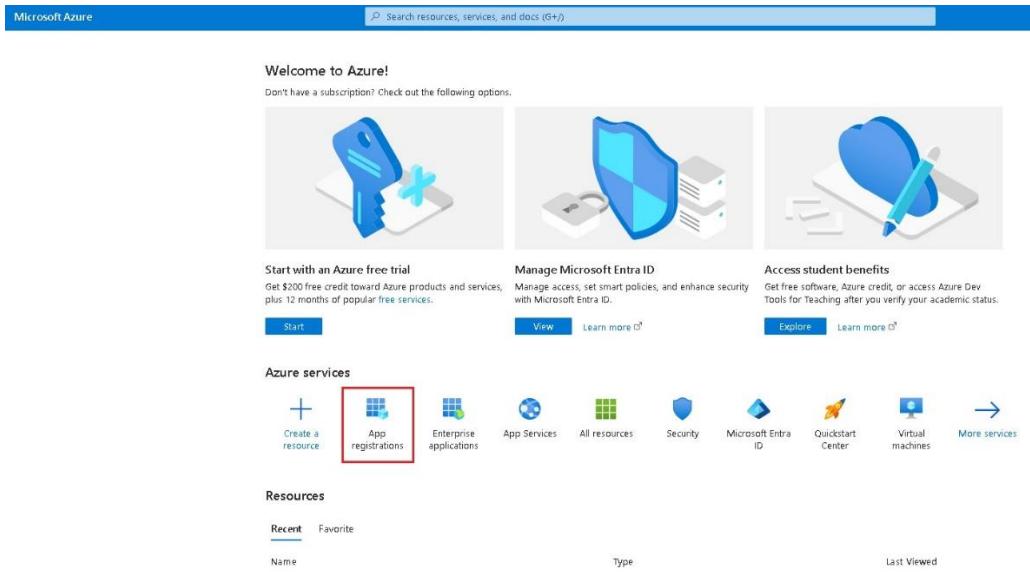
Introduction

This document describes how to import users from Microsoft 365 to FortiMail.

Configuring MS365 Accounts

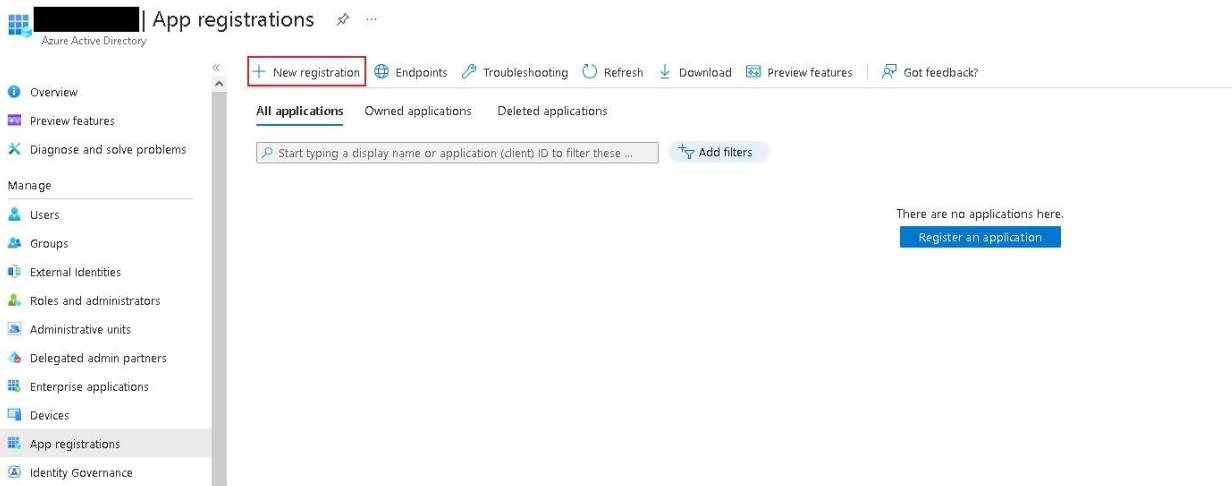
To register the application in Azure admin center

1. Log in to <https://portal.azure.com> and Select *App registrations*. (You may also search it in the search bar).



The screenshot shows the Microsoft Azure portal homepage. At the top, there is a search bar and a 'Welcome to Azure!' message with three promotional cards: 'Start with an Azure free trial', 'Manage Microsoft Entra ID', and 'Access student benefits'. Below these are sections for 'Azure services' (with 'App registrations' highlighted by a red box) and 'Resources' (Recent and Favorite). The 'App registrations' section shows a table with columns for Name, Type, and Last Viewed, with a note 'There are no applications here.' and a 'Register an application' button.

2. Select *New registration*.



The screenshot shows the 'App registrations' page in the Azure Active Directory portal. The left sidebar shows 'Manage' sections: Overview, Preview features, Diagnose and solve problems, Users, Groups, External identities, Roles and administrators, Administrative units, Delegated admin partners, Enterprise applications, Devices, App registrations (which is selected and highlighted with a red box), and Identity Governance. The main area has a header with 'New registration', 'Endpoints', 'Troubleshooting', 'Refresh', 'Download', 'Preview features', and 'Got feedback?'. Below the header are tabs for 'All applications', 'Owned applications', and 'Deleted applications'. A search bar says 'Start typing a display name or application (client) ID to filter these ...' and a 'Add filters' button. A note says 'There are no applications here.' and a 'Register an application' button is visible.

3. Register an application, you may select the supported account type based on your requirements.

Register an application

* Name

The user-facing display name for this application (this can be changed later).

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only ([REDACTED] - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

 Select a platform

e.g. <https://example.com/auth>

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

[Register](#)

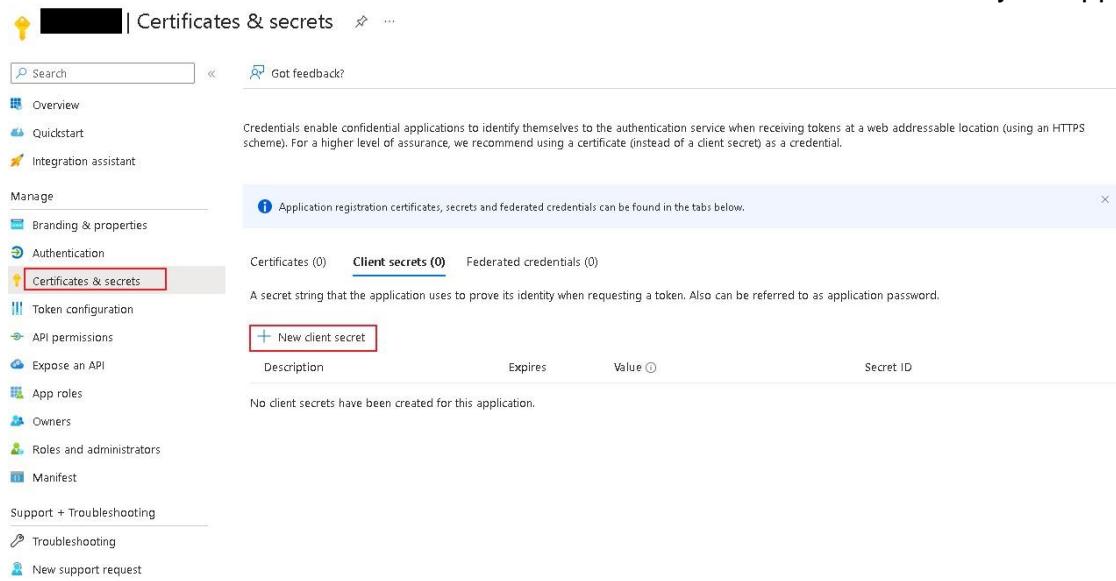
Once completed, you will find your *Application ID* and *Tenant ID* here.

The screenshot shows the Azure portal interface for an application registration. The left sidebar has 'Overview' selected. The main content area shows the following details:

Essentials	
Display name	: [REDACTED]
Application (client) ID	: [REDACTED]
Object ID	: [REDACTED]
Directory (tenant) ID	: [REDACTED]
Supported account types	: My organization only

On the right, there are links for 'Client credentials', 'Redirect URIs', 'Application ID URI', and 'Managed application in ...'. At the bottom, there are 'Get Started' and 'Documentation' buttons.

4. Go to *Certificates & secrets* > *New client secret* to create a secret for your application.



Search | Certificates & secrets | ...

Overview Quickstart Integration assistant

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Manage

- Branding & properties
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators
- Manifest

Support + Troubleshooting

Troubleshooting New support request

Application registration certificates, secrets and federated credentials can be found in the tabs below.

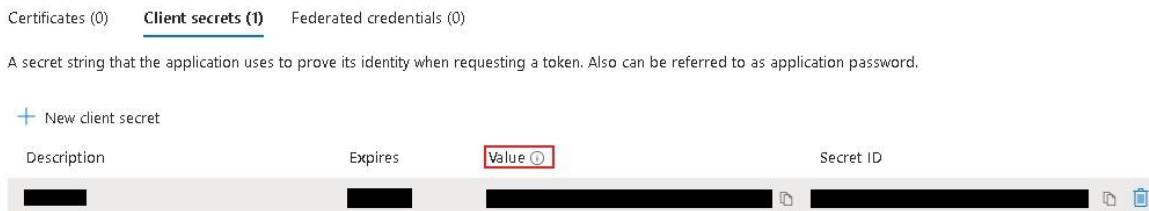
Certificates (0) Client secrets (0) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Warning: Once the secret has been created, you must copy and save your secret value. It will not be shown again after you close the page.



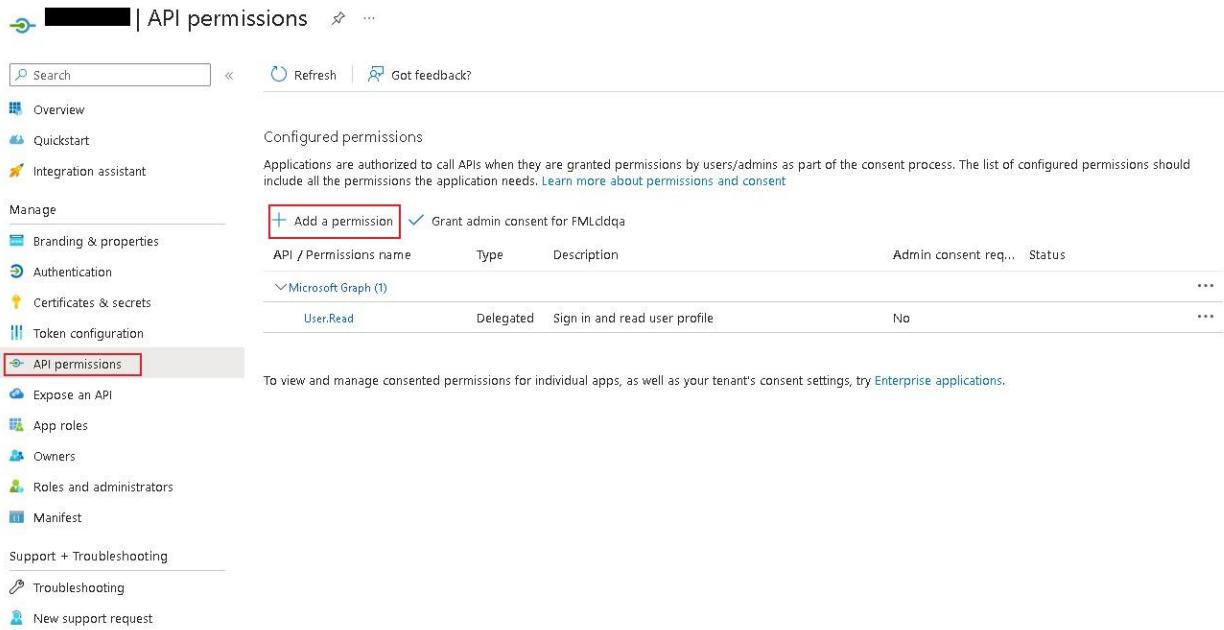
Certificates (0) Client secrets (1) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

5. Go to *API permissions* > *Add a permission* to set up API permissions for the application.



Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (1)	User.Read	Delegated	Sign in and read user profile	No

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

Add the following permissions for the admin in MS365:

- User.Read
- User.Read.All

Note that *User.Read* is added by default. You may find the other three permissions under *Microsoft Graph > Application permissions*.

Request API permissions

Select an API

[Microsoft APIs](#) APIs my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

 **Azure Communication Services**
Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams

 **Azure Rights Management Services**
Allow validated users to read and write protected content

 **Azure Service Management**
Programmatic access to much of the functionality available through the Azure portal

 **Azure Storage**
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

 **Data Export Service for Microsoft Dynamics 365**
Export data from Microsoft Dynamics CRM organization to an external destination

 **Dynamics 365 Business Central**
Programmatic access to data and functionality in Dynamics 365 Business Central

 **Dynamics CRM**
Access the capabilities of CRM business software and ERP systems

 **Flow Service**
Embed flow templates and manage flows

 **Intune**
Programmatic access to Intune data

 **Office 365 Management APIs**
Retrieve information about user, admin, system, and policy actions and events

 **Power BI Service**
Programmatic access to Dashboard resources such

 **SharePoint**
Interact remotely with SharePoint data

Request API permissions

X

[All APIs](#)

 **Microsoft Graph**
<https://graph.microsoft.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Search for *User.Read* to find the required permissions.

Request API permissions

X

◀ All APIs

Microsoft Graph

<https://graph.microsoft.com/> Docs

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

User.Read	Permission	Admin consent required
IdentityRiskyUser		
User (1)		
<input checked="" type="checkbox"/> User.Read.All ⓘ	Read all users' full profiles	Yes
<input type="checkbox"/> User.ReadBasic.All ⓘ	Read all users' basic profiles	Yes
<input type="checkbox"/> User.ReadWrite.All ⓘ	Read and write all users' full profiles	Yes

Once you have added all the permissions, click *Grant admin consent for (your application)*. The permission status will change to *Granted for (your application)*.

 | API permissions

Search | Refresh | Got feedback?

Overview | Quickstart | Integration assistant

Successfully granted admin consent for the requested permissions.

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization.

Configured permissions

APIs are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for [REDACTED]

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (2)				...
User.Read	Delegated	Sign in and read user profile	No	Granted for [REDACTED] ...
User.Read.All	Application	Read all users' full profiles	Yes	Granted for [REDACTED] ...

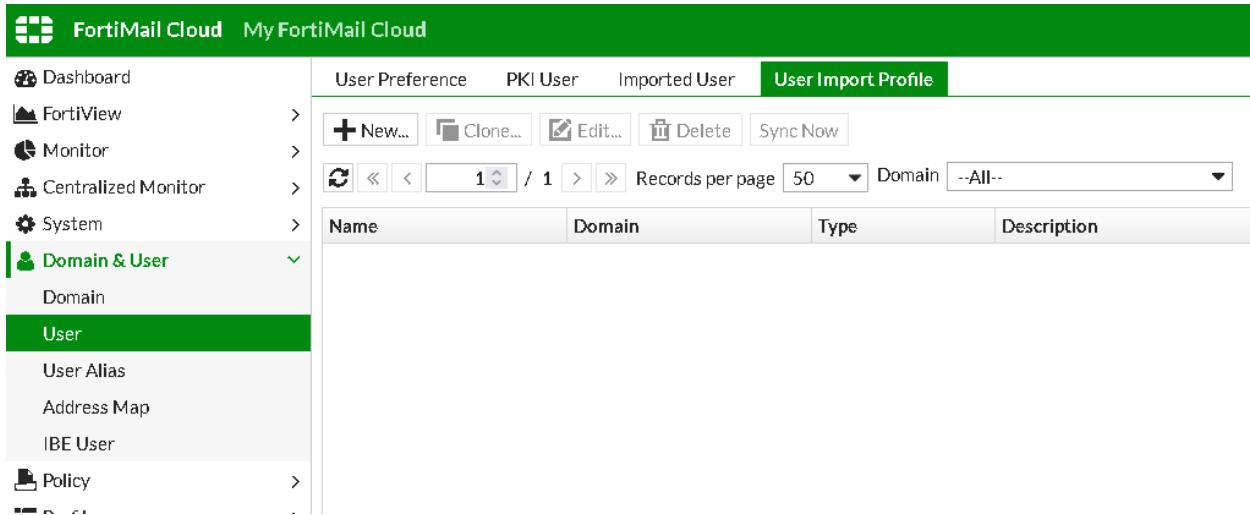
To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

Support + Troubleshooting | Troubleshooting | New support request

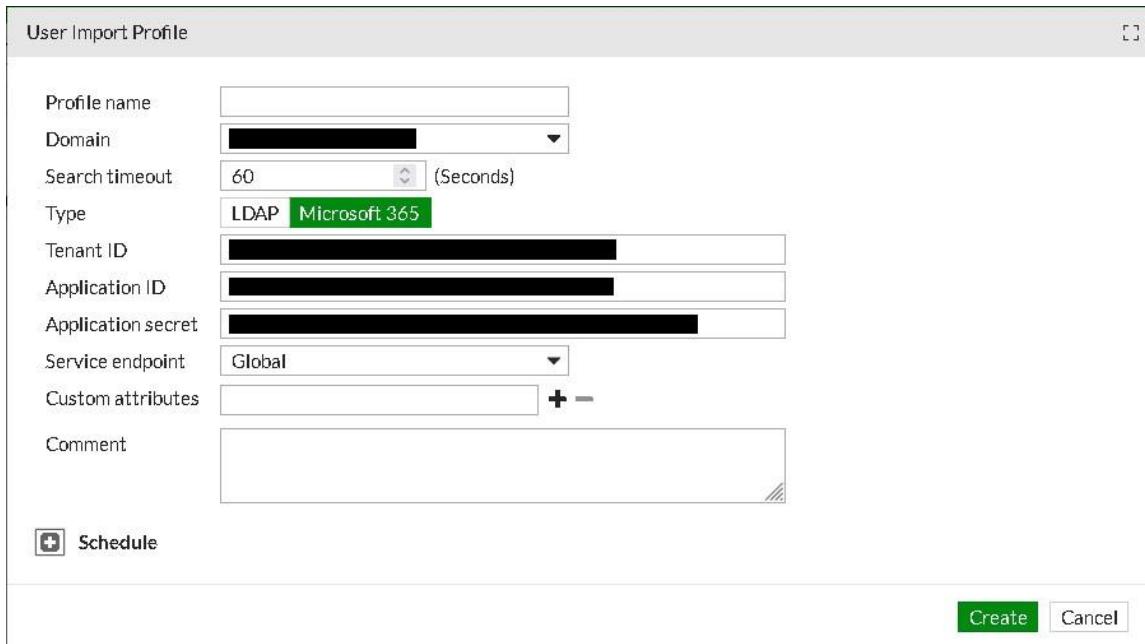
Configuring FortiMail Cloud with Tenant ID, Application ID, and Application Secret

Note: This feature requires MSSP license.

1. Go to your FortiMail Cloud instance, then go to *Domain & Users > User > User Import Profile*.



2. Fill in your Azure AD application info: *Tenant ID*, *Application ID*, and *Application Secret* value.



Profile name	<input type="text"/>
Domain	<input type="text"/>
Search timeout	60 <input type="button"/> (Seconds)
Type	LDAP <input checked="" type="radio"/> Microsoft 365 <input type="radio"/>
Tenant ID	<input type="text"/>
Application ID	<input type="text"/>
Application secret	<input type="text"/>
Service endpoint	<input type="text"/>
Custom attributes	<input type="text"/> <input type="button"/> <input type="button"/>
Comment	<input type="text"/>
<input type="checkbox"/> Schedule	
<input type="button"/> Create <input type="button"/> Cancel	

Once created, you can either configure the schedule to synchronize or manually synchronize the user list by clicking on *Sync Now*. It will take some time to synchronize and the status will change to *syncing*.

User Preference PKI User Imported User **User Import Profile**

Sync Now

Selected: 1 / 1

Name	Domain	Type	Description	Schedule	Sync Status	Last Sync
test	[REDACTED]	Microsoft 365		Not Scheduled	[REDACTED]	[REDACTED]

After synchronized, the status will change to succeeded. And you will be able to check and manage the user list from *Domain & Users > User > Imported User* under corresponding domain.

FortiMail Cloud My FortiMail Cloud

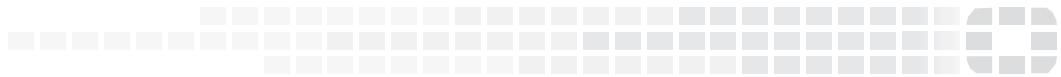
User Preference PKI User **Imported User** User Import Profile

Imported User

Stat...	Display Name	Email	Type	Profile
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	test
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	test
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	test
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	test
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	test
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	test
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	test



High Performance Network Security



Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.