

# Administration Guide

Identity & Access Management 25.2



**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](mailto:techdoc@fortinet.com)



May 03, 2025

Identity & Access Management 25.2 Administration Guide

57-252-1142352-20250503

# TABLE OF CONTENTS

<b>Change Log</b>	<b>6</b>
<b>Introduction</b>	<b>7</b>
Key Features	7
What's new in version 25.2	8
<b>Requirements</b>	<b>9</b>
<b>Identity &amp; Access Management Portal</b>	<b>10</b>
Permission Profiles	10
Users	11
User Groups	11
Migrate Sub Users	12
<b>User management models</b>	<b>13</b>
Basic function mode	13
Advanced mode	13
Sub User Model	13
IAM User Model	14
IAM user types	14
Feature comparison chart	15
<b>Permission profiles</b>	<b>16</b>
Portals with resource-based permission	16
Asset Management	17
IAM	17
FortiCare	18
Permission scope	19
Creating a permission profile	19
Managing permission profiles	21
Editing a permission profile	22
Disabling a permission profile	23
Deleting a permission profile	23
<b>Users</b>	<b>24</b>
IAM users	24
Adding IAM users	25
Managing IAM users	29
Validating IAM users	32
Logging in as an IAM user	35
Migration of existing users	36
API users	38
Adding an API user	39
Managing API users	40
Accessing FortiAPIs	41
External IdP roles	43
Adding external IdP roles	44
Selecting IdP roles	45

Bulk updating users .....	47
<b>User groups .....</b>	<b>49</b>
Adding an IAM user group .....	49
Managing IAM user groups .....	50
Editing user groups .....	51
Adding and removing users .....	52
Updating user group permission .....	53
<b>Migrating sub users .....</b>	<b>54</b>
FortiGate Cloud Legacy users .....	54
<b>Account management .....</b>	<b>57</b>
My Account .....	57
Account Profile .....	58
Account Preferences .....	59
Creating connected accounts (Partners) .....	61
User Information .....	62
Security Credentials .....	63
Password .....	63
Contacts .....	65
Two-Factor Authentication .....	70
<b>Organization user management .....</b>	<b>78</b>
Enabling Organizations .....	78
Permission scope with Organizations .....	80
Local and Organization scope .....	80
Available and selected scope .....	81
Permission profiles within Organizations .....	82
Creating users, user groups, and roles within Organizations .....	84
Logging into an OU account .....	89
OU context switch .....	90
<b>External IdP .....</b>	<b>92</b>
Enrolling for external IdP .....	92
Enrolling with Okta .....	93
Enrolling with Microsoft Entra ID .....	95
Configuring external IdP .....	97
Configuring with Okta .....	98
Configuring with Entra ID .....	98
Adding external IdP roles to the application .....	99
Adding roles in Okta .....	99
Adding roles in Entra ID .....	102
Setting a co-exist end date .....	104
Troubleshooting external IdP .....	105
Verifying SAML assertion values with SAML tracer .....	105
FortiCloud errors .....	107
SAML login portal errors .....	109
The option to add an External IdP Role in the FortiCloud IAM portal is missing .....	110
Permission details of an external IdP role display Not Supported for some of the cloud portal permissions even though they are enabled in permission profile .....	110

---

<b>FAQ .....</b>	<b>111</b>
General questions .....	111
IAM users .....	111
External IdP roles .....	112
Legacy sub accounts .....	113

## Change Log

Date	Change Description
2025-05-03	Initial release.

# Introduction

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

## Key Features

### Permission model

The permission model has been updated with multi-dimensional permission model to provide fine grained control and easy of use. It comes with following two factors:

- *Permission Profile*: Defines the enabled portals and the access permissions available to an assigned user. Instead of assigning portal permissions directly when creating an IAM user, external IdP role, and so on, the user is assigned to a permission profile. The permission profile must be created before being assigned to a user. Permission profiles can be assigned to multiple users and user groups.
- *Permission Scope*: The permission scope defines the scope of access within the account. Management of the account is dependent on the available and selected scope.

### IAM user

The IAM user type provides more control and flexibility when assigning user permissions. Save time creating new users by applying the permissions of an existing user to a new user or adding the user to a group. Account administrators can temporarily disable vulnerable IAM users and enforce Two-Factor Authentication at the account level. Migrate sub users to the IAM portal to manage all of your users in one place.

### User Groups

Organize IAM users into user groups to assign portal and asset permissions to multiple users at the same time. You can create a group based on the user roles, asset permissions, or any other category of your choosing. Remove a user from a group without deleting their profile from the portal or temporarily disable a vulnerable group.

### IAM API user

The IAM portal lets you quickly create and manage IAM API users for programmatic access to the API. IAM API user access types are specific to each portal.

### External IdP roles

External IdP roles allow IdP users to log in to a cloud portal with their organization's ID provider. External IdP roles allow you to create one role for many users while leveraging all of the benefits of the IAM user type. One account can have more than one external IdP role. User accounts with multiple roles are required to select a role before they can access a portal.

## Multi-factor Authentication (2FA)

Two-Factor Authentication is fast and easy to configure. Users can choose to receive Two-Factor Authentication security codes sent to them through FortiToken, SMS, email, or a third-party authenticator each time they log in.

## What's new in version 25.2

Identity & Access Management version 25.2 includes the following new features. See the [FortiCloud Services Release Notes](#) for more information.

### External IdP role permission profile updates

When creating or viewing an external IdP role, if the permission profile selected includes portals that do not support external IdP, the portals will be marked as *Not Supported*. See [Adding external IdP roles on page 44](#) and [Troubleshooting external IdP on page 105](#).

### Log in and password reset UI updates

When logging into an account or resetting an account password, the option to hide or display the password is available. Likewise, when resetting the password, password criteria, such as necessary character length, are listed. As you reset the password, the criteria will update to confirm which criteria have been successfully included and which are still outstanding. See [Logging in as an IAM user on page 35](#) and [Adding IAM users on page 25](#).

# Requirements

The following items are required to use the Identity & Access Management portal:

- FortiCloud Account, IAM user, or external IdP role
- Supported Browser



The IAM portal is only available in English at this time. For information on language support and supported browsers, see the [Release Notes](#).

---

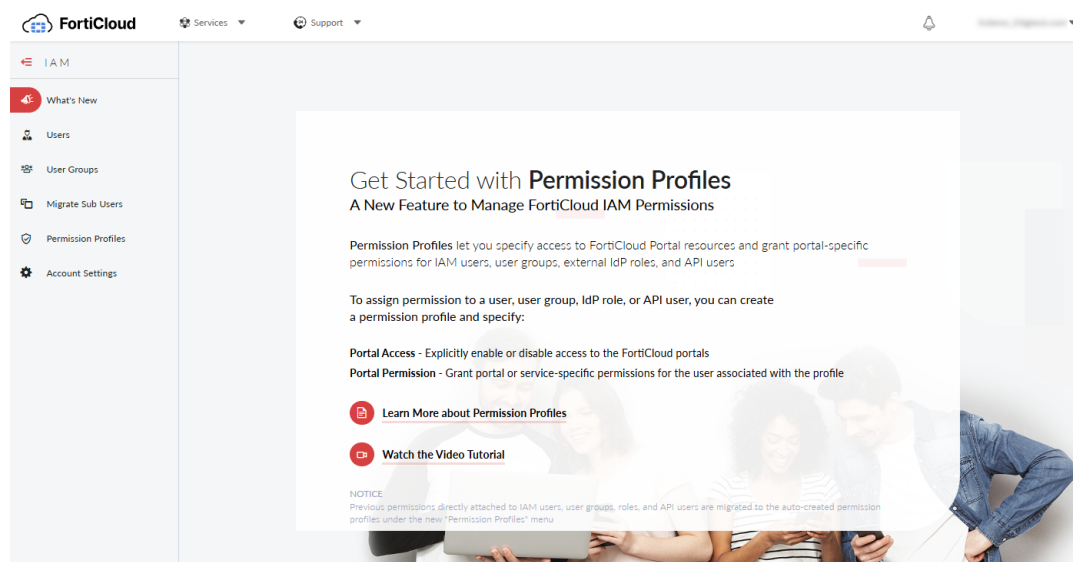
# Identity & Access Management Portal

The navigation menu provides access to features for adding and managing users and user groups.



Select the search icon in the top banner to perform a search for user information in the entire Identity & Access Management portal. Select the *Search* field in the page to perform a search within the current page.

Navigate through the Identity & Access Management portal by selecting one of the available pages in left-hand navigation menu.



## Permission Profiles

The *Permission Profiles* page displays the list of permission profiles. Permission profiles are necessary for the creation of IAM users, user groups, API users, and IdP roles. The Permission Profiles page can be accessed from the left-hand navigation tree. See [Permission profiles on page 16](#).

**Permission Profiles** ⓘ

Search... Q Disable Delete Add New

Total Records **4**

<input type="checkbox"/>	PROFILE NAME ⓘ	PROFILE DESCRIPTION ⓘ	TYPE ⓘ	# OF ACCESSIBLE PORTALS ⓘ	CRE
<input type="checkbox"/>	SysAdmin	Default profile <span>System Built-In</span>	N/A	3/58	
<input type="checkbox"/>	AM_FlexVM_Admin_Users	AM and FlexVM Admin API Users	Local	2/58	202
<input type="checkbox"/>	MS TEST Profilename		Local	0/58	202
<input type="checkbox"/>	ReadOnlyAccess-FlexVM-AMPortal		Local	2/58	202

## Users

The *Users* page displays the list of users and the user's details including *Username*, *Type*, *Permission Profile*, *Group*, and *Status*. Use this page to add and delete users, or temporarily disable a user. Click the user's *Full Name* to edit their profile, update their permission profile, and reset their password. See [Users on page 24](#).

**Users** ⓘ

Search... Q Add New

Total Records **7**

<input type="checkbox"/>	USERNAME/ROLE/ID ⓘ	DESCRIPTION ⓘ	TYPE ⓘ	PERMISSION PROFILE ⓘ	PERMISSION SCOPE ⓘ	STATUS ⓘ	ACTION
<input type="checkbox"/>	iam_fcdemo3		IAM User	ReadOnlyAccess-FlexVM-...	MyAssets	Active	<span>ⓘ</span> <span>🗑️</span>
<input type="checkbox"/>	mstestIAMid		IAM User	MS test - MS TEST Profil...	MyAssets	Active	<span>ⓘ</span> <span>🗑️</span>
<input type="checkbox"/>	abctest		IAM User	MS TEST Profilename	MyAssets	Active	<span>ⓘ</span> <span>🗑️</span>
<input type="checkbox"/>	DocUser		IAM User	SysAdmin	MyAssets	Active	<span>ⓘ</span> <span>🗑️</span>
<input type="checkbox"/>	test1	test1	API User	SysAdmin	MyAssets	Active	<span>ⓘ</span> <span>🗑️</span>
<input type="checkbox"/>			API User	AM_FlexVM_Admin_Users	MyAssets	Active	<span>ⓘ</span> <span>🗑️</span>

## User Groups

The *User Groups* page displays a list of user groups in the portal. You can add users, disable a group, or delete a group directly from the page. Click a user group to view and edit the group's users and permission profile. See [User groups on page 49](#).

User Groups ⓘ

Search...

🔍

⌛ Disable

🗑 Delete

➕ Add User

👤 Add IAM User Group

Total Records ⓘ 1

<input type="checkbox"/>	GROUP NAME ⓘ	NUMBER OF USERS ⓘ	DESCRIPTION ⓘ	UPDATED ⓘ	STATUS ⓘ
<input type="checkbox"/>	MS test	1	ms test manual	2024-10-03	Active

## Migrate Sub Users

The *Migrate Sub Users* wizard guides you through the process of migrating a sub user to an IAM user. After the migration is complete, the sub user account is converted to an IAM user. You cannot revert a sub user after the process is complete. See [Migrating sub users on page 54](#).

1. Sub User Migration Agreement

PLEASE READ THE FOLLOWING INFORMATION CAREFULLY:

- Following migration, current Sub User(s) will be automatically removed from your FortiCloud account
- Newly created IAM users will need to set new Security Credentials (password and token) for themselves
- IAM user support can differ from portal to portal, please verify your permission and access once the migration is complete
- Some Cloud Portals don't currently support IAM users

☐ I have read, understood and accepted the statements above

Next

# User management models

IAM user accounts are similar to FortiCloud accounts. The legacy Sub User Model allows full and limited permissions for access and assets to individual users. The IAM User Model uses permission profiles for more control and improved security.

## Basic function mode

The basic functionality for the Identity & Access Management portal includes all of the major features, including:

- Permission profiles
- IAM users
- IAM user groups
- Sub user migration
- External IdP roles
- Access to account management

## Advanced mode

The advanced management mode of the Identity & Access Management portal includes the same capabilities as the basic function mode, with the addition of organization support. See [Organization user management on page 78](#).

## Sub User Model



This model will be deprecated in the near future. It is strongly recommended that you use the IAM User Model to take full advantage of the new features.

---

The Sub User Model has two types of user: The master user (or Account Owner) and sub user. The master user is the person who created the FortiCloud account. Master users have full Admin permissions in all of the portals associated with the FortiCloud account including:

- Creating users
- Assigning full admin or limited access permissions and assets to sub users



The Sub User Model only supports one master user for the account. The master user's email address must be unique.

Master user's can change their email address as long as the new email address remains unique. A master user can change their email address up to five times in a 24-hour period.

---

A master user can assign *Full Access* or *Limited Access* permissions to a sub user as well as the devices the sub user can access. Assigning *Full Access* permissions to sub users grants them the same permissions as the master user with limitations. *Limited Access* allows the master user to select the sub user's permissions and assets. See [User permissions](#) in the Asset Management Administration Guide for more information on the different access levels.

Only the master user can access the Identity & Access Management portal and make changes, such as migrating sub users to IAM users. The sub user cannot access the portal regardless if they have *Full Access* or *Limited Access*.

## IAM User Model

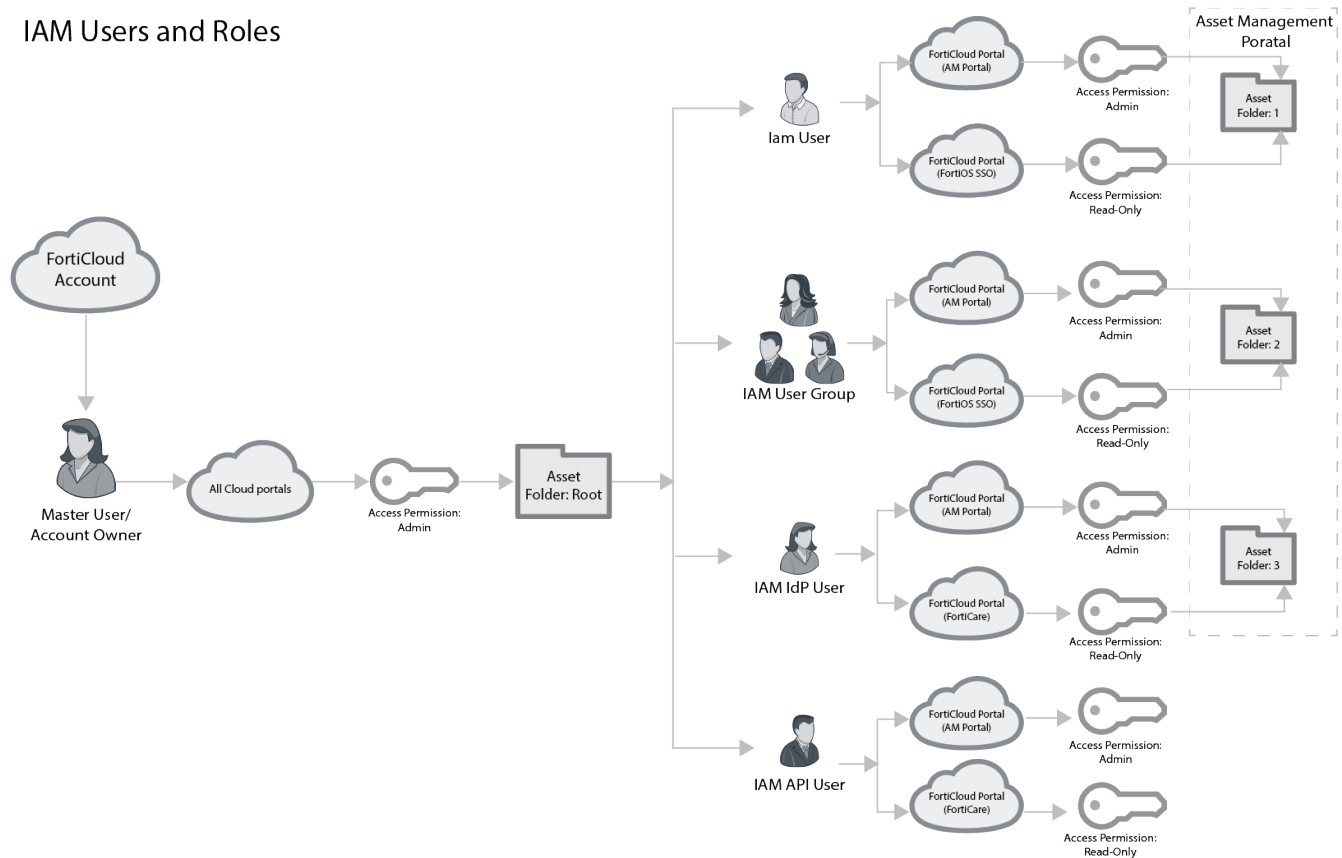
The IAM User Model uses portal-based permission profiles to manage users' access and asset permissions. Instead of assigning *Full Access* permissions or *Limited Access* for the user account, an IAM administrator selects an access type as defined by the portal when creating a permission profile. Permission scope asset permissions are based on the Organizational Unit or asset folders in the Asset Management (AM) portal. This allows for a more granular combination of access and asset permissions.

A master user (Account Owner) can access the IAM portal. IAM Users have access to the portal based on the permissions set by the master user for the IAM portal. Sub users cannot access the IAM Portal.

## IAM user types

User type	Description
<b>IAM user</b>	IAM users can access Fortinet cloud portals with a FortiCloud account. Each IAM account requires an Account ID/Alias, User Name, and password to log in to a portal. Administrators can assign permission profiles to an IAM user or to an IAM user group.
<b>API users</b>	<p>API users can access FortiCloud services through the API. API users can only use OAuth 2.0 for authentication to access web service APIs provided by each FortiCloud service portal.</p> <p>API user IDs and passwords are generated by the IAM service portal. One FortiCloud account can have multiple API users. The IAM service administrator can define which cloud portals the user can access, as well as the user's read/write permissions.</p>
<b>External IdP roles</b>	<p>External IdP roles allow external users to log in to a cloud portal using their organization's ID provider. External IdP roles are authenticated with a custom login page. After the user is authenticated, they are redirected to a jump page where they can select the cloud portal(s) assigned to their account.</p> <p>One account can have more than one external IdP role. User accounts with multiple roles are required to select a role before they can access a portal. Users with no roles assigned to their account are blocked.</p>

## IAM Users and Roles



## Feature comparison chart

Identity & Access Management introduces an enhanced user model for improved security, scalability, and management. The following table compares the features in the legacy Sub User Model with the IAM User Model.

Feature	Sub User Model	IAM User Model
<b>Account Access Management</b>	Add sub users to the account	Add IAM users to the account
<b>Permission Control</b>	Account level (Full Access/Limited Access)	Fine grained permissions for each FortiCloud Service
<b>Asset Permissions</b>	List of devices/Asset Groups (limited)	Asset folders or OUs with permissions hierarchy
<b>User Groups &amp; Permissions</b>	User group (limited)	User groups and group-level permissions
<b>Portal Access</b>	No per portal control	Allow or Deny access per portal
<b>API User Support</b>	No	Granular permissions for each FortiCloud Service APIs
<b>User 2FA Management</b>	No	Enforce (or exempt) 2FA for IAM users

# Permission profiles

Before you can create IAM users, user groups, external IdP roles, or API users, you must create a permission profile. Permission profiles define the level of portal access and permissions a user has. Permission profiles allow you to explicitly enable or disable access to FortiCloud portals and grant portal-specific permissions for the enabled portals.

Permissions can be role-based or resource-based depending on the portal:

- Role-based permissions can be read-only, read and write, or admin levels with more specific permissions available depending on the portal. These permissions account for all portal features unless specified in the *Additional Permissions*.
- Resource-based permissions can be read-only, read and write, or no access and can be assigned to specific resources within the portal. A permission profile can assign different access types for each of the portal resources listed. See [Portals with resource-based permission on page 16](#) for examples of resource-based permissions. See the respective portal administration guide for more information on the specific access types for each portal.



A portal can only support one permission model at a time. If an existing permission profile includes a portal that has been converted from role-based permissions to resource-based permissions, the existing role-based permissions will be migrated to resource-based permissions based on portal-specific rules. Migration settings vary between portals.

---

Once a permission profile has been created, IAM users, user groups, external IdP roles, and API users can be assigned to the profile. See [Users on page 24](#) and [User groups on page 49](#).

The *Permission Profiles* page can be accessed from the left-hand navigation menu. See [Identity & Access Management Portal on page 10](#).

This section contains the following topics:

- [Permission scope on page 19](#)
- [Creating a permission profile on page 19](#)
- [Managing permission profiles on page 21](#)

## Portals with resource-based permission

Resource-based permissions allow user permissions to be assigned by feature, instead of assigning permissions for the entire portal. The following FortiCloud portals use resource-based permissions to allow access:

- [Asset Management on page 17](#)
- [IAM on page 17](#)
- [FortiCare on page 18](#)




The permission details of other portals can be found in their respective product guides.

---

## Asset Management

The Asset Management portal uses resource-based permissions to control access to various features and portal pages. See the [Asset Management Guide](#) for more information.

Resources	Read Only	Read & Write	No Access
Entitlement Management ⓘ	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Asset Maintenance ⓘ	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Renewal Notice ⓘ	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Vulnerability List ⓘ	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Account Services ⓘ	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Resource	Description
<b>Entitlement Management</b>	Provide control over entitlements, including entitlement (product, contract, license) registration, <i>Pending Registration</i> , and <i>Marketplace</i> features. The user can be granted <i>Read Only</i> , <i>Read &amp; Write</i> , or <i>No Access</i> privileges.
<b>Asset Maintenance</b>	Provide control over available assets, including license downloading, decommissioning, deregistration, <i>TradeUp</i> , transfer, and folder management. The user can be granted <i>Read Only</i> , <i>Read &amp; Write</i> , or <i>No Access</i> privileges.
<b>Renewal Notice</b>	Provide the user with product renewal notifications. The user can be granted <i>Read Only</i> or <i>No Access</i> privileges.
	 <p>The user must have access to the root folder.</p>
<b>Vulnerability List</b>	Provide the user access to the product vulnerability list. The user can be granted <i>Read Only</i> or <i>No Access</i> privileges.
<b>Account Services</b>	Provide access to account-level products or services, including <i>Account Services</i> , <i>FortiMeter</i> , and the <i>ELA Profile</i> . The user can be granted <i>Read Only</i> , <i>Read &amp; Write</i> , or <i>No Access</i> privileges.

## IAM

The Identity & Access Management portal uses resource-based permissions to control access to their own account and the creation and management of other users.


Resources	Read Only	Read & Write	No Access
User / Permissions	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Account	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Credentials	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>



Resource	Description
<b>User/Permissions</b>	Provide control over users, user groups, permission profiles, and migrating sub users. The user can be granted <i>Read Only</i> , <i>Read &amp; Write</i> , or <i>No Access</i> privileges.
<b>Account</b>	Provide account management capabilities, including managing <i>Account Settings</i> . The user can be granted <i>Read Only</i> , <i>Read &amp; Write</i> , or <i>No Access</i> privileges.
<b>Credentials</b>	Provide control over account <i>Security Credentials</i> . The user can be granted <i>Read Only</i> , <i>Read &amp; Write</i> , or <i>No Access</i> privileges.

## FortiCare

The FortiCare portal uses resource-based permissions to control access to ticketing features. The FortiCare permissions can be assigned using the *FortiCare New* option.

FortiCare New			
Resources	Read Only	Read & Write	No Access
Customer Service Tickets ⓘ	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Technical Support Tickets ⓘ	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
RMA Tickets ⓘ	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Advanced Service Requests ⓘ	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Incident Response Ticket ⓘ	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Web Chat ⓘ	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Survey Tickets ⓘ	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Support Resources	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Resource	Description
<b>Customer Service Tickets</b>	Allow the user to create and track tickets pertaining to contracts and account management. The user can be granted <i>Read Only</i> , <i>Read &amp; Write</i> , or <i>No Access</i> privileges.
<b>Technical Support Tickets</b>	Allow the user to create and track tickets for technical issues. The user can be granted <i>Read Only</i> , <i>Read &amp; Write</i> , or <i>No Access</i> privileges.
<b>RMA Tickets</b>	Allow the user to create and track tickets pertaining to DOA and RMA assets. The user can be granted <i>Read Only</i> , <i>Read &amp; Write</i> , or <i>No Access</i> privileges.
<b>Advanced Service Requests</b>	<p>Allow the user to submit an Advanced Service request for professional assistance. The user can be granted <i>Read Only</i>, <i>Read &amp; Write</i>, or <i>No Access</i> privileges.</p> <hr/> <div>  <p>For the <i>Advanced Services</i> page to appear in the FortiCare portal, the user must have:</p> <ul style="list-style-type: none"> <li>• <i>Read Only</i> or <i>Read &amp; Write</i> permissions</li> <li>• Access to the root folder in their permissions scope</li> <li>• A Premium Support entitlement</li> </ul> </div> <hr/>
<b>Incident Response Ticket</b>	Allow the user to submit an Incident Response ticket for evaluation. The user can be granted <i>Read Only</i> , <i>Read &amp; Write</i> , or <i>No Access</i> privileges.

Resource	Description
	 <p>For the <i>Incident Response</i> page to appear in the FortiCare portal, the user must have:</p> <ul style="list-style-type: none"> <li>• <i>Read Only</i> or <i>Read &amp; Write</i> permissions</li> <li>• Access to the root folder in their permissions scope</li> <li>• An Incident Retainer Service entitlement</li> </ul>
<b>Web Chat</b>	Allow the user to join live web chats with Fortinet support. The user can be granted <i>Read &amp; Write</i> or <i>No Access</i> privileges.
<b>Survey Tickets</b>	Allow the user to submit feedback in the ticket survey. The user can be granted <i>Read &amp; Write</i> or <i>No Access</i> privileges.
<b>Support Resources</b>	Allow the user to view support resources, such as resource documents, Firmware downloads, and the customer support bulletin. Partners can also view the <i>Bug Tracker</i> . The user can be granted <i>Read Only</i> or <i>No Access</i> privileges.
 <p>The FortiCare Legacy portal permissions can be assigned using the role-based <i>FortiCare Legacy</i> option.</p>	

## Permission scope

A feature of the new permission model is the permission scope. The permission scope defines what an IAM user, user group, external IdP roles, and API users can access in terms of the resources, including users, asset folders, devices, and so on.

If applicable, the permission scope also defines if the assigned users will have *Local* or *Organization* type access. If an account does not have Organizational Unit access enabled, the scope will default to the *Local* type and therefore link to asset folders. The default *Local* type is used by the majority of FortiCloud clients and allows the IAM user, user group, and so on access only to the current account. For the purpose of this document, the default *Local* access is assumed.

For information on enabling Identity & Access Management portal features with *Organization* access, see [Organization user management on page 78](#).

## Creating a permission profile

A new permission profile can be made from the *Permission Profiles* page. Permission profiles must be created before an IAM user, user group, and so on.

**Permission Profiles** ⓘ

Search... Q Disable Delete Add New

Total Records **4**

<input type="checkbox"/>	PROFILE NAME ⓘ	PROFILE DESCRIPTION ⓘ	TYPE ⓘ	# OF ACCESSIBLE PORTALS ⓘ	CRE
<input type="checkbox"/>	SysAdmin	Default profile <span>System Built-In</span>	N/A	3/58	
<input type="checkbox"/>	AM_FlexVM_Admin_Users	AM and FlexVM Admin API Users	Local	2/58	202
<input type="checkbox"/>	MS TEST Profilename		Local	0/58	202
<input type="checkbox"/>	ReadOnlyAccess-FlexVM-AMPortal		Local	2/58	202

The *SysAdmin* permission profile is a default permission profile available at all times. When a user is assigned to *SysAdmin*, they will have full access to the Asset Management portal, Identity & Access Management portal, and FortiCare. You can find the *SysAdmin* permission profile at the top of the *Permission Profiles* list. You cannot edit, disable, or delete the default *SysAdmin* permission profile.

### To create a permission profile:

1. Select *Permission Profiles* from the left-hand navigation menu. The *Permission Profiles* page opens.
2. Select *Add New*. The *New Portal Permission Profiles* page is displayed.

**New Portal Permission Profile** Cancel Submit

**BASIC INFO**

Permission Profile Name: \*

Status: \*

Description

**PERMISSION PROFILE** Add Portal

3. Enter a name for the profile in the *Permission Profile Name* field.



Once the permission profile is saved, the permission profile type cannot be changed.

4. Set the *Status* to *Active*.
5. Enter a description of the portal permissions in the *Description* field.
6. Click *Add Portal*. A list of available portals is displayed.

## ADD THESE PORTALS TO MY ACCOUNTS

Total Selected 0 Select All

<input type="checkbox"/> Asset Management	<input type="checkbox"/> FortiCASB	<input type="checkbox"/> FortiDLP (Beta)	<input type="checkbox"/> FortiMonitor	<input type="checkbox"/> FortiSIEM Cloud	<input type="checkbox"/> Managed FortiGate
<input type="checkbox"/> CTAP (Beta)	<input type="checkbox"/> FortiClient EMS Cloud	<input type="checkbox"/> FortiEdge Cloud	<input type="checkbox"/> FortiOS SSO	<input type="checkbox"/> FortiSOAR Cloud	<input type="checkbox"/> OC-VPN Portal
<input type="checkbox"/> FGaaS	<input type="checkbox"/> FortiClient Services	<input type="checkbox"/> FortiEDR	<input type="checkbox"/> FortiPhish	<input type="checkbox"/> FortiTest Permissions	<input type="checkbox"/> Overlay as a Service
<input type="checkbox"/> FortiAnalyzer Cloud	<input type="checkbox"/> FortiCNP	<input type="checkbox"/> FortiExtender Cloud	<input type="checkbox"/> FortiPortal Cloud	<input type="checkbox"/> FortiTIP	<input type="checkbox"/> Security Awareness (Beta)
<input type="checkbox"/> FortiAppSec Cloud	<input type="checkbox"/> FortiConverter	<input type="checkbox"/> FortiFlex	<input type="checkbox"/> FortiPresence	<input type="checkbox"/> FortiToken Cloud	<input type="checkbox"/> SOCaaS
<input type="checkbox"/> FortiCamera Cloud	<input type="checkbox"/> FortiDAST	<input type="checkbox"/> FortiGate Cloud	<input type="checkbox"/> FortiProxy Cloud	<input type="checkbox"/> FortiTrustID	
<input type="checkbox"/> FortiCare	<input type="checkbox"/> FortiDeceptor DaaS Cloud	<input type="checkbox"/> FortiGate CNF	<input type="checkbox"/> FortiRecon	<input type="checkbox"/> FortiVoice	
<input type="checkbox"/> FortiCare Elite (Beta)	<input type="checkbox"/> FortiDemo	<input type="checkbox"/> FortiInsight	<input type="checkbox"/> FortiSandbox Cloud	<input type="checkbox"/> FortiZTP	
<input type="checkbox"/> FortiCare Legacy	<input type="checkbox"/> FortiDevice	<input type="checkbox"/> FortiMail	<input type="checkbox"/> FortiSASE	<input type="checkbox"/> IAM	
<input type="checkbox"/> FortiCART	<input type="checkbox"/> FortiDevSec	<input type="checkbox"/> FortiManager Cloud	<input type="checkbox"/> FortiSASE Sovereign	<input type="checkbox"/> Lacework FortiCNAPP	

Cancel Add

7. Select the portals you want to enable or deny access to.
8. Click *Add*. The portals are displayed in cards.
9. For each portal card, define portal permissions:



If you want to deny access to a portal, add the portal to the permission profile but do not enable any resource or portal access.

Excluding a portal from a permission profile does not deny access to that portal. If you do not add the portal to the permission profile, its status will be considered undefined. Therefore, it may be possible for the user to still access the portal from the *Services* dropdown menu if the portal itself provides open access to some features.

- For portals with resource-based permission capabilities, specify the *Resources* access type.

Resources	Read Only	Read & Write	No Access
<b>Asset Management</b>			
Entitlement Management	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Asset Maintenance	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Renewal Notice	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Vulnerability List	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Account Services	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Resources	Read Only	Read & Write	No Access
<b>FortiGate Cloud</b>			
Configuration Management	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Logging and Reporting	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Cloud Sandbox	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
IOC	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Resources	Read Only	Read & Write	No Access
<b>IAM</b>			
User / Permissions	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Account	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Credentials	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

- For portals with role-based permissions, enable *Access* and specify the portal *Access Type* and any *Additional Permissions*.

Access	Access Type	Additional Permission
<b>FortiSOAR Cloud</b>		
<input checked="" type="checkbox"/>	<input checked="" type="radio"/> Admin	
	<input type="radio"/> Read/Write	
	<input type="radio"/> Read Only	

Access	Access Type	Additional Permission
<b>FortiExtender Cloud</b>		
<input checked="" type="checkbox"/>	<input checked="" type="radio"/> Admin	
	<input type="radio"/> Read/Write	
	<input type="radio"/> Read Only	

10. Click *Save*. The permission profile is now available to be assigned to users.

## Managing permission profiles

Permission profiles are listed on the *Permission Profiles* page. By selecting a permission profile, you can review specific details of the profile:

- **Permission Profile Info** tab: Displays *Basic Info* and *Permission Details*, including linked portals and portal permissions.

AM\_FlexVM\_Admin\_Users ⓘ

ⓘ Permission Profile Info

ⓘ Assigned To

BASIC INFO

Permission Profile Name

AM\_FlexVM\_Admin\_Users

Description

AM and FlexVM Admin API Users

Status

Active

Edit

PERMISSION PROFILE

PERMISSION DETAILS

FortiFlex

Access	Access Type	Additional Permission
✓	Admin	

Asset Management

Resources	Read Only	Read & Write	No Access
Entitlement Management ⓘ		✓	
Asset Maintenance ⓘ		✓	
Renewal Notice ⓘ			✓
Vulnerability List ⓘ			✓
Account Services ⓘ		✓	

- **Assigned To** tab: Lists all user accounts linked to the permission profile.

AM\_FlexVM\_Admin\_Users ⓘ

ⓘ Permission Profile Info

ⓘ Assigned To

Total Records 2

NAME ⓘ	EMAIL ⓘ	USER TYPE ⓘ	UPDATED ON ⓘ	STATUS ⓘ
AM_FlexVM_Admin_Users		API User	2024-09-05	Active
AM_FlexVM_Admin_Users		API User	2025-01-22	Active

You can edit, disable, and delete permission profiles from the *Permission Profiles* page.



You cannot edit, disable, or delete the default *SysAdmin* permission profile. See [Creating a permission profile on page 19](#).

## Editing a permission profile

Permission profile *Basic Info* and portal permissions can be edited.

**To edit a permission profile:**

1. Select *Permission Profiles* from the left-hand navigation menu. The *Permission Profiles* page opens.
2. Select the permission profile you want to edit. The *Permission Profiles / <profile\_name>* page is displayed.

**AM\_FlexVM\_Admin\_Users** ⓘ

① Permission Profile Info

Assigned To ⓘ

**BASIC INFO**

Permission Profile Name  
AM\_FlexVM\_Admin\_Users

Status  
Active

Description  
AM and FlexVM Admin API Users

**PERMISSION PROFILE**

PERMISSION DETAILS

FortiFlex			Asset Management			
Access	Access Type	Additional Permission	Resources	Read Only	Read & Write	No Access
✓	Admin		Entitlement Management ⓘ		✓	
			Asset Maintenance ⓘ		✓	
			Renewal Notice ⓘ			✓
			Vulnerability List ⓘ			✓
			Account Services ⓘ		✓	

[Edit](#)

3. Click *Edit*.
4. Make changes as required to *Description* and portal permissions.
5. Click *Update*. The profile has been updated for all users assigned to it.

## Disabling a permission profile

If a permission profile is not needed at the moment, but may be required in the future, it can be temporarily disabled. A permission profile cannot be disabled if an active IAM user is assigned to it.

### To disable a permission profile:

1. Select *Permission Profiles* from the left-hand navigation menu. The *Permission Profiles* page opens.
2. Select the profile you want to disable.
3. Click *Disable*. The profile and any assigned users are disabled.

## Deleting a permission profile

You can permanently delete a permission profile that is no longer needed. A permission profile cannot be deleted if an active IAM user is assigned to it.

### To delete a permission profile:

1. Select *Permission Profiles* from the left-hand navigation menu. The *Permission Profiles* page opens.
2. Select the profile you want to delete.
3. Click *Delete*.

# Users

The *Users* page displays information on all registered users, including the user *Type*, *Permission Profile*, and *Permission Scope*.

Users ⓘ

Search...

🔍

👤

Add New

Total Records 7

<input type="checkbox"/>	USERNAME/ROLE/ID ⓘ	DESCRIPTION ⓘ	TYPE ⓘ	PERMISSION PROFILE ⓘ	PERMISSION SCOPE ⓘ	STATUS ⓘ	ACTION
<input type="checkbox"/>	iam_fcdemo3		IAM User	ReadOnlyAccess-FlexVM-...	MyAssets	Active	<div>🔄🗑️</div>
<input type="checkbox"/>	mstestIAMid		IAM User	MS test - MS TEST Profil...	MyAssets	Active	<div>🔄🗑️</div>
<input type="checkbox"/>	abctest		IAM User	MS TEST Profilename	MyAssets	Active	<div>🔄🗑️</div>
<input type="checkbox"/>	DocUser		IAM User	SysAdmin	MyAssets	Active	<div>🔄🗑️</div>
<input type="checkbox"/>	test1	test1	API User	SysAdmin	MyAssets	Active	<div>🔄🗑️</div>
<input type="checkbox"/>			API User	AM_FlexVM_Admin_Users	MyAssets	Active	<div>🔄🗑️</div>



You can use the *Search* field to find a specific user. Partial results are returned as you enter information.



- Select the download button to export a list of the IAM users as an Excel or CSV file. Information included in the file include:
- Username
  - Description
  - Email
  - Type
  - Permission Profile
  - Permission Scope
  - Status

The types of users accessible from the *Users* page include:

- [IAM users on page 24](#)
- [API users on page 38](#)
- [External IdP roles on page 43](#)

## IAM users

The IAM user details can be found in the *Users* page, including *Username*, *Type*, *Permission Profile*, *Group*, and *Status*. Use this page to add and delete users, or temporarily disable a user. Click the user's *Username* to edit their profile, update their permission profile, and reset their password.

Use the *Add New* wizard to create a new IAM user. You can also migrate FortiCloud sub users to create a new IAM user. After the user is created, you can update the user's permission profile at any time from the *User Permission* tab.

The *Users* page can be accessed from the left-hand navigation menu. See [Identity & Access Management Portal on page 10](#).

USERNAME/ROLE/ID	DESCRIPTION	TYPE	PERMISSION PROFILE	PERMISSION SCOPE	STATUS	ACTION
iam_fcdemo3		IAM User	ReadOnlyAccess-FlexVM-...	MyAssets	Active	<input type="checkbox"/>
mstestIAMid		IAM User	MS test - MS TEST Profil...	MyAssets	Active	<input type="checkbox"/>
abctest		IAM User	MS TEST Profilename	MyAssets	Active	<input type="checkbox"/>
DocUser		IAM User	SysAdmin	MyAssets	Active	<input type="checkbox"/>
test1		API User	SysAdmin	MyAssets	Active	<input type="checkbox"/>
AM_FlexVM_Admin_Users		API User	AM_FlexVM_Admin_Users	MyAssets	Active	<input type="checkbox"/>



IAM users are separate, additional users to the FortiCloud account. Even if an IAM user and the FortiCloud account use the same login credentials, they are independent of each other.

This section contains the following topics:

- [Adding IAM users on page 25](#)
- [Managing IAM users on page 29](#)
- [Validating IAM users on page 32](#)
- [Logging in as an IAM user on page 35](#)
- [Migration of existing users on page 36](#)

## Adding IAM users

Use *Add New* to configure IAM users and generate their login credentials.

To save time, you can apply a permission profile or assign the user to a group. Before you can create IAM users, you must create a permission profile. See [Permission profiles on page 16](#).

To add a new IAM user, you must:

1. Create the new user account. See [Creating a new IAM user on page 26](#).
2. Generate the password reset link and share it with the selected IAM user. See [Generating the password reset link on page 28](#).

## Creating a new IAM user

You can create a new IAM user with the *Add New* wizard.

### To create an IAM user with the wizard:

1. Select *Users* from the left-hand navigation menu. The *Users* page opens.
2. Click *Add New > IAM User*. The *User Details* pane opens.
3. (Optional) Click *Apply same permissions as existing User*, and then select a user from the dropdown. You can configure the permissions later.
4. Enter the user's details and click *Next*.

<b>Username</b>	Type the username with no spaces.
<b>Full Name</b>	Type the user's first and last name.
<b>Email</b>	Type the user's email address.
<b>Phone</b>	Select the country code from the dropdown, and type the user's phone number.
<b>Description (Optional)</b>	Type a description of the user.

1. User Details

**IAM USER INFORMATION**  
**Username: \***  
  
**Full Name: \***  
  
**Email: \***  
  
**Phone: \***  
  
**Description**

**ADOPT PERMISSIONS**  
☐ **Apply same permissions as existing User :**  
  
NOTE  
Checking 'Apply same permission as an existing User' allows you to easily assign a pre-configured Permission setup. User Permission settings are still fully configurable in the next step.

5. (Optional) Add the user to an IAM user group. See [User groups on page 49](#).

a. Select **Yes** from *Basic Info*.

2. User Permissions

IAM User Name: Doc\_IAM\_User

**BASIC INFO**

Do you want your permission controlled by an IAM User Group?

The User will adopt the permissions of the assigned User Group. You cannot edit the User's Asset or Portal Permissions while the User is assigned to a Group. Remove the User from the Group to enable editing of their permissions.

Yes No

**PERMISSION SCOPE**

Select an Asset Folder \*

None

**PERMISSION PROFILE**

Select a Permission Profile\*

None

Cancel Back Next

A dropdown list of user groups is displayed.

## b. Select a user group from the dropdown.

c. Click **Next**, and proceed to Step 10.6. From the *Permission Scope* dropdown, select an asset folder or Organizational Unit.

*Permission Scope* hierarchy and options depend on the type you select in the previous step.

Select an Asset Folder \*

None

☐ My Assets

☐ Level1

7. In the *Permissions Profile* dropdown, select a profile.

Select a Permission Profile\*

None

SysAdmin Default profile

AM\_FlexVM\_Admin\_Users AM and FlexVM Admin API Users

MS TEST Profilename

ReadOnlyAccess-FlexVM-AMPortal

The *Permission Details* assigned to the selected profile are displayed.

Select a Permission Profile\*

AM\_FlexVM\_Admin\_Users

PERMISSION DETAILS

FortiFlex			Asset Management			
Access	Access Type	Additional Permission	Resources	Read Only	Read & Write	No Access
✓	Admin		Entitlement Management ⓘ		✓	
			Asset Maintenance ⓘ		✓	
			Renewal Notice ⓘ			✓
			Vulnerability List ⓘ			✓
			Account Services ⓘ		✓	



If the *SysAdmin* profile is selected, a message will display instead of portal cards to denote that the user has full access to the Asset Management, IAM, and FortiCare portals. *SysAdmin* has access to *Assets&Accounts* and *Support* but does not provide access to *Cloud Management* or *Cloud Services*. See [Creating a permission profile on page 19](#).

8. Click *Next*. The *Confirmation* page is displayed.
9. Review the user information, and click *Confirm*. The user's details are displayed.

Account credentials must be shared with the user. The account password can be configured using *Generate Password*. See [Generating the password reset link on page 28](#) to configure the account password and share user credentials.

## Generating the password reset link

You can choose to generate the password reset link and share it with the selected IAM user.

### To generate the password reset link:

1. On the *Successful User Registration* page, click *Generate Password*. The *Login with the Generated Link* dialog opens.

#### LOGIN WITH THE GENERATED LINK

Pressing 'Generate Password' will generate a reset password link for the user to login. The new generated link will **make the previous one invalid** and **expire in 5 days**.

Cancel

Generate Password

2. Click *Generate Password*. A reset link is generated.

#### LOGIN WITH THE GENERATED LINK

Pressing 'Generate Password' will generate a reset password link for the user to login. The new generated link will **make the previous one invalid** and **expire in 5 days**.

Cancel

Copy Reset Link

3. Click *Copy Reset Link*. The reset link is copied to your clipboard and you can now share it with the IAM user.
4. For the IAM user to reset their password, paste the reset link into your browser. The *Reset Password* page opens and account credentials are displayed.

### Reset Password

Please adhere to our password requirements to ensure a strong and secure reset for the email: docuser25@... Username: DocUser25 Account ID: ...

NEW PASSWORD

CONFIRM NEW PASSWORD

Your new password must contain

- At least one uppercase letter
- At least one lowercase letter
- At least one numeric character
- At least one non-alphanumeric character (e.g., \$!%#)
- Password cannot match the username
- Password length must be a minimum of 8 characters

RESET PASSWORD

5. Enter the password in the *New Password* and *Confirm New Password* fields.



When resetting the password, password criteria, such as necessary character length, are listed. As you reset the password, the criteria will update to confirm which criteria have been successfully included and which are still outstanding.

6. Click *Reset Password*. A confirmation message displays.



### Password Successfully Reset

Please click the button below to log in again.

LOGIN AGAIN




The *Generate Password* link can also be accessed on *Security Credentials* tab of the *Users > IAM* user page. See [Resetting an IAM user password on page 32](#).

Send the credentials to the user.

## Managing IAM users

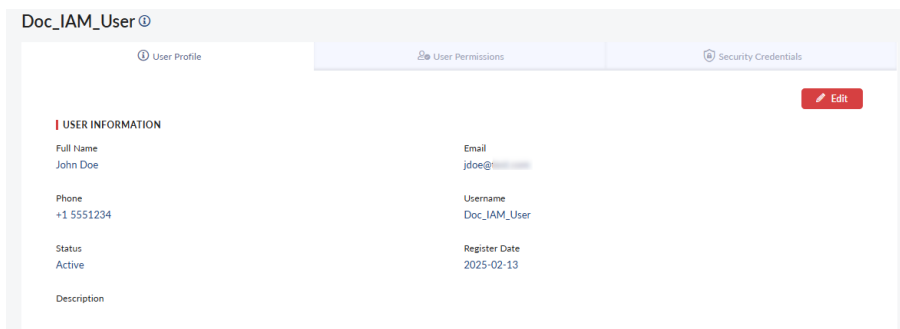
Select an IAM user from the *Users* page to update a user's details or generate the password reset link.

The *Users > IAM* user page displays the following information:

Column	Description
<b>Username</b>	The user's display name.
<b>Full Name</b>	The user's first and last name.
<b>Email</b>	The email address for the IAM user account.
	 Updating the email address in the <i>User Profile</i> tab will also change the IAM user's email address in the <i>Security Credentials &gt; Contacts</i> page. See <a href="#">Contacts on page 65</a> .
<b>Updated</b>	The date the user's information was updated.
<b>Group</b>	The user group the user is assigned to.
<b>Status</b>	The user's status ( <i>Active/Disabled</i> ).

## Updating user details

To update the user name, ID, email, and status, go to the *User Profile* tab.




If you change the email address used by the user, email Two-Factor Authentication tokens will be sent to the new email address. See [Two-Factor Authentication on page 70](#) for more information.

### To update user details:

1. Select *Users* from the left-hand navigation menu. The *Users* page opens.
2. Select the IAM user *Username*.
3. Click *Edit*.
4. Edit the user's information, and click *Update*.

### To activate a user:

1. Select *Users* from the left-hand navigation menu. The *Users* page opens.
2. Select the IAM user *Username*.
3. Click *Edit*.

4. From the *Status* dropdown, select *Active*.
5. Click *Update*.

### Updating user status

You can enable, disable, and delete an IAM user from the *Users* page.



You can also update multiple user statuses at once from the *Users* page. See [Bulk updating users on page 47](#).

---

#### To enable a user:

1. Select *Users* from the left-hand navigation menu. The *Users* page opens.
2. Find the user you want to enable.
3. Under *Actions*, click *Enable*. The *Confirm to Enable User* dialog is displayed.
4. Click *Yes, I want to continue*.

#### To delete a user:

1. Select *Users* from the left-hand navigation menu. The *Users* page opens.
2. Select a user from the list, and click *Delete*. The *Delete User(s)* dialog opens.
3. Click *Confirm*.

#### To disable user:

1. Select *Users* from the left-hand navigation menu. The *Users* page opens.
2. Select a user in the list.
3. Click *Disable*. The *Permission Changed Confirmation* dialog opens..
4. Click *Confirm*.

### Updating a user in a user group

You can add or remove a user from a group.

#### To add a user to a user group:

1. Select *Users* from the left-hand navigation menu. The *Users* page opens.
2. Select the user's *Username*. The *Users > IAM user* page is displayed.
3. Click *User Permissions*.
4. Click *Edit*.
5. In *Basic Info*, select *Yes* to add a user to a user group.

2. User Permissions

IAM User Name: Doc\_IAM\_User

**BASIC INFO**

Do you want your permission controlled by an IAM User Group?  
 The User will adopt the permissions of the assigned User Group. You cannot edit the User's Asset or Portal Permissions while the User is assigned to a Group. Remove the User from the Group to enable editing of their permissions.

Yes No

**PERMISSION SCOPE**

Select an Asset Folder \*

None

**PERMISSION PROFILE**

Select a Permission Profile\*

None

Cancel Back Next

6. Select the user group from dropdown list.

7. Click *Update*.

## Resetting an IAM user password

You can generate a reset IAM user password link and enable Two-Factor Authentication.



You cannot regenerate a password if the user has enabled Two-Factor Authentication at the account level.

### To generate a password:

1. Select *Users* from the left-hand navigation menu. The *Users* page opens.
2. Select the user's *Username*. The *Users > IAM user* page is displayed.
3. Click *Security Credentials*.
4. (Optional) Click *Two Factor Authentication*.
5. Click *Generate Password*. The password is generated.
6. Click *Copy Reset Link*. The link is copied to your clipboard.
7. Share the password reset link with the IAM user.

## Validating IAM users

IAM users are required to verify their email address if it has been changed.



When Two-Factor Authentication (2FA) is enabled, new IAM users will bypass this step and set up 2FA authorization instead. See [Logging in with Two-Factor Authentication for the first time on page 72](#).

**To validate a new email address:**

1. Go to [www.forticloud.com](http://www.forticloud.com) and click *Login*.
2. Select *IAM user*.

**Log in as**

☒ IAM user ☐ Email user

ACCOUNT ID / ALIAS

USERNAME


PASSWORD [Forgot password?](#)

LOG IN AS IAM USER

3. Enter the *Account ID* or *Alias ID*, as well the *Username* and *Password* provided by the account administrator. The *Welcome to FortiCloud* page opens.
4. Click *Get Verification Code*. A verification code is emailed to you.

**Welcome to FortiCloud**

To ensure access to your FortiCloud account is simple and secure, please complete the following 'quick setup' process below:

 Please verify your Email Address  
This is a 'one-time' action - you won't be asked again for this information

Email :


GET VERIFICATION CODE

VERIFY >

5. Enter the codes in the *Validation Code* and *Enter Captcha Code* fields.


## Welcome to FortiCloud

To ensure access to your FortiCloud account is simple and secure, please complete the following 'quick setup' process below:

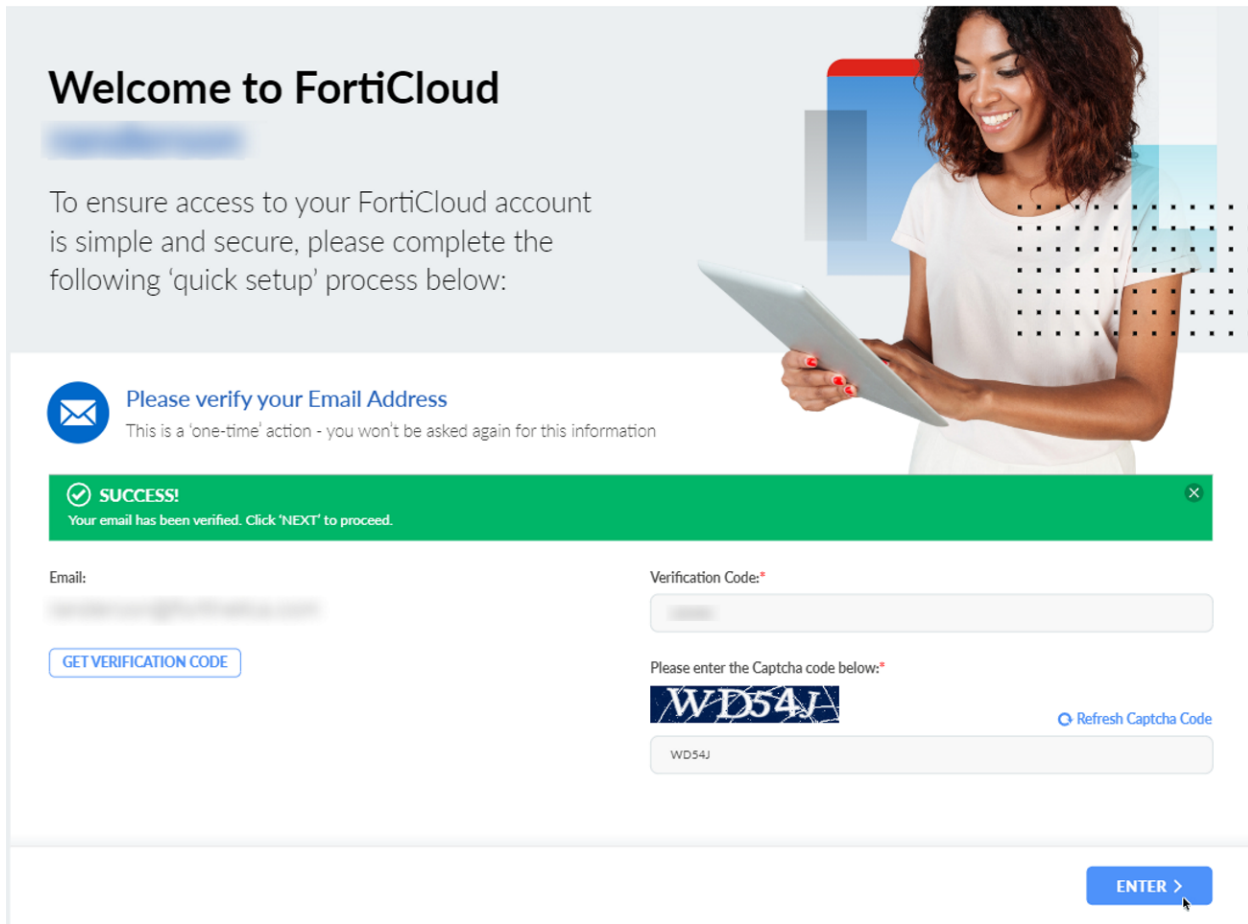
**Please verify your Email Address**  
This is a 'one-time' action - you won't be asked again for this information

**ⓘ ACTION REQUIRED !**  
An email has been sent to your email address. Please enter the verification code you've received.

Email :  
  
[GET VERIFICATION CODE](#)


Verification Code: \*  
  
Please enter the Captcha code below: \*  
  
[Refresh Captcha](#)  
  
[VERIFY >](#)


6. Click *Verify*. The *Welcome to FortiCloud* page opens.

7. Click *Enter*.

**Welcome to FortiCloud**

To ensure access to your FortiCloud account is simple and secure, please complete the following 'quick setup' process below:


 **Please verify your Email Address**  
This is a 'one-time' action - you won't be asked again for this information

 **SUCCESS!**  
Your email has been verified. Click 'NEXT' to proceed.

Email:

[GET VERIFICATION CODE](#)

Verification Code:

Please enter the Captcha code below: 

[Refresh Captcha Code](#)

[ENTER >](#)

## Logging in as an IAM user

Users can access FortiCloud services and support as an IAM user with their IAM user credentials.



While it is optional, it is strongly recommended that you enable Two-Factor Authentication (2FA). If the administrative account enforces 2FA for the entire account, IAM users should complete 2FA setup after logging in to [www.forticloud.com](http://www.forticloud.com) for the first time. See [Two-Factor Authentication on page 70](#).

### To log in as an IAM user:

1. Go to [www.forticloud.com](http://www.forticloud.com).
2. Select *Login*. The log in portal opens.
3. Select *IAM user*.

**Log in as**

☒ IAM user ☐ Email user

ACCOUNT ID / ALIAS

USERNAME

PASSWORD

[Forgot password?](#)

LOG IN AS IAM USER

4. Enter your credentials in the *Account ID/Alias*, *Username*, and *Password* fields.



You can enter either your account ID number or alias in the *Account ID/Alias* field.



When entering your password, select the eye icon to show or hide your password.

5. Click *Log In as IAM User*. The default page will be displayed.

## Migration of existing users

The new permission profile model is replacing the previous portal permission model. While the portal permission model had portal permissions configured directly for an IAM user, user group, IdP role, or API user, the permission profile is configured separate of users and can be linked to multiple IAM users.

To effectively convert the Identity & Access Management portal to the new permission profile model, any pre-existing IAM users, user groups, and so on will automatically be converted to the new model. This migration of users will result in the existing IAM user being split into an IAM user and a permission profile following the conversion to the new permission profile model. Therefore, any permissions assigned to the IAM user will be used to create a new permission profile containing the same portals and permissions that is automatically assigned to the IAM user.



Each pre-existing IAM user with unique portal permissions will result in a unique permission profile following the migration. For example, if before the conversion to the new model there are five IAM users, each with independently created portal permissions assigned, then there will be five IAM users and five permission profiles following the migration.

## Example of IAM user migration to the new permission profile model

The following scenario describes the migration of an IAM user to the new permission profile model.

Before the conversion to the new model, an IAM user named Jane Test has portal permissions directly assigned to it. These portal permissions allow administrative access to the Asset Management portal and read only access to the IAM portal.

IAM Users > Jane Test

User Profile

User Permissions

Security Credentials

EDIT

☐ IAM User Group (Permissions controlled by IAM User Group)

None

\* NOTE : User will adopt the Permission of the assigned Group. You cannot edit Asset or Portal Permissions while user is assigned to a Group. Remove user from any group to enable Permissions to be editable.

Asset Permissions \*

My Assets

Portal Permissions

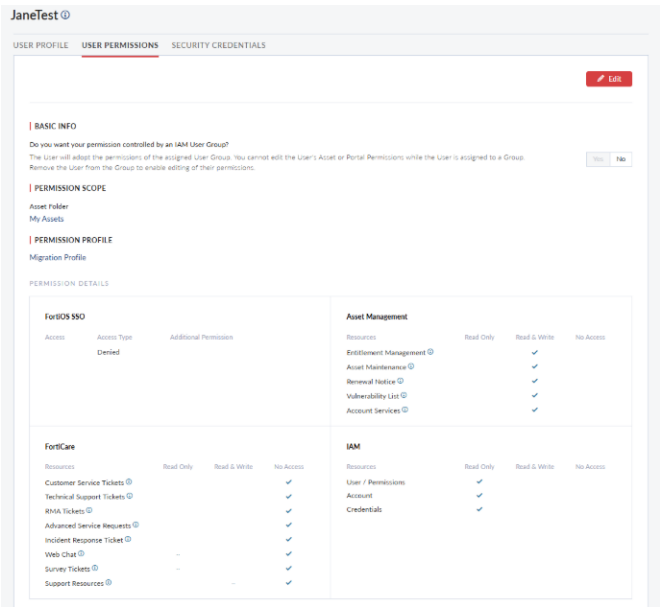
Portals	Access	Access Type	Additional Permission	Cloud Management & Service	Access	Access Type	Additional Permission
Asset Management	✓	Admin	-				
FortiCare	✗	Denied	-				
FortiOS SSO	✗	Denied	-				
IAM	✓	Read Only	-				

No Rows To Show

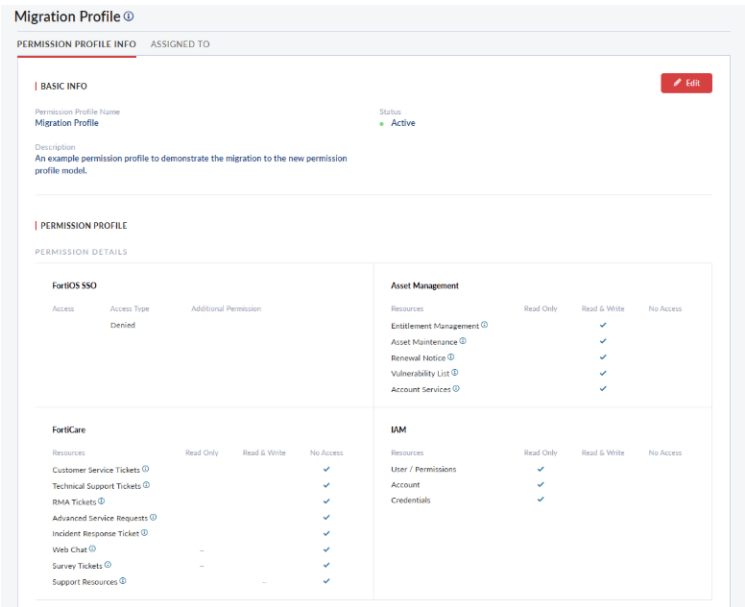
Following the conversion to the new model, the Jane Test IAM user can be found in the *IAM Users* page. It has been migrated forward with the same *User Profile* information but it no longer has portal permissions directly assigned to it. Instead, Jane Test is assigned to a permission profile that has automatically been created when the conversion occurred. The permission profile defines the same permissions and access as the portal permissions before the conversion: administrative access to the Asset Management portal and read-only access to the Identity & Access Management portal.



For the purpose of this example, the permission profile has been named *Migration Profile* for clarity. When migration of an IAM user occurs following the conversion in a real-world scenario, it will not follow this naming convention.



You can review and edit the permission profile by selecting it from the *Permission Profiles* page.



## API users

API users can access FortiCloud services through the API. API users can only use OAuth 2.0 for authentication then access web service APIs provided by each FortiCloud service portal.

You can disable or delete a user directly from the *Users* page. Click the *ID* to update the user's status and permissions. The *Users* page can be accessed from the left-hand navigation menu. See [Identity & Access Management Portal on page 10](#).

**Users** ⓘ

Search...

**Total Records** 7

<input type="checkbox"/>	USERNAME/ROLE/ID ⓘ	DESCRIPTION ⓘ	TYPE ⓘ	PERMISSION PROFILE ⓘ	PERMISSION SCOPE ⓘ	STATUS ⓘ	ACTION
<input type="checkbox"/>	iam_fcdemo3		IAM User	ReadOnlyAccess-FlexVM-...	MyAssets	Active	
<input type="checkbox"/>	mstestIAMid		IAM User	MS test - MS TEST Profil...	MyAssets	Active	
<input type="checkbox"/>	abctest		IAM User	MS TEST Profilename	MyAssets	Active	
<input type="checkbox"/>	DocUser		IAM User	SysAdmin	MyAssets	Active	
<input type="checkbox"/>	test1	test1	API User	SysAdmin	MyAssets	Active	
<input type="checkbox"/>			API User	AM_FlexVM_Admin_Users	MyAssets	Active	

This section contains the following topics:

- [Adding an API user on page 39](#)
- [Managing API users on page 40](#)
- [Accessing FortiAPIs on page 41](#)

## Adding an API user

Use *Add New* to generate API user IDs and passwords. IAM users can use their credentials to obtain an OAuth token from FortiAuthenticator.

Before you can create API users, you must create a permission profile. See [Permission profiles on page 16](#).

### To create an API user:

1. Select *Users* from the left-hand navigation menu. The *Users* page opens.
2. Click *Add New > API User*.

**Add API User** ⓘ

**API USER DETAILS**

Description

Enter description

Type

Local

**PERMISSION SCOPE**

Asset Folder

My Assets

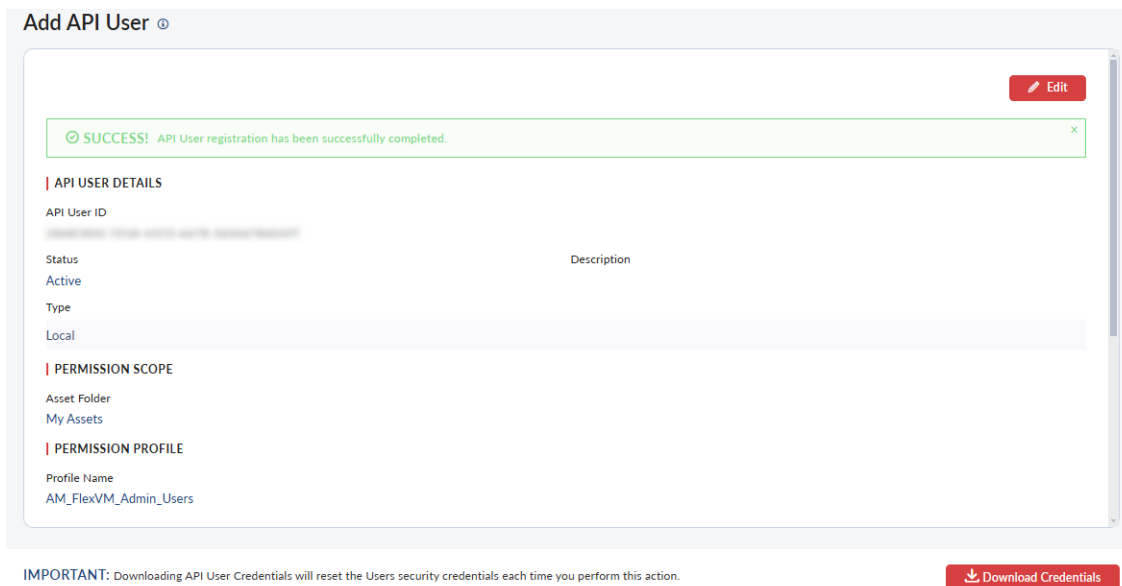
**PERMISSION PROFILE**

Select a Permission Profile: \*

None

Cancel Add

3. (Optional) In the *Description* field, enter a description of the user.
4. Select a permission profile from the *Permission Profile* dropdown list.

**5. Click *Add*.**

IMPORTANT: Downloading API User Credentials will reset the Users security credentials each time you perform this action.

**6. Click *Download Credentials*. The *Security Check* dialog opens.**

Downloading API user credentials will reset the user's security credentials each time you perform this action. The API user only exists within the account scope.

**7. Enter your password to protect the credential file and click *Proceed*. The credentials are downloaded to your computer.****SECURITY CHECK**

We are keeping your info safe. To prevent fraud, please input a password for your credential file protection.

PASSWORD

Cancel

Proceed

**8. Request an authorization token. See [Accessing FortiAPIs on page 41](#)**

## Managing API users

You can delete or temporarily disable an API user by selecting the user from the *Users* page.



You can also update multiple user statuses at once from the *Users* page. See [Bulk updating users on page 47](#).

The *Users > API user* page displays the following information:

Column	Description
API User ID	The user's API ID. Click the user ID to update the user details.
Description	A description of the user.
Updated	The date the user profile was updated.
Status	The status ( <i>Active/Disabled</i> )

## Updating API user permissions

### To disable an API user:

1. Select *Users* from the left-hand navigation menu. The *Users* page opens.
2. Select an *ID* in the list. The *API User Information* pane opens.
3. Click *Disable*. The *Permission Changed Confirmation* dialog opens.
4. Click *Confirm*.

### To activate an API user:

1. Select *Users* from the left-hand navigation menu. The *Users* page opens.
2. Select an *ID* in the list. The *API User Information* pane opens.
3. Click *Edit*.
4. From the *Status* dropdown, select *Active*.
5. Click *Update*.

### To update an API user's portal permissions:

1. Select *Users* from the left-hand navigation menu. The *Users* page opens.
2. Select an *ID* in the list. The *API User Information* pane opens.
3. Click the *Edit* button.
4. Select a new *Permission Profile*.
5. Click *Update*.

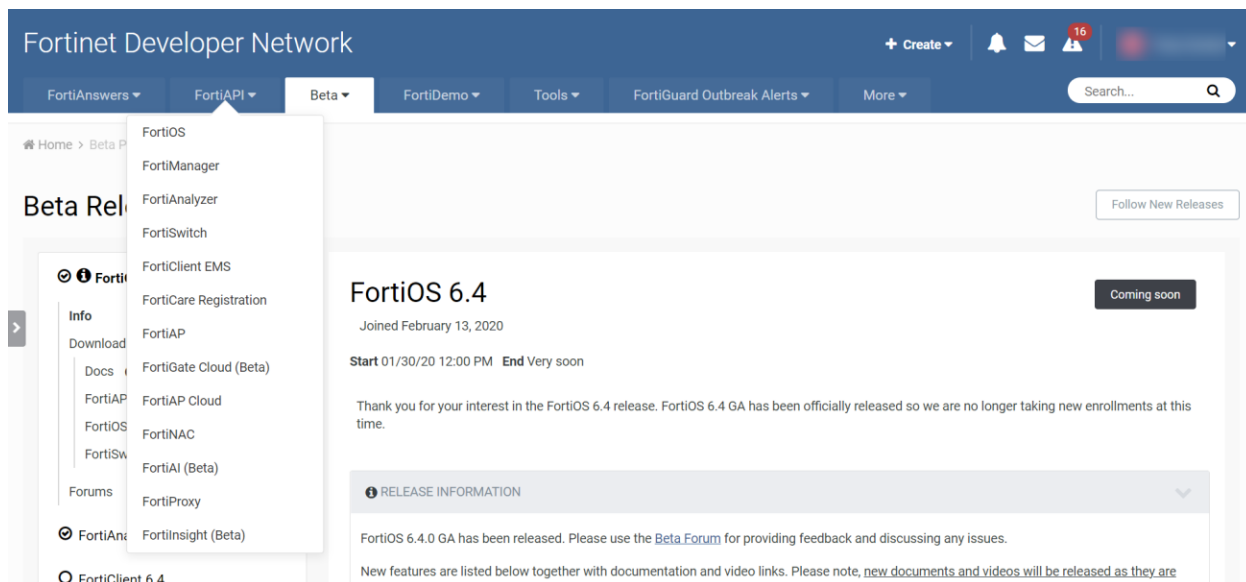
## Accessing FortiAPIs

FortAPIs are located in the [Fortinet Developer Network](#). To access the APIs, click *FortiAPI* and select a product from the list.



The Fortinet Developer Network can only be accessed if you have an account registered.

---



## Authorization

To obtain an OAuth token, an API user must send their credentials to the [FortiAuthenticator API](#). Once the token is obtained, it should be sent in the *Authorization* header of the request with *Bearer* scheme, as in the example below:

Authorization: Bearer jVSjRMx5hpw5ZfASK8Hj016X

For information about creating an OAuth token, see the *FortiAuthenticator REST API Solution Guide* > [OAuth server token \(/oauth/token/\)](#).

### To obtain an access token:

1. Log in to the IAM portal as an IAM User with Admin permissions.
2. Create an IAM API user and configure the relevant permissions for the required product APIs. See [Adding an API user on page 39](#).
3. Download the IAM API user credentials (API Key, Password, client ID).
4. Request the access token. For example:

```
$curl -H 'Content-Type: application/json' -X POST
<https://customerapiauth.fortinet.com>/api/v1/oauth/token/ -d '{
  "username": <API Key>,"password": <password>, "client_id": <clientId for FortiGate
  Cloud>,"grant_type": "password"}'
```

Response:

```
{
  "access_token": "paLreKW6YGDfgSUfreEH90UCc1915v3",
  "expires_in": 14400,
  "message": "successfully authenticated",
  "refresh_token": "WpD0HVYUdshsiWlMBR0Q6uUoV2TGUIa",
  "scope": "read write",
  "status": "success",
  "token_type": "Bearer"
}
```

5. Refresh the token. For example:

```
$curl -k -v -X POST <auth_url>/api/v1/oauth/token/ -H 'Content-Type: application/json' -d
```

```
'{"client_id": "fortigatecloud", "grant_type": "refresh_token", "refresh_token": "WpD0HvYUdshsiWlMBR0Q6uUoV2TGUIa", }'
```

Response:

```
{
  "access_token": "qeOreKW6YGDfgSUfreEH90UCc1915v3",
  "expires_in": 14400,
  "message": "Token has been refreshed successfully",
  "refresh_token": "xpD0HVVUdshsiWlMBR0Q6uUoV2TDSa",
  "scope": "read write",
  "status": "success",
  "token_type": "Bearer"
}
```

## External IdP roles

External IdP roles allow external users to log in to a cloud portal using their company's user credentials with a third-party ID provider. External IdP users are authenticated by their company's ID provider. After the user is authenticated, they can access the cloud application based on their role.

For more information on enrolling for and configuring external IdP, see [External IdP on page 92](#).



When an IdP user clicks *Logout*, they are only logging out of the portal, not their company's ID provider.

If applicable, the external IdP roles can be accessed from the *Users* page in the left-hand navigation menu. See [Identity & Access Management Portal on page 10](#).

Users ⓘ

Search...

🔍

👤

Add New

Total Records 5							
<input type="checkbox"/>	USERNAME/ROLE/ID ⓘ	DESCRIPTION ⓘ	TYPE ⓘ	PERMISSION PROFILE ⓘ	PERMISSION SCOPE ⓘ	STATUS ⓘ	ACTION
<input type="checkbox"/>	iam_1		IAM User	234234 - AdminIAM	MyAssets	Active	<div><div>🔄</div><div>🗑️</div></div>
<input type="checkbox"/>	IDP_AdminAll		External IdP Role	SysAdmin	MyAssets	Active	<div><div>🔄</div><div>🗑️</div></div>
<input type="checkbox"/>	IDP_AdminIAM		External IdP Role	AdminIAM	MyAssets	Active	<div><div>🔄</div><div>🗑️</div></div>
<input type="checkbox"/>	IDP_AdminAsset		External IdP Role	AdminIAM	MyAssets	Active	<div><div>🔄</div><div>🗑️</div></div>
<input type="checkbox"/>	234234		Partner Role	AdminIAM	MyAssets/sub1	Active	<div><div>🔄</div><div>🗑️</div></div>



FortiCloud external IdP integration supports only FortiCloud services. FortiGate directly supports SAML SSO which can be enabled in FortiOS.

This section contains the following topics:

- [Adding external IdP roles on page 44](#)
- [Selecting IdP roles on page 45](#)

## Adding external IdP roles

Create external IdP roles to allow users to log in to a cloud portal with their organization's user credentials using a third-party ID provider.

Before you can create external IdP roles, you must create a permission profile. See [Permission profiles on page 16](#).

### To add an external user role:

1. Select *Users* from the left-hand navigation menu. The *Users* page opens.
2. Click *Add New > External IdP Role*. The *External IdP Role* page opens.
3. In the *Role Name* field, type the name of the role. For more information on what to name the role, see [Adding external IdP roles to the application on page 99](#).
4. (Optional) In the *Description* field, enter a description of the role.
5. From the *Permission Scope* dropdown, select an asset folder.

Select an Asset Folder \*

None

☐ My Assets

☐ Level1

6. In the *Permissions Profile* dropdown, select a profile.

Select a Permission Profile\*

None

SysAdmin  
AM\_FlexVM\_Admin\_Users  
MS TEST Profilename  
ReadOnlyAccess-FlexVM-AMPortal

Default profile  
AM and FlexVM Admin API Users

The *Permission Details* assigned to the selected profile are displayed.

PERMISSION DETAILS			
CTAP (Beta)		FortiCare Legacy	
Access	Access Type	Access	Access Type
✓	ReadWrite	✓	ReadOnly
Not Supported		Not Supported	
Asset Management		IAM	
Resources	Read Only	Resources	Read Only
Entitlement Management ⓘ		User / Permissions	✓
Asset Maintenance ⓘ		Account	✓
Renewal Notice ⓘ		Credentials	✓
Vulnerability List ⓘ			
Account Services ⓘ			



If the *SysAdmin* profile is selected, a message will display instead of portal cards to denote that the user has full access to the Asset Management, IAM, and FortiCare portals. *SysAdmin* has access to *Assets&Accounts* and *Support* but does not provide access to *Cloud Management* or *Cloud Services*. See [Creating a permission profile on page 19](#).  
If the permission profile selected includes portals that do not support external IdP, the portals will be marked as *Not Supported*.

7. Click *Add Role*.

## Managing external IdP roles

You can manage external IdP roles from the *Users* page, including enabling, disabling, and deleting users.

### To delete a role:

1. Select *Users* from the left-hand navigation menu. The *Users* page opens.
2. Select a role from the list.
3. Click *Delete*. The *Delete Third Party IdP Role(s)* dialog is displayed.
4. Click *Confirm*.

### To disable a role:

1. Select *Users* from the left-hand navigation menu. The *Users* page opens.
2. Select a role from the list.
3. Click *Disable*. The *Disable User Third Party IdP Role(s)* dialog is displayed.
4. Click *Confirm*.

### To enable a role:

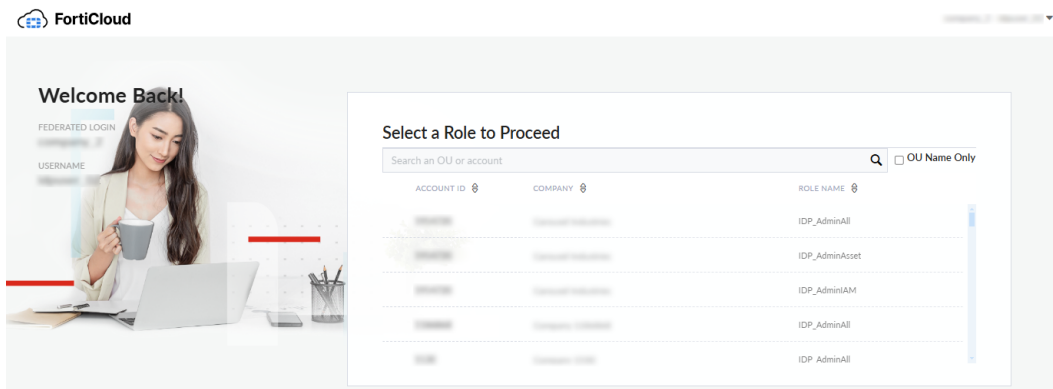
1. Select *Users* from the left-hand navigation menu. The *Users* page opens.
2. Double-click the disabled role. The *Manage External IdP Roles ><name>* pane opens.
3. Click *Edit*.
4. From the *Status* dropdown, select *active*.
5. Click *Update*.

## Selecting IdP roles

An external user can be assigned to more than one IdP role. When a user logs into a cloud portal through a third-party ID provider, their user account is mapped to their IdP roles in the portal.

After the user logs in with the third-party ID provider, the roles connected to the user's account determines their access to the portal.

- If no roles are assigned to the account, a blocker message appears.
- If only one role is assigned to the account, the user proceeds directly to the portal.
- If multiple roles are assigned to the account, the *Select a Role to Proceed* page opens, and the user must select a role before proceeding to the portal.



## Logging into an IdP role

Users can access FortiCloud using external IdP roles when logging in with their company's ID provider.

### To access the external IdP role:

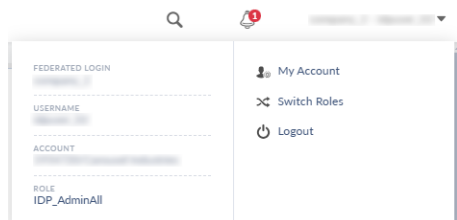
1. Log in using your company's ID provider. The log in portal opens.
2. Select the *Service Provider*.
3. Select *External IDP Role*. The roles available based on your credentials are displayed.
4. Hover over the role you want to choose and click *Select*.  
The *Dashboard* is displayed.

## Switching from an IdP role

If you are logged into an external IdP role, you can switch to another linked role.

### To switch to an IdP role:

1. Click the profile menu in the top right.



2. Select *Switch Roles*. The *Select a Role to Proceed* dialog is displayed.

## Select a Role to Proceed

Search an OU or account <input type="text"/>			<input type="checkbox"/> OU Name Only
ACCOUNT ID	COMPANY	ROLE NAME	
...	...	IDP_AdminAll	<a href="#">Current Role</a>
...	...	IDP_AdminAsset	
...	...	IDP_AdminIAM	
...	...	IDP_AdminAll	
...	...	IDP_AdminAll	
> ...	...	IDP_AdminAsset	
> ...	...	IDP_AdminAll	
...	...	IDP_AdminIAM	
...	...	IDP_AdminAll	
...	...	IDP_AdminAsset	

3. Hover over the role you want to change to and click **Select**.  
You will be redirected to the *Dashboard* of the selected account.

## Bulk updating users

You can take bulk actions on users statuses, including enabling, disabling, and deleting users.

### To enable users in bulk:

1. Select *Users* from the left-hand navigation menu. The *Users* page opens.
2. Select the users you want to enable. The bulk action buttons are displayed.

Users ⓘ

Search...

Total Records 7

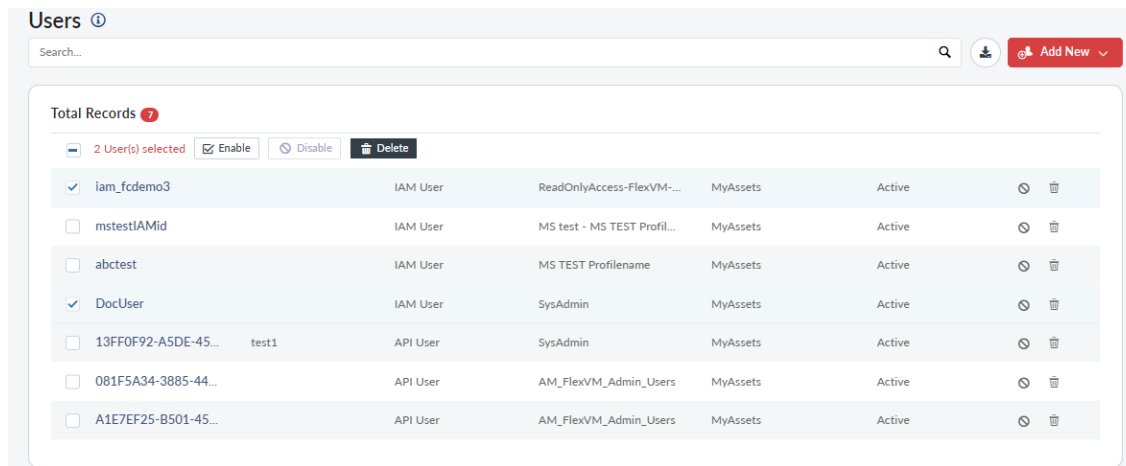
☒ 2 User(s) selected

<input checked="" type="checkbox"/>	iam_fcdemo3	IAM User	ReadOnlyAccess-FlexVM-...	MyAssets	Active	<input type="button" value="ⓘ"/>	<input type="button" value="🗑"/>	
<input type="checkbox"/>	mstestIAMid	IAM User	MS test - MS TEST Profil...	MyAssets	Active	<input type="button" value="ⓘ"/>	<input type="button" value="🗑"/>	
<input type="checkbox"/>	abctest	IAM User	MS TEST Profilname	MyAssets	Active	<input type="button" value="ⓘ"/>	<input type="button" value="🗑"/>	
<input checked="" type="checkbox"/>	DocUser	IAM User	SysAdmin	MyAssets	Active	<input type="button" value="ⓘ"/>	<input type="button" value="🗑"/>	
<input type="checkbox"/>	13FF0F92-A5DE-45...	test1	API User	SysAdmin	MyAssets	Active	<input type="button" value="ⓘ"/>	<input type="button" value="🗑"/>
<input type="checkbox"/>	081F5A34-3885-44...	API User	AM_FlexVM_Admin_Users	MyAssets	Active	<input type="button" value="ⓘ"/>	<input type="button" value="🗑"/>	
<input type="checkbox"/>	A1E7EF25-B501-45...	API User	AM_FlexVM_Admin_Users	MyAssets	Active	<input type="button" value="ⓘ"/>	<input type="button" value="🗑"/>	

3. Click **Enable**. The *Confirm to Enable User(s)* dialog is displayed.
4. Click **Yes, I want to continue**.

### To disable users in bulk:

1. Select *Users* from the left-hand navigation menu. The *Users* page opens.
2. Select the users you want to disable. The bulk action buttons are displayed.



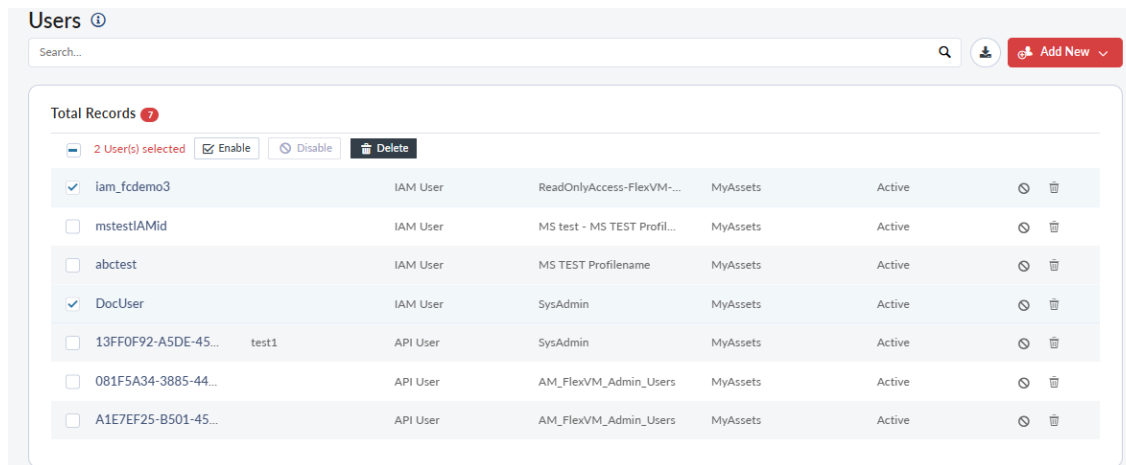
The screenshot shows the 'Users' page with a search bar and an 'Add New' button. Below the search bar, it indicates 'Total Records 7'. A selection bar shows '2 User(s) selected' and bulk action buttons for 'Enable', 'Disable', and 'Delete'. The table lists the following users:

Selected	User Name	User Type	Profile Name	Assets	Status	Actions
<input checked="" type="checkbox"/>	iam_fcdemo3	IAM User	ReadOnlyAccess-FlexVM-...	MyAssets	Active	
<input type="checkbox"/>	mstestIAMid	IAM User	MS test - MS TEST Profil...	MyAssets	Active	
<input type="checkbox"/>	abctest	IAM User	MS TEST Profilename	MyAssets	Active	
<input checked="" type="checkbox"/>	DocUser	IAM User	SysAdmin	MyAssets	Active	
<input type="checkbox"/>	13FF0F92-A5DE-45...	API User	SysAdmin	MyAssets	Active	
<input type="checkbox"/>	081F5A34-3885-44...	API User	AM_FlexVM_Admin_Users	MyAssets	Active	
<input type="checkbox"/>	A1E7EF25-B501-45...	API User	AM_FlexVM_Admin_Users	MyAssets	Active	

3. Click *Disable*. The *Confirm to Disable User(s)* dialog is displayed.
4. Click *Yes, I want to continue*.

### To delete users in bulk:

1. Select *Users* from the left-hand navigation menu. The *Users* page opens.
2. Select the users you want to delete. The bulk action buttons are displayed.



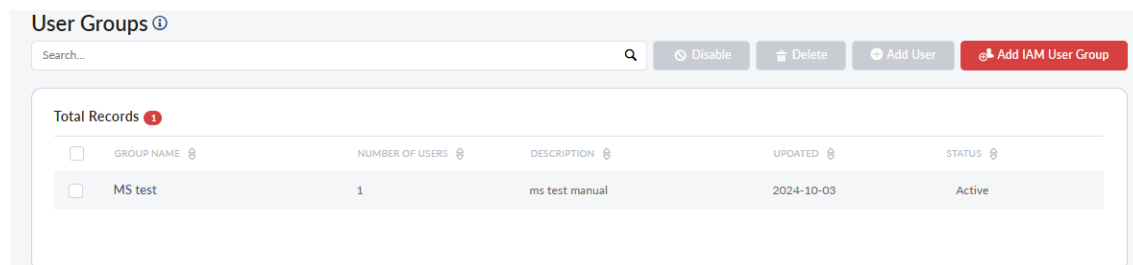
This screenshot is identical to the one above, showing the 'Users' page with the same list of users and bulk action buttons. The '2 User(s) selected' status is maintained.

3. Click *Delete*. The *Confirm to Delete User(s)* dialog is displayed.
4. Click *Yes, I want to continue*.

# User groups

User groups save time assigning asset and portal permissions to users. Use a group to create sets of conditions and then assign users to the group. A user can only belong to one group at a time.

The *User Groups* page can be accessed from the left-hand navigation menu. See [Identity & Access Management Portal on page 10](#).



This section contains the following topics:

- [Adding an IAM user group on page 49](#)
- [Managing IAM user groups on page 50](#)

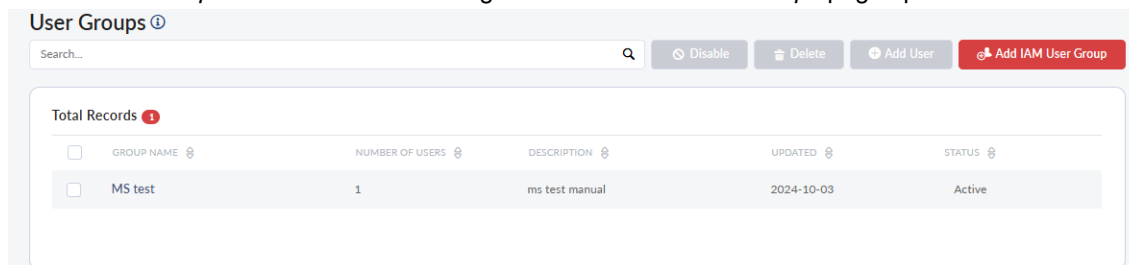
## Adding an IAM user group

Create a group of asset and portal permissions, and then assign users to the group.

Before you can create IAM user groups, you must create a permission profile. See [Permission profiles on page 16](#).

### To create a user group:

1. Select *User Groups* from the left-hand navigation menu. The *User Groups* page opens.



2. Click *Add IAM User Group*. The *IAM User Group Information* page is displayed.
3. In the *Group Name* field, enter a name for the group.
4. (Optional) In the *Description* field, describe the group.
5. (Optional) Set the *Status* to *Disabled*. The status is *Active* by default.
6. Click *Next*.
7. From the *Permission Scope* dropdown, select an asset folder.

8. In the *Permissions Profile* dropdown, select a profile. The *Permission Details* assigned to the selected profile are displayed.

**PERMISSION PROFILE**

Select a Permission Profile\*

Test ▼

**PERMISSION DETAILS**

Managed FortiGate				Overlay as a Service		
Access	Access Type	Additional Permission		Access	Access Type	Additional Permission
✓	Admin				Denied	

Asset Management			
Resources	Read Only	Read & Write	No Access
Entitlement Management ⓘ	✓		
Asset Maintenance ⓘ	✓		
Renewal Notice ⓘ			✓
Vulnerability List ⓘ			✓
Account Services ⓘ			✓



If the *SysAdmin* profile is selected, a message will display instead of portal cards to denote that the user has full access to the Asset Management, IAM, and FortiCare portals. *SysAdmin* has access to *Assets&Accounts* and *Support* but does not provide access to *Cloud Management* or *Cloud Services*. See [Creating a permission profile on page 19](#).

9. Click *Next*. The *Add IAM user(s)* page is displayed.
10. Assign users to the group.
- Click *Add User*.
  - (Optional) Click *Filter users by Group*, to view users in a group. Selecting a user in a group will remove the user from that group.
  - (Optional) Enter a username in the search bar, and enter the user name. As you type, partial results are returned.
  - Select the users and click *Add*.
  - Click *Next*. The *Confirmation* page is displayed.
11. Review the group permissions, and click *Confirm*.
12. (Optional) Click *Add Another Group*.

## Managing IAM user groups

You can update the members in a group and their permissions from the *Group Information* page. Use the *Status* setting to temporarily suspend a group's permissions.

The *User Group* page displays the following information:

Column	Description
Group Name	The name of the user group.

Column	Description
Number of Users	The number of users assigned to the group.
Description	The description of the group.
Updated	The date the group was updated.
Status	The group's status ( <i>Active/Disabled</i> )

This section contains the following topics:

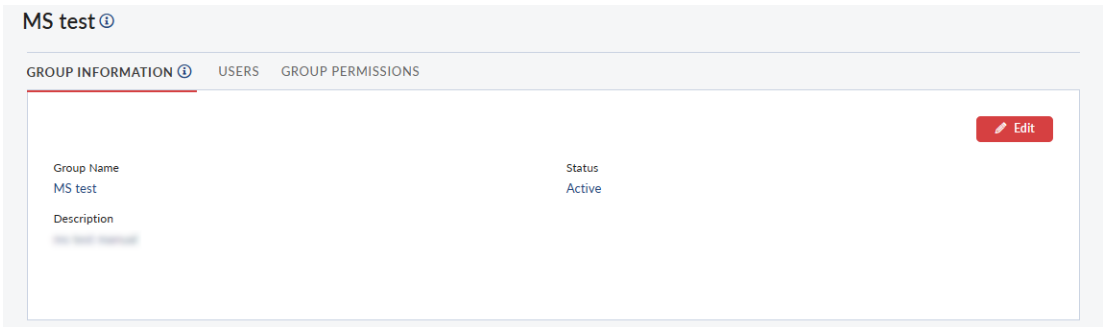
- [Editing user groups on page 51](#)
- [Adding and removing users on page 52](#)
- [Updating user group permission on page 53](#)

## Editing user groups

User groups can be added, edited, disabled, or deleted from the *User Groups* page.

### To update group details:

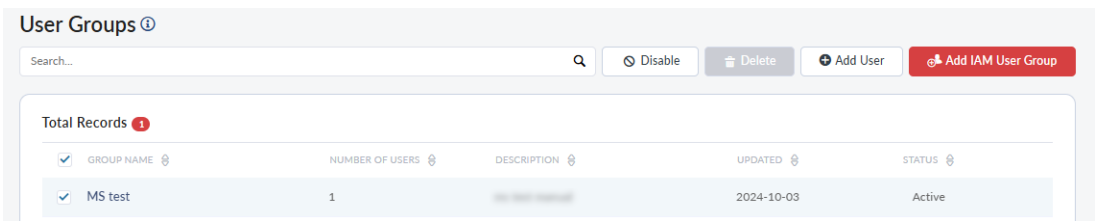
1. Select *User Groups* from the left-hand navigation menu. The *User Groups* page opens.
2. Click the *Group Name*. The *IAM User Groups / <name>* pane is displayed.



3. Click *Edit*.
4. Update the *Group Name*, *Status*, and *Description*, and then click *Update*.

### To disable a user group:

1. Select *User Groups* from the left-hand navigation menu. The *User Groups* page opens.
2. Select a group(s) in the list.



3. Click *Disable*. The *Permission Changed Confirmation* dialog opens.

- Click **Yes**. The group's *Status* is changed to *Disabled* and the members' portal permissions are suspended until you re-activate the group.

#### To activate a user group:

- Select *User Groups* from the left-hand navigation menu. The *User Groups* page opens.
- Click the *Group Name*. The *IAM User Group > <group\_name>* page is displayed.
- Click *Edit*.
- From the *Status* dropdown, select *Active*.

- Click *Update*. The group's *Status* changes to *Active* and the members' portal permissions are restored.

#### To delete a user group:



You cannot delete a group that has members or a group with *Status* of *Disabled*.

- Go to *IAM User Groups*.
- Select the user group(s), and click *Delete*. The *Permission Changed Confirmation* dialog is displayed.
- Click **Yes**. The group is removed from the list.

## Adding and removing users

Add or remove users from the *Users* tab in the group details page.

#### To add users to a group:

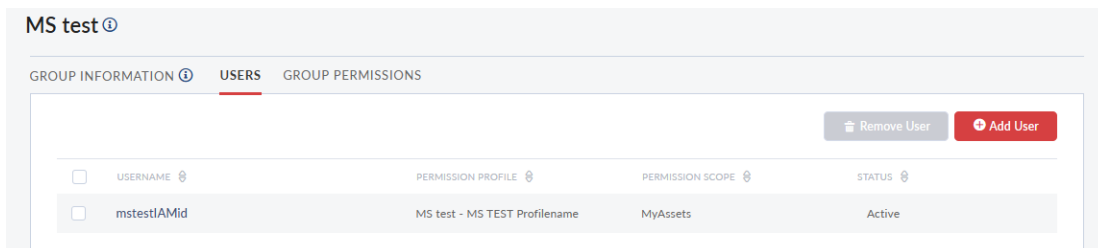
- Select *User Groups* from the left-hand navigation menu. The *User Groups* page opens.
- Select a user group, and click *Add User*. The *Add User:<group\_name>* dialog appears.
- Select users from the list. You can filter the list with the *Filter Users by Group* dropdown, or use the *Search* field to find a specific user.
- Click *Add*.



You can also add users to a group from the *Users* tab in the group details.

**To remove a user from a group:**

1. Select *User Groups* from the left-hand navigation menu. The *User Groups* page opens.
2. Click the *Group Name*. The *Manage IAM User Group > <group\_name>* page is displayed.
3. Click the *Users* tab.



4. Select the user(s), and then click *Remove User*. The *Remove User from User Group* dialog opens.
5. Configure the user's permission profile and click *Confirm*. If you do not configure the permissions the user will lose access to the portal.
6. Click *Confirm*.

## Updating user group permission

The *Permission Scope* and *Permission Profile* of a user group can be edited from the *Group Permissions* tab. Any changes made to *Group Permissions* will automatically affect any users within the group.

**To update portal permissions:**

1. Select *User Groups* from the left-hand navigation menu. The *User Groups* page opens.
2. Click the *Group Name*. The *IAM User Group > <group\_name>* page is displayed.
3. Click the *Group Permissions* tab.
4. Click *Edit*.
5. Select the *Permission Scope* from the dropdown list.
6. Select the *Permission Profile* from the dropdown list.
7. Click *Update*.

# Migrating sub users

You can migrate a sub user account from FortiCloud and convert it to an IAM user. After a sub user is migrated, they are required to update their login credentials the next time they access a portal.



Most of the Fortinet Inc. Cloud portals support IAM users at this time.

After migration is complete:

- The sub user is automatically removed from your FortiCloud account. A sub user cannot be restored in FortiCloud.
- The user's data and settings in the cloud portals are migrated with the user.

The *Migrate Sub Users* page can be accessed from the left-hand navigation menu. See [Identity & Access Management Portal on page 10](#).

## FortiGate Cloud Legacy users

A FortiGate Cloud Legacy user can be migrated to an IAM user using the same process as a sub user. If Legacy users are available for migration, they will be listed in the active sub users page in the *Source* column. Select *Ignore FortiGate Cloud legacy user* to hide the *Source* column.

3. Select active Sub User(s)

Total Records 1						<input type="checkbox"/> Ignore FortiGateCloud legacy users
<input type="checkbox"/>	FULL NAME	EMAIL	PHONE	DESCRIPTION	SOURCE	ACCESS LEVEL
<input type="checkbox"/>	John Doe	john.doe@corp.com	999-999-9999		Sub User	Full
<input type="checkbox"/>	Jane	jane@corp.com	1234567890		Sub User	Full
<input type="checkbox"/>	Bob	bob@corp.com	555-555-5555		Sub User	Full
<input type="checkbox"/>	John Doe, Jr.	john.doe.jr@corp.com	555-555-5555	John Doe, Jr.	Sub User	Full
<input type="checkbox"/>	Bob	bob@corp.com	555-555-5555		Sub User	Full
<input type="checkbox"/>	Test User	test.user@corp.com			Legacy User	ReadOnly
<input type="checkbox"/>	Test User	test.user@corp.com			Legacy User	ReadOnly
<input type="checkbox"/>	Test User	test.user@corp.com			Legacy User	ReadOnly
<input type="checkbox"/>	Test User	test.user@corp.com			Legacy User	ReadOnly



When you are migrating FortiGate Cloud Legacy users and assigning permission profiles for the new IAM users, if the permission profile selected does not have FortiGate Cloud permissions enabled, an error will display and the Legacy users cannot be migrated.

**To migrate a sub or Legacy user:**

1. Select *Migrate Sub Users* from the left-hand navigation menu.

1. Sub User Migration Agreement

PLEASE READ THE FOLLOWING INFORMATION CAREFULLY:

- Following migration, current Sub User(s) will be automatically removed from your FortiCloud account
- Newly created IAM users will need to set new Security Credentials (password and token) for themselves
- IAM user support can differ from portal to portal, please verify your permission and access once the migration is complete
- Some Cloud Portals don't currently support IAM users

☐ I have read, understood and accepted the statements above

Next

2. Read and accept the terms of migration, and click *Next*.
3. Select a User ID formatting option, and click *Next*.

Format	Description
Use email account name	Maps the user's FortiCloud <i>Email (Account ID)</i> to the IAM <i>User ID</i> field.
Use username as ID and filter with space	Maps the user's FortiCloud <i>Name</i> to the IAM <i>User ID</i> field.

4. Select users from the list, and click *Next*.

3. Select active Sub User(s)

Total Records 9 ☐ Ignore FortiGateCloud legacy users

<input type="checkbox"/>	FULL NAME	EMAIL	PHONE	DESCRIPTION	SOURCE	ACCESS LEVEL
<input type="checkbox"/>	John Doe	John.Doe@fortinet.com	999-999-9999		Sub User	Full
<input type="checkbox"/>	Jane	Jane@fortinet.com	111-111-1111		Sub User	Full
<input type="checkbox"/>	Bob	Bob@fortinet.com	111-111-1111		Sub User	Full
<input type="checkbox"/>	William B. McCloud	William.B.McCloud@fortinet.com	111-111-1111	William B. McCloud	Sub User	Full
<input type="checkbox"/>	Bob	Bob@fortinet.com	111-111-1111		Sub User	Full
<input type="checkbox"/>	Test user	Test.user@fortinet.com			Legacy User	ReadOnly
<input type="checkbox"/>	Test user	Test.user@fortinet.com			Legacy User	ReadOnly
<input type="checkbox"/>	Test user	Test.user@fortinet.com			Legacy User	ReadOnly
<input type="checkbox"/>	Test user	Test.user@fortinet.com			Legacy User	ReadOnly

The *User Details* page is displayed.



Select *Ignore FortiGate Cloud legacy user* to hide the *Source* column.

5. Review the user's details, and click *Next*. The *User Group, Asset and Portal Permissions* pane opens.

5. User Group, Asset and Portal Permissions

**BASIC INFO**

Do you want your permission controlled by an IAM User Group?

The User will adopt the permissions of the assigned User Group. You cannot edit the User's Asset or Portal Permissions while the User is assigned to a Group. Remove the User from the Group to enable editing of their permissions.

Yes No

Select a Type\*

Select the type as Local for accessing the current account and Organization for accessing the OU accounts

Local

**PERMISSION SCOPE**

Asset Permissions \*

My Assets

**PERMISSION PROFILE**

Select a Permission Profile\*

None



Legacy users being migrated must be assigned to a permission profile with FortiGate Cloud permissions enabled.

6. (Optional) Add the user to an IAM user group. See [User groups on page 49](#).
  1. Select Yes from *Basic Info*, and select a group from the dropdown.
  2. Click *Next* to proceed to Step 10.
7. Select an asset folder from the *Asset Permissions* dropdown.
8. Select a permission profile from the *Choose A Permission Profile* dropdown.
9. Click *Next*. The *Confirmation of Sub User(s) to migrate* page is displayed.
10. Click *Confirm*. The *Confirmation* page is displayed.
11. Click *Download IAM User Credentials* and send them to the user.

# Account management

Use the Account menu to update your account information, change your password and enable Two-Factor Authentication. To open the account menu, click the your account email at the top-right of the page.

This section contains the following topics:

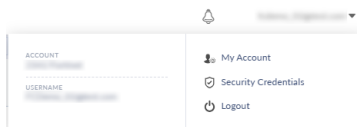
- [My Account on page 57](#)
- [User Information on page 62](#)
- [Security Credentials on page 63](#)

## My Account

Use the *My Account* portal to update your account information and preferences. You can also use the portal to enable the Organizations feature.

**To access the My Account portal:**

1. Log in to [FortiCloud](#). The *Asset Management* portal opens.
2. At the top-right of the page, click the Account menu. This is your email address.



3. Click *My Account*. The *Account Profile* page opens.

Account	fname 1015827 lname 1015827	Company: company 1015827 Title: title 1015827 Email: 1015827@test.com Telephone: phone 1015827	Activated Since 2020-02-20
---------	-----------------------------	---	-------------------------------

**Account**

- Account Profile
- Change Account ID (Email)
- Manage User
- My Account (IAM version)

### Account Profile

#### Account Information

company

Phone:

Industry:

Organization Size:

#### Master User

Email:

Name:

Title:

All ticket process via Email:

*For more information about Email Interaction, please [Click Here](#)*

Edit

4. Click *My Account (IAM version)*. The *Credential Portal* opens.

**IDENTITY MANAGEMENT**

- Account Profile
- Account Preferences

My Account / Account Profile

### Account Profile

EDIT

#### ACCOUNT INFORMATION

Account ID	Account Alias
Company Fortinet	Address
Phone	Fax
Industry Technology	Organization Size 1000-2499 employees

#### MASTER USER

First Name	Last Name
Title Miss	Email

## Account Profile

The *Account Profile* page displays the *Account Information* such as the company name and address, as well is the name and contact information of the master user for the account. Only the master user can access the *Account Profile*.

The master user is the person who created the account. An account can only have one master user. You cannot change the master user of the account. Master users can add users to the account and assign roles, permissions, and assets to the users.

The screenshot shows the 'Account Profile' page within the 'IDENTITY MANAGEMENT' section. The page is titled 'Account Profile' and has an 'EDIT' button in the top right corner. The page is divided into two main sections: 'ACCOUNT INFORMATION' and 'MASTER USER'. The 'ACCOUNT INFORMATION' section contains fields for Account ID, Account Alias, Company (Fortinet), Address, Phone, Fax, Industry (Technology), and Organization Size (1000-2499 employees). The 'MASTER USER' section contains fields for First Name, Last Name, Title (Miss), and Email. A 'Document Library' icon is visible in the bottom left corner.

### To edit the Account Profile:

1. Go to *Account Profile*.
2. Click *Edit*.
3. Update the account information and click *Update*.

## Account Preferences

Use the *Account Preferences* page to enable ticket processing by email and link a partner to the account by default.

### PSIRT Contact

You can specify a *PSIRT Contact* to receive Monthly and Out-of-cycle Critical PSIRT Advisories. This ensures that the emails are directed to the appropriate contact.

## To add a *PSIRT Contact*:

1. Log in as a Master Account user and go to *My Account*.

The screenshot shows the 'Account Profile' page. At the top, there's a header with 'Account' and a green banner. Below the banner, a sidebar on the left lists 'Account Profile', 'Change Account ID (Email)', 'Manage User', and 'My Account (IAM version)'. The main content area is titled 'Account Profile' and contains two sections: 'Account Information' and 'Master User'. The 'Account Information' section includes fields for 'Fortinet', 'Phone', 'Industry', and 'Organization Size'. The 'Master User' section includes fields for 'Email', 'Name', and 'Title'. A note at the bottom states 'All ticket process via Email: Y' and provides a link for more information about email interaction. An 'Edit' button is located at the bottom right of the 'Master User' section.

2. Select *My Account (IAM version)*.

The screenshot shows the 'Account Profile' page with the 'My Account' section selected. The sidebar on the left lists 'Account Profile' and 'Account Preferences'. The main content area is titled 'Account Profile' and contains two sections: 'ACCOUNT INFORMATION' and 'MASTER USER'. The 'ACCOUNT INFORMATION' section includes fields for 'Account ID', 'Account Alias', 'Company', 'Address', 'Phone', 'Fax', 'Industry', and 'Organization Size'. The 'MASTER USER' section includes fields for 'First Name', 'Last Name', 'Title', and 'Email'. An 'EDIT' button is located at the top right of the 'ACCOUNT INFORMATION' section.

3. Select *Account Preferences*.

The screenshot shows the 'Account Preferences' page. The sidebar on the left lists 'Account Profile' and 'Account Preferences'. The main content area is titled 'Account Preferences' and contains a section for 'Consolidate all your accounts into an Organization'. Below this, there are two sections: 'TICKET PROCESSING' and 'DEFAULT PARTNER'. The 'TICKET PROCESSING' section includes a checkbox for 'Allow Ticket Processing by Email' and a dropdown menu for 'None'. The 'DEFAULT PARTNER' section includes a text input field for 'PSIRT CONTACT'. An 'EDIT' button is located at the top right of the 'Consolidate all your accounts into an Organization' section.

4. Click *Edit*.
5. Add the contact in the *PSIRT Contact* field.
6. Click *Update*.

## Ticket Processing

*Enabling Ticket Processing by Email* allows Customer Support to manage your help desk processes via email as well as other built-in procedures. Ticket processing by email automatically routes tickets to the proper technician and updates your customer.

### To enable ticket processing by email:

1. Go to *Account Preferences*.
2. Click *Edit*.
3. Select *Allow Ticket Processing by Email*.
4. Click *Update*.

## Default Partner

You can select a partner to be linked to this account by default. You can change this selection at any time.

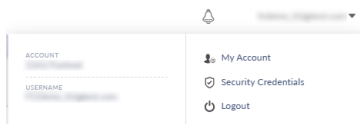
1. Go to *Account Preferences*.
2. Click *Edit*.
3. From the *Default Partner* dropdown, select a partner account from the list.
4. Click *Update*.

## Creating connected accounts (Partners)

Partners can be connected to one account, or connected to multiple accounts as a master or sub user.

### To create a connected account:

1. Click the Account dropdown (your email) and select *My Account*. You are redirected to FortiCloud.



2. Click *Connect Account*. The *Connect Registered Account* page opens.

 A screenshot of the 'Connect Registered Account' page. The page has a green header with a 'PARTNER' label and a background image of green leaves. The header also displays 'Fortinet (Americas)', 'Email:', and a 'Connected Account' section with fields for Name, Telephone, Address, Postal Code, Region, and a large number '22'. On the left, a sidebar titled 'Manage Account' contains links for 'Connected Accounts', 'Create an Account', and 'Connect Account' (which is highlighted). The main content area is titled 'Connect Registered Account' and contains a 'Connect Account' section with two input fields: 'Account ID (Email):\*' and 'Password:\*. A blue 'Search' button is located to the right of the password field.

3. Click *Account ID (Email)* and select a user from the list. The *Password* field is updated.

4. Click *Search*. The available accounts are displayed.

PARTNER

Fortinet (Americas)  
Email:

Name:  
Telephone:  
Address:  
Postal Code:  
Region:

Connected Account  
22

Manage Account

Connected Accounts

Create an Account

Connect Account

Connect Registered Account

Connect Account

Account ID (Email):\*

Password:\*

Search

Account	Company	Name	Email
<input type="checkbox"/>			

Connect

5. Select the account(s) and click *Connect*.

# User Information

If you are logged in as an IAM user, you can access the *User Information* page from the profile menu.

ACCOUNT  
Fortinet

USERNAME  
DocUser

My Account

User Information

Security Credentials

Logout

The *User Information* page provides information on your current IAM user account in multiple tabs:

- *User Profile*: Displays information about your current IAM user account, including *Name*, *Phone*, *Account ID*, *Email*, and *Username*.

IDENTITY MANAGEMENT

User Profile

Permissions

User Information

EDIT

USER PROFILE

Name  
Doc Test

Phone  
+1 5551234

Account ID  
123456789

Group

Registration Date  
2024-10-18

Email  
test@doc.com

Username  
DocUser

Account Alias

Status  
Active

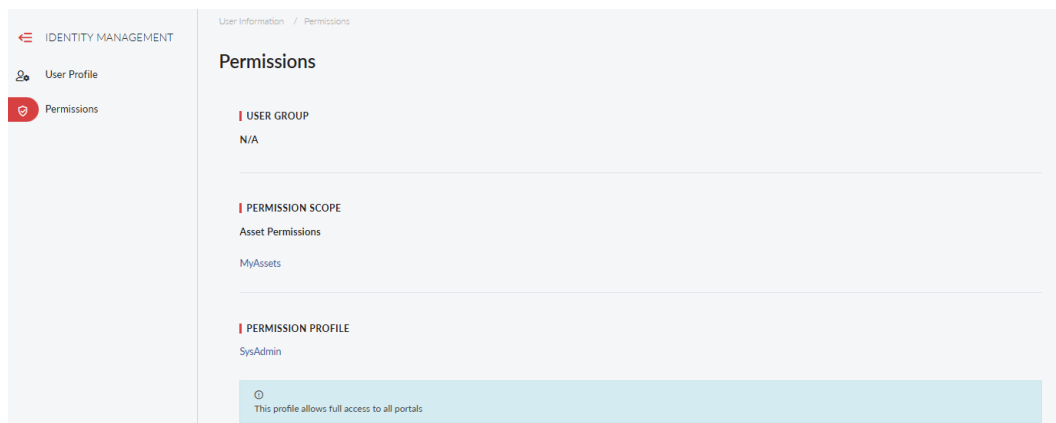
Description  
N/A

USER TYPE

User Type  
IAMUser

- *Permissions*: Displays information about your permission scope, current permission profile, and any user group

your IAM user is a part of.



## Security Credentials

Use the *Security Credentials* settings to change your account password, update your contact information, and enable Two-Factor Authentication (2FA).

This section contains the following topics:

- [Password on page 63](#)
- [Contacts on page 65](#)
- [Two-Factor Authentication on page 70](#)

### Password

The account password can be managed in the *Security Credentials > Change Password* page.

#### To change the account password:

1. Click the account menu at the top-right of the page. This is your account email address.
2. Click *Security Credentials*. The *Change Password* page opens.
3. Click *Edit*.

A screenshot of the 'Change Password' form. It has a title 'Change Password' and two buttons: 'CANCEL' and 'UPDATE'. The form contains two input fields: 'New Password: \*' and 'Confirm New Password: \*'. Below the fields, there are password requirements: 'Minimum 8 characters', 'Must contain numbers (0-9)', 'Both uppercase (A-Z) and lowercase (a-z) letters', and 'Some special characters'.

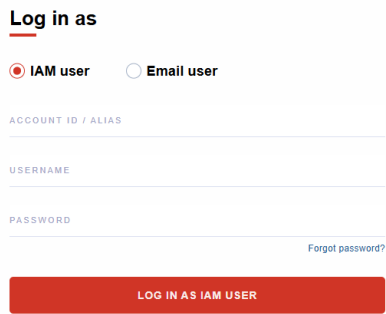
4. In the *New Password* field, enter your new password.
5. In the *Confirm New Password* field, re-enter you new password.
6. Click *Update*.

## Resetting the account password

If you have forgotten your password, you can reset the password in the login page.

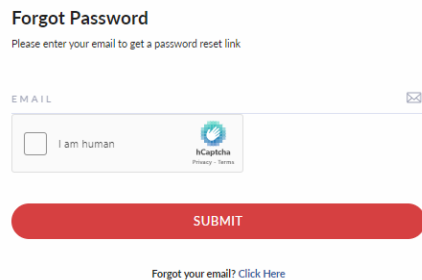
### To reset the password:

1. On the login page, click *Forgot password?*.



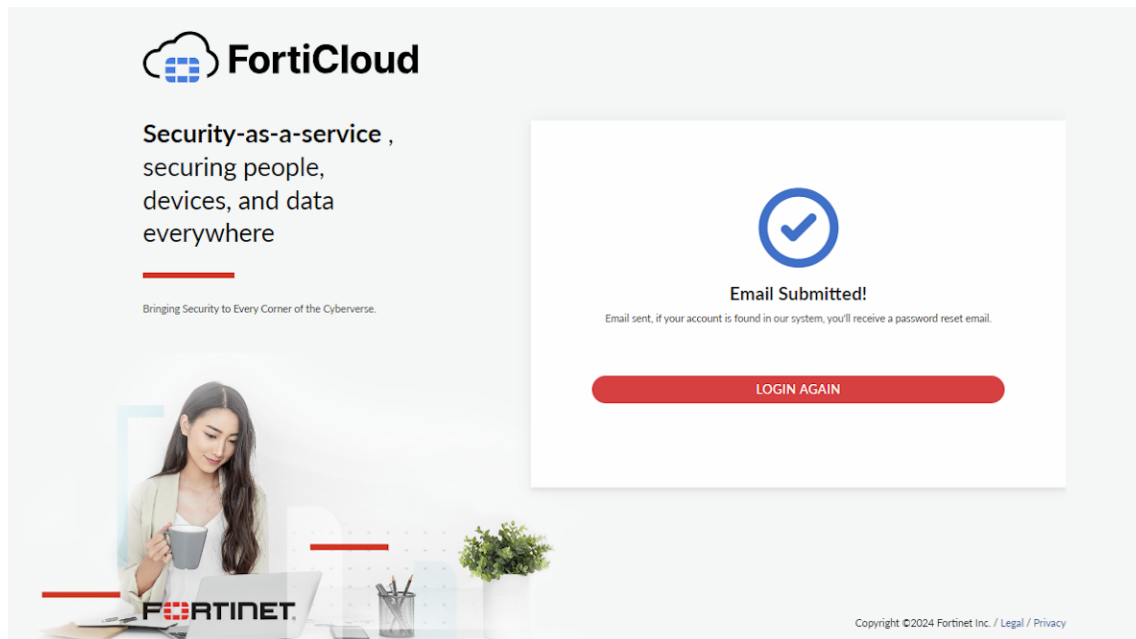
The screenshot shows the 'Log in as' section of the login page. It features two radio buttons: 'IAM user' (selected) and 'Email user'. Below these are three input fields labeled 'ACCOUNT ID / ALIAS', 'USERNAME', and 'PASSWORD'. A link 'Forgot password?' is located to the right of the password field. At the bottom is a red button labeled 'LOG IN AS IAM USER'.

2. Enter the account information:
  - a. Enter the account *Email*.
  - b. Select *I am a human*.



The screenshot shows the 'Forgot Password' section. It has a heading 'Forgot Password' and a subtext 'Please enter your email to get a password reset link'. Below this is an email input field with a placeholder 'EMAIL' and an envelope icon. Under the input field is a box containing an 'I am human' checkbox and a reCAPTCHA logo. At the bottom is a red button labeled 'SUBMIT'. A link 'Forgot your email? Click Here' is located below the button.

3. Click *Submit*. An email will be sent that includes a reset link.



4. Follow the instructions in the email.
5. If you have Two-Factor Authentication enabled:
  - a. Enter the FortiToken, SMS code, or both in the provided fields.



The verification codes required when resetting your password depends on the information included in your account. If you have FortiToken enabled and a mobile number included in your account, you will be required to enter verifications received from both methods. If you only have one method included in your account, you will only be required to enter one verification code. See [Contacts on page 65](#) and [Two-Factor Authentication on page 70](#).

- b. Click *Confirm*.
6. Enter the new password twice in the *Reset Password* link.
7. Click *Reset Password*.
8. Log into your account using the new password.

## Contacts

The *Contacts* page contains information on your email address and mobile number, which can be used for Two-Factor Authentication codes, notifications, or FortiToken and password retrieval. See [Password on page 63](#) and [Two-Factor Authentication on page 70](#).

### Email address

The account email address is used for one-time password verification, notifications, and FortiToken or password retrieval.

**To update the email address:**

1. Click the account menu at the top-right of the page.
2. Go to *Security Credentials > Contacts*.

**Contacts**  
Set up your email and mobile number to receive security codes for secure logins. Stay protected by keeping your information up-to-date.

**Set Up Your Contact Settings To Receive Security Codes**

**EMAIL ADDRESS**  
Please enter an email address where you can receive your One-Time Password (OTP) for each login. Ensure it's accessible for receiving notifications to safeguard your credentials effectively.

Notification Email\*

**MOBILE NUMBER**  
Please provide a mobile number to receive SMS codes and assist in retrieving your FortiToken or password if necessary.

Mobile Number

3. Enter the new email address in the *Notification Email* field.

**Contacts**  
Set up your email and mobile number to receive security codes for secure logins. Stay protected by keeping your information up-to-date.

**Set Up Your Contact Settings To Receive Security Codes**

**EMAIL ADDRESS**  
Please enter an email address where you can receive your One-Time Password (OTP) for each login. Ensure it's accessible for receiving notifications to safeguard your credentials effectively.

Notification Email\*

**MOBILE NUMBER**  
Please provide a mobile number to receive SMS codes and assist in retrieving your FortiToken or password if necessary.

Mobile Number

4. Click *Update*.
5. Enter your password in the *Verify Identity* dialog.

**Contacts**  
Set up your email and mobile number to receive security codes for secure logins. Stay protected by keeping your information up-to-date.

**Set Up Your Contact Settings To Receive Security Codes**

**EMAIL ADDRESS**  
Please enter an email address where you can receive your One-Time Password (OTP) for each login. Ensure it's accessible for receiving notifications to safeguard your credentials effectively.

Notification Email\*

**MOBILE NUMBER**  
Please provide a mobile number to receive SMS codes and assist in retrieving your FortiToken or password if necessary.

Mobile Number

**Verify Identity**  
Enter your password to save your changes.

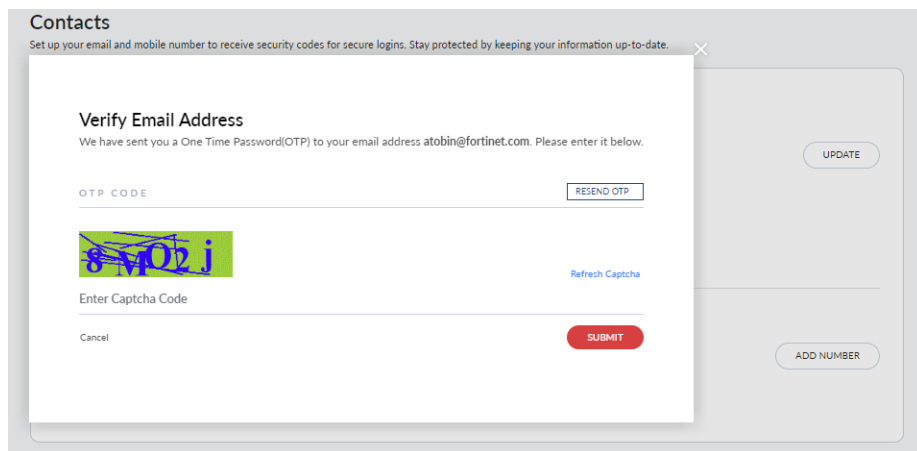
PASSWORD

Cancel

SUBMIT

6. Click *Submit*.

7. Verify your email address:
  - a. Enter the *One Time Password* that was emailed to you.
  - b. Enter the *Captcha Code*.
  - c. Click *Submit*.



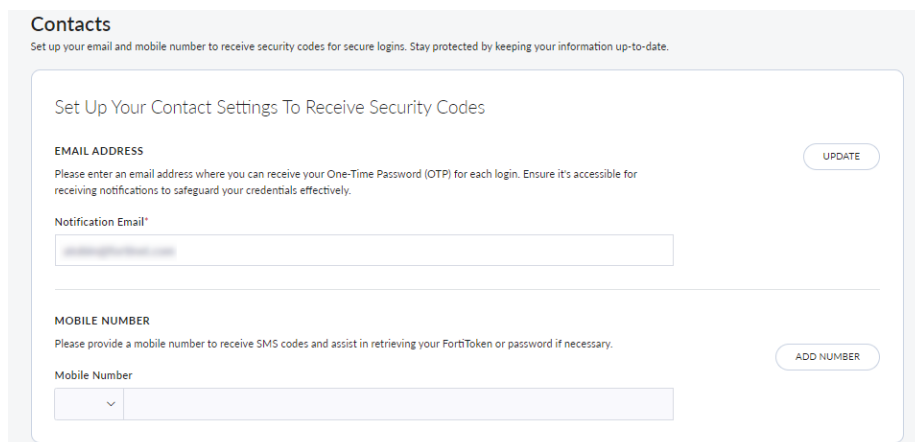
The screenshot shows a 'Verify Email Address' modal window. The title is 'Verify Email Address'. Below the title, it says: 'We have sent you a One Time Password(OTP) to your email address atobin@fortinet.com. Please enter it below.' There is a text input field for the 'OTP CODE' with a 'RESEND OTP' button to its right. Below the input field is a captcha image showing the characters '8402j'. To the right of the captcha is a 'Refresh Captcha' link. Below the captcha is another text input field labeled 'Enter Captcha Code'. At the bottom left of the modal is a 'Cancel' link, and at the bottom right is a red 'SUBMIT' button. In the background, the 'Contacts' page is visible, showing an 'UPDATE' button and an 'ADD NUMBER' button.

## IAM users

If an IAM user is updating the email address in the *Contacts* page, the IAM user email address will also change in the *Users > IAM Users > User Profile* tab in the Identity & Access Management portal. See [Managing IAM users on page 29](#).

### To change the email address of an IAM user:

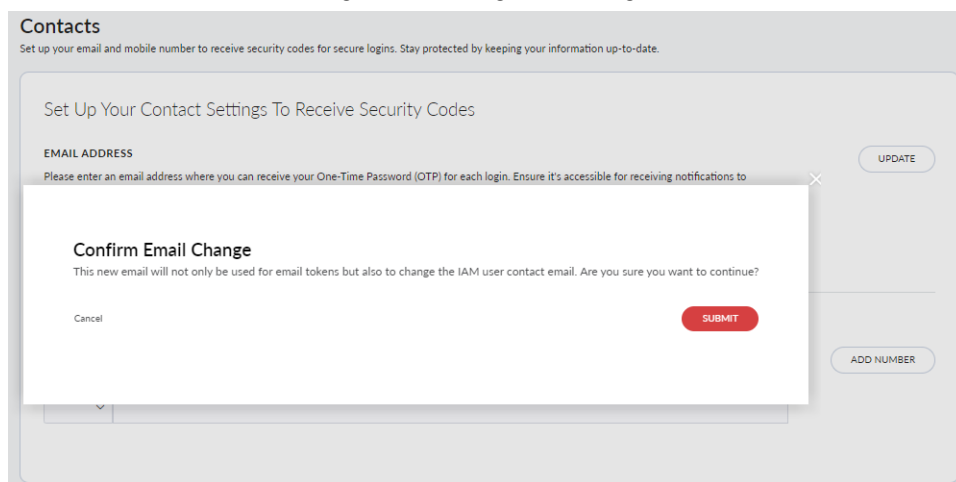
1. Click the account menu at the top-right of the page.
2. Go to *Security Credentials > Contacts*.
3. Enter the new email address in the *Notification Email* field.



The screenshot shows the 'Contacts' page. The title is 'Contacts'. Below the title, it says: 'Set up your email and mobile number to receive security codes for secure logins. Stay protected by keeping your information up-to-date.' There is a section titled 'Set Up Your Contact Settings To Receive Security Codes'. Inside this section, there is a sub-section 'EMAIL ADDRESS' with the text: 'Please enter an email address where you can receive your One-Time Password (OTP) for each login. Ensure it's accessible for receiving notifications to safeguard your credentials effectively.' There is a text input field for the 'Notification Email' with the value 'atobin@fortinet.com'. To the right of the input field is an 'UPDATE' button. Below the 'EMAIL ADDRESS' section is a sub-section 'MOBILE NUMBER' with the text: 'Please provide a mobile number to receive SMS codes and assist in retrieving your FortiToken or password if necessary.' There is a text input field for the 'Mobile Number' with a dropdown arrow on the left. To the right of the input field is an 'ADD NUMBER' button.

4. Click *Update*.

5. Click **Submit** in the email change acknowledgment dialog.



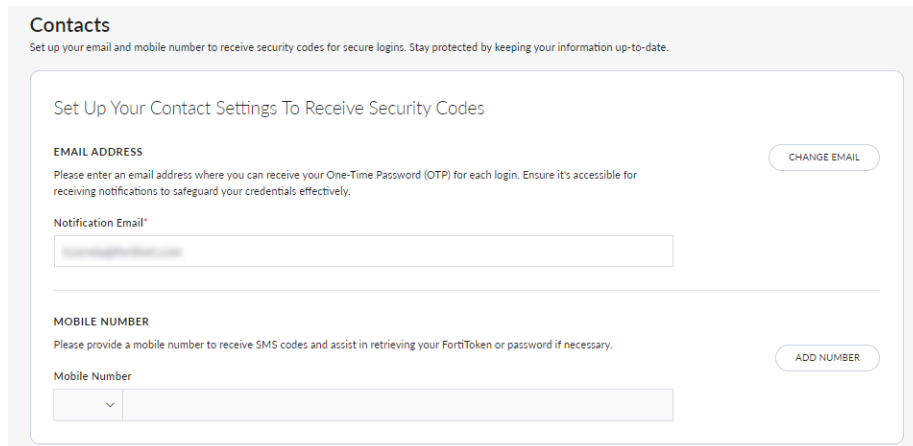
The screenshot shows the 'Contacts' settings page. At the top, it says 'Set up your email and mobile number to receive security codes for secure logins. Stay protected by keeping your information up-to-date.' Below this is a section titled 'Set Up Your Contact Settings To Receive Security Codes'. There are two main sections: 'EMAIL ADDRESS' and 'MOBILE NUMBER'. The 'EMAIL ADDRESS' section has a text input field with a placeholder 'Please enter an email address where you can receive your One-Time Password (OTP) for each login. Ensure it's accessible for receiving notifications to'. To the right of this field is an 'UPDATE' button. The 'MOBILE NUMBER' section has a dropdown menu for the region code and a text input field for the number. To the right of this field is an 'ADD NUMBER' button. A modal dialog box titled 'Confirm Email Change' is overlaid on the page. It contains the text: 'This new email will not only be used for email tokens but also to change the IAM user contact email. Are you sure you want to continue?'. At the bottom of the dialog are two buttons: 'Cancel' and 'SUBMIT'.

## Mobile number

The account mobile number is used for one-time password verification, and FortiToken or password retrieval.

### To add a mobile number:

1. Click the account menu at the top-right of the page.
2. Go to *Security Credentials > Contacts*.



The screenshot shows the 'Contacts' settings page. At the top, it says 'Set up your email and mobile number to receive security codes for secure logins. Stay protected by keeping your information up-to-date.' Below this is a section titled 'Set Up Your Contact Settings To Receive Security Codes'. There are two main sections: 'EMAIL ADDRESS' and 'MOBILE NUMBER'. The 'EMAIL ADDRESS' section has a text input field with a placeholder 'Please enter an email address where you can receive your One-Time Password (OTP) for each login. Ensure it's accessible for receiving notifications to safeguard your credentials effectively.' To the right of this field is a 'CHANGE EMAIL' button. The 'MOBILE NUMBER' section has a dropdown menu for the region code and a text input field for the number. To the right of this field is an 'ADD NUMBER' button.

3. Select a region code and enter the mobile number.

**Contacts**  
Set up your email and mobile number to receive security codes for secure logins. Stay protected by keeping your information up-to-date.

**Set Up Your Contact Settings To Receive Security Codes**

**EMAIL ADDRESS**  
Please enter an email address where you can receive your One-Time Password (OTP) for each login. Ensure it's accessible for receiving notifications to safeguard your credentials effectively.

Notification Email\*

**MOBILE NUMBER**  
Please provide a mobile number to receive SMS codes and assist in retrieving your FortiToken or password if necessary.

Mobile Number

+1

CHANGE EMAIL

UPDATE

4. Click *Update*.
5. Enter your password in the *Verify Identity* dialog.

**Contacts**  
Set up your email and mobile number to receive security codes for secure logins. Stay protected by keeping your information up-to-date.

**Verify Identity**  
Enter your password to save your changes.

PASSWORD

Cancel

SUBMIT

CHANGE EMAIL

UPDATE

Mobile Number

+1

6. Click *Submit*.
7. Verify your mobile number:
  - a. Enter the verification code that was texted to your mobile number in the *SMS Code* field.
  - b. Enter the *Captcha Code*.
  - c. Click *Submit*.

**Contacts**  
Set up your email and mobile number to receive security codes for secure logins. Stay protected by keeping your information up-to-date.

**Verify Your Mobile Number**  
We have sent you a 6-digit SMS code to +1 . Please enter it here. The code will expire in 5 minutes.

SMS CODE

Resend SMS Code

8 6 4 x v

Refresh Captcha

Enter Captcha Code

Cancel

SUBMIT

CHANGE EMAIL

UPDATE

**To remove a mobile number:**

1. Click the account menu at the top-right of the page.
2. Go to *Security Credentials > Contacts*.
3. Click *Remove Number* in the *Mobile Number* section.



If SMS tokens are enabled for Two-Factor Authentication, you must change the Two-Factor Authentication method before you can remove the mobile number. See [Switching Two-Factor Authentication methods on page 73](#).

---

## Two-Factor Authentication

Two-Factor Authentication (2FA) requires users to enter a security code to log in to a portal.

Users can choose to receive Two-Factor Authentication security codes sent to them through FortiToken, SMS, email, or a third-party authenticator each time they log in. Email authentication is enabled as the default method for new accounts. However, FortiToken is the recommended method of authentication for greater security.

FortiToken Two-Factor Authentication is enforced for all email account users if it has been selected at the Organization or Account level that the email account belongs to.

This section contains the following topics:

- [Enabling Two-Factor Authentication on page 70](#)
- [Logging in with Two-Factor Authentication for the first time on page 72](#)
- [Switching Two-Factor Authentication methods on page 73](#)
- [Resetting tokens for Two-Factor Authentication on page 74](#)



For information on transferring tokens from one mobile device to another for Two-Factor Authentication, see the [FortiToken Frequently Asked Questions](#) guide.

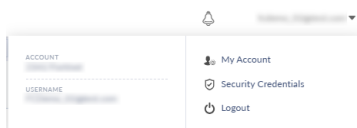
---

## Enabling Two-Factor Authentication

You can select the Two-Factor Authentication method at the user level or the account level. See [Settings](#) in the Organization Portal guide for information on enforcing Two-Factor Authentication at the Organization level.

**To enable Two-Factor Authentication for your account:**

1. Click the *Account* menu at the top-right of portal and select *Security Credentials*.



2. In the navigation pane, click *Two Factor Authentication*. The *Two Factor Authentication* page opens.

## Two-Factor Authentication

Two-Factor Authentication requires you to enter a security code to log in to a portal to enhance the security of your account.

**Please enable Two-Factor Authentication (2FA) for your login. Our system will soon enforce 2FA with email as the default method, but we strongly suggest choosing FortiToken for added convenience and optimal security.**

### Select Your Two-Factor Authentication Method

#### FORTITOKEN

Use this option if you want to use your mobile device as security device, you will need to download and install FortiToken Mobile application from Apple App Store or Google Play Store. For more details about how to use FortiMobile Token please click [here](#).



#### EMAIL

Use this two-factor authentication option to receive an email containing a One-Time Password(OTP). For details on how to use and update your email id, please click [here](#).



#### SMS

Use this two-factor authentication option to receive a SMS containing a secure code. For details on how to use and update your mobile number, please click [here](#).



#### THIRD-PARTY AUTHENTICATOR APP

Use this option if you want to use external Authenticator apps, you will need to download and install authenticator apps such as Microsoft Authenticator, Google Authenticator, etc from Apple App Store or Google Play Store. For more details about how to use Authenticator apps (other) please click [here](#).



### 3. Enable the Two-Factor Authentication option you prefer.

## Two-Factor Authentication

Two-Factor Authentication requires you to enter a security code to log in to a portal to enhance the security of your account.

CANCEL

UPDATE

**Please enable Two-Factor Authentication (2FA) for your login. Our system will soon enforce 2FA with email as the default method, but we strongly suggest choosing FortiToken for added convenience and optimal security.**

### Select Your Two-Factor Authentication Method

#### FORTITOKEN

Use this option if you want to use your mobile device as security device, you will need to download and install FortiToken Mobile application from Apple App Store or Google Play Store. For more details about how to use FortiMobile Token please click [here](#).



#### EMAIL

Use this two-factor authentication option to receive an email containing a One-Time Password(OTP). For details on how to use and update your email id, please click [here](#).



#### SMS

Use this two-factor authentication option to receive a SMS containing a secure code. For details on how to use and update your mobile number, please click [here](#).



#### THIRD-PARTY AUTHENTICATOR APP

Use this option if you want to use external Authenticator apps, you will need to download and install authenticator apps such as Microsoft Authenticator, Google Authenticator, etc from Apple App Store or Google Play Store. For more details about how to use Authenticator apps (other) please click [here](#).



While email authentication is the default method, FortiToken is the recommended Two-Factor Authentication method to give your account the best security. Email accounts that already have email-based Two-Factor Authentication enabled cannot change the email address used and are encouraged to switch to FortiToken. See [Switching Two-Factor Authentication methods on page 73](#).



SMS Two-Factor Authentication will only be available if a mobile number has been added to the account. See [Contacts on page 65](#).

---

4. Click *Update*.
5. A verification dialog will open. The dialog that appears is dependent on the authentication method you chose. Follow the steps provided in the dialog to complete verification.
6. Click *Submit*.

## Managing user authentication

You can edit the email address used for Two-Factor Authentication for a user in the *User > User Profile* tab. See [Managing IAM users on page 29](#).

If a user has FortiToken or a third-party authenticator app enabled for Two-Factor Authentication and needs to reset it on a new device, you can temporarily change their authentication method to email. This allows the user to access their account using email authentication and re-enable the token for their new device.

### To modify the Two-Factor Authentication method for a user:

1. Go to *Users* and select the user from the list.
2. Go to the *Security Credentials* tab.
3. Under *Two Factor Authentication*, click *Switch to Email Token*.

## Logging in with Two-Factor Authentication for the first time

Users are required to validate and set up Two-Factor Authentication the first time they log in to [www.forticloud.com](http://www.forticloud.com) if it is being enforced by their account or Organization.

## Email users

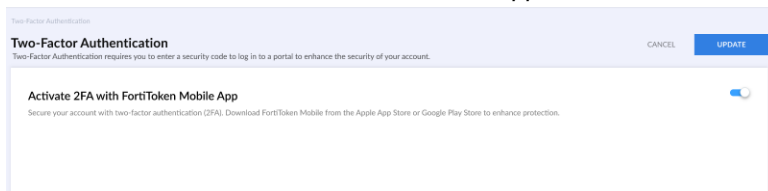
Master and legacy sub users logging in with an email account will be forced to enable Two-Factor Authentication using FortiToken if it is being enforced at the account or OU level. See [Enabling Two-Factor Authentication on page 70](#) for information on enforcing Two-Factor Authentication at the account level. See [Settings](#) in the Organization Portal guide for information on enforcing Two-Factor Authentication at the Organization level.

## To set up Two-Factor Authentication for FortiToken if you are in an Organization:

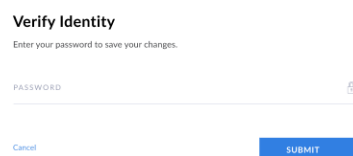
1. Log in using your email account credentials. You will be redirected to the *Two-Factor Authentication* page.



2. Enable *Activate 2FA with FortiToken Mobile App*.



3. Click *Update*. The *Verify Identity* dialog opens.



4. Enter your account password and click *Submit*.
5. (Optional) Click *Test Token Now* to verify Two-Factor Authentication has been enabled.
  - a. Enter the security code and click *Submit*. A dialog opens if the test is successful.
6. Log in using your email credentials again and use FortiToken to verify your account.

## IAM users

Users logging in with an IAM account can set up Two-Factor Authentication for email, SMS, FortiToken, or through a third-party authenticator app. See [Enabling Two-Factor Authentication on page 70](#).



SMS Two-Factor Authentication will only be available if a mobile number has been added to the account. See [Contacts on page 65](#).

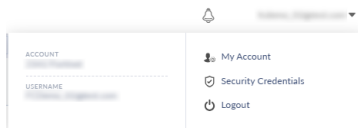
## Switching Two-Factor Authentication methods

You can switch authentication methods from your account settings. Users logging in using email account credentials cannot switch to the email Two-Factor Authentication method and are encouraged to switch to the FortiToken method for

better security.

### To switch Two-Factor Authentication methods:

1. Log in to the portal.
2. Click the *Account* menu at the top-right of portal and select *Security Credentials*.



3. In the navigation pane, click *Two Factor Authentication*. The *Two Factor Authentication* page opens.
4. Select the new authentication method and click *Update*.

5. A verification dialog will open. The dialog that appears is dependent on the authentication method you chose. Follow the steps provided in the dialog to complete verification.
6. Click *Submit*.

## Resetting tokens for Two-Factor Authentication

You can reset tokens for FortiToken Mobile and third-party authenticator apps:

- [Resetting a FortiToken on page 74](#)
- [Resetting a third-party authenticator app token on page 76](#)

### Resetting a FortiToken

You can reset FortiToken for Two-Factor Authentication from your account from the *Welcome* page after you log into a portal. For example, you have upgraded your phone and you want to configure FortiToken on your new device to use with Two-Factor Authentication.

### To reset FortiToken for Two-Factor Authentication for a new device:

1. Install the FortiToken app on the new device.
2. Log in to the portal with the FortiToken app on the old device and go to *Security Credentials > Two Factor Authentication*.
3. Click *Reset Token* under *FortiToken*.  
If a mobile number is included in your account, an SMS code will be sent to the number.
4. Enter the *SMS Code* and account *Password*.
5. Click *Submit*. A FortiToken reset email will be sent to the account email address.
6. Configure the FortiToken app for your new device and log in.

### Lost FortiToken device

You can reset the FortiToken for a lost device if you have added the mobile number to the account. If you have not added a mobile number to the account, contact Customer Service. See [Contacts on page 65](#).

### To reset FortiToken for a lost device:

1. Attempt to log into the portal.
2. When you are directed to the *Input Security Code* page, select *Lost FortiToken*.

**Input Security Code**  
Check your email or token application for the security code.

SECURITY CODE

**GO**

[Need Help?](#)

**Email Login Users:**  
[Forgot Username](#) | [Forgot Password?](#) | [Change My Security Device](#) | [Lost FortiToken](#) | [Lost Token on Third-Party App](#)


**IAM Users:**  
 Please contact the administrator that provided your username for assistance

3. Enter your account email address and verify the Captcha.

**Lost Token Help**  
Please enter your email to initiate the FortiToken reset process

EMAIL

Please confirm you're not a robot: \*

☐ I am human 

**SUBMIT**

[Forgot your email? Click Here](#)

4. Click *Submit*.
5. Enter the verification that was sent to your email.
6. Click *Next*.  
If a mobile number is included in your account, an SMS code will be sent to the number.

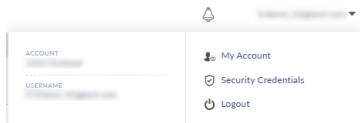
7. Enter the *SMS Code* and account *Password*.
8. Click *Next*. A FortiToken reset email will be sent to the account email address.

## Resetting a third-party authenticator app token

You can also reset the token for a third-party authenticator app if that is your chosen mode of authentication.

### To reset a third-party authenticator token:

1. Click the *Account* menu at the top-right of portal and select *Security Credentials*.



2. In the navigation pane, click *Two Factor Authentication*. The *Two Factor Authentication* page opens.
3. Click *Reset Token* under *Third-Party Authenticator App*.
4. Enter your password to verify your identity and click *Next*.  
If a mobile number is included in your account, an SMS code will be sent to the number.
5. Enter the *SMS Code* and account *Password*.
6. Click *Next*.
7. Scan the QR code from the authenticator app or enter the activation code.
8. Click *Next*.
9. Enter the token code from the authenticator app.
10. Click *Next*. A confirmation message is displayed.

### Lost token on a third-party authenticator app

You can reset the token of a third-party authenticator app from the login page.

### To reset a third-party authenticator:

1. Attempt to log into the portal.
2. When you are directed to the *Input Security Code* page, select *Lost Token on Third-party app*.

**Input Security Code**  
Check your email or token application for the security code.

SECURITY CODE

**GO**

[Need Help?](#)

**Email Login Users:**  
[Forgot Username](#) | [Forgot Password?](#) | [Change My Security Device](#) | [Lost FortiToken](#) | [Lost Token on Third-Party App](#)

**IAM Users:**  
 Please contact the administrator that provided your username for assistance

3. Enter your account email address and verify the Captcha.

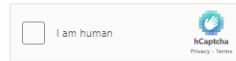
### Lost Token Help

Please enter your email to initiate the FortiToken reset process

EMAIL



Please confirm you're not a robot: \*



SUBMIT

Forgot your email? [Click Here](#)

4. Click *Submit*.
5. Enter the verification that was sent to your email.
6. Click *Next*.  
If a mobile number is included in your account, an SMS code will be sent to the number.
7. Enter the *SMS Code* and account *Password*.
8. Click *Next*.
9. Scan the QR code from the authenticator app or enter the activation code.
10. Click *Next*.
11. Enter the token code from the authenticator app.
12. Click *Next*. A confirmation message is displayed.

# Organization user management

Advanced management features are available when using organizations. An Organization and Organizational Units can be created in the Organization portal and are used to enhance your company's security.

IAM users, user groups, and so on can be created and associated with Organizational Units and OU accounts with the proper permissions. If you are using OUs to organize your company, you will need to create permission profiles that reflect this hierarchy so that the necessary users, user groups, and roles can be assigned.

For more information on the Organization portal, see the [Organization Portal Administration Guide](#).



An IAM administrative user must be created to manage IAM users for the Organization's OUs. The IAM administrative user must have the user type as *Organization* and permissions for the IAM portal. See [Overview of creating and managing Organizations](#) in the Organization Portal guide.

---

This section contains the following topics:

- [Enabling Organizations on page 78](#)
- [Permission scope with Organizations on page 80](#)
- [Permission profiles within Organizations on page 82](#)
- [Creating users, user groups, and roles within Organizations on page 84](#)
- [Logging into an OU account on page 89](#)
- [OU context switch on page 90](#)

## Enabling Organizations

Enable the Organizations feature to arrange all accounts into distinct Organizational Units to centrally apply permissions across multiple accounts in the cloud.

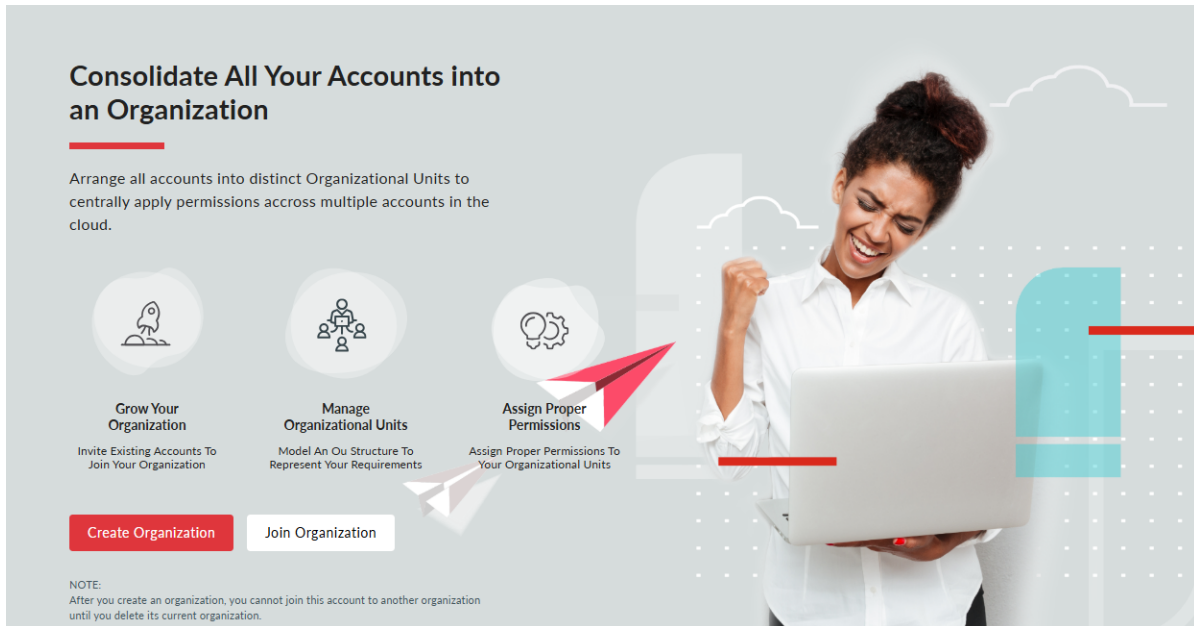


Only the master user can enable the Organizations feature.

---

**To enable Organizations from the Organization portal:**

1. From the *Services* dropdown menu, select *Organizations*.
2. Click *Create Organization*.



### Consolidate All Your Accounts into an Organization

Arrange all accounts into distinct Organizational Units to centrally apply permissions across multiple accounts in the cloud.

- Grow Your Organization**  
Invite Existing Accounts To Join Your Organization
- Manage Organizational Units**  
Model An Ou Structure To Represent Your Requirements
- Assign Proper Permissions**  
Assign Proper Permissions To Your Organizational Units

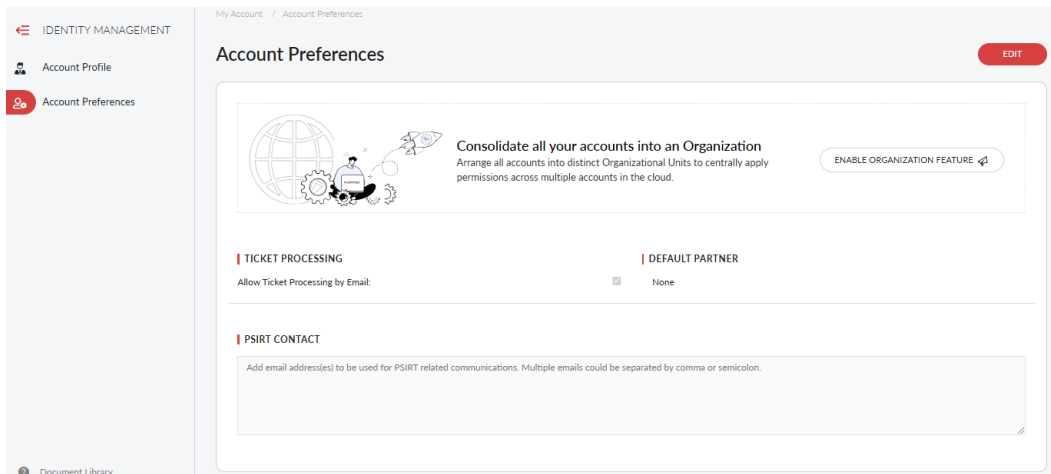
**Create Organization** **Join Organization**

NOTE:  
After you create an organization, you cannot join this account to another organization until you delete its current organization.

3. Create an Organization. For information, see the [Organization Portal Administration Guide](#).

### To enable Organizations from *My Account*:

1. From the profile menu, select *My Account*.
2. Select *My Account (IAM version)*.
3. Go to *Account Preferences*.
4. Click *Enable Organization Feature*.



My Account / Account Preferences

#### Account Preferences

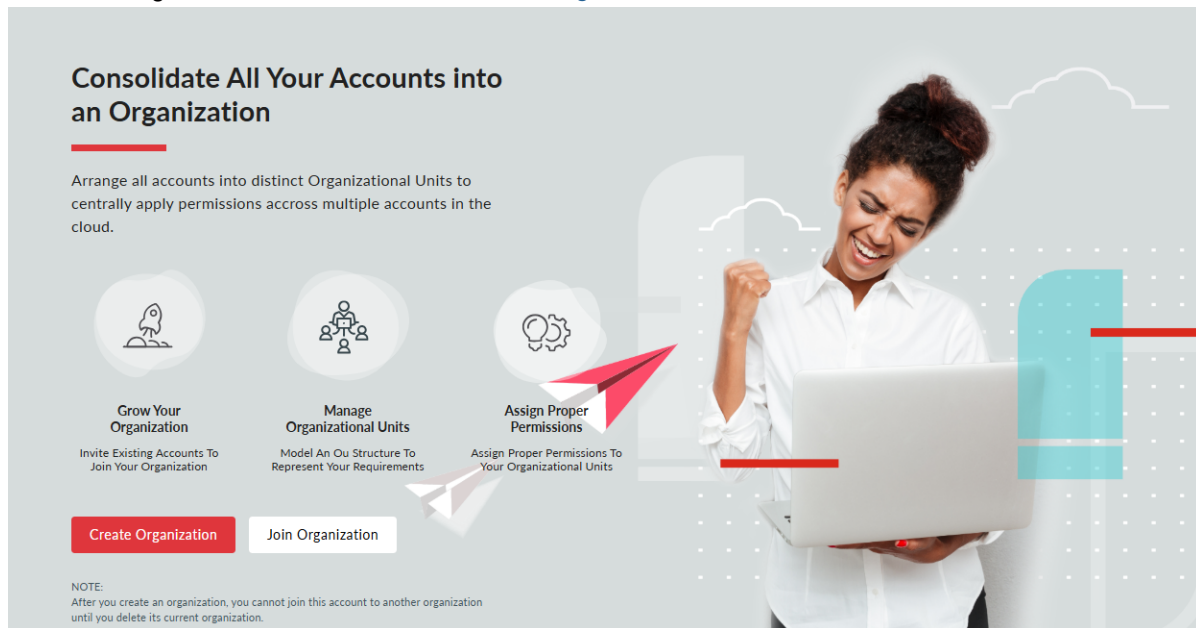
**Consolidate all your accounts into an Organization**  
Arrange all accounts into distinct Organizational Units to centrally apply permissions across multiple accounts in the cloud.

**ENABLE ORGANIZATION FEATURE**

**TICKET PROCESSING**  
Allow Ticket Processing by Email: ☐ **DEFAULT PARTNER**  
None

**PSIRT CONTACT**  
Add email address(es) to be used for PSIRT related communications. Multiple emails could be separated by comma or semicolon.

5. Create an Organization. For information, see the [Organization Portal Administration Guide](#).



## Permission scope with Organizations

Permission scope is assigned when creating a permission profile or an IAM user, user group, or IdP role. It defines the scope of access a user has in terms of asset folders or OU hierarchy.

### Local and Organization scope

Permission scope is further defined by *Local* versus *Organization* access type. *Local* access is the default for the Identity & Access Management portal. IAM users, user groups, and so on can be created as usual when in the *Local* type and will be limited to the asset folders in the selected account. See [Permission scope on page 19](#).

However, if organizations are enabled and created in the Organization portal, the *Organization* type can be used for more advanced settings. This more advanced version allows IAM users, user groups, and so on to be assigned to OUs and OU member accounts that define your company's organization structure.

Permission scope can be defined as *Local* or *Organization* using the *Select A Type* feature. The *Local* type is automatically assigned to all permission profiles when OU access is not enabled. However, if a login user does have OU access enabled, the scope can be set to either the *Local* or *Organization* type. Once selected, permission scope can then be based on hierarchical OU (*Organization* type) or asset folder (*Local* type) paths in the Organization portal and Asset Management portal, respectively.

Select a Type\*

Select the type as Local for accessing the current account and Organization for accessing the OU accounts

Organization	▼
Local	
Organization	



If you are logged in with OU permissions scope, you can see both *Local* and *Organization* permission profiles in the *Permission Profiles* page. However, if you are logged in to your local account, you will only be able to see *Local* permission profiles.

---

## Available and selected scope

A user's permission scope is independent to the account they belong to. Once specified, in OU context, the selected scope is not necessarily the same as the available scope:

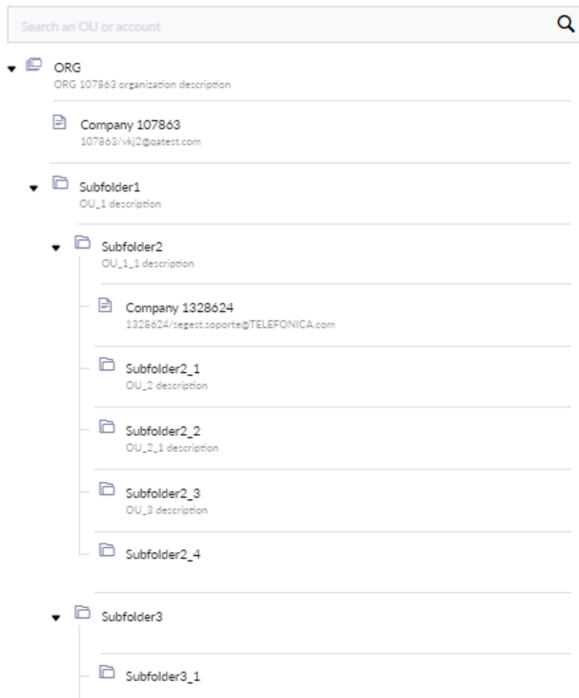
- **Available scope:** The available scope refers to the total accessing scope the login user is assigned with. It covers all organizations, OUs, and member accounts the user can access. The available scope defines what a user is capable of doing and is assigned with the permission scope. This scope can include up to and including the organization account if the user has the proper permissions. Available scope is applied when the current login user tries to configure IAM user or external IdP roles permission scopes.
- **Selected scope:** The selected scope refers to the current login user's selected OU context within the current session. It can be changed at anytime within this session. It includes the current account a user is accessing and any accounts below this level in the hierarchy. The selected scope is used to focus your view within the available scope. The selected scope defines what is visible and available to the user. For example, if the user is currently accessing an OU account, the Asset Management portal *Dashboard* will display an aggregated view of the member accounts under that OU. See [Organizational Unit account views](#) in the Asset Management Administration Guide.

The selected scope can be changed to another account within the available scope by selecting a new account from the context switch dropdown. See [OU context switch on page 90](#).

## Example of selected scope

If the current selected scope is lower in the organization hierarchy than the available scope, this does not limit the overall abilities of the user. The user will be able to assign users and permission profiles to any level of the organization within their available scope; including higher in the hierarchy than the selected scope.

The following organization structure will be used for the example.



If a user has permissions up to and including the *ORG* account but they select *Subfolder2* when logging in, the scope of their account is:

- Available scope: The *ORG* account and all OUs and member accounts within it.
- Selected scope: The *Subfolder2* account and all accounts below it in the hierarchy.

While they are accessing *Subfolder2*, the information they see in the portals will relate to that OU and the member accounts within it. However, since they have an available scope of *ORG*, they are not limited to the selected scope. For example, when creating a new IAM user, they can delegate that IAM user to any account within *ORG*, such as *Subfolder1* which is higher in the organization hierarchy than *Subfolder2*.

## Permission profiles within Organizations

Permission profiles are required before you can create IAM users, user groups, and so on. Permission profiles allow you to define access to portals and the level of access within the portal, such as admin or read only permissions. When creating an IAM user, user group, and so on while having access to OUs in the Organization portal, a permission scope must be defined to allow for current account access, OU access, or OU account access.

If you have organizations enabled and created in the Organization portal, permission profiles can be created for a specific OU or OU account using the *Organization* type, or the current account using the *Local* type. Once a permission profile is created, IAM users, user groups, and so on can be created and assigned to the permission profile.

### To create a permission profile:

1. Select *Permission Profiles* from the left-hand navigation menu. The *Permission Profiles* page opens.
2. Select *Add New*. The *New Portal Permission Profiles* page is displayed.

New Portal Permission Profile

Cancel

Submit

BASIC INFO

Permission Profile Name: \*

Enter Permission Profile Name

Status: \*

Active

Description

Enter Permission Profile Description

Select a Type

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

Local

PERMISSION PROFILE

Add Portal

- Enter a name for the profile in the *Permission Profile Name* field.



Once the permission profile is saved, the permission profile type cannot be edited.

- Set the *Status* to *Active*.
- Enter a description of the portal permissions in the *Description* field.
- Select the profile type from the *Choose A Type* dropdown.

Select a Type\*

Select the type as Local for accessing the current account and Organization for accessing the OU accounts

Organization

Local

Organization



Once the permission profile is saved, the type cannot be edited.

- Click *Add Portal*. A list of available portals is displayed.

#### ADD THESE PORTALS TO MY ACCOUNTS

Total Selected 0

Select All

<input type="checkbox"/> Asset Management	<input type="checkbox"/> FortiCASB	<input type="checkbox"/> FortiDLP (Beta)	<input type="checkbox"/> FortiMonitor	<input type="checkbox"/> FortiSIEM Cloud	<input type="checkbox"/> Managed FortiGate
<input type="checkbox"/> CTAP (Beta)	<input type="checkbox"/> FortiClient EMS Cloud	<input type="checkbox"/> FortiEdge Cloud	<input type="checkbox"/> FortiOS SSO	<input type="checkbox"/> FortiSOAR Cloud	<input type="checkbox"/> OC-VPN Portal
<input type="checkbox"/> FGaaS	<input type="checkbox"/> FortiClient Services	<input type="checkbox"/> FortiEDR	<input type="checkbox"/> FortiPhish	<input type="checkbox"/> FortiTest Permissions	<input type="checkbox"/> Overlay as a Service
<input type="checkbox"/> FortiAnalyzer Cloud	<input type="checkbox"/> FortiCNP	<input type="checkbox"/> FortiExtender Cloud	<input type="checkbox"/> FortiPortal Cloud	<input type="checkbox"/> FortiTIP	<input type="checkbox"/> Security Awareness (Beta)
<input type="checkbox"/> FortiAppSec Cloud	<input type="checkbox"/> FortiConverter	<input type="checkbox"/> FortiFlex	<input type="checkbox"/> FortiPresence	<input type="checkbox"/> FortiToken Cloud	<input type="checkbox"/> SOCaaS
<input type="checkbox"/> FortiCamera Cloud	<input type="checkbox"/> FortiDAST	<input type="checkbox"/> FortiGate Cloud	<input type="checkbox"/> FortiProxy Cloud	<input type="checkbox"/> FortiTrustID	
<input type="checkbox"/> FortiCare	<input type="checkbox"/> FortiDeceptor DaaS Cloud	<input type="checkbox"/> FortiGate CNF	<input type="checkbox"/> FortiRecon	<input type="checkbox"/> FortiVoice	
<input type="checkbox"/> FortiCare Elite (Beta)	<input type="checkbox"/> FortiDemo	<input type="checkbox"/> FortiInsight	<input type="checkbox"/> FortiSandbox Cloud	<input type="checkbox"/> FortiZTP	
<input type="checkbox"/> FortiCare Legacy	<input type="checkbox"/> FortiDevice	<input type="checkbox"/> FortiMail	<input type="checkbox"/> FortiSASE	<input type="checkbox"/> IAM	
<input type="checkbox"/> FortiCART	<input type="checkbox"/> FortiDevSec	<input type="checkbox"/> FortiManager Cloud	<input type="checkbox"/> FortiSASE Sovereign	<input type="checkbox"/> Lacework FortiCNAPP	

Cancel

Add

- Select the portals you want to include in the permission profile.
- Click *Add*. The portals are displayed in cards.

Asset Management			
Resources	Read Only	Read & Write	No Access
Entitlement Management ⓘ	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Asset Maintenance ⓘ	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Renewal Notice ⓘ	<input type="radio"/>	<input checked="" type="radio"/>	<input 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"/>

10. For each portal card, define portal permissions:



If you want to deny access to a portal, add the portal to the permission profile but do not enable any resource or portal access.

Excluding a portal from a permission profile does not deny access to that portal. If you do not add the portal to the permission profile, its status will be considered undefined. Therefore, it may be possible for the user to still access the portal from the *Services* dropdown menu if the portal itself provides open access to some features.

- For portals with resource-based permission capabilities, specify the *Resources* access type.

Asset Management			
Resources	Read Only	Read & Write	No Access
Entitlement Management	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Asset Maintenance	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Renewal Notice	<input type="radio"/>	<input checked="" type="radio"/>	<input 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"/>

FortiGate Cloud			
Resources	Read Only	Read & Write	No Access
Configuration Management	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Logging and Reporting	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Cloud Sandbox	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
IOC	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

IAM			
Resources	Read Only	Read & Write	No Access
User / Permissions	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Account	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Credentials	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

- For portals with role-based permissions, enable *Access* and specify the portal *Access Type* and any *Additional Permissions*.

FortiSOAR Cloud		
Access	Access Type	Additional Permission
<input checked="" type="checkbox"/>	<input checked="" type="radio"/> Admin	
	<input type="radio"/> Read/Write	
	<input type="radio"/> Read Only	

FortiExtender Cloud		
Access	Access Type	Additional Permission
<input checked="" type="checkbox"/>	<input checked="" type="radio"/> Admin	
	<input type="radio"/> Read/Write	
	<input type="radio"/> Read Only	

11. Click **Save**. The permission profile is now available to be assigned to users.

## Creating users, user groups, and roles within Organizations

New IAM users, user groups, API users, and IdP roles can be created from the appropriate Identity & Access Management portal pages. When you configure the details, the *Choose a Type* and *Permission Scope* features can be used to define *Local* or *Organization* type, and the asset folder or OU path, respectively.

### To create an IAM user:

- Select *Users* from the left-hand navigation menu. The *Users* page opens.
- Click *Add New > IAM User*. The *User Details* pane opens.
- (Optional) Click *Apply same permissions as existing User*, and then select a user from the dropdown. You can configure the permissions later.

4. Enter the user's details and click *Next*.

<b>Username</b>	Type the username with no spaces.
<b>Full Name</b>	Type the user's first and last name.
<b>Email</b>	Type the user's email address.
<b>Phone</b>	Select the country code from the dropdown, and type the user's phone number.
<b>Description (Optional)</b>	Type a description of the user.

1. User Details

**IAM USER INFORMATION**

Username: \*

Full Name: \*

Email: \*

Phone: \*

Description

**ADOPT PERMISSIONS**

☐ Apply same permissions as existing User:

Select an existing User ▼

NOTE  
Checking 'Apply same permission as an existing User' allows you to easily assign a pre-configured Permission setup. User Permission settings are still fully configurable in the next step.

5. (Optional) Add the user to an IAM user group. See [User groups on page 49](#).
- Select *Yes* from *Basic Info*. A dropdown list of user groups is displayed.
  - Select a user group from the dropdown.
  - Click *Next*, and proceed to Step 10.
6. Select the *Organization* user type from *Select A Type* dropdown list.

Select a Type: \*

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

Local

Local

**Organization**

7. Select the scope from the *Permission Scope* dropdown.



*Permission Scope* options depend on the type you select in the previous step. For example, if the *Organization* type is selected, the OU scope will be selected here. The available scope will be applied in this case.

**PERMISSION SCOPE**

Select an Organization Unit or Account: \*

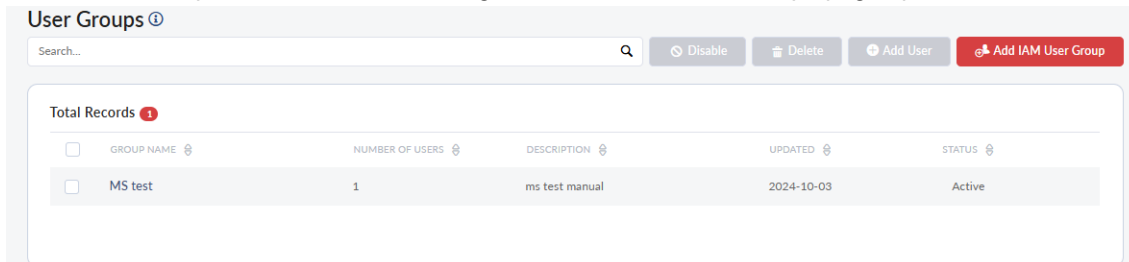
None

- In the *Permissions Profile* dropdown, select a profile. The *Permission Details* assigned to the selected profile are displayed.
- Click *Next*. The *Confirmation* page is displayed.
- Review the user information, and click *Confirm*. The user's details are displayed.

Account credentials must be shared with the user. The user can generate a password reset link and share it with the newly created IAM user.

### To create a user group:

1. Select *User Groups* from the left-hand navigation menu. The *User Groups* page opens.



2. Click *Add IAM User Group*. The *IAM User Group Information* page is displayed.
3. In the *Group Name* field, enter a name for the group.
4. (Optional) In the *Description* field, describe the group.
5. (Optional) Set the *Status* to *Disabled*. The status is *Active* by default.
6. Click *Next*.
7. Select the user type from *Select A Type* dropdown list.
8. Select the scope from the *Permission Scope* dropdown.



*Permission Scope* options depend on the type you select in the previous step. For example, if the *Organization* type is selected, the OU scope will be selected here. The available scope will be applied in this case.

#### PERMISSION SCOPE

Select an Organization Unit or Account: \*

None

9. In the *Permissions Profile* dropdown, select a profile. The *Permission Details* assigned to the selected profile are displayed.
10. Click *Next*. The *Add IAM user(s)* page is displayed.
11. Assign users to the group.
  - a. Click *Add User*.
  - b. (Optional) Click *Filter users by Group*, to view users in a group. Selecting a user in a group will remove the user from that group.
  - c. (Optional) Enter a username in the search bar, and enter the user name. As you type, partial results are returned.
  - d. Select the users and click *Add*.
  - e. Click *Next*. The *Confirmation* page is displayed.
12. Review the group permissions, and click *Confirm*.
13. (Optional) Click *Add Another Group*.

### To create an API user:

1. Select *Users* from the left-hand navigation menu. The *Users* page opens.
2. Click *Add New > API User*.
3. (Optional) In the *Description* field, enter a description of the user.

4. Select the *Organization* user type from *Select A Type* dropdown list.

Select a Type: \*

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

Local

Local

Organization



When creating an API user that can be added to an Organization, if the user is set to the *Local* type instead, they will be unable to specify the permission scope. They will automatically be assigned *My Assets* for the permission scope.

5. Select the scope from the *Permission Scope* dropdown.



*Permission Scope* options depend on the type you select in the previous step. For example, if the *Organization* type is selected, the OU scope will be selected here. The available scope will be applied in this case.

PERMISSION SCOPE

Select an Organization Unit or Account: \*

None

6. Select a permission profile from the *Permission Profile* dropdown list.
7. Click *Add*.
8. Click *Download Credentials*. The *Security Check* dialog opens.



Downloading API user credentials will reset the user's security credentials each time you perform this action. The API user only exists within the account scope.

9. Enter your password to protect the credential file and click *Proceed*. The credentials are downloaded to your computer.
10. Request an authorization token. See [Accessing FortiAPIs on page 41](#)

## To add an external user role:

1. Select *Users* from the left-hand navigation menu. The *Users* page opens.
2. Click *Add New > External IDP Role*. The *External IdP Role* page opens.

External IdP Role

ROLE DETAILS

Role Name: \*

Enter role name

Description

Enter role 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

3. In the *Role Name* field, type the name of the role.
4. (Optional) In the *Description* field, enter a description of the role.
5. Select the *Organization* user type from *Select A Type* dropdown list.

Select a Type: \*

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

Local

Local

Organization

6. From the *Permission Scope* dropdown, select an asset folder or Organizational Unit.



*Permission Scope* options depend on the type you select in the previous step. For example, if the *Organization* type is selected, the OU scope will be selected here. The available scope will be applied in this case.

PERMISSION SCOPE

Select an Organization Unit or Account: \*

None

7. In the *Permissions Profile* dropdown, select a profile. The *Permission Details* assigned to the selected profile are displayed.
8. Click *Add Role*.

## Logging into an OU account

Users can access FortiCloud using IAM user accounts or an OU account when logging in with their IAM user credentials. Once the login credentials have been verified, users can then choose to proceed with an Organizational Unit (OU) account. OU access is dependent on the permission profile assigned to your login credentials. Available OUs and member accounts will turn blue when hovered over and display the *Select* button.

**To access Organizational Unit accounts with IAM user credentials:**

1. Go to [www.forticloud.com](http://www.forticloud.com).
2. Select *Login*. The log in portal opens.

3. Select *IAM user*.
4. Enter your credentials in the *Account ID/Alias*, *Username*, and *Password* fields.



You can enter either your account ID number or alias in the *Account ID/Alias* field.

5. Click *Log In*. If the current user has Organization/OU scope configured, a list of Organizational Units and member accounts is displayed.

6. Select the access method:
  - Hover over an OU and click *Select* to log in to a root account.

- Hover over a member account and click *Select* to log into the account.



For OU and member account selection, it depends on the target portal. Most of the portals only support the user selecting a member account. The Asset Management portal supports the user selecting an OU.

---

The *Dashboard* is displayed.

#### To access Organizational Unit accounts with external IdP credentials:

1. Log in using your company's ID provider. The log in portal opens.
2. Select the *Service Provider*.
3. Select *Organizations*. A list of Organizational Units and member accounts is displayed.
4. Select the access method:
  - Hover over an OU and click *Select* to log in to a root account.
  - Hover over an OU member account and click *Select* to log into the account.

The *Dashboard* is displayed.

## OU context switch

You can change your selected scope from the context switch dropdown menu when you are logged in using IAM user or external IdP role credentials. See [Available and selected scope on page 81](#).

The Asset Management portal can support both OUs (with aggregated information on the member accounts within the OU) and OU member accounts. Therefore, if you are in the Asset Management portal, you can switch to either OUs or OU member accounts.

However, other portals, such as the Identity & Access Management portal, can only support OU member accounts. Therefore, you can only switch to other OU member accounts through the OU dropdown menu.

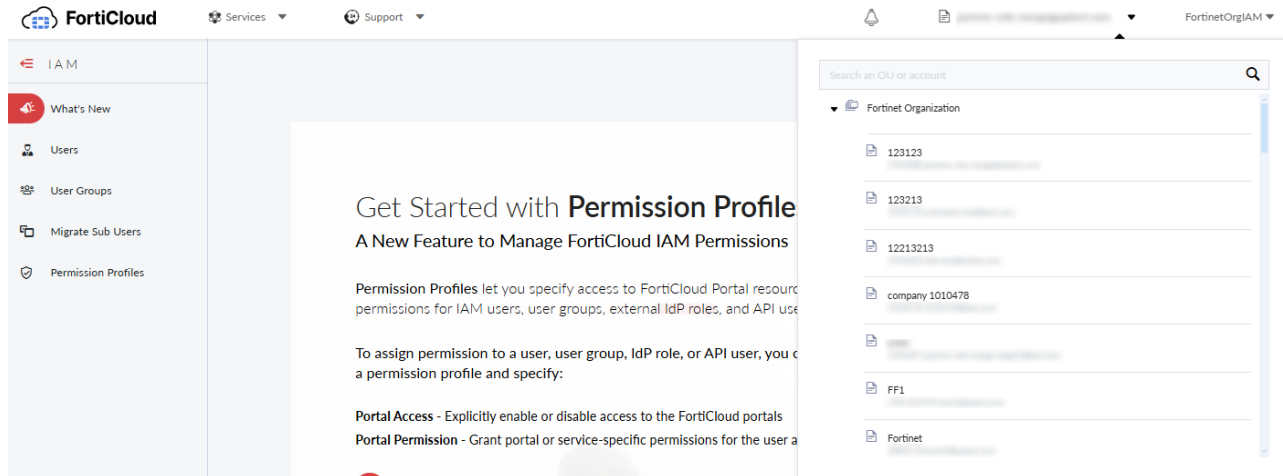


If multiple roles are available for one OU, the OU will be repeated in the list.

---

## To switch to a different OU account:

1. Select the context switch dropdown menu. Accounts within the organization are displayed.



2. Select an account within your available scope:
  - Hover over a folder and click *Select* to switch to an OU.
  - Select the OU folder dropdown arrow to see available OU member accounts for that OU. Hover over the OU member account you want to switch to and click *Select*.



If you are not in the Asset Management portal, you will only be able to select an OU member account.

If you are logged in with an external IdP role, you can only switch within the current organization. To switch to a different organization, use the *Switch Roles* option in the profile menu. See [Selecting IdP roles on page 45](#).

# External IdP

FortiCloud supports using an external identity provider with SAML 2.0 and IdP initiated authentication. Once the setup is complete, external users can authenticate with the desired provider and access FortiCloud services based on the roles defined by the administrator.

FortiCloud supports fine grained permission profile for external IdP users through external IdP IAM role. External IdP roles allow external users to log in to a cloud portal using their organization's ID provider. External IdP roles are authenticated with a custom login page. After the user is authenticated, they are redirected to a page where they can select the cloud portals assigned to their account.

Once external IdP has been configured for the account, you can proceed with creating external IdP roles. External IdP roles can then access the account and the various FortiCloud Services portals. See [Selecting IdP roles on page 45](#) for more information on accessing the portal with an external IdP role.



This document only covers configuring external IdP with Okta and Microsoft Entra ID. However, multiple external identity providers are supported by FortiCloud.

---

This section includes:

- [Enrolling for external IdP on page 92](#)
- [Configuring external IdP on page 97](#)
- [Adding external IdP roles to the application on page 99](#)
- [Setting a co-exist end date on page 104](#)
- [Troubleshooting external IdP on page 105](#)

## Enrolling for external IdP

Before you can access the external IdP features supported by FortiCloud, you must first enroll for the service.

To enroll for external IdP access to FortiCloud, you must:

1. Contact your Fortinet sales representative.
2. Configure your IdP application.
3. Fill out the enrollment form with information about your IdP application and FortiCloud account.
4. Download and share the IdP Metadata file with your Fortinet sales representative.

Once your enrollment has been approved, you should:

- Update the application URLs based on what you received from your Fortinet sales representative. See [Configuring external IdP on page 97](#).
- Configure external IdP roles with which to access the account and FortiCloud Services portals. See [Adding external IdP roles to the application on page 99](#) and [External IdP roles on page 43](#).
- Configure a co-exist end date for any IAM or sub-users in your account.

All IAM and sub-users of the account will be disabled following the IdP transition period. You can extend this if necessary by setting a co-exist date. See [Setting a co-exist end date on page 104](#).

This document only covers configuring external IdP with Okta and Microsoft Entra ID. However, multiple external identity providers are supported by FortiCloud. This topic includes the following enrollment examples:

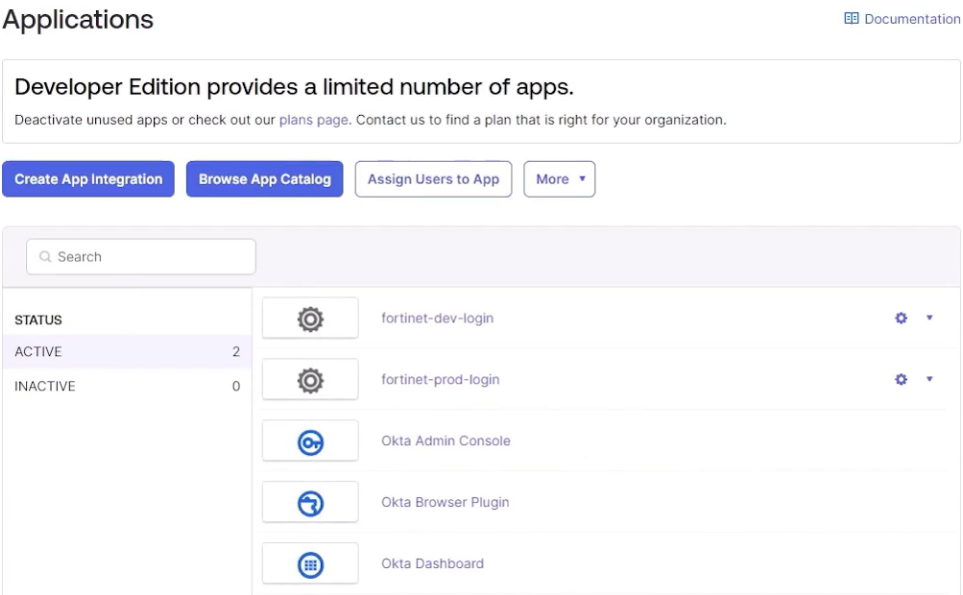
- [Enrolling with Okta on page 93](#)
- [Enrolling with Microsoft Entra ID on page 95](#)

## Enrolling with Okta

External IdP can be enrolled with Okta.

**To enroll for external IdP with Okta:**

1. Contact your Fortinet sales representative about enrolling for external IdP.
2. Prepare the application:
  - a. In Okta, go to *Applications > Applications*.



- b. Click *Create App Integration*.
  - c. Select *SAML 2.0*.

## Create a new app integration

Sign-in method

[Learn More](#)

- ☐ **OIDC - OpenID Connect**  
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
- ☒ **SAML 2.0**  
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
- ☐ **SWA - Secure Web Authentication**  
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
- ☐ **API Services**  
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

Cancel

Next

d. Click *Next*.e. Enter an *App Name*.


## Create SAML Integration



<b>1</b> General Settings	2 Configure SAML	3 Feedback
---------------------------	------------------	------------

**1 General Settings**

App name

App logo (optional)



App visibility

- ☐ Do not display application icon to users
- ☐ Do not display application icon in the Okta Mobile app

Cancel
Next

f. Click *Next*.


g. Enter a temporary URL into the *Single sign-on URL* and *Audience URI (SP Entity ID)* fields, such as `https://customersso1.fortinet.com/`.



After enrollment is complete, your Fortinet sales representative will provide you with the necessary URLs.

h. Click *Next*.i. Select the *App type*.j. Click *Finish*. The Metadata file is generated.

← Back to Applications



**forticloud-demo**

Active

View Logs Monitor Imports

General
Sign On
Mobile
Import
Assignments

Settings Edit

**Sign on methods**

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3<sup>rd</sup> party application.

Application username is determined by the user profile mapping. [Configure profile mapping](#)

SAML 2.0

Default Relay State

**Metadata details**

Metadata URL

Copy

More details

k. Download and save the Metadata file.

3. Fill out the enrollment form. The following information must be included in the enrollment form:

- Company name
- SAML 2.0 IdP name (Okta)
- Account ID and the Master user email
- Company administrator and Fortinet Inc. contact
- IdP Metadata file



The account ID and email can be found in your FortiCloud account dropdown menu. To find the information, log into the Master account. In the top, right corner, select the account. A dropdown menu is displayed that lists the account ID and email information on the left side.

4. Send the enrollment form and Metadata file to your Fortinet sales representative.

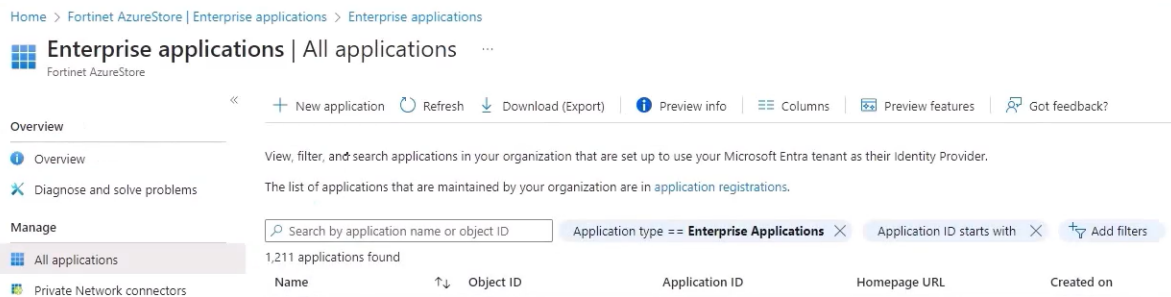
Once you have been approved, you will receive an email with the next steps and SAML information.

## Enrolling with Microsoft Entra ID

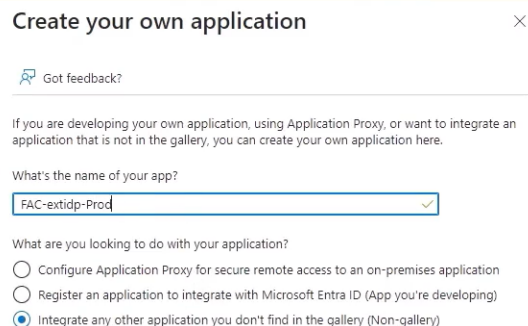
External IdP can be enrolled with Entra ID.

## To enroll for external IdP with Microsoft Entra ID:

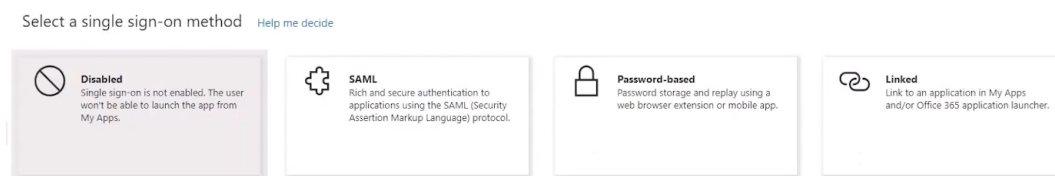
1. Contact your Fortinet sales representative about enrolling for external IdP.
2. Prepare the application:
  - a. In Microsoft Azure, select *Microsoft Entra ID*.
  - b. Go to *Enterprise applications*.



- c. Click *New application*.
- d. Click *Create your own application*. The *Create your own application* pane is displayed.



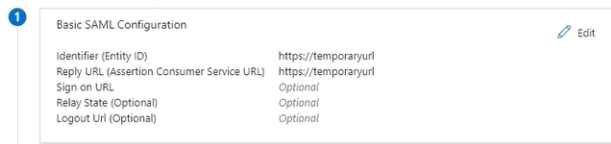
- e. Enter the name of the application.
- f. Click *Create*. The *Overview* page is displayed.
- g. Select *Set up single sign on*.



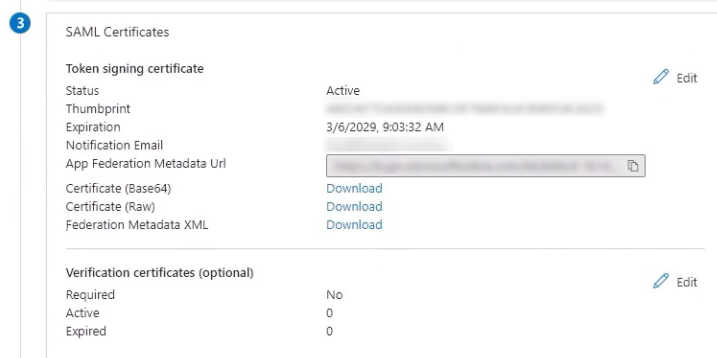
- h. Select *SAML*.
- i. Edit the *Basic SAML Configuration*:
  - i. Enter a temporary URL for the *Identifier (Entity ID)* and *Reply URL (Assertion Consumer Service URL)* fields, such as `https://customersso1.fortinet.com/`.



After enrollment is complete, your Fortinet sales representative will provide you with the necessary URLs.

ii. Click **Save**.


Basic SAML Configuration		Edit
Identifier (Entity ID)	https://temporaryurl	
Reply URL (Assertion Consumer Service URL)	https://temporaryurl	
Sign on URL	Optional	
Relay State (Optional)	Optional	
Logout URL (Optional)	Optional	

j. Download the *Federation Metadata XML* file from the *SAML Certificates* section.


SAML Certificates		Edit
Token signing certificate	Active	
Status	Active	
Thumbprint		
Expiration	3/6/2029, 9:03:32 AM	
Notification Email		
App Federation Metadata Url		
Certificate (Base64)	Download	
Certificate (Raw)	Download	
Federation Metadata XML	Download	
Verification certificates (optional)		Edit
Required	No	
Active	0	
Expired	0	

## 3. Fill out the enrollment form. The following information must be included in the enrollment form:

- Company name
- SAML 2.0 IdP name (Microsoft Entra ID)
- Account ID and the Master user email
- Company administrator and Fortinet Inc. contact
- IdP Metadata file



The account ID and email can be found in your FortiCloud account dropdown menu. To find the information, log into the Master account. In the top, right corner, select the account. A dropdown menu is displayed that lists the account ID and email information on the left side.

## 4. Send the enrollment form and Metadata file to your Fortinet sales representative.

Once you have been approved, you will receive an email with the next steps and SAML information.

## Configuring external IdP

After you have successfully enrolled for external IdP for your FortiCloud account, you can begin to configure the external IdP with the URLs provided by Fortinet Inc..

This document only covers configuring external IdP with Okta and Microsoft Entra ID. However, multiple external identity providers are supported by FortiCloud. This topic includes the following configuration examples:

- [Configuring with Okta on page 98](#)
- [Configuring with Entra ID on page 98](#)

## Configuring with Okta

External IdP can be configured with Okta.

### To configure external IdP with Okta:

1. In Okta, go to *Applications > Applications*.
2. Navigate to the application you created when enrolling.
3. Edit the *General > SAML Settings*:
  - a. Replace the temporary URLs with the information provided by Fortinet Inc. team:

Entra ID field	Fortinet Inc. external IdP information
Single sign-on URL	SP Login (Assertion Consumer Service ACS) URL
Audience URI (SP Entity ID)	SP Entity ID
Default RelayState	Portal URL (Relay State)

- b. Click Save.

## Configuring with Entra ID

External IdP can be configured with Okta.

### To configure external IdP with Entra ID:

1. In Microsoft Azure, select *Microsoft Entra ID*.
2. Go to *Enterprise applications*.
3. Navigate to the application you created when enrolling.
4. Select *Set up single sign on*.
5. Edit the *Basic SAML Configuration*:
  - a. Replace the temporary URLs with the information provided by Fortinet Inc. team:

Entra ID field	Fortinet Inc. external IdP information
Identifier (Entity ID)	SP Entity ID
Reply URL (Assertion Consumer Service URL)	SP Login (Assertion Consumer Service ACS) URL
Relay State	Portal URL (Relay State)
Logout Url	SP Logout (SLS)

- b. Click Save.

## Adding external IdP roles to the application

Once you have configured the external IdP application, you can begin to add external IdP roles. For more information on roles, see [External IdP roles on page 43](#).

This document only covers configuring external IdP with Okta and Microsoft Entra ID. However, multiple external identity providers are supported by FortiCloud. This topic includes the following examples on adding external IdP roles:

- [Adding roles in Okta on page 99](#)
- [Adding roles in Entra ID on page 102](#)

### Adding roles in Okta

External IdP roles can be added in Okta.

#### To add external IdP roles in Okta:

1. In Okta, go to *Applications > Applications*.
2. Navigate to the application you created when enrolling.
3. Edit the *General > SAML Settings*:
  - a. In *Group Attribute Statements*, set the *Name* to *Role* and the *Filter* to *Contains > externidp\_*.

Group Attribute Statements (optional)

Name	Name format (optional)	Filter
Role	Unspecified ▾	Contains ▾ externidp_

[Add Another](#)

- b. Click *Next*.
  - c. Click *Finish*.
4. Assign the users and groups:

- a. Go to *Directory > Groups*.

**Groups** [Help](#)

All Rules

Search by group name

Advanced search ▾

Group source type  Showing 5

Group name	People	Applications
Everyone All users in your organization	3	0
extidp_sysadmin No description	3	2
extidp_admin No description	1	1
system admin No description	1	1
Okta Administrators Okta manages this group, which contains all administrators in your organization.		

- b. Click *Add group*.
- c. Set the *Name* to *extidp\_<name>*.

Add group

Name

Description (optional)

- d. Click *Save*.
- e. Select *Group name > Everyone*.
- f. Select the group you created.

**extidp\_demo** Actions ▾

🕒 Created: 5/8/2024 🕒 Last modified: 5/8/2024 [View logs](#)


[People](#) [Applications](#) [Profile](#) [Directories](#) [Admin roles](#)

### People

Search for users by first name, primary email or username 🔍

Advanced search ▾ Assign people

Showing 0 of 0

Person & username	Status
 <p>There are no members in this group</p>	

- g. Click *Assign people* to select the users you want to add.
  - h. Go to the *Applications* tab and click *Assign applications* to select the application you created.
5. Create the external IdP roles:
- a. Go to *Applications > Applications*.
  - b. Select the application and go to the *Assignments* tab.
  - c. Copy the group name.

← Back to Applications

**forticloud-demo** Active ▾ View Logs Monitor Imports

[General](#) [Sign On](#) [Mobile](#) [Import](#) [Assignments](#)

Assign ▾ Convert assignments ▾ Search... Groups ▾

Filters	Priority	Assignment		
People	1	extidp_sysadmin No description	✎	✕
Groups	2	extidp_demo No description	✎	✕

- d. In the FortiCloud IAM portal, create an external IdP role with the role *Name* set to the group name you copied. See [Adding external IdP roles on page 44](#).

**External IdP Role**

**ROLE DETAILS**

Role Name: \*  
extidp\_demo

Description  
Enter role description

**PERMISSION SCOPE**

Select an Asset Folder: \*  
My Assets

**PERMISSION PROFILE**

Select a Permission Profile: \*  
okta\_extidp\_demo\_permission\_profile

**PERMISSION DETAILS**

Asset Management				IAM			
Resources	Read Only	Read & Write	No Access	Resources	Read Only	Read & Write	No Access
Entitlement Management ⓘ		✓		User / Permissions	✓		
Asset Maintenance ⓘ		✓		Account	✓		
Renewal Notice ⓘ		✓		Credentials	✓		
Vulnerability List ⓘ		✓					
Account Services ⓘ		✓					

Cancel Add Role

- e. Repeat these steps for other groups, as needed.

You can now log into FortiCloud Services using the external IdP roles. See [Selecting IdP roles on page 45](#).

## Adding roles in Entra ID

External IdP roles can be added in Entra ID.

### To add external IdP roles in Entra ID:

1. In Microsoft Azure, select *Microsoft Entra ID*.
2. Go to *Enterprise applications*.
3. Navigate to the application you created when enrolling.
4. Select *Set up single sign on*.
5. Edit *Attributes & Claims*:
  - a. Click *Add new claim* to create a username source attribute.
  - b. Click *Add a group claim* to create a role group claim.

### Group Claims ×

Manage the group claims used by Microsoft Entra ID to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

☐ None  
☐ All groups  
☐ Security groups  
☐ Directory roles  
☒ Groups assigned to the application

Source attribute \*

Group ID ▼

☐ Emit group name for cloud-only groups ⓘ

^ Advanced options

☐ Filter groups

Attribute to match ▼

Match with ▼

String

☒ Customize the name of the group claim

Name (required)

Role ✓

6. Assign the users and groups:
  - a. Go to *Overview > Assign users and groups*.
  - b. Click *Add user/group*.
  - c. Select *Users and groups*.
  - d. Search for the desired groups and select them.

### Users and groups ×

Try changing or adding filters if you don't see what you're looking for.

Search

forticloud ×



2 results found

All Users Groups

	Name	Type	Details
<input checked="" type="checkbox"/>	forticloud-azure-demo	Group	
<input checked="" type="checkbox"/>	forticloud-azure-sysadmin	Group	

Selected (2)

↶ Reset

-  forticloud-azure-demo ✕
-  forticloud-azure-sysadmin ✕

- e. Click *Assign*.
7. Create the external IdP roles:
  - a. Go to *Overview > Assign users and groups*.
  - b. Select the group.
  - c. Copy the *Object Id*.

Delete | Got feedback?

**forticloud-azure-demo**  
 For testing ext idp

Membership type	Assigned
Source	Cloud
Type	Security
Object Id	...
Created at	9/25/2023, 11:34:57 AM

- d. In the FortiCloud IAM portal, create an external IdP role with the role *Name* set to the *Object Id*. See [Adding external IdP roles on page 44](#).

External IdP Role

**ROLE DETAILS**  
 Role Name: \*

Description

**PERMISSION SCOPE**  
 Select an Asset Folder: \*

**PERMISSION PROFILE**  
 Select a Permission Profile: \*

**PERMISSION DETAILS**

Asset Management	Read Only	Read & Write	No Access
Resources			
Entitlement Management		✓	
Asset Maintenance		✓	
Renewal Notice		✓	
Vulnerability List		✓	
Account Services		✓	

IAM	Read Only	Read & Write	No Access
Resources			
User / Permissions	✓		
Account	✓		
Credentials	✓		

Cancel Add Role

- e. Repeat these steps for other groups, as needed.

You can now log into FortiCloud Services using the external IdP roles. See [Selecting IdP roles on page 45](#).

## Setting a co-exist end date

External IdP integration enables users managed by the SAML 2.0 IdP to access their FortiCloud Accounts through external IdP roles defined in IAM portal. During the transition to external IdP user management, sub users or IAM users can be granted temporary access to FortiCloud using the co-exist date setting.

The co-exist date is the deadline until which sub users, IAM users, and external IdP users can access the IAM portal. Once the co-exist end date has passed, sub user and IAM user access are disabled.

### To set a co-exist end date:

1. Go to *Account Settings*.
2. Click *Edit*.

- Click the *Select 'user co-exist' end date* calendar icon. A calendar is displayed.

The screenshot shows the 'Account Settings' window. At the top right are 'Cancel' and 'Update' buttons. Below them is an important message: 'Important You can temporarily grant access to email users and IAM users by selecting a co-exist end date.' The main section is titled 'SELECT 'USER CO-EXIST' END DATE'. It contains a text input field with the value '2031-09-30' and a calendar icon. A calendar modal is open, showing February 2025. The calendar has a grid with days of the week (Mo to Su) and dates. The 'Select' button is at the bottom right of the calendar, and a 'Cancel' button is at the bottom left.

- Select the date that you want to limit the account to external IdP users only.
- Click *Select*.
- Click *Update*. A confirmation message is displayed.

## Troubleshooting external IdP

The following topic provides possible errors encountered from external IdP and troubleshooting suggestions. Content covered in this topic includes:

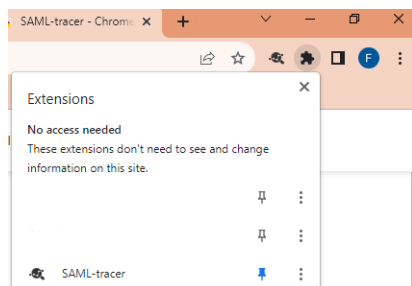
- [Verifying SAML assertion values with SAML tracer on page 105](#)
- [FortiCloud errors on page 107](#)
- [SAML login portal errors on page 109](#)
- [The option to add an External IdP Role in the FortiCloud IAM portal is missing on page 110](#)
- [Permission details of an external IdP role display Not Supported for some of the cloud portal permissions even though they are enabled in permission profile on page 110](#)

## Verifying SAML assertion values with SAML tracer

If there are any SAML-related errors, a SAML tracer plugin may be useful to verify if the required fields are in the SAML assertion.

### To use the Chrome SAML-tracer:

- Install the [SAML-tracer](#) chrome extension from Chrome Web Store.
- Clear your browser cookies or open an incognito browser.
- Open the SAML tracer from the extensions.



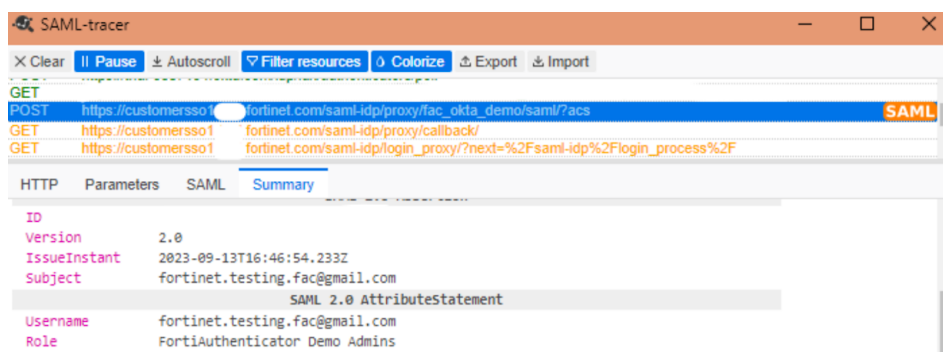
4. Begin recording the login process.
5. Log in with the external IdP and navigate to FortiCloud Services.
6. Click *Pause* after login process is done.
7. Verify the SAML assertion values:
  - a. In the SAML tracer, locate the `https://customersso1.fortinet.com/saml-idp/proxy/{REALM}/saml/?acs` POST API call.
  - b. Check that both the *Subject* field with the username and the *Role* attribute are included in the SAML assertion. See [POST request from IdP to https://customersso1.fortinet.com on page 106](#) and [POST request from https://customersso1.fortinet.com to https://support.fortinet.com on page 106](#) for more information.
8. If there are errors in the SAML assertion, click *Export* to export the file and send it to the Fortinet Inc. team. For more information on potential errors, see [FortiCloud errors on page 107](#).



The process should be similar for Firefox and other web browsers.

## POST request from IdP to https://customersso1.fortinet.com

Under the POST request, after the redirect from external IdP, make sure that there are two attribute statements (*Username* and *Role*). Take note of the *Role* value and make sure there is a corresponding FortiCloud IAM portal external IdP role.

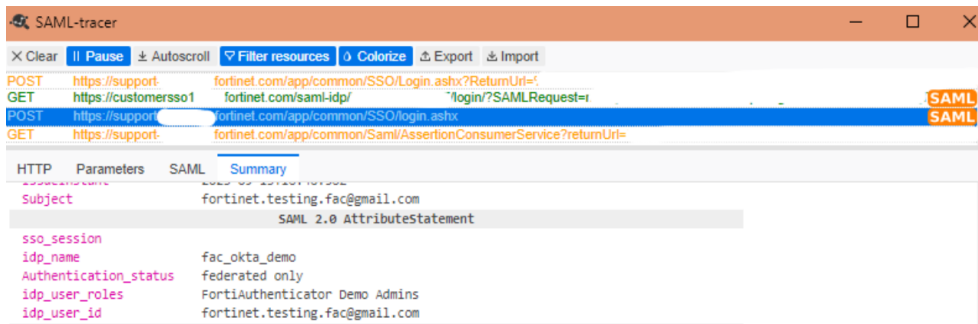


## POST request from https://customersso1.fortinet.com to https://support.fortinet.com

After customersso1 redirects to support.fortinet.com, make sure that there are three key attributes:

- *idp\_name*: The realm name assigned during enrollment (<https://customersso1.fortinet.com/saml-idp/proxy/{realm name}/saml/?acs>)
- *idp\_user\_roles*: The external IdP role
- *idp\_user\_id*: The username

If errors continue, please provide a screenshot of the error, the IdP information, and SAML tracer logs to Fortinet Inc. team.



## FortiCloud errors

After successful login, you will redirect to [support.fortinet.com](https://support.fortinet.com). The landing page is the FortiCare portal.

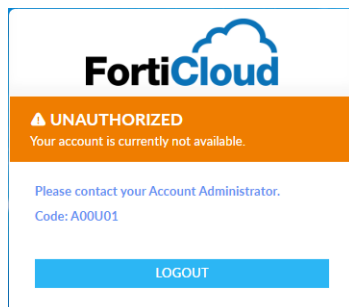
The following are errors that may be encountered inside FortiCloud Services.

### A00U01 error

If there is an A00U01 error shown, this is mostly caused by a missing or incorrectly spelled *Role* attribute in the SAML assertion. Make sure that *Role* is set under the attributes section of the IdP configuration.



*Role* is case sensitive.



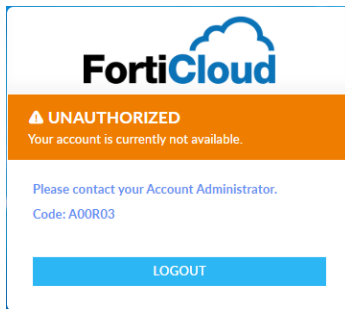
#### To troubleshoot the A00U01 error:

1. Run a SAML tracer. See [Verifying SAML assertion values with SAML tracer on page 105](#).
2. In the *Summary* tab, check if the *Role* attribute is absent. If it is absent:

- a. Navigate to the SAML settings of your IdP application.
- b. Add the *Role* information and save the settings.
- c. Log in again to see if the issue has been resolved. If it has not been resolved, contact Fortinet Inc. Support.

## A00R03 error

If there is an A00R03 error shown, this is mostly caused by a mismatch in the value of the *Role* attribute in the SAML assertion to an external IdP role in the FortiCloud IAM portal.

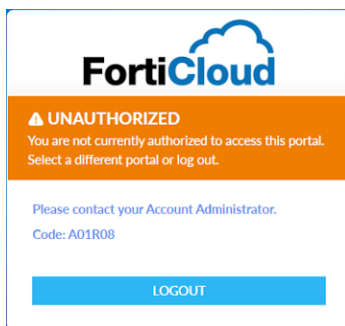


### To troubleshoot the A00R03 error:

1. Run a SAML tracer to identify the *Role* attribute. See [Verifying SAML assertion values with SAML tracer on page 105](#).
2. In the FortiCloud IAM portal, check to see if an external IdP role that matches the *Role* from the SAML tracer exists.
3. If the role is missing, create an external IdP role with the same name as the *Role* attribute. See [Adding external IdP roles on page 44](#).
4. Log in again to see if the issue has been resolved. If it has not been resolved, contact Fortinet Inc. Support.

## A01R08 error

If there is an A01R08 error shown, this is mostly caused by the external IdP role (assigned to the user) not having the permissions needed to access the Asset Management portal.



### To troubleshoot the A01R08 error:

1. Using the master account, navigate to the IAM portal.
2. Review the permission profile assigned to the external IdP role.

3. If they do not have permissions for the Asset Management portal, select *Asset Management* in *Add Portal*.
4. Configure the access level of the role.
5. Log in again as the external IdP role to see if the issue has been resolved. If it has not been resolved, contact Fortinet Inc. Support..

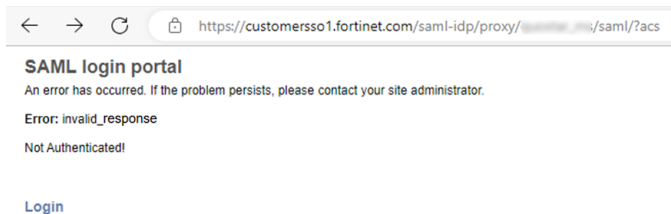
## SAML login portal errors

Below are possible errors that may be encountered when an IdP redirects to customersso1.fortinet.com.

### invalid\_response error

The *invalid\_response* error may occur when:

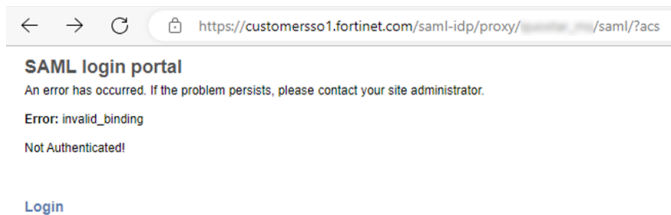
- The wrong ACS or Entity ID URL is used in the SAML assertion. For example, the incorrect use of http versus https, or vice versa.
- The incorrect attributes are provided in the SAML assertion. For example, since the *Role* attribute is case sensitive, entering *role* would result in an error.
- The ACS or Entity ID URL was inputted into the incorrect place while setting up the IdP.
- The certificate configured in the IdP does not match the certificate provided in the IdP Metadata during enrollment. New Metadata would need to be provided to the Fortinet Inc. team.



### invalid\_binding error

The *invalid\_binding* error may occur when:

- No attributes are provided in the SAML assertion. For example, the *Username* or *Role* attribute is missing.
- No account is bound to the external IdP. Contact the Fortinet Inc. team.
- The ACS URL is called with POST binding but there is no SAML response. The ACS URL generally accepts only HTTP-POST binding.
- The ACS URL is used as the login URL instead of the portal URL.



## The option to add an *External IdP Role* in the FortiCloud IAM portal is missing

After successfully logging into FortiCloud Services, in order to add external IdP roles in the IAM portal, the user account and account ID should be provided to the Fortinet Inc. team in the Enrollment Form during setup. See [Enrolling for external IdP on page 92](#).

If there is no *External IDP Role* option under *Add New* in the IAM portal *Users* page, make sure the correct account ID and username was provided to the Fortinet Inc. team. If more FortiCloud users are required to have this permission, please send the list of account IDs and username to Fortinet Inc. team.

The account ID and username can be found when the user is logged into FortiCloud Services and clicks in the top right corner. The dropdown should show a six or seven digit number, which is the account ID.

After the user is given access to external IdP feature, there will be an *External IDP Role* option under *Add New* in the IAM portal *Users* page. See [Adding external IdP roles on page 44](#).

## Permission details of an external IdP role display *Not Supported* for some of the cloud portal permissions even though they are enabled in permission profile

The permission profile is a generic set of permissions that can be used for IAM users, API users, and external IDP roles. The permission details card is marked as *Not Supported* if the Cloud service does not support external IDP role permissions.

# FAQ

## General questions

### 1. Can anyone access the IAM portal or does it require special permissions?

Any Account Owner (the person who created the account, also known as the master user) can access the IAM portal. IAM users have access to the portal based on the permission profile assigned. See [Permission profiles on page 16](#).

### 2. Why are you changing user management?

FortiCloud supports many cloud services all accessible with a unified FortiCloud account. IAM introduces granular access control for various cloud services and improved common user management for all services. For example, an IAM user can be created by an admin with access to specific services with a designated role such as admin or read only.

### 3. What benefit does IAM offer me?

IAM provides in-depth access and permission control for services. Permission profiles provide additional security and strong access control for account admins.

## IAM users

### 1. Do I need to be a master user to create IAM users?

Master users can create IAM users. IAM users with Admin/Read-Write permissions to the IAM portal can also create IAM users. See [Adding IAM users on page 25](#).

### 2. Which FortiCloud portals support IAM users?

Most FortiCloud portals include IAM user support. Refer to the product portal administration guides for more information about IAM user support and permissions.

### 3. What is the *alias* for IAM users?

Each account is identified with a unique Account ID. Instead of remembering the Account ID, the account admin can set an alias (a unique string) to easily identify the account. An account alias can be used by IAM users when they log in to a portal.

### 4. Is an alias required?

Adding an account alias is optional. IAM users can use an Account ID or alias if set.

### 5. Can I modify or change the alias?

Yes, admins can update the alias from the *My Account* menu in the top menu bar.



If you are using the legacy Sub User Model, only the master user can change the alias.

---

### 6. How do I set a password for an IAM user?

When creating an IAM user, the system generates a link to create a password which can be shared with the IAM user. After the IAM user is logged in, they can set a new password of their choice. See [Adding IAM users on page 25](#).

- 7. Do I have to provide new IAM users with the generated password file?**  
You should provide the generated reset password link to the IAM user.
- 8. Can admins update or edit an IAM user's permissions to portals or assets?**  
Yes. An admin (master user or IAM user with Admin/Read-Write permissions) can change the permissions from IAM Portal after creating the IAM user.
- 9. Can I change an IAM user's individual permissions in a user group?**  
Once an IAM user is added to a user group, only the group permission profile applies. See [Managing IAM users on page 29](#).
- 10. How do IAM users log in to the FortiCloud account?**  
On the Login screen, select *IAM Login* and enter the Account ID (or Alias), IAM username and password. See [Logging in as an IAM user on page 35](#).

## External IdP roles

- 1. After enabling external IdP, if the external IdP has any problem, is it possible to still access the FortiCloud account?**  
The master user can always access the account even if external IdP is enabled. Using one user management method is recommended. That said, if a local IAM User is needed for some scenario, you can configure a co-exist date to use both the local IAM users and external IdP roles. See [Setting a co-exist end date on page 104](#).
- 2. Can I login directly to [www.forticloud.com](http://www.forticloud.com) with the users in my external IdP?**  
Users are stored in an external IdP (such as Azure, Okta, and so on) and FortiCloud does not store user information or credentials. Therefore, logging in directly to [www.forticloud.com](http://www.forticloud.com) using the email or IAM login tab would not work. Only IAM users (and legacy sub-users) created under the master account can login directly through [www.forticloud.com](http://www.forticloud.com), however that access will expire when the co-exist period ends.
- 3. How do you resolve the *Receive Microsoft error: Authentication method by which the user authenticated with the service doesn't match requested authentication method 'Password, Protected Transport. Contact the FortiCloud Application owner error?***  
Please contact your Fortinet Sales representative or the Customer Service team through a ticket with the screenshots of the error and URLs.
- 4. Why does logging into FortiCloud as an IAM User or legacy sub-user no longer work?**  
Once the transition period stated in the enrollment form is passed, only the master account will be able to log in directly. IAM users and sub users will not be able to log in anymore. The co-exist end date may be updated to allow for more transition time. See [Setting a co-exist end date on page 104](#).
- 5. How do you disable the External IdP feature?**  
Contact your Fortinet Sales representative or the Customer Service team through a ticket to disable the feature.
- 6. Do we need to reach out to Fortinet every time we want to add new users within external IdP?**  
No. User management is handled on the external IdP (such as Azure, Okta, and so on) and permissions may be controlled through the *Role* attribute value mapping to corresponding external IdP role and permission profile in FortiCloud.
- 7. Why does the FortiCloud account not show the option to add an external IdP role in the FortiCloud IAM portal?**

The option to add external IdP roles is displayed only for accounts enrolled for external IdP. If external IdP is enabled for the FortiCloud account, ensure that the user is logged in as the master user with the account ID matching that of the enrollment form.

- 8. How do you update the certificate for External IdP when it is going to expire?**

Contact your Fortinet Sales representative or the Customer Service team through a ticket in advance with the new certificate. It may be updated on Fortinet side with specified date, time, and time zone.
- 9. Can I have multiple *Role* values for a single user?**

Yes, multiple values of the *Role* attribute can be passed to FortiCloud. When multiple roles are configured, users will be prompted by a screen to select a role to proceed. Each value of Role must have a corresponding external IdP role in the master account.
- 10. Can I use External IdP to log into a FortiGate?**

No. SSO on devices from external IdP is not supported for now. Instead, the external IdP can be configured directly onto the device. See [Configuring SAML SSO login for FortiGate administrators with Entra ID acting as SAML IdP](#).
- 11. How do I link a different account number to my external IdP?**

Provide your account number and Fortinet SAML URLs to your Fortinet Sales representative or the Customer Service team through a ticket.
- 12. How do I update the IdP meta data?**

Contact your Fortinet Sales representative or the Customer Service team through a ticket with the new IdP metadata file and Fortinet SAML URLs.
- 13. Can I have both external IdP users and IAM users?**

It is recommended to use one method of managing users. However, a co-exist date may be updated until the customer feels ready to transition to external IdP fully.
- 14. Will the master user access expire after the co-exist period ends?**

No. The master user access with email and password credentials to the FortiCloud account is not impacted by co-exist period. You can always login with master user and update co-exist period if needed.
- 15. What do I do if the URL is not redirecting to IdP login page?**

Try the login in incognito mode and use the portal URL provided by Fortinet team:  
<https://customersso1.fortinet.com/saml-idp/proxy/{ext-idp-id}/login/>
- 16. Is External IdP supported when using FortiCloud Organization?**

External IdP works with FortiCloud Organizations.  
Please ensure the following:

  - The external IdP is connected to the organization root account.
  - The permission profile is set to type Organizations. See [Permission scope on page 19](#).
  - The external IdP role type is also set to Organizations with required scope.

## Legacy sub accounts

- 1. Can I still create traditional sub accounts?**

Yes, however we strongly recommend migrating your users to the IAM portal to take advantage of the security features. The IAM portal includes a sub user migration wizard for easy migration.
- 2. Will you stop supporting sub accounts, and if so, when?**

While both models co-exist currently, the legacy user management model is expected to be deprecated in the near future. The timeline for deprecation will be communicated later.

**3. What limitations do legacy sub accounts have?**

Legacy sub accounts have limited permission controls. The IAM permission model enhances the access control with fine grained permissions for various cloud products and services.



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2025 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.