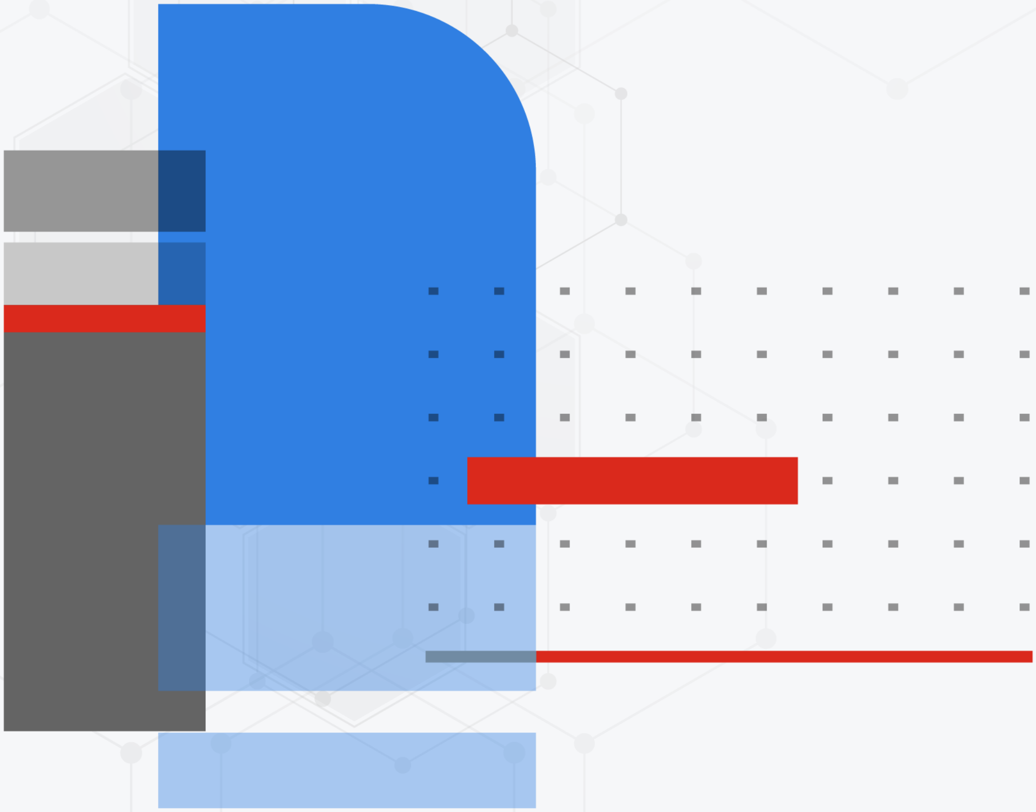
Administration Guide

Identity & Access Management 24.1



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

February 03, 2024
Identity & Access Management 24.1 Administration Guide
57-241-986043-20240203

TABLE OF CONTENTS

Change Log

Date	Change Description
2024-02-03	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.

IdP roles are a limited beta feature.

Multi-factor Authentication (2FA)

Two-Factor Authentication is fast and easy to configure. Users can authenticate using FortiToken or with an emailed security token. IAM administrators can enforce 2FA for all users at the account level. If a user disables 2FA for their account, they cannot access Fortinet applications until they enable it again.

What's new in version 24.1

Resource-based permissions for the FortiCare portal

There is a new permissions card available for the FortiCare New portal. When assigning permissions for the FortiCare New portal, the user can be assigned access using resource-based permissions. The FortiCare Legacy portal will continue to use role-based permissions. See Portals with resource-based permission on page 15 and User access in the FortiCare guide.

Enforcing two-factor authentication

Email users will be forced to enable two-factor authentication with the FortiToken mobile app if is has been enforced at the Organization or Account level. When logging into your email account, you will be prompted to set up two-factor authentication before you can proceed with logging in. Two-factor authentication is recommended to improve your security by forcing you to enter a security code when you log into the portals. See Two-Factor Authentication (2FA) on page 63.

Requirements

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

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

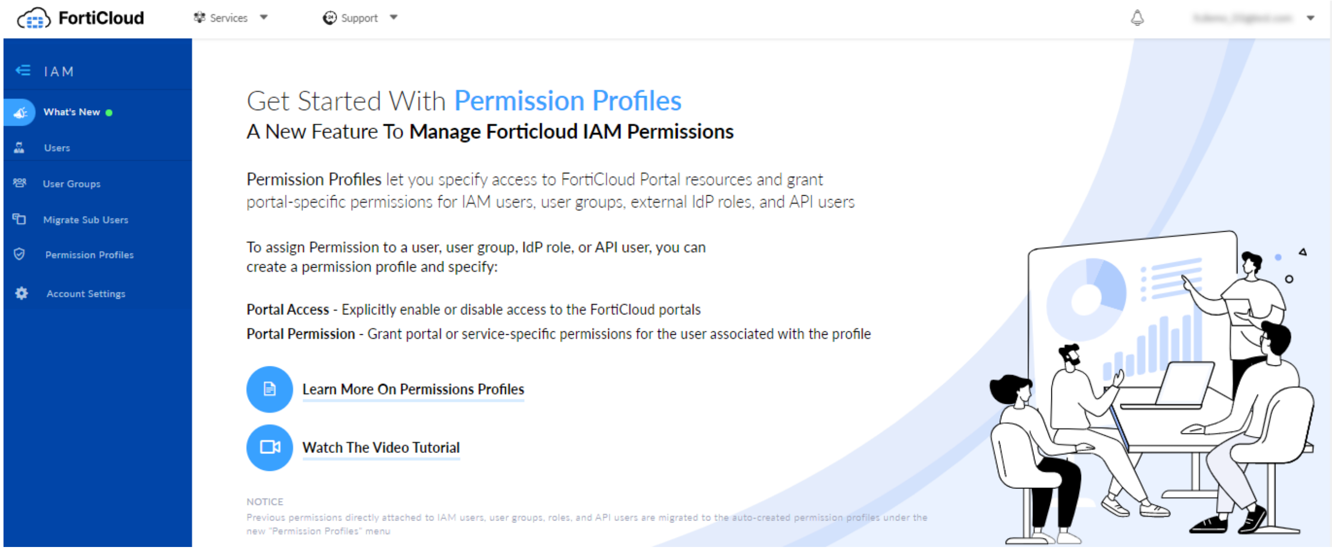
The IAM portal is only available in English at this time. For information on language support and supported browsers, see the Release Notes.

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.



Get Started With **Permission Profiles**

A New Feature To **Manage Forticloud IAM Permissions**

Permission Profiles let you specify access to FortiCloud Portal resources and grant portal-specific permissions for IAM users, user groups, external IdP roles, and API users

To assign Permission to a user, user group, IdP role, or API user, you can create a permission profile and specify:

Portal Access - Explicitly enable or disable access to the FortiCloud portals

Portal Permission - Grant portal or service-specific permissions for the user associated with the profile

Learn More On Permissions Profiles

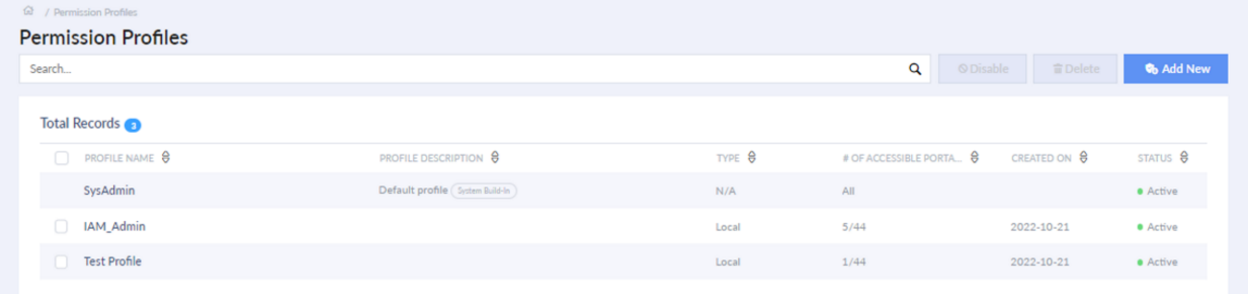
Watch The Video Tutorial

NOTICE

Previous permissions directly attached to IAM users, user groups, roles, and API users are migrated to the auto-created permission profiles under the new "Permission Profiles" 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 access from the left-hand navigation tree. See Permission profiles on page 15.



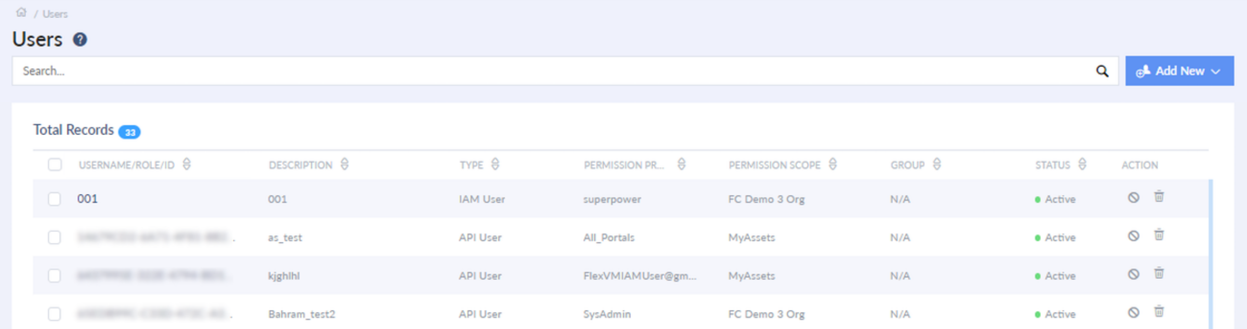
Permission Profiles

Total Records 3

	PROFILE NAME	PROFILE DESCRIPTION	TYPE	# OF ACCESSIBLE PORTA...	CREATED ON	STATUS
	SysAdmin	Default profile System Build-In	N/A	All		● Active
□	IAM_Admin		Local	5/44	2022-10-21	● Active
□	Test Profile		Local	1/44	2022-10-21	● Active

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 22.

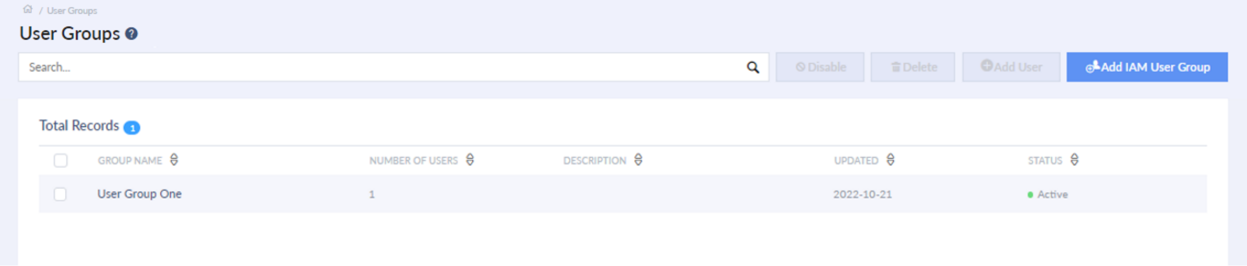


Total Records 33

□	USERNAME/ROLE/ID	DESCRIPTION	TYPE	PERMISSION PR...	PERMISSION SCOPE	GROUP	STATUS	ACTION
□	001	001	IAM User	superpower	FC Demo 3 Org	N/A	● Active	⊘ 🗑
□	[redacted]	as_test	API User	All_Portals	MyAssets	N/A	● Active	⊘ 🗑
□	[redacted]	kjghlhl	API User	FlexVMIAMUser@gm...	MyAssets	N/A	● Active	⊘ 🗑
□	[redacted]	Bahram_test2	API User	SysAdmin	FC Demo 3 Org	N/A	● Active	⊘ 🗑

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 47.

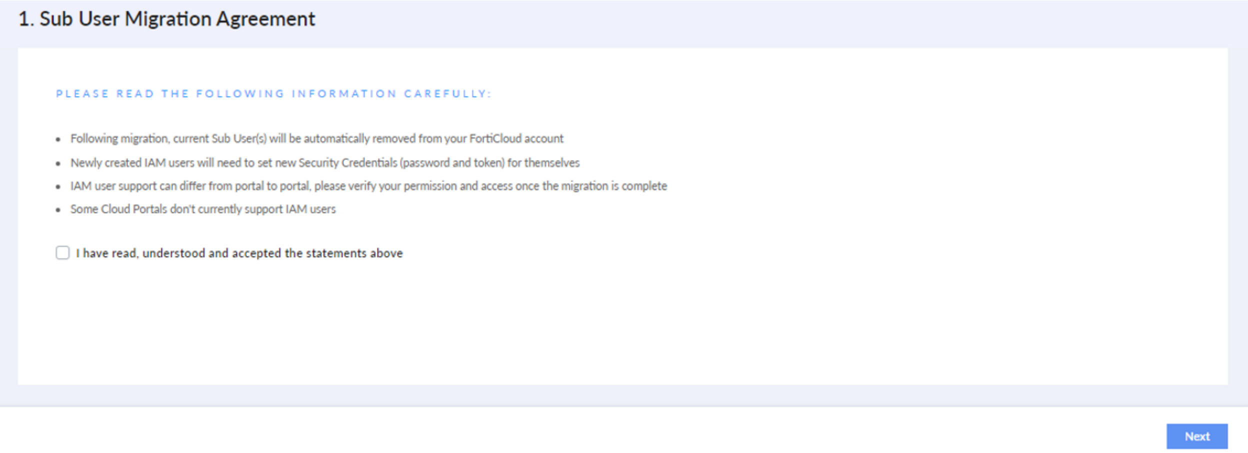


Total Records 1

□	GROUP NAME	NUMBER OF USERS	DESCRIPTION	UPDATED	STATUS
□	User Group One	1		2022-10-21	● 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 53.



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

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 70.

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*.

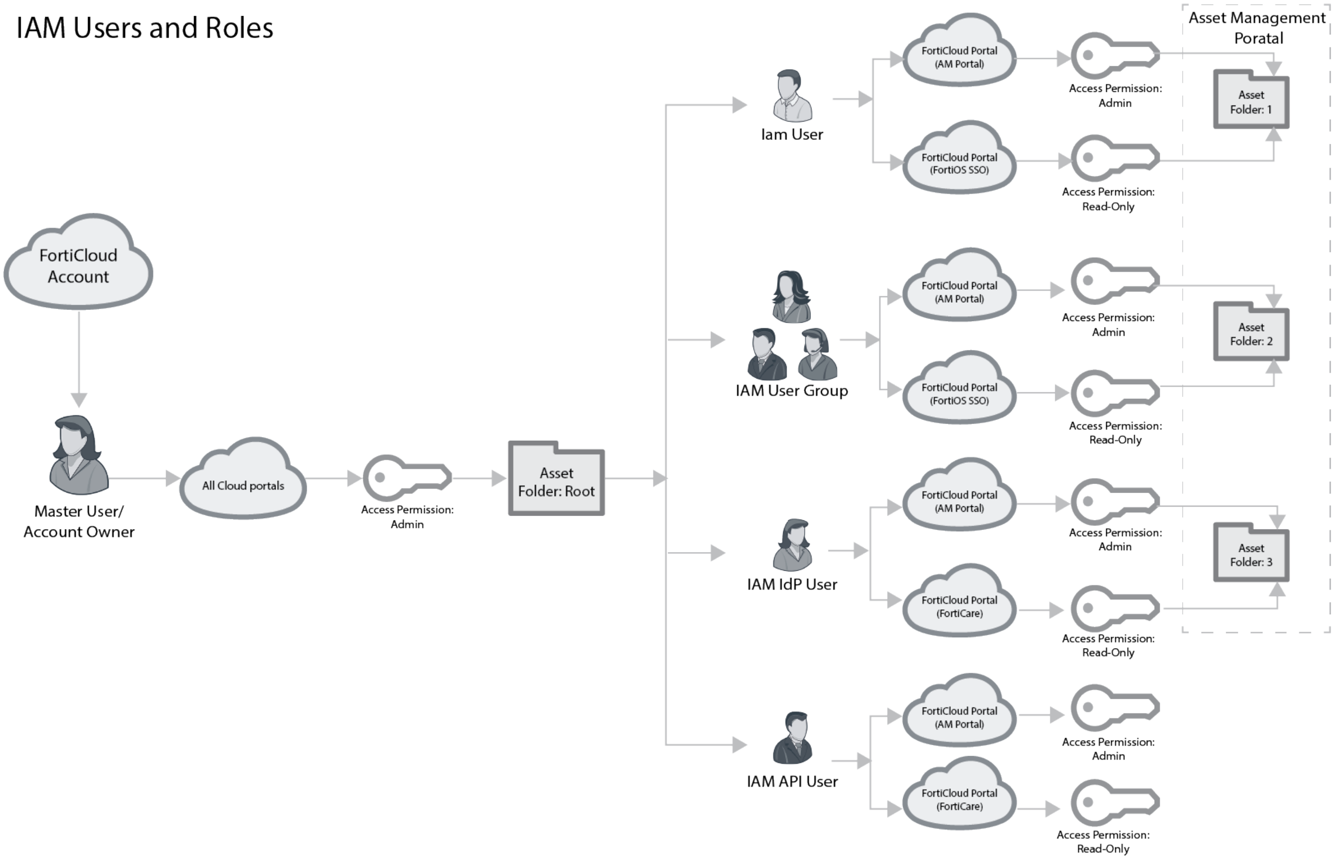
IAM User Model

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
IAM user	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.
API users	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. 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.
External IdP roles	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. 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. IdP roles are a limited beta feature.


IAM Users and Roles
FortiCloud Account
Master User/ Account Owner
All Cloud portals
Access Permission: Admin
Asset Folder: Root
Iam User
IAM User Group
IAM IdP User
IAM API User
FortiCloud Portal (AM Portal)
FortiCloud Portal (FortiOS SSO)
FortiCloud Portal (AM Portal)
FortiCloud Portal (FortiOS SSO)
FortiCloud Portal (AM Portal)
FortiCloud Portal (FortiCare)
FortiCloud Portal (AM Portal)
FortiCloud Portal (FortiCare)
Access Permission: Admin
Access Permission: Read-Only
Access Permission: Admin
Access Permission: Read-Only
Access Permission: Admin
Access Permission: Read-Only
Access Permission: Admin
Access Permission: Read-Only
Asset Management Poratal
Asset Folder: 1
Asset Folder: 2
Asset Folder: 3

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
Account Access Management	Add sub users to the account	Add IAM users to the account
Permission Control	Account level (Full Access/Limited Access)	Fine grained permissions for each FortiCloud Service
Asset Permissions	List of devices/Asset Groups (limited)	Asset folders or OUs with permissions hierarchy
User Groups & Permissions	User group (limited)	User groups and group-level permissions
Portal Access	No per portal control	Allow or Deny access per portal
API User Support	No	Granular permissions for each FortiCloud Service APIs
User 2FA Management	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 15 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 22 and User groups on page 47.

The *Permission Profiles* page can be accessed from the left-hand navigation menu. See Identity & Access Management Portal on page 9.

This section contains the following topics:

- Permission scope on page 18
- Creating a permission profile on page 18
- Managing permission profiles on page 20

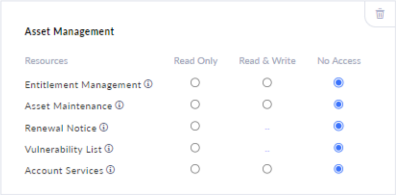
Portals with resource-based permission

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 15
- IAM on page 16
- FortiCare on page 17

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.



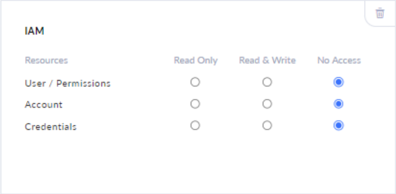
Asset Management

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

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



IAM

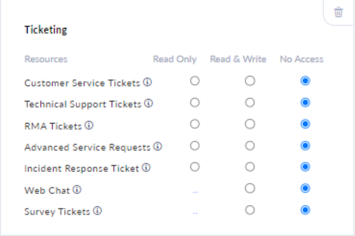
Resources	Read Only	Read & Write	No Access
User / Permissions	○	○	●
Account	○	○	●
Credentials	○	○	●

Resource	Description
User/Permissions	Provide control over users, user groups, permission profiles, and migrating sub users. The user can be granted *Read Only*, *Read & Write*, or *No Access* privileges.

Resource	Description
Account	Provide account management capabilities, including managing *Account Settings*. The user can be granted *Read Only*, *Read & Write*, or *No Access* privileges.
Credentials	Provide control over account *Security Credentials*. The user can be granted *Read Only*, *Read & Write*, or *No Access* privileges.

FortiCare

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



Ticketing

Resources	Read Only	Read & Write	No Access
Customer Service Tickets ⓘ	○	○	●
Technical Support Tickets ⓘ	○	○	●
RMA Tickets ⓘ	○	○	●
Advanced Service Requests ⓘ	○	○	●
Incident Response Ticket ⓘ	○	○	●
Web Chat ⓘ	--	○	●
Survey Tickets ⓘ	--	○	●

Resource	Description
Customer Service Tickets	Allow the user to create and track tickets pertaining to contracts and account management. The user can be granted *Read Only*, *Read & Write*, or *No Access* privileges.
Technical Support Tickets	Allow the user to create and track tickets for technical issues. The user can be granted *Read Only*, *Read & Write*, or *No Access* privileges.
RMA Tickets	Allow the user to create and track tickets pertaining to DOA and RMA assets. The user can be granted *Read Only*, *Read & Write*, or *No Access* privileges.
Advanced Service Requests	Allow the user to submit an Advanced Service request for professional assistance. The user can be granted *Read Only*, *Read & Write*, or *No Access* privileges.
Incident Response Ticket	Allow the user to submit an Incident Response ticket for evaluation. The user can be granted *Read Only*, *Read & Write*, or *No Access* privileges.
Web Chat	Allow the user to join live web chats with Fortinet support. The user can be granted *Read & Write* or *No Access* privileges.
Survey Tickets	Allow the user to submit feedback in the ticket survey. The user can be granted *Read & Write* or *No Access* privileges.

The FortiCare Legacy portal permissions can be assigned using the role-based *FortiCare* option.

Permission scope

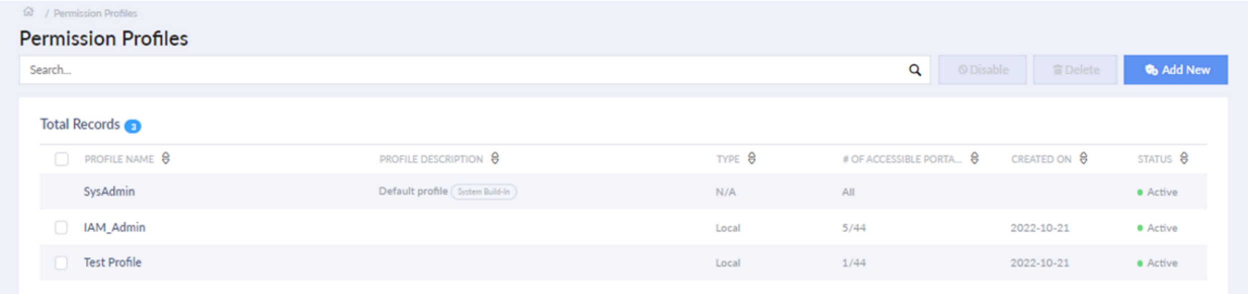
A feature of the new permission model is the permission scope. The permission scope defines what an IAM user, user group, external IdP roles, and API users can access in terms of the resources, including users, asset folders, devices, and so on.

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 70.

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.

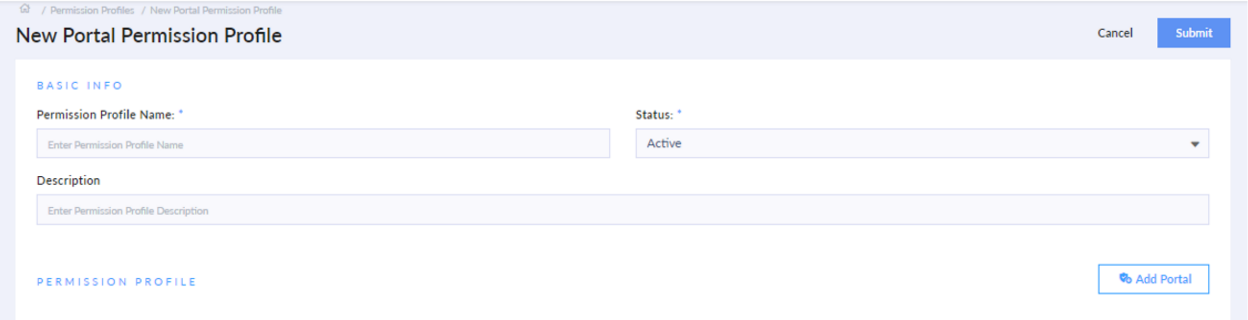


	PROFILE NAME	PROFILE DESCRIPTION	TYPE	# OF ACCESSIBLE PORTA...	CREATED ON	STATUS
	SysAdmin	Default profile System Build-In	N/A	All		● Active
□	IAM_Admin		Local	5/44	2022-10-21	● Active
□	Test Profile		Local	1/44	2022-10-21	● Active

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.


/ Permission Profiles / New Portal Permission Profile
New Portal Permission Profile
Cancel
Submit
BASIC INFO
PERMISSION PROFILE
Add Portal

Permission Profile Name: * Enter Permission Profile Name

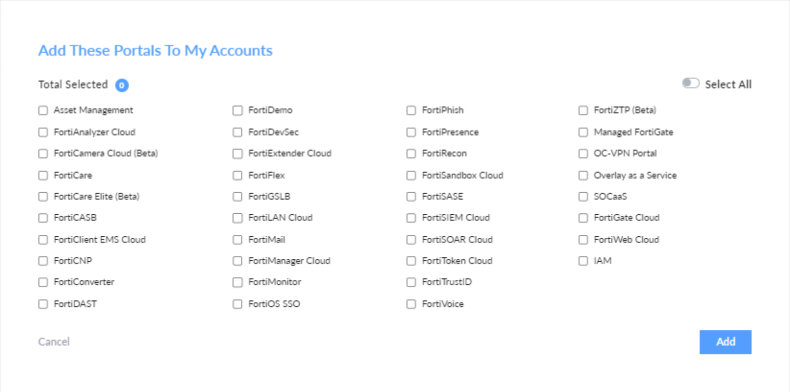
Status: * Active

Description: Enter Permission Profile Description

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

- □ Asset Management
- □ FortiAnalyzer Cloud
- □ FortiCamera Cloud (Beta)
- □ FortiCare
- □ FortiCare Elite (Beta)
- □ FortiCASB
- □ FortiClient EMS Cloud
- □ FortiCNP
- □ FortiConverter
- □ FortiDAST
- □ FortiDemo
- □ FortiDevSec
- □ FortiExtender Cloud
- □ FortiFlex
- □ FortiGSLB
- □ FortiLAN Cloud
- □ FortiMail
- □ FortiManager Cloud
- □ FortiMonitor
- □ FortiOS SSO
- □ FortiPhish
- □ FortiPresence
- □ FortiRecon
- □ FortiSandbox Cloud
- □ FortiSASE
- □ FortiSIEM Cloud
- □ FortiSOAR Cloud
- □ FortiToken Cloud
- □ FortiTrustID
- □ FortiVoice
- □ FortiZTP (Beta)
- □ Managed FortiGate
- □ OC-VPN Portal
- □ Overlay as a Service
- □ SOCaaS
- □ FortiGate Cloud
- □ FortiWeb Cloud
- □ IAM

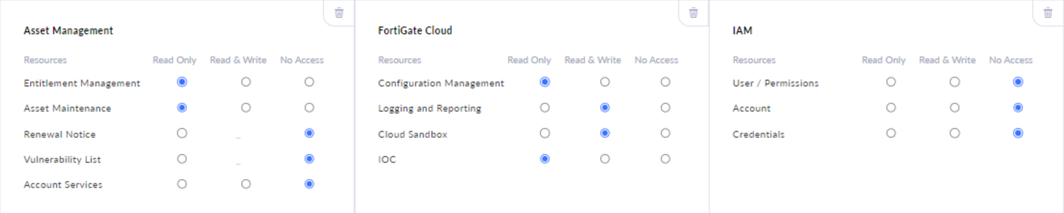
Cancel — Add

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.



Asset Management

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

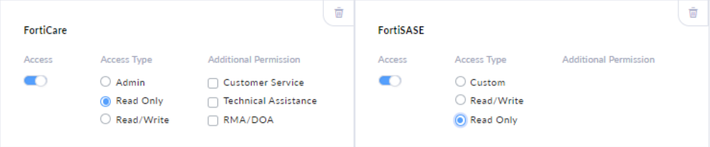
FortiGate Cloud

Resources	Read Only	Read & Write	No Access
Configuration Management	●	○	○
Logging and Reporting	○	●	○
Cloud Sandbox	○	●	○
IOC	●	○	○

IAM

Resources	Read Only	Read & Write	No Access
User / Permissions	○	○	●
Account	○	○	●
Credentials	○	○	●

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



FortiCare

Access: on

Access Type: ○ Admin ● Read Only ○ Read/Write

Additional Permission: □ Customer Service □ Technical Assistance □ RMA/DOA

FortiSASE

Access: on

Access Type: ○ Custom ○ Read/Write ● Read Only

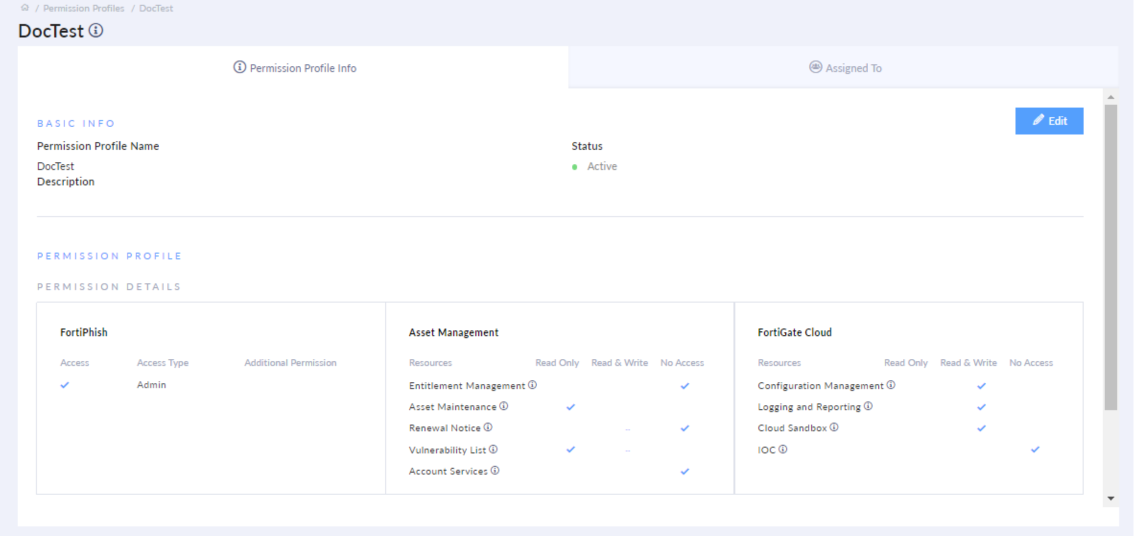
Additional Permission

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.



DocTest

BASIC INFO

Permission Profile Name
DocTest
Description

Status
● Active

PERMISSION PROFILE

PERMISSION DETAILS

FortiPhish

Access	Access Type	Additional Permission
✓	Admin	

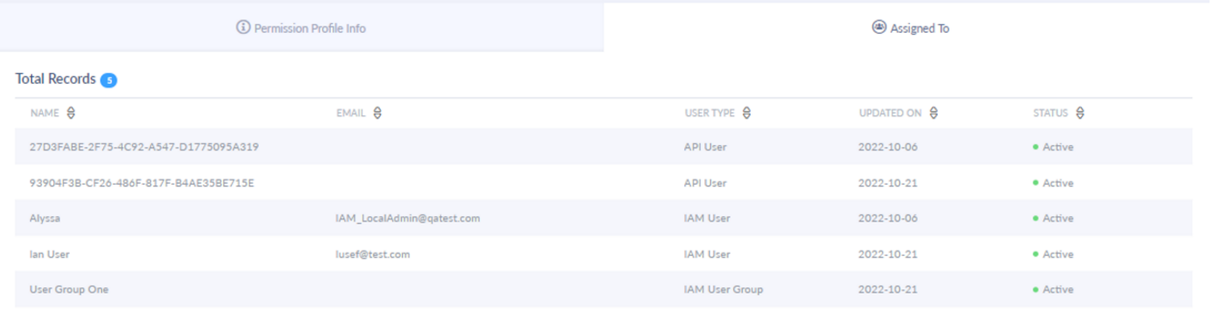
Asset Management

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

FortiGate Cloud

Resources	Read Only	Read & Write	No Access
Configuration Management		✓	
Logging and Reporting		✓	
Cloud Sandbox		✓	
IOC			✓

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



Total Records 5

NAME	EMAIL	USER TYPE	UPDATED ON	STATUS
27D3FABE-2F75-4C92-A547-D1775095A319		API User	2022-10-06	● Active
93904F3B-CF26-486F-817F-B4AE35BE715E		API User	2022-10-21	● Active
Alyssa	IAM_LocalAdmin@qatest.com	IAM User	2022-10-06	● Active
Ian User	Iusef@test.com	IAM User	2022-10-21	● Active
User Group One		IAM User Group	2022-10-21	● Active

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

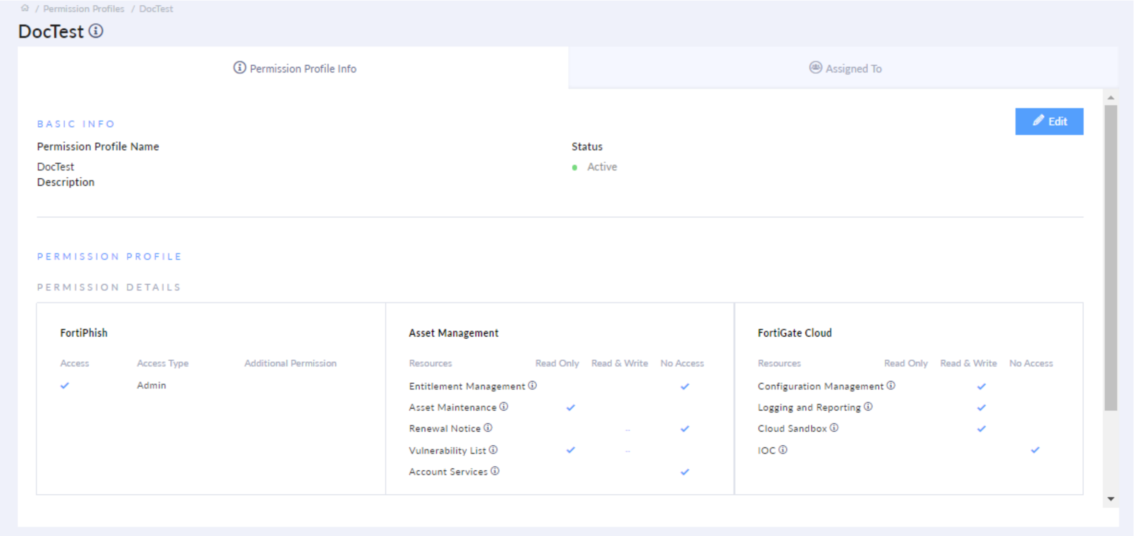
You cannot edit, disable, or delete the default *SysAdmin* permission profile. See Creating a permission profile on page 18.

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.



DocTest ⓘ

BASIC INFO

Permission Profile Name
DocTest

Description

Status
● Active

PERMISSION PROFILE

PERMISSION DETAILS

FortiPhish

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 ⓘ			✓

FortiGate Cloud

Resources	Read Only	Read & Write	No Access
Configuration Management ⓘ		✓	
Logging and Reporting ⓘ		✓	
Cloud Sandbox ⓘ		✓	
IOC ⓘ			✓

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

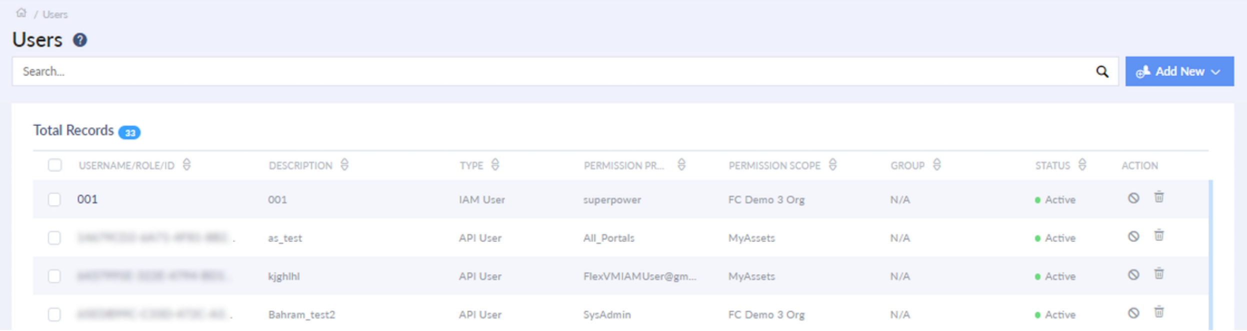
You can permanently delete a permission profile that is no longer needed. A permission profile cannot be deleted if an active IAM user is assigned to it.

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 *IAM Users*, *API Users*, and *External IdP Roles* pages have been combined into the *Users* page. The *Users* page displays information on all registered users, including the user *Type*, *Permission Profile*, and *Permission Scope*.



Total Records 33

□	USERNAME/ROLE/ID	DESCRIPTION	TYPE	PERMISSION PR...	PERMISSION SCOPE	GROUP	STATUS	ACTION
□	001	001	IAM User	superpower	FC Demo 3 Org	N/A	● Active	⃠ 🗑
□	[redacted]	as_test	API User	All_Portals	MyAssets	N/A	● Active	⃠ 🗑
□	[redacted]	kjghlhl	API User	FlexVMIAMUser@gm...	MyAssets	N/A	● Active	⃠ 🗑
□	[redacted]	Bahram_test2	API User	SysAdmin	FC Demo 3 Org	N/A	● Active	⃠ 🗑

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

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

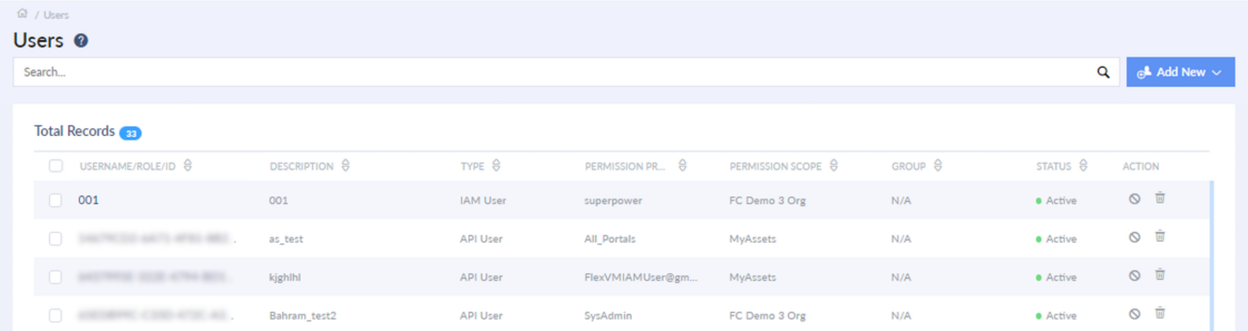
- IAM users on page 22
- API users on page 35
- External IdP roles on page 40

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* wizards 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 9.



Total Records 33

	USERNAME/ROLE/ID	DESCRIPTION	TYPE	PERMISSION PR...	PERMISSION SCOPE	GROUP	STATUS	ACTION
□	001	001	IAM User	superpower	FC Demo 3 Org	N/A	● Active	⦸ 🗑
□	[redacted]	as_test	API User	All_Portals	MyAssets	N/A	● Active	⦸ 🗑
□	[redacted]	kjghlhl	API User	FlexVMIAMUser@gm...	MyAssets	N/A	● Active	⦸ 🗑
□	[redacted]	Bahram_test2	API User	SysAdmin	FC Demo 3 Org	N/A	● Active	⦸ 🗑

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 23
- Managing IAM users on page 27
- Validating new IAM users on page 30
- Logging in as an IAM user on page 32
- Migration of existing users on page 33

Adding IAM users

Use the *Add New* wizard 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.

To add a new IAM user, you must:

1. Create the new user account. See Creating a new IAM user on page 23.
2. Generate the password reset link and share it with the selected IAM user. See Generating the password reset link on page 26.

Creating a new IAM user

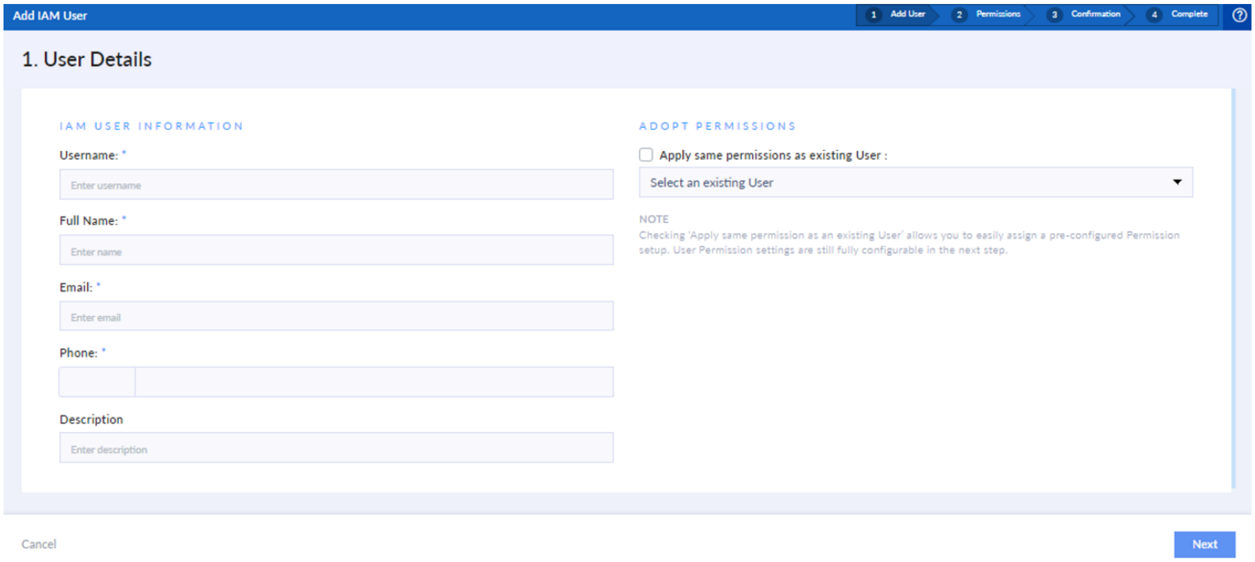
You can create a new IAM user with the *Add New* wizard.

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*.

Username	Type the username with no spaces.

Full Name	Type the user's first and last name.
Email	Type the user's email address.
Phone	Select the country code from the dropdown, and type the user's phone number.
Description (Optional)	Type a description of the user.



Add IAM User

1. User Details

IAM USER INFORMATION

Username: *

Enter username

Full Name: *

Enter name

Email: *

Enter email

Phone: *

Description

Enter description

ADOPT PERMISSIONS

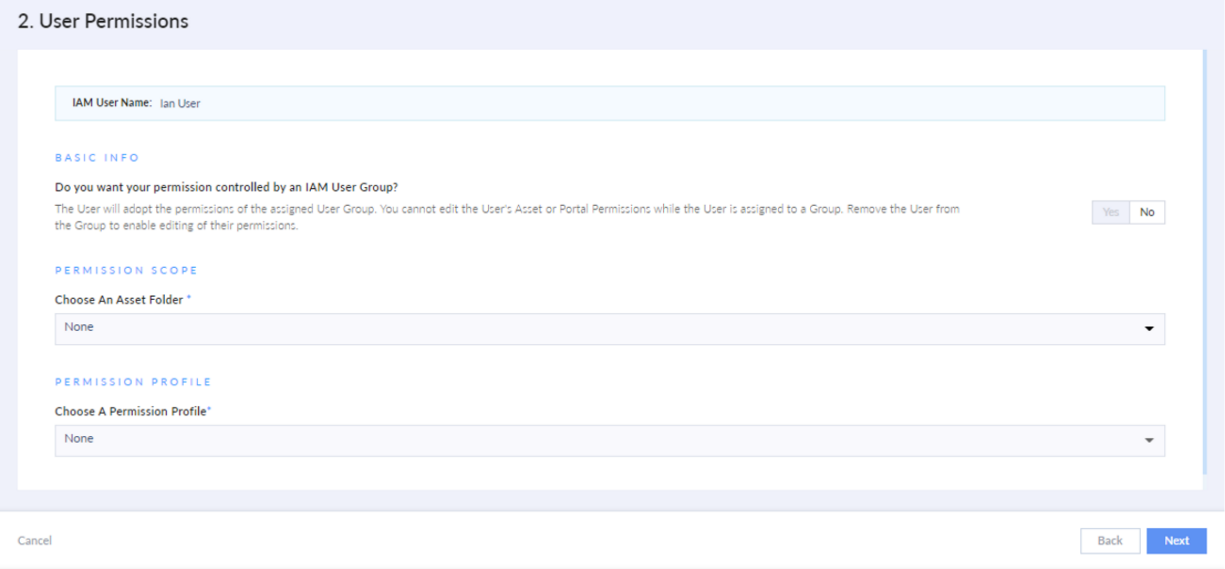
□ Apply same permissions as existing User :

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 47.
   a. Select *Yes* from *Basic Info*.



2. User Permissions

IAM User Name: Ian 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

Choose An Asset Folder *

None

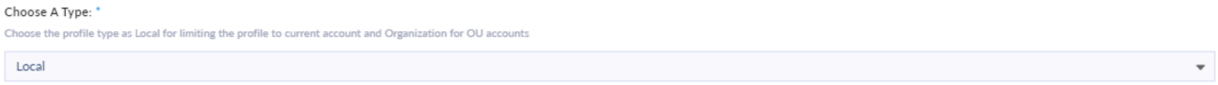
PERMISSION PROFILE

Choose A Permission Profile*

None

   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. Select the user type from *Choose A Type* dropdown list.



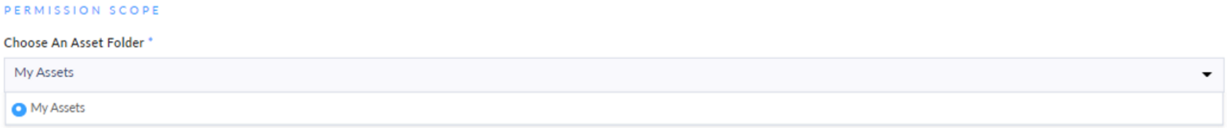
Choose A Type: *

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

Local

7. 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.



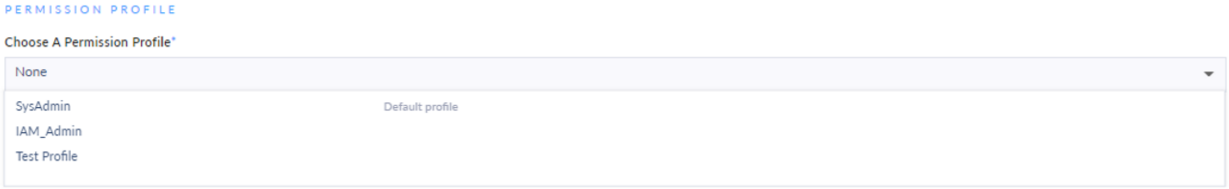
PERMISSION SCOPE

Choose An Asset Folder *

My Assets

● My Assets

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



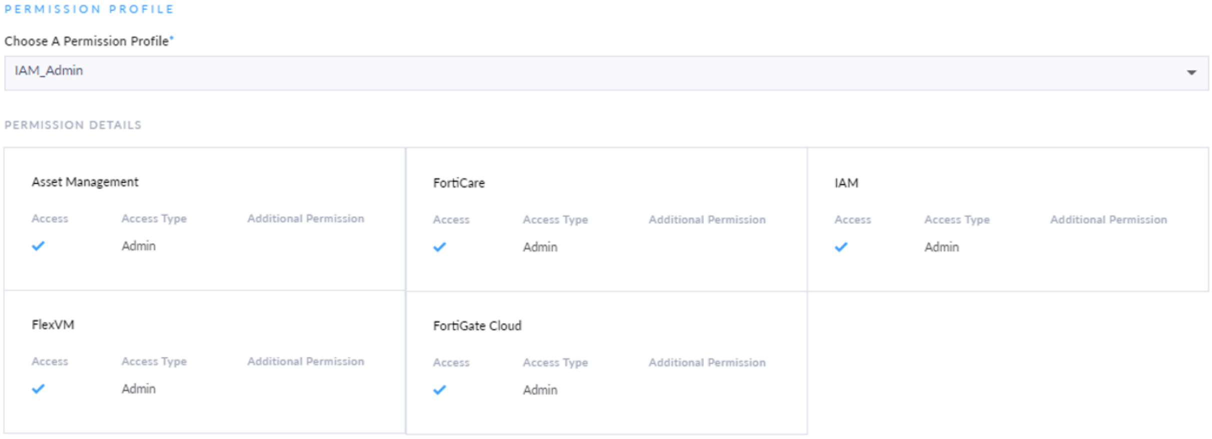
PERMISSION PROFILE

Choose A Permission Profile*

None

SysAdmin — Default profile
IAM_Admin
Test Profile

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



PERMISSION PROFILE

Choose A Permission Profile*

IAM_Admin

PERMISSION DETAILS

Asset Management

Access	Access Type	Additional Permission
✓	Admin	

FortiCare

Access	Access Type	Additional Permission
✓	Admin	

IAM

Access	Access Type	Additional Permission
✓	Admin	

FlexVM

Access	Access Type	Additional Permission
✓	Admin	

FortiGate Cloud

Access	Access Type	Additional Permission
✓	Admin	

> If the *SysAdmin* profile is selected, a message will display instead of portal cards to denote that the user has full access to all portals.

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

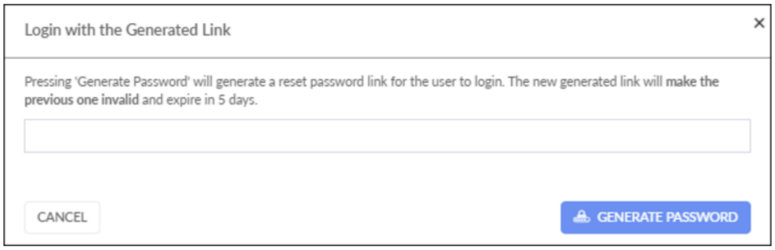
Account credentials must be shared with the user. The account password can be configured using *Generate Password*. See Generating the password reset link on page 26 to configure the account password and share user credentials.

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:

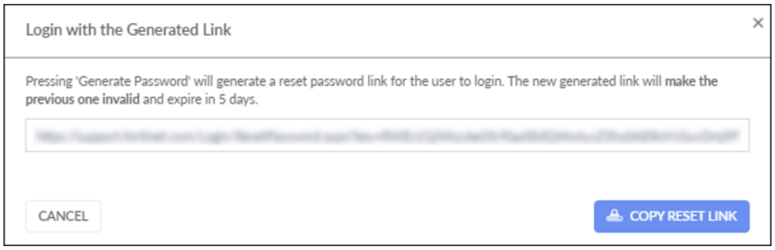
1. On the *Successful User Registration* page, click *Generate Password*. The *Login with the Generated Link* dialog opens.



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.

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

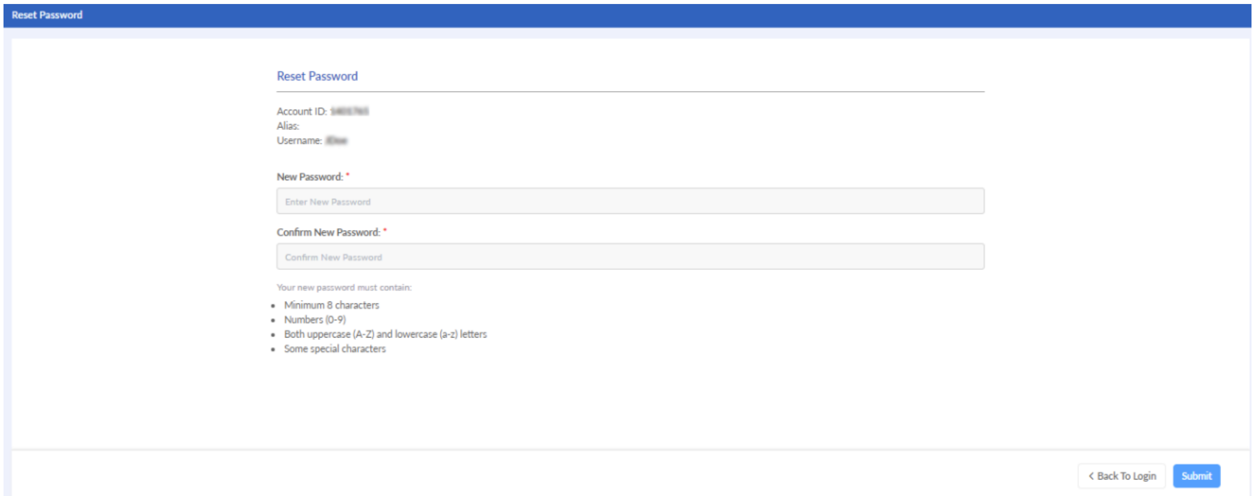


Login with the Generated Link

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.

[redacted]

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

Reset Password

Account ID: [redacted]
Alias:
Username: [redacted]

New Password: *
Enter New Password

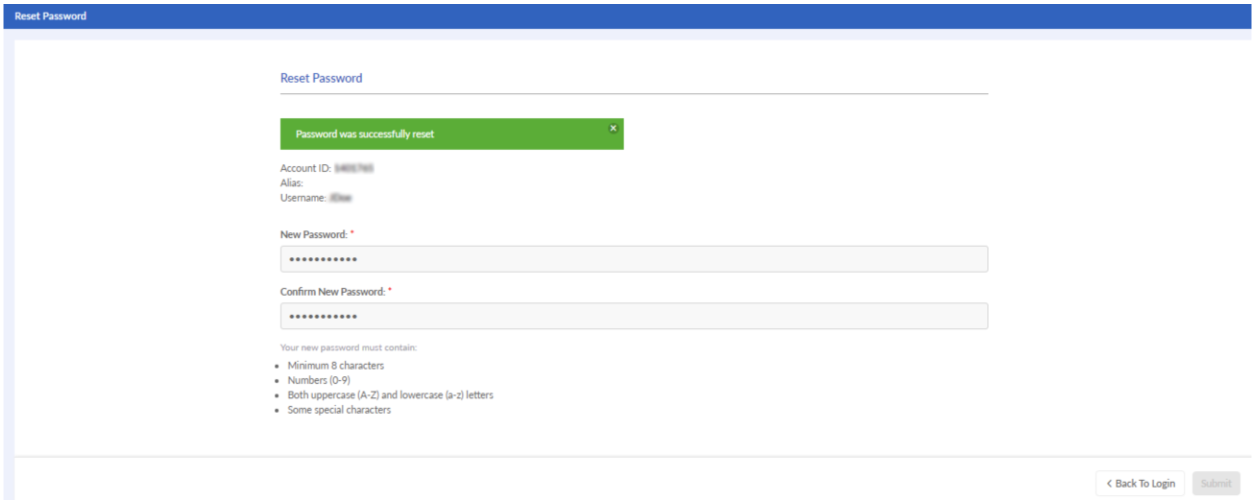
Confirm New Password: *
Confirm New Password

Your new password must contain:

- Minimum 8 characters
- Numbers (0-9)
- Both uppercase (A-Z) and lowercase (a-z) letters
- Some special characters

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

6. Click *Submit*. A confirmation message displays.



Reset Password

Password was successfully reset

Account ID: [redacted]
Alias:
Username: [redacted]

New Password: *

••••••••••••

Confirm New Password: *

••••••••••••

Your new password must contain:

- Minimum 8 characters
- Numbers (0-9)
- Both uppercase (A-Z) and lowercase (a-z) letters
- Some special characters

The *Generate Password* link can also be accessed on *Security Credentials* tab of the *Users* > *IAM user* page. See Resetting a password on page 29.

Send the credentials to the user. New IAM users are required to perform a validation check the first time they log in to a portal. See Validating new IAM users on page 30.

Managing IAM users

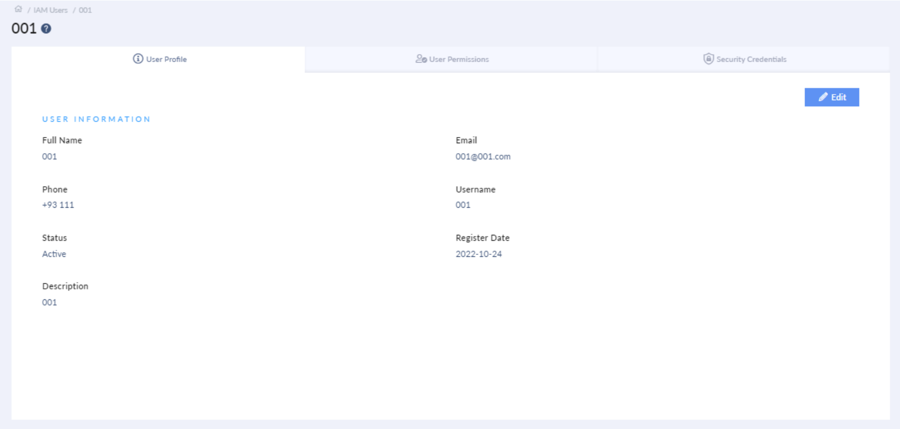
Select an IAM user from the *Users* page to update a user's details or generate the password reset link.

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

Column	Description
Username	The user's display name.
Full Name	The user's first and last name.
Email	The email address for the IAM user account.
Updated	The date the user's information was updated.
Group	The user group the user is assigned to.
Status	The user's status (*Active*/*Disabled*).

Updating user details

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



001

USER INFORMATION

Full Name
001

Email
001@001.com

Phone
+93 111

Username
001

Status
Active

Register Date
2022-10-24

Description
001

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 45.

To enable a user:

1. Select *Users* from the left-hand navigation menu. The *Users* page opens.
2. Find the user your 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:

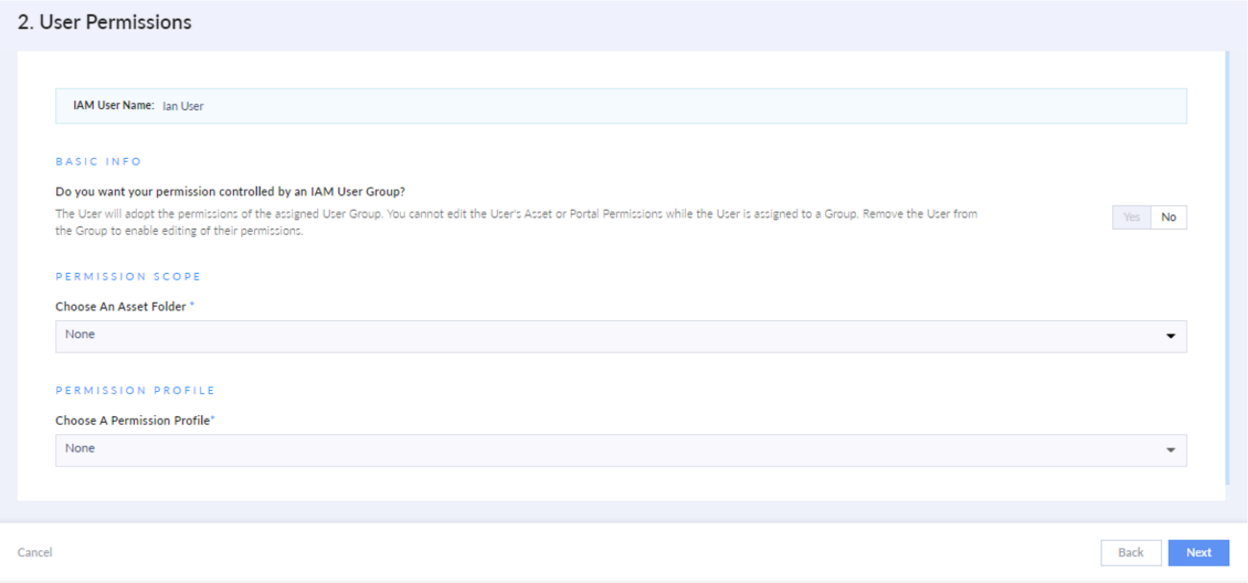
1. Select *Users* from the left-hand navigation menu. The *Users* page opens.
2. Select a user in the list.
3. Click *Disable*. The *Permission Changed Confirmation* dialog opens..
4. Click *Confirm*.

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: Ian 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

Choose An Asset Folder *

None

PERMISSION PROFILE

Choose A Permission Profile*

None

6. Select the user group from dropdown list.
7. Click *Update*.

Resetting a 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.

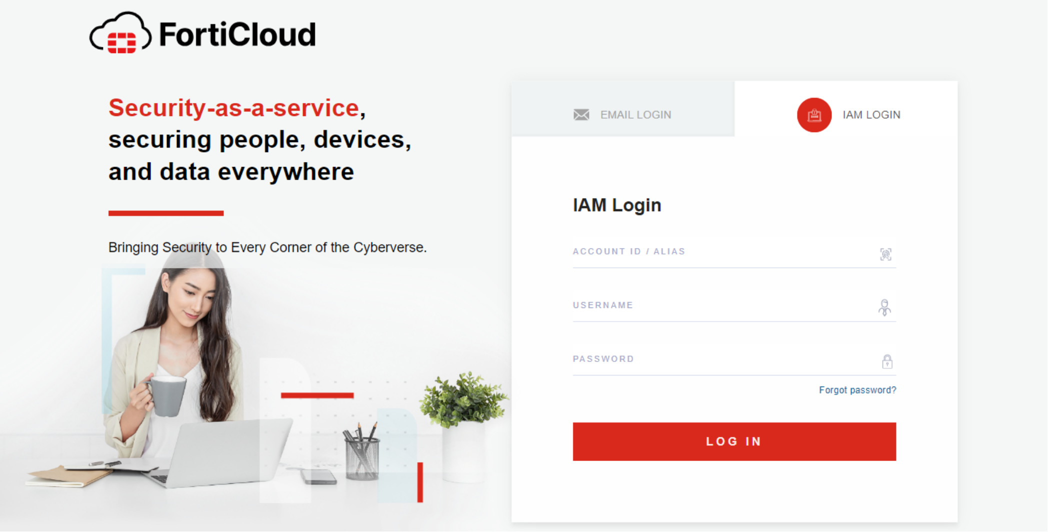
Validating new IAM users

New IAM users are required to verify their email address the first time they log in to a portal or after they change their email address.

When Two-Factor Authentication (2FA) is enabled, new IAM users will bypass this step and set up 2FA authorization instead. See Logging in with 2FA for the first time on page 65.

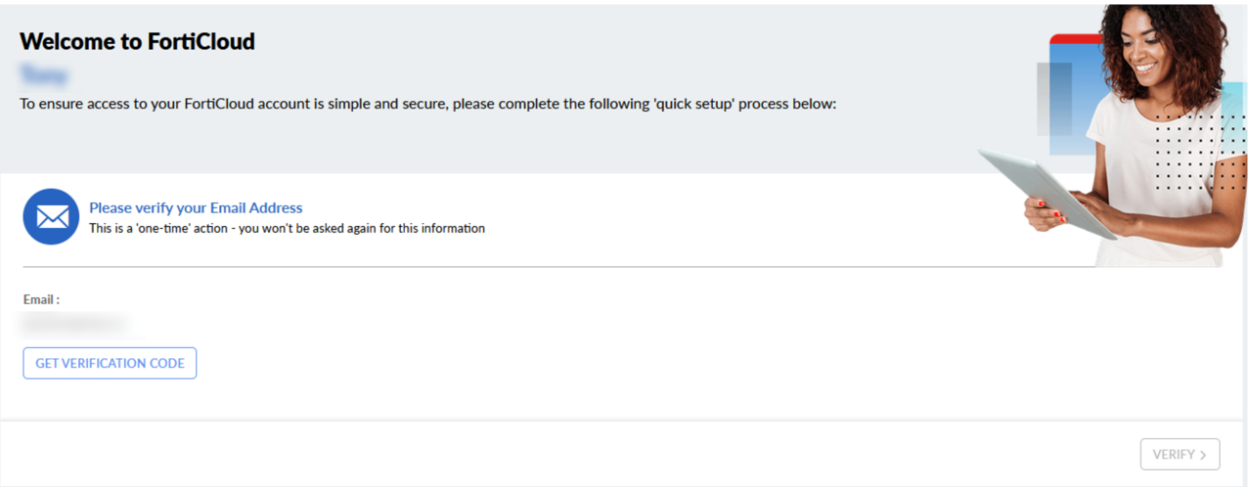
To validate a new email address:

1. Go to FortiCloud and click *Login Now*.
2. Click *IAM Login*.


FortiCloud
Security-as-a-service, securing people, devices, and data everywhere
Bringing Security to Every Corner of the Cyberverse.
EMAIL LOGIN
IAM LOGIN
IAM Login
ACCOUNT ID / ALIAS
USERNAME
PASSWORD
Forgot password?
LOG IN

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

[redacted]

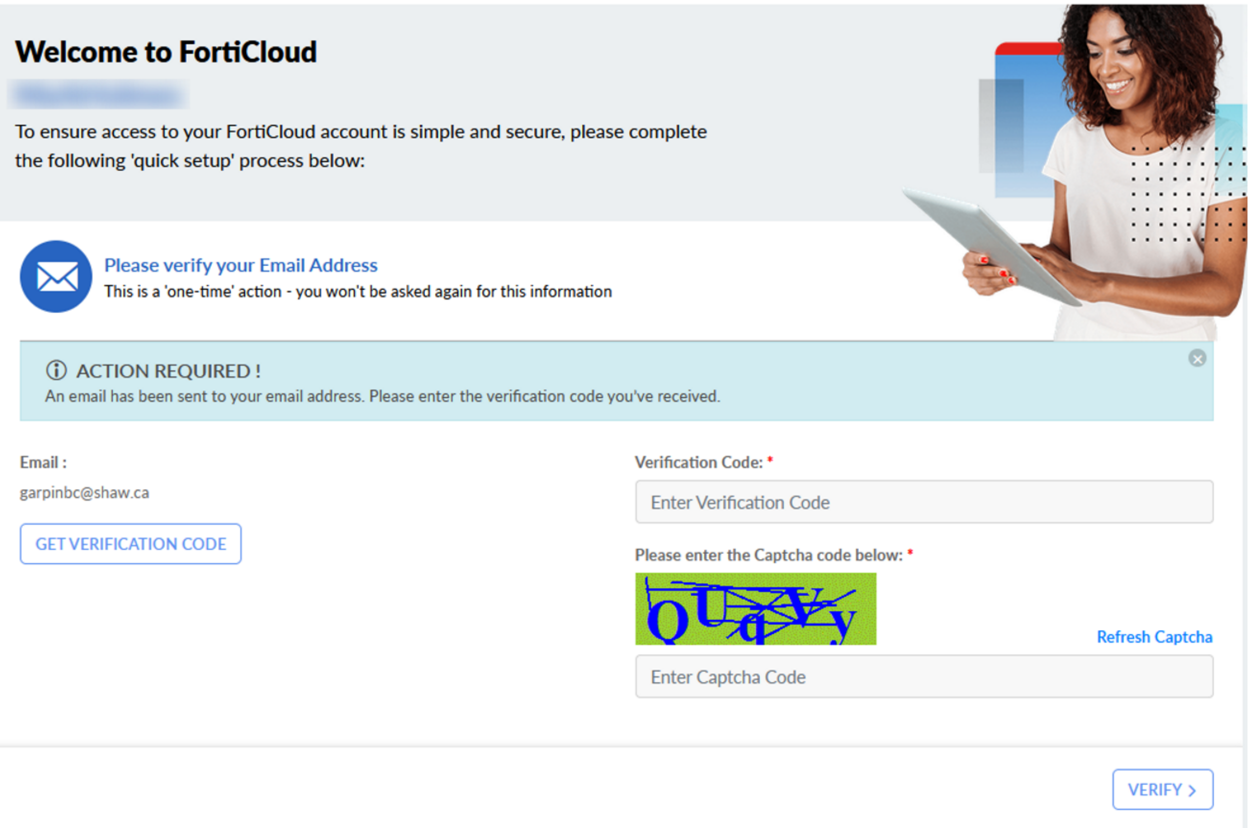
To ensure access to your FortiCloud account is simple and secure, please complete the following 'quick setup' process below:

Please verify your Email Address

This is a 'one-time' action - you won't be asked again for this information

Email : [redacted]

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



Welcome to FortiCloud

[redacted]

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 : garpinbc@shaw.ca

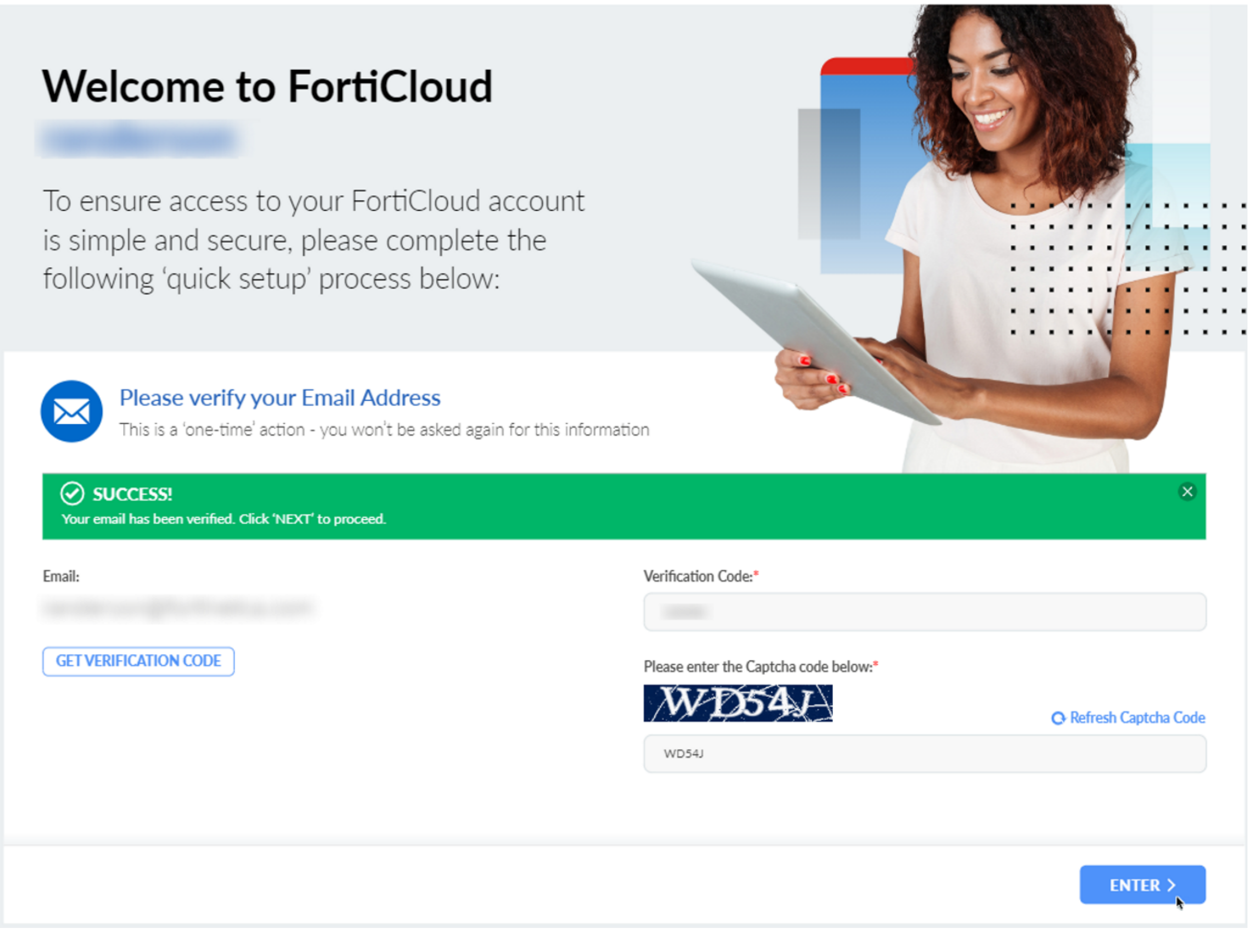
Verification Code: * Enter Verification Code

Please enter the Captcha code below: *

Enter Captcha Code

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

7. Click *Enter*.



Welcome to FortiCloud

[redacted]

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: [redacted]

Verification Code:* [redacted]

Please enter the Captcha code below:* WD54J

WD54J

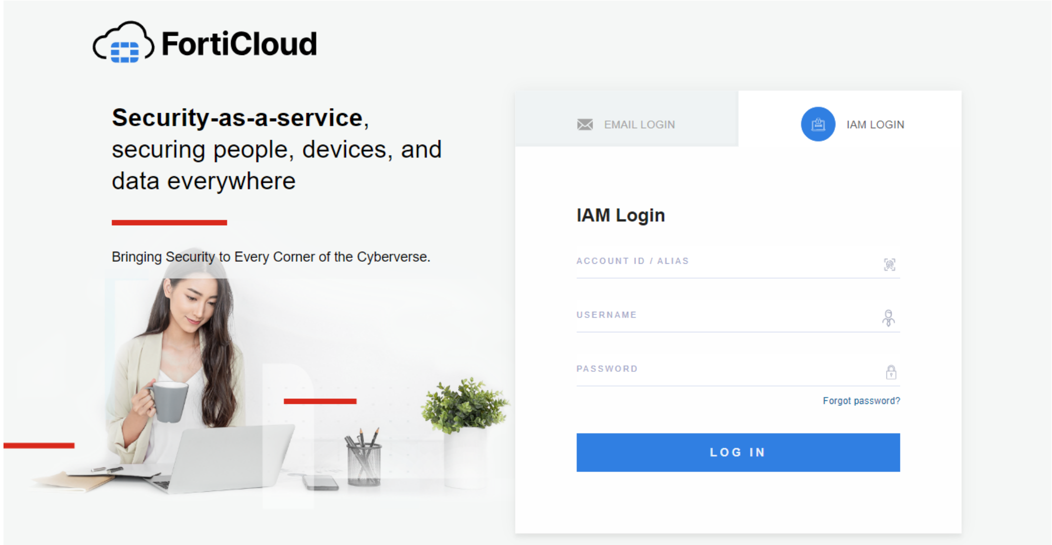
Logging in as an IAM user

Users can access FortiCloud services and support as an IAM user with their IAM user credentials. Once the login credentials have been verified, users can then proceed using the account 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 https://support.fortinet.com for the first time. See Two-Factor Authentication (2FA) on page 63.

To log in as an IAM user:

1. Go to https://support.fortinet.com.
2. Select *Login Now*. The log in portal opens.
3. Select *IAM Login*.


FortiCloud
Security-as-a-service, securing people, devices, and data everywhere
Bringing Security to Every Corner of the Cyberverse.
EMAIL LOGIN
IAM LOGIN
IAM Login
ACCOUNT ID / ALIAS
USERNAME
PASSWORD
Forgot password?
LOG IN

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*. 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.

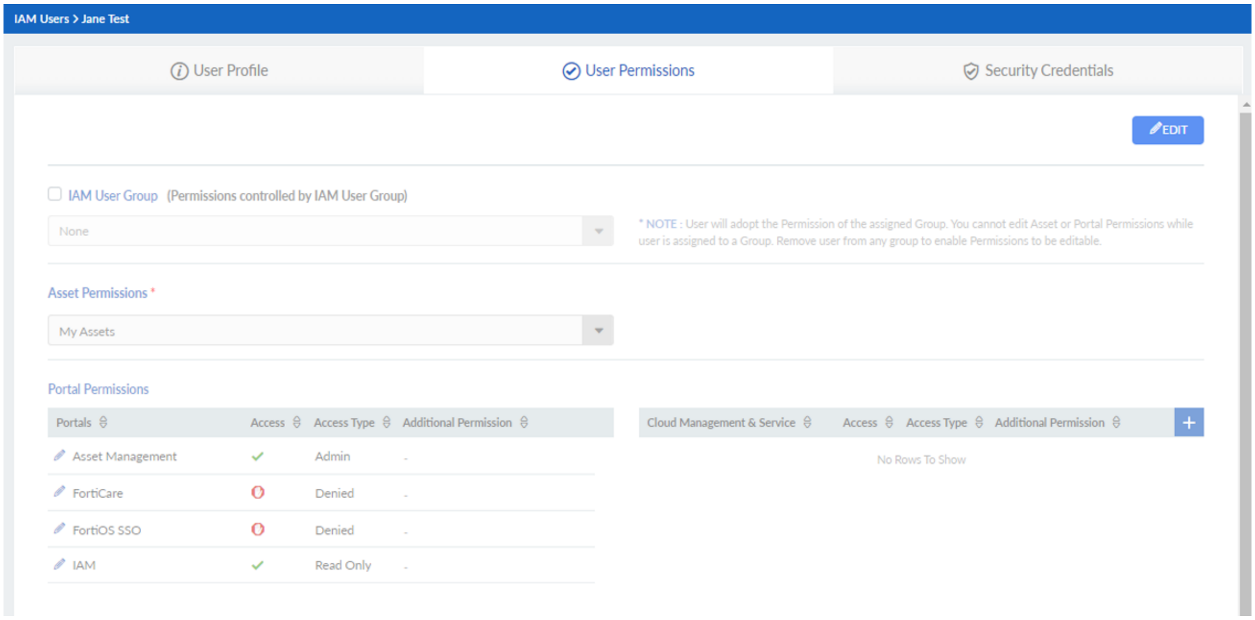
To effectively convert the Identity & Access Management portal to the new permission profile model, any pre-existing IAM users, user groups, and so on will automatically be converted to the new model. This migration of users will result in the existing IAM user being split into an IAM user and a permission 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

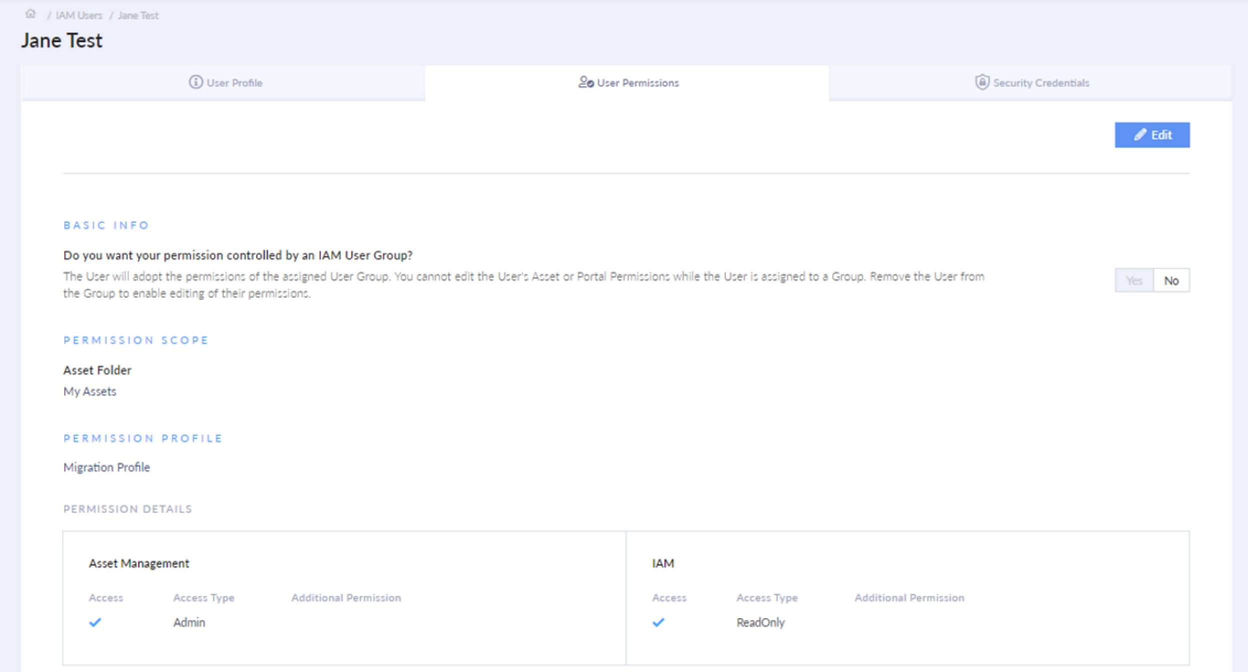
Portal Permissions

Portals	Access	Access Type	Additional Permission
Asset Management	✓	Admin	-
FortiCare	⊘	Denied	-
FortiOS SSO	⊘	Denied	-
IAM	✓	Read Only	-

Cloud Management & Service	Access	Access Type	Additional Permission
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.



/ IAM Users / Jane Test

Jane Test

User Profile | User Permissions | Security Credentials

Edit

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

Asset Folder

My Assets

PERMISSION PROFILE

Migration Profile

PERMISSION DETAILS

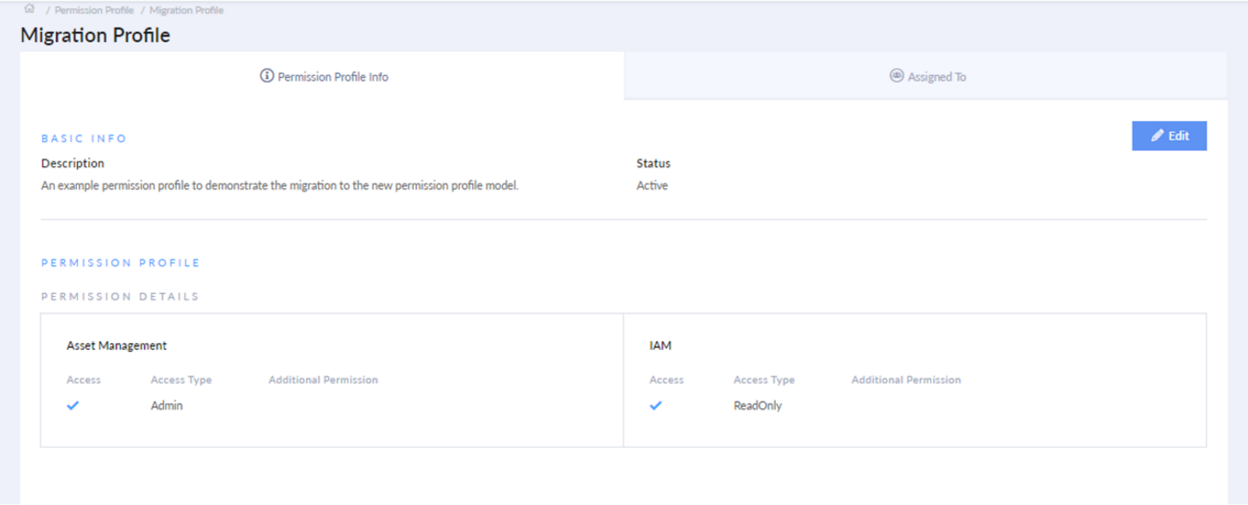
Asset Management

Access	Access Type	Additional Permission
✓	Admin	

IAM

Access	Access Type	Additional Permission
✓	ReadOnly	

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



BASIC INFO

Description

An example permission profile to demonstrate the migration to the new permission profile model.

Status

Active

PERMISSION PROFILE

PERMISSION DETAILS

Asset Management

Access	Access Type	Additional Permission
✓	Admin	

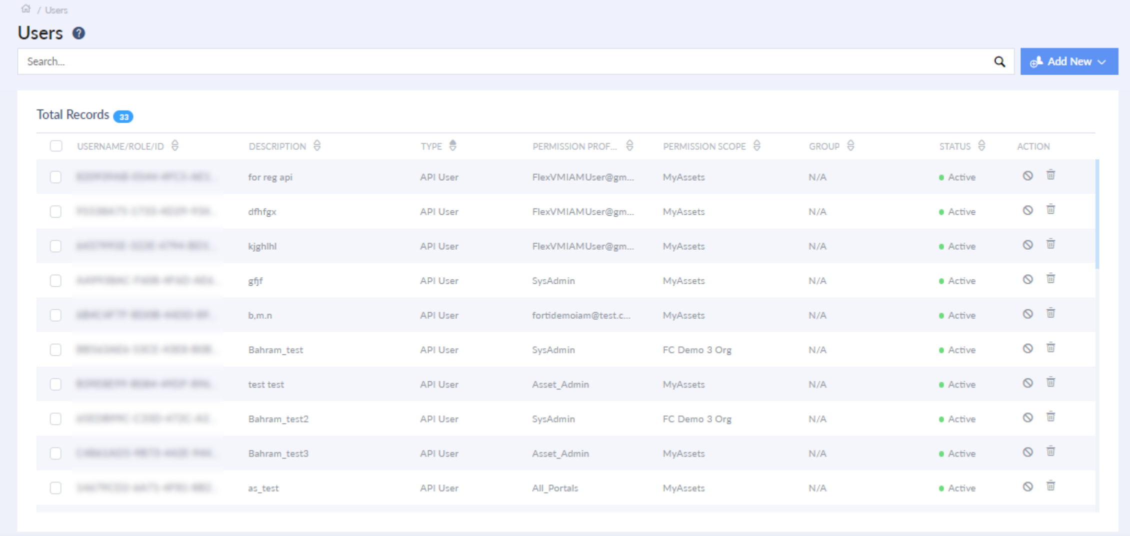
IAM

Access	Access Type	Additional Permission
✓	ReadOnly	

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 9.



Total Records 33

□	USERNAME/ROLE/ID	DESCRIPTION	TYPE	PERMISSION PROF...	PERMISSION SCOPE	GROUP	STATUS	ACTION
□	[redacted]	for reg api	API User	FlexVMIAMUser@gm...	MyAssets	N/A	● Active	⃠ 🗑
□	[redacted]	dfhfgx	API User	FlexVMIAMUser@gm...	MyAssets	N/A	● Active	⃠ 🗑
□	[redacted]	kjghlhl	API User	FlexVMIAMUser@gm...	MyAssets	N/A	● Active	⃠ 🗑
□	[redacted]	gfjf	API User	SysAdmin	MyAssets	N/A	● Active	⃠ 🗑
□	[redacted]	b,m.n	API User	fortidemoiam@test.c...	MyAssets	N/A	● Active	⃠ 🗑
□	[redacted]	Bahram_test	API User	SysAdmin	FC Demo 3 Org	N/A	● Active	⃠ 🗑
□	[redacted]	test test	API User	Asset_Admin	MyAssets	N/A	● Active	⃠ 🗑
□	[redacted]	Bahram_test2	API User	SysAdmin	FC Demo 3 Org	N/A	● Active	⃠ 🗑
□	[redacted]	Bahram_test3	API User	Asset_Admin	MyAssets	N/A	● Active	⃠ 🗑
□	[redacted]	as_test	API User	All_Portals	MyAssets	N/A	● Active	⃠ 🗑

This section contains the following topics:

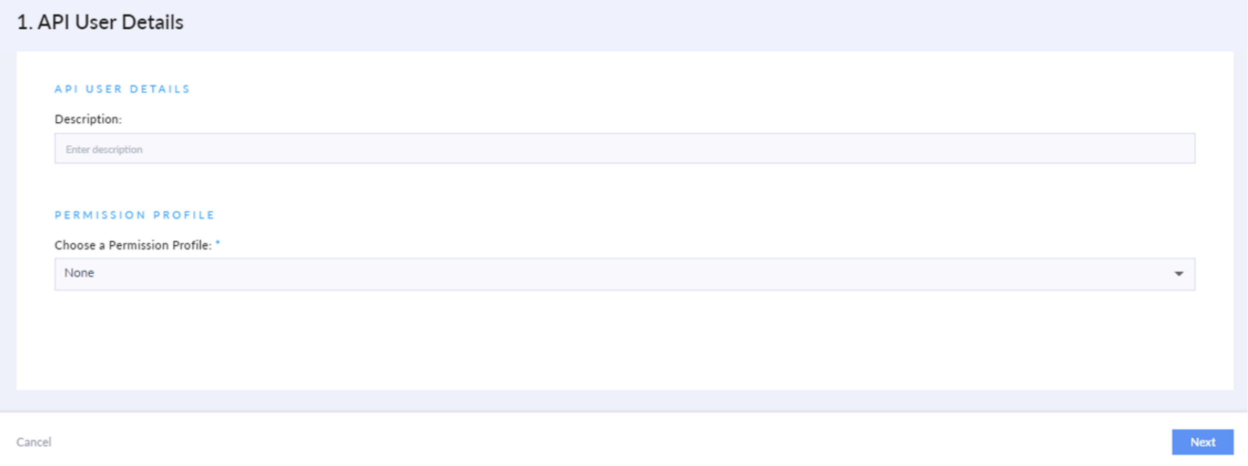
- Adding an API user on page 36
- Managing API users on page 37
- Accessing FortiAPIs on page 38

Adding an API user

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

To create an API user:

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



1. API User Details

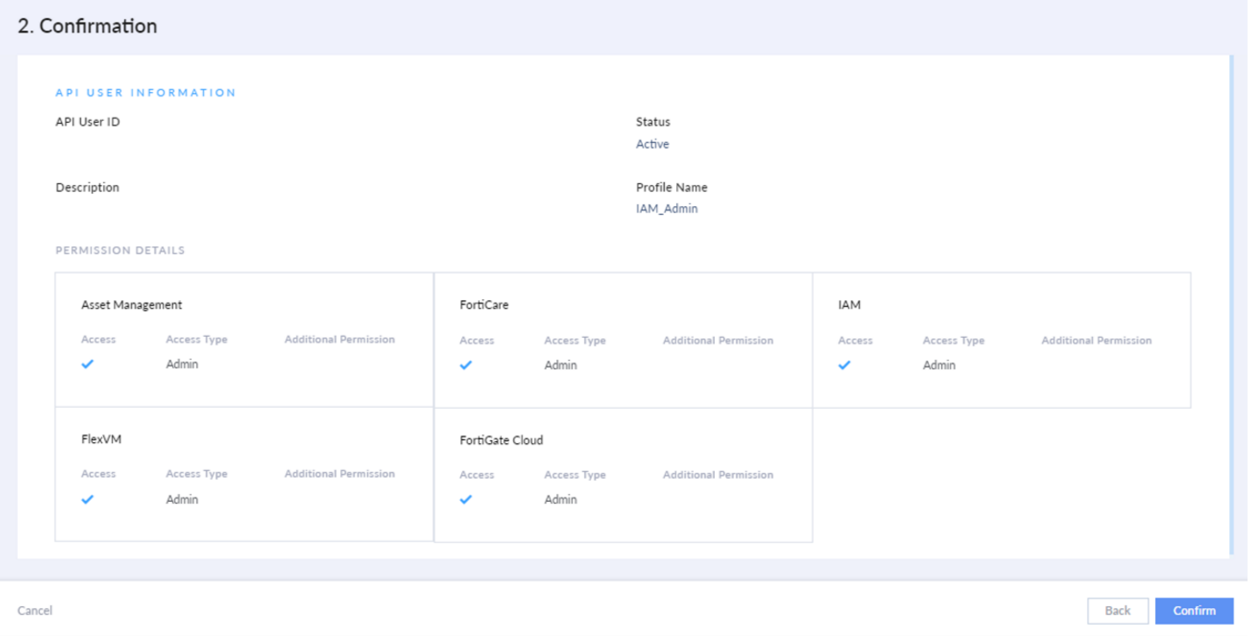
API USER DETAILS

Description: Enter description

PERMISSION PROFILE

Choose a Permission Profile: * None

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 *Next*.
6. Review the user's information, and click *Confirm*.



2. Confirmation

API USER INFORMATION

API User ID

Status: Active

Description

Profile Name: IAM_Admin

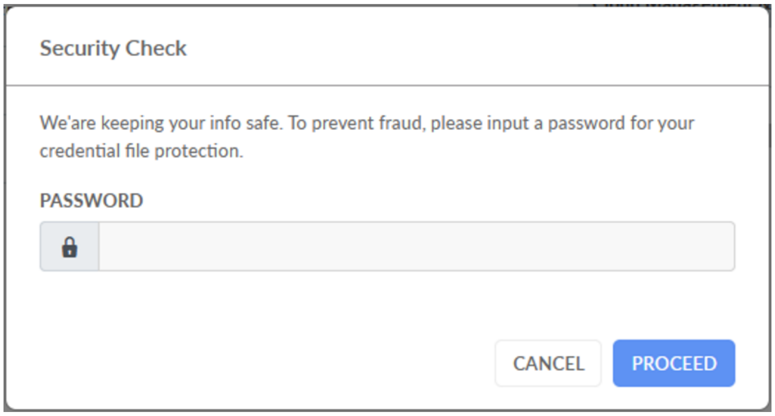
PERMISSION DETAILS

	Access	Access Type	Additional Permission
Asset Management	✓	Admin	
FortiCare	✓	Admin	
IAM	✓	Admin	
FlexVM	✓	Admin	
FortiGate Cloud	✓	Admin	

7. 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.

8. 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

9. Request an authorization token. SeeAccessing FortiAPIs on page 38

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 45.

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 (*Active*/*Disabled*)

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*.

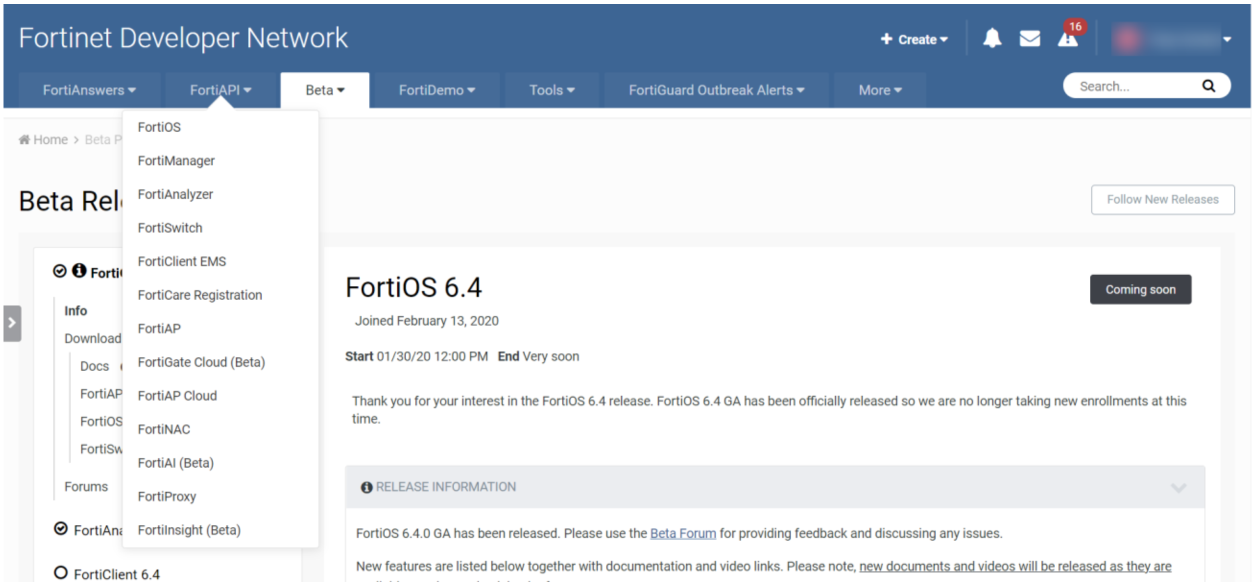
To update an API user's portal permissions:

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.



FortiOS 6.4

Joined February 13, 2020

Start 01/30/20 12:00 PM **End** Very soon

Thank you for your interest in the FortiOS 6.4 release. FortiOS 6.4 GA has been officially released so we are no longer taking new enrollments at this time.

FortiOS 6.4.0 GA has been released. Please use the Beta Forum for providing feedback and discussing any issues.

New features are listed below together with documentation and video links. Please note, new documents and videos will be released as they are

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 jVSjRMx5hpw5ZfASk8Hjo16X
```

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 36.
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": "xpD0HVYUdshsiWlMBR0Q6uUoV2TDSa",
   "scope": "read write",
   "status": "success",
   "token_type": "Bearer"
}
```

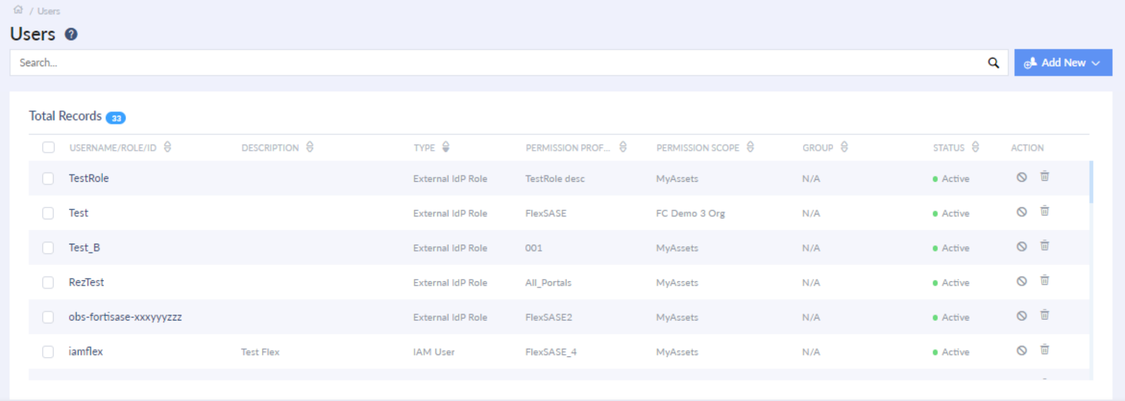
External IdP roles

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.

IdP roles are a limited beta feature.

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 9.



□	USERNAME/ROLE/ID	DESCRIPTION	TYPE	PERMISSION PROF...	PERMISSION SCOPE	GROUP	STATUS	ACTION
□	TestRole		External IdP Role	TestRole desc	MyAssets	N/A	● Active	⊘ 🗑
□	Test		External IdP Role	FlexSASE	FC Demo 3 Org	N/A	● Active	⊘ 🗑
□	Test_B		External IdP Role	001	MyAssets	N/A	● Active	⊘ 🗑
□	RezTest		External IdP Role	All_Portals	MyAssets	N/A	● Active	⊘ 🗑
□	obs-fortisase-xxxyyyzzz		External IdP Role	FlexSASE2	MyAssets	N/A	● Active	⊘ 🗑
□	iamflex	Test Flex	IAM User	FlexSASE_4	MyAssets	N/A	● Active	⊘ 🗑

This section contains the following topics:

- Adding external IdP roles on page 40
- Selecting IdP roles on page 42
- Setting a co-exist end date on page 44

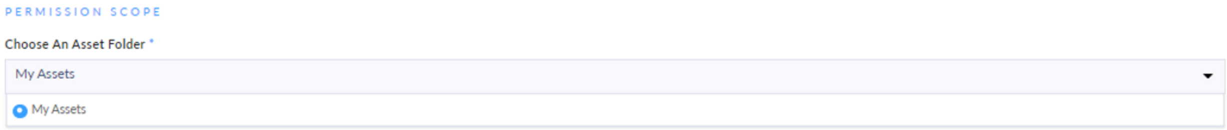
Adding external IdP roles

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.

IdP roles are a limited beta feature.

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 User*. The *External IdP Role* page opens.
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. From the *Permission Scope* dropdown, select an asset folder.



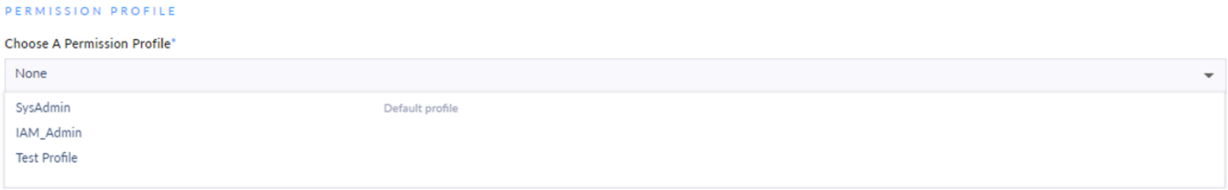
PERMISSION SCOPE

Choose An Asset Folder *

My Assets

● My Assets

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



PERMISSION PROFILE

Choose A Permission Profile*

None

SysAdmin Default profile

IAM_Admin

Test Profile

If the *SysAdmin* profile is selected, a message will display instead of portal cards to denote that the user has full access to all portals.

7. Click *Add Role*.

After the IAM user is created, the IAM user account holder is required to perform a validation check.

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*.

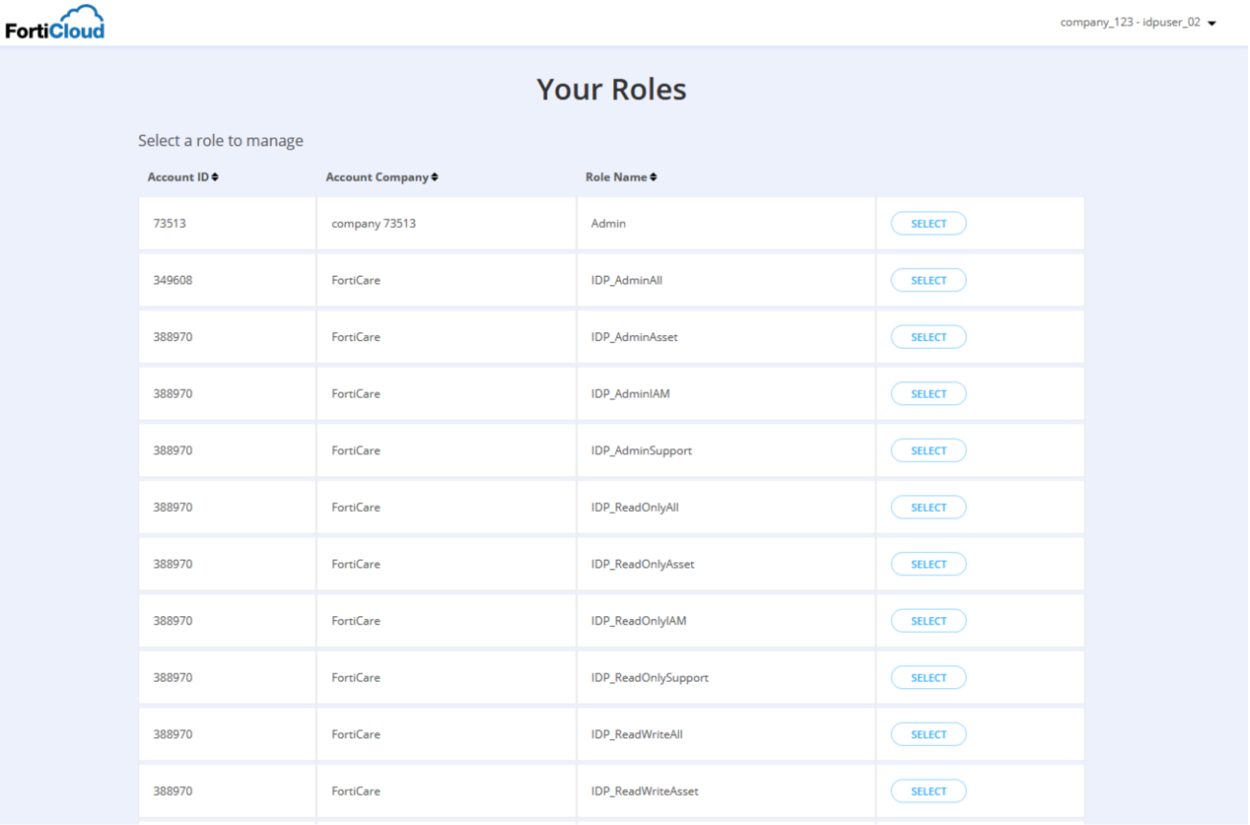
Selecting IdP roles

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 *Your Roles* page opens, and the user must select a role before proceeding to the portal.

The *Your Roles* page appears as a pop-up window in the *Account* menu of the Asset Management portal.



Your Roles

Select a role to manage

Account ID	Account Company	Role Name	
73513	company 73513	Admin	SELECT
349608	FortiCare	IDP_AdminAll	SELECT
388970	FortiCare	IDP_AdminAsset	SELECT
388970	FortiCare	IDP_AdminIAM	SELECT
388970	FortiCare	IDP_AdminSupport	SELECT
388970	FortiCare	IDP_ReadOnlyAll	SELECT
388970	FortiCare	IDP_ReadOnlyAsset	SELECT
388970	FortiCare	IDP_ReadOnlyIAM	SELECT
388970	FortiCare	IDP_ReadOnlySupport	SELECT
388970	FortiCare	IDP_ReadWriteAll	SELECT
388970	FortiCare	IDP_ReadWriteAsset	SELECT

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:

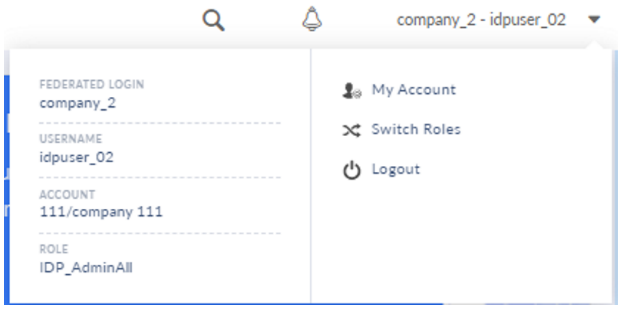
1. Log in using your company's ID provider. The log in portal opens.
2. Select the *Service Provider*.
3. Select *External IDP Role*. The roles available based on your credentials are displayed.
4. Hover over the role you want to choose and click *Select*.
   The *Dashboard* is displayed.

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.



company_2 - idpuser_02

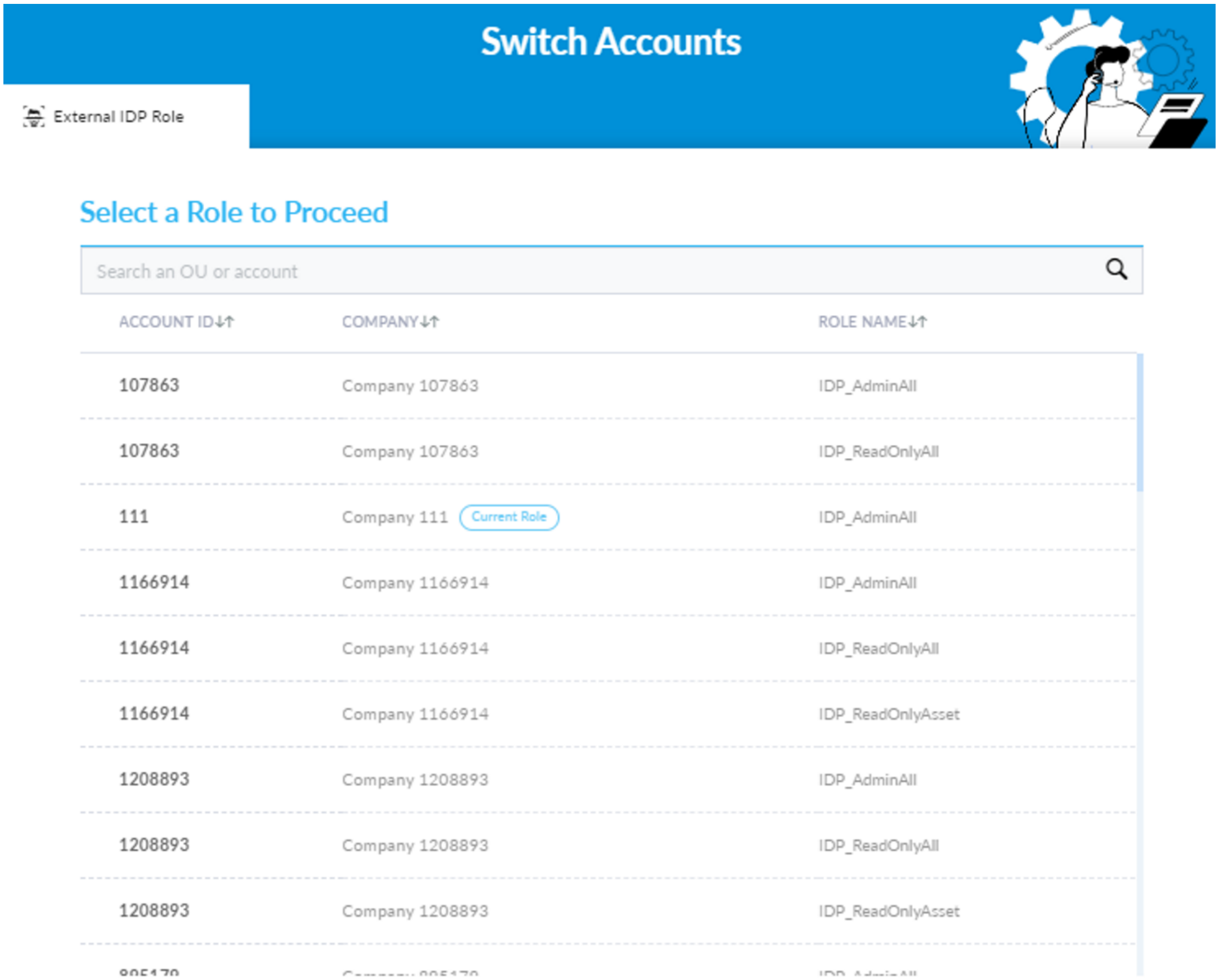
FEDERATED LOGIN
company_2

USERNAME
idpuser_02

ACCOUNT
111/company 111

ROLE
IDP_AdminAll

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



ACCOUNT ID↓↑	COMPANY↓↑	ROLE NAME↓↑
107863	Company 107863	IDP_AdminAll
107863	Company 107863	IDP_ReadOnlyAll
111	Company 111 Current Role	IDP_AdminAll
1166914	Company 1166914	IDP_AdminAll
1166914	Company 1166914	IDP_ReadOnlyAll
1166914	Company 1166914	IDP_ReadOnlyAsset
1208893	Company 1208893	IDP_AdminAll
1208893	Company 1208893	IDP_ReadOnlyAll
1208893	Company 1208893	IDP_ReadOnlyAsset
995179	Company 995179	IDP_AdminAll

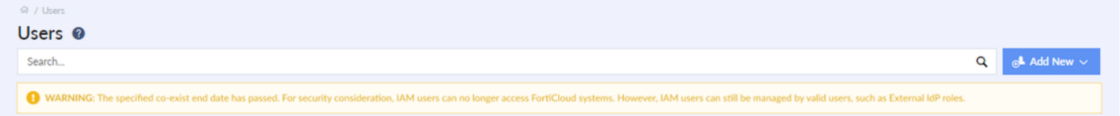
3. Select the *External IDP Role* tab. A list of linked roles is displayed.
4. Hover over the role you want to change to and click *Select*.

   You will be redirected to the *Dashboard* of the selected account.

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.

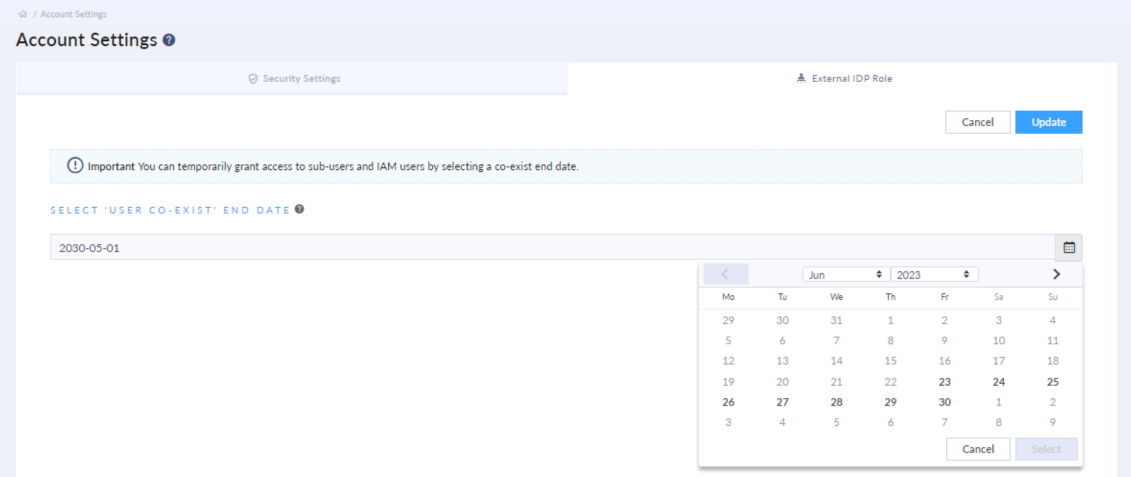
The co-exist date is the deadline until which sub users, IAM users, and external IdP users can access the IAM portal. Once the co-exist end date has passed, sub user and IAM user access are disabled.



WARNING: The specified co-exist end date has passed. For security consideration, IAM users can no longer access FortiCloud systems. However, IAM users can still be managed by valid users, such as External IdP roles.

To set a co-exist end date:

1. Go to *Account Settings* > *External IdP Role*.
2. Click *Edit*.
3. Click the *Select 'user co-exist' end date* calendar icon. A calendar is displayed.



Important You can temporarily grant access to sub-users and IAM users by selecting a co-exist end date.

SELECT 'USER CO-EXIST' END DATE

2030-05-01

Mo	Tu	We	Th	Fr	Sa	Su
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	1	2
3	4	5	6	7	8	9

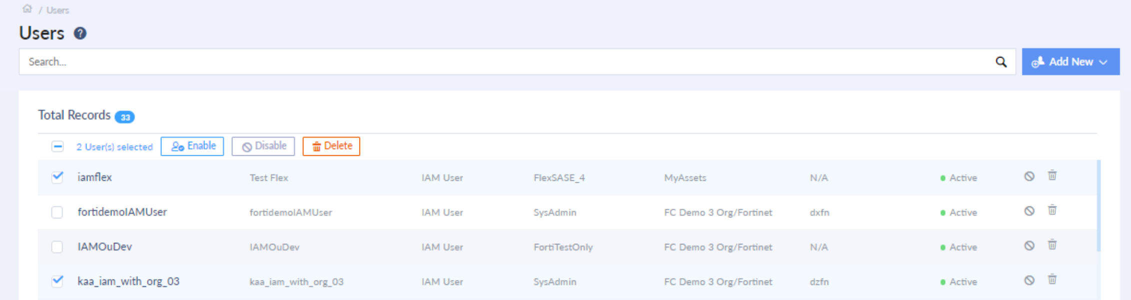
4. Select the date that you want to limit the account to external IdP users only.
5. Click *Select*.
6. Click *Update*. A confirmation message is displayed.

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.

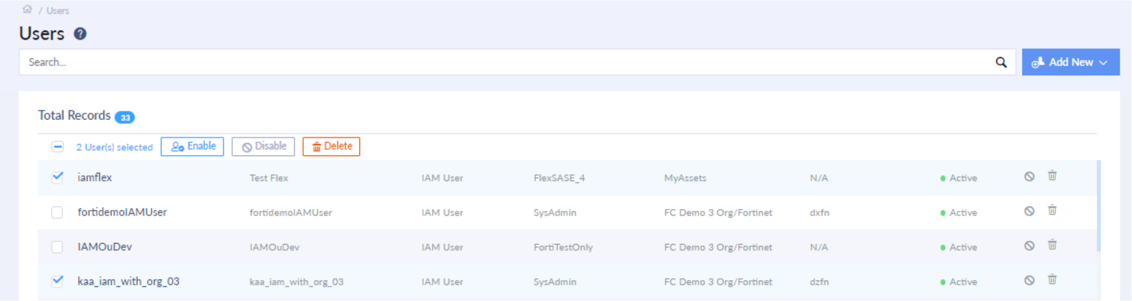


☑	iamflex	Test Flex	IAM User	FlexSASE_4	MyAssets	N/A	● Active
□	fortidemoIAMUser	fortidemoIAMUser	IAM User	SysAdmin	FC Demo 3 Org/Fortinet	dxfn	● Active
□	IAMOuDev	IAMOuDev	IAM User	FortiTestOnly	FC Demo 3 Org/Fortinet	N/A	● Active
☑	kaa_iam_with_org_03	kaa_iam_with_org_03	IAM User	SysAdmin	FC Demo 3 Org/Fortinet	dzfn	● Active

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.

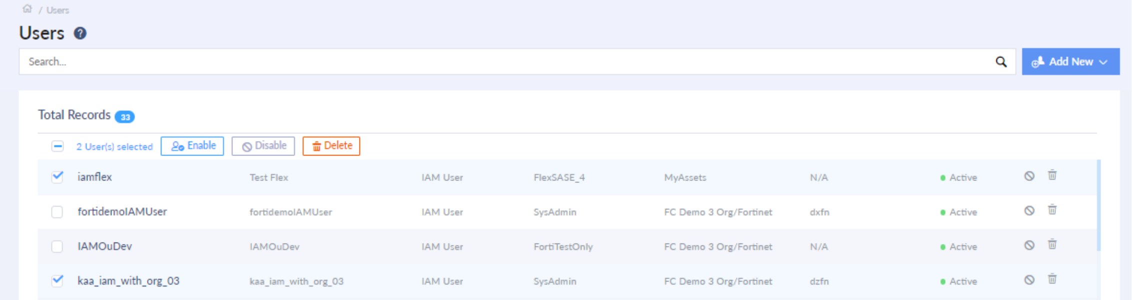


☑	iamflex	Test Flex	IAM User	FlexSASE_4	MyAssets	N/A	● Active
□	fortidemoIAMUser	fortidemoIAMUser	IAM User	SysAdmin	FC Demo 3 Org/Fortinet	dxfn	● Active
□	IAMOuDev	IAMOuDev	IAM User	FortiTestOnly	FC Demo 3 Org/Fortinet	N/A	● Active
☑	kaa_iam_with_org_03	kaa_iam_with_org_03	IAM User	SysAdmin	FC Demo 3 Org/Fortinet	dzfn	● 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.



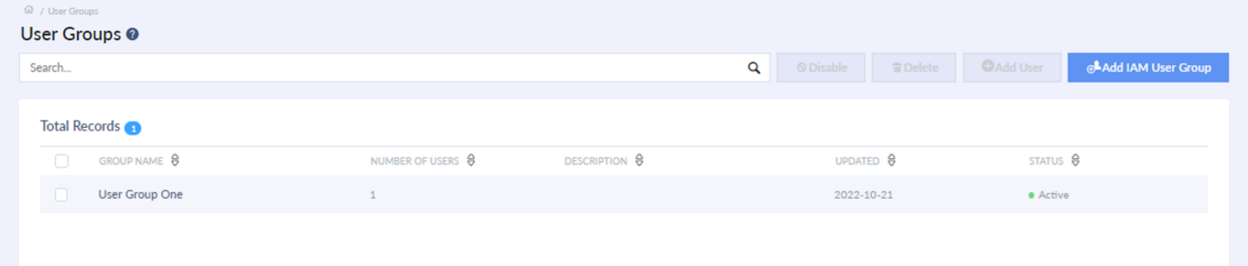
☑	iamflex	Test Flex	IAM User	FlexSASE_4	MyAssets	N/A	● Active
□	fortidemoIAMUser	fortidemoIAMUser	IAM User	SysAdmin	FC Demo 3 Org/Fortinet	dxfn	● Active
□	IAMOuDev	IAMOuDev	IAM User	FortiTestOnly	FC Demo 3 Org/Fortinet	N/A	● Active
☑	kaa_iam_with_org_03	kaa_iam_with_org_03	IAM User	SysAdmin	FC Demo 3 Org/Fortinet	dzfn	● Active

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 9.



Total Records 1

	GROUP NAME	NUMBER OF USERS	DESCRIPTION	UPDATED	STATUS
□	User Group One	1		2022-10-21	● Active

This section contains the following topics:

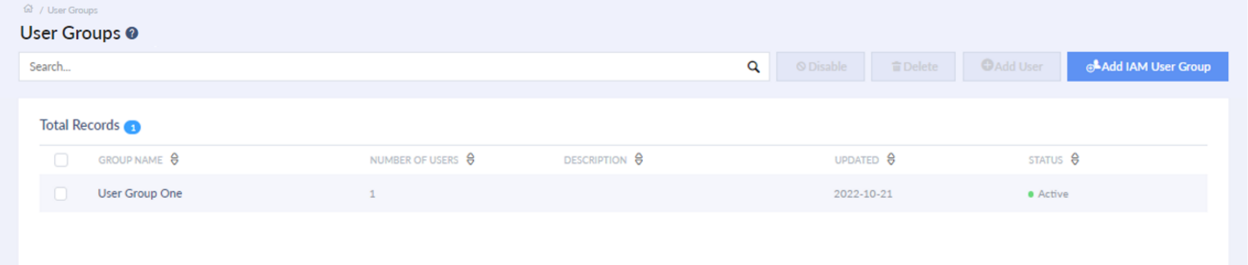
- Adding an IAM user group on page 47
- Managing IAM user groups on page 49

Adding an IAM user group

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

To create a user group:

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

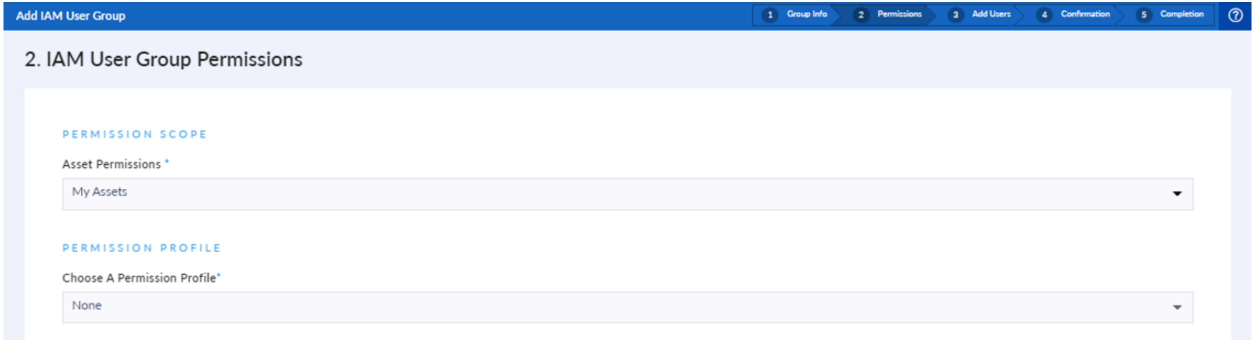


Total Records 1

	GROUP NAME	NUMBER OF USERS	DESCRIPTION	UPDATED	STATUS
□	User Group One	1		2022-10-21	● Active

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.



2. IAM User Group Permissions

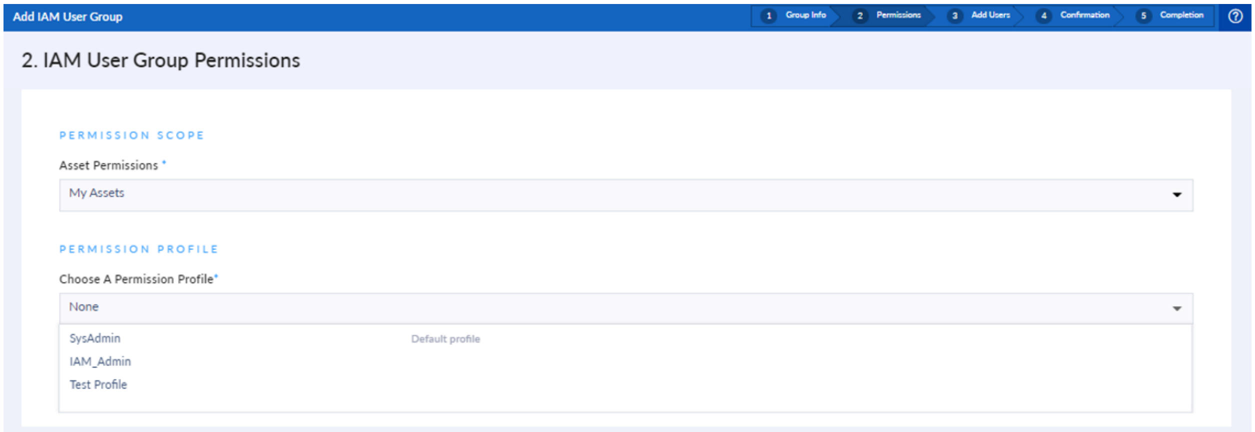
PERMISSION SCOPE

Asset Permissions *: My Assets

PERMISSION PROFILE

Choose A Permission Profile*: None

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



2. IAM User Group Permissions

PERMISSION SCOPE

Asset Permissions *: My Assets

PERMISSION PROFILE

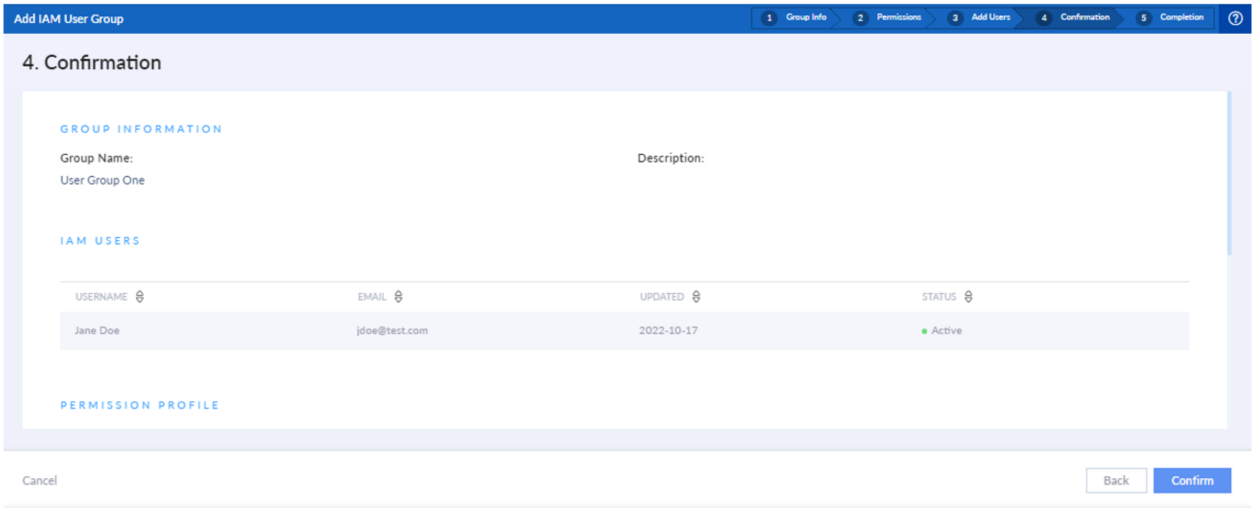
Choose A Permission Profile*: None

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

> If the *SysAdmin* profile is selected, a message will display instead of portal cards to denote that the user has full access to all portals.

9. Click *Next*. The *Add IAM user(s)* page is displayed.
10. 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.

11. Review the group permissions, and click *Confirm*.



4. Confirmation

GROUP INFORMATION

Group Name: User Group One

Description:

IAM USERS

USERNAME	EMAIL	UPDATED	STATUS
Jane Doe	jdoe@test.com	2022-10-17	● Active

PERMISSION PROFILE

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.
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 (*Active*/*Disabled*)

This section contains the following topics:

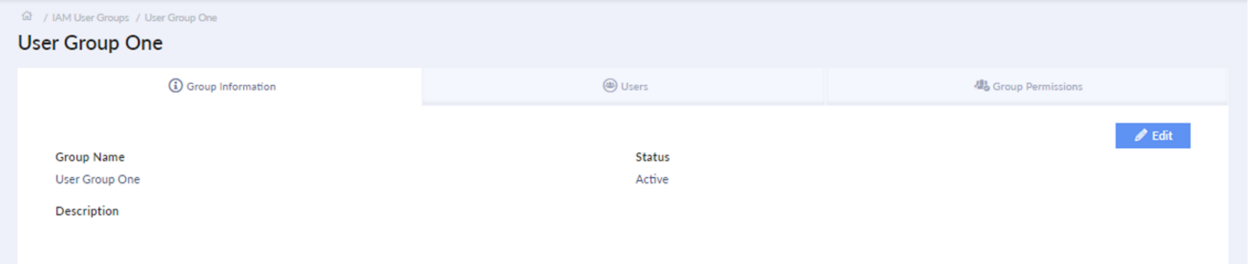
- Editing user groups on page 49
- Adding and removing users on page 51
- Updating user group permission on page 52

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.



Group Name
User Group One

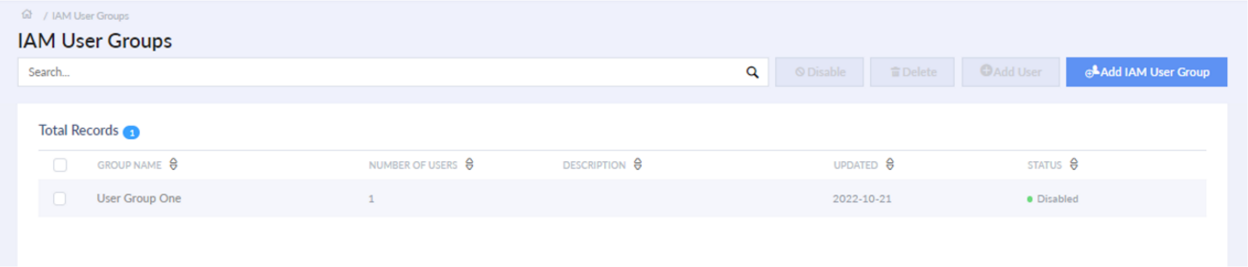
Status
Active

Description

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

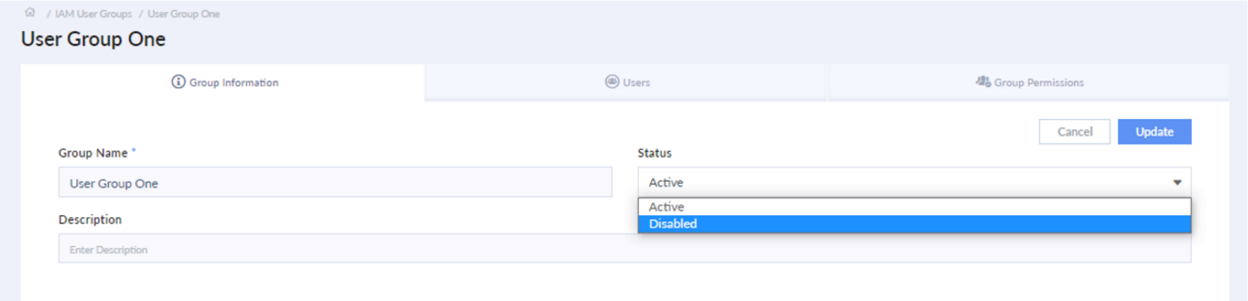


Total Records 1

	GROUP NAME	NUMBER OF USERS	DESCRIPTION	UPDATED	STATUS
□	User Group One	1		2022-10-21	● Disabled

To activate a user group:

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 *Edit*.
4. From the *Status* dropdown, select *Active*.



Group Name *
User Group One

Status
Active
Active
Disabled

Description
Enter Description

5. 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*.

1. Go to *IAM User Groups*.
2. Select the user group(s), and click *Delete*. The *Permission Changed Confirmation* dialog is displayed.
3. 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.

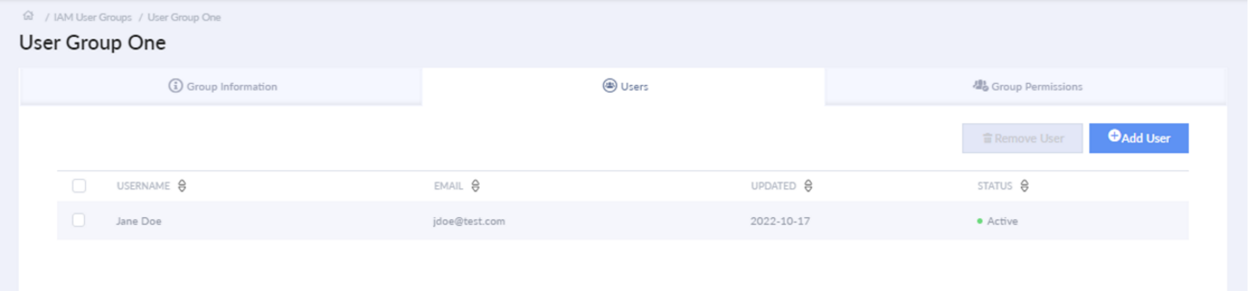
To add users to a group:

1. Select *User Groups* from the left-hand navigation menu. The *User Groups* page opens.
2. Select a user group, and click *Add User*. The *Add User:<group_name>* dialog appears.
3. 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.
4. 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.



□	USERNAME	EMAIL	UPDATED	STATUS
□	Jane Doe	jdoe@test.com	2022-10-17	● Active

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.

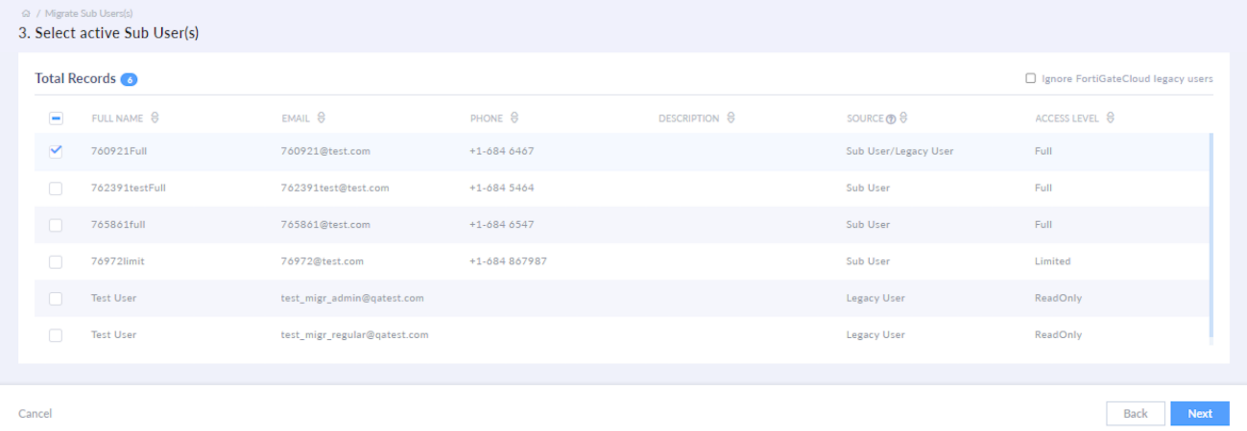
After migration is complete:

- 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 9.

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.



/ Migrate Sub Users(s)

3. Select active Sub User(s)

Total Records 6

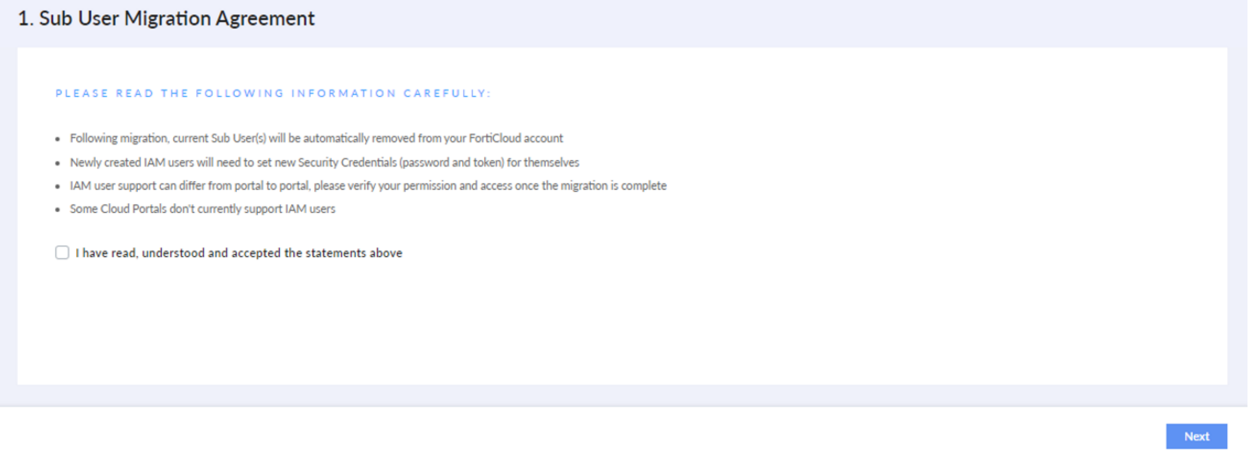
□ Ignore FortiGateCloud legacy users

▬	FULL NAME	EMAIL	PHONE	DESCRIPTION	SOURCE	ACCESS LEVEL
☑	760921Full	760921@test.com	+1-684 6467		Sub User/Legacy User	Full
□	762391testFull	762391test@test.com	+1-684 5464		Sub User	Full
□	765861full	765861@test.com	+1-684 6547		Sub User	Full
□	76972limit	76972@test.com	+1-684 867987		Sub User	Limited
□	Test User	test_migr_admin@qatest.com			Legacy User	ReadOnly
□	Test User	test_migr_regular@qatest.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:

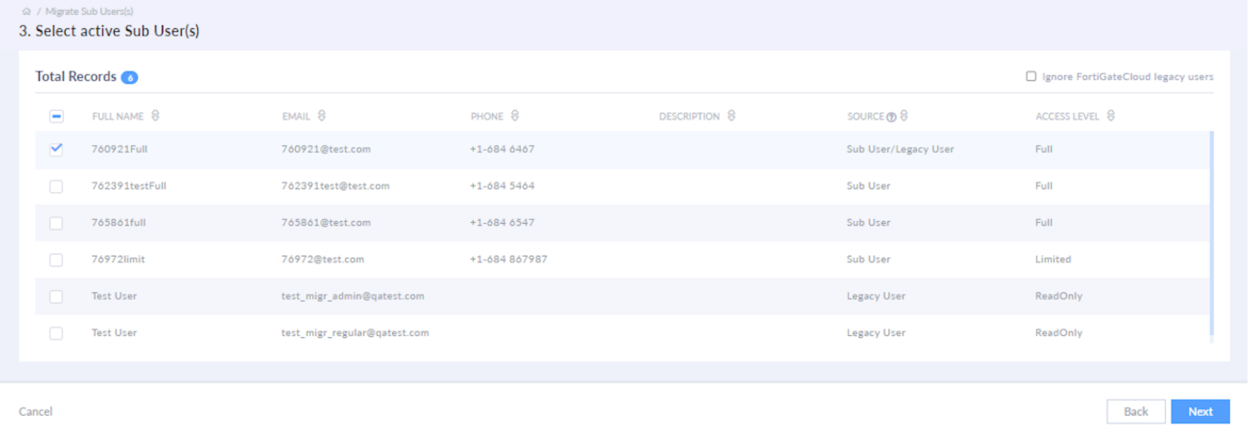
- Following migration, current Sub User(s) will be automatically removed from your FortiCloud account
- Newly created IAM users will need to set new Security Credentials (password and token) for themselves
- IAM user support can differ from portal to portal, please verify your permission and access once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

☐ I have read, understood and accepted the statements above

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 *Email (Account ID)* to the IAM *User ID* field.
Use username as ID and filter with space	Maps the user's FortiCloud *Name* to the IAM *User ID* field.

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



3. Select active Sub User(s)

Total Records 6

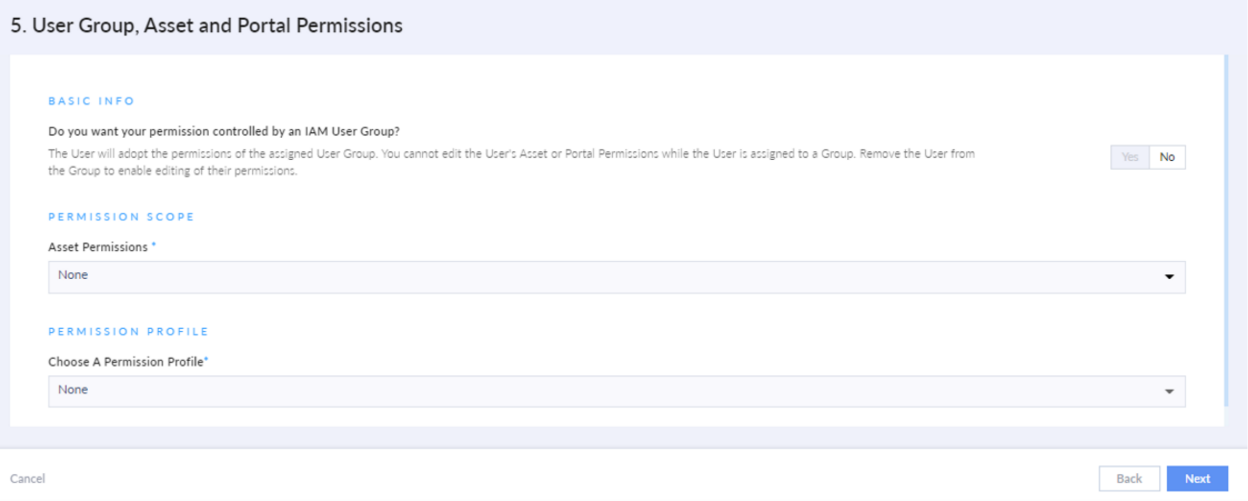
☐ Ignore FortiGateCloud legacy users

☐	FULL NAME	EMAIL	PHONE	DESCRIPTION	SOURCE	ACCESS LEVEL
☑	760921Full	760921@test.com	+1-684 6467		Sub User/Legacy User	Full
☐	762391testFull	762391test@test.com	+1-684 5464		Sub User	Full
☐	765861full	765861@test.com	+1-684 6547		Sub User	Full
☐	76972limit	76972@test.com	+1-684 867987		Sub User	Limited
☐	Test User	test_migr_admin@qatest.com			Legacy User	ReadOnly
☐	Test User	test_migr_regular@qatest.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.

PERMISSION SCOPE

Asset Permissions *

None

PERMISSION PROFILE

Choose 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 47.
    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:

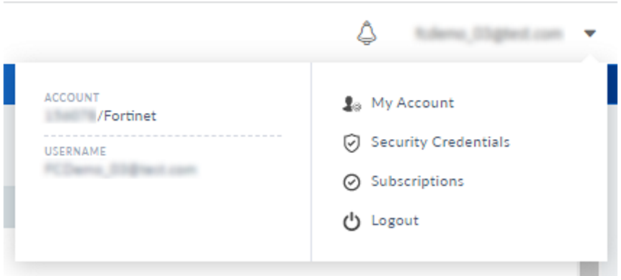
- My Account on page 56
- User Information on page 61
- Security Credentials on page 62
- Subscriptions on page 69

My Account

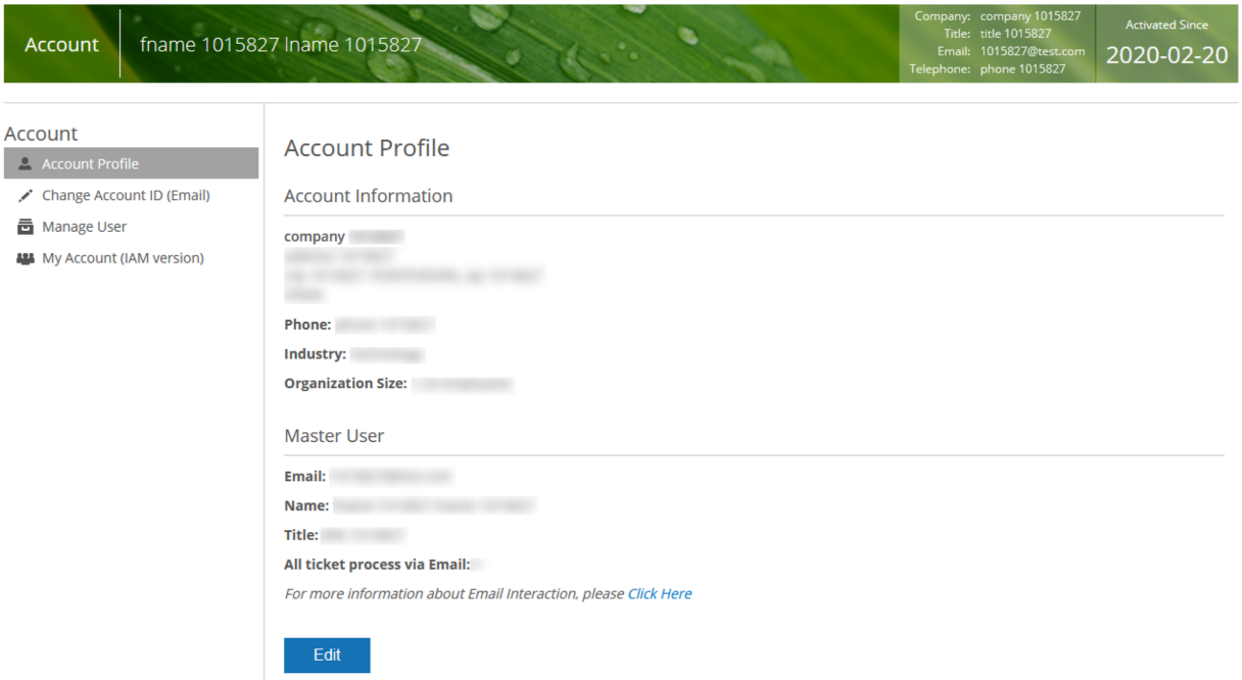
Use the *My Account* portal to update your account information and preferences. You can also use the portal to enable the Organizations feature.

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 [redacted]

Phone: [redacted]

Industry: [redacted]

Organization Size: [redacted]

Master User

Email: [redacted]

Name: [redacted]

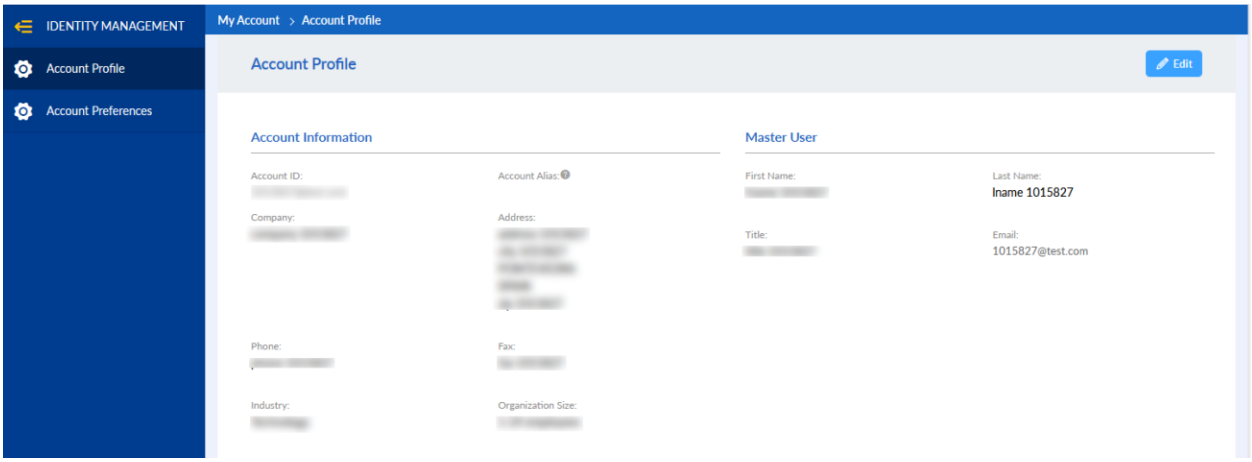
Title: [redacted]

All ticket process via Email: [redacted]

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: [redacted]
Account Alias:
Company: [redacted]
Address: [redacted]
Phone: [redacted]
Fax: [redacted]
Industry: [redacted]
Organization Size: [redacted]

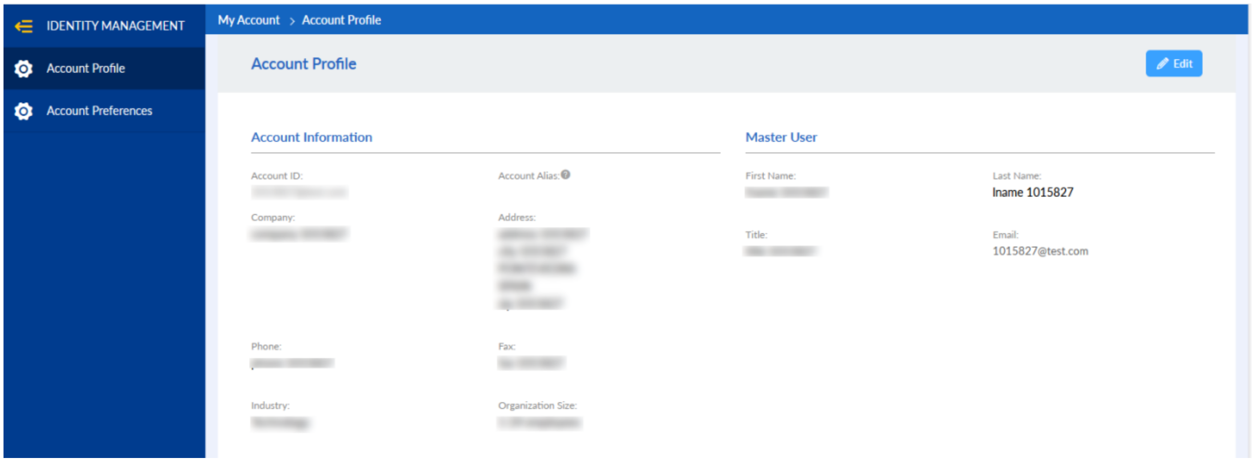
Master User

First Name: [redacted]
Last Name: lname 1015827
Title: [redacted]
Email: 1015827@test.com

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.



Account Profile

Account Information

Account ID: [redacted]

Account Alias:

Company: [redacted]

Address: [redacted]

Phone: [redacted]

Fax: [redacted]

Industry: [redacted]

Organization Size: [redacted]

Master User

First Name: [redacted]

Last Name: lname 1015827

Title: [redacted]

Email: 1015827@test.com

To edit the Account Profile:

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

Account Preferences

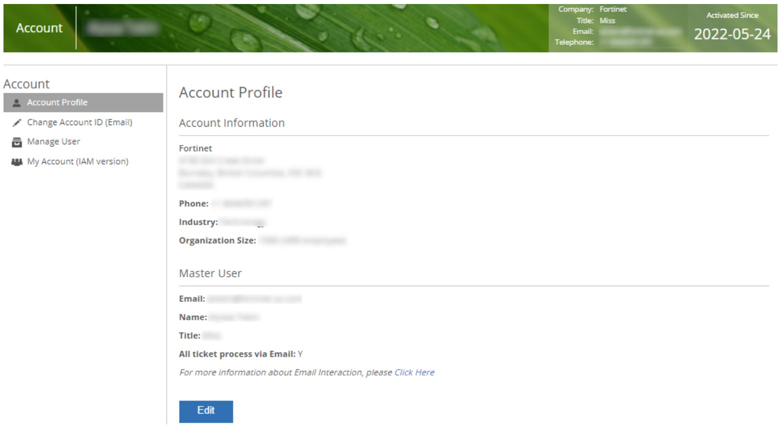
Use the *Account Preferences* page to enable ticket processing by email and link a partner to the account by default.

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. If the customer has a TAM service, they may receive ANB notification based on the PSIRT Advisory.

To add a *PSIRT Contact*:

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



[redacted]

Company: Fortinet
Title: Miss
Email: [redacted]
Telephone: [redacted]

Activated Since 2022-05-24

Account Profile

Account Information

Fortinet
[redacted]

Phone: [redacted]

Industry: [redacted]

Organization Size: [redacted]

Master User

Email: [redacted]

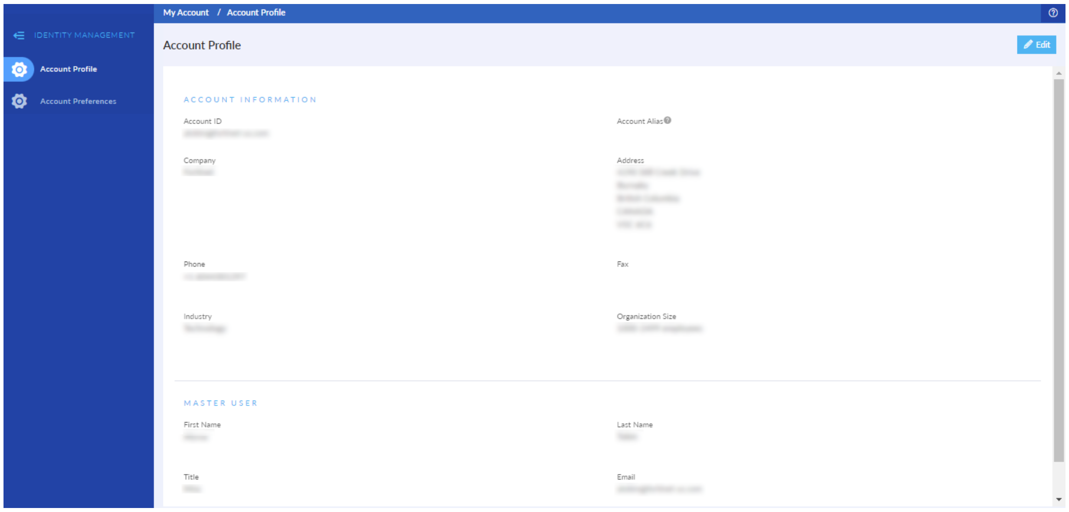
Name: [redacted]

Title: [redacted]

All ticket process via Email: Y

For more information about Email Interaction, please Click Here

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



Account Profile

ACCOUNT INFORMATION

Account ID

Account Alias

Company

Address

Phone

Fax

Industry

Organization Size

MASTER USER

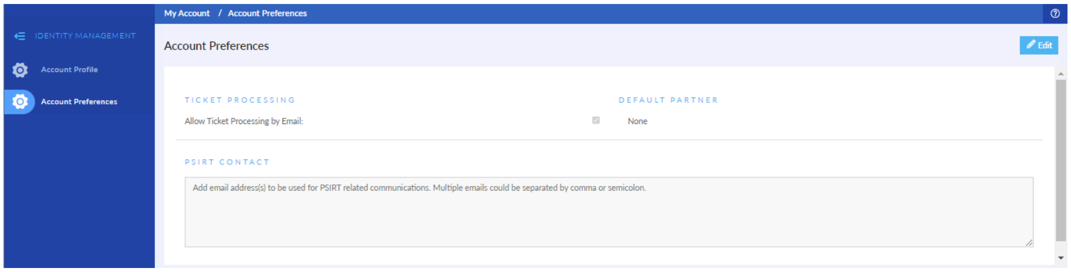
First Name

Last Name

Title

Email

3. Select *Account Preferences*.



Account Preferences

TICKET PROCESSING

Allow Ticket Processing by Email: ☑

DEFAULT PARTNER

None

PSIRT CONTACT

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

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*.

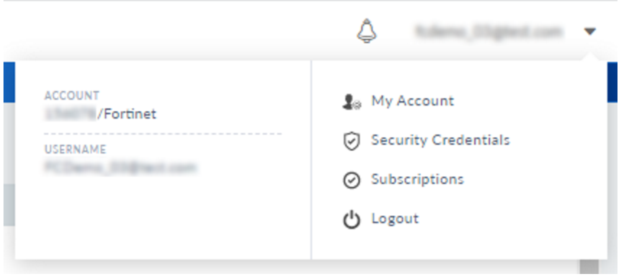
3. From the *Default Partner* dropdown, select a partner account from the list.
4. Click *Update*.

Creating connected accounts (Partners)

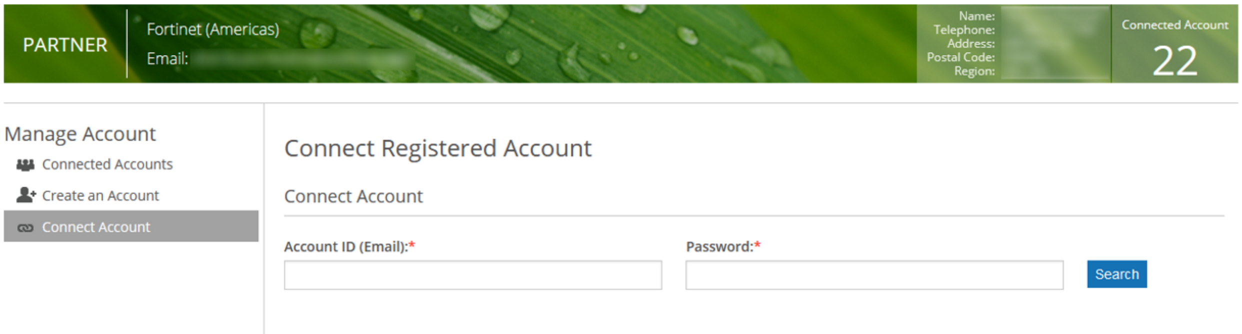
Partners can be connected to one account, or connected to multiple accounts as a master or sub user.

To create a connected account:

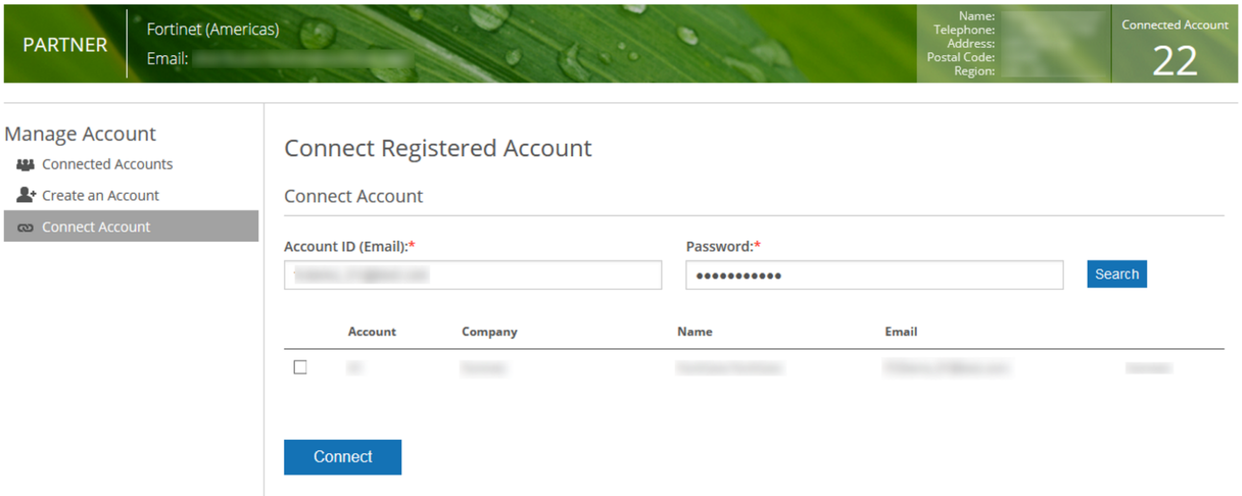
1. Click the Account dropdown (your email) and select *My Account*. You are redirected to FortiCloud.



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



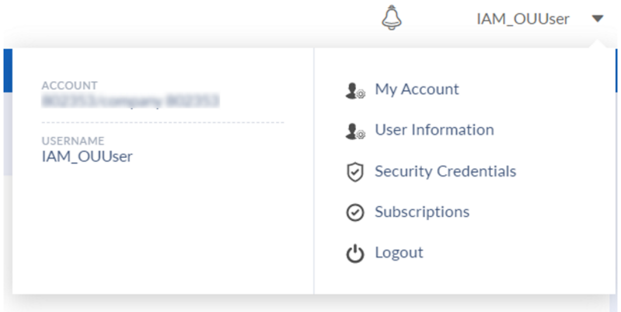
3. Click *Account ID (Email)* and select a user from the list. The *Password* field is updated.
4. Click *Search*. The available accounts are displayed.



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

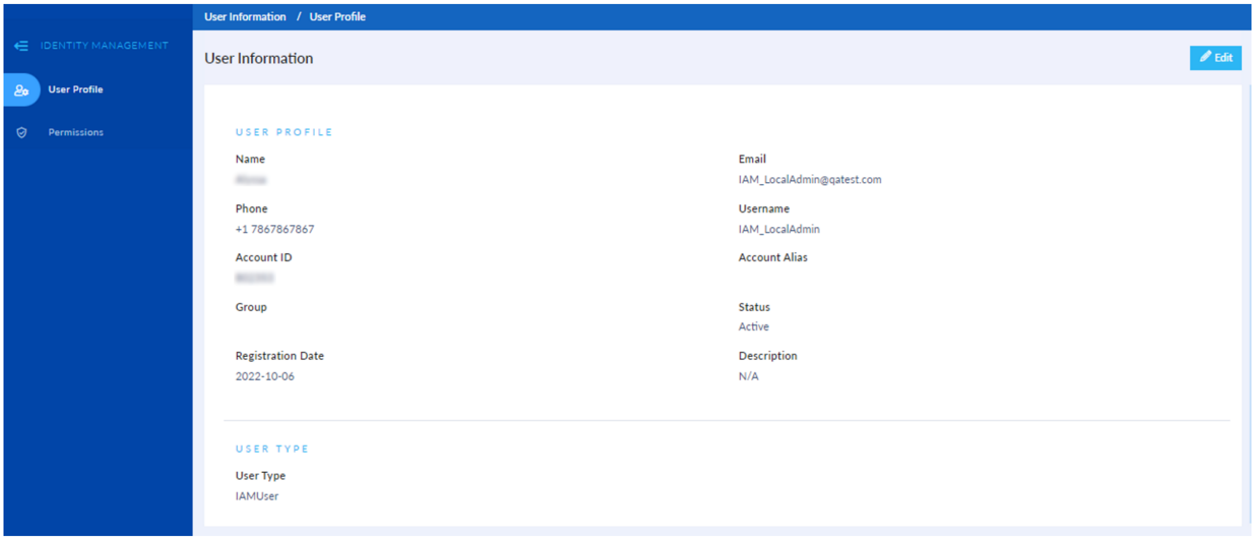
User Information

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



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*.



USER PROFILE

Name
[redacted]

Email
IAM_LocalAdmin@qatest.com

Phone
+1 7867867867

Username
IAM_LocalAdmin

Account ID
[redacted]

Account Alias

Group

Status
Active

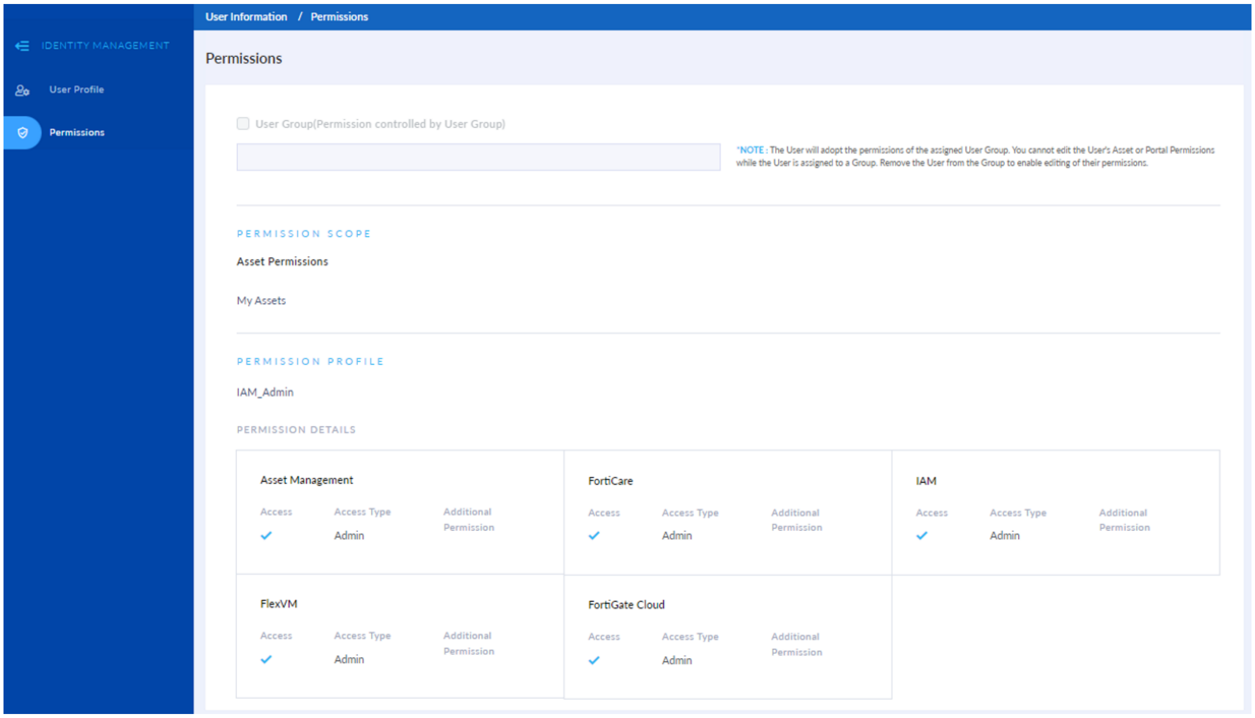
Registration Date
2022-10-06

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.



Permissions

□ User Group(Permission controlled by User Group)

*NOTE : 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.

PERMISSION SCOPE

Asset Permissions

My Assets

PERMISSION PROFILE

IAM_Admin

PERMISSION DETAILS

	Access	Access Type	Additional Permission
Asset Management	✓	Admin	
FortiCare	✓	Admin	
IAM	✓	Admin	
FlexVM	✓	Admin	
FortiGate Cloud	✓	Admin	

Security Credentials

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

This section contains the following topics:

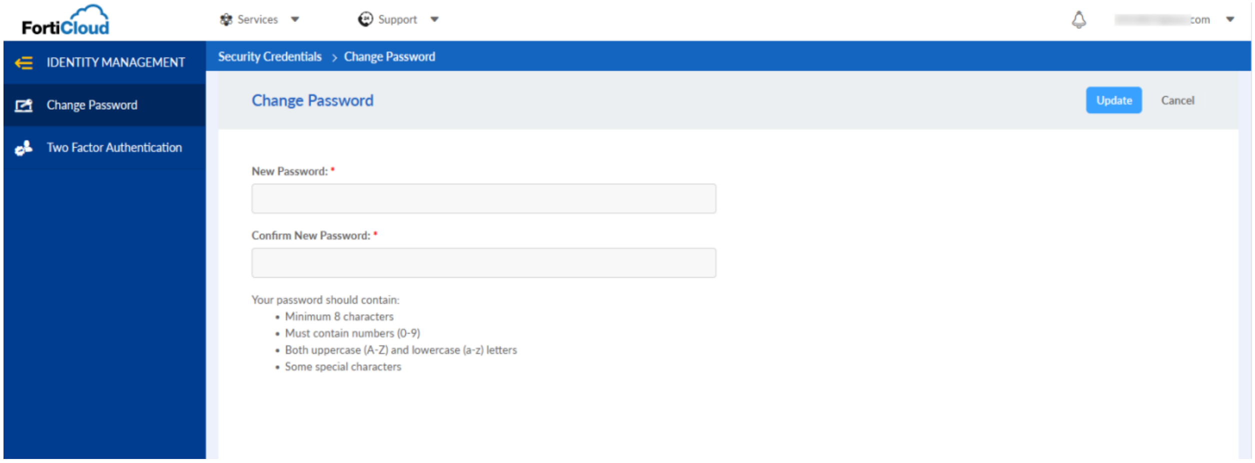
- Change password on page 62
- Two-Factor Authentication (2FA) on page 63

Change password

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*.
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*.



Change Password

New Password: *

Confirm New Password: *

Your password should contain:

- Minimum 8 characters
- Must contain numbers (0-9)
- Both uppercase (A-Z) and lowercase (a-z) letters
- Some special characters

Two-Factor Authentication (2FA)

Two-Factor Authentication requires users to enter a security code to log in to a portal. Users can choose to use FortiToken or have the security token emailed to them each time they log in.

FortiToken 2FA is enforced for all email account users if it has been selected at the Organization or Account level that the email account belongs to. If email 2FA has been enabled for an email account, it can continue to be used, although the email address cannot be changed and it is recommended that the user switch to FortiToken 2FA.

For information on transferring tokens from one mobile device to another for 2FA, see the FortiToken Frequently Asked Questions guide.

This section contains the following topics:

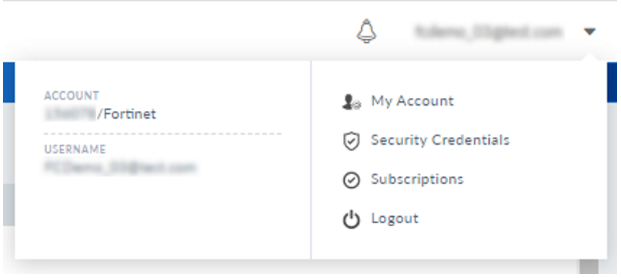
- Enabling Two-Factor Authentication on page 63
- Logging in with 2FA for the first time on page 65
- Switching 2FA authentication methods on page 67
- Resetting FortiToken for 2FA on page 68

Enabling Two-Factor Authentication

You can enable Two-Factor Authentication (2FA) at the user level or the account level. See Settings in the Organization Portal guide for information on enforcing 2FA at the Organization level.

To enable 2FA 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.
3. Click *Edit*.
4. Select *Enable Two Factor Authentication*.
5. Select the 2FA option, *FortiToken* or *Email*. See Logging in with 2FA for the first time on page 65.

> FortiToken is the recommended 2FA method to give your account the best security. FortiToken 2FA will be enforced for new email accounts. Email accounts that already have email-based 2FA enabled cannot change the email address used and are encouraged to switch to FortiToken. See Switching 2FA authentication methods on page 67.

6. Click *Update*.

To enable 2FA at the account level and exempt users:

1. Go to *Account Settings > Security Settings*.
2. Click *Edit*.
3. Set *Enforce 2FA* to *Yes*.
4. (Optional) Exempt users from 2FA.

> By adding a users to the exemption list, you are allowing the user to bypass the Two-Factor Authentication process.

   a. Set *Enable 2FA User Exemption* to *Yes*.
   b. In the *2FA User Exemption List*, click the plus (+) sign. The *Add User/s to 2FA User Exemption List* dialog opens.
   c. From the *Select User Type* dropdown, select *IAM User* or *Email User*.

   > An Email User is a legacy sub user in FortiCloud. For information, see User permissions in the Asset Management Administration Guide.

   d. Select a users from the list and click *Add*.
   e. Click *Confirm*.
5. Click *Update*.

A user can still disable 2FA at the user at the user level. However, they cannot log in to the portal until they enable it again.

To enable 2FA for a user:

1. Go to *IAM users* and select a user from the list.
2. Click the *Security Credentials* tab.
3. Click *Two Factor Authentication*.

For information, see Managing IAM users on page 27 and Managing IAM user groups on page 49.

Logging in with 2FA for the first time

Users are required to validate and set up 2FA for the IAM user the first time they log in to https://support.fortinet.com.

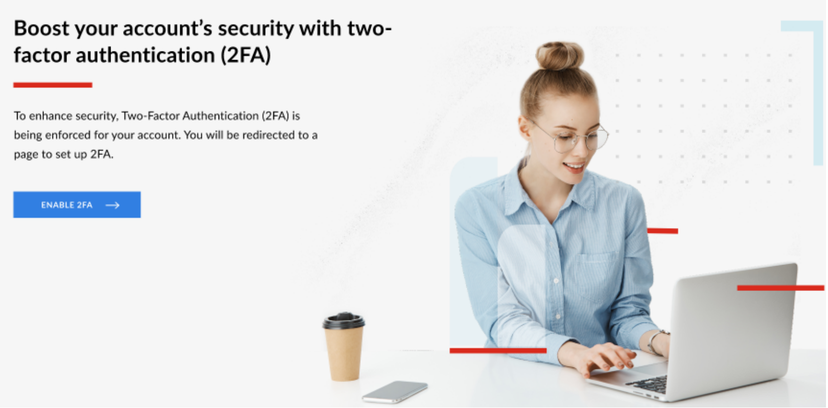
Email users

Master and legacy sub users logging in with an email account will be forced to enable 2FA using FortiToken if it is being enforced at the account or OU level. See Enabling Two-Factor Authentication on page 63 for information on enforcing 2FA at the account level. See Settings in the Organization Portal guide for information on enforcing 2FA at the Organization level.

If it is not being enforced, you can choose to enable 2FA for your email account. See Enabling Two-Factor Authentication on page 63.

To set up 2FA for FortiToken if it is being enforced at the Organization or Account level:

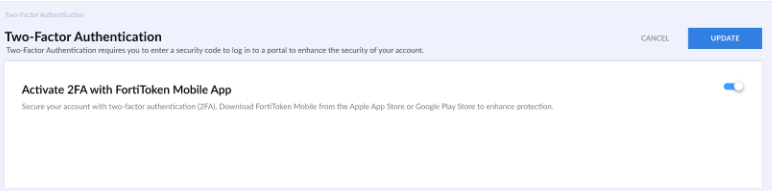
1. Log in using your email account credentials. You will be redirected to the *Two-Factor Authentication* page.



Boost your account's security with two-factor authentication (2FA)

To enhance security, Two-Factor Authentication (2FA) is being enforced for your account. You will be redirected to a page to set up 2FA.

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



Two-Factor Authentication

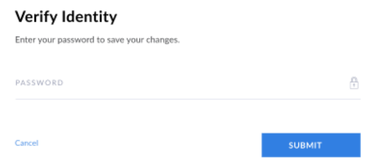
Two-Factor Authentication

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

Activate 2FA with FortiToken Mobile App

Secure your account with two-factor authentication (2FA). Download FortiToken Mobile from the Apple App Store or Google Play Store to enhance protection.

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



Verify Identity

Enter your password to save your changes.

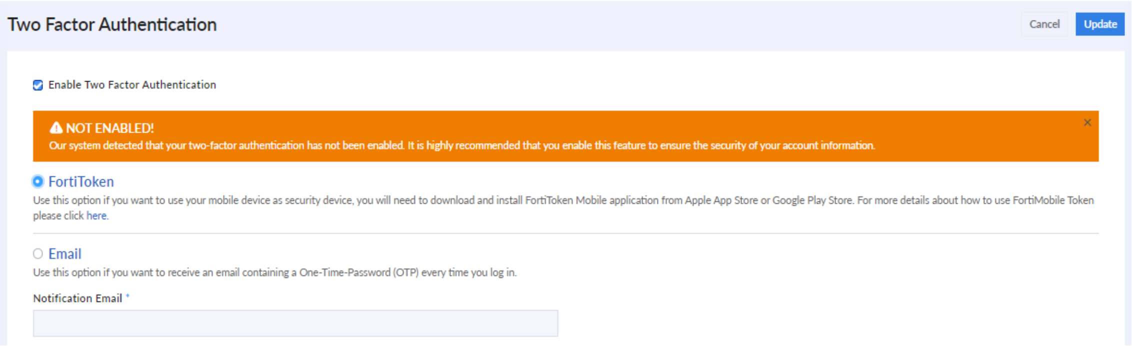
4. Enter your account password and click *Submit*.
5. (Optional) Click *Test Token Now* to verify 2FA has been enabled.
    a. Enter the security code and click *Submit*. A dialog opens if the test is successful.
6. Log in using your email credentials again and use FortiToken to verify your account.

IAM users

Users logging in with an IAM account can set up 2FA for email or FortiToken.

To set up 2FA for FortiToken:

1. On the *Security Credentials* > *Two Factor Authentication* page, select *Edit*.
2. Enable *Enable Two-Factor Authentication* and click *FortiToken*.



Two Factor Authentication

☑ Enable Two Factor Authentication

NOT ENABLED!
Our system detected that your two-factor authentication has not been enabled. It is highly recommended that you enable this feature to ensure the security of your account information.

● FortiToken

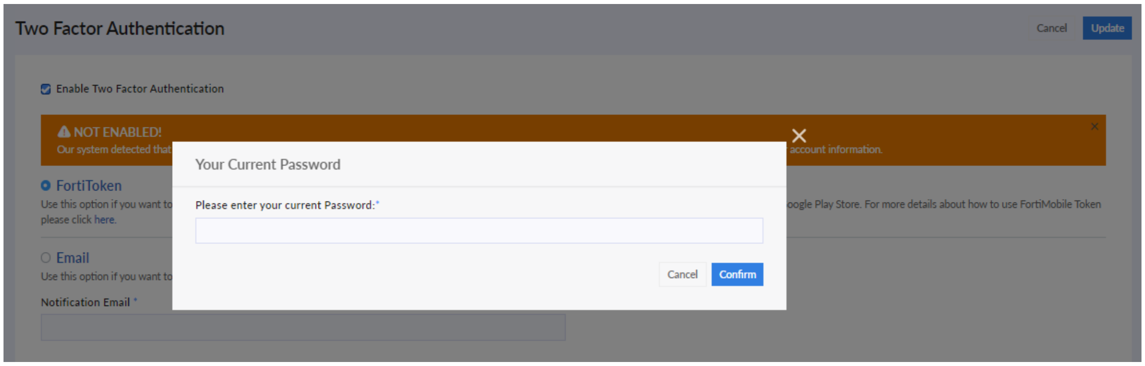
Use this option if you want to use your mobile device as security device, you will need to download and install FortiToken Mobile application from Apple App Store or Google Play Store. For more details about how to use FortiMobile Token please click here.

○ Email

Use this option if you want to receive an email containing a One-Time-Password (OTP) every time you log in.

Notification Email *

3. Click *Update*. The *Your Current Password* dialog opens.



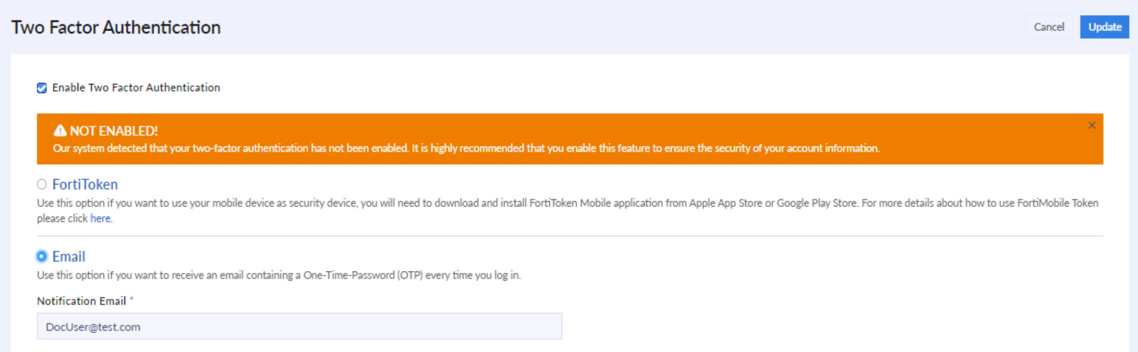
Your Current Password

Please enter your current Password:*

4. Enter your IAM user password and click *Submit*.
5. (Optional) Click *Test Token Now* to verify 2FA has been enabled.
6. Enter the security code and click *Submit*. A dialog opens if the test is successful.
7. Log in using your IAM user credentials again and use FortiToken to verify your account.

To set up 2FA for email:

1. On the *Security Credentials* > *Two Factor Authentication* page, select *Edit*.
2. Enable *Enable Two-Factor Authentication* and click *Email*.
   Your IAM user account email will appear in the Notification Email field. This email address cannot be changed.



Two Factor Authentication

☑ Enable Two Factor Authentication

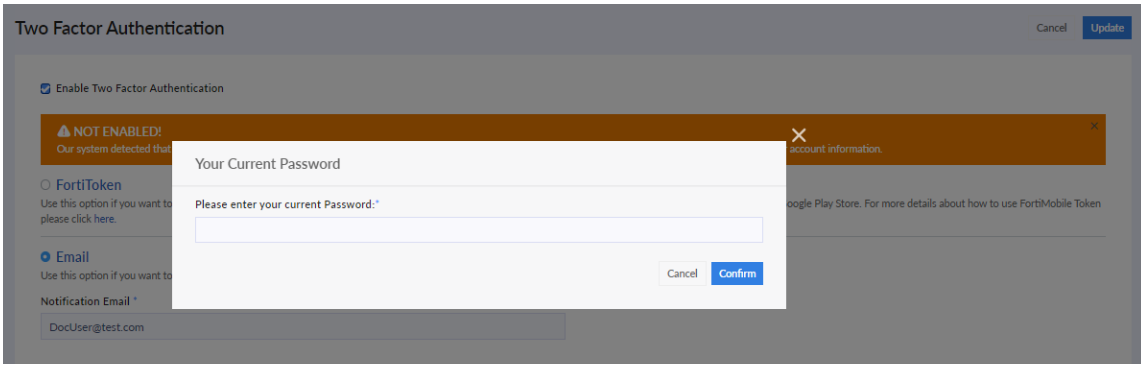
NOT ENABLED!
Our system detected that your two-factor authentication has not been enabled. It is highly recommended that you enable this feature to ensure the security of your account information.

○ 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 option if you want to receive an email containing a One-Time-Password (OTP) every time you log in.

Notification Email *
DocUser@test.com

3. Click *Update*. The *Password Required* dialog opens.



Your Current Password

Please enter your current Password:*

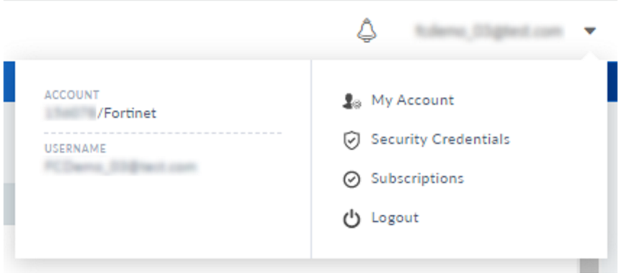
4. Enter your password and click *Confirm*. If the authentication is successful a confirmation page appears.
5. Log in to the portal again.
   The next time you log in to the portal you be prompted to enter a verification code.

Switching 2FA authentication methods

You can switch authentication methods from your account settings. Users logging in using email account credentials cannot switch to the email 2FA method and are encouraged to switch to the FortiToken method for better security.

To switch 2FA authentication methods:

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

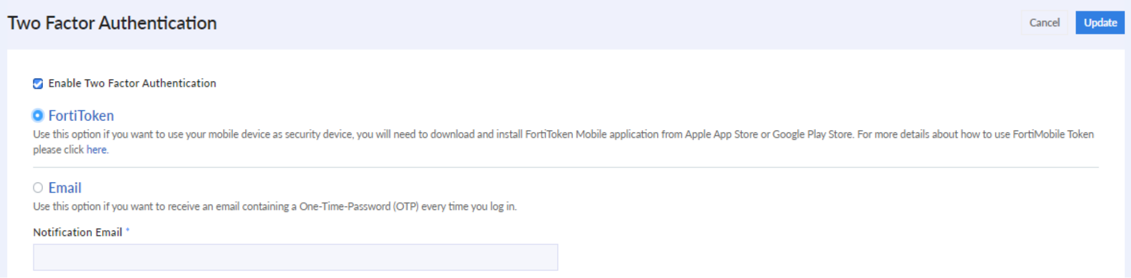


[redacted]

ACCOUNT
[redacted]/Fortinet

USERNAME
[redacted]

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



Two Factor Authentication

☑ Enable Two Factor Authentication

● 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 option if you want to receive an email containing a One-Time-Password (OTP) every time you log in.

Notification Email *

4. Select the authentication method and click *Update*.

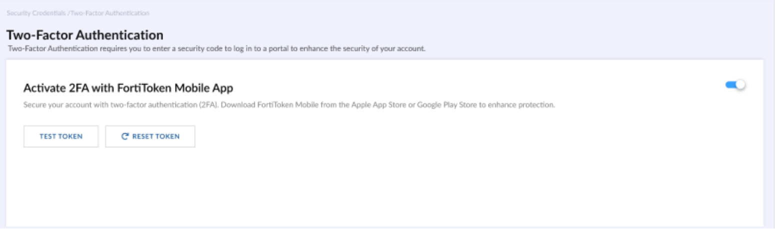
Resetting FortiToken for 2FA

You can reset FortiToken for 2FA 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 2FA.

To reset for FortiToken for a lost device, contact Customer Service.

To reset FortiToken for 2FA:

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*.

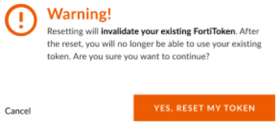


Security Credentials /Two-Factor Authentication

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.

Activate 2FA with FortiToken Mobile App
Secure your account with two-factor authentication (2FA). Download FortiToken Mobile from the Apple App Store or Google Play Store to enhance protection.

3. Click *Reset Token*. A warning dialog opens.



Warning!

Resetting will **invalidate your existing FortiToken**. After the reset, you will no longer be able to use your existing token. Are you sure you want to continue?

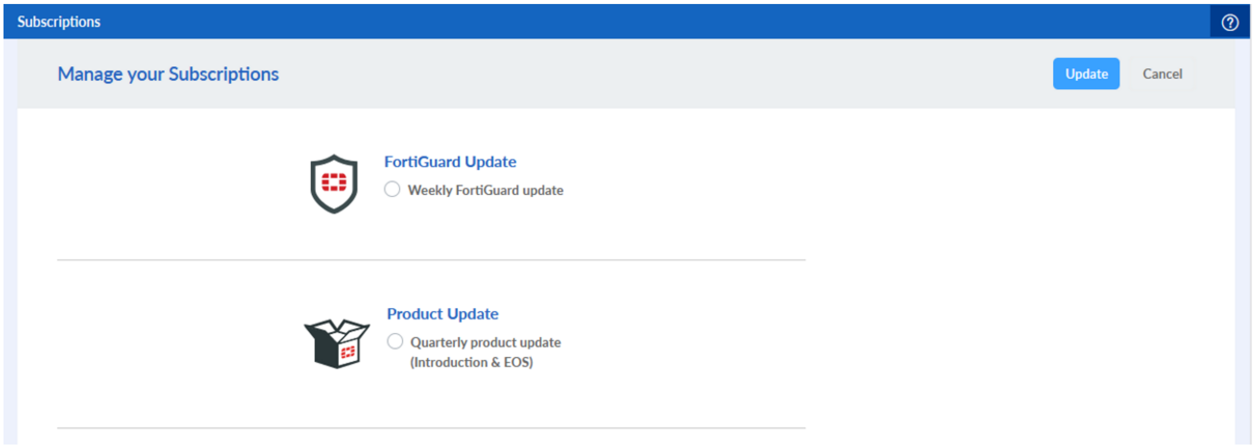
4. Click *Yes, Reset My Token*.
5. Configure the FortiToken app for your new device and log in.

Subscriptions

Subscribe to the receive weekly FortiGuard update and quarterly product update.

To subscribe to FortiGuard and product updates:

1. Click the Account menu at the top-right of the page.
2. Click *Subscriptions*. The *Manage your Subscriptions* page opens.



FortiGuard Update
○ Weekly FortiGuard update

Product Update
○ Quarterly product update (Introduction & EOS)

3. Click *Edit*.
4. Select *FortiGuard Update* or *Product Update*.
5. Click *Update*.

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 70
- Permission scope with Organizations on page 71
- Permission profiles within Organizations on page 73
- Creating users, user groups, and roles within Organizations on page 75
- Logging into an OU account on page 79
- OU context switch on page 81

Enabling Organizations

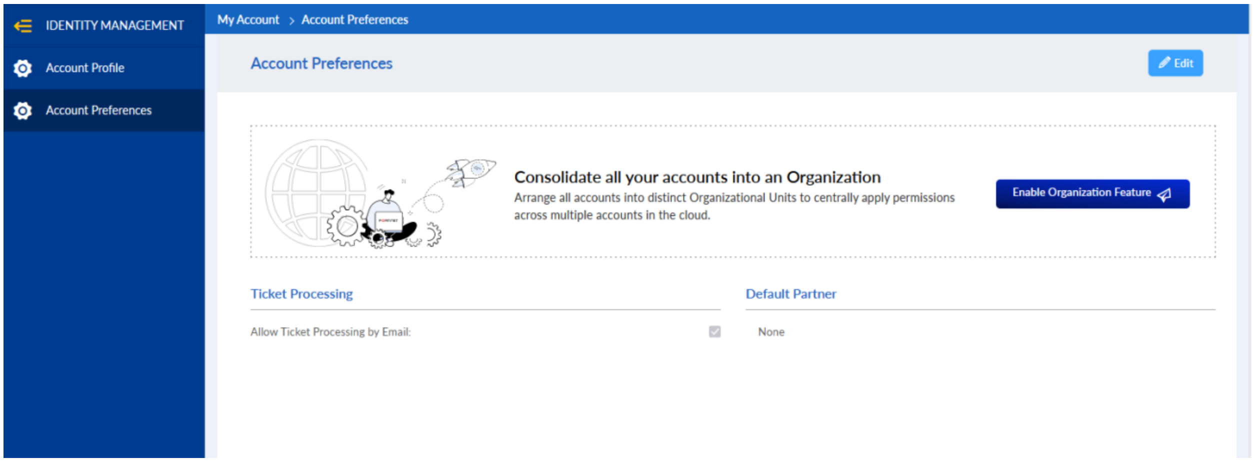
Enable the Organizations feature to arrange all accounts into distinct Organizational Units to centrally apply permissions across multiple accounts in the cloud.

Only the master user can enable the Organizations feature.

To enable Organizations:

1. From the profile menu, select *My Account*.
2. Go to *Account Preferences*.

3. Click *Enable Organization Feature*.



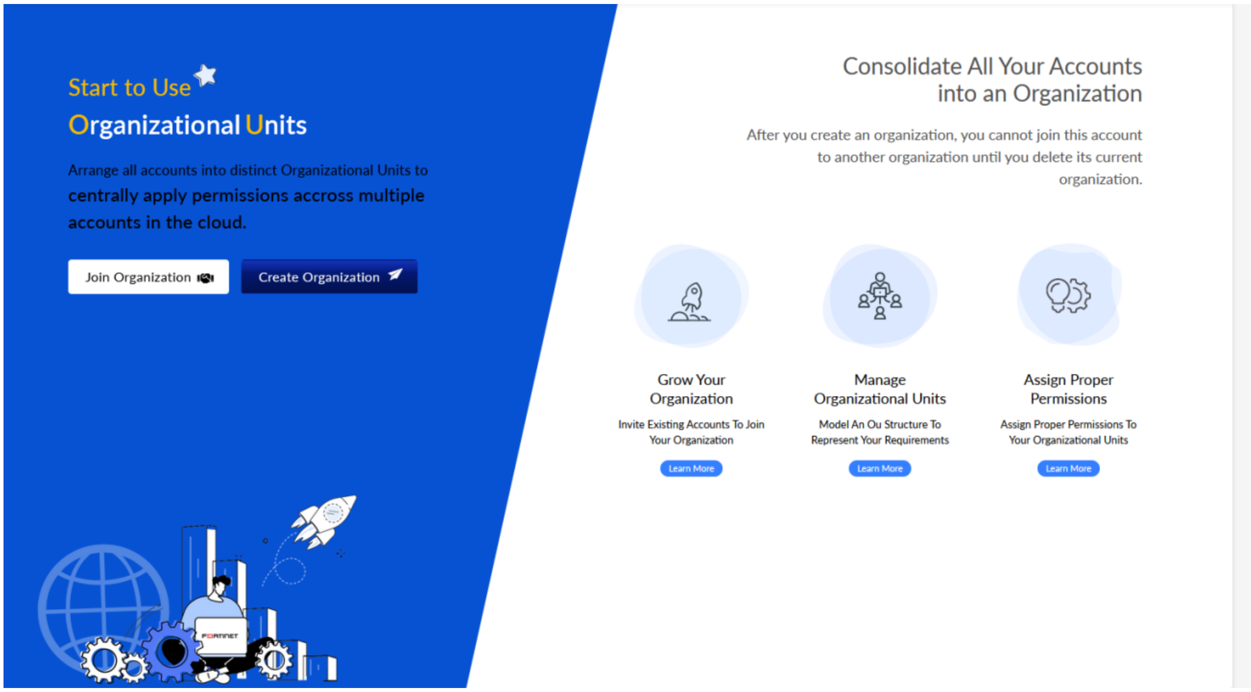
Consolidate all your accounts into an Organization

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

Allow Ticket Processing by Email: ☑

None

4. Create an Organization. For information, see the *Organization Portal Administration Guide*.



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

Consolidate All Your Accounts into an Organization

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

Invite Existing Accounts To Join Your Organization

Model An Ou Structure To Represent Your Requirements

Assign Proper Permissions To Your Organizational Units

Permission scope with Organizations

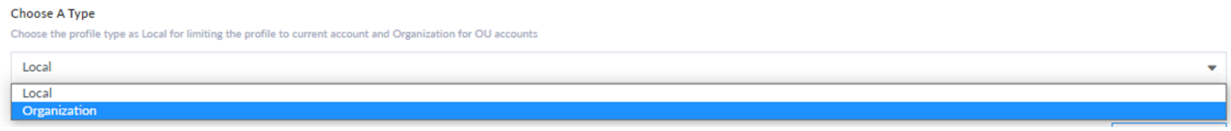
Permission scope is assigned when creating a permission profile or an IAM user, user group, or IdP role. It defines the scope of access a user has in terms of asset folders or OU hierarchy.

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 18.

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 *Choose 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.



Choose A Type

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

Local

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:

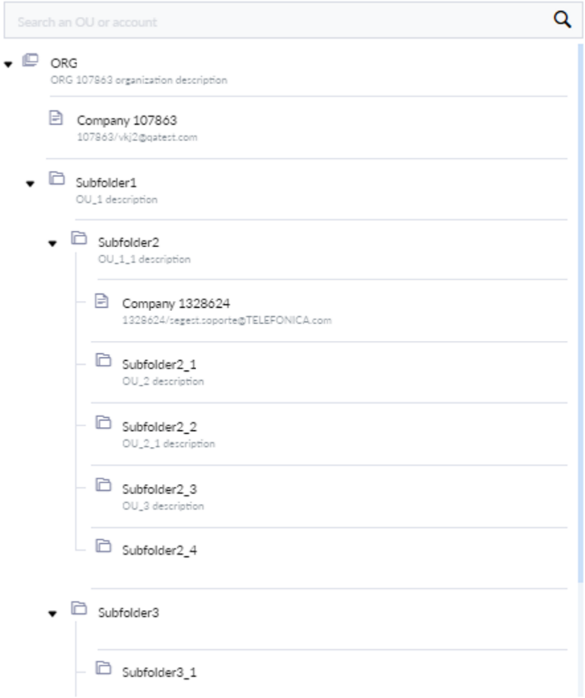
- **Available scope**: The available scope refers to the total accessing scope the login user is assigned with. It covers all organizations, OUs, and member accounts the user can access. The available scope defines what a user is capable of doing and is assigned with the permission scope. This scope 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 81.

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.



Search an OU or account

- ORG
  ORG 107863 organization description
  - Company 107863
    107863/vkj2@qatest.com
  - Subfolder1
    OU_1 description
    - Subfolder2
      OU_1_1 description
      - Company 1328624
        1328624/segest.soporte@TELEFONICA.com
      - Subfolder2_1
        OU_2 description
      - Subfolder2_2
        OU_2_1 description
      - Subfolder2_3
        OU_3 description
      - Subfolder2_4
    - Subfolder3
      - Subfolder3_1

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*.

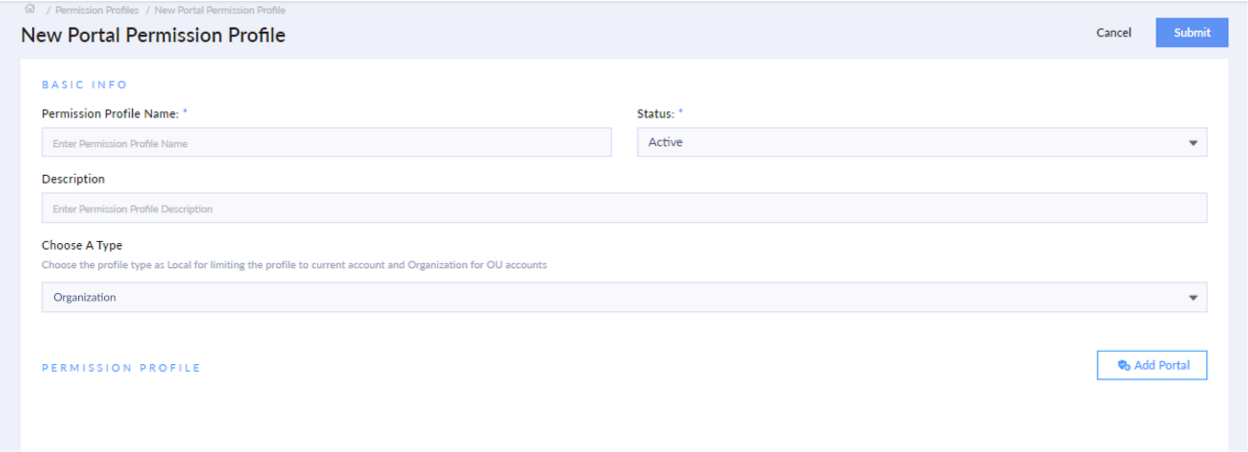
Permission profiles within Organizations

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

BASIC INFO

Permission Profile Name: * Enter Permission Profile Name

Status: * Active

Description: Enter Permission Profile Description

Choose A Type

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

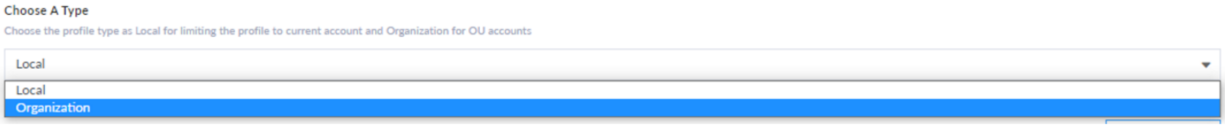
Organization

PERMISSION PROFILE

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 edited.

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



Choose A Type

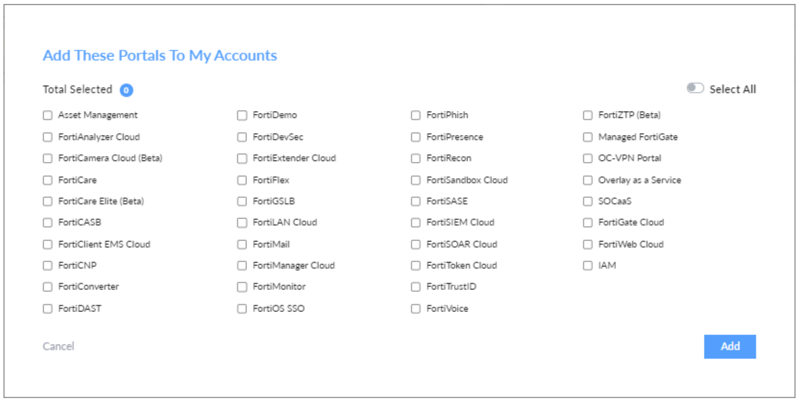
Choose the profile type as Local for limiting the profile to current account and Organization for OU accounts

Local

- Local
- Organization

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

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



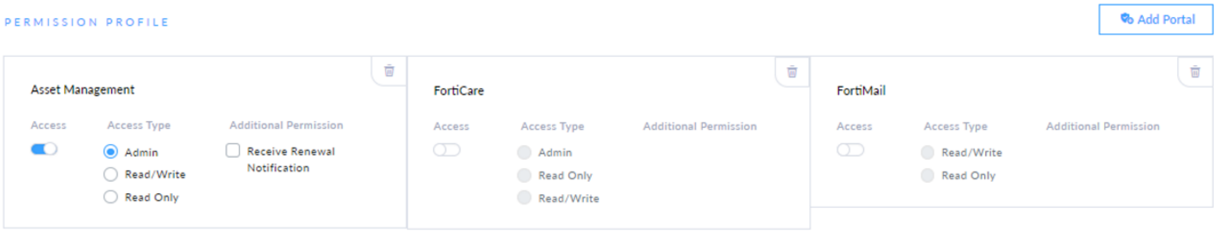
Add These Portals To My Accounts

Total Selected 0

Select All

☐ Asset Management
☐ FortiAnalyzer Cloud
☐ FortiCamera Cloud (Beta)
☐ FortiCare
☐ FortiCare Elite (Beta)
☐ FortiCASB
☐ FortiClient EMS Cloud
☐ FortiCNP
☐ FortiConverter
☐ FortiDAST
☐ FortiDemo
☐ FortiDevSec
☐ FortiExtender Cloud
☐ FortiFlex
☐ FortiGSLB
☐ FortiLAN Cloud
☐ FortiMail
☐ FortiManager Cloud
☐ FortiMonitor
☐ FortiOS SSO
☐ FortiPhish
☐ FortiPresence
☐ FortiRecon
☐ FortiSandbox Cloud
☐ FortiSASE
☐ FortiSIEM Cloud
☐ FortiSOAR Cloud
☐ FortiToken Cloud
☐ FortiTrustID
☐ FortiVoice
☐ FortiZTP (Beta)
☐ Managed FortiGate
☐ OC-VPN Portal
☐ Overlay as a Service
☐ SOCaaS
☐ FortiGate Cloud
☐ FortiWeb Cloud
☐ IAM

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



10. For each portal card:
    a. Enable *Access*.
    b. Select the *Access Type*.
    c. Select *Additional Permission* as required.

Some portals use resource-based permission profiles. See Permission profiles on page 15 and Creating a permission profile on page 18 for more information.

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

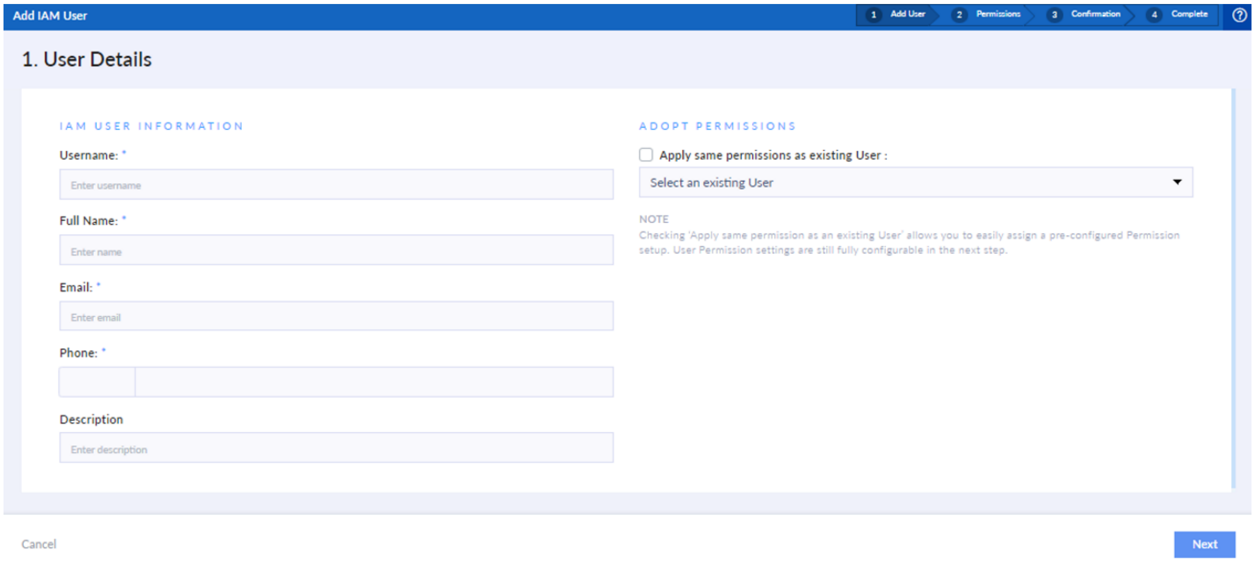
Creating users, user groups, and roles within Organizations

New IAM users, user groups, 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:

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*.

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



Add IAM User

1 Add User 2 Permissions 3 Confirmation 4 Complete

1. User Details

IAM USER INFORMATION

Username: *

Enter username

Full Name: *

Enter name

Email: *

Enter email

Phone: *

Description

Enter description

ADOPT PERMISSIONS

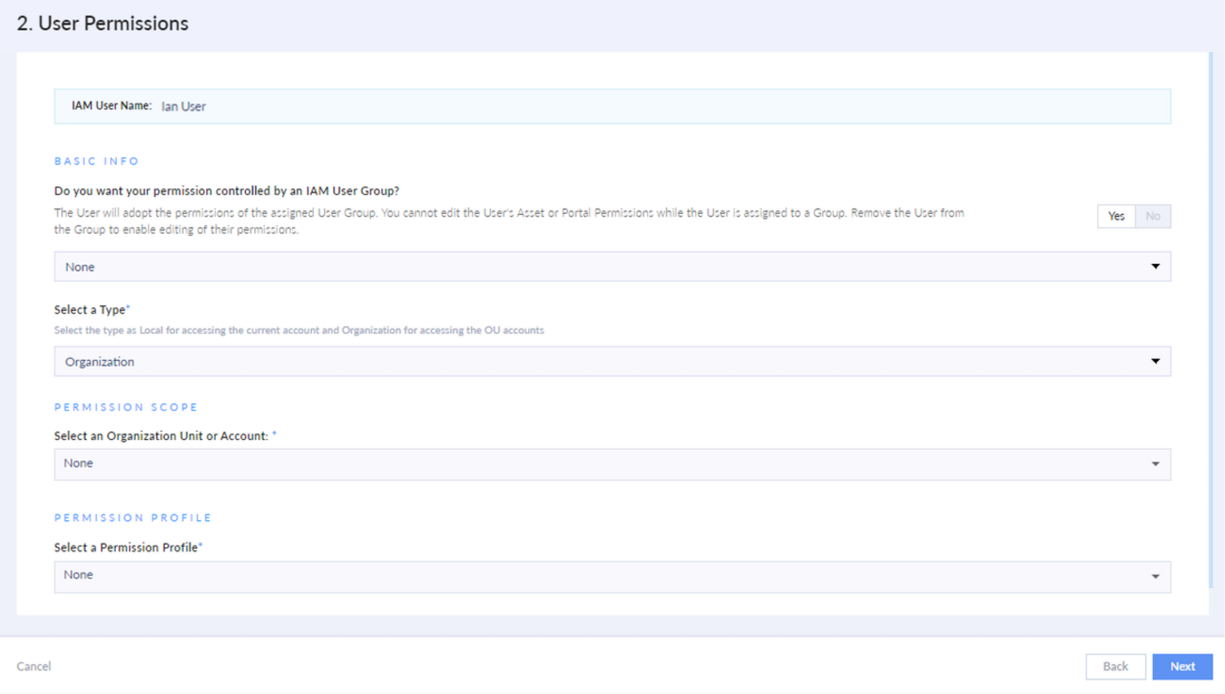
□ Apply same permissions as existing User :

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 47.
   a. Select *Yes* from *Basic Info*.



2. User Permissions

IAM User Name: Ian 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

None

Select a Type*

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

Organization

PERMISSION SCOPE

Select an Organization Unit or Account: *

None

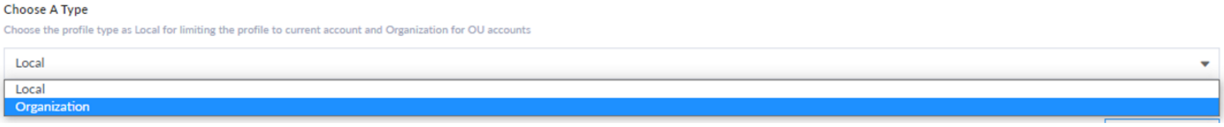
PERMISSION PROFILE

Select a Permission Profile*

None

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



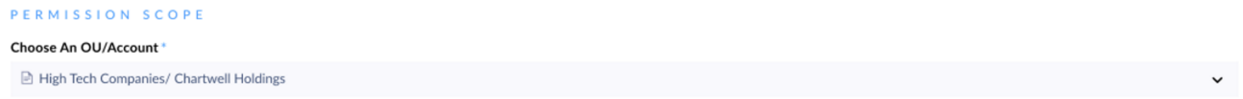
Choose A Type

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

Local

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

Choose An OU/Account *

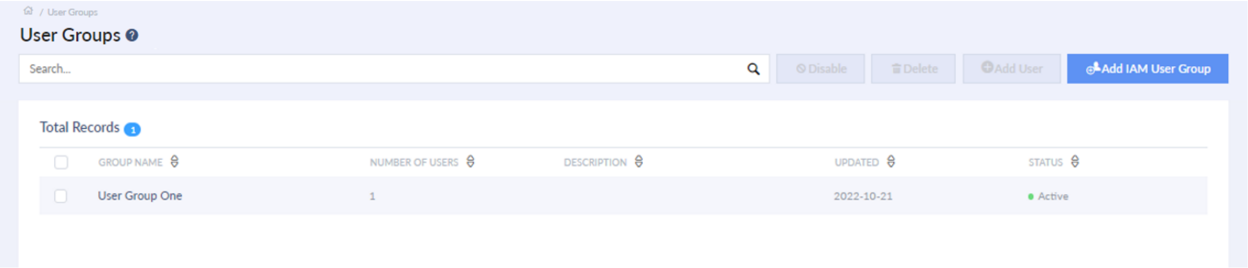
High Tech Companies/ Chartwell Holdings

8. In the *Permissions Profile* dropdown, select a profile. The *Permission Details* assigned to the selected profile are displayed.
9. Click *Next*. The *Confirmation* page is displayed.
10. 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:

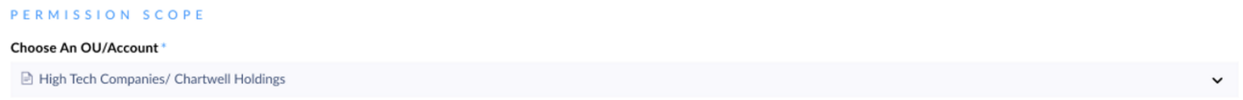
1. Select *User Groups* from the left-hand navigation menu. The *User Groups* page opens.



□	GROUP NAME	NUMBER OF USERS	DESCRIPTION	UPDATED	STATUS
□	User Group One	1		2022-10-21	● Active

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 *Choose 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.



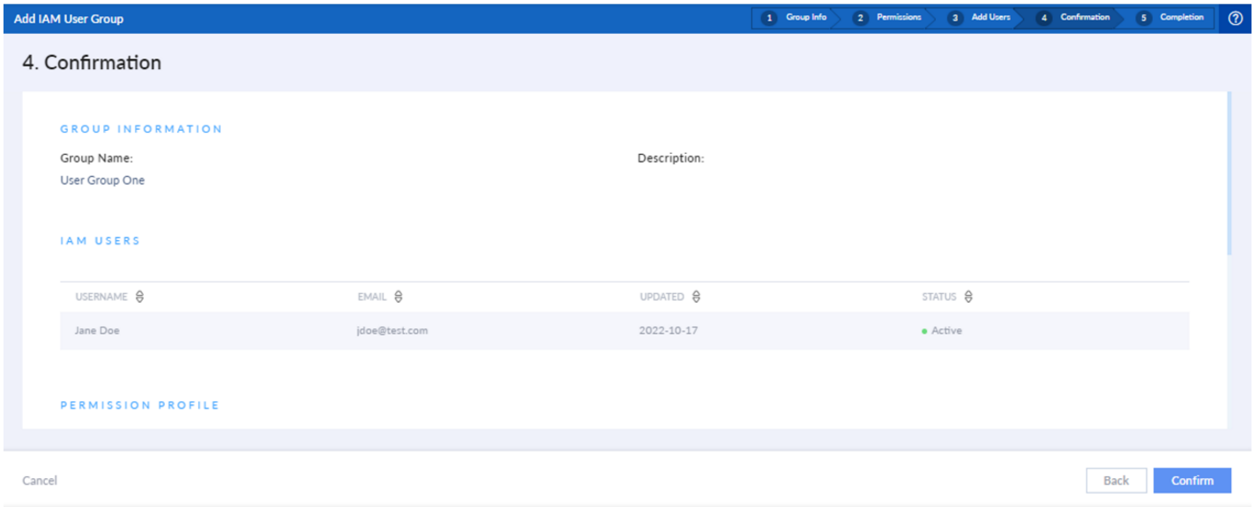
PERMISSION SCOPE

Choose An OU/Account *

High Tech Companies/ Chartwell Holdings

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*.



Add IAM User Group

4. Confirmation

GROUP INFORMATION

Group Name: User Group One

Description:

IAM USERS

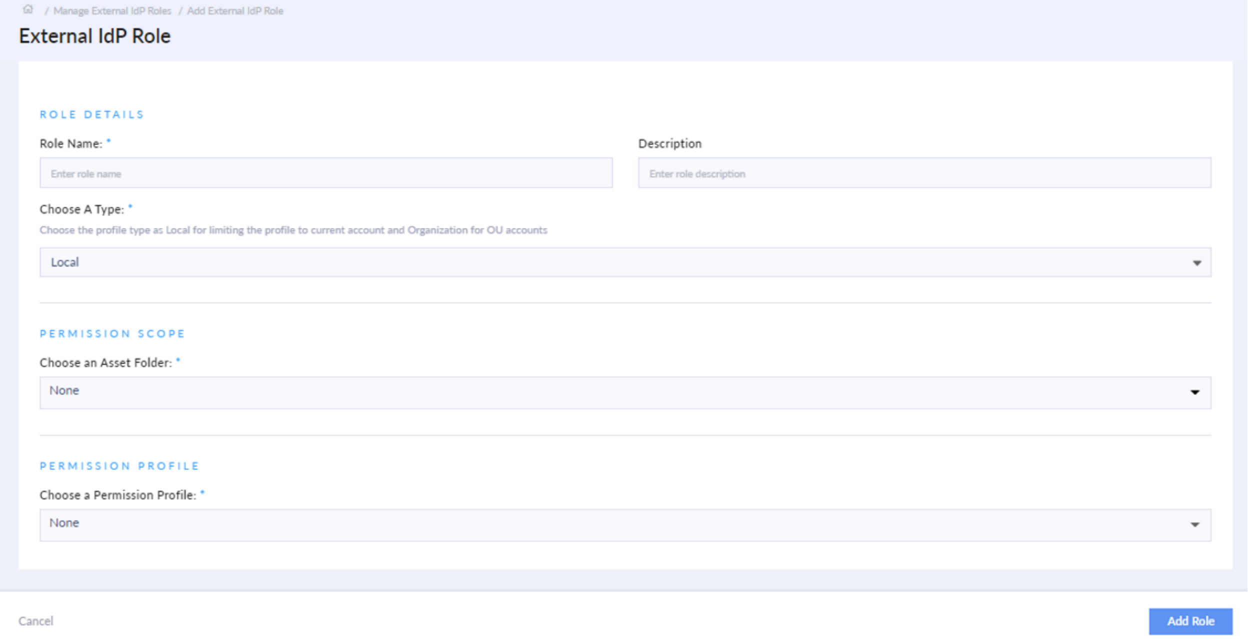
USERNAME	EMAIL	UPDATED	STATUS
Jane Doe	jdoe@test.com	2022-10-17	● Active

PERMISSION PROFILE

13. (Optional) Click *Add Another Group*.

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.



/ Manage External IdP Roles / Add External IdP Role

External IdP Role

ROLE DETAILS

Role Name: * Enter role name

Description: Enter role description

Choose A Type: *
Choose the profile type as Local for limiting the profile to current account and Organization for OU accounts
Local

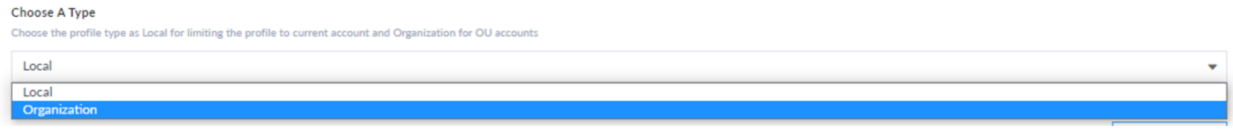
PERMISSION SCOPE

Choose an Asset Folder: * None

PERMISSION PROFILE

Choose a Permission Profile: * None

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 *Choose A Type* dropdown list.

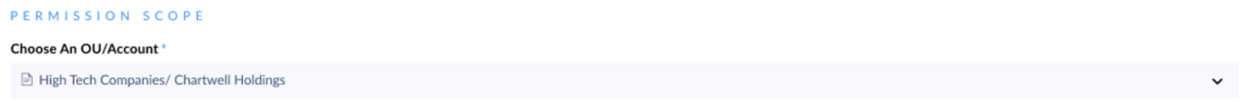


Choose A Type

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

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

Choose An OU/Account *

High Tech Companies/ Chartwell Holdings

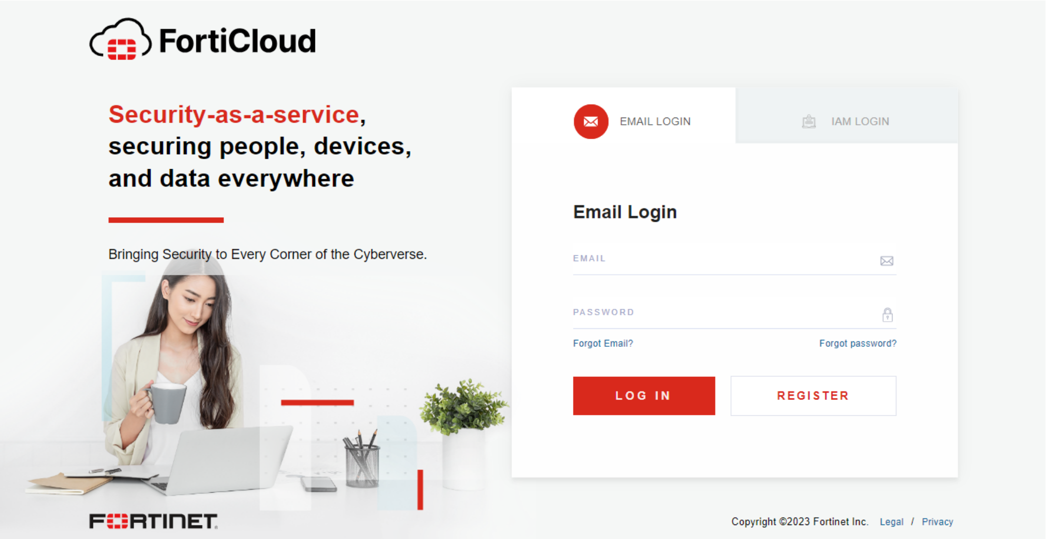
7. In the *Permissions Profile* dropdown, select a profile. The *Permission Details* assigned to the selected profile are displayed.
8. Click *Add Role*.

Logging into an OU account

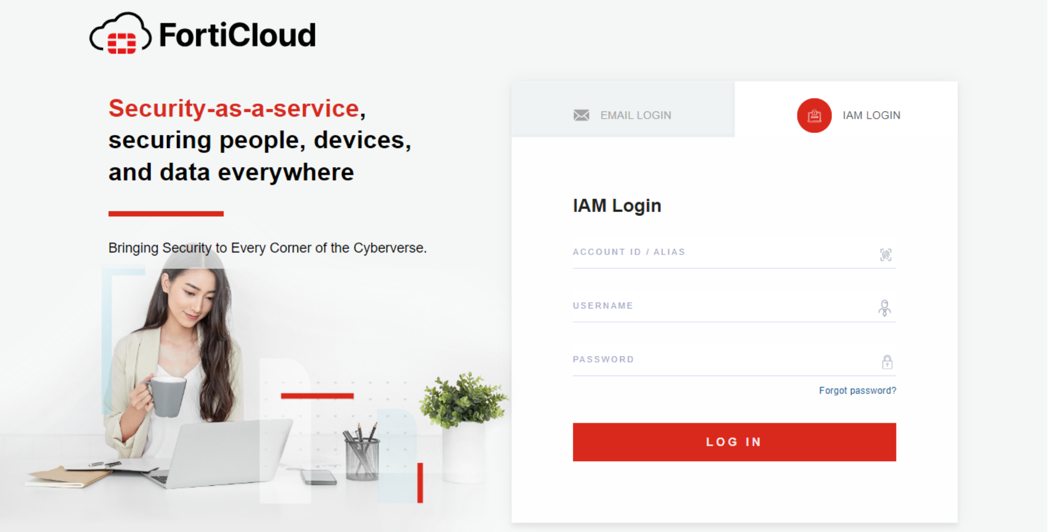
Users can access FortiCloud using IAM user accounts or an OU account when logging in with their IAM user credentials. Once the login credentials have been verified, users can then choose to proceed with an Organizational Unit (OU) account. OU access is dependent on the permission profile assigned to 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 https://support.fortinet.com.
2. Select *Login Now*. The log in portal opens.


FortiCloud
Security-as-a-service, securing people, devices, and data everywhere
Bringing Security to Every Corner of the Cyberverse.
EMAIL LOGIN
IAM LOGIN
Email Login
EMAIL
PASSWORD
Forgot Email?
Forgot password?
LOG IN
REGISTER
FORTINET
Copyright ©2023 Fortinet Inc. Legal / Privacy

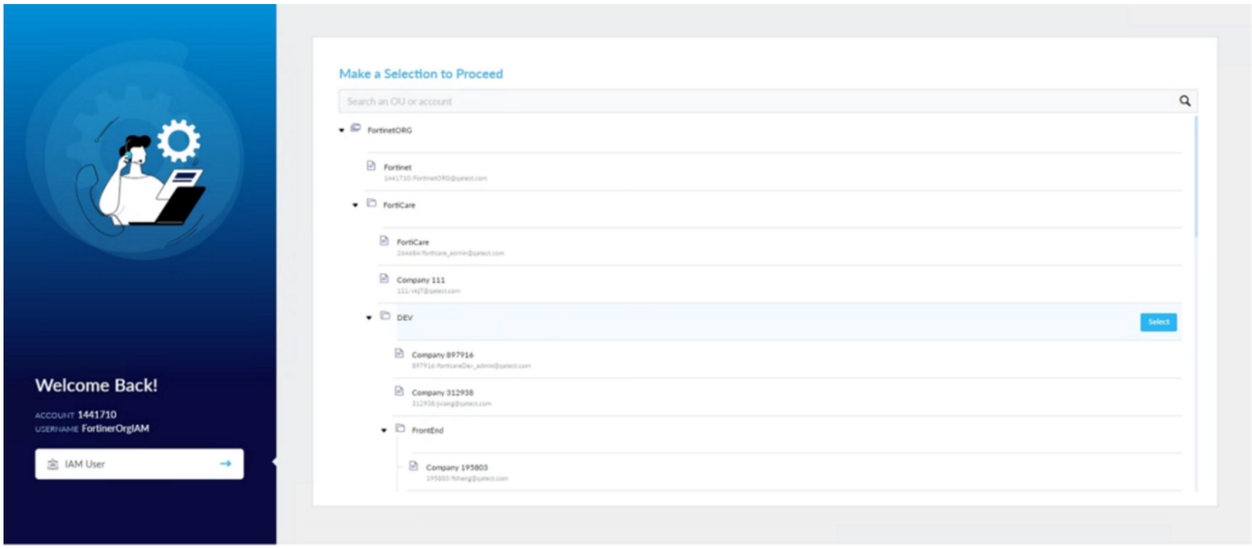
3. Select *IAM Login*.


FortiCloud
Security-as-a-service, securing people, devices, and data everywhere
Bringing Security to Every Corner of the Cyberverse.
EMAIL LOGIN
IAM LOGIN
IAM Login
ACCOUNT ID / ALIAS
USERNAME
PASSWORD
Forgot password?
LOG IN

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.



Welcome Back!

ACCOUNT 1441710
USERNAME FortinerOrgIAM

Make a Selection to Proceed

- FortinetORG
  - Fortinet
    1441710/FortinetORG@qatest.com
  - FortiCare
    - FortiCare
      264684/forticare_admin@qatest.com
    - Company 111
      111/vkj7@qatest.com
    - DEV
      - Company 897916
        897916/forticareDev_admin@qatest.com
      - Company 312938
        312938/jvang@qatest.com
      - FrontEnd
        - Company 195803
          195803/fcheng@qatest.com

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 and external IdP role credentials. See Available and selected scope on page 72.

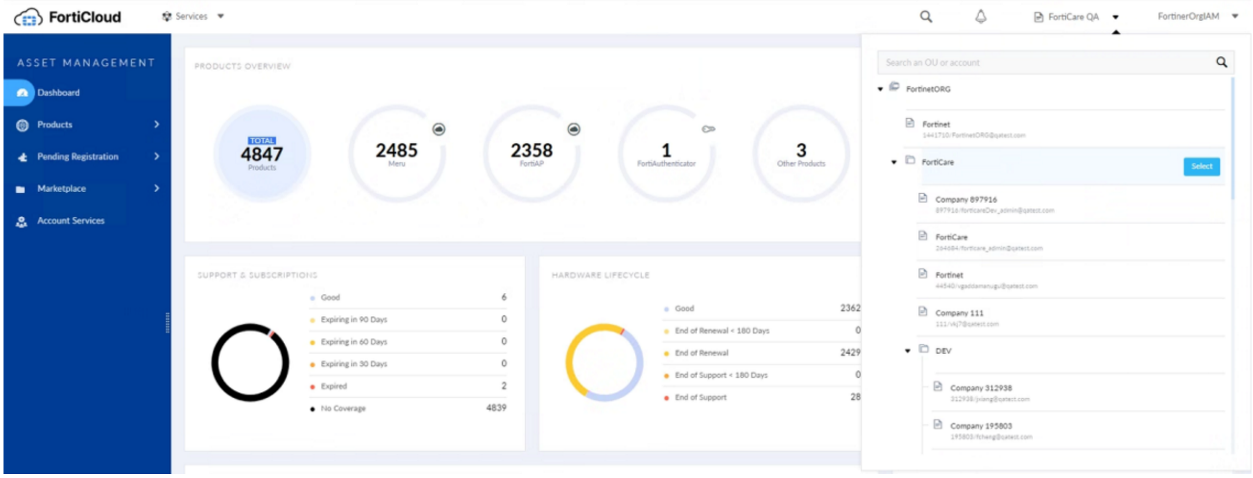
The Asset Management portal can support both OUs (with aggregated information on the member accounts within the OU) and OU member accounts. Therefore, if you are in the Asset Management portal, you can switch to either OUs or OU member accounts.

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 42.

FAQ

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 15.

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.

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.

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.

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.

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.

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.

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.

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.

Is an alias required?

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

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.

How do I set a password for an IAM user?

When creating an IAM user, the system generates a temporary password the IAM user can log in with. After the IAM user is logged in, they can set a new password of their choice. See Adding IAM users.

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.

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 IAMuser. See Updating user permissions.

Can I can 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 user groups.

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 32.

Can I access the IAM portal with my Partner account?

No. The IAM portal is not available in the *Services* menu when you log in with a Partner account.

Why am I being forced to use Two-Factor Authorization to log into a portal?

When Two-Factor Authentication (2FA) is enabled at the account level, all users including legacy sub users, are forced to set up 2FA to log into the portal.

Legacy sub users that use the same email address for multiple accounts may notice they can log into one account with an email address but are forced to log in with 2FA for another account. This is because one account has 2FA enabled while the other does not.

Users can disable 2FA for their account even when it is enabled at the account level. However, the user will not be able to log into the portal until 2FA is enabled again.

FORTINET®

www.fortinet.com