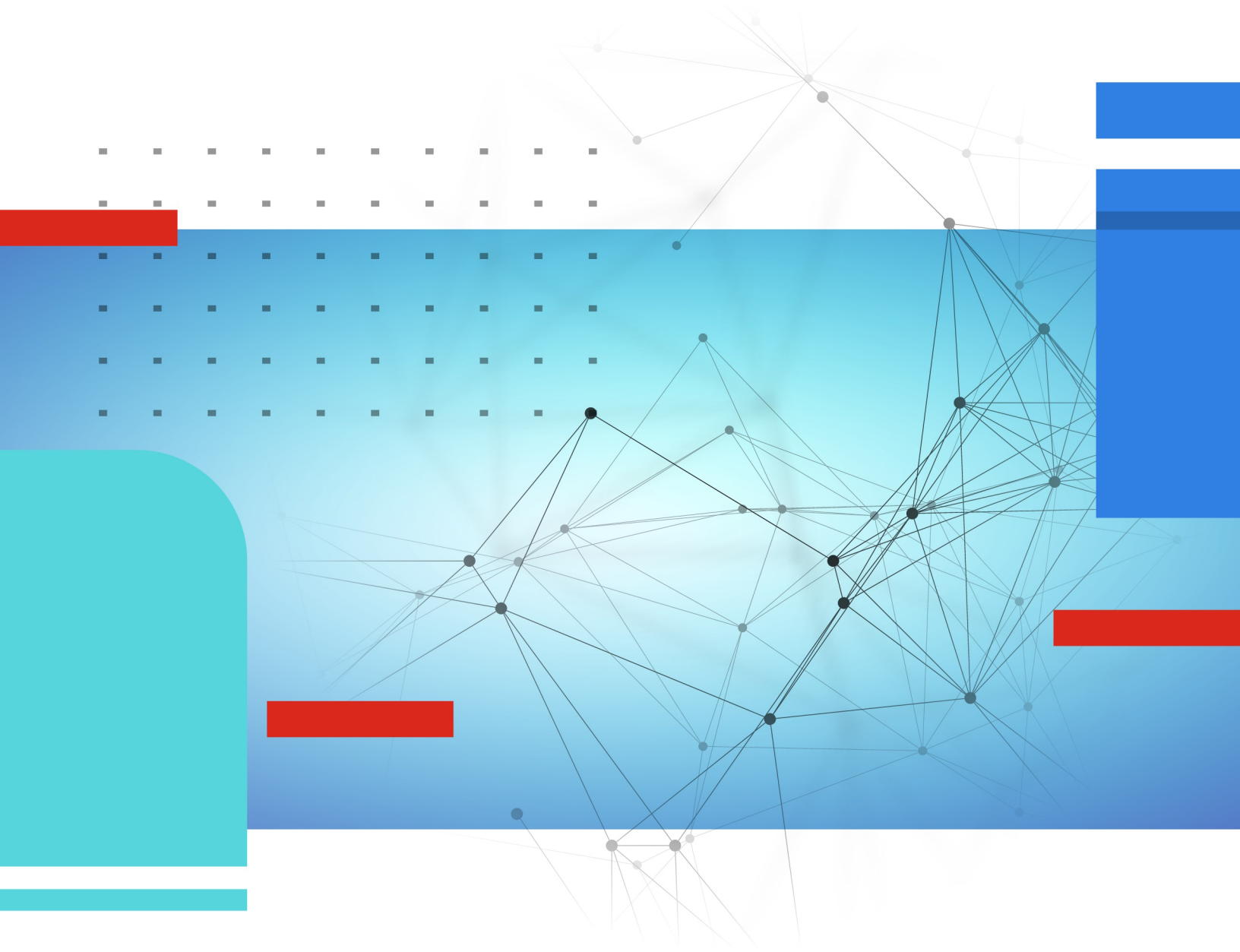
FORTINET

Admin Guide

Fortildentity Cloud 25.3.c



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

September 10, 2025
FortiIdentity Cloud 25.3.c Admin Guide

TABLE OF CONTENTS

Introduction

Many of today's most damaging security breaches could have been prevented by the use of multi-factor authentication (MFA). FortiIdentity Cloud solves this by offering a secure, easy-to-use, MFA-as-a-service for users of Fortinet products such as FortiGate (FGT) and FortiAuthenticator (FAC) as well as third-party web applications.

From provisioning to revocation, FortiIdentity Cloud offers a robust platform for managing your multi-factor authentication deployment. Its intuitive dashboard is accessible anywhere over the internet. It's a highly available platform that can scale support from organizations with a single FortiGate to managed service providers managing hundreds of FortiProducts and/or third-party Web apps.

FortiIdentity Cloud is easily deployed without additional hardware, software, or ACL changes, and expands as your needs grow. FortiIdentity Cloud is a subscription service available through the purchase of time-based licenses, where all licenses are stackable with co-termed renewal options.

FortiIdentity Cloud has many innovative features to proactively reduce the risk of data breach while making it convenient and simple for your end-users to use.

Licensing and availability

Subscription licensing

Fortildentity Cloud is a subscription-based MFA cloud service. To take advantage of the service, you must subscribe by purchasing a license (i.e., SKU) based on the number of FIC service end-users in your account for the year. Refer to Time-based SKUs and their services on page 12 for more information.

- Your FIC license is valid for one year only, and must be activated within one year after the date of purchase.
- Licenses that are not activated automatically expire one year after the date of purchase.

Time-based SKUs and their services

The following table lists licensing options of the time-based subscriptions by SKU.

SKU	User Limit	Description
FC1-10-IDCLD-445-02-12	25 - 499	Annual, per-user, cloud-managed Fortildentity subscription, including 125 SMS credits per user and FortiCare Premium Support per year.
FC2-10-IDCLD-445-02-12	500 - 1,999	Annual, per-user, cloud-managed Fortildentity subscription, including 125 SMS credits per user and FortiCare Premium Support per year.
FC3-10-IDCLD-445-02-12	2,000 - 9,999	Annual, per-user, cloud-managed Fortildentity subscription, including 125 SMS credits per user and FortiCare Premium Support per year.

SKU	User Limit	Description
FC4-10-IDCLD-445-02-12	10,000 or more	Annual, per-user, cloud-managed FortiIdentity subscription 10,000 or more users, including 125 SMS credits per user and FortiCare Premium Support per year.

Stackable co-termed licenses

FortiIdentity Cloud offers four licenses (SKUs) for you to choose from.

Suppose that you start FIC service on August 1, 2025 with a 500-user license (i.e., FC3-10-IDCLD-445-01-12) which expires on August 1, 2026. On October 15, 2025, you decide to add 100 more end-users to your account, so you purchase another license for 100 end-users (i.e., FC2-10-IDCLD-445-01-12). Those two licenses are independent of each other. The 500-user license will expire on August 1, 2026, and the 100-user license will expire on October 15, 2026.

You can also add licenses to an old SKU with a new SKU. If you have a license with the TKCLD SKU before the name change to FortiIdentity Cloud, you can add a license with the new IDCLD SKU. For example, on December 1, 2025, you want to add a 25-user license and you want it to expire on the same date as your 500-user license does. In this case, the new co-termed license will be stacked on top of the original 500-user license. The cost of the new license will be prorated so that it expires on August 1, 2026; it will have the same expiration date as the original 500-user license, but with a new limit of 525 users.

In the first case, the new license is independent of the original license, which can be purchased based on its SKU. In the second case, you will have to reach out to our license renewal team (renewals@fortinet.com) for assistance.

For more information, see Time-based SKUs and their services on page 12 and SKUs vs. applications and realms supported in the Admin Guide.

Resource rules

For a licensed account, when the total purchased user quota is x among the licenses, the related resource quota is calculated as follows:

Resource	Quota
Users	x
Realms	If x ≤ 500, then x; if x > 500, then 500 + x/10
Web Applications & Mgmt Applications	Maximum (x/10, 5)
SAML Applications	Maximum (x/10, 5)
User Sources	Maximum (x/10, 5)
Certificates	Maximum (x/10, 5)

Resource	Quota
Brandings	Maximum (x/10, 5)
Domains	Maximum (x/10, 5)
User Groups	Maximum (x/10, 5)
Profile	100
Policies	200

- x/10 will truncate any decimal places if the result is not an integer. For example, if x = 49, x/10 is counted as 4.
- For realms, if the total purchased user quota is x and x is equal to or less than 500, the maximum number of realms allowed is also x; if the total purchased user quota is greater than 500, the maximum number of realms allowed is 500 + x/10. For example, if user quota is 400, the maximum number of realms allowed is 400; if user quota is 600, the maximum number of realms allowed is 560.
- For maximum (x/10, 5), if the total purchased user quota is x, the maximum number of the target resource is the greater value between x/10 and 5. For example, if user quota is 40, the maximum number of the target resource is 5; if user quota is 60, the maximum number of the target resource is 6.

Free trial license

If you have registered under FortiCloud on support.fortinet.com, FortiIdentity Cloud (FIC) automatically enables your 30-day free trial license when you log into the FIC portal (FIC.fortinet.com) for the first time. The free trial license only supports up to five end users and five realms, and does not include SMS service.

You will receive a welcome email after activating the free trial license. The email includes, among other things, the expiration date of the free trial license and instructions on how to purchase a paid license.

If, at the end of your free trial, you want to continue using FIC service, you can purchase a license (SKU) that best fits your needs to take full advantage of FIC MFA cloud service offerings. For license information, see Licensing options.

You will receive another welcome email when activating a paid license. The email shows, among other things. the user quota and expiration date of your license.

FIC also offers a free three-user licenses that can be activated from the UI of supported Fortinet devices, such as FortiGate and FortiAuthenticator, as long as the device has a valid support contract in FortiCare. Neither the free license nor the 30-day free trial includes SMS quota.

The free three-user license includes three realms and IdP proxy for unlimited downstream Fortinet devices and five applications. The free three-user license expires at the same time as the support contract of the device does.

If trial is enabled from the FortiIdentity Cloud portal, it allocates a quota of five users and five realms only for 30 days. If the account has a supported device with a valid contract, the free three-user license can be activated after the 30-day trial ends.

SMS licensing

FortiIdentity Cloud uses credits-based SMS accounting. Each regular license (SKU) option allows for 125 SMS credits for each end user annually. If you need more SMS credits, refer to the following table.

SKU	SMS Credits	Description
FIC-SMS-2500	2,500	One or more SMS credits may be consumed per SMS message sent based on Country Code. The license must be activated within one year of purchase. Unused SMS credits expire three years after the date of activation.
FIC-SMS-10K	10,000	One or more SMS credits may be consumed per SMS message sent based on Country Code. The license must be activated within one year of purchase. Unused SMS credits expire three years after the date of activation.
FIC-SMS-25K	25,000	One or more SMS credits may be consumed per SMS message sent based on Country Code. License must be activated within one year of purchase. Unused SMS credits expire three years after the date of activation.

The number of credits that FIC charges for SMS use varies, depending on where the end-user's phone number is registered. For more information, see SMS Rate Card.

Email notification on license balance status

Once the user count in your account becomes greater than the user quota, your account will be marked as an expired account. After your account expires, FIC offers a 30-day grace period. During the 30-day grace period, you (the FIC admin) still have full admin access to the FIC portal, existing users in your account are still able to authenticate using FIC, and your account usage will continue to be calculated, but you will not be able to add more users to your account.

After the 30-day grace period, if there is no new license applied, your account will be marked as disabled, and the existing users will not be able to get authenticated by FIC. FIC will send out email reminders to your account at 30-, 14-, and 1-day intervals to remind you that the account is going to be disabled.

After 90 days of being disabled, your account will be deleted from the FIC system if there is no license applied. FIC will send out email reminders to the account at 30-, 14-, and 1-day intervals to remind you that the account is going to be deleted.

FIC provides a switch button for enabling/disabling email notifications (*Settings > Global > Account Disable/Delete Notification*.) The default setting of this feature is to receive all email notifications.

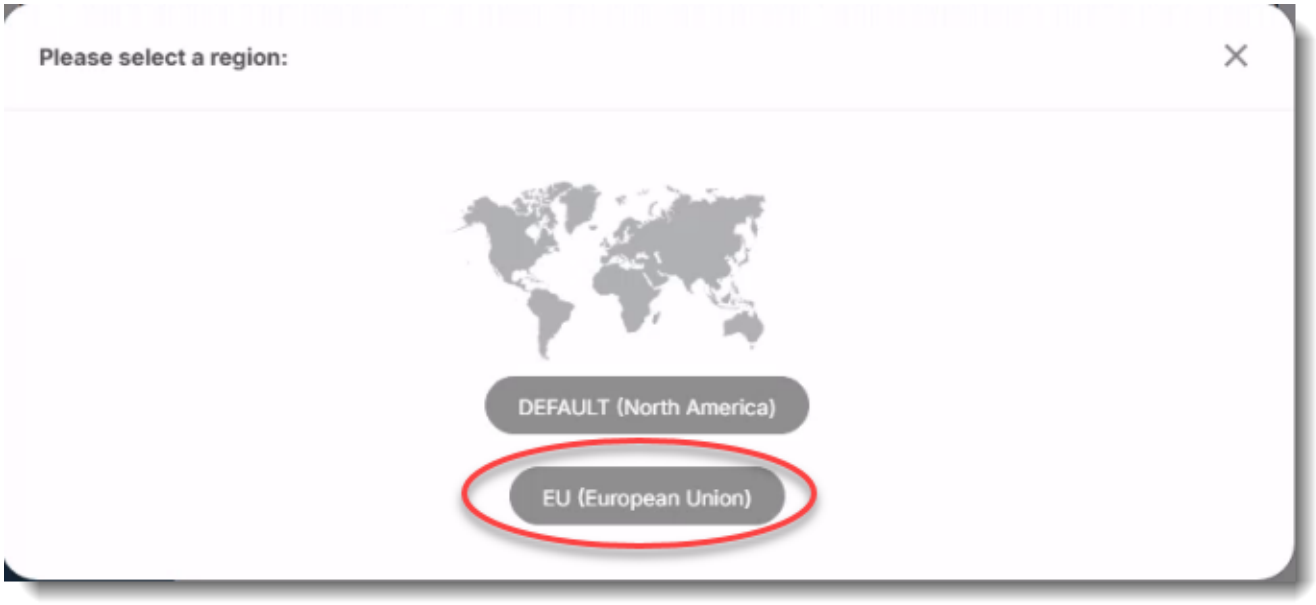
Support for EU GDPR

Fortildentity Cloud (FIC) supports EU's General Data Protection Regulation (GDPR) compliance by offering data residency in European Union (EU)-based data centers, ensuring that personal data remains within GDPR jurisdictions. It collects only minimal personal information necessary for authentication and ensures that all data is encrypted both in transit and in residency. The service supports user consent management, data access, and deletion requests in line with GDPR rights. With granular access controls, audit logging, and documented breach response procedures, FIC enables organizations to maintain accountability and transparency. Fortinet also provides Data Processing Agreements (DPAs) to clarify roles and responsibilities under the regulation.

FIC's Support for EU GDPR enables our EU customers to select data centers located within the European Union. This regional support enhances data sovereignty, supports lawful data processing, and aligns with the GDPR's requirements for data residency, security, and user rights.

New customers

New EU customers can sign up directly through the `eufic.fortinet.com` portal by selecting EU (European Union) during sign-up to have their account provisioned for the EU region, as shown in the following screen capture. The admin can then register any new device to this account.



Alternatively, if you have a device running on FortiOS 7.4.8, you can update the system global to point to Europe and initiate the account from the FortiGate CLI:

1. In FortiOS, run `config system global`.

   Make sure that `"set fortitoken-cloud-region"` is set to `"eufic.fortinet.com"`, as shown in the following screen capture.

```
FGVM32TM25000448 (global) # show
config system global
    set alias "FGVM32TM25000448"
    set fortitoken-cloud-region "eufic.fortinet.com"
    set gui-auto-upgrade-setup-warning disable
    set hostname "FGVM32TM25000448"
    set sslvpn-web-mode enable
    set timezone "US/Pacific"
end
```

2. Run "`execute fortitoken-cloud trial`". This should set the FIC account specifically for the EU region.

```
FGVMULTM2[redacted] (Interim)# execute fortitoken-cloud trial
[redacted]
FortiToken Cloud service status: licensed. Region code: 01. Region name: eu.
Service balance: 3.00 users. Expiration date: 2026-06-18. Customer ID: [redacted]
```

Device Migration

Existing FIC customers in EU countries with their accounts originally set up for North America cannot migrate their data or services to the EU region retroactively. Instead, they must delete end users from the devices and their FIC account, create their new accounts by selecting the EU region, and add the devices and end users to their new accounts.

Case 1: Migrating devices from an existing account in North America to a new account in EU

1. Delete all users on the device(s) using FIC portal. Ensure that the device(s) is/are deleted in FIC as well.
2. Submit a request with FortiCare (support.fortinet.com) to transfer the device(s) to your new EU account.
3. Refer to Transferring devices on FIC.
4. After successful transferring the device(s) to your EU account, add the users to the device(s). This will synch the users and the device(s) to your new EU account.

Case 2: Moving the same account from North America to EU

1. Delete all users from the device(s) and FIC using FIC portal.
2. In FortiOS 7.4.8, reset the region first before proceeding to the next steps.

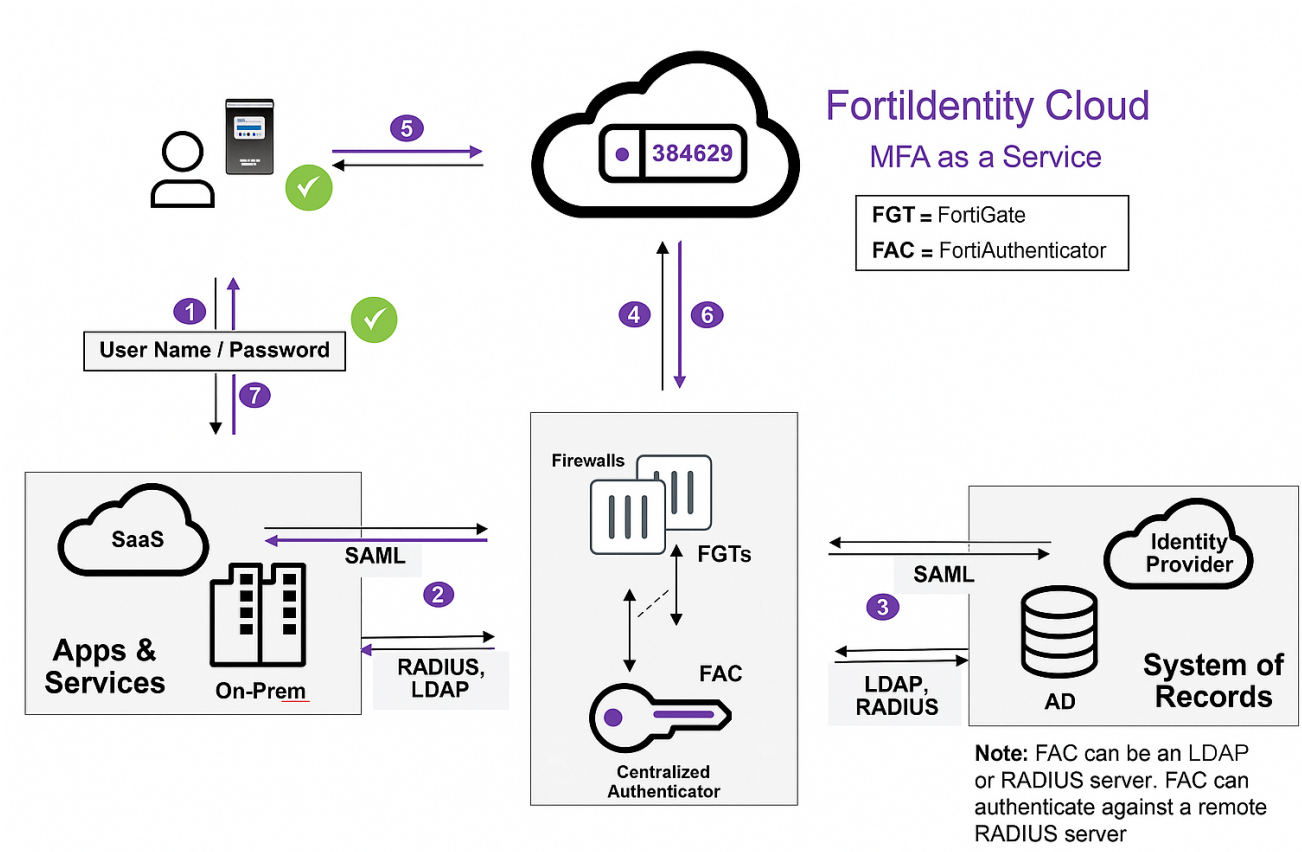
3. Run the command "`execute fortitoken cloud region-reset`".
4. Log in to eufic.fortinet.com with the same account and be sure to choose EU (European Union) when setting the region.
5. Alternatively, in a FortiOS 7.4.8 device that is registered with the account, you can set global config to EU, and then add a user which will synch to the EU account. Other devices in the same account will now be able to synch to the EU account.

For existing accounts using SSO application

1. Create a new account in FIC EU.
2. Recreate all SSO applications, user source(s), and SSO application users in the new EU account. (Note: The same step applies to local IdP users as well.)

Architecture

The following topology highlights the network architecture of the FortiIdentity Cloud end-to-end solution.



The following describes the workflow of the FIC MFA authentication process:

1. The user enters their username and password which will be first sent over to the connected apps or services.
2. The apps or services will then relay the credentials to the connected Fortinet devices.
3. The Fortinet devices will then consult the connected system of records (e.g., SAML, LDAP, or RADIUS servers) to verify the credentials.
4. Upon successful verification, a FortiIdentity Cloud code will be sent to the user.
5. Once the user enters the code either manually or via push notification, FIC will verify the code.
6. If the code verification is successful, the Fortinet devices will be notified.
7. At this point, the authentication process is completed, and the user should be able to successfully log into their apps or services.

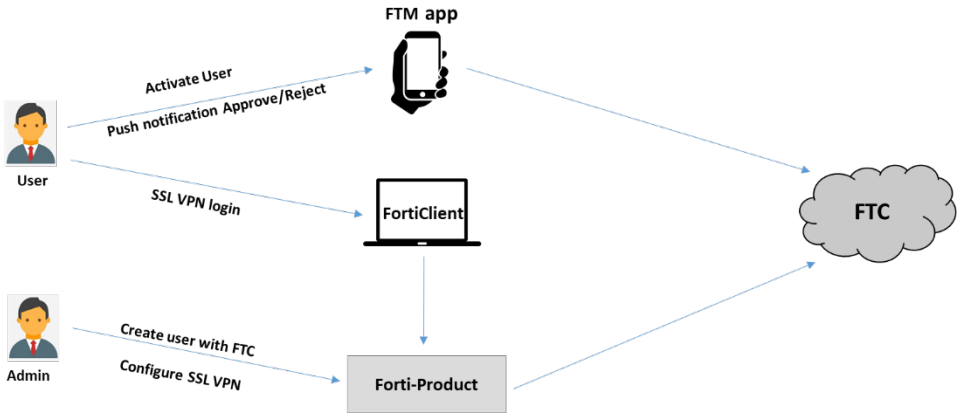
Acronyms and abbreviations

The table below lists the acronyms and/or abbreviations used in this document and/or on the FIC portal.

Acronym/Abbreviation	Terminology
2FA	Two-factor authentication **Note:** This term is used in FortiGate/FortiOS. It carries the same meaning as "MFA" (listed below) used in FortiIdentity Cloud.
MFA	Multi-factor authentication.
Auth	Authentication
FAC	FortiAuthenticator
FC	FortiCloud
FGT	FortiGate
FOS	FortiOS
FIC	FortiIdentity Cloud
FTK	FortiToken (hardware token)
FTM	FortiToken Mobile (software token)
IdP	Identity Provider
OIDC	OpenID Connect
OU	Organizational Unit
OTP	One-time password
SAML	Security Assertion Markup Language
SCIM	System for Cross-domain Identity Management
SMS	Short message service
SP	Service Provider
SSO	Single sign-on
TOTP	Time-based one-time password
UTC	Universal Time Coordinated (or Coordinated Universal Time)

Quickstart guide

This quickstart guide shows how to configure an application to use FIC service for end-to-end authentication. The instructions are for configuring a local FortiGate SSL VPN user to log in using MFA with FIC push notification.



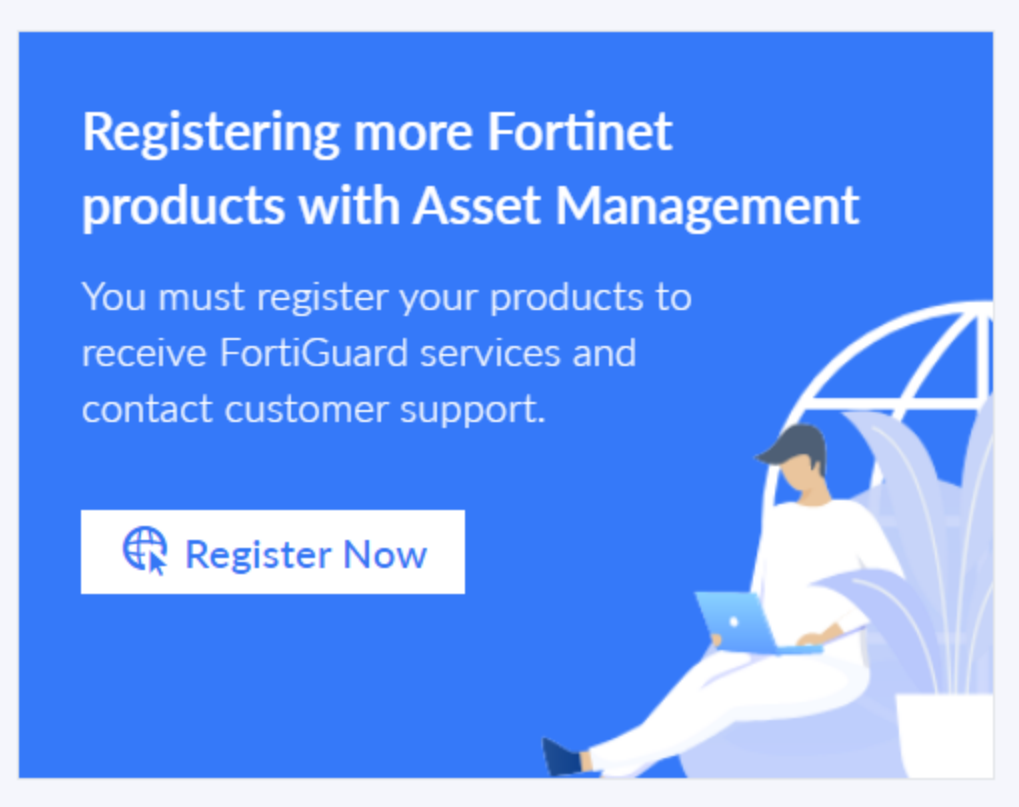
What you need:

- FortiGate or FortiAuthenticator
- FortiClient
- FortiToken Mobile app

For information on the compatibility of the aforementioned Fortinet applications, refer to Compatible Fortinet applications on page 38.

Step 1: Registering FortiProduct (FortiGate)

Register the FortiGate (FGT) under your FortiCloud (FC) account. If you don't have an FC account, go to https://support.fortinet.com/ to register a new FortiCloud account. Register your FGT license under your FC account, and then, if a license file is required for you to use your device (e.g., FortiGate VM), you can download the license file from https://support.fortinet.com/.



Step 2: Getting FIC license

FIC provides free trial licenses and paid licenses. You can choose one based on your preference. The following instructions show you how to get a license:

Option 1: Trial license

If you have registered under FortiCloud from support.fortinet.com, FortiIdentity Cloud (FIC) automatically enables your 30-day free trial license when you log into the FIC portal (FIC.fortinet.com) for the first time. The free trial license can only support up to five end users and five realms. It does not include SMS support.

Option 2: Paid license

- How to purchase FIC licenses
- How to register your FIC license

Step 3: Configuring SSL VPN and a local user on FGT with FortiIdentity Cloud enabled for MFA

Configure SSL VPN and a local user on FGT. See SSL VPN setting up on FGT.

Step 4: Activating the local user on FTM app

Install the FTM app on your phone, and activate the user created by scanning the activation code in the email that the user sent with the FTM app. Make sure that system notifications have been enabled for the FTM phone to ensure that it can receive notifications.

- FortiToken Mobile on page 47
- Supported FortiToken Mobile apps on page 47
- Activating FTM tokens on page 48
- Activating third-party tokens on page 48
- Using FTM tokens on page 48

Step 5: Configuring FortiClient on the login server

Install FortiClient on the server that you are going to use for logging in the user. Configure the SSL VPN tunnel which connects to the FGT from FortiClient.

Link: Connecting from FortiClient to SSL VPN

Step 6: User login authentication

The user logs in with FortiClient on the server. After entering the username and password, the user will receive a notification from the FTM app on your phone. Click *Approve* to log into the system via SSL VPN.

Getting started—FGT-FIC users

By default, FIC service is enabled on FGT VDOMs. So an FGT VDOM with a valid FIC license automatically becomes an application of FIC the moment it is created.

FIC supports up to four MFA methods, namely FTM, FTK, SMS, and email. The MFA method is set on a per-realm basis. The default method is FTM, but the admin user can change it to another method if needed. Sub-admins can then further change the MFA methods for end-users in their assigned realms to something other than the default (i.e., FTM). See Managing users on page 103 for MFA methods used by end-users.

If you use FGT as an authentication client of FIC, you may complete the following steps to get started with FIC:

1. Registering your FIC subscription on page 25.
2. Upgrading FortiOS on page 26.
3. Logging into the FortiIdentity Cloud portal on page 26.
4. Activating FGT VDOMs for FIC service on page 26.
5. Adding an admin user for FIC service on page 27.
6. Adding a local user for FIC service on page 27.
7. Adding remote FortiGate users for FIC service on page 28.

Registering your FIC subscription

Upon purchasing your FIC service subscription, you'll receive via email a license certificate (a .PDF file) with a registration code in it. Your first step is to register your FIC subscription on FortiCloud.

Be sure to register your FIC subscription to the same FortiCloud (FC) account under which your FGT is registered.

To register your FIC subscription:

1. Have your FIC license certificate ready.
2. Launch your web browser.
3. Log into FortiCloud at https://support.fortinet.com/ with your FortiCloud username and password.
4. On the FortiCloud banner across the top of the page, click *Services* to open the drop-down menu.
5. Click *Asset Management* to open the *Asset Management* page.
6. From the side menu, click *Register Product*.
7. Follow the prompts onscreen to complete the registration.

Upgrading FortiOS

FortiIdentity Cloud requires FortiOS (FOS) version 7.0.0 or later, 7.2.0 or later, or 7.6.0 or later. Be sure to upgrade your FortiOS to a supported version, if needed.

To upgrade your FortiOS:

1. Log into your FGT device.
2. From the menu (on the left), click *System>Firmware*.
3. Click *Browse* to browse for FOS version 7.0.x/7.2.x/7.6.x.
4. Follow the instructions onscreen to complete upgrading your FOS on the device.

Logging into the FortiIdentity Cloud portal

All FortiCloud (FC) registered users can access the FIC portal. If your organization has multiple FIC accounts, you'll see a list of your FIC accounts after you sign in on FortiCloud. You can then select an account to open it on the FIC portal. During a session, you can switch from one account to another using the *Account* drop-down menu in the upper-right corner of the GUI.

Access to FIC is managed by FortiCloud SSO authentication via FortiAuthenticator (FAC). Upon receiving your login request, the system redirects you to FortiCloud which is the FortiCloud (FC) SSO page. From there, you must use your FC master account username and password to log in. After authenticating your identity using multi-factor authentication (MFA), the system grants you access to the FIC portal.

To log in to the FIC portal:

1. Open your web browser, point to https//fic.fortinet.com, and press the *Enter* key on your keyboard.
2. In the upper-right corner of the page, click *LOGIN*.
3. Enter your FC master account username and password, and press *LOGIN*.
   Once you've logged in, the FortiIdentity Cloud landing page opens, showing your FIC account (or a list of accounts if your organization has multiple FIC accounts).
4. Click your account or one of your accounts to open it.
   The FIC *Dashboard* page opens.

Activating FGT VDOMs for FIC service

In order for your FortiGate (FGT) users to take advantage of the MFA feature provided by FortiIdentity Cloud, make sure that FIC service is enabled on the FGT device.

By default, FortiIdentity Cloud service is enabled in FortiOS. However, if for some reason, FIC is not enabled on your FGT, you must manually enable it to proceed.

Only an FGT global admin user can activate FIC service on a per-FGT device basis, not by specific VDOMs.

To activate FGT VDOMs for FIC service:

```
FortiGate-VM64 # config global
FortiGate-VM64 (global) # config system global
FortiGate-VM64 (global) # set fortitoken-cloud enable
FortiGate-VM64 (global) # end
```

`set FortiIdentity-cloud enable` is a "local" command and does not trigger communication with the FIC server. It simply enables FGT VDOM admin users to manage FIC users locally using the FGT CLI.

Adding an admin user for FIC service

You can add FGT VDOM admin users for FIC service using the following commands:

```
config system admin
   edit <admin_username>
      set accprofile <super_admin>
      set vdom root
      set two-factor fortitoken-cloud
      set email-to <admin_user@fortinet.com>
      set password ENC SH2aEArTfqHbNJ8E2O87zSFAYqak8t14t+AiQxH+XWhZMKJQMfoPZS002MDPCo=
   next
end
```

For more information, see Configuring admin users on page 249.

Adding a local user for FIC service

Once you are sure that your FIC service is enabled on your FGT device, you can add VDOM users and enable them for FIC service using the following commands:

```
config user local
    edit <username>
        set type password
        set two-factor fortitoken-cloud
        set email-to <user@abc.com>
        set passwd-time 2018-05-15 08:41:35
        set passwd ENC
51sXDNIDYqPgRvahKx6jh+HACElPinhC+yXCDva6ytEaH+bHM5G0+AFkwFVJdEpidKBIY0xn2LlLPpvSmWRhXhAFAP77OofUdF
Ss9eydatFw/BY/4WgCimfir1EOLdtTRjVO9oaCj6LTPBYzZJsyrImmKx7benWG1tTOXWgmktUy88WR02rdUB8ZZdBTfDfDoBAL
2Q==
```

```
    next
end
```

As an option for two-factor authentication, “FortiIdentity-cloud” becomes available only when FIC service is enabled on FGT.

Upon execution of the above commands, a local FGT user is created and is set to use FIC for MFA authentication. Information about the user automatically appears on the Users page of the FIC portal. If the user is the first user of the FGT VDOM that you've added for FIC service, the VDOM appears on the applications page as well.

For more information, see Configuring local users on page 250.

.

Adding remote FortiGate users for FIC service

Your can use the following commands to configure FortiGate wildcard LDAP users to use FortiIdentity Cloud for MFA:

```
config user ldap
      edit "EngLDAP"
            set server "xxx.xx.xxx.xx"
            set cnid "uid"
            set dn "dc=srv,dc=world"
            set type regular
            set two-factor fortitoken-cloud
            set username "cn=Manager,dc=srv,dc=world"
            set password ENC LWdyb+/k6e4TtSk070tODaCZAcbgEGKohA==
      next
end
```

Wildcard LDAP users are those of a remote LDAP server user group, whose user configuration is unknown to FortiGate. Each end-user should have the following attributes configured on the LDAP server:

- mail: user_email_address (e.g., mail: user1@abc.com)
- mobile: user_phone_number (e.g., mobile: +14080123456)

- In FortiOS, the "mail" attribute is mandatory and required of each user, while the "mobile" attribute is optional.
- FIC requires that the phone number be in the format of " +(country_code) (areacode_number)".
- All end-users under the “dn” on LDAP server are synchronized to FIC, which could be a large number. Setting “dn” to a proper level of the LDAP directory can manage the number of users who have FIC enabled.

See Configuring wildcard LDAP users for FIC service on page 251 for more information.

Getting started—FAC-FIC users

- Tasks such as creating FAC users and enabling them for FIC service can and must be performed on the FAC GUI only; no FAC Console commands are available for such operations.
- FIC supports token activation via SMS and synchronization of mobile numbers for end-users with FortiAuthenticator as the application. For FortiAuthenticator and FIC compatibility, refer to Compatible Fortinet applications on page 38.
- FIC supports OTP via email or SMS as an MFA method for end users with FAC as an application, as long as the realm associated with the FAC (or end-user) MFA method is provisioned properly.

If you use FAC as an authentication client of FIC, you can complete the following steps to get started with FIC:

1. Registering your FIC subscription on page 29.
2. Upgrading FortiAuthenticator OS on page 30.
3. Logging into the FortiIdentity Cloud portal on page 30.
4. Activating FAC for FIC service on page 30.
5. Adding an admin user for FIC service on page 31.
6. Adding a local user for FIC service on page 31.
7. Enabling FIC service for remote users on page 32

Registering your FIC subscription

Upon purchasing your FIC service subscription, you'll receive via email a license certificate (a .PDF file) with a registration code in it. Your first step is to register your FIC subscription on FortiCloud.

Be sure to register your FIC subscription to the same FortiCloud (FC) account where your FortiAuthenticator (FAC) is registered.

To register your FIC subscription:

1. Have your FIC license certificate ready.
2. Launch your web browser.
3. Log into FortiCloud at https://support.fortinet.com/ with your FortiCloud username and password.
4. On the FortiCloud banner across the top of the page, click *Services* to open the drop-down menu.
5. Click *Asset Management*.
6. From the side menu, click *Register Product*.
7. Follow the prompts onscreen to complete the registration.

Upgrading FortiAuthenticator OS

FortiIdentity Cloud requires FortiAuthenticator (FAC) version 6.4.0 or later, or 6.5.0 or later. Be sure to upgrade your FortiAuthenticator to a supported version, if needed.

To upgrade your FAC OS:

1. Log into your FAC device.
2. From the menu (on the left), click *System>Firmware*.
3. Click *Browse* to browse for FAC version 6.4.x/6.5.x.
4. Follow the instructions onscreen to complete upgrading your FAC OS on the device.

Logging into the FortiIdentity Cloud portal

All FortiCloud (FC) registered users can access the FIC portal. If your organization has multiple FIC accounts, you'll see a list of your FIC accounts after you sign in on FortiCloud. You can then select an account to open it on the FIC portal. During a session, you can switch from one account to another using the Account drop-down menu at the bottom of the main menu.

Access to FIC is managed by FortiCloud SSO authentication via FortiAuthenticator (FAC). Upon receiving your login request, the system redirects you to FortiCloud which is the FortiCloud (FC) SSO page. From there, you must use your FC master account username and password to log in. After authenticating your identity using multi-factor authentication (MFA), the system grants you access to the FIC portal.

To log in to the FIC portal:

1. Open your web browser, point to https//fic.fortinet.com, and press the *Enter* key on your keyboard.
2. In the upper-right corner of the page, click *LOGIN*.
3. Enter your FC master account username and password, and press *LOGIN*.
   Once you've logged in, the FortiIdentity Cloud landing page opens, showing your FIC account (or a list of accounts if your organization has multiple FIC accounts).
4. Click your account or one of your accounts to open it.
   The FIC *Dashboard* page opens.

Activating FAC for FIC service

In order for your FortiAuthenticator (FAC) users to take advantage of the MFA feature provided by FortiIdentity Cloud, you must make sure that FIC service is enabled on your FAC devices.

By default, FIC service is enabled on FAC. If, for some reason, FIC is not enabled on the FAC, you must manually enable it to proceed.

Only the FAC admin user can activate FIC service on FAC devices.

Adding an admin user for FIC service

You may add an FAC admin user for FIC service using the following procedures:

1. From the FAC menu, click *Authentication>User Management>Local Users*.
2. From the top of the page, click *Create New*.
3. Specify a unique username.
4. For *Role,* select the *Administrator* radio button.
5. Click *Full permission* to enable it.
6. Click *OK*.The page refreshes.
7. On the *Edit User* page (depending on your FAC version), select *One-Time Password (OTP) authentication > FortiToken > Choose Hardware or Mobile > Choose Default, Email or SMS* if Mobile was chosen.
8. Click *User Information*.
9. Enter the user's email address or SMS information as needed based on the option you chose earlier.
10. Click *OK*.

Names of FIC users created on FAC show up on the FIC GUI and in email notifications with some unwanted characters in corner brackets before and after them.

Adding a local user for FIC service

Once you are sure that your FIC service is enabled on your FAC device, you can create local FAC users and enable them for FIC service using the following procedures:

1. From the FAC menu, click *Authentication>User Management>Local Users*.
2. From the top of the page, click *Create New*.
3. Specify a unique username.
4. For *Role,* select the *User* radio button.
5. Click *OK*.
6. On the *Edit User* page (depending on your FAC version), select *One-Time Password (OTP) authentication > FortiToken > Choose Hardware or Mobile > Choose Default, Email or SMS* if Mobile was chosen.
7. Click *User Information*.
8. Enter the user's first name and last name.
9. Enter the user's email address or SMS information as needed based on the option you chose earlier.
10. Click *OK*.

Once a user is created on FAC, information about the user automatically appears on the *Users* page of the FIC portal. If the user is the first user of the FAC that you've added for FIC service, the FAC device appears on the applications page as well.

FAC supports local and remote users. FAC remote users are those imported into FAC form an LDAP/AD or RADIUS server. They are stored in FAC without their passwords (which are still kept in the remote directory). Such imported users are stored in FAC as Remote Users, and are unique per directory.

Names of FIC users created on FAC show up on the FIC GUI and in email notifications with some unwanted characters in corner brackets before and/or after them.

Enabling FIC service for remote users

If you already have some remote users configured, you can also enable FIC service for those remote users (e.g., remote LDAP, RADIUS and SAML users).

For more detailed configuration instructions regarding remote servers and users, refer to the FAC cookbook https://docs.fortinet.com/document/fortiauthenticator/6.4.0/cookbook.

1. From the FAC menu, click *Authentication>User Management>Remote Users*.
2. On the top right, select the type of user (e.g., LDAP, RADIUS, SAML, etc.).
3. Click in the row of the user you wish to edit.
4. On the *Edit User* page (depending on your FAC version), select *One-Time Password (OTP) authentication > FortiToken > Choose Hardware or Mobile > Choose Default, Email or SMS* if Mobile was chosen.
5. Click *User Information*.
6. Enter the user's email address or SMS information as needed based on the option you chose earlier.
7. Click *OK*.

Main features

FortiCloud SSO

Integration with FortiCloud provides unified single sign-on (SSO) access to all your Fortinet cloud service offerings.

Free trial licenses

FIC offers a 30-day free trial license which can support up to five FIC end users and five realms for FortiCloud accounts. (SMS messages are not included.)

Time-based annual subscriptions

FIC offers time-based subscriptions that are stackable and co-termed, giving you the flexibility to scale up your FIC MFA service with ease.

Authentication and Management logs

FIC provides comprehensive authentication and management logs to keep you informed of all authentication and management events that have happened in your account.

Global administrator and sub-admin support

FIC now enables the global admin to create sub-admin accounts to better allocate and manage resources across all the accounts under management.

Access to all accounts by admin users

Global admins are able to access all FIC accounts belonging to their organization, choose which of their accounts to open upon login, and switch to any of their other accounts during the session.

Realm support

FIC enables admin users to create realms to effectively allocate resources and better manage end users.

Multi-factor authentication (MFA) for FGT and FAC devices

FIC provides a cloud-based MFA solution for all your Fortinet products, such as FortiGate (FGT) and FortiAuthenticator (FAC), and third-party web apps as applications.

Integration with FOS

FIC works seamlessly with FortiOS (FOS). For more information, refer to Compatible Fortinet applications on page 38.

Support for MFA bypass and new token request

FIC admin users can allow end uses to bypass MFA and request new tokens on behalf of end users easily from the GUI.

Automatic lockout of users for excessive MFA failures

FIC automatically locks out end users when they have breached their specified MFA failure threshold, ensuring security and integrity of your account.

Temporary token

You can enable your end users to use temporary tokens for MFA authentication when they do not have their authentication devices with them, while leaving their existing authentication methods intact. If an end user forgets to carry his/her FTM device around and needs to log into the firewall or SSLVPN using MFA, you can enable the temporary token for the user and set the expiration time. The user can log into the firewall or SSL VPN using the temporary token until it expires. The user can get temporary tokens by email or SMS.

Disabling MFA after account disabled

FortiIdentity Cloud can enable existing users in disabled accounts to bypass MFA. There have been many customer cases when users are locked out due to expired licenses or exceeded quotas. With this feature, you are able to delete users by performing a user sync or delete a particular user. In the portal, you are able to change user settings, including bypass MFA. After MFA is bypassed, auth requests should succeed.

Secure, cross-platform token transfer

You can securely transfer your FIC and third-party tokens between iOS and Android devices using the FortiToken Mobile (FTM) app.

Support for remote FortiGate users

You can configure FortiGate wildcard LDAP users to use FIC for MFA.

Auto log-out

FIC automatically logs out a user if the GUI has been idle for more than ten minutes, safeguarding the security and integrity of your asset on FIC.

Real-time usage statistics

You can view daily, monthly, and current usage data easily from the GUI.

Support for HA clusters

FIC supports FGT and FAC HA cluster configuration. You can add or remove auth devices to or from the FIC portal. You can view your FGT and FAC devices in any cluster from the applications page.

Support for custom logo

You can upload custom logo images to replace the default Fortinet banner at the bottom of the FTM app on your end users' mobile devices.

Support for multiple MFA options

FIC offers four MFA methods —FTM (FortiToken Mobile), email, SMS, and FTK (FortiToken, which is a hardware token).

Auto-alias by email

Many FIC end-users have different usernames in different applications and different domains. For the same token, a single FIC user may have different usernames in different FIC applications. FIC now allows for different usernames to be attributed to the same user (i.e., same person) so that only one token (FTM or FTK) needs to be assigned to that same user. It does this by providing an Auto-alias by Email option, which, once turned on, enables FIC to automatically put usernames into an alias if they use the same email address.

Realm-based user quota

Global admins can allocate user quota by realm to effectively manage their assets and end users.

If you are a Managed Security Service Provider (MSSP), you can split out your user quota to sub-accounts. Sub-account holders can create their own passwords and have their private login portal. They can use MFA, bypass, block, and realm configurations to manage their own end users. An MSSP can manage all their sub-accounts from the FortiIdentity Cloud portal.

Export of logs in .CSV

You can export FIC authentication and management logs in .CSV format for record-keeping and sharing.

SMS usage

The *SMS Log* page enables you to view your SMS usage.

Device ownership transfer

You can transfer device ownership with or without device data.

Replay protection

You have three (high, medium, and low) levels of MFA replay protection to choose from when configuring realm settings.

Effective end-user management

You can effectively monitor and manage your end users from the FIC portal.

Support for pagination

Pagination enables you to limit the number of records returned in each API request. This ensures that the system can respond to API requests faster, and present information in a more organized and user-friendly manner. For more information, refer to the FortiIdentity Cloud API.

SMS usage restriction

This mechanism prevents users from using FIC's SMS function if the destination is a restricted country by law. Once implemented, FIC will automatically pop up a message on its GUI, informing users of the restriction when it detects the SMS messages that are being sent to a restricted country.

IdP Proxy

Identity Provider Proxy (IdP) combines the capability of IdP and Service Provider (SP) in one. With FortiIdentity Cloud providing the SAML and OIDC interface, applications can be part of the FIC SaaS service and take full advantage of the existing SSO protocol to integrate with not only the Forti-ecosystem, but third-party applications and IdPs as well.

Passkeys

FIC supports passkeys using Webauth, which is a core component of FIDO Alliance's FIDO2 set of specifications. The web-based API allows websites to update their login pages to add FIDO-based authentication on supported browsers and platforms. This enables end users to leverage common devices to easily authenticate to online services in both mobile and desktop environments.

SCIM

SCIM provides a standardized, secure methodology for exchanging information between IT systems. It ensures interoperability across domains without expensive custom integrations. SCIM auto-provisioning can free up valuable IT resources for critical tasks while boosting productivity across the entire organization.

Migrate FTM tokens from FortiGate and FortiAuthenticator

FortiGate and FortiAuthenticator (FAC) administrators can migrate their FTM tokens to FIC. Upon completion of migration, FIC automatically generates a one-year free transfer license for the migrated account to cover the number of end users corresponding to the total number of FTM tokens that have been transferred. For more information, visit Migrate FTM tokens to FortiIdentity Cloud.

Batch-add User

This features enables admin users to batch-add end-users from different realms manually or by importing end-user information in .cvs files.

User group

This feature enables admin users to set up authorization groups of users, grant different access rights to users by user group.

Integration with Microsoft Entra ID

FIC now can be configured as an Entra MFA external authentication method (EAM) method provider. See Configuring FIC as Microsoft Entra external authentication service provider on page 68.

End-user Portals

This feature enables end users to update their profiles, phone numbers, and MFA methods and register FIDO tokens on their own based on the permissions granted by the administrator. See Managing End-User Portal on page 172.

FortiSASE VPN user SSO through FortiIdentity Cloud

Working in tandem with FortiClient, this feature enables customers to use FIC MFA to manage their FortiSASE VPN users SSO. See Enabling FortiSASE VPN users to use FIC MFA on page 74.

Allow end users to use additional MFA methods

This feature enables end users to use MFA methods other than the default set in their realm to authenticate, especially when they are unable to access or use the default MFA method, for example, mobile phones. If email is chosen as an additional MFA method, FIC will automatically switch from SMS to email when SMS service becomes unavailable (for instance, due to no or inadequate SMS quota or geographical limitation or restrictions). See .

Support for Local IdP

FortiIdentity Cloud's local IdP feature enables end users to log into their End-user Portal and applications using their user username and password local to FortiIdentity Cloud rather than any external identity provider, such as Google, Azure, etc. For more information, see Local IdP.

Support for OIDC Provider

FortiIdentity Cloud can be configured as an OpenID Provider (OP) for authenticating users and issuing tokens to a Relying Party (RP). When configured in tandem with its local IdP, FIC can be the authentication source and provide end-to-end OP functionality. For more information, see FortiIdentity Cloud as OIDC provider on page 76.

Allow rooted device

This features enables administrators to effectively manage rooted devices in their environment. For more information, see General settings on page 231.

Support for subdomain for End-user Portal

This feature enables you to create the End-user Portal using your custom URL rather than the URL generated by FortiIdentity Cloud. For more information, see Configuring End-User Portal on page 172.

Compatibility

Compatible Fortinet applications

FortiIdentity Cloud 25.3.c works in tandem with the following Fortinet applications:

Fortinet Application	Application Version
FortiOS	• 7.0.0 or later • 7.2.0 or later • 7.4.0 or later • 7.6.0 or later
FortiClient for Windows	• 7.0.0 or later
FortiClient for MacOS	• 7.0.0 or later
FortiClient for Linux	• 7.0.0 or later
FortiAuthenticator	• 6.4.0 or later • 6.5.0 or later
FortiSandbox	• 3.2.0 or later
FortiADC	• 7.1.3 or later • 7.2.1 or later • 7.4.0 or later • 7.6.0 or later
FortiManager	• 7.2.2 or later • 7.4.0 or later
FortiAnalyzer	• 7.2.2 or later • 7.4.0 or later • 7.6.0 or later
FortiPortal	• 7.0.0 or later
FortiPAM	• 1.2 or later 1.3.0 or later 1.4.0 or later

Fortinet Application	Application Version
FortiToken Mobile for iOS	• 5.5.1 or later
FortiToken Mobile for Android	• 5.4.1 or later
FortiToken Mobile for Windows	• 5.0 or later

- FortiIdentity Cloud does not work well with FortiOS 7.0.2. We recommend upgrading to FortiOS 7.0.5 or later for best performance.
- Using IPsec with FortiClient as a SAML application with FIC is not supported on FortiClient versions 7.2 and earlier.

Supported browsers

FortiIdentity Cloudsupports the latest versions of the following web browsers:

- Google Chrome
- Mozilla Firefox

Other web browsers may work as well, but have not been rigorously tested.

Important notes

This section discusses some important notes regarding the use of FIC.

Trial account API request limit

FIC offers limited access to its REST APIs for its trial customers. Trial customers can test out FIC's Web application APIs and IdP-related APIs for free as long as they abide by the following restrictions:

- Each trial account can make up to 60 API requests with a 5-minute period.
- Any request exceeding the aforementioned limit will be rejected. In such a case, the user will get a "`429 Too Many Requests HTTP`" error, along with the message "`Trial request limit exceeded. Please retry after 5 minutes.`"
- Trial users who exceed 240 API requests within a 5-minute period risk having their accounts disabled altogether.

The same token for the same user on multiple applications

FortiIdentity Cloud allows the same end-user created on two or more applications to use the same FortiToken Mobile (FTM) or FortiToken (FTK) token for its services, as long as:

- The applications are FIC-supported apps, such as Fortinet products or third-party Web apps.
- The applications are assigned to the same realm in FortiIdentity Cloud.

The same end-user created on the applications can be of different usernames. For more detailed information, see A single FIC user in multiple applications on page 41.

A single FIC user in multiple applications

A given FIC end-user can be in two or more applications (FGT and/or FAC devices), resulting in the so-called "a-single-user-in-multiple-appications" situation. For example, User-1 can be in FGT-1 and FGT-2. An FIC admin user is able to see all applications (FGTs) for a given end-user on the FIC portal.

You must keep the following two important points in mind when handling such a situation:

(1) When you disable (remove) User-1 from FGT-1, it still exists in FGT-2. As a result, User-1 still remains in FIC. The only way to remove User-1 from FIC is to remove it from both FGT-1 and FGT-2.

(2) Suppose you have enabled User-1 for FIC in FGT-1 and FGT-2, and User-1 has a token from FIC. You disable User-1 in FGT-1, but leave it still enabled in FGT-2 so that it still exists in FIC. Later on, if you enable User-1 again without assigning a new FIC token to it, User-1 will continue to use the same FIC token that it has used before. Now suppose, instead of enabling User-1 again in FGT-1, you assign SMS from FGT-1 (an FGT internal feature that is not available in FIC) as the MFA method for User-1. This is what is going to happen: If User-1 attempts to log into FGT-1, the user will get an SMS from FGT-1; but if User-1 attempts to log into FGT-2, the user will have to use the FIC token.

FortiIdentity Cloud uses the multi-realm concept. As a result, two identical end-users can co-exist on two different applications assigned to two different realms.

Admin accounts and realms

The FIC account of a customer organization that has logged in to the FIC portal first and/or your master account in FortiCloud will be automatically assigned the FIC global admin role; all accounts under your FortiCloud master account will be assigned the sub-admin role by default, with no realm assigned (including the default realm) to them, and therefore will not be able to see any FIC data. The global admin must create admin groups and map the sub-admins with realms in order for them to view and manage realm resources.

For more information on how to create admin groups and grant permissions to sub-admins, see Managing admin groups on page 97.

Supported OTP hard tokens

FortiIdentity Cloud supports FortiToken (FTK) FTK-200B and FTK-210 OTP hard tokens only. The FTK-200CD tokens (with token serial number prefix FTK-211) are NOT supported.

Supported FIDO security key

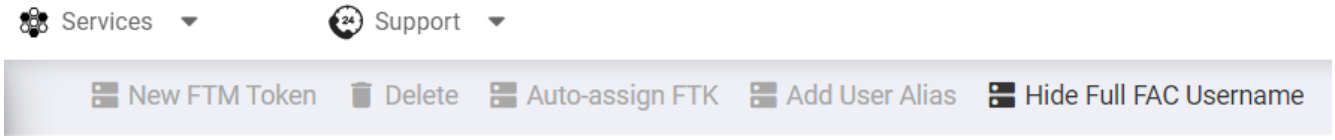
FortiToken 410 (FTK-410) is required for use with Passkey. For more information about FTK-410, visit FortiToken 410.

No SMS MFA with FAC as LDAP server

FortiIdentity Cloud (FIC) does not support SMS MFA authentication for end users configured on FortiAuthenticator as a native LDAP server, because a FortiAuthenticator native LDAP server does not allow FIC to query users' phone numbers.

FAC users' name issues on FIC GUI

Names of FIC end-users created on FortiAuthenticator (FAC) earlier than v.6.6.0 show up with prefixed and suffixed characters in corner brackets on the FIC GUI and in email notifications. This is because FAC differentiates the same username populated by multiple user sources to FAC. To remove the prefix and the suffix from a FAC username, select the FAC username and click the *Hide Full FAC username'*button.



How to use FortiClient

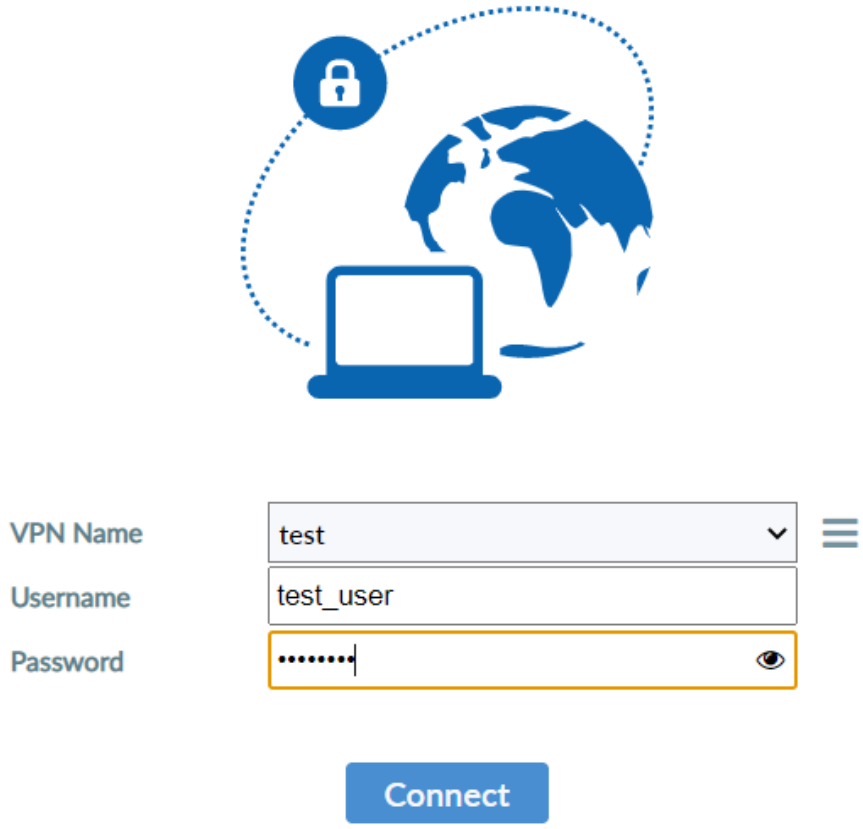
FortiIdentity Cloud supports FortiClient for both auto push and manual OTP. To use FortiClient with FortiIdentity Cloud, you must make sure that *Notification*is enabled on the FortiToken Mobile app on your mobile device. For

auto push, you must also ensure that *Enable push* is selected in *Settings>Realm>FTM* on the FortiIdentity Cloud portal.

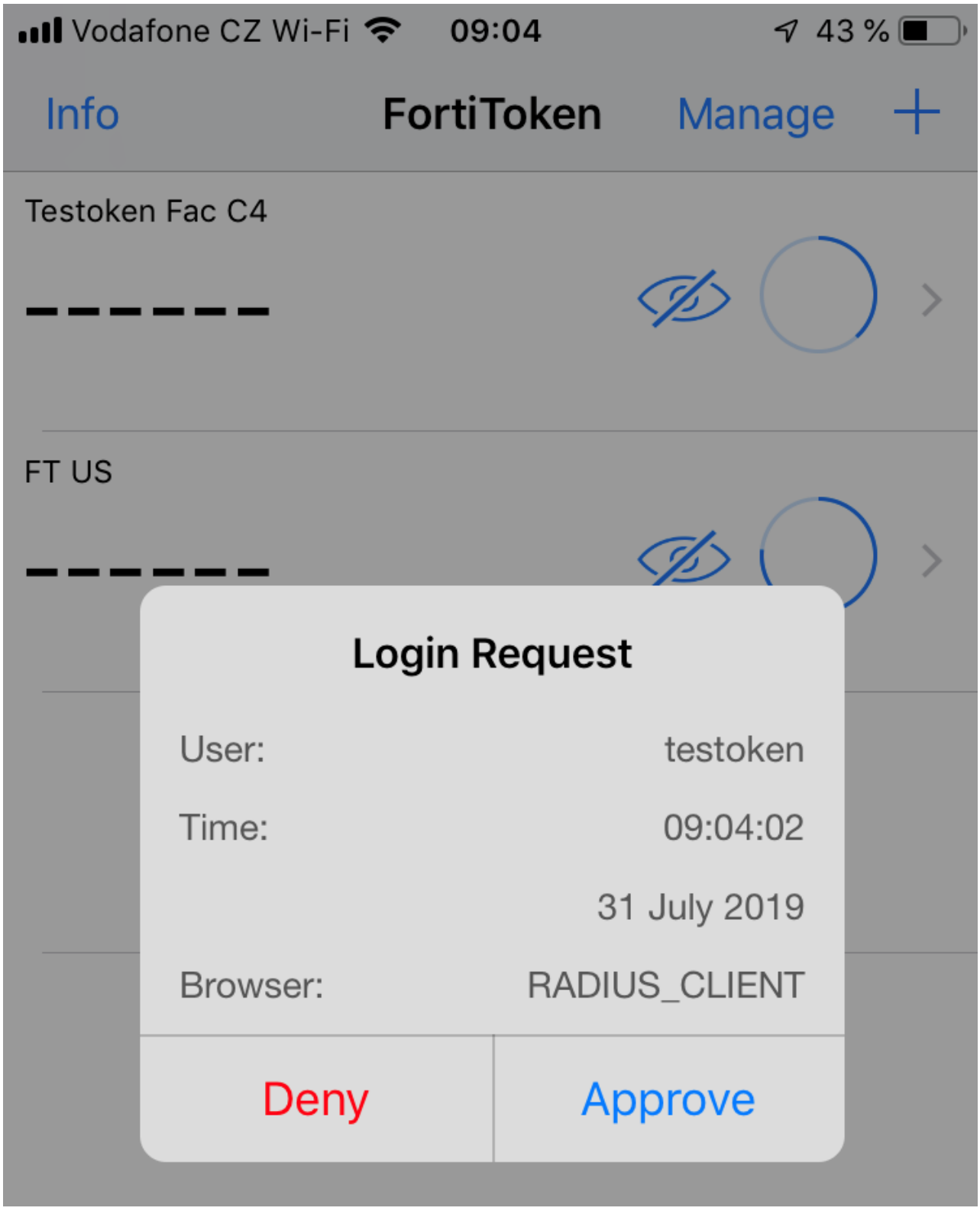
Use auto push

Upon entering your username and password, do the following:

1. On FortiClient, log in with your username and password.



2. On your mobile device, press ***Approve.***

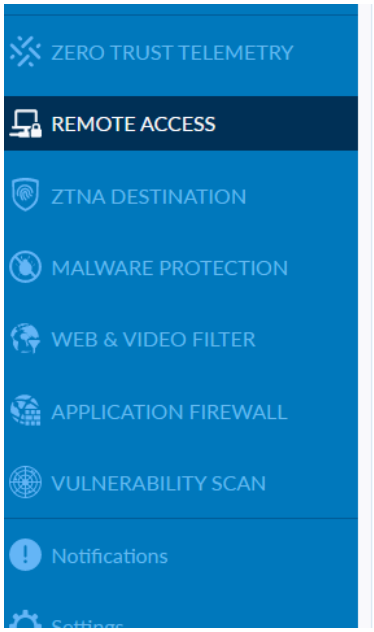


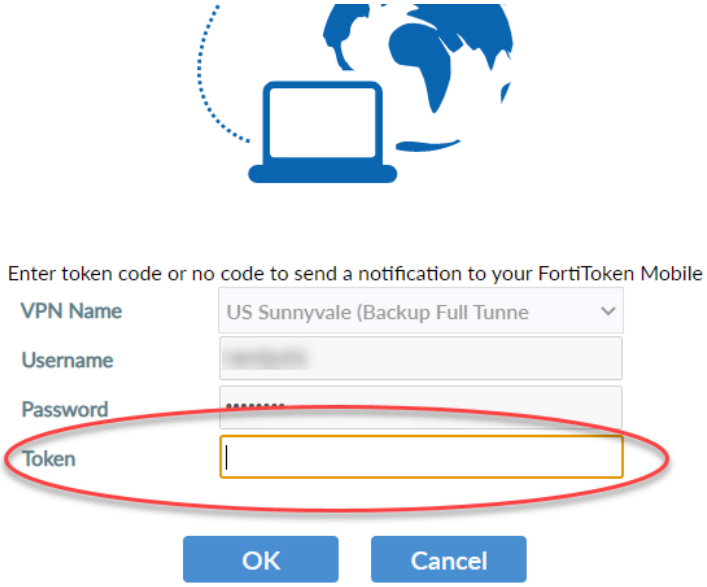
3. Wait for FortiClient to complete the remote access login.

Use OTP

Upon entering your username and password, do the following:

1. In the Token window on FortiClient, enter the OTP obtained from your mobile device, and click *OK*.





2. Wait for FortiClient to complete the remote access login.

Enabling/Disabling FIC end-users on FortiGate

If you have end-users with FortiIdentity Cloud for 2FA enabled on a FortiGate, they will remain on the FIC portal if you disable them on the FortiGate because FIC keeps a record of its end users regardless of the their status on FGT. If you want to remove the end users from the FIC portal, you must do one of the following:

- Delete the end users from the FGT.
- Revoke the tokens from the end users.
- Delete the end users from the FIC portal (**Note**: This method does not delete the end users on the FGT, so it is best to delete them from the FGT.)

Account disablement and closure

FortiIdentity Cloud will disable an account 30 days after its license has expired, and close the account 90 days after it has been disabled. Before disabling or closing the account, FIC will send out email notifications to the customer 30,14, and 1 day(s) in advance about the pending account expiration or closure. To avoid service

interruption, it is your responsibility to ensure that your account is in good status, and renew your license before it expires.

FortiToken Mobile

FTM is an OATH-compliant, event- and time-based, one-time password (OTP) generator application for mobile devices. It generates OTP codes on your mobile device without the need for a physical token. It allows you to install Fortinet tokens and third-party tokens, including tokens for multi-factor authentication used by Dropbox, Google Authenticator, Amazon, Facebook, Microsoft, Yahoo, Snapchat, PayPal, eBay, and LastPass.

This section covers the following topics:

Supported FortiToken Mobile apps

This FIC release supports FTM for mobile devices running on the latest versions of Apple iOS or Google Android, as described below.

FTM app	Supported mobile OS	Supported devices
FortiToken Mobile for iOS 5.5.1 or later	Apple iOS 12 and later	iPhone and iPad
FortiToken Mobile for Android 5.4.1 or later	Google Android 10 and later	Android phone and tablet
FortiToken Mobile for Windows 5.0 or later	Windows 10 version 14393.0 or higher	Windows PC, tablet, and phone

You can download and install the app directly onto your Apple iOS or Google Android devices. No cellular network is required. If you do not have cellular service, use your WiFi access instead.

To get FTM for iOS:

1. Start your iOS device.
2. Go to **App Store**.
3. Search for **FortiToken Mobile**.
4. Download and install the app.

To get FTM for Android:

1. Start your Android device.
2. Go to **Google Play**.
3. Search for **FortiToken Mobile**.
4. Download and install the app.

To get FTM for Windows:

1. Start your Windows device.
2. Go to **Microsoft Store**.
3. Search for **FortiToken Windows**.
4. Download and install the app.

Activating FTM tokens

After your system administrator assigns you a token, you receive a notification with an activation code via SMS or email depending on the option your system administrator has chosen.

You must activate your token by the expiration date. Otherwise, you will have to contact your system administrator for the token to be reassigned for activation.

For more information, refer to Activating FortiToken Mobile on a mobile phone.

Activating third-party tokens

The steps for activating a third-party token are the same as those for activating a Fortinet token. Depending on the token vendor, you may be able to activate the token by scanning the QR code as well.

Please refer to our REST API QuickStart Guide for more information on how to create a third-party user https://docs.fortinet.com/document/fortiidentity-cloud/latest/rest-api/698584/get-access-token-and-create-users-from-web-apps.

Using FTM tokens

Upon opening the FTM app on your iPhone, your token will be visible on the app's home screen. The token is a 6-digit OTP which updates dynamically every 30 seconds.

If you have multiple tokens installed, they all show up on the home screen.

To use an FTM token:

1. From your iPhone, start the **FortiToken Mobile** app.
2. On the home screen, press and hold on an OTP code, and tap **Copy**.
3. From your iPhone, start FIC.
4. Log in with your username and password.
5. Paste the OTP code when prompted.

You should be able to log into FIC after you pass the MFA process.

For more information on FTM Push with CLI configuration for FortiGate, refer to: https://docs.fortinet.com/document/fortigate/7.2.4/administration-guide/927108/fortitoken-mobile-push.

Use cases

One Token shared by different applications

You can share the same token used by one end-user but with different applications. A single end-user can be defined by the same user name on different applications but in the same realm or the same email address on different applications. If multi-realm mode is enabled, the newly registered application will be assigned to a new realm; if multi-realm mode is disabled, the newly registered application will only be assigned to the “default” realm.

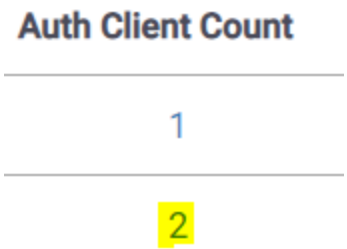
For example, if you have one user named “user1” with FIC MFA on FGT, you need to create a new user named “user1” with FIC MFA on FAC, “user1” can share the first token without allocating a new token for the “user1” on FAC if the application for FGT and FAC are under the same realm on FIC. Having the same user name is the default condition for sharing the same token between different applications on FIC. The same email address can be set for token-sharing from FIC as well.

This use case also applies when you have the same auth device but the auth device serial number is changed. If there are multiple users with FIC MFA on one application, but the application serial number is changed for any reason, the users can be synced to FIC with the new serial number under the same realm as the application with the preceding serial number. Then all users can keep the previous token without going through the re-activation process.

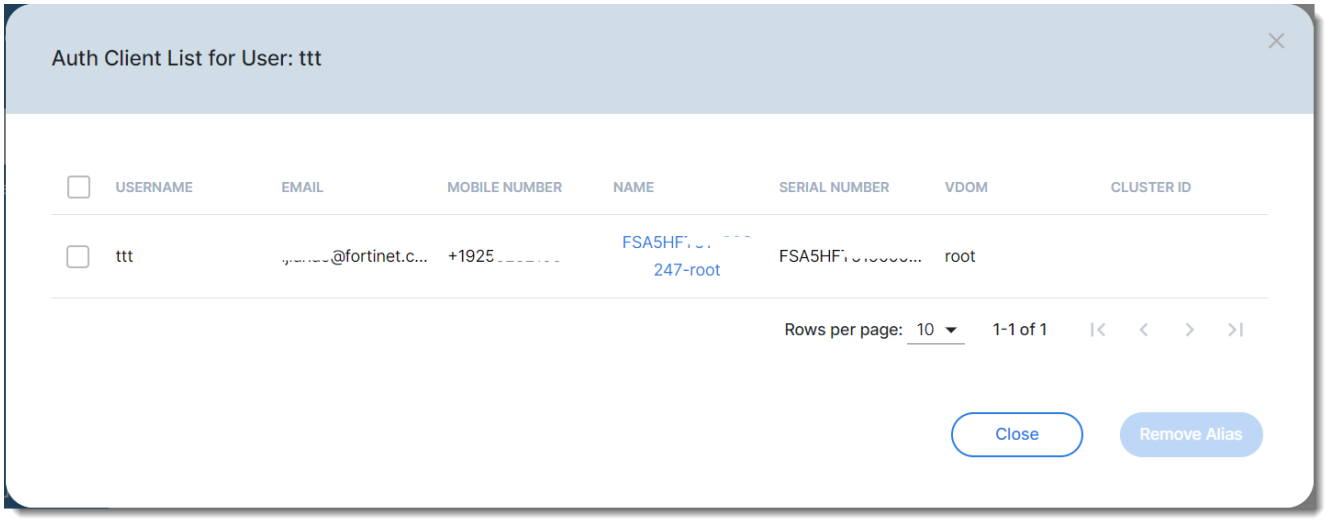
If you are trying to add a new FortiGate and are having difficulties with getting the new FortiGate’s application(s) to show up, it may help to use the `exec fortiidentity-cloud update` command in the CLI on the new FortiGate.

1. Create a user “user1” in the application “client1”, which is assigned under the realm “realm1”. For more information, see https://docs.fortinet.com/document/fortiidentity-cloud/latest/admin-guide/367002/add-a-local-user-for-FIC-service.
2. Activate the token in the FortiToken Mobile.
3. Create a user with the same username “user1” in another application “client2”, which is also assigned under the same realm “realm1”. Note that if you are trying to assign the token on the FortiGate, there may be a warning message that says that you don’t have enough resources to add the new user. This is a false negative and you should still click “OK” after editing the user.
4. The activated token will also be assigned to the newly created user in “client2” which can use MFA login.

Once you have completed the steps above, the application count for the user should be higher than 1 and it should look like this:



And if you click the number, you should be able to see the details about the user having more applications under it:



Changing separate tokens to a single token

When you change the Multi-Realm Mode from *enable* to *disable*in FortiIdentity Cloud *(Settings>Realm>Multi-Realm Mode)*, the same user in different client applications (even with different usernames) will use the same

token. The following illustrates how switching Multi-Realm Mode from *enable* to *disable* will impact the behavior of FIC.

1. FortiGate1 with the serial number (FG200ETK1990xxxx) and FortiGate2 with the serial number (FG300ETK1990xxxx) are registered under the FC account (fortinet_account@gmail.com).
2. As long as the realm has enough resources, FIC will automatically create two realms: “FG200ETK1990xxxx-root” and “FG300ETK1990xxxx-root”, and FGT1 and FGT2 will be assigned to those two separate realms.
3. In this case, a user created in FGT1 named “Jack Talyor” is assigned one token, and a user created in FGT2 named “Jack Talyor” is assigned a new token. They are two separate users with the same username but use separate tokens.
4. If you want to switch to one-token login mode (Users with the same username use one token only), the FIC admin can move FGT1 and FGT2 to the same realm, for example, the “default” realm, from the two realms “FG200ETK1990xxxx-root” and “FG300ETK1990xxxx-root”.
5. The users will be merged on the *Users* page, the two users named “Jack Taylor” will be merged into one “Jack Taylor” and the application count will increase to “2”. The same token will be shared by the two users named “Jack Taylor”. By default, the token will be kept for the application migrated to the “default” realm first, and the token for the user in the second migrated application will be removed.
6. Right now, “Jack Taylor” will only need one token to log into the two FGT resources.
7. Additionally, if you want to always use one-token login mode, the FIC admin can navigate to Settings>Global and disable Multi-realm Mode. He must also move all existing applications to the same realm, for example the “default” realm.
8. After Step 7, the existing applications will use single token mode and newly assigned applications will also migrate to the “default” realm and use single token mode.

Independent token

When *Multi-Realm Mode* is enabled in FIC *(Settings>Global>Multi-Realm Mode)*, newly registered applications will be assigned to new realms. This function is very convenient for admin users who want to become an Managed Security Service Provider (MSSP).

1. FortiGate1 with serial number (FG200ETK1990xxxx) and FortiGate2 with serial number (FG300ETK1990xxxx) are registered under the same FC account.
2. As long as the realm has enough resources, FIC will automatically create two realms: FG200ETK1990xxxx-root and FG300ETK1990xxxx-root, and FGT1 and FGT2 will be assigned to those two separated realms.
3. In this case, a user created in FGT1 named “Jack Talyor” is assigned one token, and a user created in FGT2 named “Jack Talyor” is assigned a new token. They are two separate users with the same username but use separate tokens.
4. If the two “Jack Taylors” exist in two realms, some events could be confusing. For example, if “Jack Taylor” is deleted from FGT1, the “Jack Taylor” still exists in FIC. This scenario looks like "Jack Taylor" has never been deleted on FGT1. In fact, the “Jack Taylor” is no longer in FGT1, but only exists in FGT2.
5. Solution: Log into FGT2 and delete “Jack Taylor”. Then execute the console command “exec fortiidentity-cloud sync” in FGT. This will remove the user “Jack Taylor” in FIC. After deleting the user in FGT2, assign application FGT1 and application FGT2 to the same realm, for example, the “default” realm. This will prevent the situation from happening.

Auto-Alias features—using the same email address

Many FIC end users with the same email address have different usernames in different applications and different domains. For the same token, a single FIC user may have different usernames in different applications. FIC allows for different usernames to be attributed to the same user (i.e., same person) so that only one token (FTM or FTK) needs to be assigned to that same user. It does this using its auto-alias by email option.

Auto-alias by email is disabled by default, but you can enable it using the following procedures:

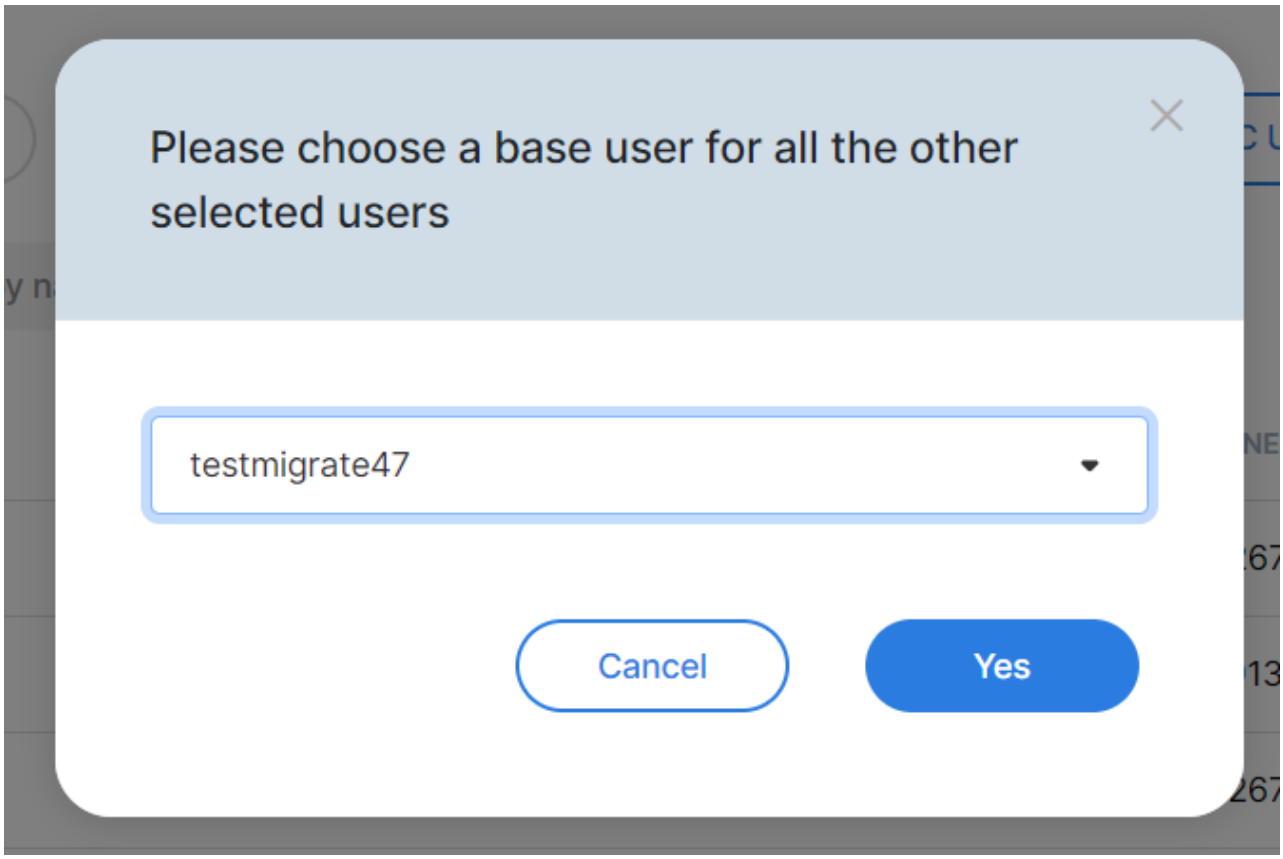
1. Click *Settings>Realm*.
2. Scroll down until you see the *Auto-alias by Email* option, and enable it.

Once the *Auto-alias by Email* feature is enabled, all newly created usernames with the same email address are automatically set as an alias under the same username. The existing usernames with the same email address will not be grouped into an alias, but you can manually set up alias users. See Managing users on page 103.

It is important to note that aliased users must be in the same realm. Usernames with the same email address are still set as unique users if they are in different realms, even when the auto-alias feature is enabled.

FIC also allows you to set up user aliases manually. In this way, the users are not required to have the same email. To enable this feature, just follow the steps below:

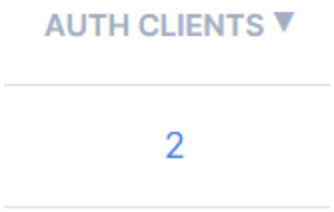
1. Click *User Management >Users*.
2. Select any number of users in the same realm.
3. Click *Add User Alias* on the top of the page.
4. Select the base username when prompted, and click *Yes*.



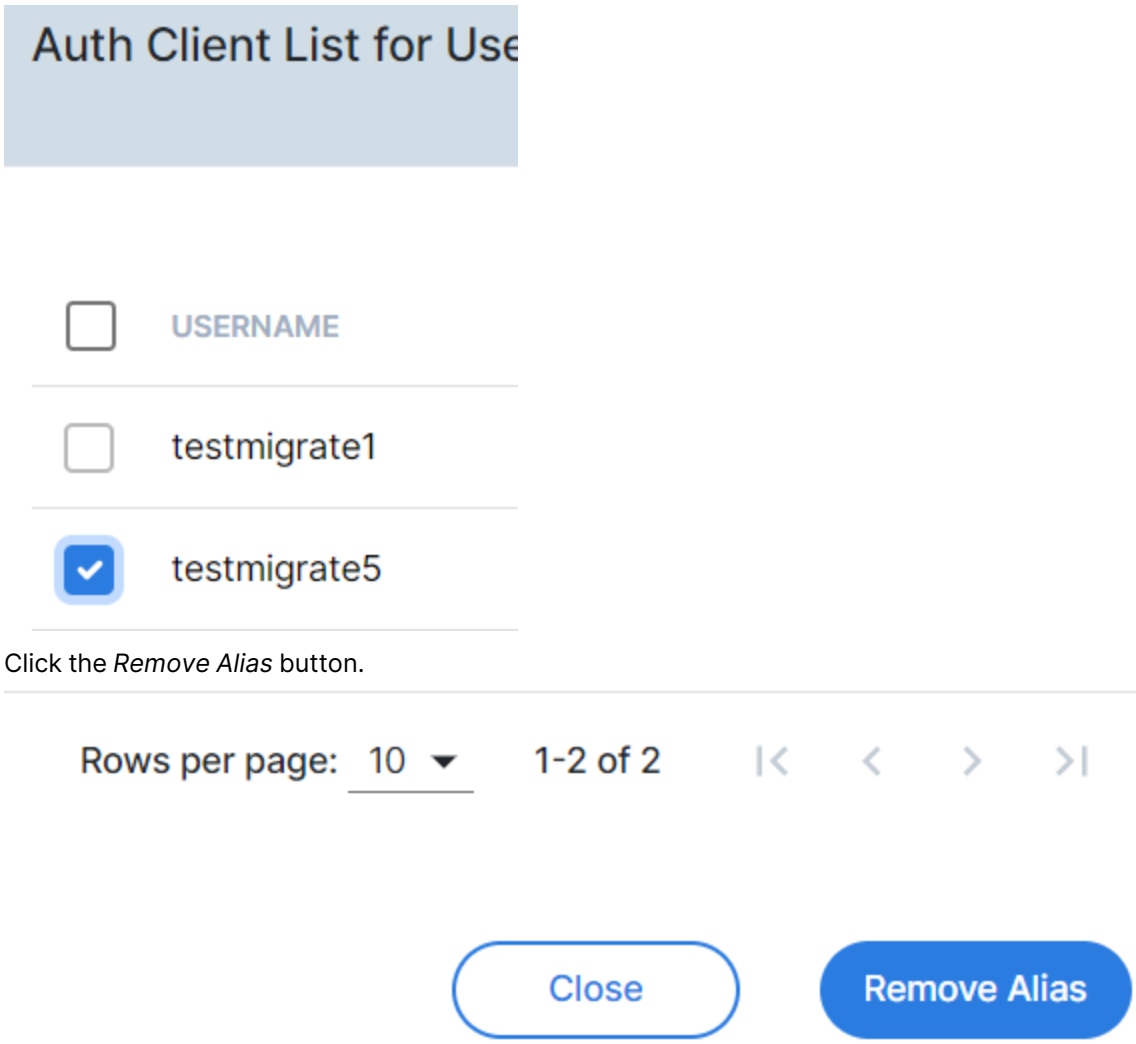
Once the user alias is formed, the base user's username changes to boldfaced and the application Count will be increased based on how many users are selected in Step 2.

To remove the user aliases that have different email addresses:

1. Find any user alias you want to remove, and click the number in the application Count column.



2. Select any users you want to remove from the user alias group by clicking the checkbox.



3. Click the *Remove Alias* button.

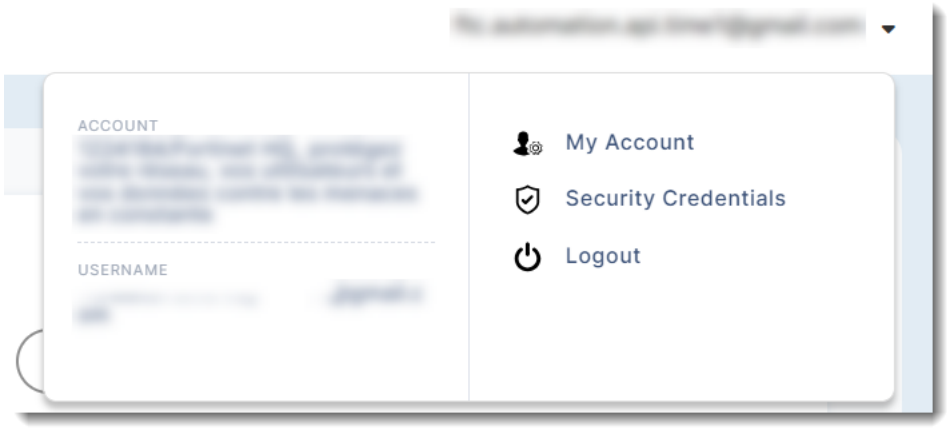
To remove the user aliases that have the same email address, be sure to disable the *Auto-alias by Email* option first in the *Settings>Realm* page. Once the auto-alias feature is disabled, the steps are the same as before.

Spliting user quota to different realms

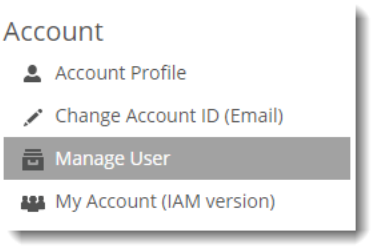
Fortildentity Cloud enables you to split out user quota to sub-accounts. Sub-accounts can also use functions like MFA, bypass, block, and realm configuration. This is the so-called “Managed Security Service Provider” capability. The host account holder can create sub-accounts and assign user quotas to the sub-accounts. Each sub-account can create its own password and has its own private login portal. The account holder is the security service provider and can manage all of the sub-accounts on the Fortildentity Cloud portal.

To create a sub-account:

1. Log in to fic.fortinet.com using the host account holder's credential.
2. Click the username (email) in the top-right corner, and select *My Account*.

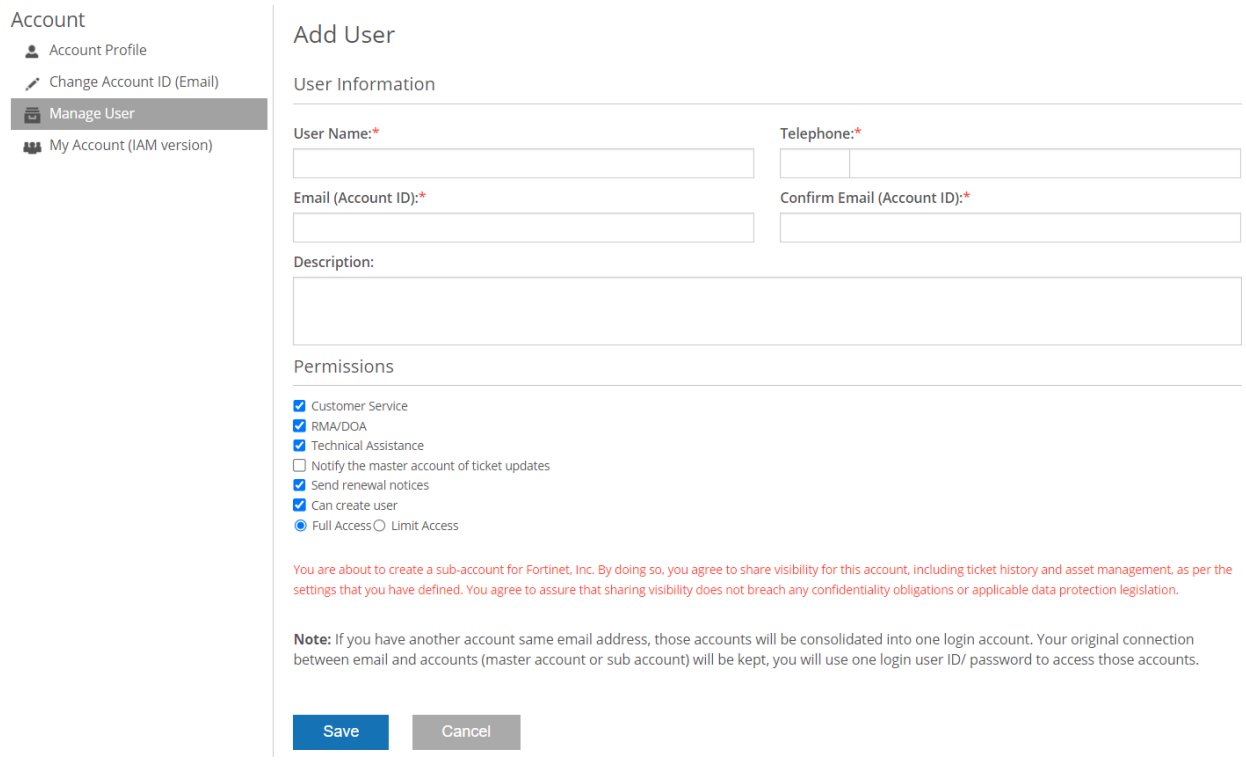


3. The browser will be navigated to support.fortinet.com automatically.
4. Click *Manage User* in the left sidebar to open the sub-users list.



5. In the upper-right corner of the sub-users list, click the Add user button.

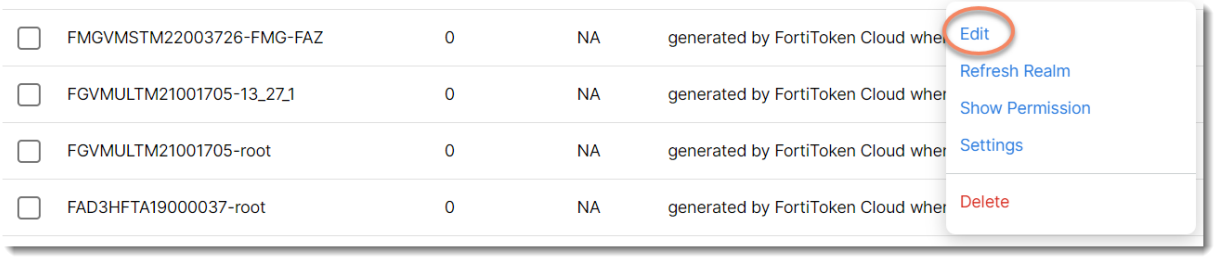
6. Enter the sub-user client information, including User Name, Email (Account ID), and Telephone. Additionally, enter some details, such as “purchased 10 user quotas”, in the Description field.
7. Select Limit Access, which allows you (the host account holder) to assign specific devices to this sub-user, like a FortiGate for creating users.
8. Click *Save*.



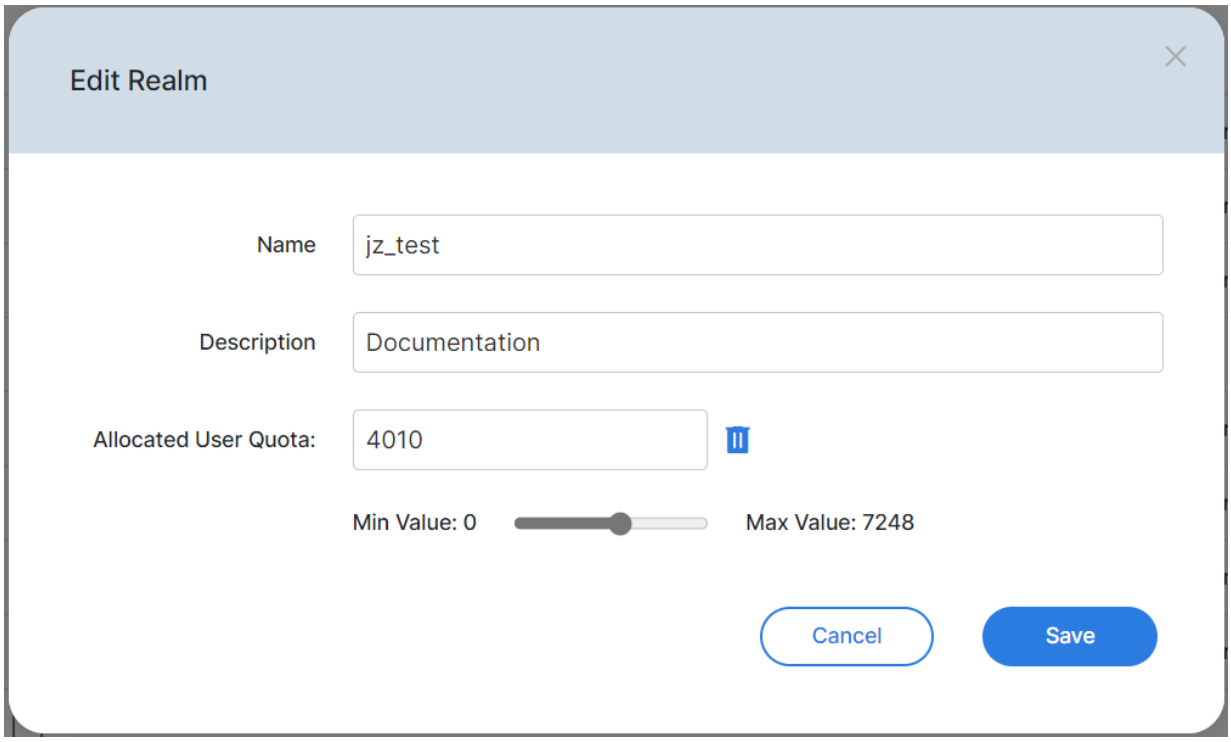
9. The sub-user clients will receive an email, asking them to create their own passwords for logging into fic.fortinet.com.
10. After sub-users are created, the host account holder can assign resources to sub-users, including user quotas, realms, and applications. For more details of assigning resources, see Managing admin groups on page 97.

The following steps show how to use this feature:

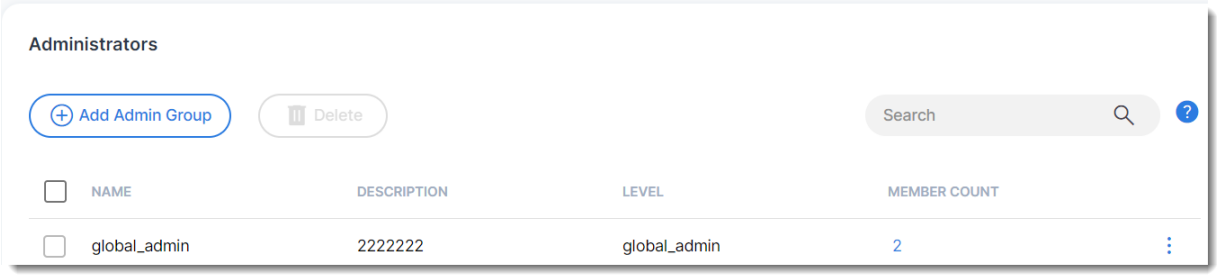
1. The host account holder creates a sub-user “subuser1” by using the provided client’s email. Clients can use their own email and password to log into FIC.fortinet.com, and can see the user quota assigned to them by the host account holder.
2. The host account holder can assign a user quota to a client in FIC:
   a. Navigate to *User Management >Realms*, and click *Add Realm*.
   b. Mouse over the newly created realm, select *Edit* in the pop-up tool menu.



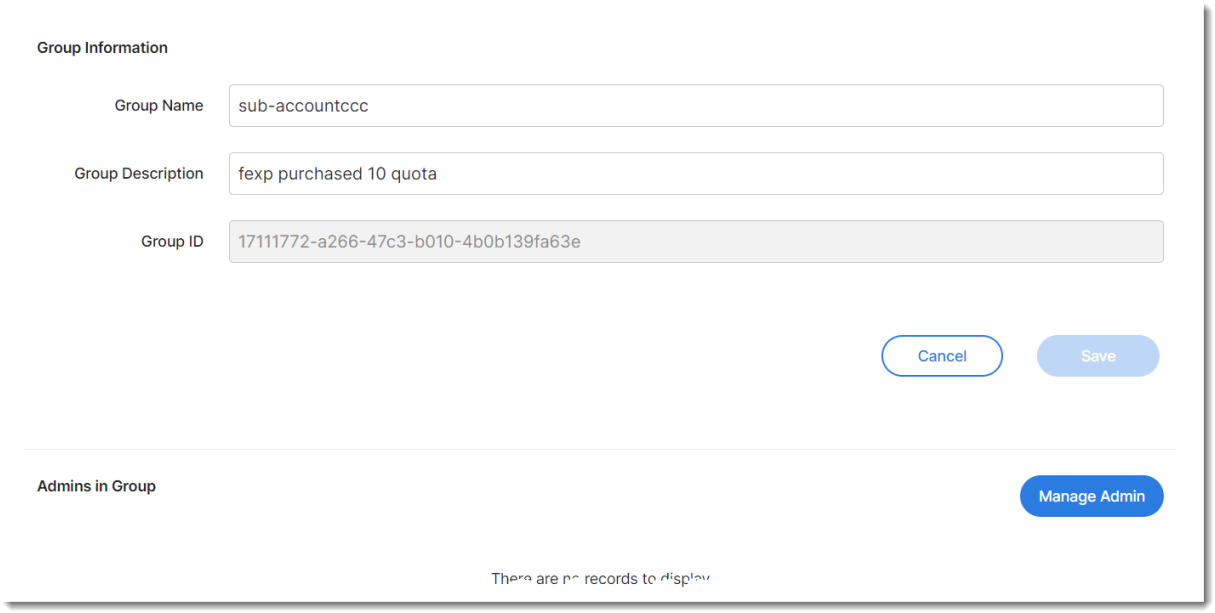
   c. Assign a user quota, and click *Save*.



3. The host account holder can assign the realms to a client in FIC:
   a. Navigate *Settings>Administrators*, and click *Add Admin Group*.



   b. Edit the admin group by clicking the new group name.
   c. Assign to this group the sub-account in *Admins in Group* and the realm in *Managed Realms* which were created in Step 2, and click *Apply*.

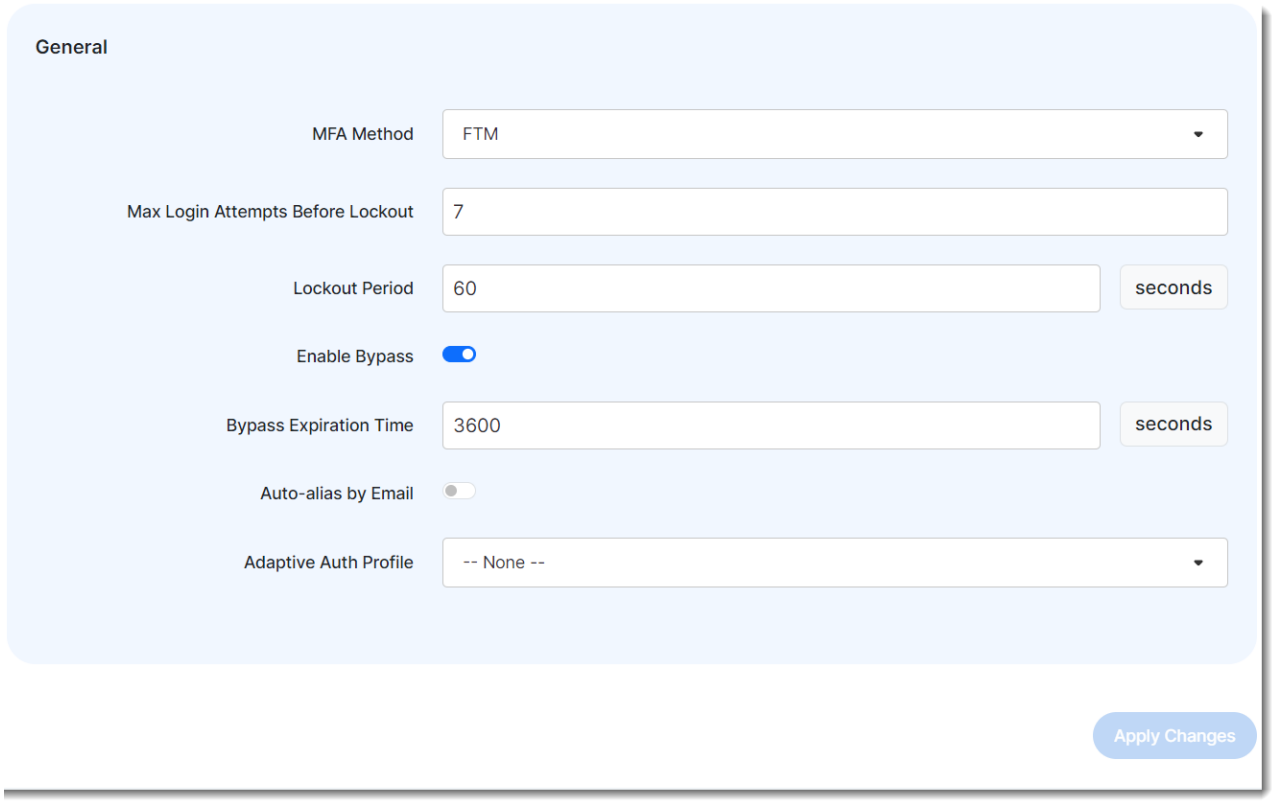


4. The host account holder can assign application to the client by selecting *Applications>FortiProducts*.
5. The client can see the users created by the host on the assigned FortiProduct, for example, FortiGate.

FIC account lockout (2FA)

You may find yourself unable to log in as an FGT admin. For example, Jack is an FIC admin and manages two FortiGates FGT1 and FGT2. He has enabled MFA for FGT admin login. When the FIC account is validated, everything is working fine. By missing the disabled email notification sent by FIC, Jack's FIC account is disabled. In this situation, the MFA login function is blocked. The behavior is that MFA login automatically fails after the user enters the correct username/password. Jack can't log into the FGT admin portal to see users who are enabled for MFA login authentication. Jack is allowed to log into his account and perform some limited activities, including enable bypass, setup bypass for users, and delete auth devices.

1. Log into the FIC portal, fic.fortinet.com, navigate to *Settings>Realm*, find the realm which contains the users for whom Jack wants to set up bypass, select *Enable Bypass,* and click *Apply Changes*.



2. Navigate to *User Management* > *Users*, find the FGT admin user, click *Edit*, and click *bypass* in the *Status* row.
3. Now, the FGT admin is not required to use MFA to log in anymore. Jack can log into the FGT admin portal and remove the FIC setup in the admin user until he renews the license.

Managing access to FIC

As an FIC global administrator, you can view your associated sub-accounts and assign realms to different admin groups for better realm management. For example, you can manage your headquarters realm and several realms assigned to its local branches. You can create one sub-account for each of your branch administrators and each admin group, and then assign realms to each admin group.

1. Log into the master account which is the global administrator or the first sub-admin inside your master account. Note: Only a global administrator or the first sub-admin can edit the *Administrators* page.
2. Click *User Management* > *Administrators*, identify the group of interest and mouse over it.
3. From the pop-up tool menu, click *Edit*.
4. To change the group name, highlight the Group Name and type a new name over it.
5. To modify the description of the group, highlight the Group Description, and type a new one over it.
6. To add more sub-admins to the group, click *Manage Admin*, and select the admins of interest, and click *Apply*.
7. To delete a sub-admin, identify the sub-admin and click the *Delete* icon.
8. To add more realms to the group, click *Manage Realm*, select the realms of interest, and click *Apply*.

9. To delete a realm, identify the realm and click the *Delete* icon.

Controling risky conditions

Adaptive Authentication

You can bypass OTP verification of MFA under certain “safer” conditions and deny such attempts under some otherwise “risky” conditions. You can pre-configure OTP verification of MFA based on trusted subnet/geo-location and time of day/day of week. For more details about how to configure it, go to Adaptive authentication on page 240.

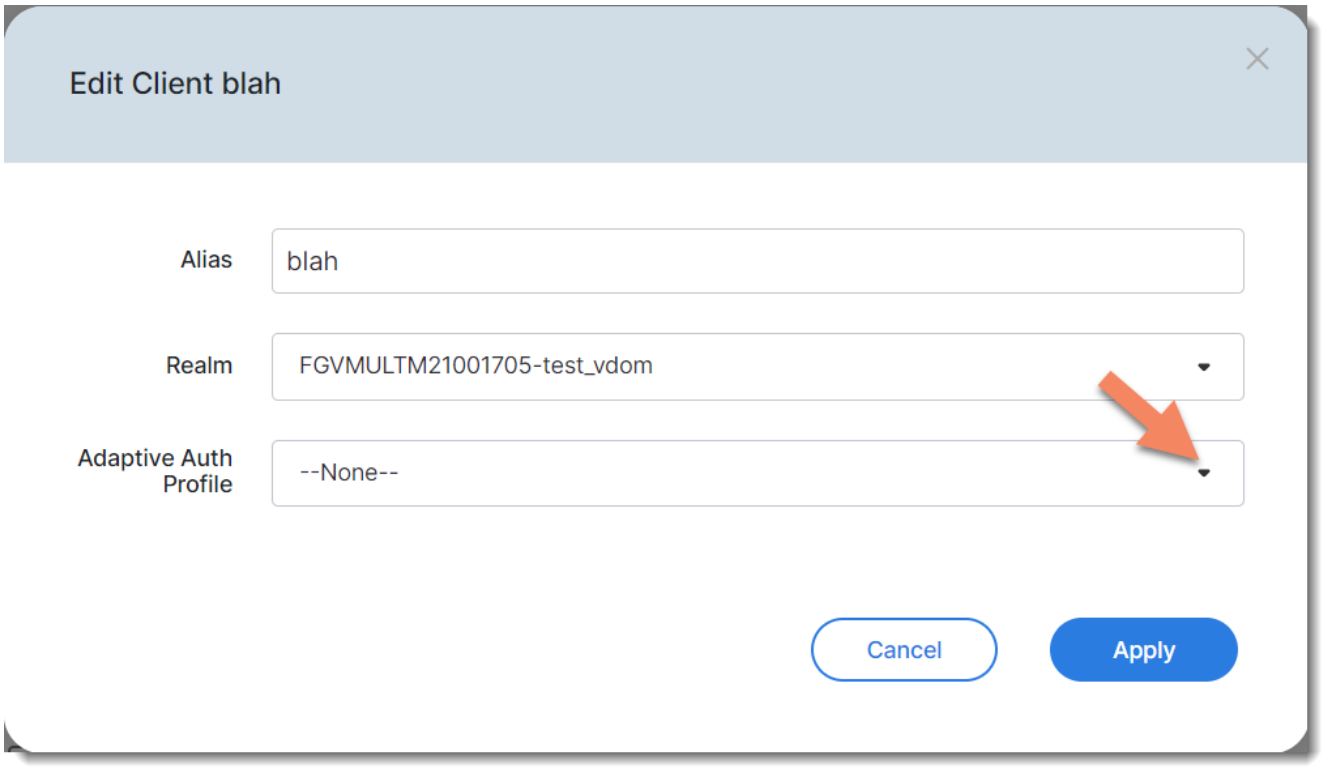
Creating adaptive authentication policy

1. Click *Settings>Adaptive Auth>Policies*.
2. Click *Add Policy*.
3. Make the desired entries and/or selections.
4. Click *Apply*.

Creating adaptive authentication profile

1. Click *Settings>Adaptive Auth > Profiles*.
2. Click *Add Profile*.
3. Make the entries and/or selections.
4. Click *Apply*.

Applying adaptive authentication profile to an application



1. Click *Applications* > *FortiProducts*.
2. Locate the application of interest, and click *Edit* in the pop-up tool menu.
3. Select an adaptive auth profile.
4. Click *Apply*.

Applying adaptive authentication profile to a realm

1. Click *Settings* > *Realm* > *General*.
2. Scroll down to *Adaptive Auth Profile*, and select a profile.
3. Click *Apply Changes*.

Last login

The *Last Login* feature enables you to let end-users use trusted IPs or subnets to log in by bypassing the MFA requirement within a specified time period.

Enabling the Last Login feature in Adaptive Auth Policy

1. Click *Settings* > *Adaptive Auth* > *Policies*.
2. Specify a unique name.

3. For Action, select *Bypass MFA*
4. For Filters, select *Subnet Filter*.
5. In the Subnets field, enter the IP address or subnet, and click the + sign. (**Note**: The IP or Subnet must be supported by the FortiProducts).
6. Click *Last Login* and specify a reasonable MFA Interval time period (**Note**: The range of this period is from 1 to 72 hours.)
7. Select a schedule configuration set in Schedule section
8. Click Apply.
9. Add the newly created policy to a profile and select the same action, i.e., Bypass MFA.
10. Apply the newly created profile to any applications (including FortiProducts and Web Apps) and any realms whose users are going to use those trusted IPs or Subnets.

Impossible travel

The Impossible Travel feature enables FIC to detect and block suspicious login attempts. Upon detecting a login request coming far away from the normal geographical location, for example, a login request from Russia for a device used by an employee who is based in the United States, FIC will block it. Using this feature, FIC can effectively identify suspicious sign-in attempts based on the distance and time elapsed between two subsequent user sign-in attempts. The feature works with IP addresses in the format that FortiProducts support.

Enabling the Impossible Travel feature in Adaptive Authentication Policy:

1. Click *Adaptive Auth > Policy > Add Policy*.
2. Give a unique name.
3. For Actions, select *Enforce MFA/Block*.
4. Select *Location Filter*.
5. Select the country or countries.
6. Click *Impossible Travel*.
7. Select a schedule configuration in the Schedule section.
8. Click *Apply*.
9. Add the policy to any profile. Be sure to select the same action, .i.e., Enforce MFA/Block.
10. Apply the profile to any applications (including FortiProducts and Web Apps) and any Realms whose users are going to log in from those locations.

Synchronizing LDAP remote users in wildcard user group from FortiGate

LDAP is commonly used in user management. FortiIdentity Cloud supports different types of LDAP, including ADLDAP, Open LDAP, etc. In FortiGate, for example, we can set up a filter to manage a group of users that have the same attributes, such as the same organization, department, or role.

Group filters can be used to reduce the number of the Active Directory users returned, and only synchronize the users who meet the group filter criteria. Use of LDAP filters for FortiGate and FortiAuthenticator are discussed separately below:

User case

This feature is supported on FortiGate devices running on FOS 7.4.5 or later, or FOS 7.6.0 or later.

To synchronize Active Directory users and apply two-factor authentication using FortiIdentity Cloud, two-factor authentication must be enabled in the user LDAP object definition in FortiOS.

Two-factor authentication for LDAP group filtering can only be configured in the CLI:

```
FGVMULTM00000000 (root) # show user ldap
config user ldap
    edit <string>
        set server <ip address>
        set cnid <string>
        set dn <string>
        set type {Simple | Anonymous | Regular}
        set two-factor <fortitoken-cloud>
        set two-factor-filter <string>
        set username <string>
        set password <string>
    next
end
```

In the following examples, a `user ldap` object is defined to connect to an Active Directory on a Windows server. The search will begin in the root of the `cloudsolutionsqa.com` directory.

```
FGVMULTM00000000 (root) # show user ldap
config user ldap
    edit "ad-136"
        set server "00.000.00.0"
        set cnid "sAMAccountName"
        set dn "DC=cloudsolutionsqa,DC=com"
        set type regular
        set two-factor fortitoken-cloud
        set two-factor-filter "(&(objectClass=user)(memberOf=Cn=ftc-
ops,ou=QA,dc=cloudsolutionsqa,dc=com))"
        set username "ldapadmin"
        set password ********************************************************************
    next
end
```

When a group filter is not used, all users in Active Directory with a valid email or mobile number will be retrieved; when a group filter is used, only users in that group will be filtered. In the example above, the group filter is `ftc-ops`.

For more syntax and diagnostic details, please check FortiOS Release Notes at Administration Guide | FortiGate / FortiOS 7.4.5 | Fortinet Documentation Library.

Transferring devices on FIC

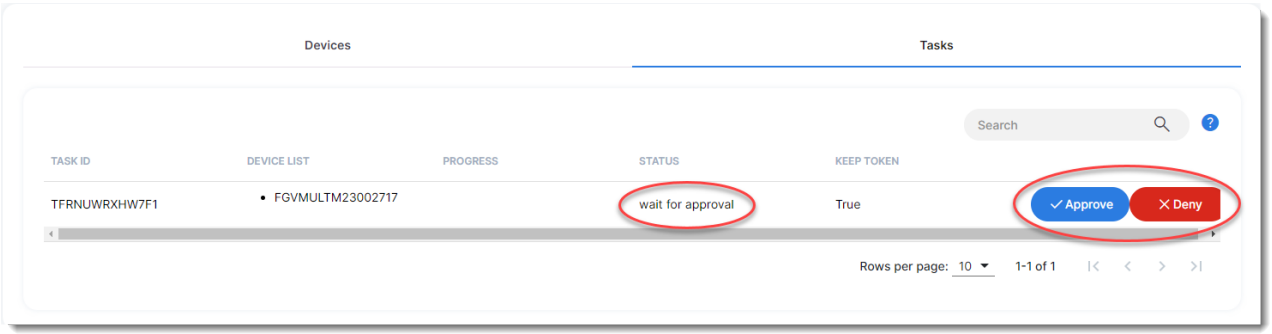
You can transfer devices from one FIC account to another using the FIC portal. While the transfer is being processed, your end users should not notice any changes in their user experience. For example, if they have logged in through VPN, they can continue using VPN while the device is being transferred.

Fortildentity Cloud approves device transfer requests automatically if the source account has been removed or merged into another account in FortiCare. We strongly recommend clearing any sensitive user data off the device before removing it from the source account or merging it with another FortiCare account.

To transfer a device with data:

1. Submit a device ownership transfer ticket in FortiCare.
2. Wait until after the ticket is processed and the ownership is transferred to the new owner in FortiCare. For example, Account A is the original owner and Account B is the new owner.
3. Now the owner of either Account A or B can start the device transfer by selecting *Applications* > *FortiProducts* > *Ownership*.
4. Click *Go to*.
5. Under *Devices*, locate the device whose *OWNERSHIP STATUS* is marked *Inconsistent*.
6. Click the tool icon, and select*Transfer*.
7. If you are NOT the owner of the new account who has initiated the device ownership transfer, click *Applications >FortiProducts>Ownership>Tasks,* locate the transfer task, and click *Approve*.

   - Device ownership transfer tasks are viewable by both parties involved in the transfer process.
   - A device ownership transfer task cannot be initiated and approved by the same party. If you have initiated a device ownership transfer task, you must wait for the other party to approve it.



8. Wait until the *Progress* column shows 100% and the *Status* column shows *Complete*. By then, the ownership of the device should have been transferred to the new owner, and any old data left on the device should have been wiped out.

Transfer tasks will remain on the page for 24 hours before being deleted automatically.

To transfer a device without data:

If all data related to the old account has been removed from the device, FIC can automatically transfer the device ownership to the new owner. However, the device will not appear in the new account.

To establish a new connection between the FIC portal and the application (FortiGate for this case), you must log in to the FortiGate device and run the CLI command "`execute forttoken-cloud update`".

ZTNA HTTPS access proxy with FIC MFA

1. Configure a ZTNA HTTPS access proxy on FortiGate by following the instructions in ZTNA HTTPS access proxy example.
2. Configure FIC MFA for end-users. If you use LDAPS to authenticate end-users on an internal Microsoft AD, you can set up FIC MFA by referring to the instructions in ZTNA session-based form authentication.

Adding FIC MFA to remote access IPsec VPN

This use case shows how to add FIC multi-factor authentication (MFA) to a FortiClient dialup VPN configuration (see FortiClient as dialup client).

Creating users

To create users from the GUI:

1. Select *User & Device* > *User Definition*.
2. Select *Create New*.
3. Select *Local User*, and click *Next*.
4. Name the user "test-ipsec".
5. Enable the *User Account Status*.
6. Enter a unique password for the user.
7. Enter the user's email address.
8. Enable two-factor Authentication, and set the *Authentication Type* to *FortiIdentity Cloud*.
9. Click *OK*.
10. Repeat Steps 1 through 9 to create another user named "testipsec2".

To create users from the Console:

```
config user local
    edit "test-ipsec"
        set type password
        set passwd <user-password>
        set two-factor fortitoken-cloud
        set email-to <user@abc.com>
    next
end


config user local
    edit "testipsec2"
        set type password
        set passwd <user-password>
        set two-factor fortitoken-cloud
        set email-to <user@abc.com>
    next
end
```

Creating a user group

To create a user group from the GUI:

1. Select *User & Device* > *User Groups*.
2. Click *Create New*.
3. Name the user group "ipsecgrp".
4. Set *User Group Type* to *Firewall* .
5. Click the + sign (*Add*) in the Member box to add users "test-ipsec" and "testipsec2" to the user group.
6. Click *OK*.

To create a user group from the Console:

```
config user group
    edit "ipsecgrp"
        set member "test-ipsec" "testipsec2"
    next
end
```

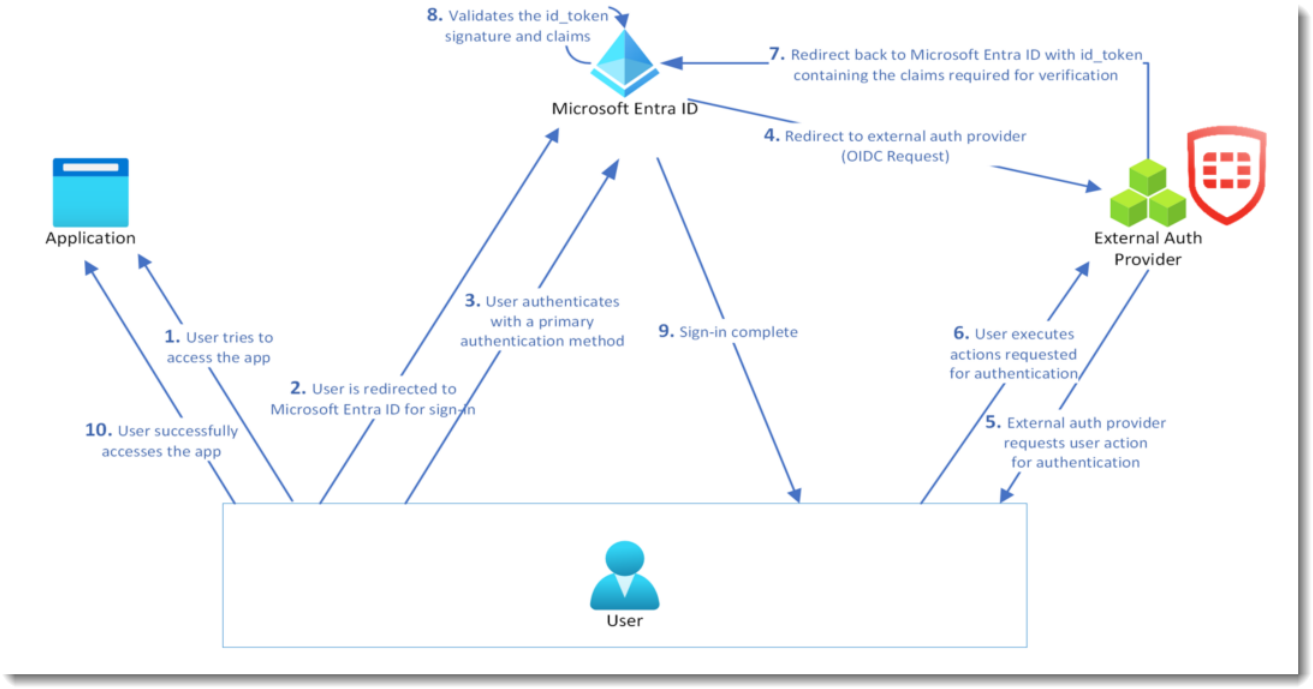
Configuring FIC as Microsoft Entra external authentication service provider

In May 2024, Microsoft introduced Entra ID external authentication method provider feature. An external authentication provider can integrate with Entra ID tenants as an external authentication method (EAM) provider, which can satisfy the second factor of the MFA requirement.

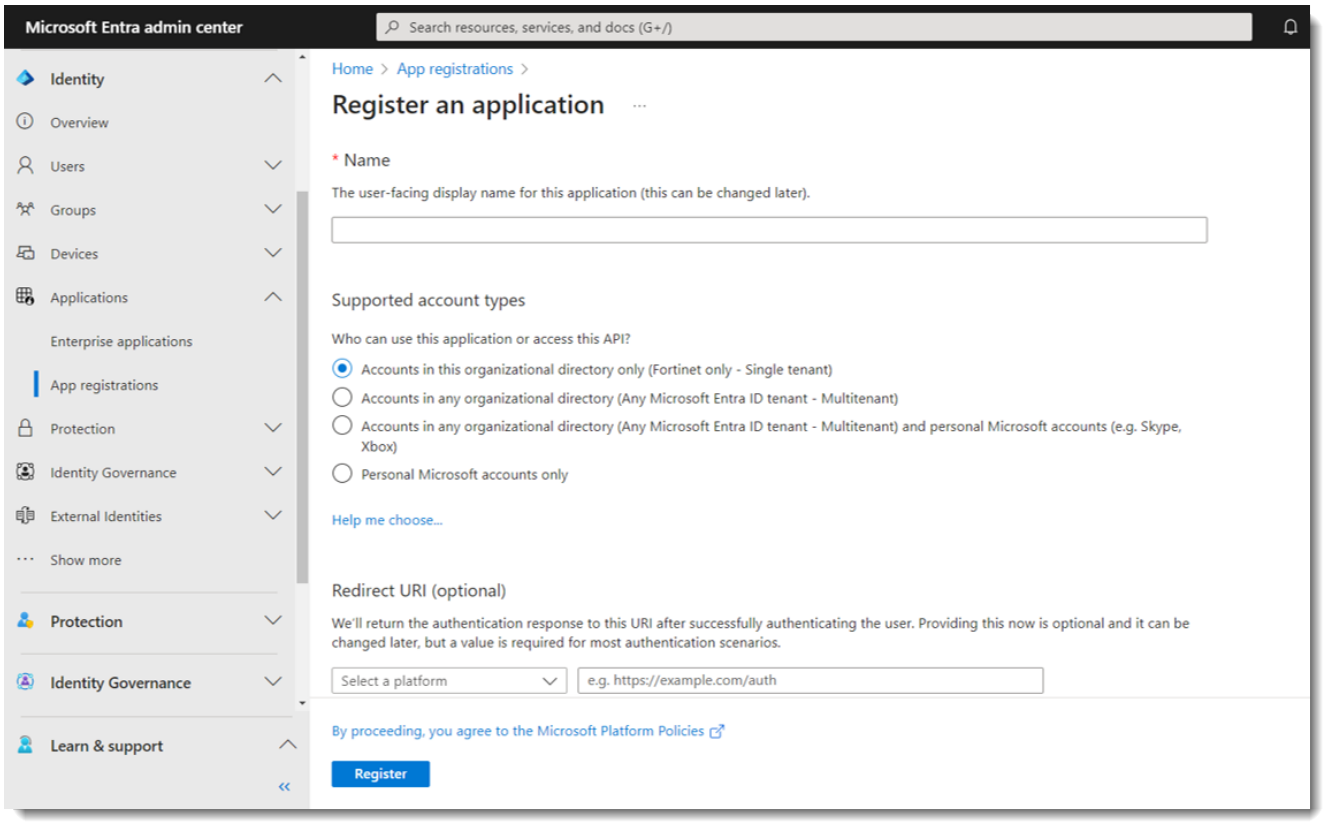
An EAM must be implemented on top of Open ID Connect (OIDC). This implementation requires at least three public facing endpoints:

- An OIDC discovery endpoint
- A valid OIDC authentication endpoint
- The public certificates of the EAM provider

The following diagram shows the network topology of the configuration:



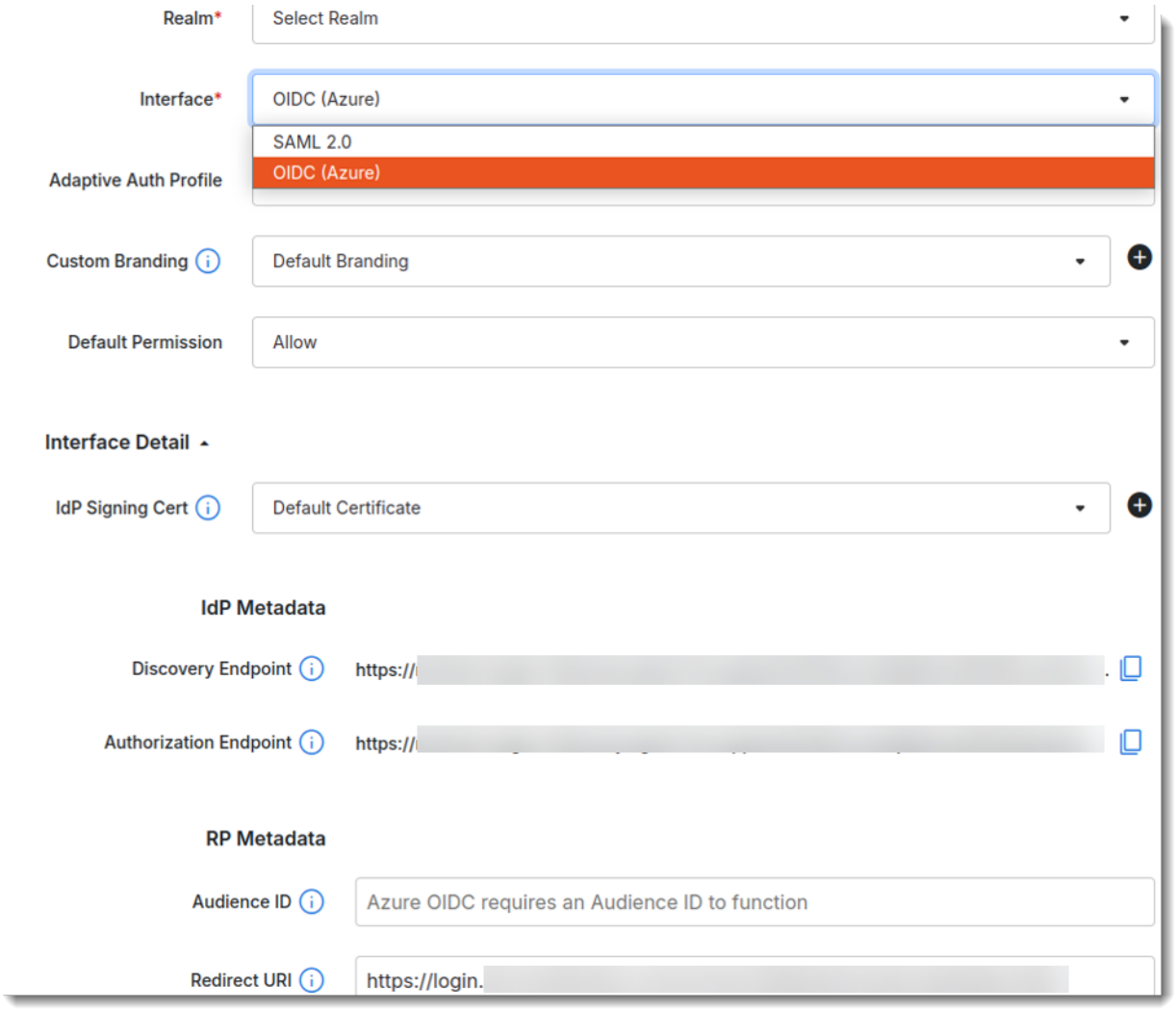
Step 1: Adding FIC app on Entra admin center



1. Log onto Microsoft Entra admin center.
2. Select *Applications >App registrations*.
3. Enter a unique name for the app.
4. For Redirect URL (optional), select None. (**Note**: The redirect URL will be generated on the FIC portal later.)
5. Click *Register*.

Upon successful registration, you will receive the Application (client) ID that Microsoft generated. Be sure to save the Application (client) ID as you will need it later in the configuration.

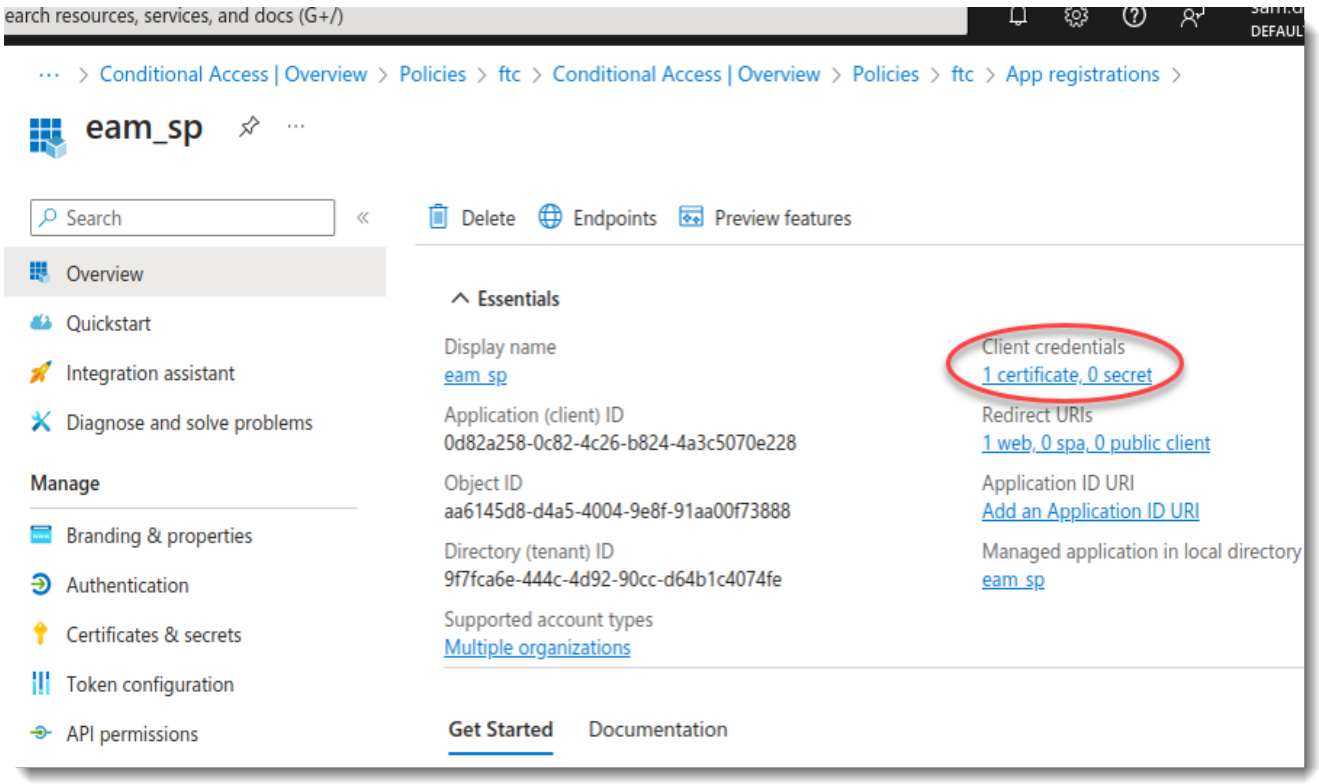
Step 2: Creating the Microsoft app on FIC portal



1. Select *Applications* > *SSO*.
2. Click *Add SSO Application*.
3. Name the Microsoft app.
4. For *Realm*, select the realm on which the end users of the Microsoft app reside.
5. For *Audience ID*, enter the Application (client) ID that you have saved on Microsoft Entra admin center.
6. For *Redirect URI*, enter the default Microsoft URI.
7. Make the other entries and/or selections on the page.
8. Click *Next*.
9. Follow the prompts onscreen to complete the configuration.

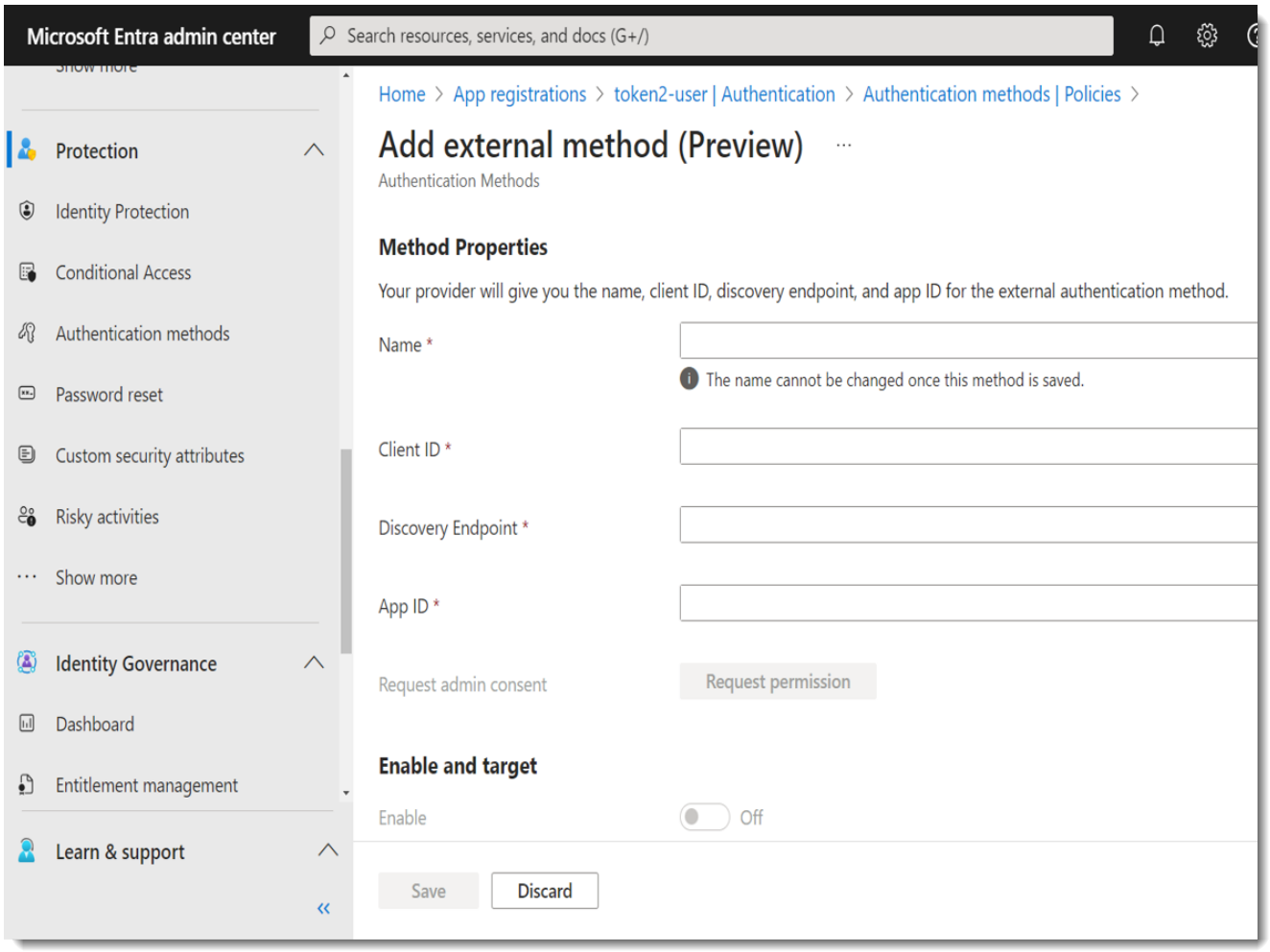
- Once the Microsoft app has been created, you will receive the FIC App ID, the discovery endpoint, and the authorization endpoint.
- If no Signing Cert is provided, the application will use the default certificate for authentication.

Step 3: Updating the FIC app on Entra admin center



1. On Microsoft Entra admin center, select *Applications* > *App registrations* > *All Applications*.
2. Locate the FIC app, click to open it, and make the desired updates to its Client credentials and redirect URI.
3. To add client credentials, go to *Certificates* and upload the public key downloaded from the FIC portal.
4. To add redirect URI, go to Redirect URI, click *Add a platform,* choose Web Applications, and enter the authorization endpoint generated from the FIC portal.

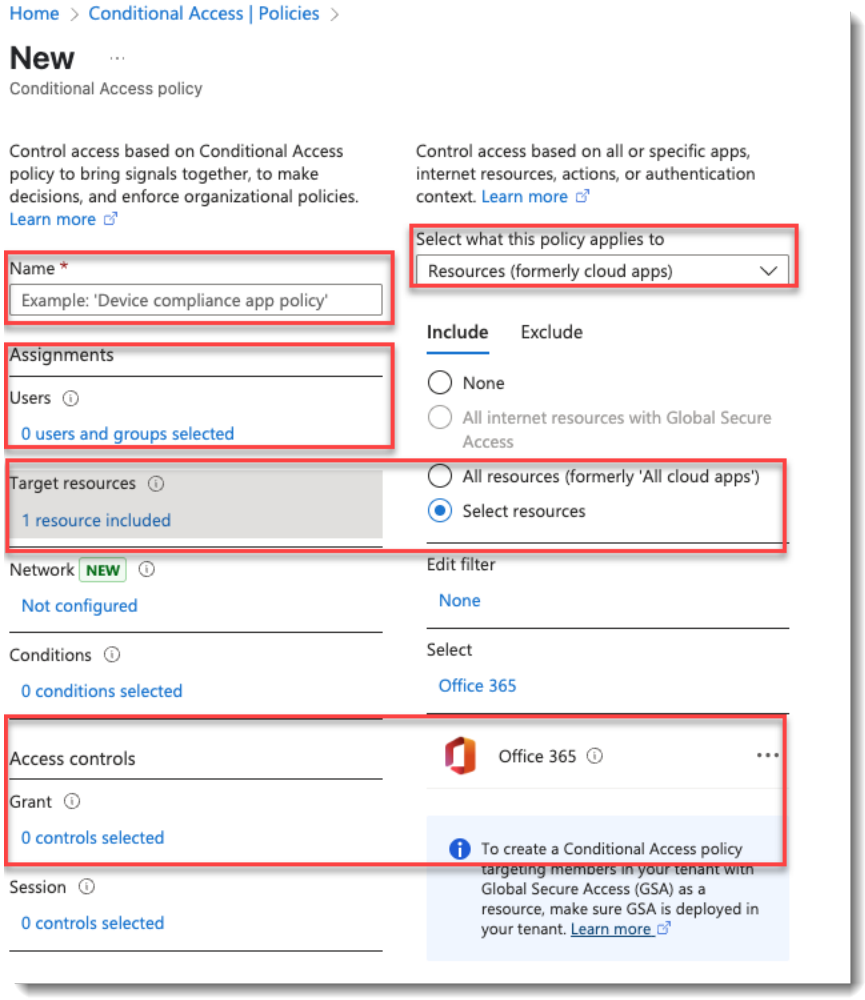
Step 4: Registering FIC as Entra MFA external method provider



1. On Microsoft Entra admin center, select *Protection -> Authentication methods -> Policies -> Add external method(Preview)*.
2. For Client ID, enter the Application ID generated from the FIC portal.
3. For Discovery Endpoint, enter the discovery endpoint generated from FIC portal.
4. For App ID, enter the Application (client) ID generated from Microsoft.
5. Upon securing the permission, enable *Enable and target*.

- Up to this point, FIC should have been successfully set up as the EMA. With this configuration, all apps in your Microsoft account will use FIC for MFA.
- If you prefer using MFA methods other than FIC for your different Microsoft apps, you can take advantage of Microsoft's custom authentication strengths feature. For more information, visit `https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-strength-advanced-options`. Keep in mind that "Password + Software AUTH token" is the MFA setting that you should pick when configuring custom authentication strength in Microsoft that corresponds to the type of MFA that Microsoft considers FIC to be in this case.

Step 5: Setting Conditional Access policy to assign users to EMA



1. Select *Protection -> Conditional Access -> Policies*.
2. Create a new policy, and assign users or groups to it. For *Target resources*, select *All resources (formerly 'All cloud apps')* or *Selected resources*. (Note: If you choose *Selected resources*, you must select one, for example, Office 365.)
3. For *Access Controls*, select *Grant access > Require multifactor authentication*.
4. Set *Enable policy* to *On*.

Make sure to create a new user in FIC with the same username as the preferred username for the target user on Microsoft Entra admin center for identification.

Enabling FortiSASE VPN users to use FIC MFA

Scenario

This use case presents a scenario in which a customer has both FortiSASE and FortiIdentity Cloud in their network ecosystem. They would like end users in their Google user base to be able to log into VPN through SSO. They also would like to control their end users MFA with FIC when they are logging into VPN using FortiSASE VPN with FortiClient configuration.

Enabling FortiSASE VPN users to use FortiIdentity Cloud for MFA involving configurations on both FortiIdentity Cloud and FortiSASE, as discussed in the following sections.

Configuration On FIC:

Step 1: Setting up the authentication user source from Google.

1. Create a realm. See Managing realms on page 100.
2. Navigate to *Authentication* and choose the realm created above and create an authentication source.
3. Provide your Google SAML app details for the Identity Provider (IdP).
4. In your Google SAML app, make sure that this FIC authentication source is configured as the SP.

Step 2: Setting up the SSO application

1. Navigate to *Applications >SSO Applications>Create a new SSO Application*.
2. Make sure that the application is in the same realm where the end users reside.
3. For *SP Metadata*, provide the metadata from the FortiSASE VPN User SSO configuration file.
4. For *Authentication>User Source*, select the Google authentication source configured in Step 1.
5. (Optional), if you want to let your end users change their MFA methods, do the following:
   a. Select *Settings > Realm* and choose your realm from the drop-down list.
   b. For *Allow Additional MFA Methods,* select the alternative MFA methods that you would like the end users to use.

Step 3: Enabling End-user Portals

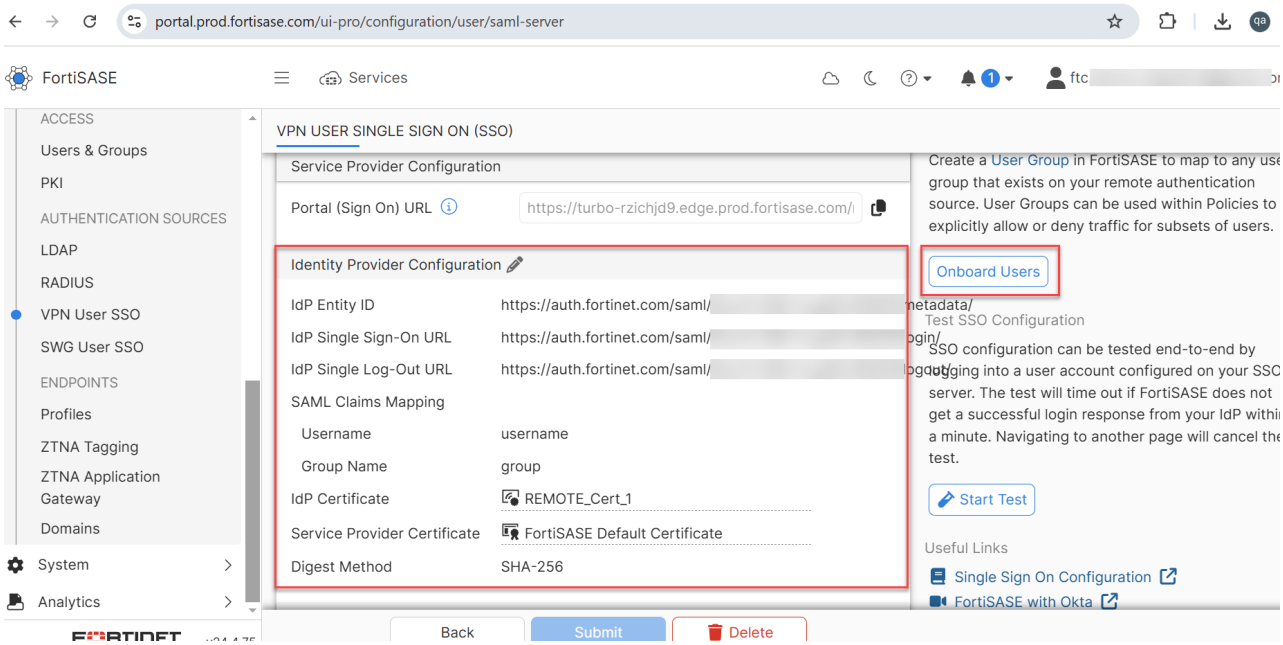
FIC offers the *End-user Portal* function which the administrators can enable or disable from the FIC portal. Once enabled. the feature gives the end users the freedom to use MFA methods other than the one configured on the realm, and make changes or updates to their profiles according to the permissions granted by their administrator.

1. Navigate to *Applications > End-user Portals > Add User Portal*.
2. For Realm, be sure to select the same realm which was used in Steps 1 through 2 above.
3. Create a custom branding theme, if you like.
4. Click *Save*.

Configuration on FortiSASE

Step 1: Configuring the FIC SSO application as IdP for FortiSASE VPN user SSO

1. On the FortiSASE portal, select *VPN User SSO* to configure a VPN user SSO.
2. For *Identity Provider Configuration*, make the required entries or selections as highlighted in the following screen shot.



3. Click *Submit*.
4. Then, click the *Onboard Users* button on the right (highlighted above) to help the end users to download and install FortiClient on their devices.

You can let your end users download FortiClient using any of the following options (highlighted in the following screen shot):

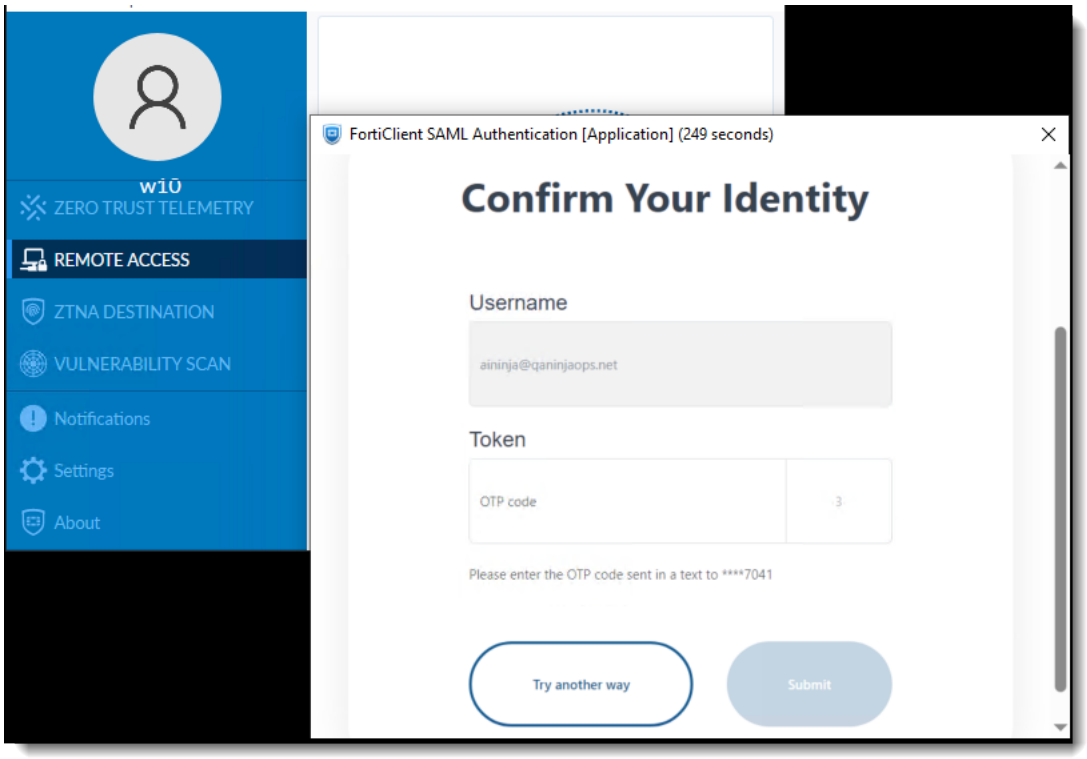
- Download installer
- Send link to users
- Send Invitation code

Refer to FortiSASE documentation for instructions on how to use each of these options.

5. Click *Close* when done.

Step 2: FortiSASE VPN end-user SSO experience with FIC MFA

Upon successful installation of FortiClient, the users can access the VPN server anytime from FortiClient. Each time, their requests will trigger FIC authentication with the default MFA method set by the administrator.



If you (the FIC admin) have enabled the End-user Portals function on FIC for the end users (as mentioned earlier in Configurations on FIC), they will have the ability to access their own FIC end-user portal where they can change or update their mobile phone numbers, MFA methods, and so on based on the permissions that you have granted them. For more information, see Manage end-user portals.

FortiIdentity Cloud as OIDC provider

FortiIdentity Cloud (FIC) can be configured as an OpenID Provider (OP) for authenticating users and issuing tokens to a Relying Party (RP). When configured in tandem with its local IdP, FIC can be the authentication source as well and provide end-to-end OP functionality.

Keep in mind that Local IdP is only a beta feature in FIC 25.2.a release and must be enabled by an FIC admin. For instructions on how to enable Local IdP, see Enable local IDP beta feature.

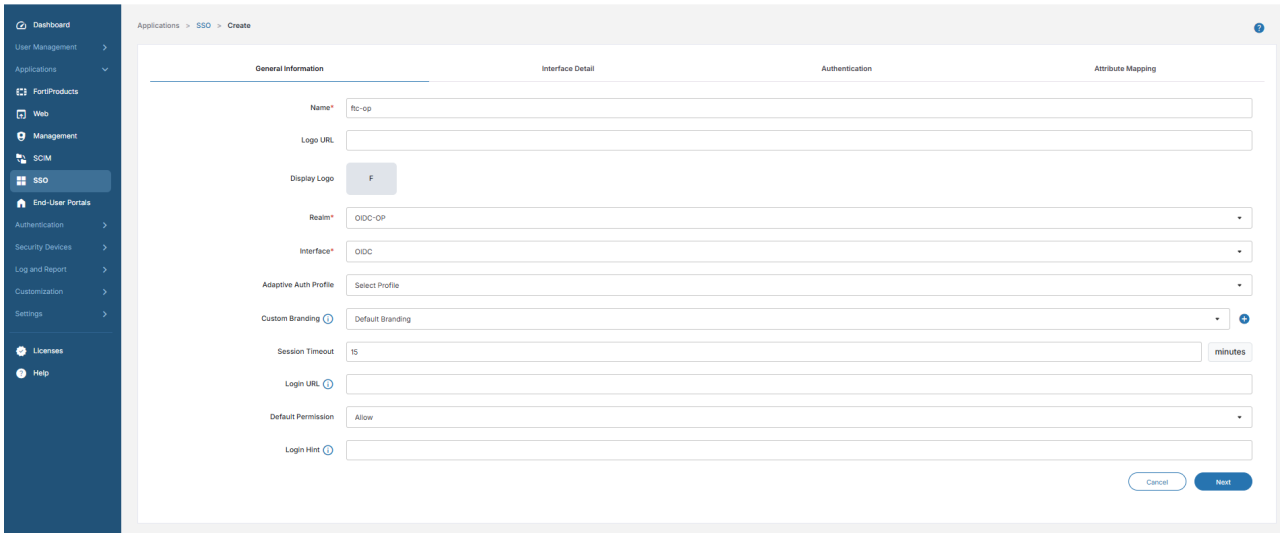
You may also configure other third-party IdP providers as authentication user sources based on the your environment. For configurations supported by FIC as OIDC OP, refer to the ./well-known/opened-configuration generated by FIC once the configuration is complete.

While Implcit grant type is supported, we do not recommend using it unless there is no other alternative for your application.

Configuring FIC as an OIDC provider

In the following example, we demonstrate the steps to configure FIC as an OIDC OP and a test on-prem grafana setup as RP. We also use FIC Local IdP as the user source for the first factor authentication.

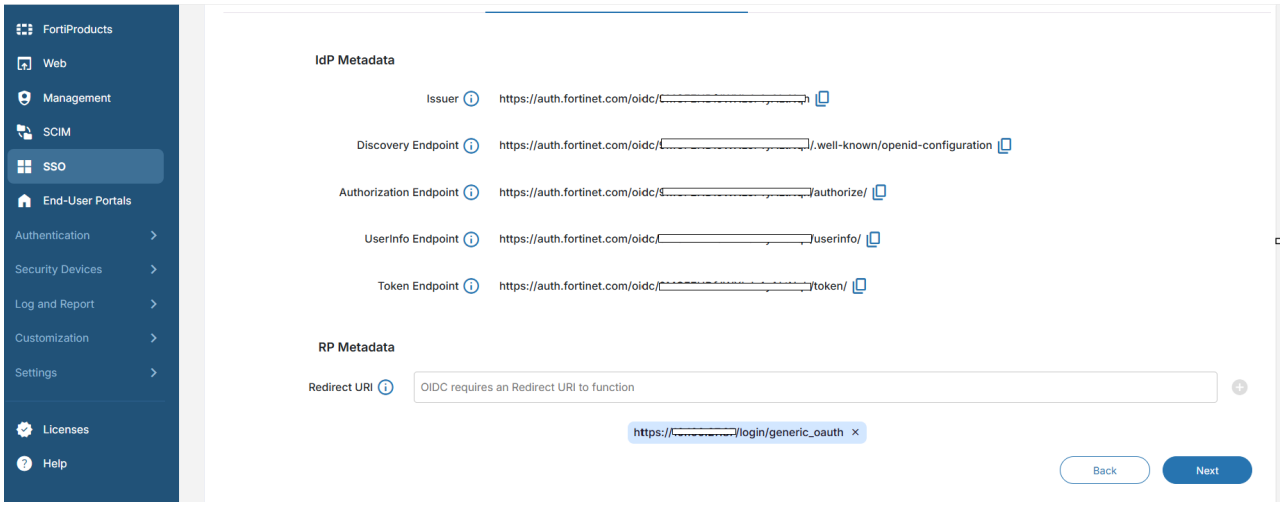
1. Navigate to *Applications* > *SSO*.
2. Click *Add SSO Application*.
3. For Interface, select OIDC, and provide the other necessary details as in the following sample.



4. Click *Next*.

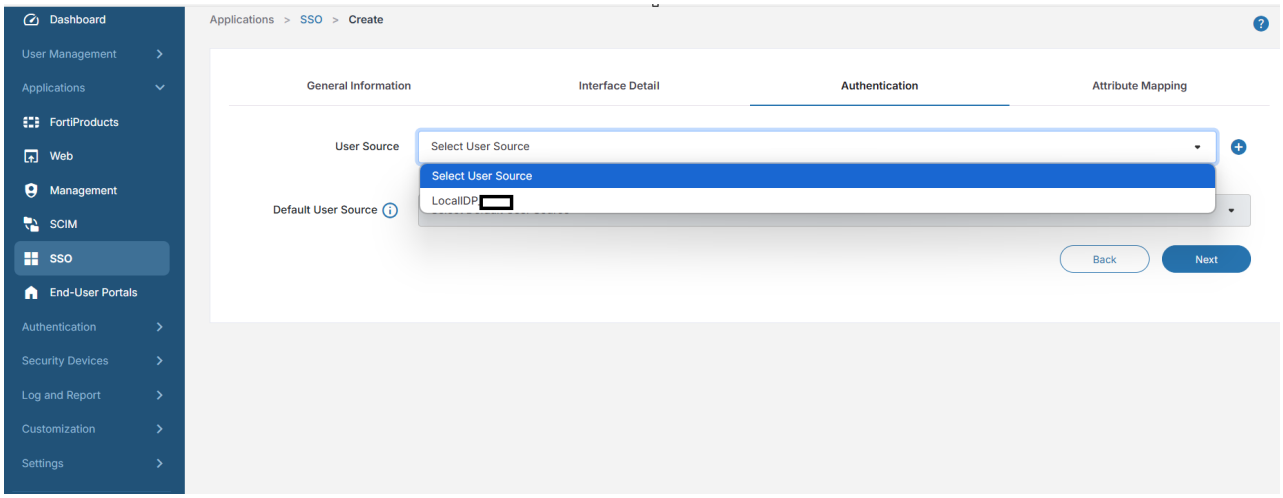
   Under *Interface Detail*, the IdP metadata will be generated by FIC and will be displayed as in the following screenshot.

For the Redirect URI, ensure to provide a valid Redirect URI as documented by your RP. In this sample we use an on-prem grafana setup and the redirect URI provided by grafana is `https://<grafana ip>:<grafana port>/login/generic_oauth`. Make sure to click the '+' button to have the redirect URI added.

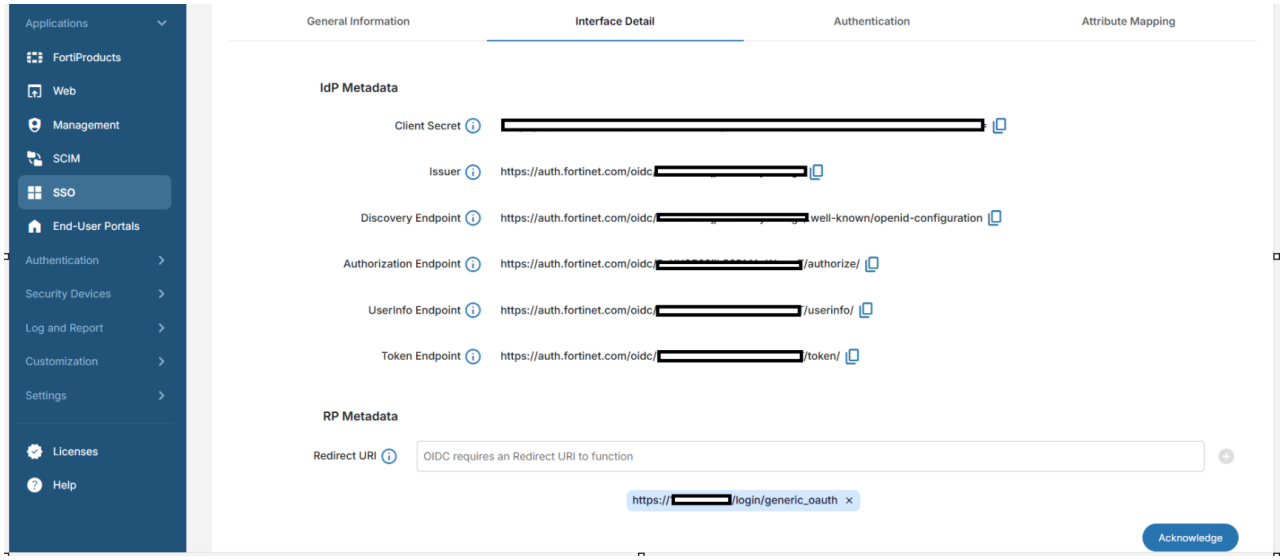


5. Click *Next*, and choose an appropriate user source under *Authentication*.

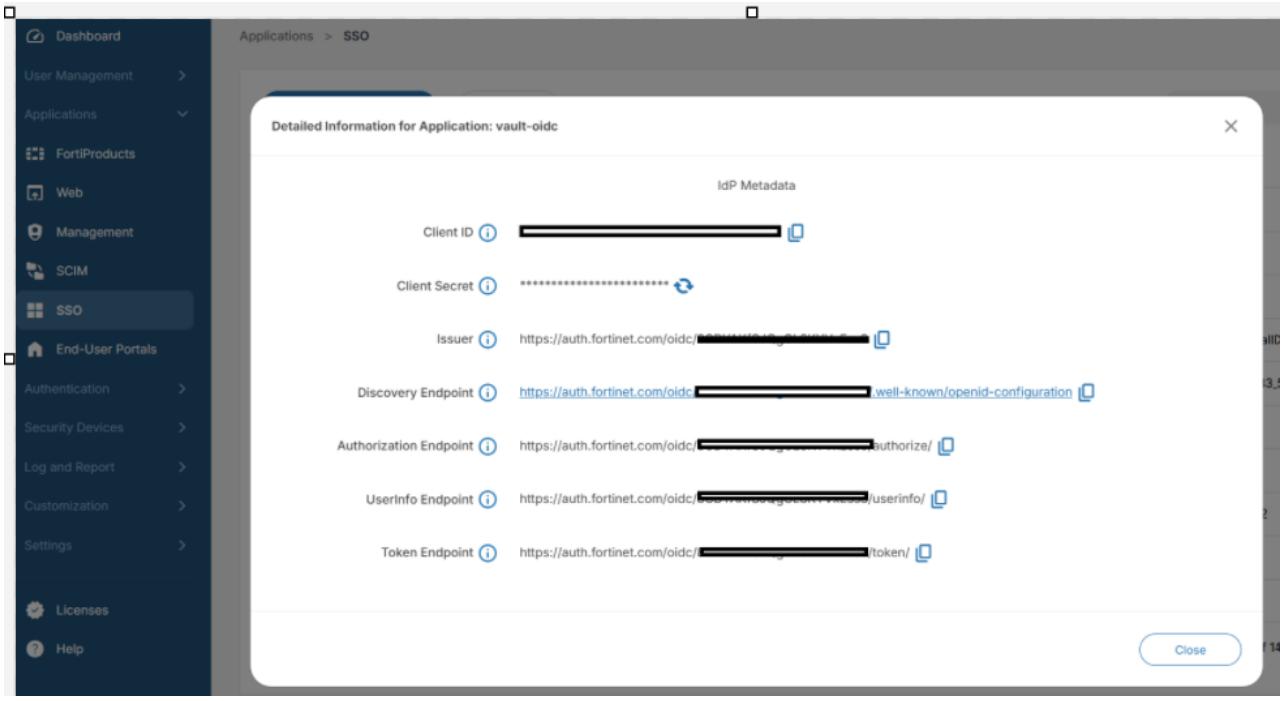
In this example, we use a Local IdP source which is a beta feature to demonstrate the capability for FIC to act as an OIDC provider along with local user source.



6. Click *Next*.
7. Under *Attribute Mapping*, enter any attribute mapping that might be needed by the RP, and click *Save*.



8. Copy the client Secret as it will be visible only once, and click *Acknowledge*.
9. Once the configuration is completed, click the tools pop-up menu (three vertical dots) at the right of the row, and click *Details* to view all the required IdP metadata.



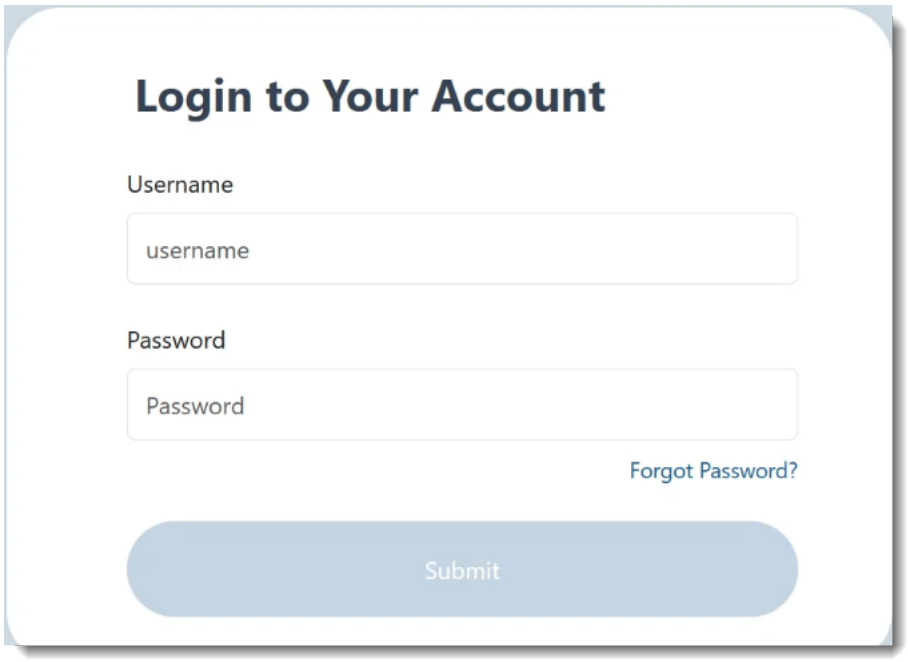
10. On your RP, furnish the IdP metadata from FIC as shown in the above screenshot.
    The following sample shows the configuration done for this test of on-prem grafana setup acting as RP.

```
  - name: GF_AUTH_GENERIC_OAUTH_ENABLED
    value: "true"
  - name: GF_AUTH_GENERIC_OAUTH_NAME
    value: OIDC
  - name: GF_AUTH_GENERIC_OAUTH_CLIENT_ID
    value: [redacted]
  - name: GF_AUTH_GENERIC_OAUTH_CLIENT_SECRET
    value: [redacted]
  - name: GF_AUTH_GENERIC_OAUTH_AUTH_URL
    value: https://auth.fortinet.com/oidc/[redacted]A/authorize/
  - name: GF_AUTH_GENERIC_OAUTH_TOKEN_URL
    value: https://auth.fortinet.com/oidc/B[redacted]A/token/
  - name: GF_AUTH_GENERIC_OAUTH_SCOPES
    value: openid profile email
  - name: GF_AUTH_GENERIC_OAUTH_USE_PKCE
    value: "true"
  - name: GF_AUTH_GENERIC_OAUTH_USE_REFRESH_TOKEN
    value: "true"
  - name: GF_AUTH_GENERIC_OAUTH_DISCOVERY_URL
    value: https://auth.fortinet.com/oidc/B[redacted]A/.well-known/openid-configuration
```

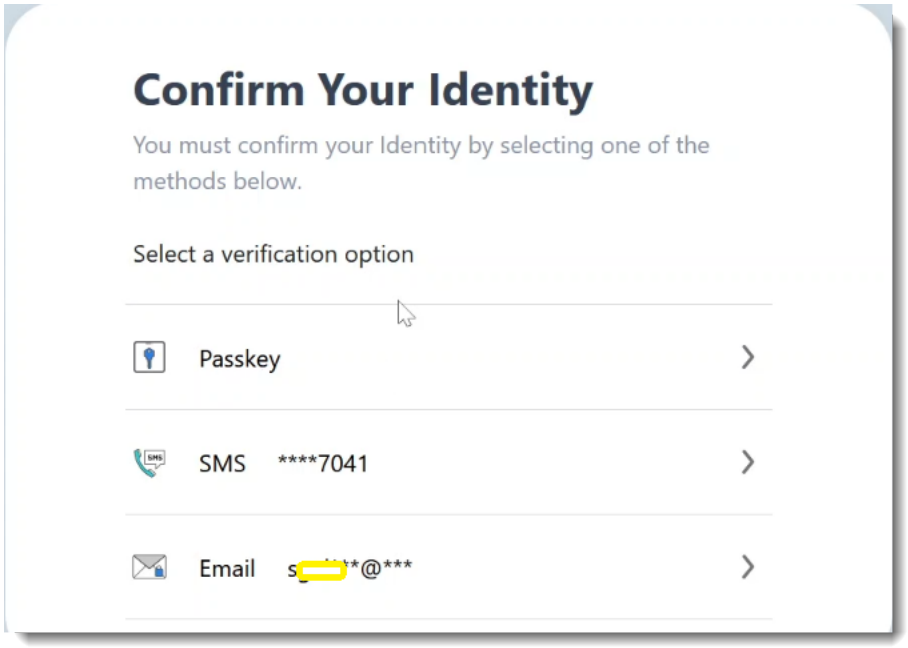
11. Click User Management>Users, and create users in your realm to facilitate login.
12. Make sure that the user type is Local User for the first factor authentication to be performed by FIC.

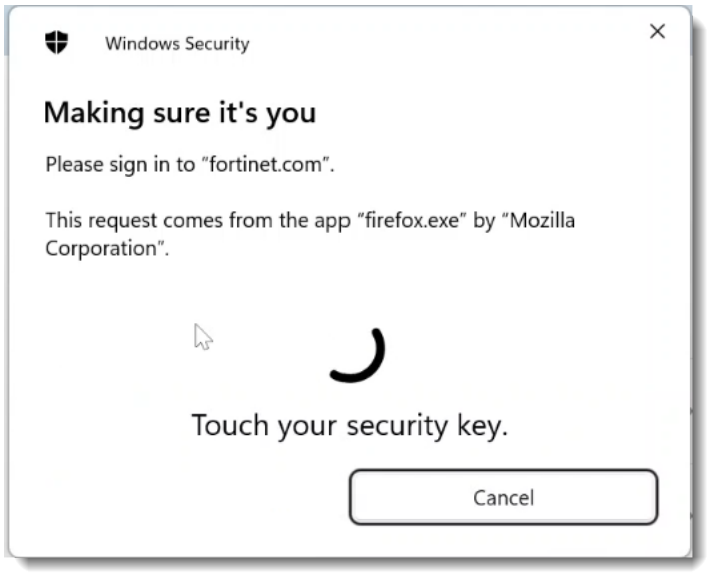
End-user experience

1. In the RP (on-prem grafana in this case), select Sign in with OIDC.
   With Local IdP beta feature enabled for this account and Local IdP configured as the user source, FIC will perform the first factor authentication.
2. Observe the user gets navigated to FIC's `auth.fortinet.com` page. Enter the username and password configured on the FIC for the user.

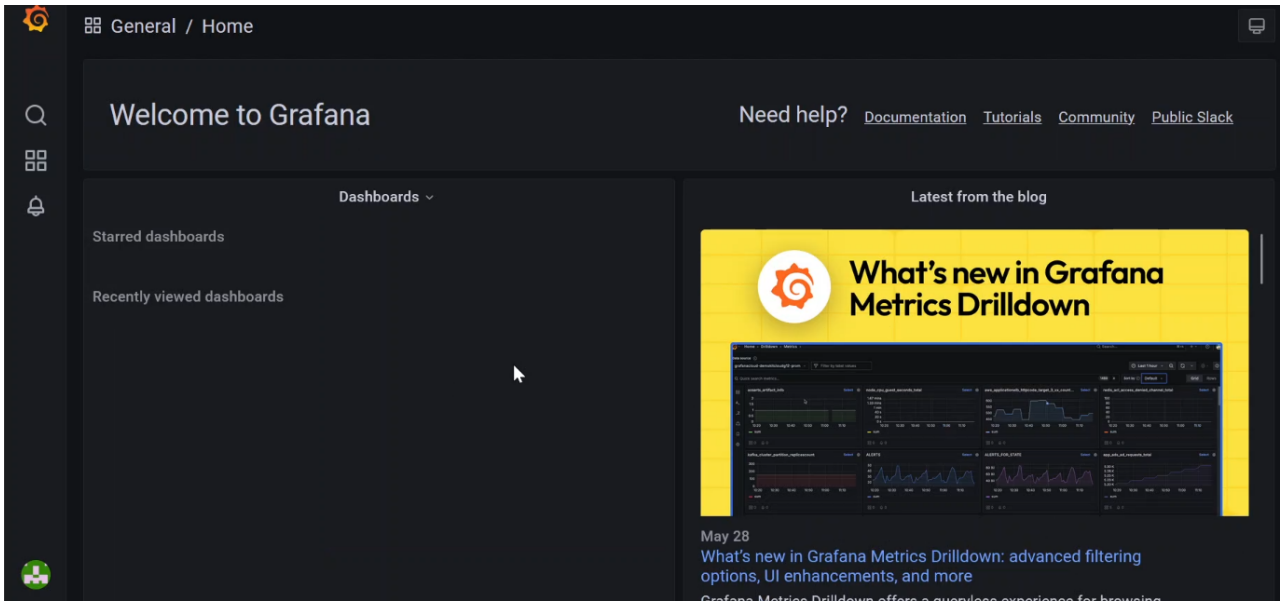


After successful first factor authentication, the user is prompted for MFA by FIC based on the users MFA method. In this example, the user has Passkey configured, so passkey will be prompted by default.





After successful second factor authentication, the user can successfully log into grafana.



In this sample demonstrates that with FIC Local IdP for first factor and a variety of MFA methods to choose from, administrators can secure their applications by configuring FIC as the OIDC provider.

Maintenance

Adding, syncing, and deleting users

When a user is created with FIC as the authentication method on an application (e.g., FortiGate), the user data is automatically added to the FIC system.

When a user with FIC as auth method on an application is deleted, the user data is automatically deleted from the FIC system. Deleting an application from the FIC portal deletes all users on the application. Additionally, you can delete individual users in the *Users* page of the FIC portal. You can sync user data anytime from the application (FortiGate in this case) to FIC by running the "`exec fortitoken-cloud sync`" command, as discussed in the following use case.

Use case

1. Create or delete users in FGT.
2. Run "`exec fortitoken-cloud sync`" on FGT to sync users with FIC auth method to FIC:
   - If syncing works well, the output will show:

     ```
     Sync status: {"status": "complete", "msg": {"delete": {"success": 0, "failure": 0},
     "modify": {"success": 0, "failure": 0}, "create": {"success": 3, "failure": 0}}}
     User synchronization completed!
     ```

   - If syncing failed, the output will show:

     ```
     Sync status: {"status": "complete", "msg": {"delete": {"success": 0, "failure": 0},
     "modify": {"success": 0, "failure": 0}, "create": {"success": 0, "failure": 3}}}
     User synchronization completed!
     ```

   - If you encounter the "failure" as shown above, check to see if this application exists in the FIC side by searching the SN in the *applications* > *FortiProducts* page.
     - If it does not exist, check to see if the switch *Auto-create Auch Client* is enabled in the *Settings* > *Global* page.
     - If it does exist, check to see if the user quota has reached the maximum, or if the realm assigned has available quota and if the *Share-quota Mode* is disabled.
   - If the connection to FIC is unstable or unavailable, the output will show:

```
Cannot find fic server!
Cannot retrieve user information from FortiToken Cloud!
Command fail. Return code -1
```

Adding, syncing, and deleting applications (FortiProducts)

When an application communicates to FIC for the first time, this application will be added to the FIC system automatically. The first communication can be triggered by creating an FIC user on the application or by running some CLI commands on the application. The application can be deleted from the FIC portal by choosing *Applications>FortiProducts or Web*.

Use cases

- Register a new FortiProduct, for example FortiGate, using the license or serial number of the device, create a new VDOM in FGT, or delete a VDOM.
- Run "`exec fortitoken-cloud update`" on FGT to sync VDOMs (applications in FIC) to FIC.
- If syncing works well, the output will show:

  ```
  List of VDOMs updated to FortiToken Cloud.
  ```

- After syncing, if the *Multi-realm Mode* is disabled, any new application will be assigned to the default realm. When *Multi-realm Mode* is enabled, any new application registered in FIC will be automatically assigned to a new realm.

How to debug

FortiIdentity Cloud has special debug mode in the FOS (ex. FortiGate) side. Before you perform any user sync/delete/add operation, the debug mode can be opened by running:

```
config global (if the multi-vdom mode is enabled)
diag fortitoken-cloud debug enable (to enable the FTC debug mode)
diagnose debug console timestamp enable (to add the timestamp to log output)
diag debug appl fnbamd -1
diag debug application httpsd 255
diag debug enable (to start the show debug message)
```

After running the CLI commands shown above, if any FIC user sync/delete/add action is triggered, the log message will show in the CLI. Or, if another CLI is open and executes "`exec fortitoken-cloud update`", the log will also display because it manually triggers the FortiIdentity Cloud user update in FOS (ex. FortiGate).

If you are unable to fix the error message using the aforementioned commands, the FortiIdentity Cloud support team is standing by to provide any assistance if needed. Just create a support ticket and submit it to our TAC team. We will respond to your service request and resolve your issue as soon as possible. It's recommended that you attach the debug log output in the ticket to enable the TAC team or the FortiIdentity Cloud Support Team to investigate the error faster. To contact technical support, visit Technical Support.

Service debugging

You can debug the service from the FIC portal logs page if there is any auth failure or your end-users fail to receive OTP or push notifications when using the FIC service. There are two categories of logs: one is for authentication requests and responses, and the other is for management operations such as creating, deleting. or updating user. To find out if the FIC server is available, you check the Service Status (https://status.fortistatus.com/guest-portal/fortitoken/incident/overview)

Applications

An application can be hardware, software, or a third-party web application that FIC uses to perform user authentication. When creating a user, it is mandatory to have an application which is assigned to a realm in order for FIC to perform authentication with FortiProducts or third-party web apps. Once an application is created, you will be able to set the realms and adaptive auth profiles that the application uses. Note that by default, an application is automatically created when you connect your FortiGate to FIC. If you do not see the application (i.e., FortiGate) after connecting it to FIC, you can run the `execute fortitoken-cloud update` command which sends an updated list of VDOMs to FortiIdentity Cloud so that applications can be created for each VDOM on the FortiIdentity Cloud portal. Ensure that *Auto-create application* is enabled on the *Settings > Global* page. For how to get started with applications, see QuickStart Guide.

Creating FortiProduct applications

While you can create web app and management applications directly from the FIC portal, applications under *Applications > FortiProducts* can be created only when you successfully link the devices to your FortiIdentity Cloud account. That is to say, you must create a user on a FortiProduct (e.g., FortiGate) and select FIC as the 2FA method.

For more information on how to set up your FortiProducts, please visit our DOCUMENT LIBRARY (https://docs.fortinet.com/).

Transferring application (FC account lockout)

If one of your account owners has left your organization, the associated account will be locked out. If you still want to keep using the application which was registered under the locked account, you can transfer the ownership of the application from one FC account to another FC account.

To transfer an application to a new account:

1. Transfer the FortiGate to the new account by submitting a ticket (*Support > FORTICARE > Create a Ticket):* Fortinet Service & Support.
2. Log into the FIC portal with the new FC account to validate the device ownership from the Devices (HA) page.

3. Choose either of the following options:
   - Delete—Clicking the Delete button to remove all existing user information in FIC side and transfer the ownership afterward.
   - Transfer—Clicking the Transfer button to migrate all existing user information in FIC side and transfer the ownership afterward.
4. Refer to Transferring devices on FIC on page 181 for instructions on how to migrate device data.

application clean-up/migration may take some time, so be sure to validate the device again until the device has been transferred to the new FC account. If *Delete* is selected, all users with FIC MFA on the FGT can be synced to FIC, and the end-users need to be re-activated with a new token if you want to keep the users on the FGT. If *Transfer* is selected, all users with FIC MFA on the FGT can be migrated to the new FIC account and do not need to be re-activated.

Replacing an old FortiGate with a new one

When replacing a FortiGate device, the most important thing to remember is to back up the FortiGate configuration and restore it to the new FortiGate. For backup issue, refer to Administration Guide | FortiGate / FortiOS 7.2.2 | Fortinet Documentation Library.

In the FortiIdentity Cloud:

1. Select *Applications* > *FortiProducts*.
2. Find the old FGT by searching its serial number in search bar.
3. Select the device from the application list, and click *Delete*.

After the old FortiGate is removed, you can register the new FortiGate to your FC account by entering the registration code from the device or the license number if it is a VM. After the device is registered under the FC account, you can enable FortiIdentity Cloud on the FortiGate. This is important because you are going to restore the users who are using FortiIdentity Cloud as the MFA method in the next step.

Now, it's time to restore the configuration from the old FortiGate. After the basic configuration is restored, the end-users will also be restored. (Note: If the users exist in VDOMs, you need to back up/restore the VDOMs configuration.)

Finally, the users and applications will be updated if *Auto-create application* is enabled in the *Settings* > *Global* page. Otherwise, you need to run the `exec fortitioken-cloud update` command to manually update the VDOMs information from the FortiGate to FortiIdentity Cloud and update the users' information.

After you finish all these steps, the new FortiGate should be set up and ready to use.

Applications in HA mode

Applications in an HA cluster are shared by all members of the cluster. This is to ensure that the cluster members are using the same applications to preserve HA functionality. For more information about how to configure HA clusters in the GUI, see the FortiProducts section.

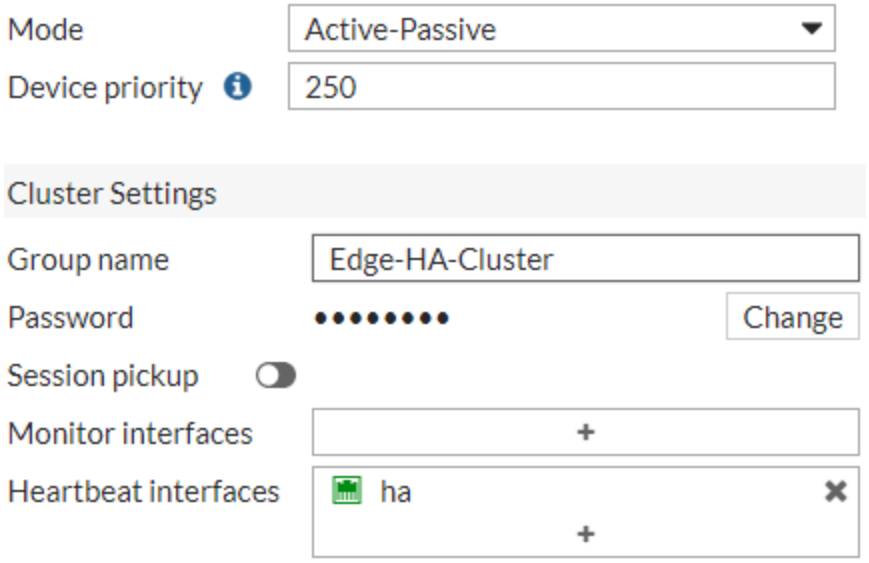
Before creating an HA cluster, make sure that the FortiGates are running the same version of the FortiOS and that the interfaces are not configured to get their addresses from DHCP or PPPoE. Also, switch ports are not allowed to be used as HA heartbeat interfaces. If necessary, convert switch ports to individual interfaces.

Configuring the primary FortiGate

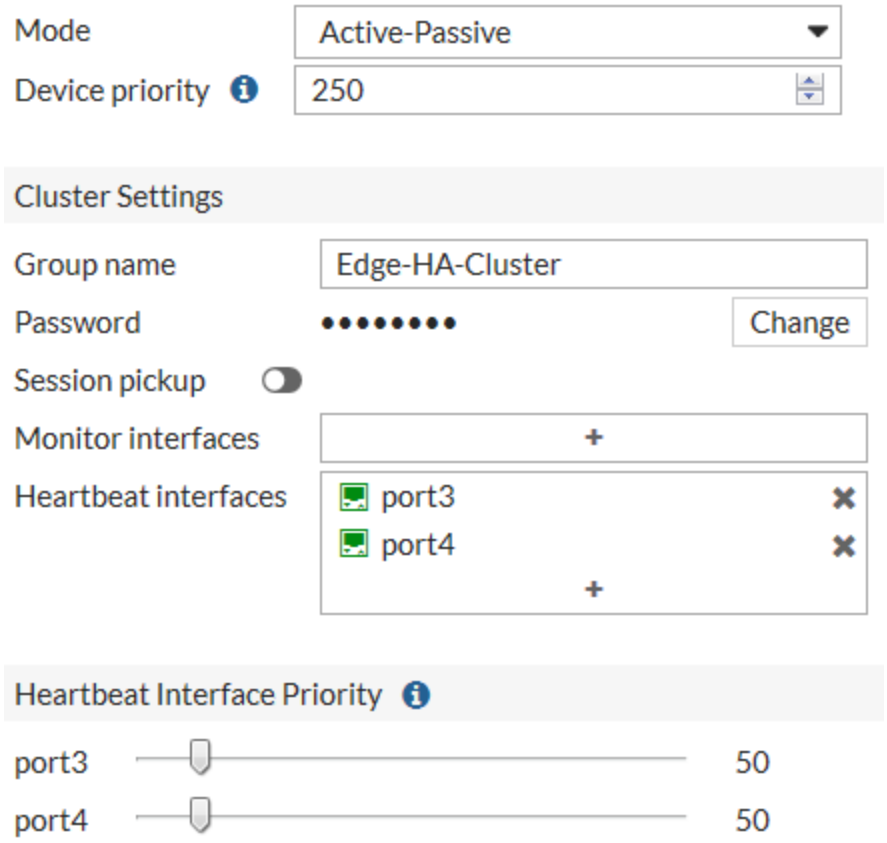
1. On the primary FortiGate, go to *System* > *Settings* and change the Host name to identify it as the primary FortiGate in the HA cluster.

2. Go to *System* > *HA* and set the Mode to Active-Passive. Set the Device priority to a higher value than the default (in the example, 250) to ensure that this FortiGate will always be the primary FortiGate. Also, set the group name and password.
3. Make sure you select the Heartbeat interfaces (in the example, the HA port if it exists; it does not have to use port3 or port4).

Single heartbeat interface:



Multiple heartbeat interfaces:



Configuring a backup FortiGate

1. On the backup FortiGate, go to *System* > *Settings* and change the Host name to identify it as the backup FortiGate in the HA cluster.

2. Go to *System* > *HA* and set the Mode to Active-Passive. Set the Device priority to a lower value than the primary (for example, 200) to ensure that this FortiGate will always be the backup FortiGate, only to be activated when the primary FortiGate is down. Also, set the group name and password.

You can use the FIC MFA service with a cluster of auth devices. Both single and multiple auth devices in a cluster are supported. You can add or remove auth devices on the FIC portal. For example, let's say you have a system admin who maintains multiple auth devices, and some of them are FortiGate HA cluster members. The system admin has set one FortiGate cluster member to be a standalone device. The FIC system admin can check if FortiGate standalone device has been removed from the FIC device cluster. If it still shows up in the cluster due to it being out-of-sync between FortiGate and FIC, the system admin can manually take it out.

Applications for third-party usage

- Web apps — https://docs.fortinet.com/document/fortiidentity-cloud/latest/rest-api/597289/web-app
- Management apps — https://docs.fortinet.com/document/fortiidentity-cloud/latest/rest-api/816036/management-app

The links above provide instructions on how to configure applications from the GUI and examples for how to use the applications with Python, Curl and Postman.

FortiCloud

As part of FortiCloud (FC) — the umbrella of Fortinet's Cloud service offerings, the top of the FortiIdentity Cloud portal provides a one-stop access to all services and resources available on FC as well as tools for managing your FC account, as shown in the screen capture below.

You can access the FortiCloud page by clicking your username (email address) in the upper-right corner of the FortiIdentity Cloud portal.

Your FortiCloud account

As shown in the image above, the upper-right corner of the FIC portal shows your FortiCloud account ID, which typically is the email address that you've registered on FC. Clicking your account ID or the down arrow next to it opens a drop-down menu with a list of options for managing your FC account.

Logging into an OU account

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

For more information about Organizations and OUs, see the Organization Portal Guide.

For more information on IAM, see the Identity & Access Management Guide.

To access Organizational Unit accounts with IAM user credentials:

1. In the upper-right corner of the FIC portal, click the ftc_iam drop-down and select an OU account.
2. Enter the username and password, and click LOG IN. A list of Organizational Units and member accounts is displayed.
3. 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.

To access Organizational Unit accounts with external IdP credentials:

1. Log in using your company's ID provider.
2. Select the Service Provider.
3. Select Organizations.
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.

Launching FortiIdentity Cloud

After your FortiIdentity Cloud (FIC) account is created, you can log on to the FIC portal from anywhere using a web browser and your login credentials.

Logging in as a regular FIC user

Regular FIC users are admin users that are created on FortiProducts (e.g., FortiGate, FortiAuthenticator, etc.).

To log in as a regular FIC user:

1. Start your web browser.
2. Point to https://fic.fortinet.com, and press the *Enter* key on your keyboard.
3. On the FortiIdentity Cloud landing page, click *LOGIN*.
4. Select *Email user*.
5. Enter your FIC *EMAIL* and *PASSWORD*.
   Note: The email address that you provided when creating your FIC account is your FIC username or account name. Be sure to use the same email address when logging in to the FIC portal.
6. Click *LOGIN AS EMAIL USER*.
7. Start your email application, open the email notification, copy the security code and paste it in the *SECURITY CODE* field, and click *GO*.
8. Click the desired FIC account (if you have more than one account) to open it.

Logging in as an IAM user

The Identity and Access Management (IAM) portal is an advanced feature of FortiCloud. An IAM user is one created by the super-admin of a FortiCloud account. IAM users of FIC can only assume the role of a sub-admin on the FIC portal.

To log in as an IAM user of FIC:

1. Start your web browser.
2. Point to https://fic.fortinet.com, and press *Enter* on your keyboard.
3. In the upper-right corner of the FortiIdentity Cloud landing page, click *LOGIN*.
4. Select *IAM user*.
5. Enter your *ACCOUNT ID/ALIAS, USERNAME* (email address), and *PASSWORD*.
6. Click *LOG IN AS IAM USER*.

FortiIdentity Cloud GUI

- Both the global admin and sub-admin users can access the FortiIdentity Cloud portal, but sub-admin users will not be able to see any data until the global admin has delegated realms to them.
- The global admin is the first account from your organization that has logged in to the FIC portal. The owner/user of the main FC account of your organization is your de facto FIC global admin.

The FIC GUI has the following main menus:

Menu	Description
Dashboard	Provides some key statistics about your account. The content of the page varies, depending on the type of license you are using. For more information, see Dashboard on page 95.
User Management	• *Users* — Shows information of your FIC users. See Managing users on page 103. • *User Groups* — Shows information of your FIC users. See Managing user groups on page 109. • *Realms* — Shows realms assigned to a sub-admin and provides tools for adding and deleting realms, viewing realm permission, and viewing or changing realm settings. See Managing realms on page 100. • *Administrators* — (Accessible to the global admin only) enables the global admin to create sub-admin groups and assign realms to them. See Managing admin groups on page 97.
Applications	*FortiProducts* — View and manage FortiProducts as authentication applications. See FortiProducts on page 111. *Web* — View and manage web applications. See Web Applications on page 114. *Management* — View and manage web applications. See Management Applications on page 116. *SCIM* — View and manage SCIM applications. See SCIM client integration on page 117. *SSO* — View and manage SSO applications. See Using SSO applications on page 138. *En-User Portals* — View and manage end-user portals. See Managing End-User Portal on page 172.
Authentication	• *User Source* — Configures user sources for SSO applications. See Adding user source on page 175. • *Domain Mapping* — Configures domain mapping for SSO applications. See Configuring domain mapping on page 178.

Menu	Description
Security Devices	• *Mobile Token*—Shows mobile tokens available in your realm or account, and provides tools for adding or deleting hard tokens. See Using mobile tokens on page 186. • *Hardware Token* —Shows hardware tokens available in your realm or account, and provides tools for adding or deleting hard tokens. See Using hardware tokens on page 187. • *Passkey* — View passkeys. See Using passkeys on page 190.
Logs and Report	*Usage* — Shows your account usage data. See Usage data on page 216. *Authentication Logs*— Shows your authentication event logs. See Authentication logs on page 216. *Management Logs*— Shows your management event logs. See Management logs on page 218. *SMS Logs*— Shows your SMS usage logs. See SMS logs on page 220.
Customization	*Templates* — Customize your FIC message templates. See Using templates on page 222. *Branding* — Customize the look and feel of your SSO applications or end-user portals. See Managing custom branding on page 225.
Settings	Opens the *Settings* menu which has the following options: • *Global* — Manage certain settings at the system level. See Managing global settings on page 228. • *Realm* — View and manage the settings of the selected realm. See Multi-Realm Mode on page 228. • *Alarm* — Create and manage alarm events. See Alarms on page 238. • *Alarm Routing* — Create and manage alarm receiver groups. See Alarm routing on page 239. • *Adaptive Auth* — Manage adaptive authentication profiles and policies. See Adaptive authentication on page 240. • *Certificates* — Manage Identity Provider (IdP) Signing Certificates. See Managing certificates on page 247.
Licenses	Shows all the licenses in your account. See Licenses on page 255. **Note:** This menu is visible to users of time-based subscriptions only, and is not available to users of credit-based subscriptions.
Help	The *Help* menu has the following options: • Contact Support • Purchasing Guide • SMS Rate • Online Help • FAQ • Status Monitoring

Dashboard

By default, the *Dashboard*page opens upon log-in. During a session, you can navigate to this page from any of the other pages by clicking *Dashboard* on the main menu.

The Dashboard presents the following information about your account:

Parameter	Description
FORTIPRODUCTS	The number of FortiProducts (e.g., FortiGate, FortiAuthenticator, etc.).
SMS CREDITS	The number of available SMS credits.
ALARM EVENT	The number of alert events that have been triggered vs. the number of alert events that have been configured.
EXPIRATION DATE	The date when your current license expires.
APPLICATIONS / MAX APPLICATIONS	The number of applications currently in your account vs. the maximum number of applications that your license can support.
USERS / MAX USERS	The number of users currently in your account vs. the maximum number of users that your license can support.
REALMS / MAX REALMS	The number of realms currently in your account vs. the maximum number of realms that your license can support,
Authentication Attempts	The most recent 10 authentication attempts over the past 30 days. See the following paragraph for details.

Last 10 authentication attempts in 30 days

This section of the Dashboard shows the 10 most recent authentication attempts over the past 30 days, with the following information about each log:

Column	Description
Timestamp	The date and time of the authentication event. **Note:** FIC captures the time of the event in UTC time, and then converts it to the client browser's local time which is the time shown in the timestamp.
Username	The username of the FIC end-user who requested authentication.
application	The authentication client that made the request.
Action	The type of authentication action.

Column	Description
Result	The outcome of the authentication request, which can be either of the following: • *Success* • *Failed*
Message	A system-generated message about the authentication request.

FIC extracts the data from its Authentication logs. You can sort the logs by clicking the column headers (except for the Result column) of the table.

Monitoring FIC status

FortiIdentity Cloud provides the monitor system for FIC's core service, includes API Services, Portal, FortiCloud Login, MFA, Email, SMS and FTM push. The monitor page shows the health status of those services in the past one month and current status. If customers have met any unexpected behaviors, both FortiIdentity Cloud team or customers can come to check the health status history. Based on the case, FIC team can do more investigation or customers can be notified of what happened in that period.

To access the Status Monitoring, select Help>Status Monitoring. In addition, you can access the the page directly by typing fic.fortinet.com/status.

Pagination for accounts with multiple sub-admin users

To avoid taking too long to query multiple sub-users within a master account all at once when logging in, FIC paginate the list of accounts by 5 per page.

Managing admin groups

Fortildentity Cloud has two levels of admins: global_admin (global administrator) and sub_admin (sub-administator). Anyone from a customer organization with a valid user account on FortiCloud (FC) can log on to the FIC portal using their FC username and password. By default, the FC account holder from your organization who logs onto the FIC portal first automatically becomes the global_admin of your FIC account. In addition, the main FC account holder of your organization is the de facto global_admin of your FIC account.

The *Administrators* menu is accessible to global_admin users only; sub_admin users will not be able to see this menu.

The *Administrators* page shows all the admin groups that the global_admin has created. It also provides the tools for the global_admin to manage admin groups. By default, all admins created by the global_admin become sub_admins.

You (the global_admin) can access the *Administrators* page by click *Administrators* on the main menu.

The following table highlights the information of sub-admin group configuration shown on the *Administrators* page.

Column Header	Description
NAME	The name of an admin group.
DESCRIPTION	The description of the group. (Optional)
LEVEL	The level of administration of the group: • *global_admin*—The highest level of administration. **Note:**The global_admin group is the default admin account, and cannot be deleted. • *sub_admin*—Any admin group that the global admin has added. Users in a sub-admin group are all sub-admin users. They can only access the realms assigned to their group, and manage the applications in those realms and the users on those applications .
MEMBER COUNT	The number of sub-admins in the group. **Note:** The numeric value indicates the number of users (sub-admins) in a given admin group. Clicking the value opens a pop-up window that shows the usernames, email addresses, and user IDs of those users.
Tools	The tool bar slides in from the right end of the row when you mouse over the entry in the table. It shows the following tools: • *Edit*—Edits the administrator group. • *Delete*—Deletes the administrator group.

- Creating a sub-admin group on page 98
- Adding users to the admin group on page 98

Creating a sub-admin group

1. Click *User Management* > *Administrators*, and click *Add Admin Group*.
2. Specify the group name.
   Note: The group name can only contain lower-case letters from "a" to "z" and/or numeric values from "0" to "9", and special characters such as underscore "_" and/or hyphen "-". It must be between 3 and 36 characters in length.
3. (Optional) Enter a brief description of the group.
4. Click *Save*.
   Note: The sub-admin group that you've just created appears on the Administrators page. Your then need to add sub-admin users and assign realms to the group, as discussed in the following sections.

Adding users to the admin group

You must have sub-admin users already in your account to add them to a sub-admin group.

1. Locate the administrator that you've just created, click the tool icon, and select *Edit*.
2. Click *Manage Admin*.
3. Select the admin(s), and click *Apply*.

Adding realms to the admin group

Once you have added sub-admins to a group, you must assign realms to the group to enable the sub-admins to manage the applications and FIC end users in those realms.

- Only the global admin can add realms to an admin group.
- You must have realms created first before assigning them to a sub-admin group. See Managing realms on page 100.
- Sub-admin users cannot see any data on the FIC portal until/unless the global admin has assigned realms to their group.

1. Click *Manage Realm*.
2. Select the realm(s), and click *Apply*.

Editing sub-admin group configuration

You can edit an admin group by changing its name and description, and/or by adding or deleting sub-admins and realms in the group.

1. Click *User Management* > *Administrators*.
2. Locate the group of interest.
3. Click the tools icon and select *Edit*.
4. Make the desired changes, and click *Apply*.

Deleting a sub-admin group

The global admin can delete any sub-admin group, except the default *'global_admin"* group. Also, when deleting an admin group with sub-admins in it, you must delete the sub-admin users from the group first before deleting the group.

1. Click *User Management* > *Administrators*.
2. Locate the admin group.
3. Click the tool icon, and click *Delete*.
4. Click *Yes*.

Managing realms

In Fortildentity Cloud, a realm is a container that has a set of users that can be referenced to other users in the same realm and can be controlled by the same realm settings, including MFA method and adaptive auth profile. With realms, admin users can control settings such as user quota and MFA method. FIC comes with a default realm for your convenience.

The *Realms* page shows information about the realms under your management. It also provides tools for managing realms. If you are a global admin, you can see all realms assigned to all sub-admin groups in your account; if you are a sub-admin user, you can see the realms assigned to your sub-admin group only.

You can open the *Realms* page by clicking *User Management* > *Realms*.

The following table highlights the information on the *Realms* page.

Parameter	Description
Check box	Enables you to select a realm. **Note:** The *Delete* button above the table becomes activated when a realm is selected. You can click the button to delete the realm. Alternatively, you can delete a realm by clicking the corresponding *Delete* icon in the Actions column. For more information, see Deleting a realm on page 101.
NAME	The name of a realm.
USER COUNT	The number of users in the realm.
USER QUOTA	The number of user quota allocated to the realm.
DESCRIPTION	A brief description about the realm that the global admin added when creating the realm.
APPLICATION COUNT	The number of applications assigned to the realm.
Tool	The tool bar slides in from the right end of the row when you hover the cursor over an entry. It has the following tools: • *Edit Realm*—Edits the name and/or description of the selected realm. If you are on a time-based subscription, you are also able to set or change the user quota allocation to the selected realm within the set value range. • *Refresh Realm*—Get the latest data about the realm. • *Show Permission*—Opens a dialog which shows the sub-admin groups that have access to the realm. You can also remove sub-admin groups from the access list by deleting them. • *Settings*—Opens the Settings page which shows the settings of the realm. See . • *Delete*—Deletes the realm. See Deleting a realm on page 101.

- Viewing realm permission on page 102
- Removing sub-admin groups from a realm access list on page 102
- Viewing realm settings on page 102

Creating a custom realm

1. Click *User Management Realms*.
2. Click *Add Realm*.
3. Specify the name of the realm.
4. (Optional) Enter a brief description.
5. Click *Save*.
6. On the *Realms* page, locate the realm that you have just created.
7. Click the tool icon, and select the *Edit*.
8. Set the user quota to be allocated to the realm.
9. Click *Save*.

Editing a realm

1. On the *Realms* page, identify the realm.
2. Click the tool icon, and select *Edit* .
3. Make the desired changes to the realm name and the description.
4. Click *Save*.

Deleting a realm

1. On the *Realms* page, identify the realm.
2. Click the tool icon, and select *Delete*.
3. Click *Yes*.

- The default realm cannot be modified or deleted.
- If a realm has applications assigned to it, you must delete the applications from the realm before deleting the realm.

Viewing realm permission

1. On the *Realms* page, identify the realm.
2. Click the tool icon, and select*Show Permission*.
3. View the sub-admin groups that have access to the realm in the *Access List for Realm* dialog.
4. Click *Close. when done.*

Removing sub-admin groups from a realm access list

1. On the *Realms* page, identify the realm.
2. Click the tool icon, and select *how Permission*.
3. In the *Access List for Realm* dialog, identify the sub-admin group(s), and click the **X** sign *(Delete)*.

Viewing realm settings

1. On the *Realms* page, identify the realm.
2. Click the tool icon, and select *Settings*.

Managing users

The term "users" refers to end-users of FortiIdentity Cloud. The *Users* page displays the following information about FIC end-users in your account. You can open the *Users* page by clicking *Users* on the main menu.

Column	Description
Checkbox	This checkbox only applies to users who use FTM for MFA. It enables you to select a user, and then click the *NEW FTM TOKEN* button to request a new FTM token for the user. See Getting a new FTM token on page 107.
USERNAME	The username of the user.
STATUS	The status of the user, which can be a combination of any of the following: •  **(active)**—The user is enabled. **Note:** By default, all new users are enabled to use FIC for MFA. The FIC administrator can click this button to quickly deactivate a user when necessary. For more information, see the following bullet. •  **(disabled)**—This button enables the administrator to temporarily stop the user from using FIC. **Note:** If a user is disabled, FIC will deny all log-in requests from the user. It must be noted that disabling a user only prevents the user from using FIC, but does not remove the user from your account. FIC will continue counting it toward your user quota for the user until the user is removed from your account. The admin user can also click this button to enable the user if the user is disabled. •  **(locked)**—The user is locked out. **Note:** FIC locks a user out when the user has exceeded the specified maximum number of log-in attempts allowed. See Managing realm settings on page 231. •  **(unlocked)**—The user is unlocked. **Note:** FIC automatically unlocks users based on their lockout settings. The admin user can also manually unlock a locked user by clicking the  **(locked)** button. •  (Temporary token deactivated)—Temporary token is deactivated.  (Temporary token activated)— Temporary token is activated. •  **(pending)**—A token assigned to the user has not been activated yet. •  **(expired)**—The user's token activation code has expired. •  **(bypass)**—The user is allowed to bypass MFA.

Column	Description
	•  **(no bypass)**—The user is not allowed to bypass MFA. **Note:** The admin user can enable MFA bypass on a user from here only if *Enable Bypass* is enabled on the *Settings* page. See Managing realm settings on page 231. Otherwise, when you click the  **(no bypass)** icon, a tool tip will appear asking you to turn on *Enable Bypass on the Settings* page.
MFA	The MFA method used by the user, which can be one of the following: • *FTM* (soft token) • *Email* • *SMS* • *FTK* (FortiToken, a hardware token)
NOTIFICATION	The method by which FIC sends FTM token activation/transfer notifications to the user, which can be either of the following: • *Email*—FIC sends FTM token activation/transfer notifications to the user's email address. • *SMS*—FIC sends FTM token activation/transfer notifications by SMS to the user's mobile phone. **Note:** If the user's notification method is set to SMS, make sure that the mobile phone number in the system is valid, and that you have enough credits in your account to send OTPs by SMS. For more information, see Managing realm settings on page 231.
EMAIL	The user's email address. **Note:** The admin user is able to edit users' email addresses.
MOBILE PHONE	The user's mobile phone number, if available. **Note:** The phone number must be in the format of "+ Country Code Area Code Phone Number", e.g., +1 4082221234. You can edit an end-user's mobile phone numbers.
REALM	The realm where the user resides.
TYPE	User type: remote or local
REF COUNT	The number of applications with referenced to the user.
LAST LOGIN	The timestamp of the user's last successful login.
Tool	The tool bar slides in from the right end of the row when you hover the cursor over an entry. It has the following options: • *Edit* — Edits the user's settings. • *Manage Passkey* — Manages the user's passkeys. • *Delete* — Deletes the user.

- Batch-adding users on page 105
- Enabling Auto-alias by Email on page 105
- Adding user aliases on page 106
- Auto-assigning FTKs to selected users on page 106

Batch-adding users

1. Click *User Management >Users*.
2. Click *Batch Add* .
3. Select a realm.
4. Enter the user's username, email, and mobile phone number.
5. Click the + sign.
6. Click *Save*.

All users you have entered are added to the Users page at once.

Alternatively, you can add multiple users all at once by downloading the `Users_template.csv` file, filling it out with the required user information, and then uploading it to FIC.

To batch-add users using the Users_template:

1. Click *User Management > Users > Batch Add*.
2. Click *Download CSV Template*.
3. Open the `Users_template.csv` file, and populate it with the username, email address, and mobile phone number of the user(s) to be added.
4. Save the file.
5. Click *Upload CSV file*.
6. Click *Save*.

Enabling Auto-alias by Email

Many FIC end-users have different usernames in different applications and different domains. By the same token, a single FIC user may have different usernames in different FIC applications. For example, John Doe II may have the following usernames:

- `user1` in VPN
- `user_one` in a web app
- `u1` as a system admin
- `user1@company.com` on an email server

FIC allows for different usernames to be attributed to the same user (i.e., same person) so that only one token (FTM or FTK) needs to be assigned to the same user. It does this by providing an Auto-alias by Email option, which, once turned on, enables FIC to automatically put usernames into an alias if they use the same email address.

Auto-alias by Email is disabled by default, but you can enable it using the following procedures:

1. Click *Settings>Realm>General*.
2. Scroll down until you see *Auto-alias by Email* and select it.

Once *Auto-alias by Email*is enabled, all usernames with the same email address are automatically set as an alias under the same username.

It is important to note that aliased users must be in the same realm. Usernames with the same email address but are in different realms are still set as unique users, even when the auto-alias feature is enabled.

Adding user aliases

The *Add User Alias* button becomes available only when *Auto-alias by Email* is enabled on the*Settings* page of a realm. It enables you to select users of interest on the *Users* page, and group them together using an alias. Aliased users show up in boldface on the *Users* page.

1. Click *User Management>Users*.
2. Select the users of interest.
3. Click *Add User Alias*.
4. Choose a base user.
5. Click *Yes*.

Auto-assigning FTKs to selected users

The *Auto-Assign FTK* button enables FIC to automatically assign hardware tokens to selected users.

1. Click *User Management > Users*.
2. Select the user(s).
3. Click *Auto-Assign FTK* .
4. Click *Yes*.

Getting a new FTM token

You can request a new FTM token for an end-user only if the user's current MFA method is FTM.

1. Click *User Management* > *Users*.
2. Select the user(s).
3. Click *New FTM Token*.
4. Click *Yes*.

Hiding/showing full FortiAuthenticator username

By default, the usernames of FIC users created on FortiAuthenticator (FAC) show up with prefixed and suffixed characters in corner brackets on the FIC GUI. This is due to the fact that FAC differentiates the same username populated by multiple user sources. The *Users* page provides an option to let you toggle between showing and hiding those extra characters.

To hide/show the extra characters in the usernames of users added on FAC, click *Hide/Show Full FAC Username*.

Viewing a user's applications

1. Click *User Management* >*Users*.
2. Identify the user of interest.
3. Click the numeric value in the *REF COUNT* column.

Using a temporary token

The temporary token feature enables end-users, who do not have their authentication devices with them, to use MFA function temporarily. The Temporary Token icon can be found in the *Users* >*Edit* page. The Temporary Token icon is greyed out when the feature is disabled, and turns green when it is enabled. When activated, the user will receive OTP for MFA authentication either by email or SMS. Temporary token is deactivated when the user is using an authentication device for MFA authentication, or when the temporary token has expired.

To assign a temporary token to a user:

1. *Click User Management > Users*.
2. Locate the user, click the tool icon, and select *Edit*.
3. In the *Status* field, click the grey temporary token icon.
4. Select a*Temporary Auth Method*, and set the *Expiration Time*.
5. Click *Apply*.

Editing a user

1. Click *User Management >Users*.
2. Locate the user.
3. Click the tool icon and select *Edit*.
4. Make the desired changes as described in the following table, and click *Apply*.

Changes that you've made here become effective when you click *Apply*. An error message will pop up if the system encounters an error when validating the changes. In that case, you must correct the error and try to apply the changes again.

Deleting users from FIC

- Before deleting a user, pay special attention to the confirmation message.
- Make sure that the user is not in use any more. Deleting a user in use will result in authentication failure of the user.
- The same user may be referenced by multiple Fortinet devices. Make sure that the user is not in use by any other Fortinet devices before deleting it.

Users that are deleted from a FortiGate can still show up on the FIC portal if the two are out of sync. To prevent this, you can either run the `execute fortitoken-cloud sync` command on the FortiGate or remove users directly from the FIC portal.

1. Click *User Management > Users*.
2. Highlight the user that has already been deleted from FortiGate.
3. Click the tool icon and select *Delete*.
4. Click *Yes*.

Managing user groups

The *User Groups* page shows the user groups that you have created. It shows the following information:

Parameter	Description
NAME	Name of the user group.
DESCRIPTION	Description of the group.
REALM	Realm the user group is associated with.
USER COUNT	Number of users in the group.
Tool	• Edit. See Editing a user group on page 109. • Delete. See Deleting a user group on page 110.

Adding a user group

1. *Click User Management >User Groups*.
2. Click *Add User Group*.
3. Under the *Group Information* tab, enter the required information, and click *Next*.
4. Under the *Users* tab, select the user(s) and click *Next*.
5. Under the *Permissions* tab, select an option in the *CUSTOMIZED PERMISSION* column.
6. Click *Save*.

Editing a user group

1. Click *User Management >User Groups*.
2. Identify the user group.
3. Click the tool icon, and select *Edit*.
4. Make the desired changes.
5. Click *Save*.

Deleting a user group

To delete a user group, you must remove all users from the user group first.

1. Click *User Management >User Groups*.
2. Identify the user group.
3. Click the tool icon, and select *Edit* .
4. Delete all users in the group. to remove them from the user group.
5. On the *User Groups* page, click the tool icon and select *Delete*.
6. Click *Yes*.

FortiProducts

The *FortiProducts* page shows information about all Fortinet products as applications in your FIC account. You can open the *FortiProducts* page by clicking *Applications* > *FortiProducts* on the main menu.

The following table highlights the information on the *FortiProducts* page.

Column	Description
Checkbox	Unchecked by default. If checked, the application becomes selected and the *DELETE* button is enabled. You can then click the *DELETE* button to remove the selected applications. For more information, see Deleting a FortiProduct on page 112. **Note:** You can select all the applications at once by checking the checkbox in the column header.
ALIAS	The alias of the application.
NAME	The name of the application.
TYPE	The type of application, which can be any of the following: • *FortiAuthenticator* • *FortiGate* • *FortiGateVM* • *FortiSandbox* **Note:** FIC assigns applications type based on the serial number and model of the product.
COUNT	The number of FIC end-users on the applications. **Note:** Clicking the numeric value opens a dialog which shows the list of FIC end-users on an applications, along with some basic user information.
REALM NAME	The name of the realm to which the applications is assigned.
Tools	The tool bar slides in from the right end of the row when you hover the cursor over an entry. It provides the following tools: • *Edit* — Change certain settings of the application. • *Details* — Shows some detailed information of the application. • *Delete* — Deletes the applications.

- FIC is able to detect an FortiGate device as soon as the FIC API activates it for FIC, and populates the applications page with information of the device.
- You can sort the table by clicking any of the column headers.

Editing a FortiProduct

1. Click *Applications >FortiProducts*.
2. Identify the FortiProduct.
3. Click the tool icon, and select *Edit*.
4. Make the desired changes.
5. Click *Apply*.

Viewing additional information about an application

1. On the *FortiProducts* page, identify the FortiProduct.
2. Click the tool icon, and select *Details*.

Deleting a FortiProduct

Deleting an application removes all FIC end-users from it unless a user is also on another application.

1. *Click Applications > FortiProducts*.
2. Identify the FortiProduct.
3. Click the tool icon, and select *Delete*.
4. Be sure to read the message.
5. Click *Yes*.

Assigning a FortiProduct to a realm

A FortiProduct must be assigned to a realm. Otherwise, you cannot add users to or sync users from it. For more information, see Managing realms on page 100.

1. Click *Applications > FortiProducts*.
2. Locate the unassigned FortiProduct.

3. Click the tool icon, and select *Edit* .
4. Click the *Realm* drop-down menu, and select a realm.
5. Read the message.
6. Click *Yes*.
7. Click *Apply*.

Web Applications

The *Applications Web* page enables you to manage web applications in your account. You can open the page by clicking *Applications* > *Web* on the main menu.

The following table highlights the information on the *Web* page.

Parameter	Description
NAME	The name of a web app.
CLIENT ID	A unique, read-only ID that FIC has generated for an application.
COUNT	The number of FIC end-users on the application.
REALM NAME	The name of the realm to which the application is assigned.
SECRETE	Part of the secret. **Note:** Click the icon to regenerate the secret for the application.
AUTH SCOPE	Can be either of the following: • Self • Realm
LAST UPDATE	The time when the application was last updated.
Tools	The tool bar slides in from the right end of the row when you hover the cursor over an entry. It provides the following tools: • *Edit*—Edits the settings of a web app as application • *Delete*—Deletes the web app as application.

- Adding a web app on page 114
- Regenerating API credentials on page 115
- Editing a web app on page 115
- Deleting a web app on page 115

Adding a web app

When a new application is added, FIC assigns it the default name *"MyAuthClient"* which can be edited. If you add more applications of the same type, FIC will append a sequence number starting with "1" to the subsequent application names, e.g., *"MyAuthClient1", "MyAuthClient2",* and so on.

You need to select a realm from the list of realms in your account and assign the new application to it. Otherwise, the application will be assigned to the default realm. You must assign the application to a custom realm to add end-users to it.

When creating an application, FIC generates a unique read-only Client ID. It also generates the API credentials which the application needs when accessing the FortiIdentity Cloud API server.

Paid customers have full access to FortiIdentity Cloud APIs; trial customers only have limited access to the APIs with certain restrictions. For more information, refer to Trial account API request limit on page 40.

1. Click *Applications* > *Web*.
2. Click *Add Web Application*.
3. Make the required entries or selections.
4. Click *Save*.

Regenerating API credentials

1. Click *Applications* > *Web*.
2. Locate the web application.
3. In the *SECRETE* column, click the *regenerate secret* icon, and select either of the following:
   - *Display on portal*—Shows the secret on the GUI.
   - *Send to email*—Sends the secret to the email address that you have specified. You must open the email to retrieve it. The email message contains instructions on how to use the secret.
4. Click *Save*.

Editing a web app

1. Click *Applications* > *Web*.
2. Locate the web application.
3. Click the tool icon, and select *Edit*.
4. Make the desired changes.
5. Click *Save*.

Deleting a web app

1. Click *Applications* > *Web*.
2. Locate the web application.
3. Click the tool icon, and select *Delete*.
4. Read the message.
5. Click *Yes*.

Management Applications

In FortiIdentity Cloud, a management application is a special type of web application. It is a solution for remote API access and management of customer resources, such as realms, applications, users, and tokens, etc. You can set the scope of management applications to your entire account or the realm that you specify.

Creating a management application

1. Click *Applications* > *Management*.
2. Click *Add Mgmt Application*.
3. Specify the name of the application.
4. Select a *Management Scope*.
5. Click *Save*.

Regenerating management application secret

1. Click *Applications* >*Management*.
2. Identity the application.
3. In the *SECRET* column, click the regenerate icon.
4. Select a method for receiving the new secret.
5. Click *Save*.

Deleting a management application

1. Click *Applications* >*Management*.
2. Identify the application.
3. Click the tool icon, and select *Delete*.
4. Read the message.
5. Click *Yes*.

SCIM client integration

Fortildentity Cloud has integrated with SCIM client applications. SCIM, which stands for System for Cross-domain Identity Management, is an open standard for cloud-based user provisioning. SCIM provides a standardized, secure methodology for exchanging information between IT systems or identity domains. This ensures interoperability across domains without expensive custom integrations. SCIM auto-provisioning increases productivity across the entire organization. Besides freeing up IT resources to focus on more mission-critical tasks. SCIM, in tandem with access management systems, can reduce the time needed to grant access to backend infrastructure and boost employee productivity at the same time.

Features and benefits

FIC and SCIM client integration offers the following features and benefits:

User provisioning

Automated creation of user accounts in target systems based on changes in the identity provider (IdP). When a new user is added to the IdP or updates are made to existing user attributes, the SCIM server communicates these changes to the connected applications or services, ensuring that user accounts are consistently provisioned across the ecosystem.

User deprovisioning

When a user is deactivated or removed from the identity provider, the SCIM server ensures that corresponding actions are taken in connected systems to deactivate or delete the user account.

Attribute synchronization

Synchronize user attributes (such as name, email, group memberships, roles, etc.) between the identity provider and connected systems. Changes made to user attributes in one system are propagated to other systems, ensuring consistency and accuracy of user data across the organization's IT infrastructure.

Group management

Manage user groups and their memberships across different systems. Group-provisioning and deprovisioning functionalities enable organizations to efficiently manage access permissions by automatically updating group

memberships based on changes in the identity provider.

Security

Implement security measures such as authentication, authorization, and secure communication protocols (e.g., HTTPS) to ensure the confidentiality, integrity, and availability of sensitive identity data exchanged between systems.

Standards compliance

SCIM is built on standard web protocols such as HTTP and JSON, making it interoperable with and widely supported by various identity management solutions, cloud services, and applications. A SCIM server streamlines identity management processes, reduces manual effort, enhances security, and improves the efficiency of user lifecycle management in organizations with complex IT environments. Compliance with SCIM specifications ensures seamless integration and compatibility with other SCIM-compliant systems.

Supported SCIM client applications

FIC and SCIM integration involves configuration of FIC as the SCIM server and one or more SCIM-compliant cloud-based applications as SCIM clients. For current release, FIC has been fully tested with the following SCIM client applications:

- Okta
- Azure
- FortiAuthenticator

FortiIdentity Cloud is fully compliant with SCIM specifications and, therefore, can work with any SCIM client application on the market.

Use case

Imagine a large multinational corporation with offices spread across the globe. Each office has its own identity management system, handling employee accounts, permissions, and access to resources. However, managing user identities across these disparate systems is not an easy task. This is where SCIM comes in handy.

In this scenario, the corporation decides to implement SCIM to streamline the management of user identities across all its offices. Here's how it works:

- Centralized identity management — With SCIM, the corporation can establish a central identity management system that serves as the authoritative source of user identities. The system contains a master user directory where all employee identities are stored.

- Automated user provisioning — Whenever a new employee joins the company, their information is entered into the central identity management system. SCIM allows for automated provisioning, meaning that user accounts can be automatically created in the various office-specific identity systems without manual intervention.
- Consistent user data — SCIM ensures that user data remains consistent across all systems. If an employee updates their profile information (such as changing their job title or contact details), those changes are automatically propagated to all relevant systems via SCIM.
- Simplified access management — With SCIM, access permissions can be managed centrally. When an employee leaves a company or changes roles in the company, access privileges are updated in real time across all the systems, reducing the risk of unauthorized access.
- Interoperability — SCIM provides a standardized way for different identity management systems to communicate with each other. This ensures interoperability between systems from different vendors, allowing the corporation to use the best-in-class solutions for each office while still maintaining a cohesive identity management strategy.
- Audit trail and compliance — SCIM provides a comprehensive audit trail, allowing administrators to track changes to user identities and access permissions. This is crucial for compliance purposes because it ensures that the corporation meets regulatory requirements related to data security and privacy.

Overall, by implementing SCIM, the corporation can achieve greater efficiency, consistency, and security in managing user identities across its distributed infrastructure

Integrating FIC with SCIM clients

Suppose your organization is using Okta, Azure, and/or FortiAuthenticator to manage user identity, you must integrate these applications with FIC and sync their users or user groups to FIC. In so doing, you are turning FIC into a SCIM server and those applications SCIM clients. The integration enables end-users of those applications to authenticate themselves through FIC — the SCIM server.

FIC-SCIM client integration requires the following two major steps:

1. Configure FIC as the SCIM server.
2. Configure one or more SCIM client applications (i.e., Okta, Azure, or FortiAuthenticator) as SCIM client(s).

For detailed steps for configuring the SCIM server and SCIM clients, refer to the following sections:

- Configuring FIC as SCIM server on page 119
- Configuring Okta as SCIM client on page 120
- Configuring Azure as SCIM client on page 120
- Configuring FortiAuthenticator as SCIM client on page 120

Configuring FIC as SCIM server

1. Go to https://FIC.fortinet.com.
2. From the main menu, select *Applications* > *SCIM*.
3. Select *Add SCIM Application*.
4. Make the desired entries or selections.

5. Click *Save*.

Configuring Okta as SCIM client

1. Log into your Okta admin account.
2. Select *Application* > *Browse App Catalog*, search for SCIM 2.0 Test App (Header Auth), and add the application.
3. Select *Add Integrations* > *Provisioning* > *Enable API integration*, and configure the following:
   a. Base URL: https://fic.fortinet.com:9696/api/v2/scim/
   b. API Token: (Bearer+space-Copied Secret)
   c. Click Test API Credentials
4. Assignments:
   a. Add the users (Tom/Mike) or group.
   b. Remove the users or group.

Configuring Azure as SCIM client

1. Go to https://portal.azure.com, and log into your corp account.
2. Click *Enterprise Applications* > *New Applications* to create a new application.
3. Upon creation of the new application, click *Provisioning* > *Select Automatic* > *Admin Credentials*, and configure the following:
   a. Tenant URL: https://fic.fortinet.com:9696/api/v2/scim/
   b. Secret Token: Copied Secret
   c. Test Connection
4. Manage users and groups:
   a. To add a user or group, click *Add user/group*, select the user or group, and click *Assign*.
   b. To remove a user, select the user and remove the assignment.

Configuring FortiAuthenticator as SCIM client

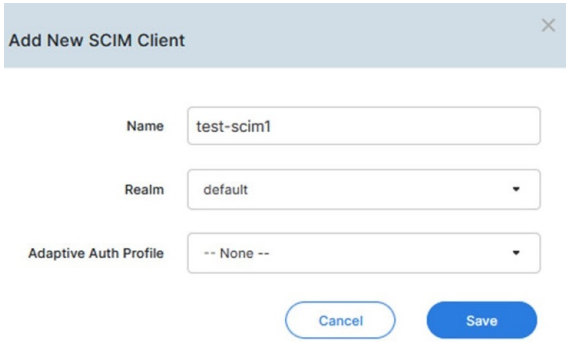
1. Log into your FAC admin account.
2. Click *Authentication* > *SCIM* > *Service Provider* >*Create New*.
3. In the *Create New SCIM Service Provider* window, configure the following:
   a. Name:test-scim
   b. SCIM endpoint: https://fic.fortinet.com:9696/api/v2/scim/
   c. Access Token: copied secret
4. Click *Sync* to automatically add exiting users to the SCIM server.

Demo configurations

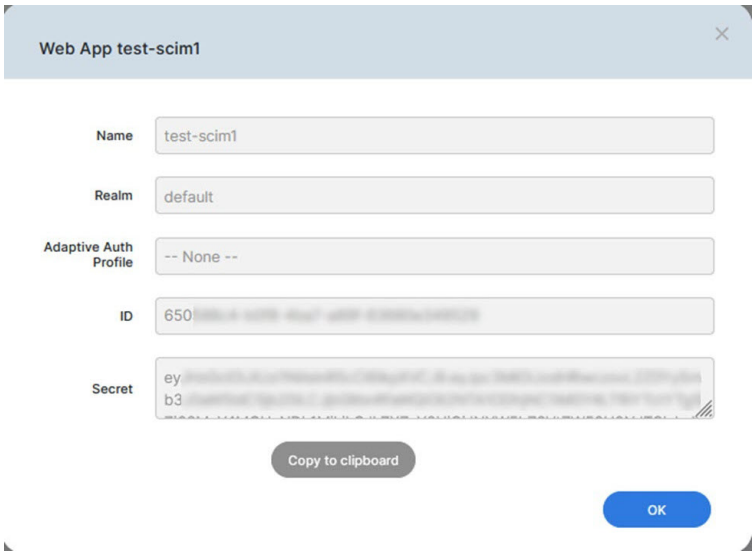
This sections provides sample configurations for FIC and SCIM client integration.

Demo: Configuring FIC as the SCIM server

1. Go to http://fic.fortinet.com and log in.
2. Click *Applications>SCIM >Add SCIM Application,* and configure the following:



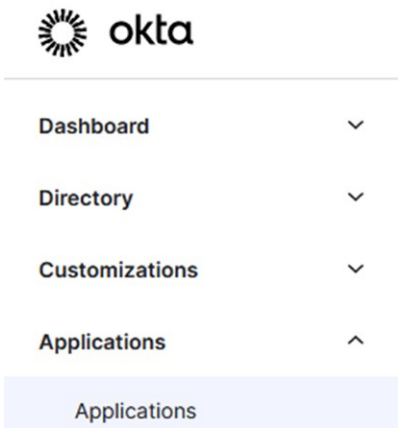
   - *Name:* test-scim1, for example
   - *Realm :* <default>
   - Adaptive Auth Profile: --None--
3. Click *Save*. The following page opens.



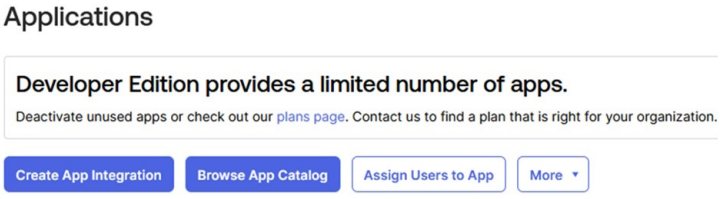
4. Copy the secret. Be sure to apply the secret to the SCIM clients (i.e., Okta, Azure, or FortiAuthenticator) that you are going to configure.

Demo: Configuring Okta as SCIM client

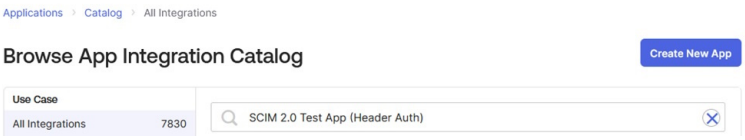
1. Go to http://okta.com, and log in with your Corp account.



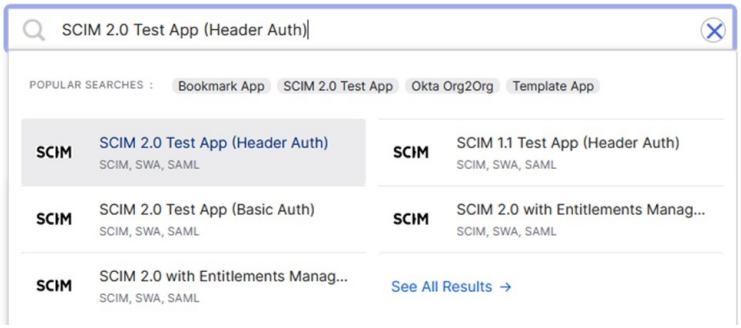
2. Click *Applications* > *Browse App Catalog*.



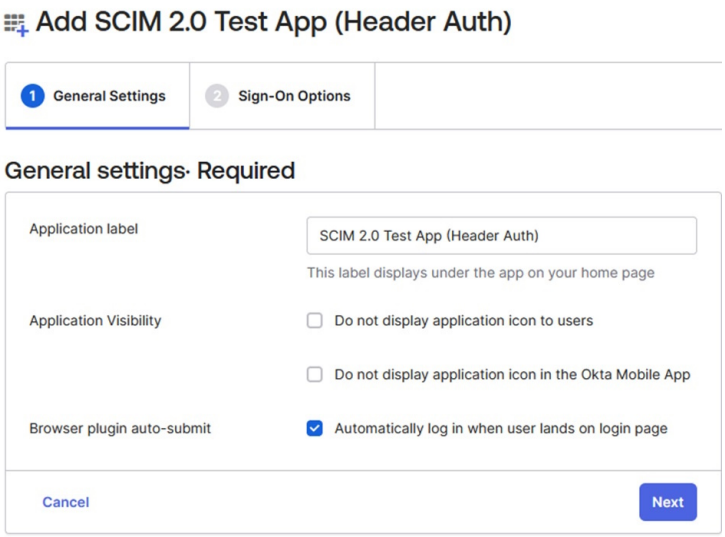
3. Search for *SCIM 2.0 Test App (Header Auth)*.



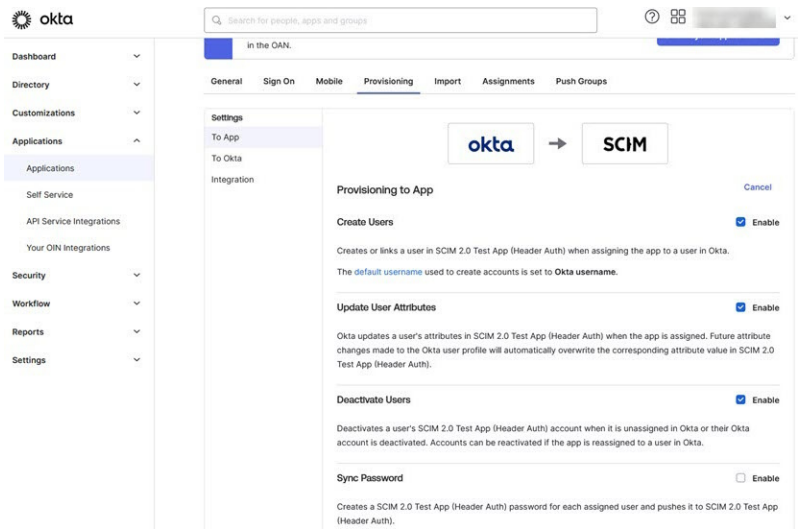
4. Click *SCIM 2.0 Test App (Header Auth)* and *Add Integration*.



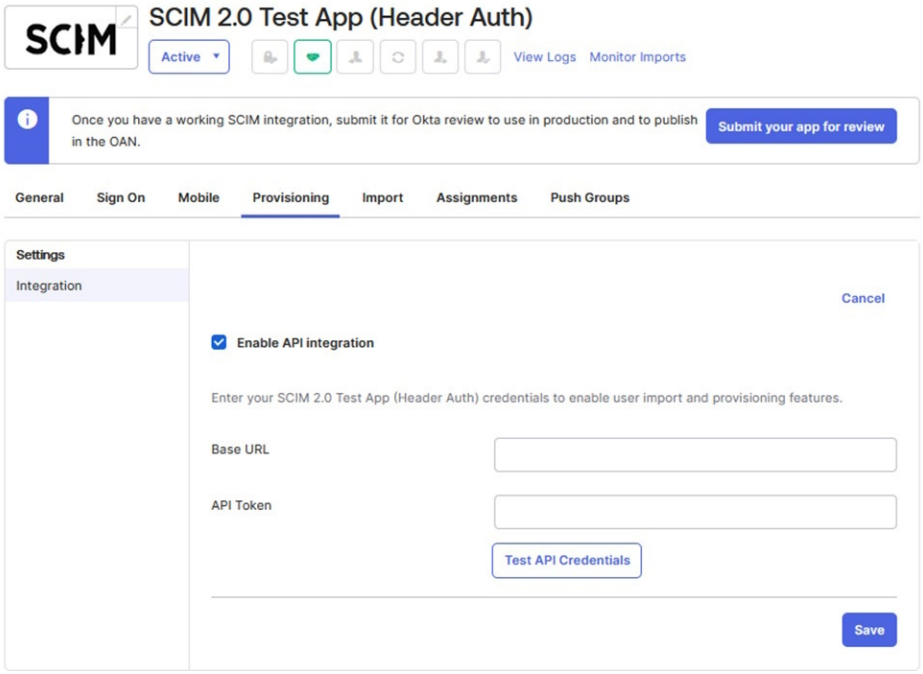
5. Okta Add SCIM Provisioning:
   a. After your integration is created, click the *General* tab.
   b. Click Edit.
   c. In the *Provisioning* section, select *SCIM* and click *Save*.



6. Choose Provisioning options:
   - From the integration settings page, choose the *Provisioning* tab. The SCIM connection settings appear under *Settings Integration*.



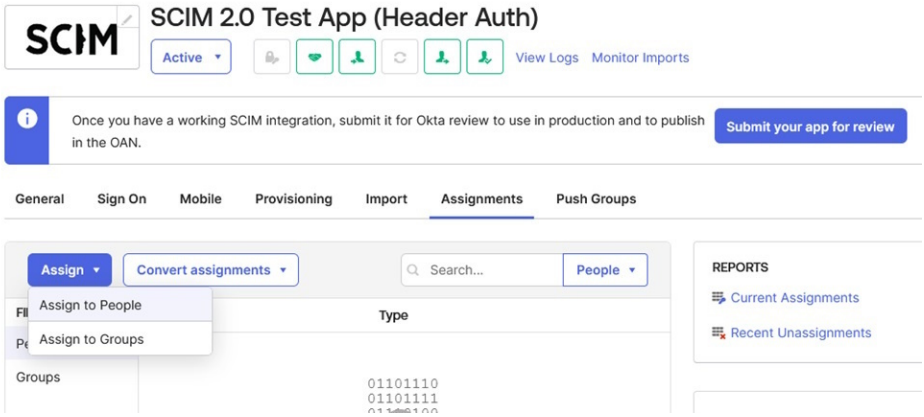
7. Click *Edit*.
   - Specify the SCIM connector base URL and the field name of the unique identifier for your users on your SCIM server.



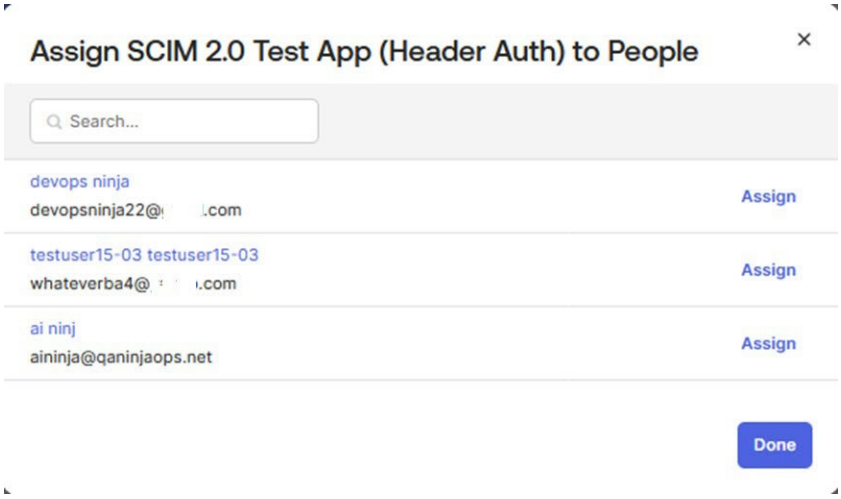
   Base URL: https://FIC.fortinet.com:9696/api/v2/scim/

   API Token: (Bearer+space-Copied Secret)

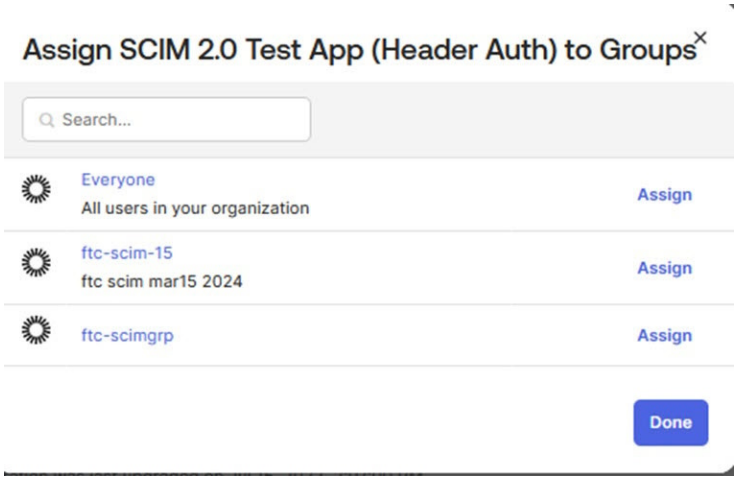
8. Assign the users to the applications by selecting *Applications* > *Assignments* > *Assign to People*, and click *Assign*.



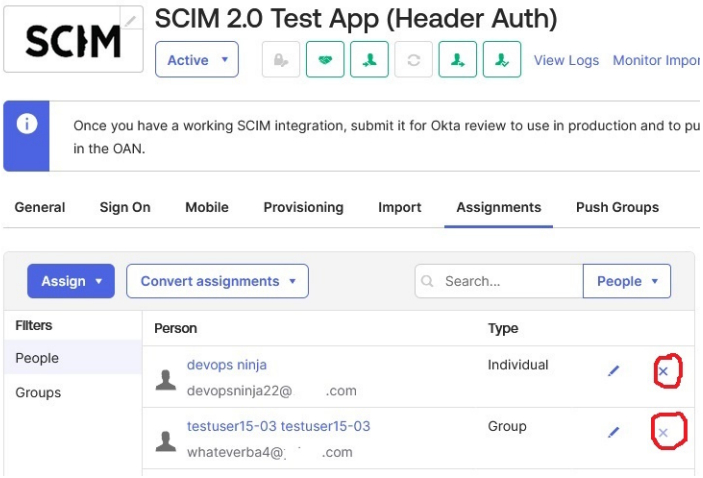
9. Add the users:
   a. Create the Okta new user and add the email id field.



10. Add the groups:
   a. Create the okta new group and add the user to the group
   b. Assign the users to the applications by selecting *Applications* > *Assignments* > *Assign to group*, and *Assign*.

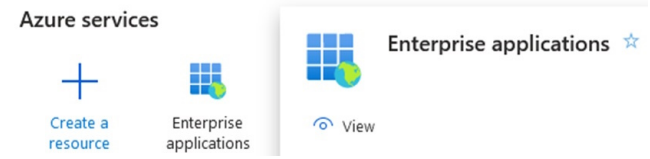


11. Remove the users and groups from the app:
    a. Click the X button remove the user or group.

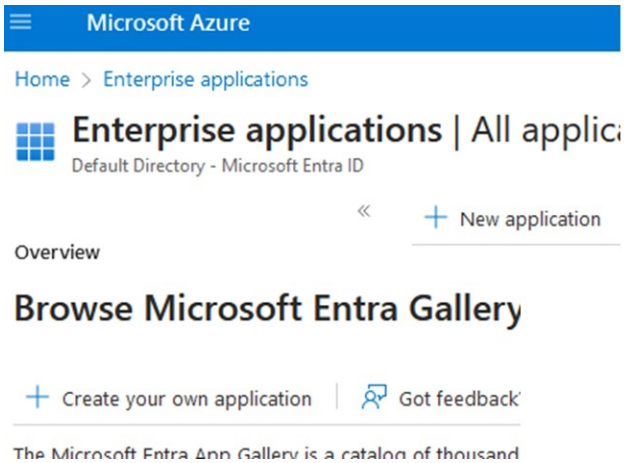


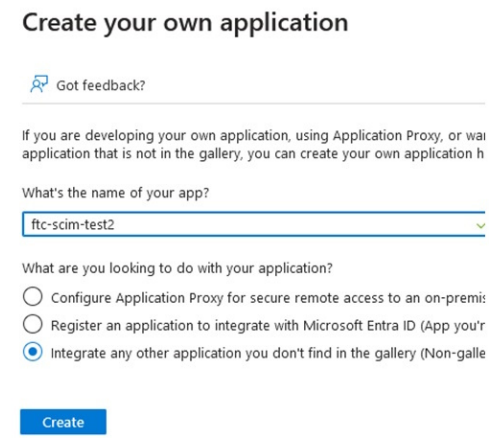
Demo: Configuring Azure as SCIM client

1. Go to https://portal.azure.com.
2. Click *Enterprise Applications*.

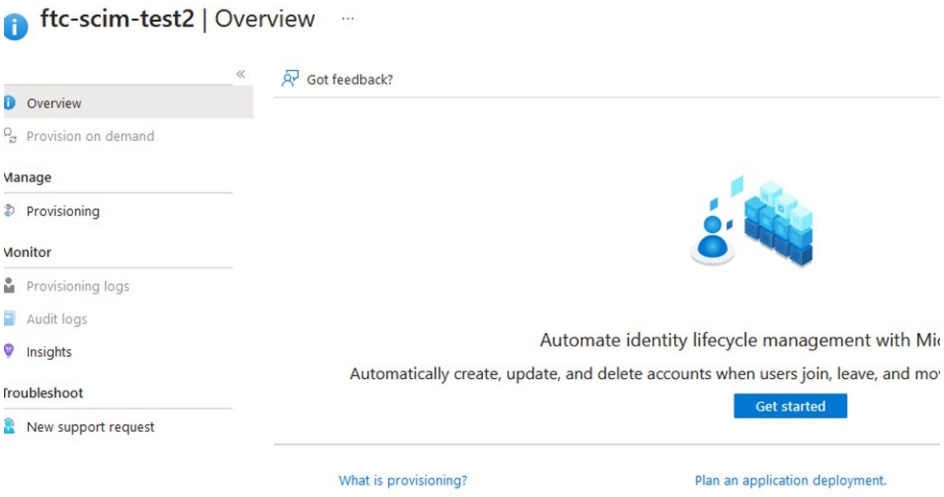


3. Click *Create your Own applications*.

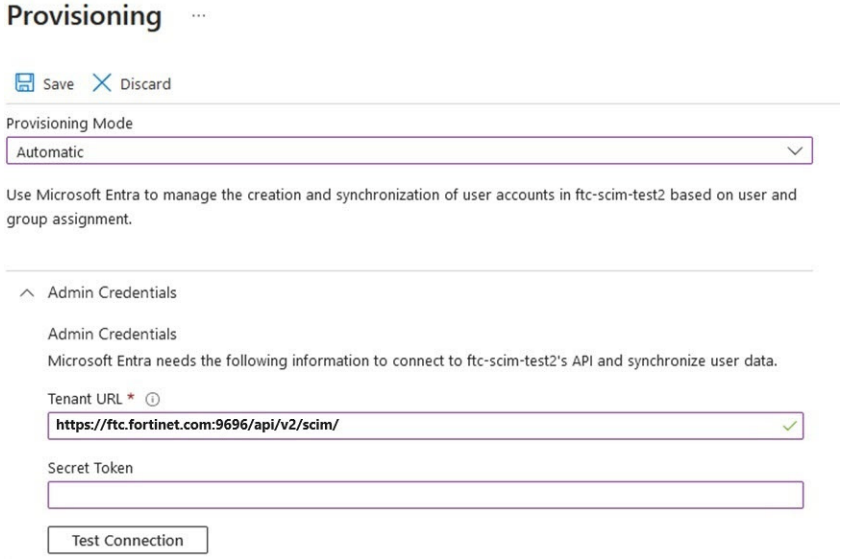




4. Review the application that you've just created.

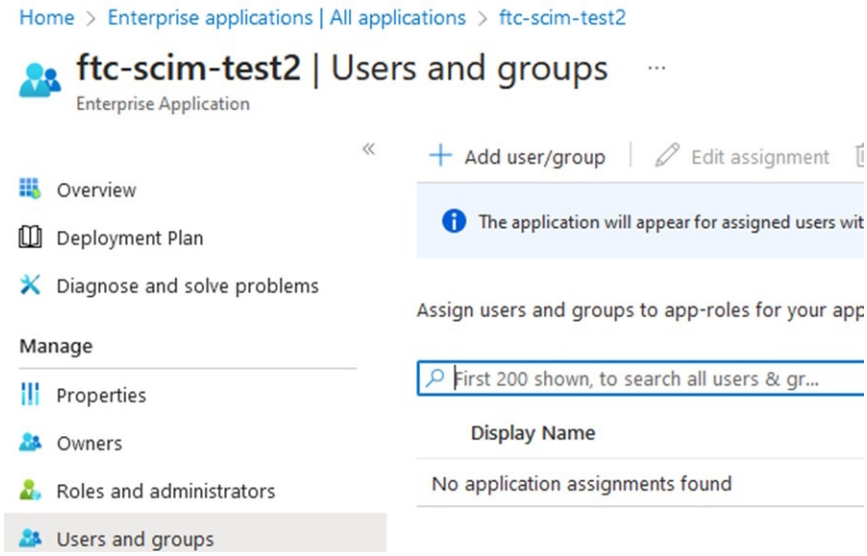


5. Click *Provisioning* and select *Automatic* Provisioning Mode.

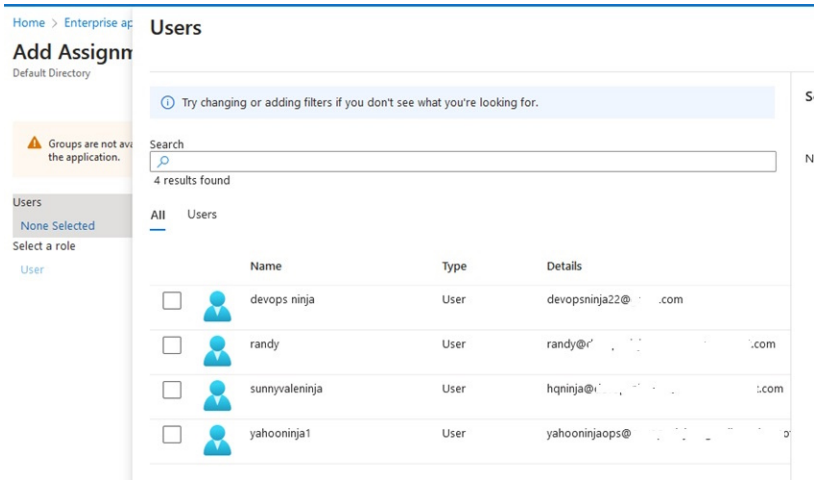


6. Add the users to the applications:

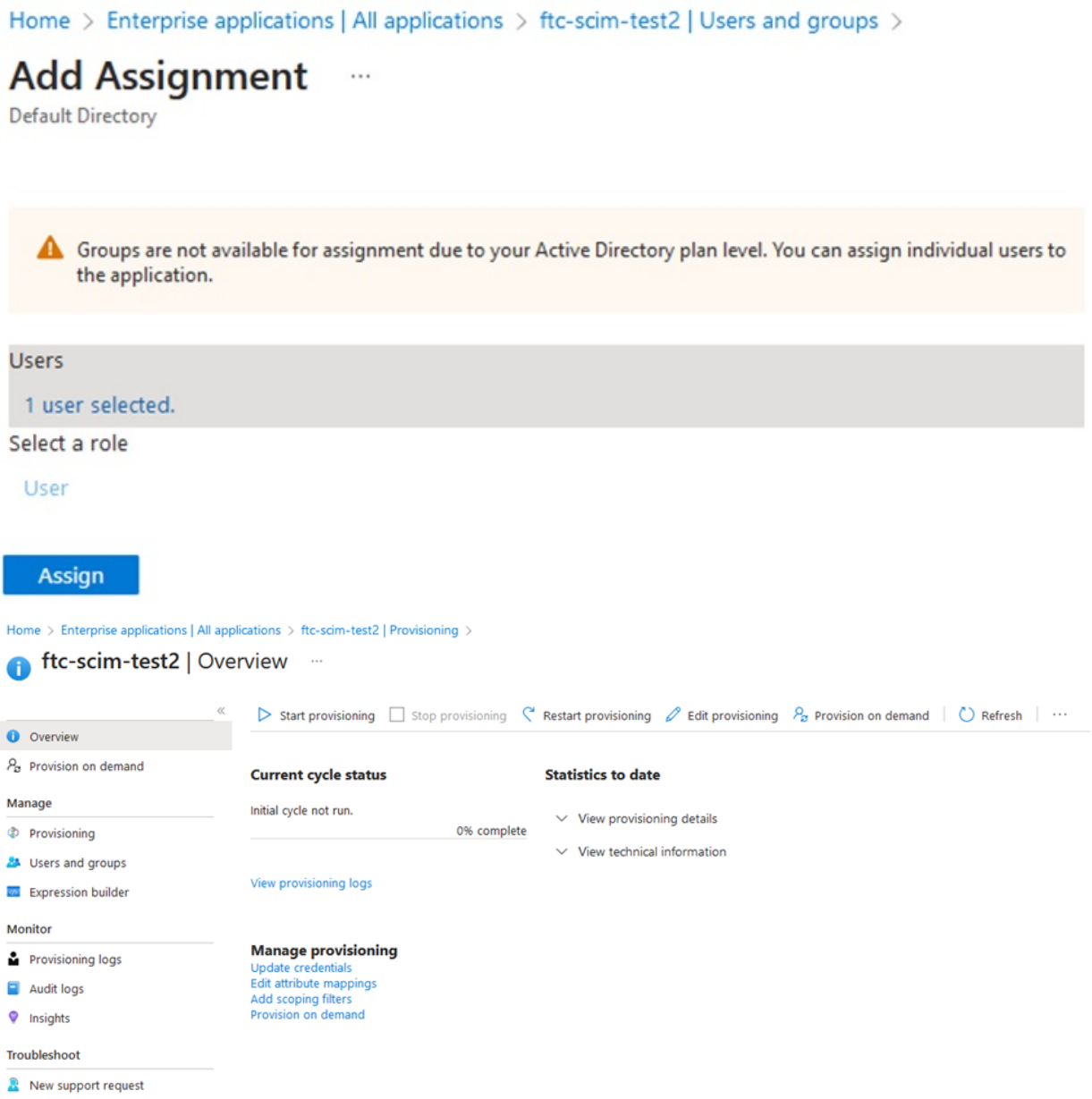
a. Go to the applications and click the newly created the application FIC-scim-test2.



b. Click *Add user/group*, select the user(s), and click *Assign*.

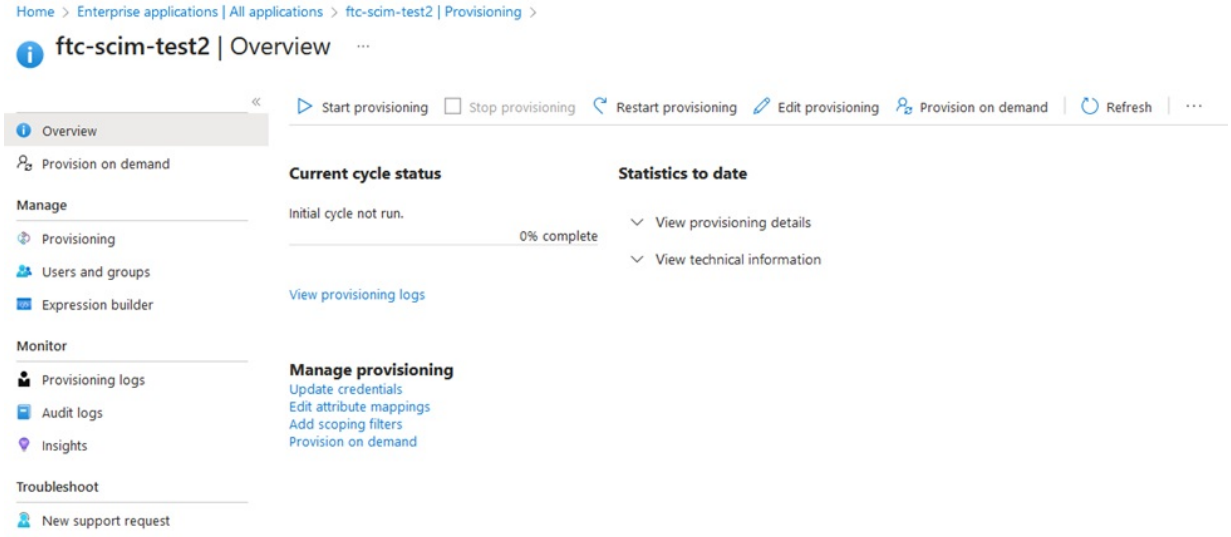


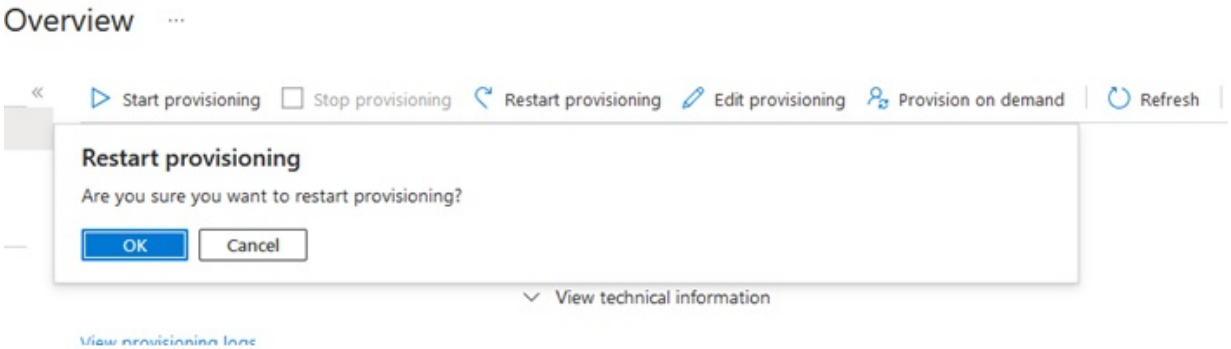
c. Add to the assignment and click *Assign*.

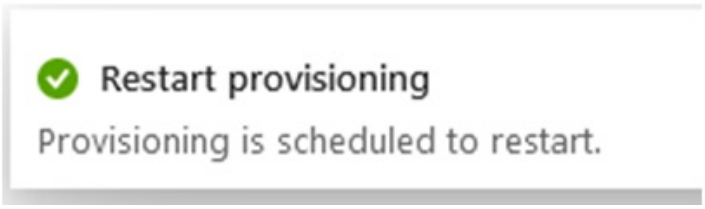

Home > Enterprise applications | All applications > ftc-scim-test2 | Users and groups >
Add Assignment
Default Directory
Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.
Users
1 user selected.
Select a role
User
Assign
Home > Enterprise applications | All applications > ftc-scim-test2 | Provisioning >
ftc-scim-test2 | Overview
Overview
Provision on demand
Manage
Provisioning
Users and groups
Expression builder
Monitor
Provisioning logs
Audit logs
Insights
Troubleshoot
New support request
Start provisioning
Stop provisioning
Restart provisioning
Edit provisioning
Provision on demand
Refresh
Current cycle status
Initial cycle not run.
0% complete
View provisioning logs
Statistics to date
View provisioning details
View technical information
Manage provisioning
Update credentials
Edit attribute mappings
Add scoping filters
Provision on demand

Provisioning:

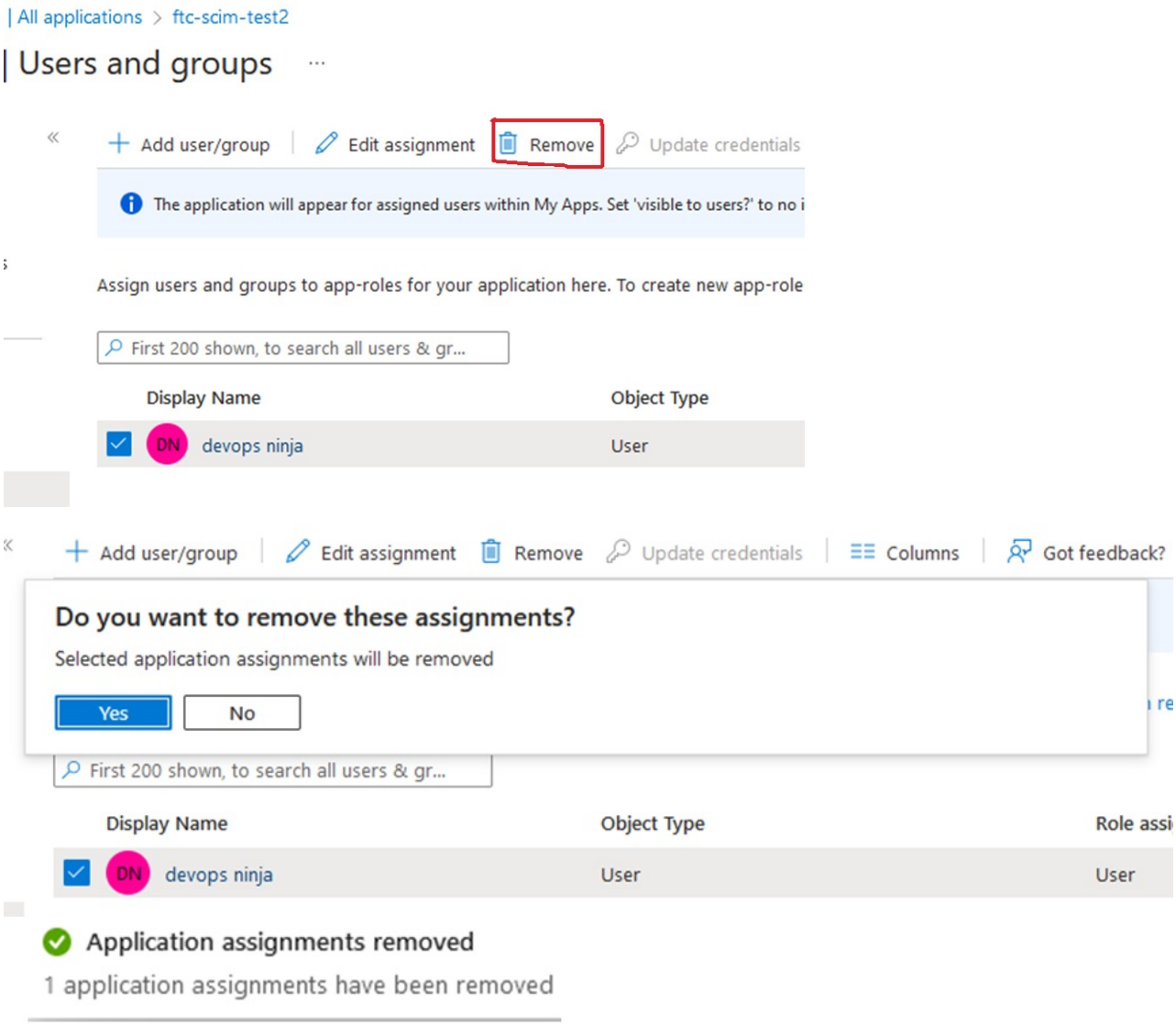
a. Click *Provisioning and Restart*.







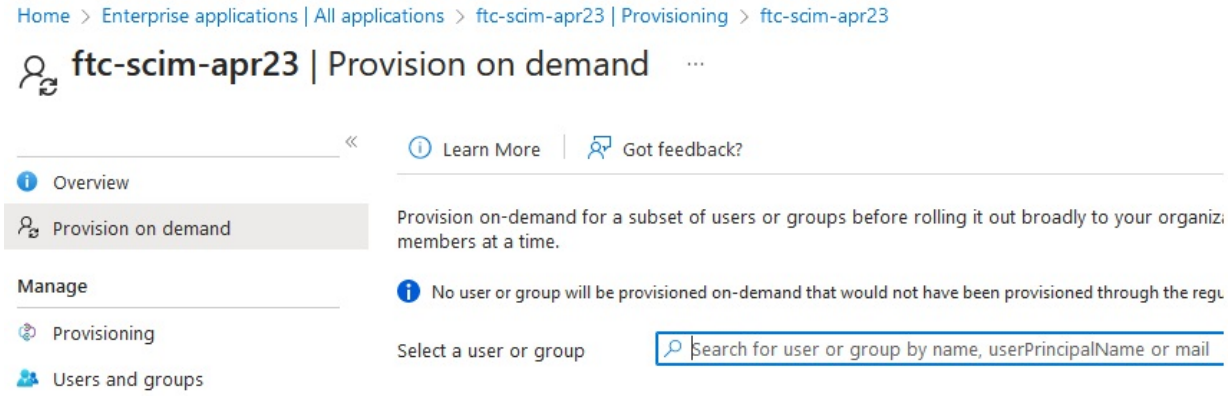
Remove User:



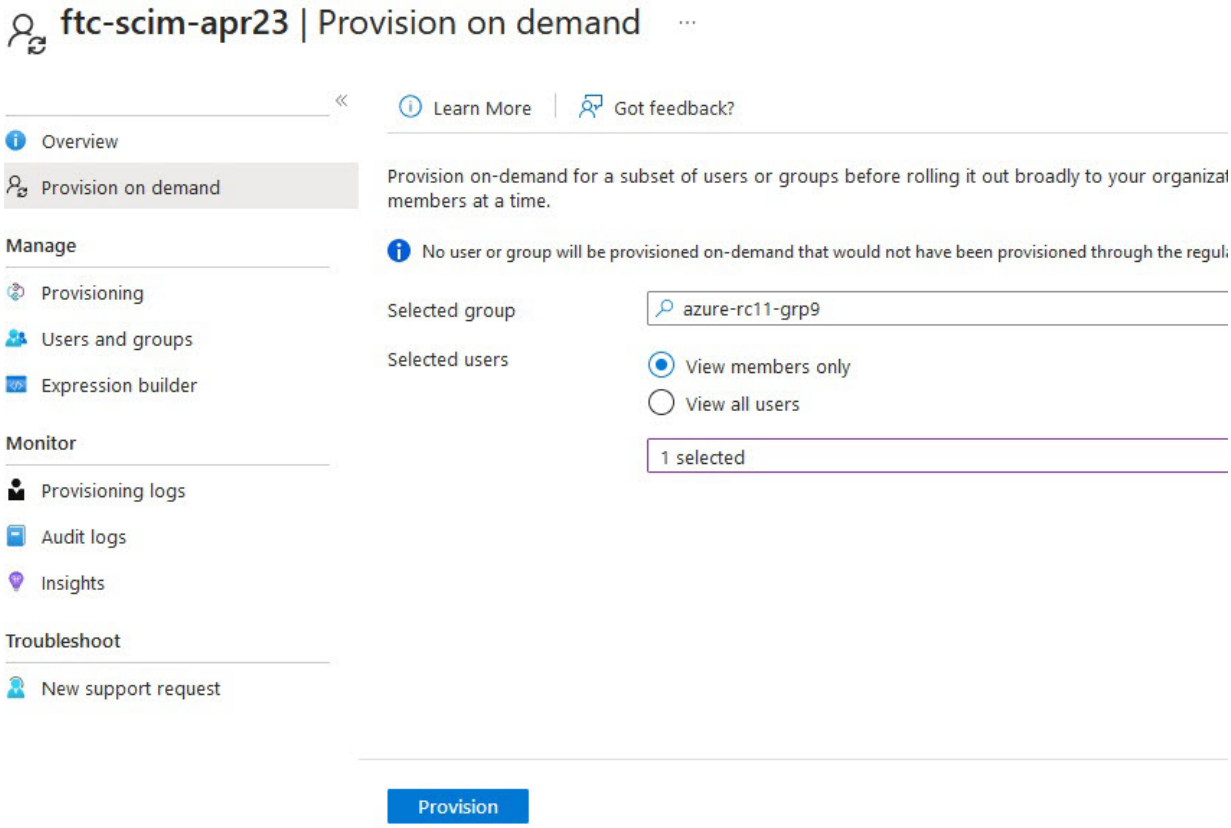
On-Demand Provision:

Go to *Enterprise Applications>All Applications>your-Applications>Provisioning>Provision on demand.*
Example:

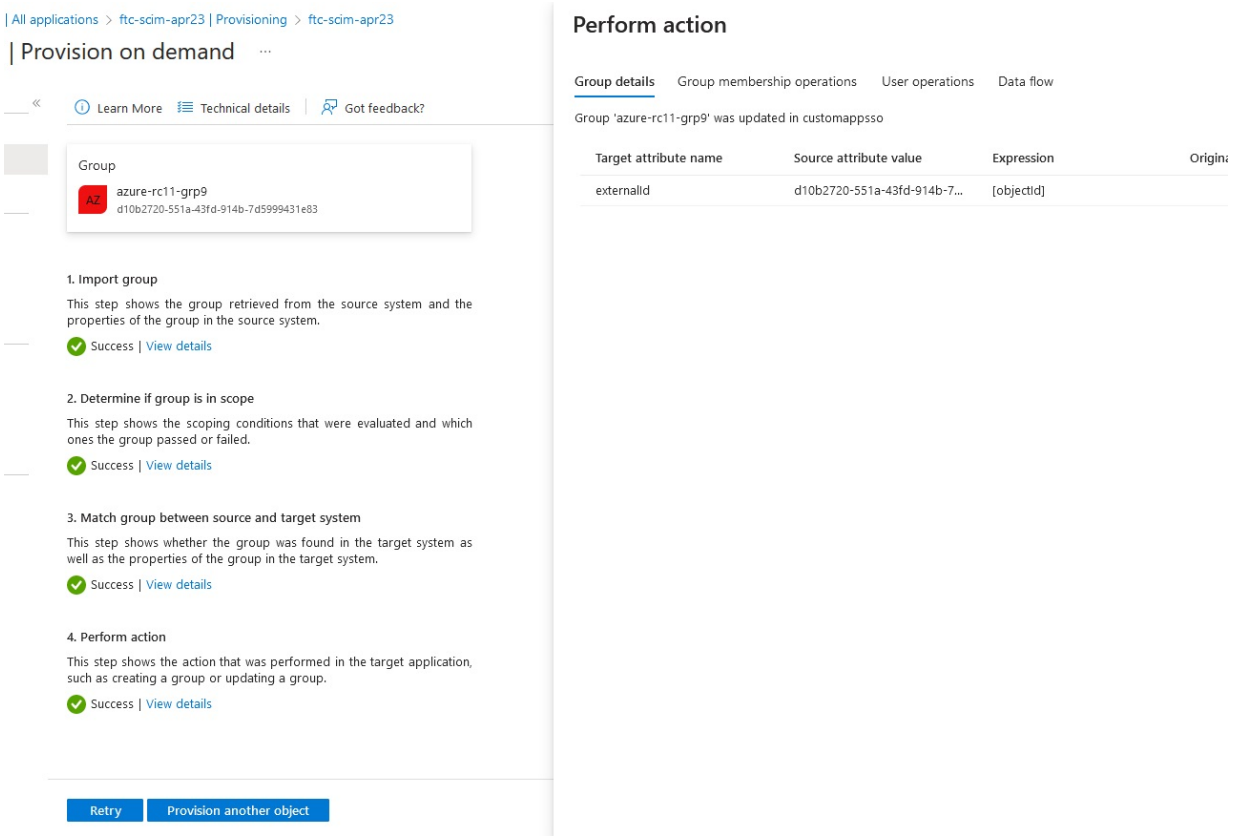
a. Search and select the user or group.



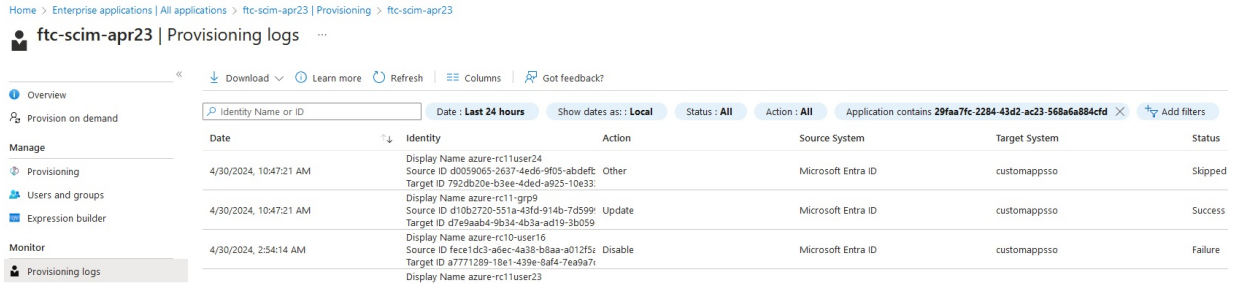
b. For groups, select the members.



c. Click *Provision*.



d. Check the *Provision* logs:

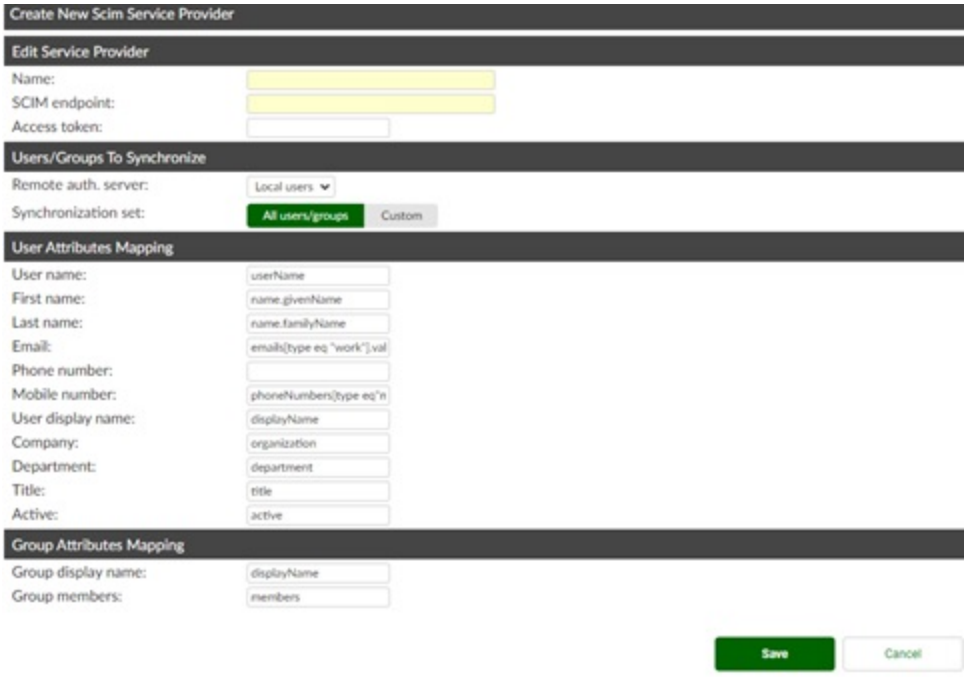


Demo: Configuring FortiAuthenticator as SCIM client

- This demo is conducted using FortiAuthenticator VM v6.6.1, Build 1660 (GA) release.
- For more information about FortiAuthenticator, visit https://docs.fortinet.com/document/fortiauthenticator/6.6.0/administration-guide/684814/service-providers.

Configure the SCIM service provider

1. Click *Authentication>SCIM>Service Provider>Create New*.



2. Make the entries and/or selections as described in the following table, and click *Save*.

Edit Service Provider

Parameter	Description
Name	Enter the name of the SCIM service provider (SP).
SCIM endpoint	Enter the SCIM SP IP address.
Access token	Enter the SCIM SP access token.

Users/Groups To Synchronize

Parameter	Description
Remote auth. server	From the drop-down, select a remote authentication server (LDAP, RADIUS, or SAML) or select local users.
Synchronization set	Select from the following two options to synchronize users/groups: • All users/groups (default) • Custom (**Note:** If selected, you must select the user groups from the Available Groups list and move them to the Chosen Groups list. Only selected user groups and members of those user groups are synced. For remote LDAP servers, only groups with the list of users are included. These are groups without LDAP filter.)

User Attributes Mapping

Parameter	Description
User name	Enter the user name. The default value is `userName`.
First name	Enter the user's first name. The default value is `name.givenName`.
Last name	Enter the user's last name. The default value is `name.familyName`.
Email	Enter the user's email address. The default value is `emails[type eq "work"].value`.
Phone number	Enter the user's phone number.
Mobile number	Enter the user's mobile number. The default value is `phoneNumbers[type eq"mobile"].value`.
User display name	Enter the user's display name. The default value is `displayName`.
Company	Enter the user's company name. The default value is `organization`.
Department	Enter the user's department. The default value is `department`.
Title	Enter the user's title. The default value is `title`.
Active	Enter the user status. The default value is `active`. Custom fields configured in *Authentication>User Account Policies>Custom User Fields*.

Group Attributes Mapping

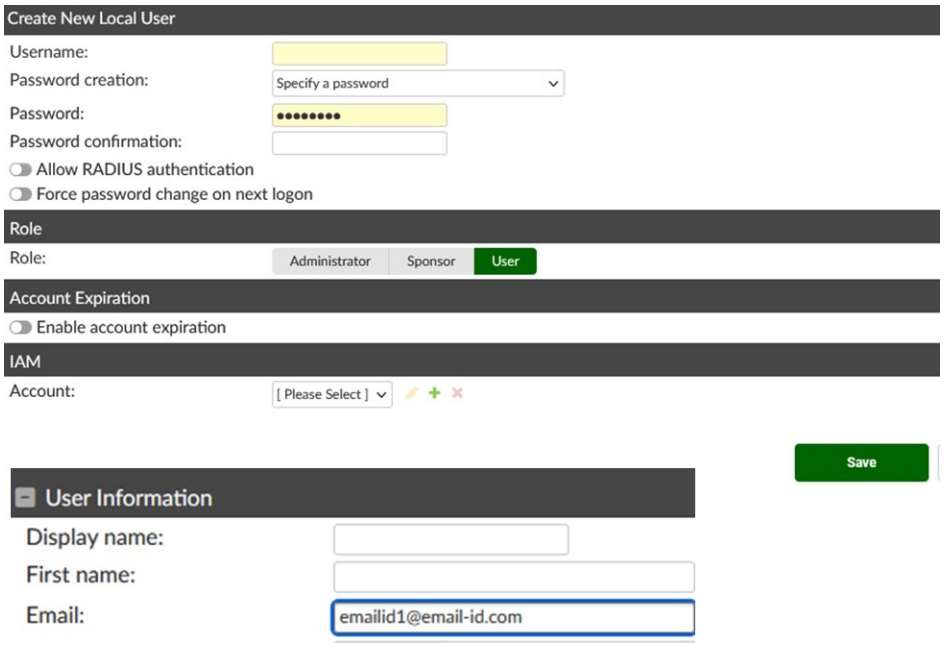
Parameter	Description
Group display name	Enter the group's display name. The default value is `displayName`.
Group members	Enter the group's members. The default value is `members`.

Sync users/groups to FortiIdentity Cloud

1. From the main menu, click *Authentication >SCIM>Service Provider*.
2. Checkmark the SCIM service provider that you've just created.
3. Click *Edit* to open the Edit SCIM Service Provider page.
4. Click *Sync*.

Add a local user

1. From the main menu, click *Authentication>User Management>Local Users>Create New*.
2. Make the required entries and selection as shown in the following screenshot.
3. Click *Save*.



The user that you have just created is now added to FortiAuthenticator and FIC (the SCIM server).

1. Checkmark the user of interest, and click *Delete*.
2. Click *Yes, I'm sure* to the confirmation.

The selected user is now removed from both FortiAuthenticator and FIC.

Known issues and special notes

Common to all SCIM client applications:

- FIC (the SCIM server) allows no more than eight fields in a user profile to be updated at any given time.

Okta-specific:

- For Primary Phone Type, you must specify "mobile".
- Deactivated and deleted users are not reflected on FIC.
- When deactivating and re-activating a user, you must assign the user to the application again.
- Users disabled on FIC are not removed from the group.
- Users added to exiting groups do not show up on FIC.

- Users removed from one group and then assigned to another are not reflected on FIC.

Azure-specific:

Because Azure auto-provisioning happens once every 40 minutes, the following operations carried out on Azure are not reflected on FIC in real time:

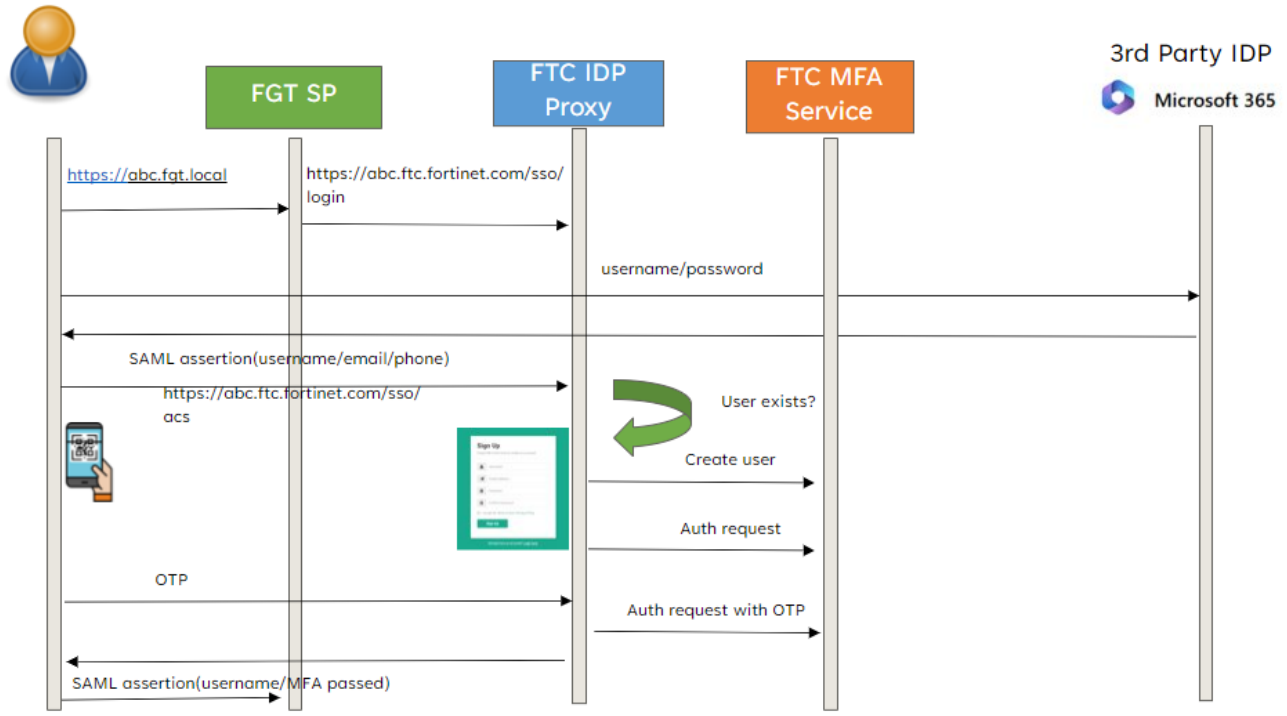
- Removing users from a group
- Re-assigning users to a group
- Adding new users to exiting groups
- Removing users from one group and assigning them to other groups

FortiAuthenticator-specific:

- Assigning users to or removing them from a user group
- Re-assigning users to another group
- Removing user groups
- Adding users to an exiting group
- Moving users between groups

Using SSO applications

An SSO application serves as a bridge or gateway between a federation of SAML IdPs and a federation of SAML SPs, as illustrated in the following diagram:



To an SP, an IdP Proxy looks like an ordinary IdP. Likewise, to an IdP, an IdP Proxy looks like an SP. Thus an IdP Proxy has the combined capability of both an IdP and an SP.

With FIC providing the SAML and OIDC IdP interface, we can move the application into the scope of FIC SaaS service and make use of existing SSO protocol to integrate with the Fortinet ecosystem, which already supports SAML log-in. This relieves Fortinet devices from private integration with FIC, as long as they use SAML SP for authentication. FIC can introduce new features such as FIDO and adaptive authentication without downstream support.

Furthermore, customers no longer need to worry about device serial numbers and FIC license ownership.

For more information, see Use Cases on page 139.

Use Cases

- Most IdP vendors require a subscription for full access to their services. Be sure to check with your IdP and SPs vendors to see if a premium subscription is required to access their services.
- This feature is only available to FIC customers with a full subscription. It is not available to trial customers.

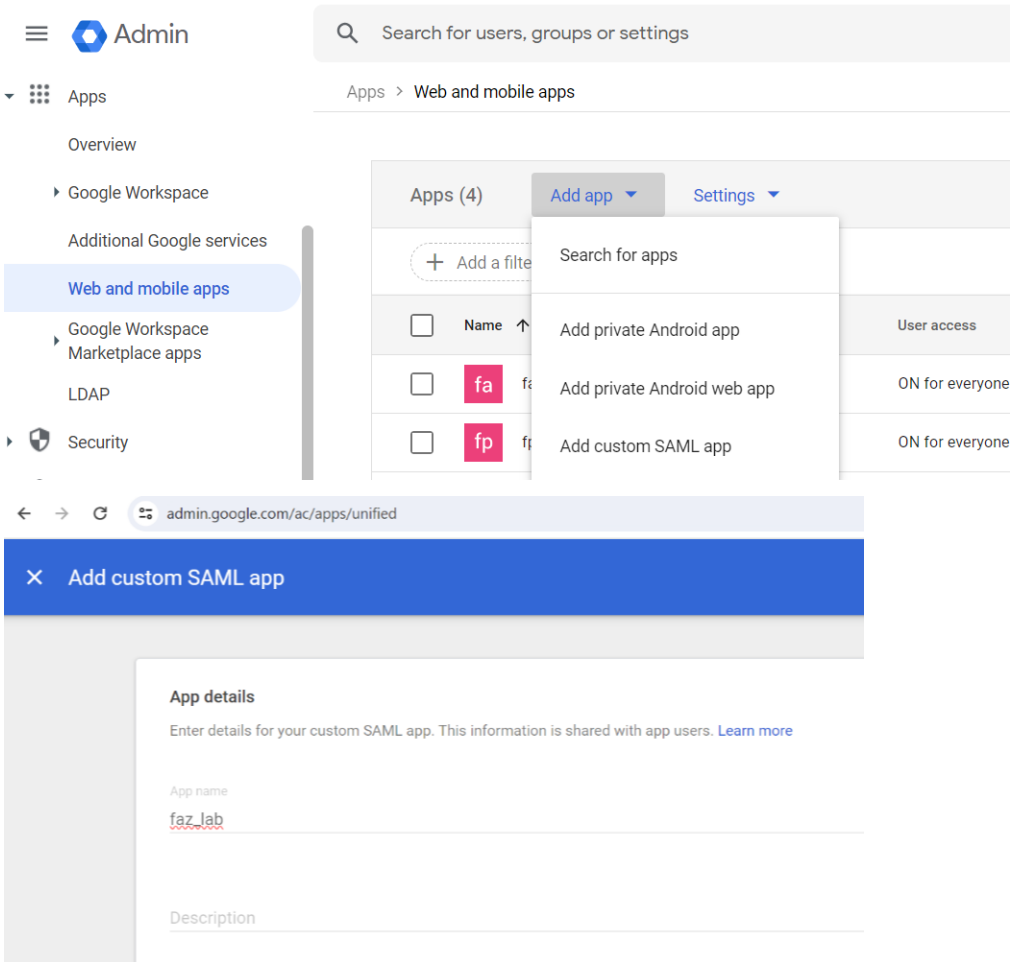
One example would be that a customer already has a setup with an IdP and multiple SPs, but doesn't have MFA. Let's say that they're using Google as the IdP to provide the user source and SSL VPN through a FortiGate as the SP. With their current setup, if their end-users try to log in through SSL VPN, they will be directed to the Google login page, where once they input their username and password, they will immediately be allowed to log into SSL VPN. With FIC's IdP Proxy setup, the end-users will experience following instead:

Google login > FIC 2FA OTP page > FGT SSL VPN.

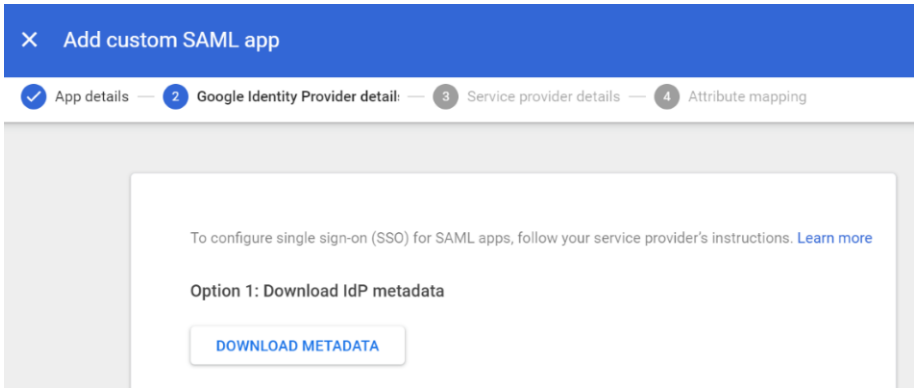
Example 1: Google SAML as IdP and FortiGate SSL VPN as SP

The FortiGate device used in this example setup is running on FortiOS 7.4.3.

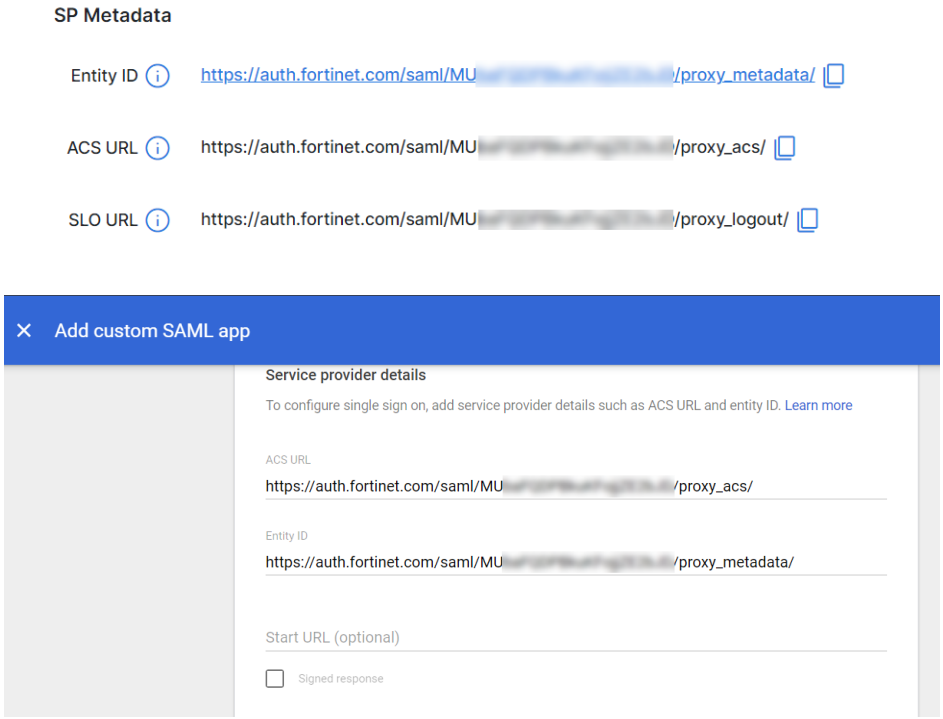
1. Go to *Authentication > User Source* and click *Add User Source*:
2. Configure the *Source Information*. Note that Google cannot use Login Hint.
3. On admin.google.com, go to *Apps > Web and mobile apps*, and then add a custom SAML app:



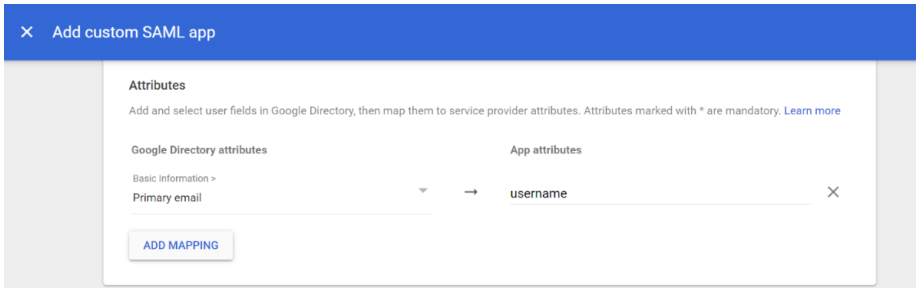
4. Download the metadata, and get the certificate from this page and click *Continue*.



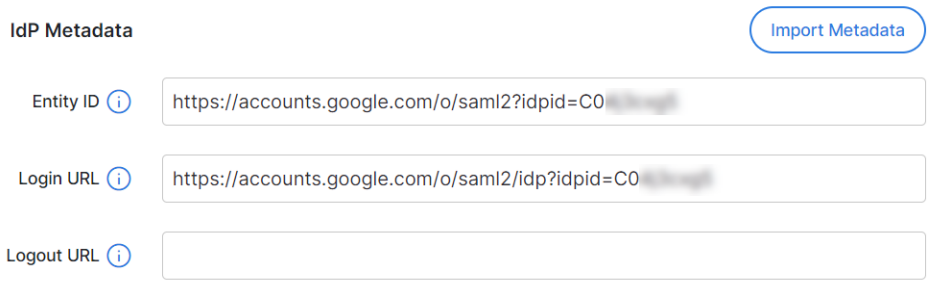
5. Provide SP metadata details from FIC (under Interface Detail) on Google.



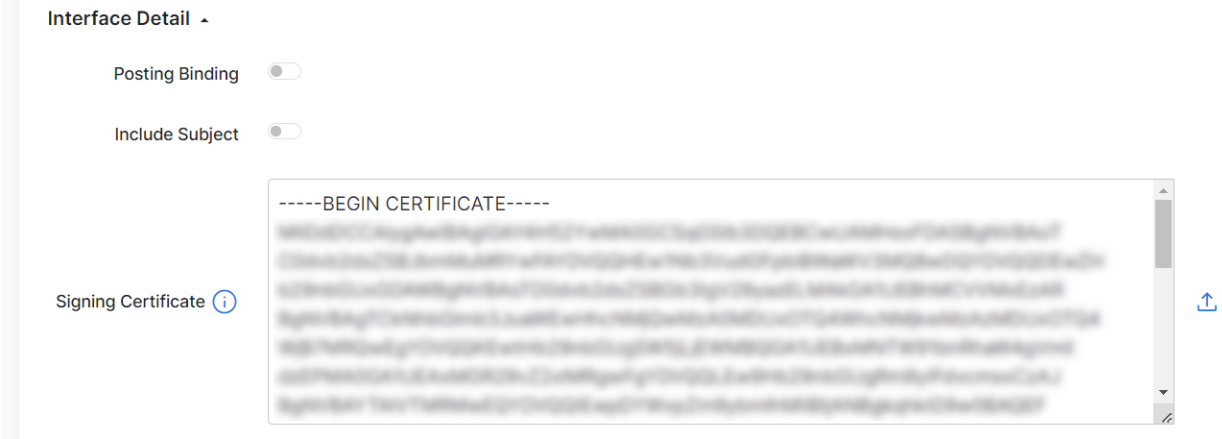
6. In this example we map the primary email attribute to the username attribute.



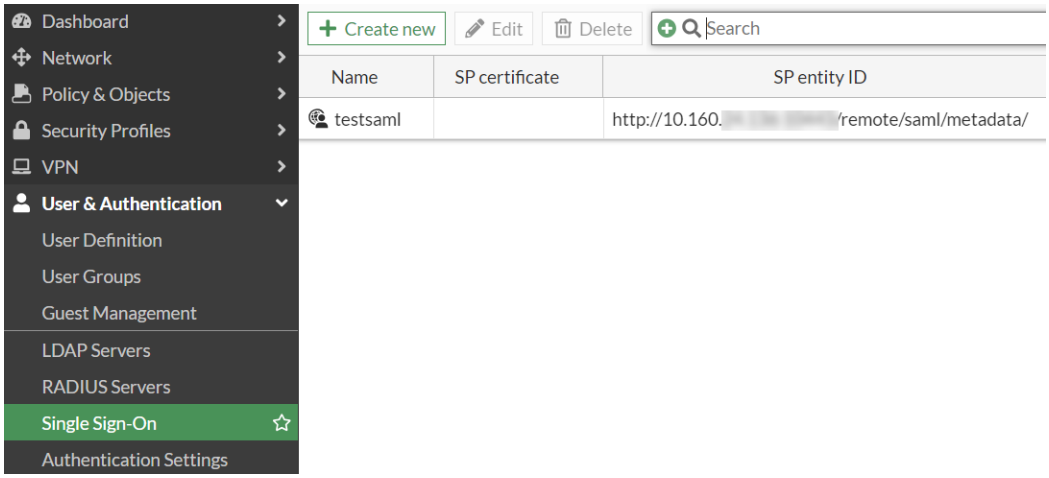
7. On FIC, click *Import Metadata* and import the metadata file you downloaded earlier in Step 4. Note that Google does not have a Logout URL.



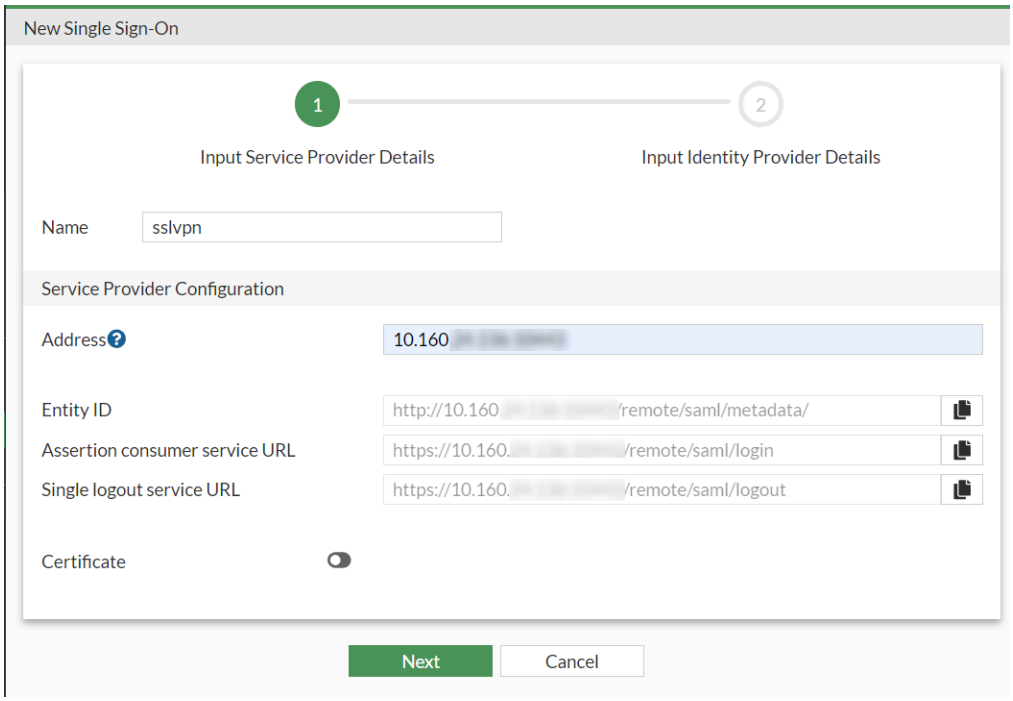
8. Load the certificate that you got in Step 4 here in FIC, and click *Save* now to save the entire user source setting.



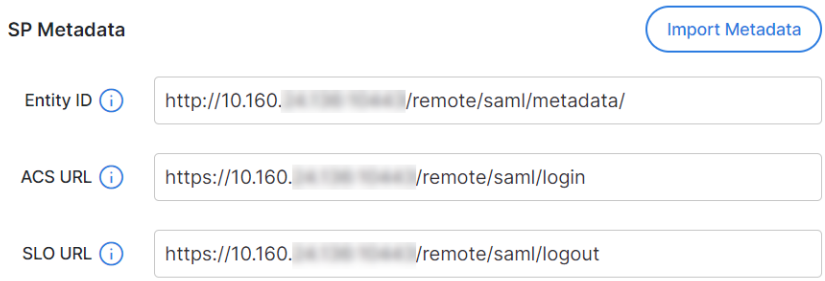
9. On FIC, go to *Applications* > *SSO* > *Add SSO Application*:
10. Configure the *General Information*.
11. On FGT, we assume you already have SSL VPN set up. Create a new single sign-on under *User & Authentication* > *Single Sign-On*.



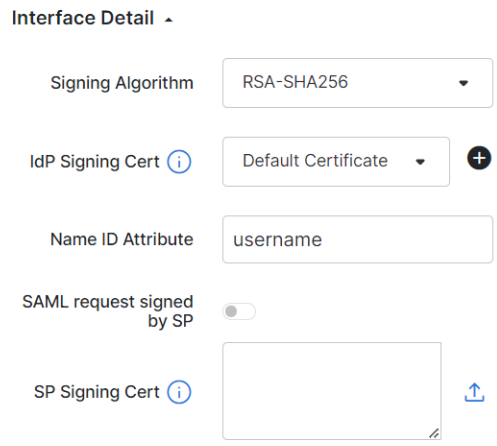
12. Put your SSL VPN address into the *Address* field and take note of the *Entity ID*, *Assertion consumer service URL*, and *Single logout service URL*.



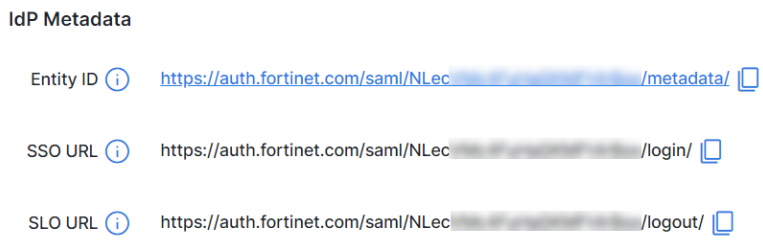
13. Add the details into the *SP Metadata* section on FIC.



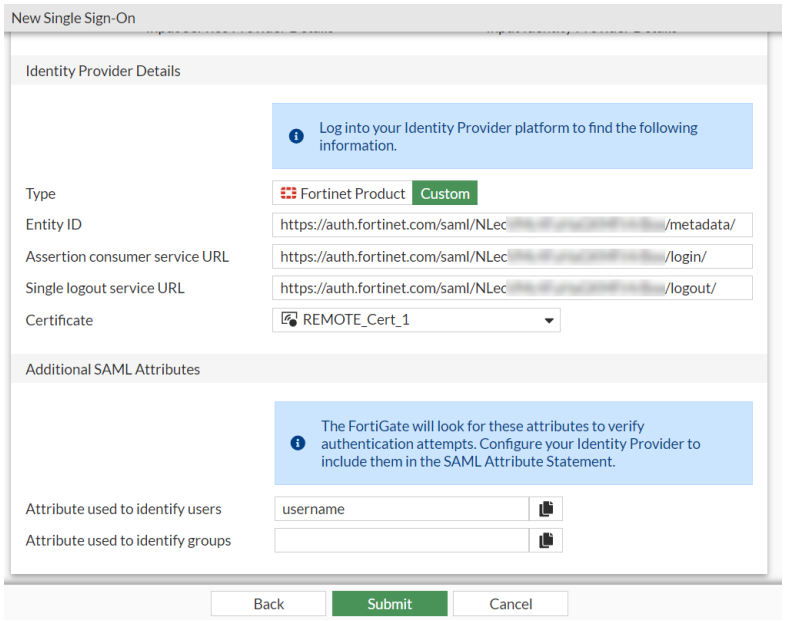
14. For *Interface Detail*, set it like this in this example.



15. Get the IdP Metadata and input it into the next page on the FGT single sign-on wizard.

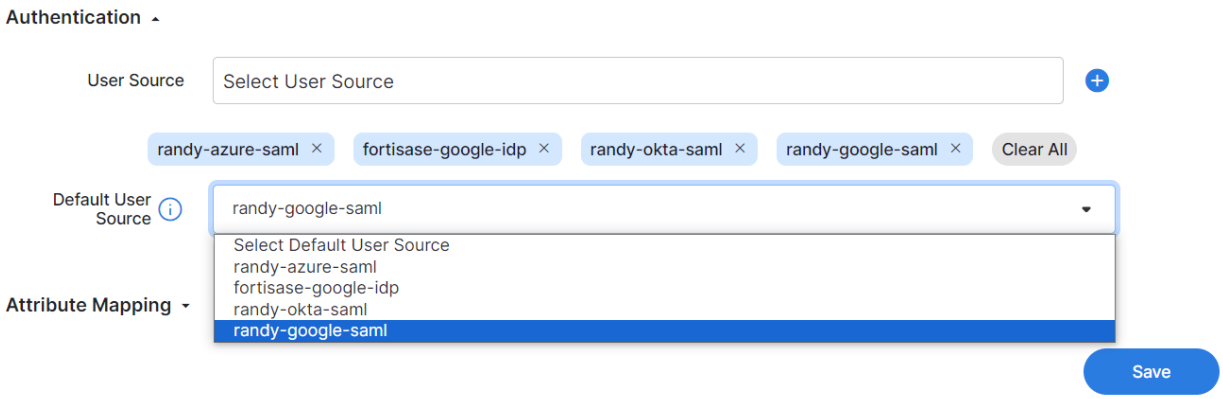


16. Configure as such and click *Submit*. You then need to add the SAML server that you've just created to the user group and your SSL VPN firewall policy as well.

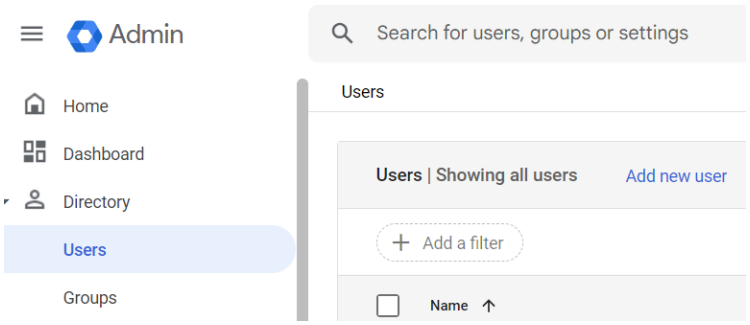


17. To obtain the certificate, go to *Applications* > *SSO*, locate the SAML application, click the tool icon, select *Details*, download the *Signing Certificate*, and import it into FGT.

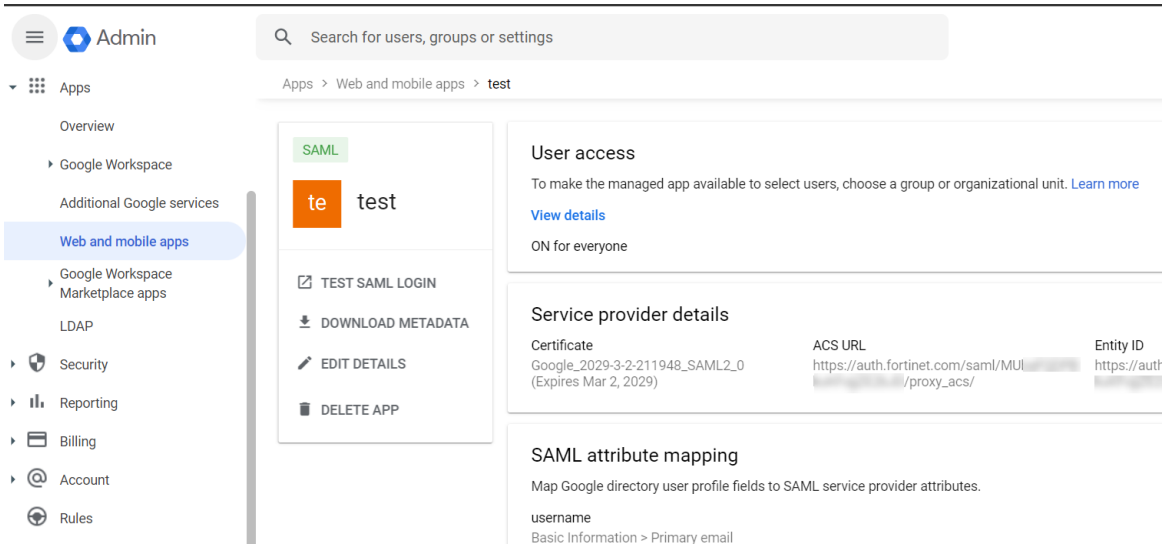
18. On FIC, map your new SP to the IdP that you configured earlier, and click *Save* .



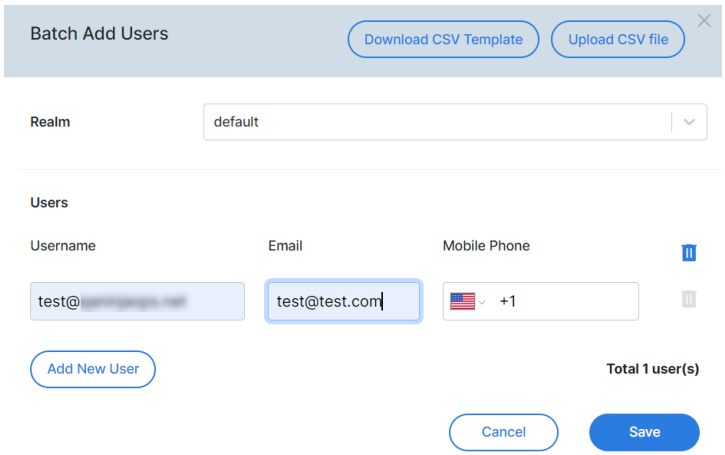
19. To add users on Google, go to *Directory > Users > Add new user*:



20. You can manage user access here. In our example we've turned the access on for all users on our Google account.



21. On FIC, add the same user using the same username (the email in our example) by going to *User Management > Users > Batch Add*.

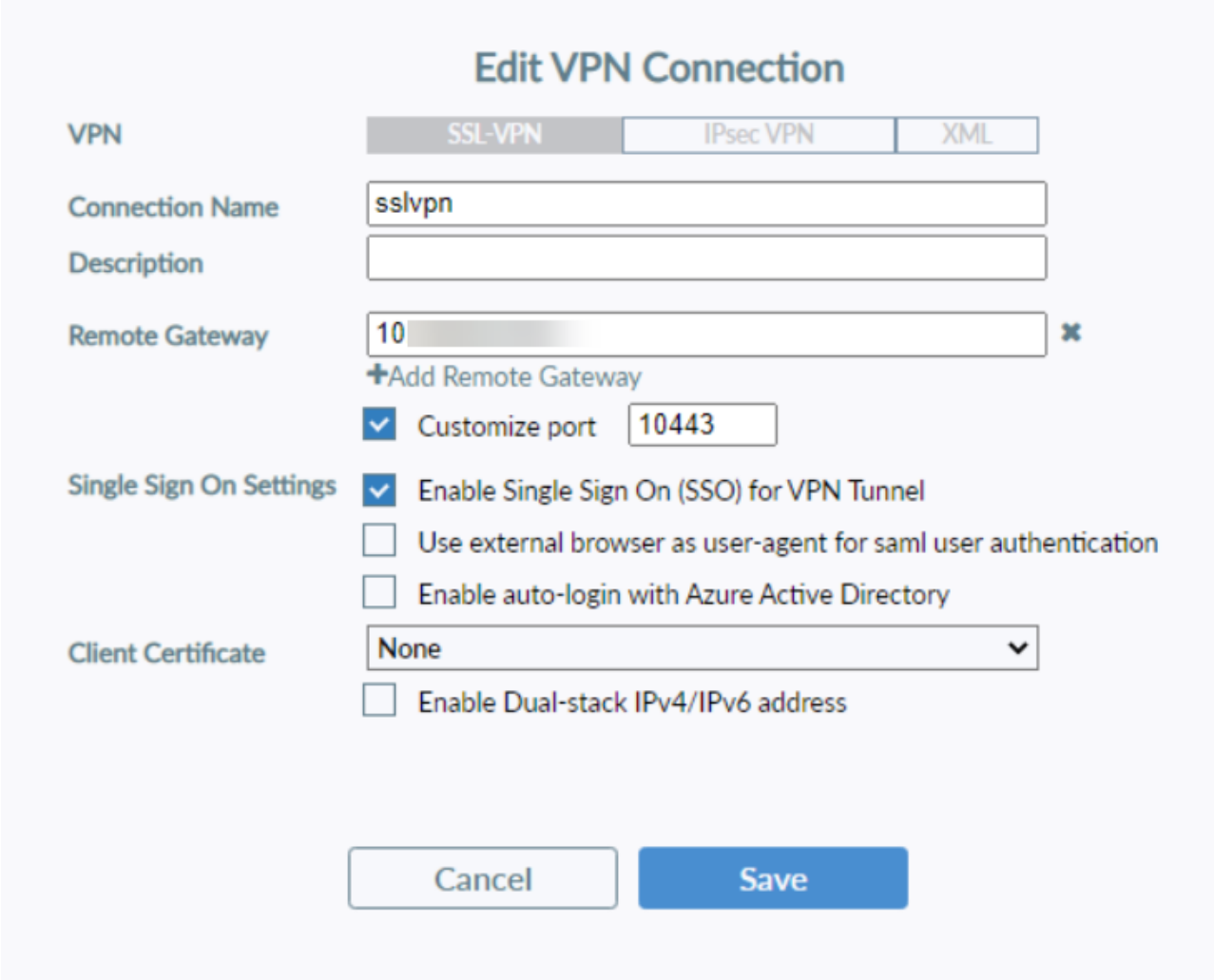


22. Once the users is added, set up FortiClient to be used to log in to this SSL VPN setup. First of all, change the `remoteauthtimeout` parameter in the CLI because its default value of 5 is too short for end-users to properly log into SSL VPN.

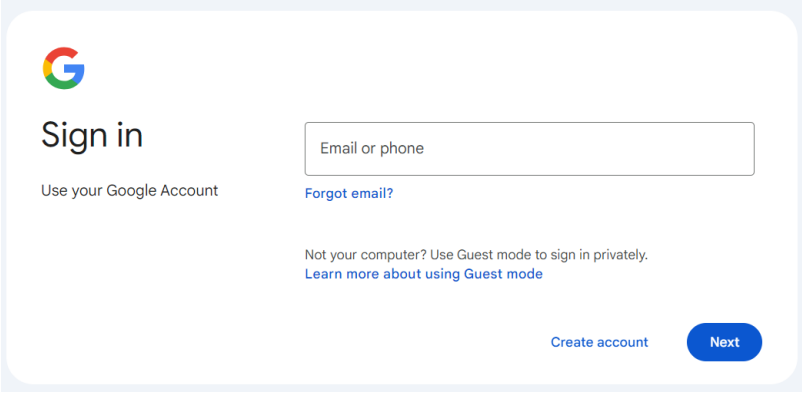
```
config system global
    set remoteauthtimeout 300
end
```

    In this example, we set `remoteauthtimeout` to the maximum value of 300. You can set it to a lower value to suit your needs as long as it gives your end-users enough time to go through the login process.

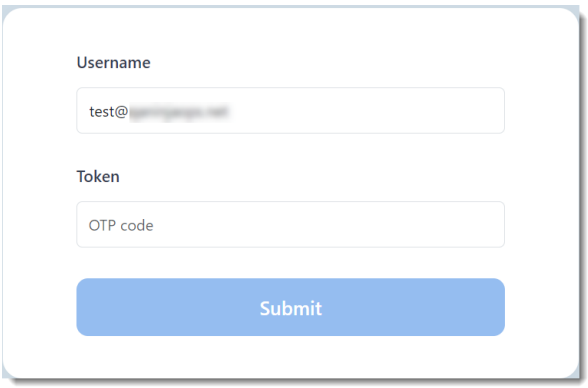
23. In FortiClient, create a new VPN connection as shown in the following illustration. You can choose to use FortiClient's internal browser or your own computer's default browser if you select *"Use external browser as user-agent for saml user authentication."*



24. Click *Save*. You will be taken to the following Google's sign-in page when trying to connect to the VPN:



25. Log in, and you are now taken to the OTP page.

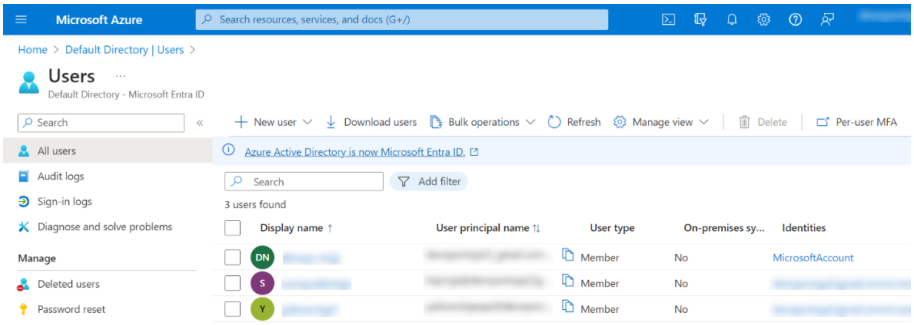


26. Verify the token using your selected MFA method when you created the user on FIC earlier. Now the end-user should be able to log into the SSL VPN through FortiClient.

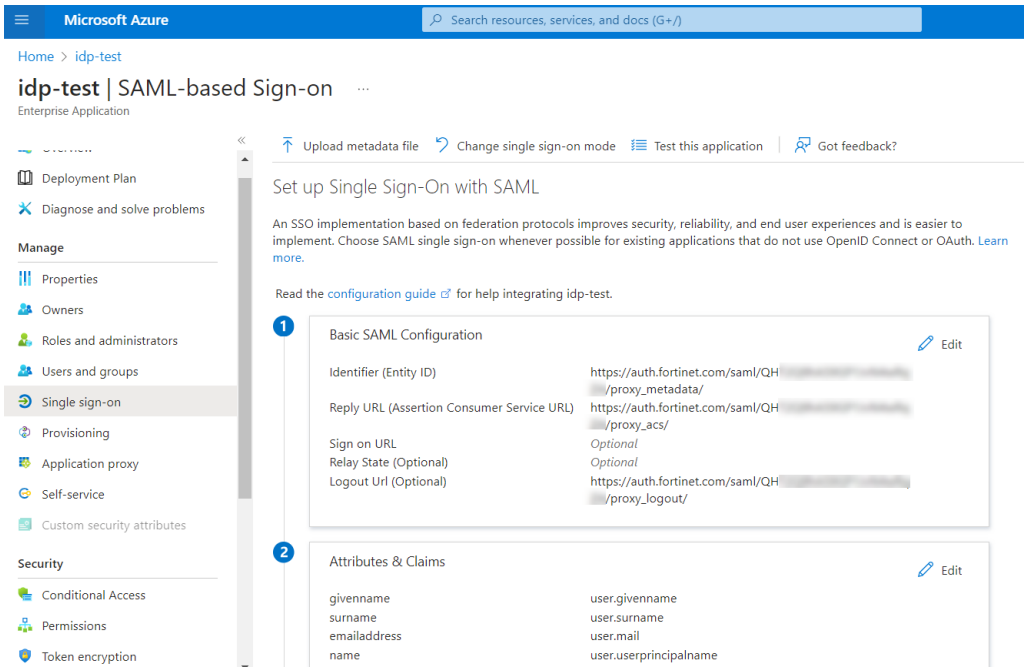
Example 2: Azure as SAML IdP and FortiGate as SP

The FortiGate device used in this example setup is running on FortiOS 7.4.3.

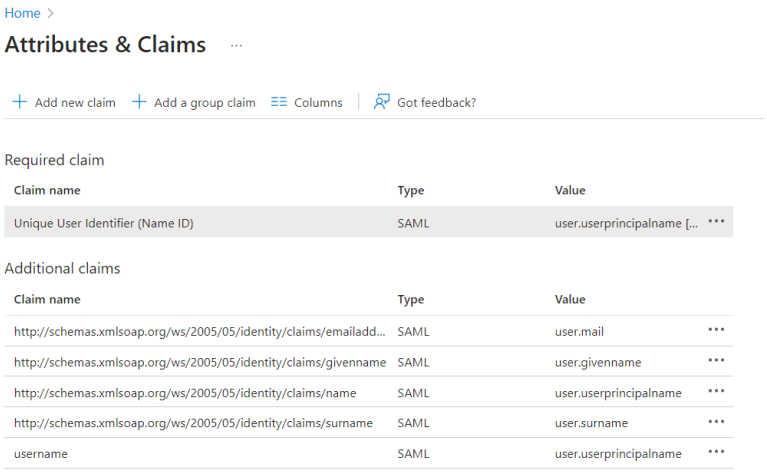
1. Create users on Azure on portal.azure.com. *Go to Home > Default Directory > Users > All users > New user.*



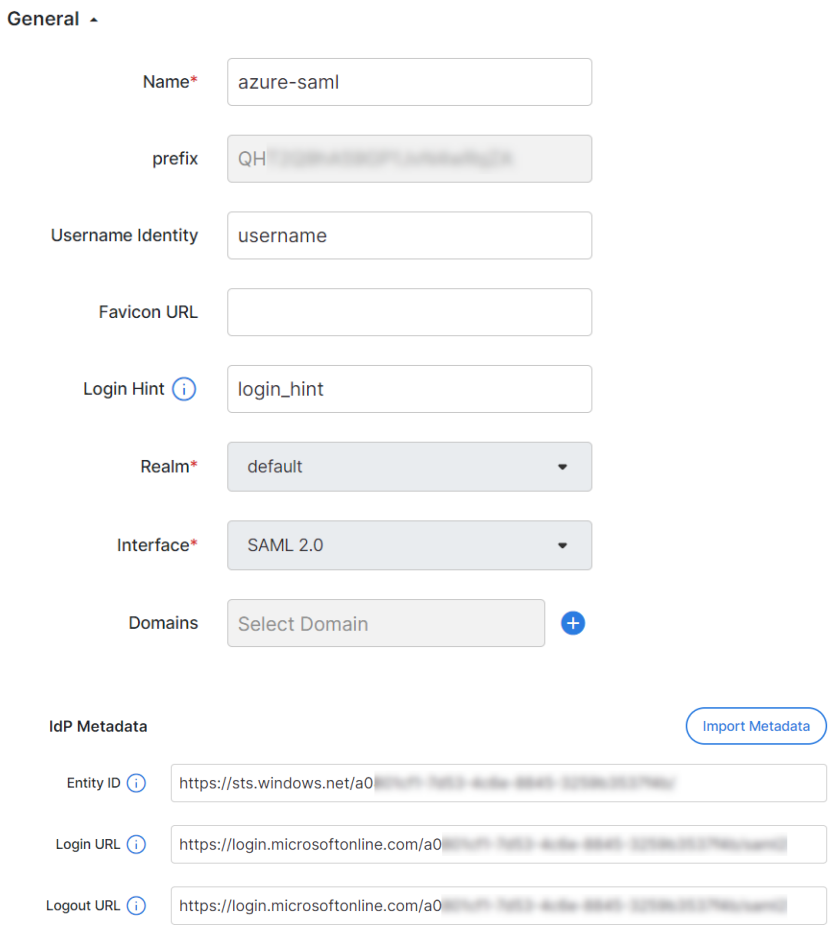
2. Create a single sign-on app in *Home > Enterprise Application*. This is also where you will be pasting in your SP metadat as we did with the Google example.



3. While creating the app, add a claim for the username. The following illustration shows the setting used in our example.



4. Here is the example that shows FIC configured for Azure as the IdP. Note that the *Login Hint* is "login_hint" for Azure.

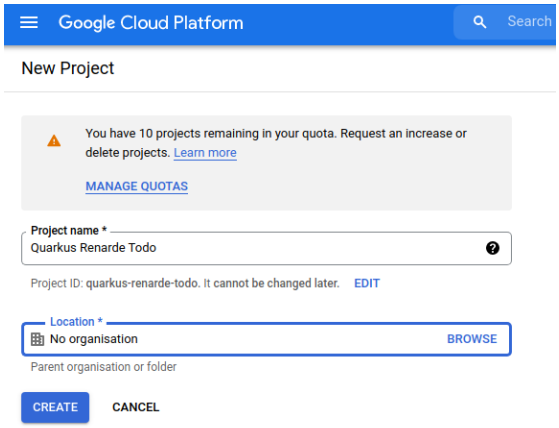


5. Click *Save*. For the rest of the setup, the SP config should be the exact same as the other example with Google. See Example 1: Google SAML as IdP and FortiGate SSL VPN as SP on page 139.

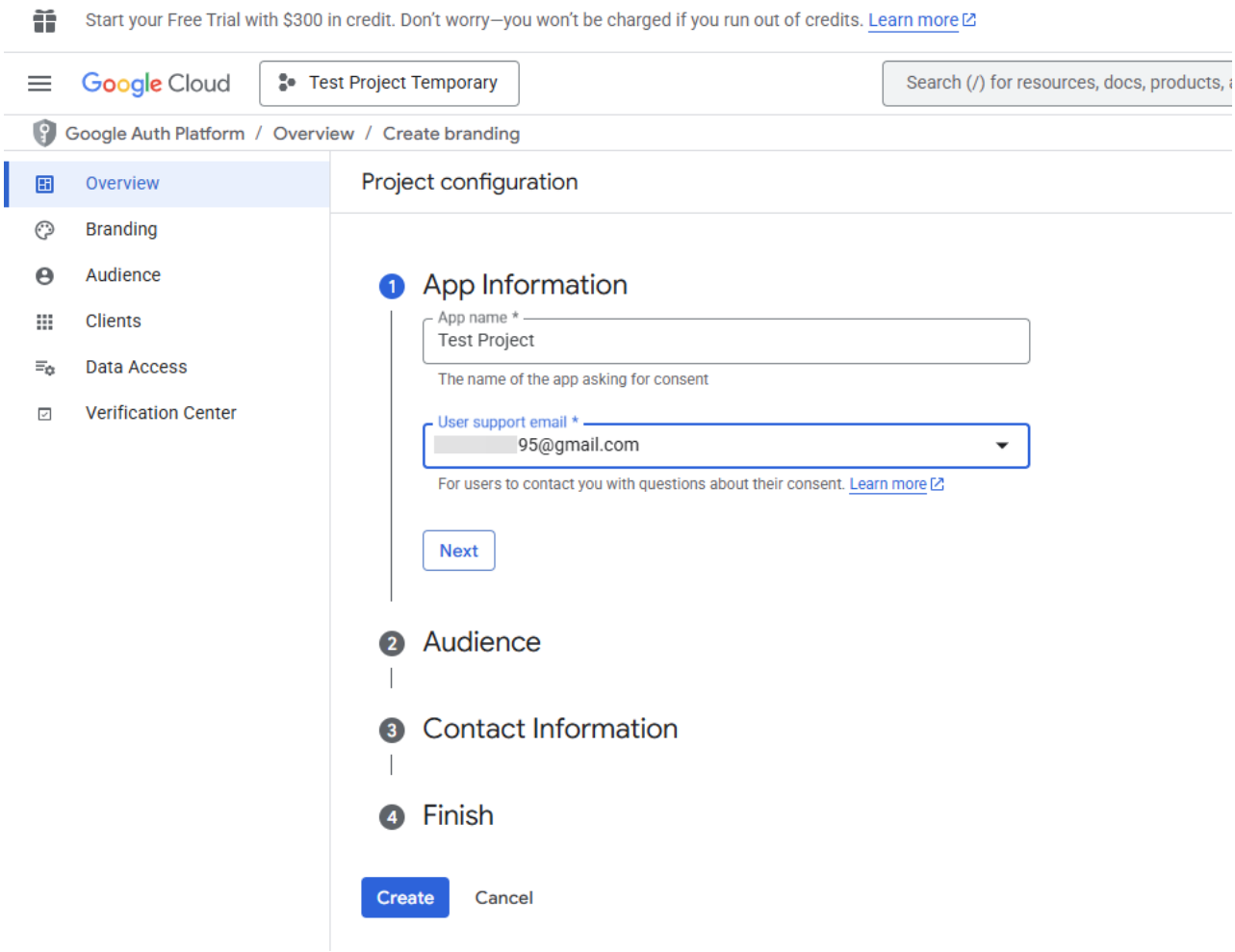
Example 3: Google OIDC as IdP

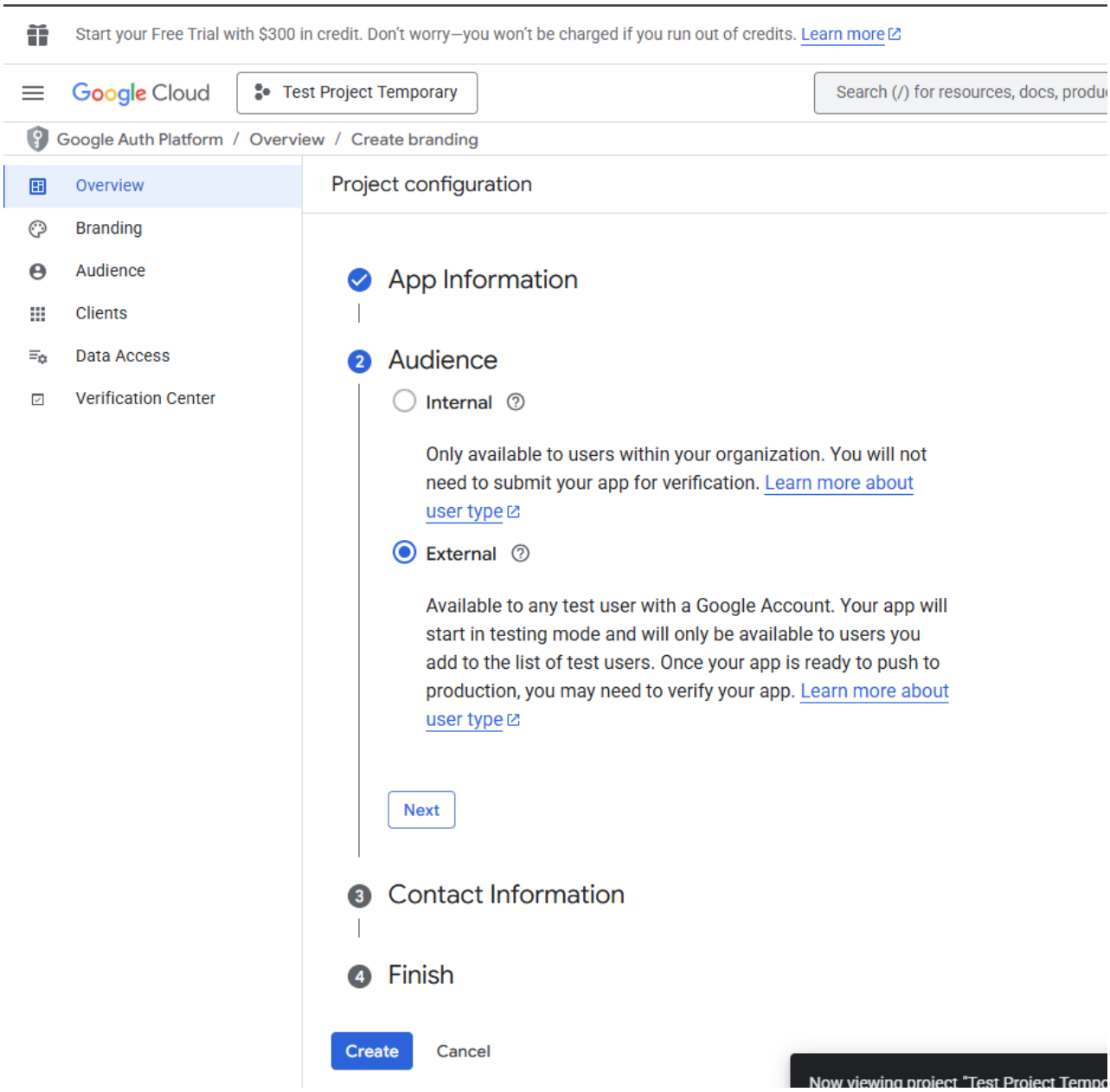
In this example, the SP can be any supported Fortinet application. For a complete list of supported Fortinet applications, see Compatible Fortinet applications on page 38.

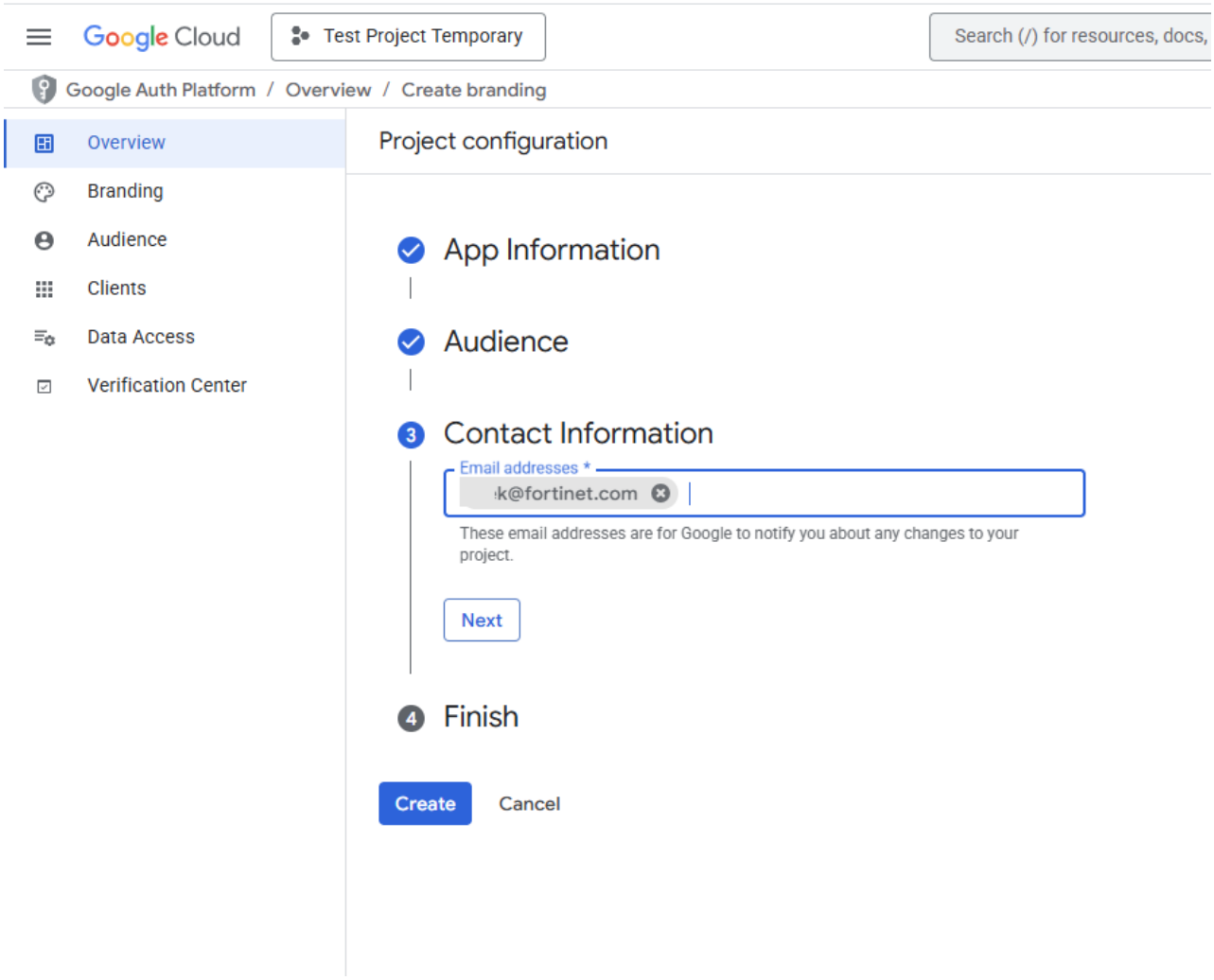
1. To set up OPenID Connect (OIDC) using Google, you need to create a project in your Google Cloud Platform.

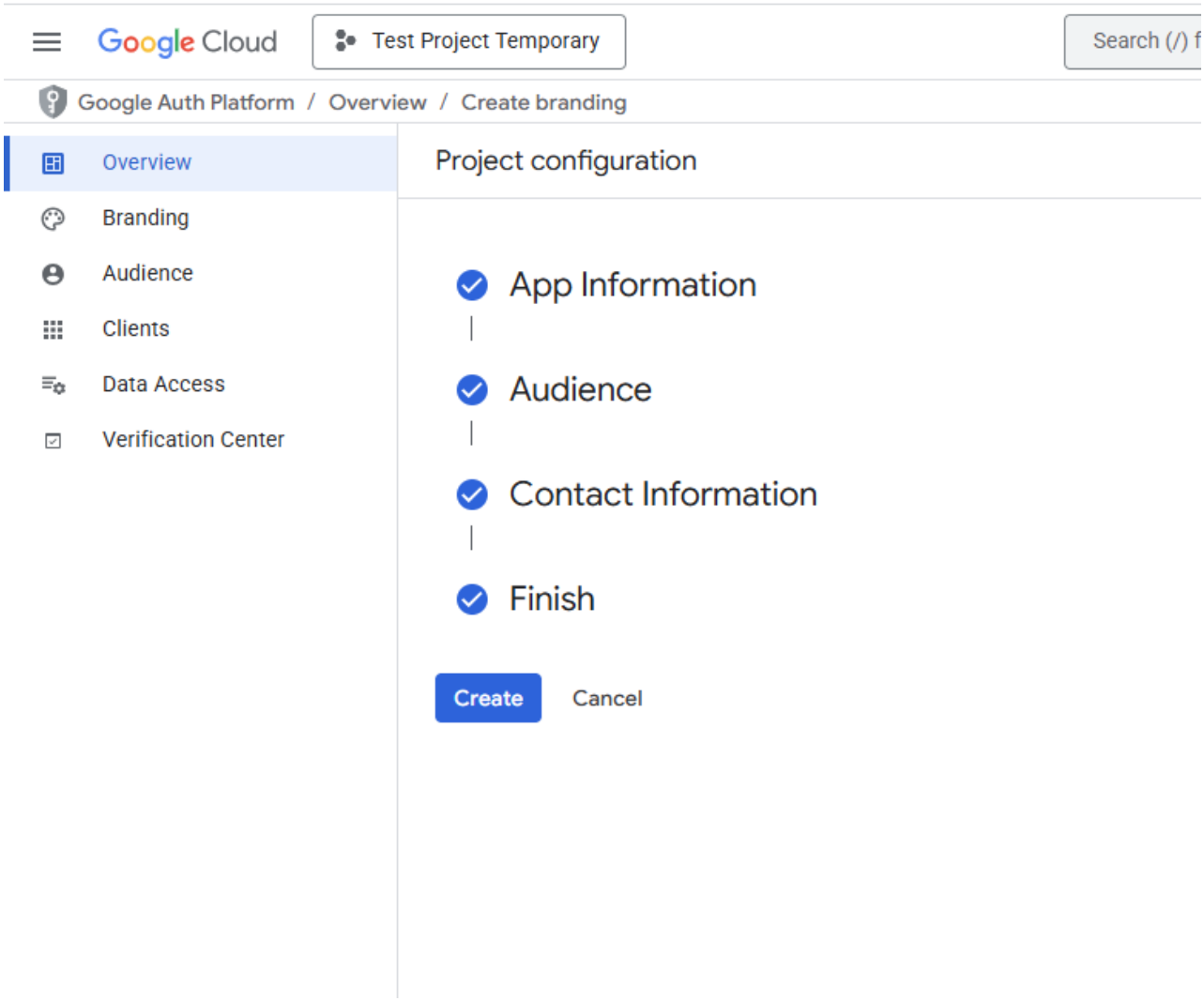


2. Follow the prompts onscreen to configure the project, as shown in the following screenshots.

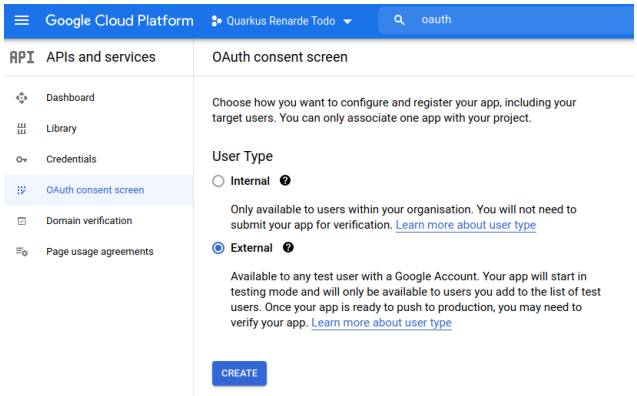



Start your Free Trial with $300 in credit. Don't worry—you won't be charged if you run out of credits. Learn more
Google Cloud
Test Project Temporary
Search (/) for resources, docs, produ
Google Auth Platform / Overview / Create branding
Overview
Branding
Audience
Clients
Data Access
Verification Center
Project configuration
App Information
2 Audience
Internal
Only available to users within your organization. You will not need to submit your app for verification. Learn more about user type
External
Available to any test user with a Google Account. Your app will start in testing mode and will only be available to users you add to the list of test users. Once your app is ready to push to production, you may need to verify your app. Learn more about user type
Next
3 Contact Information
4 Finish
Create
Cancel
Now viewing project "Test Project Tempo

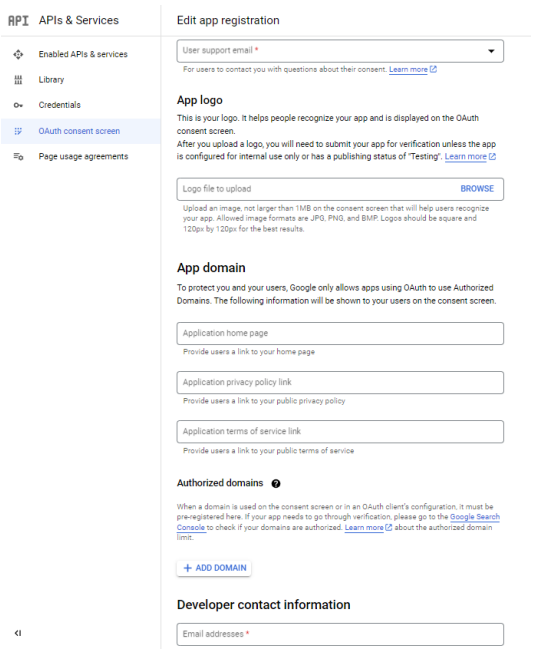

Google Cloud
Test Project Temporary
Search (/) for resources, docs,
Google Auth Platform / Overview / Create branding
Overview
Branding
Audience
Clients
Data Access
Verification Center
Project configuration
App Information
Audience
3 Contact Information
Email addresses *
k@fortinet.com
These email addresses are for Google to notify you about any changes to your project.
Next
4 Finish
Create
Cancel



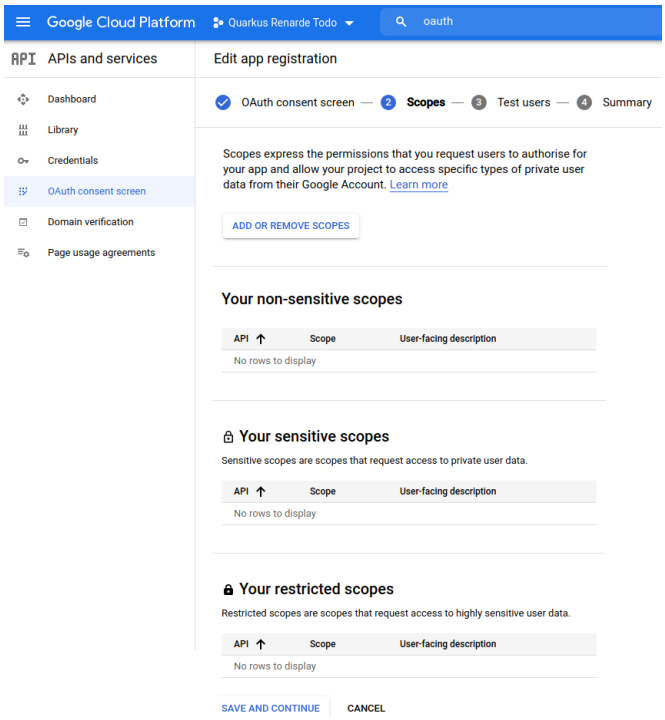
3. Select *External* to authorize any Google user to log into your application and press *CREATE*.



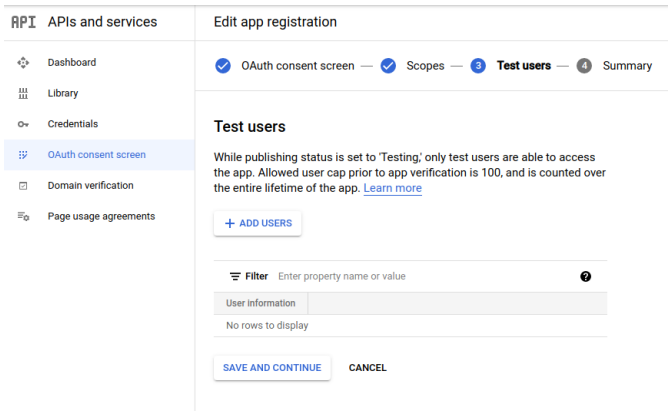
4. Now you can fill in your application name, your support email, your developer contact information and press *SAVE AND CONTINUE*.



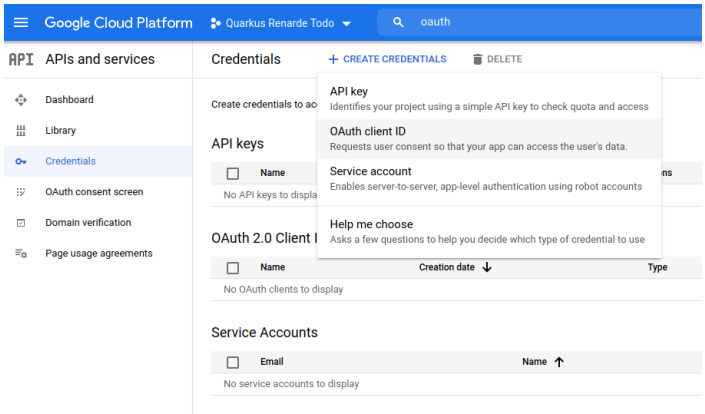
5. Do not add any scopes on the next page, and press *SAVE AND CONTINUE*:



6. Add some test users on the next page if you'd like, and press *SAVE AND CONTINUE*.

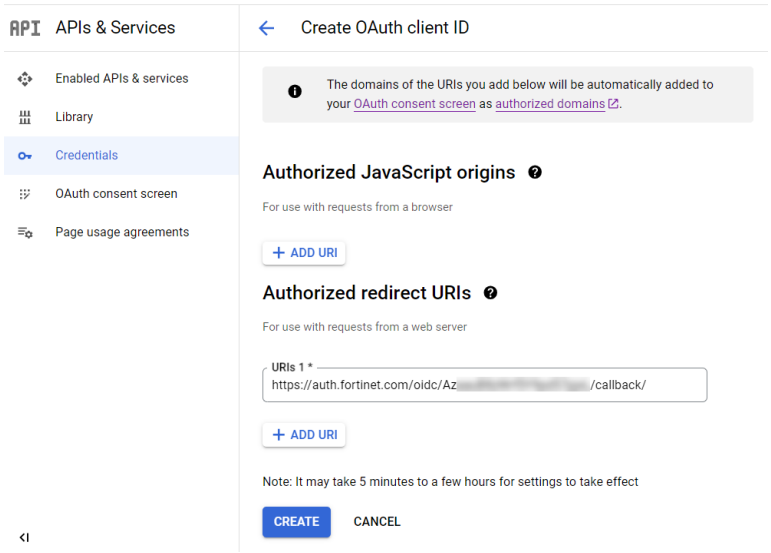


7. Click on the top menu *CREATE CREDENTIALS > OAuth client ID*.

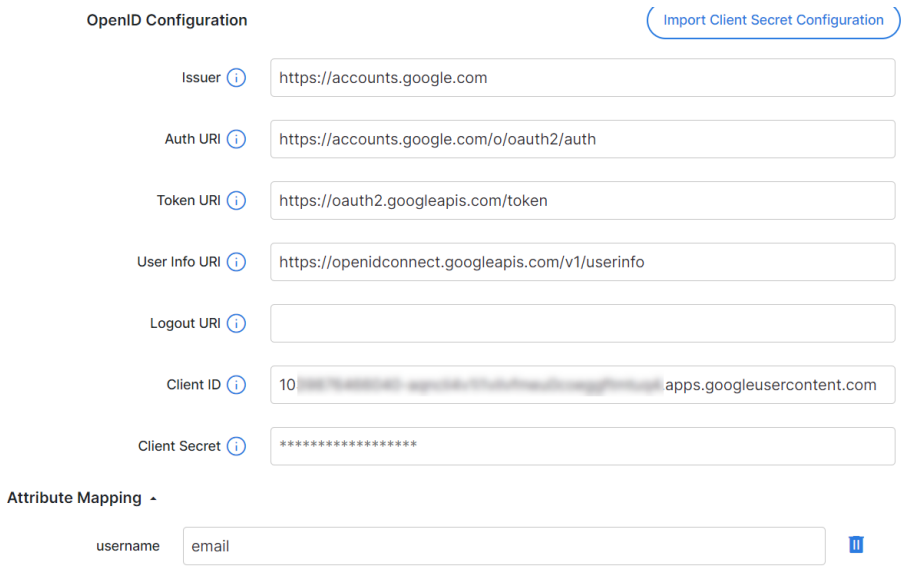


8. Now before we continue to the next page, on FIC, create a new user source and set the *Interface* to *OIDC*.
9. Take note of the *Callback URL* in the following screenshot.

10. Select *Web application* as *Application type*, and add the *Callback URL* in the *Authorized redirect URIs* list, then press *CREATE*.



11. Then copy your *Client ID* and *Client Secret* and fill out the rest of the fields as shown in the following illustration.



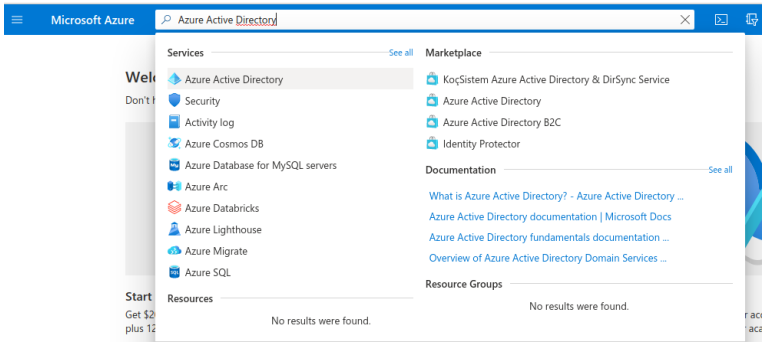
In the example above, we are mapping the "username" attribute to "email" because we're identifying the users on Google via email, and the attribute we're using to identify the users is "username."

12. When you're done, click *Save*. This should work with the existing SPs that you've set up on FIC.

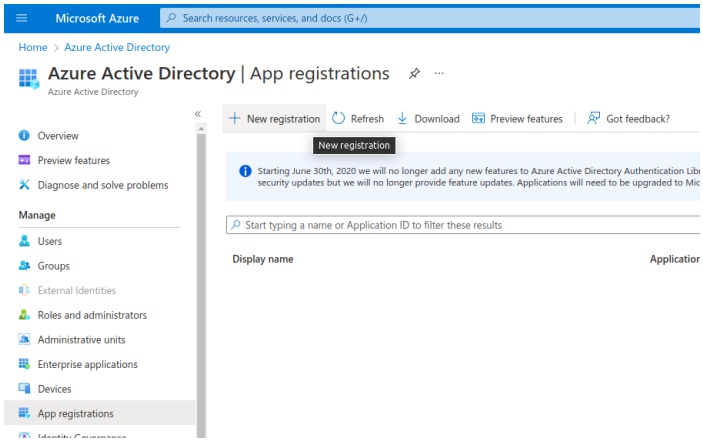
Example 4: Azure OIDC as IdP

In this example, the SP can be any supported Fortinet application. For a complete list of supported Fortinet applications, see Compatible Fortinet applications on page 38.

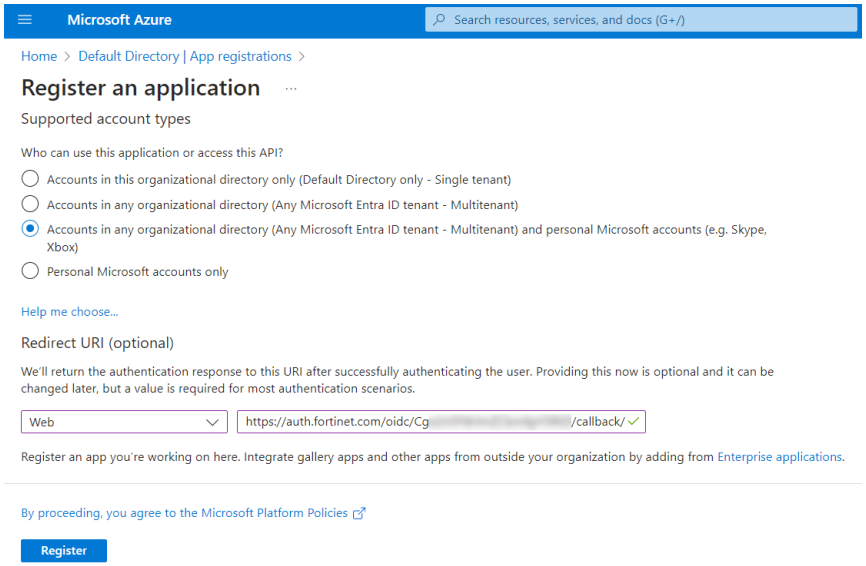
1. In order to set up OIDC for Microsoft, you need to go to your Microsoft Azure Portal, search for Azure Active Directory, and click it.



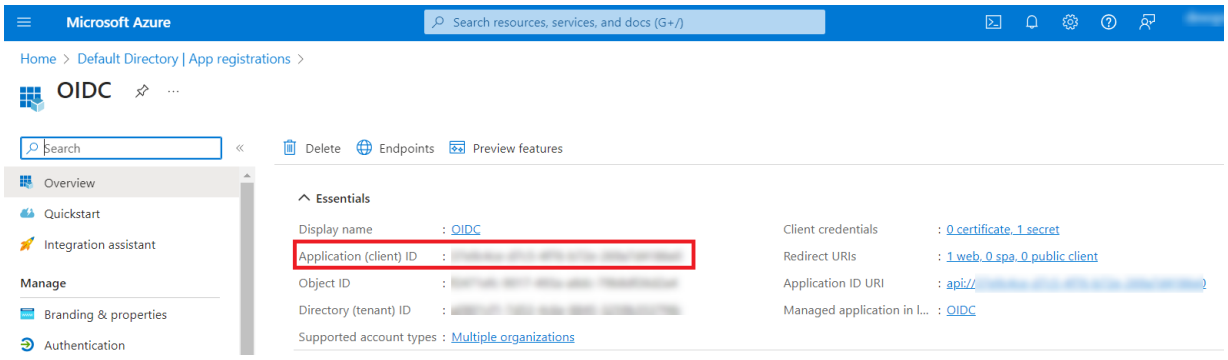
2. *Select Manage > App registrations*, and click *New registration*.



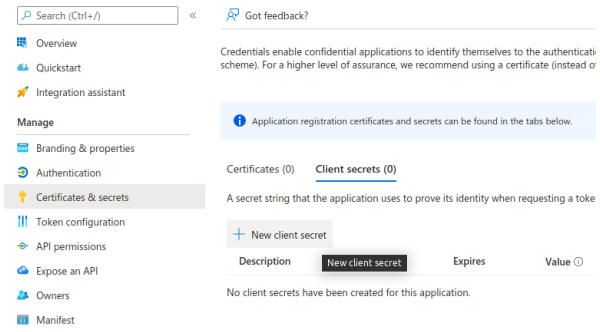
3. On FIC, create a new user source and set the Interface to OIDC just like in the Google OIDC example. Take note of the callback URL. Then, on the next page in Azure, fill in your application name, select *Accounts* in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox) to allow anyone to log in, add a Web Redirect URI with the callback URL from FIC, and click *Register*.



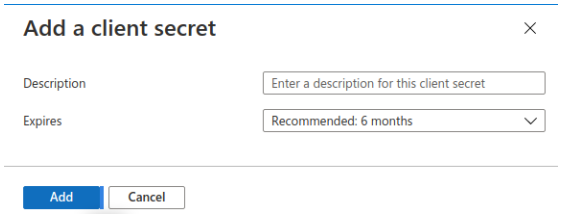
4. On that resulting page, copy the *Client Id* (under Application (client) ID, and click *Add a certificate or secret:*



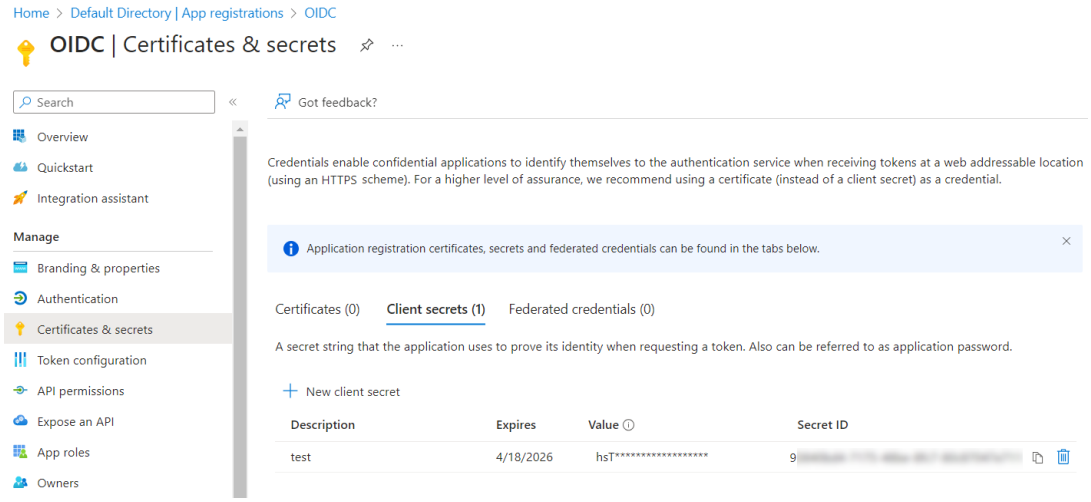
5. Now, under *Client secrets* (0), click *New client secret*:



6. Click *Add* in that dialog without changing anything.

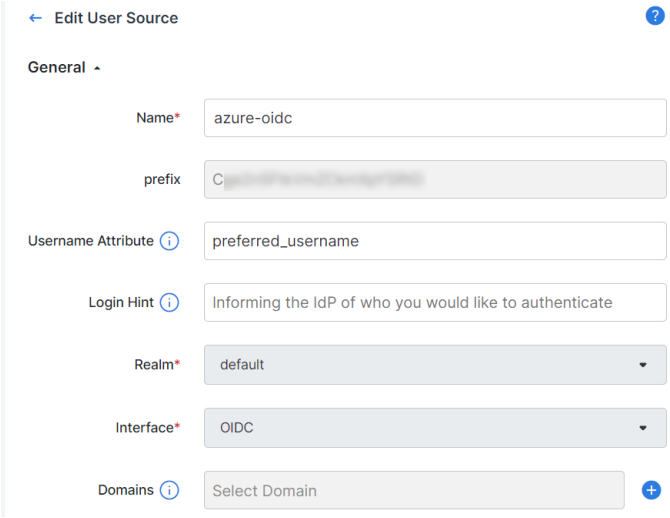


7. On the resulting page, copy your *Secret Value*.

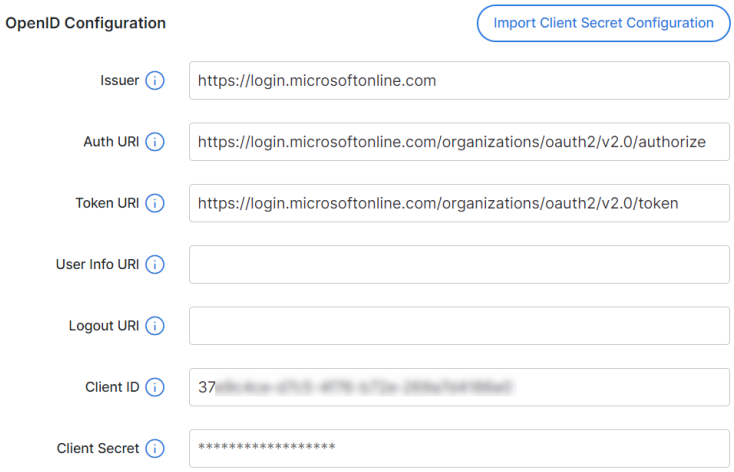


8. Going back to the FIC configuration, note that if your users do not have any email set on them in Azure, then you'll need to configure a custom username attribute. In our example, we do not had any email configured on our Azure users so we're configuring the username attribute with Microsoft Azure's "preferred_

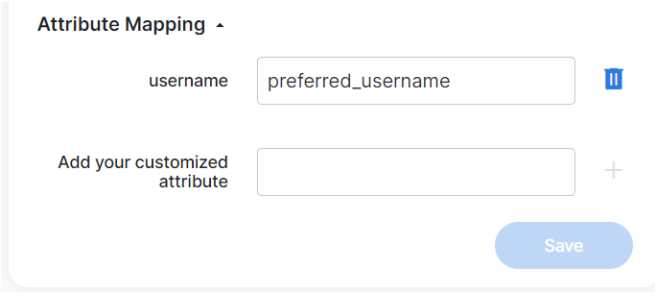
username" field in order for FIC to be able to identify the username from the access token. You can read up more in Microsoft's documentation about which fields are included their OIDC access tokens if you wish to use different fields:



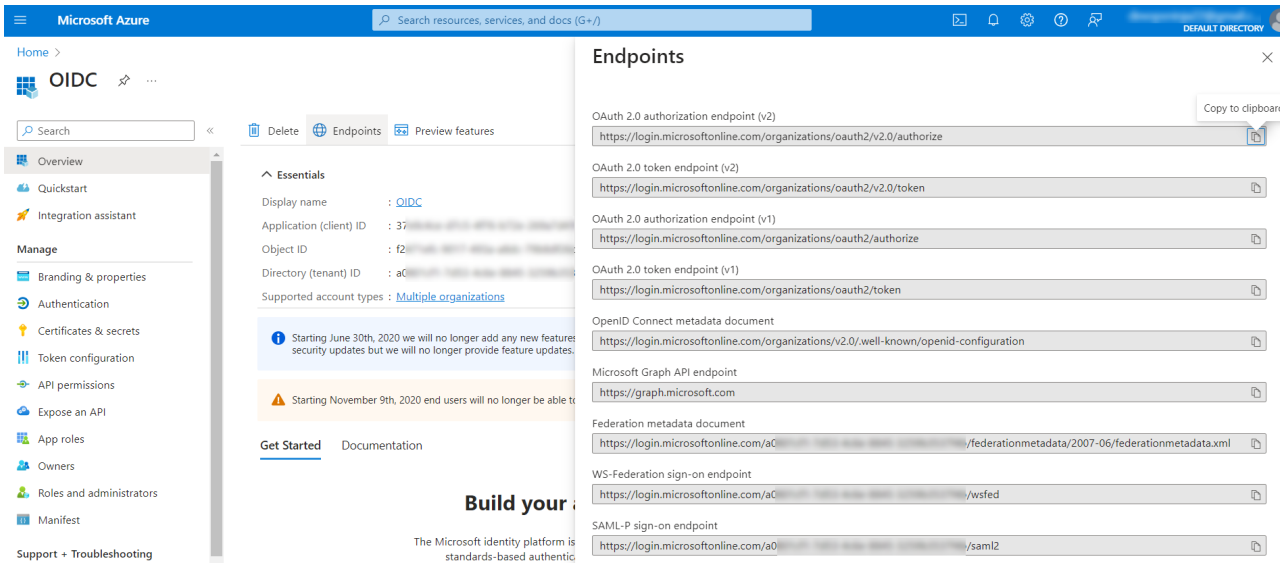
9. And here is what we are going to put in the *OpenID Configuration* section for our example:



10. If you used "preferred_username", make sure to configure the attribute mapping as well:



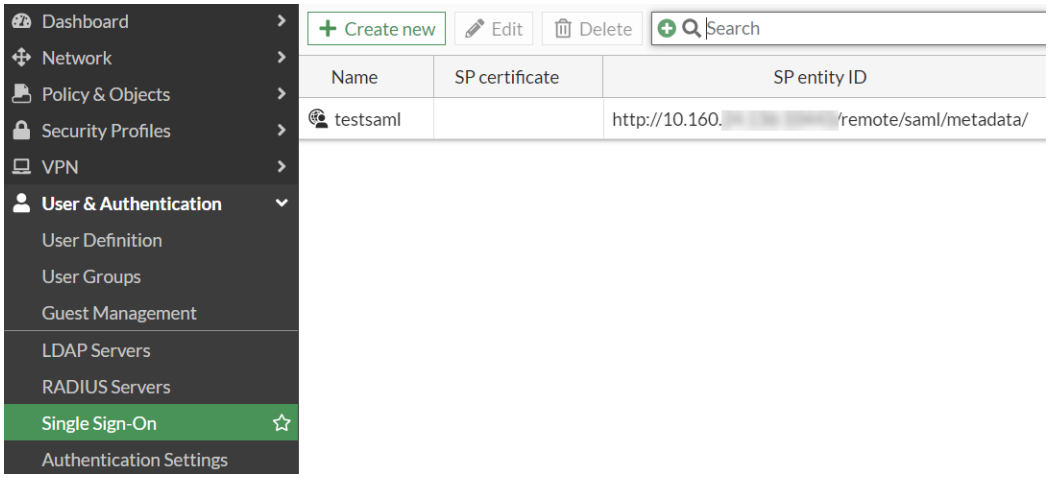
11. You already got the client and the secret from earlier. If you need to reference the other fields, you can get it from here in Azure by clicking Endpoints in the Overview page of your app:



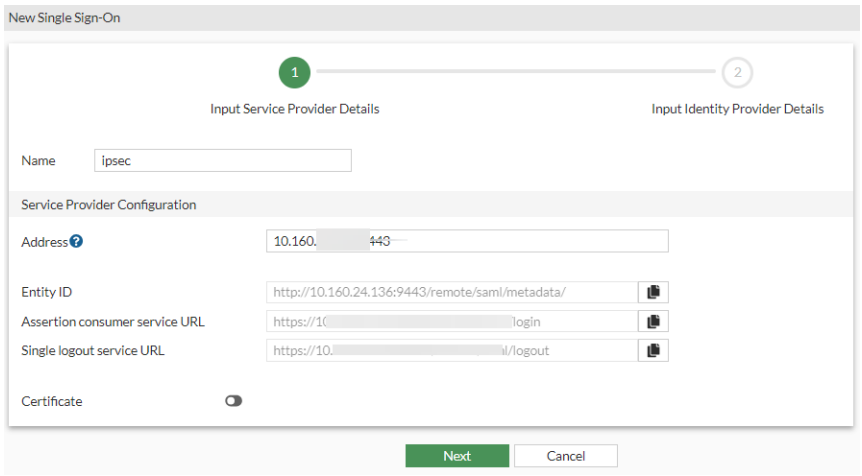
12. After clicking *Save* in FIC, this Azure OIDC IdP should be ready to be added into your FIC IdP proxy setup.

Example 5: FortiGate IPsec as SP

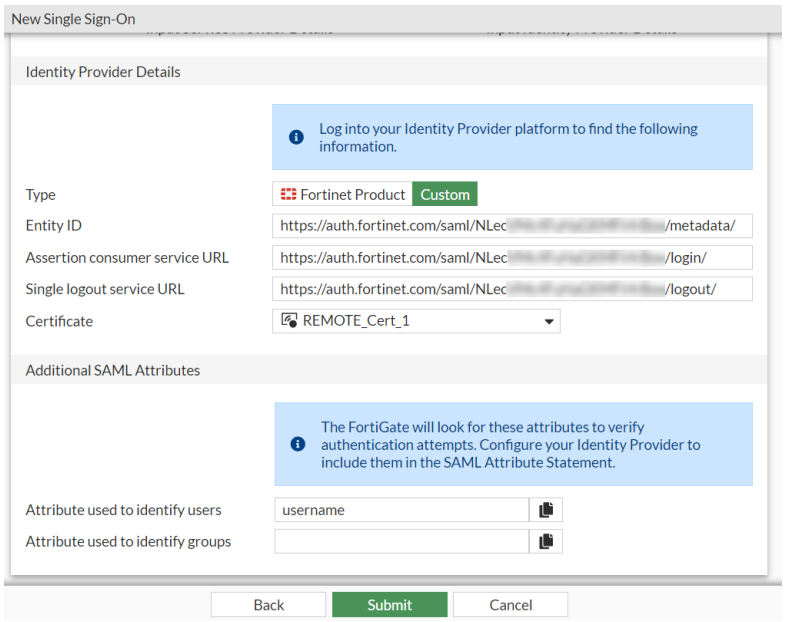
1. On the FIC portal, click *Applications* > *SSO* > *Add SSO Application*.
2. In the *General Information* and *Interface Detail* sections, make the required entries and selections.
3. Leave the FIC GUI page open, launch the FortiGate GUI, and click *User & Authentication* > *Single Sign-On*.



4. In the *Address* field, enter the IPsec address that you want to use. In this example, we use Port 9443 for the `auth-ike-saml-port`, so make sure to append the port number to the address. Then take note of the Entity ID, Assertion consumer service URL, Single logout service URL, and copy and paste them into the *SP Metadata* section in the FIC SAML app that you have added in Steps 1 through 2.



5. Click *Next*.
6. Then go back to the FortiGate GUI, copy the Entity ID, SSO URL, and SLO URL from the IdP Metadata section on FIC to the Identity Provider Details section on FortiGate.



7. Go back to the FIC portal to complete configuring the SAML app that you left off in Step 2 by clicking *Applications* > *Web* > *Authentication* to configure its authentication settings, (optionally) add any customized attribute that you may want, and click *Save*.
8. Click *Applications* >*Web*, and locate the SAML application that you have created. Then click the tool icon, select *Details*, and download the signing certificate to your local machine.

9. Go back to the FortiGate GUI (Step 4 above), and import the certificate to the FortiGate, and click *Submit*.
10. Now on the FortiGate, launch the Console interface and start configuring the IPsec VPN using the following CLI command.

```
config system global
    set auth-ike-saml-port 9443
end
```

11. The `ike-saml-server` setting enables a configured SAML server to listen on a FortiGate interface for SAML authentication requests from FortiClient remote access IPsec VPN clients. Currently, this setting can only be configured in the CLI as follows. Here, “vpnsaml” is the name we used in the single sign-on setting we configured earlier.

```
config system interface
    edit <name>
        set ike-saml-server vpnsaml
    next
end
```

12. Next, configure the IPsec VPN certificate either from the FortiGate GUI or Console interface.

    To configure the IPsec VPN certificate from the GUI:

    a. Go to *User & Authentication* > *Authentication Settings*, and select the certificate from the Certificate drop-down menu.
    b. Import the certificate on the FortiGate by following the procedures in Import a certificate.

    To configure the IPsec VPN certificate in the CLI:

    a. Make sure that the certificate (i.e., VPN-Certificate) has been imported to the FortiGate.
    b. Execute the following commands:

```
config user setting
    set auth-cert "VPN_Certificate"
end
```

13. Configure IPsec VPN on the FortiGate with FortiClient as the dial-up client:
    a. Go to *VPN* > *IPsec Tunnels*.
    b. Click *Create New* > *IPsec Tunnel*.

       The *VPN Creation Wizard* is displayed.
    c. Enter the *Name* as *FCT_SAML*.

       Note: This example does not use the VPN wizard for the IPsec tunnel configuration, but configures a *Custom* IPsec tunnel instead.

d. Configure the *Template* type as *Custom*.
e. Click *Next*.
f. Configure the following options:

Parameter	Description
Name	*FCT_SAML*
Comments	(Optional)
Network	
IP Version	*IPv4*
Remote Gateway	*Dialup User*
Interface	*port1* Select the IPsec tunnel gateway interface.
Mode Config	*Enable*
Use system DNS in mode config	(Optional) Enable FortiClient to use the host's DNS server after it connects to VPN.
Assign IP From	*Enable* Select Address/Address Group from the dropdown list.
IPv4 mode config	
Client Address Range	*VPN_Client_IP_Range* *VPN_Client_IP_Range* is configured from *10.212.134.1* to *10.212.134.200*. If it is not already created, select *Create > Address* from the dropdown menu to create a new address object. See Subnet for more information.
Subnet Mask	*255.255.255.255*
DNS Server	*8.8.8.8*
Authentication	
Method	*Pre-shared key*
Pre-shared key	Enter the pre-shared key of at least six characters.
IKE	
Version	*2*
Peer Options	
Accept Types	*Any peer ID*
Phase 1 Proposal	
Encryption	*AES128*
Authentication	*SHA256*

Parameter	Description
	Select the desired Encryption and Authentication algorithms that should also match with Phase1 Proposals configured on FortiClient. See Configuring IPsec VPN profile on FortiClient.

g. Keep the other settings as default.
h. Click *OK*. The newly created IPsec tunnel should now be visible under *VPN > IPsec Tunnels*.
i. Because IKEv2 uses EAP for user authentication, enable EAP using the following CLI command inside the configured IPsec tunnel for user authentication:

```
config vpn ipsec phase1-interface
    edit "FCT_SAML"
        set eap enable
        set eap-identity send-request
    next
end
```

For advanced custom configurations as per your requirement, see Remote access.

14. Configure firewall policies using the following steps:
    a. Go to *Policy & Object > Firewall Policy*.
    b. Click *Create New*.
    c. Make the following entries:

Parameters	Description
Name	*IPsec to DMZ* Enter the desired name.
Incoming Interface	*FCT_SAML* Select the configured IPsec tunnel.
Outgoing Interface	*DMZ* Select the interfaces that FortiClient needs access to when it connects to VPN.
Source	Under *Address*, select *VPN_Client_IP_Range*. Under *User*, select *vpnsaml* .  The group under *User* is the SAML user group configured in the earlier steps. You need to add the single sign-on server you made into a user group and then add that user group to this policy.
Destination	*DMZ subnet* Click *Create* if it is not already created. See Subnet for more information.

Parameters	Description
Service	*ALL*

d. Click *OK*.

e. Because the IPsec tunnel is configured as a full-tunnel, create another policy to allow traffic from IPsec to Internet and to allow FortiClient to access Internet through IPsec tunnel.

15. Configure the IPsec VPN profile on FortiClient:

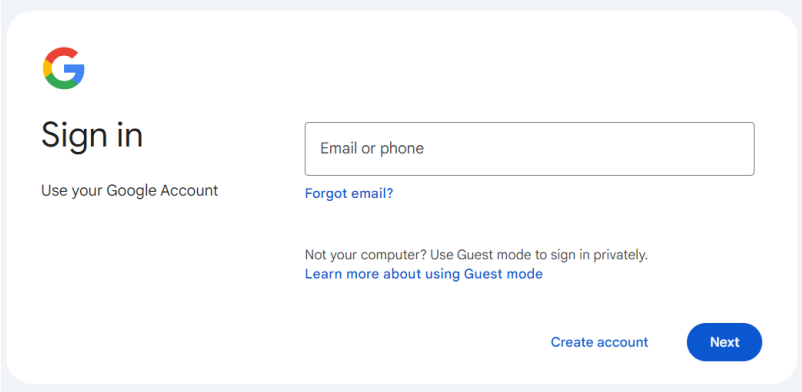
a. In FortiClient, go to *Remote Access* > *Configure VPN* or *Add a new connection*.

b. Configure the following settings to set up an IPsec IKEv2 profile on FortiClient:

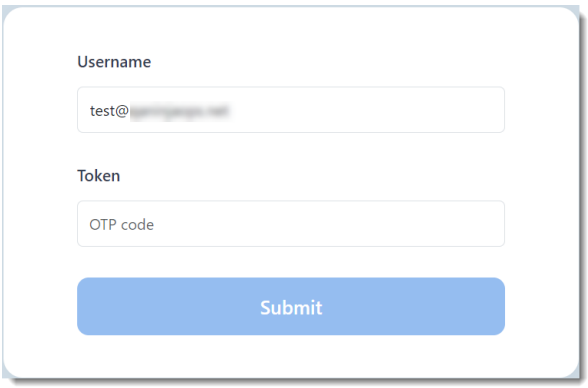
Parameter	Description
Connection Name	*VPN-Tunnel*
Remote Gateway	*<VPN Gateway FQDN> or <VPN Gateway IP>*
Authentication Method	*Pre-shared key with Enable Single Sign On (SSO) for VPN Tunnel* enabled.
Customize port	*9443*
Advanced Settings > VPN Settings	
IKE	*Version 2*
Options	*Mode Config*

To explore additional custom options to configure IPsec VPN profile, see Configuring an IPsec VPN connection.

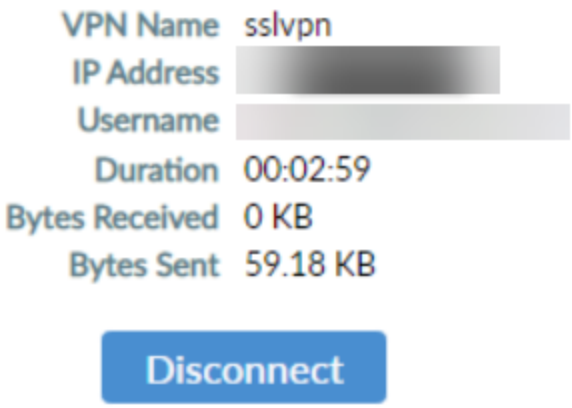
16. After clicking *Save*, if you try to connect to the VPN, you now should be taken to your IdP's sign-in page.



17. Log in, and you should be taken to the OTP page.

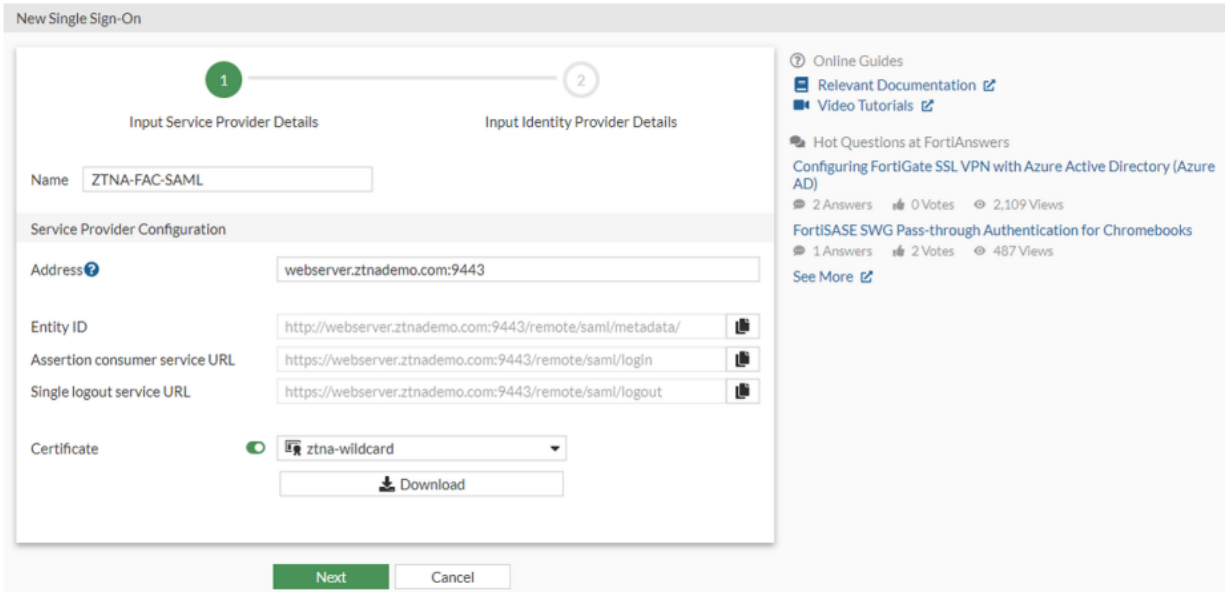


18. Verify the token using the MFA method you selected when creating the user on FIC earlier. Now the end user should be able to log into the IPsec VPN through FortiClient, as shown in the following illustration.

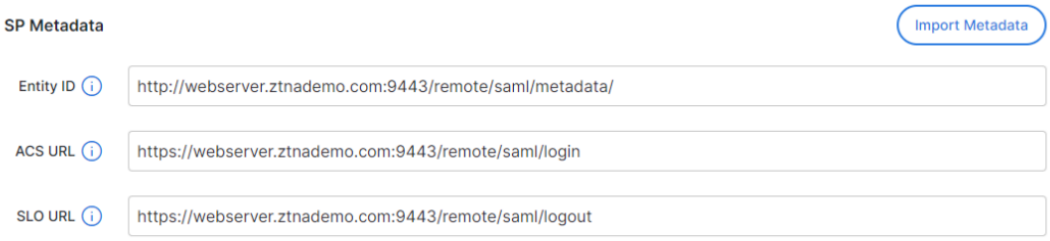


Example 6: ZTNA application gateway with SAML as SP

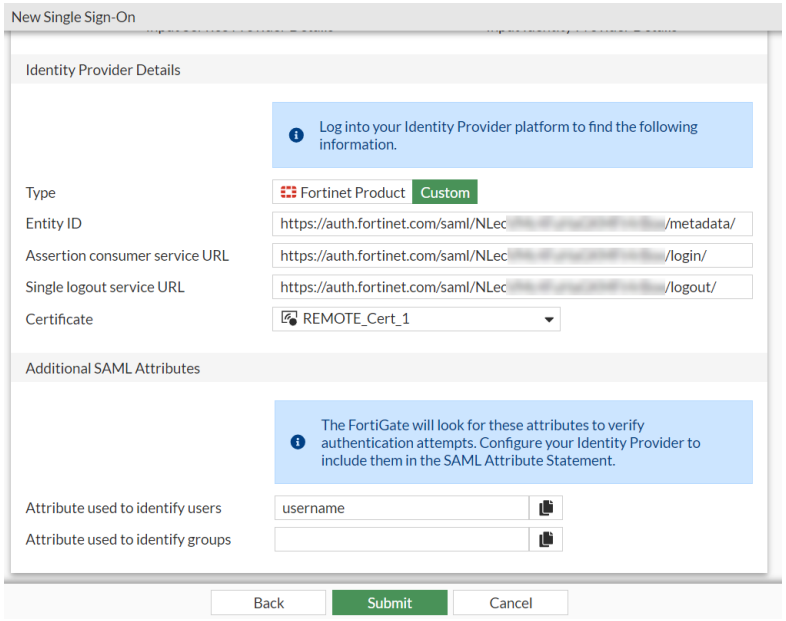
1. Complete the initial setup by following the instructions in Configure ZTNA HTTPS access proxy.
2. Create a new SAML user/server on FortiGate GUI:
   a. On the FortiGate, click *User & Authentication* > *Single Sign-On*.
   b. Click *Create New*.
   c. Set *Address* to `webserver.ztnademo.com:9443`.
   Note: The *Entity ID*, *Assertion consumer service URL*, and *Single logout service URL* will be updated.
   d. Take note of the aforementioned updates, for you will be prompted to enter them into FIC.
   e. Enable *Certificate*, and select the certificate used for the client.
   In this example, the *ztna-wildcard* certificate is a local certificate that is used to sign SAML messages that are exchanged between the client and the FortiGate SP.



   f. Click *Next*.
   g. Use the settings from FIC to fill the custom *Identity Provider Details*. On FIC, go to *Applications* > *SSO* > *Add SSO Application*, and get the IdP Metadata details from the page:
      - Where the REMOTE_Cert_1 certificate is a remote certificate that is used to identify the IdP. You'll want to use the certificate you get from after you create the FIC SSO application if you click the tool icon, select *Details* , and click to download the *Signing Certificate*.
      - In the meantime, on FIC fill out the *SP Metadata* section with the *Entity ID, Assertion consumer service URL and Single logout service URL:*



h. Set *Attribute used to identify users* to username. (**Note:** Attributes to identify users and groups are case-sensitive.)



i. Click *Submit* to save the settings.

3. Create a user group for the SAML user object:
   a. Click *User & Authentication* > *User Groups* > *Create New*.
   b. Set *Name* to *ztna-saml-users*.
   c. Under *Remote Groups*, click *Add*.
   d. For *Remote Server*, select *ZTNA-FAC-SAML*.
   e. Click *OK*.
   f. Click *OK* again to save the settings.
4. Apply the SAML sever to proxy authentication:
   a. Go to *Policy & Objects* > *Authentication Rules*.
   b. Click *Create New* > *Authentication Scheme*.
   c. Set *Name* to *ZTNA-SAML-scheme*.
   d. Set *Method* to *SAML*.
   e. Set *SAML SSO server* to *ZTNA-FAC-SAML*.
   f. Click *OK*.
   g. Go to *Policy & Objects* > *Authentication Rules*.
   h. Click *Create New* > *Authentication Rule*.

i. Set *Name* to *ZTNA-SAML-rule*.
j. Set *Source Address* to *all*.
k. Set *Incoming Interface* to *port3*.
l. Set *Protocol* to *HTTP*.
m. Enable *Authentication Scheme* and select *ZTNA-SAML-scheme*.
n. Set *IP-based Authentication* to *Disable*.
o. Click *OK*.

5. Configure the active authentication scheme and captive portal:
   a. Go to *User Authentication > Authentication Settings*.
   b. Enable *Authentication scheme*.
   c. Select *ZTNA-SAML-scheme*.
   d. Set *Captive portal type* to *FQDN*.
   e. Enable *Captive Portal*.
   f. Select the firewall address *webserver.ztnademo.com*. (**Note:** Choose this firewall address if you have not already done so.)
   g. Click *Apply* to save the configuration.
6. Configure a ZTNA application gateway to allow SAML authentication requests to the SP:
   a. Configure the ZTNA server:
      i. Go to *Policy & Objects > ZTNA > ZTNA Servers > Create New*.
      ii. Configure the following:

Parameter	Desription
Name	ZTNA-access
Interface	Any
IP	10.0.3.10
Port	9443
SAML	Enabled
SAML SSO Server	ZTNA-FAC-SAML
Default certificate	ztna-wildcard

      iii. Click *OK*.
   b. Define the full ZTNA policy to allow access tto the ZTNA server:
      i. Go to *Policy & Objects > Proxy policy > Create New*.
      ii. Configure the following:

Parameter	Description
Name	ZTNA-Rule
Type	ZTNA
Incoming Interface	port3
Source (Address)	all

Parameter	Description
Source (User)	ztna-saml-users
Destination	all
ZTNA Server	ZTNA-access
Action	Accept
Log Allowed Traffic	All Sessions

iii. Click *OK*.

Once all of the aforementioned configurations are completed on your FGT and the SAML application and User Source(s) are set up on FIC, end-users should be able to start going through the FIC SAML login process when trying to access web servers through ZTNA.

Managing End-User Portal

End-user portals enable FIC end users to manage their own settings according to the permissions granted by their administrator.

End-user portals are realm-specific and must be implemented by the administrator on a per-realm basis. Before starting to configure end-user portals on a realm, ensure that the realm has already had a functioning IdP user source configured on it. For information about IdP user source configurations, refer to Configuring IdP user source on page 173. Your end users in the IdP user source are able to authenticate and log into their end-user portals once you have enabled the End-user Portals function on the realm.

Similar to SSO applications, the look and feel of end-user portals can be customized to align with your company's corporate theme and style. For more information, refer to Creating an End-User Portal branding theme on page 225and Applying custom branding theme to End-User Portal on page 226.

End users' mobile phone numbers and email addresses are validated through verification codes when they are trying to log into their portals and then saved to the FIC database upon successful validation. After logging into their end-user portals, end users are able to update their mobile phone numbers if the administrator grants them the permission to do so when enabling the end-users portals.

Configuring End-User Portal

1. From the main menu, click *Applications>End-User Portals*.
2. Click *Add User Portal*.
3. Make the entries and/or selections as described in the following table.
4. Click *Save* to enable the end-user portal.

Parameter	Description
General	• *Name* — Specify a name for the end-user portal to be created. • *Subdomain* — Enter your subdomain. This feature enables users of the End-user Portal to access the portal using your custom URL rather than the URL generated by FortiIdentity Cloud. After entering your subdomain, click the (!) icon to validate it. If the domain is available, the validation will succeed. Otherwise, choose another domain and try again. • *Realm*— Select the realm to which the end-user portal is to be added.

Parameter	Description
	• *Custom Branding* — Click the down arrow to select a branding theme from the drop-down list or click the + (Add) to add a new one. For more information, see Creating an End-User Portal branding theme on page 225 and Applying custom branding theme to End-User Portal on page 226. • *Session Timeout*— Set the length of time (in minutes) each portal session lasts before it times out. **Note:** This setting is not visible on end-user portals, and cannot be modified by end users.
User-Customizable Settings	 When an end-user portal is created, all the end-users will inherit the existing settings of their realm. You can use the following radio buttons to allow/disallow the end users to customize their portal settings after they have logged into their end-user portals. • *Profile* — Allow/Disallow end users to update their profiles. • *Passkey* — Allow/Disallow end users to set or delete their passkeys. • *Token Renewal* — Allow/Disallow end users to renew their FTM tokens. • *MFA Method* — Allow/Disallow end users to change their MFA methods.
Authentication	• *User Source* — The IdP user source from the same realm. Users from the IdP user source will be able to log into the end user portals. • Default User Source — If selected, this user source will be by default if multiple user sources are available.

Configuring IdP user source

An end-user portal is automatically enabled and ready to use by the end users in the realm when it is created by the administrator. However, before starting to creating an end-user portal, you must ensure that the realm has already had an IdP user source configured on it.

Following are examples of how to configure user sources for an end-user portal:

- Example 1: Google SAML as IdP and FortiGate SSL VPN as SP
- Example 2: Azure as SAML IdP and FortiGate as SP
- Example 3: Google OIDC as IdP
- Example 4: Azure OIDC as IdP

Keeping SSO applications off End-User Portal

SSO applications that are configured in the same realm where the end-user portals are enabled automatically show up under the *Applications* menu on the end-user portal. The end users can then launch the SSO apps directly from the portals by clicking the shortcuts to the apps after they have successfully logged into the portal.

To prevent end users from accessing the SSO apps from the end-users portal, you must remove the login URLs of the SSO applications from the SSO application configurations on the FIC portal.

To keep the SSO app off the end-user portals:

1. From the main menu, click *Applications>SSO Applications*.
2. Locate the SSO app, click the drop-down menu at the end of the row, and select *Edit*.
3. In the General setting of the Edit Application page, locate the Login URL field, and remove the URL.
4. Click *Save*.

- Once you have saved the change, the SSO application becomes inaccessible to the end users and will not show up as a shortcut on the end-users portal.
- Removing the login URL in the configuration of an SSO application only removes end-users' direct access to it from the end-user portals, but has no impact on the function of the SSO application.
- Repeat the steps mentioned above to remove all the login URLs

Adding user source

1. Click *Authentication* > *User Source*.
2. Click *Add User Source*.
3. Under *Source Information*, make the following configurations and click *Next*.

Parameter	Description
Name	Specify the user source name.
prefix	System-generated; no action is needed.
Username Attribute	Enter a specific attribute in the SAML application or user profile that is used in the username.
Login Hint	Enter a key that help the IdP to identify the user to authenticatem
Realm	Select a realm.
Interface	Select an interface.
Domain	Select a domain to add domain mapping, or click the + sign to add an new domain mapping.

4. Under *Interface Detail*, make the following configurations, and click *Next*.

Parameter	Description
POST Binding	If enabled, SAML messages will be encoded and sent in the body of HTML POST requests.
Include Subject	If enabled, the <Subject> element that specifies the user expected in authentication assertions will included be included. This allows the IdP to bypass the username input on the login page.
Signing Certificate	Upload the signing certificate.
SP Metadata	• *Entity ID* — The Entity ID of the IdP Proxy. • *ACS URL* — The Assertion Consumer Service URL automatically generated for your user source. • *SLO URL* —The Single Logout URL automatically generated for your user source.
IdP Metadata	• *Entity ID* — The Entity ID associated with your IdP. • *Login URL* — The Login URL of your IdP. • *Logout URL* — The Logout URL if your IdP.

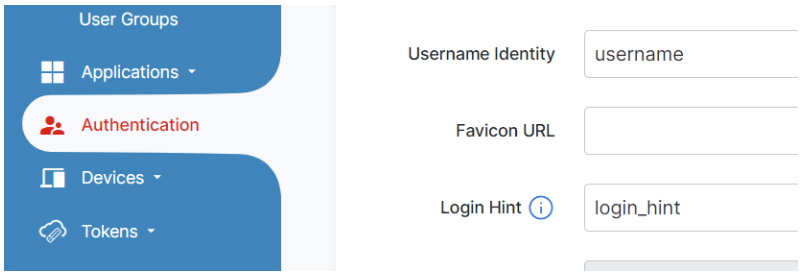
5. Under *Attribute Mapping*, enter your customized attribute, click the + sign, add the mapped attribute, and click *Save*.

For more information, see Using SSO applications on page 138.

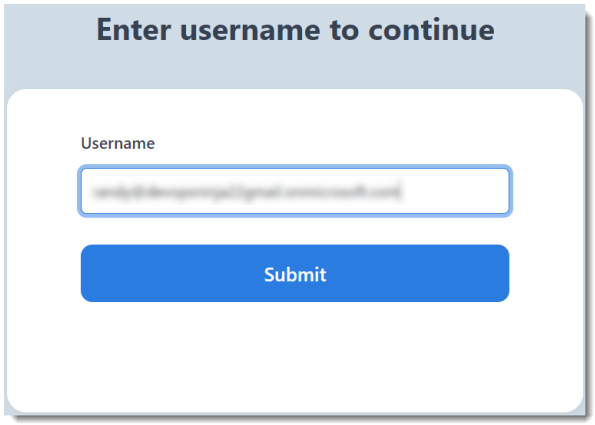
Login hint

The login hint setting is used so that when an end user inputs their username from the "Enter username to continue" page. It is automatically populated in the username field once they are redirected to the IdP login page. For example, with our Azure example from earlier where we set login hint to "login_hint," this is what it would look like:

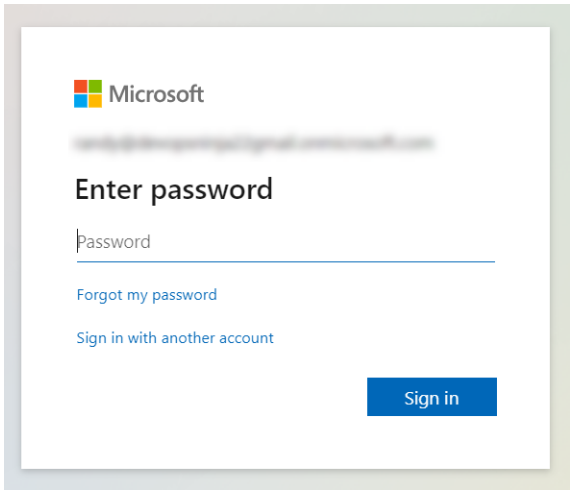
Login Hint setting:



Input username into "Enter username to continue" page when a domain mapping is configured:



Username is automatically populated:



Some IdP vendors, such as Google, do not have a logout URL for you to configure into the IdP metadata field. In this case, logging out of the SP does not fully log the end user out.

Configuring domain mapping

With domain mapping, end users are prompted to enter their username when trying to log into the SP. Upon inputting their username, they are automatically directed to the SP's sign-in page if the domain of their username matches the configuration.

To configure domain mapping:

1. Click *Authentication* **>** *Domain Mapping*:
2. Click *Add Domain*.
3. Specify the domain name.
4. Select the realm.
5. Select the user source.
6. Click *Save*.

Managing device ownership

The *FortiProducts >Ownership >Devices* page shows all devices under your management.

Column	Description
SN	The serial number of the device.
CLUSTER ID	The ID of the HA cluster to which the device belongs.
OWNERSHIP STATUS	The status of the device ownership: • Consistent — The ownership of the device belongs to the current account. • Inconsistent — The ownership of the device does not belong to the current account and some data from the old account still remains on the device.
Tool	The slide-in toolbar provides the following tools: • Validate — Refresh the ownership status of the device. See Validating device ownership on page 180. • Delete — (1) Remove all user and application data that the preceding owner has left on the device. (2) Remove the device information from the *Manage Device Ownership>Devices* table on both the preceding owner's and the current owner's sides. After the delete is completed, if the current owner wants to sync up the data for this device, they must execute the command `exec fortiidentity-cloud update` from the device, for example FortiGate. (**Note:** This option is available only when the ownership status of the device is "Inconsistent".) • Transfer — Start the device transfer task which will show up under the Tasks tab. (**Note:** This option is available only when the ownership status of the device is "Inconsistent".) See Managing device transfer on page 182.

This section discusses the following topics:

Validating device ownership

FIC is able to handle device ownership transfer without human intervention, automatically cleaning up user data on the transferred device from the source account.

Below are the use cases that show how FIC handles change of device ownership:

- If you move a device (e.g., FortiGate) license and the FIC license to a new account, your FIC service will continue after the transfer.
- If you move the FIC license to a new account but leave the device in the old account with no other FIC license, there will be no FIC service for the device.
- If you move the device license to a new account where there is another (new) FIC license and leave the old FIC license in the old account, usage from that device now will count against the new FIC license (not the old one).
- If you move the FIC license to a new account but leave the device in the old account, and then add a new FIC license to the old account, usage from that device will count against the new license (not the old one).

To validate the ownership of a device:

1. Click *Applications* > *FortiProducts* > *Ownership*.
2. Under *Devices*, Identify the device.
3. Click the tool icon, and select *Validate*.
4. Click *Yes*.

Transferring devices

Device transfer must be handled through the FortiCare ticket system.

You must have your FortiGate serial number ready and provide the source account email and the target account email. The FortiCare team will send out authorization email to the email recipients for approval. Once they have received the authorization email, the FortiCare team will start the transfer process and notify you when the device transfer has been completed.

Clean up user data from the source account

Clean-up of user data from the source account can be performed from the FIC portal only. See Transferring devices on FIC on page 181.

1. Log into `fic.fortinet.com` using the source or target FC account.
2. Click *Applications* > *FortiProducts*> Ownership.
3. Identify the device whose *OWNERSHIP STATUS* is marked *Inconsistent*.
4. Click the tool icon, and select*Validate*.

5. Read the messages onscreen.
6. Click the tool icon, and select *Delete* if you want to remove the users from the account.
7. In the warning message. click*Yes*.

Wait for a few minutes for the clean-up process to complete before clicking*Validate*.

If you click the *Validate* button while the clean-up is in progress, you will see the message, *"Data under this device is being deleted...."*

The clean-up process is completed if you see the *"This device ownership info is up to date...."* message after clicking *Validate* from the target account or the *"Not allowed to check the device info."* message when clicking *Validate* from the source account.

Transferring devices on FIC

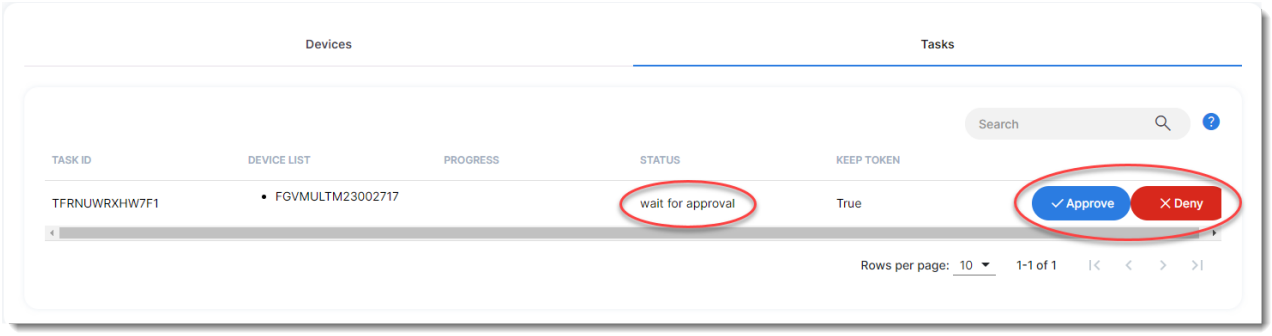
You can transfer devices from one FIC account to another using the FIC portal. While the transfer is being processed, your end users should not notice any changes in their user experience. For example, if they have logged in through VPN, they can continue using VPN while the device is being transferred.

FortiIdentity Cloud approves device transfer requests automatically if the source account has been removed or merged into another account in FortiCare. We strongly recommend clearing any sensitive user data off the device before removing it from the source account or merging it with another FortiCare account.

To transfer a device with data:

1. Submit a device ownership transfer ticket in FortiCare.
2. Wait until after the ticket is processed and the ownership is transferred to the new owner in FortiCare. For example, Account A is the original owner and Account B is the new owner.
3. Now the owner of either Account A or B can start the device transfer by selecting *Applications* > *FortiProducts* > *Ownership*.
4. Click *Go to*.
5. Under *Devices*, locate the device whose *OWNERSHIP STATUS* is marked *Inconsistent*.
6. Click the tool icon, and select*Transfer*.
7. If you are NOT the owner of the new account who has initiated the device ownership transfer, click *Applications* >*FortiProducts*>*Ownership*>*Tasks,* locate the transfer task, and click *Approve*.

- Device ownership transfer tasks are viewable by both parties involved in the transfer process.
- A device ownership transfer task cannot be initiated and approved by the same party. If you have initiated a device ownership transfer task, you must wait for the other party to approve it.



8. Wait until the *Progress* column shows 100% and the *Status* column shows *Complete*. By then, the ownership of the device should have been transferred to the new owner, and any old data left on the device should have been wiped out.

Transfer tasks will remain on the page for 24 hours before being deleted automatically.

To transfer a device without data:

If all data related to the old account has been removed from the device, FIC can automatically transfer the device ownership to the new owner. However, the device will not appear in the new account.

To establish a new connection between the FIC portal and the application (FortiGate for this case), you must log in to the FortiGate device and run the CLI command "`execute forttoken-cloud update`".

Managing device transfer

The *Applications>FortiProducts > Ownership>Tasks* page provides tools for managing the transfer of devices.

Cloumn	Description
Task ID	A system-generated identifier of the task.
Device List	The list of all devices in the transfer task.
Progress	The percentage of completion of the transfer task.
Status	The status of the transfer task, which could be one of the following: • Wait For Approve (non-clickable) • Complete (non-clickable) • In Progress (You can click to view the transfer result.) • Failed (You can click to view the transfer result.)
Keep Token	Shows either of the following : • True — all users will keep their token. If selected, the new owner of the device does not need to re-activate the end-users.

Cloumn	Description
	• False — If selected. the new owner of the device must reactive the end-users.
Action	Shows the following options: Approve — Approve the transfer task (This option is disabled for the party who requests the device transfer.) Delete — Deny and remove the device transfer task.

Performing factory reset

If you want to remove all data from a FortiGate device that uses FIC for MFA authentication before transferring or disposing the device, we strongly recommend doing the following:

1. Before performing a factory reset, remove all data on the FortiGate by executing the CLI command `"execute fortitoken-cloud sync"` in the Global VDOM.
2. After the factory reset, log in to the FIC portal and remove any data related to the device that still remains in the portal.

For instructions on how to delete user-related data from the FIC portal, refer to Deleting users from FIC on page 108and Deleting a FortiProduct on page 112.

Managing HA clusters

The *Applications >FortiProducts>Clusters* page provides tools for managing HA cluster configuration using devices in your account.

Searching for a standalone device

On the top of the *Standalone Devices* panel is a *Search by device's SN* tool. It enables you to search for standalone devices by serial number (SN). It comes in handy when you want to locate a standalone device and add it to an existing cluster.

- You can search for a device by any part of its serial number (SN). However, the more specific your entry, the more accurate your search result.

To search for a standalone device:

1. In the *Standalone* panel.
2. Type in any part of the name or serial number of the device.
3. Click *Search*.

The device or devices that match your entry now show up in the table.

Adding devices to a cluster

You can add any device in the *Standalone Devices* panel to any cluster in the *Clusters* panel. Once a standalone device is added to a cluster, it becomes part of the cluster and will be removed from the *Standalone Devices* panel.

Before adding a standalone device to a cluster, make sure that the change you are going to make to the cluster is consistent with its actual configuration.

1. In the *Clusters* panel, locate the cluster of interest.
2. In the *Standalone Devices* panel, locate the standalone device of interest. See Searching for a standalone device on page 184.
3. Select the device, and click *Move in*.
4. When the *Device Management*dialog pops up, be sure to read the message, and click *OK*.

Moving devices between clusters

You can also move devices between clusters in the Clusters panel.

Before moving a device from one cluster to another, you must make sure that the change you are going to make to the clusters is consistent with the actual configurations of your network.

1. In the *Clusters* panel, locate the clusters of interest.
2. Select the device of interest.
3. Click *Move out*. The *Device Management* dialog opens.
4. Read the message, click *OK*.

Removing devices from a cluster

You can remove a device from any cluster in the *Clusters* panel. Once a device is removed from a cluster, it becomes standalone and shows up in the *Standalone Devices* panel.

Before removing a device from a cluster, you must make sure that the change you are going to make to the cluster is consistent with its actual configuration.

1. In the *Clusters* panel, locate the cluster of interest.
2. Click the down arrow to view the devices in the cluster.
3. Highlight the device of interest, and click *Moved Out*.
4. Read the message, and click *OK*.

The device is now removed from the cluster, and appears in the Standalone Devices panel.

Using mobile tokens

The term "mobile" refers to FortiToken Mobile (FTM) tokens for mobile devices. The *Mobile Token* page is read-only and shows all FTMs used by users in your account.

You can access the page by clicking *Security Devices >Mobile* Token.

Column	Description
SERIAL NUMBER	The serial number of an FTM.
USERNAME	The username of the FIC end-user to whom the FTM has been assigned.
REALM	The realm to which the end-user of the FTM has been assigned. **Note:** The field shows "default" if the application associated with the end-user has not been assigned to any custom realm.
PLATFORM	The mobile platform of the FTM, which can be either of the following: • *Android* • *iOS*
ALGORITHM	The algorithm of time-based one-time password authentication used by the token: • *TOTP*
REGISTRATION ID	The registration ID of the FTM.

Using hardware tokens

The term "hardware" refers to FortiToken (FTK) which is the only hardware token that FIC currently supports. The *Hardware* page shows all FortiTokens used by end-users in your account. It also offers tools for adding and deleting FTKs.

You can access the *Hardware* page by clicking *Tokens* > *Hardware* on the main menu. The following table describes the information on the *Hardware* page.

Column	Description
Checkbox	If checked, the corresponding hardware token becomes selected and the *Delete* button enabled. You can then click the button to delete that hard token. For more information, see Deleting hard tokens on page 189. **Note:** You can also check the checkbox in the column header to select all the hard tokens and delete them all at once.
SERIAL NUMBER	The serial number of the hardware token.
MODEL	The model of the hardware token, which can be one of the following: • *FTK200, FTK200B, and FTK210*
USERNAME	The username of the FIC user to whom a FortiToken has been assigned. **Note:** If this field is blank, it means that the FortiToken has not been assigned to any user yet.
LAST UPDATE	The date and time of the most recent update of the hard token.

The *Import Tokens* button enables you to add hard tokens to your account. You can either manually add serial numbers of hard tokens one by one or batch-upload them by importing a .csv file which contains the serial numbers of the hard tokens you want to add to your account. See Batch-uploading hard tokens on page 188.

FTK200CD and FTK200BCD (with the serial number prefix FTK211) are NOT supported.

Adding hard tokens manually

If FTK is set as the default MFA method in the settings of a realm, you can select users on the *Users* page and let FIC automatically assign FTKs to them by clicking the *Auto-assign FTK* button. See Managing users on page 103.

To add hard tokens manually:

1. *Click Security Devices > Hardware Tokens*.
2. Click the *Import Tokens*.
3. Enter the serial number of the hardware token.
4. Click the + sign.
5. Repeat Steps 2 through 3 above to add as many hard tokens as you have available.
6. Click *Save*.
   The *Import Hard Token* dialog closes, and a message pops up in the upper-right corner of the *Hardware* page, informing you how many hard tokens have been successfully added and how many have failed (if any) to be added. You can either click *OK* to dismiss the message, or wait for a few seconds to let it automatically close itself. The serial numbers of the hardware tokens that are successfully added now appear on the *Hardware* Tokens page.

Batch-uploading hard tokens

You can also batch-upload all the hard tokens you want to add at once if you have access to a .csv file that contains the serial numbers of the hard tokens to be added.

Be sure to have the .csv file ready before starting the following procedures.

To batch-upload hard tokens:

1. Click *Security Devices > Hardware Tokens*.
2. Click *Import Token*s.
3. In the upper-right corner of the dialog, click *Upload CSV file*.
4. Locate the .csv file with information about the hardware tokens in your file system, and click *Open*.
   The *Windows Upload File* dialog closes, and all the serial numbers of the hard tokens in the .csv file are now added to the *Import Hard Tokens* dialog.
5. Click *OK*.
   The *Import Hard Token* dialog closes, and a message pops up in the upper-right corner of the *Hardware* page, informing you how many hard tokens have been successfully added and how many have failed (if any) to be added. You can either click *OK* to dismiss the message, or wait for it to automatically close itself in a few seconds. The serial numbers of the hard tokens that are successfully added now appear on the *Hardware* page.

Assigning a hard token to a user

A hard token shown on the *Hardware* page without a username means that it has not been assigned to any end-user yet, and can be assigned to any end-user in your FIC account.

To assign a free hard token to a user:

1. Click *User Management* > *Users*.
2. Identify the user, click the tool icon, and select *Edit*.
3. For Auth Method, select *FTK*.
4. Click *Apply*.

Deleting hard tokens

The *Hardware* page provides tools to delete hard tokens that are no longer needed. You can delete one, multiple, or all the hard tokens at once.

Only unassigned FTK tokens can be deleted.

To delete a hardware tokens:

1. Click *Security Devices* > *Hardware Tokens*.
2. Identify the hardware token, and select it (with the checkbox).
3. Click *Delete*.
4. Click *Yes*.

Using passkeys

Support for passkeys has been implemented in FIC using WebAuthn. According to FIDO Alliance, Web Authentication (WebAuthn), a core component of FIDO Alliance's FIDO2 set of specifications, is a web-based API that allows websites to update their login pages to add FIDO-based authentication on supported browsers and platforms. FIDO2 enables users to leverage common devices to easily authenticate to online services in both mobile and desktop environments.

Passkeys are becoming the norm for enhanced protection in many sites. With passkey support, customers are able to meet higher security standards and protect their organizations from threats like phishing.

Use Case

For example, there are two users, John and Todd, in Company A. Bob is the FIC admin for the organization. The company wants to require all end-users in their company to use passkeys using either the FortiToken 410 USB key or their mobile phones.

To add the FortiToken 410 USB key as the passkey for John, Bob and John must do the following:

1. Bob sets up a PIN for the FortiToken 410 USB key.
2. Bob launches FIC, navigates to *User Management >Users*, locates John, and clicks the tool icon and selects *Manage Passkeys*.
3. Bod then adds the FortiToken 410 USB key to John's profile.
4. John will get the registered FortiToken 410 USB key from Bob, and Bob will share the PIN with him.
5. John can change the PIN for the FortiToken 410 through Security key management in his computer.
6. John can now choose to use 'Login with Registered Passkey' for any SP configured with the FIC's IdP Proxy and use FortiToken 410 USB as Passkey.

To add a SmartPhone as passkey for Todd, the following must be done:

1. Todd needs to bring his phone to Bob
2. Bob launches FIC, navigates to *User Management >Users*, locates Todd, and clicks the tool icon and selects *Manage Passkeys*.
3. Bob choose Todd's iPhone or Android device to save the Passkey and a QR code is be generated.
4. Todd then scans the QR code to his phone and adds the passkey to his device.
5. If Todd is a new employee who gets a company provided phone, Bob can scan the QR code in Todd's company-provided phone.

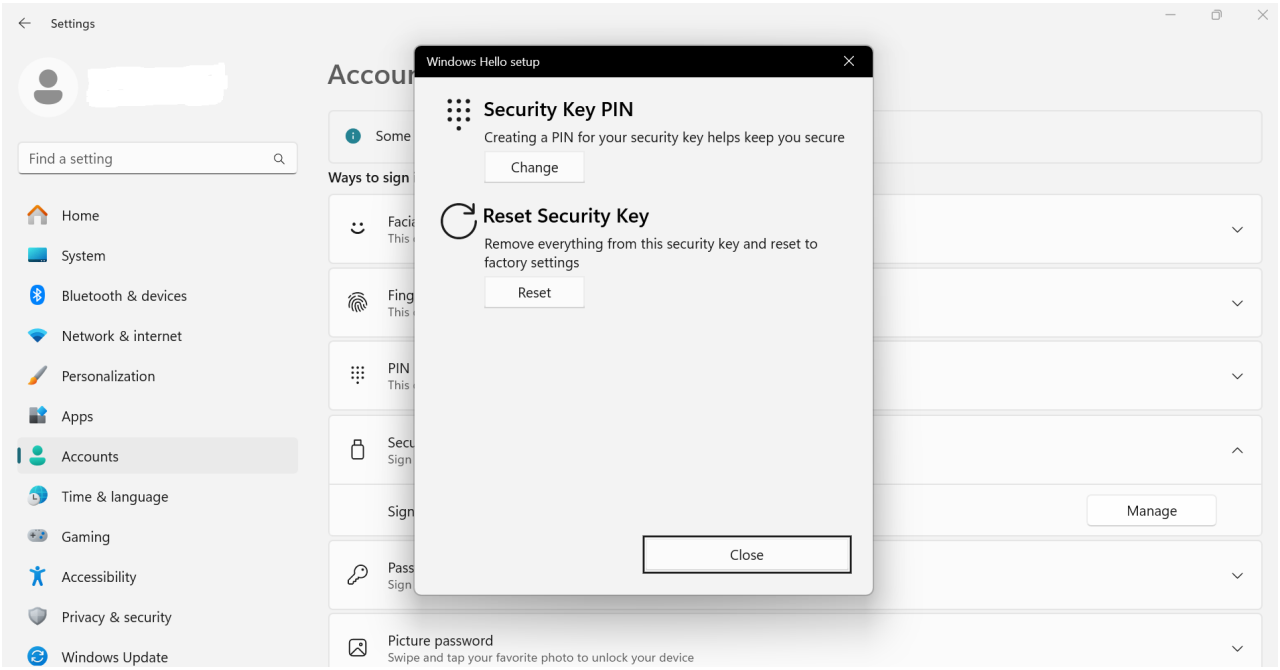
Currently, end users are not able to provision their passkeys by themselves. It must be done by an FIC admin. To register their SmartPhones, end users must bring their phones to their FIC admin who can scan the QR code generated to their phones.

Registering FortiToken 410 USB key in Windows devices

Before registering a USB key, a PIN has to be set up for the key first. The following are the sample steps to set up the PIN for a FortiToken 410 key in Windows 11 machine.

In the use case above, Bob , the FIC admin, needs to set a PIN for the FortiToken 410 USB key to be used by John, using the following steps:

1. After inserting the FortiToken 410 key in a USB slot in the Windows machine, search for *Setup Security Key* in the Windows taskbar search. Then choose *Security Key > Sign in to apps with Security key > Manage*.

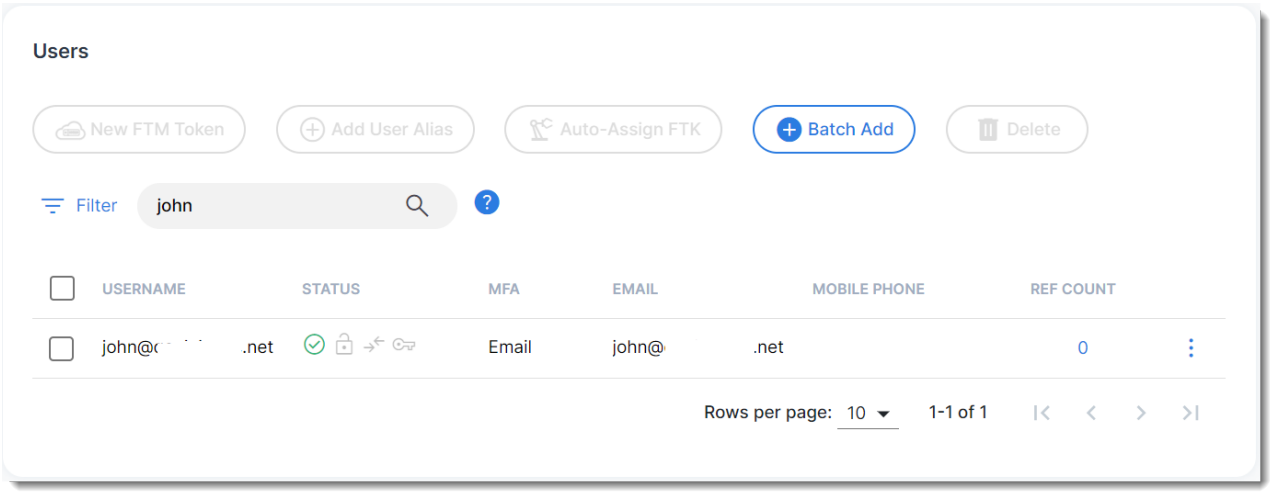


2. Choose *Security Key PIN* and set up a PIN for the key.

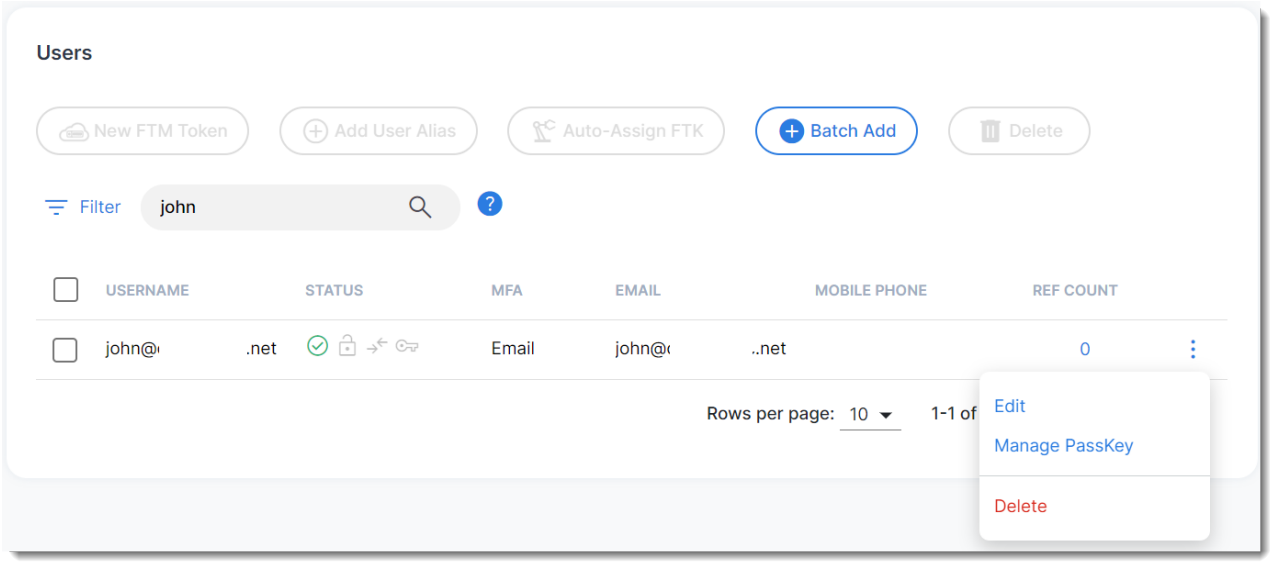
Registering a USB passkey for an end user

To add a FortiToken 410 USB key as passkey for John, Bob must do the following:

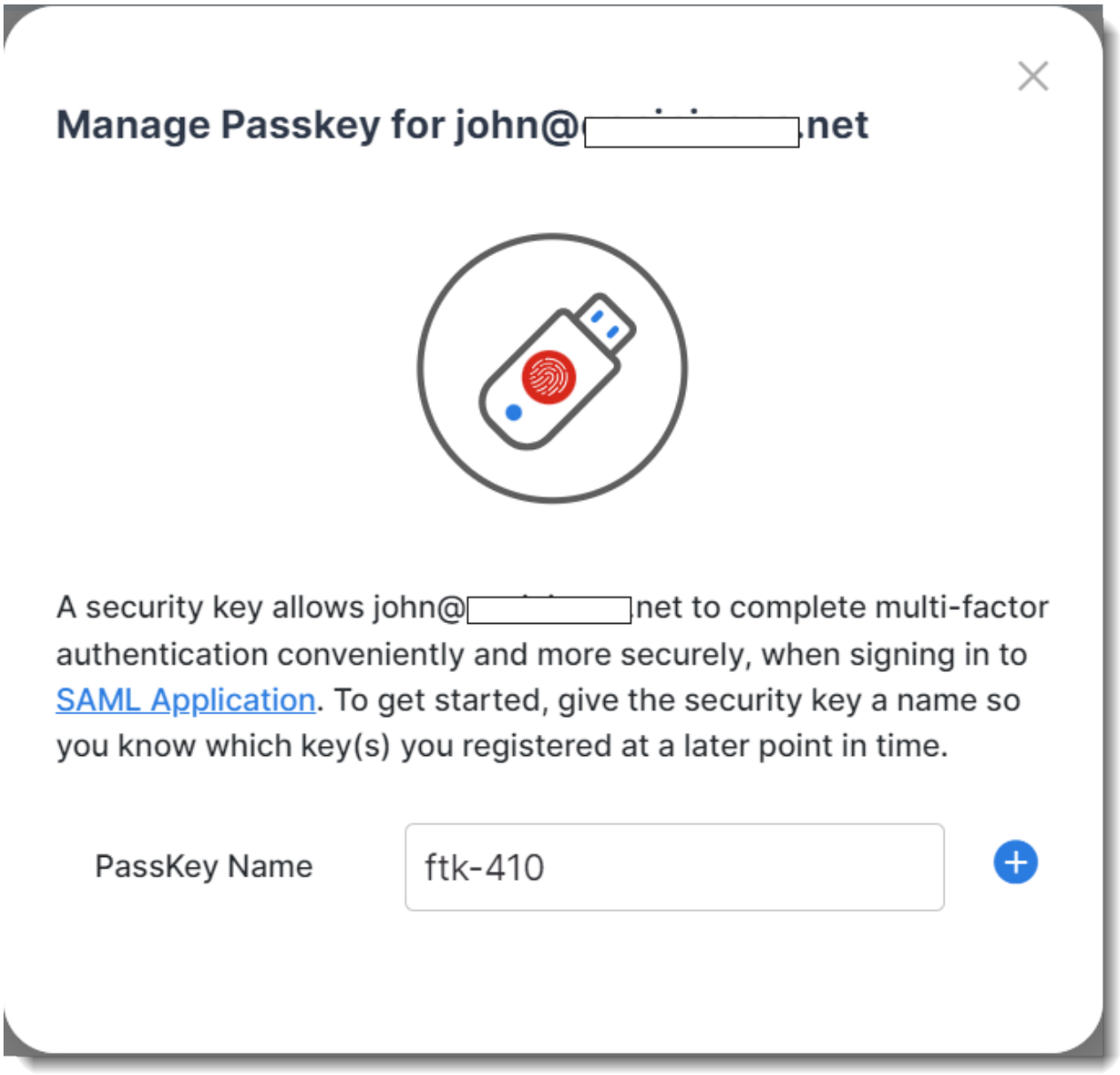
1. Click *User Management* > *Users*, and search for John (end user) in this example.



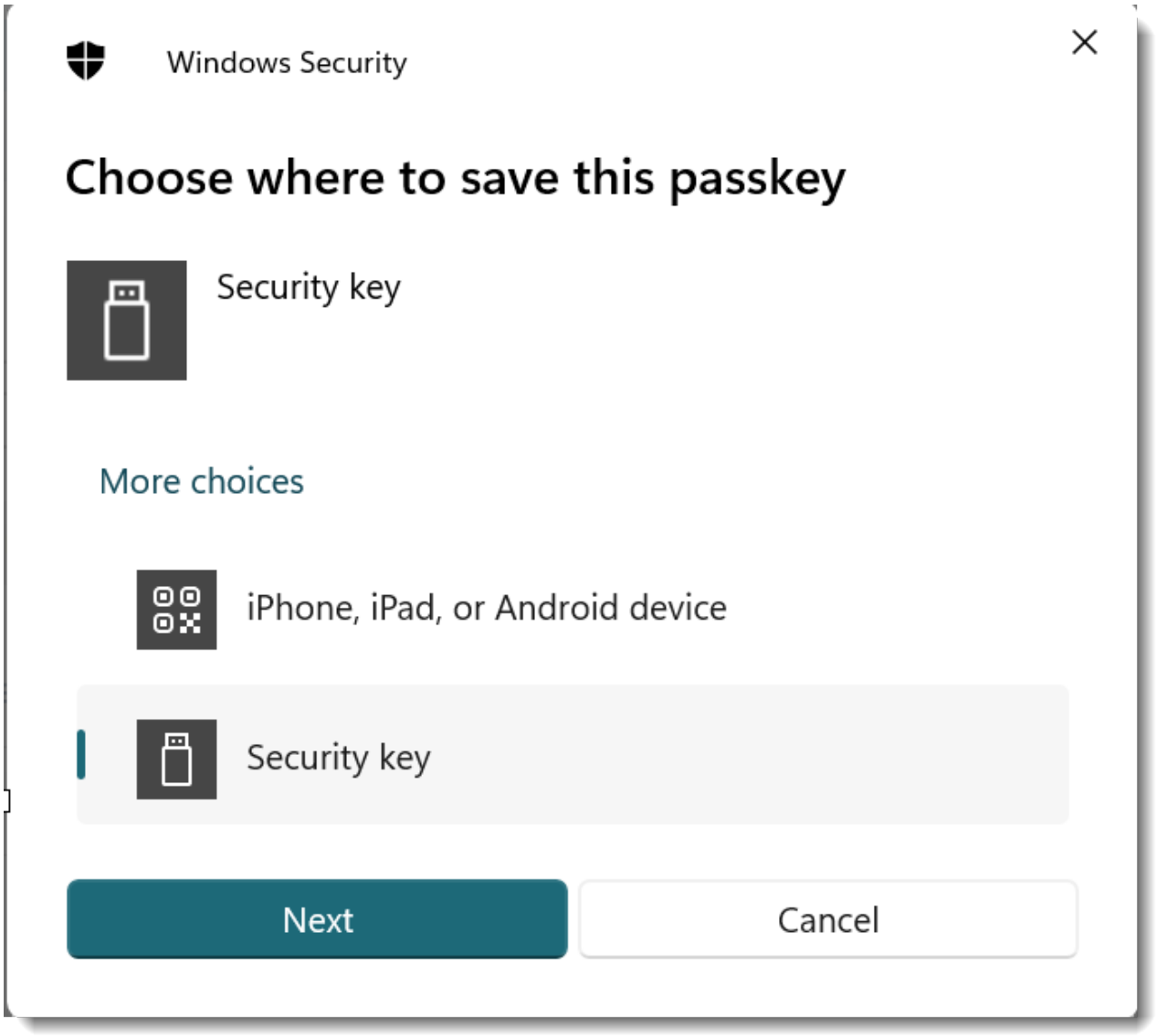
2. Click the tool icon, and select *Manage Passkey*.



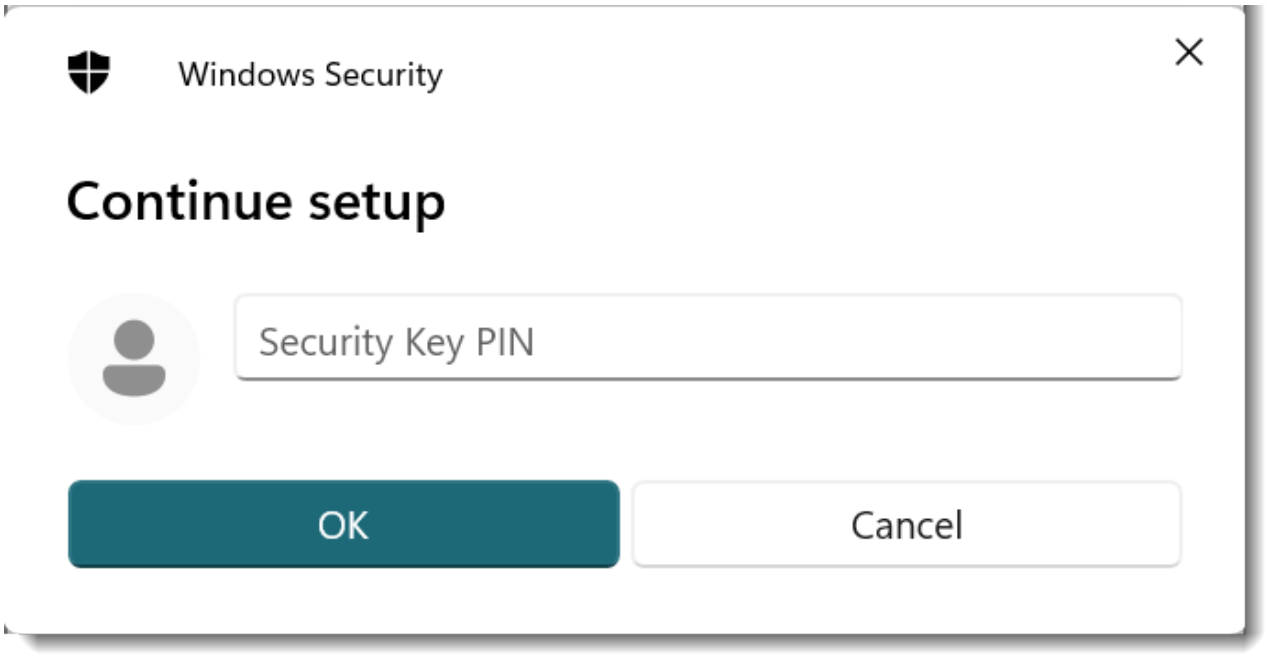
3. Provide a name for the passkey (e.g., ftk-410 in the example shown in the following screen shot).



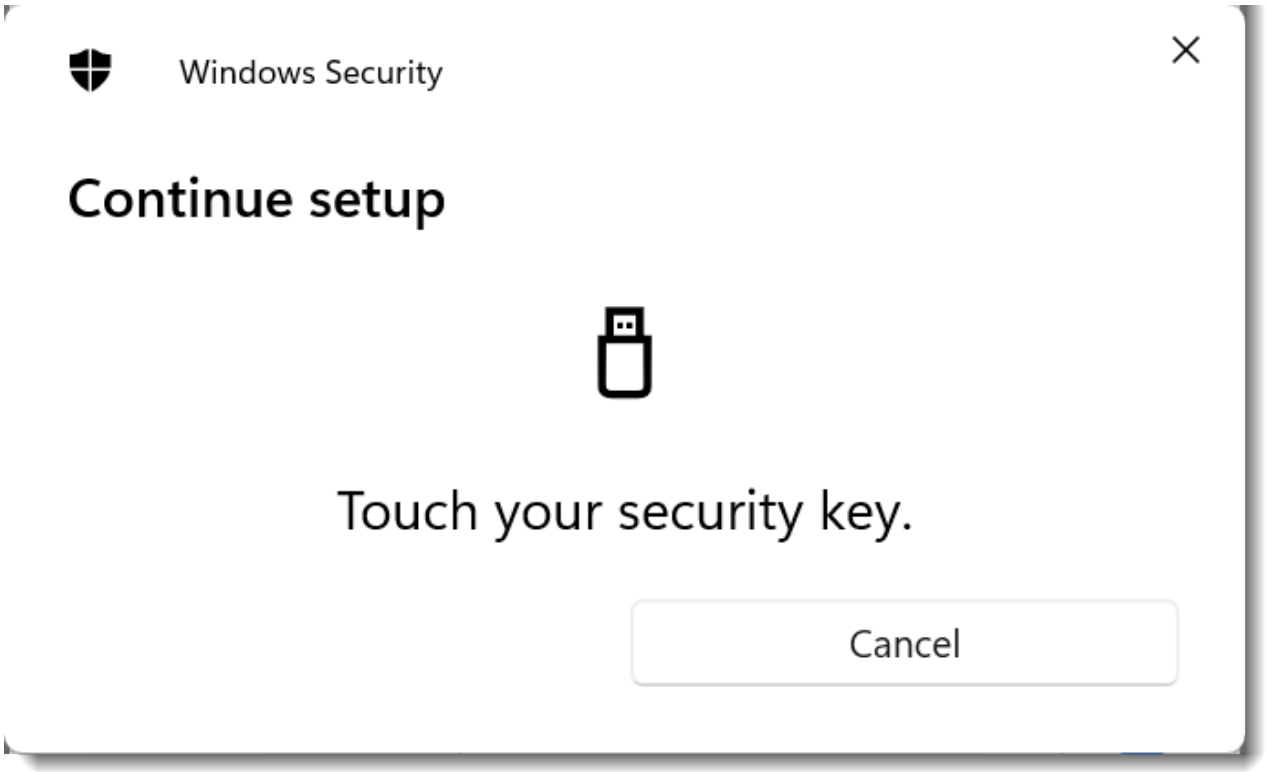
4. Choose *Security Key* in the Wprompt,



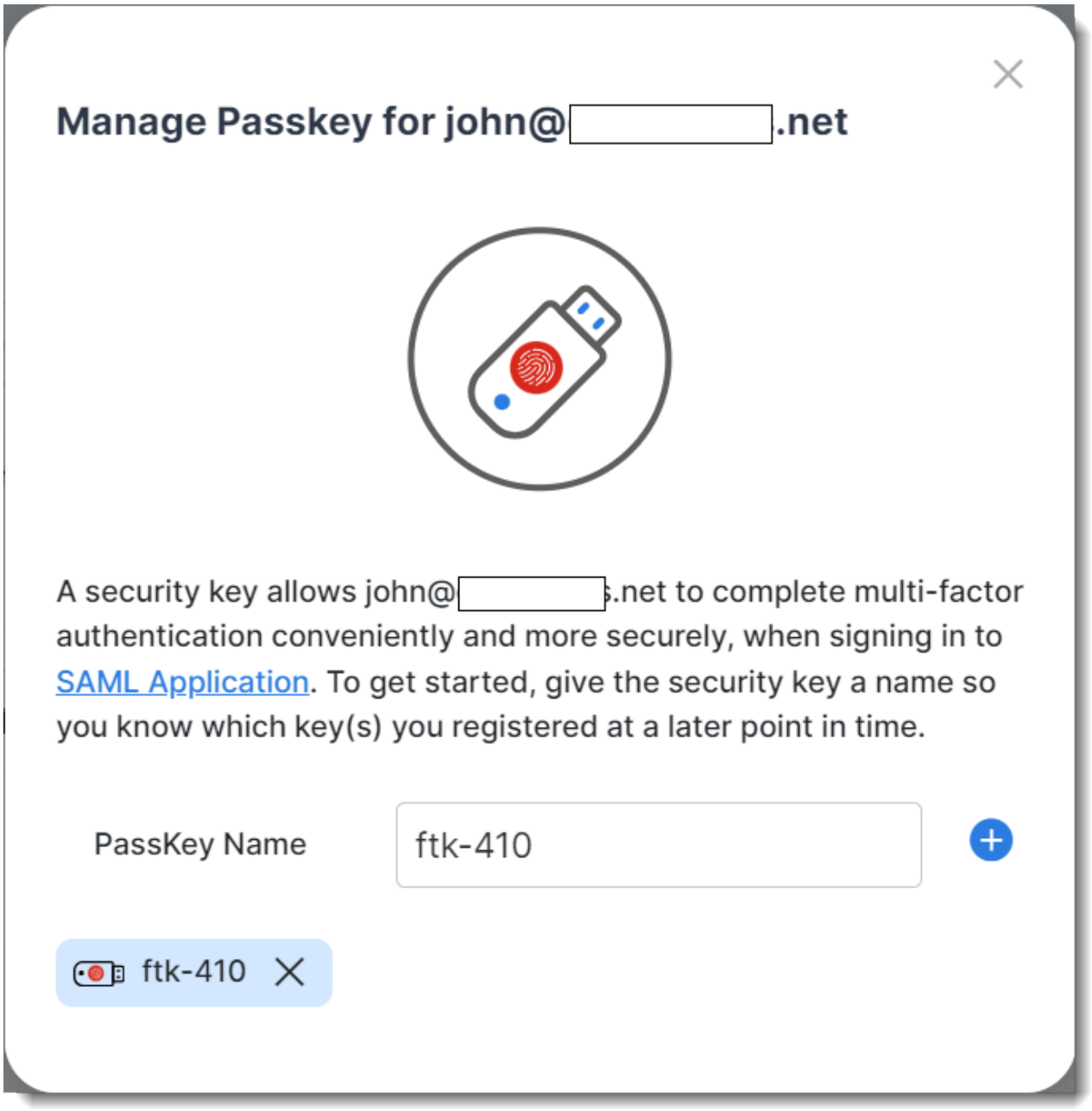
5. Provide the PIN for the FortiToken 410 configured in the section *Register FortiToken 410 USB key in Windows devices* (at the beginning of this section).



6. Once the PIN is authenticated, the system will prompt Bob to press the security key.

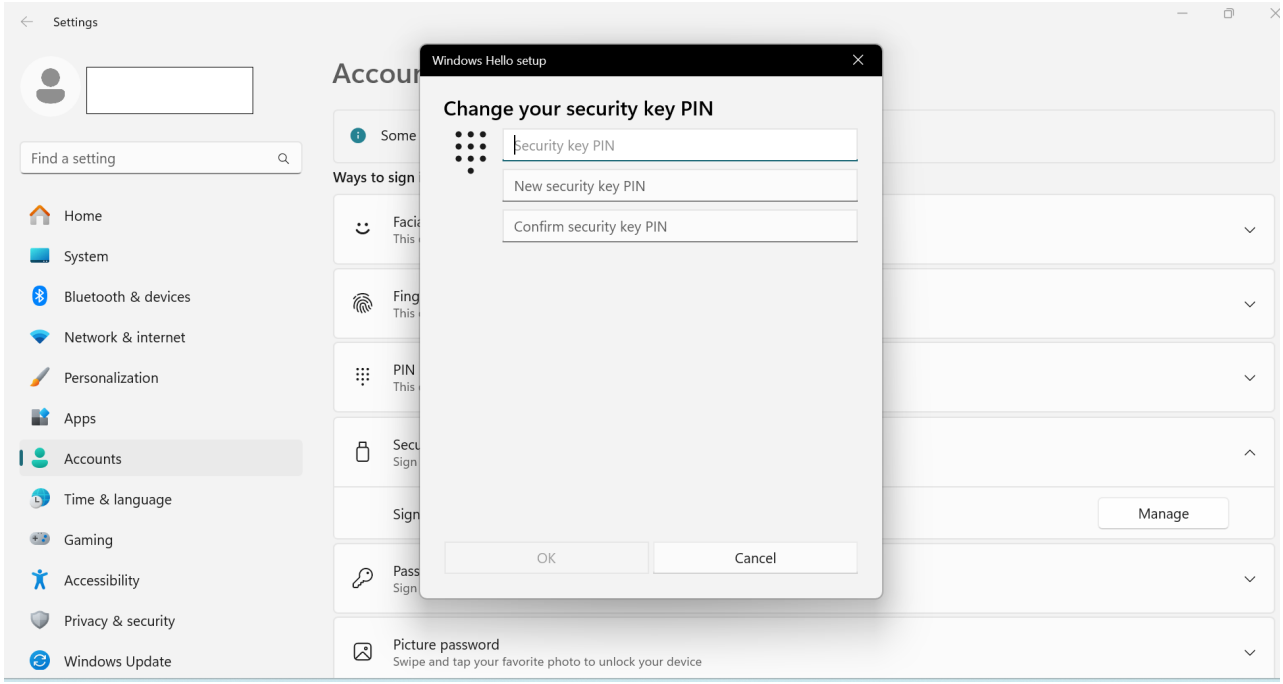


7. Once the key is successfully registered, the key appears on the screen, as illustrated in the following image.

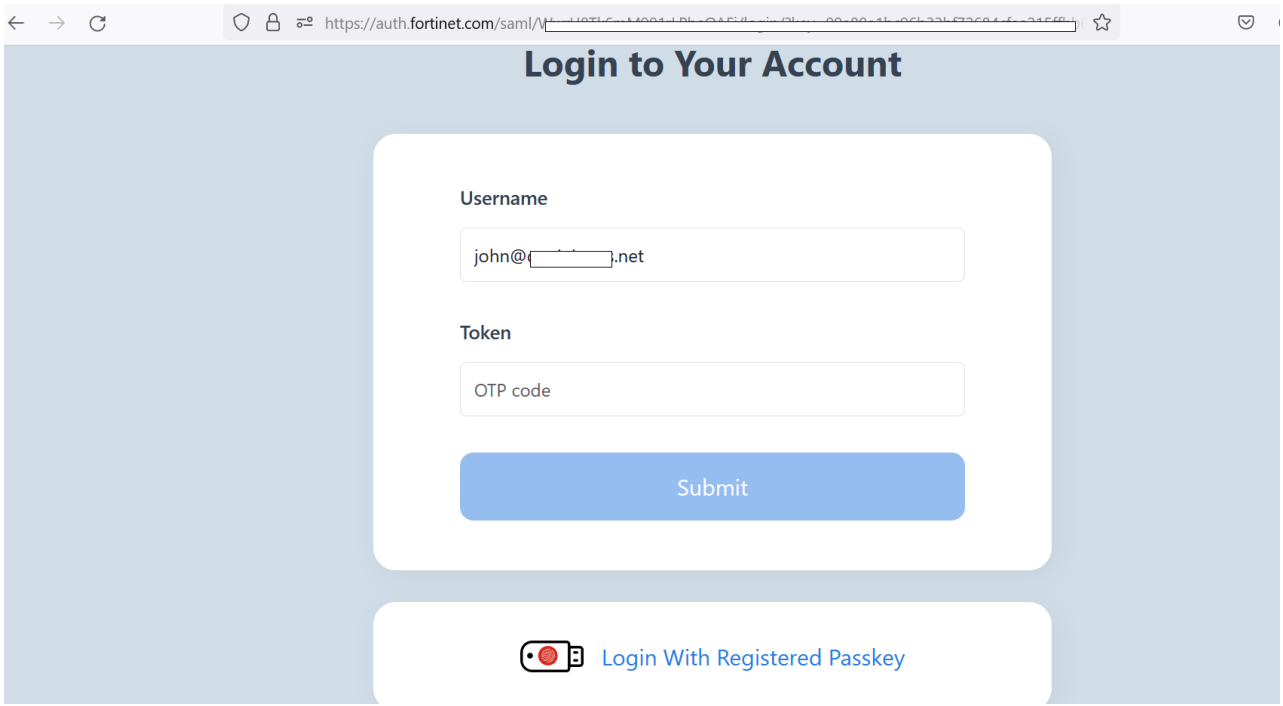


Authenticating with the USB passkey in IdP proxy

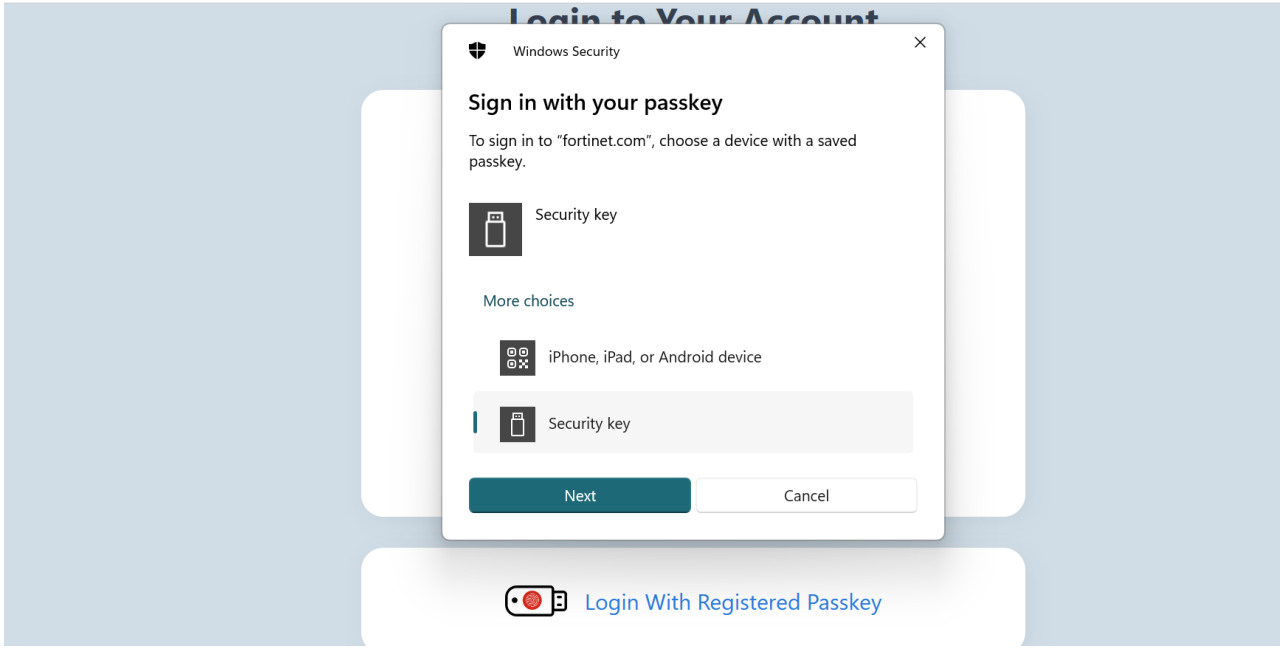
1. Before trying to authenticate with any SP, John will first change the PIN shared by Bob for the FortiToken 410 key. After inserting the FortiToken 410 key in a USB slot in the machine, John must search for *Setup Security Key* in the Windows taskbar search, choose *Security Key > Sign in to apps with Security key > Manage*, provide the existing PIN that Bob has shared, and then update the PIN.



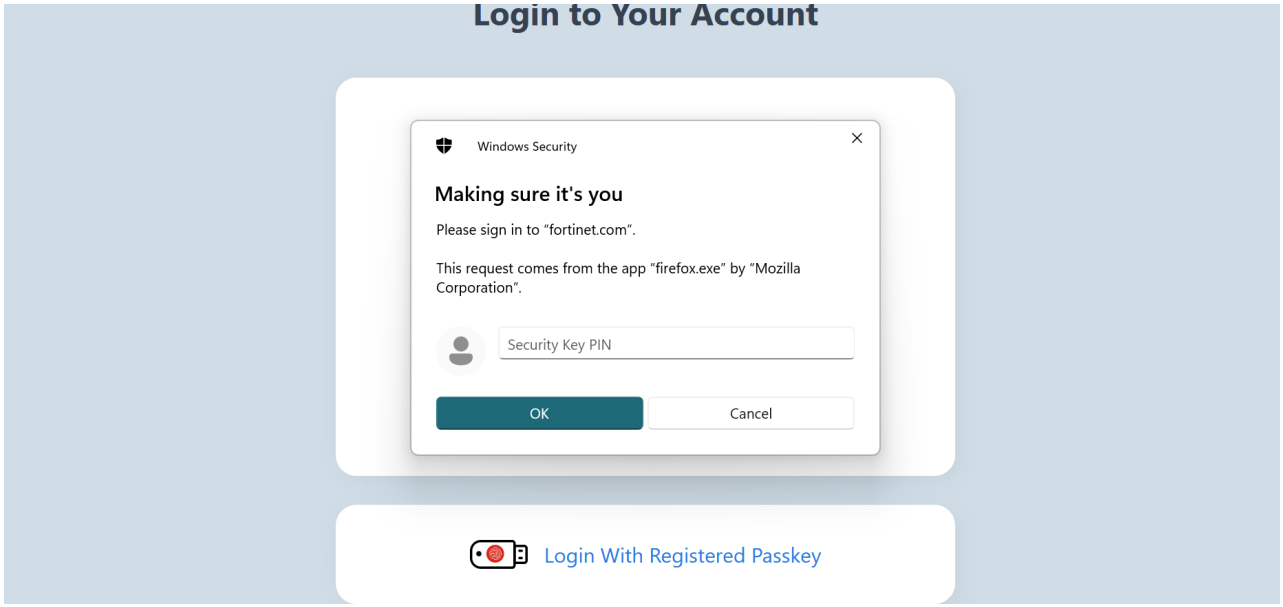
2. After successfully changing the PIN, John opens any SP configured with FIC's IDP proxy.
3. After successful authentication with the external identity provider to access a service provider, John is presented with the auth.fortinet.com page from FIC for MFA. John then needs to choose *Login with Registered Passkey*.



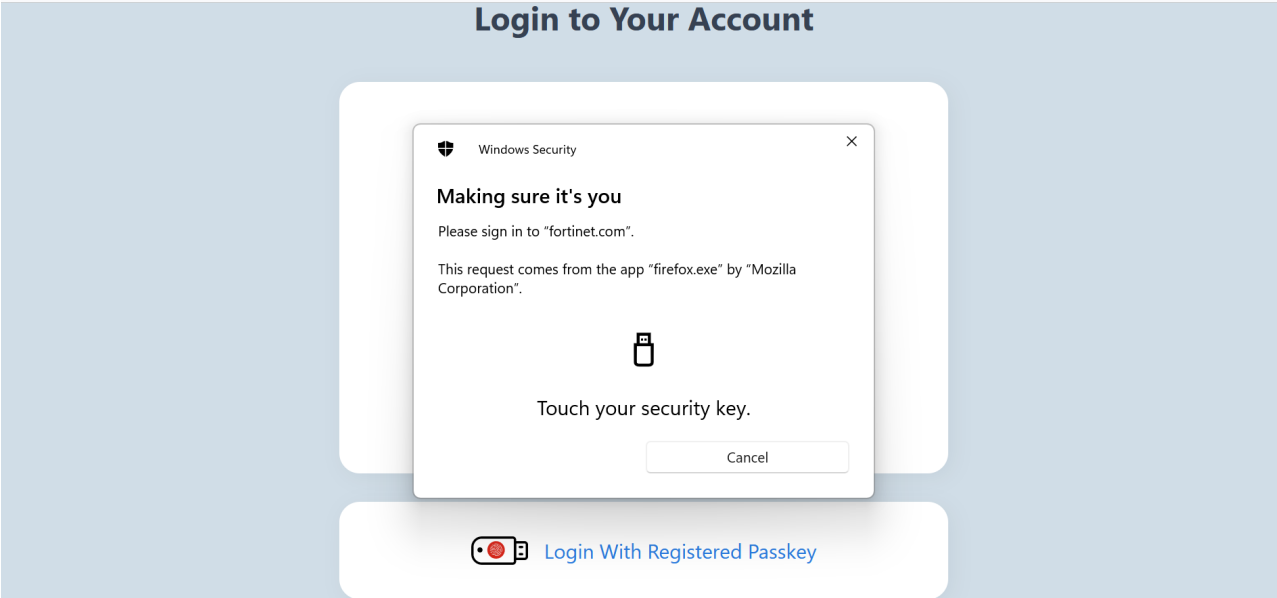
4. John chooses *Security key* to use the FortiToken 410 USB passkey.



5. John provides the PIN for the FortiToken 410 passkey.



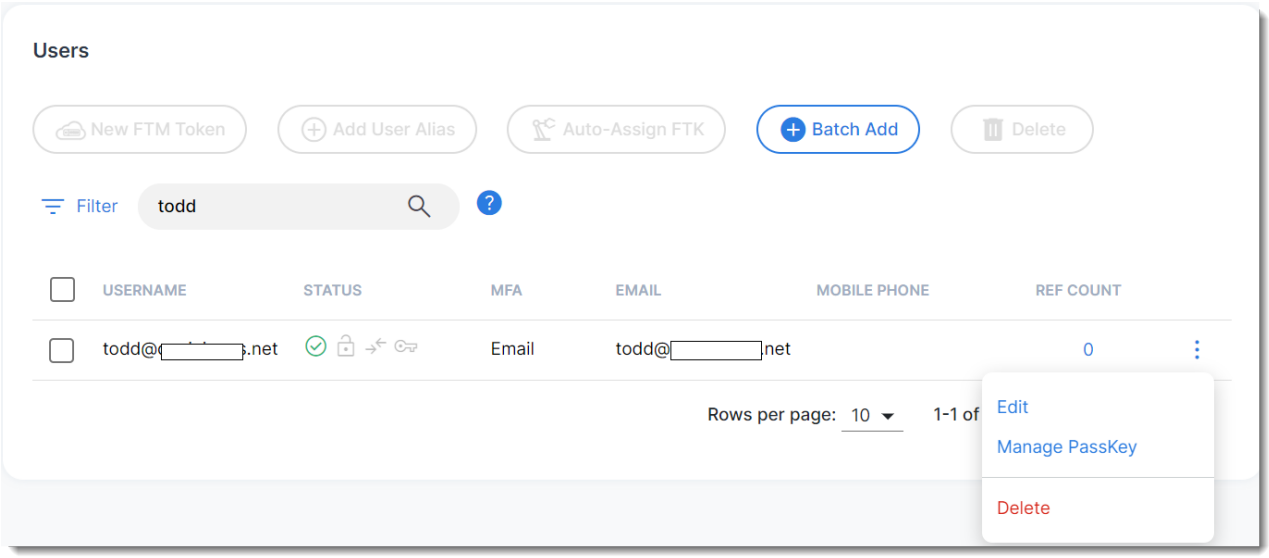
6. After the PIN is validated, John must follow the instructions and touch the FortiToken 410 passkey.



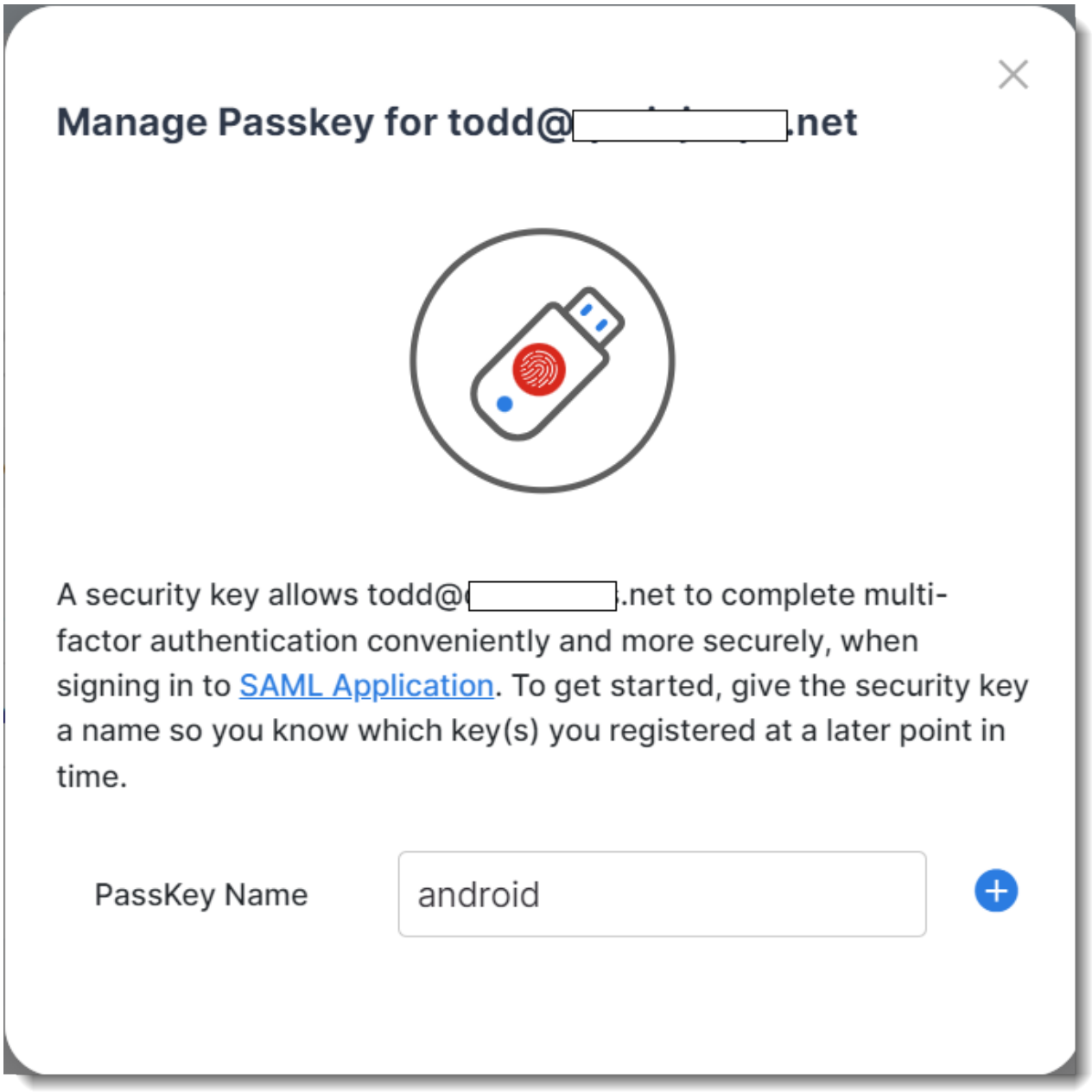
Registering phone passkeys for an end user

For a phone to be added as passkey for Todd (end user), Bob must do the following:

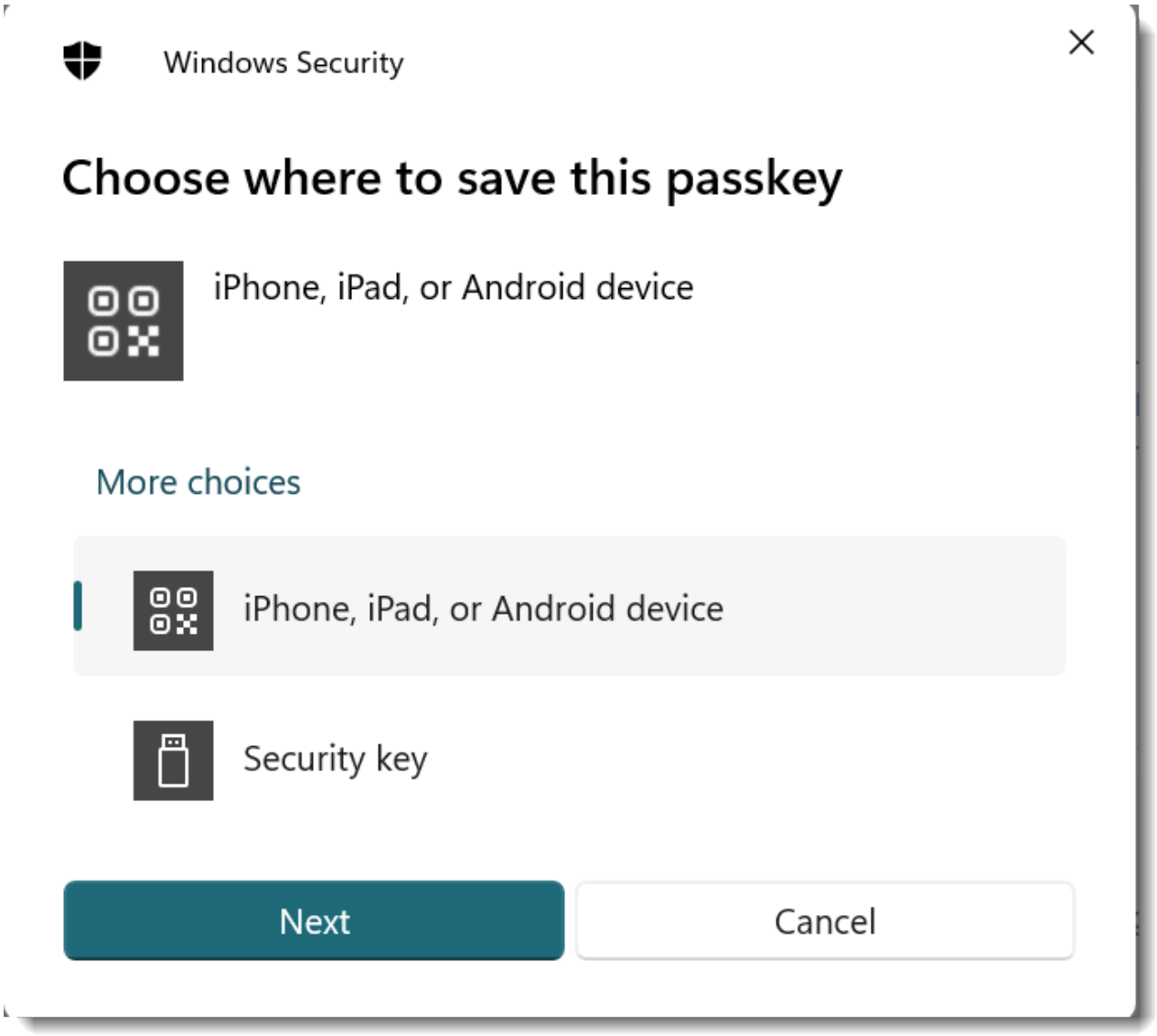
1. Click *User Management* > *Users*, search for the user, "Todd", in the following example, and choose *Manage Passkey* from the tool menu.



2. Provide a name for the passkey, 'android' in the following screenshot.



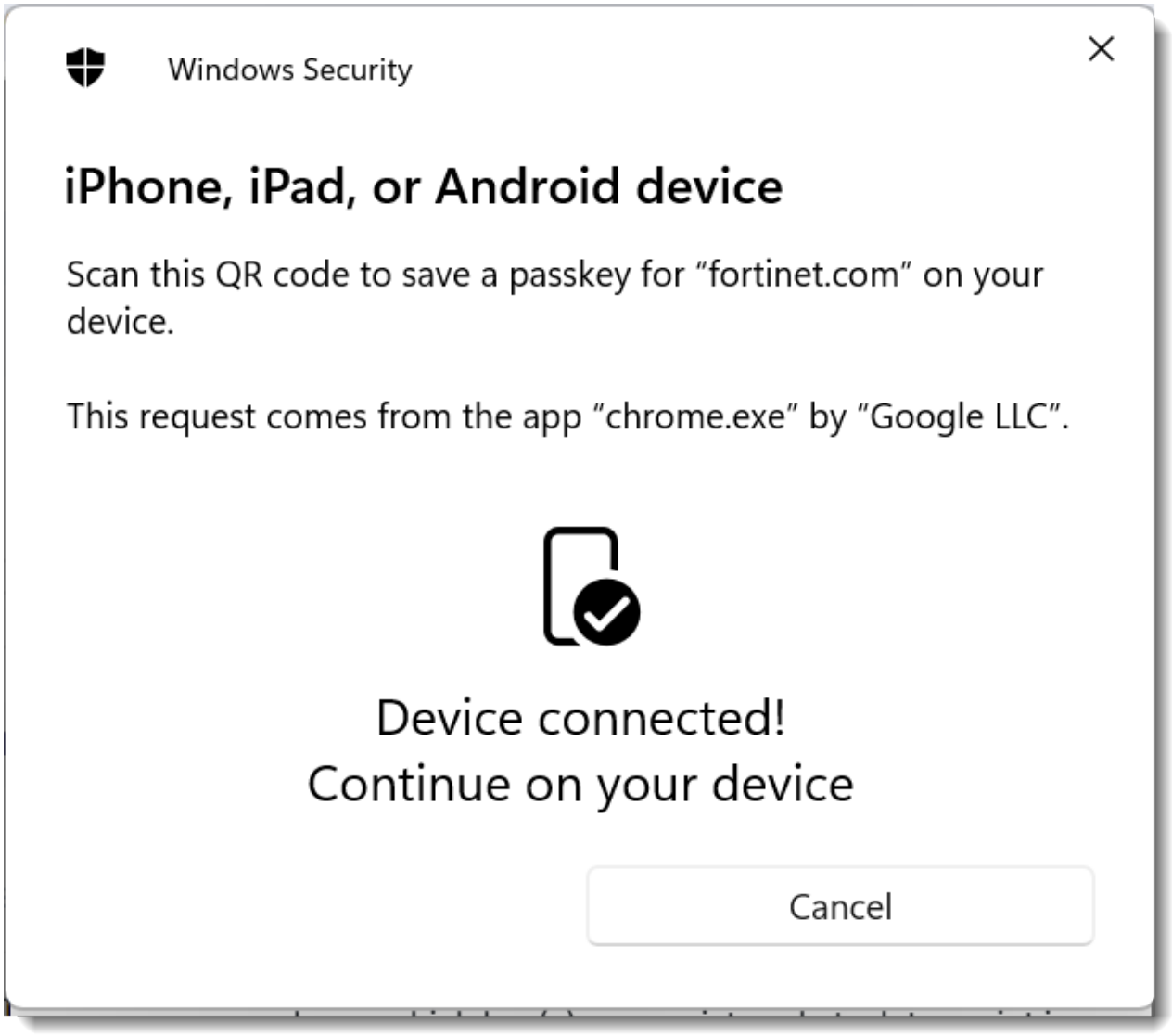
3. Select *iPhone, iPad, or Android device* from the prompt.



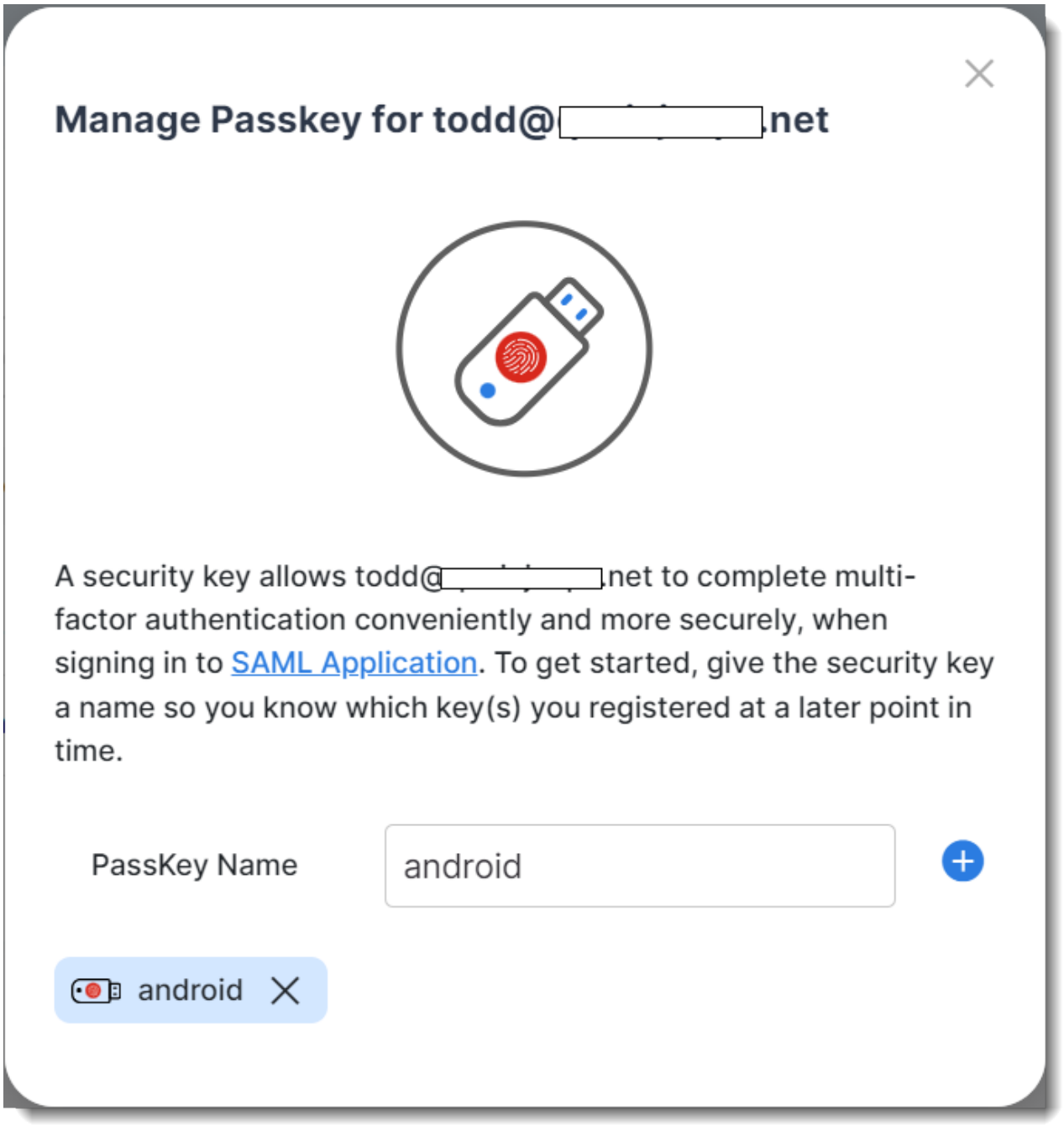
4. Ensure Bluetooth is enabled in both his computer and the phone and scan the QR code. In this case , Todd's phone will be used to scan the QR code.

5. The phone will automatically prompt to provide the screen lock or other protection mechanism configured in the phone. Follow the instructions on the phone to add the passkey.

6. Once the passkey is successfully added, the following confirmation will appear on the FIC portal screen to admin Bob.

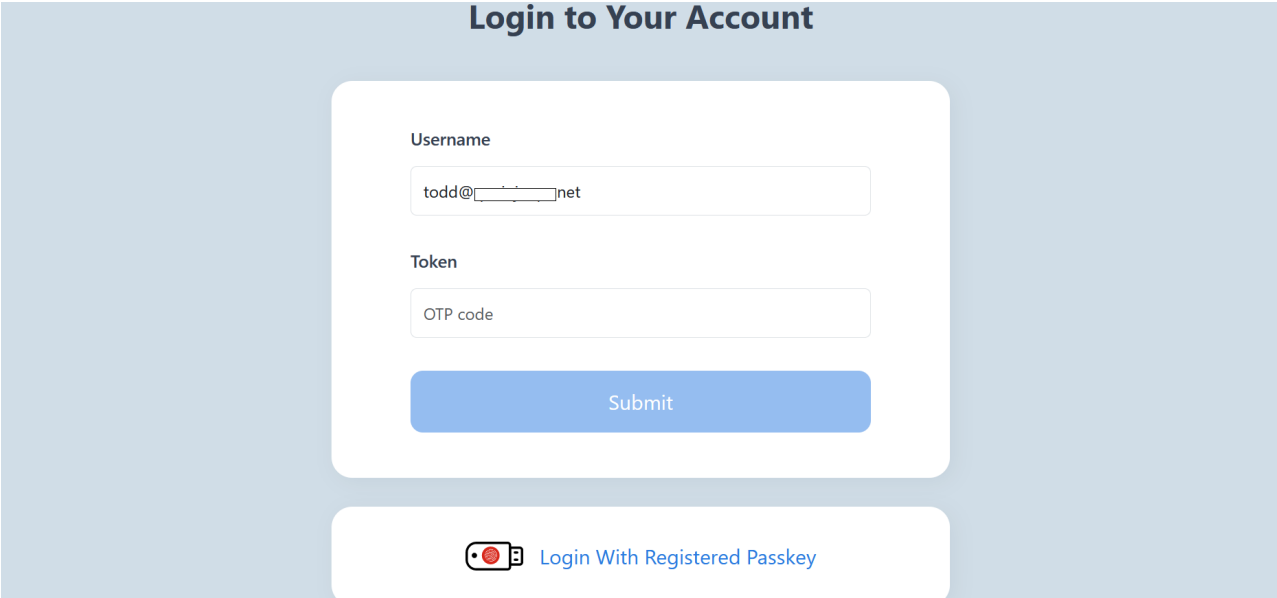


7. Once the phone is successfully added, Bob will see the following confirmation on the FIC portal.



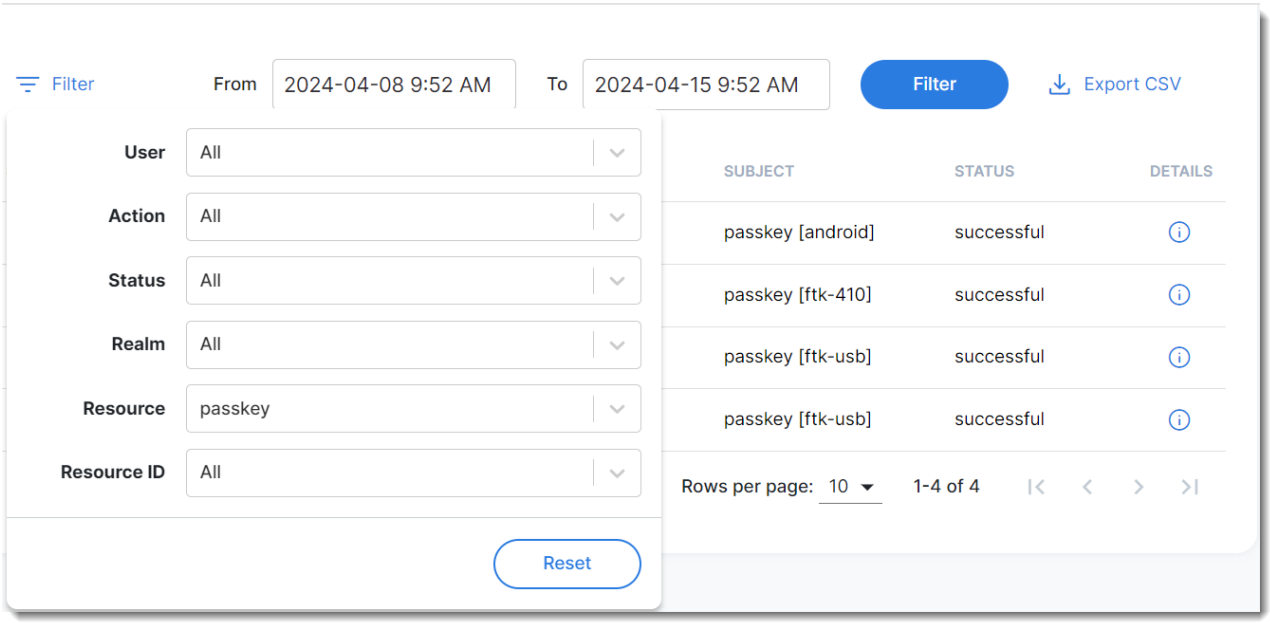
Authenticating with a phone passkey in IdP proxy

1. After successful authentication with the external identity provider in his computer for a configured service provider, the user (Todd in this case) will be presented with the auth.fortinet.com page from FIC for MFA. Choose *Login with Registered Passkey*.

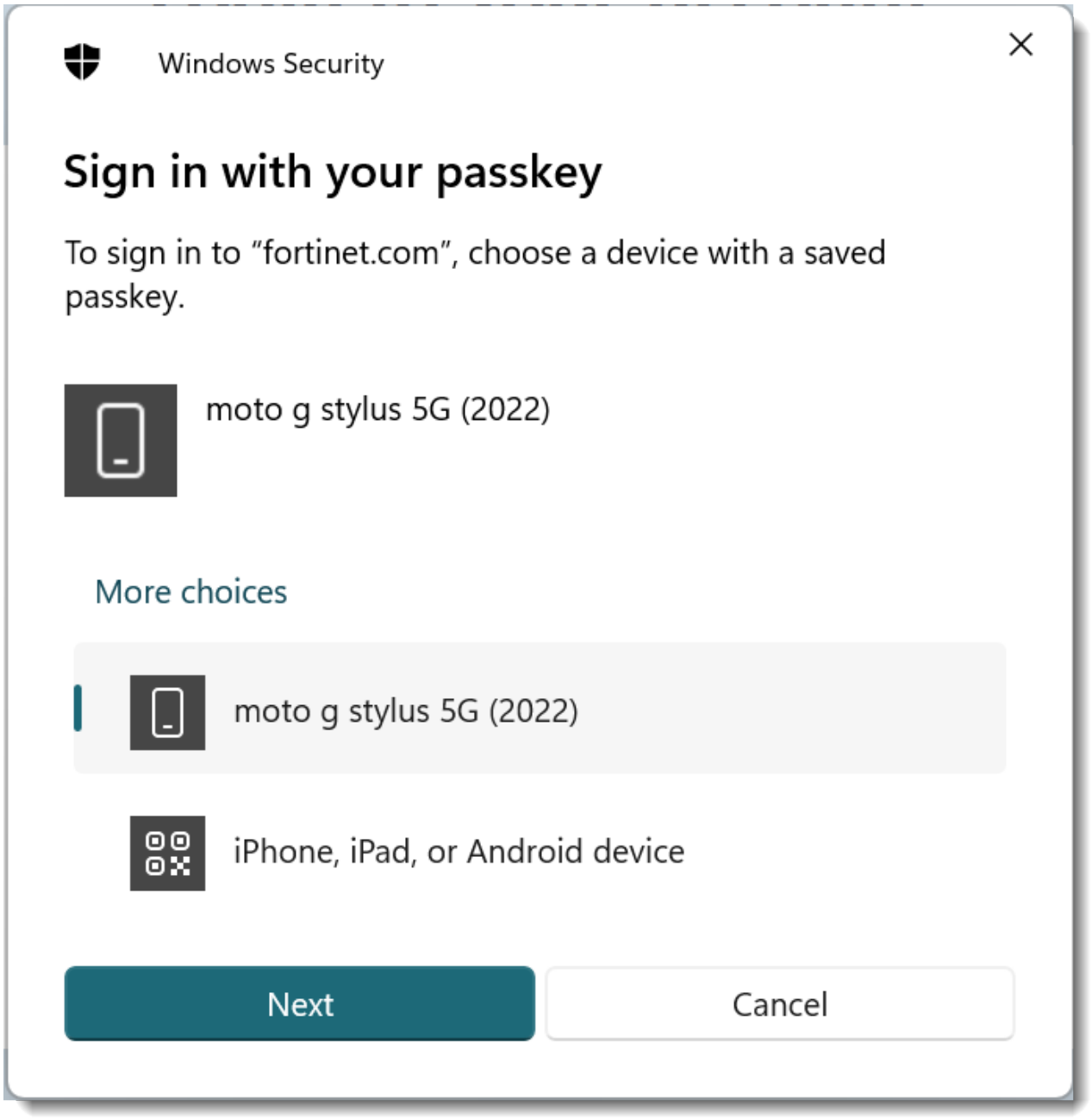


2. As the phone is used for the first time after provisioning, a QR code will pop up. Todd will scan the QR code.

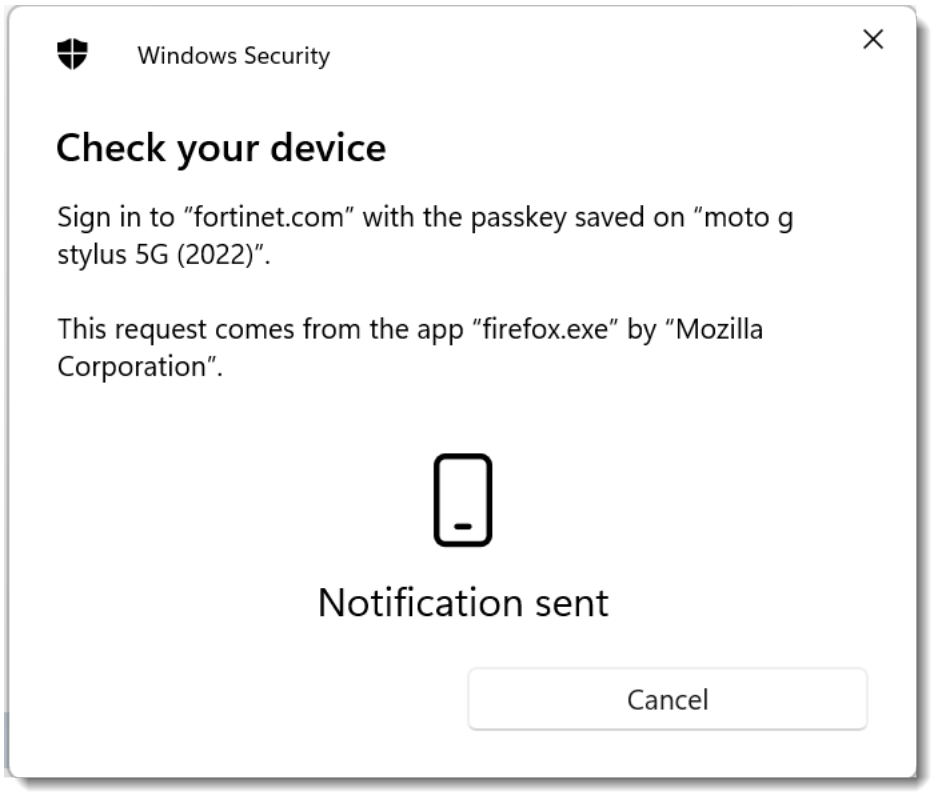
3. Follow the instruction on the phone to provide the screen lock or other authentication mechanisms in the phone.



4. After the phone is set up successfully, Todd will be able to log into the service provider.
5. Now that the Android phone is registered with Todd's computer, when Todd tries to log in the next time, his phone will be listed as one of the choices *(moto gstylus 5G (2022)* in the following screenshot).



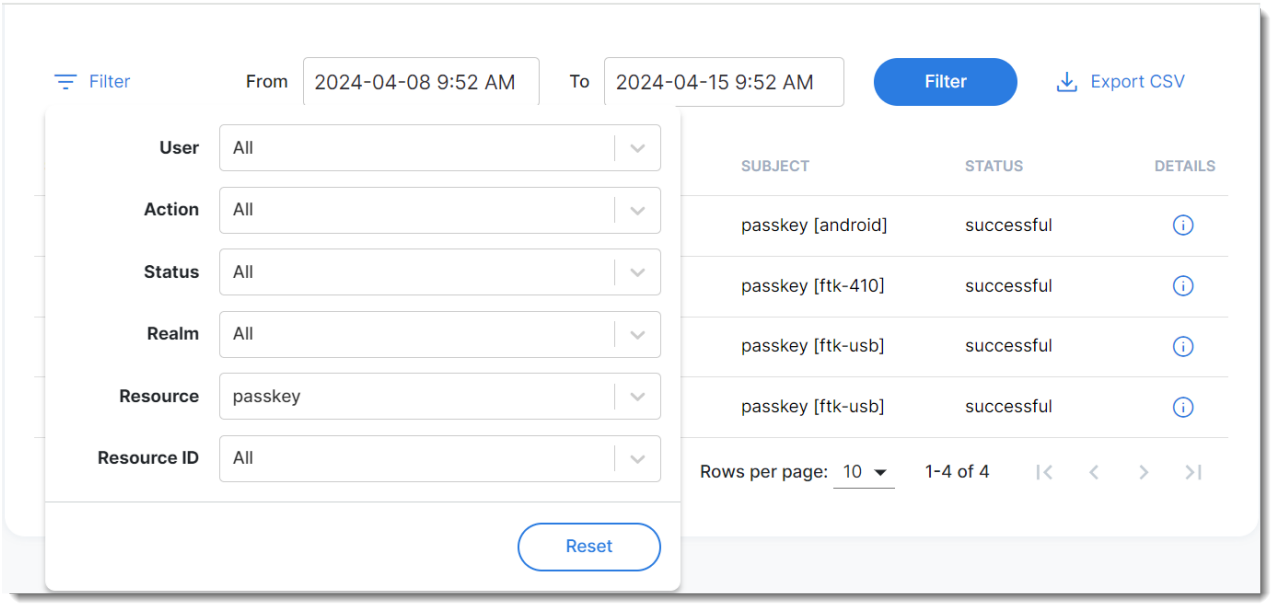
6. Clicking on the phone will send a notification to the phone and the user will then have to provide the screen lock or other authentication mechanisms configured in the phone to authenticate.


Windows Security
Check your device
Sign in to "fortinet.com" with the passkey saved on "moto g stylus 5G (2022)".
This request comes from the app "firefox.exe" by "Mozilla Corporation".
Notification sent
Cancel

Viewing logs for passkeys

Management log:

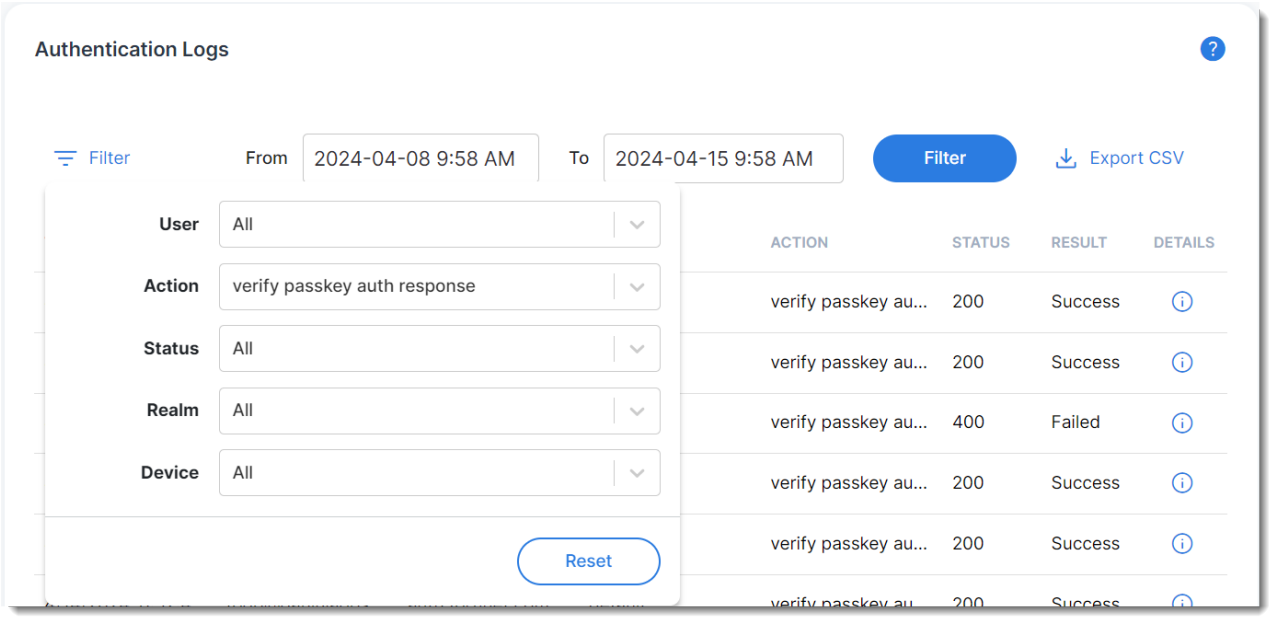
1. Navigate to *Logs and Reports* > *Management Logs*, click Filter, and select *Passkey* in the *Resource* field.



2. Click the *Details* icon to view log details.

Authentication log:

1. Navigate to *Logs and Reports >Management Logs*, click *Filter*, and select *verify passkey auth response* in the *Action* column to narrow down the search to passkey auth responses.



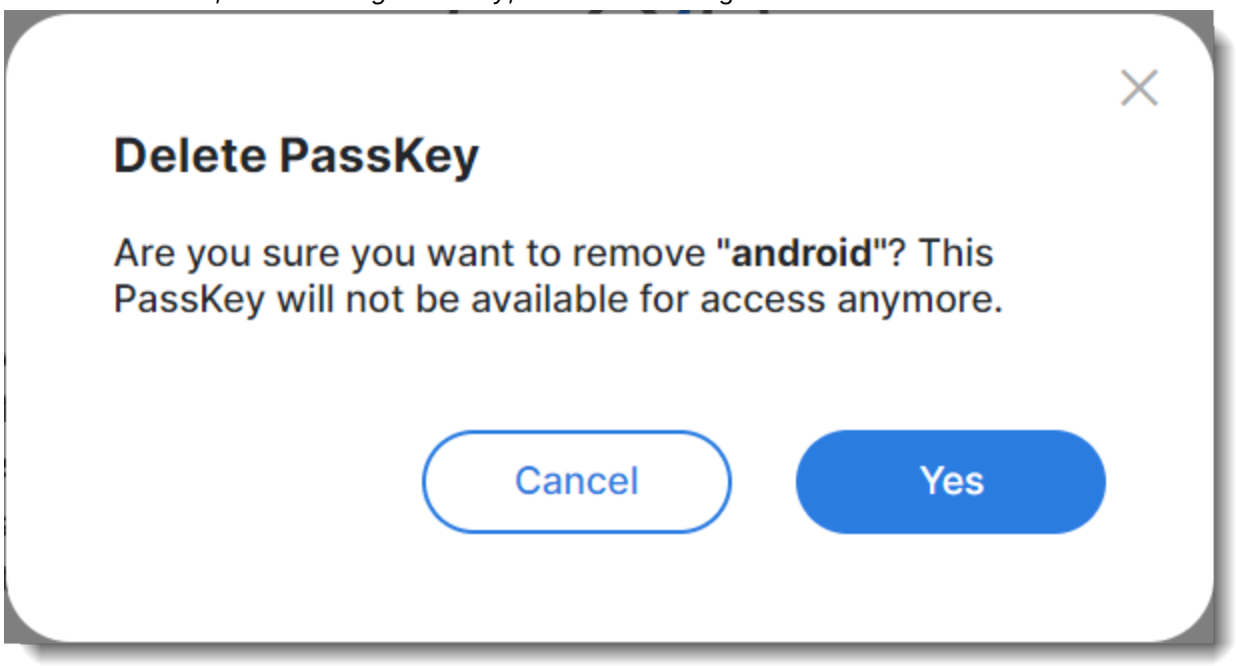
2. Click the *Details* icon to view log details.

Deleting a passkey

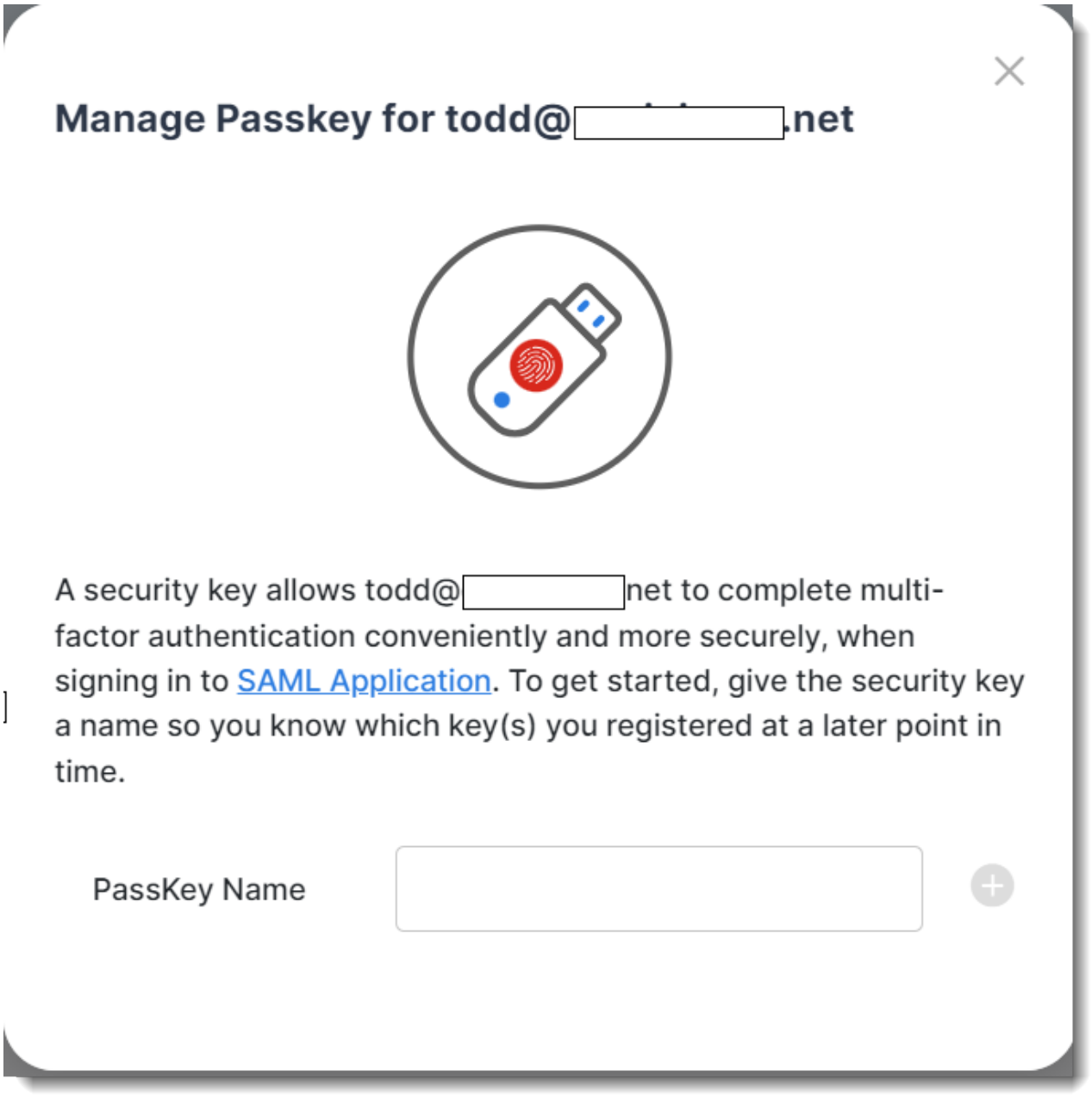
There are two ways to delete passkeys.

User Management menu:

1. Navigate to *User Management* >*Users*, and locate the user,
2. Click the tool icon, select *Manage Passkey*, and click the X sign.

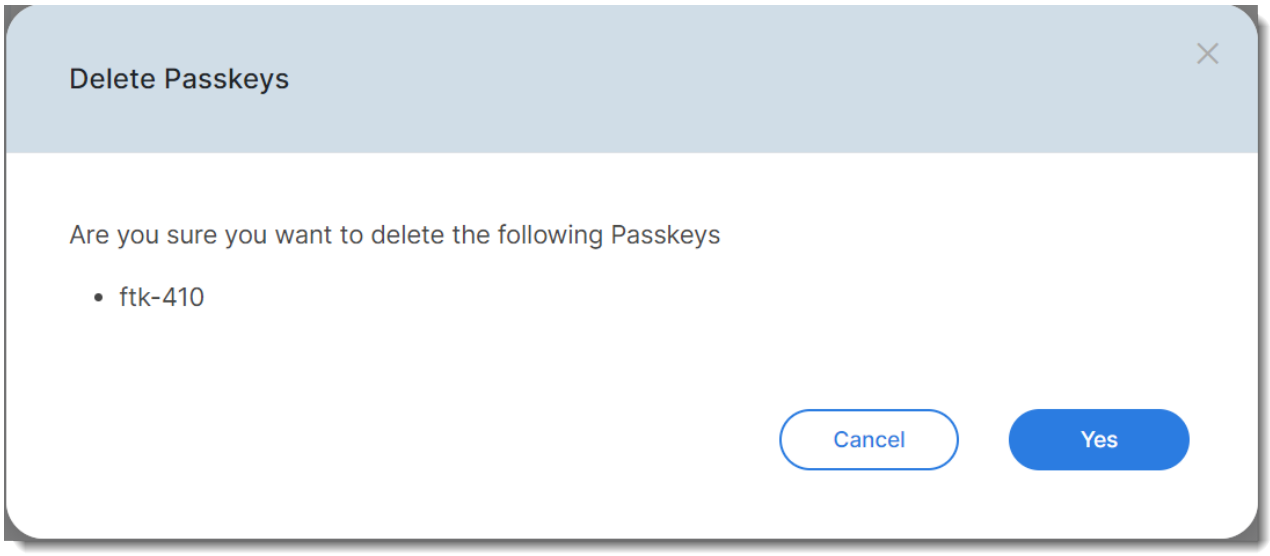


3. Click *Yes*.



Security Devices menu:

1. Navigate to *Security Devices* > *Passkey*, select the passkey, and click *Delete*.
2. Click *Yes*.


Delete Passkeys
Are you sure you want to delete the following Passkeys
ftk-410
Cancel
Yes

Logs

Logs capture operational and administrative events that happened on FIC. Events can be performed by an FGT VDOM admin user or FIC itself.

FIC has two types of logs:

Usage data

The usage graph shows the number of user quota/SMS credits consumed. If you want to view usage by user only, click SMS to turn SMS usage data off, and vice verse.

1. Click *Logs and Reports* > *Usage*.
2. Click the *Realm*s drop-down, and select a realm of interest.
3. On top of the page, select *Daily*, *Monthly, or Current,*
4. Click in the *From* box, and set the start date or month of the year.
5. Click in the *To* box, and set the end date or month of the year.
6. Click *Filter*.
7. If you've select *Daily* (in Step 2 above), click the *Usage Type* drop-down menu and select one of the viewing options.
8. Click the legend at the bottom of the usage chart to show or hide usage data of your choice.
9. Mouse over a bar to view the total number of user quota/SMS credits for the given time period.
10. While in *Daily* view, click *View Usage Details* to view detailed daily usage data, or click *Export CSV* to export the usage data in a .csv file.

Authentication logs

Authentication logs capture authentication attempts that your FIC end-users have made.

Viewing authentication logs

1. Click *Logs and Reports >Authentication Logs*.
2. Click *Filters*.
3. Select the filter(s).
4. Click *OK*.

Each authentication log captures the following data:

Column	Description
TIMESTAMP	The date and time of an authentication request. **Note:** FIC captures the time of an event in UTC time, and then converts it to the client browser's local time zone, which is the time shown in the timestamp.
USERNAME	The username of the user who made the request.
APPLICATION	Shows either of the following: • The serial number and VDOM name if the application is an FGT device. • The source IP address if the application is a third-party device.
REALM	The realm ID of the realm from which the authentication request is attempted.
ACTION	The authentication action.
STATUS	The status of the authentication request expressed in standard HTTP status codes. See List of HTTP Status Codes.
RESULTS	The outcome of an authentication request, which can be either of the following: • *Success* • *Failed*
DETAILS	View log details.

Filtering logs by date and time

This option enables you to display logs for the period of time you specify.

1. In the upper-left corner of the page, choose the start date and time and the end date and time.
2. Click *Filter*.

Filtering logs by user

This option enables you to filter the logs by username.

1. In the upper-left corner of the page, below the *Start date* and *End date* filter, click *user*.
2. From the drop-down menu, select a username.

Filtering logs by status

This option allows you to filter logs by HTML status code.

1. In the upper-left corner of the page, below the *Start date* and *End date* filter, click *status*.
2. From the drop-down menu, select an HTML status code.

Sorting the log table

You can sort the entries in the log table by clicking any of the column headers, namely:

- *Timestamp*
- *Username*
- *applications*
- *Results*

Management logs

Management logs show management activities that have occurred in your account.

Viewing management logs

1. Click *Logs and Report* > *Management Logs*.
2. Click *Filters*.
3. Select the filter(s).
4. Click *OK*.

A management log entry contains the following data:

Column	Description
SOURCE	The source of the request, which can be either of the following: • *application* • *FIC portal*
TIMESTAMP	The date and time of the request. **Note:** FIC captures the time of an event in UTC time, and then converts it to the client browser's local time zone, which is the time shown in the timestamp.
AMINISTRATOR	The authorized entity that made the request, which can be either of the following: • The serial number of FGT if the request was made from FGT. • The username of the FIC user if the request was made from the FIC

Column	Description
	portal.
ACTION	The type of action.
RESOURCE	The t of an action. For example, who or what is changed? **Note:** If the subject is an end user, it includes the account to which the user belongs.
STATUS	The status of a management event.
REALM	The realm involved in the event.
DETAILS	View log details.

Filtering logs by date and time

This option enables you to display logs for the period of time you specify.

1. In the upper-left corner of the page, choose the start date and time and the end date and time.
2. Click *Filter*.

Filtering logs by user

This option enables you to filter the logs by username (email address).

1. In the upper-left corner of the page, below the *Start date* and *End date* filter, click *User*.
2. From the drop-down menu, select a username.

Filtering logs by action

This option allows you to filter logs by action.

1. In the upper-left corner of the page, below the *Start date* and *End date* filter, click *Action*.
2. From the drop-down menu, select an action.

Filtering logs by status

This option allows you to filter logs by status.

1. In the upper-left corner of the page, below the *Start date* and *End date* filter, click *Status*.
2. From the drop-down menu, select a status.

Filtering logs by realm

This option allows you to filter logs by realm ID.

1. In the upper-left corner of the page, below the *Start date* and *End date* filter, click *Realm*.
2. From the drop-down menu, select a realm ID.

Filtering logs by subject

This option allows you to filter logs by subject.

1. In the upper-left corner of the page, below the *Start date* and *End date* filter, click *Subject*.
2. From the drop-down menu, select a subject.

Filtering logs by subject ID

his option allows you to filter logs by subject ID.

1. In the upper-left corner of the page, below the *Start date* and *End date* filter, click *Subject ID*.
2. From the drop-down menu, select a subject ID.

Sorting the log table

You can sort the log entries in the table by clicking any of the column headers, namely:

- *Source*
- *Timestamp*
- *Administrator*
- *Action*
- *Subject*

SMS logs

The SMS logs page shows all logs of your SMS usage. The following table shows the information about log entries.

Viewing SMS logs

1. Click *Logs and Report > SMS Logs*.
2. Click *Filters*.
3. Select the filter(s).
4. Click *OK*.

Parameter	Description
TIMESTAMP	The date and time the log entry was generated. Note: This is the timestamp of the web browser in which FIC is operated.
APPLICATION	The application that sent SMS message.
REALM	The realm to which the application is assigned.
ACTION	The action that FIC took.
USER	The end-user upon whom the action was performed.
COUNTRY	The country or region where the end-user's phone number is registered.
RATE	The wireless phone rate.

Filtering SMS logs

1. In the upper-left corner of the *SMS* page, click the *Filters* icon.
2. Make the desired selections.
3. Click *ok*.

Filtering logs by date

1. Click the *From* field and select a start date.
2. Click the *To* field and select an end date.
3. Click *Filter*.

Exporting SMS logs

1. In the upper-right corner of the SMS page, click the *Export CSV* button.
2. In the Download pop-up, click *Open file*.
3. Save the file on your computer or a location on your network.

Using templates

Fortildentity Cloud (FIC) templates are the message templates that FIC uses to send OTP and token activation or transfer notifications to its end users. FIC can notify its end users of such activities either by email or SMS, depending on your configuration. Not only can you choose from the default templates, but also create templates of your own.

Column	Description
NAME	The name of the template.
METHOD	The way the template is used.
TYPE	The template type.
DEFAULT	Whether the template is a default one.

The default templates are read-only, and cannot be altered.

- Creating a custom template on page 222
- Editing a template on page 223
- Using templates on page 223
- Deleting a template on page 224

Creating a custom template

1. Click *Customization>Templates*.
2. Click *Add Template*.
3. For *Method,* select a notification method.
   Note: Method refers to the means that FIC uses to send OTP and token activation or transfer notifications to its end-users. To use email, you must provide a valid email address; to use SMS, you must provide a valid phone number with the correct country code for each and every end-user.
4. For *Type,* select a desired message template.
   Note: FIC offers three types of template, and each template is for a specific purpose. Be sure to create all the three types of template to take full advantage of this feature.
5. Click *Confirm*.
6. Specify a unique template name.
7. Make the required changes to the message subject.
8. Make the desired changes to the message content, if you like.
9. Click *Preview* to review the message.

10. Click *Save*.

Editing a template

Only custom templates can be edited. Default templates are read-only and cannot be edited.

To edit a template:

1. Click *Customization>Templates*.
2. Locate the custom template of interest.
3. Click the tool icon and select *Edit*.
4. Make the desired changes.
5. Click *Preview* to review the changes.
6. Click *Save*.

Using templates

All templates are applied at the realm level.

Applying a token activation/transfer notification template

1. Click *User Management > Realms*.
2. Locate the realm of interest.
3. Click the tools icon and select *Settings*.
4. Click the *FTM* tab.
5. Select the desired template.
6. Click *Apply Changes*.

Applying an email OTP template

1. Click *User Management* > *Realms*.
2. Locate the realm of interest.
3. Click the tool icon and select *Settings*.
4. Click the *Email MFA* tab.
5. Select the desired template.
6. Click *Apply Changes*.

Applying an SMS OTP template

1. Click *User Management* > *Realms*.
2. Locate the realm of interest.
3. Click the tool menu, and select *Settings*.
4. Click the *SMS MFA Setting* tab.
5. Select the desired template.
6. Click *Apply Changes*.

Deleting a template

Only custom templates can be deleted. Default templates are read-only, and cannot be edited or deleted.

To delete a template:

1. Click *Customization>Templates*.
2. Locate the template.
3. Click *Delete*.
4. Click *Yes*.

Managing custom branding

The branding feature enables you to customize the look and feel of your SSO applications or end-user portals with your own branding theme. This includes background color, text color, and button color, etc. You can also use your own logos or tag lines.

Creating an SSO application branding theme

1. Click *Customization* > *Branding*.
2. Click *Add Branding* .
3. Make the entries and selections as described in the following table.
4. Click *Save*.

Parameter	Description
Name	Enter a unique name for the SSO application branding theme configuration.
Site	Single Sign-On
Primary Color	Select the primary color of the SSO application branding theme.
Accent Color	Select the accent color of the SSO application branding theme.
Logo	Copy and paste the link to your logo image file here.

Creating an End-User Portal branding theme

1. Click *Customization* > *Branding*.
2. Click *Add Branding*.
3. Make the entries and selections as described in the following table.
4. Click *Save* .

Parameter	Description
Name	Enter a unique name for the end-user portal branding theme configuration.
Site	Select *End-User Portal*.
Button Background Color	Select the button background color.
Button Color	Select the button color.
Sidebar Menu Background Color	Select the sidebar menu background color.
Sidebar Menu Active Background Color	Select the menu active background color.
Sidebar Menu Font Color	Select the sidebar menu font color.
Landing Logo	Copy and paste the link to your landing logo image file here.
Logo	Copy and paste the link to your logo image file here.
Tagline	Enter your tagline.
Subtagline	Enter your subtagline.

Applying custom branding theme to SSO application

1. Click *Applications* > *SSO Applications*.
2. Under *General Information*, select a *Custom Branding* theme.

Applying custom branding theme to End-User Portal

1. Click *Applications* > *End-User Portals*.
2. Click *Add User Portal*.
3. Under *General*, select a *Custom Branding* theme.

Deleting a branding scheme configuration

1. Click *Customization >Branding*.
2. Locate the branding scheme configuration.
3. Click the tool button, and select *Delete*.
4. Click *Yes*.

Managing global settings

This feature is accessible to global admin users only.

The *Settings>Global* menu enables the global admin to make system-wide changes that affect all realms in their account. It has the following options:

Multi-Realm Mode

Fortildentity Cloud comes with a default realm. By enabling *Multi-Realm Mode*, the global admin can create custom realms and associate them with applications to better allocate and manage applications and end-users.

By design, *Multi-Realm Mode* is enabled for new FIC customers. When *Multi-Realm Mode* is disabled, new applications are assigned to the default realm; when multi-realm mode is enabled, new applications registered in FIC are automatically assigned to a new realm.

While there is no need for new customers to enable *Multi-Realm Mode,* existing customers must enable it to take advantage of its benefits. When *Multi-Realm Mode* is enabled, you can create custom realms and assign applications to them. You must assign an application to a custom realm to add users to and sync users from it. Otherwise, it will be assigned to the default realm where you cannot assign users to or sync users from it.

Even if your applications support the "pre-generated applications" feature and *Multi-Realm Mode* is enabled, you cannot add users to or sync users from pre-generated applications until/unless the global admin has associated them with a realm.

Enabling Multi-Realm Mode

If *Multi-Realm Mode* is disabled in your FIC global settings, you can enable it by taking the following steps:

1. Click *Settings>Global* .
2. Click *Multi-Realm Mode*.
3. Click *Apply Changes*.
4. Read the message.

5. Click *Apply*.

Disabling Multi-Realm Mode

While *Multi-Realm Mode* is enabled, click *Multi-Realm Mode* to disable it. For more information on realms, see Managing realms on page 100.

Share-Quota Mode

By default, *Share-Quota Mode* is enabled. In that case, the remaining user quotas will be shared among all realms. When *Share-Quota Mode* is disabled, the remaining user quotas will not be shared among realms.

Account Disable/Delete Notification

Once your license has expired, FortiIdentity Cloud will periodically send notifications to your account, alerting you that your account will be disabled or closed if the license is not renewed in time.

By default, *Account Disable/Delete Notification* is enabled. You can click the button to disable it.

Auto-Create Application

This feature applies to FortiGate/FortiOS VDOMs only.

Normally, the FortiGate administrator can add a VDOM to FIC as an application by enabling the first user on the VDOM for FIC (if the VDOM has not already been assigned to a realm). So when FIC receives a VDOM list from FortiOS with a new VDOM with a user enabled for FIC service, it automatically adds that VDOM as an application. This may inadvertently allow unintended applications to consume your FIC quotas or credits. To prevent this from happening, FIC has introduced the *Auto-create application* option to make the "add-auth-client-on-creation-of-first-user" feature optional in its global settings.

By default, *Auto-Create Application* is enabled. You can click the button to disable it.

Username Case & Accent Sensitive

By default, the *Username Case & Accent Sensitive* option is enabled in both FortiOS and FIC, but you can disable it in FGT and FIC, respectively. To use this feature, you must ensure that they are set in the same way in both FortiOS and FIC, whether they are "enabled" or "disabled". If they are different, the setting in the FortiOS overrides the one in FIC.

When *Username Case & Accent Sensitive* is disabled, FIC ignores case and accent variations in usernames when processing login requests; when enabled, FIC checks the case and accent conformity in a username and approves the login request only when it matches exactly what is in the database.

This feature only applies to individually imported LDAP users with `set username-case-sensitivity enable/disable;` it does not apply to wildcard LDAP users.

Local Identity Provider

Select this option to enable local user identity management within FortiIdentity Cloud. This beta feature supports FIC as the sole source for user identity management for integration with authentication workflow. No remote IdP is required.

For more information, see Local IDP in FortiIdentity Cloud.

Managing realm settings

The *Settings>Realm* page provides tools for managing the settings of a selected realm.

General settings

To configure the *General* settings of a realm:

1. Click *Settings>Realm*.
2. Select the realm.
3. Click *General*.
4. Set or update the parameters as described in the following table.
5. Click *Apply Changes*.

Parameter	Default value
Default MFA Method	Select one of the following as the default MFA method that your FIC uses to authenticate end users: • *FTM* (default)—FIC sends a unique one-time passcode (OTP) to the FortiToken Mobile app on end-users' smart phones. **Note:** This option requires that your end users must have the FortiToken Mobile app installed on their smart phones. • *SMS*—FIC sends an OTP via text message to your end-users' smart phones. Upon receiving the OTP, the end-user must enter it on the log-in page to gain access to the application. **Note:** To use this option, FIC must have the end users' valid smart phone numbers in its database. • *Email*—FIC sends a unique OTP to the end users' email addresses on file. The users then have to manually copy and past the OTP to FIC to gain access to the application (i.e., FGT or FAC). • *FTK*—FIC requires end-users to provide the OTP generated by their FortiToken (hardware token) for MFA. **Note:** To use this option, the FIC admin must first add the serial numbers of the FortiTokens to FIC, and assign them to the end-users. Upon receiving an end-user's username and password, FIC prompts the user for an OTP from the FortiToken device. The user must press the

Parameter	Default value
	FortiToken to get the OTP, and then manually enters it. See Using hardware tokens on page 187. Also, when FTK is set as the MFA method for a realm, you can let FIC automatically assign FTKs to selected users by clicking the *Auto-assign FTK* button on the *Users* page. See Managing users on page 103.
Max Login Attempts Before Lockout	Click above the horizontal line and specify the number of failed login attempts allowed before lockout. Valid values range from 1 to 25. The default is 7. **Note**: FIC does not allow locked users to authenticate. Instead, it displays the message "Locked, please try again in <lockout interval> minutes."
Lockout Period	Click above the horizontal line and specify a lockout period, which ranges from 60 to 7,200 seconds. The default is 60 seconds.
Enable Bypass	Enable or disable bypass. • *Enable*—End-users can bypass MFA. If enabled, you must also set the *Bypass Expiration Time*, as described below. • *Disable* (default)—End-users cannot bypass MFA. **Note:** If *Enable Bypass* is disabled on the *Settings* page, the admin user can not enable bypass for FIC end-users on the *Users* page. See Managing users on page 103.
Bypass Expiration Time	(Available only when *Enable Bypass* is enabled.) Specify the length of time bypass remains in effect. Valid values range from 5 minutes to 72 hours. The default is 1 hour (3,600 seconds).
Auto-alias by Email	Enable or disable the *Auto-alias by Email* feature. **Note:** The feature is disabled by default. For more information, see Enabling Auto-alias by Email on page 233.
Allow Rooted Device	This option is enabled by default. When it is disabled, FIC will remove all the tokens it has issued for rooted devices when end users are trying to activate new tokens using the devices. This will render the devices unusable with FIC. When you re-enale the option, rooted devices can be used to activate new tokens.
Replay Protection	*HIGH (fortbid all replays)* — The authentication follows the current mechanism and does not allow any OTP replay. *MEDIUM (ignore FTM push replay)* — The authentication counts OTP replays for manual input only. All the requests from push authentications are not counted and are not restricted by OTP replay protection. *LOW (ignore FTM/FTK auth relpay)* — OTP replay protection is disabled. **Note:** For email and SMS, OTP replay are always rejected no matter what the setting is.
Adaptive Auth Profile	Select an adaptive auth profile.

Parameter	Default value
Allowed MFA Methods	 • This feature enables end users of SSO applications to authenticate using MFA methods other than the default setting, based on the configuration made by the administrator. • If the Default MFA Method is set to SMS, setting Email to be an allowed MFA method here will let FIC automatically switch to email authentication and send OTP codes by email if the end users are unable to use SMS. The drop-down menu shows all the MFA methods that you may allow your end users to use. By default, all the options except Email are preselected. If you are satisfied with the default settings, do nothing; otherwise, you can use the tools here to customize your allowed MFA methods. • *All* — Select all allowed options at once. • *Passkey* (preselected) — Select Passkey. • *FTK*(preselected) — Select FTK. • *FTM*(preselected) — Select FTM. • *SMS*(preselected) — Select SMS. • *Email* — Select Email. Refer to the note above.

Enabling Auto-alias by Email

Many FIC end-users have different usernames in different applications and domains. By the same token, the same FIC end-user may have different usernames in different applications. For example, a user by the name of John Doe II may have the following usernames:

- `user1` in VPN
- `user_one` in a web app
- `u1` as a system admin
- `user1@company.com` on an email server

FIC allows for different usernames to be attributed to the same user so that only one token needs to be assigned to that user. It does this by providing an *Auto-alias by Email* option, which, once turned on, enables FIC to automatically put different usernames in an alias if they use the email address.

By default, *Auto-alias by Email* is disabled, you can enable it using the following procedures:

1. On the main menu, click *Settings>Realm* to open the settings page of the current realm.
2. Scroll down the page until you see the *Auto-alias by Email* option.
3. Click the *Auto-alias by Email* button to enable it.

It is important to note that aliased users must be in the same realm. Usernames with the same email address are still set as unique users if they are in different realms, even when *Auto-alias by Email* is enabled.

FTM MFA settings

To configure the *FTM* settings of a realm:

1. Click *Settings>Realm*.
2. Select the realm.
3. Click *FTM*.
4. Set or update the parameters as described in the following table.
5. Click *Apply Changes*.

Parameter	Default value
Settings	
Enable Push	Click the button to enable or disable push notification.
Notification Method	From the drop-down menu, select either of the following: • *Email*—Token activation/transfer codes are sent to users' email addresses. • *SMS*—Token activation/transfer codes are sent by SMS to users' mobile phone numbers. **Note:** When *Notification Method* is set to *SMS*, make sure that the users' mobile phone numbers in the system are valid. Otherwise, you will get an error when requesting a new token for users on the *Users* page. See Managing users on page 103. **Note:** FIC deducts one credit from your credit balance for every 250 SMS messages it sends to deliver OTPs. You may experience some problem sending OTPs by SMS when your credit balance is low, and you will get an error message when trying to send an OTP if there is no credit remaining on your account. In both cases, we strongly recommend that you purchase more credits before attempting to use this feature.
App PIN Required	Click the button to enable or disable this feature. • *Disabled* (default)—No app PIN is required. • *Enable*—If enabled, you must select a PIN Length and PIN Required Mode, as described below.
PIN Length	Click the down arrow and, from the drop-down menu, select one of the following: • *4* • *6 (default)* • *8* **Note:** PIN length refers to the number of digits contained in an app PIN.
PIN Required Type	Click the down arrow and, from the drop-down menu, select either of the following: • *Anytime*—App PIN is required all the time. • *Unlock*—If selected, end-users must have a PIN either on their device or FTM app to access FIC. If an end-user has a PIN on the device, FIC

Parameter	Default value
	won't ask for a PIN when using FTM; if an end-user does not have a PIN on the device, FIC will ask for a PIN to use FTM.
OTP Algorithm	• *TOTP* (default). No action is needed.
OTP Time Step	Click the down arrow and, from the drop-down menu, select either of the following: • *30 (default)* • *60* **Note:***OTP Time Step* refers to the frequency in which FTM token codes are updated. For example, FIC will update FTM token codes once every 30 seconds when OTP Time Step is set to 30.
OTP Validation Window	The number of time steps the validation server takes to validate OTPs. Upon receiving an OTP from a client, the validation server computes the OTP using the shared secret key and its current timestamp (not the one used by the client) and compares the OTPs: if the OTPs are generated within the same time step, they match and the validation is successful.
OTP Display Length	Click the down arrow and, from the drop-down menu, select either of the following: • *6 (default)* • *8* **Note:** OTP Display Length refers to the number of digits contained in a token activation/transfer code.
Activation Expiration Time	Click above the horizontal line and specify the length of time token activation codes remain valid. Valid values range from 1 to 336 hours. The default is 72 hours. **Note:** An FTM Token code must be activated within the set *Activation Expiration Time*. Otherwise, it will expire and you must request a new token.
Notification Templates	
Token Activation Email	An email template for FIC to send token activation notifications to your end-users.
T*oken Transfer Email*	An email template for FIC to send token transfer notifications to your end-users.
Token Activation SMS	An SMS template for FIC to send token activation notifications to your end-users.
Token Transfer SMS	An SMS template for FIC to send token transfer notifications to your end-users.

Email MFA settings

When an end-user is enabled for MFA, FIC sends a unique OTP to the end-user's email address on file. The end-user must manually copy and past the OTP to FIC to gain access to the auth client (e.g., FGT or FAC).

To configure the *Email MFA* settings of a realm:

1. Click *Settings>Realm*.
2. Select the realm.
3. Click *Email MFA*.
4. Set or update the parameters as described in the following table.
5. Click *Apply Changes*.

Parameter	Description
Settings	
OTP Expiration Time	Click the down arrow to select an OTP expiration time. **Note:** An OTP is valid only within the specified OTP expiration time, and expires beyond that. The default is 5 minutes.
OTP Display Length	Click the down arrow to select an OTP display length, which is the number of digits displayed. The default is 6.
Templates	
OTP Template	Click the down arrow to select an OTP email template. **Note:** You can view the content of the selected template by clicking the view button on the right.

SMS MFA settings

Once an end-user is enabled for MFA, FIC sends an OTP via text message to the end-users' smart phone. Upon receiving the OTP, the end-user must enter it on the log-in page to gain access to the application.

To configure the *SMS MFA* settings of a realm:

1. Click *Settings>Realm*.
2. Select the realm.
3. Click *SMS MFA*.
4. Set or update the parameters as described in the following table.
5. Click *Apply Changes*.

Parameter	Description
Settings	

Parameter	Description
OTP Expiration Time	Click the down arrow to select an OTP expiration time. **Note:** An OTP is valid only within the specified OTP expiration time, and expires beyond that. The default is 5 minutes.
OTP Display Length	Click the down arrow to select an OTP display length, which is the number of digits displayed. The default is 6.
Templates	
OTP Template	Click the down arrow to select an OTP SMS template. **Note:** You can view the content of the selected template by clicking the view button on the right.

Managing password policy

The Password Policy enables to manage your password policies.

To set the *Password Policy* of a realm:

1. Click *Settings* > *Realm*.
2. Select the realm.
3. Click *Password Policy*.
4. Set the password policy.
5. Click *Apply Changes*.

Alarms

The *Alarms* page enables you to configure alarm events to notify users when their consumption of user quota or SMS credits has reached the specified threshold. Alarms can be applied to your entire account or specific realms in your account. FIC sends out email messages to users specified in the alarm event configuration when the alarm is triggered.

- Creating a user quota alarm on page 238
- Creating an SMS credit balance alarm on page 238

Configuration of an alarm event starts with the configuration of receivers and receiver groups. Receivers are users who receive alert notifications. See Configuring receiver groups on page 239 and Configuring receivers on page 239.

Creating a user quota alarm

1. Click *Settings* > *Alarm*.
2. Click *Add Alarm*.
3. For *Resources*, select *Users*.
4. For *Level*, select *Realm* or *Global*. (Note: If Global is selected, the alarm will be applied to your entire account; if Realm is selected, you must select the specific realm or realms from list of realms.)
5. For *Threshold*, enter a value between 0 and 99 as a percentage.
6. Enter a description of the alarm event. (Optional)
7. For *Groups*, select the receiver group(s). See Configuring receiver groups on page 239.
8. Click *Save*.

Creating an SMS credit balance alarm

1. Click *Settings* > *Alarm*.
2. Click *Add Alarm*.
3. For *Resources*, select *SMS*.
4. For *Level*, select *Realm* or *Global*. (Note: If Global is selected, the alarm will be applied to your entire account; if Realm is selected, you must select the specific realm or realms from the list of realms.)
5. For *Threshold*, enter the numeric value to be used as the SMS credit threshold.
6. Enter a description of the alarm event. (Optional)
7. For *Groups*, select the receiver group(s). See Configuring receiver groups on page 239.
8. Click *Save*.

Alarm routing

Alarm routing enables you to create receiver groups so that the same alarm can be send to al receivers at once.

- Configuring receivers on page 239
- Configuring receiver groups on page 239

Configuring receiver groups

1. *Click Settings>Alarm Routing >Groups.*
2. Click *Add Group.*
3. Specify the group name.
4. Enter a group description. (Optional).
5. Select the receivers.
6. Click *Save.*
7. Repeat the above steps to add more receiver groups.

Configuring receivers

1. Click *Settings>Alarm Routing>Receivers.*
2. Click *Add Receiver.*
3. Specify the receiver name.
4. Enter a description. (Optional)
5. Enter the receiver's email address.
6. Click *Save.*
7. Repeat the above steps to add more receivers.

Adaptive authentication

Multi-factor authentication provides more security than password-only login, but it comes at the cost of inconvenience for end-users. The adaptive authentication feature uses the available information regarding a login attempt (for example, time of day, geo-location, and so on) to evaluate the circumstantial risk of a given login attempt. The second authentication factor is required only when that risk is higher than a predetermined threshold. Furthermore, you might choose to block an authentication attempt entirely if the circumstantial risk is deemed high enough.

FortiIdentity Cloud (FIC) allows end-users to bypass OTP verification of MFA under certain “safer” conditions and denies such attempts under certain otherwise “riskier” conditions. Upon receiving a request to bypass the OTP verification for MFA authentication, the FIC server assesses the situation and decides whether to deny the attempt to bypass the pre-configured OTP verification of MFA based on the following conditions:

- Trusted subnet/geo-location
- Time of day/day of week

Token bypass is allowed if the end-user meets one of the following conditions:

- End-user IP address is from a trusted subnet
- End-user IP address is from a trusted geo-location
- Time is within the expected schedule

Token bypass is denied if the end-user meets one of the following conditions:

- End-user IP address is NOT from a trusted subnet
- End-user IP address is NOT from a trusted geo-location
- Time is outside of the expected schedule

This section covers the following topics:

Viewing adaptive authentication policies

The *Adaptive Auth* > *Policies* page displays all the adaptive auth policies in your account.

Parameter	Description
NAME	The name of the policy.
ACTION	The action specified in the policy, which can be one of the following: • *Multi-factor Authentication* (default) • *Block* • *Bypass* **Note:** The FIC server takes the specified action when an authentication request matches the policy.
PROFILE REFERENCES	The adaptive authentication profile that uses the policy.
LAST UPDATE	The date and time of the most recent update of the policy.

Creating an adaptive authentication policy

1. Click *Adaptive Auth*.
2. Click *Policies*.
3. Click *Add Policy*.
4. Make the desired entries and/or selections, as described in the following table.
5. Click *Apply*.

Parameter	Description
Name	Specify a unique name for the policy.
Action	Select one of the following: • *Enforce MFA* — By default, the FIC server will require login attempts from the specified source to use MFA. • *Block* — The FIC server will block login attempts from the specified source. • *Bypass MFA* — The FIC server will let the login attempts from the specified source bypass the MFA requirement. **Note:** The FIC server takes the specified action when an authentication request matches the policy settings.
Filters	Select the filter • *Subnet Filter* — See *Subnet Filter* below. • *Location Filter* — See *Location Filter* below.

Parameter	Description
	• *No Source Filter* — Select this option if you do not want to use any filter. • *Schedule* — Check the checkbox to enable scheduling. See *Schedule* below for details.
Subnet Filter	**Note:** This option is available only when *Subnet Filter* is selected in the *Filters* field above. Specify the subnet in one of the following formats: • IP address, e.g., 10.10.1.1 • IP range, e.g., 10.10.0.0 - 10.10.10.2 • CIDR notation, e.g., 10.10.1.0/24 **Note:** The *No IP* option is for devices that do not support subnet filtering. If enabled, the policy will be applied to auth requests that do not have IP information.
Location Filter	**Note:** This option is available only when *Location Filter* is selected in the *Filters* field above. • Use the list menu to select the countries or regions of interest. • Select Unknown Country or Region if the location is unknown.
Schedule	**Note:** This option becomes available only when *Schedule* is selected in the *Filters* field above. Set the schedule using the following parameters: • *Weekdays* — Select the days of the week. • *Timezone* — Select the timezone, which is the timezone of the web browser by default. When an authentication request comes in, the FIC server uses the time of this timezone to match the request. • *Time Range*— Select either *All day* (default) or a specific time frame of the day. **Note:** If the start time is less than or equal to the end time, then the time range would be start time — end time; otherwise, the time range would be 0:00 — end time, start time - 23:59.

Editing an adaptive auth policy

1. On the *Adaptive Auth* > *Policies*.
2. Identify the policy.
3. Click the tool icon and select *Edit*.
4. Make the desired changes.
5. Click *Apply*.

Deleting an adaptive auth policy

1. Click *Adaptive Auth* > *Policies*.
2. Identify the policy.
3. Click the tool icon, and select *Delete*.
4. Click *Yes*.

Viewing adaptive auth profiles

The *Adaptive Auth* > *Profiles* page displays all the adaptive auth policy profiles in your account.

Parameter	Description
NAME	The name of the adaptive auth profile.
ACTION	The action specified in the policy, which can be one of the following: • *Multi-factor Authentication* (default) • *Block* • *Bypass* **Note:** The FIC server takes the specified action when an authentication request matches the profile.
REALM REFERENCE	The number of realm that are using the profile.
APPLICATION REFERENCES	The number of applications that are using this profile.

Creating an adaptive authentication profile

To create an adaptive authentication profile:

1. Click *Adaptive Auth* > *Profiles*.
2. Click *Add Profile* .
3. Make the entries and/or selections as described in the following table.
4. Click *Apply*.

Parameter	Description
Name	Specify a unique profile name.
Default Action	Select a default action, which can be one of the following: • *Multi-factor Authentication* (default)

Parameter	Description
	• *Block* • *Bypass* (**Note:** If an authentication did not fall into any policies, FIC will take this action on the authentication request.)
Policy Sequence	Select the priority of the policies to be selected below. **Note:** The two policy fields below could be empty (no selection). If no policy is selected, the FIC server takes the default action specified above. When two policies are selected, Policy 1 takes priority over Policy 2.
Policy 1	Select a policy as Policy 1. (Optional)
Policy 2	Select a policy as Policy 2. (Optional)

Applying adaptive authentication profiles

Adaptive authentication profiles can be applied to applications and/or realms. A profile applied to applications has higher priority than a profile applied to realms. For example, an authentication from application C under Realm R. Client C has Profile A and Realm R has Profile B. In this case, Profile A is the one that is in effect.

To apply an adaptive auth profile to Web application:

1. Click *Applications* > *Web*.
2. Identify the Web app,
3. Click the tool icon, and select *Edit*.
4. Select the *Adaptive Auth Profile*.
5. Click *Save*.

To apply an adaptive auth profile to a realm:

1. Click *Settings* > *Realm*.
2. Select the realm.
3. Click *General*.
4. Select the *Adaptive Auth Profile*.
5. Click *Apply Changes*.

Editing an adaptive auth profile

1. Click *Adaptive Auth* > *Profiles*.
2. Locate the profile.
3. Click the tool icon, and click *Edit*.

4. Make the desired changes.
5. Click *Apply*.

Deleting an adaptive authentication profile

To delete an adaptive authentication profile:

1. Click *Adaptive Auth > Profiles*.
2. Identify the profile.
3. Click the tool icon, and select *Delete*.
4. Click *Yes*.

Creating a last-login policy

The *Last Login* feature enables FortiIdentity Cloud admins to let end-users use the trusted IP or the trusted subnet login MFA bypass within a specified time period. In so doing, end-users using the trusted IP resources can use the MFA feature more easily in their daily work.

To enable the *Last Login* feature in an adaptive authentication policy:

1. Click *Adaptive Auth>Policies*.
2. Click *Add Policy*.
3. Specify the name of the policy.
4. For *Action*, select *Bypass MFA*.
5. For *Filters*, select *Subnet Filter*.
6. For *Subnets*, specify the IP or subset. (Note: The IP and subnet must be supported by FortiProducts).
7. Select the *Last MFA* and specify a reasonable *MFA Interval*. (Note: The valid values range from 1 to 72 hours.)
8. For *Schedule*, select a schedule set.
9. Click *Apply*.
10. Add the new policy to a profile and be sure to select the same action *(Bypass MFA)*.
11. Add the new profile to any application (including FortiProducts and web apps) and any realms whose users are going to use the specified trusted IPs or subnets.

Creating an impossible-to-travel policy

The Impossible Travel feature helps to improve the security level and blocks suspicious login attempts when FortiIdentity Cloud detects an unusual login request far away from a reasonable geographical location, for example, a login request from Russia for a device used by an employee who is living in the United States. In that case, FIC will block it. FIC is able to identify suspicious sign-in attempts based on distance and time elapsed between two subsequent user sign-in attempts. The default is 500 miles per hour. Bear in mind that the user IP must be supported by FortiProducts.

To enable the Impossible Travel feature in an adaptive authentication policy:

1. Click *Adaptive Auth > Policies*.
2. Select *Add Policy*.
3. Specify the policy name.
4. For *Action*, select *Enforce MFA or Block*.
5. For *Filters*, select *Location Filter*.
6. For *Location Filter*, select the countries for normal login location.
7. Select the Impossible Travel button to enable it.
8. For *Schedule*, select a desired schedule set.
9. Click *Apply*.
10. Add the new policy into a profile, and be sure to select the same action *(Enforce MFA or Block)*.
11. Add the new profile into any application (including FortiProducts and web apps) and any realm whose users are going to log in from the specified locations.

Managing certificates

The *Certificates* page enables you to upload Identity Provider (IdP) Signing Certificates. The certificates are used by the IdP Proxy to sign SAML assertions, ensuring that data exchanged between the IdP and Service Provider (SP) is secure and authentic.

To upload a certificte:

1. Click *Settings* > *Certificates*.
2. Click *Add Certificate*.
3. Specify the certificate name.
4. Upload the *Certificate*.
5. Upload the *Private Key*.
6. Click *Save*.

FortiOS CLI commands for FortiIdentity Cloud

This section discusses the FortiOS CLI commands that FIC supports.

Global system configuration

FortiOS comes with a "`config system global`" command which enables the FortiGate admin to enable or disable FIC service on FortiGate. If FIC is disabled, all APIs to FIC will be disabled, except the "`show`" command under "`execute fortitoken-cloud?`". This provides a way to control the communication between the whole FortiGate device so that individual applications (VDOMs) will not be able to set up their connections or communicate with the remote FIC server.

By default, FIC is enabled in FortiOS. If it is disabled, you will not have the option of FIC service as an MFA method when configuring a user.

```
config system global
    set alias "FG101ETK00000000"
    set hostname "FG101ETK00000000"
    set fortitoken-cloud enable
    set switch-controller enable
    set timezone 04
end
```

This global configuration does not invoke any FortiGate-FortiIdentity Cloud API.

Accessing FIC management commands

This global command enables you to access the following command options to manage FIC service on your FortiGate.

```
FG101ETK00000000 #  execute fortitoken-cloud ?
new       Send new activation code for a user.
show      Show service status of this FortiGate.
sync      Synchronize users to FortiIdentity Cloud.
trial     Activate free trial.
update    Update VDOM list to FortiToken Cloud.

FG101ETK00000000 #  execute fortitoken-cloud new ?
<user name>    User name for new token.

FG101ETK00000000 #  execute fortitoken-cloud sync ?
<user type>    {Enter <return> | all | local | remote}

FG101ETK00000000 #  execute fortitoken-cloud trial ?
<Enter>

FG101ETK00000000 #  execute fortitoken-cloud update
<Enter>
```

The `# execute fortitoken-cloud show` command yields the FIC service status of the FortiGate, which can be one of the following:

- Licensed—The FortiGate has a valid FIC service license.
- Service ready—The FortiGate is ready for FIC service.
- Service balance—The remaining FIC account balance in terms of credits, for example, 11474.40 credits.

The `execute fortitoken-cloud update` command sends an updated list of VDOM names to FortiIdentity Cloud so that they can be assigned to realms on the FortiIdentity Cloud portal.

Configuring admin users

Use the following commands to add an admin user account.

```
config system admin
    edit "admin1"
        set accprofile "super_admin"
        set vdom "root"
        set two-factor fortitoken-cloud
        set email-to “admin1@fortinet.com”
        set sms-phone “+14150123456”
        set password ENC SH2w9YIyuuKUMy+xmpxksgsJ9CfAMIjG8ZOVu8yGDk=
```

```
   next
end
```

Command	Description
`config system admin`	Starts the configuration of a system admin user.
`edit <username>`	Specify the admin username.
`set accprofile`	Specify the admin account profile name. For example, `super_admin`.
`set vdom`	Specify the VDOM name. For example, `root`.
`set two-factor`	Select an MFA method: • `disable` —No MFA. • `fortitoken`—FortiToken (FTK) or FortiToken Mobile (FTM). • `email`—Email. • `sms`—Simple message service. This option requires an SMS server and SMS phones. • `fortitoken-cloud`—FortiIdentity Cloud. **Note:** FortiIdentity Cloud is the default MFA method.
`set email-to`	Specify the email address to which FIC sends MFA activation codes.
`set sms-phone`	Specify the mobile phone number for receiving SMS messages.
`set password`	A system-generated password.

Configuring local users

Use the following commands to add a local user.

```
config user local
   edit "user1"
      set type password
      set two-factor fortitoken-cloud
      set email-to "user1@fortinet.com"
      set sms-phone "+14080123456"
      set passwd-time 2019-06-14 16:38:12
      set passwd ENC EKhmlTBu1hmHUokESNTkNjxV8mBQ+AgyRPlInw==
   next
end
```

Command	Description
`config user local`	Starts the configuration of a local user.
`edit <username>`	Create the username.
`set type password`	Set type to password (authentication).
`set two-factor`	Select the MFA method:

Command	Description
	• `disable`—No MFA. • `fortitoken`—FortiToken (FTK) or FortiToken Mobile (FTM). • `email`—Email. • `sms`—Simple message service. **Note:** This option requires an SMS server and SMS phones. • `fortitoken-cloud`—FortiIdentity Cloud. **Note:** FIC is the default MFA method.
`set email-to <email address>`	Specify the email address to which the authentication code is sent.
`set sms-phone`	Set the mobile phone number for receiving SMS messages.
`set passwd-time`	Set the time the password is created.
`set passwd`	Set the password .

Configuring local LDAP users for FIC service

Your can use the following commands to configure FortiGate local LDAP users to use FortiIdentity Cloud for MFA. In this case, verification of the LDAP user passwords verification is done through the LDAP server EngLDAP, but the other settings are the same as those of a regular local user.

```
config user local
   edit "ldap-user1"
      set type ldap
      set two-factor fortitoken-cloud
      set email-to "ldap-user1@fortinet.com"
      set sms-phone "+14080123456"
      set ldap-server “EngLDAP”
      set passwd ENC EKhmlTBu1hmHUokESNTkNjxV8mBQ+AgyRPlInw==
   next
end
```

Configuring wildcard LDAP users for FIC service

Your can use the following commands to configure FortiGate wildcard LDAP users to use FortiIdentity Cloud for MFA.

```
   config user ldap
         edit "EngLDAP"
               set server "xx.xxx.xx.xx"
               set cnid "uid"
               set dn "dc=srv,dc=world"
               set type regular
               set two-factor fortitoken-cloud
               set username "cn=Manager,dc=srv,dc=world"
               set password ENC LWdyb+/k6e4TtSk070tODaCZAcbgEGKohA==
```

```
        next
    end
```

Wildcard LDAP users are those of a remote LDAP server user group, whose user configuration is unknown to FortiGate. Each end-user should have the following attributes configured on the LDAP server:

- `mail: user_email_address (e.g., mail: user1@abc.com)`
- `mobile: user_phone_number (e.g., mobile: +14080123456)`

- In FortiOS, the "`mail`" attribute is mandatory and required of each user, while the "`mobile`" attribute is optional.
- FIC requires that the phone number be in the format of " `+(country_code)(areacode_number)`".

During user configuration, the FortiGate-FIC user APIs are called for add-user, delete-user, modify-user with the following information in each API:

- Username
- VDOM name
- FortiGate serial number (SN)
- HA cluster membership information (if it's part of an HA configuration)

If an API requires the user ID, e.g., the delete-user API, FortiOS must use the GET API to retrieve the user ID from FIC.

- Wildcard LDAP users are automatically synced from the remote AD/LDAP to FIC by FOS when FOS is configured to use FIC for remote wild card users on the remote AD/LDAP server. The frequency of this auto-sync for wildcard AD/LDAP users is once every 24 hours.
- sAMAccountName as cnid is not supported before FOS 6.4.6.

Configuring local RADIUS users for FIC service

Your can use the following commands to configure FortiGate local RADIUS users to use FortiIdentity Cloud for MFA. In this case, verification of the RADIUS user passwords verification is done through the RADIUS server EngRadius, but the other settings are the same as those of a regular local user.

```
config user local
        edit  “radius-user1”
              set type radius
              set type password
              set two-factor fortitoken-cloud
              set email-to "radius_user1@anycompany.com"
              set sms-phone "+14081234567"
               set radius-server  “EngRadius”
              set passwd-time 2020-02-18 16:00:59
              set passwd ENC M27kJaZ3I3VeHjQun8yqSHWvA
```

```
                next
        end
```

Diagnosing FortiIdentity Cloud

Use the following commands to diagnose and troubleshoot FIC issues.

```
debug          Enable/disable debug output.
server         IP address port number and https.
show           Display diagnostics information.
delete         Command to delete a user.
clear          Clear server connection settings for diagnostics.
migrate-ftm    Perform FTM license migration.
set-http       Set HTTP status return code for diagnostics only.
sync           Synchronize user information with FortiToken Cloud.
```

Examples

```
FG100D3G00000000 (global) # diag fortitoken-cloud debug {enable | disable}
```

```
FG100D3G00000000 (global) # diag fortitoken-cloud server
```

```
FG100D3G00000000 (global) # diag fortitoken-cloud show {server | realm | users | user <username>
<VDOM>}
```

```
FG100D3G00000000 (global) # diag fortitoken-cloud delete <username>
```

```
FG100D3G00000000 (global) # diag fortitoken-cloud set-http <number>
```

```
FG100D3G00000000 (global) # diag fortitoken-cloud clear <Enter>
```

```
FG100D3G00000000 (global) # diag fortitoken-cloud sync { <Enter> | all | local | remote }
```

The `diag fortitoken-cloud sync` command requires you to specify the type of user to sync to FortiIdentity Cloud:

```
diagnose fortitoken-cloud sync ?
<user type> {Enter <return> | all | local | remote}
```

```
FGVM01TM00000000 (global) # diagnose fortitoken-cloud migrate-ftm
<string>    Enter command: show, start, abort, add-users, delete-users, ftm2ftc.
FGVM01TM00000000 (global) # diagnose fortitoken-cloud migrate-ftm show
<string>    FTM license number.

FGVM01TM00000000 (global) # diagnose fortitoken-cloud migrate-ftm start
<string>    FTM license number.
```

```
FGVM01TM00000000 (global) # diagnose fortitoken-cloud migrate-ftm abort
<string>    FTM license number.

FGVM01TM00000000(global) # diagnose fortitoken-cloud migrate-ftm add-users
<string>    FTM license number.

FGVM01TM00000000 (global) # diagnose fortitoken-cloud migrate-ftm delete-users
<string>    FTM license number.

FGVM01TM00000000 (global) # diagnose fortitoken-cloud migrate-ftm ftm2ftc
<string>    FTM license number.
```

The above diagnose CLI command shows FTM license migration status, start migration process, abort migration process, add-users into FIC and delete-users from FIC, and force to covert two-factor authentication from FortiToken to FortiIdentity Cloud during the migration.

Showing user ldap

Starting from FortiOS 7.2.1, the `group-filter` setting has been replaced with `two-factor-filter`, as shown in the following example command:

```
FGVMULTM24003711 (root) # show user ldap
config user ldap
    edit "ad-136"
        set server "10.160.13.6"
        set cnid "sAMAccountName"
        set dn "DC=cloudsolutionsqa,DC=com"
        set type regular
        set two-factor fortitoken-cloud
        set two-factor-filter "(&(objectClass=user)(memberOf=Cn=FIC-
ops,ou=QA,dc=cloudsolutionsqa,dc=com))"
        set username "ldapadmin"
        set password ENC
```

```
    next
end
```

In this configuration, only users from group `FIC-ops` will be synched to FortiIdentity Cloud when running the `execute fortitoken-cloud sync` command. If the sync command is not run, only users from the configured group will be synched to FIC after the first login.

Licenses

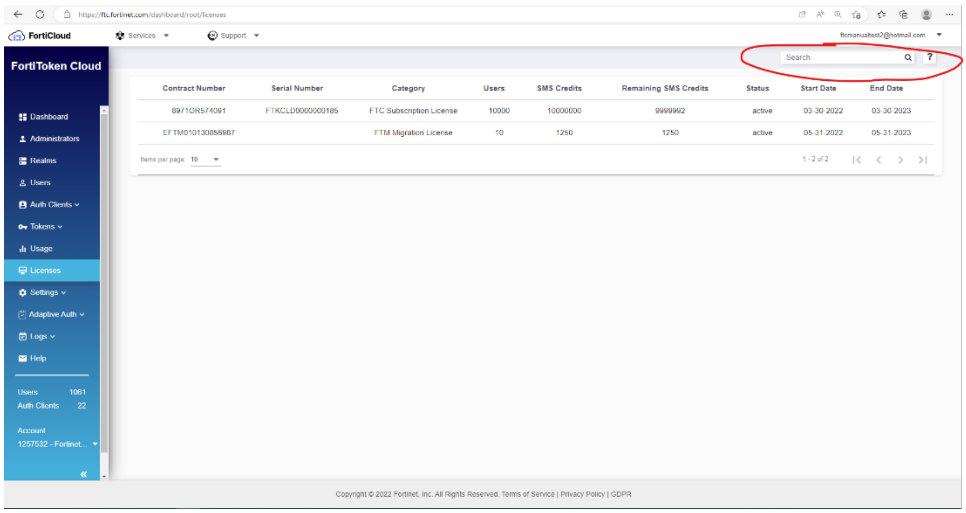
The *Licenses* page applies to customers of time-based subscriptions only. For more information about the time-based subscriptions, see Subscription licensing on page 12.

The *Licenses* page shows all time-based licenses in your account. The table below describes the information on the *Licenses* page.

Column	Description
CONTRACT NUMBER	The contract number of the license.
SERIAL NUMBER	The serial number of the license.
CATEGORY	The license category.
USERS	The maximum number of end-users that the license can support.
SMS BALANCE / TOTAL	The remaining SMS credits / total SMS credits of the license.
STATUS	The status of the license.
START DATE	The date on which the license is registered for use.
END DATE	The date on which the license expires.

License search bar

There is a newly added search bar on the Licenses page which enables you to search licenses by keywords. This makes it easier to find your licenses if you have many licenses in your account.


FortiCloud
Services
Support
FortiToken Cloud
Search
Dashboard
Administrators
Realms
Users
Auth Clients
Tokens
Usage
Licenses
Settings
Adaptive Auth
Logs
Help
Users 1061
Auth Clients 22
Account
1257532 - Fortinet...
Contract Number
Serial Number
Category
Users
SMS Credits
Remaining SMS Credits
Status
Start Date
End Date
89710R574091
FTKCLD0000000185
FTC Subscription License
10000
10000000
9999992
active
03-30-2022
03-30-2023
EFTM01013085867
FTM Migration License
10
1250
1250
active
05-31-2022
05-31-2023
Items per page: 10
1 - 2 of 2
Copyright © 2022 Fortinet, Inc. All Rights Reserved. Terms of Service | Privacy Policy | GDPR

Product documentation and support

The following are the FortiIdentity Cloud product documentation and support information:

- For information about the current release, see the Release Notes.
- For detailed information about product features, click the  (Help) on the GUI or see Admin Guide.
- For product API, see REST API.
- For frequently asked questions, see FAQs.
- For SSL VPN configuration instructions, see SSL VPN Configuration Guide.
- For terms of service, see Service Descriptions.
- For licensing, see Purchasing Guide.
- For SMS rates, see SMS Rate Card.
- For migrating FTM tokens to FortiIdentity Cloud, see Migrating FTM tokens.
- For End-User Portal, see End-User Portal Guide.
- For product support, see Technical Support.

Release history

This section highlights the major feature changes or updates in each of the releases of FortiIdentity Cloud since its GA release. For a complete list of product features, see Main features on page 33.

25.3.c

Release date: August 22, 2025

Patch release only. No new feature has been implemented in this release.

25.3.b

Release date: August 4, 2025

Product name change from "FortiToken Cloud" to "FortiIdentity Cloud".

25.3.a

Release date: July 9, 2025

Patch release only. No new feature has been implemented in this release.

25.2.b

Release date: June 20, 2025

Patch release only. No new feature has been implemented in this release.

25.2.a

Release date: June 9, 2025

- Revamp of FortiIdentity Cloud GUI
- Support for Local IdP (beta feature)
- New terms for the free trial license
- Allow Rooted Device in realm settings.
- Support for OIDC OpenID Provider (OP)

25.1.a

Release date: January 16, 2025

- End-user Portals
- Integration with Microsoft Entra ID
- Allow additional MFA methods
- Integration with FortiClient to provide MFA service for FortiSASE VPN users

24.3.a

Release date: July 30, 2024

- Simplification of FortiGate SP configuration
- Default user source for IdP Proxy
- Addition of location and IP address to Management logs
- Limited access to Web application APIs and IdP-related APIs for trial customers
- FIC Introduction page for potential customers

24.2.a

Release date: May 3, 2024

- IdP Proxy
- Passkeys
- SCIM

- Batch-add users
- User groups
- FTM token migrations from FAC to FIC

23.4.b

Release date: December 21, 2023

- GUI revamping

23.4.a

Release date: November 16, 2023

- SMS rate update
- Support for pagination
- SMS restriction alert

23.3.b

Release date: August 11, 2023

Fortildentity Cloud 23.3.b is a patch release only; no new feature or enhancement has been implemented in this release.

23.3.a

Release date: July 28, 2023

- **Data migration enhancement**—The *Devices (HA)* page has been updated to provide better user experience in managing transfer of device ownership. See Transferring devices on FIC on page 181.
- **Last Login**—The Last Login column of the *Users* page now shows the timestamp of the user's most recent successful MFA login. See Managing users on page 103.
- **Welcome email**—FIC now sends welcome email messages to customers when they start their free trial license or activate their paid license. See Purchasing Guide.

- **Replay protection**—FIC now offers three levels of replay protection in realm setting configuration. See General settings on page 231.

23.1.a

Release date: March 16, 2023

- **Delete users from FIC portal** —FortiIdentity Cloud now allows you to delete users on the portal. (Note: Changes made on the portal will not automatically sync up with the applications.)
- **Process future licenses and update service notification**—FortiIdentity Cloud will send email alerts to customers who don't have enough user quota or whose licenses are to expire in the next 30 days. FortiIdentity Cloud supports and considers the purchased future co-term licenses when counting the expiration date.
- **OU login**—OU login enables OU admins to manage resources of different customer IDs that join the same organization/OU.
- **Self-service device transfer with data**—You can now transfer devices along with related data from one customer to another on the portal with the *Validate Device Ownership* button on the *application > Devices (HA)* page.
- **Management client** —FIC has introduced the new concept of management client as a special type of web app client. The management client is a solution for remote API access & management to selected or all customer's resources such as realms, applications, users, and tokens, etc.
- **Customized alarm based on a specific resource usage—**This feature enables you to configure alarm events to notify specified recipients when consumption of resources like user quota or SMS credits has reached the specified threshold. Alarms can be applied to your entire account or specific realms in your account.

22.4.a

Release date: November 28, 2022

FortiIdentity Cloud 22.4.a offers the following new feature:

- Temporary tokens for activated users
- Restricted access for disabled customers
- FortiIdentity Cloud services status on the monitoring page
- More information of realm/user quota usage on the Realms page
- A new button on the Realms page to show whether share-quota mode is enabled
- Last login
- Impossible to travel

22.3.a

Release date: July 19, 2022

Fortildentity Cloud 22.3.a is a patch release only; no new feature or enhancement has been implemented in this release.

22.2.d

Release date: June 30, 2022

Fortildentity Cloud 22.2.d is a patch release; it also offers the following new feature:

- Account Disable/Delete Notification

22.2.c

Release date: June 1, 2022

Fortildentity Cloud 22.2.c is a patch release only; no new feature or enhancement has been implemented in this release.

22.2.b

Release date: May 9, 2022

Fortildentity Cloud 22.2.b is a patch release only; no new feature or enhancement has been implemented in this release.

22.2.a

Release date: May 4, 2022

Fortildentity Cloud 22.2.a offers the following new features and enhancements:

- Location Filter by country/region on Adaptive Auth page
- application hyperlink on Users page
- FTM migration email notification enhancement

- Email notification to notify customers of the upcoming closure or removal of their accounts
- FortiTrust License support
- SMS License support
- User post/put API enhancement
- FortiAuthenticator SMS notification API
- SMS logs for time-based accounts on Logs page
- SMS usage from count to credit for time-based accounts

21.4.d

Release date: January 18, 2022

- FTM token migration from FGT to FIC

21.4.a

Release date: October 11, 2021

FortiIdentity Cloud 21.4.a is a patch release only; no new feature or enhancement has been implemented in this release.

21.3.d

FortiIdentity Cloud 21.3.d is a patch release, with the following new feature:

- Enhancement to the Validate Device Ownership page

21.3.c

- Adaptive authentication
- Validation of device ownership
- Username case and accent sensitivity (enable/disable)

21.3.b

FortiIdentity Cloud 21.3.b is a patch release only; no new feature or enhancement has been implemented in this release.

21.3.a

FortiIdentity Cloud 21.3.a is a patch release only; no new feature or enhancement has been implemented in this release.

21.2.d

- **Time-based license model**—FortiIdentity Cloud (FIC) now features a new annual subscription model with license options for customers to choose from based on the number of FIC end-users on their account per year. The new license model allows for SMS messages in the amount of 100 multiplied by the total number of users your license can support for the year. *(Applicable to the new time-based annual subscription only.)*
- **Realm-based user quota**—The administrator of a customer with time-based license now can allocate user quota to each realm to effectively manage their assets and end-users. *(Applicable to the new time-based annual subscription only.)*
- **Export of logs in .CSV**—You can now export FIC authentication and management logs in .CSV format for record keeping and sharing.

21.2.c

FortiIdentity Cloud 21.2.c is a patch release only; no new feature or enhancement has been implemented in this release.

21.2.a

FortiIdentity Cloud 21.2.a offers the following new features and enhancements:

- New API to query credit balance with single request.
- Upgrade to FortiGuard access and authentication method.
- Read and write access to all settings, regardless of realm 2FA method.

- Custom OTP and token activation/transfer notification templates.
- FortiCloud IAM support (including new APIs).
- Dashboard Notification when free-trial credits are used.
- Miscellaneous GUI updates.

21.1.a

FortiIdentity Cloud 21.1.a is a patch release, with the following enhancements:

- The word "point(s)" has been replaced with "credit(s)" in FortiIdentity Cloud and its documentation.
- The Dashboard has been updated with the following changes:
  - The "Realms/Max Realms" meter has been relocated to the same row as the "Users/Max Users"and "Clients/Max Clients" meters.
  - The "Clients/Max Clients" meter has been renamed to "applications/Max applications"

20.4.d

FortiIdentity Cloud 20.4.d is a patch release only; no new feature or enhancement has been implemented in this release.

20.4.c

- **Commercial API**—Enables admin users to add web applications as FIC applications and serve their end-users.
- **API for generic applications**—The applications page now shows application type, application name, user count, and realm name.
- **Revamped GUI**—The applications page now has three sub-pages, with the FortiProducts sub-page showing application alias, application type, application name, user count, and realm name.
- **FortiIdentity Cloud RESTful API Specifications**—The document, available in the Docs Library, provides detailed information of the APIs and instructions on how to use them.

20.4.a

FortiIdentity Cloud 20.4.a is a patch release only; no new feature or enhancement has been implemented in this release.

20.3.e

Fortildentity Cloud 20.3.e is a patch release only; no new feature or enhancement has been implemented in this release.

20.3.d

- **Token management made easy**—This release has added the Auth Devices menu to the main menu. It has two sub-menus: Mobile Devices and Hard Tokens. It consolidates soft tokens and hard tokens in one place, enabling the user to view and manage mobile devices and hard tokens more efficiently.
- **HA cluster management**—A Devices menu has been added to the main menu. Not only can you view standalone devices and clusters of applications on the same page, but add devices to or remove them from a cluster as well.
- **User Alias**—The **Settings>Realms** page now has an "Auto-alias by Email" option. When it is enabled, all usernames with the same email address and are in the same realm are automatically set as aliases under the same username (on the Users page). In this way, FIC only needs to assign one token to the same user. When "Auto-alias by Email" is enabled in a realm, you can use the Users page to manually create aliases, modify, merge, or delete aliases.
- **Auto-create application**—The **Settings>Global** page now has added an "Auto-create application" option, which enables the global admin user to enable or disable (default) the auto-creation of applications. It applies to FortiGate VDOMs only, and offers global admin users an option to control over the auto-create-auth-client function for FortiGate VDOMs to prevent unintended applications from consuming credits.
- **Administrators page enhancements**—The Administrators page has gone through some enhancements. You are now able to select multiple realms to add to an admin group, and to view all accounts associated with a customer ID by clicking the Member Count in the Administrators page.
- **Export to CSV**—The Usage page now has an option to enable you to export usage data in .csv file format.
- **Contact Support**—The main menu now has an "Contact Support" menu, which enables you to contact Fortinet support team by email directly from the FIC portal.

20.2.c

Fortildentity Cloud 20.2.c is a patch release only; no new feature or enhancement is implemented in this release.

20.1.b

- Differentiation of user data for local and remote application users.
- Support for FTM Windows provisioning and activation.

20.1.a

- **Hard Tokens**—FIC now supports FortiToken (FTK) which is a hardware token. See Using hardware tokens on page 187.
- **Global administrator and sub-admins**—FIC now enables the global administrator to create sub-admins and allocate resources to them. See Managing admin groups on page 97.
- **Multi-realm support**—FIC now allows the global admin to create realms. See Managing realms on page 100.
- **More MFA methods**—This release adds support for e-mail, SMS, and FTK (FortiToken, which is a hardware token) as options for MFA. See .

4.4.c

FortiIdentity Cloud 4.4.c is a patch release only; no new feature or enhancement is implemented in this release.

4.4.b

- **FortiAuthenticator as authentication client**—FortiIdentity Cloud now supports FortiAuthenticator as an authentication client, in addition to FortiGate.
- **FortiIdentity Cloud enabled on FortiGate**—FortiIdentity Cloud now is enabled on FortiGate by default.

4.3.a

- **Custom logo**—Enables admin users to upload custom logo images to replace the default Fortinet logo at the bottom of the FTM app screen on end-users' devices. See for more information.
- **FTM token activation/transfer notification by SMS**—Enables admin users to let end-users receive FTM token activation or transfer notifications by SMS. See for more information.
- **Access to all accounts by admin users**—FIC admin users are able to access all FIC accounts belonging to their own organization. They can choose which of their accounts to open upon login, and switch to any of their other accounts during a session.

4.2.d

FortiIdentity Cloud 4.2.d is a patch release in support of FortiCloud upgrade, along with some bug fixes; no new feature or enhancement is implemented in this release.

4.2.c

FortiIdentity Cloud 4.2.c is a patch release only; no new feature or enhancement is implemented in this release.

4.2.b

FortiIdentity Cloud 4.2.b is the FortiIdentity Cloud GA release, which offers many of the major features of the product. For more information, see Features and benefits.

Technical support

We, Fortinet, provide free technical support to all our customers with valid product licenses.

Preparing for technical support

In order for us to expedite your technical support request, be sure to have the following information ready when creating the support ticket:

- Your FortiIdentity Cloud (FIC) account ID, the serial number and version number of your FortiProducts (e.g., FortiAuthenticator, FortiGate), including FortiClient version if using FortiClient.
- A detailed description of your problem, including relevant background information. If the issue is about login authentication failure, be sure to provide your FIC username, token serial number, and the version number of the FortiIdentity mobile app.
- Debug log(s), error messages, and/or screenshots, if available.
- Your troubleshooting steps and the result.

Getting your Fortinet product serial number ready

Providing your Fortinet product serial number will help us expedite your service request. How you get your Fortinet product serial number depends on your license, as discussed in the following paragraphs.

Licensed customers

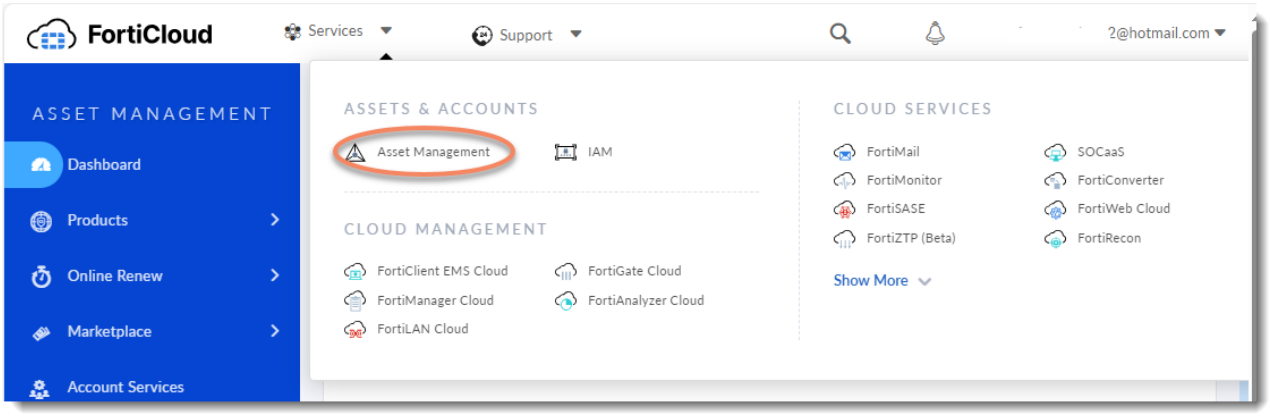
If you are using a time-based FIC license, follow the steps below to locate your Fortinet product serial number:

1. Log into the FortiIdentity Cloud portal.
2. On the left-side menu, select *Licenses* to open the Licenses page.
3. Take note of the serial number for the contract which you are having trouble with.

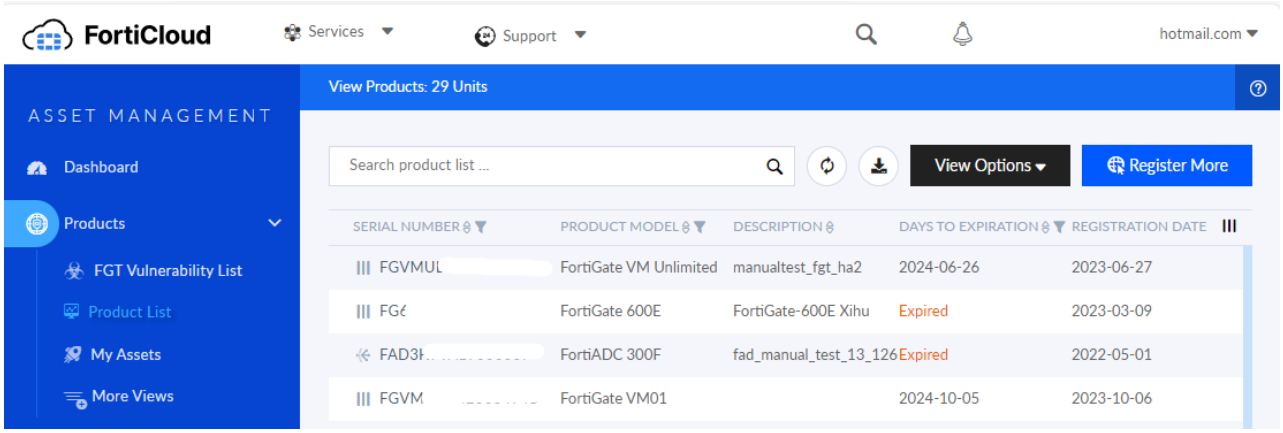
Customers with FTM tokens migrated from FortiGate to FIC

If you have migrated your FTM tokens from FortiGate to FIC, take the following steps to get your serial number:

1. Got to *Services* > *Asset Management*.

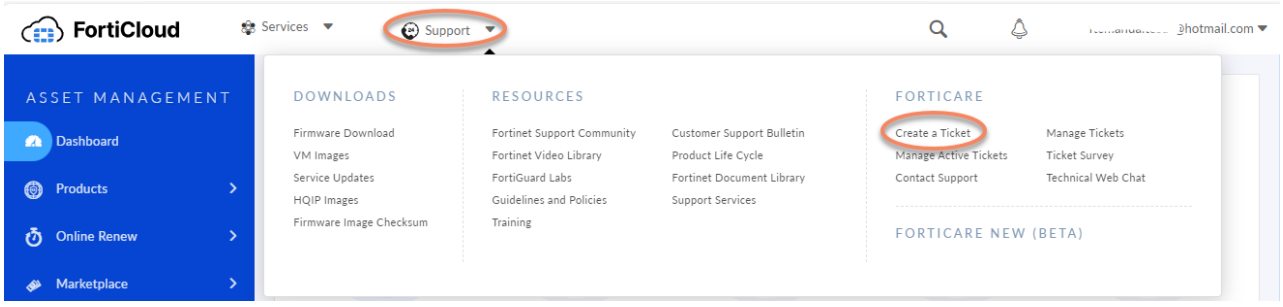


2. Click *Products* > *Product List* to get the serial number of your FortiGate.

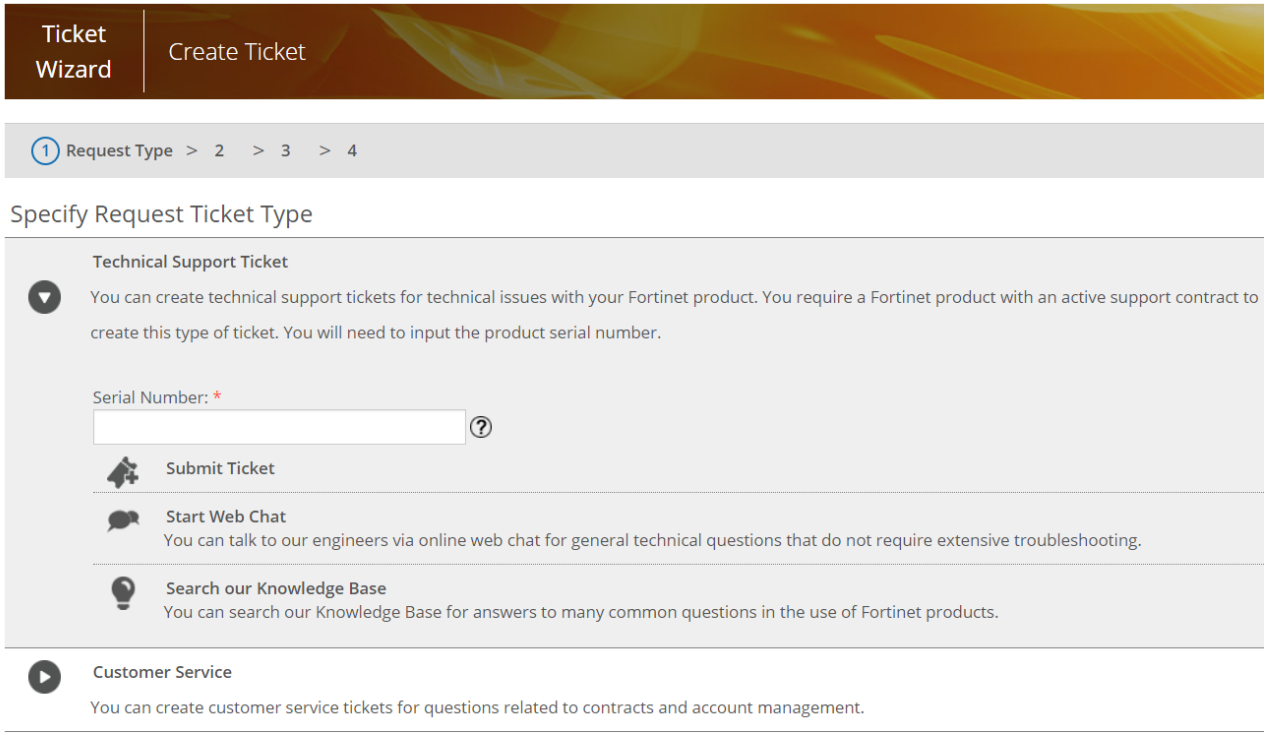


Creating a technical support ticket

1. From the top of the FIC GUI, select *Support>Create a Ticket*.



2. Select *Technical Support Ticket*, enter the serial number of your license, and click *Submit Ticket*.



The instructions above apply to paying customers with valid licenses only. If you are using a free trial version of FortiIdentity Cloud and have questions about contracts, licenses, and account management, please create a 'Customer Service' ticket instead.

Change log

Release Date	Product Version
09/03/2025	Updated the image in Architecture on page 20.
09/02/2025	Updated TKCLD SKU to IDCLD SKU in Stackable co-termed licenses on page 13, with a note that customers with old SKU are able to add licenses with a new SKU.
08/29/2025	Updated the images in Example 3: Google OIDC as IdP on page 150.
08/22/2025	FortiIdentity Cloud 25.3.c initial release.

www.fortinet.com