# Local IdP

## FortiIdentity Cloud 25.4

**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

December 7, 2025
FortiIdentity Cloud 25.4 Local IdP

# TABLE OF CONTENTS

# Local IdP in FortiIdentity Cloud

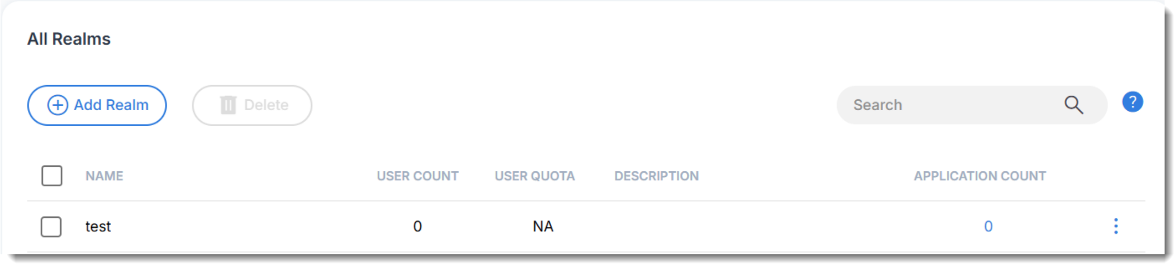
In FortiIdentity Cloud, local IdP means that the user identity (username and password) is local to FortiIdentity Cloud and is not from any external identity provider, such as Google, Azure, etc.

# Adding a Local IdP

In FortiIdentity Cloud, a local IdP is the user source for authentication to the FIC end-user portal or an application that supports SSO login. By default, Local IdP is enabled on all realms in FortiIdentity Cloud, but it can be used only when a local user is created on a realm.

## To set up a Local IdP user source:

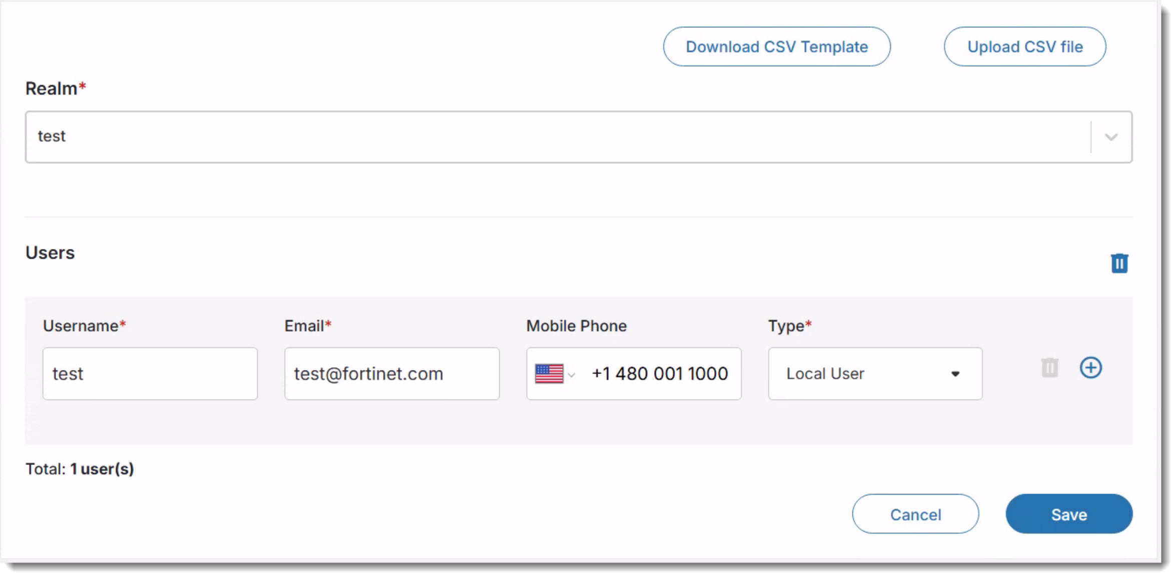
1. On the *Realms* page, click *Add Realm*. For illustration purposes, we create a realm titled "test", as shown in the following screenshot.



| | NAME | USER COUNT | USER QUOTA | DESCRIPTION | APPLICATION COUNT |
|---|---|---|---|---|---|
| □ | test | 0 | NA | | 0 |

# Adding users to the local IdP

1. *Select User Management>Users*, and click *Batch Add*.



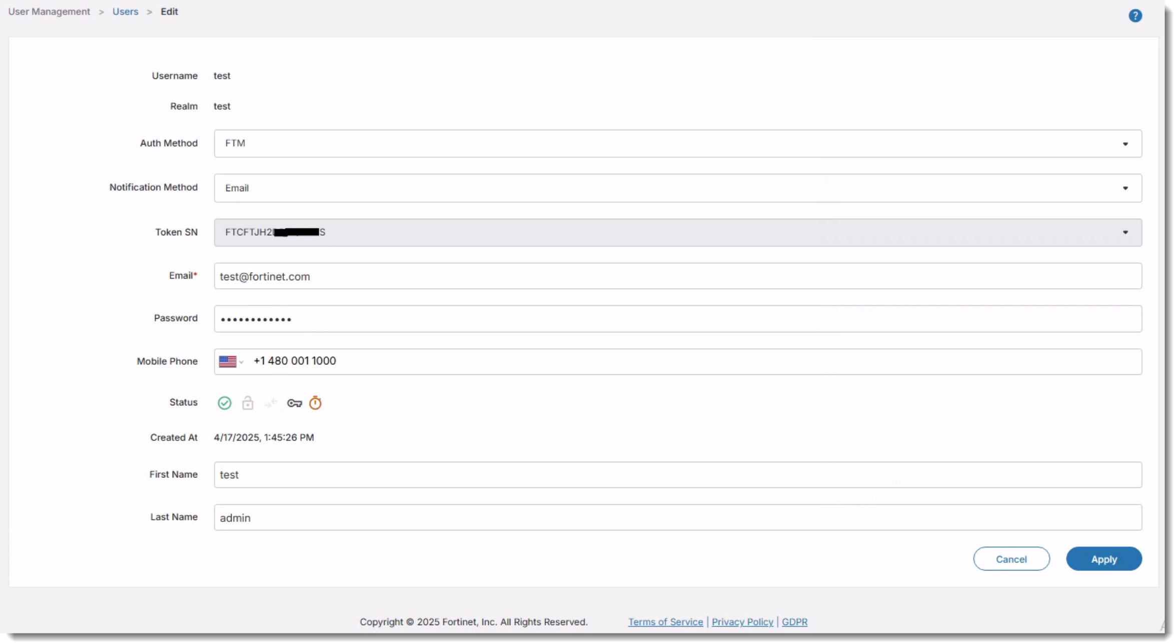
Realm*: test

Users

| Username* | Email* | Mobile Phone | Type* |
|---|---|---|---|
| test | test@fortinet.com | +1 480 001 1000 | Local User |

Total: **1 user(s)**

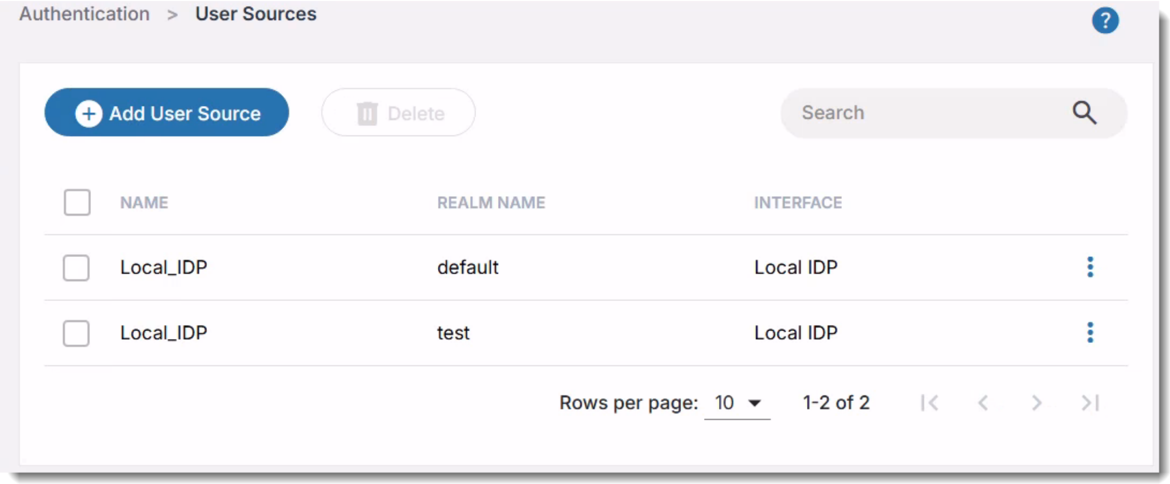
2. Select the "test" realm, enter the username, email address, and mobile phone number, and select Local User. Then click **+** (*Add*), as shown in the screenshot above.
3. After the user is added, click *User Management >Users*, locate the user that you have just added, click the pop-up menu at the far-right of the row, and select *Edit*.



| | |
|---|---|
| Username | test |
| Realm | test |
| Auth Method | FTM |
| Notification Method | Email |
| Token SN | FTCFTJH2[redacted]S |
| Email* | test@fortinet.com |
| Password | •••••••••••• |
| Mobile Phone | +1 480 001 1000 |
| Status | ✓ |
| Created At | 4/17/2025, 1:45:26 PM |
| First Name | test |
| Last Name | admin |

Copyright © 2025 Fortinet, Inc. All Rights Reserved. Terms of Service | Privacy Policy | GDPR

4. Click *Authentication >User Sources*, and you'll find a Local_IdP that FortiIdentity Cloud has automatically created for the "test" realm when a local user is created under “test” realm.

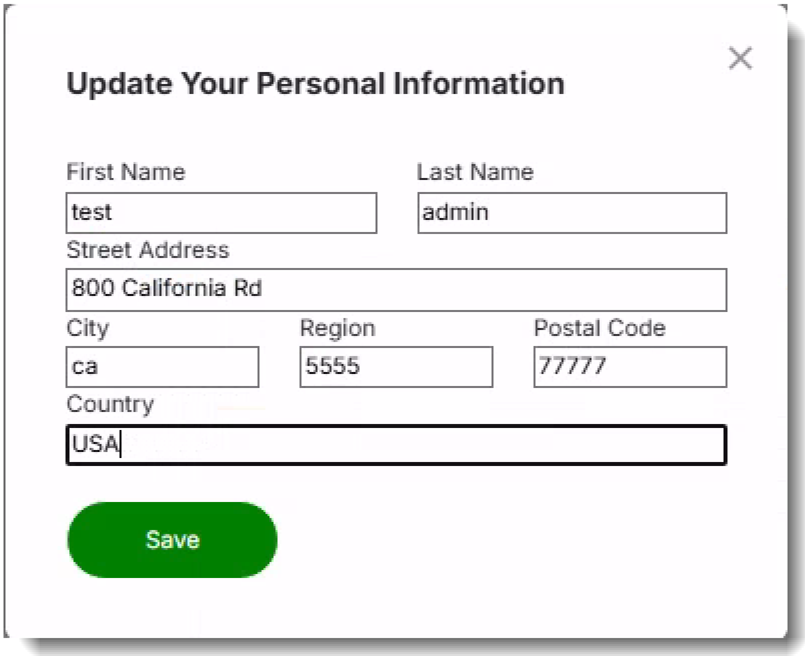


| NAME | REALM NAME | INTERFACE |
|---|---|---|
| Local_IDP | default | Local IDP |
| Local_IDP | test | Local IDP |

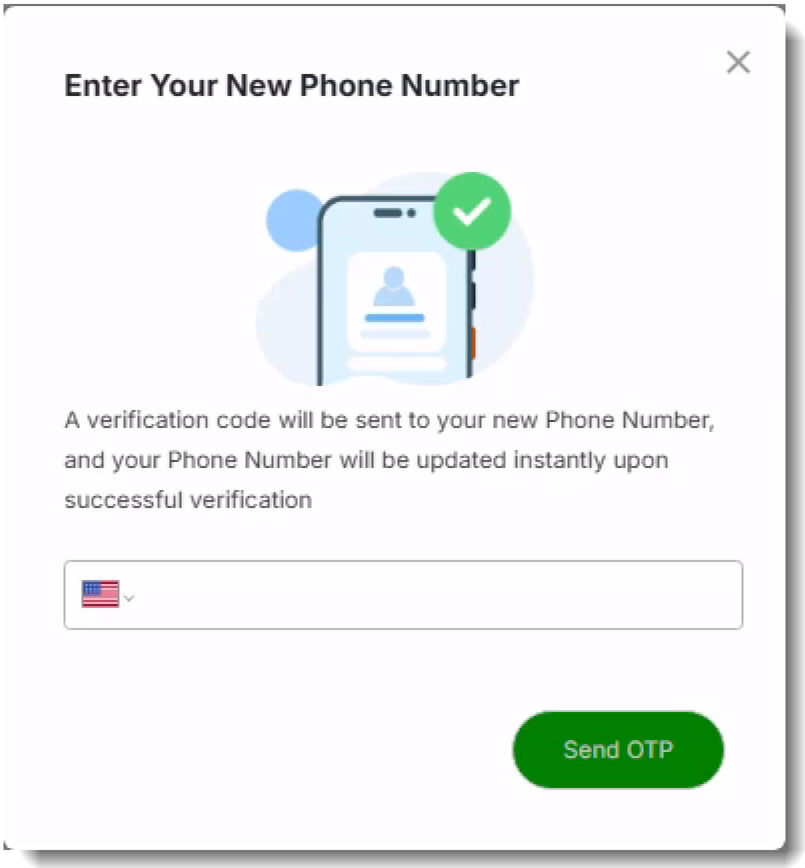
5. Set the user's Auth Method, and click *Apply*.

At this point, the user has been added to the local IdP user source, and should be able to authenticate to the FortiIdentity Cloud End-user Portal with the 1st-factor authentication (i.e., username & password) and the 2nd-factor authentication (i.e., FTK, FTM, EMAIL, SMS, or Passkey).

Once logged in to their End-user Portals, the users can also view and update their profiles, including their mobile phone numbers.


Update Your Personal Information

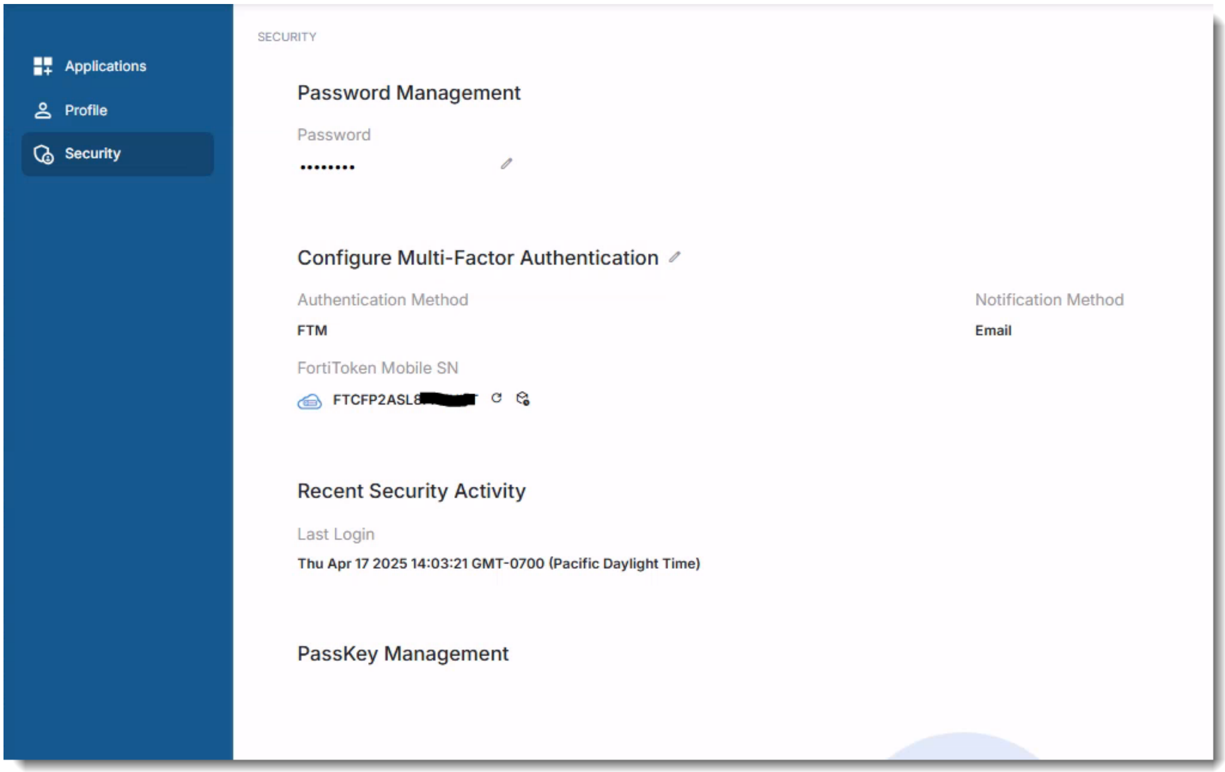
First Name: test
Last Name: admin
Street Address: 800 California Rd
City: ca
Region: 5555
Postal Code: 77777
Country: USA



Enter Your New Phone Number

A verification code will be sent to your new Phone Number, and your Phone Number will be updated instantly upon successful verification

The users can also change their passwords and select another 2nd-factor authentication method.



SECURITY

Password Management

Password

••••••••

Configure Multi-Factor Authentication

Authentication Method

FTM

Notification Method

Email

FortiToken Mobile SN

FTCFP2ASL[redacted]

Recent Security Activity

Last Login

Thu Apr 17 2025 14:03:21 GMT-0700 (Pacific Daylight Time)

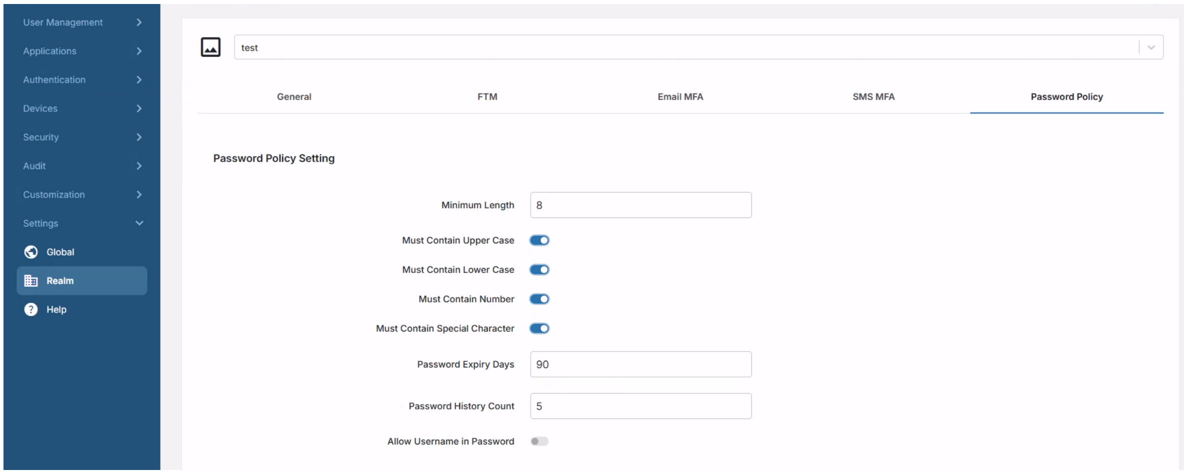
PassKey Management

# Setting End-User Portal password policy

The password policy setting for the End-user Portal uses the username and password of local user accounts as the first factor of authentication. The administrator can determine the password length, expiration date, and required characters in the setting under each individual realm.

## To set the password policy for end-users on a realm:

1. Click *Settings>Realm*.
2. Select the realm of interest, and click *Password Policy*.
3. Make the desired entries or selections, and click *Apply Changes*.



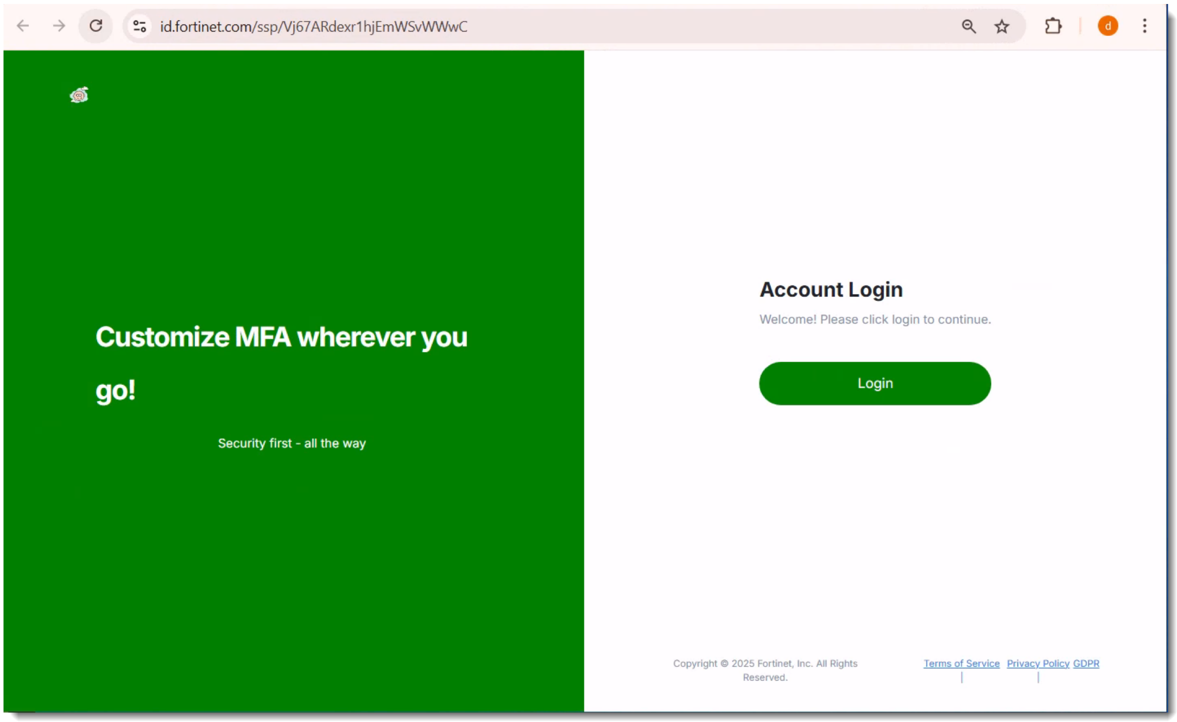
Password Policy Setting

Minimum Length: 8
Must Contain Upper Case ☑
Must Contain Lower Case ☑
Must Contain Number ☑
Must Contain Special Character ☑
Password Expiry Days: 90
Password History Count: 5
Allow Username in Password ☐

# Logging into FIC End-user Portal

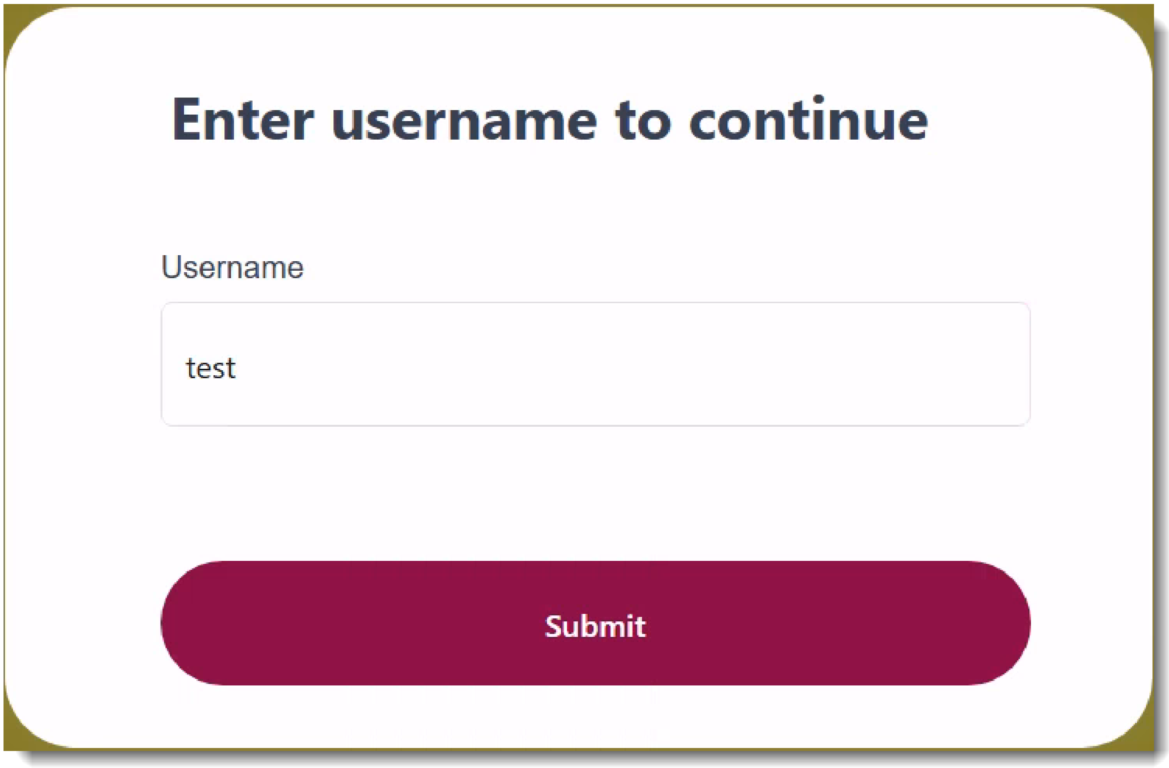
Once the user is added to the Local IdP user source, the user can log into the FortiIdentity Cloud End-user Portal using the username and password that the administrator has configured.

1. Launch the *End-user Portal*.



id.fortinet.com/ssp/Vj67ARdexr1hjEmWSvWWwC
Customize MFA wherever you go!
Security first - all the way
Account Login
Welcome! Please click login to continue.
Login
Copyright © 2025 Fortinet, Inc. All Rights Reserved.
Terms of Service | Privacy Policy | GDPR

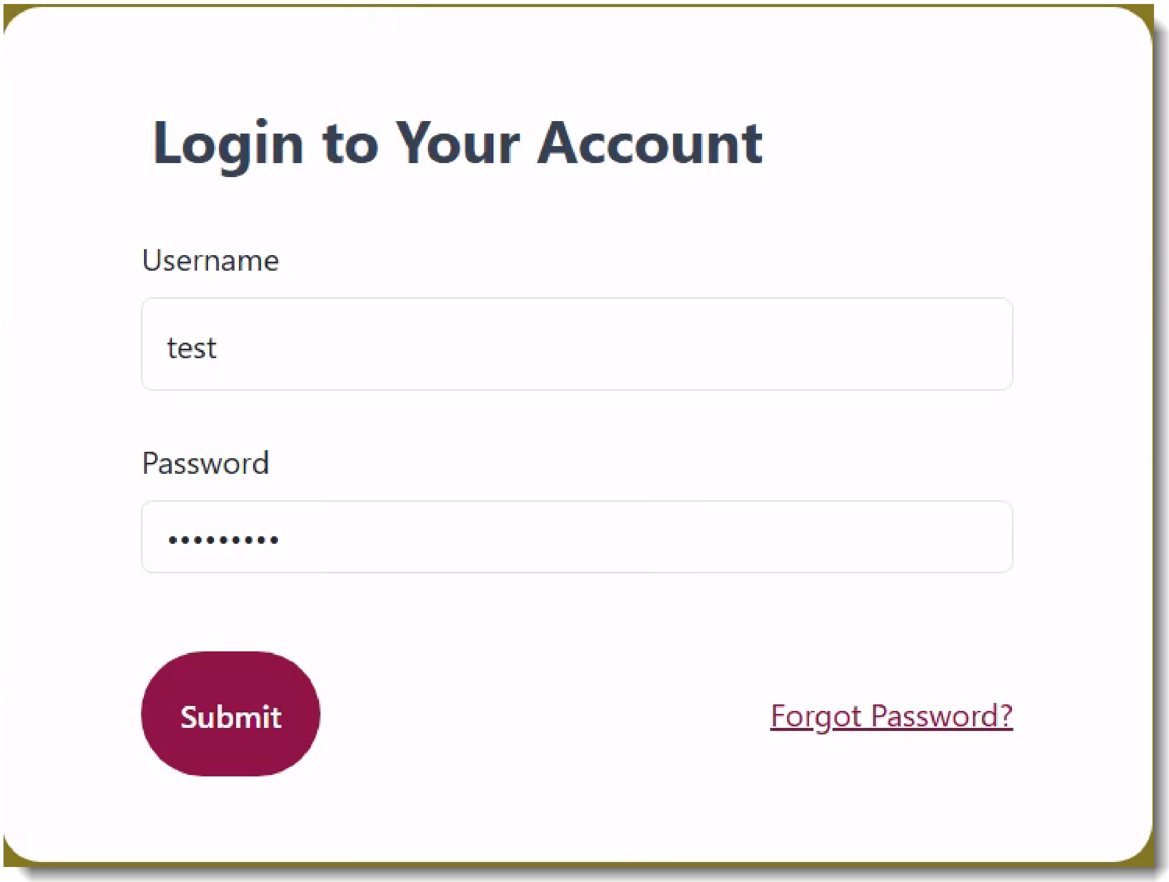
2. Click *Login*.



Enter username to continue

Username: test

3. Enter the *Username*, and click *Submit*.



Login to Your Account

Username

test

Password

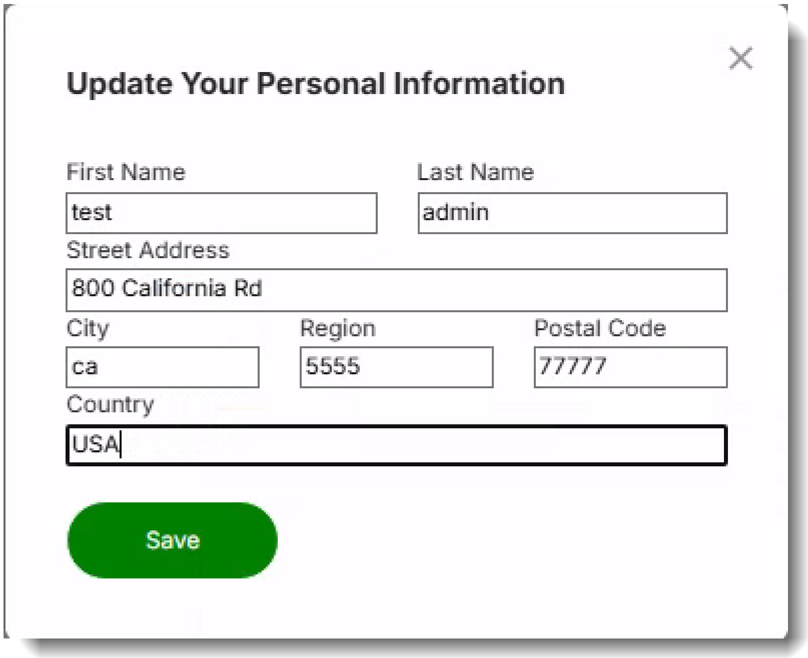
••••••••••

4. Enter the Password, and click *Submit*.
   The user now should be able to log into the portal.

# Updating end-user profile

After logging into the End-user Portal, the user is able to update the user profile on their own.

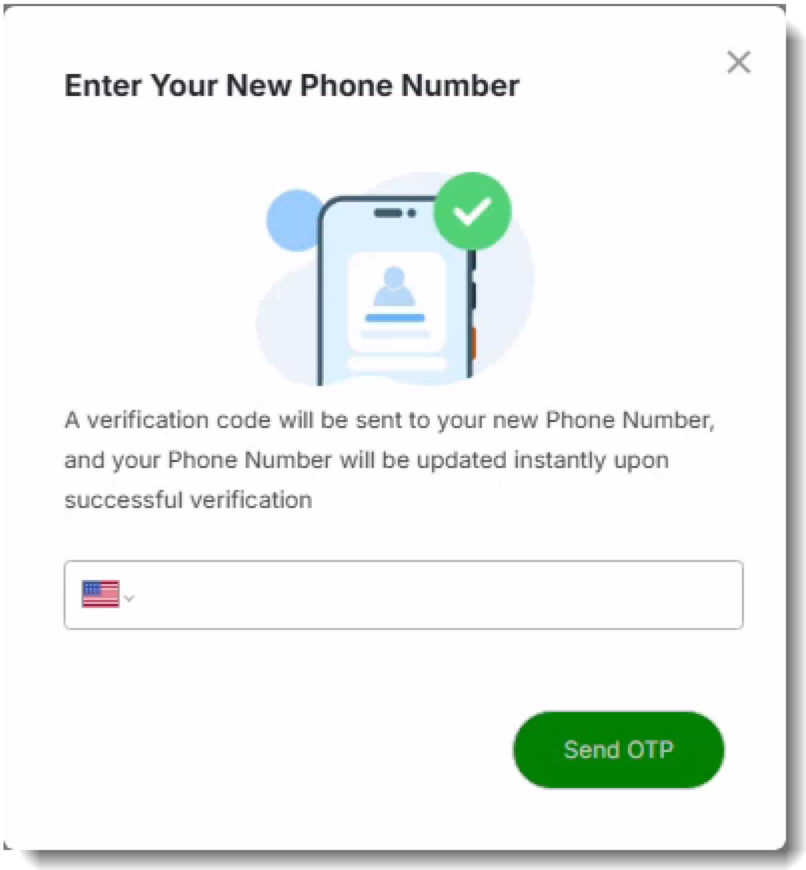
1. On the End-user Portal, click *Profile*.



Update Your Personal Information

| | | |
|---|---|---|
| First Name: test | Last Name: admin | |
| Street Address: 800 California Rd | | |
| City: ca | Region: 5555 | Postal Code: 77777 |
| Country: USA | | |

2. Make the desired changes and click *Save*.
3. To change the phone number, click the pencil icon (Edit) next to the phone number.



Enter Your New Phone Number

A verification code will be sent to your new Phone Number, and your Phone Number will be updated instantly upon successful verification

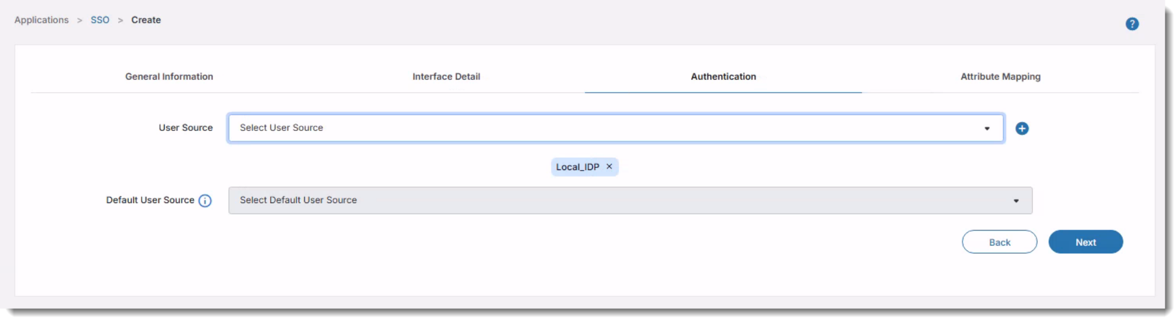
4. Enter the new mobile phone number, and click Send OTP.
5. Validate the OTP to complete updating the phone number.

# Enabling users to access SSO apps

Users of the FIC End-user Portal can access any of the SSO applications that are hosted in the same realm, if the administrator has set the Local IdP as the user source for the SSO applications.

## To enable Local IdP users to access an SSO application:

1. Click *Authentications>SSO>Create*.
2. Click the *Authentication* tab.
3. For *User Source,* select the Local IdP user source of interest.



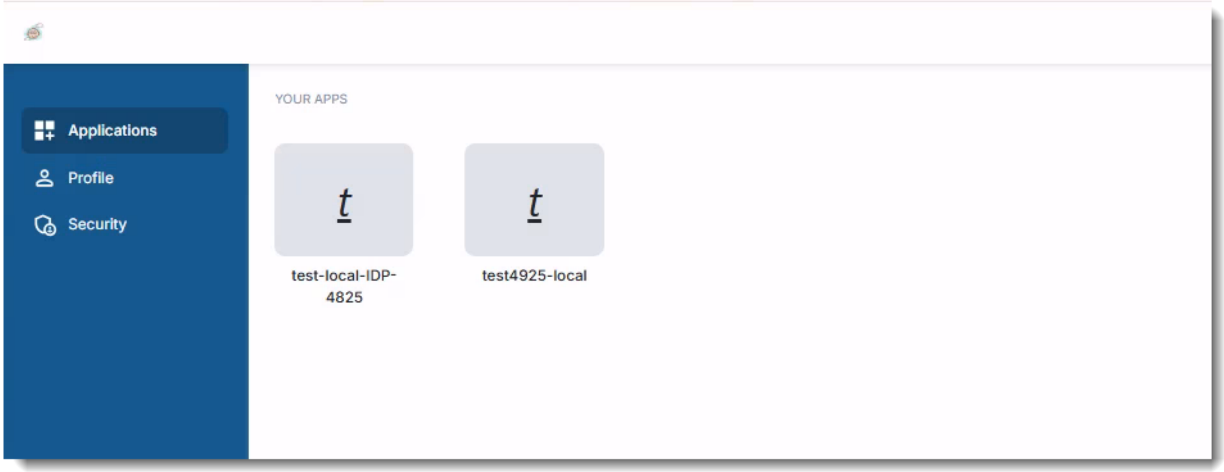
User Source: Select User Source

Local_IDP ×

Default User Source: Select Default User Source

4. Follow the prompts onscreen to complete configuring the SSO application.

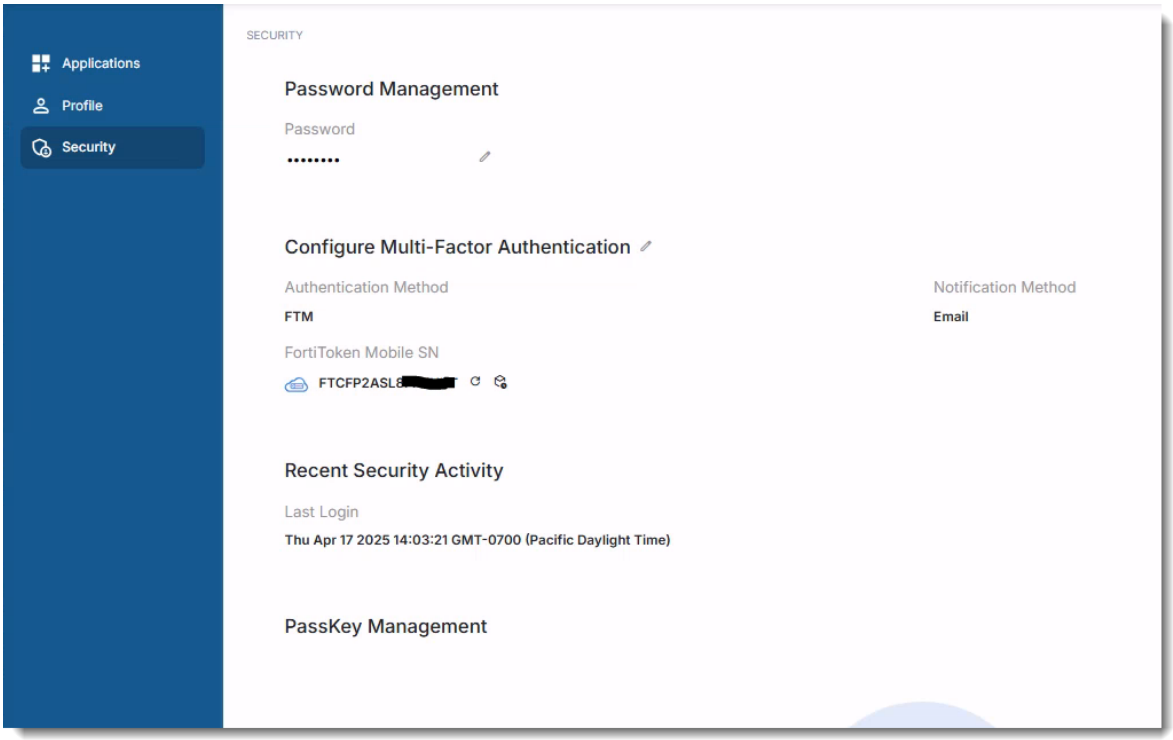
Once the Local IdP has been selected as the user source for the SSO application, the user should be able to access the application from within their End-user Portal under Applications menu, as illustrated in the following screenshot.



# Updating password and authentication method

The user can also change their password and the 2nd factor authentication method directly on the End-user Portal.

1. Click *Security*.



SECURITY

Password Management

Password
••••••••

Configure Multi-Factor Authentication

Authentication Method
FTM

Notification Method
Email

FortiToken Mobile SN
FTCFP2ASL[redacted]

Recent Security Activity

Last Login
Thu Apr 17 2025 14:03:21 GMT-0700 (Pacific Daylight Time)

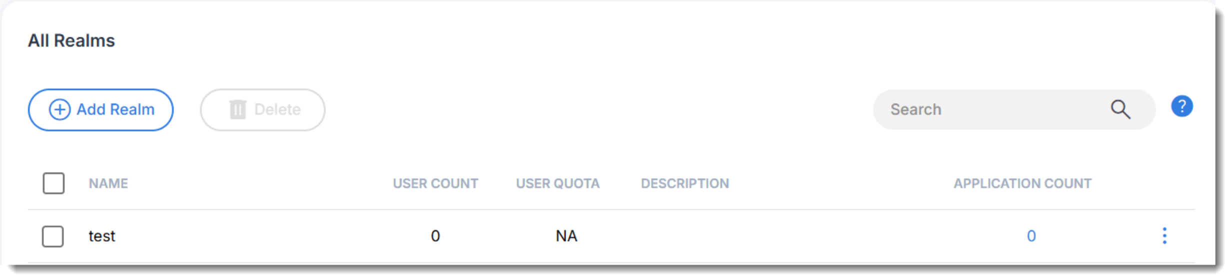
PassKey Management

2. Click the pencil icon (Edit) to *Password*, and enter a new password.
3. Select another authentication method.
4. Click Save.

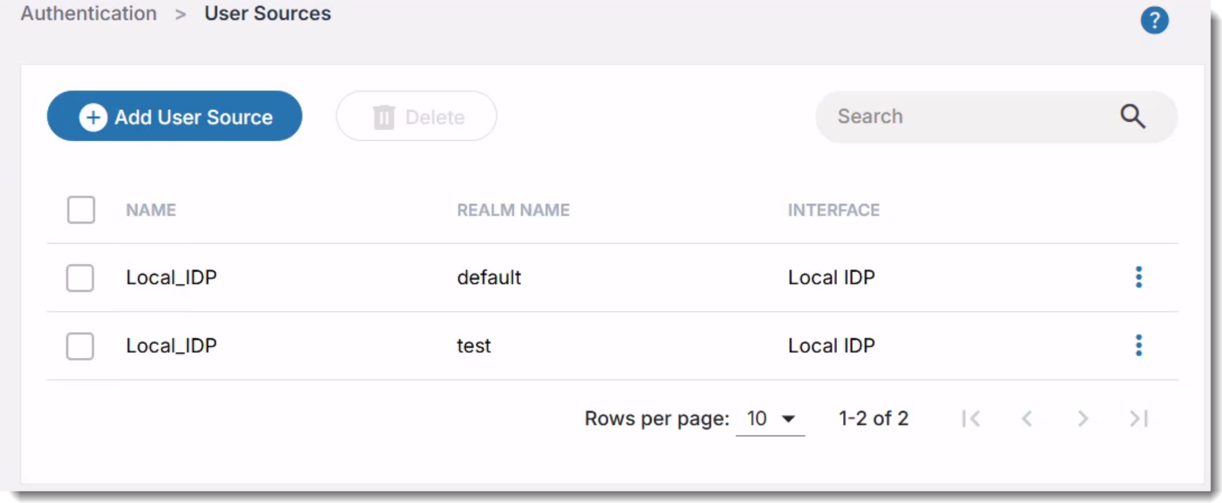
# FortiIdentity Cloud as an IdP for FortiProducts

FortiIdentity Cloud supports local users that are managed locally. This feature enables you to use FIC as the local IdP and activate the 2FA feature for each individual FortiProduct.

For example, you can create a Local IdP for the “test” realm that you created earlier.

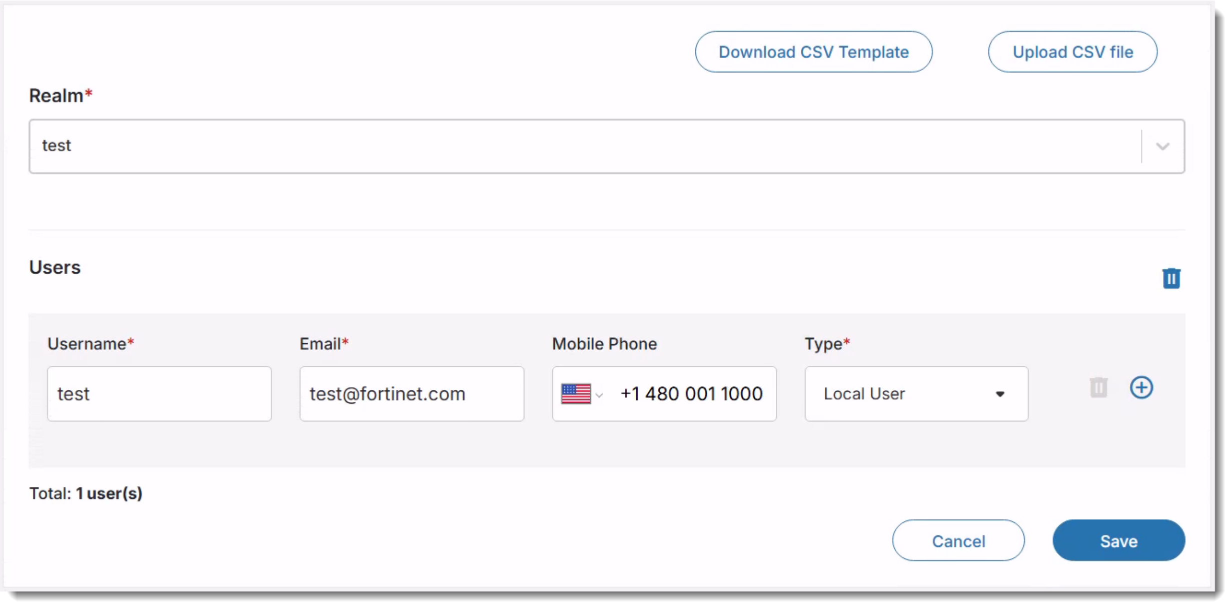


| □ | NAME | USER COUNT | USER QUOTA | DESCRIPTION | APPLICATION COUNT |
|---|---|---|---|---|---|
| □ | test | 0 | NA | | 0 |



| □ | NAME | REALM NAME | INTERFACE |
|---|---|---|---|
| □ | Local_IDP | default | Local IDP |
| □ | Local_IDP | test | Local IDP |

In the example above, a Local_IDP is the user source for authentication to the End-user Portal or any product that supports SSO login. Once a Local_IDP user source is created, you have the option to add local users in the *User Management >Users* page.

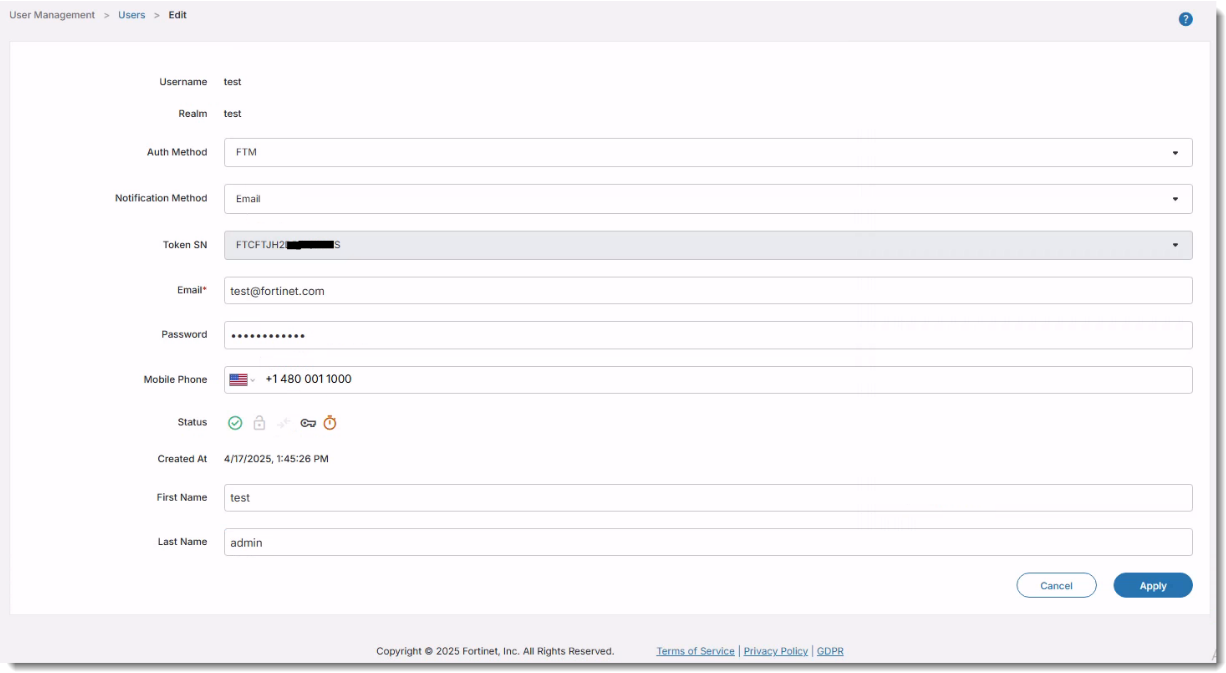


Realm*: test

Users

| Username* | Email* | Mobile Phone | Type* |
|---|---|---|---|
| test | test@fortinet.com | +1 480 001 1000 | Local User |

Total: **1 user(s)**



User Management > Users > Edit

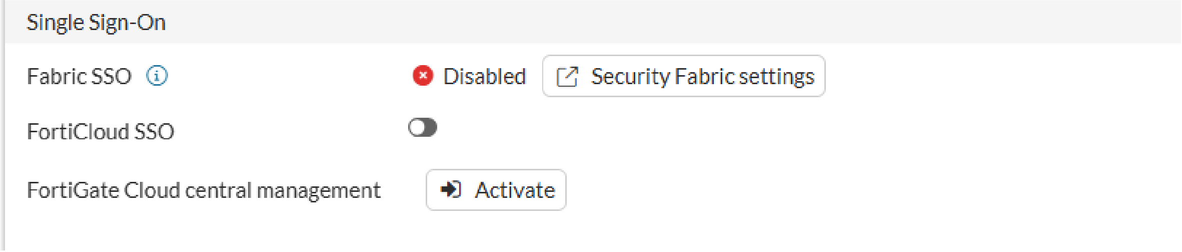
| | |
|---|---|
| Username | test |
| Realm | test |
| Auth Method | FTM |
| Notification Method | Email |
| Token SN | FTCFTJH2[redacted]S |
| Email* | test@fortinet.com |
| Password | •••••••••••• |
| Mobile Phone | +1 480 001 1000 |
| Status | |
| Created At | 4/17/2025, 1:45:26 PM |
| First Name | test |
| Last Name | admin |

Copyright © 2025 Fortinet, Inc. All Rights Reserved. Terms of Service | Privacy Policy | GDPR

Once users are added, you can customize their authentication method (FTK, EMAIL. FTM. SMS, and PASSKEY) for the second factor authentication. For the first factor authentication, both the user and the admin can configure the password on the controller. Local users can modify it on the End-user Portal.

After the local users are added, you can have them log into the SSO applications that are managed under the same realms using the following steps:

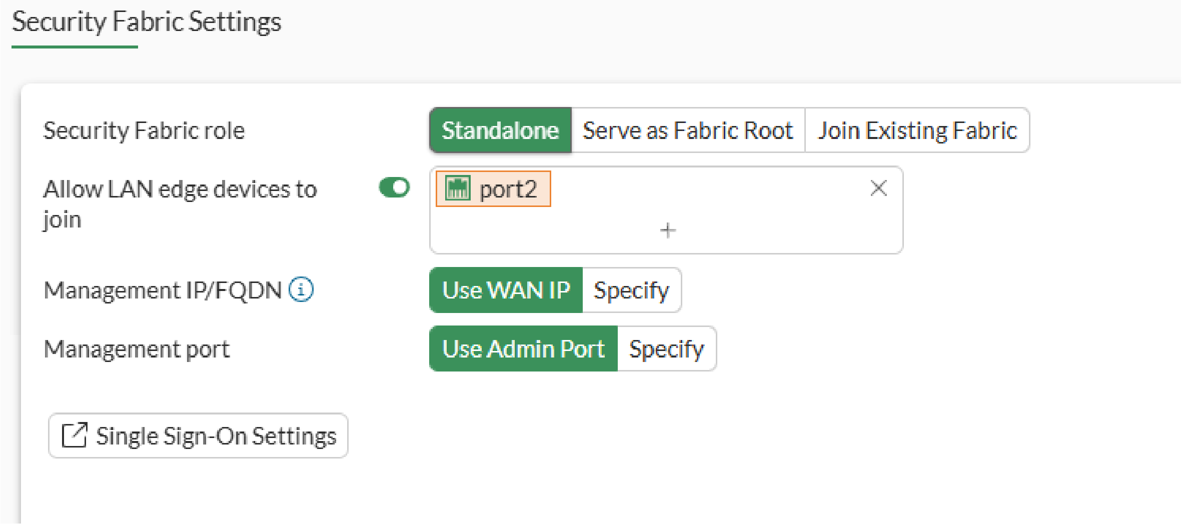
1. On the FortiGate, select the vdom *Global*, and click *Settings*.



Single Sign-On

| | |
|---|---|
| Fabric SSO ⓘ | ✖ Disabled — Security Fabric settings |
| FortiCloud SSO | ○ |
| FortiGate Cloud central management | Activate |

2. Select *Security Fabric Settings*.

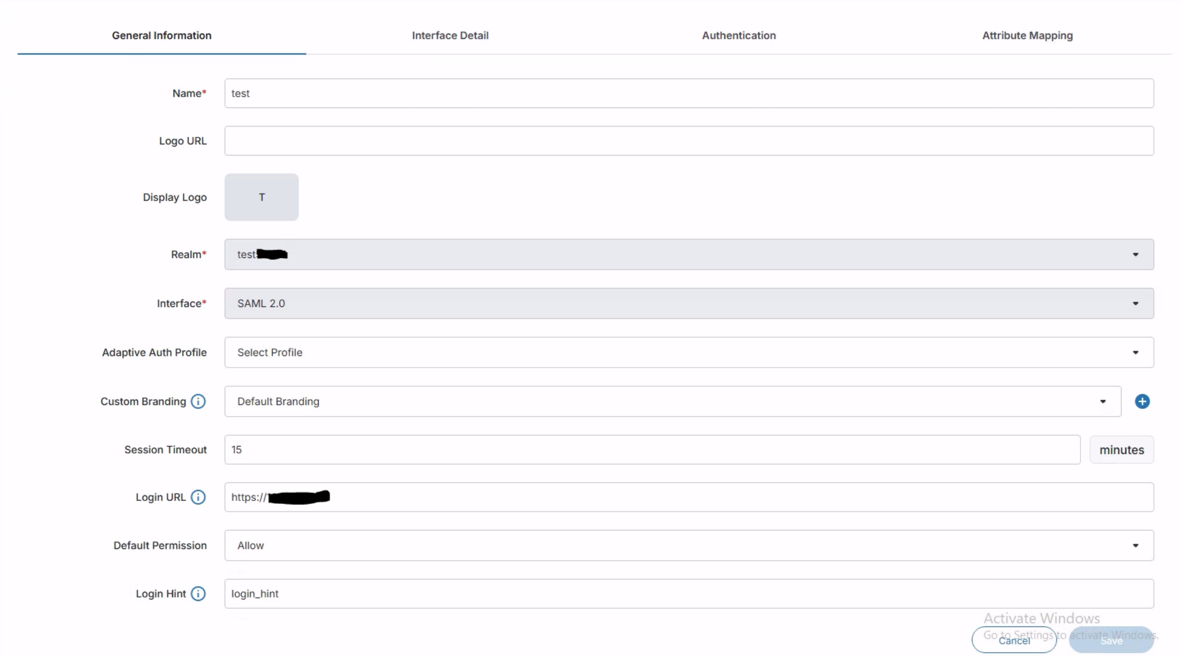


Security Fabric Settings

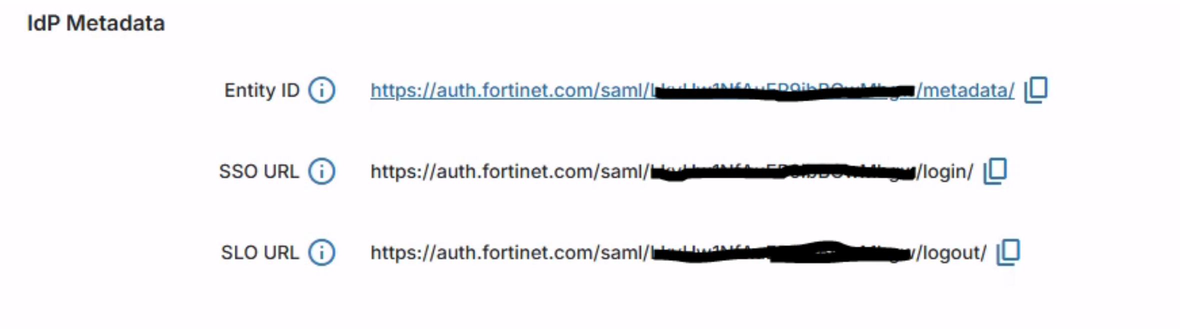
| | |
|---|---|
| Security Fabric role | [✓ Standalone] Serve as Fabric Root Join Existing Fabric |
| Allow LAN edge devices to join | ● port2 |
| Management IP/FQDN ⓘ | [✓ Use WAN IP] Specify |
| Management port | [✓ Use Admin Port] Specify |

Single Sign-On Settings

3. Click Single Sign-On Settings, and enter all the details for the IdP setting from the FIC portal under the SSO application that you have created for the application login.
4. Collect the SP Metadata details from the FortiGate and add them to the FIC SSO application configuration, along with the login URL for authentication.



| | |
|---|---|
| Name* | test |
| Logo URL | |
| Display Logo | T |
| Realm* | test[redacted] |
| Interface* | SAML 2.0 |
| Adaptive Auth Profile | Select Profile |
| Custom Branding ⓘ | Default Branding |
| Session Timeout | 15 minutes |
| Login URL ⓘ | https://[redacted] |
| Default Permission | Allow |
| Login Hint ⓘ | login_hint |



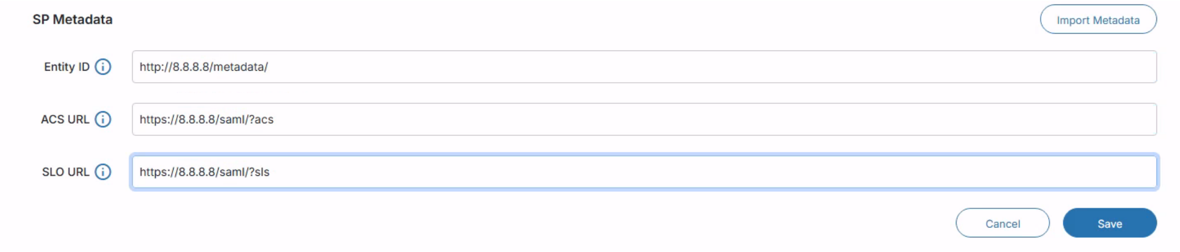
IdP Metadata

Entity ID: https://auth.fortinet.com/saml/[redacted]/metadata/

SSO URL: https://auth.fortinet.com/saml/[redacted]/login/

SLO URL: https://auth.fortinet.com/saml/[redacted]/logout/

5. Enter the SP Metadata details that are collected from the FortiGate, and copy the IdP Metadata details to the FortiGate as show in the following screenshot.

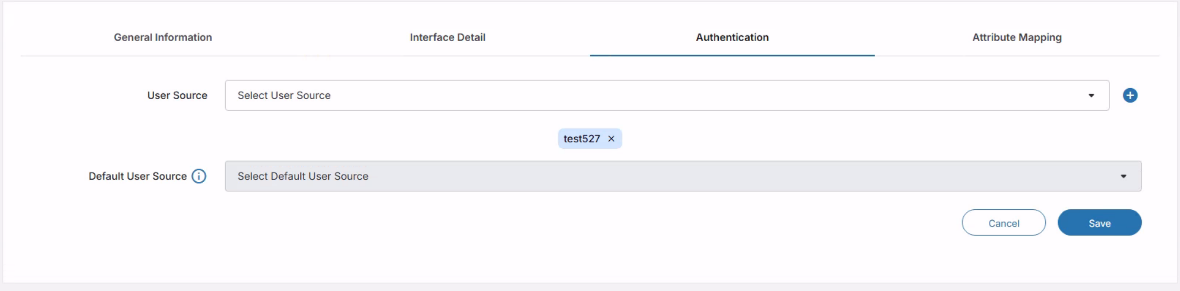


SP Metadata

Entity ID: http://8.8.8.8/metadata/

ACS URL: https://8.8.8.8/saml/?acs

SLO URL: https://8.8.8.8/saml/?sls

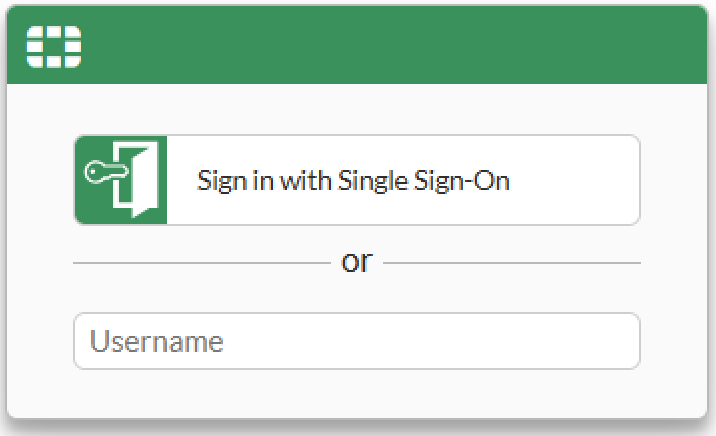


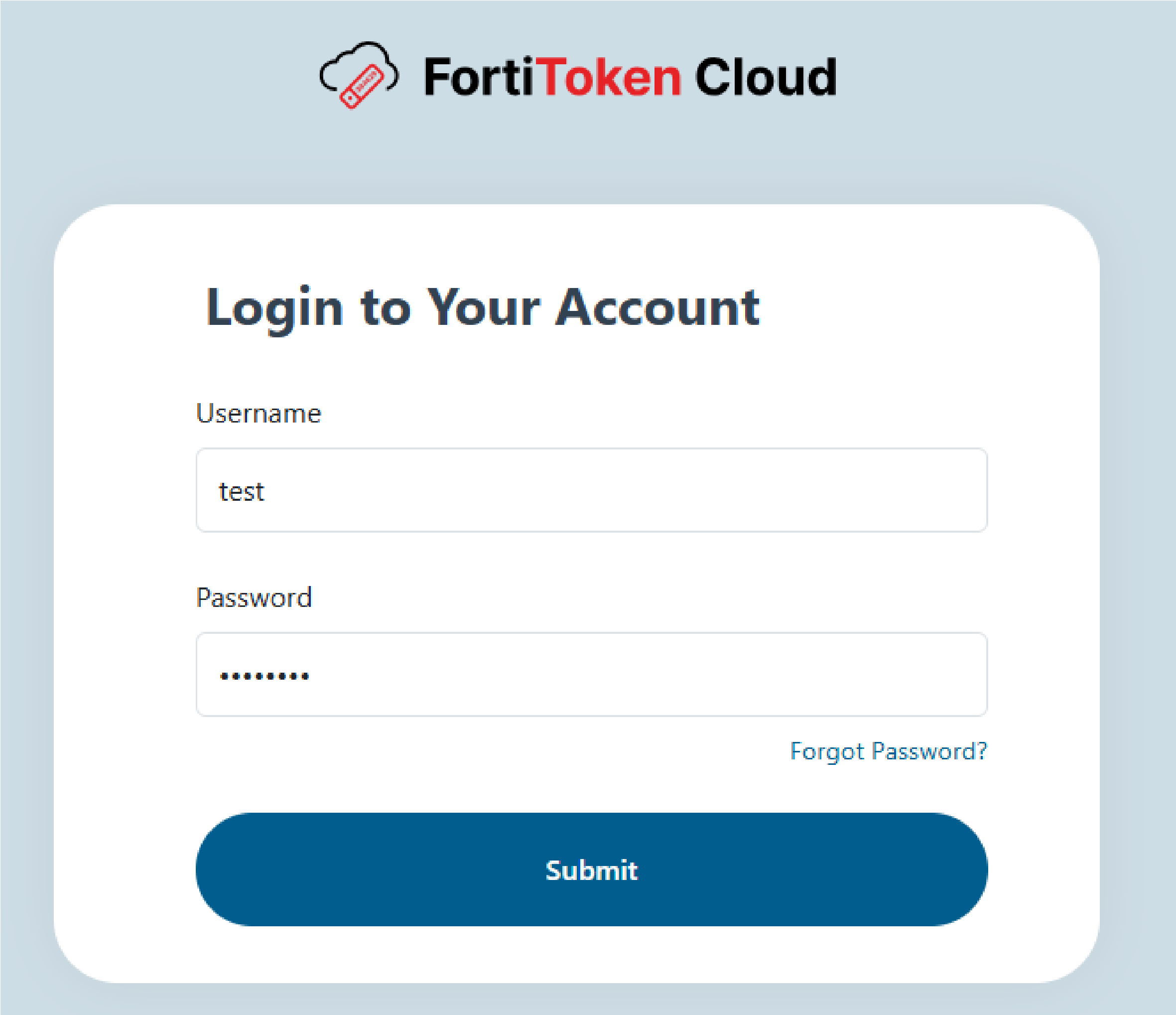
User Source: Select User Source

test527 ×

Default User Source: Select Default User Source

6. Once the configuration is completed, log into the FortiGate using the local user that is configured in the FIC portal.





Login to Your Account

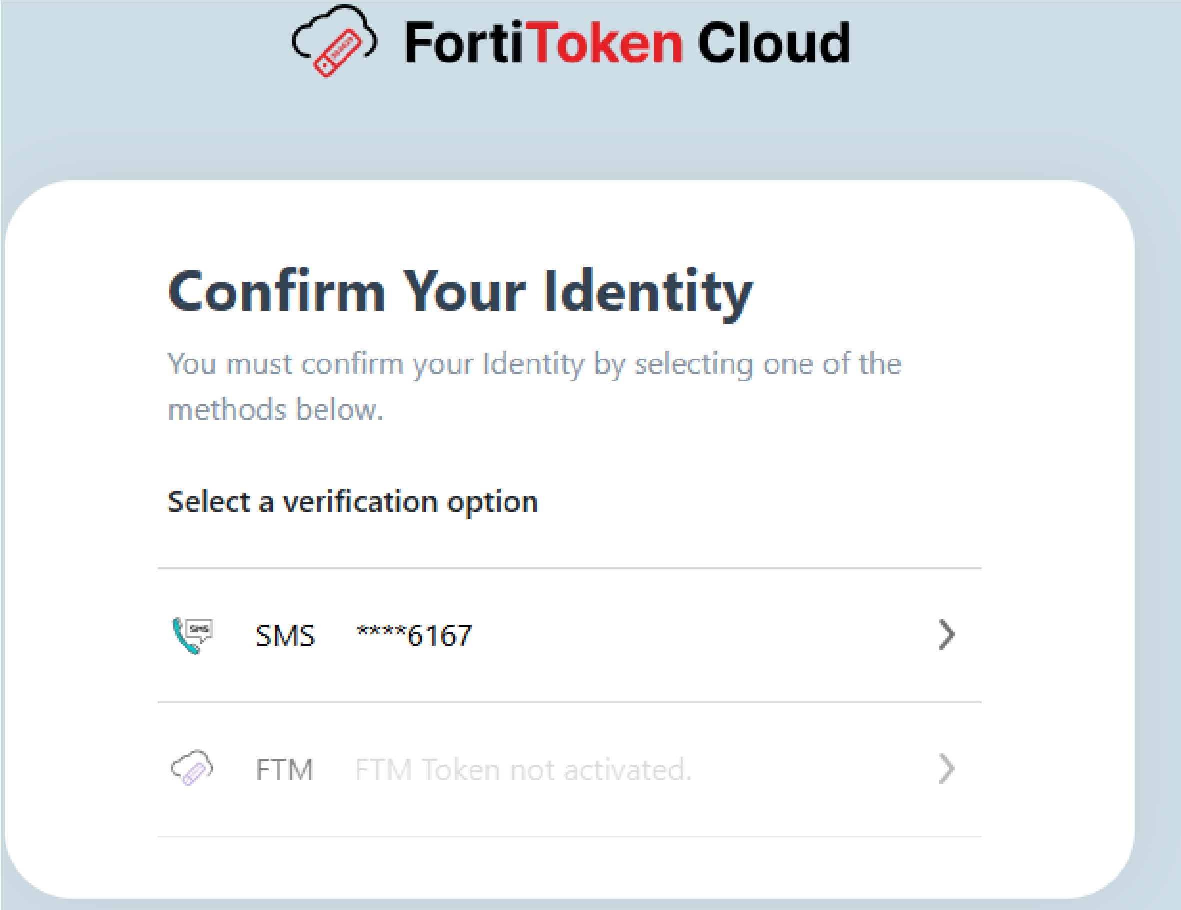
Username

test

Password

•••••••••

7. Enter the Local IDP user's credentials, and select the MFA method to authenticate to the FortiGate.



Confirm Your Identity

You must confirm your Identity by selecting one of the methods below.

Select a verification option

SMS ****6167

FTM FTM Token not activated.

# Change Log

| Date | Description |
|---|---|
| December 7, 2025 | Initial release. |

FURTINET®

www.fortinet.com