

Local IdP

Fortidentity Cloud 26.2



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

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

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



May 1, 2026

Fortidentity Cloud 26.2 Local IdP

TABLE OF CONTENTS

Local IdP in Fortidentity Cloud	4
Adding a Local IdP	5
Adding users to the local IdP	6
Setting End-User Portal password policy	10
Logging into FIC End-User Portal	11
Updating end-user profile	14
Enabling users to access SSO apps	16
Updating password and authentication method	17
Fortidentity Cloud as an IdP for FortiProducts	18
Change Log	24

Local IdP in Fortidentity Cloud

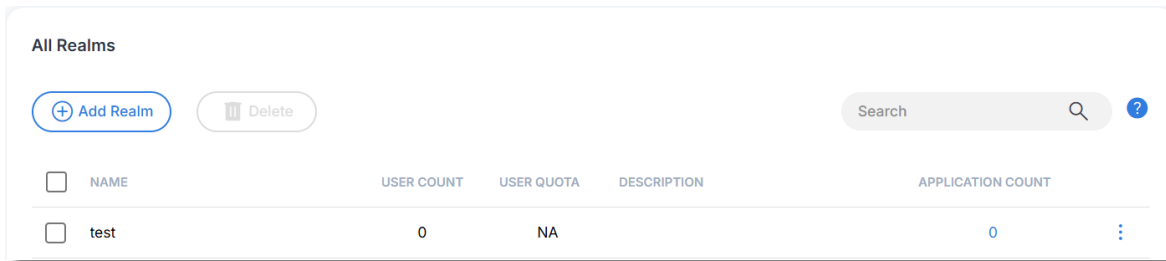
In Fortidentity Cloud, local IdP means that the user identity (username and password) is local to Fortidentity Cloud and is not from any external identity provider, such as Google, Azure, etc.

Adding a Local IdP

In Fortidentity 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 Fortidentity 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.



Adding users to the local IdP

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

Download CSV Template Upload CSV file

Realm*
test

Users

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

Total: 1 user(s)

Cancel Save

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*.

User Management > Users > Edit

Username test

Realm test

Auth Method FTM

Notification Method Email

Token SN FTCFTJH2...

Email* test@fortinet.com

Password

Mobile Phone +1 480 001 1000

Status Active

Created At 4/17/2025, 1:45:26 PM

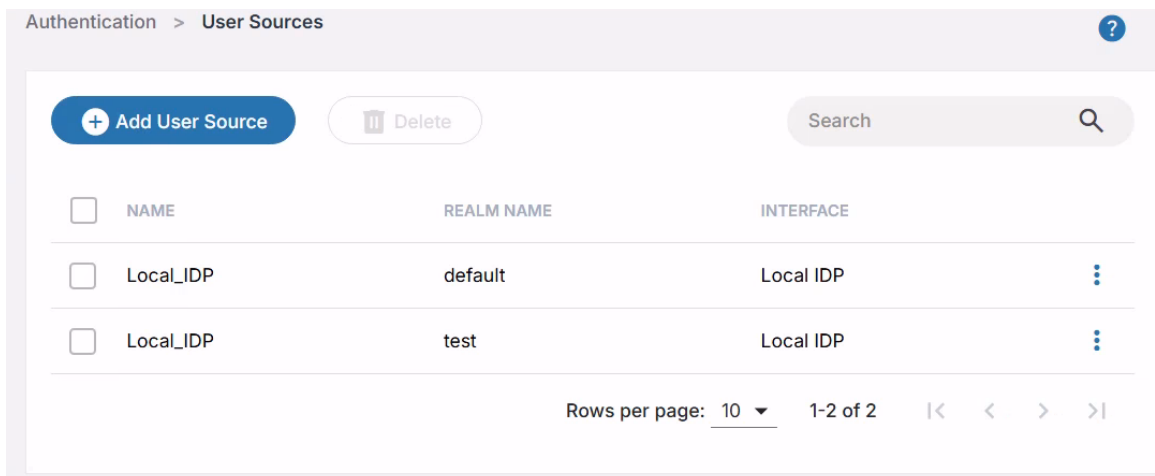
First Name test

Last Name admin

Cancel Apply

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 Fortidentity Cloud has automatically created for the "test" realm when a local user is created under "test" realm.

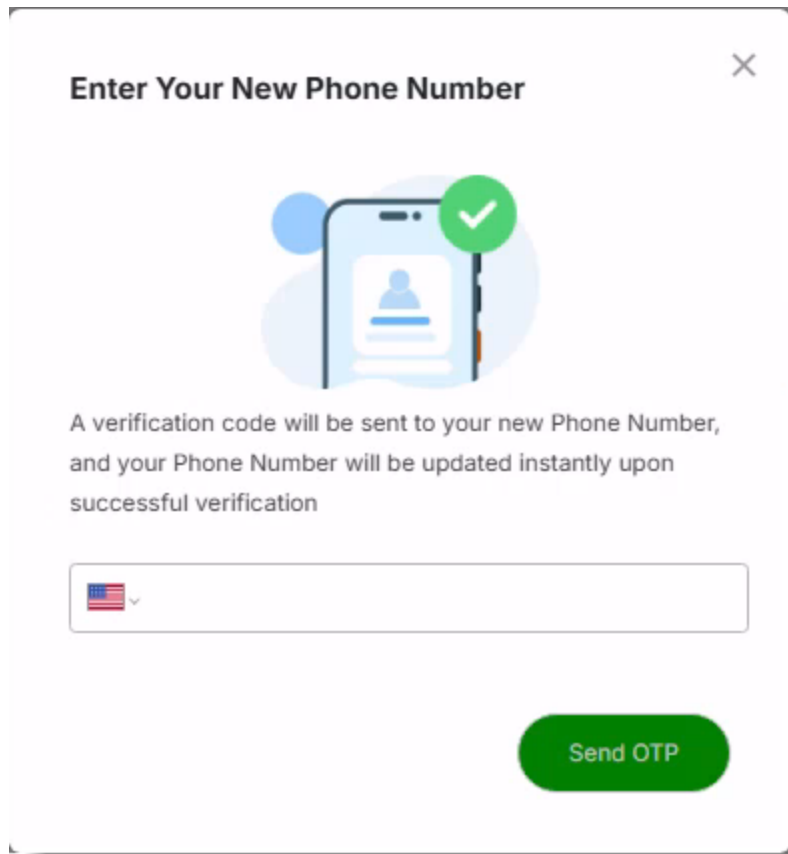


- 5. Set the user's Auth Method, and click *Apply*.

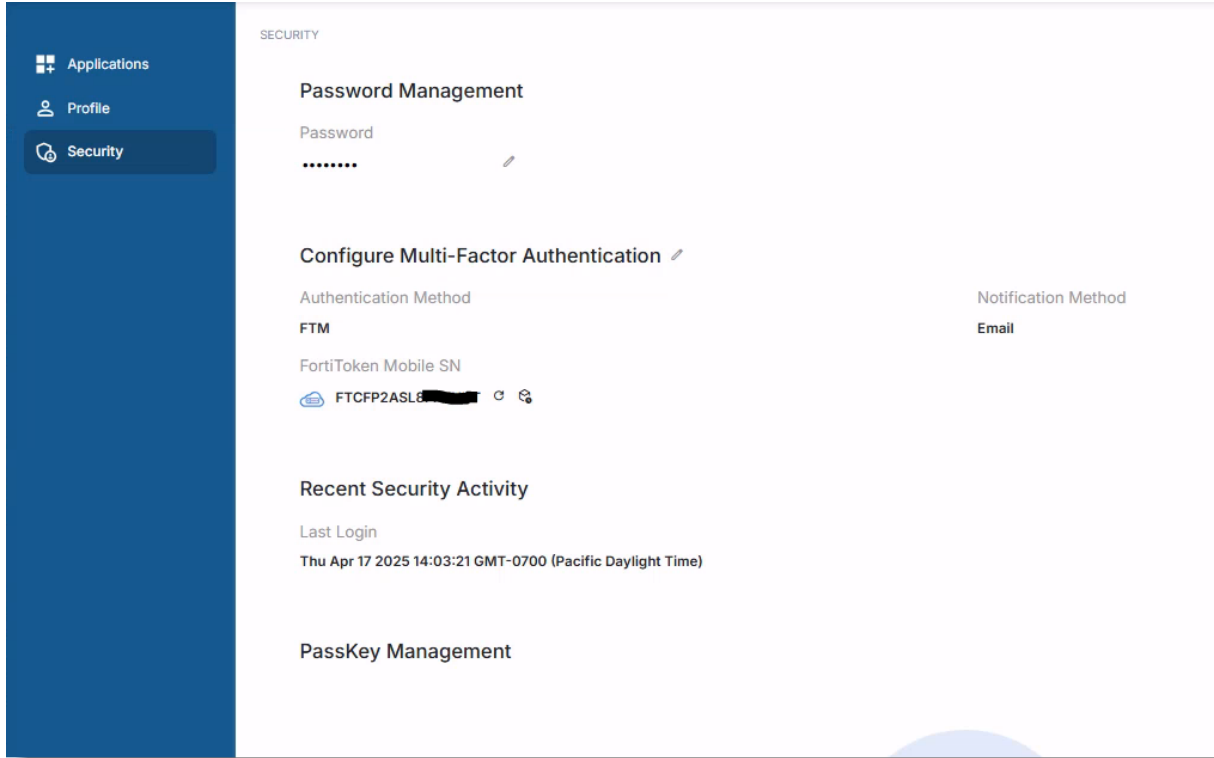


At this point, the user has been added to the local IdP user source, and should be able to authenticate to the Fortidentity Cloud End-User Portal with the 1st-factor authentication (i.e., username & password) and the 2nd-factor authentication (i.e., FTK, FTM, EMAIL, SMS, or Passkey).

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



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

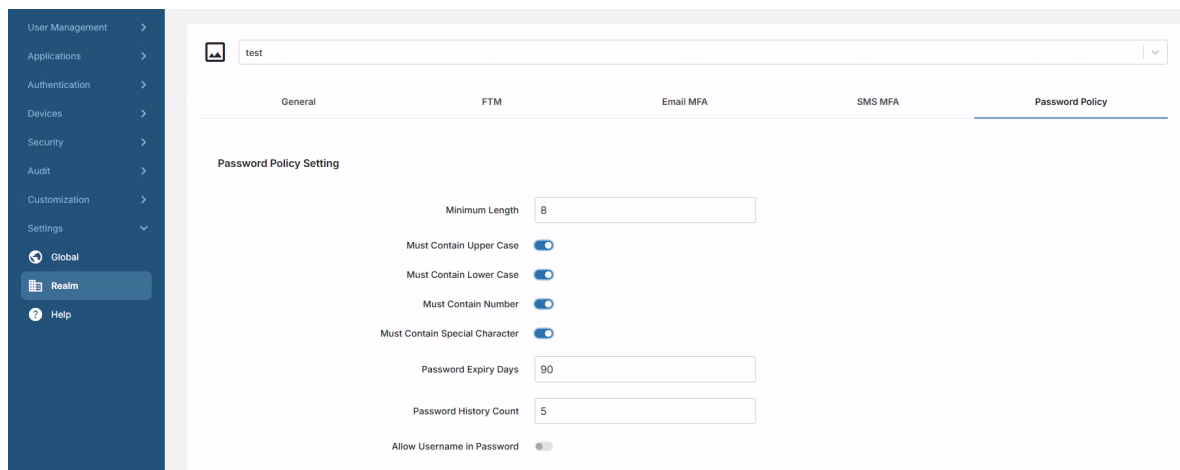


Setting End-User Portal password policy

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:

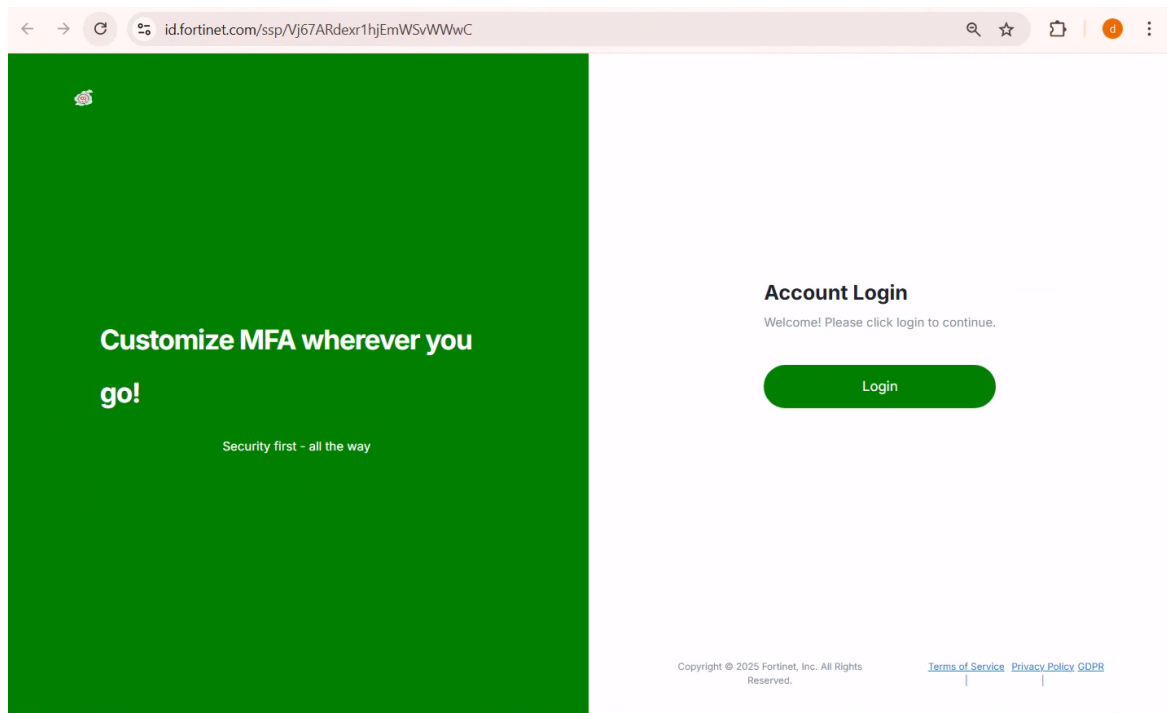
1. Click *Settings>Realm*.
2. Select the realm of interest, and click *Password Policy*.
3. Make the desired entries or selections, and click *Apply Changes*.



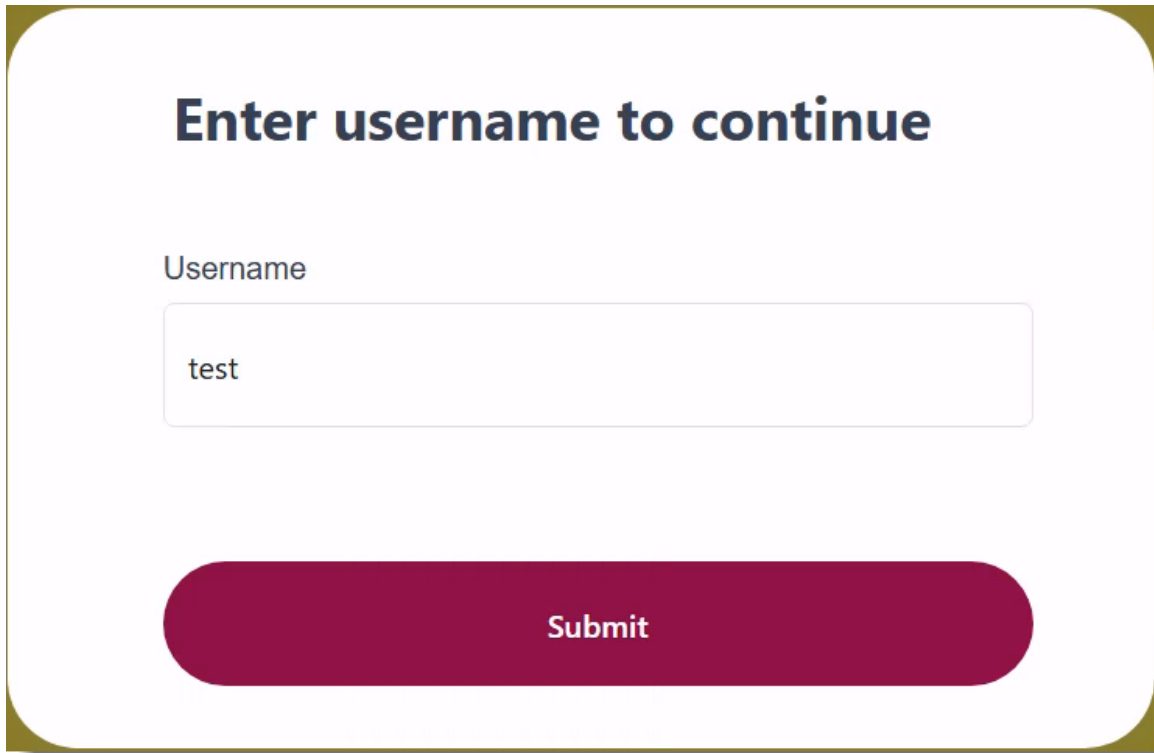
Logging into FIC End-User Portal

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

1. Launch the *End-User Portal*.



2. Click *Login*.



Enter username to continue

Username

Submit

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

Login to Your Account

Username

Password

Submit

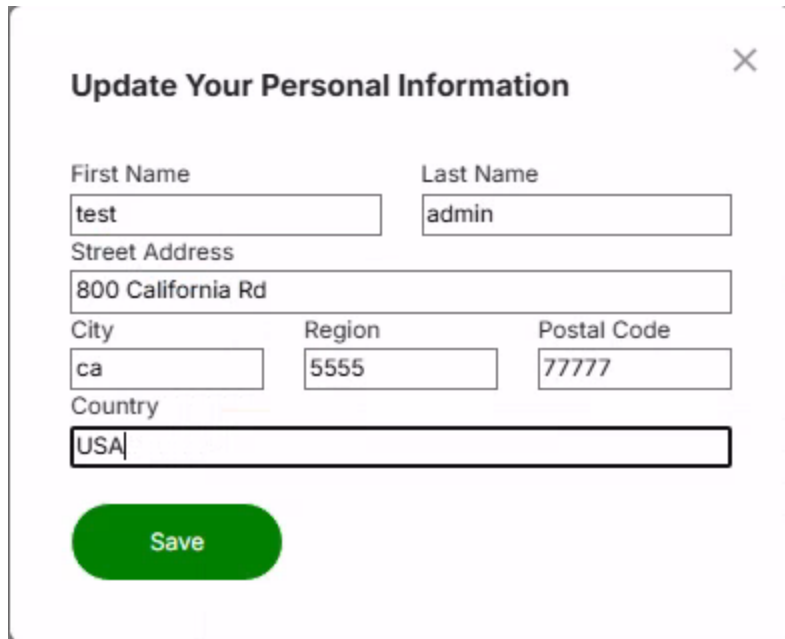
[Forgot Password?](#)

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 Last Name


Street Address

City Region Postal Code

Country

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

Send OTP

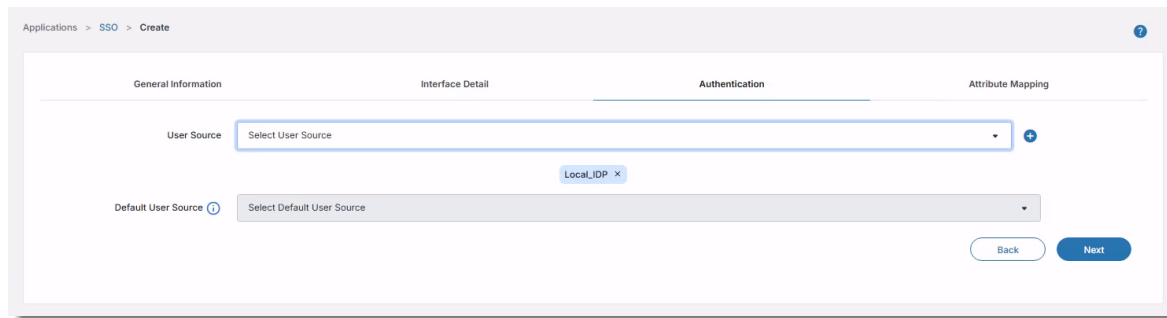
4. Enter the new mobile phone number, and click Send OTP.
5. Validate the OTP to complete updating the phone number.

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.

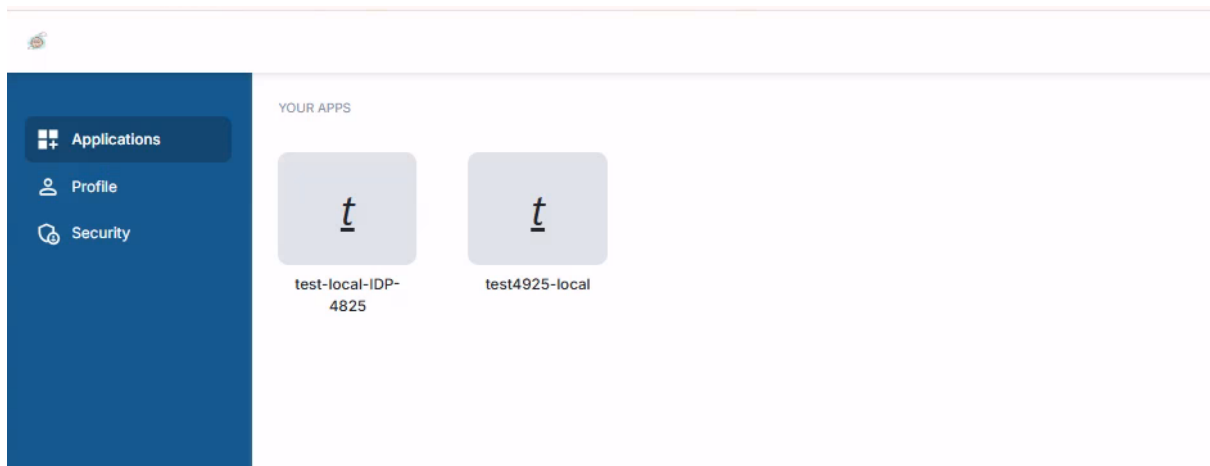
To enable Local IdP users to access an SSO application:

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



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

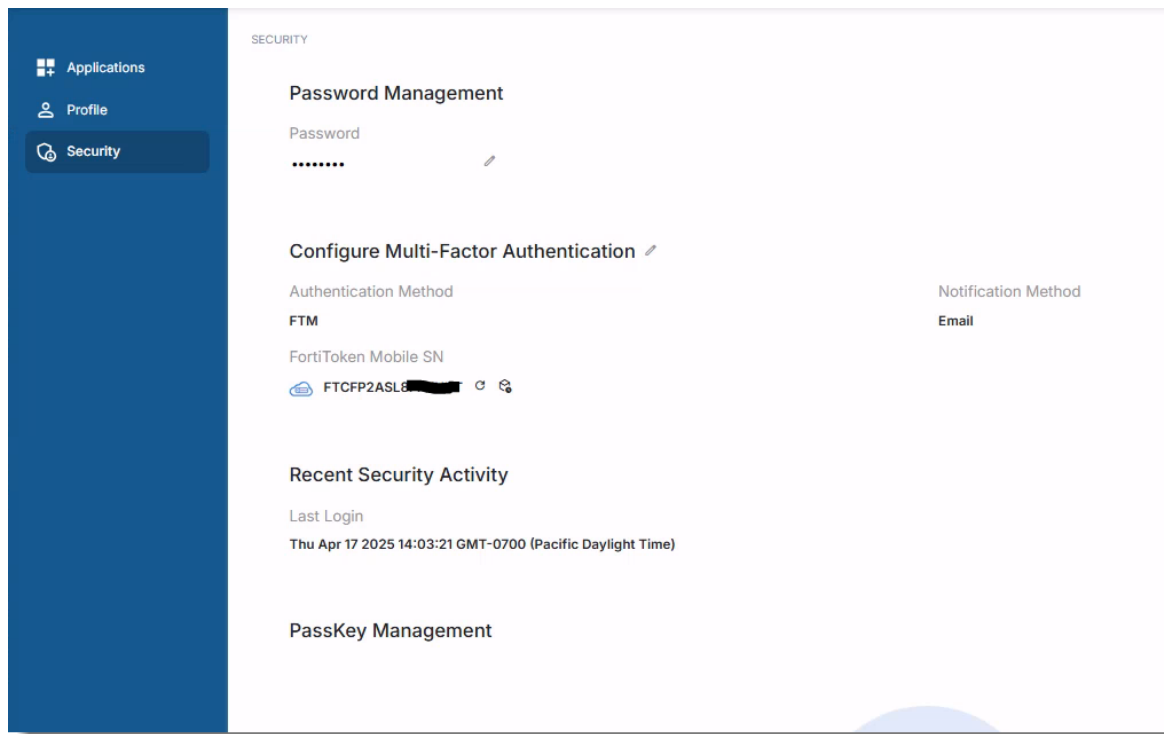
Once the Local IdP has been selected as the user source for the SSO application, the user should be able to access the application from within their End-User Portal under Applications menu, as illustrated in the following screenshot.



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*.



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

Fortidentity Cloud as an IdP for FortiProducts

Fortidentity 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.

The image shows two screenshots of the Fortidentity Cloud management interface. The top screenshot displays the 'All Realms' page, which includes a table with columns for NAME, USER COUNT, USER QUOTA, DESCRIPTION, and APPLICATION COUNT. A single realm named 'test' is listed with 0 users and a quota of NA. The bottom screenshot shows the 'Authentication > User Sources' page, which includes a table with columns for NAME, REALM NAME, and INTERFACE. Two 'Local_IDP' user sources are listed, one for the 'default' realm and one for the 'test' realm. Both are associated with the 'Local IDP' interface.

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.

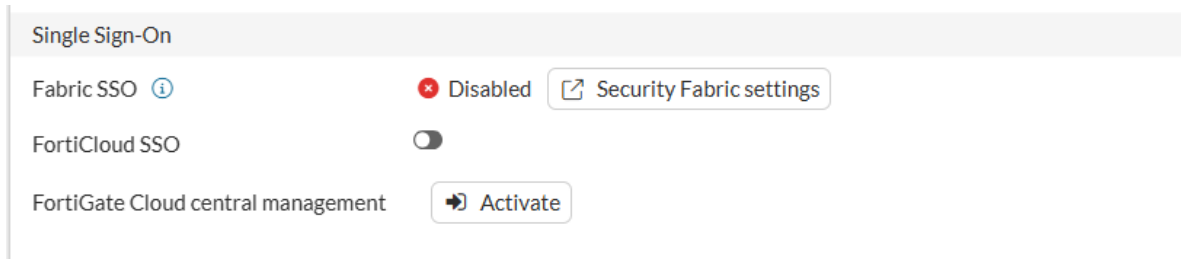
The screenshot shows the 'Users' management interface. At the top right, there are buttons for 'Download CSV Template' and 'Upload CSV file'. Below this is a 'Realm*' dropdown menu with 'test' selected. The main section is titled 'Users' and contains a table with columns for 'Username*', 'Email*', 'Mobile Phone', and 'Type*'. The 'test' user is listed with email 'test@fortinet.com' and mobile phone '+1 480 001 1000'. The 'Type*' is set to 'Local User'. At the bottom left, it says 'Total: 1 user(s)'. At the bottom right, there are 'Cancel' and 'Save' buttons.

The screenshot shows the 'Edit' form for a user. The breadcrumb navigation is 'User Management > Users > Edit'. The form fields are: Username (test), Realm (test), Auth Method (FTM), Notification Method (Email), Token SN (FTCFTJH2...), Email* (test@fortinet.com), Password (masked with dots), Mobile Phone (+1 480 001 1000), Status (Active), Created At (4/17/2025, 1:45:26 PM), First Name (test), and Last Name (admin). At the bottom right, there are 'Cancel' and 'Apply' buttons. At the bottom of the page, there is a copyright notice: 'Copyright © 2025 Fortinet, Inc. All Rights Reserved.' and links for 'Terms of Service', 'Privacy Policy', and 'GDPR'.

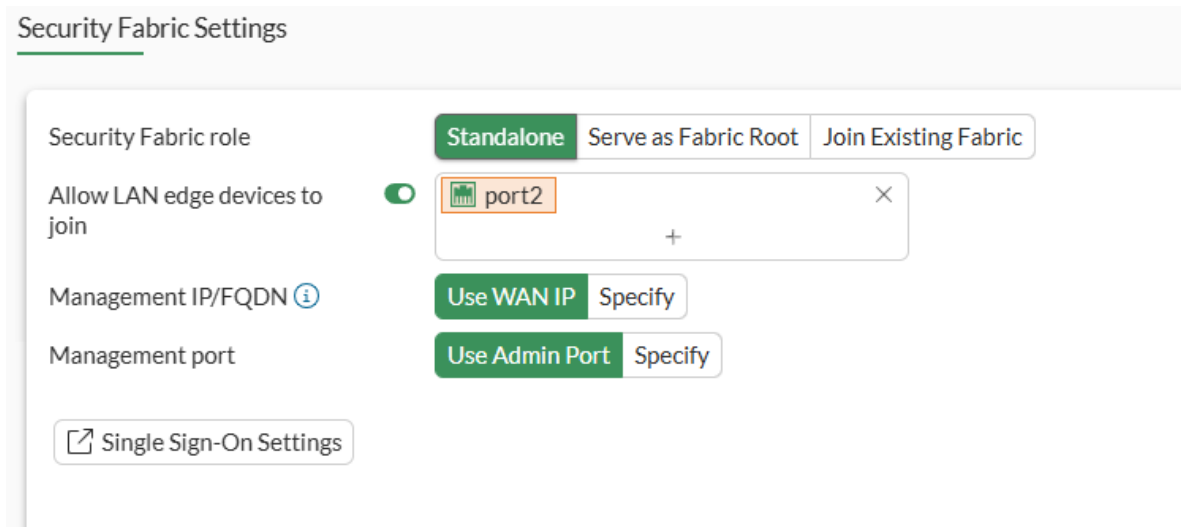
Once users are added, you can customize their authentication method (FTK, EMAIL, FTM, SMS, and PASSKEY) for the second factor authentication. For the first factor authentication, both the user and the admin can configure the password on the controller. Local users can modify it on the End-User Portal.

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:

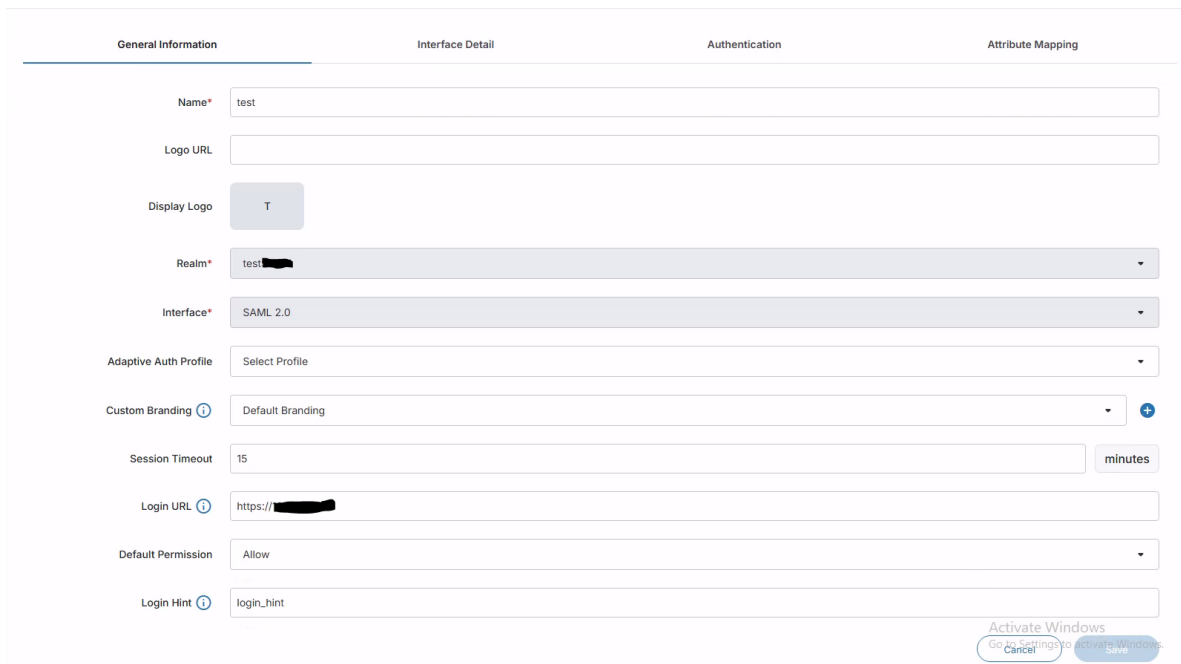
1. On the FortiGate, select the vdom *Global*, and click *Settings*.

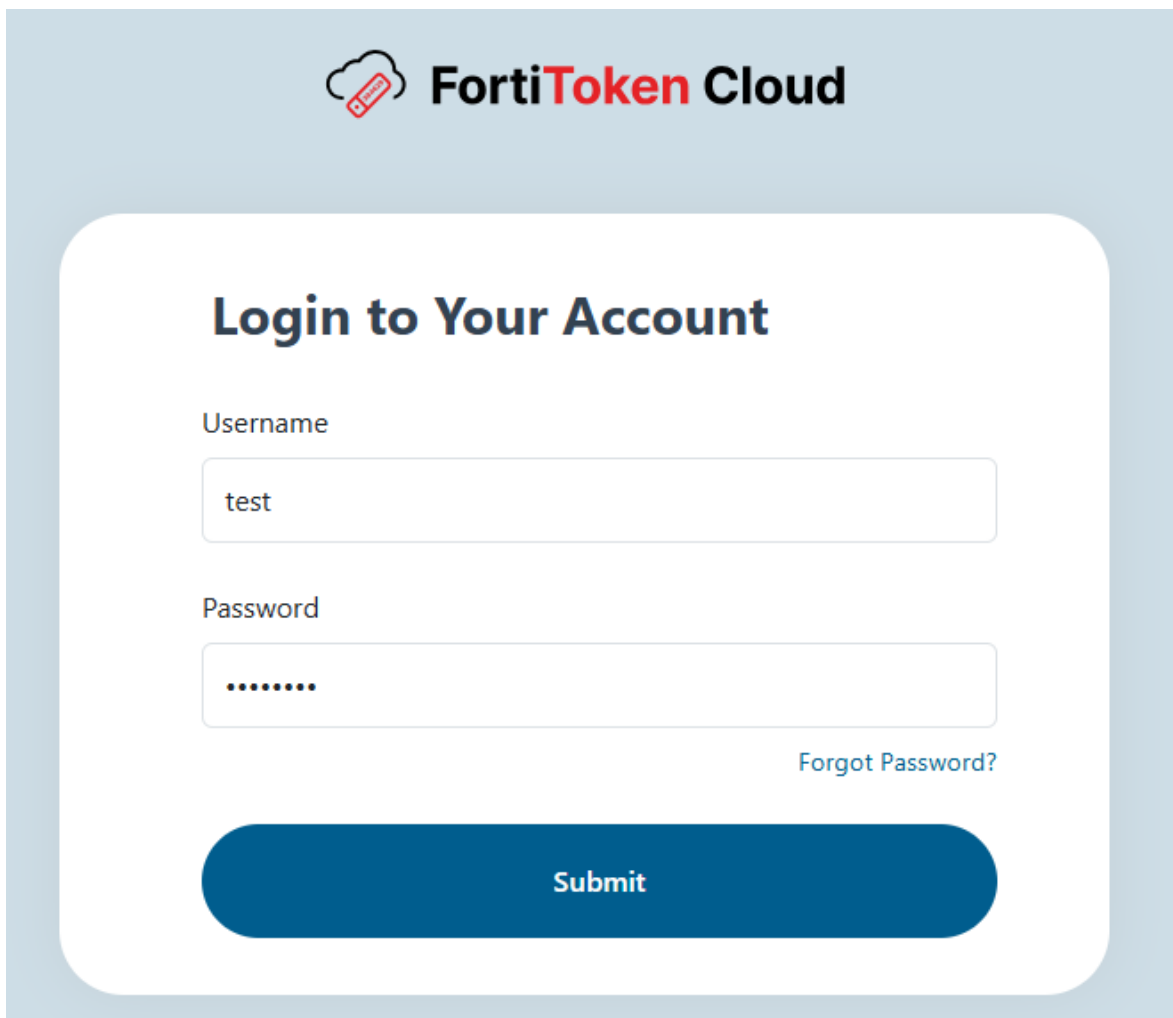



2. Select *Security Fabric Settings*.



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.





 **FortiToken Cloud**

Login to Your Account

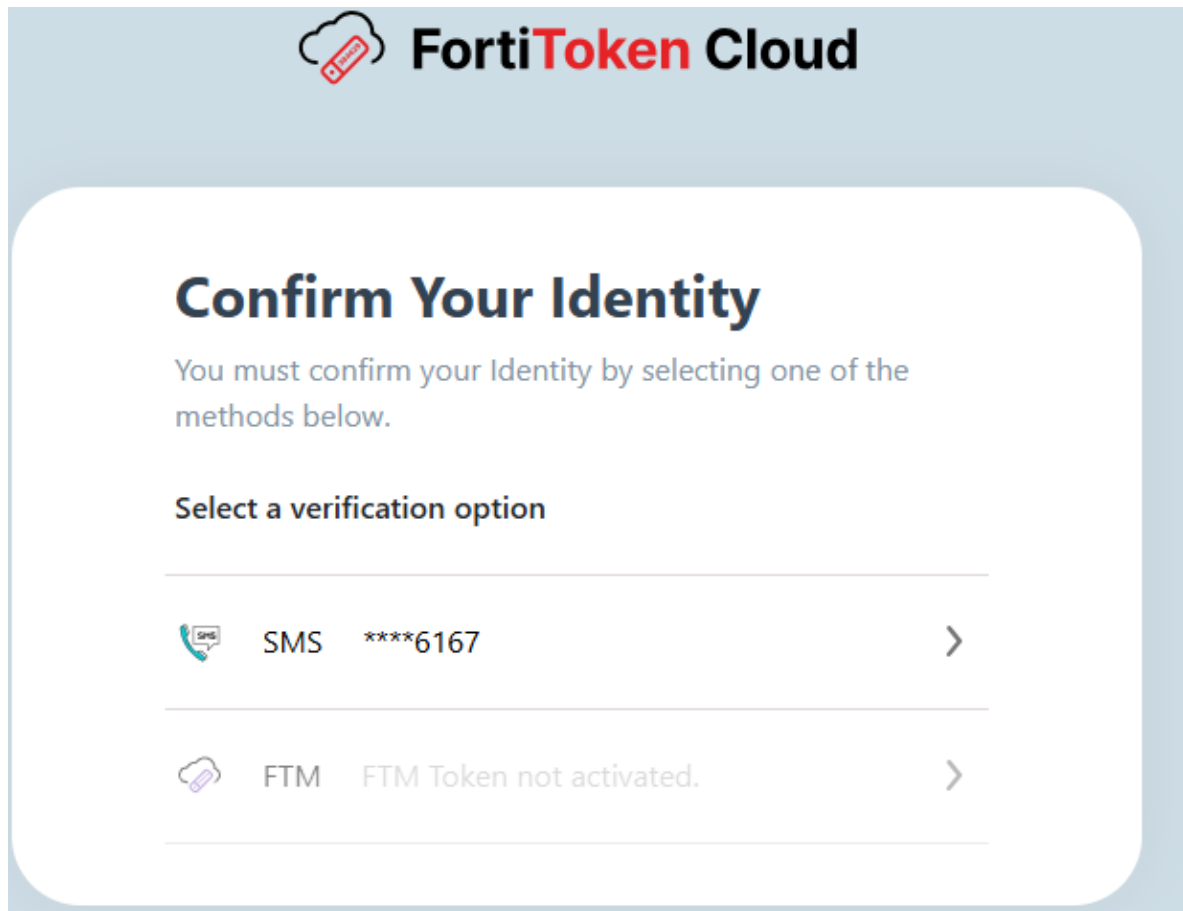
Username

Password

[Forgot Password?](#)

Submit

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



Change Log

Date	Description
May 1, 2026	Initial release.



www.fortinet.com

Copyright© 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.