Traverse Two-Factor Authentication

User Guide | August 2020

Traverse Two-Factor Authentication

Release 9.5.28 | Version 1.0

www.kaseya.com

Copyright Agreement

This page is intentionally left blank.

Contents

Chapter 1: Two-Factor Authentication

Two-factor authentication in Traverse has been designed to provide an extra level of authentication and security. The feature is meant to prevent unauthorized users from accessing Traverse account data.

About 2FA

Enabled 2FA feature obliges a user to provide not only the credentials (username and password), but to submit a Time-based, One-Time Password (TOTP) in order to access the Traverse account.

TOTP is an authorization code generated by an Authenticator application and is valid for a limited time. We recommend using the following Authenticator applications:

- Google Authenticator
- Microsoft Authenticator
- Passly Authenticator

Note: The Authenticator should be configured prior to enrolling into 2FA in Traverse. (See Authenticator application Set up and Configuration for Traverse 2FA for more information on the Authentication application configuration.)

Authenticator application Set up and Configuration for Traverse 2FA

Authenticator application is a software designed to generate Time-based, One-Time passwords (TOTP). The TOTP is used as a separate verification step in the 2-factor authentication process to login Traverse application.

To have the Authenticator application generate the TOTP for Traverse application, users have to add the Traverse account to the Authenticator application during the 2FA enrollment process only. Afterwards, Authenticator application will automatically generate authorization codes for user's subsequent logins.

Authenticator application for mobile devices

To set up a mobile Authenticator app, please follow the following steps:

1. Download and install one of the following applications in App Store for MacOS and in Google Play for Android OS:

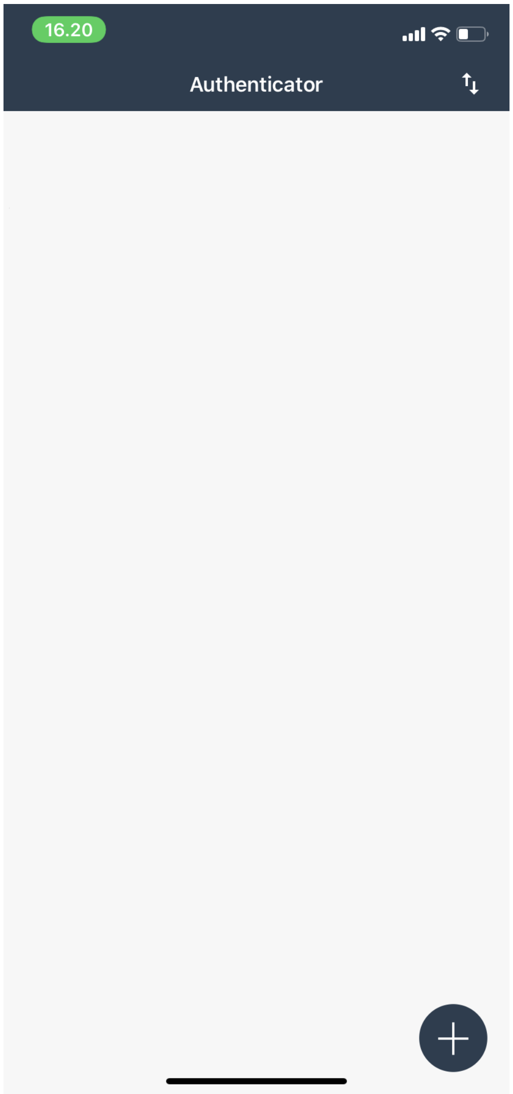
   MacOS:

   - Google Authenticator: https://apps.apple.com/us/app/google-authenticator/id388497605
   - Microsoft Authenticator: https://apps.apple.com/app/microsoft-authenticator/id983156458
   - Passly Authenticator: https://apps.apple.com/us/app/passly-authenticator/id1506832710

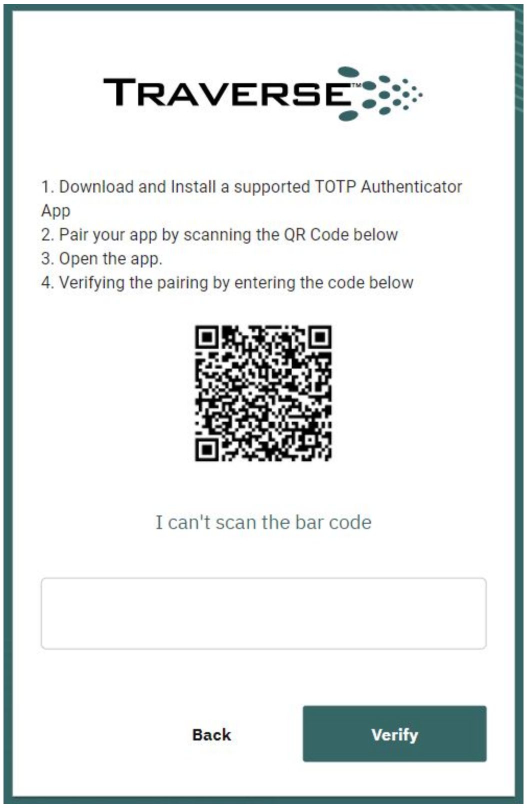
   Android:

   - Google Authenticator: https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2
   - Microsoft Authenticator: https://play.google.com/store/apps/details?id=com.azure.authenticator&hl=en
   - Passly Authenticator: https://play.google.com/store/apps/details?id=com.passly.authenticator&hl=en

2. Launch the installed mobile Authenticator application.
3. Select the option to add an Account to the mobile app.

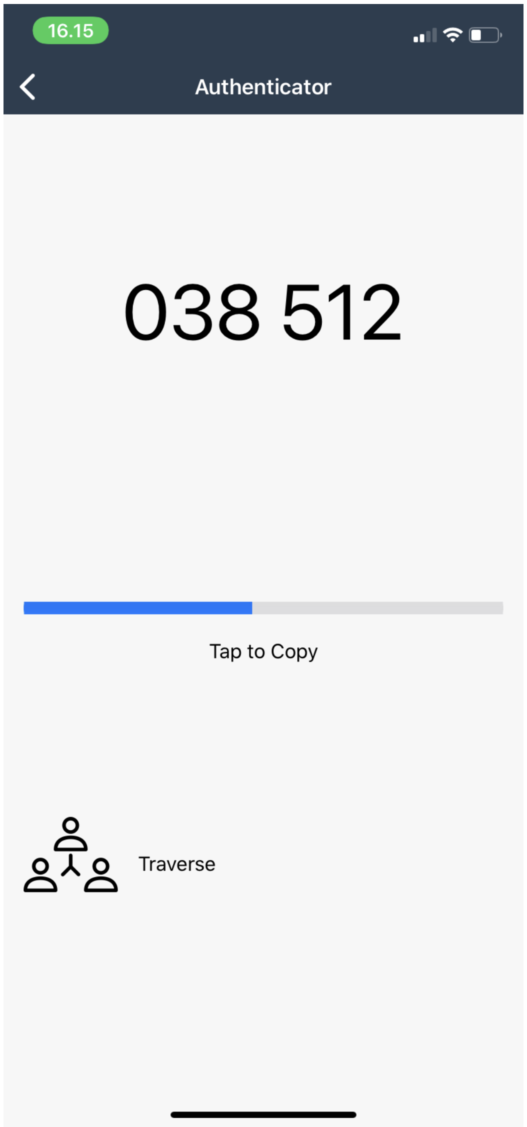


4 Scan the QR code displayed in the Traverse.

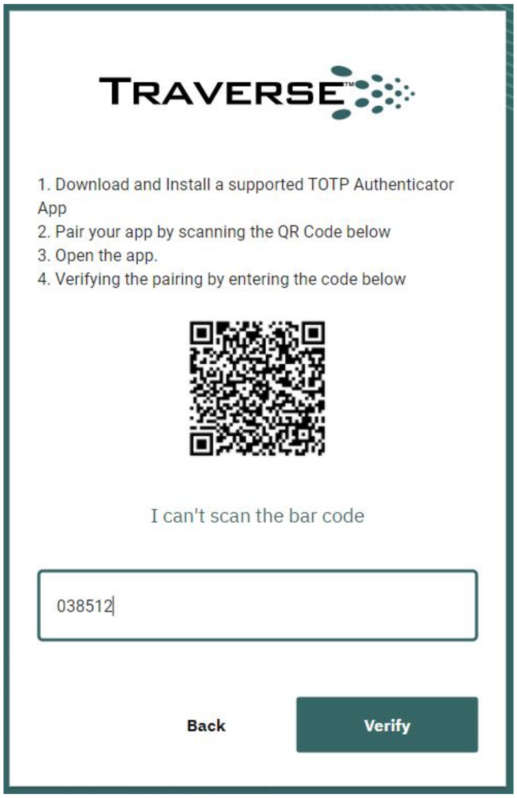


1. Download and Install a supported TOTP Authenticator App
2. Pair your app by scanning the QR Code below
3. Open the app.
4. Verifying the pairing by entering the code below

5 Find the Traverse Account in the Accounts list in the mobile Authenticator application.



6 Enter the Time-based, One-Time Password (TOTP) displayed in the Authenticator application in the Traverse and click the Verify button.



1. Download and Install a supported TOTP Authenticator App
2. Pair your app by scanning the QR Code below
3. Open the app.
4. Verifying the pairing by entering the code below

I can't scan the bar code

038512

Note: The Authentication Code should be entered within the 30-second period. Otherwise, you should enter the next non-expired Authentication code displayed in the Authenticator application. The code expiration is tracked in the Authenticator application.

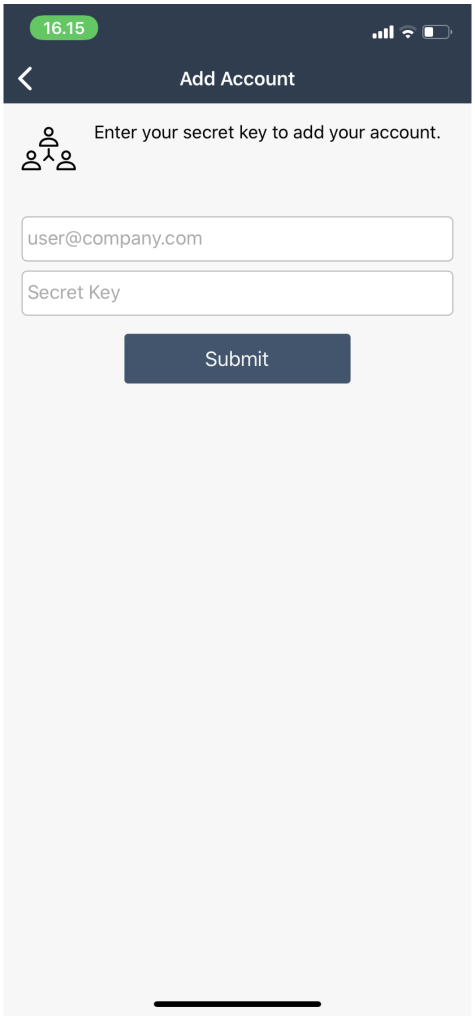
Note: The Traverse Account should be displayed on the Accounts list in the mobile application.

Workaround for mobile Authenticator application setup

If you have issues at scanning the QR code, you can add your Traverse Account manually in a mobile Authenticator application:

1. Select Add an Account option in the installed mobile application.
2. Enter Email and the Secret Key.

Note: To view the Key, click the **I can't scan the bar code** option in the Traverse application. The key will be displayed as **Your TOTP Authenticator code** in the Traverse application instead of the QR code.



Enter your secret key to add your account.

3 Enter an authorization code generated by the Authenticator application into the Traverse and click the Submit button.

Issue you may face during the Authenticator application setup on a mobile device

- If you have added your Traverse account to the Authenticator application, but the generated code does not work, make sure that the Authentication Code has not expired. If it has, enter a new valid authentication code while it is valid.
- If you have added your Traverse account to the Authenticator application and have entered a valid Authentication code, delete your Traverse Account in the mobile Authenticator application and complete 2FA steps again.

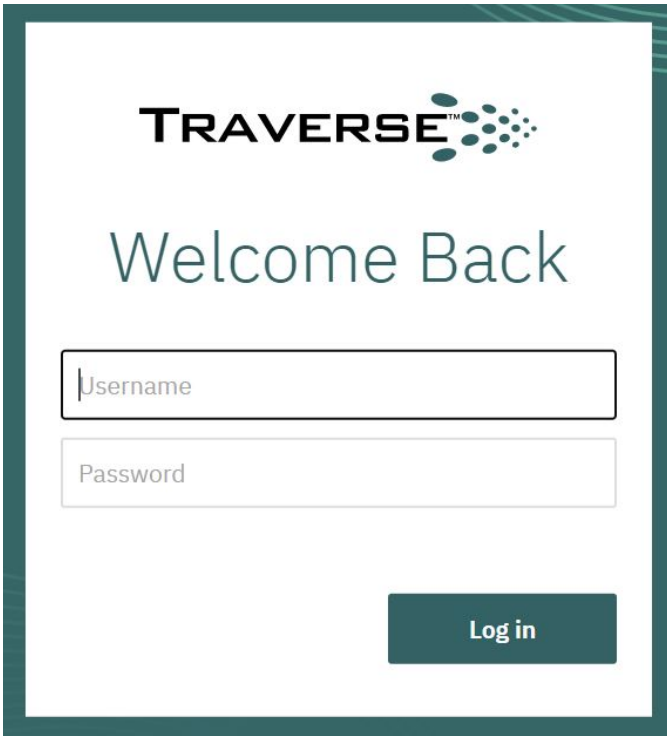
Two-Factor Authentication Enrollment Process

2FA enrollment flow

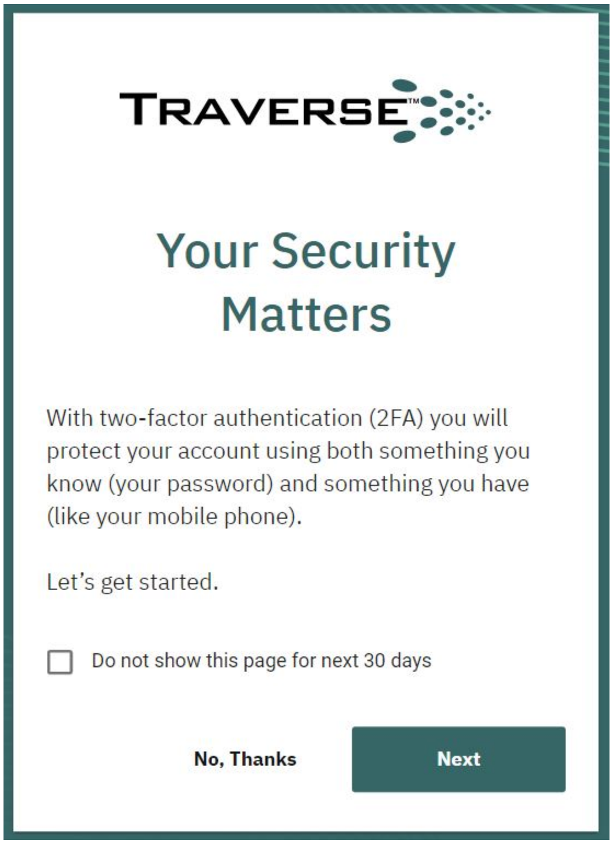
Once the 2FA feature is toggled as required for all users in Traverse or an entire department or for a particular users within a department, such users must enroll in 2FA:

1 Download the TOTP Authenticator application on a mobile device OR add Authenticator Extension in the Chrome browser.

2 Launch Traverse application and enter credentials as usual.



3 Click **Next** in the Your Security Matters screen.



Your Security Matters

With two-factor authentication (2FA) you will protect your account using both something you know (your password) and something you have (like your mobile phone).

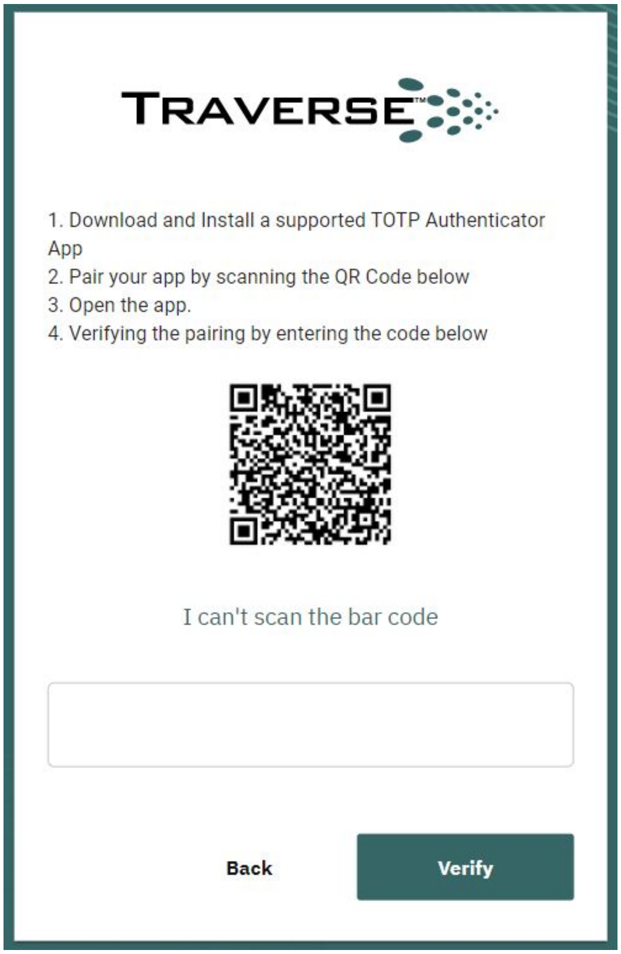
Let’s get started.

☐ Do not show this page for next 30 days

4 Launch the Authenticator application.

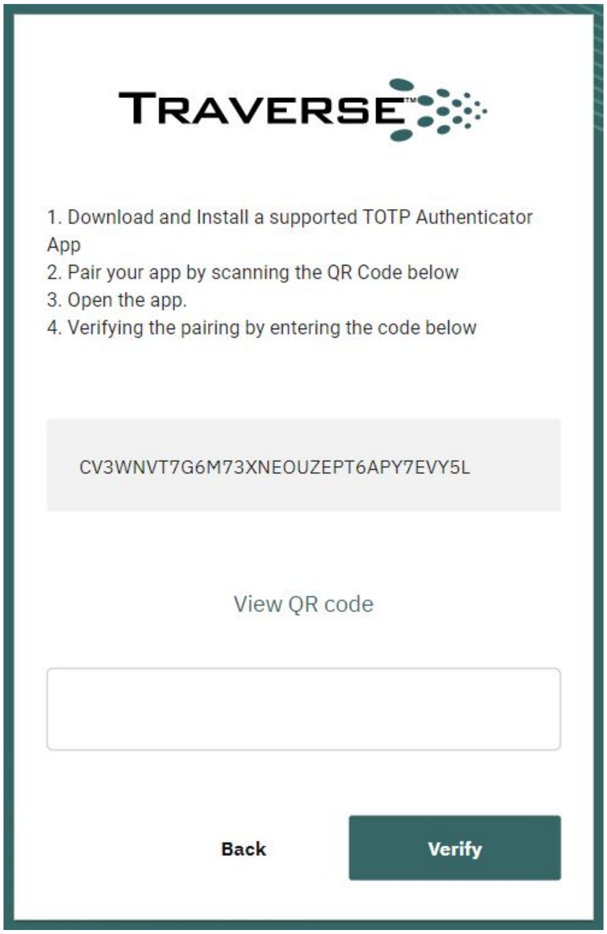
5 Add your Traverse account to the Authenticator application:

- by scanning the QR code displayed in the Traverse with the Authenticator application.



1. Download and Install a supported TOTP Authenticator App
2. Pair your app by scanning the QR Code below
3. Open the app.
4. Verifying the pairing by entering the code below

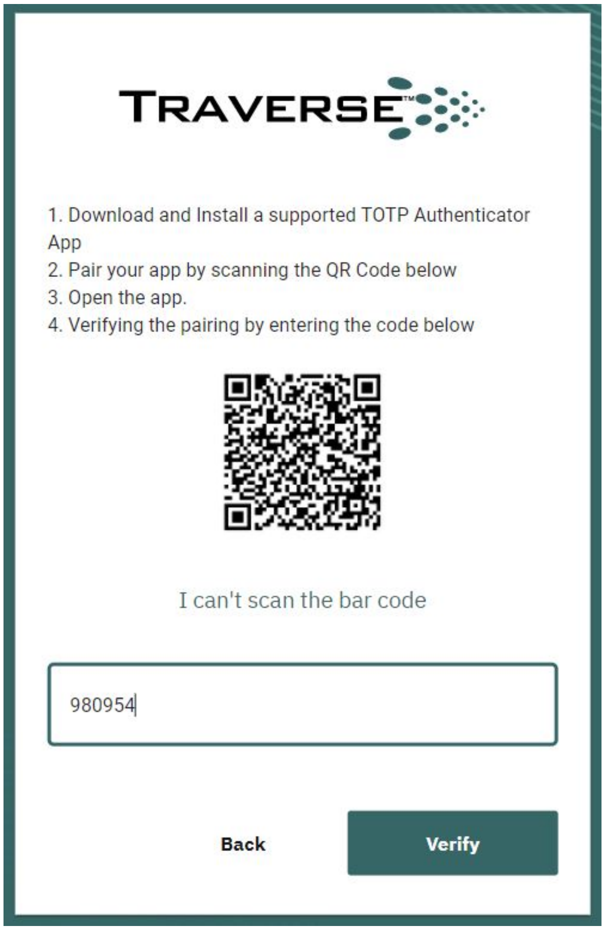
- by manually entering the Alphanumeric Code displayed in the Traverse in the Authenticator application.



1. Download and Install a supported TOTP Authenticator App
2. Pair your app by scanning the QR Code below
3. Open the app.
4. Verifying the pairing by entering the code below

CV3WNVT7G6M73XNEOUZEPT6APY7EVY5L

6 Enter Authentication Code generated by your Authenticator application into Traverse application screen and click enabled **Verify** button.



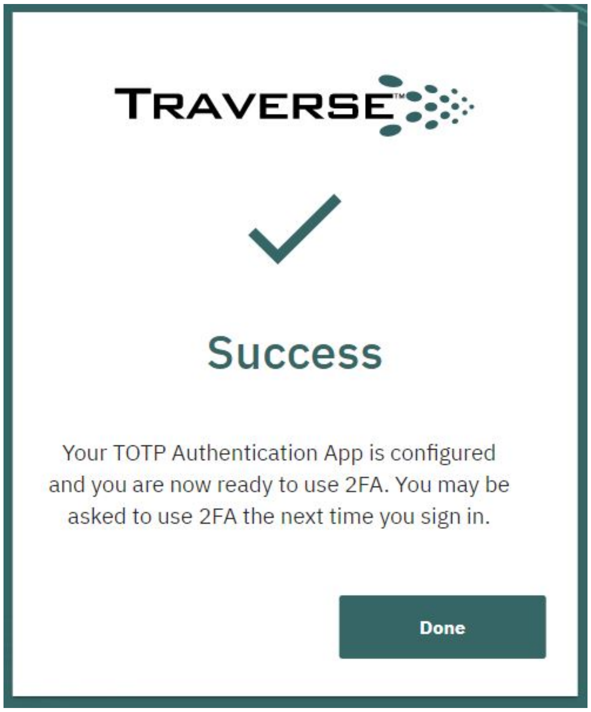
1. Download and Install a supported TOTP Authenticator App
2. Pair your app by scanning the QR Code below
3. Open the app.
4. Verifying the pairing by entering the code below

I can't scan the bar code

980954

Note: The Authentication Code should be entered within the 30-second period. Otherwise, you should enter the next non-expired Authentication code displayed in the Authenticator application. The code expiration is tracked in the Authenticator application.

7 Click **Done** button to access Traverse home page.



Success

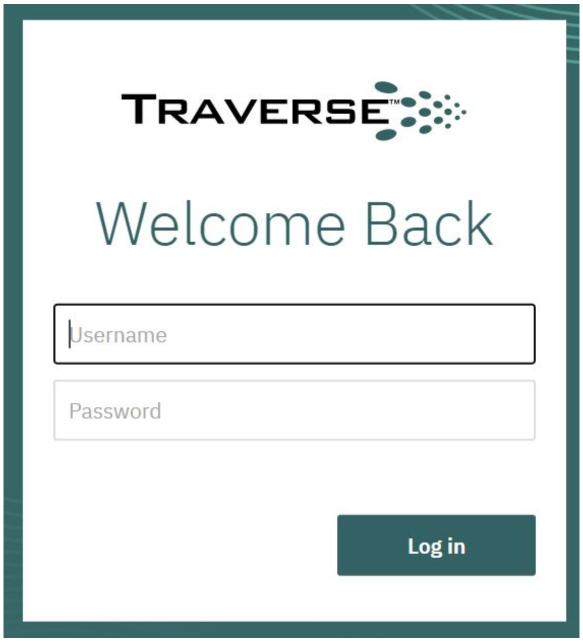
Your TOTP Authentication App is configured and you are now ready to use 2FA. You may be asked to use 2FA the next time you sign in.

Note: If the 2FA enrollment process was not completed because internet connection has been lost, or browser has been closed by accident, the user will restart from scratch the enrollment process upon next login attempt.

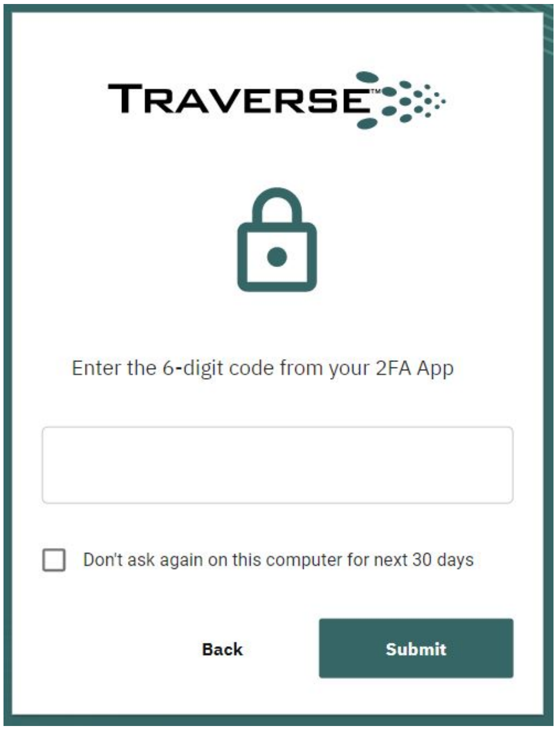
2FA Subsequent Login

Once you have enrolled in Traverse 2FA, you will have to walk through 2 steps to access your Traverse account each time you login the Traverse application:

1 Provide credentials at the 1st authentication step, as usual.



2 Provide Authentication Code generated in the configured Authenticator application, at the second step to access your Traverse.



Enter the 6-digit code from your 2FA App

□ Don't ask again on this computer for next 30 days

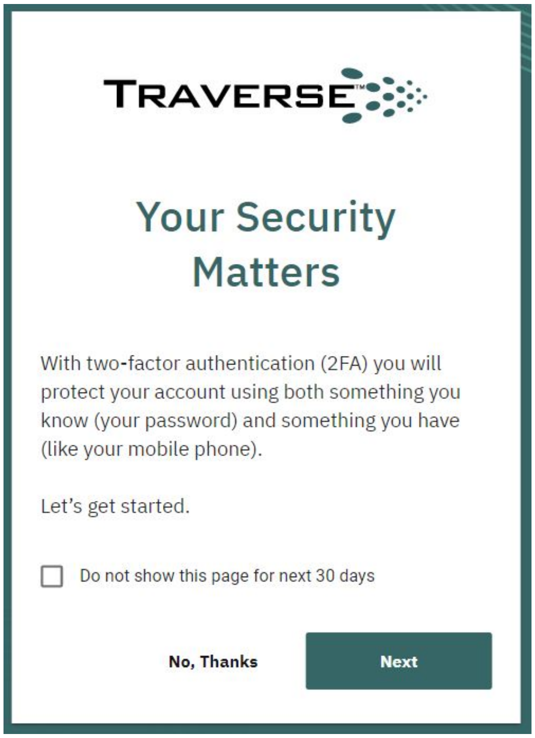
3 Access the Traverse application.

2FA Skip Flow

If the 2FA enrollment is toggled as optional for a particular users, these Traverse users can skip the two-factor authorization process:

1 Enter credentials in the Traverse Login page.

2 Select **No,Thanks** button.



Your Security Matters

With two-factor authentication (2FA) you will protect your account using both something you know (your password) and something you have (like your mobile phone).

Let’s get started.

☐ Do not show this page for next 30 days

3 Access the Traverse application.

Chapter 2: Two Factor Authentication Settings

By default, 2FA is set to optional for all Traverse users. It is recommended that 2FA is configured as a mandatory login process.

2FA in Traverse can be configured at three levels for:

- Two-factor Authentication for Individual Users ;
- Two-factor Authentication for All Department Users;
- Two-factor Authentication for All Traverse Users.

Two-factor Authentication for Individual Users

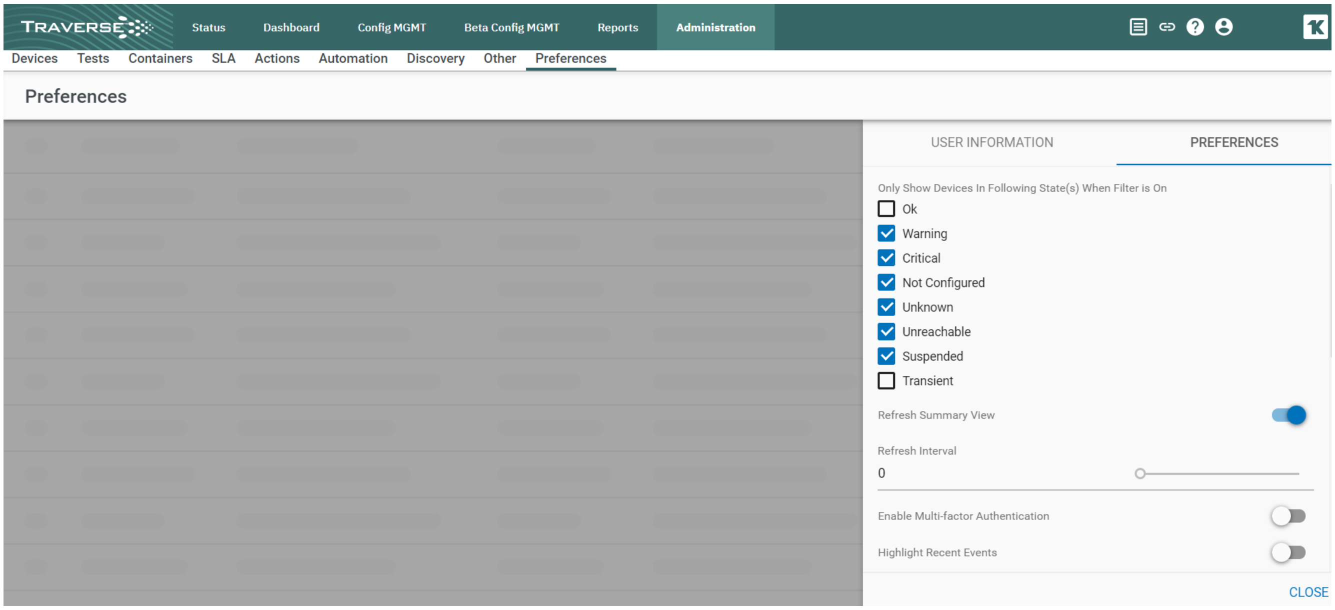
Users can protect their accounts by enabling MFA setting on Administration > Preferences > **Preferences** tab.

Note: If the MFA setting has been enabled for department user belongs or for all Traverse users, this setting will be gray out.

To enable MFA in Traverse for an Individual user:

1 Login to Traverse with the corresponding permissions.

2 Navigate to Administration > Preferences > Preferences tab.



Only Show Devices In Following State(s) When Filter is On

☐ Ok
☑ Warning
☑ Critical
☑ Not Configured
☑ Unknown
☑ Unreachable
☑ Suspended
☐ Transient

Refresh Summary View

Refresh Interval
0

Enable Multi-factor Authentication

Highlight Recent Events

3 Enable the **Enable Multi-factor Authentication** toggle button.

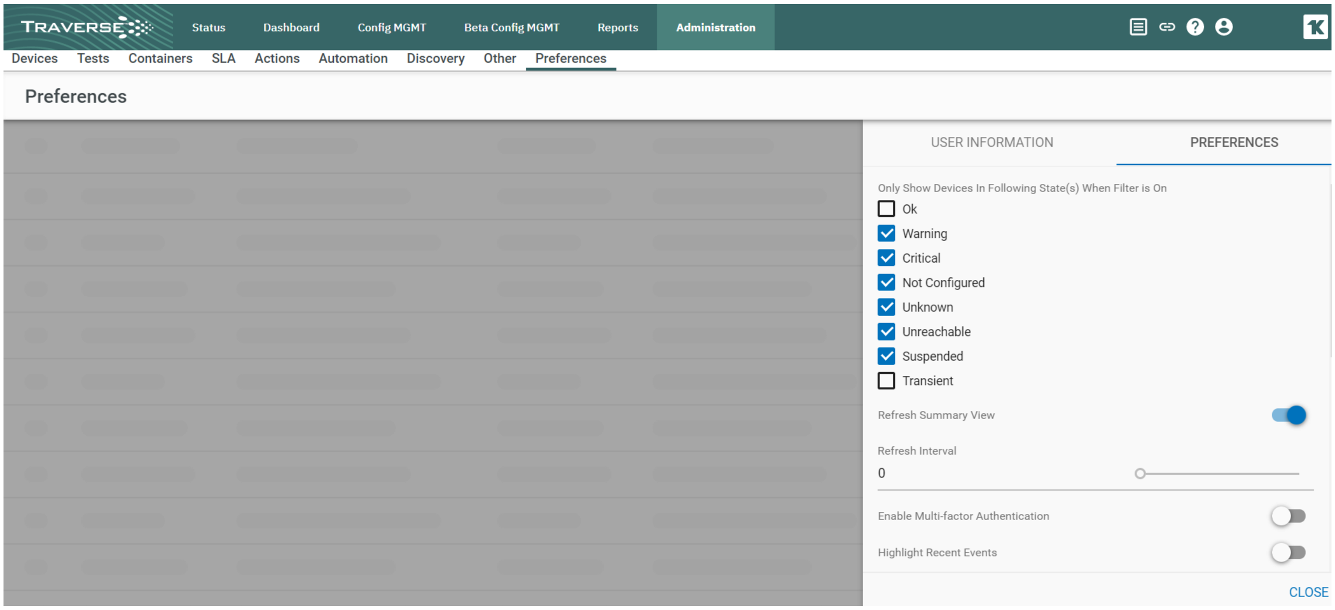
4 Click the **Apply** button.

Now user will have to follow the 2FA process to login to Traverse account.

To disable MFA in Traverse for an Individual user:

1 Login to Traverse with the corresponding permissions.

2 Navigate to Administration > Preferences > Preferences tab.



Preferences

Only Show Devices In Following State(s) When Filter is On

- □ Ok
- ☑ Warning
- ☑ Critical
- ☑ Not Configured
- ☑ Unknown
- ☑ Unreachable
- ☑ Suspended
- □ Transient

Refresh Summary View ●

Refresh Interval

0

Enable Multi-factor Authentication ○

Highlight Recent Events ○

3 Disable the **Enable Multi-factor Authentication** toggle button.

4 Click the **Apply** button.

Two-factor Authentication for All Department Users

Admin Class users or SuperUsers with admin privileges over a admin group or a department can enable or disable MFA setting for all users in admin group or in department.

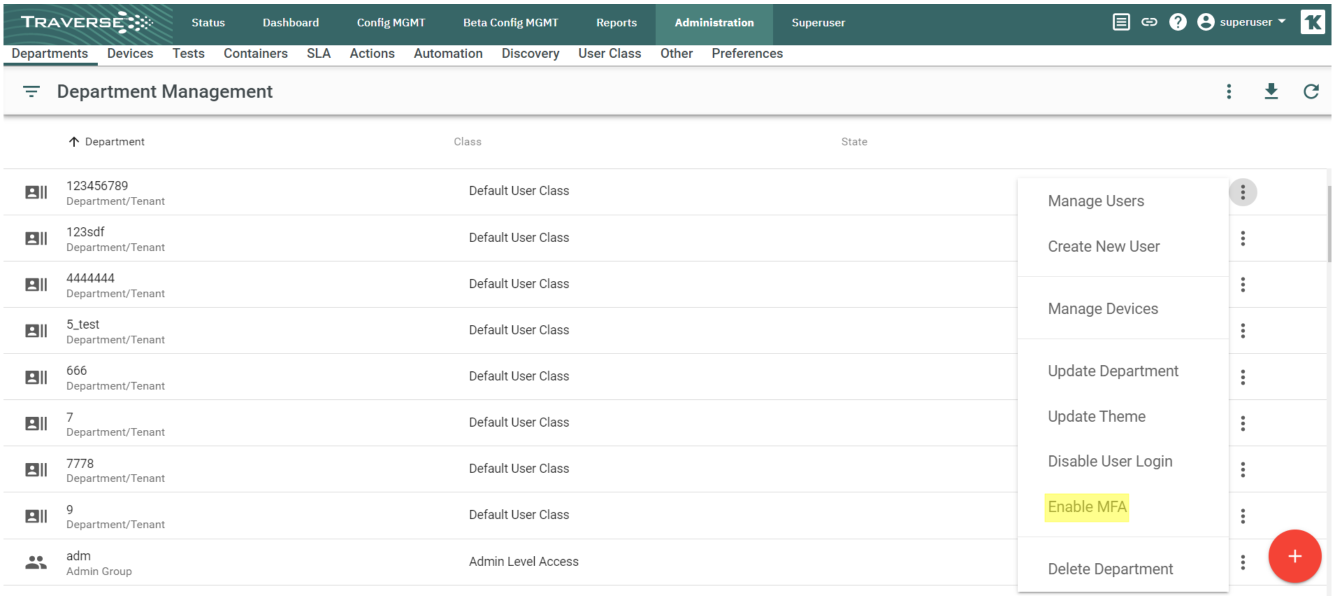
To enable MFA in Traverse for a admin group or a department:

1 Login to Traverse with the corresponding permissions.

2 Navigate to Administration > Departments page.

3 Click the ⋮ icon on the admin group or department you want to enable MFA setting.

4 Select the **Enable MFA** option.



Department	Class	State
123456789 Department/Tenant	Default User Class	
123sdf Department/Tenant	Default User Class	
4444444 Department/Tenant	Default User Class	
5_test Department/Tenant	Default User Class	
666 Department/Tenant	Default User Class	
7 Department/Tenant	Default User Class	
7778 Department/Tenant	Default User Class	
9 Department/Tenant	Default User Class	
adm Admin Group	Admin Level Access	

5 Click **Yes** to enable MFA.

Now the users in admin group or in department will have to follow the 2FA process to login their Traverse account.

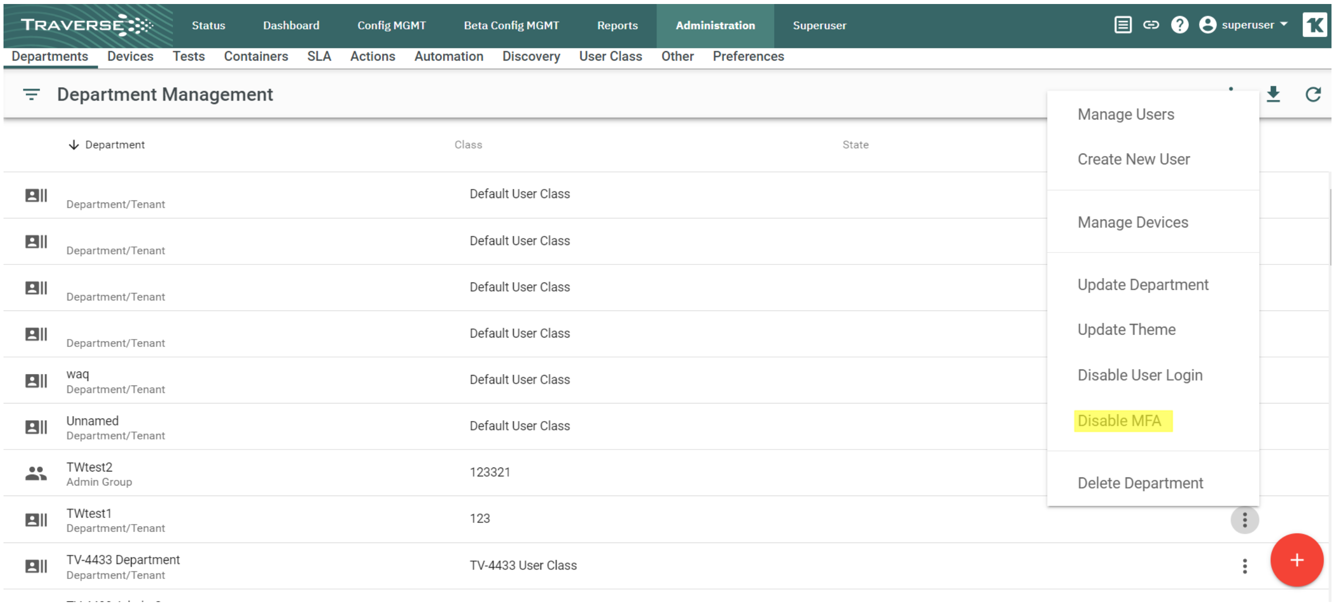
To diable MFA in Traverse for a admin group or a department:

1 Login to Traverse with the corresponding permissions.

2 Navigate to Administration > Departments page.

3 Click the ⋮ icon on the admin group or department you want to disable MFA setting.

4 Select the **Disable MFA** option.



Department	Class	State
Department/Tenant	Default User Class	
Department/Tenant	Default User Class	
Department/Tenant	Default User Class	
Department/Tenant	Default User Class	
waq Department/Tenant	Default User Class	
Unnamed Department/Tenant	Default User Class	
TWtest2 Admin Group	123321	
TWtest1 Department/Tenant	123	
TV-4433 Department Department/Tenant	TV-4433 User Class	

5 Click **Yes** to disable MFA.

Two-factor Authentication for All Traverse Users

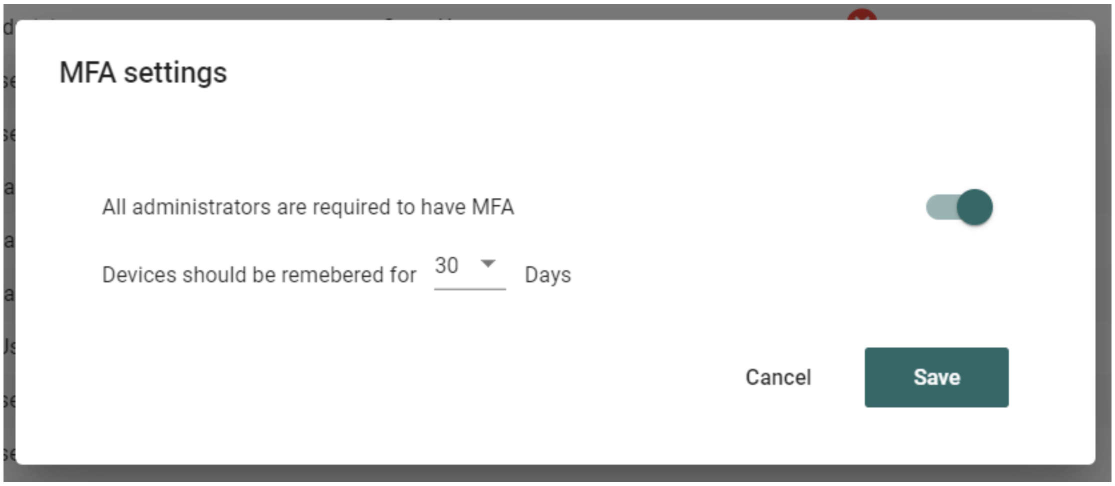
SuperUsers can configure MFA setting for all Traverse users on Superuser > Global config > **MFA Settings** page.

To enforce MFA in Traverse for all administrators:

1 Login to Traverse with the corresponding permissions.

2 Navigate to Superuser > Global config > **MFA Settings** page.

3 At the top right corner click the ⚙ icon, then enable the **All administrators are required to have MFA** toggle button.



MFA settings

All administrators are required to have MFA ●

Devices should be remebered for 30 Days

4 Click the **Save** button.

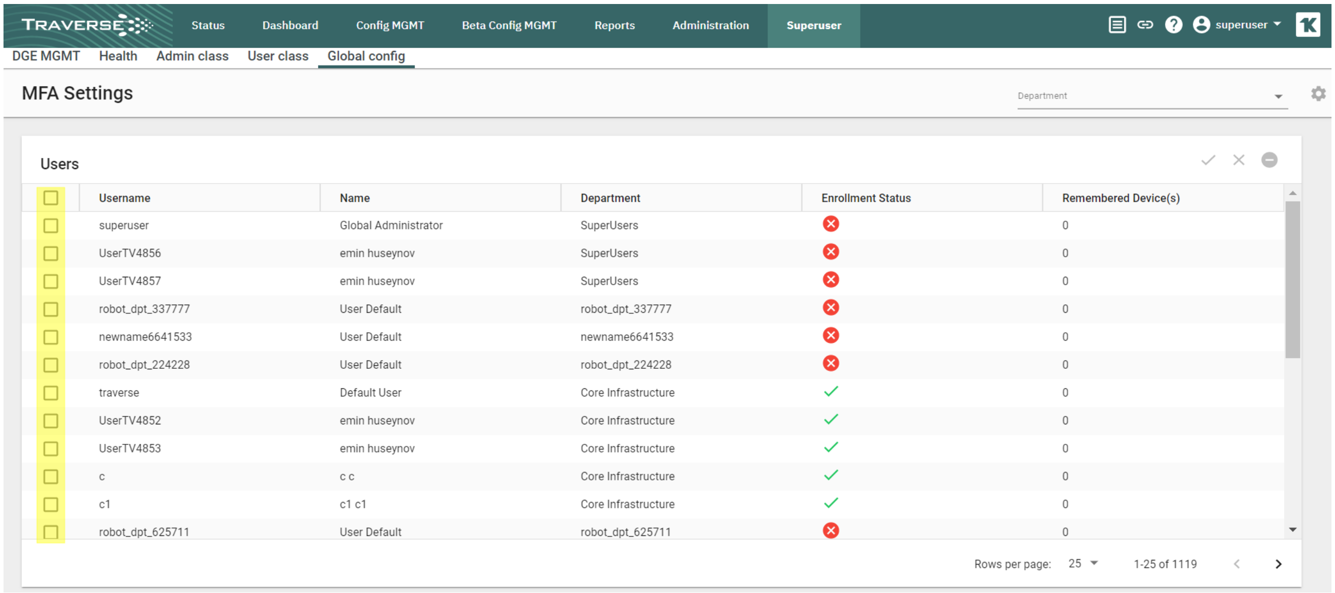
Now all administrators will have to follow the 2FA process to login their Traverse account.

To enforce MFA in Traverse for all users or a particular user:

1 Login Traverse application with the corresponding permissions.

2 Navigate to Superuser > Global config > **MFA Settings** page.

3 Select all users or a particular user that you would like to oblige to follow the MFA process.



MFA Settings

Users

□	Username	Name	Department	Enrollment Status	Remembered Device(s)
□	superuser	Global Administrator	SuperUsers	⊗	0
□	UserTV4856	emin huseynov	SuperUsers	⊗	0
□	UserTV4857	emin huseynov	SuperUsers	⊗	0
□	robot_dpt_337777	User Default	robot_dpt_337777	⊗	0
□	newname6641533	User Default	newname6641533	⊗	0
□	robot_dpt_224228	User Default	robot_dpt_224228	⊗	0
□	traverse	Default User	Core Infrastructure	✓	0
□	UserTV4852	emin huseynov	Core Infrastructure	✓	0
□	UserTV4853	emin huseynov	Core Infrastructure	✓	0
□	c	c c	Core Infrastructure	✓	0
□	c1	c1 c1	Core Infrastructure	✓	0
□	robot_dpt_625711	User Default	robot_dpt_625711	⊗	0

Rows per page: 25 1-25 of 1119

4 Click the ✓ icon to enable MFA for selected users, the click the **Enable** button.

Now the selected users will have to follow the 2FA process to login their Traverse account.

Multi-Factor Authentication Enrollment Process Monitoring

Traverse users with the corresponding permissions can monitor the status of MFA enrollment process by Enrollment Status per each user within a department.

Currently, there are two MFA Enrollment Status available:

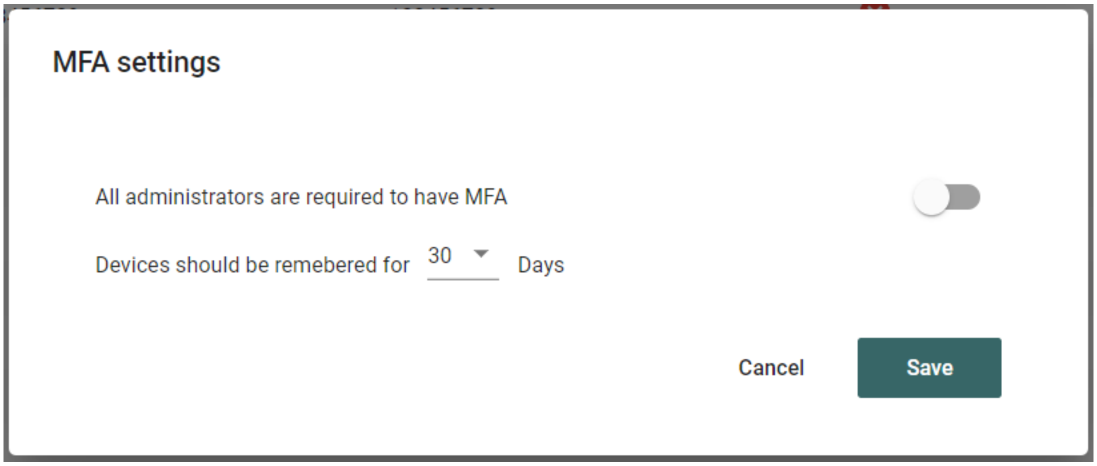
- ⊗ - Traverse 2FA is not enabled for user.
- ✓ - Traverse 2FA is enabled for user.

To disable MFA in Traverse for all administrators:

1 Login to Traverse with the corresponding permissions.

2 Navigate to Superuser > Global config > **MFA Settings** page.

3 At the top right corner click the ⚙ icon, then disable the **All administrators are required to have MFA** toggle button.



MFA settings

All administrators are required to have MFA

Devices should be remebered for 30 Days

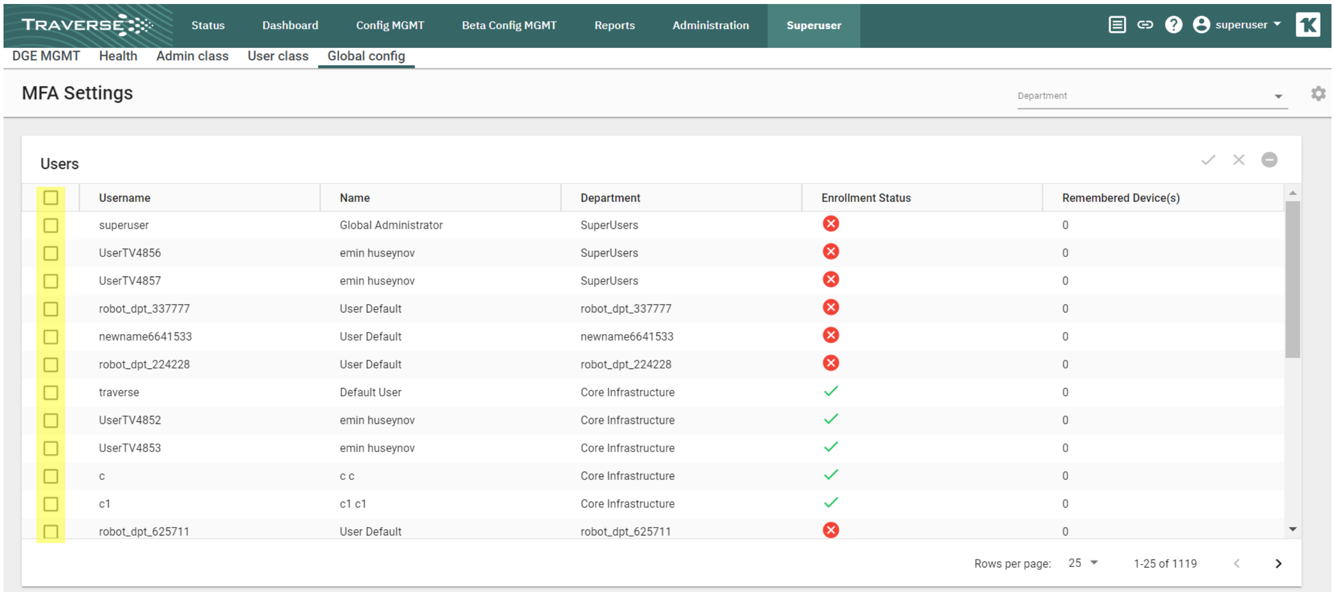
4 Click the **Save** button.

To disable MFA in Traverse for all users or a particular user:

1 Login Traverse application with the corresponding permissions.

2 Navigate to Superuser > Global config > **MFA Settings** page.

3 Select the users that you would like to disable the MFA process.



MFA Settings

Users

□	Username	Name	Department	Enrollment Status	Remembered Device(s)
□	superuser	Global Administrator	SuperUsers	✕	0
□	UserTV4856	emin huseynov	SuperUsers	✕	0
□	UserTV4857	emin huseynov	SuperUsers	✕	0
□	robot_dpt_337777	User Default	robot_dpt_337777	✕	0
□	newname6641533	User Default	newname6641533	✕	0
□	robot_dpt_224228	User Default	robot_dpt_224228	✕	0
□	traverse	Default User	Core Infrastructure	✓	0
□	UserTV4852	emin huseynov	Core Infrastructure	✓	0
□	UserTV4853	emin huseynov	Core Infrastructure	✓	0
□	c	c c	Core Infrastructure	✓	0
□	c1	c1 c1	Core Infrastructure	✓	0
□	robot_dpt_625711	User Default	robot_dpt_625711	✕	0

Rows per page: 25 1-25 of 1119

4 Click the ✕ icon to disable MFA for selected users, then click the **Clear** button.

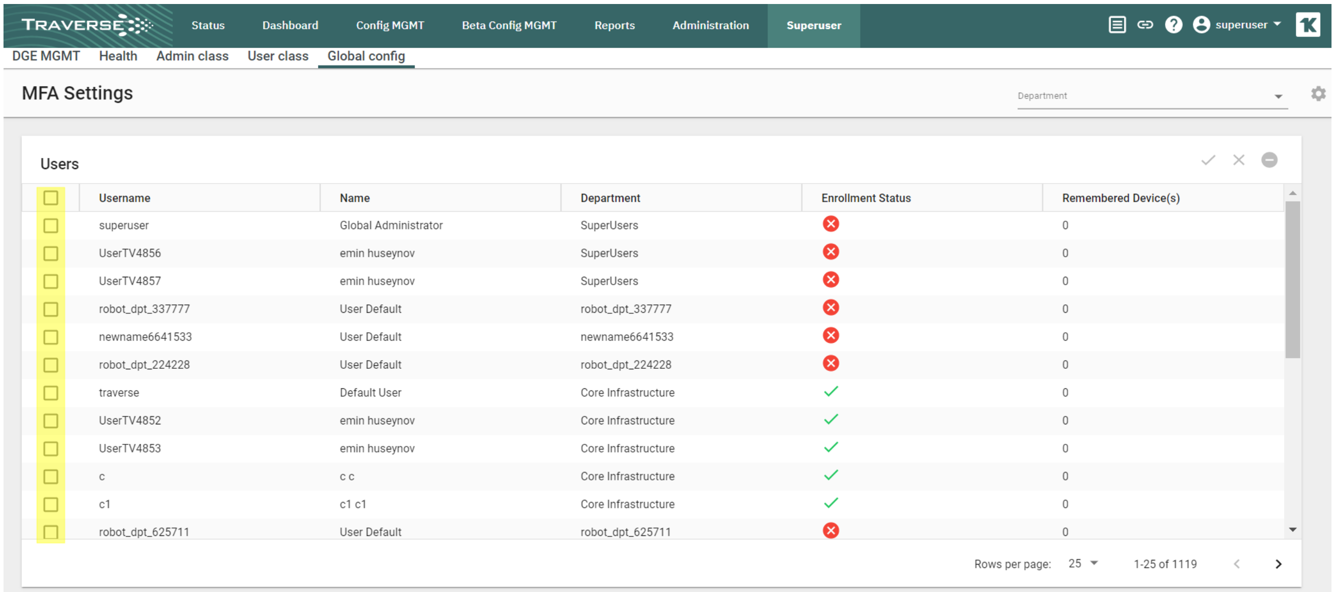
Note: Users removed from the MFA Enrollment will have to complete the MFA enrollment process next time they log into the Traverse.

To remove 2FA Remembered Devices for all users or a particular user:

1 Login Traverse application with the corresponding permissions.

2 Navigate to Superuser > Global config > **MFA Settings** page.

3 Select the users that you would like to clear Remembered Devices.



MFA Settings

Department

Users

□	Username	Name	Department	Enrollment Status	Remembered Device(s)
□	superuser	Global Administrator	SuperUsers	☒	0
□	UserTV4856	emin huseynov	SuperUsers	☒	0
□	UserTV4857	emin huseynov	SuperUsers	☒	0
□	robot_dpt_337777	User Default	robot_dpt_337777	☒	0
□	newname6641533	User Default	newname6641533	☒	0
□	robot_dpt_224228	User Default	robot_dpt_224228	☒	0
□	traverse	Default User	Core Infrastructure	✓	0
□	UserTV4852	emin huseynov	Core Infrastructure	✓	0
□	UserTV4853	emin huseynov	Core Infrastructure	✓	0
□	c	c c	Core Infrastructure	✓	0
□	c1	c1 c1	Core Infrastructure	✓	0
□	robot_dpt_625711	User Default	robot_dpt_625711	☒	0

Rows per page: 25 1-25 of 1119

4 Click the ⛔ icon to clear remembered devices for selected users, then click the **Clear** button.