VSA Two-Factor Authentication User Guide

VSA User Guide | November 2019

VSA Two-Factor Authentication User Guide

Release 9.5.0.24 | Version 1.0

Copyright Agreement

Contents

About Two-Factor Authentication in VSA

Two-factor authentication in VSA Admin Portal has been designed to facilitate and empower security access for users. The feature is meant to prevent unauthorized users from accessing VSA 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 VSA 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

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

2FA in VSA can be configured at three levels:

- at User Level
- at Tenant Level
- at Server Level

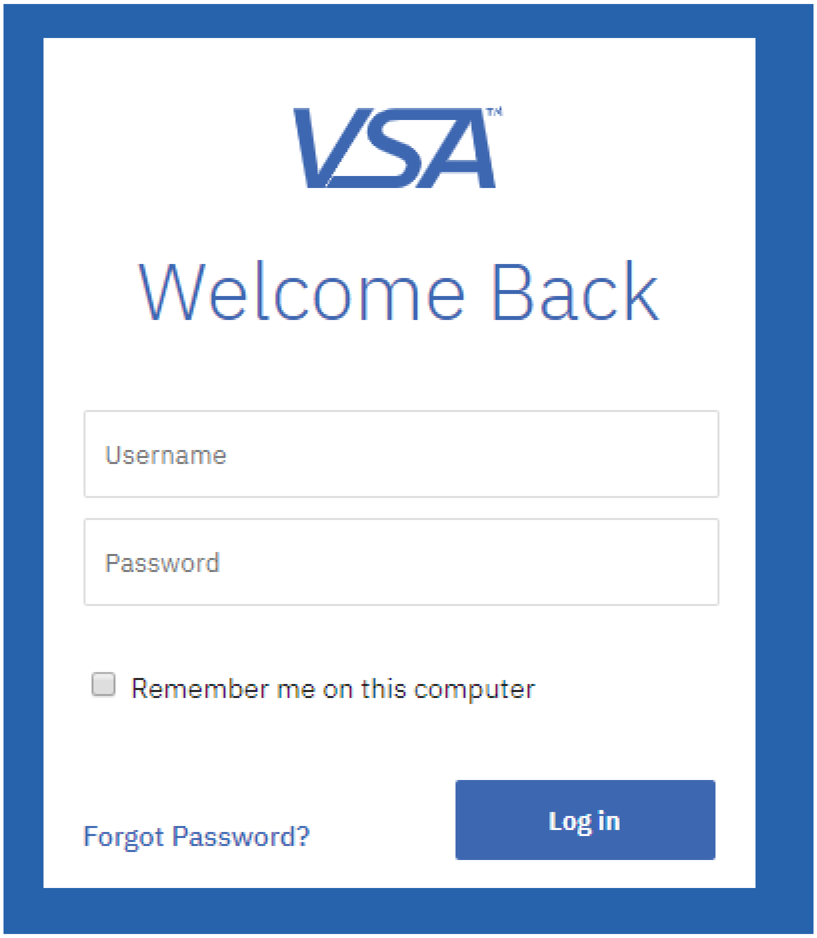
Two-Factor Authentication at User Level - Standard Role Admin

Two-Factor Authentication Enrollment Process

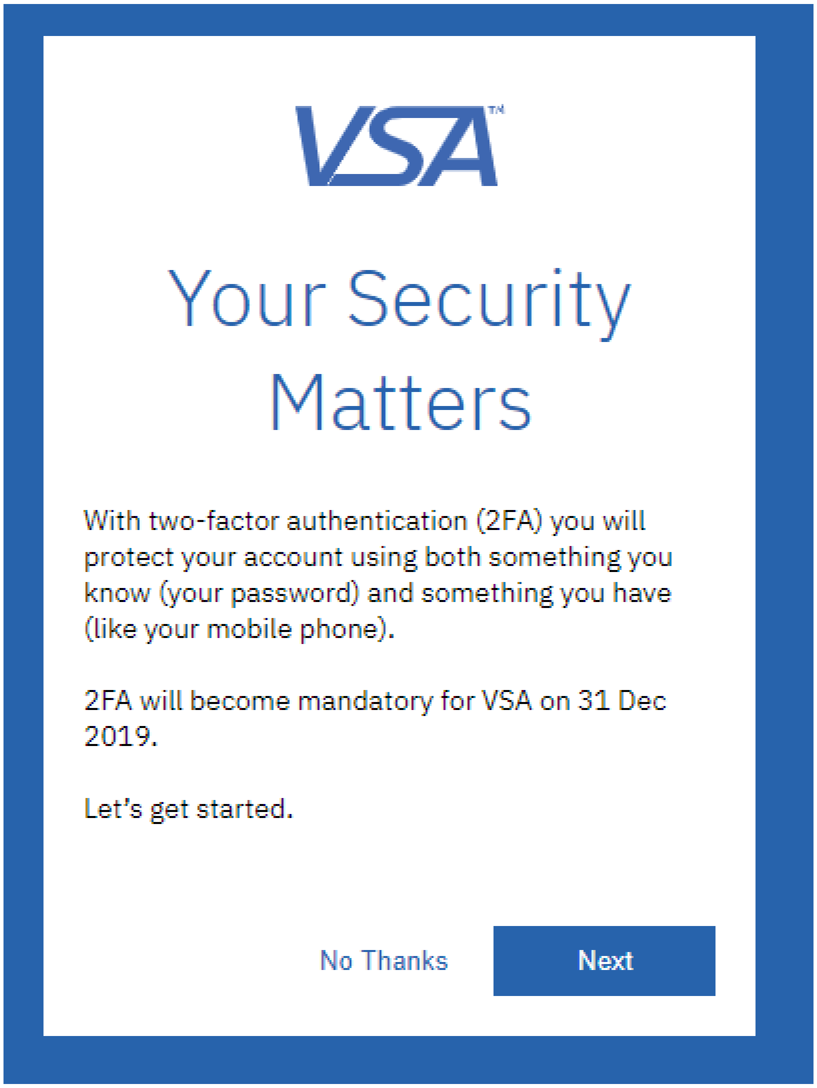
2FA enrollment flow

Once the 2FA feature is toggled as required for an entire tenant by Tenant Admin or for particular users within a tenant by System Role user, such a user within the tenant that logs in the VSA Admin Portal must enroll in 2FA:

1. Download the TOTP Authenticator application on a mobile device OR add Authenticator Extension in the Chrome browser.
2. Launch VSA Admin Portal 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).

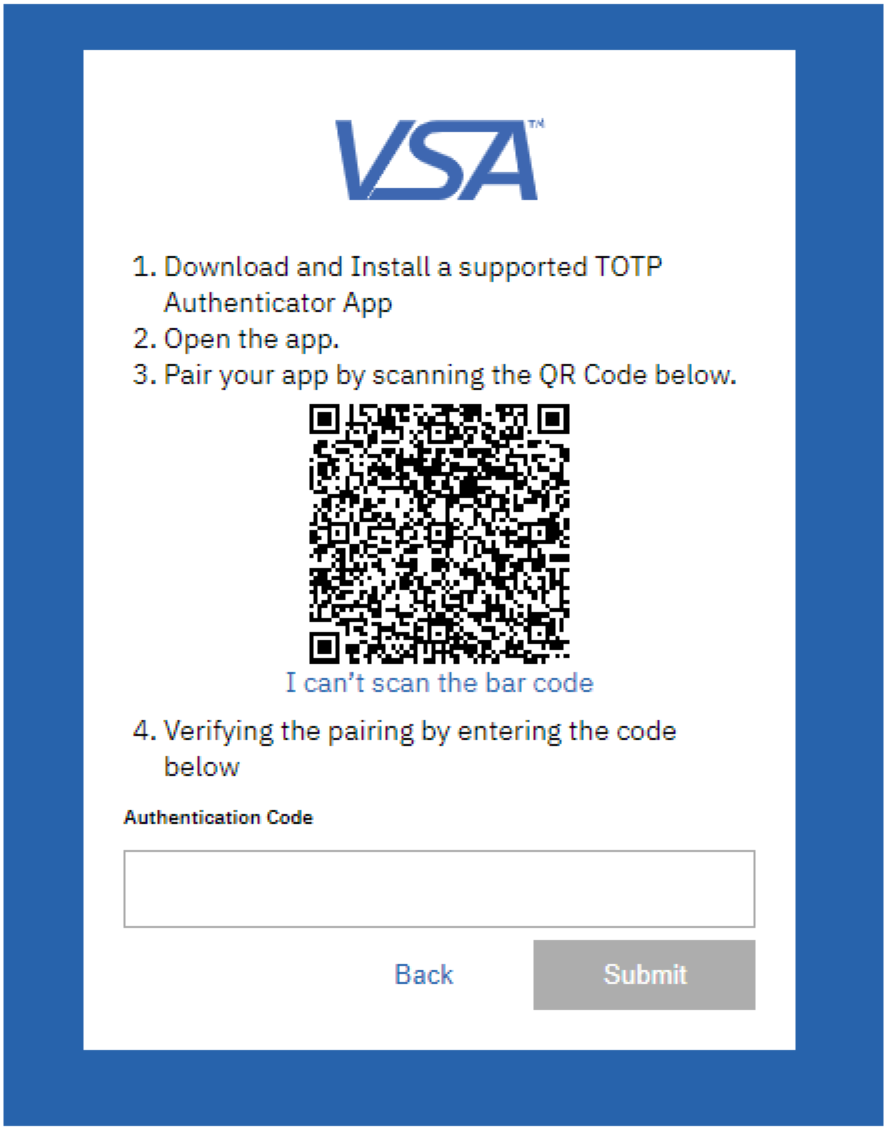
2FA will become mandatory for VSA on 31 Dec 2019.

Let's get started.

4 Launch the Authenticator application.

5 Add your VSA Admin Portal account to the Authenticator application:

a. by scanning the QR code displayed in the VSA with the Authenticator application.

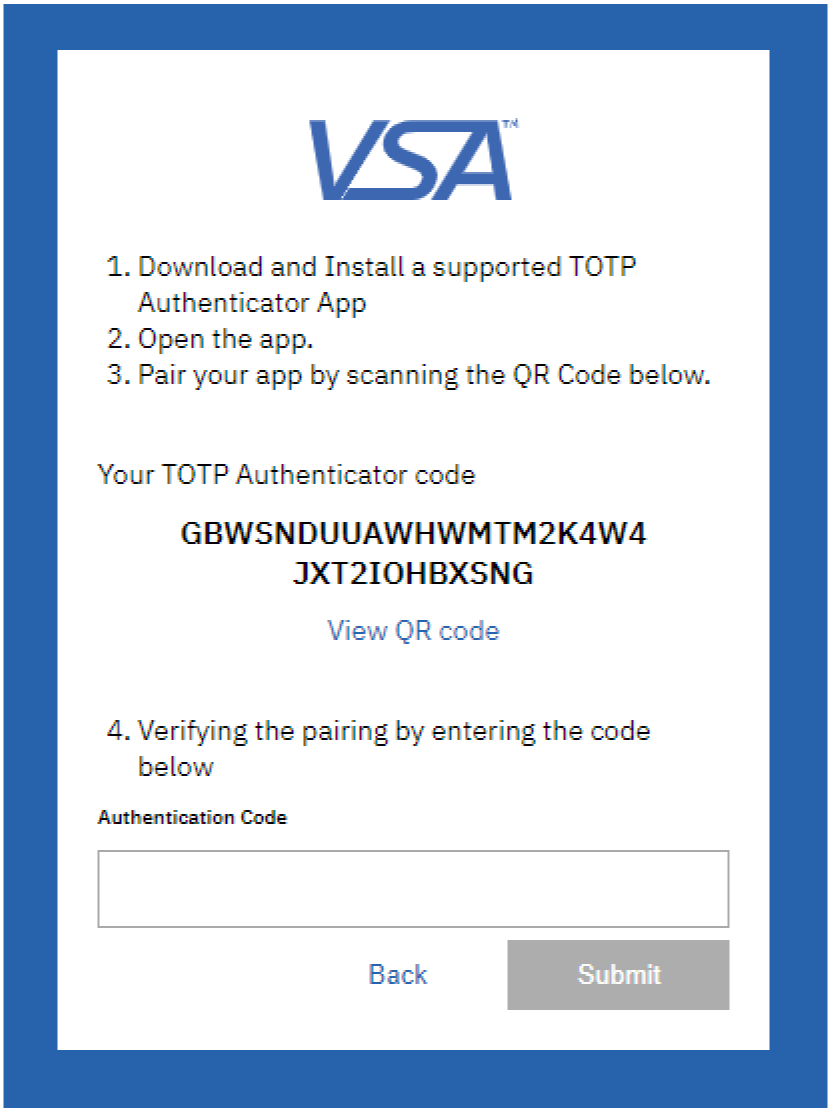


1. Download and Install a supported TOTP Authenticator App
2. Open the app.
3. Pair your app by scanning the QR Code below.

4. Verifying the pairing by entering the code below

Authentication Code

b. by manually entering the Alphanumeric Code displayed in the VSA in the Authenticator application.



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

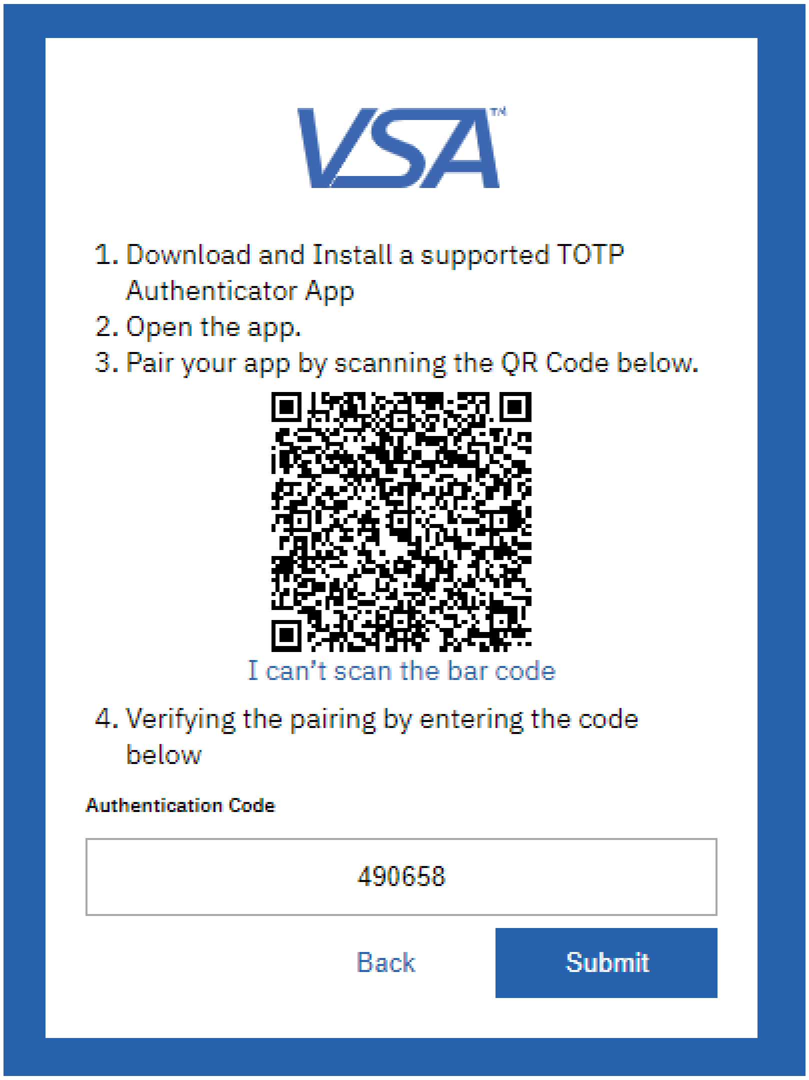
Your TOTP Authenticator code

GBWSNDUUAWHWMTM2K4W4
JXT2IOHBXSNG

4. Verifying the pairing by entering the code below

Authentication Code

6 Enter Authentication Code generated by your Authenticator application into VSA Admin Portal screen and click enabled **Submit** button.



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

I can't scan the bar code

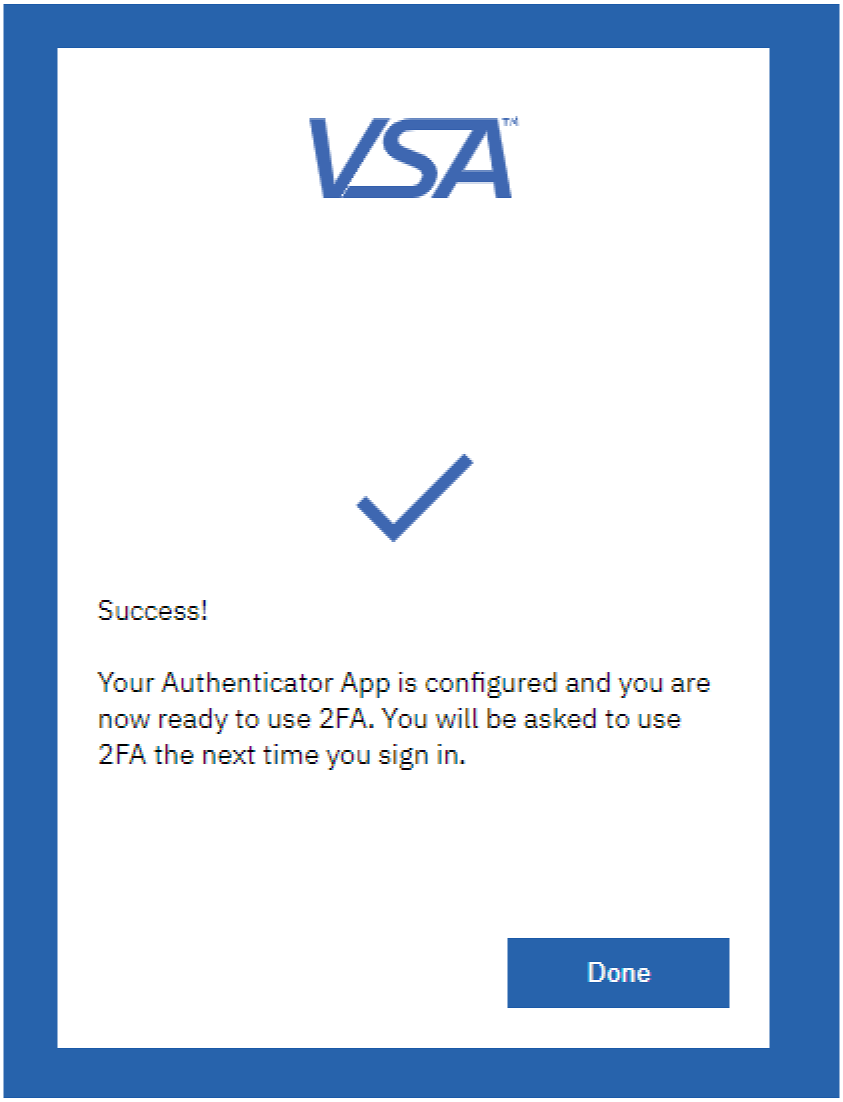
4. Verifying the pairing by entering the code below

Authentication Code

490658

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 VSA home page.



Success!

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

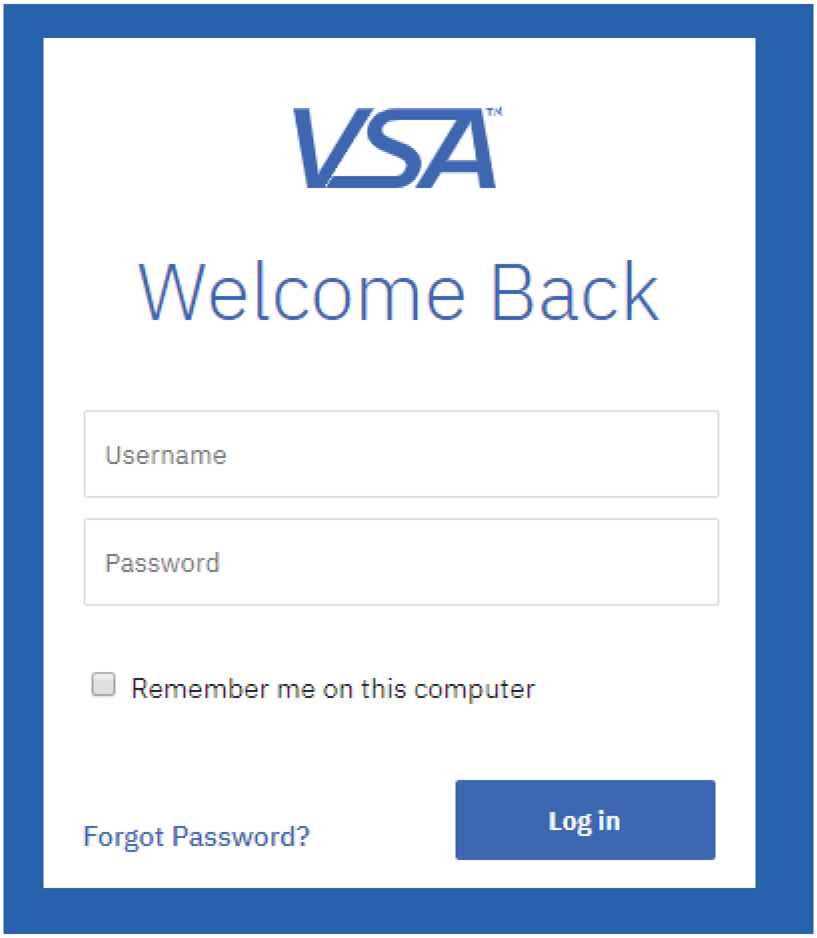
Note: If the 2FA enrollment process was not completed because internet connection has been lost, or browser has been closed by accident, the user will restart from scratch the enrollment process upon next login attempt.

Note: If a user is unable to access the mobile device, System Role User within their tenant has the ability to reset the 2FA status. This will enable the user to go through the 2FA enrollment again.

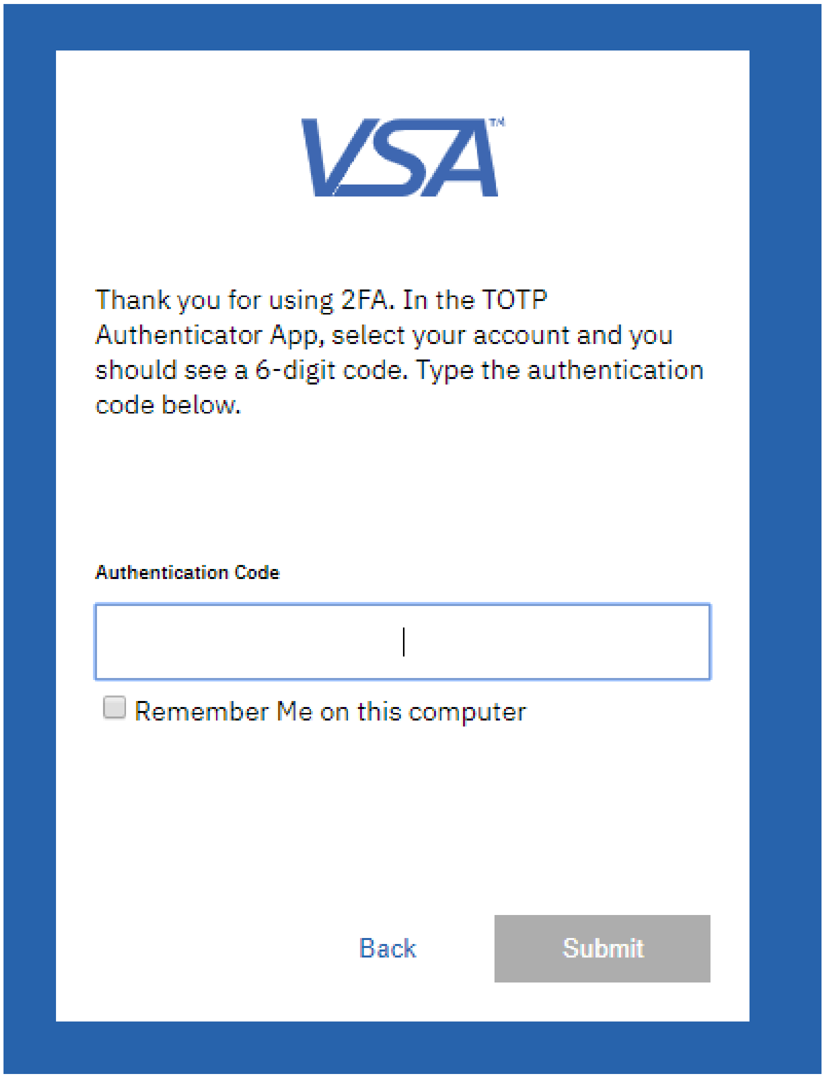
Two-Factor Authentication Subsequent Login

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

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 VSA.



Thank you for using 2FA. In the TOTP Authenticator App, select your account and you should see a 6-digit code. Type the authentication code below.

Authentication Code

□ Remember Me on this computer

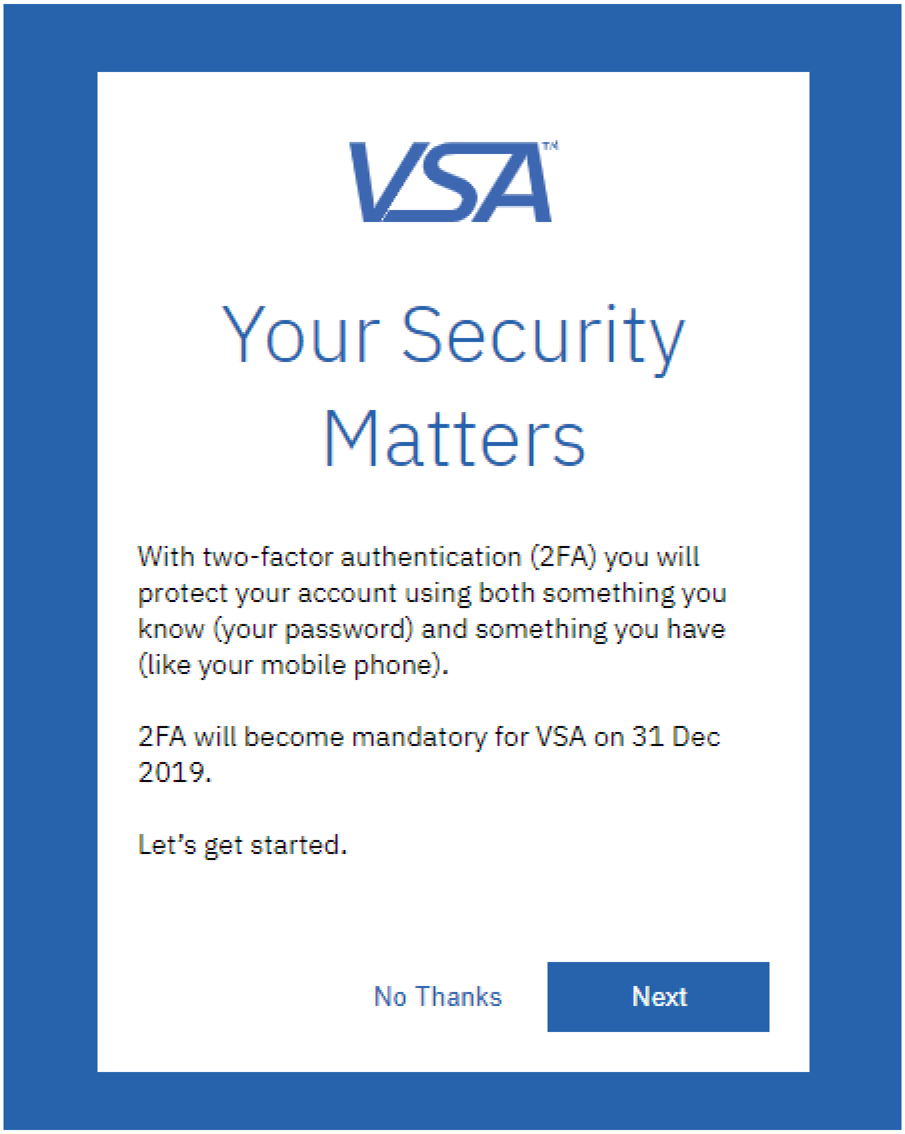
3 Access the VSA Admin Portal.

Two-Factor Authentication Skip Flow

If the 2FA enrollment is toggled as optional for an entire tenant or particular users within a tenant, these VSA Users can skip the two-factor authorization process:

1 Enter credentials in the VSA Admin Portal page.

2 Select **No,Thanks** button.



VSA™

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).

2FA will become mandatory for VSA on 31 Dec 2019.

Let's get started.

3 Access the VSA Admin Portal.

WARNING! Two-factor Authentication Enrollment will be mandatory for **all VSA users for all tenants** starting on 01/01/2020.

Two-Factor Authentication Security Rules

1 Once enrolled in 2FA, users will have to provide Credentials each time they login VSA. The TOTP-entry step can be skipped, if users choose to remember their device(s) for the time defined at the tenant level.

2 If a user fails 2FA verification the number of attempts defined by the Lockout Settings at the tenant level, the user's account will be locked out.

Note: The Lockout will occur, if user enters incorrect values the number of times that exceeds the number of attempts defined by Lockout Settings **in either the login page or TOTP-entry screens**.

3 If a user fails 2FA verification cycle (entering the credentials and the Time-based, One-Time Code) the number of times defined by the tenant Lockout Policy, the User Account will be locked out. To unlock it, please contact a System Role User in your tenant.

Note: Users with active AAoD accounts and AAoD Module enabled for their tenant will be able to continue using the same authentication procedure.

Authenticator application Set up and Configuration for VSA 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 VSA Admin portal (see Two-Factor Authentication Enrollment Process).

To have the Authenticator application generate the TOTP for VSA Admin Portal, users have to add the VSA 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 iOS and in Google Play for Android OS:

IOS:

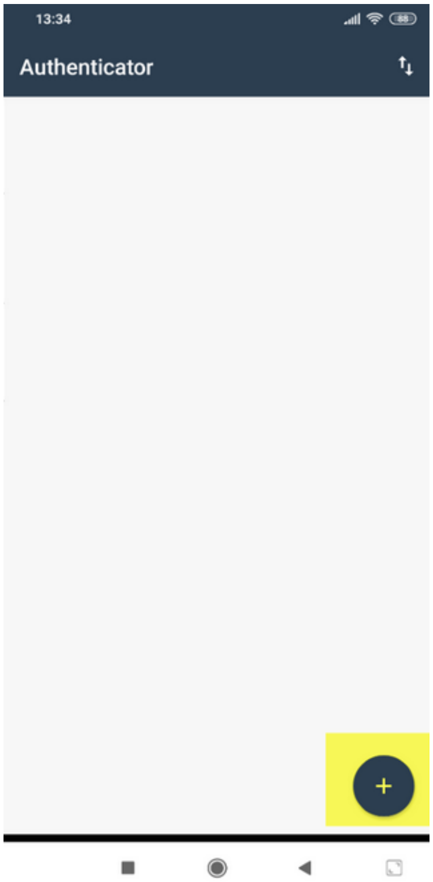
- Google Authenticator: https://apps.apple.com/us/app/google-authenticator/id388497605
- Microsoft Authenticator: https://apps.apple.com/app/microsoft-authenticator/id983156458

Android:

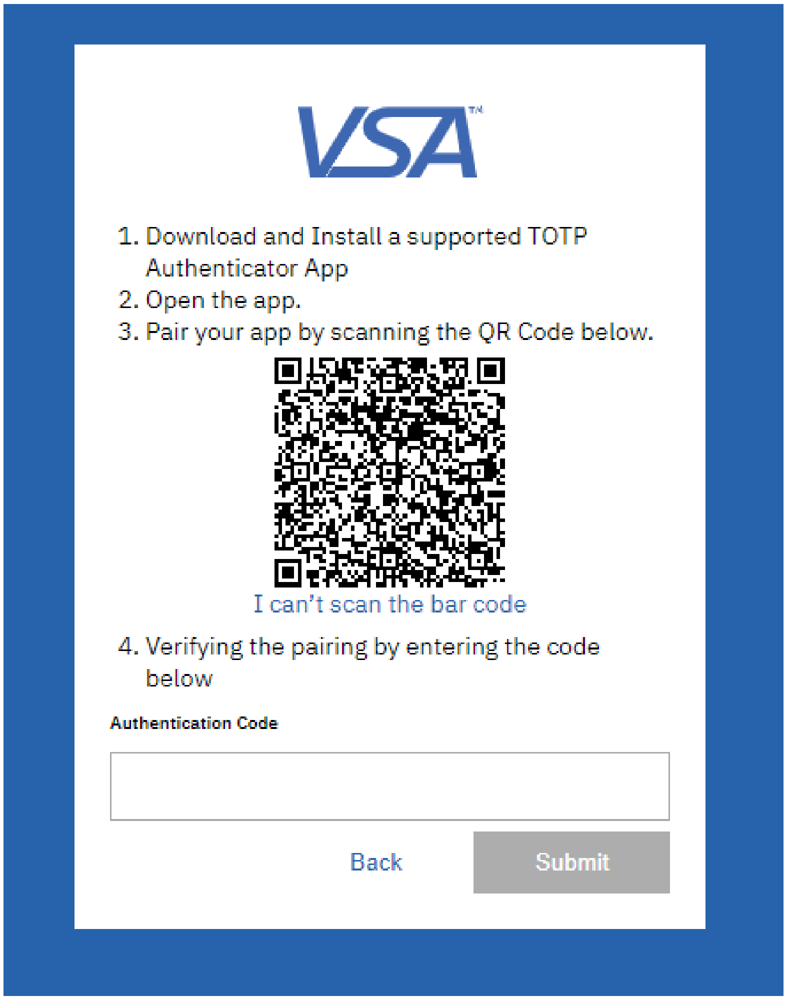
- Google Authenticator: https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2
- Microsoft Authenticator: https://play.google.com/store/apps/details?id=com.azure.authenticator&hl=en

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 VSA.

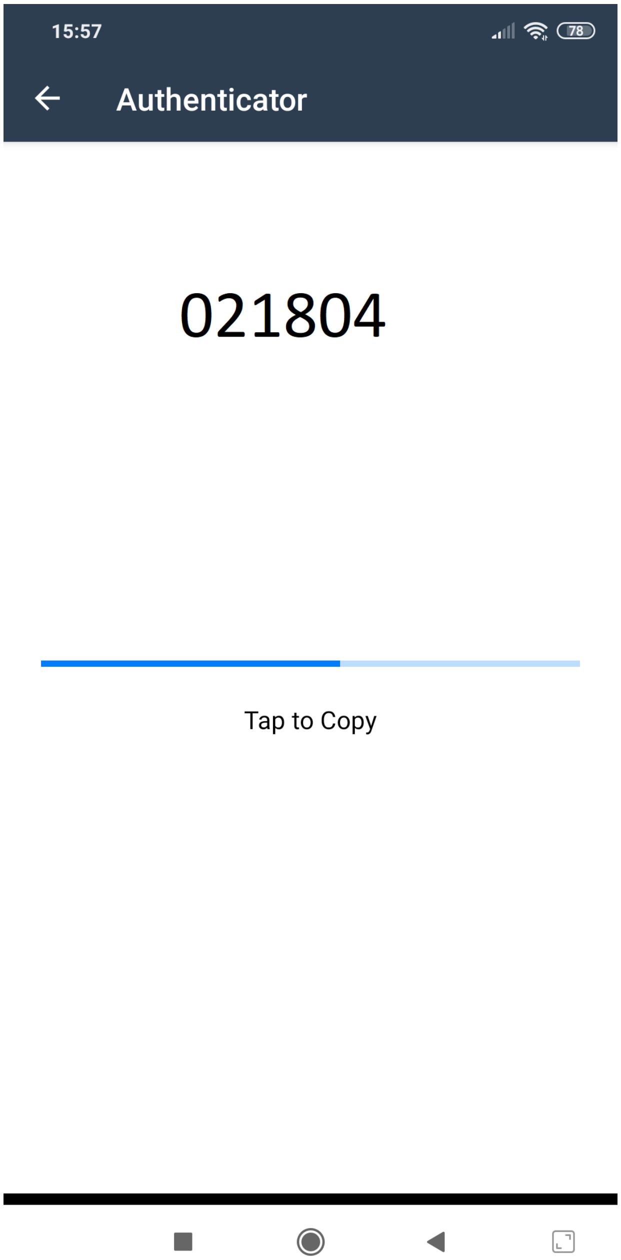


1. Download and Install a supported TOTP Authenticator App
2. Open the app.
3. Pair your app by scanning the QR Code below.

4. Verifying the pairing by entering the code below

Authentication Code

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



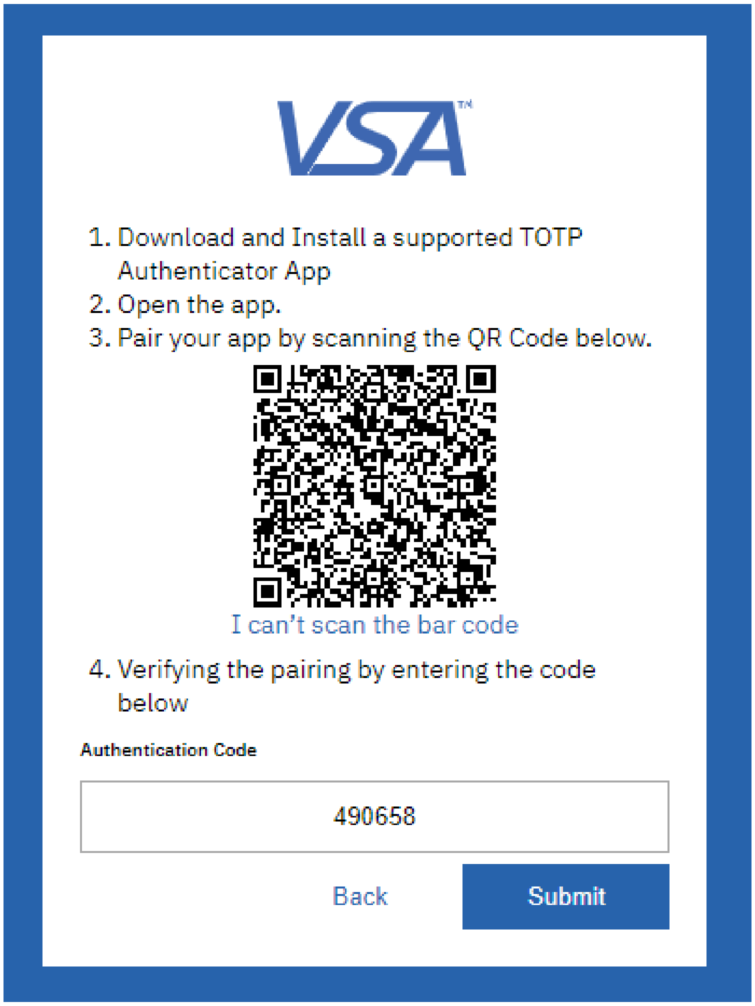
15:57

Authenticator

021804

Tap to Copy

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



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

4. Verifying the pairing by entering the code below

Authentication Code: 490658

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 VSA Account should be displayed on the Accounts list in the mobile application.

(See Two-Factor Authentication Subsequent Login for more information.)

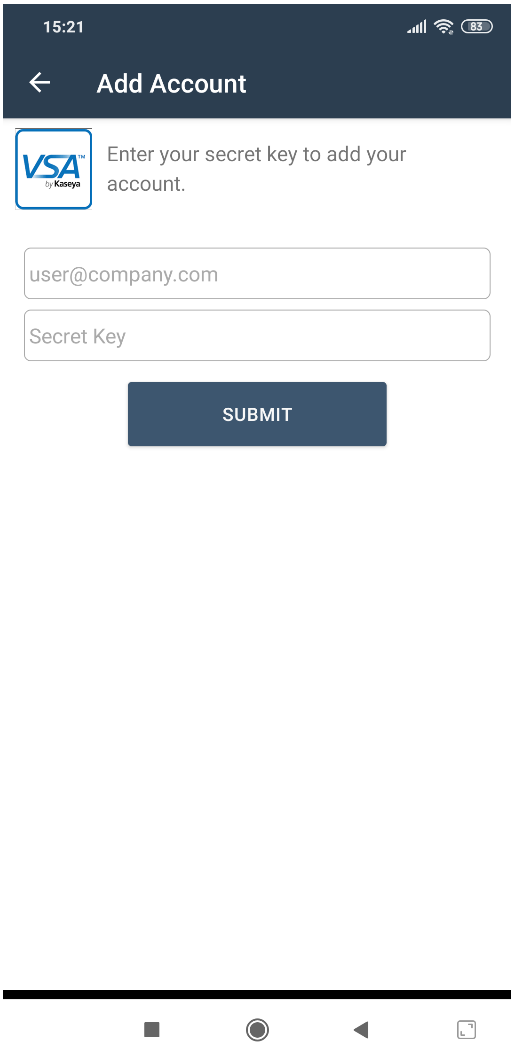
Workaround for mobile Authenticator application setup

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

1 Select Add an Account option in the installed mobile application.

2 Enter Username and the Key.

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



15:21

Add Account

Enter your secret key to add your account.

user@company.com

Secret Key

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

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

- If you have added your VSA 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 VSA account to the Authenticator application and have entered a valid Authentication code, delete your VSA Account in the mobile Authenticator application and complete 2FA steps from again.

Two-Factor Authentication at Tenant Level - Master Role Admin

Two-Factor Authentication Configuration and Monitoring

Users in the System and Master Role can configure 2FA feature within their tenant.

VSA Users that have read-write access to System > Server Management> **Logon Policy** settings can also view and configure the 2FA feature, depending on their role permissions.

2FA configuration in VSA includes the following functions:

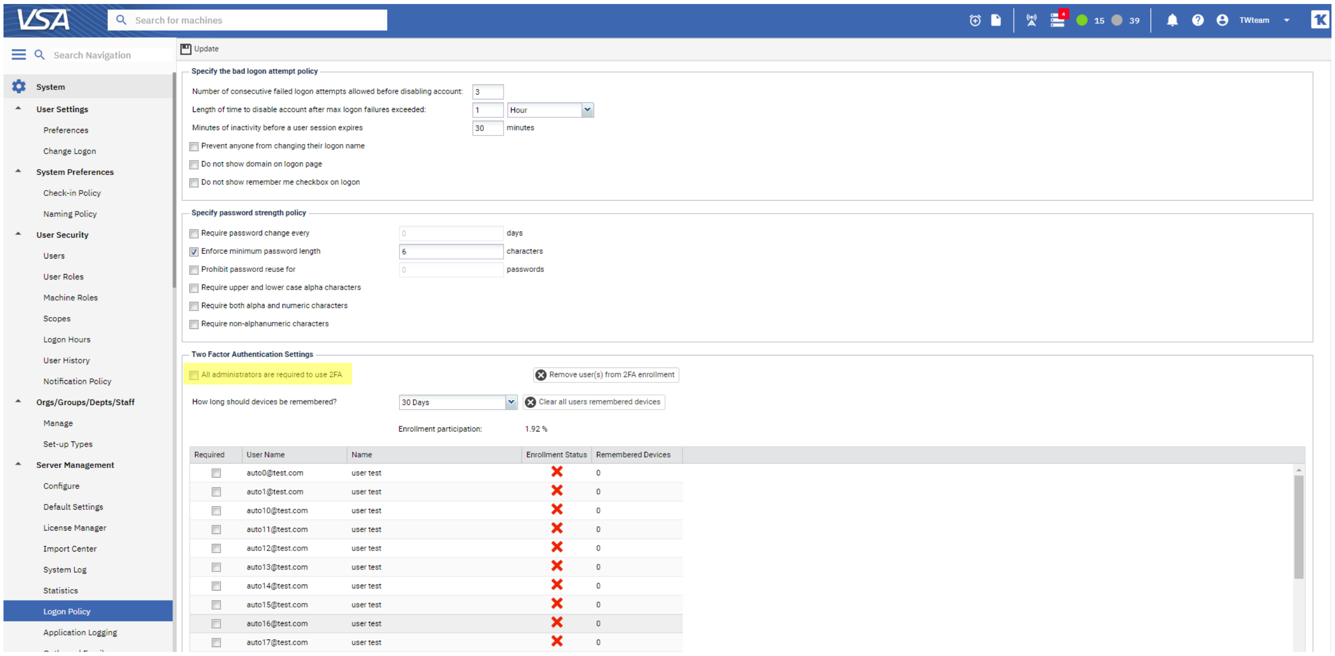
- Enforce VSA 2FA for a tenant when logging the VSA Admin Portal. 2FA enforcement can be applied to particular Users within a tenant organization.
- Monitor VSA 2FA enrollment process status within a tenant.
- Reset VSA 2FA for a User or multiple Users within a tenant.
- Reset VSA 2FA devices for a User or multiple Users within a tenant.

VSA 2FA Enforcement

By default, 2FA is set to optional for all VSA tenants. To add security to user accounts within a tenant, it is recommended that each tenant configures 2FA as a mandatory login process.

To enforce 2FA in VSA for all user within a tenant:

1. Login to VSA with the corresponding permissions.
2. Navigate to System > Server Management> **Logon Policy** page.
3. Enable the **All administrators are required to use 2FA** checkbox.



Specify the bad logon attempt policy

Number of consecutive failed logon attempts allowed before disabling account: 3

Length of time to disable account after max logon failures exceeded: 1 Hour

Minutes of inactivity before a user session expires 30 minutes

□ Prevent anyone from changing their logon name

□ Do not show domain on logon page

□ Do not show remember me checkbox on logon

Specify password strength policy

□ Require password change every 0 days

☑ Enforce minimum password length 6 characters

□ Prohibit password reuse for 0 passwords

□ Require upper and lower case alpha characters

□ Require both alpha and numeric characters

□ Require non-alphanumeric characters

Two Factor Authentication Settings

□ All administrators are required to use 2FA

Remove user(s) from 2FA enrollment

How long should devices be remembered? 30 Days

Clear all users remembered devices

Enrollment participation: 1.92 %

Required	User Name	Name	Enrollment Status	Remembered Devices
□	auto0@test.com	user test	✗	0
□	auto1@test.com	user test	✗	0
□	auto10@test.com	user test	✗	0
□	auto11@test.com	user test	✗	0
□	auto12@test.com	user test	✗	0
□	auto13@test.com	user test	✗	0
□	auto14@test.com	user test	✗	0
□	auto15@test.com	user test	✗	0
□	auto16@test.com	user test	✗	0
□	auto17@test.com	user test	✗	0

4 Save the changes.

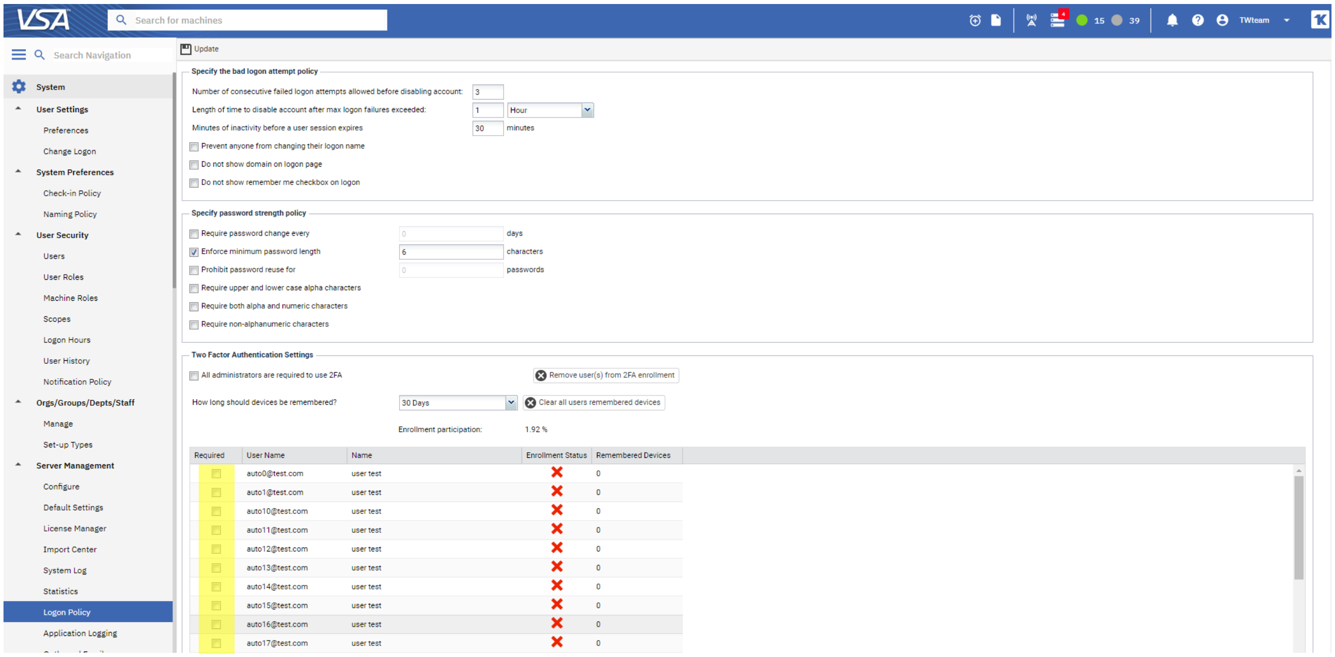
Now every user within the tenant will have to follow the 2FA process to login their VSA account.

To enforce 2FA in VSA for particular user(s) within a tenant:

1 Login VSA app with the corresponding permissions (see above).

2 Navigate to System > Server Management> **Logon Policy** page.

3 Select the users within a tenant that you would like to oblige to follow the 2FA process.



Specify the bad logon attempt policy

Number of consecutive failed logon attempts allowed before disabling account: 3

Length of time to disable account after max logon failures exceeded: 1 Hour

Minutes of inactivity before a user session expires 30 minutes

□ Prevent anyone from changing their logon name

□ Do not show domain on logon page

□ Do not show remember me checkbox on logon

Specify password strength policy

□ Require password change every 0 days

☑ Enforce minimum password length 6 characters

□ Prohibit password reuse for 0 passwords

□ Require upper and lower case alpha characters

□ Require both alpha and numeric characters

□ Require non-alphanumeric characters

Two Factor Authentication Settings

□ All administrators are required to use 2FA

Remove user(s) from 2FA enrollment

How long should devices be remembered? 30 Days

Clear all users remembered devices

Enrollment participation: 1.92 %

Required	User Name	Name	Enrollment Status	Remembered Devices
□	auto0@test.com	user test	✗	0
□	auto1@test.com	user test	✗	0
□	auto10@test.com	user test	✗	0
□	auto11@test.com	user test	✗	0
□	auto12@test.com	user test	✗	0
□	auto13@test.com	user test	✗	0
□	auto14@test.com	user test	✗	0
□	auto15@test.com	user test	✗	0
□	auto16@test.com	user test	✗	0
□	auto17@test.com	user test	✗	0

Note: If you do not have the checkboxes to select particular users, please make sure you have the **All administrators are required to use 2FA** checkbox unselected.

4 Save the changes.

Now the selected user within the tenant will have to follow the 2FA process to login their VSA account.

2-Factor Authentication Enrollment Process Monitoring

VSA Users with the corresponding permissions can monitor the status of 2FA enrollment process by Enrollment Status per each user within a tenant.

Currently, there are three 2FA Enrollment Status available:

✗ - user is not enrolled in VSA 2FA.

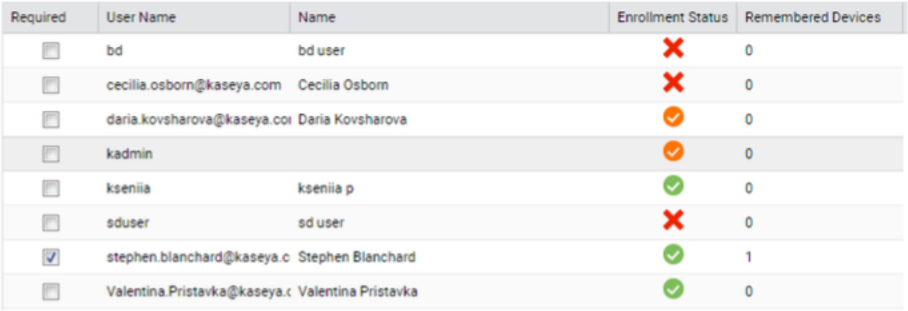
✓ - user is successfully enrolled in VSA 2FA.

✓ - user is partially enrolled in VSA 2FA. It means that user has not completed the 2FA enrollment process by entering the TOTP for some reason. These users will have to complete the 2FA enrollment process upon next log in.

To monitor 2FA Enrollment Status of each user:

1 Login VSA app with the corresponding permissions.

2 Navigate to System > Server Management> **Logon Policy** page.



Required	User Name	Name	Enrollment Status	Remembered Devices
☐	bd	bd user	✗	0
☐	cecilia.osborn@kaseya.com	Cecilia Osborn	✗	0
☐	daria.kovsharova@kaseya.coı	Daria Kovsharova	✓	0
☐	kadmin		✓	0
☐	kseniia	kseniia p	✓	0
☐	sduser	sd user	✗	0
☑	stephen.blanchard@kaseya.c	Stephen Blanchard	✓	1
☐	Valentina.Pristavka@kaseya.c	Valentina Pristavka	✓	0

2FA Rest Options

VSA Users with the corresponding permissions can reset the 2FA enrollment status for each user within a tenant in any 2FA Enrollment phase. This is helpful, for example, if users have completed the 2FA enrollment process, but for some reason they cannot log into VSA successfully.

There are 2 ways for a Master or System Role User to modify a user's 2FA enrollment:

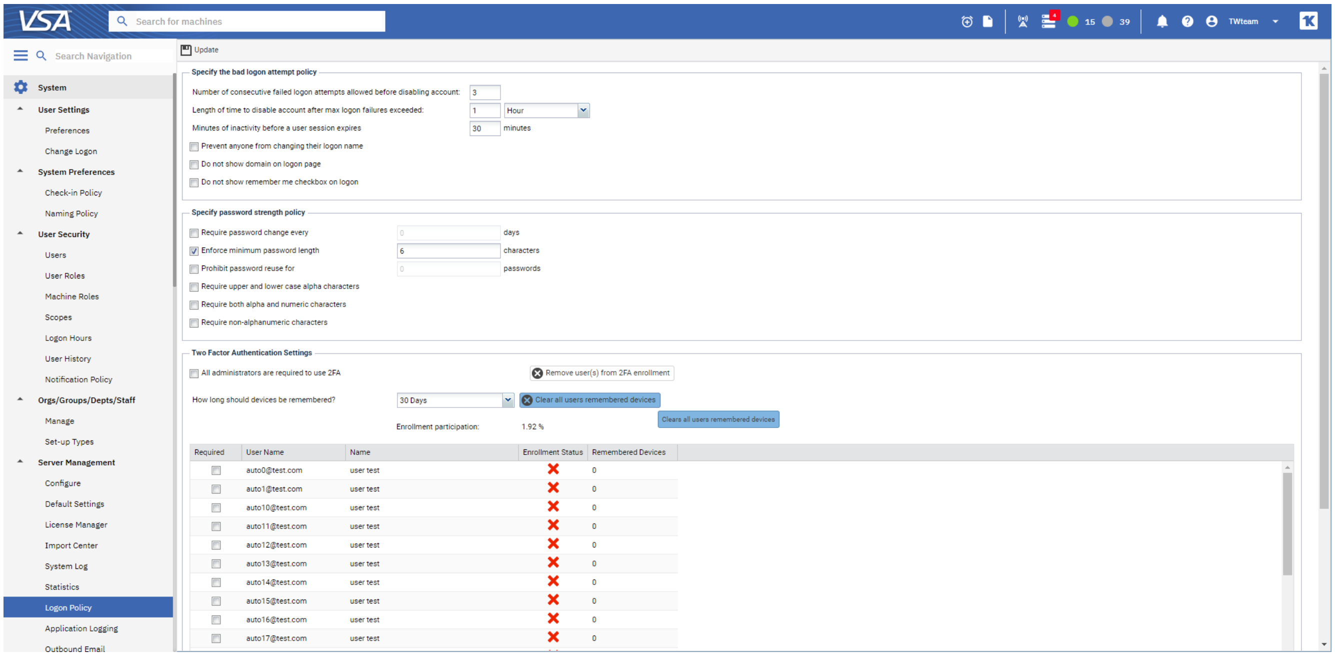
Step 1: By removing 2FA Remembered Devices for *all users* within a tenant.

> **Note:** Removing user's devices will not unenroll the User from 2FA. The user will have to enter a one-time password.

Step 2: By unenrolling a particular user or multiple users. This will also remove the user's remembered devices.

To remove 2FA Remembered Devices for all users

1. Log into VSA with the corresponding permissions.
2. Navigate to System > Server Management> **Logon Policy** page.
3. Click the **Clear all users remembered devices** button.



Specify the bad logon attempt policy

Number of consecutive failed logon attempts allowed before disabling account: 3

Length of time to disable account after max logon failures exceeded: 1 Hour

Minutes of inactivity before a user session expires 30 minutes

□ Prevent anyone from changing their logon name

□ Do not show domain on logon page

□ Do not show remember me checkbox on logon

Specify password strength policy

□ Require password change every 0 days

☑ Enforce minimum password length 6 characters

□ Prohibit password reuse for 0 passwords

□ Require upper and lower case alpha characters

□ Require both alpha and numeric characters

□ Require non-alphanumeric characters

Two Factor Authentication Settings

□ All administrators are required to use 2FA

How long should devices be remembered? 30 Days

Enrollment participation: 1.92 %

Required	User Name	Name	Enrollment Status	Remembered Devices
□	auto0@test.com	user test	✗	0
□	auto1@test.com	user test	✗	0
□	auto10@test.com	user test	✗	0
□	auto11@test.com	user test	✗	0
□	auto12@test.com	user test	✗	0
□	auto13@test.com	user test	✗	0
□	auto14@test.com	user test	✗	0
□	auto15@test.com	user test	✗	0
□	auto16@test.com	user test	✗	0
□	auto17@test.com	user test	✗	0

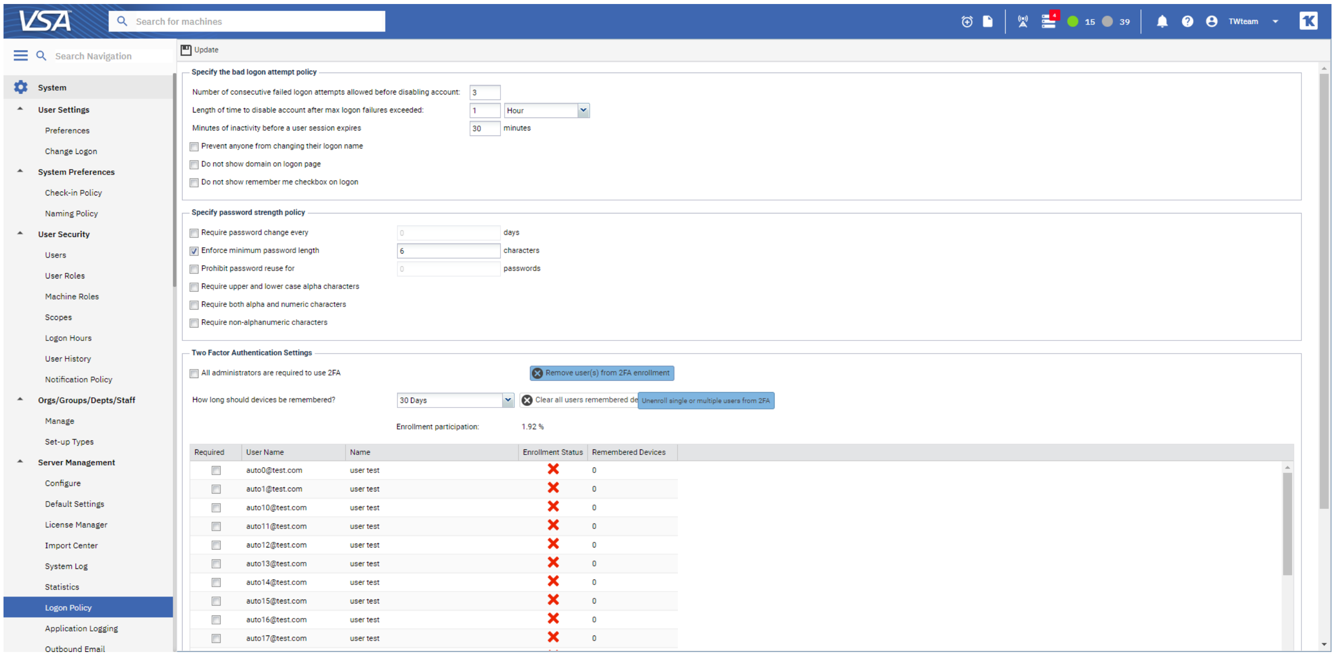
Note: The 2FA Enrollment Status for all users within a tenant will stay unchanged after clicking the **Clear all users remembered devices** button.

To unenroll a particular user or multiple users

1 Log into VSA with the corresponding permissions.

2 Navigate to System > Server Management> Logon Policy page.

3 Click the **Remove user(s) from 2FA Enrollment** button.



Specify the bad logon attempt policy

Number of consecutive failed logon attempts allowed before disabling account: 3

Length of time to disable account after max logon failures exceeded: 1 Hour

Minutes of inactivity before a user session expires 30 minutes

□ Prevent anyone from changing their logon name

□ Do not show domain on logon page

□ Do not show remember me checkbox on logon

Specify password strength policy

□ Require password change every 0 days

☑ Enforce minimum password length 6 characters

□ Prohibit password reuse for 0 passwords

□ Require upper and lower case alpha characters

□ Require both alpha and numeric characters

□ Require non-alphanumeric characters

Two Factor Authentication Settings

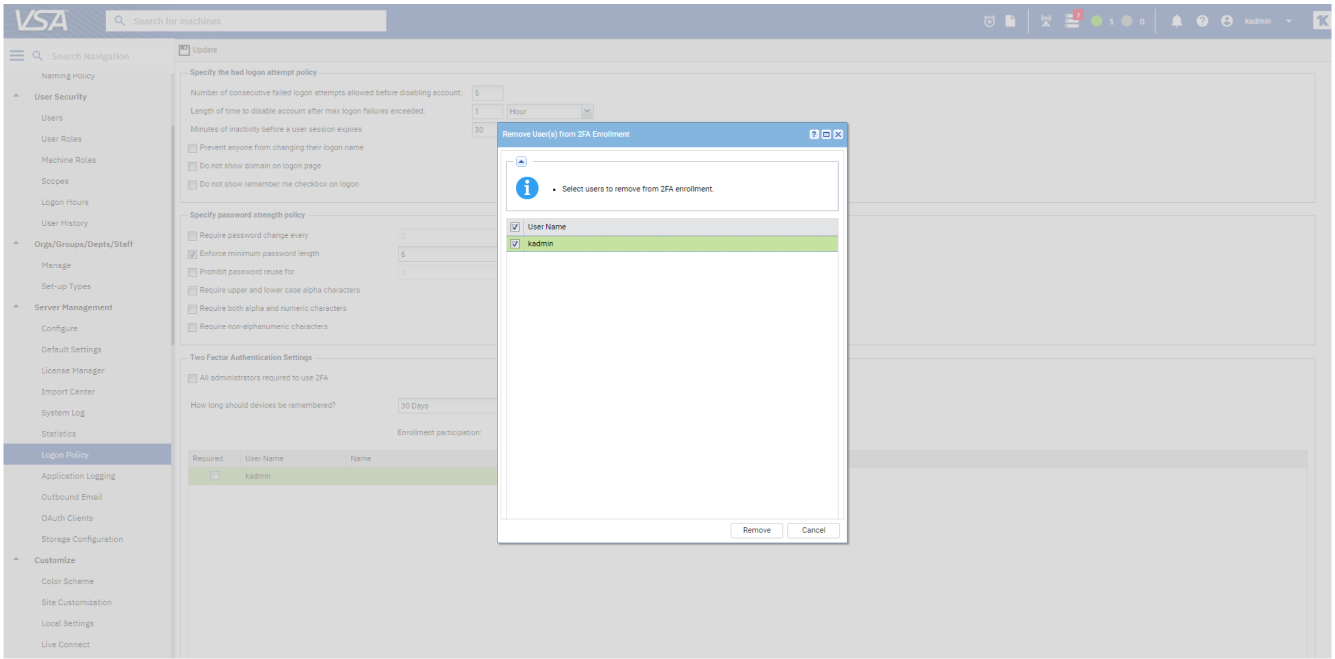
□ All administrators are required to use 2FA

How long should devices be remembered? 30 Days

Enrollment participation: 1.92 %

Required	User Name	Name	Enrollment Status	Remembered Devices
□	auto0@test.com	user test	✗	0
□	auto1@test.com	user test	✗	0
□	auto10@test.com	user test	✗	0
□	auto11@test.com	user test	✗	0
□	auto12@test.com	user test	✗	0
□	auto13@test.com	user test	✗	0
□	auto14@test.com	user test	✗	0
□	auto15@test.com	user test	✗	0
□	auto16@test.com	user test	✗	0
□	auto17@test.com	user test	✗	0

4 Select user(s) you would like to reset 2FA enrollment for.



Specify the bad logon attempt policy

Number of consecutive failed logon attempts allowed before disabling account: 5

Length of time to disable account after max logon failures exceeded: 1 Hour

Minutes of inactivity before a user session expires 30

□ Prevent anyone from changing their logon name

□ Do not show domain on logon page

□ Do not show remember me checkbox on logon

Specify password strength policy

□ Require password change every 0

☑ Enforce minimum password length 6

□ Prohibit password reuse for 0

□ Require upper and lower case alpha characters

□ Require both alpha and numeric characters

□ Require non-alphanumeric characters

Two Factor Authentication Settings

□ All administrators required to use 2FA

How long should devices be remembered? 30 Days

Enrollment participation:

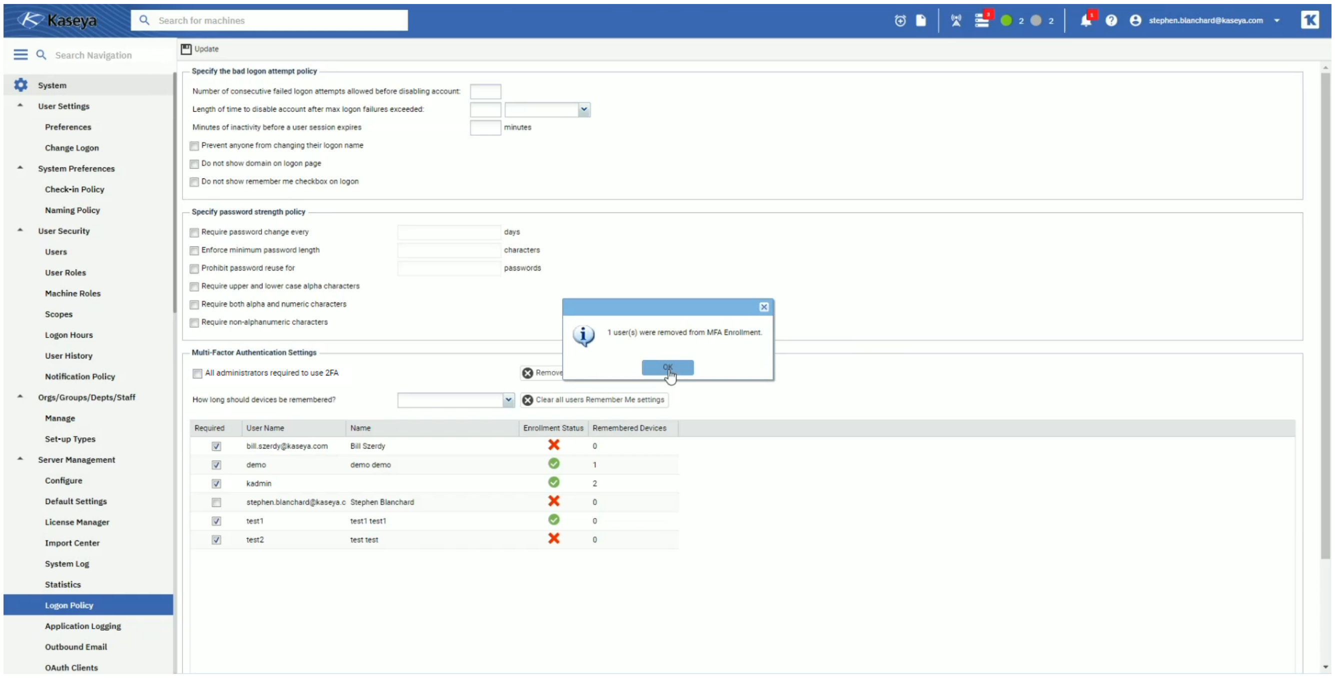
Required	User Name	Name
□	kadmin	

Remove User(s) from 2FA Enrollment

- Select users to remove from 2FA enrollment.

☑	User Name
☑	kadmin

5 Receive unenrollment confirmation for the select user(s).



Specify the bad logon attempt policy

Number of consecutive failed logon attempts allowed before disabling account:

Length of time to disable account after max logon failures exceeded:

Minutes of inactivity before a user session expires minutes

□ Prevent anyone from changing their logon name

□ Do not show domain on logon page

□ Do not show remember me checkbox on logon

Specify password strength policy

□ Require password change every days

□ Enforce minimum password length characters

□ Prohibit password reuse for passwords

□ Require upper and lower case alpha characters

□ Require both alpha and numeric characters

□ Require non-alphanumeric characters

Multi-Factor Authentication Settings

□ All administrators required to use 2FA

How long should devices be remembered?

1 user(s) were removed from MFA Enrollment.

Required	User Name	Name	Enrollment Status	Remembered Devices
☑	bill.szerdy@kaseya.com	Bill Szerdy	✗	0
☑	demo	demo demo	✓	1
☑	kadmin		✓	2
□	stephen.blanchard@kaseya.c	Stephen Blanchard	✗	0
☑	test1	test1 test1	✓	0
☑	test2	test test	✗	0

Note: Users removed from the 2FA Enrollment will have to complete the 2FA enrollment process next time they log into the VSA.