Security Officer Guide

Advanced Authentication

Version 5.4

MICRO FOCUS

Legal Notice

Contents

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate—day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with—for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ Web site in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **Add Comment** at the bottom of any page in the HTML version of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit community.netiq.com.

About this Book

Advanced Authentication user documentation is designed for security officers and describes how to manage users' authenticators.

Intended Audience

This book provides information for individuals responsible for understanding administration concepts and implementing a secure, distributed administration model.

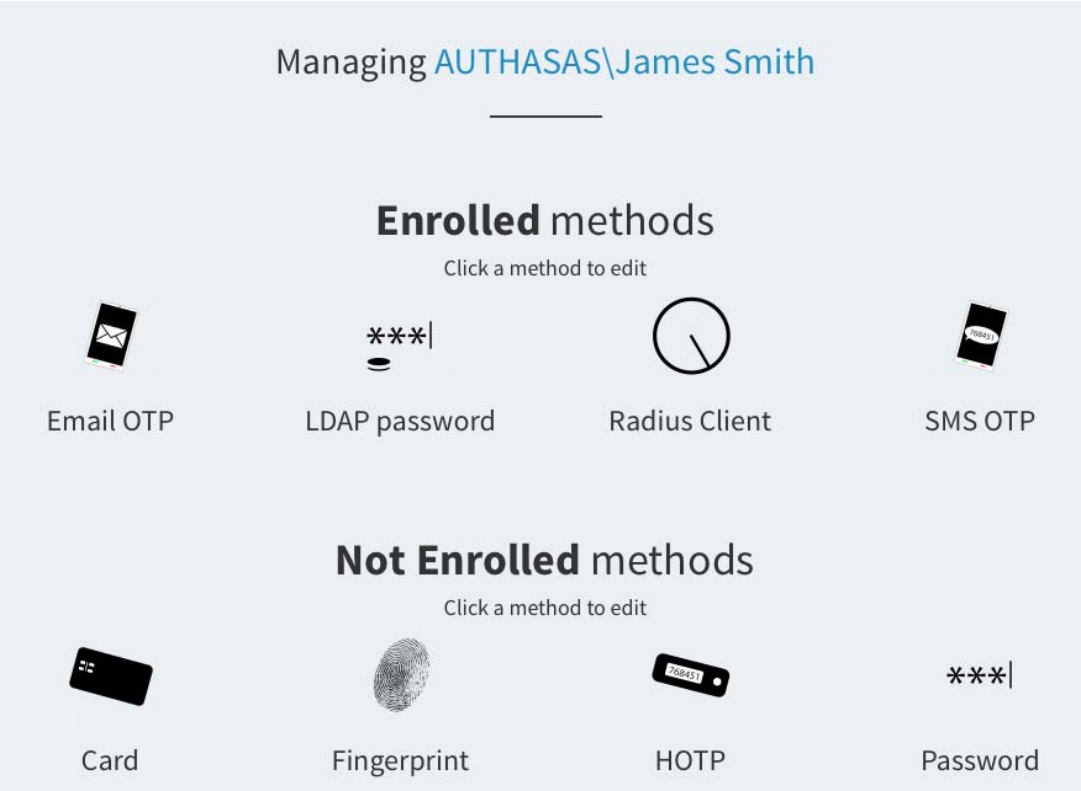
1 Authenticators Management

To use the Advanced Authentication a user needs to have at least one enrolled **authenticator**. Authenticator is a set of encrypted data, which contains your authentication data and which you can use to perform log on to Windows, MacOS, remote resources (if applicable) or Advanced Authentication Access Manager etc. Some of the authenticators (like **SMS**, **Email** and **RADIUS**) are enrolling automatically and if user needs to use only one or some of them, he/she can skip the enrollment stage.

The enrollment can be performed on the Advanced Authentication Helpdesk Portal. Ask your system administrator to provide you the URL.

1. Open the URL in your browser and you will see the **User name** prompt.
2. Enter your user name and click **Next** button.
3. Enter your password and click **Next** button. If the provided information is correct you will get access to the Helpdesk Portal.
4. Enter name of user which you need to manage. Click **Next**.
5. Enter user credentials (if applicable) to get access for user management.
6. You can change the language from the drop-down list on the top right corner of the Advanced Authentication Administrative Portal main page.

   The languages supported are: Arabic, Chinese Simplified, Chinese Traditional, Danish, Dutch, French, German, Italian, Japanese, Polish, Portuguese (Brazilian), Russian, Spanish, Hebrew, and Swedish.
7. Select one of the available methods to manage.



Methods which enroll automatically:

1. Email OTP
2. LDAP Password
3. Radius Client
4. SMS OTP

Not Enrolled methods:

1. Card
2. Emergency Password
3. Fingerprint
4. HOTP
5. Password (PIN)
6. PKI
7. NotarisID
8. Security Questions
9. Smartphone
10. TOTP
11. U2F
12. Voice Call
13. Swisscom Mobile ID Method

After enrollment a method will be moved to the **Enrolled methods** section.

To change a managed user click a user name in caption **Managing <username>** and then click **OK**.

An alternative way is to click your user name in top right corner and then click **Change user**.

From the same menu you can log out from the Helpdesk Portal. To do it click **Log Out**.

1.1 Card

NOTE: You must install Advanced Authentication Device Service before you enroll a card. Some card readers are supported only for Microsoft Windows. Contact your administrator for more information.

To enroll a card click the Card  icon.

Then follow the steps below:

1. You see a message `Press button "Save" to begin`.
2. You may enter a comment in **Comment** field. It should be a text like `my white card`.
3. Ensure that your card reader is connected to the machine.
4. Click **Save** button. You will see a message `Waiting for card...`
5. Tap a card on the reader. For a second you will see a message `Card has been detected`, then the Card enrollment page will be closed and you will see a message `Authenticator "Card" enrolled`.

TIP: If you see a message `Card Service unavailable` ensure that you have the Advanced Authentication Smartcard Service installed.

If you see a message `Card reader not detected` ensure that you have a card reader properly connected to the machine and the reader is available in Device Manager.Try to reconnect the reader.

You may get the message `Card reader detected` on Mac OS X. It is related to an improper work of a system service pcscd. To fix the issue, run Terminal and run the following commands:

```
kill pcscd
```

```
kill pcscdlite
```

Then reconnect the reader and re-initiate the enrollment.

To test the authenticator follow the next steps:

1. Click the Card icon in the **Enrolled methods** section.
2. Click **Test** button. You will see a message `Waiting for card...`
3. Tap a card on the reader. For a second you will see a message `Card has been detected`, then the Card enrollment page will be closed and you will see a message `Authenticator "Card" passed the test`. If the provided card is invalid you will see a message `Wrong smartcard`.

1.2 Email OTP

The Email OTP authentication method sends an email to your email address with a one-time password (OTP). You can use this OTP to authenticate withing a certain time frame.

This authenticator enrolls automatically and it's not possible to remove it.

To test the enrolled authenticator follow the steps below:

1. Click the Email OTP icon  in the **Enrolled methods** section.
2. Ensure that your email address (specified after the text **The email address your One-Time Password is sent to is:**) is valid. Contact your system administrator to change the email address if it's invalid.
3. Click **Test** button. In few seconds you will see a message `OTP password sent, please enter`.
4. Check your email. You should get an email message with one-time password.
5. Enter the OTP to the **Password** field.
6. Click **Next**. You will see a message `Authenticator "Email OTP" passed the test`. If the provided authenticator is invalid you will see a message `Wrong answer, try again.`

1.3 Emergency Password

The Emergency Password is a temporary password which can be enrolled for the users who forgot smartphone or lost a card. Enrollment of the Emergency Password authenticator by users is forbidden intentionally by security reason.

To enroll an emergency password authenticator click the Emergency Password icon in the Helpdesk Portal. Then follow the steps below:

1. You may enter a comment in Comment field. It should be a text like `lost a card`.
2. Specify **Password** and enter its **Confirmation** in the appropriate fields.
3. Check the **Start date (UTC)** and **End date (UTC)** when the authenticator is valid. You may change the dates if applicable.
4. You may also change the **Maximum logons** value (if applicable).

To test the enrolled authenticator follow the steps below:

1. Click the Emergency Password icon in the **Enrolled methods** section.
2. Click **Test** button.
3. Enter the emergency password to the **Password** field.
4. Click **Next**. You will see a message **Authenticator "Emergency Password" passed the test**. If the provided authenticator is invalid you will see a message **Wrong password**.

1.4 Fingerprint

TIP: Fingerprint enrollment is supported only on Microsoft Windows. You must install Advanced Authentication Device Service.

To enroll a card click the Fingerprint  icon.

Then follow the steps below:

1. You see a message **Press button "Save" and put your finger on the reader**.
2. You may enter a comment in **Comment** field. It should be a text like `left index finger`.
3. Ensure that your fingerprint reader is connected to the machine.
4. Click **Save** button. You will see a message **Put your finger on the reader**.
5. Put your finger in case of touch sensor or swipe your finger in case of swipe sensor. You will see a message **Authenticator "Fingerprint" added**.

IMPORTANT: It's strongly recommended to test the authenticator after enrollment. If you are not able to get a successful test, please delete the authenticator and enroll it again.

TIP: If you see a message `Fingerprint Service unavailable` ensure that you have the Advanced Authentication Smartcard Service installed.

TIP: If you see a message `Enroll failed: Fingerprint reader is not connected` ensure that a fingerprint reader is properly connected to the machine and the reader is available in Device Manager.

To test the authenticator follow the next steps:

1. Click the Fingerprint icon in the **Enrolled methods** section.
2. Click **Test** button. You will see a message `Put your finger on the reader`
3. Put your finger in case of touch sensor or swipe your finger in case of swipe sensor. You will see a message `Authenticator "Fingerprint" passed the test`. If the provided fingerprint is invalid you will see a message `Mismatch`.

1.5 HOTP

HOTP is a counter-based one-time password. This method uses a counter that is in sync with your HOTP token and the server.

To enroll the HOTP authenticator you should follow recommendations of your system administrator. The following cases are possible:

1. A new token is already assigned to your account and enrollment is not needed.
2. A used token is assigned to your account and the HOTP counter synchronization is required.
3. You get an information about serial number of your token and need to assign it to your account.
4. You want to enroll the authenticator manually.

To enroll a HOTP authenticator click the HOTP  icon.

B. A used token is assigned to your account and the HOTP counter synchronization is required.

To perform the HOTP counter synchronization follow the steps below:

1. Click the HOTP icon in the **Enrolled methods** section.
2. Enter an OTP from your token, or in case of an OATH HOTP compliant YubiKey token usage connect your token to the workstation, set cursor to the **HOTP 1** field and press the token's button.
3. Repeat the actions described in point 3 for the **HOTP 2** and **HOTP 3** fields.
4. Click **Save** button.

C. You get an information about serial number of your token and need to assign it to your account.

To assign an existing token for your account follow the steps below:

1. Click the HOTP icon in the **Enrolled methods** section.
2. You can specify an optional comment in **Comment** field.
3. Enter the token's serial number provided by your system administrator to the **OATH Token Serial** field.
4. Enter three consecutive one-time passwords to the **HOTP 1**, **HOTP 2**, **HOTP 3** fields.
5. Click **Save** button.

D. You want to enroll the authenticator manually.

To enroll a new authenticator manually follow the steps below:

1. Click the HOTP icon in the **Enrolled methods** section.
2. You can specify an optional comment in **Comment** field.
3. Enter three consecutive one-time passwords to the **HOTP 1**, **HOTP 2**, **HOTP 3** fields.
4. Enter 40 hexadecimal characters secret code to the **Secret (if you know)** field.
5. Click **Save** button.

1.6 LDAP Password

The LDAP password is a password of your corporate account.

This authenticator enrolls automatically and it's not possible to remove it.

To test the enrolled authenticator follow the steps below:

1. Click the LDAP password  icon in the **Enrolled methods** section.
2. Click **Test** button.
3. Enter your password to the **Password** field.
4. Click **Next**. You will see a message `Authenticator "LDAP password" passed the test`. If the provided authenticator is invalid you will see a message `Invalid credentials`.

1.7 NotarisID

To enroll a NotarisID authenticator, perform the following steps:

1. Click the NotarisID  icon.
2. Enter a comment in the **Comment** text box.
3. Enter your username in the **NotarisID** username text box.
4. Click **Save** to save the enrollment.

To test the NotarisID authenticator, you need to use the NotarisID smartphone app with your registered account and perform the following steps:

1. Click the NotarisID  icon in the **Enrolled methods** section.
2. Click **Test**. The following message is displayed:

   `The user should accept your request with his/her smartphone app`
3. Open the NotarisID smartphone app and enter your PIN code.
4. Tap the string `Inloggen bij:` ... and then tap  to sign the request. A message `Authenticator "NotarisID" passed the test` is displayed.

   An authentication request can be rejected only by time out. If you tap  to reject the request, the authentication is not rejected because NotarisID does not notify Advanced Authentication appliance about the rejection.

1.8 Password (PIN)

The Password (PIN) authenticator is a password stored in the Advanced Authentication appliance, that is not connected to your corporate directory. This could be a PIN or simple password.

To enroll a password (PIN) click the Password (PIN)  icon.

Then follow the steps below:

1. You can specify an optional comment in **Comment** field.
2. Enter a **Password (PIN)** and its **Confirmation** in the appropriate fields. The password (PIN) must be not less 5 characters (by default, it may be changed by your system administrator).
3. Click **Save** button. You will see a message `Authenticator "Password (PIN)" added`.

To test the authenticator follow the next steps:

1. Click the Password (PIN) icon in the **Enrolled methods** section.
2. Click **Test** button.

3. Enter your password (PIN).
4. Click **Next**. You will see a message `Authenticator "Password (PIN)" passed the test`. If the provided authenticator is invalid you will see a message `Wrong password (PIN)`.

WARNING: You will not get notification about the password (PIN) expiration. It's required to sign in to the Self-Service Portal and change the password each 42 days.

1.9 PKI

NOTE: You must install Advanced Authentication Device Service for the PKI method enrollment.

To enroll a PKI method, perform the following steps:

1. Click the PKI icon  .
2. Click **Save** to begin the enrollment.
3. Enter a comment in **Comment**. For example, `black crypto stick`.
4. A message `Waiting for card....` is displayed. Present your card or plug in your crypto stick to the machine.
5. A message `Use an existing certificate or generate a key pair` is displayed. Select a key from **Key** or leave the **Generate a key pair** option as blank.
6. Enter the PIN code of the device in **PIN**.
7. Click **Save**. The message `Authenticator "PKI" enrolled` is displayed.

NOTE: If an error `Card reader connected` is displayed, ensure that a card is presented on the reader/ crypto stick is connected.

If an error `Enroll failed: Cannot check revocation status for …` is displayed, then the certificate on your device has no information about where to find the revocation status, or the information is presented but the Certificate Authority is not available to check the revocation status.

If an error `Card service unavailable` is displayed, restart your machine.

If an error `Key not found. Wrong Card?` is displayed, you might have enrolled the PKI authenticator in RDP session. Re-enroll the authenticator in normal session.

The following unexpected error codes (the errors are from a PKCS#11 module) could be displayed:

- `CKR_DEVICE_ERROR:` The token or USB slot is broken. Try to use a different USB slot.
- `CKR_DEVICE_MEMORY`: No space left on token or other problems with the token's memory.
- `CKR_MECHANISM_INVALID:` An invalid mechanism was specified to the cryptographic operation.
- `CKR_PIN_EXPIRED`: Ensure that the card has been initialized, or you do not use the default PIN and the PIN has not expired.
- `CKR_PIN_LOCKED:` The user PIN is locked.
- `CKR_TOKEN_NOT_RECOGNIZED`: The token has not been recognized.
- `OPERATION FAILED:` Contact your system administrator to analyze the debug logs.

To test the authenticator, perform the following steps:

1. Click the PKI icon in the **Enrolled methods** section.
2. Click **Test**. A message `Waiting for card...` is displayed.
3. Present your card or connect your crypto stick to the machine.
4. Enter PIN code of the device in **PIN**. A message `Authenticator "PKI" passed the test` is displayed. If the authenticator is invalid, a message `Wrong card` is displayed.

1.10 Radius Client

The Radius Client authentication method forwards your authentication request to a third-party Radius Server.

This authenticator enrolls automatically and it's not possible to remove it.

By default a user name from your corporate directory is used. To change it specify a required name in the **User name** field. Then click **Save** button.

To test the enrolled authenticator follow the steps below:

1. Click the Radius Client  icon in the **Enrolled methods** section.
2. Click **Test** button.
3. Enter Radius password to the **Password** field.
4. Click **Next**. You will see a message `Authenticator "Radius Client" passed the test.`

1.11 Security Questions

The Security Questions authenticator allows you to enroll answers to an administrator-defined number of security questions. When you authenticate using security questions, Advanced Authentication asks you all of the security questions or a subset of the security questions.

To enroll an authenticator click the Security Questions  icon.

Then follow the steps below:

1. You can specify an optional comment in **Comment** field.
2. Enter answers to the security questions. Each answer must contain not less 1 character (by default, it may be changed by your system administrator).
3. Click **Save** button. You will see a message `Authenticator "Security Questions" added.`

To test the authenticator follow the next steps:

1. Click the Security Questions icon in the **Enrolled methods** section.
2. Click **Test** button.
3. Enter answers to the security questions.
4. Click **Next**. You will see a message `Authenticator "Security Questions" passed the test`. If at least one of the provided answers is invalid you will see a message `Wrong answers`.

1.12 Smartphone

TIP: To enroll the Smartphone authenticator it's required to use the Advanced Authentication smartphone app (Apple iOS app (https://itunes.apple.com/us/app/netiq-advanced-authentication/id843545585), Google Android app (https://play.google.com/store/apps/details?id=com.netiq.oathtoken)).

To enroll a smartphone authenticator click the Smartphone  icon.

Then follow the steps below:

1. You see a message `Press button "Save" to start smartphone enrolling`.
2. You may enter a comment in **Comment** field. It should be a text like `my iPhone`.
3. Click **Save** button. You will see a QR code.
4. Move a cursor out of the QR code and open the Advanced Authentication smartphone app.

5. Tap **Offline authentication** button in the app.
6. Tap **+** button to add a new authenticator in the app.
7. Use camera of your smartphone to scan the QR code.
8. You will see a message `Authenticator "Smartphone" added`.
9. Enter your username and an optional comment in the smartphone app.
10. Save the authenticator on your smartphone.

TIP: You may get the error `Enroll failed: Enroll timeout` if you didn't enroll the authenticator during few minutes. In this case refresh the browser page and initialize enrollment again.

TIP: If you are not able to scan the QR code with Advanced Authentication app, try to do the following:

1. try to scan the zoomed QR code by making a zoom of the page to 125-150%.
2. ensure that nothing overlaps the QR code (mouse cursor, text).

To test the authenticator follow the next steps:

1. Click the Smartphone icon in the **Enrolled methods** section.
2. Click **Test** button. You will see a message `Waiting for smartphone data...`
3. Open the Advanced Authentication smartphone app. You will get an authentication request message.
4. Tap **Accept** button to accept the authentication request. You will see the message `Authenticator "Smartphone" passed the test`. If you tap the **Reject** button, the authentication will be declined and you will see the message **Auth rejected**. If you ignored the authentication request, in a couple of minutes you will get a message `Auth confirmation timeout`.

1.13 SMS OTP

The SMS OTP authentication method uses your mobile phone number from your account attribute. The authenticator sends an SMS message to your mobile phone. The message contains One-Time Password (OTP). You can use this OTP to authenticate withing a certain time frame.

This authenticator enrolls automatically and it's not possible to remove it.

To test the enrolled authenticator follow the steps below:

1. Click the SMS OTP  icon in the **Enrolled methods** section.
2. Ensure that your mobile phone number (specified after the text **The mobile number where an SMS OTP is sent:**) is valid. Contact your system administrator to change the mobile number if it's invalid.
3. Click **Test** button. In few seconds you will see a message `OTP password sent, please enter`.
4. Check your SMS. You should get an SMS message with one-time password.
5. Enter the OTP to the **Password** field.
6. Click **Next**. You will see a message `Authenticator "SMS OTP" passed the test`. If the provided authenticator is invalid you will see a message `Wrong answer, try again`.

1.14 TOTP

TOTP is a time-based one-time password. This method uses a predefined time step, which is equal to 30 seconds by default. It means that each 30 seconds a new one-time password will be generated.

To enroll the TOTP authenticator you should follow recommendations of your system administrator. TOTP method supports different cases of usage:

1. Using Advanced Authentication smartphone app (Apple iOS ap (https://itunes.apple.com/us/app/netiq-advanced-authentication/id843545585), Google Android app (https://play.google.com/store/apps/details?id=com.netiq.oathtoken)).

2. Using Google Authenticator app.
3. Using OATH TOTP compliant hardware token.
4. Using OATH TOTP compliant software token.

WARNING: Format of QR codes for the Advanced Authentication and Google Authenticator apps are different, so you need to ask your system administrator which of the apps you should use.

To enroll a TOTP authenticator click the TOTP  icon.

A. Using Advanced Authentication smartphone app

In you want to enroll an authenticator using Advanced Authentication smartphone app follow the next steps:

1. You may enter a comment in **Comment** field. It should be a text like `my iPhone`.
2. Move a cursor out of the QR code and open the Advanced Authentication smartphone app.
3. Tap **Offline authentication** button in the app.
4. Tap **+** button to add a new authenticator in the app.
5. Use camera of your smartphone to scan the QR code.
6. Click **Save** button.
7. You will see a message `Authenticator "TOTP" added`.
8. Enter your username and an optional comment in the smartphone app.
9. Save the authenticator on your smartphone.

TIP: If you are not able to scan the QR code with Advanced Authentication app, try to do the following:

---

1. try to scan the zoomed QR code by making a zoom of the page to 125-150%.
2. ensure that nothing overlaps the QR code (mouse cursor, text).
3. try to scan it using the Google Authenticator app.

If it doesn't work, contact your system administrator.

B. Using Google Authenticator app

Follow the steps below to enroll an autheticator using the Google Authenticator app:

1. You may enter a comment in **Comment** field. It should be a text like `my iPhone`.
2. Move a cursor out of the QR code and open the Google Authenticator app.
3. Tap **BEGIN SETUP** text in the app.
4. Tap **Scan barcode** button to add a new authenticator in the app.
5. Use camera of your smartphone to scan the QR code.
6. Click **Save** button.
7. You will see a message **Authenticator "TOTP" added**.

TIP: You may get the `Invalid barcode` error. It means that probably the QR code is compatible with Advanced Authentication app.

C. Using OATH TOTP compliant hardware token

To enroll OATH TOTP compliant hardware token follow the steps below:

1. You may enter a comment in **Comment** field. It should be a text like `HID token`.
2. Enter your token's serial number to the **OATH Token Serial** field. You may get the information on back side of your token.
3. Press the token's button and enter the OTP to the **OTP** field.
4. Click **Save** button.
5. You will see a message `Authenticator "TOTP" added`.

D. Using OATH TOTP compliant software token

To enroll OATH TOTP compliant software token follow the steps below:

1. You may enter a comment in **Comment** field. It should be a text like `A phone app`.
2. Expand the **Enter TOTP secret manually**.
3. Enter 40 hexadecimal characters in **Secret** field.
4. Check the **Google Authenticator format of secret (Base32)** option if you use the Google Authenticator app.
5. Change the **Period** value if required (30 seconds by default).
6. Click **Save** button.
7. You will see a message `Authenticator "TOTP" added`.

1.15 U2F

TIP: You must install Advanced Authentication Device Service for all browsers except Google Chrome. It contains a built-in module.

To enroll a FIDO U2F authenticator click the U2F  icon.

Then follow the steps below:

1. You see a message `Press button "Save" to begin enrolling`.
2. You may enter a comment in **Comment** field. It should be a text like `YubiKey token`.
3. Ensure that your FIDO U2F token is properly connected to the machine.
4. Click **Save** button. You will see a message `Please touch the flashing U2F device now.` You may be prompted to allow the site permissions to access your security keys.
5. Look at the FIDO U2F token. If it's flashing, press a FIDO U2F button. You will see a message `Authenticator "U2F" enrolled`. If it doesn't flash wait 10 seconds, if it still doesn't flash then reconnect your token and repeat the steps.

TIP: If you see a message `Cannot reach local FIDO U2F Service. Ask your admin to enable it. You may use Google Chrome browser, it has a built-in U2F support` ensure that you have the Advanced Authentication FIDO U2F Service installed.

TIP: If you see a message `Timeout. Press "Save" to start again` click **Save** again.

To test the authenticator follow the next steps:

1. Click the U2F icon in the **Enrolled methods** section.
2. Click **Test** button. You will see a message `Please touch the flashing U2F device now. You may be prompted to allow the site permissions to access your security keys`
3. Press a FIDO U2F button. You will see a message `Authenticator "U2F" passed the test`. If the provided card is invalid you will see a message `Token is not registered`.

1.16 Voice Call

The Voice Call authenticator initiates a phone call to your mobile number. The phone call asks you to enter your PIN. You need to specify the PIN during enrollment.

To enroll a Voice Call authenticator click the Voice  icon.

Then follow the steps below:

1. Ensure that a valid phone number is set in the field **The mobile number where a Voicecall is sent:**.
2. You can specify an optional comment in **Comment** field.
3. Specify a **PIN**. By default it must contain at least 3 digits.
4. Click **Save** button. You will see a message `Authenticator "Voice" added`.

TIP: You may get the error `Enroll failed: User has no phone number. Please contact administrators/helpdesk and register your phone`. In this case contact your system administrator and ask to add your phone number for your account.

To test the authenticator follow the next steps:

1. Click the Voice icon in the **Enrolled methods** section.
2. Click **Test** button.
3. Take up the phone and listen to the answerphone.
4. Enter your PIN and tap hash sign (#).
5. You will see a message `Authenticator "Voice" passed the test`. If the provided PIN is invalid you will see a message `Wrong PIN`.

WARNING: You will not get notification about the PIN expiration. It's required to sign in to the Self-Service Portal and change the PIN each 42 days.

1.17 Swisscom Mobile ID Method

The Swisscom Mobile ID authentication method uses your mobile phone number from your account attribute. The authenticator sends an authentication request to your mobile phone. You need to accept it.

This authenticator enrolls automatically and it is not possible to remove it.

To test the Swisscom Mobile ID authenticator, click the Swisscom Mobile ID  icon in the **Enrolled methods** section and perform the following steps:

1. Click **Test**. A message is displayed indicating that the you must accept the request on the mobile phone.
2. Accept the request. A message `Authenticator "Swisscom Mobile ID" passed the test` is displayed.

2 Sharing Authenticators

You can allow users to authenticate to another user’s account by using their own authenticators. For example, if the sharing authenticator option is enabled, the secretary's account can be linked to the account of boss and the secretary will be able to authenticate to the account of boss by using her own authenticators.

The authenticators that can be linked are: TOTP, HOTP, Password, Fingerprint, Card, and FIDO U2F.

To share the authenticators of a user with another user, perform the following steps:

1. Login and specify the name of the user to whom you want to link the authenticators to.
2. Click **Linked Authenticators** tab on the screen.
3. Specify the user name whose authenticator you want to use. For example, if you want to use secretary's fingerprint to authenticate to the account of boss, specify the name as Secretary-Fingerprint.
4. Click **Save**.

   Secretary will now be able to authenticate to the account of boss by authenticating with her own fingerprint.