User Guide

Advanced Authentication

Version 5.6

NetIQ

Legal Notices

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 all users and describes how to enroll authenticators and use the assigned authentication chains for different endpoints (Windows Client, MacOS Client, and Access Manager Advanced Authentication plug-in).

Intended Audience

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

1 Authenticators Management

To perform authentication with Advanced Authentication you must have at least one enrolled authenticator. An authenticator is a set of encrypted data that contains your authentication data which you can use to log on to Windows, MacOS, remote resources (if applicable) or Advanced Authentication Access Manager, and so on. Some of the authenticators such as **SMS**, **Email**, **Voice OTP, Swisscom Mobile ID, LDAP Password** and **RADIUS** enroll automatically for default category and other categories added. If you need to use only one or some of them, you can skip the enrollment stage.

You can enroll the authenticators on the Advanced Authentication Self-Service Portal. Ask your system administrator to provide you the URL.

1. Open the URL in your browser.
2. Enter your user name and password.
3. Click **Next**.
4. Select the language from the drop-down list next to **User name**.

   You can also 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, and Swedish.

   If the information you provided is correct, you can access the Self-Service Portal.

NOTE: A set of **Not Enrolled methods** may vary. Contact your system administrator if you do not see a method that you need to enroll.

5. Select a method to enroll.

Methods that enroll automatically are:

1. Email OTP
2. LDAP Password
3. Radius Client
4. SMS OTP
5. Swisscom Mobile ID
6. Voice OTP

Methods that can be enrolled by a security officer only are:

1. Emergency Password

Not Enrolled methods:

1. Bluetooth
2. Card
3. Email OTP
4. Fingerprint
5. HOTP
6. LDAP Password

7. Password (PIN)
8. PKI
9. Radius Client
10. Security Questions
11. Smartphone
12. SMS OTP
13. Swisscom Mobile ID
14. TOTP
15. U2F
16. Voice

After the enrollment, a method is moved to the **Enrolled methods** section.

To re-enroll an existing authenticator, click the enrolled method, change settings (if applicable) and click **Save**. To delete an existing authenticator, click **Delete**.

To delete all your user data including the enrolled methods, click **Delete me** from your user name drop-down list in top right corner of Self-Service Portal. Click **OK** in the confirmation message to delete all your user data.

NOTE: **Delete me** option can be hidden by administrator.

To log out from the Self-Service Portal, click your user name in top right corner and then click **Log Out**.

1.1 Bluetooth

The Bluetooth authentication method allows to authenticate using your Bluetooth enabled mobile device.

NOTE: To use the Bluetooth method for authentication, you must install the Advanced Authentication Device Service. For more information on Device Service, see Advanced Authentication - Device Service guide.

To enroll the Bluetooth method perform the following steps:

1. Click the Bluetooth  icon.
2. Specify a comment in **Comment** field, if required.
3. Select the required category from the **Category** list, if applicable.
4. Turn on the Bluetooth in your mobile device and also ensure that it is discoverable to other Bluetooth devices.
5. Select your Bluetooth enabled mobile device from the list.

   NOTE: If your mobile device is not listed, click **Refresh list** to reload the mobile devices.

   ---

6. Click **Save.**

To test the authenticator perform the following steps:

NOTE: During authentication, your mobile device can just be discoverable to only the paired devices.

1. Click the Bluetooth icon in the **Enrolled methods** section.
2. Click **Test.** A message `Waiting for Bluetooth service` is displayed and then a message is displayed indicating the result of the test.

1.2 Card

TIP: You must install the Advanced Authentication Device Service before you enroll a card. For more information on Device Service, see the *Advanced Authentication - Device Service* guide. Some card readers are supported only for Microsoft Windows. Contact your administrator for more information.

To enroll a Card, perform the following steps:

1. Click the Card  icon.

   A message `Press button "Save" to begin` is displayed.
2. Enter a comment in **Comment**.

   Ensure that your card reader is connected to the machine.
3. Select the required category from the **Category** list.
4. Click **Save**. A message `Waiting for card is displayed.`
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`.

1.3 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 within a certain time frame.

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

NOTE: If there is no email address in the account profile for the user in the repository, then the Email method is not enrolled automatically. However, you can manually enroll the Email method from the **Not Enrolled methods** section, by entering the email address and then clicking **Save**.

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. Change the email address if it is 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`.

1.4 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. In the **Add Fingerprint authenticator** screen, enter a comment in **Comment** field, if required.
2. Select the required category from the **Category** list.
3. Click on the required finger for enrollment.
4. Place your finger on the reader or swipe your finger on the swipe sensor.
5. Repeat steps 2-3 to add more fingers for authentication.

   NOTE: Number of fingers to be enrolled and the number of scans performed for each finger will be mentioned on the **Add Fingerprint authenticator** screen.

   ---

6. Click **Save.**

IMPORTANT: It is recommended to test the authenticator after enrollment. If the test fails, delete the authenticator and enroll it again.

TIP: If `Fingerprint Service unavailable` message is displayed, ensure that the Advanced Authentication Smartcard Service installed.

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

To test the authenticator perform the following steps:

1. Click the Fingerprint icon in the **Enrolled methods** section.
2. Click **Test** button.
3. Place your finger on the reader or swipe your finger on the swipe sensor. Appropriate message is displayed indicating the result of the test.

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 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. Select the required category from the **Category** list.
3. 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).
4. 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 (PIN) each 42 days.

1.8 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. Select the required category from the **Category** list.
5. A message `Waiting for card....` is displayed. Present your card or plug in your crypto stick to the machine.
6. 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.
7. Enter the PIN code of the device in **PIN**.
8. 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.

1.9 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`.

1.10 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. Select the required category from the **Category** list.
3. Enter answers to the security questions. Each answer must contain not less 1 character (by default, it may be changed by your system administrator).
4. 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`.

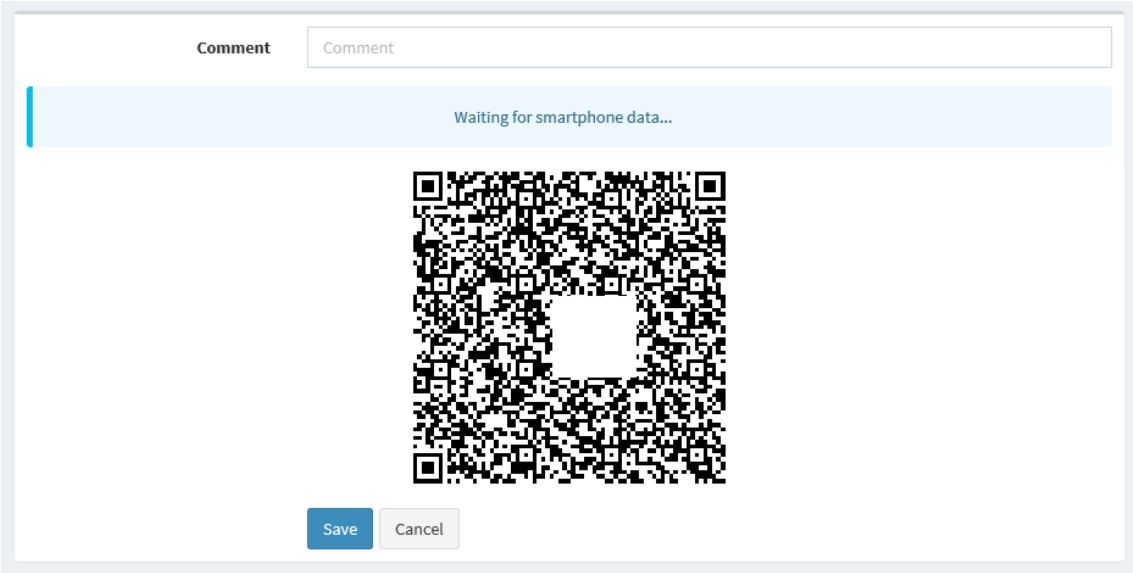
1.11 Smartphone

TIP: To enroll the Smartphone authenticator it's required to use the Advanced Authentication smartphone app Apple iOS app, Google Android app.

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. Select the required category from the **Category** list.
4. Click **Save** button. You will see a QR code.
5. Move a cursor out of the QR code and open the Advanced Authentication smartphone app.



6. Tap **Offline authentication** button in the app.
7. Tap **+** button to add a new authenticator in the app.
8. Use camera of your smartphone to scan the QR code.
9. You will see a message `Authenticator "Smartphone" added`.
10. Enter your username and an optional comment in the smartphone app.
11. 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.

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`.

1.12 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 within a certain time frame.

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

NOTE: If there is no phone number in the account profile for the user in the repository, then the SMS OTP method is not enrolled automatically. However, you can manually enroll the SMS OTP method from the **Not Enrolled methods** section, by entering the phone number and then clicking **Save.**

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. Change the mobile number if it is 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`.

1.13 Swisscom Mobile ID

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.

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, Google Android app).
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. Select the required category from the **Category** list.
3. Move a cursor out of the QR code and open the Advanced Authentication smartphone app.
4. Tap **Offline authentication** button in the app.
5. Tap **+** button to add a new authenticator in the app.
6. Use camera of your smartphone to scan the QR code.
7. Click **Save** button.
8. You will see a message `Authenticator "TOTP" added`.
9. Enter your username and an optional comment in the smartphone app.
10. 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. Select the required category from the **Category** list.

3. Move a cursor out of the QR code and open the Google Authenticator app.
4. Tap **BEGIN SETUP** text in the app.
5. Tap **Scan barcode** button to add a new authenticator in the app.
6. Use camera of your smartphone to scan the QR code.
7. Click **Save** button.
8. 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. Select the required category from the **Category** list.
3. Enter your token's serial number to the **OATH Token Serial** field. You may get the information on back side of your token.
4. Press the token's button and enter the OTP to the **OTP** field.
5. Click **Save** button.
6. 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. Select the required category from the **Category** list.
3. Expand the **Enter TOTP secret manually**.
4. Enter 40 hexadecimal characters in **Secret** field.
5. Check the **Google Authenticator format of secret (Base32)** option if you use the Google Authenticator app.
6. Change the **Period** value if required (30 seconds by default).
7. Click **Save** button.
8. 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. Select the required category from the **Category** list.
4. Ensure that your FIDO U2F token is properly connected to the machine.
5. 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.
6. 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 FIDO U2F Service installed.

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

If a message `Enroll failed: Device not attested. Ask your administrator to upload your token attestation certificate` is displayed, contact your administrator to add your token attestation certificate.

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

The Voice 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 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. Select the required category from the **Category** list.
4. Specify a **PIN**. By default it must contain at least 3 digits.
5. 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 Voice OTP

The Voice OTP authenticator initiates a phone call to your mobile number. You will receive the voice OTP in the phone call.

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

NOTE: If there is no phone number in the account profile for the user in the repository, then the Voice OTP method is not enrolled automatically. However, you can manually enroll the Voice OTP method from the **Not Enrolled methods** section, by entering the phone number and then clicking **Save**.

To test the enrolled authenticator follow the steps below:

1. Click the Voice OTP  icon in the Enrolled methods section.
2. Click **Test.**
3. Receive the call on your phone and listen to the voice OTP.
4. Enter the One-Time Password in the **Password** field.
5. Click **Next.** A message `Authenticator "Voice OTP" passed the test` is displayed. If the provided authenticator is invalid you will see a message Wrong answer, try again.

2 Logging In to Linux

To log in to Linux with the Advanced Authentication, perform the following steps:

1. Specify the repositoryname\username (e.g. company\pjones) and click **Next**.
2. Choose an authentication chain from the list by entering the number of the chain.
3. Authenticate with the required authentication method(s) of the chain.

NOTE: If you log in to a non-domain joined workstation for the first time, you will be asked to provide credentials for your local account to map the domain account to the local account. In the **Enter a standalone user name**, specify the username of local account. In the next step, specify the local account's password.

The following authentication methods, which can be combined in an authentication chain, help you to authenticate based on your requirement.

- Card
- Email
- Emergency Password
- FIDO U2F
- HOTP
- LDAP Password
- Password (PIN)
- PKI
- RADIUS
- Security Questions
- Smartphone
- SMS
- TOTP
- Voice

NOTE: On SUSE Linux Enterprise, do not enter anything until a message `Please wait` is displayed, else you will not be able to unlock the operating system.

2.1 Card

NOTE: To use the card for authentication, you must install the Advanced Authentication Device Service.

To authenticate by using the **Card** method, perform the following steps:

1. Ensure that the card reader is connected to your machine.
2. Tap your card on the reader.

If an error message `Wrong card` is displayed, you might be using a wrong card. Repeat with another card or re-enroll the authenticator in Self-Service Portal, or contact the security officer.

If you get the error `Connect reader`, ensure that the reader is properly connected. Try to connect it to a different USB slot.

If you get the error `<Your user name> has no authenticator for Card`, you need to go to the Self-Service Portal to enroll the authenticator or contact the security officer.

2.2 Email

To authenticate by using the **Email** method, perform the following steps:

1. Check your email. You should get an email with a One Time Password (OTP).
2. Enter the OTP from Email.
3. Click **Next**.

If you get the error `Wrong answer`, either the OTP that you have entered is incorrect or you entered the OTP after the OTP expiration.

If you get the error `Cannot send OTP. User does not have an email`, contact your system administrator to add your email address to the account properties.

2.3 Emergency Password

To authenticate by using the **Emergency Password** method, perform the following steps:

1. Enter the emergency password.
2. Click **Next**.

If you get the error `Wrong password`, you might be using a wrong emergency password.

If you get the error `<Your user name> has no authenticator for Emergency Password`, contact your security officer.

2.4 FIDO U2F

NOTE: You must install the Advanced Authentication Device Service for the FIDO U2F authentication.

To authenticate by using the **FIDO U2F** method, perform the following steps:

1. Ensure that the FIDO U2F token is connected to the workstation.

   The message `Please touch the flashing U2F device now` is displayed.
2. If you see a blink, touch the token's button. If it does not blink, wait for 10-15 seconds. If it is still not blinking, then reconnect your token and repeat the steps.

If you get the error `Wrong token. Try another one`, the token is incorrect. Repeat with another token or re-enroll the authenticator in Self-Service Portal, or contact the security officer.

If you get the error `Connect a token`, check that the token is properly connected to the workstation.

If you get the error `<Your user name> has no authenticator for U2F`, you need to go to the Self-Service Portal to enroll the authenticator or contact the security officer.

2.5 HOTP

To authenticate by using the **HOTP** method, perform the following steps:

1. Enter the HOTP manually or if you use a hardware USB token, press the token's button.
2. Click **Next**.

If you get the error `Wrong answer,` the OTP you have provided is incorrect.

If you get the error `<Your user name> has no authenticator for HOTP`, you need to go to the Self-Service Portal to enroll the authenticator or contact your security officer.

2.6 LDAP Password

To authenticate by using the **LDAP Password** method, perform the following steps:

1. Enter your domain password.
2. Click **Next**.

If you get the error `Invalid credentials`, the domain password you have provided is incorrect.

2.7 Password (PIN)

To authenticate by using the Password (PIN) method, perform the following steps:

1. Enter the password (PIN) for your Advanced Authentication account.
2. Click **Next**.

If you get the error `Wrong password` (PIN), the password (PIN) you have provided is incorrect.

If you get the error `<Your user name> has no authenticator for Password` (PIN), you need to go to the Self-Service Portal to enroll the authenticator or contact the security officer.

2.8 PKI

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

To enroll a PKI, perform the following steps:

1. Insert a card or plug in a crypto stick to your machine.
2. Enter a PIN code.

If you get the error `Wrong card`, the authenticator that is used is incorrect. Repeat with another card or crypto stick or re-enroll the authenticator in Self-Service Portal or contact the helpdesk.

If you get the error `Present card`, ensure that the PKI device is properly connected. Try to connect it to a different USB slot.

If you get the error `<Your user name> has no authenticator for PKI`, you need to go to the Self-Service Portal to enroll the authenticator or contact the helpdesk.

2.9 RADIUS

To authenticate by using the RADIUS method, perform the following steps:

1. Enter the RADIUS password.
2. Click **Next.**

If you get the error `Wrong answer` you are trying to use a wrong RADIUS password.

2.10 Security Questions

To authenticate by using the Security Questions method, perform the following steps:

1. Enter your answer for the specified security question.
2. Click **Next**.
3. Repeat steps 1 to 2 for all the required security questions.

If you get the error `Wrong answer` you might have entered a wrong answer.

If you get the error `<Your user name> has no authenticator for Security Questions`, enroll the authenticator or contact the security administrator from the Self-Service portal.

2.11 Smartphone

To authenticate by using the Smartphone method, perform the following steps:

1. If there is an internet connection in your smartphone, open the Smart Authenticator smartphone app and accept the authentication request.

NOTE: In Linux, you cannot authenticate with your smartphone in the offline mode.

You will get the error `Auth rejected` if you decline the authentication request.

If you get the error `<Your user name> has no authenticator for smartphone`, enroll the authenticator or contact the security administrator from the Self-Service portal.

2.12 SMS

To perform authentication by the **SMS** method, perform the following steps:

1. Check your phone. You should get an SMS message with an OTP.
2. Enter the OTP from SMS.
3. Click **Next**.

If you get the error `Cannot send OTP. User does not have a cell phone`, contact your system administrator to add your mobile phone number to the account properties.

If you get the error `Login failed`, either the OTP that you have entered is incorrect or you entered the OTP after the OTP expiration. Try to authenticate again.

2.13 TOTP

To perform authentication by the **TOTP** method, perform the following steps:

1. Enter the TOTP from your hardware or software token.
2. Click **Next.**

If you get the error `Wrong answer` you might be using a wrong OTP.

If you get the error `<Your user name> has no authenticator for TOTP`, you need to go to the Self-Service Portal to enroll the authenticator or contact your security officer.

2.14 Voice

To perform authentication by the **Voice** method, perform the following steps:

1. You will see "`Wait a phone call...`". Answer the call, listen to the answer on the phone and then enter your PIN code.
2. Enter the `#` (hash sign).

3 Logging In to Mac

To log in to Mac with the Advanced Authentication, perform the following steps:

1. Select a user from the Mac login screen or enter the user's name in the **Other user** screen.

   NOTE: You can switch between languages by clicking the flag icon beside the text box.

2. Click **Next**.
3. Choose an authentication chain from the list.
4. Authenticate with the required authentication method(s) of the chain.

NOTE: If you log in to a non-domain joined workstation for the first time, you will be asked to provide credentials for your local account to map the domain account to the local account. In **username**, specify the username of local account. In the next step, specify the local account's password.

The following authentication methods, which can be combined in an authentication chain, help you to authenticate based on your requirement.

1. Card
2. Email
3. Emergency Password
4. HOTP
5. LDAP Password
6. Password (PIN)
7. PKI
8. RADIUS
9. Security Questions
10. Smartphone
11. SMS
12. TOTP
13. FIDO U2F
14. Voice

3.1 Card

NOTE: You must install the Advanced Authentication Device Service for the **Card** authentication.

To authenticate by using the **Card** method, perform the following steps:

1. Ensure that the card reader is connected to your machine.
2. Tap your card on the reader or insert a smart card to the reader.

If an error message `Wrong card` is displayed, you might be using a wrong card. Repeat with another card or re-enroll the authenticator in Self-Service Portal, or contact your security officer.

If you get the error `Connect reader`, ensure that the reader is properly connected. Try to connect it to a different USB slot.

If you get the error `<Your user name> has no authenticator for Card`, you need to go to the Self-Service Portal to enroll the authenticator or contact the security officer.

3.2 Email

To authenticate by using the **Email** method, perform the following steps:

1. Check your email. You should get an email message with a One Time Password (OTP).
2. Enter the OTP from Email.
3. Click **Next**.

If you get the error `Wrong answer`, check the OTP you entered is correct. The error may be displayed if you try to enter the OTP after some minutes due to the OTP expiration. Retry the authentication.

If you get the error `Cannot send OTP. User does not have an email`, contact your system administrator to add your email address to the account properties.

3.3 Emergency Password

To authenticate by using the **Emergency Password** method, perform the following steps:

1. Enter your emergency password.
2. Click **Next**.

If you get the error `Wrong password`, you might be using a wrong emergency password.

If you get the error `<Your user name> has no authenticator for Emergency Password`, contact the security officer.

3.4 FIDO U2F

NOTE: Advanced Authentication Device Service must be installed for the **FIDO U2F** authentication.

To authenticate by using the **FIDO U2F** method, perform the following steps:

1. Ensure that the FIDO U2F token is connected to the workstation. The message `Please touch the flashing U2F device now` is displayed.
2. If you see a blink, touch the token's button. If it does not blink, wait for 10-15 seconds. If it is still not blinking, then reconnect your token and repeat the steps.

If you get the error `Wrong token. Try another one`, you might be using a wrong token. Repeat with another token or re-enroll the authenticator in Self-Service Portal, or contact your security officer.

If you get the error `Connect a token`, check that the token is properly connected to the workstation.

If you get the error `<Your user name> has no authenticator for U2F`, you need to go to the Self-Service Portal to enroll the authenticator or contact the security officer.

3.5 HOTP

To authenticate by using the **HOTP** method, perform the following steps:

1. Enter your HOTP manually or if you use a hardware USB token, press the token's button.
2. Click **Next**.

If you get the error `Wrong answer` you might be using a wrong OTP.

If you get the error `<Your user name> has no authenticator for HOTP`, you need to go to the Self-Service Portal to enroll the authenticator or contact the security officer.

3.6 LDAP Password

To authenticate by using the **LDAP Password** method, perform the following steps:

1. Enter your domain password.
2. Click **Next**.

If you get the error `Invalid credentials`, you might be using a wrong domain password.

3.7 Password (PIN)

To authenticate by using the **Password (PIN)** method, perform the following steps:

1. Enter the password (PIN) for your Advanced Authentication account.
2. Click **Next**.

If you get the error `Wrong password (PIN)`, the password (PIN) you have provided is incorrect.

If you get the error `<Your user name> has no authenticator for Password` (PIN), you need to go to the Self-Service Portal to enroll the authenticator or contact the security officer.

3.8 PKI

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

To enroll a **PKI**, perform the following steps:

1. Insert a card or plug in a crypto stick to your machine.
2. Enter a PIN code.

If you get the error `Wrong card`, you might be using a wrong authenticator. Repeat with another card or crypto stick or re-enroll the authenticator in Self-Service Portal or contact the helpdesk.

If you get the error `Present card`, ensure that the PKI device is properly connected. Try to connect it to a different USB slot.

If you get the error `<Your user name> has no authenticator for PKI`, you need to go to the Self-Service Portal to enroll the authenticator or contact the helpdesk.

3.9 RADIUS

To authenticate by using the **RADIUS** method, perform the following steps:

1. Enter your RADIUS password.
2. Click **Next.**

If you get the error `Wrong answer` you are trying to use a wrong RADIUS password.

3.10 Security Questions

To authenticate by using the **Security Questions** method, perform the following steps:

1. Enter your answer for the specified security question.
2. Click **Next**.
3. Repeat steps 1 to 2 for all the required security questions.

If you get the error `Wrong answer` you might have entered a wrong answer.

If you get the error `<Your user name> has no authenticator for Security Questions`, you need to go to the Self-Service Portal to enroll the authenticator or contact the security officer.

3.11 Smartphone

To authenticate by using the **Smartphone** method, perform the following steps:

1. If there is internet connection in your smartphone, open the Advanced Authentication smartphone app and accept the authentication request.
2. If there is no internet connection in your smartphone, then perform the following steps:
    a. Open the Advanced Authentication smartphone app.
    b. Enter the one-time password from the smartphone app.
    c. Click **Next.**

You will get the error `Auth rejected` if you decline the authentication request.

You will get the error `Wrong TOTP password` if you are using an offline authentication and entered a wrong TOTP password, or the time on your smartphone is not synchronized.

An error `TOTP login is disabled` is displayed if you are using the offline authentication and if geo-fencing is enabled. Contact the administrator for further assistance.

If you get the error `<Your user name> has no authenticator for smartphone`, you need to go to the Self-Service Portal to enroll the authenticator or contact the security officer.

3.12 SMS

To authenticate by using the **SMS** method, perform the following steps:

1. Check your phone. You should get an SMS message with an OTP.
2. Enter the OTP from SMS.
3. Click **Next**.

If you get the error `Cannot send OTP. User does not have a cell phone`, contact your system administrator to add your mobile phone number to the account properties.

3.13 TOTP

To authenticate by using the **TOTP** method, perform the following steps:

1. Enter the TOTP from your hardware or software token.
2. Click **Next.**

If you get the error `Wrong answer` you might be using a wrong OTP.

If you get the error `<Your user name> has no authenticator for TOTP`, you need to go to the Self-Service Portal to enroll the authenticator or contact the security officer.

3.14 Voice

To authenticate by using the **Voice** method, perform the following steps:

1. You will see "`Wait a phone call...`". Answer the call, listen to the answer on the phone and then enter your PIN code.
2. Enter the `#` (hash sign).

4 Logging In to Windows

To log in to Windows with Advanced Authentication, perform the following steps:

1. Enter the user's name in the **Other user** screen.

   NOTE: To log in to the local account, enter `<computer name>\<Username of local account>` or.`\<Username of local account>`.

2. Press **Enter** or click **Next**.
3. Choose an authentication chain from the list.
4. Authenticate with the required authentication method(s) of the chain.

NOTE: If you log in to a non-domain joined workstation for the first time, you will be asked to provide credentials for your local account to map the domain account to the local account. In the **user name** field, enter `<computer name>\<Username of local account>` or.`\<Username of local account>`. Then enter the local account's password and click **Next**.

The following authentication methods, which can be combined in an authentication chain, help you to authenticate based on your requirement.

1. Bluetooth
2. Card
3. Email
4. Emergency Password
5. Fingerprint
6. FIDO U2F
7. HOTP
8. LDAP Password
9. Password (PIN)
10. PKI
11. RADIUS
12. Security Questions
13. Smartphone
14. SMS
15. Swisscom Mobile ID
16. TOTP
17. Voice
18. Voice OTP

4.1 Bluetooth

NOTE: To use the **Bluetooth** method for authentication, you must install the Advanced Authentication Device Service. For more information on Device Service, see the *Advanced Authentication - Device Service* guide.

To authenticate with the Bluetooth method, ensure that Bluetooth is turned on in your mobile device and discoverable to the paired devices. The Device Service detects your bluetooth device and authenticates.

NOTE: If **Enable reaction on device removal** option for Bluetooth method is enabled by the administrator, then Operating System automatically locks if the Bluetooth device is disabled or it is out of range.

4.2 Card

NOTE: To use the **Card** method for authentication, you must install the Advanced Authentication Device Service. For more information on Device Service, see the *Advanced Authentication - Device Service* guide.

To authenticate with the **Card** method, perform the following steps:

1. Ensure that the card reader is connected to your machine.
2. Tap your card on the reader or insert a smart card to the reader.

IMPORTANT: The **Card** method supports the `1:N` feature that indicates that Advanced Authentication automatically detects the user name. You can authenticate by pressing **CTRL+ALT+DEL** and then placing a card to the reader.

While authenticating with the **Card** method, some error messages might be displayed:

- If an error message `Wrong card` is displayed, you might be using a wrong card. Repeat with another card or re-enroll the authenticator in the Self-Service Portal, or contact the security officer.
- If you get the error `Connect reader`, ensure that the reader is properly connected. Try to connect it to a different USB slot.
- If you get the error `<Your user name> has no authenticator for Card`, you need to enroll the authenticator in the Self-Service Portal, or contact the security officer.
- If you get the error `No template for Card`, either the card is not enrolled or you are trying to log in with the non-cached authenticator in the offline mode.

IMPORTANT: An administrator can configure an automatic session lock or log off on card events. In such a scenario, you must:

- Leave a card on the reader during login and after you log in when **Tap&Go** is disabled and you can lock the operating system or log off automatically when you take off the card from the reader.

  Or

- Tap a card on the reader to log in and to lock, unlock, or log off when **Tap&Go** is enabled.

4.3 Email

To authenticate with the **Email** method, perform the following steps:

1. Check your email. You must receive an email with an OTP (One Time Password).
2. Enter the OTP from Email.
3. Click **Next**.

If you get the error `Wrong answer`, either the OTP that you have entered is incorrect or you entered the OTP after the OTP expiration.

If you get the error `Cannot send OTP. User does not have an email`, contact your system administrator to add your email address to the account properties.

4.4 Emergency Password

To authenticate with the **Emergency Password** method, perform the following steps:

1. Enter the emergency password.
2. Click **Next**.

If you get the error `Wrong password`, you might be using a wrong emergency password.

If you get the error `<Your user name> has no authenticator for Emergency Password`, contact your security officer.

4.5 Fingerprint

NOTE: To use the **Fingerprint** method for authentication, you must install the Advanced Authentication Device Service. For more information on Device Service, see the *Advanced Authentication - Device Service* guide.

To authenticate with the **Fingerprint** method, perform the following steps:

1. Ensure that a fingerprint reader is connected to the required device.
2. Place your finger on the reader when using a touch sensor or swipe your finger when using a swipe sensor.

While authenticating with the **Fingerprint** method, some error messages might be displayed:

- If you get the error `Please connect a scanner`, ensure that the reader is properly connected. Try to connect it to a different USB slot.
- If you get the error `Mismatch`, ensure that you are using the same fingerprint that was enrolled and try to authenticate again.
- If you get the error `<Your user name> has no authenticator for Fingerprint`, you need to enroll the authenticator in the Self-Service Portal, or contact the security officer.

4.6 FIDO U2F

NOTE: To use the **FIDO U2F** method for authentication, you must install the Advanced Authentication Device Service. For more information on Device Service, see the *Advanced Authentication - Device Service* guide.

To authenticate with the **FIDO U2F** method, perform the following steps:

1. Ensure that the FIDO U2F token is connected to the workstation.

   The message `Please touch the flashing U2F device now` is displayed.
2. If you see a blink, touch the token's button. If it does not blink, wait for few seconds. If it does not blink, then reconnect your token and repeat the steps.

NOTE: Administrator can configure an automatic session lock or log off on U2F events. When a user returns to his workstation, the user needs to insert the U2F device into the computer and unlock the workstation.

While authenticating with the **FIDO U2F** method, some error messages might be displayed:

- If you get the error `Wrong token. Try another one`, the token is incorrect. Repeat with another token or re-enroll the authenticator in Self-Service Portal, or contact the security officer.
- If you get the error `Connect a token`, check that the token is properly connected to the workstation.
- If you get the error `<Your user name> has no authenticator for U2F`, you need to enroll the authenticator in the Self-Service Portal, or contact the security officer.

4.7 HOTP

To authenticate with the **HOTP** method, perform the following steps:

1. Enter the HOTP manually or if you use a hardware USB token, press the token's button.
2. Click **Next**.

If you get the error `Wrong answer,` the OTP you have provided is incorrect.

If you get the error `<Your user name> has no authenticator for HOTP`, you need to enroll the authenticator in the Self-Service Portal, or contact the security officer.

4.8 LDAP Password

To authenticate with the **LDAP Password** method, perform the following steps:

1. Enter your domain password.
2. Click **Next**.

If you get the error `Invalid credentials`, the domain password you have provided is incorrect.

4.9 Password (PIN)

To authenticate with the **Password (PIN)** method, perform the following steps:

1. Enter the password (PIN) for your Advanced Authentication account.
2. Click **Next**.

If you get the error `Wrong password` (PIN), the password (PIN) you have provided is incorrect.

If you get the error `<Your user name> has no authenticator for Password` (PIN), you need to enroll the authenticator in the Self-Service Portal, or contact the security officer.

4.10 PKI

NOTE: To use the **PKI** method for authentication, you must install the Advanced Authentication Device Service. For more information on Device Service, see the *Advanced Authentication - Device Service* guide.

To enroll a **PKI**, perform the following steps:

1. Insert a card or plug in a crypto stick to your machine.
2. Enter a PIN code.

IMPORTANT: The PKI method supports the `1:N` feature. The user name is detected automatically by the Advanced Authentication. You can authenticate by pressing **CTRL+ALT+DEL** and then plugging in your PKI device.

While authenticating with the **PKI** method, some error messages might be displayed:

- If you get the error `Wrong card`, the authenticator that is used is incorrect. Repeat with another card or crypto stick or re-enroll the authenticator in Self-Service Portal or contact the helpdesk.
- If you get the error `Present card`, ensure that the PKI device is properly connected. Try to connect it to a different USB slot.
- If you get the error `<Your user name> has no authenticator for PKI`, you need to enroll the authenticator in the Self-Service Portal or contact the helpdesk.
- If you get the error `No template for Card`, either the card is not enrolled or you are trying to log in with the non-cached authenticator in the offline mode.

NOTE: In a scenario where you leave a card on the reader or a crypto stick connected, and once you log in you can lock the operating system automatically even if you take off the card from the reader or unplug your crypto stick (if it is configured by the system administrator). Then you can place a card back to the reader or plug your crypto stick to unlock the operating system.

You must put the card again to the reader to unlock the operating system. Advanced Authentication does not support locking or unlocking an operating system by tapping a card.

4.11 RADIUS

To authenticate with the **RADIUS** method, perform the following steps:

1. Enter the RADIUS password.
2. Click **Next.**

If you get the error `Wrong answer` you are trying to use a wrong RADIUS password.

4.12 Security Questions

To authenticate with the **Security Questions** method, perform the following steps:

1. Enter your answer for the specified security question.
2. Click **Next**.
3. Repeat steps 1 to 2 for all the required security questions.

If you get the error `Wrong answer` you might have entered a wrong answer.

If you get the error `<Your user name> has no authenticator for Security Questions`, enroll the authenticator or contact the security administrator from the Self-Service portal.

4.13 Smartphone

To authenticate with the **Smartphone** method, perform the following steps:

1. If there is an internet connection in your smartphone, open the Advanced Authentication smartphone app and accept the authentication request.
2. If there is no internet connection in your smartphone, then perform the following steps:
   a. Open the Advanced Authentication smartphone app.
   b. Enter the OTP from the smartphone app.
   c. Click **Next.**

An error `Auth rejected` is displayed if you decline the authentication request.

An error `Wrong TOTP password` is displayed if you are using the offline authentication and entered a wrong TOTP password, or the time on your smartphone is not synchronized.

An error `TOTP login is disabled` is displayed if you are using the offline authentication and if geo-fencing is enabled. Contact the administrator for further assistance.

If an error `<Your user name> has no authenticator for smartphone` is displayed, then enroll the authenticator or contact the security administrator from the Self-Service portal.

4.14 SMS

To authenticate with the **SMS** method, perform the following steps:

1. Check your phone. An SMS message with an OTP must be sent to your phone.
2. Enter the OTP from the SMS.
3. Click **Next**.

If you get the error `Cannot send OTP. User does not have a cell phone`, contact your system administrator to add your mobile phone number to the account properties.

4.15 Swisscom Mobile ID

To authenticate with the **Swisscom Mobile ID** method, perform the following steps:

1. A request message is displayed on your mobile phone.
2. Accept the request.

NOTE: To authenticate with Swisscom Mobile ID method, you must activate the Mobile ID service for your Swisscom SIM card.

4.16 TOTP

To authenticate with the **TOTP** method, perform the following steps:

1. Enter the TOTP from your hardware or software token.
2. Click **Next.**

If you get the error `Wrong answer` you might be using a wrong OTP.

If you get the error `<Your user name> has no authenticator for TOTP`, you need to enroll the authenticator in the Self-Service Portal or contact your security officer.

4.17 Voice

To authenticate with the **Voice** method, perform the following steps:

1. You will see "`Wait a phone call...`". Answer the call, listen to the answer on the phone and then enter your PIN code.
2. Enter the `#` (hash sign).

4.18 Voice OTP

To authenticate by using Voice OTP method, perform the following steps:

1. Receive the call on your phone and listen to the voice OTP.
2. Enter the One-Time Password in the **Password** filed.
3. Click **Next.**

5 Logging In to Advanced Authentication Access Manager

To perform a log on to Advanced Authentication Access Manager using the Advanced Authentication select an appropriate card (if applicable).

The following links will help you to get information on how to authenticate using a specific method of assigned authentication chain:

1. Card
2. Dynamic Method
3. Email
4. Emergency Password
5. FIDO U2F
6. HOTP
7. Password (PIN)
8. RADIUS
9. Security Questions
10. Smartphone
11. SMS
12. TOTP
13. Voice
14. Voice OTP

5.1 Card

NOTE: Advanced Authentication Device Service must be installed. Some card readers are supported only on Microsoft Windows. Contact your administrator for further information.

To perform authentication by Card method follow the steps below:

1. Ensure that the card reader connected to your machine.
2. Tap your card on the reader or insert a smart card to the reader.

If you get the error `Authorization by smartcard failed` you are likely trying to use a wrong card. Repeat with another card if you have it or re-enroll the authenticator in Self-Service Portal or contact your security officer.

If you get the error `The smartcard reader is not connected, please connect the smartcard reader and try again`, ensure that the reader is properly connected. Try to connect it to a different USB slot, the click `try again`.

If you get the error `<Your user name> has no authenticator for Smartcard`, you need to go to the Self-Service Portal to enroll the authenticator or contact your security officer.

5.2 Dynamic Method

To perform authentication by Dynamic method perform the following steps:

1. Select one of the available chains (if applicable).
2. Authenticate using methods of the selected chain.

For more information about authentication using the different methods, see Logging In to Advanced Authentication Access Manager.

NOTE: The following methods are supported in the Dynamic configuration only (there are no separate classes for them):

- Fingerprint
- PKI

For both the methods, you must install Advanced Authentication Device Service.

5.3 Email

To perform authentication by Email method follow the steps below:

1. Check your email. You should get an email message with one-time password.
2. Enter the OTP from Email to the **Email Password** field.
3. Click **Login** button.

If you get the error `This cannot be OTP password`, please check if the entered OTP is correct. You may get the error if you try to enter the OTP after some minutes because of the OTP expiration. Retry the attempt.

If you get the error `Can't send OTP. User has not an email`, please ask your system administrator to add your email address to the account properties.

5.4 Emergency Password

To perform authentication by Emergency Password follow the steps below:

1. Ensure that your user name is entered (if applicable).
2. Set focus to the **Password** field and enter your emergency password.
3. Click **Login** button.

If you get the error `Login failed, please try again` you are likely trying to use a wrong emergency password.

5.5 FIDO U2F

NOTE: Advanced Authentication Device Service must be installed for all browsers except for Google Chrome. It contains a built-in module.

To perform authentication by FIDO U2F method follow the steps below:

1. Ensure that the FIDO U2F token is connected to the workstation.
2. Press the token's button.

If you get the error `Authorization by Fido U2F failed`, you are likely trying to use a wrong token. Repeat with another token if you have it or re-enroll the authenticator in Self-Service Portal or contact your security officer.

If you get the error `<Your user name> has no authenticator for U2F`, you need to go to the Self-Service Portal to enroll the authenticator or contact your security officer.

5.6 HOTP

To perform authentication by HOTP method follow the steps below:

1. Enter your HOTP manually to the **OTP Password** field or if you use a hardware USB token set focus to the field and click the token's button.
2. Click **Login** button.

If you get the error `Authorization by OTP failed. The counter-based password was wrong` you are likely trying to use a wrong OTP.

If you get the error `<Your user name> has no authenticator for HOTP`, you need to go to the Self-Service Portal to enroll the authenticator or contact your security officer.

5.7 Password (PIN)

To perform authentication by Password (PIN) follow the steps below:

1. Ensure that your user name is entered (if applicable).
2. Set focus to the **Password** (PIN) field and enter your password (PIN).
3. Click **Login** button.

If you get the error `Login failed, please try again` you are likely trying to use a wrong password (PIN).

5.8 RADIUS

To perform authentication by RADIUS method follow the steps below:

1. Enter your RADIUS password.
2. Click **Login** button.

If you get the error `Authorization by RADIUS failed` you are trying to use a wrong RADIUS password.

5.9 Security Questions

To perform authentication by Security Questions method follow the steps below:

1. Enter your answers to the security question.
2. Click **Login** button.

If you get the error `Authorization by Security Question failed. The answers was wrong` you have entered the wrong answers.

If you get the error `<Your user name> has no authenticator for Security Questions`, you need to go to the Self-Service Portal to enroll the authenticator or contact your security officer.

5.10 Smartphone

To perform authentication by Smartphone method follow the steps below:

1. If your smartphone has an internet connection open the Advanced Authentication smartphone app and accept the authentication request.
2. If your smartphone doesn't have an internet connection click `here` in the text.
   a. Open the Advanced Authentication smartphone app.
   b. Enter the one-time password from the smartphone app to the **Smartphone OTP** field.
   c. Click **Login** button.

If you get the error `Authorization by smartphone failed. The password was wrong` you have entered a wrong Smartphone OTP or rejected the authentication or authentication has been rejected by timeout.

If you get the error `<Your user name> has no authenticator for smartphone`, you need to go to the Self-Service Portal to enroll the authenticator or contact your security officer.

5.11 SMS

To perform authentication by SMS method follow the steps below:

1. Check your phone. You should get an SMS message with one-time password.
2. Enter the OTP from SMS to the **SMS Password** field.
3. Click "Login" button.

If you get the error `Authorization by sms failed. The password was wrong` you have entered the wrong OTP.

If you get the error `Can't send OTP. User has not a mobile phone`, please ask your system administrator to add your mobile phone number to the account properties.

5.12 TOTP

To perform authentication by TOTP method follow the steps below:

1. Enter TOTP from your hardware or software token.
2. Click **Login** button.

If you get the error `Authorization by OTP failed. The time-based password was wrong` you are likely trying to use a wrong OTP.

If you get the error `<Your user name> has no authenticator for TOTP`, you need to go to the Self-Service Portal to enroll the authenticator or contact your security officer.

5.13 Voice

To perform authentication by Voice method follow the steps below:

Take a call, listen to the answerphone, then enter your PIN code. After it enter hash sign (#).

5.14 Voice OTP

To authenticate by using Voice OTP method, perform the following steps:

1. Receive the call on your phone and listen to the voice OTP.
2. Enter the One-Time Password in the **Password** filed.
3. Click **Next.**