Legal Notices

Copyright 2014 - 2023 Open Text

The only warranties for products and services of Open Text and its affiliates and licensors ("Open Text") are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

For additional information, such as certification-related notices and trademarks, see https://www.microfocus.com/en-us/legal (https://www.microfocus.com/en-us/legal).
Contents

About this Book

1 Logging In to Advanced Authentication Self-Service Portal

2 Managing Authenticators

Enrolling Multiple Authenticators of the Same Type ................................................. 16

Apple Touch ID ................................................................. 17

  Enrolling the Apple Touch ID Authenticator ......................................................... 18
  Testing the Apple Touch ID .................................................................................... 18

Bluetooth .............................................................. 19

  Enrolling the Bluetooth Authenticator .................................................................. 19
  Testing the Bluetooth Authenticator ...................................................................... 20

Bluetooth eSec .......................................................... 20

  Enrolling the Bluetooth eSec Authenticator .......................................................... 20
  Testing the Bluetooth eSec Authenticator .............................................................. 21

Card .................................................. 21

  Enrolling the Card Authenticator ......................................................................... 21
  Testing the Card Authenticator ............................................................................. 21

  Enrolling NFC Card Authenticator ....................................................................... 22
  Testing NFC Card Authenticator ........................................................................... 22

Device Authentication ........................................ 23

  Enrolling Device Authentication Authenticator ................................................... 23
  Testing Device Authentication Authenticator ....................................................... 24

Email OTP .................................................. 24

  Enrolling the Email OTP Authenticator ............................................................... 24
  Testing the Email OTP Authenticator ................................................................... 24

Facial Recognition ........................................ 25

  Enrolling the Face Authenticator ........................................................................ 25
  Testing the Face Authenticator .......................................................................... 25

Flex OTP .................................................. 26

  Enrolling the Flex OTP Authenticator ............................................................... 26
  Testing the Flex OTP Authenticator ................................................................... 26

FIDO2 .................................................. 26

  Enrolling the FIDO2 Authenticator ................................................................. 26
  Testing the FIDO2 Authenticator ....................................................................... 28

FIDO U2F .................................................. 28

  Enrolling the FIDO U2F Authenticator ............................................................. 28
  Testing the FIDO U2F Authenticator ............................................................... 29

Fingerprint .................................................. 30

  Duress Finger .................................................. 30
  Enrolling the Fingerprint Authenticator Using Single Finger Reader .................. 31
  Enrolling the Fingerprint Authenticator Using Multi-Finger Reader ................. 31
  Assigning a Finger as Duress ............................................................................... 32
  Testing the Fingerprint Authenticator ............................................................... 32

Home Affairs National Identification System (HANIS) Fingerprint ................. 33

  Enrolling the HANIS Fingerprint Authenticator ............................................... 33
3 Managing Authenticators New UI

Apple Touch ID ................................................................. 63
Enrolling the Apple Touch ID Authenticator ............................. 63
Testing the Apple Touch ID .................................................... 63
Bluetooth ........................................................................... 64
Enrolling the Bluetooth Authenticator ....................................... 65
Testing the Bluetooth Authenticator ......................................... 65
Bluetooth eSec ................................................................. 65
Enrolling the Bluetooth eSec Authenticator .............................. 66
Testing the Bluetooth eSec Authenticator ............................... 66
Card ................................................................................. 67
Enrolling the Card Authenticator ............................................ 67
Testing the Card Authenticator .............................................. 67
Enrolling NFC Card Authenticator ......................................... 68
Testing NFC Card Authenticator ............................................ 68
Device Authentication ........................................................... 69
Enrolling Device Authentication Authenticator ......................... 69
Testing Device Authentication Authenticator ............................ 69
Email OTP ........................................................................ 70
Enrolling the Email OTP Authenticator .................................... 70
Testing the Email OTP Authenticator ..................................... 70
Facial Recognition ................................................................ 71
Enrolling the Face Authenticator ............................................ 71
Testing the Face Authenticator .............................................. 71
Flex OTP ........................................................................... 72
Enrolling the Flex OTP Authenticator ..................................... 72
Testing the Flex OTP Authenticator ....................................... 72
FIDO2 .............................................................................. 72
Enrolling the FIDO2 Authenticator .......................................... 74
Testing the FIDO2 Authenticator .......................................... 74
FIDO U2F ......................................................................... 74
Enrolling the FIDO U2F Authenticator ..................................... 75
Testing the FIDO U2F Authenticator ..................................... 75
Fingerprint ......................................................................... 76
Duress Finger ..................................................................... 76
Enrolling the Fingerprint Authenticator Using Single Finger Reader 77
Enrolling the Fingerprint Authenticator Using Multi-Finger Reader 77
Assigning a Finger as Duress ................................................. 78
Testing the Fingerprint Authenticator ..................................... 78
Home Affairs National Identification System (HANIS) Fingerprint ..................................................... 79
Enrolling the HANIS Fingerprint Authenticator ....................... 79
Testing the HANIS Fingerprint Authenticator ......................... 79
HANIS Face ....................................................................... 80
Enrolling the HANIS Face Authenticator .................................. 80
Testing the HANIS Face Authenticator ................................... 81
Contents

HOTP .............................................................. 82
   Enrolling the HOTP Authenticator ............................................. 82
   Testing the HOTP Authenticator ................................................. 84
LDAP Password .................................................. 84
   Enrolling the LDAP Password Authenticator ................................... 84
   Testing the LDAP Password Authenticator .................................... 85
Out-of-Band ..................................................... 85
   Enrolling the Out-of-Band Authenticator ..................................... 85
   Testing the Out-of-Band Authenticator ....................................... 85
Password .......................................................... 86
   Enrolling the Password Authenticator ........................................ 86
   Testing the Password Authenticator ........................................... 86
PKI ................................................................. 86
   Enrolling the PKI Authenticator Using PKI Device .......................... 87
   Enrolling the PKI Authenticator Using Virtual Smartcard ................. 87
   Testing the PKI Authenticator .................................................... 88
RADIUS Client .................................................. 89
   Enrolling the RADIUS Client Authenticator ................................ 89
   Testing the RADIUS Client Authenticator .................................... 90
SAML Service Provider .......................................... 90
   Enrolling the SAML Service Provider Authenticator ....................... 90
   Testing the SAML Service Provider Authenticator ......................... 90
Security Questions ............................................... 90
   Enrolling the Security Questions Authenticator .............................. 91
   Testing the Security Questions Authenticator ................................ 91
Smartphone ....................................................... 91
   Enrolling the Smartphone Authenticator ....................................... 91
   Testing the Smartphone Authenticator ....................................... 93
SMS OTP .......................................................... 93
   Enrolling the SMS OTP Authenticator ........................................ 94
   Testing the SMS OTP Authenticator ........................................... 94
Swedish BankID .................................................. 95
   Enrolling the Swedish BankID Authenticator ................................. 95
   Testing the Swedish BankID Authenticator .................................. 95
Swisscom Mobile ID .............................................. 96
   Testing the Swisscom Mobile ID Authenticator .............................. 96
TOTP ............................................................... 96
   Enrolling the TOTP Authenticator ............................................. 96
   Testing the TOTP Authenticator ................................................. 99
Voice .............................................................. 99
   Enrolling the Voice Authenticator ............................................. 100
   Testing the Voice Authenticator .............................................. 100
Voice OTP ........................................................ 100
   Enrolling the Voice OTP Authenticator ....................................... 101
   Testing the Voice OTP Authenticator ....................................... 101
Web Authentication Method ....................................... 101
   Enrolling the Web Authentication Authenticator ............................. 101
   Testing the Web Authentication Authenticator ............................... 102
Windows Hello .................................................. 102
   Configuring the System Settings for Windows Hello ....................... 102
   Enrolling the Windows Hello Authenticator ................................ 103
   Testing the Windows Hello Authenticator ................................... 104
   Enrolling Multiple Methods of a Chain in Sequence ....................... 104
4 Logging In to Authentication Agent for Windows

Bluetooth .............................................................. 110
Bluetooth eSec ......................................................... 110
Card ................................................................. 111
Device Authentication ............................................... 112
Email OTP .......................................................... 113
Emergency Password ............................................... 113
Facial Recognition .................................................. 114
Flex OTP ............................................................. 115
Fingerprint .......................................................... 115
Home Affairs National Identification System (HANIS) .................................................. 116
HOTP ................................................................. 116
LDAP Password ...................................................... 117
Password ............................................................. 117
PKI ..................................................................... 118
RADIUS Client ........................................................ 119
Security Questions ..................................................... 119
Smartphone ............................................................ 120
SMS OTP .............................................................. 121
Swisscom Mobile ID .................................................. 122
TOTP ................................................................. 122
FIDO U2F .............................................................. 123
Voice ................................................................. 124
Voice OTP ............................................................. 124
Windows Hello ........................................................ 124

5 Logging In to Linux .................................................. 127

Logging In As a Local User ............................................ 127
Authenticators for Linux Client .................................... 128
  Authentication Agent ............................................... 129
  Bluetooth .......................................................... 130
  Card ................................................................. 130
  Device Authentication ............................................... 131
  Email OTP .......................................................... 132
  Emergency Password ............................................... 132
  Facial Recognition .................................................. 133
  Flex OTP ............................................................. 134
  Fingerprint .......................................................... 134
  HANIS Face ........................................................ 134
  HOTP ................................................................. 135
  LDAP Password ...................................................... 135
  Out-of-Band ........................................................ 136
  Password ............................................................. 137
  PKI ..................................................................... 137
  RADIUS Client ........................................................ 138
  Security Questions ..................................................... 138
  Smartphone ............................................................ 139

Contents
Fingerprint ......................................................... 177
Home Affairs National Identification System (HANIS) ........................................... 178
HOTP ................................................................. 178
LDAP Password ................................................ 179
Password ......................................................... 179
PKI ................................................................. 180
RADIUS Client .................................................. 181
Security Questions .......................................... 181
Smartphone ...................................................... 182
SMS OTP .......................................................... 183
Swisscom Mobile ID .......................................... 184
TOTP ............................................................... 184
FIDO U2F .......................................................... 185
Voice ............................................................... 186
Voice OTP ......................................................... 186
Windows Hello ............................................... 186

10 Logging In to Windows 189

Authentication Agent ........................................ 190
Bluetooth ......................................................... 191
Bluetooth eSec .................................................. 192
Card ............................................................... 192
Device Authentication ....................................... 193
Email OTP ....................................................... 194
Emergency Password ....................................... 195
Facial Recognition ........................................... 195
Flex OTP .......................................................... 196
FIDO2 ............................................................. 196
Fingerprint ...................................................... 197
HANIS Face ...................................................... 198
HOTP ............................................................... 199
LDAP Password .............................................. 199
Out-of-Band .................................................... 200
Password ......................................................... 200
PKI ................................................................. 201
RADIUS Client ............................................... 202
Security Questions .......................................... 202
Smartphone ...................................................... 203
SMS OTP .......................................................... 203
Swisscom Mobile ID .......................................... 204
TOTP ............................................................... 204
FIDO U2F .......................................................... 205
Voice ............................................................... 206
Voice OTP ......................................................... 206
Windows Hello ............................................... 206

11 Logging In to Virtual Desktop Authentication Agent 209

Bluetooth ......................................................... 210
<table>
<thead>
<tr>
<th>Method</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card</td>
<td>211</td>
</tr>
<tr>
<td>In-Line Enrollment</td>
<td>212</td>
</tr>
<tr>
<td>Email OTP</td>
<td>213</td>
</tr>
<tr>
<td>Emergency Password</td>
<td>213</td>
</tr>
<tr>
<td>Facial Recognition</td>
<td>214</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>215</td>
</tr>
<tr>
<td>HOTP</td>
<td>215</td>
</tr>
<tr>
<td>LDAP Password</td>
<td>216</td>
</tr>
<tr>
<td>Password</td>
<td>216</td>
</tr>
<tr>
<td>PKI</td>
<td>217</td>
</tr>
<tr>
<td>RADIUS Client</td>
<td>218</td>
</tr>
<tr>
<td>Security Questions</td>
<td>218</td>
</tr>
<tr>
<td>Smartphone</td>
<td>219</td>
</tr>
<tr>
<td>SMS OTP</td>
<td>220</td>
</tr>
<tr>
<td>Swisscom Mobile ID</td>
<td>220</td>
</tr>
<tr>
<td>TOTP</td>
<td>221</td>
</tr>
<tr>
<td>FIDO U2F</td>
<td>221</td>
</tr>
<tr>
<td>Voice</td>
<td>222</td>
</tr>
<tr>
<td>Voice OTP</td>
<td>223</td>
</tr>
<tr>
<td>Windows Hello</td>
<td>223</td>
</tr>
</tbody>
</table>
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 (Linux Client, Windows Client, and MacOS Client).

Intended Audience

This book provides information for individuals responsible for understanding administration concepts and implementing a secure, distributed administration model.
1 Logging In to Advanced Authentication Self-Service Portal

Advanced Authentication provides the Self-Service portal where you can enroll and test the authenticators. You can use the enrolled authenticator to get authorized access to any device and service that is secured with Advanced Authentication.

To access the Self-Service portal, specify <https://<hostname>/account in your browser. Contact your system administrator for the URL.

1 Open the URL <https://<hostname>/account in the browser.
2 Specify the User name.
3 If the administrator has configured the Google reCAPTCHA option in the server configurations, you will be prompted to go through the reCAPTCHA to prove that you are a human and not a robot. A series of images are displayed based on a specific criteria and you must select the appropriate images.
4 Click Next.
5 Select the preferred language from the list on the upper right corner of the login page.

You can also change the language from the list on the upper right corner of the Self-Service portal. The languages supported are: Arabic, Canadian French, Chinese Simplified, Chinese Traditional, Danish, Dutch, English, French, German, Italian, Japanese, Polish, Portuguese (Brazilian), Russian, Spanish, and Swedish.
NOTE: In the Add Authenticator section, if you do not see a method that you need to enroll, contact your system administrator.

NOTE: For 6.3 Service Pack 1 and newer versions, see Managing Authenticators New UI. For prior versions, see Managing Authenticators.

6 Select a method to enroll and test.

To log out from the Self-Service portal, click your user name in the upper-right corner and click Log Out.
Managing Authenticators

To perform authentication with Advanced Authentication, you must enroll all methods of an authentication chain which you can use for authentication. An authenticator is a set of encrypted data that contains your authentication information. You can use authenticators to log in to different operating systems such as Linux, Mac OS, and Windows. With these authenticators, you can also log in to VPN and web portals such as Citrix NetScaler, Office 365, SalesForce, and so on. Some of the authenticators such as SMS, Email, Voice OTP, Swisscom Mobile ID, LDAP Password, Flex OTP, and RADIUS are enrolled automatically.

Advanced Authentication provides the following authenticators:

- “Enrolling Multiple Authenticators of the Same Type” on page 16
- “Apple Touch ID” on page 17
- “Bluetooth” on page 19
- “Bluetooth eSec” on page 20
- “Card” on page 21
- “Device Authentication” on page 23
- “Email OTP” on page 24
- “Facial Recognition” on page 25
- “Flex OTP” on page 26
- “FIDO2” on page 26
- “FIDO U2F” on page 28
- “Fingerprint” on page 30
- “Home Affairs National Identification System (HANIS) Fingerprint” on page 33
- “HANIS Face” on page 34
- “HOTP” on page 35
- “LDAP Password” on page 38
- “Denmark National ID” on page 38
- “Out-of-Band” on page 39
- “Password” on page 40
- “PKI” on page 41
- “RADIUS Client” on page 44
- “SAML Service Provider” on page 44
- “Security Questions” on page 45
- “Smartphone” on page 45
- “SMS OTP” on page 48
- “Swedish BankID” on page 49
The following authenticators are enrolled by default:

- Email OTP
- LDAP Password
- RADIUS Client
- SMS OTP
- Swisscom Mobile ID
- Voice OTP
- Flex OTP

**Editing an Authenticator**

1. Click the enrolled method in the Enrolled Single Methods for sign in section.
2. Change the settings and click Save.

**Deleting an Authenticator**

1. Click the enrolled method in the Enrolled Single Methods for sign in section.
2. Click the delete icon.

**Deleting All Enrolled Authenticators**

1. Click the user name in the upper-right corner of the Self-Service portal.
2. Click Delete me.
3. Click OK.

---

**NOTE:** An administrator has the privilege to hide the Delete me option in the Self-Service portal.

**NOTE:** If you are a user of Local repository, using the Delete me option will completely remove your account.

---

**Enrolling Multiple Authenticators of the Same Type**

If the administrator creates multiple event categories, you can enroll multiple authenticators of the same type. During enrollment, you are required to select an appropriate category according to the administrator’s guidance. Later, during authentication to the Windows workstation, you might get a
prompt to select a category where you must choose one of the categories. For some methods, the category selection prompt is not displayed. However, Advanced Authentication selects an appropriate authenticator automatically.

Sample Scenario: Authenticating to Windows Client with the Multi-Enrollment Supported Method and Non-Supported Method

Thomas, an administrator, has performed the following steps to allow users to enroll the Card and Smartphone methods with multiple devices:

1. Created CAT1 category in addition to the default category in the Event Categories policy.
2. Created a chain with the Card and Smartphone methods.
3. Set All Categories to ON (default) in the Windows Logon event and map the chain to the event.

Paul, an end user, has two cards and two mobile phones (Android and iOS) with NetIQ Auth app installed on both. He enrolls each card and phone to a category. He logs in to the Self Service portal and performs the following actions:

- Enrolls the following methods to the default category:
  - Smartphone method: Android phone
  - Card method: Card 1
- Enrolls the following methods to the CAT1 category:
  - Smartphone method: iOS phone
  - Card method: Card 2

After enrollment, Paul selects the chain with Card and Smartphone methods. He can authenticate to the Windows workstation by performing one of the following actions:

- Tap Card 1. Select default from the category selection prompt and then accept the push notification on android phone.
- Tap Card 1. Select CAT1 from the category selection prompt and then accept the push notification on iOS phone.
- Tap Card 2. Select default from the category selection prompt and then accept the push notification on android phone.
- Tap Card 2. Select CAT1 from the category selection prompt and then accept the push notification on iOS phone.

Apple Touch ID

Apple Touch ID enables you to authenticate to Mac operating system using the electronic fingerprint recognition feature available in Mac device. During enrollment, the Apple Touch ID captures the fingerprint. When you try to authenticate to a Mac device, the presented fingerprint is matched with the enrolled fingerprint. If the fingerprints match, you are authenticated.

NOTE: Ensure to install the Advanced Authentication Device Service before you enroll Apple Touch ID. For more information about the Device Service, see the Advanced Authentication - Device Service guide.
NOTE: You can enroll Apple Touch ID only for current login sessions in Mac operating system, and Touch ID session should be active for current users.

Enrolling the Apple Touch ID Authenticator

Perform the following steps to enroll the Apple Touch ID authenticator:

1. Click the Apple Touch ID icon in Add Authenticator.
2. (Optional) Specify a comment related to the Apple Touch ID authenticator in Comment.
3. Specify the current login session account name in Account Name.
   User can see the current username in the right corner of the menu bar.
4. Click Save to start enrolling.
   Two messages Please wait and "TouchIdservice" is trying to enroll are displayed.
   NOTE: If you are enrolling for another user who has logged in but not the current user, only Please wait message is displayed.
5. Place the finger on the Touch ID reader.
   A message Authenticator "Apple Touch ID" has been added is displayed.

Testing the Apple Touch ID

Perform the following steps to test Apple Touch ID authenticator:

1. Click the Apple Touch ID icon in Enrolled Authenticators.
2. Click Test.
3. Click Next
   Two messages Please wait and "TouchIdservice" is trying to authenticate are displayed.
   NOTE: If you are enrolling for another user who has logged in but not the current user, only Please wait message is displayed.
4. Place the finger on the Touch ID reader.
   If the test is successful, a message Authenticator "Apple Touch ID" passed the test is displayed.

The following table describes the possible error messages along with the workaround for the Apple Touch ID authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>User is not found</td>
<td>There is no such account for the current Mac device. Check the account name and try again</td>
</tr>
</tbody>
</table>
Bluetooth

The Bluetooth method enables you to authenticate using any Bluetooth enabled device that is within the range. When you initiate authentication, the Advanced Authentication server searches for the enrolled Bluetooth device. If the enrolled device is within the range, you are authenticated successfully.

For example, Susanne, who is a doctor, attends many in-patients in the hospital. She accesses the computer located in each room to monitor and update the health status of the patient. In this case, Susane can specify her first-factor authentication details and use her Bluetooth enabled mobile phone to log in to the computer automatically when she is within range of a particular room. When she exits the room, she is logged out of that computer automatically.

NOTE: To use this method, you must install the Advanced Authentication Device Service. For more information about Device Service, see Advanced Authentication - Device Service guide.

Enrolling the Bluetooth Authenticator

1 Click the Bluetooth icon in Add Authenticator.
2 (Optional) Specify a comment related to the Bluetooth authenticator in Comment.
3 (Optional) Select the preferred category from Category.
4 Turn on the Bluetooth in your device and ensure that it is discoverable to the other Bluetooth devices.
5 Select your Bluetooth enabled device from the list in the Add Bluetooth authenticator page.

NOTE: If your device is not listed, click Refresh List to reload the Bluetooth enabled devices.

6 Click Save.

A message The "Bluetooth" authenticator has been saved is displayed.
Testing the Bluetooth Authenticator

**NOTE:** During authentication, ensure that your mobile device is discoverable.

1. Click the Bluetooth icon in **Enrolled Authenticators**.
2. Click **Test**.
   
   A message *Waiting for the Bluetooth service* is displayed. If the enrolled Bluetooth device is within the range, a message *Authenticator "Bluetooth" passed the test* is displayed.

If the Advanced Authentication Device Service is not installed on the system where you want to authenticate, an error message *Bluetooth service is not available* is displayed. Install the Device Service and try to authenticate again.

Bluetooth eSec

The Bluetooth eSec method allows you to authenticate with wireless technology using any Bluetooth supported mobile device within the short range. When you initiate authentication, the Advanced Authentication Server detects the enrolled Bluetooth device within the define range. If the enrolled device is available, then authentication successfully.

**NOTE:** Before enrolling this method, you must install the Advanced Authentication Device Service. For more information about Device Service, see *Advanced Authentication - Device Service Guide*.

Enrolling the Bluetooth eSec Authenticator

**NOTE:** Enable Bluetooth in your device and ensure that it is discoverable to the other Bluetooth devices.

1. Click the Bluetooth eSec icon in **Add Authenticator**.
2. (Optional) Specify a comment related to the authenticator in **Comment**.
   
   A message *Loading the devices list* is displayed.
3. (Conditional) Select the preferred category from **Category**.
4. Select your Bluetooth enabled device from the list in the **Add Bluetooth eSec authenticator** page.

**NOTE:** If your device is not listed, click *Search for Devices* to reload the Bluetooth enabled devices.

**NOTE:** Ensure to stay on the Bluetooth screen on your mobile device till the enrollment is successful.

5. Click **Save**.
   
   A message *The "Bluetooth" authenticator has been saved* is displayed.
Testing the Bluetooth eSec Authenticator

NOTE: During authentication, ensure that your mobile device is discoverable.

1. Click the Bluetooth eSec icon in Enrolled Authenticators.
2. Click Test.

A message Waiting for the Bluetooth service is displayed. If the enrolled Bluetooth device is within the range, a message Authenticator "Bluetooth" passed the test is displayed.

If the Advanced Authentication Device Service is not installed on the system where you want to authenticate, an error message Bluetooth device is not available is displayed. Install the Device Service and try to authenticate again.

The following table describes the possible error messages along with the workaround for the Bluetooth eSec authenticator:

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Timeout</td>
<td>The Device Service is unable to detect the Bluetooth device in the range.</td>
</tr>
<tr>
<td>&lt;bluetooth name&gt; device is Enrolled, but not connected</td>
<td>When the Bluetooth of enrolled device is OFF while testing the authenticator.</td>
</tr>
</tbody>
</table>

Card

The Card method enables you to authenticate using the contactless smart card (with the card serial number) and Near-Field Communication (NFC) cards in the following ways:

- While using contactless cards, when you try to authenticate on any device, the recorded serial number of the card is compared with the actual serial number. If the card serial numbers are identical, you are authenticated successfully.
- In the case of NFC cards, when you place your NFC tag near the NFC reader (smartphone), the NFC reader (smartphone) identifies your NFC tag, and you are authenticated successfully.

TIP: Ensure to install the Advanced Authentication Device Service before you enroll a card. For more information about the Device Service, see the Advanced Authentication - Device Service guide.

Some card readers are supported only for Microsoft Windows. For more information about the list of supported card readers, see Supported Card Readers and Cards.

Enrolling the Card Authenticator

Before enrolling the Card authenticator, ensure that the card reader is connected to the computer.

1. Click the Card icon 🔄 in Add Authenticator.

A message Click "Save" to begin is displayed.
2 (Optional) Specify a comment related to the Card authenticator in Comment.
3 (Optional) Select the preferred category from the Category.
4 Click Save.
   A message Waiting for the card is displayed.
5 Tap a card on the reader.
   A message Authenticator "Card" has been added is displayed.

Testing the Card Authenticator

1 Click the Card icon in Enrolled Authenticators.
2 Click Test.
   A message Waiting for the card is displayed.
3 Tap a card on the reader.
   A message Card has been detected is displayed for a moment. If the provided card passes the test, a message Authenticator "Card" passed the test is displayed. If the card is invalid, a message Incorrect Card is displayed.

Enrolling NFC Card Authenticator

You must have a smartphone with NFC support and Google Chrome browser to enroll this method.

1 In your smartphone Google Chrome browser, open the URL <https://<hostname>/account>.
2 (Optional) if you are using webNFC for the first time, tap Allow in the smartphone.
3 Specify the credentials and log in.
4 Tap the Card icon in Add Authenticator.
   A message Click "Save" to begin is displayed.
5 (Optional) Specify a comment related to the Card authenticator in Comment.
6 Click Save.
   A message Waiting for the card is displayed.
7 Place the NFC tag near your NFC reader (smartphone).
   A message Authenticator "Card" has been added is displayed.

Testing NFC Card Authenticator

1 Click the Card icon in Enrolled Authenticators.
2 Click Test.
   A message Waiting for the card is displayed.
3 Place the NFC tag near your smartphone.
   A message Card has been detected is displayed for a moment. If the provided card passes the test, a message Authenticator "Card" passed the test is displayed. If the card is invalid, a message Incorrect Card is displayed.
The following table describes the possible error messages along with the workarounds for the Card authentication.

**Table 2-1  Card authenticator - error messages**

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card Service unavailable</td>
<td>The Advanced Authentication Device Service is not installed on the system. Install the Device Service and try authenticating again.</td>
</tr>
<tr>
<td>Card reader has not been detected</td>
<td>The card reader is not connected properly or reader is not available in the Device Manager. Check the card reader connection settings and then try authenticating again.</td>
</tr>
<tr>
<td>Card reader detected</td>
<td>Due to an improper functioning of a system service pcsd in the Mac OS X. To fix this issue, open Terminal application and run the following commands: kill pcsd kill pcsd-lite Then reconnect the reader and try to enroll again.</td>
</tr>
</tbody>
</table>

**Device Authentication**

Device Authentication method enables you to authenticate using a valid certificate or a key pair and a PIN. During enrollment, a key pair is generated and is secured with the PIN. When you try to authenticate on any device, the certificate or key pair is validated along with PIN. If the specified PIN matches with enrolled PIN, you are authenticated successfully.

**NOTE:** Ensure to enroll the Device Authentication method using the workstation where you would perform further authentication. Enrollment on one machine and authentication on another machine is not supported.

**Enrolling Device Authentication Authenticator**

1. Click the Device Authentication icon 🗝️ in Add Authenticator.
2. *(Optional)* Specify a comment in the Comment.
3. *(Optional)* Select the preferred category from the Category.
4. Select the valid certificate from Key.
   - If the Windows TPM smart card is generated in the workstation, the certificate type and expiry date of certificate is populated in Key automatically.
5. *(Conditional)* To generate key pair, select Generate a key pair from Key and specify PIN.
6. Click Save.
   - A message Authenticator "Device Authentication" has been added is displayed.
Testing Device Authentication Authenticator

1. Click the Device Authentication icon in Enrolled methods.
2. Click Test.
3. Specify the PIN.

If the test is successful, a message Authenticator "Device Authentication" passed the test is displayed. If the specified PIN is invalid, a message Incorrect PIN is displayed.

Email OTP

The Email OTP method enables you to authenticate using the one-time password (OTP) that is sent to the registered email address. When you try to authenticate on any device, the server sends an email to the registered email address with the OTP. You can use this OTP for single authentication within a short time frame.

**NOTE:** If an email address is not registered in the repository for a user profile, then the Email OTP method is not enrolled automatically. However, you can specify the email address in Override Email and click Save to enroll manually.

Enrolling the Email OTP Authenticator

This authenticator is enrolled automatically and you cannot remove it.

1. Click the Email OTP icon in Add Authenticator.
2. (Optional) Specify a comment related to Email OTP authenticator in Comment.
3. (Optional) Select the preferred category from Category.
4. Specify the email address in Email.
   A message Verification is sent to <email address> is displayed.
5. Specify the verification code in Enter verification code to confirm the email address is valid.
6. Click Save.
   A message Authenticator "Email OTP" has been added is displayed.

**NOTE:** An administrator has the privilege to hide the Email and verification code to prevent users from providing new email address that is not registered in the repository.

Testing the Email OTP Authenticator

1. Click the Email OTP icon in Enrolled Authenticators.
2. Ensure that your email address (specified after the text The email address to which the OTP is sent to is) is valid. If the set email address in invalid, update the email address.
3. Click Test.
   A message OTP password sent, please specify is displayed.
4 Check your email. You must have received an email with the OTP.
5 Specify the OTP in Password.

**NOTE:** Ensure to specify the OTP sequence prompted on the screen.

6 Click Next.

A message Authenticator "Email OTP" passed the test is displayed. If the provided OTP is invalid, a message Incorrect OTP password is displayed.

### Facial Recognition

The Facial Recognition method enables you to get automatically authenticated by presenting your face. You need to register your facial image using the web camera. When you try to authenticate on an application, the recorded image is compared with the actual image. If the images match, you are successfully authenticated.

The Facial Recognition method works with both integrated and external web cameras.

### Enrolling the Face Authenticator

1 Click the Face icon in Add Authenticator.
2 Click Save to start enrolling the face.
   A message Face Detecting is displayed.
3 Your face will be captured by the camera and enrolled.
   A message Authenticator "Facial Recognition" has been added is displayed.

**NOTE:**
- Facial recognition authentication method works with or without the Device Service installed. If the Device Service is not installed, then the browser support is used for capturing the face.
- To use the Facial recognition method for OAuth 2.0 and SAML 2.0 integrations, you must have the Advanced Authentication Device Service installed.

### Testing the Face Authenticator

1 Click the Face icon in Enrolled Authenticators.
2 Click Test.
3 Present your face in front of the camera.
   If your face matches with the enrolled face, the facial authentication is successful and a message Authenticator "Facial Recognition" passed the test is displayed.

The following table describes the possible error messages along with the workaround for the Face authentication.
Table 2-2  
**Facial Recognition authenticator- error messages**

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capture Device cannot be opened</td>
<td>The camera is not connected properly. Check your camera settings and try again.</td>
</tr>
<tr>
<td>Mismatch</td>
<td>The enrolled face and presented face does not match. You must present your face again for the authentication.</td>
</tr>
<tr>
<td>Timeout</td>
<td>The session has timed out. You must present your face again for the authentication.</td>
</tr>
</tbody>
</table>

**Flex OTP**

The Flex OTP authenticator facilitates you to authenticate by using your otp password from any of HOTP, TOTP and Smartphone (Offline) authenticator. When you try to authenticate to any device, the OTP in the token is compared with the OTP generated in any of HOTP, TOTP and Smartphone (Offline) authenticators. If the OTPs are valid, you are authenticated successfully.

**Enrolling the Flex OTP Authenticator**

This authenticator enrolls automatically if the HOTP, TOTP or Smartphone (Offline) authenticator is enrolled.

**NOTE:** The Flex OTP method is not visible in Self-Service portal until the user authenticates using Flex OTP once in any event.

**Testing the Flex OTP Authenticator**

1. Click the Flex OTP icon 🌐 in **Enrolled Authenticators**.
2. Click Test.
3. Specify a One-Time Password from any of HOTP, TOTP and Smartphone (Offline) authenticators in **Password**.
   - If the password is valid, a message **Test successful** is displayed. If the provided password is invalid, a message **Incorrect password** is displayed.
4. Click OK.

**FIDO2**

The FIDO2 method facilitates you to use any FIDO compliant device either in-built with the system or connected through USB to register and authenticate to the web environment. When you try to authenticate, FIDO compliant device and user gesture, such as tap on token and swipe fingerprint on reader are validated.
NOTE: If the FIDO2 method is enrolled using the Windows Hello in Microsoft Edge 17 or earlier supported browser versions then you must authenticate using the same browser. After upgrading to the latest version of Edge that supports the FIDO 2.0 standards, you must re-enroll the FIDO2 method.

NOTE: On the Safari browser, while authenticating to a web application with the FIDO2 method, click Next to initiate the authentication. This applies irrespective of the order of the FIDO2 method in a chain.

FIDO2 Terms

- **Resident Key**: A security key that gets stored on the FIDO2 device during enrollment and is discoverable to the browser during the FIDO2 testing and authentication. This is supported on few browsers like Google Chrome, Microsoft Edge.

- **User Verification**: A mechanism to verify the identity of a user with PIN or biometrics.

The above actions are displayed on the Self Service Portal based on the settings configured by the administration.

The following table lists the supported and unsupported browsers for the enrollment, testing and authentication with the FIDO2 method on the old Enrollment Portal:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Browser</th>
<th>User Verification</th>
<th>Resident Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>Chrome</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Firefox</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Mac OS</td>
<td>Chrome</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Firefox</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Safari</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows</td>
<td>Chrome</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Firefox</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Edge</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Android (with built-in FIDO2 device)</td>
<td>Chrome</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Firefox</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Android (with external FIDO2 device)</td>
<td>Chrome</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Firefox</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>iOS</td>
<td>Safari</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
NOTE: Some platform and/or browser combinations do not support User Verification or Resident Key for FIDO2 devices. Therefore, FIDO2 enrollment and authentication fails if the administrator has configured User Verification and Resident Key Requirement as required.

### Enrolling the FIDO2 Authenticator

1. Click the FIDO2 icon in **Add Authenticator**.
2. (Optional) Specify a comment related to FIDO in **Comment**.
3. (Optional) Select the preferred category from **Category**.
4. Click Save.
   A message Waiting for Web Authentication data is displayed.
5. Connect the device that complies with FIDO standards.
6. Perform the action associated to the device.
   For example, if you use the FIDO2 device, connect it to the computer, set the pin, and touch the device when you see a flash.
7. Click Save.
   A message Authenticator "FIDO2" enrolled is displayed.

### Testing the FIDO2 Authenticator

1. Click the FIDO2 icon in **Enrolled Authenticators**.
2. Click **Test**.
   A message Waiting for Web Authentication data is displayed.
3. Perform the action associated to the enrolled device.
   A message Authenticator "FIDO2" passed the test is displayed.

### FIDO U2F

The FIDO U2F method facilitates you to connect the FIDO U2F compliant token to the computer or laptop and touch the flashing token to authenticate. When you try to authenticate on any device, token connected to the device is compared with the enrolled token. If the token details match, you are authenticated successfully.

The following table lists the supported and unsupported browsers for the enrollment, testing and authentication with the FIDO U2F method on the old Enrollment Portal:
Enrolling the FIDO U2F Authenticator

1. Click the U2F icon in Add Authenticator.
   A message Press button "Save" to begin enrolling. is displayed.
2. (Optional) Specify a comment related to U2F in Comment.
3. (Optional) Select the preferred category from Category.
4. Click Save.
   A message Please touch the flashing U2F device now is displayed. You may be prompted to allow the site permissions to access your security keys.
5. Touch the FIDO U2F button when there is a flash on the device.
   A message The "U2F" authenticator has been saved is displayed. If there is no flash for more than 10 seconds, reconnect your token and repeat the steps.

NOTE: To use U2F in Google Chrome on Linux, you must perform the following steps:

   If the file is already available, ensure that the content is similar to that specified in https://github.com/Yubico/libu2f-host/blob/master/70-u2f.rules.
   NOTE: If your version of UDEV is lower than 188, use the rules specified at https://github.com/Yubico/libu2f-host/blob/master/70-old-u2f.rules.
2. Save the file 70-u2f.rules and reboot the system.

Testing the FIDO U2F Authenticator

1. Click the U2F icon in Enrolled Authenticators.
2. Click Test.
   A message Please touch the flashing U2F device now is displayed. You may be prompted to allow the site permissions to access the security keys in U2F device.
3 Touch the FIDO U2F button when there is a flash on the device.

A message Authenticator "U2F" passed the test is displayed. If the connected token is invalid, a message Token is not registered is displayed.

The following table describes the possible error messages along with the workaround for the FIDO U2F authentication.

Table 2-3  FIDO U2F authenticator - error messages

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>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</td>
<td>The FIDO U2F service is not installed properly. Install the U2F service and try again.</td>
</tr>
<tr>
<td>Timeout. Press &quot;Save&quot; to start again</td>
<td>The session has timed out. Click Save and enroll again.</td>
</tr>
<tr>
<td>Enroll failed: Device not attested. Ask your administrator to upload your token attestation certificate</td>
<td>The token does not contain attested certificate. Contact your administrator to add the attestation certificate to your token.</td>
</tr>
<tr>
<td>Unexpected error: U2F token error: The visited URL does not match the application ID or it is not in use</td>
<td>The Facets are not configured appropriately. Contact you administration to check the Facets settings.</td>
</tr>
</tbody>
</table>

**Fingerprint**

The Fingerprint method enables you to authenticate using your fingerprint(s). During enrollment, the fingerprint reader captures the fingerprint. When you try to authenticate on any device, the presented fingerprint is matched with the enrolled fingerprint. If the fingerprints match, you are authenticated successfully.

You can enroll fingers for the Fingerprint method using one of the following devices:

- Single finger reader
- Multi-finger reader

**TIP:** Fingerprint(s) enrollment is supported only on Microsoft Windows and Linux RHEL kernel 3.x.x. You must install Advanced Authentication Device Service.

Linux RHEL supports the fingerprint readers: Green Bit DactyScan84c and Nitgen eNBioScan-C1 for the Fingerprint method enrollment and authentication respectively.

**Duress Finger**

The Fingerprint method also allows you to assign one of the enrolled fingers as duress. Only under an emergency or a threat, you can authenticate with the duress finger. Use of the duress finger for authentication sends an alert notification to the email address and phone number that the administrator has configured.
Enrolling the Fingerprint Authenticator Using Single Finger Reader

1. Click the Fingerprint icon in Add Authenticator.
2. (Optional) Specify a comment related to the Fingerprint authenticator in Comment.
3. (Optional) Select the preferred category from Category.
4. Select the preferred finger for enrollment and place or swipe the finger on the reader when there is a flash.

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

Red indicators below the fingerprint represents the number of captures that the administrator has configured.

5. Repeat Step 4 to add more fingers for authentication.
6. (Conditional) Select one of the enrolled finger as duress from Assign Duress Finger list.

**NOTE:** If you have not enrolled fingers for Fingerprint method, then the Assign Duress Finger list will be empty.

7. Click Save.

A message Authenticator "Fingerprint" has been saved is displayed.

You can also assign a finger as duress, after enrolling the Fingerprint method. For more information, see Assigning a Finger as Duress.

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

Enrolling the Fingerprint Authenticator Using Multi-Finger Reader

1. Click the Fingerprint icon in Add Authenticator.
2. (Optional) Specify a comment related to the Fingerprint authenticator in Comment.
3. (Optional) Select the preferred category from Category.
4. (Conditional) Set Use multi-finger reader for enrollment to ON to use multi-finger reader.

**NOTE:** An administrator has the privilege to hide the Use multi-finger reader for enrollment and force users to enroll with the multi-finger reader.

5. Select one of the highlighted fingers combination for enrollment. The fingers combination available are:

   - Four fingers of the left hand
- Four fingers of the right hand
- Two thumbs

6 Place the fingers on the reader when you see the LEDs of selected fingers flash. Wait till the reader scans the fingers. Red indicators below the fingerprint represents the number of captures that the administrator has configured.

7 (Conditional) Select one of the enrolled finger as duress from Assign Duress Finger list.

**NOTE:** If you have not enrolled fingers for Fingerprint method, then the Assign Duress Finger list will be empty.

8 Click Save. A message Authenticator "Fingerprint" has been added is displayed.

You can also assign a finger as duress, after enrolling the Fingerprint method. For more information, see Assigning a Finger as Duress.

### Assigning a Finger as Duress

1 Click the Fingerprint icon in Enrolled Authenticators.

2 Select the preferred finger as duress from Assign Duress Finger list. The Assign Duress Finger list displays the fingers that are enrolled.

3 Click Save.

### Testing the Fingerprint Authenticator

1 Click the Fingerprint icon in Enrolled Authenticators.

2 Click Test.

3 Place or swipe your finger on the reader. A message Authenticator "Fingerprint" passed the test is displayed. If the fingerprints are not identical, a message Fingerprint Mismatch is displayed.

The following table describes the possible error message along with the workarounds for the Fingerprint authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprint Service is not available</td>
<td>The Advanced Authentication Device Service is not installed. Ensure to install Advanced Authentication Device Service and try authenticating again.</td>
</tr>
<tr>
<td>Fingerprint reader is not connected</td>
<td>The fingerprint reader or vendor specific drivers are not connected properly. Ensure that the fingerprint reader and vendor specific drivers are connected properly to the machine.</td>
</tr>
</tbody>
</table>
Home Affairs National Identification System (HANIS) Fingerprint

The HANIS fingerprint method is for the citizens of South Africa. This method enables you to enroll the personal identification number or passport number issued by Home Affairs National Identification System. When you try to authenticate on any device, the presented fingerprint is matched with the enrolled fingerprint available. If the fingerprints match, you are authenticated successfully.

**NOTE:** If the Passport number or National ID is not registered in the repository for a user profile, then the HANIS method is not enrolled automatically. However, you can manually enroll the HANIS method from the Add Authenticator section.

### Enrolling the HANIS Fingerprint Authenticator

1. Click the HANIS icon in Add Authenticator.
2. (Optional) Specify a comment related to the authenticator in Comment.
3. (Optional) Select the preferred category from Category.
4. Specify the passport number or national ID in ID/Passport number.
5. Specify the mobile number in Phone number.
6. Click Save.

A message Authenticator "HANIS" added is displayed.

**NOTE:** An administrator has the privilege to hide the ID/Passport and Phone number to prevent users from providing new details that are not registered in the repository.

### Testing the HANIS Fingerprint Authenticator

1. Click the HANIS icon in Enrolled Authenticators.
2. Click Test.

A message Place your finger on the reader is displayed.

3. Place or swipe your finger on the reader.

A message Authenticator "HANIS" passed the test is displayed. If the fingerprints are not identical, a message Fingerprint Mismatch is displayed.

<table>
<thead>
<tr>
<th>Table 2-5</th>
<th>HANIS authenticator - error messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error</td>
<td>Possible Cause and Workaround</td>
</tr>
<tr>
<td>Fingerprint Service is not available</td>
<td>The Advanced Authentication Device Service is not installed. Ensure to install Advanced Authentication Device Service and try authenticating again.</td>
</tr>
</tbody>
</table>
HANIS Face

The HANIS (Home Affairs National Identification System) Face method is for the citizens of South Africa. This method enables you to enroll the personal identification number or passport number issued by Home Affairs National Identification System. When you try to authenticate on any device, the presented face is matched with the enrolled face. If the images match, you are authenticated successfully.

**NOTE:** If the Passport number or National ID is not registered in the repository for a user profile, then the HANIS method is not enrolled automatically. However, you can manually enroll the HANIS Face method from the Add Authenticator section.

Enrolling HANIS Face Authenticator

1. Click the HANIS Face icon in Add Authenticator.
2. (Optional) Specify a comment related to the authenticator in Comment.
3. (Optional) Select the preferred category from Category.
4. Specify the passport number or national ID in ID/Passport number.
5. Specify the mobile number in Phone number.
6. Click Save.
   
   A message Authenticator "HANIS Face" added is displayed.

**NOTE:** An administrator has the privilege to hide the ID/Passport and Phone number to prevent users from providing new details that are not registered in the repository.

Testing the HANIS Face Authenticator

1. Click the HANIS Face icon in Enrolled Authenticators.
2. Click Test.
3. Present your face in front of the camera.
   
   If your face matches with the enrolled face, the facial authentication is successful and a message Authenticator "HANIS Face" passed the test is displayed. If the images are not identical, a message Mismatch is displayed.
**Table 2-6  HANIS Face authenticator - Expected error messages**

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capture Device cannot be opened</td>
<td>The camera is not connected properly. Check your camera settings and try again.</td>
</tr>
<tr>
<td>Timeout</td>
<td>The session has timed out. Present your face again for authentication.</td>
</tr>
<tr>
<td>Face Angle to Large</td>
<td>The out-of-plane rotation angle (face pitch and yaw) is too large.</td>
</tr>
<tr>
<td>Face cropped</td>
<td>Partial face captured. Capture full face for authentication.</td>
</tr>
<tr>
<td>Face is occluded</td>
<td>The face is covered with the mask or hat. Ensure to present full face.</td>
</tr>
<tr>
<td>Face not found</td>
<td>The face detector cannot identify the face in the image. The face detection is sensitive to a certain extent and may ignore faces in smaller pixels.</td>
</tr>
<tr>
<td>Face too small</td>
<td>The face is not large enough for analysis. The face can be considered small for multiple reasons:</td>
</tr>
<tr>
<td></td>
<td>• Face size is too small in pixels.</td>
</tr>
<tr>
<td></td>
<td>• Interpupillary distance is too small in pixels.</td>
</tr>
<tr>
<td></td>
<td>• The difference between the image size and the face size is too large.</td>
</tr>
<tr>
<td>Too many faces</td>
<td>The face detector found multiple faces on the image.</td>
</tr>
<tr>
<td>Face close to border</td>
<td>The face is captured too close to the image borders.</td>
</tr>
<tr>
<td>Failed to predict landmarks</td>
<td>Face image captured is too blurry or of poor quality. Capture the face in a well-lit room without excessive movement.</td>
</tr>
<tr>
<td>Face too close</td>
<td>The face is too close to the camera. The distance between the face and the horizontal or vertical image borders is too small.</td>
</tr>
</tbody>
</table>

**HOTP**

HOTP is a counter-based one-time password. This method enables you to authenticate using the counter-based one-time password generated on the HOTP token. The counter on the token must be in sync with the server. You can use generic HOTP tokens that adhere to RFC 4226. You must use the static secret key and three consequent OTP generated from the token to enroll. When you try to authenticate on any device, the OTP in the token is compared with the OTP generated in the server. If the OTPs are identical, you are authenticated successfully.
Enrolling the HOTP Authenticator

To enroll the HOTP authenticator, you must follow the recommendations of your system administrator. You can enroll HOTP in one of the following ways:

- Using YubiKey Hardware token
- Using Software token (DS3 OATH)
- Synchronizing Existing Token with HOTP Counter
- Assigning a Token Serial To an Account

NOTE: If a token is already assigned to your account, enrollment is not required.

Using YubiKey Hardware Token

To enroll HOTP using YubiKey hardware token, perform the following steps:

1. Click the HOTP icon  in Add Authenticator.
2. (Optional) Specify a comment related to HOTP authenticator in Comment.
3. (Optional) Select the preferred category from Category.
4. Specify the token serial number in OATH Token Serial.
5. Specify the YubiKeyToken Key ID.
6. Place the cursor in HOTP 1 and touch the button on YubiKey. OTP from YubiKey is inserted in HOTP 1 automatically.
7. Repeat step 2 in HOTP 2 and HOTP 3 to insert consequent OTPs.
8. Click Save.
   A message Authenticator "HOTP" has been added is displayed.

Using Software Token

To enroll HOTP using RFC 4226 compliant software token, perform the following steps:

1. Click the HOTP icon  in Add Authenticator.
2. Specify first OTP that generated on the token in HOTP 1.
3. Specify consequent OTPs from the token in HOTP 2 and HOTP 3.
4. Specify 40 characters hexadecimal secret code in Secret (If you know).
5. Click Save.
   A message Authenticator "HOTP" has been added is displayed.
Synchronizing Existing Token with HOTP Counter

If an existing token is assigned to your account, perform the following steps to synchronize the HOTP counter:

1. Click the HOTP icon 🔄 in Enrolled Authenticators.
2. Specify first OTP in HOTP 1 that generated on the token. In case of YubiKey token, connect the hardware token to the system and perform the following steps:
   2a. Place cursor in HOTP 1.
   2b. Touch button on the token.
3. Specify the consequent OTPs from the token in HOTP 2 and HOTP 3. In case of YubiKey token, repeat the steps 2a and 2b.
4. Click Save.

Assigning a Token Serial To an Account

If administrator has uploaded the token details on the Advanced Authentication server and you have got the serial number of a token, perform the following steps to assign serial number to your account:

1. Click the HOTP icon 🔄 in Enrolled Authenticators.
2. (Optional) Specify a comment related to HOTP authenticator in Comment.
3. Specify the token's serial number in OATH Token Serial.
4. Specify the three consequent OTPs in HOTP 1, HOTP 2, and HOTP 3 respectively.
5. Click Save.

Testing the HOTP Authenticator

1. Click the HOTP icon in Your Enrolled Single Methods for sign in.
2. Click Test Method.
3. Specify the OTP in Password.

If the OTP is valid, a message Authenticator "HOTP" passed the test is displayed.

The following table describes the possible error message along with the workarounds for the HOTP authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incorrect OTP password</td>
<td>If the specified OTP is incorrect or the counter on the token and server are not in sync. Specify a valid OTP and try to authenticate again</td>
</tr>
<tr>
<td>Cannot derive the counter. Check your three OTPs.</td>
<td>If one of the specified OTP is incorrect during the enrollment. Try to enroll again with the new OTPs.</td>
</tr>
</tbody>
</table>
LDAP Password

The LDAP password method enables you to authenticate using the password of your corporate account. When you try to authenticate on an application, the submitted password is compared with the actual password in the corporate directory. If both the passwords are identical, you are authenticated successfully.

**NOTE:** An administrator has the privilege to prevent users from updating their existing LDAP passwords. If the administrator has prohibited the user from updating their LDAP password, the LDAP Password method will not be displayed on the Self-Service portal and users will not be able to test it.

The user can test this method by logging in to the Advanced Authentication portals or any client where the configured chain contains the LDAP Password method.

Enrolling the LDAP Password Authenticator

This authenticator enrolls automatically and you cannot remove it. However, you can update the existing password.

1. Click the LDAP password icon in Add Authenticator.
2. (Optional) Specify a comment related to LDAP password authenticator in Comment.
3. (Optional) Select the preferred category from Category.
4. Specify the existing LDAP password in Password.
5. Specify the new LDAP password and confirm it.
6. Click Save.

Testing the LDAP Password Authenticator

1. Click the LDAP password icon in Enrolled Authenticators.
2. Click Test.
3. Specify the valid password in Password.
4. Click Next.

   If the password is valid, a message Authenticator "LDAP password" passed the test is displayed. If the provided password is invalid, a message Invalid credentials is displayed.

Denmark National ID

The Denmark National ID method is for the citizens of Denmark. The Denmark National ID enables you to authenticate using Danish CPR number, password, and a pin from the code card provided during Denmark National ID enrollment.
NOTE: If the Social Security number is not registered in the repository for a user profile, then the Danish National ID method is not enrolled automatically. However, you can manually enroll the Danish National ID method from the Add Authenticator section.

Enrolling the Denmark National ID

If the Social Security number is registered in the corporate directory for your user profile, then the Danish National ID method is enrolled automatically. If the Social Security number is not registered in the corporate directory, perform the following steps to enroll Danish National ID.

1. Click the Denmark National ID icon in Add Authenticator.
2. (Optional) Specify a comment related to the authenticator in Comment.
3. Specify the Social Security number.
4. Click Save.
   
   If the enrollment is successful, a message Authenticator "Denmark National ID" added is displayed.

Testing the Denmark National ID

1. Click the Denmark National ID icon in Enrolled Authenticators.
2. Click Test.
   
   The NEM ID pop-up is displayed.
3. Specify the Danish CPR number in User ID.
4. Specify Password.
5. Click Next.
6. Specify the pin corresponding to the serial number displayed in #.

   NOTE: The pin is available in the code card provided during Denmark National ID enrollment.
7. Click Log On.
   
   If the test is successful, a message Authenticator "Denmark National ID" passed the test is displayed.

Out-of-Band

The Out-of-band method facilitates you to authenticate using the authentication request that is sent to the Out-of-band portal, Authentication Agent for Windows, or Authentication Agent for Web. When you initiate the authentication, an authentication request is sent to the Out-of-band portal, Authentication Agent for Windows, or Authentication Agent for Web. You can accept the request and get authenticated.

Enrolling the Out-of-Band Authenticator

This authenticator enrolls automatically and you cannot remove it.
Testing the Out-of-Band Authenticator

1. Click the Out-of-band icon in Enrolled Authenticators.
2. Click Test.
3. Open the Out-of-band portal and authenticate using any of the available chains.
   If you are using the Authentication Agent for Windows, the Authentication Agent window appears where you can authenticate.
4. Wait for a few seconds. If the authentication request did not appear, right click or long tap on blank space and click Reload.
5. Click Accept to accept the authentication request.
   A message Authenticator "Out-of-band" passed the test is displayed.
   If you click Decline, the authentication is declined and a message Auth rejected is displayed.
   If you ignore the authentication request, after few minutes a message Auth confirmation timeout is displayed.

Password

The Password method enables you to authenticate using a secret string. The enrolled password is stored locally in the Advanced Authentication. When you try to authenticate on any device, the specified password is compared with the actual password. If the passwords are identical, you are authenticated successfully.

Enrolling the Password Authenticator

1. Click the Password icon in Add Authenticator.
2. (Optional) Specify a comment related to Password authenticator in Comment.
3. (Optional) Select the preferred category from Category.
4. Specify Password and Confirmation.

   NOTE: Ensure that the password must contain minimum 5 characters, by default. An administrator has the privilege to change the password length.

5. Click Save.
   A message Authenticator "Password" has been added is displayed.

WARNING: You will not receive any notification about the password expiration. The password expiration value is 42 days, by default. Ensure to sign in to the Self-Service portal and change the password before it expires.

Testing the Password Authenticator

1. Click the Password icon in Enrolled Authenticators.
2. Click Test.
3 Specify Password and Confirmation.
4 Click Next.

If the test is successful, a message Authenticator "Password" passed the test is displayed. If the provided authenticator is invalid, a message Incorrect password is displayed.

PKI

The PKI method enables you to authenticate using any one of the following ways:

- PKI Device
- Virtual Smartcard

PKI Device

PKI device is a hardware device such as a contact card and USB token that contains the digital certificate. The PKI reader validates the digital certificate and the identity of users. When you try to authenticate on any device, the certificate in the device is compared with the actual certificate. If the certificates are identical, you are authenticated successfully.

**NOTE:** You must install Advanced Authentication Device Service for enrolling the PKI method using PKI device.

Virtual Smartcard

You can also enroll and authenticate the PKI method using a virtual smartcard. Virtual smartcard supports authentication to any web environment and makes use of client SSL certificate to authenticate users. In client certificate authentication, the client browser provides its client certificate to the server to confirm the identity of a user.

A client SSL certificate is a file that contains information, such as digital signature, expiration date, name of user, and name of CA (Certificate Authority). When you try to authenticate on the web environment, authenticity of the client SSL certificate is validated based on the settings that are configured by the administrator.

Enrolling the PKI Authenticator Using PKI Device

1 Click the PKI icon in Add Authenticator.
2 (Optional) Specify a comment in the Comment.
3 (Optional) Select the preferred category from Category.
   A message Waiting for the card is displayed.
4 Insert the card in reader or connect the token to the machine.
   A message Use an existing certificate or generate a key pair is displayed.
5 Select a key from Key.
   If you have connected the token or card reader, the Key automatically populates the certificate with authentication key and its expiry date.
6 (Conditional) Enable Show all to view all the certificate keys.
7 (Conditional) To generate key pair, select Generate a key pair from Key and specify PIN.
8 Click Save.
   A message Authenticator "PKI" has been added is displayed.

Enrolling the PKI Authenticator Using Virtual Smartcard

1 Try to access the third party website from the browser where your administrator has imported a valid SSL certificate.
   The Certificate dialog box is displayed.
2 Select the preferred client SSL certificate that is issued by the administrator.
   You get auto-enrolled to PKI method using virtual smartcard.

NOTE: An administrator has the privilege to disable auto-enrollment of the PKI method using virtual smartcard.

Testing the PKI Authenticator

1 Click the PKI icon in Your Enrolled Single Methods for sign in.
2 Click Test Method.
   A message Waiting for card... is displayed.
3 Insert your card or connect your token to the machine, if you are using a PKI device.
   If you are using a virtual smartcard, the client SSL certificate is detected automatically.
4 Specify the PIN of the PKI device in PIN.
   If the test is successful, a message Authenticator "PKI" passed the test is displayed. If the card is invalid, a message Wrong card is displayed. If the specified PIN is invalid, a message Incorrect PIN is displayed.

The following table describes the possible error message along with the workarounds for the PKI authentication.

Table 2-8 PKI authenticator - error messages

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card reader connected</td>
<td>When a card is not inserted to the reader or the token is not connected to the machine. Insert the card to the reader or connect token to the machine.</td>
</tr>
<tr>
<td>Enroll failed: Cannot check revocation status for ...</td>
<td>When the certificate on your device does not contain information about the revocation status location or if the information is inserted, but the Certificate Authority is not available to verify the revocation status.</td>
</tr>
</tbody>
</table>
### Table 2-9: Unexpected Error codes

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>PKI service is not available</td>
<td>The Advanced Authentication Device Service is not installed on the system. Install the Device Service and try authenticating again.</td>
</tr>
<tr>
<td>Key not found. Wrong Card?</td>
<td>You have enrolled the PKI authenticator in the RDP session. Enroll the authenticator again in normal session.</td>
</tr>
<tr>
<td>PIN is expired</td>
<td>The PIN assigned to your token has expired. Contact your administrator for the new PIN.</td>
</tr>
<tr>
<td>PIN is locked</td>
<td>After certain number of attempts with the incorrect PIN, the PIN is locked. Contact your administrator to reset the PIN.</td>
</tr>
<tr>
<td>Token is not present</td>
<td>Token is not connected to the system. Connect the token and try authenticating again.</td>
</tr>
<tr>
<td>Token is not recognized</td>
<td>The Device Service is unable to detect the DLL to recognize the token.</td>
</tr>
<tr>
<td>Unexpected service status: PLUGIN_NOT_INITTED</td>
<td>A vendor module is absent, invalid or not specified. Contact your administrator to check the configuration.</td>
</tr>
</tbody>
</table>

The following table describes the unexpected error codes that are displayed from a PKCS#11 module.

**Table 2-9 : Unexpected Error codes**

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CKR_DEVICE_ERROR</td>
<td>The token or USB slot is broken. Try to use a different USB slot.</td>
</tr>
<tr>
<td>CKR_DEVICE_MEMORY</td>
<td>There is no space available in the memory of token or there may be some other issue with the memory.</td>
</tr>
<tr>
<td>CKR_MECHANISM_INVALID</td>
<td>An invalid mechanism was specified to the cryptographic operation.</td>
</tr>
<tr>
<td>CKR_PIN_EXPIRED</td>
<td>Ensure that the card has been initialized or do not use the default PIN and the PIN has expired.</td>
</tr>
<tr>
<td>CKR_PIN_LOCKED</td>
<td>The user PIN is locked.</td>
</tr>
<tr>
<td>CKR_TOKEN_NOT_RECOGNIZED</td>
<td>The token has not been recognized.</td>
</tr>
<tr>
<td>OPERATION_FAILED</td>
<td>Contact your system administrator to analyze the debug logs.</td>
</tr>
</tbody>
</table>
**RADIUS Client**

The RADIUS Client method enables Advanced Authentication to forward the authentication request to a third-party RADIUS server. This can be any RADIUS server.

For example, you can use the RADIUS Client as an authentication method for token solutions such as RSA or Vasco.

**Enrolling the RADIUS Client Authenticator**

This authenticator is enrolled automatically and you cannot delete it.

By default, a user name from your corporate directory is set. You can change the required user name in **Override User name** and click **Save**.

**Testing the RADIUS Client Authenticator**

1. Click the RADIUS Client icon in Enrolled Authenticators.
2. Specify a user name in User name.
3. Click **Test**.
4. Specify the password of the RADIUS Client in **Password**.
5. Click Next.

   If the specified password is valid, a message **Test is successful** is displayed.

The following table describes the possible error message along with the workarounds for the RADIUS Client authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incorrect password</td>
<td>If the specified RADIUS Client password is invalid. Specify a valid password to test the authenticator.</td>
</tr>
<tr>
<td>RADIUS server does not reply</td>
<td>If the administrator has not configured RADIUS Client method appropriately. Contact your administrator and report the error message.</td>
</tr>
</tbody>
</table>

**SAML Service Provider**

SAML Service Provider enables you to use authorization on the third-party websites (Identity Providers) to access the Advanced Authentication portals.

**Enrolling the SAML Service Provider Authenticator**

This authenticator is enrolled automatically.
Testing the SAML Service Provider Authenticator

1. Click the **Saml Service Provider** icon in **Enrolled Methods**.
2. Click **Test**.
3. Click **Next**.

A message **Authenticator "Saml Service Provider" passed the test** is displayed.

Security Questions

Security Questions method enables you to enroll answers to a pre-defined set of security questions. When you authenticate using security questions, Advanced Authentication prompts you the configured security questions or a subset of the security questions. You must answer the appropriate questions and based on the correctness of the answers, you are authenticated successfully.

Enrolling the Security Questions Authenticator

1. Click the **Security Questions** icon in **Add Authenticator**.
2. (Optional) Specify an optional comment in **Comment**.
3. (Optional) Select the preferred category from **Category**.
4. Specify the answers to the security questions that have been set by the administrator. Ensure that each answer contains at least one character.
5. Click **Save**.

A message **Authenticator "Security Questions" added** is displayed.

Testing the Security Questions Authenticator

1. Click the **Security Questions** icon in **Enrolled Authenticators**.
2. Click **Test**.
3. Specify the answers to the security questions.
4. Click **Next**.

A message **Authenticator "Security Questions" passed the test** is displayed. If one of the specified answer is invalid, a message **Wrong answers** is displayed.

Smartphone

The Smartphone method facilitates you to enroll and authenticate using the smartphone app. When you initiate the authentication, a push notification is sent to the app. You can accept the request and get authenticated.

**Pre-requisite:**

To enroll the Smartphone authenticator, you must install the NetIQ Advanced Authentication app on your smartphone.
For more information about downloading and installing the smartphone app, see Installing NetIQ Advanced Authentication App.

**Enrolling the Smartphone Authenticator**

You can enroll the Smartphone method in one of the following ways:

- **Enrolling with a QR code**
- **Enrolling with a link in the email**

**Enrolling With a QR Code**

During the enrollment, you must scan a QR code that creates an authenticator on your mobile app. When you initiate the authentication, a push notification is sent to the app. You can accept the request and get authenticated.

To enroll the Smartphone method with a QR code, perform the following steps:

1. Click the Smartphone icon in Add Authenticator.
2. (Optional) Specify a comment related to the Smartphone authenticator in Comment.
3. (Optional) Select the preferred category from Category.
4. Click Save.
   
   A QR code is displayed.
5. Scan the QR code with the NetIQ Advanced Authentication smartphone app. To do this, perform the following steps:
   
   5a. Open the Advanced Authentication smartphone app.
   5b. Specify a PIN if applicable.
   5c. Click the + (plus) icon in the Enrolled Authenticators screen.
   5d. The camera of your smartphone is launched.
   5e. Scan the QR code with the camera.
      
      A message Authenticator "Smartphone" added is displayed.
   5f. Specify your user name and an optional comment in the app.
   5g. Tap Save.
      
      The smartphone authenticator is created.

If you do not enroll the Smartphone authenticator within few minutes, an error message Enroll failed: Enroll timeout is displayed. Refresh the browser and enroll again.

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

1. Zoom the page to 125-150% and scan the zoomed QR code.
2. Ensure that nothing overlaps the QR code (mouse cursor, text).
Enrolling Through a Link

An administrator will send you the link to your email or via SMS. You must click on the link on your smartphone where the NetIQ Auth app is installed and you will be redirected to the smartphone app where you can enroll and an authenticator is created.

To enroll the Smartphone method through a link, perform the following steps:

1. Check your phone for a new email or SMS. You will receive a link sent by the administrator.
2. Click on the link. You will be redirected to the smartphone app.
   - If you have not installed the smartphone app, you will be redirected to the Google Play or AppStore from where you can install the app.

   **NOTE:** In some instances, when you click on the enroll link, you will be redirected to page where the following two links are displayed:
   - Click to enroll.
   - Click to download and install Smartphone authenticator for Android.
   
   If you have the app installed on your phone, use Click to enroll link. If you do not have the app then use Click to download link.

3. Specify a PIN or a Touch ID if applicable.
4. Specify your username and password in the Enroll new authenticator screen.
5. Tap Sign In.
6. Specify an optional comment in the app.
7. Tap Save.

The smartphone authenticator is created.

Testing the Smartphone Authenticator

1. Click the Smartphone icon in Enrolled Authenticators.
2. Click Test.
3. Open the Advanced Authentication smartphone app.
   - A push notification is sent to your smartphone.
4. Tap Accept to accept the authentication request.
   - A message Authenticator "Smartphone" passed the test is displayed.
   - If you tap Reject, the authentication is declined and a message Auth rejected is displayed.
   - If you ignore the authentication request, after few minutes a message Auth confirmation timeout is displayed.
SMS OTP

The SMS OTP method facilitates you to generate a single-use password or OTP and send it to the registered mobile number for authentication. You can use this OTP to authenticate within a short time frame.

When authenticating on the same smartphone that receives SMS, you can do one of the following actions based on the platform of smartphone:

- **iOS**: The OTP auto inserts to clipboard, tap on the input field > OTP displayed above the keyboard.
- **Android 11 and later versions**: Tap Copy <OTP> in the SMS notification then tap on the input field > OTP displayed above the keyboard.
- **Android 10 and prior versions**: Open the SMS notification and copy OTP. Tap on the input field > OTP displayed above the keyboard.

**NOTE**: The OTP period is set to 120 seconds by default. An administrator has the privilege to change the OTP period.

**NOTE**: If a phone number is not registered in the repository for a user profile, then the SMS OTP method is not enrolled automatically. However, you can manually enroll the SMS OTP method from the Add Authenticator section.

### Enrolling the SMS OTP Authenticator

1. Click the SMS OTP icon in Add Authenticator.
2. (Optional) Specify a comment related to SMS OTP authenticator in Comment.
3. (Optional) Select the preferred category from Category.
4. Specify the mobile number in Phone number.
   A message Verification is sent to <phone number> is displayed.
5. Specify the verification code in Enter verification code to confirm the phone number is valid.
6. Click Save.
   A message Authenticator "SMS OTP" added is displayed.

**NOTE**: An administrator has the privilege to hide the Phone number and verification code to prevent users from providing new phone number that is not registered in the repository.

### Testing the SMS OTP Authenticator

1. Click the SMS OTP icon in Enrolled Authenticators.
2. Click Test.
3. You will receive an SMS with an OTP.
4. Specify the OTP in Password.
NOTE: If you receive multiple SMS, specify the OTP sequence prompted on the screen.

5 Click Next.

A message Authenticator "SMS OTP" passed the test is displayed.

The following table describes the possible error message along with the workarounds for the SMS OTP authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incorrect OTP password</td>
<td>The specified OTP is invalid. Specify a valid OTP and try again.</td>
</tr>
<tr>
<td>You do not have a phone number.</td>
<td>If your phone number is not registered in the repository. Contact administrator or helpdesk to</td>
</tr>
<tr>
<td>Contact administrator or Helpdesk and</td>
<td>register your phone.</td>
</tr>
<tr>
<td>register your phone</td>
<td></td>
</tr>
</tbody>
</table>

**Swedish BankID**

The Swedish BankID method enables you to authenticate using your Swedish Personal Identification Number. To enroll the Swedish BankID authenticator, you must have the BankID app either on your computer or mobile device. When you try to authenticate any device a request is sent to the BankID app, specify the security code to unlock the app. The recorded personal identification number is compared with actual identification number on the BankID app. If the identification numbers match, you are authenticated successfully.

**Enrolling the Swedish BankID Authenticator**

Before enrolling, ensure that you have the following prerequisites:

- Social Security Number (SSN)
- BankID app (either desktop or mobile version).

For more information about the BankID app, see BankID.

**NOTE:** While you set up the security code for the BankID app, ensure that the code must contain six digits in non-sequential format (for example: 221144).

To enroll the Swedish BankID, perform the following steps:

1 Click the BankID icon in Add Authenticator.
2 (Optional) Specify a comment related to BankID authenticator in Comment.
3 (Optional) Select the preferred category from Category.
4 Specify the personal identification number in Personal ID (SSN).
5 Click Save.

A message Authenticator "BankID" added is displayed.
Testing the Swedish BankID Authenticator

1. Click the BankID icon in Enrolled Authenticators.
2. Click Test.
   A message Start your BankID app is displayed.
3. Open the BankID app.
   (Conditional) Click Identify on the mobile app.
   (Conditional) Click Verify my identity on the desktop app.
If the test is successful, a message Authenticator "BankID" passed the test is displayed.

Swisscom Mobile ID

The Swisscom Mobile ID authentication method uses the phone number from your profile of the repository. The authenticator sends an authentication request to your mobile phone. You need to accept it.

This authenticator is enrolled automatically and you cannot remove it.

Testing the Swisscom Mobile ID Authenticator

1. Click the Swisscom Mobile ID icon in Enrolled Authenticators.
2. Click Test.
   A message is displayed indicating that you must accept the request on the mobile phone.
3. Accept the request.
   A message Authenticator "Swisscom Mobile ID" passed the test is displayed.

TOTP

The TOTP method enables you to authenticate using the time-based-one-time password. TOTP is generated on the hardware token, Desktop OTP tool, or the mobile app, such as NetIQ Advanced Authentication app or Google Authenticator app. The TOTP is valid for a short duration. This method uses a predefined period. The default value is 30 seconds.

You can enroll the TOTP authenticator using the Desktop OTP tool. To initiate the tool, use the link that is sent from your administrator. You must click on the link and the Desktop OTP tool is prompted where you can enroll and create an account. While authenticating to any service, you must copy the OTP from the tool and use the OTP to get authenticated.
Enrolling the TOTP Authenticator

To enroll the TOTP authenticator, follow the recommendations of your system administrator. You can enroll TOTP method using any one of the following ways:

- NetIQ Advanced Authentication App
- Google Authenticator App
- OATH Compliant Hardware Token
- Enrolling TOTP Manually
- Desktop OTP Tool

**WARNING:** The QR code format in the Advanced Authentication and Google Authenticator apps are different. Contact your system administrator to confirm the app recommended for enrollment.

NetIQ Advanced Authentication App

To enroll the TOTP authenticator using Advanced Authentication smartphone app, perform the following steps:

1. Click the TOTP icon in Add Authenticator.
2. (Optional) Specify a comment related to TOTP authenticator in Comment.
3. (Optional) Select the preferred category from Category.
4. Open the Advanced Authentication app on your phone.
5. Tap Offline authentication.
6. Tap + to add a new authenticator.
7. Scan the QR code using the camera on your phone.
8. Click Save in the Add TOTP authenticator page.
   
   A message Authenticator "TOTP" has been added is displayed.
9. Tap the new authenticator and specify account name and additional details in Account and Additional info respectively in the app.
10. Click Save.

**TIP:** If you are unable to scan the QR code with Advanced Authentication app, perform the following steps:

1. Zoom the page to 125 - 150%.
2. Scan the zoomed QR code using Google Authenticator app.
   
   Ensure that the mouse cursor is not overlapping the QR code.

If you are still unable to scan the QR code, contact your system administrator.
Google Authenticator App

To enroll the TOTP authenticator using Google Authenticator app, perform the following steps:

1. Click the TOTP icon in Add Authenticator.
2. (Optional) Specify a comment to TOTP authenticator in Comment.
3. (Optional) Select the preferred category from Category.
4. Open the Google Authenticator app on your phone.
5. Tap BEGIN SETUP in the app.
6. Tap Scan barcode to add a new authenticator in the app.
7. Scan the QR code using the camera on your phone.
8. Click Save.
   A message Authenticator "TOTP" has been added is displayed.

TIP: If you scan Advanced Authentication app compatible QR code with Google Authenticator app, a message Invalid barcode is displayed.

OATH Compliant Hardware Token

To enroll the TOTP authenticator using OATH compliant hardware token, perform the following steps:

1. Click the TOTP icon in Add Authenticator.
2. (Optional) Specify a comment related to TOTP authenticator in Comment.
3. (Optional) Select the preferred category from Category.
4. Specify the token’s serial number in OATH Token Serial.
   You can find the serial number behind the token.
5. Press the button on the token and specify the one-time password in OTP.
6. Click Save.
   A message Authenticator "TOTP" has been added is displayed.

Enrolling TOTP Manually

1. Click the TOTP icon in Add Authenticator.
2. (Optional) Specify a comment related to TOTP authenticator in Comment.
3. (Optional) Select the preferred category from Category.
4. Click + adjacent to Specify the TOTP secret manually.
5. Specify 40 hexadecimal characters in Secret.
6. Set Google Authenticator format of secret (Base32) to ON to display the Google Authenticator app compatible QR code.
By default, Google Authenticator format of secret (Base32) is set to OFF and Advanced Authentication app compatible QR code is displayed.

**NOTE:** The administrator has privilege to configure the Google Authenticator format of secret (Base32) option in the Administration portal. But you can override the administrator configured setting.

7 Set the preferred value in **Period**. 30 seconds is set by default.
8 Click **Save**.
   A message **Authenticator "TOTP" has been added** is displayed.

**NOTE:** If the administrator has disabled the manual enrollment of TOTP in the Administration portal, then the **Specify the TOTP secret manually** section is not displayed.

### Desktop OTP Tool

You can enroll the TOTP authenticator with the Desktop OTP tool in one of the following ways:

- **“Enrolling with a Link”** on page 53
- **“Enrolling with a Secret Key”** on page 53

Before enrolling the TOTP authenticator using the link, ensure that NetIQ Desktop OTP tool is installed on your system.

#### Enrolling with a Link

1 Check your registered email or phone for the enrollment link.
2 Click on the link.
   You are directed to the Desktop OTP tool.
3 Specify your LDAP repository or local username, password and optional comment in the **NetIQ Advanced Authentication OTP Tool** window.
4 Click **OK**.
   The TOTP authenticator is created in the Desktop OTP tool and enrolled in the Self-Service portal.

#### Enrolling with a Secret Key

Advanced Authentication generates a secret key in the **Specify the TOTP secret manually** section of the Self-Service portal > TOTP > Add TOTP authenticator. You can enroll the TOTP authenticator manually with the Desktop OTP tool using this secret key as a seed.

1 Click the TOTP icon in **Add Authenticator**.
2 (Optional) Specify a comment related to the TOTP authenticator in **Comment**.
3 (Optional) Select the preferred category from **Category**.
4 Ensure the **OATH Token Serial** and **OTP** fields are empty.
5 Click the + icon adjacent to **Specify the TOTP secret manually**.
6 Click the lock icon adjacent to Secret and copy the 40 hexadecimal characters.
7 Ensure the option Google Authenticator format of QR code (Key URI) is set to OFF.
8 Set the preferred value in Period. The default value is 30 seconds.
9 Click Save.
   A message Authenticator "TOTP" has been added is displayed.
10 Launch the Desktop OTP tool.
11 Click Add by seed.
12 Perform the following in the NetIQ Advanced Authentication OTP Tool window:
   • Specify a brief description related to the TOTP authenticator in Description.
   • Specify the length of OTP in Number of digits (4 -10). Ensure that the value in the Number of
digits field of the OTP tool is the same as the OTP format configured in the Administration
portal.
   • Specify the time interval to generate a new OTP in Period (sec). Ensure that the value in
Period is the same in both the OTP tool and Self-Service portal.
   • Paste the secret in Secret (hex string) that you copied in Step 5.
13 Click OK.
   This creates the TOTP authenticator in the Desktop OTP tool.

**Testing the TOTP Authenticator**

1 Click the TOTP icon in Enrolled Authenticators.
2 Click Test.
3 Specify one-time password in Password.
4 Click Next.
   If the test is successful, a message Authenticator "TOTP" passed the test is displayed.
   If the one-time password is invalid or the server time is not in sync, a message Incorrect OTP
password is displayed.

**Voice**

The Voice method initiates a call to your registered phone number. The phone call requests you to
specify the PIN in the dial pad of your mobile to authenticate. When you try to authenticate on any
device, the recorded PIN is compared with the actual PIN. If both PINs are identical, you are
authenticated successfully.

**NOTE:** If a phone number is not registered in the repository for a user profile, then the Voice method
is not enrolled automatically. However, you can specify the phone number in the Add Authenticator
section and click Save to enroll manually.
Enrolling the Voice Authenticator

1. Click the Voice icon in Add Authenticator.
2. Check whether a valid phone number is specified in Phone number.
3. (Optional) Specify a comment related to Voice authenticator in Comment.
4. (Optional) Select the preferred category from Category.
5. Specify your PIN in PIN.
   The PIN must contain minimum 3 digits, by default.
6. Click Save.
   A message Authenticator "Voice" added is displayed.

**NOTE:** An administrator has the privilege to hide Phone number to prevent users from providing new phone number that is not registered in the repository.

Testing the Voice Authenticator

1. Click the Voice icon in Enrolled Authenticators.
2. Click Test.
   A message Call has been initiated is displayed.
3. Answer the call on your phone.
4. Specify your PIN followed by a hash symbol (#) in the dial pad of your mobile phone.
   A message Authenticator "Voice" passed the test is displayed. If the specified PIN is invalid, a message Incorrect PIN is displayed.

**WARNING:** You will not receive any notification about the PIN expiration. The PIN expiration is set as 42 days, by default. You must sign in to the Self-Service Portal and change the PIN before it expires.

Voice OTP

The Voice OTP method enables you to authenticate using the OTP that is sent through the phone call to your registered phone number. You can use this OTP for authentication within a short duration. When you try to authenticate on any device, the specified OTP is compared with the OTP generated on the server. If both the OTPs are identical, you are authenticated successfully.

**NOTE:** If a phone number is not registered in the repository for a user profile, then the Voice OTP method is not enrolled automatically. However, you can manually enroll the Voice OTP method from the Your Enrolled Single Methods for sign in section, specify the phone number and click Save.
Enrolling the Voice OTP Authenticator

This authenticator enrolls automatically and you cannot remove it.

1. Click the Voice OTP icon in Add Authenticator.
2. (Optional) Specify a comment related to voice OTP authenticator in Comment.
3. (Optional) Select the preferred category from Category.
4. Specify the mobile number in Phone number.
   A message Verification is sent to <phone number> is displayed.
   Receive the call on your phone and listen to the voice OTP.
5. Specify the verification code in Enter verification code to confirm the phone number is valid.
6. Click Save.
   A message Authenticator "Voice OTP" added is displayed.

NOTE: An administrator has the privilege to hide Phone number and verification code to prevent users from providing new phone number that is not registered in the repository.

Testing the Voice OTP Authenticator

1. Click the Voice OTP icon in Enrolled Authenticators.
2. Click Test.
3. Receive the call on your phone and listen to the voice OTP.
4. Specify the OTP in Password.
5. Click Next.
   A message Authenticator "Voice OTP" passed the test is displayed. If the specified OTP is invalid, a message Incorrect answer, try again is displayed.

Web Authentication Method

Advanced Authentication enables you to use authorization on the third-party websites (Identity Providers) to access the Advanced Authentication portals.

Enrolling the Web Authentication Authenticator

1. Click the Web Authentication icon in Add Authenticator.
2. (Optional) Specify something related to the authenticator in Comment.
3. (Optional) Select the preferred category from Category.
4. Select the Identity Provider.
5. (Optional) Specify a hint for the user in Username hint.
6. Click Save.
The enrollment is redirected to the Identity Provider page that you have selected. Specify your credentials.

You will be redirected to the Enrollment page with your enrolled authenticator.

An error Web Authentication failed might be displayed after the authorization on third-party websites during enrollment. Contact your administrator to verify the Web Authentication method settings.

**Testing the Web Authentication Authenticator**

1. Click the Web Authentication icon in **Enrolled Authenticators**.
2. Click **Test**.

You will be automatically authenticated by the enrolled Identity Provider.

**Windows Hello**

The Windows Hello method facilitates you to use your Windows Hello fingerprint, facial recognition and PIN authentication to log in to the Windows 10 operating system. Advanced Authentication supports the Windows Hello fingerprint and facial recognition.

**NOTE:** To use Windows Hello for authentication, you must install the Advanced Authentication Device Service. For more information on Device Service, see the [Advanced Authentication - Device Service](#) guide.

This method supports all the devices that Windows Hello works with. For example, the Windows Hello facial recognition works with only the infrared cameras. Therefore, the Advanced Authentication Windows Hello method also supports only the infrared camera for facial recognition.

**Configuring the System Settings for Windows Hello**

Before enrolling Windows Hello, you must configure the system settings.

- “Configuring Settings for Windows Hello Fingerprint” on page 57
- “Configuring Settings for Windows Hello Face Recognition” on page 58

**NOTE:** You cannot enroll the Windows Hello authentication on an RDP session.

**Configuring Settings for Windows Hello Fingerprint**

1. Click **Start > Settings > Accounts > Sign-in options**.
   
   Under **Windows Hello**, the options for fingerprint is displayed if your PC has a fingerprint reader.
2. Click **Set up under Fingerprint**.
3. Click **Get started**.
4. Specify your PIN.
NOTE: If you do not have a PIN, you must create one to set up the fingerprint.

5 To enroll fingerprint, scan your finger on the fingerprint reader.
   You will have to place your finger multiple times to provide the scanner a good picture of your fingerprints.
6 Click Add Another if you want to add another fingerprint.

Configuring Settings for Windows Hello Face Recognition

1 Click Start > Settings > Accounts > Sign-in options.
   Under Windows Hello, the option for face recognition is displayed if your computer has an external camera.
2 Click Set up under Face Recognition.
3 Click Get started.
4 Specify your PIN.
   NOTE: If you do not have a PIN, you must create one to set up the face recognition.
5 To enroll the face, present your face to the camera. Scan your face by following the on-screen instructions.
6 Select Finish to complete scanning or choose Improve Recognition to continue scanning.
   NOTE: It is recommended that you select to improve recognition if you change your appearance often. Scanning your face again does not erase the earlier scans. It just helps Windows Hello get better at recognizing you.

For more information about Windows Hello, see the Microsoft Windows website https://support.microsoft.com/en-in/help/17215/windows-10-what-is-hello.

NOTE: To enable Windows Hello for all domain-joined Windows 10 workstations and for Windows 10 Enterprise, see https://community.spiceworks.com/topic/1840001-windows-10-fingerprint-some-settings-are-managed-by-your-organization.

Enrolling the Windows Hello Authenticator

1 Click the Windows Hello icon.
2 (Optional) Specify a Comment in Add Windows Hello authenticator.
3 (Optional) Select the preferred category from Category.
   The Category option is displayed only if the administrator has set the Event Categories option in the Administration portal.
4 Specify your username for which Windows Hello is enrolled in Windows User Name.
   NOTE: If you have enrolled Windows Hello for a local account, you must specify the \<username>.
If you want to enroll Windows Hello that is set for a Microsoft account, you can specify microsoftaccount\user@outlook.com as the user name. This is helpful if you must login to the Windows operating system using your Microsoft account.

5 Click Save.

Testing the Windows Hello Authenticator

1 Click the Windows Hello icon in Enrolled authenticators.
2 Click Test.
3 Place your finger on the reader or swipe your finger on the swipe sensor for the fingerprint authentication. Present your face for the facial recognition.
   An appropriate message is displayed indicating the result of the test.
To perform authentication with Advanced Authentication, you must enroll all methods of an authentication chain which you can use for authentication. An authenticator is a set of encrypted data that contains your authentication information. You can use authenticators to log in to different operating systems such as Linux, Mac OS, and Windows. With these authenticators, you can also log in to VPN and web portals such as Citrix NetScaler, Office 365, SalesForce, and so on. Some of the authenticators such as SMS, Email, Voice OTP, Swisscom Mobile ID, LDAP Password, and RADIUS are enrolled automatically. The new self enrollment UI enables the users to perform 2 types of enrollment. Those enrollments are:

- Enroll the methods separately in Your Enrolled Single Methods for sign in.
- Enroll the methods available in the chains for you in Your Enrolled Sequence for sign in.

Advanced Authentication provides the following authenticators:

- “Apple Touch ID” on page 63
- “Bluetooth” on page 64
- “Bluetooth eSec” on page 65
- “Card” on page 67
- “Device Authentication” on page 69
- “Email OTP” on page 70
- “Facial Recognition” on page 71
- “Flex OTP” on page 72
- “FIDO2” on page 72
- “FIDO U2F” on page 74
- “Fingerprint” on page 76
- “Home Affairs National Identification System (HANIS) Fingerprint” on page 79
- “HANIS Face” on page 80
- “HOTP” on page 82
- “LDAP Password” on page 84
- “Out-of-Band” on page 85
- “Password” on page 86
- “PKI” on page 86
- “RADIUS Client” on page 89
- “SAML Service Provider” on page 90
- “Security Questions” on page 90
- “Smartphone” on page 91
- “SMS OTP” on page 93
• “Swedish BankID” on page 95
• “Swisscom Mobile ID” on page 96
• “TOTP” on page 96
• “Voice” on page 99
• “Voice OTP” on page 100
• “Web Authentication Method” on page 101
• “Windows Hello” on page 102
• “Enrolling Multiple Methods of a Chain in Sequence” on page 104

The following authenticators are enrolled by default:

• Email OTP
• LDAP Password
• RADIUS Client
• SMS OTP
• Swisscom Mobile ID
• Voice OTP

**Editing an Authenticator**

1. Click the enrolled method in the Your Enrolled Single Methods for sign in section.
2. Change the settings and click Save.

**Deleting an Authenticator**

1. Click the enrolled method in the Your Enrolled Single Methods for sign in section.
2. Click the delete icon .

**Deleting All Enrolled Authenticators**

1. Click the user name in the upper-right corner of the Self-Service portal.
2. Click Delete me.
3. Click OK.

NOTE: An administrator has the privilege to hide the Delete me option in the Self-Service portal.

NOTE: If you are a user of Local repository, using the Delete me option will completely remove your account.
Apple Touch ID

Apple Touch ID enables you to authenticate to Mac operating system using the electronic fingerprint recognition feature available in Mac device. During enrollment, Apple Touch ID captures the fingerprint. When you try to authenticate to a Mac device, the presented fingerprint is matched with the enrolled fingerprint. If the fingerprints match, you are authenticated.

**NOTE:** Ensure to install the Advanced Authentication Device Service before you enroll Apple Touch ID. For more information about the Device Service, see the Advanced Authentication - Device Service guide.

**NOTE:** You can enroll Apple Touch ID only for current login sessions in Mac operating system, and Touch ID session should be active for current users.

---

**Enrolling the Apple Touch ID Authenticator**

Perform the following steps to enroll the Apple Touch ID authenticator:

1. Click the Add icon in Your Enrolled Single Methods for sign in on the Authentication Methods page.
2. Click the Apple Touch ID icon in Available Methods for Enrollment.
3. (Optional) Specify the Display Name.
4. Specify the current login session account name in Touch ID Account Name. User can see the current username in the right corner of the menu bar.
5. Click Save to start enrolling.

Two messages Please wait and "TouchIdservice" is trying to enroll are displayed.

**NOTE:** If you are enrolling for another user who has logged in but not the current user, only Please wait message is displayed.

6. Place the finger on the Touch ID reader.

A message The "Apple Touch ID" authenticator has been added is displayed.

---

**Testing the Apple Touch ID**

Perform the following steps to test the Apple Touch ID authenticator:

1. Click the Apple Touch ID icon in Your Enrolled Single Methods for sign in.
2. Click Test Method.
3. Click Next

Two messages Please wait and "TouchIdservice" is trying to authenticate are displayed.
NOTE: If you are enrolling for another user who has logged in but not the current user, only Please wait message is displayed.

4 Place the finger on the Touch ID reader.

If the test is successful, a message Test successful is displayed.

The following table describes the possible error messages along with the workaround for the Apple Touch ID authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>User is not found</td>
<td>There is no such account for the current Mac device. Check the account name and try again</td>
</tr>
<tr>
<td>Touch ID not enrolled</td>
<td>Touch ID isn’t enrolled for the specified user. Enable Touch ID in the Apple -&gt; System Preferences -&gt; Touch ID settings</td>
</tr>
<tr>
<td>Touch ID is locked</td>
<td>The user tried to log in with a wrong finger for five times. To enable Touch ID, log in the specified Account with Password</td>
</tr>
<tr>
<td>Touch ID is not available</td>
<td>Local user hasn’t logged in to account yet</td>
</tr>
<tr>
<td>Cancelled by timeout</td>
<td>Operation was cancelled as time for presenting fingerprint is out</td>
</tr>
<tr>
<td>Touch ID is cancelled by user</td>
<td>User not allowed for Device service to use the Touch ID</td>
</tr>
<tr>
<td>Device Service is not available</td>
<td>Device service isn’t installed</td>
</tr>
</tbody>
</table>

**Bluetooth**

The Bluetooth method enables you to authenticate using any Bluetooth enabled device that is within the range. When you initiate authentication, the Advanced Authentication server searches for the enrolled Bluetooth device. If the enrolled device is within the range, you are authenticated successfully.

For example, Susanne, who is a doctor, attends many in-patients in the hospital. She accesses the computer located in each room to monitor and update the health status of the patient. In this case, Susane can specify her first-factor authentication details and use her Bluetooth enabled mobile phone to log in to the computer automatically when she is within range of a particular room. When she exits the room, she is logged out of that computer automatically.

NOTE: To use this method, you must install the Advanced Authentication Device Service. For more information about Device Service, see Advanced Authentication - Device Service guide.
Enrolling the Bluetooth Authenticator

1. Click the Add icon in Your Enrolled Single Methods for sign in on the Authentication Methods page.
2. Click the Bluetooth icon in Available Methods for Enrollment.
3. (Optional) Specify the Display Name.
4. Turn on the Bluetooth in your device and ensure that it is discoverable to the other Bluetooth devices.
5. Click Search for Devices to detect your Bluetooth enabled device.

**NOTE:** If your device is not listed, click Search for Devices to reload the Bluetooth enabled devices.

6. Select the preferred device from the list.
7. Click Save.

A message The "Bluetooth" authenticator has been saved is displayed.

Testing the Bluetooth Authenticator

**NOTE:** During authentication, ensure that your mobile device is discoverable.

1. Click the Bluetooth icon in Your Enrolled Single Methods for sign in.
2. Click Test Method.

A message Waiting for the Bluetooth service is displayed. If the enrolled Bluetooth device is within the range, a message Test successful is displayed. If the enrolled Bluetooth device is not within the range, a message Waiting for an authentication response is displayed.

If the Advanced Authentication Device Service is not installed on the system where you want to authenticate, an error message Bluetooth service is not available is displayed. Install the Device Service and try to authenticate again.

Bluetooth eSec

The Bluetooth eSec method allows you to authenticate with wireless technology using any Bluetooth supported mobile device within the short range. When you initiate authentication, the Advanced Authentication Server detects the enrolled Bluetooth device within the define range. If the enrolled device is available, you are authenticated successfully.

**NOTE:** Before enrolling this method, you must install the Advanced Authentication Device Service. For more information about Device Service, see Advanced Authentication - Device Service Guide.
Enrolling the Bluetooth eSec Authenticator

**NOTE:** Enable Bluetooth in your device and ensure that it is discoverable to the other Bluetooth devices.

1. Click the **Add** icon in *Your Enrolled Single Methods for sign in* on the *Authentication Methods* page.
2. Click the Bluetooth eSec icon in *Available Methods for Enrollment*.
3. (Optional) Specify the **Display Name**.
4. Click **Search for Devices** to detect your Bluetooth enabled device.

**NOTE:** If your device is not listed, click **Search for Devices** to reload the Bluetooth enabled devices.

**NOTE:** Ensure to stay on the Bluetooth screen on your mobile device till the enrollment is successful.

5. Select the preferred device from the list.
6. Click **Save**.

A message *The "Bluetooth" authenticator has been saved* is displayed.

Testing the Bluetooth eSec Authenticator

**NOTE:** During authentication, ensure that your mobile device is discoverable.

1. Click the Bluetooth eSec icon in *Your Enrolled Single Methods for sign in*.
2. Click **Test Method**.

A message *Waiting for the Bluetooth service* is displayed. If the enrolled Bluetooth device is within the range, a message *Test successful* is displayed. If the enrolled Bluetooth device is not within the range, a message *Waiting for an authentication response* is displayed.

If the Advanced Authentication Device Service is not installed on the system where you want to authenticate, an error message *Bluetooth service is not available* is displayed. Install the Device Service and try to authenticate again.

The following table describes the possible error messages along with the workaround for the Bluetooth eSec authenticator:

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Timeout</td>
<td>The Device Service is unable to detect the Bluetooth device in the range.</td>
</tr>
<tr>
<td><code>&lt;bluetooth name&gt;</code> device is Enrolled, but not connected</td>
<td>When the Bluetooth of enrolled device is OFF while testing the authenticator.</td>
</tr>
</tbody>
</table>
Card

The Card method enables you to authenticate using the contactless smart card (with the card serial number) and Near-Field Communication (NFC) cards in the following ways:

- While using contactless cards, when you try to authenticate on any device, the recorded serial number of the card is compared with the actual serial number. If the card serial numbers are identical, you are authenticated successfully.
- In the case of NFC cards, when you place your NFC tag near the NFC reader (smartphone), the NFC reader (smartphone) identifies your NFC tag, and you are authenticated successfully.

TIP: Ensure to install the Advanced Authentication Device Service before you enroll a card. For more information about the Device Service, see the Advanced Authentication - Device Service guide.

Some card readers are supported only for Microsoft Windows. For more information about the list of supported card readers, see Supported Card Readers and Cards.

Enrolling the Card Authenticator

Before enrolling the Card authenticator, ensure that the card reader is connected to the computer.

2. Click the Card icon in Available Methods for Enrollment.
3. (Optional) Specify the Display Name.
4. Click Scan Card.
   A message Waiting for the card is displayed.
5. Tap a card on the reader.
   A message Enrollment is complete is displayed.
6. Click Save.
   A message The "Card" authenticator has been saved is displayed.

Testing the Card Authenticator

1. Click the Card icon in Your Enrolled Single Methods for sign in.
2. Click Test Method.
   A message Waiting for the card is displayed.
3. Tap a card on the reader.
   If the provided card passes the test, a message Test successful is displayed. If the card is invalid, a message Incorrect Card is displayed.
Enrolling NFC Card Authenticator

You must have a smartphone with NFC support and Google Chrome browser to enroll this method.

1. In your smartphone Google Chrome browser, open the URL <https://<hostname>/account>.
2. Specify the credentials and log in.
4. Click the Card icon in Available Methods for Enrollment.
5. (Optional) Specify the Display Name
6. Click Scan Card.
   A message Waiting for the card is displayed.
7. Place the NFC tag near your NFC reader (smartphone).
   A message Enrollment is complete is displayed.
8. Click Save.
   A message The "Card" authenticator has been saved is displayed.

Testing NFC Card Authenticator

1. Click the Card icon in Your Enrolled Single Methods for sign in.
2. Click Test Method.
   A message Waiting for the card is displayed.
3. Place the NFC tag near your smartphone.
   A message Card has been detected is displayed for a moment. If the provided card passes the test, a message Authenticator "Card" passed the test is displayed. If the card is invalid, a message Incorrect Card is displayed.

The following table describes the possible error messages along with the workarounds for the Card authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card Service unavailable</td>
<td>The Advanced Authentication Device Service is not installed on the system. Install the Device Service and try authenticating again.</td>
</tr>
<tr>
<td>Card reader has not been detected</td>
<td>The card reader is not connected properly or reader is not available in the Device Manager. Check the card reader connection settings and then try authenticating again.</td>
</tr>
</tbody>
</table>
Device Authentication

Device Authentication method enables you to authenticate using a valid certificate or a key pair and a PIN. During enrollment, a key pair is generated and is secured with the PIN. When you try to authenticate on any device, the certificate or key pair is validated along with PIN. If the specified PIN matches with enrolled PIN, you are authenticated successfully.

NOTE: Ensure to enroll the Device Authentication method using the workstation where you would perform further authentication. Enrollment on one machine and authentication on another machine is not supported.

Enrolling Device Authentication Authenticator


2. Click the Device Authentication icon in Available Methods for Enrollment.

3. (Optional) Specify the Display Name.

4. Select the valid certificate from Key.
   If the Windows TPM smart card is generated in the workstation, the certificate type and expiry date of certificate is populated in Key automatically.

5. (Conditional) To generate key pair, select Generate a key pair from Key and specify PIN.

6. Click Save.
   A message The "Device Authentication" authenticator has been saved is displayed.

Testing Device Authentication Authenticator

1. Click the Device Authentication icon in Your Enrolled Single Methods for sign in.

2. Click Test Method.

3. Specify the PIN.

   If the test is successful, a message Test Successful is displayed. If the specified PIN is invalid, a message Incorrect PIN is displayed.
Email OTP

The Email OTP method enables you to authenticate using the one-time password (OTP) that is sent to the registered email address. When you try to authenticate on any device, the server sends an email to the registered email address with the OTP. You can use this OTP for single authentication within a short time frame.

**NOTE:** If an email address is not registered in the repository for a user profile, then the Email OTP method is not enrolled automatically. However, you can specify the email address in Override Email and click Save to enroll manually.

Enrolling the Email OTP Authenticator

This authenticator is enrolled automatically and you cannot remove it.

2. Click the Email OTP icon in Available Methods for Enrollment.
3. (Optional) Specify the Display Name.
4. Specify the email address in Override Email.
   A message Please enter OTP is displayed.
5. Specify the verification code in Enter verification code to confirm the email address is valid.
6. Click Verify.
   A message The "Email OTP" authenticator has been saved is displayed.

**NOTE:** An administrator has the privilege to hide the Override Email and Enter verification code to prevent users from providing new email address that is not registered in the repository.

Testing the Email OTP Authenticator

1. Click the Email OTP icon in Your Enrolled Single Methods for sign in.
2. Ensure that your email address (specified after the text The email address to which the OTP is sent to is) is valid. If the set email address is invalid, update the email address.
3. Click Test Method.
   A message OTP password sent, please specify is displayed.
4. Check your email. You must have received an email with the OTP.
5. Specify the OTP in Password.
6. Click Next.
   A message Test Successful is displayed. If the provided OTP is invalid, a message Incorrect OTP password is displayed.
Facial Recognition

The Facial Recognition method enables you to get automatically authenticated by presenting your face. You need to register your facial image using the web camera. When you try to authenticate on an application, the recorded image is compared with the actual image. If the images match, you are successfully authenticated.

The Facial Recognition method works with both integrated and external web cameras.

Enrolling the Face Authenticator

1. Click the Add icon in Your Enrolled Single Methods for sign in on the Authentication Methods page.
2. Click the Facial Recognition icon in Available Methods for Enrollment.
3. (Optional) Specify the Display Name.
4. Click Start Capture to capture the face.
   A message Detecting a Face is displayed.
   Your face will be captured by the camera and enrolled. A message Enrollment is complete is displayed.
5. Click Save.

NOTE: • Facial recognition authentication method works with or without the Device Service installed. If the Device Service is not installed, then the browser support is used for capturing the face.

• To use the Facial recognition method for OAuth 2.0 and SAML 2.0 integrations, you must have the Advanced Authentication Device Service installed.

Testing the Face Authenticator

1. Click the Facial Recognition icon in Your Enrolled Single Methods for sign in.
2. Click Test Method.
3. Present your face in front of the camera.
   If your face matches with the enrolled face, the facial authentication is successful and a message Test successful is displayed.
4. Click OK.

The following table describes the possible error messages along with the workaround for the Face authentication.
Table 3-2  Facial Recognition authenticator- error messages

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capture Device cannot be opened</td>
<td>The camera is not connected properly. Check your camera settings and try again.</td>
</tr>
<tr>
<td>Mismatch</td>
<td>The enrolled face and presented face does not match. You must present your face again for the authentication.</td>
</tr>
<tr>
<td>Timeout</td>
<td>The session has timed out. You must present your face again for the authentication.</td>
</tr>
</tbody>
</table>

Flex OTP

The Flex OTP authenticator facilitates you to authenticate by using your otp password from any of HOTP, TOTP and Smartphone (Offline) authenticator. When you try to authenticate to any device, the OTP in the token is compared with the OTP generated in any of HOTP, TOTP and Smartphone (Offline) authenticators. If the OTPs are valid, you are authenticated successfully.

Enrolling the Flex OTP Authenticator

This authenticator enrolls automatically if the HOTP, TOTP or Smartphone (Offline) authenticator is enrolled.

NOTE: The Flex OTP method is not visible in Self-Service portal until the user authenticates using Flex OTP once in any event.

Testing the Flex OTP Authenticator

1. Click the Flex OTP icon in Enrolled Authenticators.
2. Click Test Method.
3. Specify a One-Time Password from any of HOTP, TOTP and Smartphone (Offline) authenticators in Password.
   - If the password is valid, a message Test successful is displayed. If the provided password is invalid, a message Incorrect password is displayed.
4. Click OK.

FIDO2

The FIDO2 method facilitates you to use any FIDO compliant device either in-built with the system or connected through USB to register and authenticate to the web environment. When you try to authenticate, FIDO compliant device and user gesture, such as tap on token and swipe fingerprint on reader are validated.
NOTE: If the FIDO2 method is enrolled using the Windows Hello in Microsoft Edge 17 or earlier supported browser versions then you must authenticate using the same browser. After upgrading to the latest version of Edge that supports the FIDO 2.0 standards, you must re-enroll the FIDO2 method.

FIDO2 Terms

- **Resident Key**: A security key that gets stored on the FIDO2 device during enrollment and is discoverable to the browser during the FIDO2 testing and authentication. This is supported on few browsers like Google Chrome, Microsoft Edge.
- **User Verification**: A mechanism to verify the identity of a user with PIN or biometrics.

The above actions are displayed on the Self Service Portal based on the settings configured by the administration.

The following table lists the supported and unsupported browsers for the enrollment, testing and authentication with the FIDO2 method on the old Enrollment Portal:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Browser</th>
<th>User Verification</th>
<th>Resident Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>Chrome</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Firefox</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Mac OS</td>
<td>Chrome</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Firefox</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Safari</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows</td>
<td>Chrome</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Firefox</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Edge</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Android (with built-in FIDO2 device)</td>
<td>Chrome</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Firefox</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Android (with external FIDO2 device)</td>
<td>Chrome</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Firefox</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>iOS</td>
<td>Safari</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**NOTE**: Some platform and/or browser combinations do not support **User Verification** or **Resident Key** for FIDO2 devices. Therefore, FIDO2 enrollment and authentication fails if the administrator has configured User Verification and Resident Key Requirement as required.
Enrolling the FIDO2 Authenticator

1. Click the Add icon in Your Enrolled Single Methods for sign in on the Authentication Methods page.

2. Click the FIDO2 icon in Available Methods for Enrollment.

3. (Optional) Specify the Display Name.

4. Connect the device that complies with FIDO standards.

5. Click Detect Device.

   A message Waiting for Web Authentication data is displayed.

6. Perform the action associated to the device.

   For example, if you use the FIDO2 device, connect it to the computer, set the pin, and touch the device when you see a flash. A message Enrollment is complete is displayed.

7. Click Save.

   A message The "FIDO2" authenticator has been saved is displayed.

Testing the FIDO2 Authenticator

1. Click the FIDO2 icon in Your Enrolled Single Methods for sign in.

2. Click Test Method.

   A message Waiting for Web Authentication data is displayed.

3. Perform the action associated to the enrolled device.

   A message Test successful is displayed.

FIDO U2F

The FIDO U2F method facilitates you to connect the FIDO U2F compliant token to the computer or laptop and touch the flashing token to authenticate. When you try to authenticate on any device, token connected to the device is compared with the enrolled token. If the token details match, you are authenticated successfully.

The following table lists the supported and unsupported browsers for the enrollment, testing and authentication with the FIDO U2F method on the New Enrollment Portal:

<table>
<thead>
<tr>
<th>Web Browser</th>
<th>Enrollment</th>
<th>Testing</th>
<th>Login or Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Chrome</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Microsoft Edge</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Firefox</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Google Chrome with Advanced Authentication Device Service</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Enrolling the FIDO U2F Authenticator

1. Click the Add icon in Your Enrolled Single Methods for sign in on the Authentication Methods page.

2. Click the FIDO U2F icon in Available Methods for Enrollment.

3. (Optional) Specify the Display Name.

4. Connect the device that complies with the U2F standards.

5. Click Detect U2F device.

   A message Please touch the flashing U2F device now. You may be prompted to allow the site permissions to access your security keys is displayed.

6. Touch the FIDO U2F button when there is a flash on the device.

   A message Enrollment is complete is displayed.

7. Click Save.

   A message The "U2F" authenticator has been saved is displayed. If there is no flash for more than 10 seconds, reconnect your token and repeat the steps.

**NOTE:** To use U2F in Google Chrome on Linux, you must perform the following steps:


   If the file is already available, ensure that the content is similar to that specified in https://github.com/Yubico/libu2f-host/blob/master/70-u2f.rules.

   **NOTE:** If your version of UDEV is lower than 188, use the rules specified at https://github.com/Yubico/libu2f-host/blob/master/70-old-u2f.rules.

2. Save the file 70-u2f.rules and reboot the system.

Testing the FIDO U2F Authenticator

1. Click the U2F icon in Your Enrolled Single Methods for sign in.

2. Click Test Method.

   A message Please touch the flashing U2F device now is displayed. You may be prompted to allow the site permissions to access the security keys in U2F device.
3. Touch the FIDO U2F button when there is a flash on the device.

A message **Test Successful** is displayed. If the connected token is invalid, a message **Token is not registered** is displayed.

The following table describes the possible error messages along with the workaround for the FIDO U2F authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cannot reach local FIDO U2F Service.</td>
<td>The FIDO U2F service is not installed properly.</td>
</tr>
<tr>
<td>Ask your admin to enable it. You may use Google Chrome browser, it has a built-in U2F support</td>
<td>Install the U2F service and try again.</td>
</tr>
<tr>
<td>Timeout. Press &quot;Save&quot; to start again</td>
<td>The session has timed out.</td>
</tr>
<tr>
<td>Enroll failed: Device not attested.</td>
<td>The token does not contain attested certificate.</td>
</tr>
<tr>
<td>Ask your administrator to upload your token attestation certificate</td>
<td>Contact your administrator to add the attestation certificate to your token.</td>
</tr>
<tr>
<td>Unexpected error: U2F token error: The visited URL does not match the application ID or it is not in use</td>
<td>The Facets are not configured appropriately. Contact your administration to check the Facets settings.</td>
</tr>
</tbody>
</table>

**Fingerprint**

The Fingerprint method enables you to authenticate using your fingerprint(s). During enrollment, the fingerprint reader captures the fingerprint. When you try to authenticate on any device, the presented fingerprint is matched with the enrolled fingerprint. If the fingerprints match, you are authenticated successfully.

You can enroll fingers for the Fingerprint method using one of the following devices:

- Single finger reader
- Multi-finger reader

**TIP:** Fingerprint(s) enrollment is supported only on Microsoft Windows and Linux RHEL kernel 3.x.x. You must install Advanced Authentication Device Service.

Linux RHEL supports the fingerprint readers: Green Bit DactyScan84c and Nitgen eNBioScan-C1 for the Fingerprint method enrollment and authentication respectively.

**Duress Finger**

The Fingerprint method also allows you to assign one of the enrolled fingers as duress. Only under an emergency or a threat, you can authenticate with the duress finger. Use of the duress finger for authentication sends an alert notification to the email address and phone number that the administrator has configured.
Enrolling the Fingerprint Authenticator Using Single Finger Reader

1. Click the Add icon in Your Enrolled Single Methods for sign in on the Authentication Methods page.

2. Click the Fingerprint icon in Available Methods for Enrollment.

3. (Optional) Specify the Display Name.

4. Select the preferred finger for enrollment and place or swipe the finger on the reader when there is a flash.

   **NOTE:** Number of fingers to be enrolled and the number of scans performed for each finger are mentioned on the SCAN FINGERPRINT screen.

5. Click Done after you scan the fingerprint.

6. Repeat Step 4 to add more fingers for authentication.

   **NOTE:** If you have not enrolled fingers for Fingerprint method, then the Assign Duress Finger list will be empty.

7. Click Save.

   A message The "Fingerprint" authenticator has been saved is displayed.

You can also assign a finger as duress, after enrolling the Fingerprint method. For more information, see Assigning a Finger as Duress.

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

Enrolling the Fingerprint Authenticator Using Multi-Finger Reader

1. Click the Add icon in Your Enrolled Single Methods for sign in on the Authentication Methods page.

2. Click the Fingerprint icon in Available Methods for Enrollment.

3. (Optional) Specify the Display Name.

4. (Conditional) Set Use multi-finger reader for enrollment to ON to use multi-finger reader.

   **NOTE:** An administrator has the privilege to hide the Use multi-finger reader for enrollment and force users to enroll with the multi-finger reader.

5. Select one of the highlighted fingers combination for enrollment. The fingers combination available are:
   - Four fingers of the left hand
Managing Authenticators New UI

- Four fingers of the right hand
- Two thumbs

6 Place the fingers on the reader when you see the LEDs of selected fingers flash. Wait till the reader scans the fingers.

Red indicators below the fingerprint represents the number of captures that the administrator has configured.

7 (Conditional) Select one of the enrolled finger as duress from Assign Duress Finger list.

**NOTE:** If you have not enrolled fingers for Fingerprint method, then the Assign Duress Finger list will be empty.

8 Click Save.

A message The "Fingerprint" authenticator has been added is displayed.

You can also assign a finger as duress, after enrolling the Fingerprint method. For more information, see Assigning a Finger as Duress.

Assigning a Finger as Duress

1 Click the Fingerprint icon in Enrolled Authenticators.
2 Select the preferred finger as duress from Assign Duress Finger list.
3 Click Save.

Testing the Fingerprint Authenticator

1 Click the Fingerprint icon in Your Enrolled Single Methods for sign in.
2 Click Test Method.
3 Place or swipe your finger on the reader.

A message Test Successful is displayed. If the fingerprints are not identical, a message Fingerprint Mismatch is displayed.

The following table describes the possible error message along with the workarounds for the Fingerprint authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprint Service is not available</td>
<td>The Advanced Authentication Device Service is not installed. Ensure to install Advanced Authentication Device Service and try authenticating again.</td>
</tr>
<tr>
<td>Fingerprint reader is not connected</td>
<td>The fingerprint reader or vendor specific drivers are not connected properly. Ensure that the fingerprint reader and vendor specific drivers are connected properly to the machine.</td>
</tr>
</tbody>
</table>
Home Affairs National Identification System (HANIS) Fingerprint

The HANIS fingerprint method is for the citizens of South Africa. This method enables you to enroll the personal identification number or password number issued by Home Affairs National Identification System. When you try to authenticate on any device, the presented fingerprint is matched with the enrolled fingerprint in the HANIS database. If the fingerprints match, you are authenticated successfully.

**NOTE:** If the Passport number or National ID is not registered in the repository for a user profile, then the HANIS method is not enrolled automatically. However, you can manually enroll the HANIS method from the Authentication Methods page.

Enrolling the HANIS Fingerprint Authenticator

1. Click the Add icon in Your Enrolled Single Methods for sign in on the Authentication Methods page.
2. Click the HANIS icon in Available Methods for Enrollment.
3. (Optional) Specify the Display Name.
4. Specify the passport number or national ID in ID/Passport number.
5. Specify the mobile number in Phone number.
6. Click Save.

A message The "HANIS Fingerprint" authenticator has been saved is displayed.

**NOTE:** An administrator has the privilege to hide the ID/Passport and Phone number to prevent users from providing new details that are not registered in the repository.

Testing the HANIS Fingerprint Authenticator

1. Click the HANIS icon in Your Enrolled Single Methods for sign in.
2. Click Test Method.

A message Place your finger on the reader is displayed.

3. Place or swipe your finger on the reader.

A message Test Successful is displayed. If the fingerprints are not identical, a message Fingerprint Mismatch is displayed.
Table 3-5  HANIS Fingerprint authenticator - error messages

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprint Service is not available</td>
<td>The Advanced Authentication Device Service is not installed. Ensure to install Advanced Authentication Device Service and try authenticating again.</td>
</tr>
<tr>
<td>Fingerprint reader is not connected</td>
<td>The fingerprint reader or vendor specific drivers are not connected properly. Ensure that the fingerprint reader and vendor specific drivers are connected properly to the machine.</td>
</tr>
<tr>
<td>The fingerprint capture does not comply with the size standard, image size should be 400 x 400 at least</td>
<td>The fingerprint reader captured images are not according to the standard size. Ensure to use a reader that provides clear fingerprint image.</td>
</tr>
</tbody>
</table>

**HANIS Face**

The HANIS (Home Affairs National Identification System) Face method is for the citizens of South Africa. This method enables you to enroll the personal identification number or passport number issued by Home Affairs National Identification System. When you try to authenticate on any device, the presented face is matched with the enrolled face in the HANIS database. If the images match, you are authenticated successfully.

**NOTE:** If the Passport number or National ID is not registered in the repository for a user profile, then the HANIS method is not enrolled automatically. However, you can manually enroll the HANIS Face method from the Authentication Methods page.

**Enrolling the HANIS Face Authenticator**

1. Click the **Add** icon in Your Enrolled Single Methods for sign in on the Authentication Methods page.
2. Click the HANIS Face icon in Available Methods for Enrollment.
3. (Optional) Specify the **Display Name**.
4. Specify the passport number or national ID in **ID/Passport number**.
5. Specify the mobile number in **Phone number**.
6. Click **Save**.
   A message The "HANIS Face" authenticator has been saved is displayed.

**NOTE:** An administrator has the privilege to hide the **ID/Passport** and **Phone number** to prevent users from providing new details that are not registered in the repository.
Testing the HANIS Face Authenticator

1. Click the HANIS Face icon in Your Enrolled Single Methods for sign in.
2. Click Test Method.
3. Present your face in front of the camera.
   
   If your face matches with the enrolled face, the authentication is successful and a message Test successful is displayed.
4. Click OK.

The following table describes the possible error messages along with the workaround for the HANIS Face authentication:

<table>
<thead>
<tr>
<th>Table 3-6  HANIS Face authenticator - Expected error messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error</td>
</tr>
<tr>
<td>Capture Device cannot be opened</td>
</tr>
<tr>
<td>Timeout</td>
</tr>
<tr>
<td>Face Angle to Large</td>
</tr>
<tr>
<td>Face cropped</td>
</tr>
<tr>
<td>Face is occluded</td>
</tr>
<tr>
<td>Face not found</td>
</tr>
<tr>
<td>Face too small</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Too many faces</td>
</tr>
<tr>
<td>Face close to border</td>
</tr>
<tr>
<td>Failed to predict landmarks</td>
</tr>
<tr>
<td>Face too close</td>
</tr>
</tbody>
</table>
HOTP

HOTP is a counter-based one-time password. This method enables you to authenticate using the counter-based one-time password generated on the HOTP token. The counter on the token must be in sync with the server. You can use generic HOTP tokens that adhere to RFC 4226. You must use the static secret key and three consequent OTP generated from the token to enroll. When you try to authenticate on any device, the OTP in the token is compared with the OTP generated in the server. If the OTPs are identical, you are authenticated successfully.

Enrolling the HOTP Authenticator

To enroll the HOTP authenticator, you must follow the recommendations of your system administrator. You can enroll HOTP in one of the following ways:

- Using YubiKey Hardware Token
- Using Software Token
- Synchronizing Existing Token with HOTP Counter
- Assigning a Token Serial To an Account

**NOTE:** If a token is already assigned to your account, enrollment is not required.

Using YubiKey Hardware Token

To enroll HOTP using YubiKey hardware token, perform the following steps:

1. Click the **Add** icon in **Your Enrolled Single Methods for sign in** on the **Authentication Methods** page.
2. Click the **HOTP** icon in **Available Methods for Enrollment**.
3. (Optional) Specify the **Display Name**.
4. Specify the token serial number in **OATH Token Serial**.
5. Specify the **YubiKeyToken Key ID**.
6. Specify the **Secret (if you know)**.
7. Place the cursor in **Value 1** and touch the button on YubiKey. OTP from YubiKey is inserted in **Value 1** automatically.
8. Repeat step 7 in **Value 2** and **Value 3** to insert consequent OTPs.
9. Click **Save**.

A message **The "HOTP" authenticator has been saved** is displayed.
**Using Software Token**

To enroll HOTP using RFC 4226 compliant software token, perform the following steps:

1. Click the **Add** icon in **Your Enrolled Single Methods for sign in** on the **Authentication Methods** page.
2. Click the **HOTP** icon in **Available Methods for Enrollment**.
3. Specify first OTP that generated on the token in **HOTP 1**.
4. Specify consequent OTPs from the token in **HOTP 2** and **HOTP 3**.
5. Specify 40 characters hexadecimal secret code in **Secret (If you know)**.
6. Click **Save**.

A message **The "HOTP" authenticator has been saved** is displayed.

**Synchronizing Existing Token with HOTP Counter**

If an existing token is assigned to your account, perform the following steps to synchronize the HOTP counter:

1. Click the **Add** icon in **Your Enrolled Single Methods for sign in** on the **Authentication Methods** page.
2. Click the **HOTP** icon in **Available Methods for Enrollment**.
3. Specify first OTP in **HOTP 1** that generated on the token. In case of YubiKey token, connect the hardware token to the system and perform the following steps:
   3a. Place cursor in **HOTP 1**.
   3b. Touch button on the token.
4. Specify the consequent OTPs from the token in **HOTP 2** and **HOTP 3**. In case of YubiKey token, repeat the steps 2a and 2b.
5. Click **Save**.

A message **The "HOTP" authenticator has been saved** is displayed.

**Assigning a Token Serial To an Account**

If administrator has uploaded the token details on the Advanced Authentication server and you have got the serial number of a token, perform the following steps to assign serial number to your account:

1. Click the **Add** icon in **Your Enrolled Single Methods for sign in** on the **Authentication Methods** page.
2. Click the **HOTP** icon in **Available Methods for Enrollment**.
3. (Optional) Specify a comment related to HOTP authenticator in **Comment**.
4. Specify the token's serial number in **OATH Token Serial**.
5 Specify the three consequent OTPs in HOTP 1, HOTP 2, and HOTP 3 respectively.
6 Click Save.

A message The "HOTP" authenticator has been saved is displayed.

Testing the HOTP Authenticator

1 Click the HOTP icon in Your Enrolled Single Methods for sign in.
2 Click Test Method.
3 Specify the OTP in Password.

If the OTP is valid, a message Authenticator "HOTP" passed the test is displayed.

The following table describes the possible error message along with the workarounds for the HOTP authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incorrect OTP password</td>
<td>If the specified OTP is incorrect or the counter on the token and server are not in sync. Specify a valid OTP and try to authenticate again</td>
</tr>
<tr>
<td>Cannot derive the counter. Check your three OTPs.</td>
<td>If one of the specified OTP is incorrect during the enrollment. Try to enroll again with the new OTPs.</td>
</tr>
</tbody>
</table>

LDAP Password

The LDAP password method enables you to authenticate using the password of your corporate account. When you try to authenticate on an application, the submitted password is compared with the actual password in the corporate directory. If both the passwords are identical, you are authenticated successfully.

Enrolling the LDAP Password Authenticator

This authenticator enrolls automatically and you cannot remove it. However, you can update the existing password.

NOTE: An administrator has the privilege to prevent users from updating their LDAP password and force users to enroll with the existing LDAP password.

If the administrator has prohibited the user from updating their LDAP password, the Change Password, Current Password, and New Password fields will not be displayed.

1 Click the Add icon in Your Enrolled Single Methods for sign in on the Authentication Methods page.
2 Click the LDAP Password icon in Your Enrolled Single Methods for sign in.
3 Click **Change Password** to update the LDAP Password.
4 Specify the existing LDAP password in **Current Password**.
5 Specify the new LDAP password in **New Password** and confirm it.
6 Click **Save**.

**Testing the LDAP Password Authenticator**

1 Click the LDAP password icon in **Your Enrolled Single Methods for sign in**.
2 Click **Test Method**.
3 Specify the valid password in **Password**.
   - If the password is valid, a message **Test successful** is displayed. If the provided password is invalid, a message **Incorrect password** is displayed.
4 Click **OK**.

**Out-of-Band**

The Out-of-band method facilitates you to authenticate using the authentication request that is sent to the Out-of-band portal, Authentication Agent for Windows or Authentication Agent for Web. When you initiate the authentication, an authentication request is sent to the Out-of-band portal, Authentication Agent for Windows or Authentication Agent for Web. You can accept the request and get authenticated.

**Enrolling the Out-of-Band Authenticator**

This authenticator enrolls automatically and you cannot remove it.

**Testing the Out-of-Band Authenticator**

1 Click the Out-of-band icon in **Your Enrolled Single Methods for sign in**.
2 Click **Test Method**.
3 Open the Out-of-band portal and authenticate using any of the available chains.
   - If you are using the Authentication Agent for Windows, the Authentication Agent window appears where you can authenticate.
4 Wait for a few seconds. If the authentication request did not appear, right click or long tap on blank space and click **Reload**.
5 Click **Accept** to accept the authentication request.
   - A message **Authenticator "Out-of-band" passed the test** is displayed.
   - If you click **Decline**, the authentication is declined and a message **Auth rejected** is displayed.
   - If you ignore the authentication request, after few minutes a message **Auth confirmation timeout** is displayed.
Password

The Password method enables you to authenticate using a secret string. The enrolled password is stored locally in the Advanced Authentication. When you try to authenticate on any device, the specified password is compared with the actual password. If the passwords are identical, you are authenticated successfully.

Enrolling the Password Authenticator

1. Click the Add icon in Your Enrolled Single Methods for sign in on the Authentication Methods page.
2. Click the Password icon in Available Methods for Enrollment.
3. (Optional) Specify the Display Name.
4. Specify Password and Confirmation.

NOTE: Ensure that the password must contain minimum 5 characters, by default. An administrator has the privilege to change the password length.
5. Click Save.

A message The"Password" authenticator has been added is displayed.

WARNING: You will not receive any notification about the password expiration. The password expiration value is 42 days, by default. Ensure to sign in to the Self-Service portal and change the password before it expires.

Testing the Password Authenticator

1. Click the Password icon in Enrolled Authenticators.
2. Click Test method.
3. Specify Password.
4. Click Next.

If the test is successful, a message Test Successful is displayed. If the provided authenticator is invalid, a message Incorrect password is displayed.

PKI

The PKI method enables you to authenticate using any one of the following ways:

- PKI Device
- Virtual Smartcard
PKI Device

PKI device is a hardware device such as a contact card and USB token that contains the digital certificate. The PKI reader validates the digital certificate and the identity of users. When you try to authenticate on any device, the certificate in the device is compared with the actual certificate. If the certificates are identical, you are authenticated successfully.

**NOTE:** You must install Advanced Authentication Device Service for enrolling the PKI method using PKI device.

Virtual Smartcard

You can also enroll and authenticate the PKI method using a virtual smartcard. Virtual smartcard supports authentication to any web environment and makes use of client SSL certificate to authenticate users. In client certificate authentication, the client browser provides its client certificate to the server to confirm the identity of a user.

A client SSL certificate is a file that contains information, such as digital signature, expiration date, name of user, and name of CA (Certificate Authority). When you try to authenticate on the web environment, authenticity of the client SSL certificate is validated based on the settings that are configured by the administrator.

Enrolling the PKI Authenticator Using PKI Device

1. Click the **Add** icon in **Your Enrolled Single Methods for sign in** on the **Authentication Methods** page.
2. Click the PKI icon in **Available Methods for Enrollment**.
3. (Optional) Specify the **Display Name**.
4. Insert the card in reader or connect the token to the machine.
5. Click **Get Certificates**.
   - A message *Use an existing certificate or generate a key pair is displayed.*
6. Select a key from **Key**.
   - If you have connected the token or card reader, the **Key** automatically populates the certificate with authentication key and its expiry date.
7. (Conditional) Enable **Show all** to view all the certificates.
8. Specify **PIN** code of the device.
9. Click **Save**.
   - A message *The "PKI" authenticator has been saved* is displayed.

Enrolling the PKI Authenticator Using Virtual Smartcard

1. Try to access the third party website from the browser where your administrator has imported a valid SSL certificate.
   - The **Certificate** dialog box is displayed.
2 Select the preferred client SSL certificate that is issued by the administrator.

You get auto-enrolled to PKI method using virtual smartcard.

**NOTE:** An administrator has the privilege to disable auto-enrollment of the PKI method using virtual smartcard.

### Testing the PKI Authenticator

1. Click the PKI icon in Your Enrolled Single Methods for sign in.
2. Click **Test Method**.
   A message *Waiting for card...* is displayed.
3. Insert your card or connect your token to the machine, if you are using a PKI device.
   If you are using a virtual smartcard, the client SSL certificate is detected automatically.
4. Specify the PIN of the PKI device in **PIN**.
   If the test is successful, a message *Test Successful* is displayed. If the card is invalid, a message *Wrong card* is displayed. If the specified PIN is invalid, a message *Incorrect PIN* is displayed.

The following table describes the possible error message along with the workarounds for the PKI authentication.

**Table 3-8 PKI authenticator - error messages**

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card reader connected</td>
<td>When a card is not inserted to the reader or the token is not connected to the machine. Insert the card to the reader or connect token to the machine.</td>
</tr>
<tr>
<td>Enroll failed: Cannot check revocation status for ...</td>
<td>When the certificate on your device does not contain information about the revocation status location or if the information is inserted, but the Certificate Authority is not available to verify the revocation status.</td>
</tr>
<tr>
<td>PKI service is not available</td>
<td>The Advanced Authentication Device Service is not installed on the system. Install the Device Service and try authenticating again.</td>
</tr>
<tr>
<td>Key not found. Wrong Card?</td>
<td>You have enrolled the PKI authenticator in the RDP session. Enroll the authenticator again in normal session.</td>
</tr>
<tr>
<td>PIN is expired</td>
<td>The PIN assigned to your token has expired. Contact your administrator for the new PIN.</td>
</tr>
<tr>
<td>PIN is locked</td>
<td>After certain number of attempts with the incorrect PIN, the PIN is locked. Contact your administrator to reset the PIN.</td>
</tr>
</tbody>
</table>
The following table describes the unexpected error codes that are displayed from a PKCS#11 module.

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CKR_DEVICE_ERROR</td>
<td>The token or USB slot is broken. Try to use a different USB slot.</td>
</tr>
<tr>
<td>CKR_DEVICE_MEMORY</td>
<td>There is no space available in the memory of token or there may be some other issue with the memory.</td>
</tr>
<tr>
<td>CKR_MECHANISM_INVALID</td>
<td>An invalid mechanism was specified to the cryptographic operation.</td>
</tr>
<tr>
<td>CKR_PIN_EXPIRED</td>
<td>Ensure that the card has been initialized or do not use the default PIN and the PIN has expired.</td>
</tr>
<tr>
<td>CKR_PIN_LOCKED</td>
<td>The user PIN is locked.</td>
</tr>
<tr>
<td>CKR_TOKEN_NOT_RECOGNIZED</td>
<td>The token has not been recognized.</td>
</tr>
<tr>
<td>OPERATION_FAILED</td>
<td>Contact your system administrator to analyze the debug logs.</td>
</tr>
</tbody>
</table>

RADIUS Client

The RADIUS Client method enables Advanced Authentication to forward the authentication request to a third-party RADIUS server. This can be any RADIUS server.

For example, you can use the RADIUS Client as an authentication method for token solutions such as RSA or Vasco.

Enrolling the RADIUS Client Authenticator

This authenticator is enrolled automatically and you cannot delete it.

By default, a user name from your corporate directory is set. You can change the required user name in Override User name and click Save.
Testing the RADIUS Client Authenticator

1. Click the RADIUS Client icon 🔄 in Your Enrolled Single Methods for sign in.
2. Click Test Method.
3. Specify the password of the RADIUS Client in Password.
   
   If the specified password is valid, a message Test successful is displayed.

The following table describes the possible error message along with the workarounds for the RADIUS Client authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incorrect password</td>
<td>If the specified RADIUS Client password is invalid. Specify a valid password to test the authenticator.</td>
</tr>
<tr>
<td>RADIUS server does not reply</td>
<td>If the administrator has not configured RADIUS Client method appropriately. Contact your administrator and report the error message.</td>
</tr>
</tbody>
</table>

SAML Service Provider

SAML Service Provider enables you to use authorization on the third-party websites (Identity Providers) to access the Advanced Authentication portals.

Enrolling the SAML Service Provider Authenticator

This authenticator is enrolled automatically.

By default, a user name from your corporate directory is set. You can change the required user name in Display name and click Save.

Testing the SAML Service Provider Authenticator

1. Click the Saml Service Provider icon 🔄 in Your Enrolled Single Methods for sign in.
2. Click Test Method.
   
   A message Test successful is displayed.

Security Questions

Security Questions method enables you to enroll answers to a pre-defined set of security questions. When you authenticate using security questions, Advanced Authentication prompts you the configured security questions or a subset of the security questions. You must answer the appropriate questions and based on the correctness of the answers, you are authenticated successfully.
Enrolling the Security Questions Authenticator

1. Click the Add icon in Your Enrolled Single Methods for sign in on the Authentication Methods page.
2. Click the Security Questions icon in Available Methods for Enrollment.
3. (Optional) Specify the Display Name.
4. (Optional) Select the preferred category from Category.
5. Specify the answers to the security questions that have been set by the administrator. Ensure that each answer contains at least one character.
6. Click Save.

A message The "Security Questions" authenticator has been saved is displayed.

Testing the Security Questions Authenticator

1. Click the Security Questions icon in Your Enrolled Single Methods for sign in
2. Click Test Method.
3. Specify the answers to the security questions.

A message Test successful is displayed. If one of the specified answer is invalid, a message Incorrect answers is displayed.

Smartphone

The Smartphone method facilitates you to enroll and authenticate using the smartphone app. When you initiate the authentication, a push notification is sent to the app. You can accept the request and get authenticated.

Pre-requisite:
To enroll the Smartphone authenticator, you must install the NetIQ Advanced Authentication app on your smartphone.

For more information about downloading and installing the smartphone app, see Installing NetIQ Advanced Authentication App.

Enrolling the Smartphone Authenticator

You can enroll the Smartphone method in one of the following ways:

- Enrolling with a QR code
- Enrolling with a link in the email
Enrolling With a QR Code

During the enrollment, you must scan a QR code that creates an authenticator on your mobile app. When you initiate the authentication, a push notification is sent to the app. You can accept the request and get authenticated.

To enroll the Smartphone method with a QR code, perform the following steps:

1. Click the **Add** icon in **Your Enrolled Single Methods for sign in** on the **Authentication Methods** page.
2. Click the **Smartphone** icon in **Available Methods for Enrollment**.
3. (Optional) Specify the **Display Name**.
4. Click **Get QR Code**.

A QR code is displayed.

5. Scan the QR code with the NetIQ Advanced Authentication smartphone app. To do this, perform the following steps:
   5a. Open the Advanced Authentication smartphone app.
   5b. Specify a PIN if applicable.
   5c. Click the + (plus) icon in the **Enrolled Authenticators** screen.
   5d. The camera of your smartphone is launched.
   5e. Scan the QR code with the camera.
   5f. Specify your user name and an optional comment in the app.
   5g. Tap **Save**.

The smartphone authenticator is created.

A message **Enrollment is complete** is displayed.

If you do not enroll the Smartphone authenticator within few minutes, an error message **Enrollment timeout** is displayed. Refresh the browser and enroll again.

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

1. Zoom the page to 125-150% and scan the zoomed QR code.
2. Ensure that nothing overlaps the QR code (mouse cursor, text).

Enrolling Through a Link

An administrator will send you the link to your email or via SMS. You must click on the link on your smartphone where the NetIQ Auth app is installed and you will be redirected to the smartphone app where you can enroll and an authenticator is created.

To enroll the Smartphone method through a link, perform the following steps:

1. Check your phone for a new email or SMS. You will receive a link sent by the administrator.
2. Click on the link. You will be redirected to the smartphone app.
If you have not installed the smartphone app, you will be redirected to the Google Play or AppStore from where you can install the app.

**NOTE:** In some instances, when you click on the enroll link, you will be redirected to page where the following two links are displayed:

- Click to enroll.
- Click to download and install Smartphone authenticator for Android.

If you have the app installed on your phone, use Click to enroll link. If you do not have the app then use Click to download link.

3 Specify a PIN or a Touch ID if applicable.
4 Specify your username and password in the Enroll new authenticator screen.
5 Tap Sign In.
6 Specify an optional comment in the app.
7 Tap Save.

The smartphone authenticator is created.

### Testing the Smartphone Authenticator

1 Click the Smartphone icon in Your Enrolled Single Methods for sign in
2 Click Test Method.
3 Open the Advanced Authentication smartphone app.
   A push notification is sent to your smartphone.
4 Tap Accept to accept the authentication request.
   A message Test successful is displayed.
   If you tap Reject, the authentication is declined and a message Authentication has been rejected is displayed.
   If you ignore the authentication request, after few minutes a message Authentication confirmation timeout is displayed.

### SMS OTP

The SMS OTP method facilitates you to generate a single-use password or OTP and send it to the registered mobile number for authentication. You can use this OTP to authenticate within a short time frame.

When authenticating on the same smartphone that receives SMS, you can do one of the following actions based on the platform of smartphone:

- **iOS:** The OTP auto inserts to clipboard, tap on the input field > OTP displayed above the keyboard.
• **Android 11 and later versions:** Tap Copy <OTP> in the SMS notification then tap on the input field > OTP displayed above the keyboard.

• **Android 10 and prior versions:** Open the SMS notification and copy OTP. Tap on the input field > OTP displayed above the keyboard.

**NOTE:** The OTP period is set to 120 seconds by default. An administrator has the privilege to change the OTP period.

**NOTE:** If a phone number is not registered in the repository for a user profile, then the SMS OTP method is not enrolled automatically. However, you can manually enroll the SMS OTP method from the Add Authenticator section, by specifying the phone number and clicking Save.

### Enrolling the SMS OTP Authenticator

1. Click the **Add** icon in Your Enrolled Single Methods for sign in on the Authentication Methods page.
2. Click the SMS OTP icon in Available Methods for Enrollment.
3. (Optional) Specify the **Display Name**.
4. If your mobile phone number is registered in the LDAP repository, then the phone number is displayed. To override the registered phone number, specify the mobile number in **Override Mobile Phone**.
   A message **Please enter OTP** is displayed.
5. Specify the verification code in **Enter verification code** to confirm the phone number is valid.
6. Click **Verify**.
   A message **The "SMS OTP" authenticator has been saved** is displayed.

**NOTE:** An administrator has the privilege to hide the Override Mobile Phone and verification code to prevent users from providing new phone number that is not registered in the repository.

### Testing the SMS OTP Authenticator

1. Click the SMS OTP icon in Your Enrolled Single Methods for sign in.
2. Click **Test Method**.
3. You will receive an SMS with an OTP.
4. Specify the OTP in **Password**.
5. Click **Test**.
   A message **Test successful** is displayed.

The following table describes the possible error message along with the workarounds for the SMS OTP authentication.
Table 3-11  SMS OTP authenticator - error messages

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incorrect OTP password</td>
<td>The specified OTP is invalid. Specify a valid OTP and try again.</td>
</tr>
<tr>
<td>You do not have a phone number.</td>
<td>If your phone number is not registered in the repository. Contact administrator or helpdesk to register phone number.</td>
</tr>
</tbody>
</table>

Swedish BankID

The Swedish BankID method enables you to authenticate using your Swedish Personal Identification Number. To enroll the Swedish BankID authenticator, you must have the BankID app either on your computer or mobile device. When you try to authenticate any device a request is sent to the BankID app, specify the security code to unlock the app. The recorded personal identification number is compared with actual identification number on the BankID app. If the identification numbers match, you are authenticated successfully.

Enrolling the Swedish BankID Authenticator

Before enrolling, ensure that you have the following prerequisites:

- Social Security Number (SSN)
- BankID app (either desktop or mobile version).
  
For more information about the BankID app, see BankID.

**NOTE:** While you set up the security code for the BankID app, ensure that the code must contain six digits in non-sequential format (for example: 221144).

To enroll the Swedish BankID, perform the following steps:

1. Click the Add icon in Your Enrolled Single Methods for sign in on the Authentication Methods page.
2. Click the BankID icon in Available Methods for Enrollment.
3. (Optional) Specify the Display Name.
4. Specify the personal identification number in Personal ID (SSN).
5. Click Save.
   
A message The "BankID" authenticator has been saved is displayed.

Testing the Swedish BankID Authenticator

1. Click the BankID icon in Your Enrolled Single Methods for sign in.
2. Click Test Method.
A message Enter your security code in the BankID app and select Identify is displayed.

3 Open the BankID app.

4 Specify Security Code.
  * ( Conditional) Click Identify on the mobile app.
  * ( Conditional) Click Verify my identity on the desktop app.

If the test is successful, a message Test successful is displayed.

Swisscom Mobile ID

The Swisscom Mobile ID authentication method uses the phone number from your profile of the repository. The authenticator sends an authentication request to your mobile phone. You need to accept it.

This authenticator is enrolled automatically and you cannot remove it.

Testing the Swisscom Mobile ID Authenticator

1 Click the My Swisscom Mobile ID icon  in Your Enrolled Single Methods for sign in.

2 Click Test Method.

A message is displayed indicating that you must accept the request on the mobile phone.

3 Accept the request.

A message Authenticator "Swisscom Mobile ID" passed the test is displayed.

TOTP

The TOTP method enables you to authenticate using the time-based-one-time password. TOTP is generated on the hardware token, Desktop OTP tool, or the mobile app, such as NetIQ Advanced Authentication app or Google Authenticator app. The TOTP is valid for a short duration. This method uses a predefined period. The default value is 30 seconds.

You can enroll the TOTP authenticator using the Desktop OTP tool. To initiate the tool, use the link that is sent from your administrator. You must click on the link and the Desktop OTP tool is prompted where you can enroll and create an account. While authenticating to any service, you must copy the OTP from the tool and use the OTP to get authenticated.

Enrolling the TOTP Authenticator

To enroll the TOTP authenticator, follow the recommendations of your system administrator. You can enroll TOTP method using any one of the following ways:
  * NetIQ Advanced Authentication App
  * Google Authenticator App
  * OATH Compliant Hardware Token
Enrolling TOTP Manually

Desktop OTP Tool

WARNING: The QR code format in the Advanced Authentication and Google Authenticator apps are different. Contact your system administrator to confirm the app recommended for enrollment.

NetIQ Advanced Authentication App

To enroll the TOTP authenticator using Advanced Authentication smartphone app, perform the following steps:

1. Click the Add icon in Your Enrolled Single Methods for sign in on the Authentication Methods page.
2. Click the TOTP icon in Available Methods for Enrollment.
3. Click Get QR Code
4. Open the Advanced Authentication app on your phone.
5. Tap Offline authentication.
6. Tap + to add a new authenticator.
7. Scan the QR code using the camera on your phone.
8. Click Save in the Add TOTP authenticator page.
   A message The "TOTP" authenticator has been saved is displayed.
9. Tap the new authenticator and specify account name and additional details in Account and Additional info respectively in the app.
10. Click Save.

TIP: If you are unable to scan the QR code with Advanced Authentication app, perform the following steps:
    1. Zoom the page to 125 - 150%.
    2. Scan the zoomed QR code using Google Authenticator app.
       Ensure that the mouse cursor is not overlapping the QR code.
    If you are still unable to scan the QR code, contact your system administrator.

Google Authenticator App

To enroll the TOTP authenticator using Google Authenticator app, perform the following steps:

1. Click the Add icon in Your Enrolled Single Methods for sign in on the Authentication Methods page.
2. Click the TOTP icon in Available Methods for Enrollment.
3. Open the Google Authenticator app on your phone.
4. Tap BEGIN SETUP in the app.
5 Tap Scan barcode to add a new authenticator in the app.
6 Scan the QR code using the camera on your phone.
7 Click Save.
   A message The "TOTP" authenticator has been saved is displayed.

**TIP:** If you scan Advanced Authentication app compatible QR code with Google Authenticator app, a message Invalid barcode is displayed.

### OATH Compliant Hardware Token

To enroll the TOTP authenticator using OATH compliant hardware token, perform the following steps:

1 Click the Add icon in Your Enrolled Single Methods for sign in on the Authentication Methods page.
2 Click the TOTP icon in Available Methods for Enrollment.
3 (Optional) Specify a comment related to TOTP authenticator in Comment.
4 (Optional) Select the preferred category from Category.
5 Specify the token's serial number in OATH Token Serial.
   You can find the serial number behind the token.
6 Press the button on the token and specify the one-time password in OTP.
7 Click Save.
   A message The "TOTP" authenticator has been saved is displayed.

### Enrolling TOTP Manually

1 Click the Add icon in Your Enrolled Single Methods for sign in on the Authentication Methods page.
2 Click the TOTP icon in Available Methods for Enrollment.
3 (Optional) Specify a comment related to TOTP authenticator in Comment.
4 (Optional) Select the preferred category from Category.
5 Click + adjacent to Specify the TOTP secret manually.
6 Specify 40 hexadecimal characters in Secret.
7 Set Google Authenticator format of secret (Base32) to ON to display the Google Authenticator app compatible QR code.
   By default, Google Authenticator format of secret (Base32) is set to OFF and Advanced Authentication app compatible QR code is displayed.
NOTE: The administrator has privilege to configure the Google Authenticator format of secret (Base32) option in the Administration portal. But you can override the administrator configured setting.

8 Set the preferred value in Period. 30 seconds is set by default.
9 Click Save.

A message The "TOTP" authenticator has been saved is displayed.

NOTE: If the administrator has disabled the manual enrollment of TOTP in the Administration portal, then the Specify the TOTP secret manually section is not displayed.

Desktop OTP Tool

Before enrolling the TOTP authenticator using the link, ensure that NetIQ Desktop OTP tool is installed on your system.

1 Check your registered email or phone for the enrollment link.
2 Click on the link.

You are directed to the Desktop OTP tool.
3 Specify your LDAP repository or local username, password and optional comment in the NetIQ Advanced Authentication OTP Tool window.
4 Click OK.

The TOTP authenticator is created in the Desktop OTP tool and enrolled in the Self-Service portal.

Testing the TOTP Authenticator

1 Click the TOTP icon in Your Enrolled Single Methods for sign in.
2 Click Test Method.
3 Specify one-time password in Password.
4 Click Next.

If the test is successful, a message Test Successful is displayed. If the one-time password is invalid or the server time is not in sync, a message Incorrect OTP password is displayed.

Voice

The Voice method initiates a call to your registered phone number. The phone call requests you to specify the PIN in the dial pad of your mobile to authenticate. When you try to authenticate on any device, the recorded PIN is compared with the actual PIN. If both PINs are identical, you are authenticated successfully.

NOTE: If a phone number is not registered in the repository for a user profile, then the Voice method is not enrolled automatically. However, you can specify the phone number in the Add Authenticator section and click Save to enroll manually.
Enrolling the Voice Authenticator

1. Click the Add icon in Your Enrolled Single Methods for sign in on the Authentication Methods page.
2. Click the Voice icon in Available Methods for Enrollment.
3. (Optional) Specify the Display Name.
4. Specify a PIN. The PIN must contain minimum 3 digits, by default.
5. If your mobile phone number is registered in the LDAP repository, then the phone number is displayed. To override the registered phone number, specify the mobile number in Override Phone.
6. Click Save.
   A message The "Voice" authenticator has been saved is displayed.

**NOTE:** An administrator has the privilege to hide Phone number to prevent users from providing new phone number that is not registered in the repository.

Testing the Voice Authenticator

1. Click the Voice icon in Your Enrolled Single Methods for sign in.
2. Click Test Method.
   A message Call has been initiated is displayed.
3. Answer the call on your phone.
4. Specify your PIN followed by a hash symbol (#) in the dial pad of your mobile phone.
   A message Test successful is displayed. If the specified PIN is invalid, a message Incorrect PIN is displayed.

**WARNING:** You will not receive any notification about the PIN expiration. The PIN expiration is set as 42 days, by default. You must sign in to the Self-Service Portal and change the PIN before it expires.

Voice OTP

The Voice OTP method enables you to authenticate using the OTP that is sent through the phone call to your registered phone number. You can use this OTP for authentication within a short duration. When you try to authenticate on any device, the specified OTP is compared with the OTP generated on the server. If both the OTPs are identical, you are authenticated successfully.

**NOTE:** If a phone number is not registered in the repository for a user profile, then the Voice OTP method is not enrolled automatically. However, you can manually enroll the Voice OTP method from the Your Enrolled Single Methods for sign in section, specify the phone number and click Save.
Enrolling the Voice OTP Authenticator

This authenticator enrolls automatically and you cannot remove it.

1. Click the Add icon in Your Enrolled Single Methods for sign in on the Authentication Methods page.
2. Click the Voice OTP icon in Available Methods for Enrollment.
3. (Optional) Specify the Display Name.
4. If your mobile phone number is registered in the LDAP repository, then the phone number is displayed. To override the registered phone number, specify the mobile number in Override Mobile Phone.
   A message Please enter OTP is displayed.
5. Specify the verification code in Enter verification code to confirm the phone number is valid.
6. Click Save.
   A message The "Voice OTP" authenticator has been saved is displayed.

**NOTE:** An administrator has the privilege to hide Override Mobile Phone and verification code to prevent users from providing new phone number that is not registered in the repository.

Testing the Voice OTP Authenticator

1. Click the Voice icon in Your Enrolled Single Methods for sign in.
2. Click Test Method.
   A message OTP password sent, please specify is displayed.
3. Receive the call on your phone and listen to the voice OTP.
4. Specify the OTP in Password.
   A message Test successful is displayed. If the specified OTP is invalid, a message Incorrect OTP password is displayed.

Web Authentication Method

Advanced Authentication enables you to use authorization on the third-party websites (Identity Providers) to access the Advanced Authentication portals.

Enrolling the Web Authentication Authenticator

1. Click the Add icon in Your Enrolled Single Methods for sign in on the Authentication Methods page.
2. Click the Web Authentication icon in Available Methods for Enrollment.
3. (Optional) Specify the Display Name.
4 Select the Identity Provider.
5 (Optional) Specify a hint for the user in Username or email.
6 Click Start.
7 Click Save.

The enrollment is redirected to the Identity Provider page that you have selected. Specify your credentials.

You will be redirected to the Enrollment page with your enrolled authenticator.

An error Web Authentication failed might be displayed after the authorization on third-party websites during enrollment. Contact your administrator to verify the Web Authentication method settings.

Testing the Web Authentication Authenticator

1 Click the Web Authentication icon in Your Enrolled Single Methods for sign in.
2 Click Test Method.

You will be automatically authenticated by the enrolled Identity Provider.

Windows Hello

The Windows Hello method facilitates you to use your Windows Hello fingerprint and facial recognition authentication to log in to the Windows 10 operating system. Advanced Authentication supports the Windows Hello fingerprint and facial recognition.

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

This method supports all the devices that Windows Hello works with. For example, the Windows Hello facial recognition works with only the infrared cameras. Therefore, the Advanced Authentication Windows Hello method also supports only the infrared camera for facial recognition.

Configuring the System Settings for Windows Hello

Before enrolling Windows Hello, you must configure the system settings.

• “Configuring Settings for Windows Hello Fingerprint” on page 102
• “Configuring Settings for Windows Hello Face Recognition” on page 103

NOTE: You cannot enroll the Windows Hello authentication on an RDP session.

Configuring Settings for Windows Hello Fingerprint

1 Click Start > Settings > Accounts > Sign-in options.

Under Windows Hello, the options for fingerprint is displayed if your PC has a fingerprint reader.
2 Click Set up under Fingerprint.
3 Click Get started.
4 Specify your PIN.

**NOTE:** If you do not have a PIN, you must create one to set up the fingerprint.

5 To enroll fingerprint, scan your finger on the fingerprint reader.
   You will have to place your finger multiple times to provide the scanner a good picture of your
   fingerprints.
6 Click Add Another if you want to add another fingerprint.

### Configuring Settings for Windows Hello Face Recognition

1 Click Start > Settings > Accounts > Sign-in options.
   Under Windows Hello, the option for face recognition is displayed if your computer has an
   external camera.
2 Click Set up under Face Recognition.
3 Click Get started.
4 Specify your PIN.

**NOTE:** If you do not have a PIN, you must create one to set up the face recognition.

5 To enroll the face, present your face to the camera. Scan your face by following the on-screen
   instructions.
6 Select Finish to complete scanning or choose Improve Recognition to continue scanning.

**NOTE:** It is recommended that you select to improve recognition if you change your appearance
   often. Scanning your face again does not erase the earlier scans. It just helps Windows Hello get
   better at recognizing you.

For more information about Windows Hello, see the Microsoft Windows website https://

**NOTE:** To enable Windows Hello for all domain-joined Windows 10 workstations and for Windows
10 Enterprise, see https://community.spiceworks.com/topic/1840001-windows-10-fingerprint-
some-settings-are-managed-by-your-organization.

### Enrolling the Windows Hello Authenticator

1 Click the Add icon in Your Enrolled Single Methods for sign in on the Authentication Methods
   page.
2 Click the Windows Hello icon in Available Methods for Enrollment.
3 (Optional) Specify the Display Name.
4 Specify your username for which Windows Hello is enrolled in Windows User Name.
NOTE: If you have enrolled Windows Hello for a local account, you must specify the
<workstationname>\<username>.

If you want to enroll Windows Hello that is set for a Microsoft account, you can specify
microsoftaccount\user@outlook.com as the user name. This is helpful if you must login
to the Windows operating system using your Microsoft account.

5 Click Save.

A message The "Windows Hello" authentication has been saved is displayed.

Testing the Windows Hello Authenticator

1 Click the Windows Hello icon in Your Enrolled Single Methods for sign in.
2 Click Test Method.
3 Place your finger on the reader or swipe your finger on the swipe sensor for the fingerprint
authentication. Present your face for the facial recognition.

An appropriate message is displayed indicating the result of the test.

Enrolling Multiple Methods of a Chain in Sequence

If the administrator creates a chain with multiple methods in it, you must enroll all methods in the
chain to perform authentication with Advanced Authentication. You can enroll the methods
individually in Your Enrolled Single Methods for sign in or sequentially in Your Enrolled Sequence for
sign in. During authentication, you might get a prompt to select the chain available for you. However,
Advanced Authentication selects an appropriate chains automatically.

Sample Scenario: Enrolling Card and U2F Methods in the
Sequence of a Chain

Sam, an administrator, has performed the following steps to create a chain with multiple methods in it:

1 Created a chain with the Card and U2F method.
2 Set All Categories to ON (default) in the Windows Logon event and map the chain to the event.

Tom, an end user, logs in to the Self Service portal and performs the following actions to enroll the
chain:

1 Click the Add icon in Your Enrolled Sequences for sign in on the Authentication Methods
page.
2 Select the chain icon in Available Sequences for Enrollment.
3 (Optional) Specify the Display Name.

Connect the card reader.
4 Click Scan Card.

A message Waiting for the card is displayed.
5 Tap a card on the reader.
   A message Enrollment is complete is displayed.
6 Click Next.
   A message The "Card" authenticator has been saved is displayed.
7 (Optional) Specify the Display Name.
   Connect the device that complies with the U2F standards.
8 Click Detect U2F device
   A message Please touch the flashing U2F device now. You may be prompted to allow the site permissions to access your security keys is displayed.
9 Touch the FIDO U2F button when there is a flash on the device.
   A message Enrollment is complete is displayed.
10 Click Finish.
   A message The "U2F" authenticator has been saved is displayed.

Testing the Authenticators

After enrollment, Tom performs the following steps to test the chain with Card and U2F methods:

1 Select the chain with Card and U2F methods in Your Enrolled Sequences for sign in.
2 Click Test Method.
   A message Test Card Method is displayed.
3 Tap the enrolled card on the reader.
   If the provided card passes the test, a message Test successful is displayed.
4 Click Next.
5 Click Test Method.
   A message Please touch the flashing U2F device now is displayed. You may be prompted to allow the site permissions to access the security keys in U2F device is displayed.
6 Touch the FIDO U2F button when there is a flash on the device.
   A message Test successful is displayed.
7 Click Finish.
Logging In to Authentication Agent for Windows

Authentication Agent for Windows enables you to perform multi-factor authentication on one device to get authorized access to another device, where it is not possible to display the user interface or connect any external authentication device. You can install the Authentication Agent for Windows on a workstation or a laptop with Microsoft Windows. When an authentication is initiated from a computer using the chain with OOB method, the Authentication Agent for Windows on another computer prompts a restricted browser where you must perform the authentication to access the Out-of-Band portal. In the Out-of-Band portal, accept the authentication request to authenticate successfully.

Scenario 1: Authenticating to Linux computer using the Authentication Agent for Windows

Mark uses the SSH to access Linux computer. But, the external devices such as FIDO U2F token and card reader are not supported in SSH. He cannot get authenticated to Linux computer because it is not possible to redirect the external devices. In this case, Mark can use Authentication Agent for Windows to perform authentication on Windows computer and get seamless access to Linux computer.

Consider the following setup:

- Windows computer is installed with the Authentication Agent for Windows and is connected with the external devices such as FIDO U2F token and card reader.
- Linux computer is not connected with the external devices.

Following sequence describes the authentication process using Authentication Agent for Windows:

1. Specify user name and select the chain with OOB method in the Linux machine. This initiates an authentication request.
2. Authentication Agent for Windows launches a restricted browser.
3. Select the chain with FIDO U2F and Card methods in the restricted browser to authenticate to the Out-of-Band portal.
4. Perform the authentication using the FIDO U2F token and card reader in the restricted browser.
5. An authentication request with Accept and Decline buttons are displayed on the portal.
6. Click Accept.
   Mark logs in to Linux computer automatically.
Scenario 2: Authenticating to Windows computer using the Authentication Agent for Windows

Thomas works on two Windows computers simultaneously. However, the external devices such as FIDO U2F token and card reader are connected to one Windows computer. He cannot get authenticated to the other computer because there are no external devices connected to this computer and cannot redirect the external devices. In this case, Thomas can use Authentication Agent for Windows to perform authentication on one Windows computer and get seamless access to another Windows computer that does not have external devices.

Consider the following setup:

- Windows A is a computer with the Authentication Agent for Windows installed and is connected with the external devices such as FIDO U2F token and card reader.
- Windows B is computer without the external devices.

The following sequence describes the authentication process using the Authentication Agent:

1. Specify user name and select the chain with OOB method in Windows B computer.
2. The Authentication Agent on Windows A computer launches a restricted browser.
3. Select the chain with FIDO U2F and Card methods in the restricted browser to authenticate to the Out-of-Band portal.
4. Perform the authentication using the FIDO U2F token and card reader in the restricted browser.
5. An authentication request with Accept and Decline buttons are displayed on the portal.
6. Click Accept.

Thomas is logged in to Windows B computer automatically.

Logging In to Authentication Agent for Windows

You can log in to the Authentication Agent in one of the following ways:

- Single Sign-on Login
- Manual Login

Ensure that you have installed the Authentication Agent for Windows as a pre-requisite.

Single Sign-on Login

If Windows Client is installed along with the Authentication Agent for Windows and when you authenticate to Windows you are automatically logged in to the Authentication Agent for Windows. Else, when Windows is loading, you are prompted with an authentication request to log in manually. You must log in to authorize the Authentication Agent for Windows to receive any authentication request.

Manual Login

To log in to the Authentication Agent for Windows manually, perform the following steps:

1. Right-click on the Authentication Agent icon in the System Tray.
2. Select Log on.
3 Authenticate using the available chain in Windows.

A prompt to select category might appear, if you have enrolled an authenticator for more than one category.

Advanced Authentication provides the following authenticators for logging in to Authentication Agent for Windows:

- “Bluetooth” on page 110
- “Bluetooth eSec” on page 110
- “Card” on page 111
- “Device Authentication” on page 112
- “Email OTP” on page 113
- “Emergency Password” on page 113
- “Facial Recognition” on page 114
- “Flex OTP” on page 115
- “Fingerprint” on page 115
- “Home Affairs National Identification System (HANIS)” on page 116
- “HOTP” on page 116
- “LDAP Password” on page 117
- “Password” on page 117
- “PKI” on page 118
- “RADIUS Client” on page 119
- “Security Questions” on page 119
- “Smartphone” on page 120
- “SMS OTP” on page 121
- “Swisscom Mobile ID” on page 122
- “TOTP” on page 122
- “FIDO U2F” on page 123
- “Voice” on page 124
- “Voice OTP” on page 124
- “Windows Hello” on page 124
**Bluetooth**

The Bluetooth method enables you to authenticate using any Bluetooth enabled device that is within the range. When you initiate authentication, the Advanced Authentication server searches for the enrolled Bluetooth device. If the enrolled device is within the range, you are authenticated successfully.

For example, Susanne, who is a doctor, attends many in-patients in the hospital. She accesses the computer located in each room to monitor and update the health status of the patient. In this case, Susane can specify her first-factor authentication details and use her Bluetooth enabled mobile phone to log in to the computer automatically when she is within range of a particular room. When she exits the room, she is logged out of that computer automatically.

**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 using the Bluetooth method, perform the following steps:

1. Ensure that Bluetooth is turned on in your device and is discoverable to the paired devices.
2. The Device Service detects your Bluetooth device and authenticates. If the paired Bluetooth device is within the range, the Bluetooth authentication is successful.

**NOTE:** If the administrator has set Enable reaction on device removal option to ON for Bluetooth method then the operating system automatically locks, if one of the following is true:

- The Bluetooth device is disabled.
- The Bluetooth device is out of range.

**Bluetooth eSec**

The Bluetooth eSec method allows you to authenticate with wireless technology using any Bluetooth supported mobile device within a short range. When you initiate authentication, the Advanced Authentication Server detects the enrolled Bluetooth device within the define range. If the enrolled device is available, you are authenticated successfully.

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

To authenticate using the Bluetooth eSec method, perform the following steps:

1. Ensure that Bluetooth is turned on in your device and is discoverable to the paired devices.
2. The device service detects your enrolled Bluetooth device and authenticates it. If the enrolled Bluetooth device is within the range, the Bluetooth authentication is successful.
NOTE:

- If the administrator has set the Required paired device (more secure) option to ON for the Bluetooth eSec method then you must authenticate to the Windows machine with only paired devices.
- If the administrator has set Enable reaction on device removal option to ON for Bluetooth eSec method then the operating system automatically locks, if one of the following is true:
  - The Bluetooth device is disabled.
  - The Bluetooth device is out of range.

## Card

The Card method enables you to authenticate using the contactless smart card (with the card serial number). When you try to authenticate on any device, the recorded serial number of the card is compared with the actual serial number. If the card serial numbers are identical, you are authenticated successfully.

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 using the Card method, perform the following steps:

1. Ensure that the card reader is connected to your system.
2. Tap your card on the reader or insert a smart card in the reader.
   
   If the Card Serial Number in the card matches with enrolled card, the card authentication is successful.

IMPORTANT: The Card method supports the 1:N feature that Advanced Authentication to detect the user name automatically. You can press CTRL+ALT+DEL then place a card to the reader to authenticate.

The following table describes the possible error messages along with the workarounds for the Card authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong card</td>
<td>The card you have placed on the reader is incorrect. Try again with another card or re-enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
<tr>
<td>Connect reader</td>
<td>The reader is not connected properly. Try to connect it to a different USB slot and try again.</td>
</tr>
</tbody>
</table>
Logging In to Authentication Agent for Windows

IMPORTANT: An administrator has the privilege to configure an automatic session lock or log off for the events with Card authentication method. In such a scenario, you must:

- When Tap&Go is disabled, you must place your card on the reader during login. After login you can remove the card from the reader to lock the operating system or log off automatically.
  Or
- When Tap&Go is enabled, you must tap a card on the reader to log in and to lock, unlock, or log off.

Device Authentication

You can authenticate to Windows workstation using the Device Authentication method using one of the following:

- Using Trusted Platform Module (TPM) chip
  The TPM chip is a crypto-processor available in Windows workstation to achieve actions, such as generating, storing, and limiting the use of cryptographic keys. Device Authentication supports authentication to Windows workstation and makes use of information available in the chip to authenticate users.
- Non-TPM mode
  In this mode, a key pair is generated in the workstation during the enrollment process that is used for further authentication on the same workstation.

NOTE: In non-TPM mode, ensure to enroll the Device Service method using the workstation where you would perform further authentication. Enrollment on one machine and authentication on another machine is not supported.

To authenticate with the Device Authentication method, perform the following steps:

1. Specify one of the following:
   - The TPM chip generated PIN
   - The enrolled PIN

2. Click Next.
   If the PIN matches with the TPM chip generated PIN or enrolled PIN, the Device Authentication is successful.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Your user name&gt; has no authenticator for Card</td>
<td>You have not enrolled the card method. You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
<tr>
<td>No template for Card</td>
<td>The card is not enrolled or you are trying to log in with the non-cached authenticator in the offline mode.</td>
</tr>
</tbody>
</table>
**Email OTP**

The Email OTP method enables you to authenticate using the one-time password (OTP) that is sent to the registered email address. When you try to authenticate on any device, the server sends an email to the registered email address with the OTP. You can use this OTP for single authentication within a short time frame.

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

1. Check your email. You will receive an email with an OTP.
2. Specify the OTP from email in Password.
3. Click Next.

   If the OTP matches with the server generated OTP, the Email OTP authentication is successful.

The following table describes the possible error messages along with the workarounds for the Email OTP authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong answer</td>
<td>The specified OTP is incorrect or is expired. Try to specify a valid OTP within the time frame.</td>
</tr>
<tr>
<td>Cannot send OTP. User does not have an email</td>
<td>Your email address is not set in the profile of the repository. Contact your system administrator to add your email address to the profile.</td>
</tr>
</tbody>
</table>

**Emergency Password**

The Emergency Password method enables you to authenticate using a temporary password with the help of helpdesk administrator if you have lost a smart card or forgot your smart phone. The emergency password is valid for certain days and is set to 3 days by default. When you try to authenticate on any device, the submitted emergency password is compared with the enrolled password in the appliance. If the emergency passwords are identical, you are authenticated successfully.

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

1. Specify the emergency password.
2. Click Next.

   If the emergency password matches with the enrolled password, the emergency password authentication is successful.

The following table describes the possible error message along with the workarounds for the Emergency Password authentication.
Facial Recognition

The Facial Recognition method enables you to get automatically authenticated by presenting your face. You need to register your face image using the web camera. When you try to authenticate on an application, the recorded image is compared with the actual image. If the images match, you will be successfully authenticated.

The Facial Recognition method works with both integrated and external web cameras.

**NOTE:** To use the Facial Recognition method for authentication, you must install the Advanced Authentication Device Service. For more information about the Device Service, see the “Advanced Authentication - Device Service” guide.

To authenticate using the Facial Recognition method, perform the following steps:

1. Ensure that a camera is connected to your device.
2. Present your face to the camera.
   
   If your face matches with the enrolled face, the face authentication is successful.

The following table describes the possible error message along with the workarounds for the Facial Recognition authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong password</td>
<td>The specified emergency password is incorrect. Specify a valid emergency password and try to authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for Emergency Password</td>
<td>You have not enrolled for Emergency Password method. Enroll the authenticator on the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
<tr>
<td>Failed to open camera</td>
<td>If the camera is not connected properly. Check your camera settings and try again.</td>
</tr>
<tr>
<td>Mismatch</td>
<td>The enrolled face and presented face does not match. You must present your face again for the authentication.</td>
</tr>
<tr>
<td>Face service is not available</td>
<td>The Device Service is not available. Ensure that the Device Service is installed.</td>
</tr>
</tbody>
</table>
Flex OTP

The Flex OTP authenticator facilitates you to authenticate by using your otp password from any of HOTP, TOTP and Smartphone (Offline) authenticator. When you try to authenticate to any device, the OTP in the token is compared with the OTP generated in any of HOTP, TOTP and Smartphone (Offline) authenticators. If the OTPs are valid, you are authenticated successfully.

To authenticate using the Flex OTP method, perform the following steps:

1. Specify the One-Time Password from any of HOTP, TOTP and Smartphone (Offline) authenticators
2. If the password is valid, the Flex OTP authentication is successful.

Fingerprint

The Fingerprint authentication method enables you to authenticate using your fingerprint. The fingerprint scanner captures the fingerprint. When you try to authenticate on any device, the recorded fingerprint is compared with the actual fingerprint. If the fingerprints are identical, you are authenticated successfully.

**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 using the Fingerprint method, perform the following steps:

1. Ensure that a fingerprint reader is connected to the computer.
2. Place your finger on the reader when using a touch sensor or swipe your finger when using a swipe sensor.
   - If the fingerprint matches with the enrolled fingerprint, the authentication is successful.

**NOTE:** Ensure to enroll the required fingers that are highlighted in the Add Fingerprint Authenticator page.

The following table describes the possible error message along with the workarounds for the Fingerprint authentication.
Home Affairs National Identification System (HANIS)

The HANIS method is for the citizens of South Africa. The HANIS method enables you to authenticate using your fingerprint that is registered in the National Identification System. The fingerprint scanner captures the fingerprint. When you try to authenticate on any device, the fingerprint available in the National Identification System is compared with the captured fingerprint. If fingerprints are identical, you are authenticated successfully.

NOTE: To use the Fingerprint method for authentication, you must install the Advanced Authentication Device Service. For more information, see Installing and Upgrading Device Service on Windows in the Advanced Authentication - Device Service.

To authenticate using the HANIS method, perform the following steps:

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

   If fingerprint matches with the fingerprint available in the National Identification System, the authentication is successful.

HOTP

HOTP is a counter-based one-time password. This method enables you to authenticate using the counter-based one-time password generated on the HOTP token. The counter on the token must be in sync with the server. You can use generic HOTP tokens that adhere to RFC 4226. You must use the static secret key and three consequent OTP generated from the token to enroll. When you try to authenticate on any device, the OTP in the token is compared with the OTP generated in the server. If the OTPs are identical, you are authenticated successfully.

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

1. Specify the OTP when using software token or some kind of hardware tokens or connect the USB token, press button on the token.
Click Next.

If the OTP on the token and the server generated OTP are identical, the HOTP authentication is successful.

The following table describes the possible error message along with the workarounds for the HOTP authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong answer</td>
<td>The OTP you have provided is incorrect. Specify a valid OTP and try again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for HOTP</td>
<td>You have not enrolled for HOTP method. You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>

**LDAP Password**

The LDAP password method enables you to authenticate using the password of your corporate account. When you try to authenticate on any device, the specified password is compared with the actual password in the corporate directory. If both the passwords are identical, you are authenticated successfully.

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

1. Specify your domain password.
2. Click Next.

If the LDAP Password matches with the password on the directory, the LDAP Password authentication is successful.

If the specified domain password is incorrect, an error message **Invalid credentials** is displayed. Specify a valid password and try to authenticate again.

**Password**

The Password method enables you to authenticate using a secret string. The enrolled password is stored locally in the Advanced Authentication. When you try to authenticate on any device, the specified password is compared with the actual password. If the passwords are identical, you are authenticated successfully.

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

1. Specify the password of your Advanced Authentication account.
2. Click Next.

If the password matches with the enrolled password, the Password authentication is successful.

The following table describes the possible error message along with the workarounds for the Password authentication.
PKI

The PKI method enables you to authenticate using any PKI device, such as a contact card and USB token that contains the digital certificate. The PKI reader validates the digital certificate and the identity of users. When you try to authenticate on an application, the certificate in the device is compared with the actual certificate. If the certificates match, you are authenticated successfully.

**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 authenticate using the PKI method, perform the following steps:

1. Insert a card or plug the token to your machine.
2. Specify the PIN.
   
   If the digital certificate in the card or token and enrolled certificate are identical, the PKI authentication is successful.

**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.

The following table describes the possible error message along with the workarounds for the PKI authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong password</td>
<td>The password you have specified is incorrect. Specify a valid password and try to authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for Password</td>
<td>You have not enrolled for Password method. You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>
Table 4-8  PKI authenticator - error messages

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong card</td>
<td>The card that is used is incorrect. Try authenticating with another valid card or token.</td>
</tr>
<tr>
<td></td>
<td>Enroll the authenticator again in Self-Service portal or contact your helpdesk administrator.</td>
</tr>
<tr>
<td>Present card</td>
<td>The PKI device is not connected properly. Try to connect it to a different USB slot and</td>
</tr>
<tr>
<td></td>
<td>authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for PKI</td>
<td>You have not enrolled for PKI method. You must enroll the authenticator in the</td>
</tr>
<tr>
<td></td>
<td>Self-Service portal or contact the helpdesk administrator.</td>
</tr>
<tr>
<td>No template for Card</td>
<td>The card is not enrolled or you are trying to log in with the non-cached authenticator in</td>
</tr>
<tr>
<td></td>
<td>the offline mode.</td>
</tr>
</tbody>
</table>

**NOTE:** To log in to a computer using the PKI authenticator, you must place the card on the reader or connect a token to the computer. After the login, you can remove the card from the reader or disconnect the token to lock the computer automatically.

Advanced Authentication does not support the tapping of a card to lock or unlock a computer.

## RADIUS Client

The RADIUS Client method enables Advanced Authentication to forward the authentication request to a third-party RADIUS server. This can be any RADIUS server.

For example, you can use the RADIUS Client as an authentication method for token solutions such as RSA or Vasco.

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

1. Specify the RADIUS password.
2. Click Next.

If you get an error Wrong answer, it could be an incorrect RADIUS password.

## Security Questions

Security Questions method enables you to enroll answers to a pre-defined set of security questions. When you authenticate using security questions, Advanced Authentication prompts you the configured security questions or a subset of the security questions. You must answer the appropriate questions and based on the correctness of the answers, you are authenticated successfully.

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

1. Specify your answer for the displayed security question.
2 Click Next.
3 Repeat steps 1 to 2 for all the security questions.
   If all the specified answers match with enrolled answers, the Security Questions authentication is successful.

The following table describes the possible error messages along with the workaround for the Security Questions authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong answer</td>
<td>The specified answer is incorrect. Specify the valid answer and try to authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for Security Questions</td>
<td>You have not enrolled for Security Questions method. Enroll the authenticator on the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>

### Smartphone

The Smartphone method facilitates you to enroll and authenticate using the smartphone app. When you initiate the authentication, a push notification is sent to the app. You can accept the request and get authenticated.

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

When you select the Smartphone method from the Chains list, a message **Accept on smartphone or enter the one-time password is displayed on your computer.**

1. Open the Advanced Authentication smartphone app.
2. Tap **Accept**.
   - If the smartphone matches with the enrolled smartphone, the authentication is successful.

To authenticate with the Smartphone method using the offline authentication, perform the following steps:

1. Open the Advanced Authentication smartphone app.
2. Click **Enrolled Authenticators** in the menu of the smartphone app.
3. Specify the OTP from the smartphone app in **Password**.
4. Click **Next**.
   - If the OTP on the smartphone app matches with server generated OTP, the authentication is successful.

The following table describes the possible error messages along with the workaround for the Smartphone authentication.
Table 4-10  Smartphone authenticator - error messages

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth rejected</td>
<td>The authentication request is declined in the smartphone app. Initiate the authentication and accept the request to authenticate again.</td>
</tr>
<tr>
<td>Wrong TOTP password</td>
<td>Specified OTP for the offline authentication is incorrect or the time on your smartphone is not synchronized. Specify the valid OTP and try authenticating again.</td>
</tr>
<tr>
<td>TOTP login is disabled</td>
<td>If the administrator has disabled TOTP login or when the geo-fencing is enabled. Contact your administrator for further assistance.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for smartphone</td>
<td>You have not enrolled for Smartphone method. Enroll the authenticator on the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>

**SMS OTP**

The SMS OTP method facilitates you to generate a single-use password or OTP and send it to the registered mobile number for authentication. You can use this OTP to authenticate within a short time frame.

**NOTE:** The OTP period is set to 120 seconds by default. An administrator has the privilege to change the OTP period.

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

1. Check your phone.
   An SMS message with an OTP is sent to your phone.
2. Specify the OTP in Password.
3. Click Next.
   If the OTP matches with the server generated OTP, the SMS OTP authentication is successful.

The following table describes the possible error messages along with the workaround for the SMS OTP authentication.
Table 4-11  SMS OTP authenticator - error messages

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong answer</td>
<td>The specified OTP is incorrect or is expired.</td>
</tr>
<tr>
<td></td>
<td>Specify a valid OTP within the time frame.</td>
</tr>
<tr>
<td>Cannot send OTP. User does not have a cell phone</td>
<td>Your email address is not set in the profile of the repository.</td>
</tr>
<tr>
<td></td>
<td>Contact your system administrator to add your phone number to the profile.</td>
</tr>
</tbody>
</table>

Swisscom Mobile ID

The Swisscom Mobile ID authentication method uses the phone number from your profile of the repository. The authenticator sends an authentication request to your mobile phone. You need to accept it.

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

1. Check your mobile phone.
   A request message is displayed on your mobile phone.
2. Accept the request.
   If the Mobile ID matches with the enrolled Mobile ID, the Swisscom Mobile ID authentication is successful.

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

TOTP

The TOTP method enables you to authenticate using the time-based-one-time password. TOTP is generated on the hardware token or the mobile app, such as NetIQ Advanced Authentication app or Google Authenticator app. The TOTP is valid for a short duration. This method uses a predefined period. The default value is 30 seconds.

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

1. Specify the TOTP from your hardware or software token.
2. Click Next.
   If the OTP on the token matches with the server generated OTP, the TOTP authentication is successful.

The following table describes the possible error message along with the workaround for the TOTP authentication.
The FIDO U2F facilitates method enables you connect the FIDO U2F compliant token to the computer or laptop and touch the flashing token to authenticate. When you try to authenticate on any device, token connected to the device is compared with the actual device. If the device details match, you are authenticated successfully.

**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 using the FIDO U2F method, perform the following steps:**

1. Ensure that the FIDO U2F token is connected to the workstation.
   
   A message **Please touch the flashing U2F device now** is displayed.

2. Touch the button on the token when you see a blink.
   
   If the token and attestation certificate in the token matches with the enrolled U2F token, the FIDO U2F authentication is successful.
   
   If the device does not blink, wait for few seconds. If you do not see the blink for more than a minute, try to reconnect your token and repeat the steps.

**NOTE:** Administrator can configure an automatic session lock or log off on the U2F events. When a user returns to the workstation, the user must connect the U2F device to the workstation to unlock.

The following table describes the possible error messages along with the workaround for the FIDO U2F authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incorrect OTP password</td>
<td>The OTP you have provided is incorrect or the server time is not in sync. Specify a valid OTP and try to authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for TOTP</td>
<td>You have not enrolled for TOTP method. You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>
Table 4-13  FIDO U2F authenticator - error messages

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong token. Try another one</td>
<td>The token that you have connected is incorrect. Try to authenticate with another token or re-enroll the authenticator in Self-Service portal or contact your helpdesk administrator.</td>
</tr>
<tr>
<td>Connect a token</td>
<td>The token is not connected properly. Try to connect it to a different USB slot and authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for U2F</td>
<td>You have not enrolled for U2F method. You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>

Voice

The Voice authenticator initiates a call to your registered phone number. The phone call requests you to specify the PIN for authentication. When you try to authenticate on an application, the recorded PIN is compared with the actual PIN. If both the PINs match, you are successfully authenticated.

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

1. Answer the phone call on your phone and listen to the request.
2. Specify your PIN code followed by the hash symbol (#) in the dial pad of your mobile phone.
   If the PIN matches with enrolled PIN, the Voice authentication is successful.

Voice OTP

The Voice OTP authenticator initiates a phone call to your registered phone number. You will receive the voice OTP in the phone call. You can use this OTP for authentication within a short time frame.

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

1. Answer the phone call on your phone and listen to the voice OTP.
2. Specify the OTP in Password.
3. Click Next.
   If the OTP matches with the server generated OTP, the Voice OTP authentication is successful.

Windows Hello

The Windows Hello method facilitates you to use your Windows Hello fingerprint and facial recognition authentication to log in to the Windows 10 operating system. Advanced Authentication supports the Windows Hello fingerprint and facial recognition.
To authenticate using the Windows Hello, perform the following steps:

1 **For fingerprint authentication**: Ensure that a fingerprint reader is connected to the required device.
   1a Place your enrolled finger on the reader when using a touch sensor or swipe your finger when using a swipe sensor.
   If the fingerprint matches with the fingerprint enrolled on Windows 10 operating system, Windows Hello authentication is successful.

2 **For facial recognition**: Ensure that an external camera is connected to your computer.

   NOTE: This method supports all the devices that Windows Hello works with. For example, the Windows Hello facial recognition works with only the infrared cameras. Therefore, the Advanced Authentication Windows Hello method also supports only the infrared camera for facial recognition.

   2a Present your face to the camera.
   If the face matches with the facial image enrolled on Windows 10 operating system, Windows Hello authentication is successful.
Logging In to Linux

You can use the enrolled authenticators to log in to the Linux operating system. You must pass through the authenticators in the chain to get authenticated.

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

1. Specify the username in the format: `repositoryname\username` (e.g. company\pjones) and click Next.
2. Specify the number of the chain to select preferred authentication chain.
3. Authenticate with the preferred authentication method(s) of the chain.
   A prompt to select category might appear, if you have enrolled an authenticator for more than one category.

**NOTE:** In case of a password change you are prompted to specify a (Current) NT password. In this case, you must specify your old domain password.

**NOTE:** If you log in to a non-domain joined workstation for the first time, you are prompted 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.

Logging In As a Local User

A local user on the Linux Client can use his password to log in even if there are bound domain users in a non-domain mode. However, if a bound domain user is still logged in, then the local user can use the authentication chains of a bound user instead of his own password.

The following two examples provide information about how a local user can log in using his own password or chains.

**Example1:** When a linux local user uses his own password with a pre-condition that the domain user is bound to a local user, and the local user performs the following:

1. Goto the login page of the linux machine.
2. Click Not listed?.
3. Specify the username of a domain user from the precondition.
4. Select a chain and submit the correct value of the chain and log in.
5. Log out.
6. Click the icon of the local user from preconditions or click Not listed?.
7. Specify the username of the local user from preconditions.

**Result:** Password of the local user is used for login.
Example 2: When Linux local user uses the chains of a bound user with a pre-condition that the domain user is bound to a local user, and the local user perform the following:

1. Goto the login page of the Linux machine.
2. Click Not listed?.
3. Specify the username of a domain user from the precondition.
4. Select a chain and submit the correct value of the chain and log in.
5. Lock the screen.
6. Press any key and click Not listed?.
7. Click the icon of the local user from preconditions or click Not listed?.
8. Specify the username of the local user from preconditions.

Result: Chains of the bound domain user are used for login.

Authenticators for Linux Client

Advanced Authentication provides the following authenticators for logging in to Linux Client:

- “Authentication Agent” on page 129
- “Bluetooth” on page 130
- “Card” on page 130
- “Device Authentication” on page 131
- “Email OTP” on page 132
- “Emergency Password” on page 132
- “Facial Recognition” on page 133
- “Flex OTP” on page 134
- “Fingerprint” on page 134
- “HANIS Face” on page 135
- “HOTP” on page 135
- “LDAP Password” on page 136
- “Out-of-Band” on page 136
- “Password” on page 137
- “PKI” on page 137
- “RADIUS Client” on page 138
- “Security Questions” on page 138
- “Smartphone” on page 139
- “SMS OTP” on page 140
- “TOTP” on page 140
- “FIDO U2F” on page 141
- “Voice” on page 142
- “Voice OTP” on page 143
NOTE: On SUSE Linux Enterprise, do not specify anything until a message **Please wait** is displayed, else you will not be able to unlock the operating system.

 NOTE: When you log in to SLES 12 Service Pack 3 as a domain user and pass all the authentication methods in the chain, if you are prompted with an error message **Sorry that didn't work** then see Domain Users Are Unable to Log In Even After Authenticating All the Methods In a Chain to resolve the issue and login to the machine successfully.

NOTE: Sometimes in Ubuntu 18.04 LTS, a current logged in user is unable to login as another user with Log in as another user option in the locked screen or after performing the following steps:

1. Click System Menu on the upper-right corner.
2. Click user name > Switch User.

This issue occurs even when the Linux PAM Client is not installed on Ubuntu 18.04.

**Authentication Agent**

Authentication Agent enables you to perform multi-factor authentication on one computer to get authorized access to another computer, where it is not possible to display the user interface or connect any external authentication devices. You can install the Authentication Agent on Windows system. When an authentication is initiated from a computer using the Authentication Agent chain, the Authentication Agent on another computer prompts a restricted browser where you must perform the authentication.

NOTE: You can install the Authentication Agent only on Windows workstation.

**IMPORTANT:** If both the Windows Client and Authentication Agent are installed on the same workstation, the Authentication Agent is logged in automatically through the SSO feature. If the Windows Client is not installed, you must log in to the Authentication Agent manually.

To log in to Linux using the Authentication Agent on Windows, perform the following steps:

1. Specify **User name** in the Linux computer.
2. Click **Next** and specify the chain number corresponding to the Authentication Agent in the list.

   For more information about enabling the Authentication Agent chain in the Linux computer, see Enabling the Authentication Agent Chain.

3. The Authentication Agent that is active on a Windows computer launches a restricted browser.

   **IMPORTANT:** If a restricted browser is not launched automatically, place the cursor on the Authentication Agent icon in System tray and ensure that the agent is logged in. If the agent is not logged in, double click the Authentication Agent icon to log in.

   The restricted browser prompts the login page. The user name that you have specified in the Linux computer is set in the login page by default.

4. Click **Next**.
5 Select and authenticate the preferred chain to log in to Linux computer in the restricted browser.

For more information, see Logging In to Authentication Agent for Windows.

6 After the successful authentication in the restricted browser, you are logged in to the Linux computer automatically.

**Bluetooth**

The Bluetooth method enables you to authenticate using any Bluetooth enabled device that is within the range. When you initiate authentication, the Advanced Authentication server searches for the enrolled Bluetooth device. If the enrolled device is within the range, you are authenticated successfully.

For example, Susanne, who is a doctor, attends many in-patients in the hospital. She accesses the computer located in each room to monitor and update the health status of the patient. In this case, Susanne can specify her first-factor authentication details and use her Bluetooth enabled mobile phone to log in to the computer automatically when she is within range of a particular room.

**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 using the Bluetooth method, perform the following steps:**

1. Ensure that Bluetooth is turned on in your device and is discoverable to the paired devices.
2. The Device Service detects your Bluetooth device and authenticates.

   If the paired Bluetooth device is within the range, the Bluetooth authentication is successful.

**Card**

The Card method enables you to authenticate using the contactless smart card (with the card serial number) and Near-Field Communication (NFC) cards in the following ways:

- While using contactless cards, when you try to authenticate on any device, the recorded serial number of the card is compared with the actual serial number. If the card serial numbers are identical, you are authenticated successfully.
- In the case of NFC cards, when you place your NFC tag near the NFC reader (smartphone), the NFC reader (smartphone) identifies your NFC tag, and you are authenticated successfully.

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

**To authenticate using the contactless card, perform the following steps:**

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

   A message *Waiting for card* is displayed.
2 Tap your card on the reader.

If the Card Serial Number in the card matches with enrolled card, the card authentication is successful.

The following table describes the possible error messages along with the workaround for the Card authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong card</td>
<td>The card you have placed on the reader is incorrect. Try again with another card or re-enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
<tr>
<td>Connect reader</td>
<td>The reader is not connected properly. Try to connect it to a different USB slot and authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for Card</td>
<td>You have not enrolled the card method. You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>

**Using Card Method on Ubuntu LightDM**

**NOTE:** When you specify the chain number corresponding to the Card method and try to authenticate to Ubuntu LightDM, the hints are not prompted. Tap your card on the reader to continue authentication.

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

2 Tap your card on the reader.

   A message Waiting for card is displayed.

   If the Card Serial Number in the card matches with enrolled card, the card authentication is successful.

**Device Authentication**

The Device Authentication method enables you to authenticate using a unique key pair stored in the workstation and PIN. During the enrollment process, a key pair is generated in the workstation and the same is used for further authentication. Device Authentication supports authentication to the Linux workstation and verifies the key pair to authenticate users.

**To authenticate with the Device Authentication method, perform the following steps:**

1 Specify the PIN.

2 Click Next.

   If the PIN matches with the enrolled PIN, the Device authentication is successful.
Email OTP

The Email OTP method enables you to authenticate using the one-time password (OTP) that is sent to the registered email address. When you try to authenticate on any device, the server sends an email to the registered email address with the OTP. You can use this OTP for single authentication within a short time frame.

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

1. Check your email. You must receive an email with OTP.
2. Specify the OTP from Email in Password.
3. Click Next.

If the OTP matches with the server generated OTP, the Email OTP authentication is successful.

The following table describes the possible error messages along with the workarounds for the Email OTP authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong answer</td>
<td>The specified OTP is incorrect or is expired. Specify a valid OTP within the time frame.</td>
</tr>
<tr>
<td>Cannot send OTP. User does not have an email</td>
<td>Your email address is not set in the profile of the repository. Contact your system administrator to add your email address to the profile.</td>
</tr>
</tbody>
</table>

Emergency Password

The Emergency Password method enables you to authenticate using a temporary password with the help of helpdesk administrator if you have lost a smart card or forgot your smart phone. The emergency password is valid for certain days and is set to 3 days by default. When you try to authenticate on any device, the submitted emergency password is compared with the enrolled password in the appliance. If the emergency passwords are identical, you are authenticated successfully.

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

1. Specify the Emergency Password.
2. Click Next.

If the Emergency Password matches with the enrolled password, the Emergency Password authentication is successful.

The following table describes the possible error messages along with the workaround for the Emergency Password authentication.
Facial Recognition

The Facial Recognition method enables you to get automatically authenticated by presenting your face. You need to register your facial image using the web camera. When you try to authenticate on an application, the recorded image is compared with the actual image. If the images match, you are successfully authenticated.

The Facial Recognition method works with both integrated and external web cameras.

NOTE: To use the Facial Recognition method for authentication, you must install the Advanced Authentication Device Service. For more information about the Device Service, see the “Advanced Authentication - Device Service” guide.

To authenticate by using the Facial Recognition method, perform the following steps:

1. Ensure that a camera is connected to your device.
2. Present your face to the camera.
   
   If your face matches with the enrolled face, the face authentication is successful.

The following table describes the possible error messages along with the workaround for the Facial Recognition authentication.

**Table 5-4 Facial Recognition - error messages**

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed to open camera</td>
<td>The camera is not connected properly. Check your camera settings and try again.</td>
</tr>
<tr>
<td>Mismatch</td>
<td>The enrolled face and presented face does not match. You must present your face again for the authentication.</td>
</tr>
<tr>
<td>Face service is not available</td>
<td>The Device Service is not installed. Ensure that the Device Service is installed.</td>
</tr>
</tbody>
</table>
Using Facial Recognition Method on Ubuntu LightDM

**NOTE:** When you specify the chain number corresponding to the Facial Recognition method and try to authenticate to Ubuntu LightDM, the hints are not prompted. Present your face to the camera to continue authentication.

1. Ensure that a camera is connected to your device.
2. Present your face to the camera.
   
   A message Detecting a face is displayed.
   
   If your face matches with the enrolled face, the face authentication is successful.

**Flex OTP**

The Flex OTP authenticator facilitates you to authenticate by using your otp password from any of HOTP, TOTP and Smartphone (Offline) authenticator. When you try to authenticate to any device, the OTP in the token is compared with the OTP generated in any of HOTP, TOTP and Smartphone (Offline) authenticators. If the OTPs are valid, you are authenticated successfully.

**To authenticate using the Flex OTP method, perform the following steps:**

1. Specify the One-Time Password from any of HOTP, TOTP and Smartphone (Offline) authenticators
2. If the password is valid, the Flex OTP authentication is successful.

**Fingerprint**

The Fingerprint method enables you authenticate using your finger print. The fingerprint scanner captures the fingerprint. When you try to authenticate on an application, the recorded fingerprint(s) are compared with the actual fingerprint. If the fingerprints match, you are authenticated successfully.

**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 enrolled finger on the reader when using a touch sensor or swipe your finger when using a swipe sensor.
   
   If the fingerprint matches with the enrolled fingerprint, the authentication is successful.
**HANIS Face**

The HANIS (Home Affairs National Identification System) Face method is for the citizens of South Africa to authenticate with their personal identification number or passport number issued by Home Affairs National Identification System and face biometric. When you try to authenticate on any device, the presented face is matched with the enrolled face. If the images match, you are authenticated successfully.

Face is captured using both integrated and external web cameras.

**NOTE:** To use the Facial Recognition method for authentication, you must install the Advanced Authentication Device Service. For more information about the Device Service, see the [Advanced Authentication - Device Service guide](#).

To authenticate by using the HANIS Face method, perform the following steps:

1. Ensure that a camera is connected to your device.
2. Select the chain with HANIS Face method for authentication.
3. Present your face to the camera.
   
   A message *Detecting a face* is displayed.

   If your face matches with the enrolled face, the HANIS Face authentication is successful.

The following table describes the possible error messages along with the workaround for the HANIS Face authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capture Device cannot be opened</td>
<td>The camera is not connected properly. Check your camera settings and try again.</td>
</tr>
<tr>
<td>Timeout</td>
<td>The session has timed out. You must present your face again for the authentication.</td>
</tr>
</tbody>
</table>

**HOTP**

HOTP is a counter-based one-time password. This method enables you to authenticate using the counter-based one-time password generated on the HOTP token. The counter on the token must be in sync with the server. You can use generic HOTP tokens that adhere to RFC 4226. You can use the static secret key and three consequent OTP generated from the token to enroll. When you try to authenticate on any device, the OTP in the token is compared with the OTP generated in the server. If both the OTPs are identical, you are authenticated successfully.

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

1. Specify the HOTP when using software token or connect the USB token, press button on the token.
2 Click Next.

If the OTP on the token matches with the server generated OTP, the HOTP authentication is successful.

The following table describes the possible errors along with the workaround for the HOTP authentication.

### Table 5-6 HOTP - error messages

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong answer</td>
<td>The OTP you have provided is incorrect or the OTP on the token and server are out of sync.</td>
</tr>
<tr>
<td></td>
<td>Specify a valid OTP and try to authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for HOTP</td>
<td>You have not enrolled for HOTP method.</td>
</tr>
<tr>
<td></td>
<td>You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>

### LDAP Password

The LDAP password method enables you to authenticate using the password of your corporate account. When you try to authenticate on an application, the submitted password is compared with the actual password in the corporate directory. If both passwords are same, you are authenticated successfully.

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

1. Specify your domain password.
2. Click Next.

   If the LDAP Password matches with the password on the directory, the LDAP Password authentication is successful.

If the specified domain password is incorrect an error message Invalid credentials is displayed. Specify a valid password and try to authenticate again.

### Out-of-Band

The Out-of-band method facilitates you to authenticate using the push notification that is sent to the Out-of-band portal or OOB agent. When you initiate the authentication, a push notification is sent to the portal or agent. You can accept the request and get authenticated.

**To authenticate by using the Out-of-band method, perform the following steps:**

When you specify the chain number corresponding to the Out-of-band method, a message Continue at https://<AdvancedAuthenticationServerdomainname>/oob/ui is displayed on your computer.

1. Open the OOB agent installed on your mobile or navigate to the OOB portal.
   A push notification is displayed.
NOTE: If the push notification does not appear after 5 seconds, tap the Refresh icon to view the push notification for the initiated authentication.

2 Tap Accept.

If the response to authentication request is from a secured origin, the authentication is successful.

**Password**

The Password method enables you to authenticate using a secret string. The enrolled password is stored locally in the Advanced Authentication. When you try to authenticate on any device, the specified password is compared with the actual password. If the passwords are identical, you are authenticated successfully.

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

1 Specify the password for your Advanced Authentication account.
2 Click Next.

If the password matches with the enrolled password, the Password authentication is successful.

The following table describes the possible error messages along with the workaround for the Password authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong password</td>
<td>The password you have provided is incorrect. Specify a valid password and try to authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for Password</td>
<td>You have not enrolled for Password method. You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>

**PKI**

The PKI method enables you authenticate using any PKI device, such as a contact card and USB token that contains the digital certificate. The PKI reader validates the digital certificate and the identity of users. When you try to authenticate on any device, the certificate in the device is compared with the actual certificate. If the certificates match, you are authenticated successfully.

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

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

1 Insert the card in the reader or connect token to your machine.
2 Specify the PIN.

If the digital certificate in the card or token and enrolled certificate are identical, the PKI authentication is successful.
The following table describes the possible error messages along with the workaround for the PKI authentication.

**Table 5-8**  PKI authenticator - error messages

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong card</td>
<td>The card that is used is incorrect. Try authenticating with another valid card or token. You can enroll the authenticator again in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
<tr>
<td>Present card</td>
<td>The PKI device is not connected properly. Try to connect it to a different USB slot and authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for PKI</td>
<td>You have not enrolled for PKI method. You must enroll the authenticator in the Self-Service portal or contact the helpdesk administrator.</td>
</tr>
</tbody>
</table>

**RADIUS Client**

The RADIUS Client method enables Advanced Authentication to forward the authentication request to a third-party RADIUS server. This can be any RADIUS server.

For example, you can use the RADIUS Client as an authentication method for token solutions such as RSA or Vasco.

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

1. Specify the RADIUS password.
2. Click Next.

If you get an error Wrong answer, it could be an incorrect RADIUS password.

**Security Questions**

Security Questions method enables you to enroll answers to a pre-defined set of security questions. When you authenticate using security questions, Advanced Authentication prompts you the configured security questions or a subset of the security questions. You must answer the appropriate questions and based on the correctness of the answers, you are authenticated successfully.

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

1. Specify the answer for the security question.
2. Click Next.
3. Repeat steps 1 to 2 for all the required security questions.

The following table describes the possible error messages along with the workaround for the Security Questions authentication.
Table 5-9  Security Questions authenticator - error messages

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong answer</td>
<td>The answer that you have provided is incorrect. Specify the correct answer and try to authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for TOTP</td>
<td>You have not enrolled the Security Questions method. You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>

Smartphone

The Smartphone method facilitates you to enroll and authenticate using the smartphone app. When you initiate the authentication, a push notification is sent to the app. You can accept the request and get authenticated.

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

When you specify the chain number corresponding to the Smartphone method, a message Accept on smartphone or enter the one-time password is displayed on your computer.

1. Open the Advanced Authentication smartphone app.
   A push notification is displayed to your smartphone.
2. Tap Accept.
   If the smartphone matches with the enrolled smartphone, the authentication is successful.

To authenticate with the Smartphone method using the offline authentication, perform the following steps:

1. Open the Advanced Authentication smartphone app.
2. Click Enrolled Authenticators from Menu in the smartphone app.
3. Specify the OTP from the smartphone app in Password.
4. Click Next.
   If the OTP on the smartphone app matches with server generated OTP, the authentication is successful.

The following table describes the possible error messages along with the workaround for the Smartphone authentication.

Table 5-10  Smartphone authenticator - error messages

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth rejected</td>
<td>You have declined the authentication request.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for TOTP</td>
<td>You have not enrolled for the Smartphone method. You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>
**SMS OTP**

The SMS OTP method facilitates you to generate a single-use password or OTP and send it to the registered mobile number for authentication. You can use this OTP to authenticate within a short time frame.

**NOTE:** The OTP period is set to 120 seconds by default. An administrator has the privilege to change the OTP period.

**To perform authentication using the SMS OTP method, perform the following steps:**

1. You will receive an SMS message with an OTP on your phone.
2. Specify the OTP from the SMS.
3. Click **Next**.

The following table describes the possible error messages along with the workaround for the SMS OTP authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cannot send OTP. User does not have a cell phone</td>
<td>Your phone number is not registered in the repository. Contact your system administrator to add your mobile phone number to the account properties.</td>
</tr>
<tr>
<td>Login failed</td>
<td>Either the OTP that you have specified is incorrect or you have specified the expired OTP. Try to authenticate again.</td>
</tr>
</tbody>
</table>

**TOTP**

The TOTP method enables you to authenticate using the time-based-one-time password. TOTP is generated on the hardware token or the mobile app, such as NetIQ Advanced Authentication app or Google Authenticator app. The TOTP is valid for a short duration. This method uses a predefined period. The default value is 30 seconds.

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

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

   If the OTP on the token matches with the server generated OTP, the TOTP authentication is successful.

The following table describes the possible error messages along with the workaround for the TOTP authentication.
Table 5-12  TOTP authenticator - error messages

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong answer</td>
<td>The OTP you have provided is incorrect. Specify a valid OTP and try to authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for TOTP</td>
<td>You have not enrolled for TOTP method. You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>

FIDO U2F

The FIDO U2F authentication method facilitates you to connect the FIDO U2F compliant token to the computer or laptop and touch the flashing token to authenticate. When you try to authenticate on any device, token connected to the device is compared with the actual device. If the device details match, you are authenticated successfully.

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

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

1. Ensure that the FIDO U2F token is connected to your computer.
   
   A message Please connect a U2F token. Please touch the flashing U2F device now is displayed.

2. Touch the button on the token when there is a flash.
   
   If the token and attestation certificate in the token matches with the enrolled U2F token, the FIDO U2F authentication is successful.
   
   If there is no flash, wait for few seconds. If there is no flash for more than a minute then try to reconnect your token and repeat the steps.

The following table describes the possible error messages along with the workaround for the FIDO U2F authentication.

Table 5-13  FIDO U2F authenticator - error messages

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong token. Try another one</td>
<td>The token that you have connected is incorrect. Try to authenticate with another token or re-enroll the authenticator in Self-Service portal or contact your helpdesk administrator.</td>
</tr>
<tr>
<td>Connect a token</td>
<td>The token is not connected properly. Try to connect it to a different USB slot and authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for U2F</td>
<td>You have not enrolled for U2F method. You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>
NOTE: To use U2F on Google Chrome, you must perform the following steps:

   If the file is already available, ensure that the content is similar to that specified in https://github.com/Yubico/libu2f-host/blob/master/70-u2f.rules.
   
   NOTE: If your version of UDEV is lower than 188, use the rules specified at https://github.com/Yubico/libu2f-host/blob/master/70-old-u2f.rules.

2. Save the `70-u2f.rules` file and reboot the system.

Using FIDO U2F on Ubuntu LightDM

NOTE: When you specify the chain number corresponding to the FIDO U2F method and try to authenticate to Ubuntu LightDM, the hints are not prompted. Connect the U2F token to the computer and touch the button when there is a flash on the token.

1. Ensure that the FIDO U2F token is connected to your computer.

2. Touch the button on the token when there is a flash.
   
   A message Please connect a U2F token. Please touch the flashing U2F device now is displayed.
   
   If the token and attestation certificate in the token matches with the enrolled U2F token, the FIDO U2F authentication is successful.

Voice

The Voice method initiates a call to your registered phone number. The phone call requests you to specify the PIN in the dial pad of your mobile to authenticate. When you try to authenticate on any device, the recorded PIN is compared with the actual PIN. If both PINs are identical, you are authenticated successfully.

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

When you specify the chain number corresponding to the Voice method, a message Wait a phone call is displayed on your computer.

1. Check your mobile phone.
   
   You will receive a phone call.

2. Answer the phone call, listen to the request on the phone.

3. Specify your PIN code followed by the hash symbol (#) in the dial pad of your mobile phone.
   
   If the PIN matches with enrolled PIN, the Voice authentication is successful.
Using Voice Method on Ubuntu LightDM

**NOTE:** When you specify the chain number corresponding to the Voice method and try to authenticate to Ubuntu LightDM, the hints are not prompted. Receive the phone call and specify your PIN followed by hash symbol in the dial pad to continue authentication.

1. Check your mobile phone.
   You will receive a phone call.
2. Answer the phone call, listen to the request on the phone.
3. Specify your PIN code followed by the hash symbol (#) in the dial pad of your mobile phone.
   A message *Wait a phone call* is displayed on your computer.
   If the PIN matches with enrolled PIN, the Voice authentication is successful.

**Voice OTP**

The Voice OTP method enables you to authenticate using the OTP that is sent through the phone call to your registered phone number. You can use this OTP for authentication within a short time frame. When you try to authenticate on any device, the specified OTP is compared with the OTP generated on the server. If both the OTPs are identical, you are authenticated successfully.

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

When you specify the chain number corresponding to the Voice OTP method, a message *Wait a phone call* is displayed on your computer.

1. Check your mobile phone.
   You will receive a phone call.
2. Answer the call on your phone and listen to the voice OTP.
3. Specify the OTP in *Password*.
4. Click *Next*.
   If the OTP matches with the server generated OTP, the Voice OTP authentication is successful.
Unlocking Linux

The Linux operating system gets locked, when the session remains inactive more than the set value (time in minutes) or when you lock manually using the Lock option. You can unlock Linux on the following platforms:

- Unlocking Linux on Cent OS 7 KDE
- Unlocking Linux on SUSE 11

Unlocking Linux on Cent OS 7 KDE

Following are the scenarios on Cent OS 7 with KDE environment, when you want to unlock Linux operating system:

**Scenario 1: Multiple Chains**

As a domain user, when you are locked on Cent OS 7 (KDE) and there are multiple chains, PAM selects the first chain based on the following criteria:

*Table 6-1  Multiple Chains - Criteria and required action*

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criterion 1:</strong> The chain consists of one of the following methods as the first method:</td>
<td>PAM selects the chain that meets the condition listed in criterion 1 and you must perform the following steps:</td>
</tr>
<tr>
<td>• Password</td>
<td>1. Specify the password.</td>
</tr>
<tr>
<td>• LDAP Password</td>
<td>2. Click Unlock.</td>
</tr>
<tr>
<td>• TOTP</td>
<td>3. Specify valid data for other methods to pass the chain.</td>
</tr>
<tr>
<td>• HOTP</td>
<td></td>
</tr>
<tr>
<td>Criteria</td>
<td>Action</td>
</tr>
<tr>
<td>----------</td>
<td>--------</td>
</tr>
</tbody>
</table>
| **Criterion 2:** There are two chains that contain one of the following methods as the first method:  
  - Password  
  - LDAP Password  
  - TOTP  
  - HOTP | PAM selects the top chain of the used list that meets the condition listed in criterion 2. You must perform the following steps:  
  1. Specify the password.  
  2. Click Unlock.  
  3. Specify valid data for other methods to pass the chain. For example: Assume that there are two chains as follows:  
    - **Chain 1:** This chain consists of methods: TOTP, FIDO U2F and Voice OTP.  
    - **Chain 2:** This chain consists of methods: Password, Card and SMS OTP. PAM selects Chain 1 that is on top of the used list and meets the condition. |
| **Criterion 3:** The chain consists of any Advanced Authentication methods (except Password, LDAP, HOTP, and TOTP methods) as the first method. | PAM selects the top chain of the used list, you must follow the chain and specify valid data to pass the chain. For example: Assume that there are two chains as follows:  
    - **Chain 1:** This chain consists of methods: Card, Email OTP, and FIDO U2F.  
    - **Chain 2:** This chain consists methods: Fingerprint, PKI and SMS OTP. PAM selects Chain 1 that is on top of the used list, you must perform the following to pass authentication:  
      1. Click Unlock without specifying the password.  
      2. Tap valid card on the reader.  
      3. Specify OTP received from email.  
      4. Tap finger on the FIDO U2F device. |

**NOTE:** In the authentication chain, irrespective of the position of Email OTP, SMS OTP, or Voice OTP method, if you specify invalid OTP, the authentication cannot be continued or initiated again. You can perform one of the following to continue or initiate the authentication:  
  - Specify a valid OTP.  
  - Wait till the login session expires.
**NOTE:** If you select the authentication chain that contains Password, LDAP Password, TOTP, or HOTP as the second method (for example, Smartphone+Password, Card+TOTP, or U2F+HOTP), then ensure to specify the Password, LDAP Password, TOTP, or HOTP in Password. Later, accept authentication request on smartphone, swipe the card or touch the U2F token.

**Scenario 2: First or Single Method in Chain**

Below table describes the behavior of the chain that consists of each method, when the method is first or single in an authentication chain:

<table>
<thead>
<tr>
<th>Method</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP password</td>
<td>You must perform the following steps:</td>
</tr>
<tr>
<td></td>
<td>1. Specify the LDAP password.</td>
</tr>
<tr>
<td></td>
<td>2. Click Unlock.</td>
</tr>
<tr>
<td>Password</td>
<td>1. Specify the password.</td>
</tr>
<tr>
<td></td>
<td>2. Click Unlock.</td>
</tr>
<tr>
<td>HOTP</td>
<td>1. Specify the HOTP.</td>
</tr>
<tr>
<td></td>
<td>2. Click Unlock.</td>
</tr>
<tr>
<td>TOTP</td>
<td>1. Specify the TOTP.</td>
</tr>
<tr>
<td></td>
<td>2. Click Unlock.</td>
</tr>
<tr>
<td>RADIUS</td>
<td>1. Specify the RADIUS password.</td>
</tr>
<tr>
<td></td>
<td>2. Click Unlock.</td>
</tr>
<tr>
<td>SMS OTP</td>
<td>1. Click Unlock.</td>
</tr>
<tr>
<td></td>
<td>2. Specify the SMS OTP.</td>
</tr>
<tr>
<td>Email OTP</td>
<td>1. Click Unlock.</td>
</tr>
<tr>
<td></td>
<td>2. Specify the Email OTP.</td>
</tr>
<tr>
<td>Voice OTP</td>
<td>1. Click Unlock.</td>
</tr>
<tr>
<td></td>
<td>2. Specify the Voice OTP.</td>
</tr>
<tr>
<td></td>
<td>2. Click Unlock.</td>
</tr>
<tr>
<td>Voice</td>
<td>1. Click Unlock to initiate phone call.</td>
</tr>
<tr>
<td></td>
<td>2. Specify the PIN.</td>
</tr>
<tr>
<td>Security questions</td>
<td>With Security questions as a first or single method in the chain, you cannot unlock operating system.</td>
</tr>
</tbody>
</table>
Unlocking Linux on SUSE 11

Following are the scenarios on SUSE 11, to unlock Linux operating system:

- **Scenario 1: Multiple Chains**
- **Scenario 2: Single Chain**

**Scenario 1: Multiple Chains**

As a domain user, when you are locked on SUSE 11 and there are multiple authentication chains, PAM selects the first chain based on the following criteria:

### Table 6-3 Criteria and required action

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criterion 1:</strong> The chain consists of a single method and the method is one of the following:</td>
<td>If PAM selects the chain with a single method as first chain, you must perform the following steps to unlock the account:</td>
</tr>
<tr>
<td>- Password</td>
<td>1. Specify the password.</td>
</tr>
<tr>
<td>- LDAP Password</td>
<td>2. Click Unlock.</td>
</tr>
<tr>
<td>- TOTP</td>
<td></td>
</tr>
<tr>
<td>- HOTP</td>
<td></td>
</tr>
</tbody>
</table>

### Smartphone

1. Click Unlock to initiate an authentication request.
2. Open the Advanced Authentication smartphone app and tap Accept.

**NOTE:** When there is no mobile data on your smartphone, you cannot unlock operating system with smartphone OTP. If you tap Reject, login fails.

### FIDO U2F

1. Click Unlock.
2. Touch U2F device when you see a flash.

**NOTE:** If you touch incorrect U2F device that is not enrolled, a new authentication session appears.

### Card

1. Click Unlock.
2. Tap card on the reader.

**NOTE:** If you tap an invalid card, a new login session appears.

### Bluetooth

With Bluetooth as a first or single method in the chain, you cannot unlock operating system.

### PKI

With PKI as a first or single method in the chain, you cannot unlock operating system.
Scenario 2: Single Chain

When a domain user is locked on SUSE 11 and there is a single chain, PAM selects this single chain for authentication. The chain can consist of one or more of the following methods:

Table 6-4 Criteria and required action

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criterion 1</strong>: The chain consists of a single method and the method is one of the following:</td>
<td>If the chain consists of a single method, user must perform the following:</td>
</tr>
<tr>
<td>- Password</td>
<td>1. Specify the password.</td>
</tr>
<tr>
<td>- LDAP Password</td>
<td>2. Click Unlock.</td>
</tr>
<tr>
<td>- TOTP</td>
<td></td>
</tr>
<tr>
<td>- HOTP</td>
<td></td>
</tr>
</tbody>
</table>

**Scenario 2: Single Chain**

When a domain user is locked on SUSE 11 and there is a single chain, PAM selects this single chain for authentication. The chain can consist of one or more of the following methods:

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criterion 2</strong>: The chain consists of the following two methods (irrespective of the order of the methods):</td>
<td>If PAM selects the chain with two methods as first chain, you perform the following steps to unlock the account:</td>
</tr>
<tr>
<td>- Password, LDAP Password, TOTP or HOTP</td>
<td>1. Specify the password.</td>
</tr>
<tr>
<td>- Out-of-band (Smartphone or Voice Call)</td>
<td>2. Accept Out-of-band method (For example: Push message on the smartphone).</td>
</tr>
</tbody>
</table>

**NOTE**: When the smartphone does not have network connection, user cannot unlock the operating system with chain that consists of Smartphone method. Therefore, click Switch User and try to log in using preferred authentication chain.

**Criterion 3**: The chain consists of more than two methods that are any of the Advanced Authentication methods.

Click Switch User and try to log in again using the same authentication chain.

**Criterion 4**: The chain consists of following methods (except Password, LDAP, HOTP, TOTP, Smartphone, and Voice Call methods):

- Card
- Email OTP
- FIDO U2F
- Fingerprint
- PKI
- SMS OTP
- Swiss Mobile ID
- Voice OTP

Click Switch User and try to log in again using the same authentication chain.

If you specify any text in the password, a error message Unable to authenticate user is displayed.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criterion 1</strong>: The chain consists of a single method and the method is one of the following:</td>
<td>If the chain consists of a single method, user must perform the following:</td>
</tr>
<tr>
<td>- Password</td>
<td>1. Specify the password.</td>
</tr>
<tr>
<td>- LDAP Password</td>
<td>2. Click Unlock.</td>
</tr>
<tr>
<td>- TOTP</td>
<td></td>
</tr>
<tr>
<td>- HOTP</td>
<td></td>
</tr>
<tr>
<td>Criteria</td>
<td>Action</td>
</tr>
<tr>
<td>----------</td>
<td>--------</td>
</tr>
<tr>
<td><strong>Criterion 2:</strong> The chain consists of the following two methods (irrespective of the order of the methods):</td>
<td>With two methods in the chain, PAM prompts the user to perform the following:</td>
</tr>
<tr>
<td>✷ Password, LDAP Password, TOTP or HOTP.</td>
<td>1. Specify the password.</td>
</tr>
<tr>
<td><strong>NOTE:</strong> When the smartphone does not have network connection, user cannot unlock the operating system with chain that consists of Smartphone method. Therefore, user must click <strong>Switch User</strong> and try to log in using preferred authentication chain.</td>
<td></td>
</tr>
<tr>
<td><strong>Criterion 3:</strong> The chain consists of more than two methods that are any of the Advanced Authentication methods.</td>
<td>The user must click <strong>Switch User</strong> and try to log in again using the same authentication chain.</td>
</tr>
<tr>
<td><strong>Criterion 4:</strong> The chain consists of following methods (except Password, LDAP, HOTP, TOTP, Smartphone, and Voice Call methods):</td>
<td>The user must click <strong>Switch User</strong> and try to log in again using the same authentication chain.</td>
</tr>
<tr>
<td>✷ Card</td>
<td>If user specifies any text in the password, an error message <strong>Unable to authenticate user</strong> is displayed.</td>
</tr>
<tr>
<td>✷ Email OTP</td>
<td></td>
</tr>
<tr>
<td>✷ FIDO U2F</td>
<td></td>
</tr>
<tr>
<td>✷ Fingerprint</td>
<td></td>
</tr>
<tr>
<td>✷ PKI</td>
<td></td>
</tr>
<tr>
<td>✷ SMS OTP</td>
<td></td>
</tr>
<tr>
<td>✷ Swiss Mobile ID</td>
<td></td>
</tr>
<tr>
<td>✷ Voice OTP</td>
<td></td>
</tr>
</tbody>
</table>
Logging In to Mac

You can use the enrolled authenticators to log in to the Mac operating system. You must pass through the authenticators in the chain to get authenticated.

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

1. Select a user from the Mac login screen or specify the user 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. Select an authentication chain from the list.
4. Authenticate with the preferred authentication method(s) of the chain.

   A prompt to select category might appear, if you have enrolled an authenticator for more than one category.

   **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.

   A domain user cannot log in, if a local user with the same username exist. For example, Mac OS has a local user Bob and a domain user mycompany\bob. Mac OS is joined to the domain Mycompany. After specifying the username of the domain user mycompany\bob, selecting a chain, an error message Network account name cannot be the same as local account name is displayed.

Advanced Authentication provides the following authenticators for logging in to Mac computer:

- “Apple Touch ID” on page 152
- “Bluetooth” on page 152
- “Authentication Agent” on page 153
- “Card” on page 153
- “Device Authentication” on page 155
- “Email OTP” on page 155
- “Emergency Password” on page 156
- “Facial Recognition” on page 157
- “Flex OTP” on page 157
- “HANIS Face” on page 158
- “HOTP” on page 158
- “LDAP Password” on page 159
- “Out-of-Band” on page 159
Apple Touch ID

Apple Touch ID enables you to authenticate to a Mac operating system using the electronic fingerprint recognition feature available in Mac device. When you try to authenticate Mac device, the presented fingerprint is matched with the enrolled fingerprint. If the fingerprints match, you are authenticated.

**NOTE:** It is not possible to perform an initial authentication using the Touch ID after boot.

**Perform the following step to authenticate using the Apple Touch ID:**

1. Place your finger on the Touch ID reader.
   
   If the fingerprint matches with the enrolled fingerprint, the authentication is successful.

Bluetooth

The Bluetooth method enables you to authenticate using any Bluetooth enabled device that is within the range. When you initiate authentication, the Advanced Authentication server searches for the enrolled Bluetooth device. If the enrolled device is within the range, you are authenticated successfully.

For example, Susanne, who is a doctor, attends many in-patients in the hospital. She accesses the computer located in each room to monitor and update the health status of the patient. In this case, Susanne can specify her first-factor authentication details and use her Bluetooth enabled mobile phone to log in to the computer automatically when she is within range of a particular room.

**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 using the Bluetooth method, perform the following steps:**

1. Ensure that Bluetooth is turned on in your device and is discoverable to the paired devices.
2 The Device Service detects your Bluetooth device and authenticates.
If the paired Bluetooth device is within the range, the Bluetooth authentication is successful.

Authentication Agent

Authentication Agent enables you to perform multi-factor authentication on one computer to get authorized access to another computer, where it is not possible to display the user interface or connect any external authentication devices. You can install the Authentication Agent on a workstation or a laptop. When an authentication is initiated from a computer using Authentication Agent chain, the Authentication Agent on another computer prompts a restricted browser where you must perform the authentication.

**NOTE:** You can install the Authentication Agent only on the Windows workstation.

**IMPORTANT:** If both the Windows Client and Authentication Agent are installed on the same workstation, the Authentication Agent is logged in automatically through the SSO feature. If the Windows Client is not installed, you must log in to the Authentication Agent manually.

**To log in to Mac using the Authentication Agent on Windows, perform the following steps:**

1. Specify User name in the Mac computer.
2. Click Next and select Authentication Agent from the Chains list.
   For more information about enabling the Authentication Agent chain in the Mac computer, see Enabling the Authentication Agent Chain.
3. The Authentication Agent that is active on a Windows computer launches a restricted browser.

**IMPORTANT:** If a restricted browser is not launched automatically, place the cursor on the Authentication Agent icon in System tray and ensure that the agent is logged in. If the agent is not logged in, double click the Authentication Agent icon to log in.

The restricted browser prompts the login page. The user name that you have specified in the Mac computer is set in the login page by default.

4. Click Next.
5. Select the preferred chain to log in to Mac computer in the restricted browser.
   For more information, see Logging In to Authentication Agent for Windows.
6. After Successful authentication in the restricted browser, you are logged in to the Mac computer automatically.

**Card**

The Card method enables you to authenticate using the contactless smart card (with the card serial number). When you try to authenticate on any device, the recorded serial number of the card is compared with the actual serial number. If the card serial numbers are identical, you are authenticated successfully.
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 the Card Serial Number in the card matches with enrolled card, the card authentication is successful.

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.

The following table describes the possible error messages along with the workaround for the Card authentication.

Table 7-1 Card authenticator - error messages

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong card</td>
<td>The card you have placed on the reader is incorrect. Try again with another card or re-enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
<tr>
<td>Connect reader</td>
<td>The reader is not connected properly. Try to connect it to a different USB slot and authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for Card</td>
<td>You have not enrolled the card method. You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>

Observations of the 1:N Behavior on Mac

The behavior of 1:N login depends on the window that is displayed when a card is placed to the card reader:

When the Username and password login window is set:

- **Case 1**: The Other user window is displayed (username of the user is not submitted). User is logged in through 1:N when the card is placed to a card reader.
- **Case 2**: The list of chains is displayed (username of the user is submitted). User is logged in through 1:N when the card is placed to a card reader.
- **Case 3**: Chain is selected (example, Password only). Enter password window is displayed. User is not logged in through the 1:N when the card is placed to a card reader.
When the List of users login window is set.

- 1:N login is performed when the login window with the list of users is displayed (authentication window is not displayed) or after selecting the Other user.

- 1-N login is not performed after selecting a user from the list when the list of chain for the user is displayed. When you select any user from the list:
  - Case 1: The list of chains is displayed: User is not logged in through 1:N, when placing the card to the card reader.
  - Case 2: Select a chain: User is not logged in through 1:N, when placing the card to the card reader.

- When you select Other user item on login window: The behavior is the same as in the case of Username and password.

**NOTE:**

- 1:N does not work in FUS. After selecting a user from the list in FUS, 1:N login cannot be performed.

- For the screens that are in the sleep or screensaver mode, the authentication window must be opened to perform 1:N login.

---

**Device Authentication**

The Device Authentication method enables you to authenticate using a unique key pair stored in the workstation and PIN. During the enrollment process, a key pair is generated in the workstation and the same is used for further authentication. Device Authentication supports authentication to the Mac workstation and verifies the key pair to authenticate users.

**To authenticate with the Device Authentication method, perform the following steps:**

1. Specify the PIN.
2. Click Next.

   If the PIN matches with the enrolled PIN, the Device authentication is successful.

---

**Email OTP**

The Email OTP method enables you to authenticate using the one-time password (OTP) that is sent to the registered email address. When you try to authenticate on any device, the server sends an email to the registered email address with the OTP. You can use this OTP for single authentication within a short time frame.

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

1. Check your email. You must receive an email with OTP.
2. Specify the OTP from email in Password.
3. Click Next.

   If the OTP matches with the server generated OTP, the Email OTP authentication is successful.

The following table describes the possible error messages along with the workarounds for the Email OTP authentication.
The Emergency Password method enables you to authenticate using a temporary password with the help of helpdesk administrator if you have lost a smart card or forgot your smart phone. The emergency password is valid for certain days and is set to 3 days by default. When you try to authenticate on any device, the submitted emergency password is compared with the enrolled password in the appliance. If the emergency passwords are identical, you are authenticated successfully.

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

1. Specify the Emergency Password.
2. Click Next.

If the Emergency Password matches with the enrolled password, the Emergency Password authentication is successful.

The following table describes the possible error messages along with the workaround for the Emergency Password authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workarount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong answer</td>
<td>The specified OTP is incorrect or is expired.</td>
</tr>
<tr>
<td></td>
<td>Specify a valid OTP within the time frame.</td>
</tr>
<tr>
<td>Cannot send OTP. User does not have an email</td>
<td>Your email address is not set in the profile of the repository.</td>
</tr>
<tr>
<td></td>
<td>Contact your system administrator to add your email address to the profile.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workarount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong password</td>
<td>The specified emergency password is incorrect.</td>
</tr>
<tr>
<td></td>
<td>Specify a valid emergency password and try to authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for Emergency Password</td>
<td>You have not enrolled for Emergency Password method.</td>
</tr>
<tr>
<td></td>
<td>Enroll the authenticator on the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>
Facial Recognition

The Facial Recognition method enables you to get automatically authenticated by presenting your face. You need to register your facial image using the web camera. When you try to authenticate on an application, the recorded image is compared with the actual image. If the images match, you are authenticated successfully.

The Facial Recognition method works with both an integrated and external web camera.

**NOTE:** To use the Facial Recognition method for authentication, you must install the Advanced Authentication Device Service. For more information about the Device Service, see the “Advanced Authentication - Device Service” guide.

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

1. Ensure that a camera is connected to your device.
2. Present your face to the camera.
   
   If your face matches with the enrolled face, the face authentication is successful.

The following table describes the possible error messages along with the workarounds for the Facial Recognition authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed to open camera</td>
<td>The camera is not connected properly.</td>
</tr>
<tr>
<td></td>
<td>Check your camera settings and try again.</td>
</tr>
<tr>
<td>Mismatch</td>
<td>There is a mismatch in the face.</td>
</tr>
<tr>
<td></td>
<td>You must present your face again for the authentication.</td>
</tr>
<tr>
<td>Face service is not available</td>
<td>Device Service is not available.</td>
</tr>
<tr>
<td></td>
<td>Ensure that the Device Service is connected.</td>
</tr>
</tbody>
</table>

Flex OTP

The Flex OTP authenticator facilitates you to authenticate by using your otp password from any of HOTP, TOTP and Smartphone (Offline) authenticator. When you try to authenticate to any device, the OTP in the token is compared with the OTP generated in any of HOTP, TOTP and Smartphone (Offline) authenticators. If the OTPs are valid, you are authenticated successfully.

**To authenticate using the Flex OTP method, perform the following steps:**

1. Specify the One-Time Password from any of HOTP, TOTP and Smartphone (Offline) authenticators
2. If the password is valid, the Flex OTP authentication is successful.
HANIS Face

The HANIS (Home Affairs National Identification System) Face method is for the citizens of South Africa to authenticate with their personal identification number or passport number issued by Home Affairs National Identification System and face biometric. When you try to authenticate on any device, the presented face is matched with the enrolled face. If the images match, you are authenticated successfully.

Face is captured using both integrated and external web cameras.

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

To authenticate by using the HANIS Face method, perform the following steps:

1. Ensure that a camera is connected to your device.
2. Select the chain with HANIS Face method for authentication.
3. Present your face to the camera.
   
   A message Detecting a face is displayed.
   
   If your face matches with the enrolled face, the HANIS Face authentication is successful.

The following table describes the possible error messages along with the workaround for the HANIS Face authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capture Device cannot be opened</td>
<td>The camera is not connected properly. Check your camera settings and try again.</td>
</tr>
<tr>
<td>Timeout</td>
<td>The session has timed out. You must present your face again for the authentication.</td>
</tr>
</tbody>
</table>

HOTP

HOTP is a counter-based one-time password. This method enables you to authenticate using the counter-based one-time password generated on the HOTP token. The counter on the token must be in sync with the server. You can use generic HOTP tokens that adhere to RFC 4226. You can use the static secret key and three consequent OTP generated from the token to enroll. When you try to authenticate on any device, the OTP in the token is compared with the OTP generated in the server. If both OTPs are identical, you are authenticated successfully.

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

1. Specify the HOTP when using software token or connect the USB token, press button on the token.
2 Click Next.

If the OTP on the token matches with the server generated OTP, the HOTP authentication is successful.

The following table describes the possible error messages along with the workaround for the HOTP authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong answer</td>
<td>The OTP you have provided is incorrect. Specify a valid OTP and try again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for HOTP</td>
<td>The HOTP authenticator is not enrolled. You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>

**LDAP Password**

The LDAP password method enables you to authenticate using the password of your corporate account. When you try to authenticate on any device, the specified password is compared with the actual password in the corporate directory. If the passwords match, you are authenticated successfully.

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

1. Specify your domain password.
2. Click Next.

If the LDAP Password matches with the password on the directory, the LDAP Password authentication is successful.

If the specified domain password is incorrect, an error message Invalid credentials is displayed. Specify a valid password and try to authenticate again.

**Out-of-Band**

The Out-of-band method facilitates you to authenticate using the push notification that is sent to the Out-of-band portal or OOB agent. When you initiate the authentication, a push notification is sent to the portal or agent. You can accept the request and get authenticated.

**To authenticate by using the Out-of-band method, perform the following steps:**

When you specify the chain number corresponding to the Out-of-band method, a message Continue at https://<AdvancedAuthenticationServerdomainname>/oob/ui is displayed on your computer.

1. Open the OOB agent installed on your mobile or navigate to the OOB portal.
   A push notification is displayed.
NOTE: If the push notification does not appear after 5 seconds, tap the Refresh icon to view the push notification for the initiated authentication.

2 Tap Accept.

If the response to authentication request is from a secured origin, the authentication is successful.

**Password**

The Password method enables you to authenticate using a secret string. The enrolled password is stored locally in the Advanced Authentication. When you try to authenticate on any device, the specified password is compared with the actual password. If the passwords are identical, you are authenticated successfully.

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

1. Enter the password for your Advanced Authentication account.
2. Click Next.

If the password matches with the enrolled password, the Password authentication is successful.

The following table describes the possible error messages along with the workaround for the Password authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong password</td>
<td>The password you have specified is incorrect.</td>
</tr>
<tr>
<td></td>
<td>Specify a valid password and try to authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for Password</td>
<td>You have not enrolled for the Password method.</td>
</tr>
<tr>
<td></td>
<td>You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>

**PKI**

The PKI method enables you to authenticate using any PKI device such as a contact card and USB token that contains the digital certificate. The PKI reader validates the digital certificate and the identity of users. When you try to authenticate on any device, the certificate in the device is compared with the actual certificate. If the certificates match, you are authenticated successfully.

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

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

1. Insert the card in the reader or connect token to your machine.
Specify the PIN.

If the digital certificate in the card or token and enrolled certificate are identical, the PKI authentication is successful.

**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.

The following table describes the possible error messages along with the workaround for the PKI authentication.

**Table 7-8 PKI authenticator - error messages**

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong card</td>
<td>The card that is used is incorrect. Try authenticating with another valid card or token. You can enroll the authenticator again in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
<tr>
<td>Present card</td>
<td>The PKI device is not connected properly. Try to connect it to a different USB slot and authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for PKI</td>
<td>You have not enrolled for PKI method. You must enroll the authenticator in the Self-Service portal or contact the helpdesk administrator.</td>
</tr>
</tbody>
</table>

**Observations of the 1:N Behavior on Mac**

The behavior of 1:N login depends on the window that is displayed when a card is placed to the card reader:

**When the Username and password login window is set:**

- **Case 1:** The Other user window is displayed (username of the user is not submitted). User is logged in through 1:N when the card is placed to a card reader.
- **Case 2:** The list of chains is displayed (username of the user is submitted). User is logged in through 1:N when the card is placed to a card reader.
- **Case 3:** Chain is selected (example, Password only). Enter password window is displayed. User is not logged in through the 1:N when the card is placed to a card reader.

**When the List of users login window is set:**

- 1:N login is performed when the login window with the list of users is displayed (authentication window is not displayed) or after selecting the Other user.
• 1-N login is not performed after selecting a user from the list when the list of chain for the user is displayed. When you select any user from the list:
  • Case 1: The list of chains is displayed: User is not logged in through 1:N, when placing the card to the card reader.
  • Case 2: Select a chain: User is not logged in through 1:N, when placing the card to the card reader.
• When you select Other user item on login window: The behavior is the same as in the case of Username and password.

NOTE: *1:N does not work in FUS. After selecting a user from the list in FUS, 1:N login cannot be performed.
• For the screens that are in the sleep or screensaver mode, the authentication window must be opened to perform 1:N login.

## RADIUS Client

The RADIUS Client method enables Advanced Authentication to forward the authentication request to a third-party RADIUS server. This can be any RADIUS server.

For example, you can use the RADIUS Client as an authentication method for token solutions such as RSA or Vasco.

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

1. Specify the RADIUS password.
2. Click Next.

If you get an error Wrong answer, it could be an incorrect RADIUS password.

## Security Questions

Security Questions method enables you to enroll answers to a pre-defined set of security questions. When you authenticate using security questions, Advanced Authentication prompts you the configured security questions or a subset of the security questions. You must answer the appropriate questions and based on the correctness of the answers, you are authenticated successfully.

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

1. Specify the answer for the security question.
2. Click Next.
3. Repeat steps 1 to 2 for all the required security questions.

The following table describes the possible error messages along with the workaround for the Security Questions authentication.
Smartphone

The Smartphone method facilitates you to enroll and authenticate using the smartphone app. When you initiate the authentication, a push notification is sent to the app. You can accept the request and get authenticated.

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

1. If there is internet connection on your smartphone, open the smartphone app and accept the authentication request.
2. If there is no internet connection on your smartphone, perform the following steps:
   2a. Open the smartphone app.
   2b. Specify the OTP that you received on your smartphone app.
   2c. Click Next.

To authenticate with the Smartphone method using the offline authentication, perform the following steps:

1. Open the Advanced Authentication smartphone app.
2. Click Enrolled Authenticators from Menu in the smartphone app.
3. Specify the OTP from the smartphone app in Password.
4. Click Next.
   If the OTP on the smartphone app matches with the server generated OTP, the authentication is successful.

The following table describes the possible error messages along with the workaround for the Smartphone authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong answer</td>
<td>The answer that you have provided is incorrect. Specify the correct answer and try to authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for security questions</td>
<td>You have not enrolled the Security Questions method. You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>

Auth rejected                                           | You have declined the authentication request.                                                 |
Wrong TOTP password                                      | You are using offline authentication and specified an incorrect TOTP password or the time on your smartphone is not synchronized. |
SMS OTP

The SMS OTP method facilitates you to generate a single-use password or OTP and send it to the registered mobile number for authentication. You can use this OTP to authenticate within a short time frame.

**NOTE:** The OTP period is set to 120 seconds by default. An administrator has the privilege to change the OTP period.

To perform authentication using the SMS OTP method, perform the following steps:

1. You will receive an SMS message with an OTP on your phone.
2. Specify 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 profile of the repository.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOTP login is disabled</td>
<td>You are using offline authentication and Geo-fencing is enabled.</td>
</tr>
<tr>
<td></td>
<td>Contact the administrator for further assistance.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for smartphone</td>
<td>You have not enrolled the smartphone method.</td>
</tr>
<tr>
<td></td>
<td>You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>

TOTP

The TOTP method enables you to authenticate using the time-based-one-time password. TOTP is generated on the hardware token or the mobile app, such as NetIQ Advanced Authentication app or Google Authenticator app. The TOTP is valid for a short duration. This method uses a predefined period. The default value is 30 seconds.

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 the OTP on the token matches with the server generated OTP, the TOTP authentication is successful.

The following table describes the possible error messages along with the workaround for the TOTP authentication.
FIDO U2F

The FIDO U2F authentication method facilitates you connect the FIDO U2F compliant token to the computer or laptop and touch the flashing token for authentication. When you try to authenticate on any device, token connected to the device is compared with the actual device. If the device details match, you are authenticated successfully.

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

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

1. Ensure that the FIDO U2F token is connected to the workstation.
   A message Please touch the flashing U2F device now is displayed.
2. Touch button on the token when there is a flash.
   If the token matches with the enrolled U2F token, the FIDO U2F authentication is successful.
   If there is no flash, wait for few seconds. If there is no flash for more than a minute then try to reconnect your token and repeat the steps.

The following table describes the possible error messages along with the workaround for the FIDO U2F authentication.

Table 7-12  FIDO U2F authenticator - error messages

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong token. Try another one</td>
<td>The token that you have connected is incorrect.</td>
</tr>
<tr>
<td></td>
<td>Try to authenticate with another token or re-enroll the authenticator in Self-Service portal or contact your helpdesk administrator.</td>
</tr>
<tr>
<td>Connect a token</td>
<td>The token is not connected properly.</td>
</tr>
<tr>
<td></td>
<td>Try to connect it to a different USB slot and authenticate again.</td>
</tr>
</tbody>
</table>
### Voice

The Voice authenticator initiates a call to your registered phone number. The phone call requests you to specify the PIN for authentication. When you try to authenticate on an application, the recorded PIN is compared with the actual PIN. If both PINs match, you are authenticated successfully.

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

1. Check your mobile phone. You must receive a phone call.
2. Answer the phone call, listen to the request.
3. Specify your PIN followed by the hash symbol (#) in the dial pad of your mobile phone.
   - If the PIN matches with the enrolled PIN, the Voice authentication is successful.

### Voice OTP

The Voice OTP method enables you to authenticate using the OTP that is sent through the phone call to your registered phone number. You can use this OTP for authentication within a short time frame. When you try to authenticate on any device, the specified OTP is compared with the OTP generated on the server. If both the OTPs are identical, you are authenticated successfully.

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

1. Answer the phone call on your phone and listen to the voice OTP.
2. Specify the OTP in **Password**.
3. Click **Next**.
   - If the OTP matches with the server generated OTP, the Voice OTP authentication is successful.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Your user name&gt; has no authenticator for U2F</td>
<td>You have not enrolled for U2F method. You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>
Switching Input Language on Mac OS

On the Mac OS system, when you use more than one language you can switch between the input languages without changing the keyboard on screens, such as login, lock, FUS, and Preferences.

Adding Input Sources

Before you switch between preferred languages, ensure to add language and make the Input menu visible in the menu bar on all screens. To add languages as input sources, perform the following steps:

1. Click the Apple icon > Keyboard > System Preferences > Input Sources on your Mac OS system.
2. Click Add button +, search for the preferred language (for example, German) and then select one or more languages.
3. Click Add.

After you add languages, the Input menu is displayed in the menu bar automatically. The Input menu allows you to quickly switch input languages as per your requirement.

Following table describes how you can switch language on different screen:

<table>
<thead>
<tr>
<th>Screen</th>
<th>Action to Switch Input Language</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login screen</td>
<td>Use one of the following ways to switch input language:</td>
</tr>
<tr>
<td></td>
<td>◦ Click Input menu in the menu bar and select the preferred language.</td>
</tr>
<tr>
<td></td>
<td>◦ Use one of the following shortcut:</td>
</tr>
<tr>
<td></td>
<td>◦ control + option + space: To view all language and switch to one language</td>
</tr>
<tr>
<td></td>
<td>◦ control + space: To switch between two input languages</td>
</tr>
<tr>
<td>Screensaver, Lock screen, or Sleep mode</td>
<td>Use one of the following shortcut:</td>
</tr>
<tr>
<td></td>
<td>◦ control + option + space: To view all language and switch to one language</td>
</tr>
<tr>
<td></td>
<td>◦ control + space: To switch between two input languages</td>
</tr>
<tr>
<td>Screen</td>
<td>Action to Switch Input Language</td>
</tr>
<tr>
<td>--------</td>
<td>---------------------------------</td>
</tr>
</tbody>
</table>
| FUS, System preferences, or authenticating during software installation | Use one of the following ways to switch input language:  
  - Click Input menu in the menu bar and select the preferred language.  
  - Use one of the following shortcut:  
    - control + option + space: To view all language and switch to one language  
    - control + space: To switch between two input languages  

**NOTE:** In some scenarios, shortcut keys do not work and you are required to use Input menu to switch language.
Logging In to Out-of-Band Portal

The Out-of-band (OOB) portal allows you to manage the authentication requests that the OOB method sends to authenticate to any device or service.

You can use the enrolled authenticators to log in to the Out-of-band portal. You must pass through the authenticators in the chain to get authenticated successfully.

To log in to Out-of-band portal, perform the following steps:

1. Log in to the Advanced Authentication OOB portal (https://<AdvancedAuthenticationServerdomainname>/oob/ui)
2. Specify the username in the format: repositoryname\username (e.g. company\pjones) and click Next.
3. Select the preferred authentication chain from the list.
4. Authenticate with the preferred authentication method(s) of the chain.
   A prompt to select category might appear, if you have enrolled an authenticator for more than one category.

Instead of logging in to OOB portal for each authentication, you can install the Authentication Agent for Web on a desktop or mobile using the Google Chrome browser. Perform the following steps to install the Authentication Agent for Web:

2. Authenticate with the preferred authentication method(s) of the chain.
   On successful authentication, the Authentication Requests page appears.
3. Perform one of the following:
   • Desktop: Click the Install icon in the address bar.
   • Mobile: Tap the Install icon adjacent to the user name.
   A message is displayed to confirm the install.
4. Click Install.
   The Authentication Agent for Web is installed on your desktop or mobile.

NOTE: To receive the push messages, you must enable the notifications in your browser for the OOB portal or Authentication Agent for Web app. By default, the notifications are blocked.

NOTE: After initiating the authentication if the push notification does not appear after 5 seconds, click the Refresh icon to view the push notification for the initiated authentication.
The following examples describe the different scenarios where the OOB portal is used:

- **Scenario 1: Authenticating to Linux using the OOB Method**
- **Scenario 2: Authenticating to VPN using the Out-of-Band Portal and Biometrics**
- **Scenario 3: Authenticating to z/OS Mainframe Using the Authentication Agent for Web on Smartphone**

### Scenario 1: Authenticating to Linux using the OOB Method

The OOB method is enrolled for Paul in the Advanced Authentication Self-Service portal. Using the OOB portal, he has installed the Authentication Agent for Web on his Android smartphone.

Consider administrator has set-up the following:

- Assigned a chain with the **Password** and TOTP methods to the OOB portal.
- Assigned a chain with the **OOB** method to the Linux machine.

Following sequence describes the authentication process using the Authentication Agent for Web:

1. Paul opens the Authentication Agent for Web that is installed on his Android smartphone and authenticates on it using the Password and TOTP methods.
2. Specify **user name** and select the chain with **Out-of-band** method in Linux computer.
   
   This initiates an authentication request.
3. An authentication request with **Accept** and **Decline** buttons is displayed on the Authentication Agent for Web.

   **NOTE:** After initiating the authentication if the push notification does not appear after 5 seconds, click the Refresh icon to view the push notification for the initiated authentication.

4. Tap **Accept**.
   
   Paul logs in to the Linux computer successfully.

### Scenario 2: Authenticating to VPN using the Out-of-Band Portal and Biometrics

An organization has secured the VPN network with strong multi-factor authentication using domain password and Windows Hello. Janet wants to connect to the corporate VPN. However, it is not possible to use fingerprint and face recognition directly in the RADIUS authentication. The organization has decided to use the Out-of-Band method for this scenario.

Janet has Windows laptop with a built-in fingerprint sensor.

Consider the following setup:

- Assigned a chain with the Windows Hello method to the OOB portal.
- Assigned a chain with the LDAP Password and Out-of-band methods to the RADIUS Server.

Following sequence describes the authentication process using the OOB portal:

1. Specify **username** and domain password in the VPN connection request.
3. Authenticate to the OOB portal using the Windows Hello method.
4 The pending authentication request appears.

**NOTE:** After initiating the authentication if the push notification does not appear after 5 seconds, click the Refresh icon 🔄 to view the push notification for the initiated authentication.

5 Click Accept.
Janet gets connected to the corporate VPN.

**Scenario 3: Authenticating to z/OS Mainframe Using the Authentication Agent for Web on Smartphone**

Nick wants to log in to the z/OS mainframe. The mainframe is secured with Advanced Authentication OOB method.

Consider the following setup:

- The Authentication Agent for Web and NetIQ Advanced Authentication applications are installed on an Android smartphone.
- Windows laptop has access to the z/OS terminal.
- Assigned a chain with the Smartphone method to the OOB portal.
- Assigned a chain with the OOB method to the Mainframe.

Following sequence describes the authentication process using the Authentication Agent for Web:

1 Initiate login to z/OS mainframe on Windows laptop and specify oob in the Password. This initiates the authentication request.
2 Authentication Agent for Web on the smartphone receives a notification about the pending authentication request.
3 Tap the notification to open Authentication Agent for Web and authenticate using the Smartphone method.
4 The pending authentication request is displayed in Authentication Agent for Web.

**NOTE:** After initiating the authentication if the push notification does not appear after 5 seconds, click the Refresh icon 🔄 to view the push notification for the initiated authentication.

5 Click Accept.
Nick connects to the z/OS mainframe.

Advanced Authentication provides the following authenticators for logging in to the Out-of-band portal:

- “Bluetooth” on page 172
- “Card” on page 173
- “Device Authentication” on page 174
- “Email OTP” on page 175
- “Emergency Password” on page 175
- “Facial Recognition” on page 176
Bluetooth

The Bluetooth method enables you to authenticate using any Bluetooth enabled device that is within the range. When you initiate authentication, the Advanced Authentication server searches for the enrolled Bluetooth device. If the enrolled device is within the range, you are authenticated successfully.

For example, Susanne, who is a doctor, attends many in-patients in the hospital. She accesses the computer located in each room to monitor and update the health status of the patient. In this case, Susane can specify her first-factor authentication details and use her Bluetooth enabled mobile phone to log in to the computer automatically when she is within range of a particular room. When she exits the room, she is logged out of that computer automatically.

**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 using the Bluetooth method, perform the following steps:**

1. Ensure that Bluetooth is turned on in your device and is discoverable to the paired devices.
2. The Device Service detects your bluetooth device and authenticates.
   
   If the paired bluetooth device is within the range, the bluetooth authentication is successful.
NOTE: If the administrator has set Enable reaction on device removal option to ON for Bluetooth method then the operating system automatically locks, if one of the following is true:

- The Bluetooth device is disabled.
- The Bluetooth device is out of range.

Card

The Card method enables you to authenticate using the contactless smart card (with the card serial number). When you try to authenticate on any device, the recorded serial number of the card is compared with the actual serial number. If the card serial numbers are identical, you are authenticated successfully.

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 using the Card method, perform the following steps:

1. Ensure that the card reader is connected to your system.
2. Tap your card on the reader or insert a smart card in the reader.
   - If the Card Serial Number in the card matches with enrolled card, the card authentication is successful.

IMPORTANT: The Card method supports the 1:N feature that Advanced Authentication to detect the user name automatically. You can press CTRL+ALT+DEL then place a card to the reader to authenticate.

The following table describes the possible error messages along with the workarounds for the Card authentication.
Table 9-1  Card authenticator - error messages

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Wrong card</strong></td>
<td>The card you have placed on the reader is incorrect. Try again with another card or re-enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
<tr>
<td><strong>Connect reader</strong></td>
<td>The reader is not connected properly. Try to connect it to a different USB slot and try again.</td>
</tr>
<tr>
<td><strong>&lt;Your user name&gt; has no authenticator for Card</strong></td>
<td>You have not enrolled the card method. You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
<tr>
<td><strong>No template for Card</strong></td>
<td>The card is not enrolled or you are trying to log in with the non-cached authenticator in the offline mode.</td>
</tr>
</tbody>
</table>

**IMPORTANT:** An administrator has the privilege to configure an automatic session lock or log off for the events with Card authentication method. In such a scenario, you must:

- When Tap&Go is disabled, you must place your card on the reader during login. After login you can remove the card from the reader to lock the operating system or log off automatically.

  Or

- When Tap&Go is enabled, you must tap a card on the reader to log in and to lock, unlock, or log off.

---

**Device Authentication**

You can authenticate to Windows workstation using the Device Authentication method using one of the following:

- **Using Trusted Platform Module (TPM) chip**
  
  The TPM chip is a crypto-processor available in Windows workstation to achieve actions, such as generating, storing, and limiting the use of cryptographic keys. Device Authentication supports authentication to Windows workstation and makes use of information available in the chip to authenticate users.

- **Non-TPM mode**
  
  In this mode, a key pair is generated in the workstation during the enrollment process that is used for further authentication on the same workstation.

**NOTE:** In non-TPM mode, ensure to enroll the Device Service method using the workstation where you would perform further authentication. Enrollment on one machine and authentication on another machine is not supported.
To authenticate with the Device Authentication method, perform the following steps:

1. Specify one of the following:
   - The TPM chip generated PIN
   - The enrolled PIN
2. Click Next.
   
   If the PIN matches with the TPM chip generated PIN or enrolled PIN, the Device Authentication is successful.

Email OTP

The Email OTP method enables you to authenticate using the one-time password (OTP) that is sent to the registered email address. When you try to authenticate on any device, the server sends an email to the registered email address with the OTP. You can use this OTP for single authentication within a short time frame.

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

1. Check your email. You will receive an email with an OTP.
2. Specify the OTP from email in Password.
3. Click Next.
   
   If the OTP matches with the server generated OTP, the Email OTP authentication is successful.

The following table describes the possible error messages along with the workarounds for the Email OTP authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong answer</td>
<td>The specified OTP is incorrect or is expired. Try to specify a valid OTP within the time frame.</td>
</tr>
<tr>
<td>Cannot send OTP. User does not have an email</td>
<td>Your email address is not set in the profile of the repository. Contact your system administrator to add your email address to the profile.</td>
</tr>
</tbody>
</table>

Emergency Password

The Emergency Password method enables you to authenticate using a temporary password with the help of helpdesk administrator if you have lost a smart card or forgot your smart phone. The emergency password is valid for certain days and is set to 3 days by default. When you try to authenticate on any device, the submitted emergency password is compared with the enrolled password in the appliance. If the emergency passwords are identical, you are authenticated successfully.

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

1. Specify the emergency password.
2 Click Next.

If the emergency password matches with the enrolled password, the emergency password authentication is successful.

The following table describes the possible error message along with the workarounds for the Emergency Password authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong password</td>
<td>The specified emergency password is incorrect. Specify a valid emergency password and try to authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for Emergency Password</td>
<td>You have not enrolled for Emergency Password method. Enroll the authenticator on the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>

Facial Recognition

The Facial Recognition method enables you to get automatically authenticated by presenting your face. You need to register your face image using the web camera. When you try to authenticate on an application, the recorded image is compared with the actual image. If the images match, you will be successfully authenticated.

The Facial Recognition method works with both integrated and external web cameras.

NOTE: To use the Facial Recognition method for authentication, you must install the Advanced Authentication Device Service. For more information about the Device Service, see the “Advanced Authentication - Device Service” guide.

To authenticate using the Facial Recognition method, perform the following steps:

1. Ensure that a camera is connected to your device.
2. Present your face to the camera.

   If your face matches with the enrolled face, the face authentication is successful.

The following table describes the possible error message along with the workarounds for the Facial Recognition authentication.
**Table 9-4  Facial Recognition authenticator - error messages**

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed to open camera</td>
<td>If the camera is not connected properly. Check your camera settings and try again.</td>
</tr>
<tr>
<td>Mismatch</td>
<td>The enrolled face and presented face does not match. You must present your face again for the authentication.</td>
</tr>
<tr>
<td>Face service is not available</td>
<td>The Device Service is not available. Ensure that the Device Service is installed.</td>
</tr>
</tbody>
</table>

**Flex OTP**

The Flex OTP authenticator facilitates you to authenticate by using your otp password from any of HOTP, TOTP and Smartphone (Offline) authenticator. When you try to authenticate to any device, the OTP in the token is compared with the OTP generated in any of HOTP, TOTP and Smartphone (Offline) authenticators. If the OTPs are valid, you are authenticated successfully.

**To authenticate using the Flex OTP method, perform the following steps:**

1. Specify the One-Time Password from any of HOTP, TOTP and Smartphone (Offline) authenticators
2. If the password is valid, the Flex OTP authentication is successful.

**Fingerprint**

The Fingerprint authentication method enables you to authenticate using your fingerprint. The fingerprint scanner captures the fingerprint. When you try to authenticate on any device, the recorded fingerprint is compared with the actual fingerprint. If the fingerprints are identical, you are authenticated successfully.

**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 using the Fingerprint method, perform the following steps:**

1. Ensure that a fingerprint reader is connected to the computer.
2. Place your finger on the reader when using a touch sensor or swipe your finger when using a swipe sensor.
   
   If the fingerprint matches with the enrolled fingerprint, the authentication is successful.

**NOTE:** Ensure to enroll the required fingers that are highlighted in the *Add Fingerprint Authenticator* page.

The following table describes the possible error message along with the workarounds for the Fingerprint authentication.
Home Affairs National Identification System (HANIS)

The HANIS method is for the citizens of South Africa. The HANIS method enables you to authenticate using your fingerprint that is registered in the National Identification System. The fingerprint scanner captures the fingerprint. When you try to authenticate on any device, the fingerprint available in the National Identification System is compared with the captured fingerprint. If fingerprints are identical, you are authenticated successfully.

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

To authenticate using the HANIS method, perform the following steps:

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

   If fingerprint matches with the fingerprint available in the National Identification System, the authentication is successful.

HOTP

HOTP is a counter-based one-time password. This method enables you to authenticate using the counter-based one-time password generated on the HOTP token. The counter on the token must be in sync with the server. You can use generic HOTP tokens that adhere to RFC 4226. You must use the static secret key and three consequent OTP generated from the token to enroll. When you try to authenticate on any device, the OTP in the token is compared with the OTP generated in the server. If the OTPs are identical, you are authenticated successfully.

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

1. Specify the OTP when using software token or some kind of hardware tokens or connect the USB token, press button on the token.
2 Click Next.

If the OTP on the token and the server generated OTP are identical, the HOTP authentication is successful.

The following table describes the possible error message along with the workarounds for the HOTP authentication.

**Table 9-6  HOTP authenticator - error messages**

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong answer</td>
<td>The OTP you have provided is incorrect. Specify a valid OTP and try again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for HOTP</td>
<td>You have not enrolled for HOTP method. You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>

**LDAP Password**

The LDAP password method enables you to authenticate using the password of your corporate account. When you try to authenticate on any device, the specified password is compared with the actual password in the corporate directory. If both the passwords are identical, you are authenticated successfully.

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

1 Specify your domain password.
2 Click Next.

If the LDAP Password matches with the password on the directory, the LDAP Password authentication is successful.

If the specified domain password is incorrect, an error message *Invalid credentials is displayed. Specify a valid password and try to authenticate again.*

**Password**

The Password method enables you to authenticate using a secret string. The enrolled password is stored locally in the Advanced Authentication. When you try to authenticate on any device, the specified password is compared with the actual password. If the passwords are identical, you are authenticated successfully.

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

1 Specify the password of your Advanced Authentication account.
2 Click Next.

If the password matches with the enrolled password, the Password authentication is successful.

The following table describes the possible error message along with the workarounds for the Password authentication.
PKI

The PKI method enables you authenticate using any PKI device, such as a contact card and USB token that contains the digital certificate. The PKI reader validates the digital certificate and the identity of users. When you try to authenticate on an application, the certificate in the device is compared with the actual certificate. If the certificates match, you are authenticated successfully.

**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 authenticate using the PKI method, perform the following steps:**

1. Insert a card or plug the token to your machine.
2. Specify the PIN.
   - If the digital certificate in the card or token and enrolled certificate are identical, the PKI authentication is successful.

**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.

The following table describes the possible error message along with the workarounds for the PKI authentication.

**Table 9-7** Password authenticator - error messages

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong password</td>
<td>The password you have specified is incorrect. Specify a valid password and try to authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for Password</td>
<td>You have not enrolled for Password method. You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>
Table 9-8  PKI authenticator - error messages

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong card</td>
<td>The card that is used is incorrect. Try authenticating with another valid card or token. Enroll the authenticator again in Self-Service portal or contact your helpdesk administrator.</td>
</tr>
<tr>
<td>Present card</td>
<td>The PKI device is not connected properly. Try to connect it to a different USB slot and authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for PKI</td>
<td>You have not enrolled for PKI method. You must enroll the authenticator in the Self-Service portal or contact the helpdesk administrator.</td>
</tr>
<tr>
<td>No template for Card</td>
<td>The card is not enrolled or you are trying to log in with the non-cached authenticator in the offline mode.</td>
</tr>
</tbody>
</table>

**NOTE:** To log in to a computer using the PKI authenticator, you must place the card on the reader or connect a token to the computer. After the login, you can remove the card from the reader or disconnect the token to lock the computer automatically.

Advanced Authentication does not support the tapping of a card to lock or unlock a computer.

**RADIUS Client**

The RADIUS Client method enables Advanced Authentication to forward the authentication request to a third-party RADIUS server. This can be any RADIUS server.

For example, you can use the RADIUS Client as an authentication method for token solutions such as RSA or Vasco.

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

1. Specify the RADIUS password.
2. Click Next.

If you get an error Wrong answer, it could be an incorrect RADIUS password.

**Security Questions**

Security Questions method enables you to enroll answers to a pre-defined set of security questions. When you authenticate using security questions, Advanced Authentication prompts you the configured security questions or a subset of the security questions. You must answer the appropriate questions and based on the correctness of the answers, you are authenticated successfully.

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

1. Specify your answer for the displayed security question.
2 Click Next.

3 Repeat steps 1 to 2 for all the security questions.

If all the specified answers match with enrolled answers, the Security Questions authentication is successful.

The following table describes the possible error messages along with the workaround for the Security Questions authentication.

<table>
<thead>
<tr>
<th>Table 9-9 Security Questions authenticator - error messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error</td>
</tr>
<tr>
<td>-------</td>
</tr>
<tr>
<td>Wrong answer</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for Security Questions</td>
</tr>
</tbody>
</table>

**Smartphone**

The Smartphone method facilitates you to enroll and authenticate using the smartphone app. When you initiate the authentication, a push notification is sent to the app. You can accept the request and get authenticated.

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

When you select the Smartphone method from the Chains list, a message Accept on smartphone or enter the one-time password is displayed on your computer.

1 Open the Advanced Authentication smartphone app.

   A push notification is sent to your smartphone.

2 Tap Accept.

   If the smartphone matches with the enrolled smartphone, the authentication is successful.

To authenticate with the Smartphone method using the offline authentication, perform the following steps:

1 Open the Advanced Authentication smartphone app.

2 Click Enrolled Authenticators in the menu of the smartphone app.

3 Specify the OTP from the smartphone app in Password.

4 Click Next.

   If the OTP on the smartphone app matches with server generated OTP, the authentication is successful.

The following table describes the possible error messages along with the workaround for the Smartphone authentication.
Table 9-10  Smartphone authenticator - error messages

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth rejected</td>
<td>The authentication request is declined in the smartphone app. Initiate the authentication and accept the request to authenticate again.</td>
</tr>
<tr>
<td>Wrong TOTP password</td>
<td>Specified OTP for the offline authentication is incorrect or the time on your smartphone is not synchronized. Specify the valid OTP and try authenticating again.</td>
</tr>
<tr>
<td>TOTP login is disabled</td>
<td>If the administrator has disabled TOTP login or when the geo-fencing is enabled. Contact your administrator for further assistance.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for smartphone</td>
<td>You have not enrolled for Smartphone method. Enroll the authenticator on the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>

SMS OTP

The SMS OTP method facilitates you to generate a single-use password or OTP and send it to the registered mobile number for authentication. You can use this OTP to authenticate within a short time frame.

**NOTE:** The OTP period is set to 120 seconds by default. An administrator has the privilege to change the OTP period.

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

1. Check your phone.
   An SMS message with an OTP is sent to your phone.
2. Specify the OTP in Password.
3. Click Next.
   If the OTP matches with the server generated OTP, the SMS OTP authentication is successful.

The following table describes the possible error messages along with the workaround for the SMS OTP authentication.
Swisscom Mobile ID

The Swisscom Mobile ID authentication method uses the phone number from your profile of the repository. The authenticator sends an authentication request to your mobile phone. You need to accept it.

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

1. Check your mobile phone.
   A request message is displayed on your mobile phone.
2. Accept the request.
   If the Mobile ID matches with the enrolled Mobile ID, the Swisscom Mobile ID authentication is successful.

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

TOTP

The TOTP method enables you to authenticate using the time-based-one-time password. TOTP is generated on the hardware token or the mobile app, such as NetIQ Advanced Authentication app or Google Authenticator app. The TOTP is valid for a short duration. This method uses a predefined period. The default value is 30 seconds.

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

1. Specify the TOTP from your hardware or software token.
2. Click Next.
   If the OTP on the token matches with the server generated OTP, the TOTP authentication is successful.

The following table describes the possible error message along with the workaround for the TOTP authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong answer</td>
<td>The specified OTP is incorrect or is expired. Specify a valid OTP within the time frame.</td>
</tr>
<tr>
<td>Cannot send OTP. User does not have a cell phone</td>
<td>Your email address is not set in the profile of the repository. Contact your system administrator to add your phone number to the profile.</td>
</tr>
</tbody>
</table>
Table 9-12  TOTP authenticator - error messages

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incorrect OTP password</td>
<td>The OTP you have provided is incorrect or the server time is not in sync. Specify a valid OTP and try to authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for TOTP</td>
<td>You have not enrolled for TOTP method. You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>

**FIDO U2F**

The FIDO U2F facilitates method enables you connect the FIDO U2F compliant token to the computer or laptop and touch the flashing token to authenticate. When you try to authenticate on any device, token connected to the device is compared with the actual device. If the device details match, you are authenticated successfully.

**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 using the FIDO U2F method, perform the following steps:

1. Ensure that the FIDO U2F token is connected to the workstation.
   - A message Please touch the flashing U2F device now is displayed.

2. Touch the button on the token when you see a blink.
   - If the token and attestation certificate in the token matches with the enrolled U2F token, the FIDO U2F authentication is successful.
   - If the device does not blink, wait for few seconds. If you do not see the blink for more than a minute, try to reconnect your token and repeat the steps.

**NOTE:** Administrator can configure an automatic session lock or log off on the U2F events. When a user returns to the workstation, the user must connect the U2F device to the workstation to unlock.

The following table describes the possible error messages along with the workaround for the FIDO U2F authentication.
**Table 9-13**  
_FIDO U2F authenticator - error messages_

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong token. Try another one</td>
<td>The token that you have connected is incorrect. Try to authenticate with another token or re-enroll the authenticator in Self-Service portal or contact your helpdesk administrator.</td>
</tr>
<tr>
<td>Connect a token</td>
<td>The token is not connected properly. Try to connect it to a different USB slot and authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for U2F</td>
<td>You have not enrolled for U2F method. You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>

**Voice**

The Voice authenticator initiates a call to your registered phone number. The phone call requests you to specify the PIN for authentication. When you try to authenticate on an application, the recorded PIN is compared with the actual PIN. If both the PINs match, you are successfully authenticated.

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

1. Answer the phone call on your phone and listen to the request.
2. Specify your PIN code followed by the hash symbol (#) in the dial pad of your mobile phone. If the PIN matches with enrolled PIN, the Voice authentication is successful.

**Voice OTP**

The Voice OTP authenticator initiates a phone call to your registered phone number. You will receive the voice OTP in the phone call. You can use this OTP for authentication within a short time frame.

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

1. Answer the phone call on your phone and listen to the voice OTP.
2. Specify the OTP in _Password_.
3. Click _Next_. If the OTP matches with the server generated OTP, the Voice OTP authentication is successful.

**Windows Hello**

The Windows Hello method facilitates you to use your Windows Hello fingerprint and facial recognition authentication to log in to the Windows 10 operating system. Advanced Authentication supports the Windows Hello fingerprint and facial recognition.
To authenticate using the Windows Hello, perform the following steps:

1 **For fingerprint authentication:** Ensure that a fingerprint reader is connected to the required device.
   
   1a Place your enrolled finger on the reader when using a touch sensor or swipe your finger when using a swipe sensor.
   
   If the fingerprint matches with the fingerprint enrolled on Windows 10 operating system, Windows Hello authentication is successful.

2 **For facial recognition:** Ensure that an external camera is connected to your computer.

   **NOTE:** This method supports all the devices that Windows Hello works with. For example, the Windows Hello facial recognition works with only the infrared cameras. Therefore, the Advanced Authentication Windows Hello method also supports only the infrared camera for facial recognition.

   2a Present your face to the camera.
   
   If the face matches with the facial image enrolled on Windows 10 operating system, Windows Hello authentication is successful.
Logging In to Windows

You can use the enrolled authenticators to log in to the Windows operating system. You must pass through the authenticators in the chain to get authenticated.

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

1. Specify the user 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. Select an authentication chain from the list.
4. Authenticate with the required authentication method(s) of the chain.
   A prompt to select category might appear, if you have enrolled an authenticator for more than one category.
5. (Conditional) If the administrator has configured Windows Hello for Business, you are required to specify Windows Hello PIN on the Windows 10 workstation as an additional factor after authenticating with the Advanced Authentication chain.

   **NOTE:** If you log in to a non-domain joined workstation for the first time, you are prompted to provide credentials of your local account to map the domain account to the local account. Specify `<computer name>\<Username of local account>` or `<Username of local account> in user name` then specify the password of your local account and click Next.

Advanced Authentication provides the following authenticators for logging in to Windows:

- “Authentication Agent” on page 190
- “Bluetooth” on page 191
- “Bluetooth eSec” on page 192
- “Card” on page 192
- “Device Authentication” on page 193
- “Email OTP” on page 194
- “Emergency Password” on page 195
- “Facial Recognition” on page 195
- “Flex OTP” on page 196
- “FIDO2” on page 196
- “Fingerprint” on page 197
- “HANIS Face” on page 198
Authentication Agent

Authentication Agent enables you to perform multi-factor authentication on one computer to get authorized access to another computer, where it is not possible to display the user interface or connect any external authentication devices. You can install the Authentication Agent on a workstation or a laptop. When an authentication is initiated from a computer using Authentication Agent chain, the Authentication Agent on another computer prompts a restricted browser where you must perform authentication.

NOTE: You can install the Authentication Agent only on the Windows workstation.

IMPORTANT: If both the Windows Client and Authentication Agent are installed on the same workstation, the Authentication Agent is logged in automatically through the SSO feature. If the Windows Client is not installed, user must log in to the Authentication Agent manually.

Consider the following setup:

- Windows 1 is computer without the devices required for authentication and where the Authentication Agent chain is enabled.
- Windows 2 is Windows computer with the Authentication Agent installed and is connected with the devices used for authentication such as, FIDO U2F token and card reader.

To log in to Windows 1 using the Authentication Agent on Windows 2, perform the following steps:

1. Specify User name in Windows 1.
2. Click Next and select Authentication Agent from the Chains list.

For more information about enabling the Authentication Agent chain in Windows computer, see Configuring to Enable the Authentication Agent Chain.
3 The Authentication Agent that is active on Windows 2 launches a restricted browser.

**IMPORTANT:** If a restricted browser is not launched automatically, place the cursor on the Authentication Agent icon in System tray and ensure that the agent is logged in. If the agent is not logged in, double click the Authentication Agent icon to log in.

The restricted browser prompts the login page. The user name that you have specified in the Windows 1 is set in the login page by default.

4 Click Next.

5 Select and authenticate the preferred chain to log in to Windows 1 in the restricted browser.
   For more information, see Logging In to Authentication Agent for Windows.

6 After successful authentication in the restricted browser, you are logged in to the Windows 1 automatically.

**Bluetooth**

The Bluetooth method enables you to authenticate using any Bluetooth enabled device that is within the range. When you initiate authentication, the Advanced Authentication server searches for the enrolled Bluetooth device. If the enrolled device is within the range, you are authenticated successfully.

For example, Susanne, who is a doctor, attends many in-patients in the hospital. She accesses the computer located in each room to monitor and update the health status of the patient. In this case, Susanne can specify her first-factor authentication details and use her Bluetooth enabled mobile phone to log in to the computer automatically when she is within range of a particular room. When she exits the room, she is logged out of that computer automatically.

**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 using the Bluetooth method, perform the following steps:**

1 Ensure that Bluetooth is turned on in your device and is discoverable to the paired devices.

2 The Device Service detects your bluetooth device and authenticates.
   If the paired bluetooth device is within the range, the bluetooth authentication is successful.

**NOTE:** If the administrator has set Enable reaction on device removal option to ON for Bluetooth method then the operating system automatically locks, if one of the following is true:

- The Bluetooth device is disabled.
- The Bluetooth device is out of range.
Bluetooth eSec

The Bluetooth eSec method allows you to authenticate with wireless technology using any Bluetooth supported mobile device within a short range. When you initiate authentication, the Advanced Authentication Server detects the enrolled device within the define range. If the enrolled device is available, the authentication successful.

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

To authenticate using the Bluetooth eSec method, perform the following steps:

1. Ensure that Bluetooth is turned on in your device and is discoverable to the paired devices. A message Present bluetooth device is displayed.
2. The Device Service detects the enrolled Bluetooth device and authenticates it. If the enrolled Bluetooth device is within the range, the Bluetooth authentication is successful.

**NOTE:** If the administrator has set the Required paired device (more secure) option to ON for the Bluetooth eSec method then you must authenticate to the Windows machine with only paired devices.

The following table describes the possible error messages along with the workarounds for the Bluetooth eSec authentication:

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Timeout</td>
<td>The Device Service is unable to detect the Bluetooth device in the range.</td>
</tr>
<tr>
<td>The Bluetooth Device is incorrect</td>
<td>When the Bluetooth is OFF on the enrolled device.</td>
</tr>
<tr>
<td>Logon failed</td>
<td>When the Bluetooth is OFF on the enrolled device and Windows machine from where you are initiating the authentication is not connected to the network.</td>
</tr>
</tbody>
</table>

Card

The Card method enables you to authenticate using the contactless smart card (with Card Serial Number). When you try to authenticate on any device, the recorded serial number of the card is compared with the actual serial number. If the card serial numbers are identical, you are authenticated successfully.

**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 in the reader.
   
   If the Card Serial Number in the card matches with enrolled card, the card authentication is successful.

**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.

The following table describes the possible error messages along with the workaround for the Card authentication.

**Table 10-1  Card authenticator - error messages**

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong card</td>
<td>The card placed on the reader is incorrect.</td>
</tr>
<tr>
<td></td>
<td>Try again with another card or re-enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
<tr>
<td>Connect reader</td>
<td>The reader is not connected properly.</td>
</tr>
<tr>
<td></td>
<td>Try to connect it to a different USB slot and try again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for Card</td>
<td>You have not enrolled the card method.</td>
</tr>
<tr>
<td></td>
<td>You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
<tr>
<td>No template for Card</td>
<td>The card is not enrolled or you are trying to log in with the non-cached authenticator in the offline mode.</td>
</tr>
</tbody>
</table>

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

- When **Tap&Go** is disabled, you must place your card on the reader during login. After login you can remove the card from the reader to lock the operating system or log off automatically.
- When **Tap&Go** is enabled, you must tap a card on the reader to log in and to lock, unlock, or log off.

**Device Authentication**

You can authenticate to Windows workstation using the Device Authentication method using one of the following:

- Using Trusted Platform Module (TPM) chip
The TPM chip is a crypto-processor available in Windows workstation to achieve actions, such as generating, storing, and limiting the use of cryptographic keys. Device Authentication supports authentication to Windows workstation and makes use of information available in the chip to authenticate users.

- Non-TPM mode

In this mode, a key pair is generated in the workstation during the enrollment process that is used for further authentication on the same workstation.

**NOTE:** In non-TPM mode, ensure to enroll the Device Service method using the workstation where you would perform further authentication. Enrollment on one machine and authentication on another machine is not supported.

To authenticate with the Device Authentication method, perform the following steps:

1. Specify one of the following:
   - The TPM chip generated PIN
   - The enrolled PIN
2. Click Next.

   If the PIN matches with the TPM chip generated PIN or enrolled PIN, the Device Authentication is successful.

**Email OTP**

The Email OTP method enables you to authenticate using the one-time password (OTP) that is sent to the registered email address. When you try to authenticate on any device, the server sends an email to the registered email address with the OTP. You can use this OTP for single authentication within a short time frame.

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

1. Check your email. You will receive an email with an OTP.
2. Specify the OTP from Email in Password.
3. Click Next.

   If the OTP matches with the server generated OTP, the Email OTP authentication is successful.

The following table describes the possible error messages along with the workaround for the Email OTP authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong answer</td>
<td>The specified OTP is incorrect or is expired. Specify a valid OTP within the time frame.</td>
</tr>
</tbody>
</table>
Emergency Password

The Emergency Password method enables you to authenticate using a temporary password with the help of helpdesk administrator if you have lost a smart card or forgot your smart phone. The emergency password is valid for certain days and is set to 3 days by default. When you try to authenticate on any device, the submitted emergency password is compared with the enrolled password in the appliance. If the emergency passwords are identical, you are authenticated successfully.

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

1. Specify the Emergency Password.
2. Click Next.

   If the Emergency Password matches with the enrolled password, the Emergency Password authentication is successful.

The following table describes the possible error messages along with the workaround for the Emergency Password authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cannot send OTP. User does not have an email</td>
<td>Your email address is not set in the profile of the repository. Contact your system administrator to add your email address to the profile.</td>
</tr>
</tbody>
</table>

Facial Recognition

The Facial Recognition method enables you to get automatically authenticated by presenting your face. You need to register your facial image using the web camera. When you try to authenticate on an application, the recorded image is compared with the actual image. If the images match, you will be successfully authenticated.

The Facial Recognition method works with both integrated and external web cameras.
NOTE: To use the Facial Recognition method for authentication, you must install the Advanced Authentication Device Service. For more information about the Device Service, see the “Advanced Authentication - Device Service” guide.

To authenticate by using the Facial Recognition method, perform the following steps:

1. Ensure that a camera is connected to your device.
2. Present your face to the camera.
   If your face matches with the enrolled face, the face authentication is successful.

The following table describes the possible error messages along with the workaround for the Facial Recognition authentication.

Table 10-4  Facial Recognition authenticator - error messages

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed to open camera</td>
<td>The camera is not connected properly.</td>
</tr>
<tr>
<td></td>
<td>Check your camera settings and try again.</td>
</tr>
<tr>
<td>Mismatch</td>
<td>There is a mismatch in the faces.</td>
</tr>
<tr>
<td></td>
<td>You must present your face again for the authentication.</td>
</tr>
<tr>
<td>Face service is not available</td>
<td>Device Service is not available.</td>
</tr>
<tr>
<td></td>
<td>Ensure that the Device Service is connected.</td>
</tr>
</tbody>
</table>

Flex OTP

The Flex OTP authenticator facilitates you to authenticate by using your otp password from any of HOTP, TOTP and Smartphone (Offline) authenticator. When you try to authenticate to any device, the OTP in the token is compared with the OTP generated in any of HOTP, TOTP and Smartphone (Offline) authenticators. If the OTPs are valid, you are authenticated successfully.

To authenticate using the Flex OTP method, perform the following steps:

1. Specify the One-Time Password from any of HOTP, TOTP and Smartphone (Offline) authenticators
2. If the password is valid, the Flex OTP authentication is successful.

FIDO2

The FIDO2 method facilitates you to use any FIDO compliant device either in-built with the system or connected through USB to register and authenticate to the Windows workstation. When you try to authenticate, FIDO compliant device and user gesture, such as a tap on the token and swipe fingerprint on the reader are validated.
**NOTE:** To use the FIDO2 method for authentication, you must install the Advanced Authentication Device Service. For more information about the Device Service, see the Advanced Authentication - Device Service guide.

**NOTE:** To use the FIDO2 method for authentication, install the Advanced Authentication Device Service 6.3.60028 or newer version.

**To authenticate with the FIDO2 method, perform the following steps:**

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

1. Perform the action associated to the device.
   
   For example, if you use the FIDO2 device, connect it to the computer, set the pin, and touch the device when you see a flash.

**Fingerprint**

The Fingerprint method enables you authenticate using your finger print. The fingerprint scanner captures the fingerprint. When you try to authenticate on an application, the recorded fingerprint is compared with the actual fingerprint. If the fingerprints match, you are authenticated successfully.

**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.
   
   If the fingerprint matches with the enrolled fingerprint, the authentication is successful.

**NOTE:** Ensure to enroll the required fingers that are highlighted on the Add Fingerprint Authenticator page.

The following table describes the possible error messages along with the workaround for the Fingerprint authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Please connect a scanner</td>
<td>The reader is not connected properly. Ensure that the reader is properly connected or try to connect it to a different USB slot.</td>
</tr>
</tbody>
</table>
The HANIS (Home Affairs National Identification System) Face method is for the citizens of South Africa to authenticate with their personal identification number or passport number issued by Home Affairs National Identification System and face biometric. When you try to authenticate on any device, the presented face is matched with the enrolled face. If the images match, you are authenticated successfully.

Face is captured using both integrated and external web cameras.

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

To authenticate by using the HANIS Face method, perform the following steps:

1. Ensure that a camera is connected to your device.
2. Select the chain with HANIS Face method for authentication.
3. Present your face to the camera.
   - A message Detecting a face is displayed.
   - If your face matches with the enrolled face, the HANIS Face authentication is successful.

The following table describes the possible error messages along with the workaround for the HANIS Face authentication.

### Table 10-6 HANIS Face error messages

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mismatch</td>
<td>There might be a mismatch in the fingerprints. Ensure that you are using the same fingerprint that was enrolled and try to authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for Fingerprint</td>
<td>You have not enrolled for Fingerprint. You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
<tr>
<td>Capture Device cannot be opened</td>
<td>The camera is not connected properly. Check your camera settings and try again.</td>
</tr>
<tr>
<td>Timeout</td>
<td>The session has timed out. You must present your face again for the authentication.</td>
</tr>
</tbody>
</table>
HOTP

HOTP is a counter-based one-time password. This method enables you to authenticate using the counter-based one-time password generated on the HOTP token. The counter on the token must be in sync with the server. You can use generic HOTP tokens that adhere to RFC 4226. You can use the static secret key and three consequent OTP generated from the token to enroll. When you try to authenticate on any device, the OTP in the token is compared with the OTP generated in the server. If both OTPs are identical, you are authenticated successfully.

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

1. Specify the HOTP when using software token or connect the USB token, press button on the token.
2. Click Next.

If the OTP on the token and the server generated OTP are identical, the HOTP authentication is successful.

The following table describes the possible error messages along with the workaround for the HOTP authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong answer</td>
<td>The OTP you have provided is incorrect.</td>
</tr>
<tr>
<td></td>
<td>Specify a valid OTP and try again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for HOTP</td>
<td>You have not enrolled for the HOTP authenticator.</td>
</tr>
<tr>
<td></td>
<td>You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>

LDAP Password

The LDAP password method enables you to authenticate using the password of your corporate account. When you try to authenticate on any device, the specified password is compared with the actual password in the corporate directory. If the passwords match, you are authenticated successfully.

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

1. Specify your domain password.
2. Click Next.

If the LDAP Password matches with the password on the directory, the LDAP Password authentication is successful.

If the specified domain password is incorrect, an error message Invalid credentials is displayed. Specify a valid password and try to authenticate again.
Out-of-Band

The Out-of-band method facilitates you to authenticate using the push notification that is sent to the Out-of-band portal or OOB agent. When you initiate the authentication, a push notification is sent to the portal or agent. You can accept the request and get authenticated.

To authenticate by using the Out-of-band method, perform the following steps:

When you specify the chain number corresponding to the Out-of-band method, a message Continue at https://<AdvancedAuthenticationServerdomainname>/oob/ui is displayed on your computer.

1 Open the OOB agent installed on your mobile or navigate to the OOB portal.
   A push notification is displayed.

   **NOTE:** If the push notification does not appear after 5 seconds, tap the Refresh icon to view the push notification for the initiated authentication.

2 Tap Accept.
   If the response to authentication request is from a secured origin, the authentication is successful.

Password

The Password method enables you to authenticate using a secret string. The enrolled password is stored locally in the Advanced Authentication. When you try to authenticate on any device, the specified password is compared with the actual password. If the passwords are identical, you are authenticated successfully.

To authenticate using the Password method, perform the following steps:

1 Specify the password of your Advanced Authentication account.
2 Click Next.
   If the password matches with the enrolled password, the Password authentication is successful.

The following table describes the possible error messages along with the workaround for the Password authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong password</td>
<td>The password you have specified is incorrect. Specify a valid password and try to authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for Password</td>
<td>You have not enrolled for the Password authenticator. You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>
The PKI method enables you to authenticate using any PKI device such as a contact card or USB token that contains the digital certificate. The PKI reader validates the digital certificate and the identity of users. When you try to authenticate on an application, the certificate in the device is compared with the actual certificate. If the certificates match, you are authenticated successfully.

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

To authenticate using the PKI method, perform the following steps:

1. Insert a card or plug the token to your machine.
2. Specify the PIN.

   If the digital certificate in the card or token and enrolled certificate are identical, the PKI authentication is successful.

**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.

The following table describes the possible error messages along with the workaround for the PKI authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong card</td>
<td>The card you have used for authentication is incorrect. Try authenticating with another valid card or token. Enroll the authenticator again in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
<tr>
<td>Present card</td>
<td>The PKI device is not connected properly. Try to connect it to a different USB slot and authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for PKI</td>
<td>You have not enrolled for the PKI authenticator. You must enroll the authenticator in the Self-Service portal or contact the helpdesk administrator.</td>
</tr>
<tr>
<td>No template for Card</td>
<td>The card is not enrolled or you are trying to log in with the non-cached authenticator in the offline mode.</td>
</tr>
</tbody>
</table>

**NOTE:** To log in to a computer using the PKI authenticator, you must place the card on the reader or connect token to the computer. After log in, you can remove the card from the reader or disconnect token to lock the computer automatically.
Advanced Authentication does not support the tapping of a card to lock or unlock a computer.

**RADIUS Client**

The RADIUS Client method enables Advanced Authentication to forward the authentication request to a third-party RADIUS server. This can be any RADIUS server.

For example, you can use RADIUS Client as an authentication method for token solutions such as RSA or Vasco.

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

1. Specify the RADIUS password.
2. Click Next.

If you get an error **Wrong answer**, it could be an incorrect RADIUS password.

**Security Questions**

Security Questions method enables you to enroll answers to a pre-defined set of security questions. When you authenticate using security questions, Advanced Authentication prompts you the configured security questions or a subset of the security questions. You must answer the appropriate questions and based on the correctness of the answers, you are authenticated successfully.

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

1. Specify the answer for the security question.
2. Click Next.
3. Repeat steps 1 to 2 for all the required security questions.

The following table describes the possible error messages along with the workaround for the Security Questions authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Wrong answer</strong></td>
<td>The answer that you have provided is incorrect. Specify the correct answer and try to authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for TOTP</td>
<td>You have not enrolled the Security Questions method. You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>
Smartphone

The Smartphone method facilitates you to enroll and authenticate using the smartphone app. When you initiate the authentication, a push notification is sent to the app. You can accept the request and get authenticated.

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

1. Open the smartphone app.
   Ensure that you have the internet connection on your phone.
2. Accept the authentication request.

To authenticate with the Smartphone method using the offline authentication, perform the following steps:

1. Open the Advanced Authentication smartphone app.
2. Click Enrolled Authenticators from Menu in the smartphone app.
3. Specify the OTP from the smartphone app in Password.
4. Click Next.
   If the OTP on the smartphone app matches with server generated OTP, the authentication is successful.

The following table describes the possible error messages along with the workaround for the Smartphone authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth rejected</td>
<td>You have declined the authentication request.</td>
</tr>
<tr>
<td>Wrong TOTP password</td>
<td>You are using offline authentication and specified an incorrect TOTP password, or the time on your smartphone is not synchronized.</td>
</tr>
<tr>
<td>TOTP login is disabled</td>
<td>You are using offline authentication and Geo-fencing is enabled.</td>
</tr>
<tr>
<td></td>
<td>Contact the administrator for further assistance.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for smartphone</td>
<td>You have not enrolled the smartphone method.</td>
</tr>
<tr>
<td></td>
<td>You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>

SMS OTP

The SMS OTP method facilitates you to generate a single-use password or OTP and send it to the registered mobile number for authentication. You can use this OTP to authenticate within a short time frame.
NOTE: The OTP period is set to 120 seconds by default. An administrator has the privilege to change the OTP period.

To perform authentication using the SMS OTP method, perform the following steps:

1. You will receive an SMS message with an OTP on your phone.
2. Specify 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 profile of the repository.

Swisscom Mobile ID

The Swisscom Mobile ID authentication method uses the phone number from your profile of the repository. The authenticator sends an authentication request to your mobile phone. You need to accept it.

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

1. Check your mobile phone.
   
   A request message is displayed on your mobile phone.
2. Accept the request.
   
   If the Mobile ID matches with the enrolled Mobile ID, the Swisscom Mobile ID authentication is successful.

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

TOTP

The TOTP method enables you to authenticate using the time-based-one-time password. TOTP is generated on the hardware token or the mobile app, such as NetIQ Advanced Authentication app or Google Authenticator app. The TOTP is valid for a short duration. This method uses a predefined period. The default value is 30 seconds.

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

1. Specify the TOTP from your hardware or software token.
2. Click Next.
   
   If the OTP on the token matches with the server generated OTP, the TOTP authentication is successful.

The following table describes the possible error messages along with the workaround for the TOTP authentication.
This authentication method facilitates you to connect the FIDO U2F compliant token to the computer or laptop and touch the flashing token for authentication. When you try to authenticate on any device, token connected to the device is compared with the enrolled token. If the token details match, you are authenticated successfully.

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

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

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

A message Please touch the flashing U2F device now is displayed.

1. You will be able to view a blink on the token. Touch the token’s button. If the token does not blink, reconnect your token.

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

The following table describes the possible error messages along with the workaround for the FIDO U2F authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong answer</td>
<td>The OTP that you have specified is incorrect.</td>
</tr>
<tr>
<td></td>
<td>Specify a valid OTP and try to authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for TOTP</td>
<td>You have not enrolled for the TOTP authenticator.</td>
</tr>
<tr>
<td></td>
<td>You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong token.Try another one</td>
<td>The token is incorrect.</td>
</tr>
<tr>
<td></td>
<td>Repeat with another token, or re-enroll the authenticator in the Self-Service portal, or contact the helpdesk administrator.</td>
</tr>
<tr>
<td>Connect a token</td>
<td>Ensure that the token is connected to the workstation.</td>
</tr>
</tbody>
</table>
Voice

The Voice method initiates a call to your registered phone number. The phone call requests you to specify the PIN in the dial pad of your mobile to authenticate. When you try to authenticate on any device, the recorded PIN is compared with the actual PIN. If both PINs are identical, you are authenticated successfully.

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

1. Answer the phone call on your phone and listen to the request.
2. Specify your PIN code followed by the hash symbol (#) in the dial pad of your mobile phone.

If the PIN matches with enrolled PIN, the Voice authentication is successful.

Voice OTP

The Voice OTP method enables you to authenticate using the OTP that is sent through the phone call to your registered phone number. You can use this OTP for authentication within a short time frame. When you try to authenticate on any device, the specified OTP is compared with the OTP generated on the server. If both the OTPs are identical, you are authenticated successfully.

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

1. Answer the phone call on your phone and listen to the voice OTP.
2. Specify the OTP in **Password**.
3. Click **Next**.

If the OTP matches with the server generated OTP, the Voice OTP authentication is successful.

Windows Hello

The Windows Hello method facilitates you to use your Windows Hello fingerprint, facial recognition authentication and PIN to log in to Windows 10 operating system. Advanced Authentication supports the Windows Hello fingerprint, facial recognition and PIN.
To authenticate using the Windows Hello, perform the following steps:

1 **For fingerprint authentication**: Ensure that a fingerprint reader is connected to the required device.
   
   1a Place your enrolled finger on the reader when using a touch sensor or swipe your finger when using a swipe sensor.

   If the fingerprint matches with the fingerprint enrolled on Windows 10 operating system, Windows Hello authentication is successful.

2 **For facial recognition**: Ensure that an external camera is connected to your computer.

   **NOTE**: This method supports all the devices that Windows Hello works with. For example, the Windows Hello facial recognition works with only the infrared cameras. Therefore, the Advanced Authentication Windows Hello method also supports only the infrared camera for facial recognition.

   2a Present your face to the camera.

   If the face matches with the facial image enrolled on Windows 10 operating system, Windows Hello authentication is successful.
Logging In to Virtual Desktop Authentication Agent

The Virtual Desktop Authentication (VDA) agent allows you to perform multi-factor authentication and get authorized access to the following desktop virtualization client softwares where you can access applicable remote computer or application:

- VMware Horizon (formerly known as VMware View)
- Microsoft Remote Desktop
- Citrix XenApp or XenDesktop

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

1. In command prompt, run one of the following command as per your requirement:
   - To launch VDA Profiles List window:
     ```
     cd C:/Program Files\NetIQ\Virtual Desktop Authentication
     AAA.VDA.Shell.exe/showProfiles
     ```
   - To launch the default VDA profile:
     ```
     cd C:/Program Files\NetIQ\Virtual Desktop Authentication\AAA.VDA.Shell.exe
     ```

2. Select the preferred profile and click OK.
The authentication window appears.

3. Specify the user name and select an authentication chain from the list.

4. Authenticate with all authentication method(s) of the chain.
   A prompt to select category might appear, if you have enrolled an authenticator for more than one category.

The VDA agent supports in-line enrollment of Card and Password method. For more information, see In-Line Enrollment.

Advanced Authentication provides the following authenticators for logging in to VDA agent:

- “Bluetooth” on page 210
- “Card” on page 211
- “Email OTP” on page 213
- “Emergency Password” on page 213
- “Facial Recognition” on page 214
- “Fingerprint” on page 215
- “HOTP” on page 215
- “LDAP Password” on page 216
- “Password” on page 216
Bluetooth

The Bluetooth method enables you to authenticate using any Bluetooth enabled device that is within the range. When you initiate authentication, the Advanced Authentication server searches for the enrolled Bluetooth device. If the enrolled device is within the range, you are authenticated successfully.

For example, Susanne, who is a doctor, attends many in-patients in the hospital. She accesses the computer located in each room to monitor and update the health status of the patient. In this case, Susanne can specify her first-factor authentication details and use her Bluetooth enabled mobile phone to log in to the computer automatically when she is within range of a particular room. When she exits the room, she is logged out of that computer automatically.

**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 using the Bluetooth method, perform the following steps:**

1. Ensure that Bluetooth is turned on in your device and is discoverable to the paired devices.
2. The Device Service detects your Bluetooth device and authenticates.
   If the paired Bluetooth device is within the range, the Bluetooth authentication is successful.

**NOTE:** If the administrator has set Enable reaction on device removal option to ON for Bluetooth method then the operating system automatically locks, if one of the following is true:

- The Bluetooth device is disabled.
- The Bluetooth device is out of range.
Card

The Card method enables you to authenticate using the contactless smart card (with Card Serial Number). When you try to authenticate on any device, the recorded serial number of the card is compared with the actual serial number. If the card serial numbers are identical, you are authenticated successfully.

**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 in the reader.
   - If the Card Serial Number in the card matches with enrolled card, the card authentication is successful.

**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.

The following table describes the possible error messages along with the workaround for the Card authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong card</td>
<td>The card placed on the reader is incorrect. Try again with another card or re-enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
<tr>
<td>Connect reader</td>
<td>The reader is not connected properly. Try to connect it to a different USB slot and try again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for Card</td>
<td>You have not enrolled the card method. You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
<tr>
<td>No template for Card</td>
<td>The card is not enrolled or you are trying to log in with the non-cached authenticator in the offline mode.</td>
</tr>
</tbody>
</table>
IMPORTANT: An administrator can configure an automatic session lock or log off on card events. In such a scenario, you must perform one of the following:

- When Tap&Go is disabled, you must place your card on the reader during login. After login you can remove the card from the reader to lock the operating system or log off automatically.
- When Tap&Go is enabled, you must tap a card on the reader to log in and to lock, unlock, or log off.

In-Line Enrollment

You can enroll the Card and Password authentication methods using the VDA agent and associate the enrolled methods to your account without logging in to the Self-Service portal. However, enrolled methods are listed under the Enrolled Authenticators section of Self-Service portal. The VDA agent supports in-line enrollment for the Card and Password methods when the methods are in the same chain.

To enroll the Card and Password methods using the VDA agent, perform the following steps:

1. In command prompt, run one of the following command as per your requirement:
   - To launch VDA Profiles List window:
     ```
     cd C:/Program Files\NetIQ\Virtual Desktop Authentication
     AAA.VDA.Shell.exe/showProfiles
     ```
   - To launch the default VDA profile:
     ```
     AAA.VDA.Shell.exe
     ```
2. (Conditional) If you have launched VDA Profiles List, select the preferred profile from the list. The VDA Authentication window appears.
3. Tap the card on the card reader.
   A message The card is not found. Do you want to enroll it? is displayed.
4. Click Yes to enroll the presented card.
5. Specify your user name and click Next.
6. Specify the LDAP password and click Next.
   A message Card is enrolled is displayed. The presented card is enrolled for your account.
7. Specify the password and confirm it then click Next.
   A message The Password is not found. Do you want to enroll it? is displayed.
8. Click Yes to enroll the specified password.
   A message Password is enrolled is displayed. The Password method is enrolled for your account.
Email OTP

The Email OTP method enables you to authenticate using the one-time password (OTP) that is sent to the registered email address. When you try to authenticate on any device, the server sends an email to the registered email address with the OTP. You can use this OTP for single authentication within a short time frame.

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

1. Check your email. You will receive an email with an OTP.
2. Specify the OTP from Email in Password.
3. Click Next.

If the OTP matches with the server generated OTP, the Email OTP authentication is successful.

The following table describes the possible error messages along with the workaround for the Email OTP authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong answer</td>
<td>The specified OTP is incorrect or is expired.</td>
</tr>
<tr>
<td></td>
<td>Specify a valid OTP within the time frame.</td>
</tr>
<tr>
<td>Cannot send OTP. User does not have an email</td>
<td>Your email address is not set in the profile of the repository.</td>
</tr>
<tr>
<td></td>
<td>Contact your system administrator to add your email address to the profile.</td>
</tr>
</tbody>
</table>

Emergency Password

The Emergency Password method enables you to authenticate using a temporary password with the help of helpdesk administrator if you have lost a smart card or forgot your smart phone. The emergency password is valid for certain days and is set to 3 days by default. When you try to authenticate on any device, the submitted emergency password is compared with the enrolled password in the appliance. If the emergency passwords are identical, you are authenticated successfully.

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

1. Specify the Emergency Password.
2. Click Next.

If the Emergency Password matches with the enrolled password, the Emergency Password authentication is successful.

The following table describes the possible error messages along with the workaround for the Emergency Password authentication.
Facial Recognition

The Facial Recognition method enables you to get automatically authenticated by presenting your face. You need to register your facial image using the web camera. When you try to authenticate on an application, the recorded image is compared with the actual image. If the images match, you will be successfully authenticated.

The Facial Recognition method works with both integrated and external web cameras.

**NOTE:** To use the Facial Recognition method for authentication, you must install the Advanced Authentication Device Service. For more information about the Device Service, see the “Advanced Authentication - Device Service” guide.

To authenticate by using the Facial Recognition method, perform the following steps:

1. Ensure that a camera is connected to your device.
2. Present your face to the camera.

   If your face matches with the enrolled face, the face authentication is successful.

The following table describes the possible error messages along with the workaround for the Facial Recognition authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong password</td>
<td>The specified emergency password is incorrect. Specify a valid emergency password and try to authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for Emergency Password</td>
<td>You have not enrolled for Emergency Password method. Enroll the authenticator on the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
<tr>
<td>Failed to open camera</td>
<td>The camera is not connected properly. Check your camera settings and try again.</td>
</tr>
<tr>
<td>Mismatch</td>
<td>There is a mismatch in the faces. You must present your face again for the authentication.</td>
</tr>
<tr>
<td>Face service is not available</td>
<td>Device Service is not available. Ensure that the Device Service is connected.</td>
</tr>
</tbody>
</table>
Fingerprint

The Fingerprint method enables you authenticate using your finger print. The fingerprint scanner captures the fingerprint. When you try to authenticate on an application, the recorded fingerprint is compared with the actual fingerprint. If the fingerprints match, you are authenticated successfully.

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.
   If the fingerprint matches with the enrolled fingerprint, the authentication is successful.

NOTE: Ensure to enroll the required fingers that are highlighted on the Add Fingerprint Authenticator page.

The following table describes the possible error messages along with the workaround for the Fingerprint authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
</table>
| Please connect a scanner | The reader is not connected properly.  
Ensure that the reader is properly connected or try to connect it to a different USB slot. |
| Mismatch | There might be a mismatch in the fingerprints.  
Ensure that you are using the same fingerprint that was enrolled and try to authenticate again. |
| <Your user name> has no authenticator for Fingerprint | You have not enrolled for Fingerprint.  
You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator. |

HOTP

HOTP is a counter-based one-time password. This method enables you to authenticate using the counter-based one-time password generated on the HOTP token. The counter on the token must be in sync with the server. You can use generic HOTP tokens that adhere to RFC 4226. You can use the static secret key and three consequent OTP generated from the token to enroll. When you try to authenticate on any device, the OTP in the token is compared with the OTP generated in the server. If both OTPs are identical, you are authenticated successfully.
To authenticate using the HOTP method, perform the following steps:

1. Specify the HOTP when using software token or connect the USB token, press button on the token.
2. Click Next.

If the OTP on the token and the server generated OTP are identical, the HOTP authentication is successful.

The following table describes the possible error messages along with the workaround for the HOTP authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong answer</td>
<td>The OTP you have provided is incorrect. Specify a valid OTP and try again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for HOTP</td>
<td>You have not enrolled for the HOTP authenticator. You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>

**LDAP Password**

The LDAP password method enables you to authenticate using the password of your corporate account. When you try to authenticate on any device, the specified password is compared with the actual password in the corporate directory. If the passwords match, you are authenticated successfully.

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

1. Specify your domain password.
2. Click Next.

If the LDAP Password matches with the password on the directory, the LDAP Password authentication is successful.

If the specified domain password is incorrect, an error message **Invalid credentials** is displayed. Specify a valid password and try to authenticate again.

**Password**

The Password method enables you to authenticate using a secret string. The enrolled password is stored locally in the Advanced Authentication. When you try to authenticate on any device, the specified password is compared with the actual password. If the passwords are identical, you are authenticated successfully.

To authenticate using the Password method, perform the following steps:

1. Specify the password of your Advanced Authentication account.
2 Click Next.

If the password matches with the enrolled password, the Password authentication is successful.

The following table describes the possible error messages along with the workaround for the Password authentication.

Table 11-7 Password authenticator - error messages

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong password</td>
<td>The password you have specified is incorrect. Specify a valid password and try to authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for Password</td>
<td>You have not enrolled for the Password authenticator. You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>

PKI

The PKI method enables you to authenticate using any PKI device such as a contact card or USB token that contains the digital certificate. The PKI reader validates the digital certificate and the identity of users. When you try to authenticate on an application, the certificate in the device is compared with the actual certificate. If the certificates match, you are authenticated successfully.

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

To authenticate using the PKI method, perform the following steps:

1. Insert a card or plug the token to your machine.
2. Specify the PIN.
   - If the digital certificate in the card or token and enrolled certificate are identical, the PKI authentication is successful.

**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.

The following table describes the possible error messages along with the workaround for the PKI authentication.
### Table 11-8  PKI authenticator - error messages

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong card</td>
<td>The card you have used for authentication is incorrect. Try authenticating with another valid card or token. Enroll the authenticator again in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
<tr>
<td>Present card</td>
<td>The PKI device is not connected properly. Try to connect it to a different USB slot and authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for PKI</td>
<td>You have not enrolled for the PKI authenticator. You must enroll the authenticator in the Self-Service portal or contact the helpdesk administrator.</td>
</tr>
<tr>
<td>No template for Card</td>
<td>The card is not enrolled or you are trying to log in with the non-cached authenticator in the offline mode.</td>
</tr>
</tbody>
</table>

**NOTE:** To log in to a computer using the PKI authenticator, you must place the card on the reader or connect token to the computer. After log in, you can remove the card from the reader or disconnect token to lock the computer automatically.

Advanced Authentication does not support the tapping of a card to lock or unlock a computer.

### RADIUS Client

The RADIUS Client method enables Advanced Authentication to forward the authentication request to a third-party RADIUS server. This can be any RADIUS server.

For example, you can use RADIUS Client as an authentication method for token solutions such as RSA or Vasco.

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

1. Specify the RADIUS password.
2. Click Next.

If you get an error Wrong answer, it could be an incorrect RADIUS password.

### Security Questions

Security Questions method enables you to enroll answers to a pre-defined set of security questions. When you authenticate using security questions, Advanced Authentication prompts you the configured security questions or a subset of the security questions. You must answer the appropriate questions and based on the correctness of the answers, you are authenticated successfully.
To authenticate using the Security Questions method, perform the following steps:

1. Specify the answer for the security question.
2. Click Next.
3. Repeat steps 1 to 2 for all the required security questions.

The following table describes the possible error messages along with the workaround for the Security Questions authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong answer</td>
<td>The answer that you have provided is incorrect. Specify the correct answer and try to authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for TOTP</td>
<td>You have not enrolled the Security Questions method. You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>

**Smartphone**

The Smartphone method facilitates you to enroll and authenticate using the smartphone app. When you initiate the authentication, a push notification is sent to the app. You can accept the request and get authenticated.

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

1. Open the smartphone app.
   Ensure that you have the internet connection on your phone.
2. Accept the authentication request.

To authenticate with the Smartphone method using the offline authentication, perform the following steps:

1. Open the Advanced Authentication smartphone app.
2. Click Enrolled Authenticators from Menu in the smartphone app.
3. Specify the OTP from the smartphone app in Password.
4. Click Next.
   If the OTP on the smartphone app matches with server generated OTP, the authentication is successful.

The following table describes the possible error messages along with the workaround for the Smartphone authentication.
### SMS OTP

The SMS OTP method facilitates you to generate a single-use password or OTP and send it to the registered mobile number for authentication. You can use this OTP to authenticate within a short time frame.

**NOTE:** The OTP period is set to 120 seconds by default. An administrator has the privilege to change the OTP period.

To perform authentication using the SMS OTP method, perform the following steps:

1. You will receive an SMS message with an OTP on your phone.
2. Specify 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 profile of the repository.

### Swisscom Mobile ID

The Swisscom Mobile ID authentication method uses the phone number from your profile of the repository. The authenticator sends an authentication request to your mobile phone. You need to accept it.

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

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

   If the Mobile ID matches with the enrolled Mobile ID, the Swisscom Mobile ID authentication is successful.
**NOTE:** To authenticate with the Swisscom Mobile ID authenticator, you must activate the Mobile ID service of your Swisscom SIM card.

### TOTP

The TOTP method enables you to authenticate using the time-based-one-time password. TOTP is generated on the hardware token or the mobile app, such as NetIQ Advanced Authentication app or Google Authenticator app. The TOTP is valid for a short duration. This method uses a predefined period. The default value is 30 seconds.

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

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

   If the OTP on the token matches with the server generated OTP, the TOTP authentication is successful.

The following table describes the possible error messages along with the workaround for the TOTP authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong answer</td>
<td>The OTP that you have specified is incorrect. Specify a valid OTP and try to authenticate again.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for TOTP</td>
<td>You have not enrolled for the TOTP authenticator. You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>

### FIDO U2F

This authentication method facilitates you to connect the FIDO U2F compliant token to the computer or laptop and touch the flashing token for authentication. When you try to authenticate on any device, token connected to the device is compared with the enrolled token. If the token details match, you are authenticated successfully.

**TIP:** To use the FIDO U2F method for authentication, you must install the Advanced Authentication Device Service. For more information about the Device Service, see the “Advanced Authentication - Device Service” guide.
To authenticate with the FIDO U2F method, perform the following steps:

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

A message Please touch the flashing U2F device now is displayed.

1. You will be able to view a blink on the token. Touch the token’s button. If the token does not blink, reconnect your token.

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

The following table describes the possible error messages along with the workaround for the FIDO U2F authentication.

<table>
<thead>
<tr>
<th>Error</th>
<th>Possible Cause and Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wrong token. Try another one</td>
<td>The token is incorrect.</td>
</tr>
<tr>
<td>Connect a token</td>
<td>Ensure that the token is connected to the workstation.</td>
</tr>
<tr>
<td>&lt;Your user name&gt; has no authenticator for U2F</td>
<td>You have not enrolled for the FIDO U2F authenticator. You must enroll the authenticator in the Self-Service portal or contact your helpdesk administrator.</td>
</tr>
</tbody>
</table>

**Voice**

The Voice method initiates a call to your registered phone number. The phone call requests you to specify the PIN in the dial pad of your mobile to authenticate. When you try to authenticate on any device, the recorded PIN is compared with the actual PIN. If both PINs are identical, you are authenticated successfully.

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

1. Answer the phone call on your phone and listen to the request.
2. Specify your PIN code followed by the hash symbol (#) in the dial pad of your mobile phone.

   If the PIN matches with enrolled PIN, the Voice authentication is successful.
Voice OTP

The Voice OTP method enables you to authenticate using the OTP that is sent through the phone call to your registered phone number. You can use this OTP for authentication within a short time frame. When you try to authenticate on any device, the specified OTP is compared with the OTP generated on the server. If both the OTPs are identical, you are authenticated successfully.

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

1. Answer the phone call on your phone and listen to the voice OTP.
2. Specify the OTP in Password.
3. Click Next.

If the OTP matches with the server generated OTP, the Voice OTP authentication is successful.

Windows Hello

The Windows Hello method facilitates you to use your Windows Hello fingerprint and facial recognition authentication to log in to Windows 10 operating system. Advanced Authentication supports the Windows Hello fingerprint and facial recognition.

To authenticate using the Windows Hello, perform the following steps:

1. For fingerprint authentication: Ensure that a fingerprint reader is connected to the required device.
   1a. Place your enrolled finger on the reader when using a touch sensor or swipe your finger when using a swipe sensor.
   
   If the fingerprint matches with the fingerprint enrolled on Windows 10 operating system, Windows Hello authentication is successful.
2. For facial recognition: Ensure that an external camera is connected to your computer.
   
   NOTE: This method supports all the devices that Windows Hello works with. For example, the Windows Hello facial recognition works with only the infrared cameras. Therefore, the Advanced Authentication Windows Hello method also supports only the infrared camera for facial recognition.
   
   2a. Present your face to the camera.

   If the face matches with the facial image enrolled on Windows 10 operating system, Windows Hello authentication is successful.