MOBILE SINGLE SIGN-ON FOR SAP FIORI USING SAP AUTHENTICATOR

TABLE OF CONTENTS
MOBILE SINGLE SIGN-ON FOR SAP FIORI ................................................................. 2
HOW THE MOBILE SINGLE SIGN-ON FOR SAP FIORI WORKS ........................................ 3
STEP-BY-STEP IMPLEMENTATION OF THE MOBILE SINGLE SIGN-ON FOR SAP FIORI ........ 4
1. SAML 2.0 IDENTITY PROVIDER SETUP ................................................................. 4
2. ONE-TIME PASSWORD AUTHENTICATION SETUP FOR SAML 2.0 IDENTITY PROVIDER .... 8
3. ADD TRUSTED SERVICE PROVIDER FOR THE SAML 2.0 IDENTITY PROVIDER .......... 11
4. CONFIGURE TWO-FACTOR AUTHENTICATION FOR MOBILE SSO ......................... 16
5. CONFIGURE CORPORATE SETTINGS FOR ONLINE ACCOUNT SETUP .................... 17
6. ADMINISTRATIVE ONLINE DEVICE ACTIVATION ON BEHALF OF THE END USER & SAP FIORI CLIENT CONFIGURATION .................................................................................. 19
7. MOBILE DEVICE SETUP: A USER SELF-SERVICE .................................................... 26
   7.1 INSTALL SAP AUTHENTICATOR MOBILE APPLICATION ........................................ 26
   7.2 ONLINE ACCOUNT SETUP BY THE USER ................................................................ 29
   7.3 MOBILE DEVICE SETUP ....................................................................................... 33
MOBILE SINGLE SIGN-ON FOR SAP FIORI

Mobile Single Sign-On (SSO) has been available with SAP Single Sign-On 2.0 since SP04. Initially the Mobile SSO was available only for SAP Fiori via the browser and other browser-based or hybrid mobile applications.

Now with the latest support package (SP06) of SAP Single Sign-On 2.0 and with the latest releases of SAP Fiori Client 1.5.0 (both released in October 2015), the native mobile SAP Fiori application is integrated and working out of the box with the SAP Authenticator application.

This document is a new version of the step-by-step guide on Mobile SSO, released early this year. In this guide, you will be able to find configuration steps about the following:

- How to enable Mobile Single Sign-On for SAP Fiori Client using SAP Authenticator
- How to enable Mobile Single Sign-On for SAP Fiori via the browser using SAP Authenticator (available also with the first version of this document)
- Configuration of the corporate settings for Online Account Setup via the OTP administrative user interfaces and how administrators can set up the SAP Authenticator on behalf of the end users (new features available with SAP Single Sign-On 2.0 SP6)
- How to set up SAP Authenticator using the user self-service for Online Account Setup (new feature available with SAP Single Sign-On 2.0 SP6)
- How to set up SAP Authenticator using the self-service for Mobile Device Setup (available also with the first version of this document)

The Mobile SSO solution is based on the Time-based One-Time Password (TOTP) Algorithm of the open standard RFC 6238. This algorithm computes a one-time passcode from a shared secret key and a current time. The server side of the TOTP implementation is an add-on module for SAP NetWeaver Application Server (AS) for Java and it is part of the SAP Single Sign-On 2.0 product. The TOTP Server is taking care of the mobile devices activation and deactivation on user level and the administration of the TOTPLoginModule per application.

SAP Authenticator is the mobile application for the TOTP Client and it is available for iOS and Android platforms. The solution requires a SAML 2.0 Identity Provider, configured to accept authentication with Time-Based One-Time Passwords. The authentication to the Identity Provider, with the respective username and passcode, triggers IDP-INITIATED SINGLE SIGN-ON mechanism.

Figure 1

Just ONE click on the link “Log On with SAP Authenticator”

Just ONE click on the respective Fiori bookmark
HOW THE MOBILE SINGLE SIGN-ON FOR SAP FIORI WORKS

Mobile SSO for the native SAP Fiori Client:
When this solution is implemented, SAP Fiori users will be able to use the Mobile SSO for SAP Fiori Client in two ways: by directly starting the SAP Fiori Client on the mobile devices and clicking the link “Log On with SAP Authenticator” or by a simple click on the SAP Fiori Client bookmark via the SAP Authenticator. See Figure 1 above.

Starting the SAP Fiori Client, by using one of these two ways, will trigger the authentication process. The SAP Authenticator generates a new passcode and sends it together with the username to the SAP Fiori Client using the parameters in the pre-configured SAP Fiori Client URL. SAP Fiori Client, on its side, opens the URL and an authentication request is sent to the SAP Identity Provider triggering the IDP-initiated single sign-on. The Identity Provider checks the credentials provided, and if the check is successful, the Identity Provider issues a SAML 2.0 assertion for this user and for the respective service provider (SAP Fiori) and SAP Fiori Client is securely opened for the user. See Figure 2 below:

Mobile SSO for SAP Fiori via the browser:
Once such solution is implemented, SAP Fiori users will be able to use SAP Fiori applications on their devices after a single click on a bookmark for SAP Fiori available in the SAP Authenticator.

When the user clicks on the respective SAP Fiori application bookmark, the SAP Authenticator generates a passcode and creates a URL with the respective parameters (service provider, RelayState, username and passcode) similar to this example: https://idp_host/saml2/idp/sso?saml2sp=fiori_sp&RelayState=fiori&j_username=[username]&j_password=[passcode]. SAP Authenticator sends this URL to the browser and then the browser opens the URL, triggering IDP-initiated single sign-on. The Identity Provider, on its side, checks the credentials provided, and if the check is successful, issues a SAML 2.0 assertion for this user and for the respective service provider (SAP Fiori in our example). On the next step, based on the HTTP-POST binding response, the SAP Fiori application is securely opened on the mobile device of the user. See Figure 2 below:
STEP-BY-STEP IMPLEMENTATION OF THE MOBILE SINGLE SIGN-ON FOR SAP FIORI

1. SAML 2.0 IDENTITY PROVIDER SETUP

If you have SAML 2.0 Identity Provider (IdP) enabled on your SAP NetWeaver AS for Java, you can skip directly to ONE-TIME PASSWORD AUTHENTICATION SETUP FOR SAML2.0 IDENTITY PROVIDER and start with the creation of a custom authentication context for your IdP.

<table>
<thead>
<tr>
<th>Explanation</th>
<th>Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Log on to SAP NetWeaver Administrator at http://&lt;host&gt;:&lt;port&gt;/nwa</td>
<td><img src="image1.jpg" alt="Screenshot 1" /></td>
</tr>
<tr>
<td>2. Navigate to Configuration &gt; Authentication and Single Sign-On: SAML 2.0 &gt; SAML 2.0 and click “Enable SAML 2.0 Support”</td>
<td><img src="image2.jpg" alt="Screenshot 2" /></td>
</tr>
<tr>
<td>3. Configure the new SAML 2.0 Local Provider as an Identity Provider. Provide a name for the new identity provider and select “Identity Provider” as operational mode from the drop-down menu. Choose “Next”.</td>
<td><img src="image3.jpg" alt="Screenshot 3" /></td>
</tr>
</tbody>
</table>
4. Make sure the Keystore View is "SAML2" (If not, select it from the drop-down menu). Choose "Browse" for the Signing Key Pair

5. Choose "Create" for the Keystore Entry.

6. Provide **Entry Name**, check "Store Certificate" and choose "Next".
7. Provide value for the mandatory field "commonName" and choose "Next".

8. Only choose "Next" on this step.

9. Choose "Finish" to confirm the configuration.
10. Choose “OK” to select the new Signing Key Pair.

11. Choose “Next” on the SAML 2.0 Local Provider Configuration.

12. Choose “Finish” to finalize the configuration.
2. **ONE-TIME PASSWORD AUTHENTICATION SETUP FOR SAML 2.0 IDENTITY PROVIDER**

**Prerequisites:** You have SSO AUTHENTICATION LIBRARY 2.0 installed on SAP NetWeaver Application Server (AS) Java. For more details on the installation, see: **ONE-TIME PASSWORD AUTHENTICATION ADMINISTRATOR’S GUIDE > INSTALLATION**

<table>
<thead>
<tr>
<th>Explanation</th>
<th>Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1: Create a new authentication context and map it to the TOTPLLoginModule</strong></td>
<td><img src="image" alt="Screenshot" /></td>
</tr>
</tbody>
</table>

13. Navigate to SAML 2.0 Configuration > Local Provider and choose “Edit”.
14. Navigate to Authentication Contexts tab and choose “Add”.
15. Create a new Authentication Context by typing an Alias and a Name for it and choose “OK”.

16. Click on the check-box to select the HTTPS setting for the newly created Authentication Context and then choose “Save” for the Local Provider settings.
Step 2: Configure your Identity Provider to use the new authentication context by default for HTTPS Authentication

17. Navigate to Local Provider and choose “Edit”.
18. Go to tab Identity Provider Settings > Supported Authentication Contexts and choose “Add”.
19. Select your new authentication context from the drop-down menu with the alias values (the one created on step 15).
20. Select the Login Module from the drop-down menu to be the “TOTPLoginModule” and choose “OK”.

Set the new authentication context to be the default HTTPS authentication context

21. Go to section Supported Authentication Context and select the new authentication context. Choose “Copy to” and select “Default HTTPS Authentication Contexts” value.

22. Your new Supported Authentication Context will appear on the right side, in the list with Default HTTPS Authentication Contexts (see the screenshot).

23. Choose “Save” to finalize the configuration for your new Identity Provider.
Step 3: Configure Login Pages

Provided that the applications are added in SAP Authenticator, users can access them from their mobile devices through mobile SSO by choosing the “Log on with SAP Authenticator” link.

The URL for this link has the following format:
sapauthenticator://<host>:<port>/<path>?j_username=[username]&j_passcode=[passcode].

In order to configure such link to appear on the login page, you have to make sure that the proper alias /otp_logon_ui_resources is used. See more details here:
HTTP://HELP.SAP.COM/SAPHELP_NWSSO20/HELPDATA/EN/6f/027e3a29eb4002ae1ab4cf781b1940/CONTENT.HTM?FRAMESET=/EN/93/017269f30f4786b161fa72205c0e0e/FRAMESET.HTM&CURRENT_TOC=/en/f1/993b18f0425d864c3f79c14dbce3/plain.htm&NODE_ID=23

24. Navigate to Authentication tab -> Properties and choose “Modify”.

25. Go to Alias of Application for Customizing Login Pages (ume.logon.application.ui_resources_alias) and use the value /otp_logon_ui_resources and “Save”.

Note: This alias is coming with the implementation of the SSO AUTHENTICATION LIBRARY 2.0
3. **ADD TRUSTED SERVICE PROVIDER FOR THE SAML 2.0 IDENTITY PROVIDER**

<table>
<thead>
<tr>
<th>Explanation</th>
<th>Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1: Download Service Provider Metadata</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Prerequisite:** Make sure you have a Local Provider created and enabled on your SAP ABAP system. This identifies your server as a system that can accept SAML assertions. Add SAML 2.0 Identity Provider created in the first section as Trusted Identity Provider for your Service Provider (SAP Fiori). For more details how to setup, see [USING SAML 2.0 AUTHENTICATION TO ACCESS FIORI APPS FROM THE PUBLIC INTERNET](#).

In our example, the SAML 2.0 Service Provider of the SAP ABAP system is “gw_fiori_sp”. The Identity Provider Metadata, necessary for the setup of the Trusted Identity Provider on the SAP ABAP system, is available here:

- Start SAP NetWeaver Administrator at `http://< host > : < port >/nwa`.
- Navigate to `Configuration > Authentication and Single Sign-On: SAML 2.0 > SAML 2.0`, select Local Provider and choose Download Metadata.

26. Log on to SAP ABAP > **TCode SAML2** for SAML 2.0 Configuration. Navigate to Local Provider and choose “Metadata”.

27. Leave all checkbox selected (as it is by default) and choose “Download Metadata”. **Save** the `metadata.xml` file provided by the system in a custom folder. If you want later to recognize it easier, you can rename it to `SP_metadata.xml`.

| Step 2: Set up a RelayState on your SAP ABAP Service Provider for SAP Fiori Launchpad | |

The RelayState is a parameter in the URL, used by the browser to open the application. The RelayState parameter provides information about the path to the application. In our example, this path will be to the SAP FIORI LAUNCHPAD. If no RelayState parameter is provided in the URL, the “Default Application Path” from the IDP settings is used.

28. Choose “Edit” on the Local provider to add a new RelayState Mapping.
29. Go to the tab “Service provider Settings” > RelayState Mapping and choose “Add” for a new RelayState.

30. Provide the name for the RelayState and provide the Path to the RelayState. (In our case, this is the path to the “SAP Fiori Launchpad”.

31. Choose “Save” for the new settings of the Local Provider.

32. Navigate to “Trusted Providers” -> Select “Identity providers” -> select your Identity Provider and choose “Edit”.

33. Navigate to “Details of Identity Provider <your IDP>” -> “Endpoints” -> Show “Single Sign-On Endpoints” -> Configure for the HTTP Redirect Location URL the following callback schema:

   ?x-callback-scheme=com.sap.fiori.client.xc allbackurl
Step 4: Add Trusted Service Provider for Your SAML 2.0 Identity Provider

34. Go back to the SAP NetWeaver Administrator at http://<host>:<port>/nwa


36. Press “Choose File” and select the SP metadata (SP_metadata.xml) file stored in the custom folder on Step 25.

37. Once the file is selected, choose “Next”.
38. The system will display the name of your Service Provider. On this step just choose “Next”.

39. Leave the default settings on this step and choose “Next”.

40. Leave the default settings for the Assertion Consumer Endpoints and choose “Next”. Location URLs here will be displayed with your <host> and <port>.

41. Leave the default settings for the Single Logout Endpoints and choose “Next”. Location URLs here will be displayed with your <host> and <port>.

42. Leave the default settings for the Artifact Endpoints and choose “Next”. Location URL here will be displayed with your <host> and <port>.
43. Leave the default settings for the NameID Endpoints and choose “Finish” to complete the Trusted Service Provider configuration.

You have to activate the Trusted Service Provider, but first you have to add a supported NameID format.

44. Select your new Trusted Service Provider and choose “Edit”.

45. Go to the “Details of the trusted provider” > Identity Federation tab > choose “Add” for a new Supported Name ID Format.

46. Select from the drop-down menu the Format Name you plan to provide for the identity federation (in our case “Unspecified”).

47. Select from the drop-down menu the respective Source Name for the selected by you Format Name (in our case “Logon ID”).

48. Click “OK” to confirm the select the Name ID Format.

49. Choose “Save” to record the changes for this Trusted Service Provider.
4. CONFIGURE TWO-FACTOR AUTHENTICATION FOR MOBILE SSO

The Mobile SSO could be configured to use single-factor authentication or two-factor authentication. With the single-factor authentication the authentication from the mobile device will be based only on the passcode (TOTP) generated and sent by the SAP Authenticator. When single-factor authentication is configured, you can enable the setting “Require Two Passcodes” and the server side will expect two consecutive passcodes for logging (recommended). When this setting is disabled, the server will expect only one passcode.

When you decide to use two-factor authentication, you need to configure mandatory the setting “First Factor Login Module”. The default value of this setting is BasicPasswordLoginModule. You can also enable “Remember Client (Persistent Cookie)”. When it is enabled, a persistent cookie is issued at the user’s first login and this cookie is used to identify the client (browser) at next user logons. This cookie allows the user to use a single-factor authentication until the cookie expires or is revoked at the server side. In our example you will find the configuration required for two-factor authentication mode.

<table>
<thead>
<tr>
<th>Explanation</th>
<th>Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>50.</strong> Log on to OTP Administrative UI at http://&lt;host&gt;:&lt;port&gt;/otpadmin</td>
<td><img src="image1.png" alt="Screen 1" /></td>
</tr>
<tr>
<td><strong>51.</strong> Navigate to <strong>Settings</strong> and choose “Edit”.</td>
<td><img src="image2.png" alt="Screen 2" /></td>
</tr>
<tr>
<td><strong>52.</strong> Navigate to <strong>Two-Factor Authentication</strong> settings and enable “Remember Client (Persistent Cookie)” and “Require User Consent”. For more details see: <a href="HTTP://HELP.SAP.COM/SAPHELP_NWSSO20/HELPDATA/EN/93/017269F30F4786B161FA72205C0E0E/CONTENT.HTM">HTTP://HELP.SAP.COM/SAPHELP_NWSSO20/HELPDATA/EN/93/017269F30F4786B161FA72205C0E0E/CONTENT.HTM</a></td>
<td><img src="image3.png" alt="Screen 3" /></td>
</tr>
<tr>
<td><strong>53.</strong> Choose “Save” for the Settings.</td>
<td></td>
</tr>
</tbody>
</table>
5. CONFIGURE CORPORATE SETTINGS FOR ONLINE ACCOUNT SETUP

The latest support package (SP06) of the SAP Single Sign-On 2.0 offers a new capability for end users and administrators called **Online Account Setup**. To enable this new functionality, administrators need to configure corporate applications for Mobile Single Sign-On, using the OTP administrative UIs and to assign proper authorizations to end user accounts (the UME role **OTP_ONLINE_USER**). See more details in the documentation: HTTP://HELP.SAP.COM/SAPHELP_NWSSO20/HELPDATA/en/6f/027e3a29eb4002ae1a84cf781b1940/CONTENT.HTM?FRAMESET=/EN/93/017269f30f4786b161fa72205c0e0e/FRAMESET.HTM&CURRENT_TOC=/EN/f1/993b18f8e0425d864c3f79c14dbce3/PLAIN.HTM&NODE_ID=23

<table>
<thead>
<tr>
<th>Explanation</th>
<th>Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td>54. While you are in the OTP Administrative UI, navigate to <strong>Devices</strong> and choose “Edit”.</td>
<td><img src="image1" alt="One-Time Password Administration" /></td>
</tr>
<tr>
<td>55. Navigate to <strong>SAP Authenticator Application &gt; Applications</strong> and choose “Add”.</td>
<td><img src="image2" alt="SAP Authenticator Configuration" /></td>
</tr>
<tr>
<td>56. Configure <strong>SAP Fiori Client</strong>: Provide application name (example <strong>SAP Fiori Client</strong>) and the SAP Fiori URL.</td>
<td><img src="image3" alt="Add Application" /></td>
</tr>
<tr>
<td>![Optional] Choose “Add” again if you want to configure one more application before to save the new settings (for example access for SAP Fiori via the browser).</td>
<td><img src="image4" alt="SAP Authenticator Configuration" /></td>
</tr>
</tbody>
</table>
58. **[Optional] Configure SAP Fiori via the browser:**
Provide application name (example SAP Fiori Client) and the URL:
https://<IDP_host>/saml2/idp/sso?
spName=<SPname>&RelayState=<state>&username=<username>
&passcode=<passcode>
Use the example to build the proper URL using the host of your SAML IDP and the name of the trusted Service Provider configuration for your SAP Fiori system.

**NOTE!** You can use the same example for configuring the Online Activation for any browser-based application that needs to be enabled for Mobile SSO via the SAP Authenticator.

59. **[Optional]** You can also configure Groups (UME Groups) for managing the list of users who need to get an application pre-configured on their devices.

**NOTE!** For every application configured for Mobile SSO, administrators can specify members of what groups will get it configured on their mobile device when Online Account Activation is used. The groups that administrators can add with the Edit Groups button are the ones in the user management engine (UME) of the AS JAVA. If no Groups are assigned, the application will be pre-configured for every user, whose device is enrolled using the Online Account Setup feature via the self-service or by an administrator.

60. Choose “Save”. This will save the SAP Authenticator Configuration.

**Assign the OTP_ONLINE_USER UME role to all users, who need to use Online Account Activation as self-service.**

61. Open the UME Administration HTTPS://<HOST>/WEBDYNPRO/DSPPATCHE/SAP.COM/TC~SEC~UME~WD~UMEADMIN/UMEADMINAPP#
62. Find the respective users and assign to them the role **OTP_ONLINE_USER**.
6. ADMINISTRATIVE ONLINE DEVICE ACTIVATION ON BEHALF OF THE END USER & SAP FIORI CLIENT CONFIGURATION

With the latest support package (SP06) for SAP Single Sign-On 2.0, administrators get a new feature: **Online Account Setup on behalf of the user** via the administrative OTP user interfaces. This is available only for users with administrative access for OTP (users assigned with the UME role **OTP_Administrator**).

During the administrative device enrolment, a **Confirmation Code** is sent via the e-mail to the owner of the account (also owner of the device). At the end of the administrative enrolment, the user account status is set to “Not Confirmed” and the SAP Authenticator is not yet available for OTP and Mobile SSO use.

The security protection using such **Confirmation Code** ensures segregation of duties. This way the administrator will not be able to misuse the credentials of the user on his or her behalf. Only the user, who is the owner of the account (and the mobile device) and possess the **Confirmation Code** (sent to his e-mail account), is able to confirm the SAP Authenticator setup (this will change the status to “Enabled”) and to proceed using it for OTP or for Mobile SSO.

**Prerequisites:**
- SAP Authenticator is installed on the mobile device (For more details how to install the SAP Authenticator, see Chapter 6.1. Install SAP Authenticator starting with the search in the AppStore/Google Play - step 92)
- The Email Configuration is completed in the administrative OTP UI - a mail server is properly configured with all relevant e-mail configuration options. See the steps below if not yet configured.
- All users, whose devices will be configured by an administrator, need to have a valid e-mail account set in their user accounts in the UME.

**Explanation** | **Screenshot**
---|---
**Prerequisite:** **Email Configuration Steps (if not yet configured):**

63. Log on to OTP Administrative UI at http://< host > : < port >/otpadmin

64. Navigate to tab **Devices** and choose ‘**Edit**’ for the configuration.

65. Configure the values for your **Mail Server** and **Sender’s Email Address** similar to the example. Keep the default settings or change, if necessary, the texts for the **Subject** and the **Body Template**.

66. Choose ‘**Save**’.
Mobile Single Sign-On For SAP Fiori Using SAP Authenticator

Mobile Device Online Activation by an Administrator

67. In the OTP Administrative UI > tab Devices, choose “Set Up Device”.

68. Use the filter and the “Search” button to find the user.

69. Select the user, whose device you want to activate and choose “Next”.

70. On this page a QR code of the setup URL is displayed and you have to:
   - Scan the QR code, using the SAP Authenticator mobile application OR [Optional] to Choose “Show Setup URL”. Once the setup URL is displayed, you can use it for the registration by typing it as an alternative to the scanning the QR code.
Prerequisite: SAP Authenticator is installed and opened on the mobile device.

[On Mobile Device]
71. Choose Add Account.

[On Mobile Device]
72. Tap to switch ON the Scan QR Code.

[On Mobile Device]
73. Scan the QR code (Displayed on step 65). This will configure the SAP Authenticator.
74. When the screen for password setup appears, lock the device or close the SAP Authenticator application, and give the mobile device to the user to proceed.

Before to start using the SAP Authenticator for Mobile SSO, users will have to activate the configuration using the confirmation code sent to them via the Email.

75. Choose Finish.
**SAP Fiori Client setup** - Prerequisite: The SAP Fiori Client is installed on the mobile device.

76. **[On Mobile Device]** Open the SAP Fiori Client on the mobile device.

77. **[On Mobile Device]** Type the SAP Fiori URL and choose Done. Make sure that the "idplogonurl" parameter in the SAP Fiori URL will be URL encoded twice. See the example below.

**Important:** The "idplogonurl" parameter value is a URL encoded twice!

**Example:**
https://<SAP_Fiori_host>/sap/bc/ui5_ui5/ui2/ushell/shells/abap/FioriLaunchpad.html?sap-client=001&saml2idp=<SAML_IDP_name>&idplogonurl=https%253a%252f%252f<SAML_IDP_host>%252fsaml2%252fsso%25253fsaml2sp%253d<SAML_SP_name>%2526RelayState%253dfiori

78. **[On Mobile Device]** Choose OK.

79. **[On Mobile Device]** You can skip the SAP Fiori Client Passcode by choosing Disable Passcode or you can also set a passcode to protect the application. (This passcode is not related to the authentication to the backend server and is just another layer of application security offered by the SAP Fiori Client solution.)
80. **On Mobile Device**
Choose **Continue** on the Tip page.

81. **On Mobile Device**
When you see this logon screen, the configuration is completed and you can close the SAP Fiori Client. Give the mobile device to the user.

---

82. **Optional** Monitoring **User Status** by the **Administrator** *(before the end user confirmation)*.

82. In the OTP Administrative UI > tab **Users**, search for the same user. You will notice that the user is with status "**Not Confirmed**".

---

83. **End User**: Activation steps required after the configuration by an Administrator.

83. The end user receives such Email in his or her inbox with a **Confirmation Code** for his account at the moment when an administrator scans the QR code for the account setup.
84. User opens the SAP Authenticator and a password configuration is necessary (if there is no password configured and if the password is configured as mandatory on corporate level).

85. Provide the password and choose Go.

86. As a next process step, the user is prompted for a Confirmation Code.

87. Enter the Confirmation Code received via the e-mail.

88. The Activation is complete and the user is able to use the SAP Authenticator for two-factor authentication with OTP and also to use it for Mobile SSO. Two applications are configured in our example. To see the configured applications, choose Applications (2).

89. You can test the Mobile SSO by choosing the bookmarks.
90. This triggers the Mobile SSO process. SAP Authenticator generates a new passcode and sends it to the server for verification. You get the message “Passcode accepted; enter your logon password”. Provide your password.

91. Select the Trust this device checkbox. This will enable the Mobile SSO. Your password is required in order to retrieve the security token that will be used from now on always in combination with a “fresh” passcode for secure Mobile SSO authentication. Note: If you miss to select the Trust this device checkbox, the security token will not be stored on your device and Mobile SSO will not be active for you next time when you try to use it.

92. Choose Log On. You are successfully authenticated.

[Optional] Monitoring User Status by the Administrator (after the end user confirmation).  

93. In the OTP Administrative UI > tab Users, search for the same user. You will notice that the user is with status “Enabled”.
7. MOBILE DEVICE SETUP: A USER SELF-SERVICE

With SAP Single Sign-On 2.0 SP06 end users can use Online Account Setup for activating their device for one-time passwords and Mobile SSO. During the online setup process, corporate applications enabled for Mobile SSO for the user, are automatically configured and ready to use after the last “confirmation” step of this process (using the code displayed on the use self-service user interface). To benefit from this new capability, users need to be assigned to the special UME role OTP_ONLINE_USER.

7. 1 INSTALL SAP AUTHENTICATOR MOBILE APPLICATION

<table>
<thead>
<tr>
<th>Explanation</th>
<th>Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>94.</strong> Log on to SAP Authenticator Setup at http://&lt;host&gt;:&lt;port&gt;/otp</td>
<td></td>
</tr>
</tbody>
</table>

![SAP NetWeaver login page](image)

| **95.** Choose “Scan QR Code” to find the installation. You have also a variant to “Install via iTunes”. |

![SAP Mobile Device Setup screen](image)

If you want to install SAP Authenticator for Android devices, follow the links under “Install Android Version”.

![Install Android Version](image)
96. When you choose “Scan QR code”, a pop-up containing a QR code with the link to iTunes/Google Store appears. [On Mobile Device]

97. Scan the QR code with a QR Code Scanner available on your iOS device and close the pop-up dialog.

[On Mobile Device]

98. Choose “Open URL” when the Scanner shows you the Actions. [On Mobile Device]

99. Choose INSTALL when the SAP Authenticator application is displayed.

[Optional] You can search for the SAP Authenticator directly in the App Store / Google Play on your mobile device [On Mobile Device]

100. For iOS, Open the App Store and search for SAP Authenticator.

Choose INSTALL to install SAP Authenticator.
101. Once SAP Authenticator is installed, choose “Open”.

102. Once the SAP Authenticator has started, choose “Start Setup”.

SAP Authenticator offers a password protection. You can configure a password to protect from unauthorized access to the application.

103. You can skip the password protection by moving the slider to OFF.

104. SAP Authenticator is successfully installed and ready for an account setup.
## 7.2 ONLINE ACCOUNT SETUP BY THE USER

<table>
<thead>
<tr>
<th>Explanation</th>
<th>Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>[On Mobile Device]</strong> Choose Add Account. <strong>[On Mobile Device]</strong> Slide the switch to ON for the <strong>Scan QR Code</strong> option.</td>
<td><img src="image1.png" alt="Screenshot" /> <img src="image2.png" alt="Screenshot" /></td>
</tr>
</tbody>
</table>

105. On Mobile Device Setup UI, choose the link **Set Up Account on Device**.

106. On your PC in the Mobile Device Setup UI, choose the link **Set Up Account on Device**.

107. The Setup procedure will be displayed.
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| **109.** | **On Mobile Device**  
Scan the QR code (displayed in the previous step). This will start the activation process.  
**REQUIREMENT:** A user has to be logged in inside the corporate network. |
| **110.** | **On Mobile Device**  
The Online Account Setup requires you to set up a password for SAP Authenticator as part of the process. That is necessary when the password protection is configured as mandatory on corporate level and when there is not a password yet configured for your SAP Authenticator during the installation process.  
You will not be allowed to proceed with the configuration before you set up a password. If you choose Cancel, this operation stops the Online Account Setup. |
| **111.** | **On Mobile Device**  
Configure a password (minimum 8 characters) for your SAP Authenticator and choose Go.  
**On Mobile Device**  
A Confirmation Code is necessary to complete the Online Account Setup. |
| **112.** | **On Mobile Device**  
The Confirmation Code is displayed as part of the Online Account Setup procedure in the self-service user interface.  
4. To complete the setup on your mobile device, you are prompted to enter a confirmation code  
Use the following confirmation code: 7amy5a4h  
Note: Use the Finish button to confirm that the account is added in the authenticator app or use the Cancel button. |
114. [On Mobile Device] Type the Confirmation Code and choose Done.

115. [On Mobile Device] The configuration is confirmed. SAP Authenticator stars to generate OTP passcodes and your account contains two applications pre-configured for Mobile SSO.


117. You get the message Account setup completed. [Optionally] You can use again the same link Set up Account On Device for configuring additional mobile devices for OTP and Mobile SSO (if you need to use more than one mobile device with these features). Now you can also use the same self-service UI to disable your account setup via the link Disable Account.
[On Mobile Device]
118. Choose Applications (2) to see the applications.

[On Mobile Device]
119. The two applications are displayed.

IMPORTANT: Before you start using the Mobile SSO for the SAP Fiori Client, you need to configure also the SAP Fiori Client itself with a proper URL. For more details about the steps necessary for this configuration, see Chapter 5 > Section SAP Fiori Client Setup (steps 76 - 79)

[On Mobile Device]
120. Once you have completed the SAP Fiori Client configuration, you first see the logon screen and choose the Log On with SAP Authenticator link.

[On Mobile Device]
121. This triggers the Mobile SSO process via SAP Authenticator, and it generates a new passcode and sends it to the server for verification. You receive the message “Passcode accepted; enter your logon password”.

[On Mobile Device]
122. Provide your password.

[On Mobile Device]
123. Select the Trust this device checkbox.

This enables Mobile SSO. Your password is required in order to retrieve the security token that is used from now on always in combination with a “fresh” passcode for secure Mobile SSO authentication.

Note: If you miss to select the Trust this device checkbox, the security token will not be stored on your device and Mobile SSO will not be active for you next time when you try to use it.

[On Mobile Device]
124. Choose Log On and you will be successfully authenticated!
7.3 MOBILE DEVICE SETUP

<table>
<thead>
<tr>
<th>Explanation</th>
<th>Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td>This is the Mobile Device Setup for users who are not authorized to use the Online Account Setup (these users are not have the UME role OTP_ONLINE_USER).</td>
<td><img src="https://example.com/screenshot.jpg" alt="Screenshot" /></td>
</tr>
<tr>
<td>125. Log on to SAP Authenticator Setup at http://&lt; host &gt; : &lt; port &gt;/otp</td>
<td><img src="https://example.com/screenshot.jpg" alt="Screenshot" /></td>
</tr>
<tr>
<td>126. Choose “Set Up Account on Device”.</td>
<td><img src="https://example.com/screenshot.jpg" alt="Screenshot" /></td>
</tr>
<tr>
<td>127. A QR Code for the setup is displayed.</td>
<td><img src="https://example.com/screenshot.jpg" alt="Screenshot" /></td>
</tr>
<tr>
<td><strong>For the Installation of the SAP Authenticator, see Chapter 6.1, Install SAP Authenticator Mobile Application.</strong></td>
<td><img src="https://example.com/screenshot.jpg" alt="Screenshot" /></td>
</tr>
</tbody>
</table>
Open the SAP Authenticator (if not opened on your device)
128. Choose Add Account.

Tap the button to enable the Scan QR Code option.

129. Tap the button to enable the Scan QR Code option.

Scan the QR code displayed on the previous step.
130. Scan the QR code displayed on the previous step.

The user name is displayed.
131. The user name is displayed. Choose “Done”.

SAP Authenticator on your mobile device start generating passcodes.
132. SAP Authenticator on your mobile device start generating passcodes.

There are no applications pre-configured for Mobile SSO with this method of Mobile Device Setup. If you want to enable applications for Mobile SSO, you need to do this manually or use the Online Device Setup described in the previous section (UME role OTP_ONLINE_USER is required in this case).
133. Choose “Finish”.

134. You receive the message “Account setup completed”.

© 2015 SAP SE or an SAP affiliate company. All rights reserved.  
No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. 
Please see HTTP://WWW.SAP.COM/CORPORATE-EN/LEGAL/COPYRIGHT/INDEX.EPX#TRADEMARK for additional trademark information and notices.