Installing SMS authentication method - SSO

Contents

Before installation

System requirements

- Ubisecure Authentication Server 6.x or later
  - For earlier versions refer to earlier versions of the installation guide.
  - For Unregistered SMS, Ubisecure SSO 7.5.0 or later is required.
- Access to an SMS Gateway with support for sending SMS via HTTP
  - This SMS gateway software may be local, using a GSM phone or modem for receiving SMS or HTTP server for receiving SMS as HTTP request.

  or

  - Using an external service provider
  - For external services, the required port must be open for outgoing HTTP connections.
- SMS Gateway must respond to successful sending with HTTP status code 200 (The request has succeeded).

System capacity planning

Consider SMS message throughput when planning system capacity. A typical single GSM modem can process one message every 6 to 12 seconds (depending on the operator and modem). Therefore there is a theoretical maximum of 5 to 10 messages per minute per GSM modem. If your operator, gateway software and modem support SMS over GPRS, speeds of up to 30 messages per second are possible with a GSM/GPRS modem connection. For high capacity systems, direct SMSC links (SMPP, HTTP, UCP/EMI) are capable of processing messages at a much faster pace.

Use with CustomerID

CustomerID installs and pre-configures SMS authentication. Separate installation is not required.*Configuration - CustomerID* – SMS section how to enable it.

Installation

Configuring an SMS Method

Registered – using username and password

SMS methods are configured in Ubisecure SSO Server in a similar way to other *Authentication methods - SSO*

To configure the SMS method in Ubisecure SSO:

1. Open the Ubisecure Management application.
2. Select **Global Method Settings** and click the **New Method...** button.
3. **Add New Method** window opens.
   Give the method a title (external name visible to end users) and name (name for internal use).
   Set the **title** to *SMS*
   Set the **name** to *ubikey.sms.1*
   Set the method type to **SPI Mobile Phone**. The Method Class is automatically selected.
   A directory must be selected, from which contains the user's password and registered telephone number. Select the **Directory** from the drop down list.
   Press **OK**.

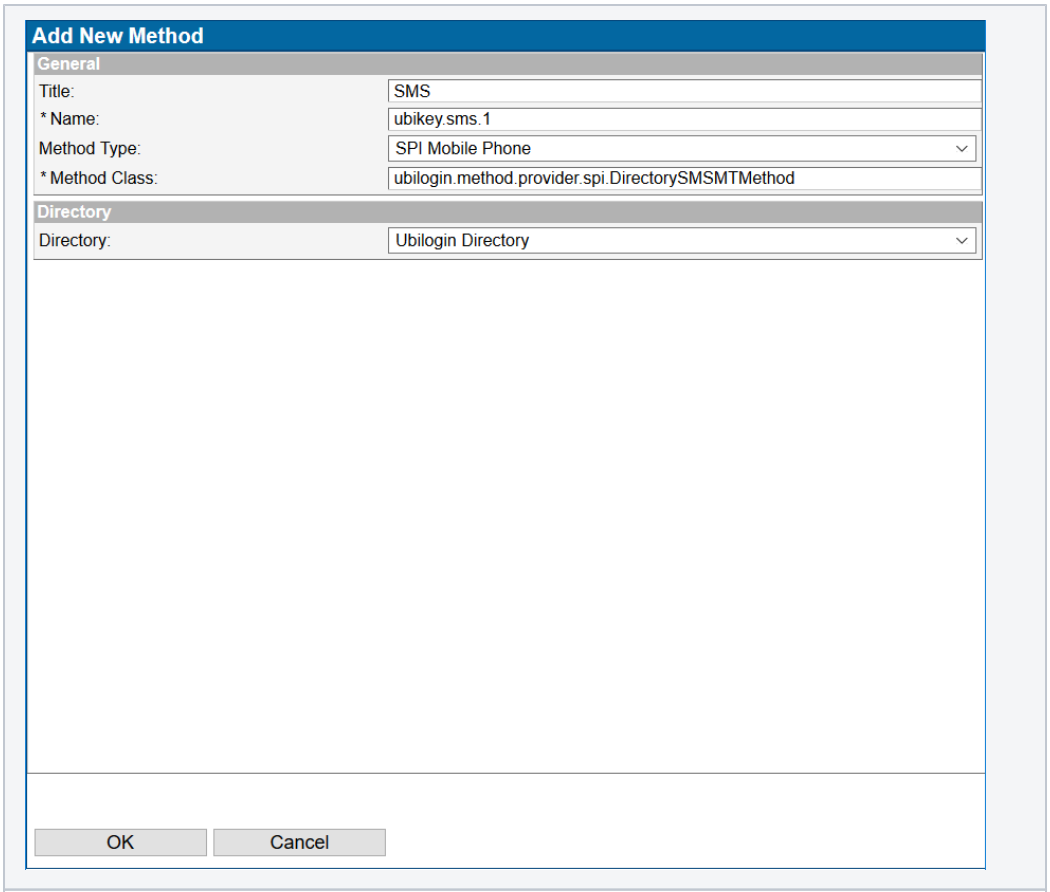
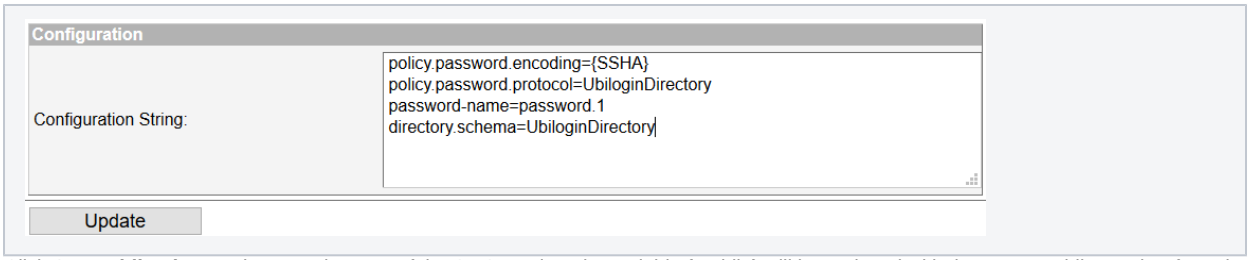


Figure 1. Adding a new SMS method to Ubisecure SSO

4. In the **Main** page of the new method, select the **Enabled** checkbox to activate the new method.
5. Add the following lines to the **Configuration String** field:

```
policy.password.encoding={SSHA}
policy.password.protocol=UbiloginDirectory
password-name=password.1
directory.schema=UbiloginDirectory
```

In this example password.1 will be used as the source for username, password and mobile phone number.



6. Click **SPI Mobile Phone** tab. Enter the URL of the SMS service.The variable {mobile} will be replaced with the users mobile number from the user directory.

   The variable {challenge} will be replaced with the text to be displayed on the mobile phone.

   Example: `http://sms-service-.com/sms/sendsms?to=`*`{mobile}`*`&content=`*`{challenge}`*

   Click **Update**.

> **NOTE:** Be sure that the configured HTTP server in URL parameter answers as HTTP status code 200 (The request has succeeded). All other response codes will be interpreted as a failure situation and the SMS authentication will not succeed. Configurable error will be shown to the user.

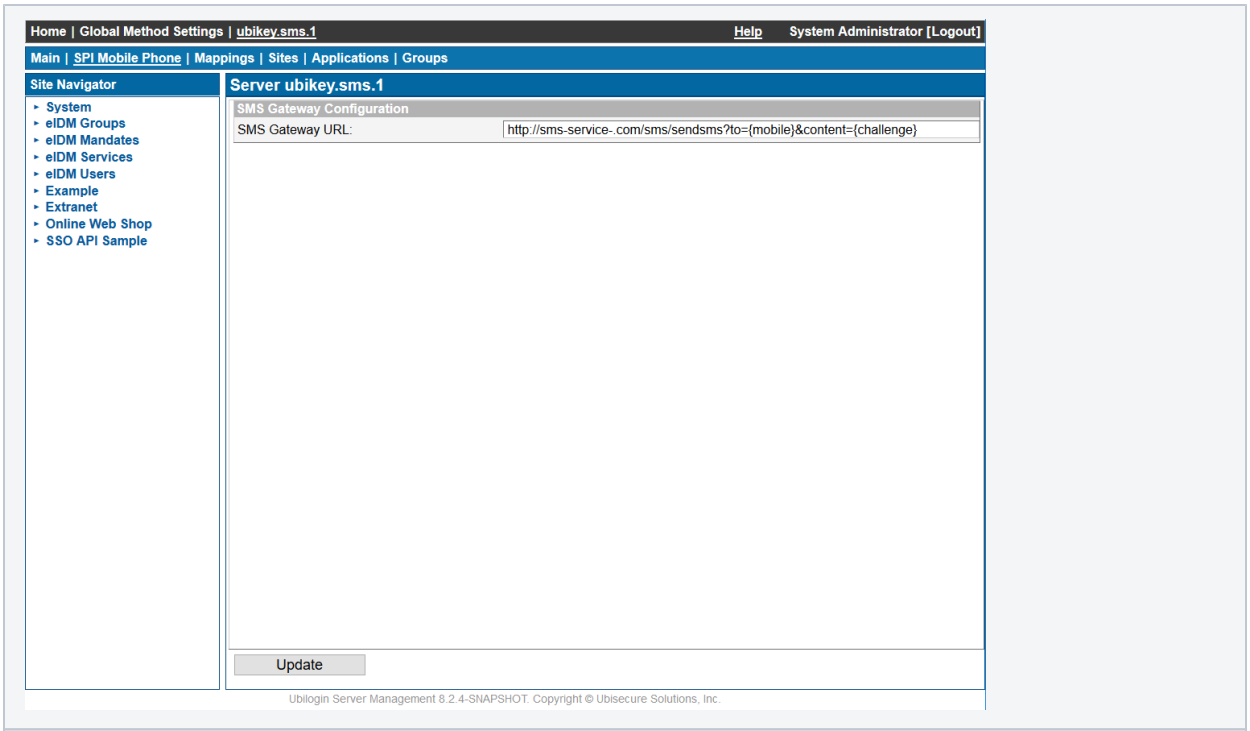


Figure 2. Defining the SMS Gateway URL for sending an SMS

> **NOTE:** This http address must be reachable from this and any other configured nodes.

7. Configure UI Text and SMS text

   The variable {challenge} will be replaced with the text to be displayed on the mobile phone. The message used can be set using the tag SMS_TEXT in the localization files, for example `uas.properties`. Please refer to the *Login user interface customization - SSO*.

   Customizing and localizing message text

   ```
   SMS_TEXT = Your one time password is {0}
   ```

   By default, SSO formats the one-time password in four number sequences. In case you want to omit this kind of formatting, you can define the message key {1} instead of the standard {0}. The message key {1} always holds a plain version of the one-time password.

   Customizing and localizing message text

   ```
   SMS_TEXT = Your one time password is {1}
   ```

   Configure remaining UI text and to match system, branding and language requirements.

8. The method is now installed. Complete the configuration and access control.

After completing these settings, Ubisecure Server is configured to use SMS as an authentication method.

Unregistered

SMS methods are configured in Ubisecure SSO Server in a similar way to other authentication methods.

To configure the SMS method in Ubisecure SSO:

1. Open the Ubisecure Management application.
2. Select **Global Method Settings** and click the **New Method...** button.

3. **Add New Method** window opens.
   Give the method a title (external name visible to end users) and name (name for internal use).
   Set the **title** to *Unregistered SMS*
   Set the **name** to *ubikey.sms.Unregistered*
   Set the method type to **Mobile Phone unregistered**. The Method Class is automatically selected.
   A directory does not need to be selected.
   Press **OK**.

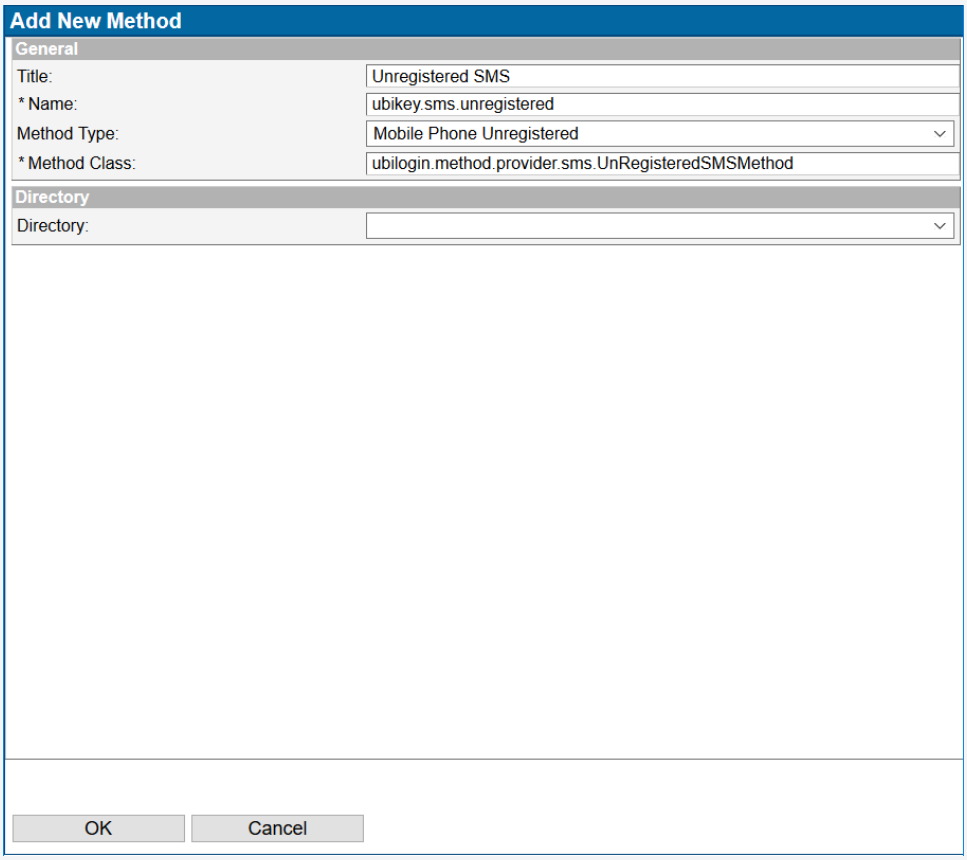


Figure 3 Adding a new unregistered method to ubisecure SSO

4. In the **Main** page of the new method, select the **Enabled** checkbox to activate the new method.
5. Add the following lines to the **Configuration String** field:

```
policy.oauth.otp.timeout=(timeout in minutes)
smsUrl=http\://localhost\:7080/smsgateway/sms?mobile\={mobile}&challenge\={challenge}
```

   Configuration parameter `policy.oauth.otp.timeout` is optional, and it's used for Oauth2 sms-mt-otp grant.
   From UI the timeout is always 10 minutes.
   The variable {mobile} will be replaced with the users mobile number from the user directory.
   The variable {challenge} will be replaced with the text to be displayed on the mobile phone.

   Example: `http://sms-service-.com/sms/sendsms?to=`*`{mobile}`*`&content=`*`{challenge}`*

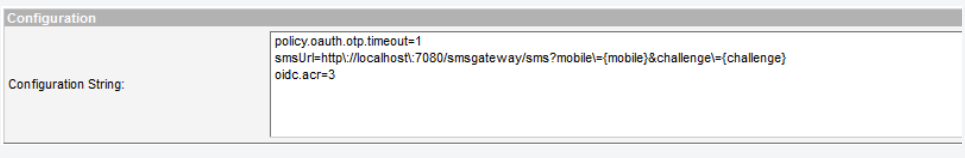


Figure 4 Unregisted sms method configuration

   Click **Update**.
6. Configure UI Text and SMS text
   a. The variable {challenge} will be replaced with the text to be displayed on the mobile phone. The message used can be set using the tag SMS_TEXT in the localization files, for example uas.properties. Please refer to the *Login user interface customization - SSO*
   b. **Customizing and localizing message text**

```
5. SMS_TEXT = Your one time password is {0}
```

Configure remaining UI text and to match system, branding and language requirements.

7. The method is now installed. Complete the configuration and access control.

After completing these settings, Ubisecure Server is configured to use unregistered SMS as an authentication method.

Additional parameters

tokenPattern

The tokenPattern parameter is defined in the authentication method's Configuration String view. This parameter defines how the one-time password should be formatted in a friendly way that is easy for a person to process. Acceptable values hold only pound characters (#) and spaces, where each pound sign represents an individual number from the one-time password and spaces represent themselves, any other characters in configuration string will revert to default behavior. One-Time passwords consist typically of 8 numbers that are printed in 4-number sequences (e.g. 1234 5678). In case you want to sequence them differently, you can use the tokenPattern configuration option to produce any kind of sequencing. For example, the configuration: "tokenPattern=## ### ## #" would change the formatting of the one-time password "1234 5678" to "12 345 67 8".

tokenLength:

The generated token's length is, by default, 8 digits. This can be modified using the tokenLength parameter. Generated tokens are split, by default, to sequences of four digits in order to make the token more easy to copy. Note that spaces are completely disregarded in token validation - they are there only to make the process more user friendly. The minimum allowed length is 4 digits - if the token is parameterized any shorter, then the default value will apply.

After Installation

Configuring Ubisecure SMS for Users and Web Applications

After installing and configuring the SMS authentication method for the Ubisecure Server, use Ubisecure Management to configure the authentication method for a user and an application. The SMS method must be enabled at the system, site, application and user levels. For detailed instructions for configuring authentication methods, please refer to the page *Management user interface - SSO*.

Logging In First Time with the Ubisecure SMS Authentication Method

Ubisecure Server sends the one-time passwords to the configured URL. For testing purposes without an HTTP capable SMS Gateway, the HTTP requests can be logged to a file in the HTTP server to verify the sent one-time passwords.
The username and password used are the same as the user's password method username and password.