

# Configuration of unregistered SMTP - SSO

## System Requirements

- Ubisecure SSO version 6.x or later
- Access to an SMTP mail server

## Configuring the Unregistered SMTP Method

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

**To configure the SMTP 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 SMTP* (This text is shown to end users on the login screen. Consider "Login using email code")  
Set the **name** to *ubikey.smtp.unregistered*  
Set the method type to **SMTP Unregistered**. The Method Class is automatically selected.  
A directory needs to be selected only if the Directory User Mapping is required. i.e. If the email address will be used to look up an existing user from a connected user repository.  
Press **OK**.

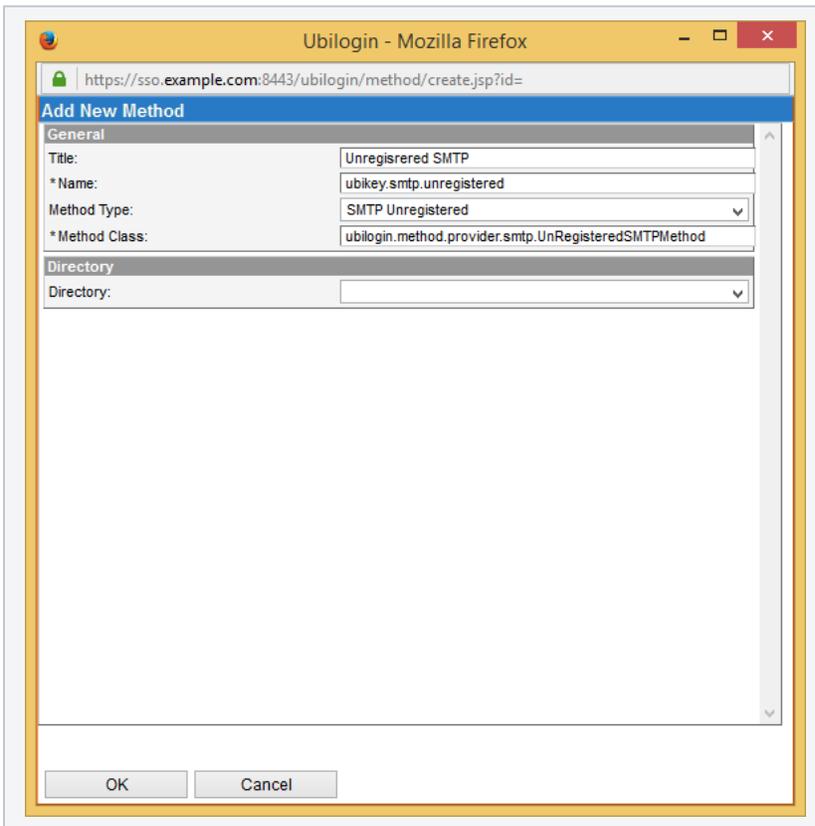


Figure 1. Adding a new unregistered SMTP method to Ubisecure SSO

4. In the **Main** page of the new method, select the **Enabled** checkbox to activate the new method.
5. Configure the email service for sending the OTP.

For production systems, a JNDI mail session must be configured in file `ubilogin/custom/tomcat/mail-resources.xml`. Note that it should contain only Resource-elements and no parent element. If the file needs to be updated, Tomcat must also be updated by running `ubilogin/config/tomcat/update.[sh|cmd]`.

#### ubilogin/custom/tomcat/mail-resources.xml

```
<Resource name="mail/Session"
  auth="Container"
  type="javax.mail.Session"
  mail.smtp.host="smtp.example.com"
  mail.smtp.port="465"
  mail.smtp.auth="true"
  mail.smtp.user="donotreply@example.com"
  password="yourPassword"
  mail.smtp.starttls.enable="true"
  mail.transport.protocol="smtps"
/>
```

SMTPS (SMTP over TLS) should always be used in production environments.

Next, set the parameter `mail-session` to refer to the mail resource's name attribute in the **Configuration String** field .

```
mail-session=mail/Session
```

An alternative solution for test or development is to add the following lines directly to the **Configuration String** field:

```
mail.smtp.host=[mail server hostname]
mail.smtp.port=[mail server port]
mail.smtp.from=[address users see the mail coming from]
```

Note that if you define both, then `mail-session` takes the precedence and any `mail.smtp.*` is completely ignored.

If none is set, then the default setting `mail-session=mail/Session` will be used.

When using SMTP unregistered method for `smtp-otp` unregistered grant, the `otp` timeout can be optionally configured to the method by adding the following line to configuration string.

```
policy.oauth.otp.timeout=[timeout in minutes]
```

When an OTP is sent from the interactive login screen via the user interface, validity time (timeout) is always 10 minutes.

#### 6. Configure UI Text and email text

The variable `{0}` will be replaced with the verification code, which is expected to be given by the user.

The message, that is shown on the SSO UI screen during the authentication, can be set using the tag `SMTP_TEXT` in the localization files. Please refer to the [Login UI Customization Guide](#)

#### Listing 1. Customizing and localizing message text

```
SMTP_HEADER = Your one time password for entry
SMTP_TEXT = Your one time password is {0}
SMTP_TEXT_CONTENT_TYPE = text/plain
```

Note that when using OAuth 2.0 [SMS-MT-OTP and SMTP-OTP grant](#), these can be overridden by setting the `x_globalsign_iam_otp_title`, `x_ubisecure_otp_content_type` and/or `x_globalsign_iam_otp_body` parameters. We support two content types for emails: `text/plain` and `text/html`.

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

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

## Additional parameters

### SSO 8.3.3

In SSO version 8.3.3 token formatting parameters were added.

## 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.

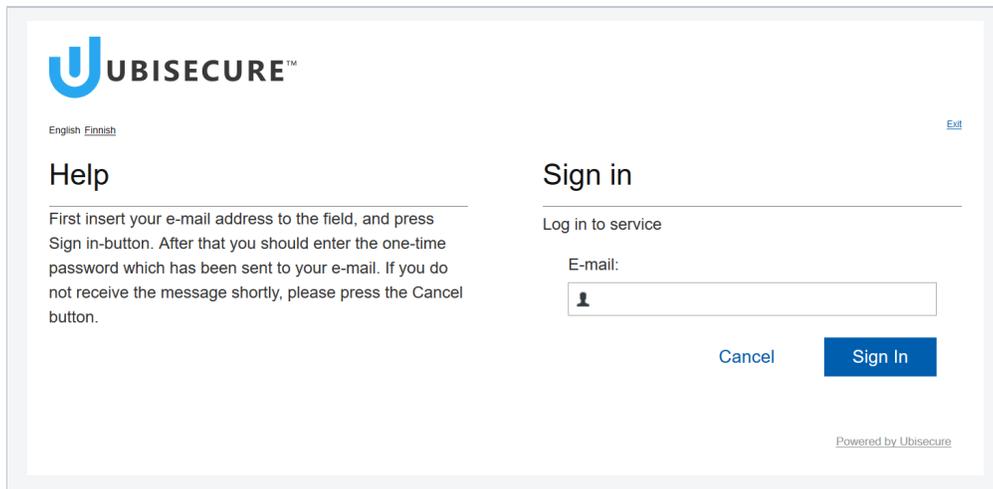
## Configuring Ubisecure Unregistered SMTP for Users and Web Applications

After installing and configuring the unregistered SMTP authentication method for the Ubisecure Server, use Ubisecure Management to configure the authentication method for an application. The unregistered SMTP method must be enabled at the system, site and application levels. An access control group should be created for users of this method and added to the Allowed To settings of the target application.

For detailed instructions for configuring authentication methods, please refer to the page [Management user interface - SSO](#).

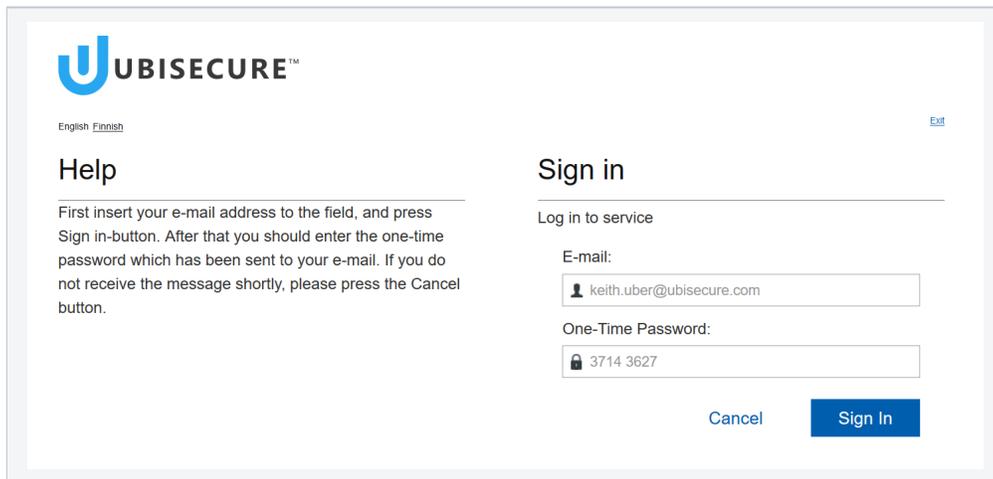
## Logging In First Time with the Unregistered SMTP Authentication Method

Ubisecure Server sends an eight digit one-time password to the user email address through the configured mail server.



The screenshot shows the Ubisecure login interface. On the left, there is a 'Help' section with instructions: 'First insert your e-mail address to the field, and press Sign in-button. After that you should enter the one-time password which has been sent to your e-mail. If you do not receive the message shortly, please press the Cancel button.' The main 'Sign in' section has a sub-header 'Log in to service' and an 'E-mail:' label above an empty input field. Below the input field are 'Cancel' and 'Sign In' buttons. At the bottom right, it says 'Powered by Ubisecure'. There are also language options 'English Finnish' and an 'Exit' link.

The user receives an email containing an eight digit code. The number must be entered in the One-Time Password field.



This screenshot shows the same Ubisecure login interface as the previous one, but with the email and one-time password entered. The 'E-mail:' field now contains 'keith.uber@ubisecure.com' and the 'One-Time Password:' field contains '3714 3627'. The 'Sign In' button is now highlighted in blue, indicating it is the active button. The rest of the interface, including the help text and footer, remains the same.

If the number is correct, login succeeds.

