OTP Printout authentication method - SSO

Introduction

This documentation describes the requirements and tasks for installing and configuring Ubisecure OTP Printout authentication method in an Ubisecure SSO.

The result of the installation described in this page is a working OTP Printout authentication method. You should refer to the Installation - SSO Guide for instructions on installing Ubisecure SSO.

Ubisecure OTP Printout Overview

Ubisecure OTP Printout is an authentication method utilising printed one-time password lists to authenticate users. User accounts may be stored either in Ubisecure CustomerID or in an external directory such as Active Directory.
To authenticate themselves, the user is required to enter the following information:

- username
- password
- one-time password

If the entered information above is correct, the user can access the web pages secured by Ubisecure SSO and its Ubisecure OTP Printout authentication method.

Before Installation

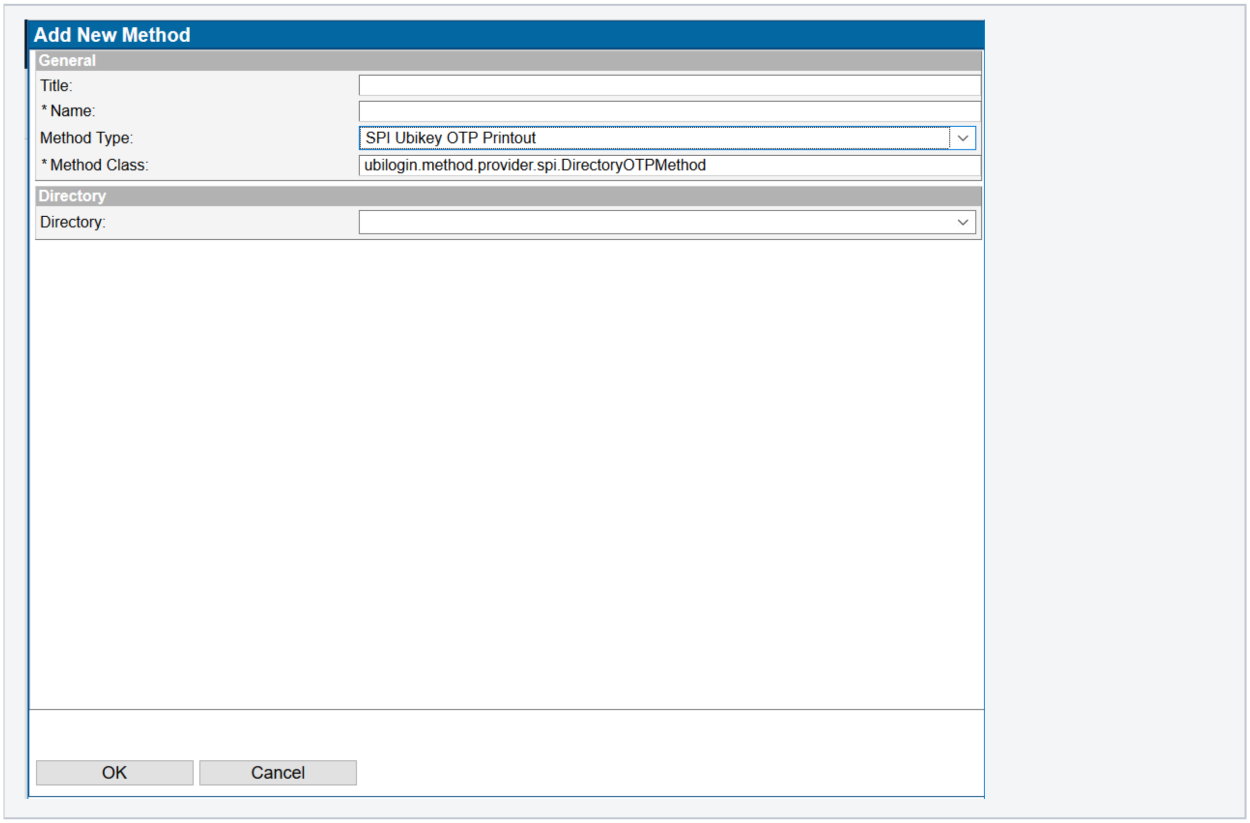
System requirements

- Ubisecure SSO 6.4 or later

Installation

Start a session with Ubisecure Management and go straight from the top level to page "Global Method Settings".

Create a new authentication method:



Add New Method

General

Title:

* Name:

Method Type: SPI Ubikey OTP Printout

* Method Class: ubilogin.method.provider.spi.DirectoryOTPMethod

Directory

Directory:

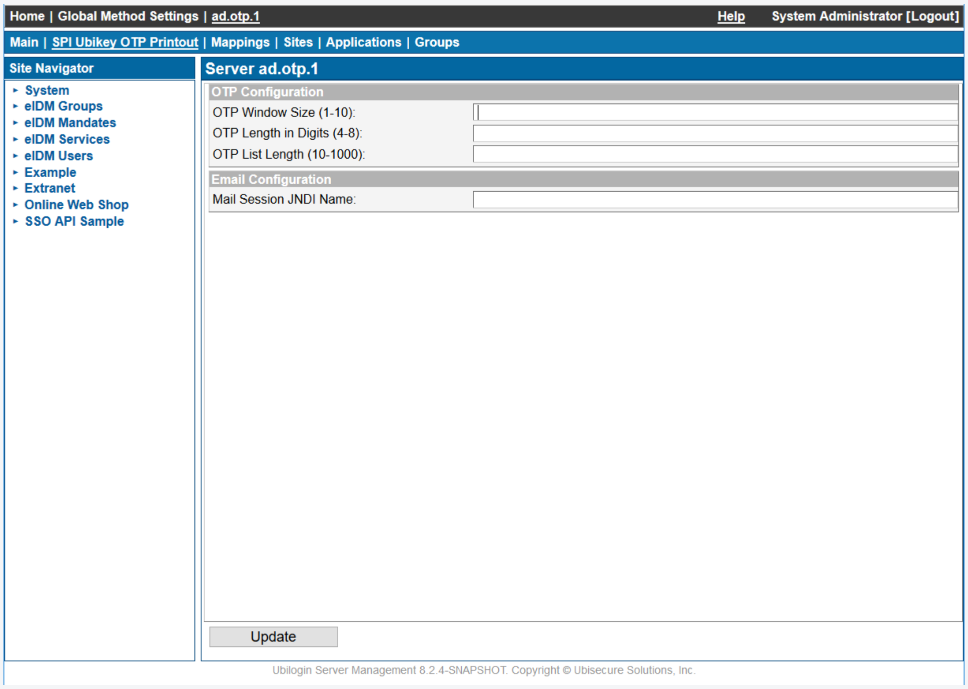
Add Title e.g: Ubisecure OTP Printout
Add name e.g: ad.otp.1
Choose Method Type: **SPI Ubikey OTP Printout**

Optionally in the Directory selection choose the Service where user accounts are stored

Open the entry "Ubisecure OTP Printout" and modify the necessary parameters in Main tab.

- Select the **Global Method Settings** in Ubisecure Management after logging in as administrator
- Select the **Ubisecure OTP Printout** authentication method
- Set **Status** enabled

Then, select the tab "SPI Ubikey OTP Printout" to configure the OTP Printout specific settings.


Home | Global Method Settings | ad.otp.1
Help
System Administrator [Logout]
Main | SPI Ubikey OTP Printout | Mappings | Sites | Applications | Groups
Site Navigator
System
eIDM Groups
eIDM Mandates
eIDM Services
eIDM Users
Example
Extranet
Online Web Shop
SSO API Sample
Update
Ubilogin Server Management 8.2.4-SNAPSHOT. Copyright © Ubisecure Solutions, Inc.

Server ad.otp.1

OTP Configuration

OTP Window Size (1-10):

OTP Length in Digits (4-8):

OTP List Length (10-1000):

Email Configuration

Mail Session JNDI Name:

Figure 1. Configuring OTP Printout authentication method

OTP Window Size (mandatory)
Specifies the number of one-time passwords the user may skip. Minimum value is 1 meaning that the user is not allowed to skip the sequences. Maximum value is 10, meaning that the user may use any of the next 10 OTPs. The purpose of this feature is to enhance usability and if there is no explicit need for this, it is recommended to use the value of 1. Changes for this setting affect also the existing OTP lists.

OTP Length in Digits (mandatory)
Specifies the number of digits in each one-time password. The minimum length is 4 and the maximum length is 8. Changes for this setting affect only the OTP lists generated after the change.

OTP List Length (mandatory)
Specifies the number of one-time passwords in each OTP list. The minimum value is 10 and the maximum value is 1000. Changes for this setting affect only the OTP lists generated after the change.

Mail Session JNDI Name (optional)
Specifies the JNDI name of the JavaMail session configured in the application server. This is required for emailing the OTP lists.

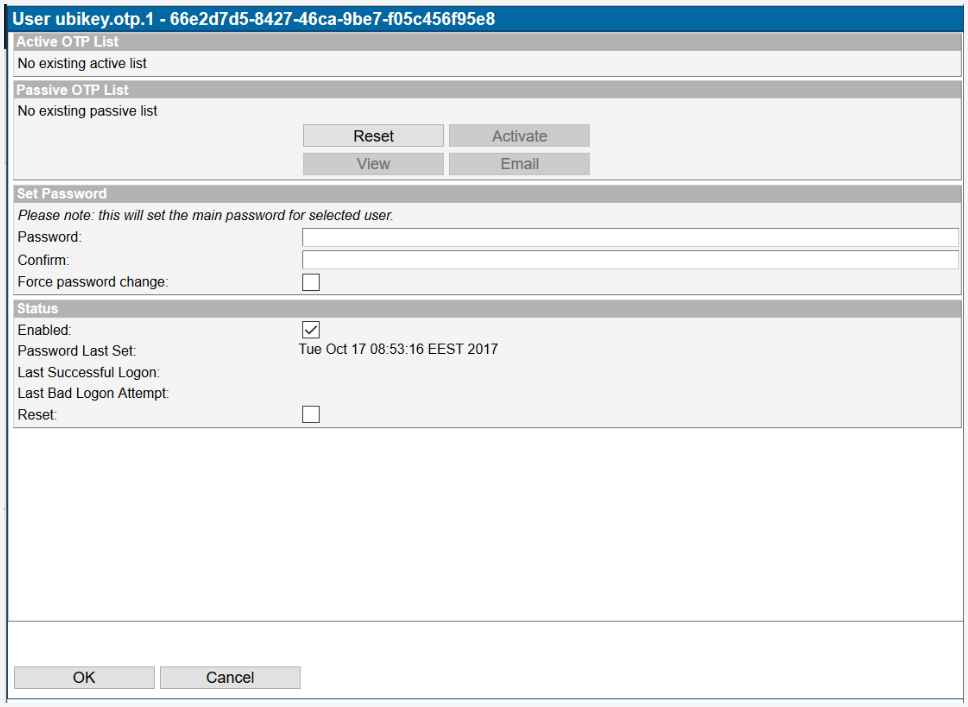
After Installation

Configuring Ubisecure OTP Printout for Users and Web Applications

After installing and configuring Ubisecure OTP Printout authentication method for the Ubisecure Server, please refer to *SSO Management Guide* for enabling an authentication method for users and applications.
For detailed instructions about maintaining and managing Ubisecure OTP Printout specific user information, such as OTP lists, please refer to the next chapter.

Managing Ubisecure OTP Printout Users

The Ubisecure OTP Printout specific user information is stored in the built-in Ubisecure Directory regardless of the directory configured in the installation chapter. In case of the external directory, each user must have a corresponding user account in Ubisecure Directory with the same username (uid) as the user account in the external directory. Also, the optional email address used to send OTP lists through email is configured in the Ubisecure user account.



User ubikey.otp.1 - 66e2d7d5-8427-46ca-9be7-f05c456f95e8

Active OTP List

No existing active list

Passive OTP List

No existing passive list

Set Password

Please note: this will set the main password for selected user.

Password:

Confirm:

Force password change: □

Status

Enabled: ☑

Password Last Set: Tue Oct 17 08:53:16 EEST 2017

Last Successful Logon:

Last Bad Logon Attempt:

Reset: □

Figure 2. Managing Ubisecure OTP Printout users

Each Ubisecure OTP Printout user has an active OTP list and a passive OTP list. Either one or both of the lists may be absent. The OTP validation process goes as follows:

1. If the active list exists, the user supplied OTP is validated against the active list. If the OTP is correct within the OTP Window Size specified in the installation chapter, the authentication is successful and the current OTP sequence number is updated. If there is no more OTPs in the list, the passive list is activated.
2. If the active list does not exist or the OTP is not correct, the OTP is validated against the first OTP of the passive list. If the OTP is correct, the authentication is successful and the passive list is activated. Consequently, the previous active list may not be used anymore.

OTP list maintenance is done in Ubisecure Management. The following operations are possible for passive lists: reset, activate, view/print, and email.

- **Reset**
  Resetting the passive list generates a new list with the list length and OTP length specified in the installation chapter. Resetting the passive list replaces the previous passive list which may not be used anymore.
- **Activate**
  Activating the passive list replaces the current active list. After activation, a new passive list may be created with reset functionality.
- **View**
  Viewing the passive list opens a new dialog showing the list and provides the functionality to print the list. Please note that it is not possible to view the list after activation.
- **Email**
  Emailing sends the passive list to the user through email. Please note that it is not possible to email the list after activation.

If the authentication is configured to use external directory as a user repository, the static password is validated by binding to the external directory and the password management is performed using the tools provided by the external directory. Otherwise, if the authentication is configured to use Ubisecure Directory as a user repository, the password management is performed using the "Set Password" section as shown in *Figure 2*.

- **Password**
  Enter a new password to change the static password for the user.
- **Confirm**
  Enter the same password to the confirm field to eliminate the possible spelling errors.

OTP List Server

OTP List Server is a REST service used for managing OTP Printouts for external directory integrations. It provides set of operations for creating, listing, activating and deleting OTP Lists for given users or list id's. A more detailed list of the operations is given in page OTP Server - SSO.

OTP List Server doesn't support managing OTP lists for users in Ubilogin Directory.

To activate OTP List Server, following steps need to be done:

1. Remove otpserver.xml from tomcat/conf/Ubilogin/[uas.url]/
2. Create a new user or select an existing user in Ubilogin Directory who will be used for authenticating OTP Server users
   For the user, the following requirements need to be fulfilled
   a. Be a member of **System / OTP Server / OTP Server Admins** group
   b. Have the method **password.1** activated and a password set for it

Localizing and Customizing UI Text

All user interface strings can be customized using the tag format below in *Listing 1*. For more information on localization and customization, please refer to the document *Server Management Guide*.

Listing 1. Localizing and Customized UI Texts in custom/messages/uas.properties

```
OTP = Ubikey Password
OTP_CHALLENGE = Next Ubikey sequence {0}
NEW_SEED = New Seed
NEW_OTP = New Ubikey Password
CONFIRM_OTP = Confirm Ubikey Password
OTP_HELP1 = Please enter your Username and Ubikey Password
OTP_HELP2 = Please enter your Ubikey Password
```

To suppress the display of the next sequence number in all circumstances, remove the {0} tag from the OTP Challenge Line.

```
OTP_CHALLENGE = The provided credentials are invalid.
```