# NetIQ Advanced Authentication Framework - Web Enrollment Wizard

**Installation Guide**

Version 5.1.0

# Table of Contents

# Introduction

## About This Document

## Purpose of the Document

This Web Enrollment Wizard Installation Guide is intended for all user categories and describes how to use the client part of NetIQ Advanced Authentication Framework solution. In particular, it gives instructions as for how to install Web Enrollment Wizard.

For more general information on NetIQ Advanced Authentication Framework™ and the authentication software you are about to use, see NetIQ Advanced Authentication Framework – Client User's Guide.

## Document Conventions

This document uses the following conventions:

**Warning.** This sign indicates requirements or restrictions that should be observed to prevent undesirable effects.

**Important notes.** This sign indicates important information you need to know to use the product successfully.

**Notes.** This sign indicates supplementary information you may need in some cases.

**Tips.** This sign indicates recommendations.

- Terms are italicized, e.g.: *Authenticator*.
- Names of GUI elements such as dialogs, menu items, and buttons are put in bold type, e.g.: the **Logon** window.

# System Requirements

⊛ Installing and removing Web Enrollment Wizard requires **Local Admins** privileges.

The following system requirements should be fulfilled:

- Microsoft Windows Server 2008 R2 SP1/Microsoft Windows Server 2012/Microsoft Windows Server 2012 R2
- Pre-installed Web Server (IIS) role

⊛ Web Enrollment Wizard cannot be used on the server with pre-installed SharePoint and Microsoft ARR (Application Request Routing).

⊛ If it is required to install Web Enrollment Wizard on a separate server, please install it only on the server with the pre-installed NetIQ RTE.

⊛ Make sure that the following IIS services are installed on the selected server: Web Service Role, Common HTTP Features, ASP.NET 4.5 (4.0.30319), .NET Extensibility, ISAPI Extensions, ISAPI Filter and Request Filtering.

⊛ An option **Allow password logon** must be enabled for users in order to use the Web Enrollment Wizard.

# Installing and Removing Web Enrollment Wizard

The NetIQ Web Enrollment Wizard allows users to enroll authenticators from any place (workstation, laptop, tablet PC or smartphone) in the web browser, without necessity to install any software.

In this chapter:

- [Installing Web Enrollment Wizard](#)
- [Configuring Web Enrollment Wizard](#)
- [Removing Web Enrollment Wizard](#)

## Installing Web Enrollment Wizard

⊛ The start of installation can be frozen for a time up to 1 minute in the case of offline mode. This delay occurs due to check of digital signature of component.

To install Web Enrollment Wizard:

1. Run the .exe file. **Web Enrollment Wizard** will be automatically installed on your computer.

2. You must restart your system for the configuration changes made to Web Enrollment Wizard to take effect. Click **Yes** to restart the system immediately or **No** if you plan to restart it later manually.

## Configuring Web Enrollment Wizard

1. During the installation of Web Enrollment Wizard, domain of the server, where Web Enrollment Wizard is being installed, will be set by default. If domain was not detected or another domain should be set, open the **web.config** file that is located in **C:\Program Files\NetIQ\NetIQ Advanced Authentication Framework\WEW**. Uncomment the code and replace **DOMAIN** with the correct domain name. If the option is commented, current domain name will be used by default.

2. It is also possible to configure the **style.css** file that is located in **C:\Program Files\NetIQ\NetIQ Advanced Authentication Framework\WEW\Content**. The **style.css** file should be configured accurately.

3. The required authentication provider should be installed on the server. Otherwise it will not be displayed in the list of available authenticators.

4. To enroll Live Ensure authentication provider using NetIQ Web Enrollment Wizard, the user's e-mail address that is linked to LiveEnsure account should be specified in the **General** tab of the **User Properties** in Active Directory Users and Computers and Live Ensure authentication provider should be configured in accordance with Live Ensure AP - Installation Guide.

5. To enroll OATH OTP authentication provider using NetIQ Web Enrollment Wizard, OATH OTP authentication provider should be configured in accordance with OATH OTP AP - Configuration Guide.

6. To enroll SMS authentication provider using NetIQ Web Enrollment Wizard, the user's telephone number that will be used for authentication should be specified in the **General** tab of the **User Properties** in Active Directory Users and Computers and SMS authentication provider should be configured in accordance with SMS AP - Installation Guide.

    ✴ It is required to specify an equal **TelephoneNumberAttribute** parameter's value in the following registry key HKEY_ LOCAL_ MACHINE\Software\Wow6432Node\BSP\ {6D890379-EC8E-483F-A927-F3489303B37A}\SMS Service on Web Enrollment Wizard server.

7. To enroll Voice Call authentication provider using NetIQ Web Enrollment Wizard, the user's telephone number that will be used for authentication should be specified in the **General** tab of the **User Properties** in Active Directory Users and Computers and Voice Call authentication provider should be configured in accordance with Voice Call AP - Installation Guide.

8. To enroll Smartphone authentication provider using NetIQ Web Enrollment Wizard, Dispatcher API interfaces should be configured in accordance with Smartphone AP - Installation Guide.

9. To enroll YubiKey OATH HOTP authentication provider using NetIQ Web Enrollment Wizard, Yubikey OATH OTP authentication provider should be configured in accordance with the YubiKey Configuration chapter and OATH OTP AP - Configuration Guide.

## YubiKey Configuration

To configure YubiKey:

1. Install YubiKey Personalization Tool.
2. Plug-in a YubiKey Token.
3. Run the **YubiKey Personalization Tool**, go to the **OATH-HOTP** tab and click the **Advanced** button.
4. Select the configuration slot.
5. Select the **OATH Token Identifier** box in the **OATH-HOTH Parameters** section. Click the **Generate MUI** button.
6. Click the **Generate** button to generate the **Secret Key**.
7. Click the **Write Configuration** button. Confirm writing the configuration. Save the **.csv** file.
8. Copy the **.csv** file to **%ProgramFiles%\ NetIQ Advanced Authentication Framework\WEW** on the server with the installed NetIQ Web Enrollment Wizard.
9. Open the **WEW** folder and open the **web.config** file with Notepad.
10. Specify the name of the **.csv** file in the string **<add key="yubikeyConfig" value="~/<filename>.csv"/>**.
11. Save the **web.config** file.

## Configuring SMS Confirmation

SMS confirmation is required when user has no enrolled authenticators, but he/she wants to enroll the one in Web Enrollment Wizard. If SMS confirmation is configured, the workflow will be the following:

1. User signs in to Web Enrollment Wizard.
2. Web Enrollment Wizard checks AD profile of the user for the mobile number.
3. Authenticore Server generates OTP and sends it to the mobile phone.
4. User enters the received OTP in Web Enrollment Wizard.
5. User has a capability to proceed to enrollment of authenticators in Web Enrollment Wizard.

To configure SMS confirmation:

1. Specify SMS authentication provider settings in the registry of the server with the installed Web Enrollment Wizard.
2. Open the **web.config** file that is located in C:\Program Files\NetIQ\NetIQ Advanced Authentication Framework\WEW.
3. Find the following line:
   <!-- Switch to true if you want to use additional SMS authentication -->
   <add key="useSmsAuthentication" value="false"/>
4. Replace **"false"** with **"true"**.
5. Save changes.

## Configuring PSKC Enrollment

NetIQ Advanced Authentication Framework v4.11 supports HID/ActivIdentity tokens enrollment in Web Enrollment Wizard. To enroll HID/ActivIdentity token, it is enough just to enter the serial number from the back side of your token.

⊗ Ensure that the **TOTP generation Step** field is set to 30 seconds in the **TOTP policy**. This policy must be applied on Authenticore Servers and workstations.

To enable HID/ActivIdentity tokens support, add the **pskc** file on the server with the installed Web Enrollment Wizard. Follow the steps:

1. Put the **pskc** file to C:\Program Files\AuthasasNetIQ\NetIQ Advanced Authentication Framework\WEW.
2. Open the **web.config** file in the same folder.
3. Change the **pskc** file name in <add key="pskcConfig" parameter (line 38).
4. Save changes.
5. Sign in to Web Enrollment Wizard.
6. Select **OATH OTP Token TOTP (by serial number)**.
7. Enter the serial number from the back side of your token.

⊗ Only one **pskc** file name can be specified in the **web.config** file.

## Using Web Enrollment Wizard From Outside the Domain

Web Enrollment Wizard can be used for authentication of users from outside the domain through NetIQ Web Service. This option is available starting from version 4.11.

To configure Web Enrollment Wizard running through NetIQ Web Service, follow the steps:

1. Open the following registry key on the server with the installed Web Enrollment Wizard: HKEY_LOCAL_MACHINE\SOFTWARE\NetIQ\NetIQ Advanced Authentication Framework
2. Specify the following parameters in the registry key:
   - IsWSLogon=1 to enable authentication via Web Service
   - WebAuthServer=https://<webserviceaddress>:<webserviceport>/Service.svc/bsc
3. Open the **web.config** file that is located in C:\Program Files\NetIQ\NetIQ Advanced Authentication Framework\WEW.
4. Find the following line:
   <!-- Switch to true if you want to use webservice (for example in DMZ). Don't forget to tune 'endpoint address' below
   This option overrides IsWSLogon and Webservice Address options in registry-->
   <!--
   <add key="useWebService" value="false"/>
   -->
5. Replace **"false"** with **"true"**.
6. Save changes.

## Removing Web Enrollment Wizard

In this chapter:

## Microsoft Windows Server 2008

1. In the **Start** menu, select **Control panel** and then double-click **Programs and Features**.
2. Select **Web Enrollment Wizard** and click **Uninstall**.
3. Confirm the removal.
4. Wait a few seconds until the removal is completed.

## Microsoft Windows Server 2012/2012 R2

1. In the **Search** menu, select **Apps > Control Panel > Programs > Programs and Features**.
2. Select **Web Enrollment Wizard** and click **Uninstall**.
3. Confirm the removal.
4. Wait a few seconds until the removal is completed.

# Troubleshooting

This chapter provides solutions for known issues. If you encounter any problems that are not mentioned here, please contact the support service.

In this chapter:

- Cannot Install Web Enrollment Wizard
- Authenticore Server Was Not Found While Web Enrollment Wizard Authentication

## Cannot Install Web Enrollment Wizard

**Description:**

Error appears while installing Web Enrollment Wizard on your computer.

**Cause:**

a. You are installing Web Enrollment Wizard on the network drive.
b. You have no space left on the disk.
c. You are installing Web Enrollment Wizard on the unsupported OS.
d. You are installing Web Enrollment Wizard on the OS with the wrong bitness.

**Solution:**

a. Change the installation path.
b. Free the amount of disk space needed for installation.
c. Check the list of supported OS.
d. Check your OS's bitness and run the installer.

## Authenticore Server Was Not Found While Web Enrollment Wizard Authentication

**Description:**

During authentication using Web Enrollment Wizard the following error occurs: "*Could not find Authenticore Server*".

**Cause:**

None of Authenticore Servers could be accessed.

**Solution:**

a. Check whether at least one Authenticore Server (from the Authenticore Server group in CN=Users in Active Directory) is running and firewall tools do not block an interaction.
b. Open the following folder on the Authenticore Server:
%ProgramFiles%\NetIQ\NetIQ Advanced Authentication Framework\
Then execute: schemaadmin.exe -import DefaultSchema.

# Index

**S**

Server  4, 8, 12-13
Software  6
System  4

**T**

Token  7
Tool  7
TOTP  9

**U**

User  6, 8