ESET

# SECURE AUTHENTICATION

## API SSL Certificate Replacement

ESET **SECURE AUTHENTICATION**



Customer Care Worldwide: www.eset.eu/support
Customer Care North America: www.eset.com/support

REV. 7/12/2013

# Contents

# 1. Introduction

The ESET Secure Authentication Authentication API uses an SSL certificate to secure API communications. The installer automatically selects an appropriate certificate installed on the machine, or generates a new self-signed certificate if another cannot be found.

This guide explains how to replace the certificate with another of your choosing by importing your new certificate into Windows and then applying it to ESA.

# 2. Prerequisites

In order to follow this guide you will need:

- An installation of the ESET Secure Authentication Core component
- Administrator access to the computer where ESET Secure Authentication is installed
- The SSL certificate you wish to use in PKCS12 format (.pfx or .p12).

  The certificate file needs to contain a copy of the private key as well as the public key

- Windows 2003 only:

  The *httpcfg.exe* tool from the Windows Support Tools pack (either on the installation CD or downloadable from http://www.microsoft.com/en-us/download/details.aspx?id=18546)

**Note**: The ESA Authentication API does not have to be enabled in order to replace the certificate.

# 3. Importing the new certificate

The new certificate needs to be placed in the Local Machine\Personal store before it can be used.

1. Press the **Windows key + R**, type **MMC.exe** in the **Open** field and then press **Enter** to open the Microsoft Management Console.
2. Add the Certificates snap-in:

**Windows Server 2003:**

a. Click **File** > **Add/Remove Snap-in** > **Add**

b. Select **Certificates**

c. Click **Add**

d. Select **Computer account**

e. Click **Next**

f. Select **Local computer**

g. Click **Finish**

h. Click **Close**

i. Click **OK**

**Windows Server 2008 and later:**

a. Click **File** > **Add/Remove Snap-in**

b. Select **Certificates** from the left column

c. Click **Add**

d. Select **Computer account**

e. Click **Next**

f. Select **Local computer**

g. Click **Finish**

h. Click **OK**

3. Click **File** > **Save** to save the snap-in for future use.
4. In the ESET Secure Authentication Management Console, select **Certificates** > **(Local Computer)** > **Personal.**
5. Right-click the certificate and select **All tasks** > **Import** from the context menu.
6. Follow the **Import Wizard**, taking care to place the certificate in the **Personal** certificate store location.
7. Double-click the certificate and make sure that "You have a private key that corresponds to this certificate" is displayed.

# 4. Replacing the ESA Certificate

**Note**: The ESA Core Authentication service will not start up without a certificate configured. If you remove the certificate, you must add another before the Core service will run correctly.

## 4.1 Determine the correct certificate to use

1. Open the MMC Certificates Manager using the steps from the Importing the new certificate section of this guide.
2. Navigate to the **Personal** folder and double-click the certificate that you want to use.
3. Make sure you see **You have a private key that corresponds to this certificate** in the **General** tab.
4. In the **Details** tab, select **Thumbprint**.
5. The certificate thumbprint is displayed in the bottom pane (sets of two hex digits separated by spaces).

## 4.2 Windows Server 2003

1. Click **Start** > **All Programs** > **Windows Support Tools** > **Command Prompt**.
2. Type *httpcfg query ssl -i 0.0.0.0:8001* and press **Enter**.
3. Copy and paste the **Hash** field somewhere safe, in case you want to re-add the existing certificate.
4. Type *httpcfg delete ssl –i 0.0.0.0:8001* and press **Enter**.
5. You should see *HttpDeleteServiceConfiguration completed with 0*.
6. Type *httpcfg set ssl –i 0.0.0.0:8001 –g {BA5393F7-AEB1-4AC6-B759-1D824E61E442} –h <THUMBPRINT>*, replacing *<THUMBPRINT>* with the values from the certificate thumbprint without any spaces and **Enter**.
7. You should see *HttpSetServiceConfiguration completed with 0*.
8. Restart the ESET Secure Authentication Core service for the new certificate to take effect.

## 4.3 Windows Server 2008

1. Click **Start** and type *cmd.exe* into the **Search** field.
2. In the list of programs, right-click **cmd.exe** and select **Run as administrator** from the context menu.
3. Type *netsh http show sslcert ipport=0.0.0.0:8001* and press **Enter**.
4. Copy and paste the content of the **Certificate Hash** field somewhere safe in case you want to re-add the existing certificate.
5. Type *netsh http delete sslcert ipport=0.0.0.0:8001* and press the **Enter**.
6. You should see the *SSL Certificate successfully deleted* message.

7. Type *netsh http add sslcert ipport=0.0.0.0:8001 appid={BA5393F7-AEB1-4AC6-B759-1D824E61E442} certhash=<THUMBPRINT>*, replacing *<THUMBPRINT>* with the values from the certificate thumbprint without any spaces and press **Enter**.
8. You should see *SSL Certificate successfully added* message.
9. Restart the ESET Secure Authentication Core service for the new certificate to take effect.