TECHNICAL PAPER

NETOP™

RemoteControl

Secure Remote Management and Support

Browser-based Support Console

Mass deployment of certificate

Netop

Netop develops and sells software solutions that enable swift, secure and seamless transfer of video, screens, sounds and data between two or more computers over the Internet. For more information, see www.netop.com.

Abstract

To remote control a host using the Browser-based Support Console without getting an invalid certificate warning message, you have to install a certificate which authenticates that the host is actually on the machine you want to connect to.

Introduction

An organization might choose using its own certificate with the Browser-based Support Console.

The system administrators should manually create a certificate from the Domain Controller, certificate which will only be valid within that domain.

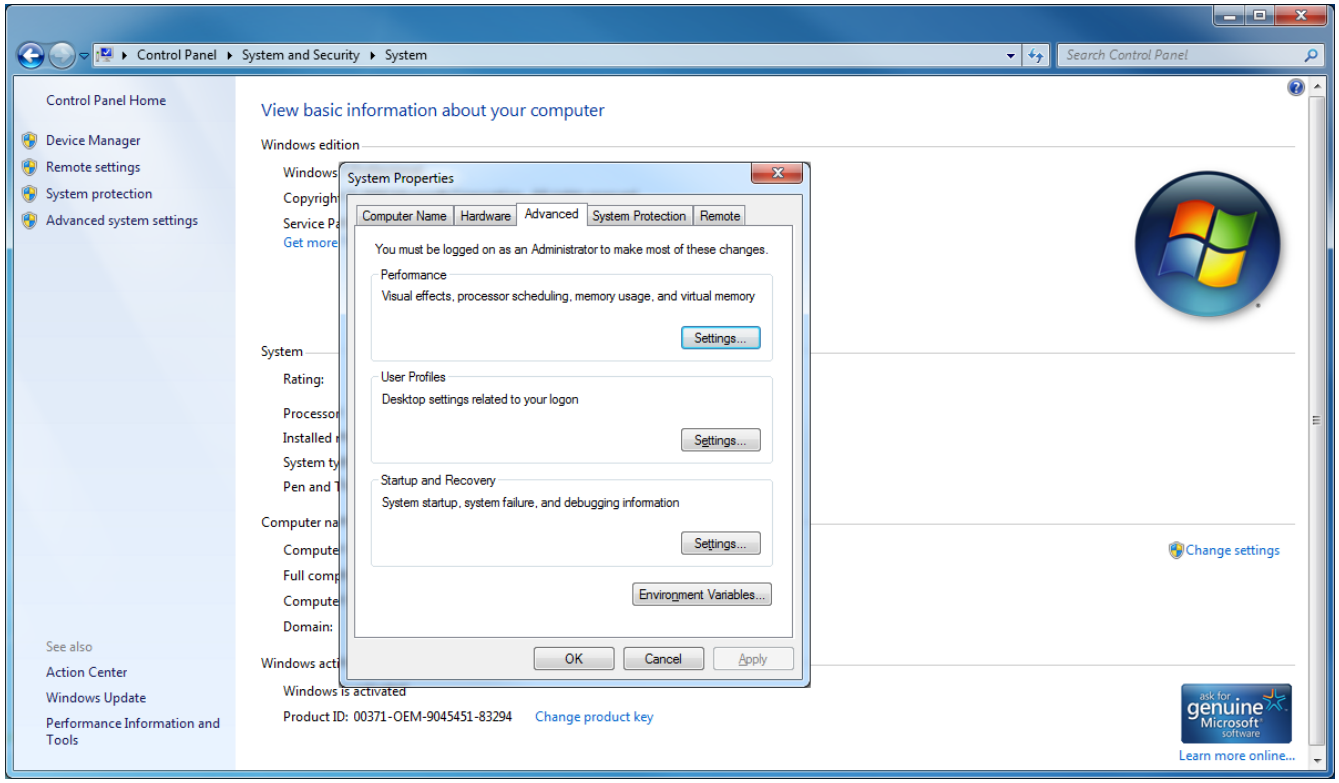
Please note that this will work only on Internet Explorer (IE) as Firefox has its own certificate management.

This article describes how to create a certificate, install it in the Trusted Root Certification Authorities Certificate Store and deploy the certificate to multiple computers.

1. Create a self-signed certificate

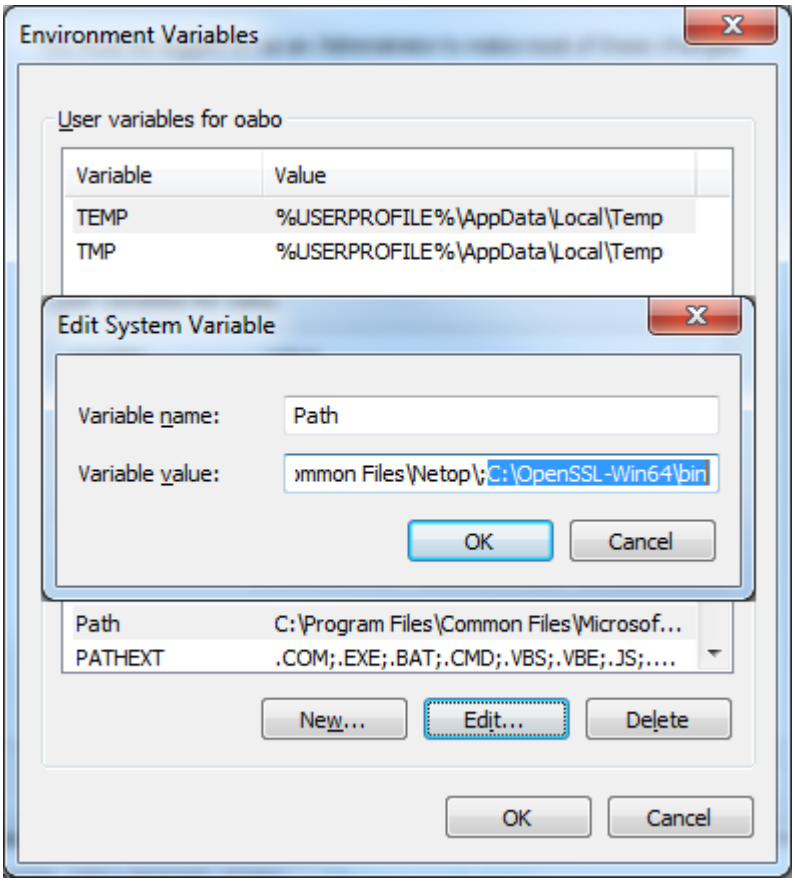
To create a self-signed (.pfx) certificate on Windows 7 or Windows XP:

1. Click here to download OpenSSL. Choose version 1.0.0L for developers.
2. Install .dll in the OpenSSL folder.
3. Add the **Openssl\bin** folder to the Path variable in the Environment Variables.
    a. Go to **Control Panel** > **System and Security** > **System** and on the left menu click **Advanced system settings**. The System Properties window displays.



b. Click the **Environment Variables** button and in the System variables section select the **Path** variable and click the **Edit** button.

c. Into the *Variable value* field, add the **OpenSSL\bin** folder and click **OK**. Please note directories are separated by semicolon.



4. From the command prompt, generate a RSA private key and a Certificate Signing Request (CSR) for your server.

   a. Go to the folder where you want to generate the private key:

   ```
   # In this sample the private key privkey will be generated into the certs folder.

   cd C:\certs
   ```

   b. Generate a RSA private key::

   ```
   # unencrypted, 2048-bit key

   openssl genrsa -out privkey.pem 2048

   # alternatively, encrypted

   openssl genrsa -des3 -out privkey.pem 2048
   ```

   Where, privkey is the filename of the private key to be generated. You can change the filename.

Note: If you choose to encrypt the key, you will have to enter the passphrase for this private key every time you start a server that uses it. This might not be possible; therefore, we recommend you to choose an unencrypted key

c. Generate the CSR:

```
openssl req –new –key privkey.pem –out req.csr
```

You will be asked to enter the following information:

- Country Name (2 letter code)
- State or Province Name (full name)
- Locality Name (e.g., city)
- Organization Name (e.g., company)
- Organizational Unit Name
- Common Name – enter the name of the machine where the host will be installed
- Email Address

You will be prompted to enter two extra (optional) attributes; afterwards the req.csr file will be created in the folder where you have chosen to create it.

5. Open the req.csr file and copy the content.
6. Submit a certificate request to the CA server:
   a. In IE, go to your Certificate Authority (CA) server and login using domain credentials.
   b. Select the Request a certificate task.
   c. Choose to submit an advanced certificate request.
   d. In the *Saved Request* field, paste the content of the req.csr file. From the *Certificate Template* drop-down list choose **NRCWebGuest**, and then click the **Submit** button. The certificate you requested is issued.
   e. Click the **Base 64 encoded** radio button and download the certificate to the folder where you have previously created the private key and CSR request.
7. From the command prompt run the following command:

```
# the name of the pfx certificate is mycertificate. You may choose another name of r the pfx certificate

openssl pkcs12 -export -in certnew.cer -inkey privkey.pem -out mycertificate.pfx
```

You have to enter export password in order to finish generating the pfx certificate. The password you enter here will be used to export the certificate on other machines.

Once you enter the password, the `mycertificate.pfx` will be created into the folder where you have previously created the private key and the CSR request.

2. Import certificate into Windows Certificate Store

To import the certificate in the Windows Store Certificate on the machine where the Netop Host is installed:

1. Open Certificate Manager by clicking the **Start** button **(for Windows 8 and later click on WINKEY and F)**, typing **mmc.exe** into the Search box, and then pressing **ENTER.**
2. Click the **File** tab and select the **Add/remove Snap-in** option.
3. In the *Available snap-in* select **Certificates** and click the **Add>** button. The *Certificates snap-in* wizard displays. Select the snap-in to always manage certificates for **Computer account** and click **Next**.
4. Select the snap-in to always manage the **Local computer** and click **Finish**.
5. Click **OK** and the wizard closes.
6. In the MMC window, go to **Console Root > Certificates (Local Computer) > Personal,** right click on *Certificates* and select **All tasks > Import…** The Certificate Import wizard opens. Click **Next**.
7. Browse to the location where the certificate is stored, select the certificate and click **Open**, then click **Next**.
8. Type the password for the private key that is included in the certificate file, select **Include all extendable properties** and click **Next**.
9. Click **Next** and **Finish**. The new certificate appears in the *Certificates (Local Computer) > Personal > Certificates* folder.

3. Configure the Netop Host to use the imported Windows Store certificate

1. Go to the Netop Host, click on the **Tools – Communication Profiles** entry menu, choose a Web profile in the list and click **Edit**. The *Communication Profile Edit* window displays.
2. Select the **Windows Certificate Store** radio button for the web communication, then click **Choose certificate…**
3. Go to **Server Authentication Certificates > Local Computer > Persona**l and choose the certificate and click **Select**.
4. Click **OK** and restart the Netop Host in order for the changes to take effect.

4. Check that the certificate warning does not display

From a machine which is in the local domain, open either Chrome or IE and enter *https:\\host-machine-name*. The “untrusted certificate” warning no longer displays as the certificate was issued by your Certificate Authority (CA) server to host-machine-name.

Note: If the Certificate Authority for the added certificate does not exist on the machine from which the Browser-based Support Console is launched, import the CA root certificate in the **Trusted Root Certification Authorities.**

5. Mass-deploying the certificate using Group Policy

This procedure describes how to deploy a certificate to multiple computers by using Active Directory Domain Services and a Group Policy Object (GPO).

Prerequisite: You should have domain administrator rights (membership in the Domain Administrators group) in order to complete this procedure.

This procedure applies to: Windows Server 2003, Windows Server 2003 R2, Windows Server 2003 with SP1, Windows Server 2003 with SP2

1. Open the Group Policy Management console. To open the console, click **Start** button, click **Control Panel**, click **Administrative Tools,** and then click **Group Policy Management**.
2. Find an existing or create a new GPO to contain the certificate settings. Ensure that the GPO is associated with the domain, site, or organizational unit whose users you want affected by the policy.
3. Right-click the GPO, and then select **Edit**.
4. Group Policy Management Editor opens, and displays the current contents of the policy object.
5. In the navigation pane, go to **Computer Configuration**>**Policies**>**Windows Settings**>**Security Settings**>**Public Key Policies**>**Trusted Publishers**.
6. On the **Action** menu, click **Import**.
7. Follow the instructions in the Certificate Import Wizard to find and import the certificate.
8. If the certificate is self-signed, and cannot be traced back to a certificate that is in the Trusted Root Certification Authorities certificate store, then you must also copy the certificate to that store. In the navigation pane, click Trusted Root Certification Authorities, and then repeat steps 5 and 6 to install a copy of the certificate to that store.

.