TECHNICAL PAPER

NETOP™

RemoteControl

Secure Remote Management and Support

Browser-based Support Console

HTTPS using self-signed 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.

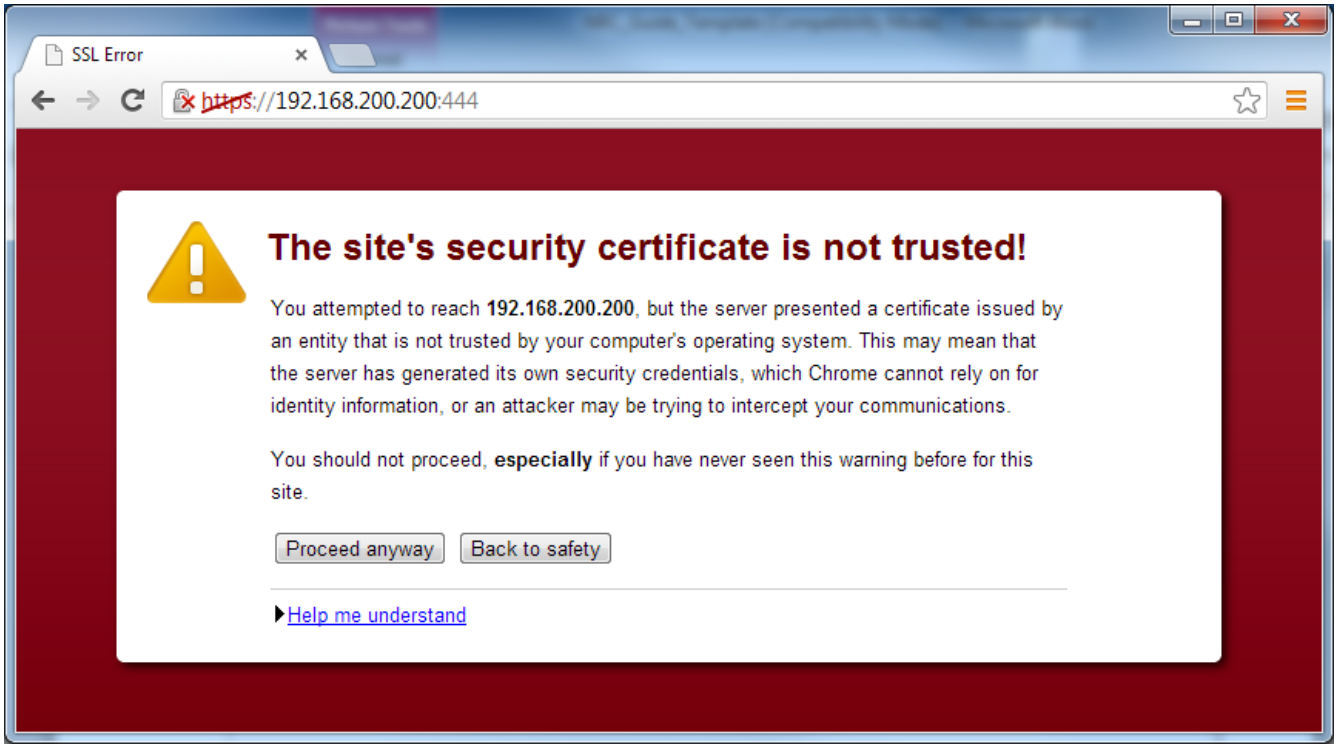
Abstract

If SSL is enabled on the Netop Host, when running the Browser-based Support Console, a warning message displays stating that the certificate is incorrect.

Introduction

If SSL is enabled on the Netop Host, to run the support console, open a browser and type **https://** and the **IP** address or **Computer Name** of the target device (e.g. https://192.168.1.10 or https://target-device).

When loading the page, you will be prompted with a message saying that the certificate is not correct.

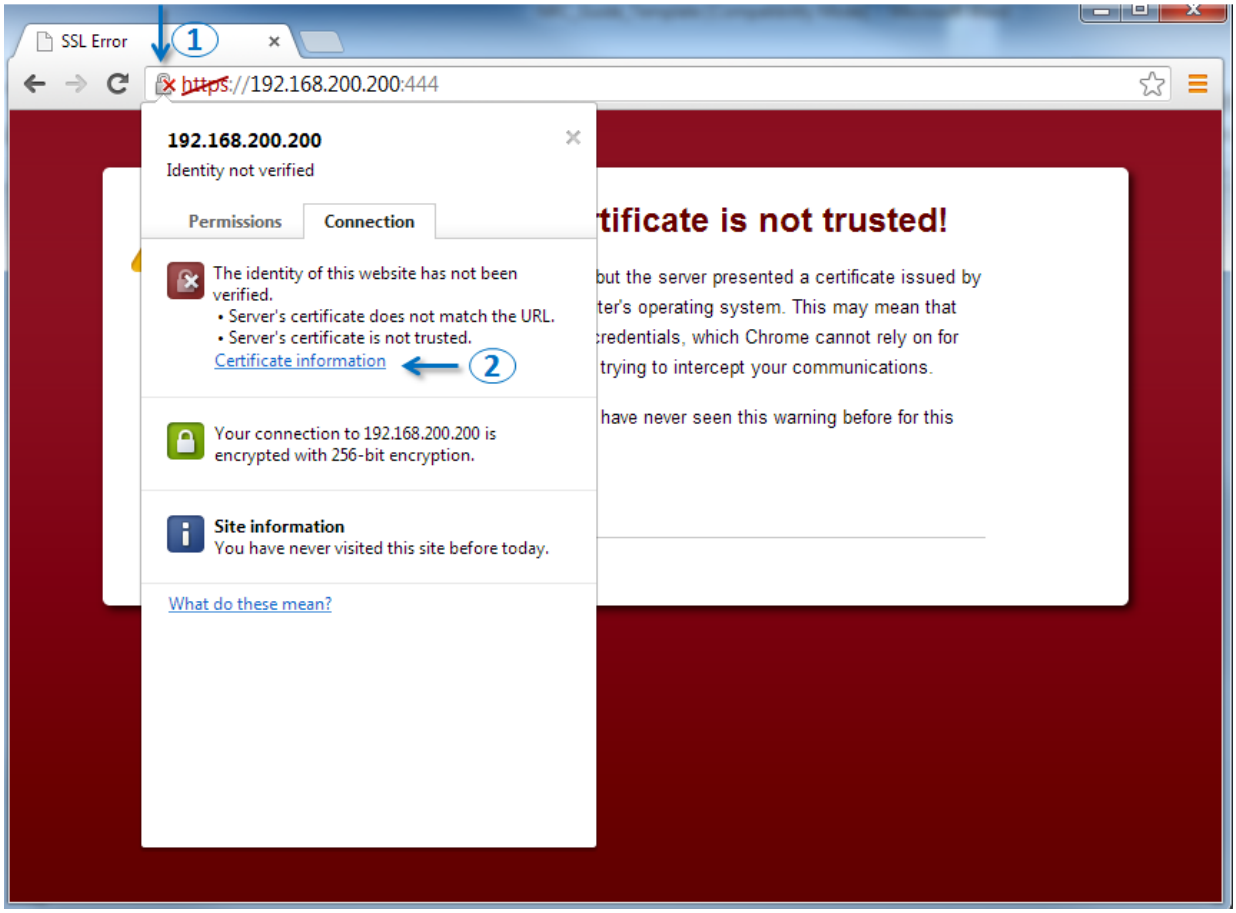


This is a result of a self-signed certificate, one not provided by a certified authority (e.g. from VeriSign or the like). This is normal behavior, but you will need to accept the certificate to establish a remote session. Despite this warning, all data, when https:// is used, is **encrypted**.

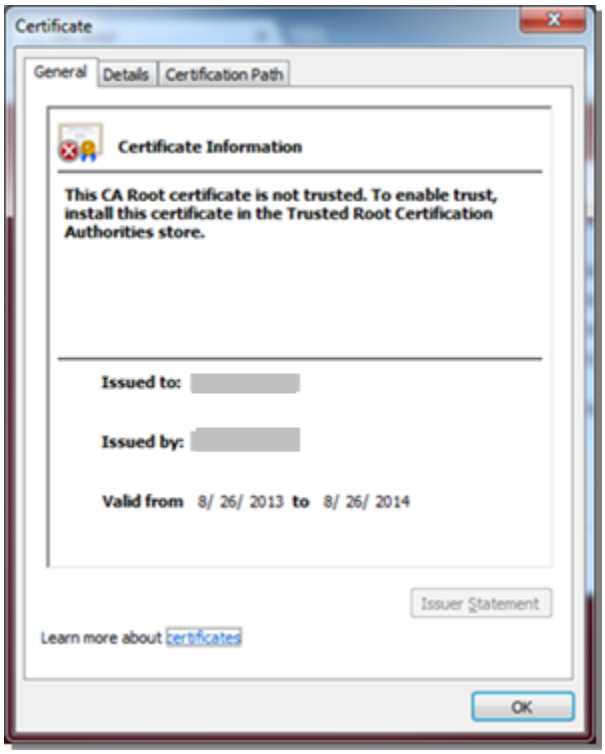
In order to have this screen not show up, go through the following steps.

Retrieve the self-signed certificate

1. Open a browser and type **https://** and the **IP address** or **Computer Name** of the target device (e.g. https://192.168.1.10 or https://target-device). A warning is displayed stating that the certificate is invalid.
2. Click the lock icon in front of the URL address.



Click Certificate information link to view certificate details.



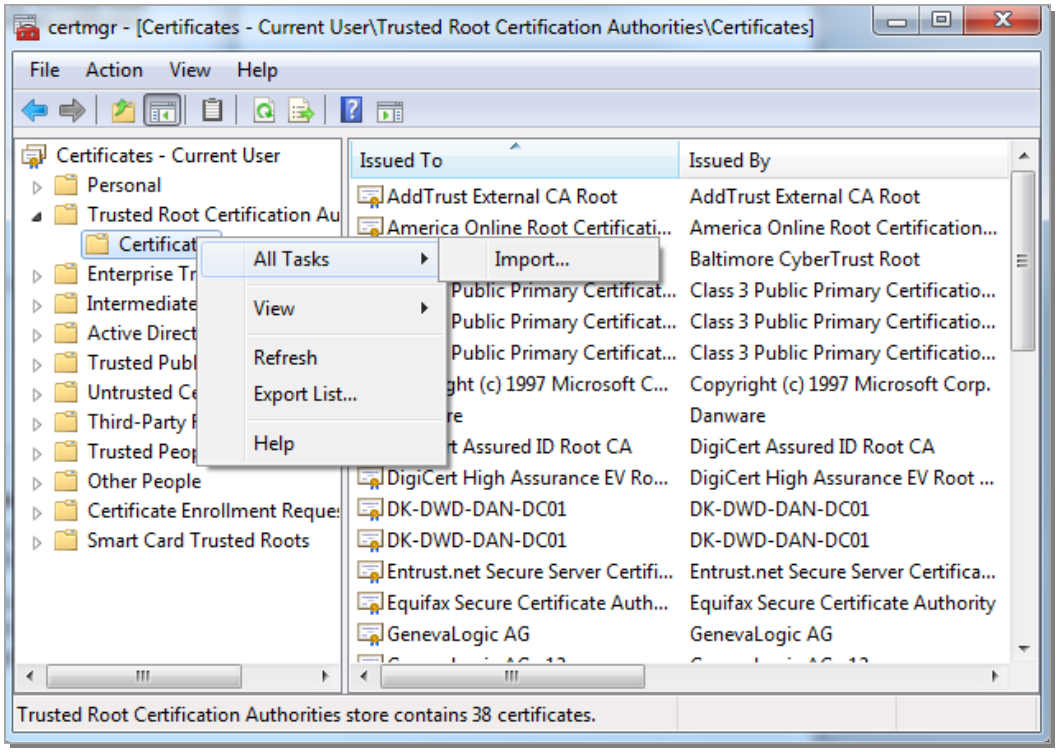
3. Export certificate to the host computer. In order to do that, go to the **Details** tab, click **Copy to File** button and complete the **Certificate Export Wizard**.

Import the certificate

The certificate can be imported using a Group Policy – Click **here** for step by step instructions.

If not, it can be imported manually on every device using the following steps:

1. Go to the Windows Certificate Manager (that is, **certmgr.msc**) section **Trusted Root Certification Authorities** > **Certificates**, right-click on Certificates and select **All Tasks** > **Import**.



2. Import the previously saved certificate. In order to import the new certificate, complete the **Import Certificate Wizard**.

Note: For Mac go through the steps described **here** in order to retrieve and import the certificate.

Once the certificate is imported into the Certificates Manager, when connecting to the host, the certificate warning message will no longer display. Please note the warning message displays if the Host certificate is regenerated in one of the following situations:

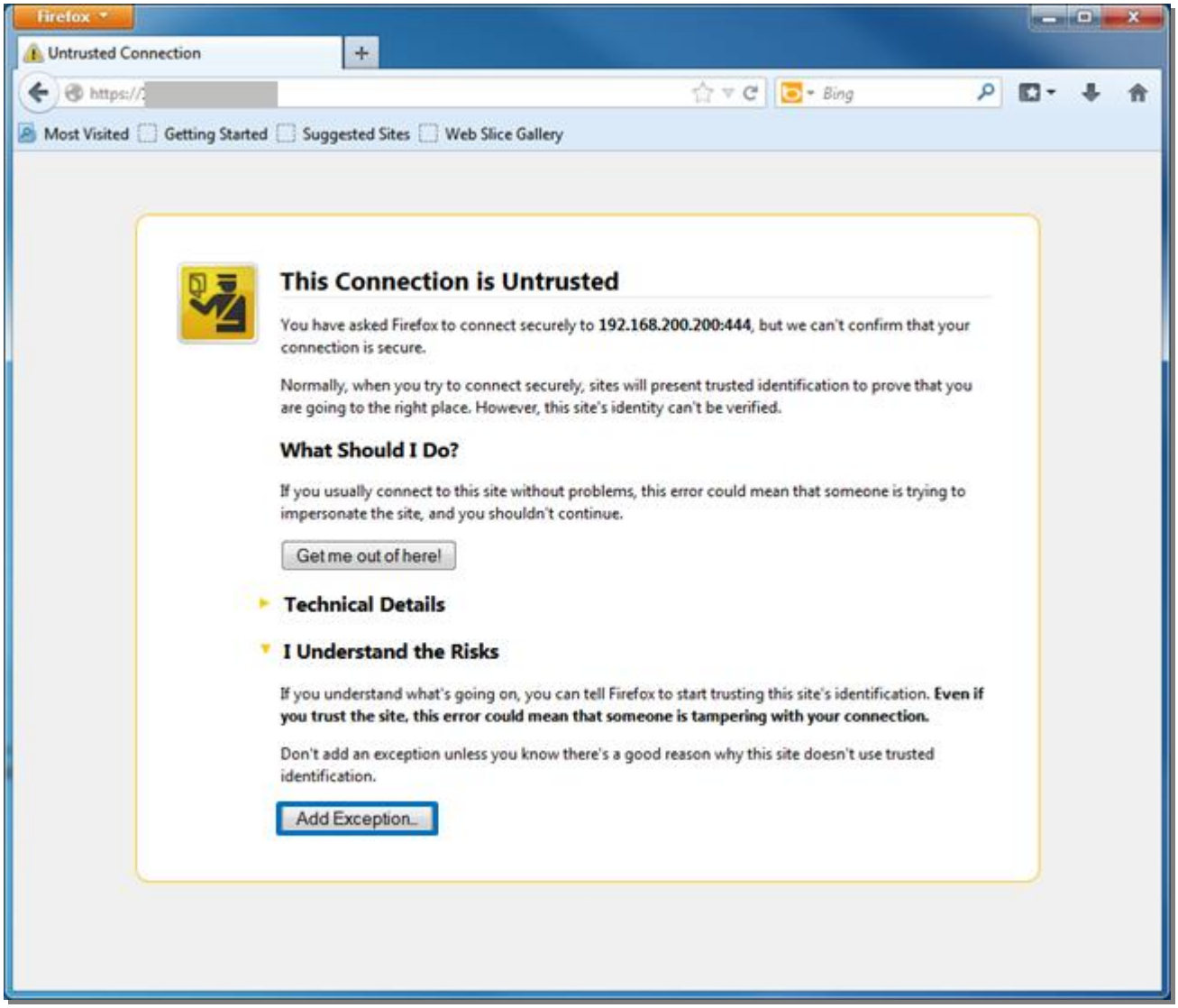
- Host reinstallation
- Certificate expired
- Certificate became invalid for varied reasons.

Note: The certificate was issued for the Host computer name, therefore once you have imported the Host certificate, connect to the Host using the computer name https://<host computer name>. Otherwise, the security certificate warning will be displayed again.

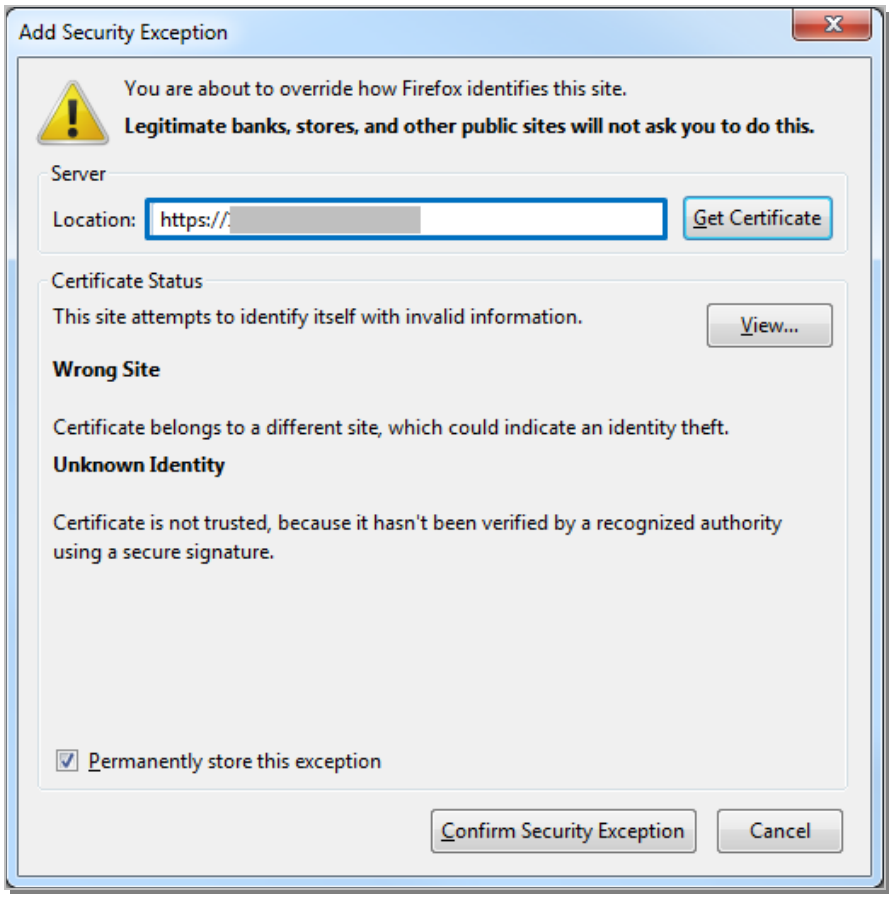
What do on Firefox

Firefox provides an easier way for importing the certificate.

When first loading the page click **Add Exception…** under **I Understand the Risks**



Click **Confirm Security Exception**



Browser Behavior after importing the certificate

The browser behavior will be the same as with a CA certificate, except:

- Chrome (Windows & Mac) - displays ~~**https**~~ instead of **https**
- Firefox (Mac) – security screen is still displayed after certificate import. You will need to use **Add exception** in order to remove all notifications.

