CA NetQoS Performance Center

Install and Configure SSL for Windows Server 2003

Release 6.1 (and service packs)

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Installing and Configuring SSL

This document shows you how to install and configure Secure Sockets Layer (SSL) for use by CA NetQoS Performance Center and its data sources. Perform the procedures in the order in which they appear in the document.

This section contains the following topics:

Prerequisites

Before attempting to configure SSL for CA NetQoS Performance Center, ensure that your data source applications are installed, configured, and registered as data sources for CA NetQoS Performance Center.

Create or Import the Certificate

SSL requires you to create a self-signed certificate or to import a certificate from CA.

Create a Self-Signed Certificate

Use this procedure if you did not receive a certificate from CA. Perform the procedure on the CA NetQoS Performance Center console server.

(*Optional*) Perform the procedure on the data source console server to enable seamless (using SSO) drill down from CA NetQoS Performance Center into the data source.

Follow these steps:

1. Download and run the IIS 6.0 Resource Kit Tools (iis60rkt.exe) from the Microsoft Download Center:

   http://www.microsoft.com/downloads/en/details.aspx?FamilyID=56fc92ee-a71a-4c73-b628-ade629c89499&DisplayLang=en

2. Open a command prompt window and navigate to the following directory:

   `C:\Program Files\IIS Resources\SelfSSL`

3. Run the following command:

   `Selfssl.exe /T /N:CN=server name`

   server name

   Provide the host name or the FQDN of the CA NetQoS Performance Center server or the data source console server. This name becomes the name of the certificate. This field can accept several options. Review the selfssl.exe options for details.

   Note: The **/T** option adds the self-signed certificate to the Trusted Certificates list. Your local browser trusts the self-signed certificate when this flag is specified.

4. Verify that the certificate is trusted:

   a. Click Start and type **mmc** in the search field. The Console Root window opens.

   b. Add the certificate snap-in for the local computer:

      - In the Console Root window, click File, Add/Remove Snap-in.
      - Double-click Certificates in the Available snap-ins list and select 'Computer account' from the Certificates snap-in dialog.
      - Click Next.
      - Select 'Local computer' in the Select Computer dialog.
      - Click Finish.
      - Click OK in the Add or Remove Snap-ins dialog.

   c. In the left pane of the Console Root window, expand Certificates (Local Computer).

   d. Expand Trusted Root Certification Authorities and click Certificates. The list of certificates appears in the center pane.

   e. Find your certificate in the list.

Import a Certificate

Use this procedure if you received a certificate from CA. Perform this procedure on the CA NetQoS Performance Center console server.

(*Optional*) Perform the procedure on the data source console server to enable seamless (using SSO) drill down from CA NetQoS Performance Center into the data source.

Follow these steps:

1. Click Start, Run, and then type **mmc**. The Console Root window opens.
2. Add the certificate snap-in for the local computer:
    a. In the Console Root window, click File, Add/Remove Snap-in.
    b. Double-click Certificates in the Available snap-ins list and select 'Computer account' from the Certificates snap-in dialog.
    c. Click Next.
    d. Select 'Local computer' on the Select Computer dialog.
    e. Click Finish.
    f. Click OK in the Add or Remove Snap-ins dialog.
3. Import the certificate:
    a. In the left pane of the Console Root window, expand Certificates (Local Computer).
    b. Right-click 'Trusted Root Certification Authorities', then click All Tasks, Import.
    c. Click Next in the Certificate Import Wizard.
    d. In the File name field, use the Browse button to find and select the certificate from CA.
    e. Click Next, and then click Finish.
4. Verify that the certificate is trusted:
    a. In the left pane of the Console Root window, expand Certificates (Local Computer).
    b. Expand 'Trusted Root Certification Authorities' and click Certificates. The list of certificates appears in the center pane.
    c. Find your certificate in the list.

Configure the IIS Application

The procedure shows you how to configure IIS to respond to SSL requests. Configuring IIS consists of configuring an SSL port for HTTPS, assigning the certificate to the web server, and modifying the HTTP header expiration.

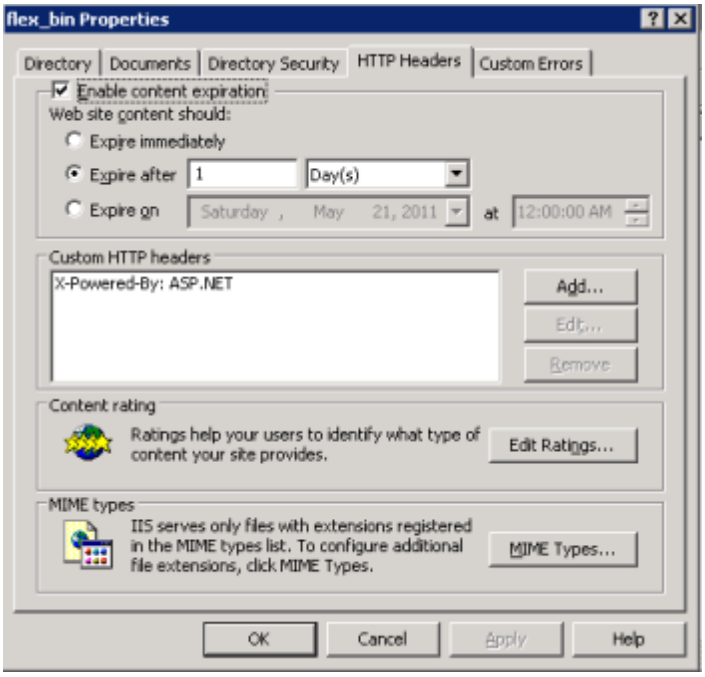
Perform the procedure on the CA NetQoS Performance Center server and the data source server.

Follow these steps:

1. Configure the SSL port and assign the certificate. By default, IIS does not have a port defined for HTTPS.
    a. Open the Internet Information Services (IIS) Manager window.
    b. In the left pane, right-click Default Web Site and select Properties.
    c. On the Web Site tab of the Default Web Site Properties dialog, enter **443** in the 'SSL port' field.
    d. Click Apply.
    e. On the Directory Security tab, click Server Certificate.
    f. In the IIS Certificate Wizard, select 'Assign an existing certificate' and then click Next.
    g. In the Available Certificates list, select the certificate you imported or created from Create or Import the Certificate (see page 7). Then click Next.
    h. In the 'SSL port this web site should use' field, enter **443**, and then click Next.
    i. Accept all default options for the remaining dialogs, clicking Next until the wizard is complete.
2. Modify the HTTP header expiration for CA NetQoS Performance Center:
    a. In the left pane of the IIS Manager window, expand the 'npc' folder.
    b. Right-click the 'flex_bin' folder and select Properties.

c. On the HTTP Headers tab of the Properties dialog select 'Enable content expiration.'

d. Select 'Expire after' and enter '**1**' and '**Day(s)**' in the fields to the right.



e. Click OK.

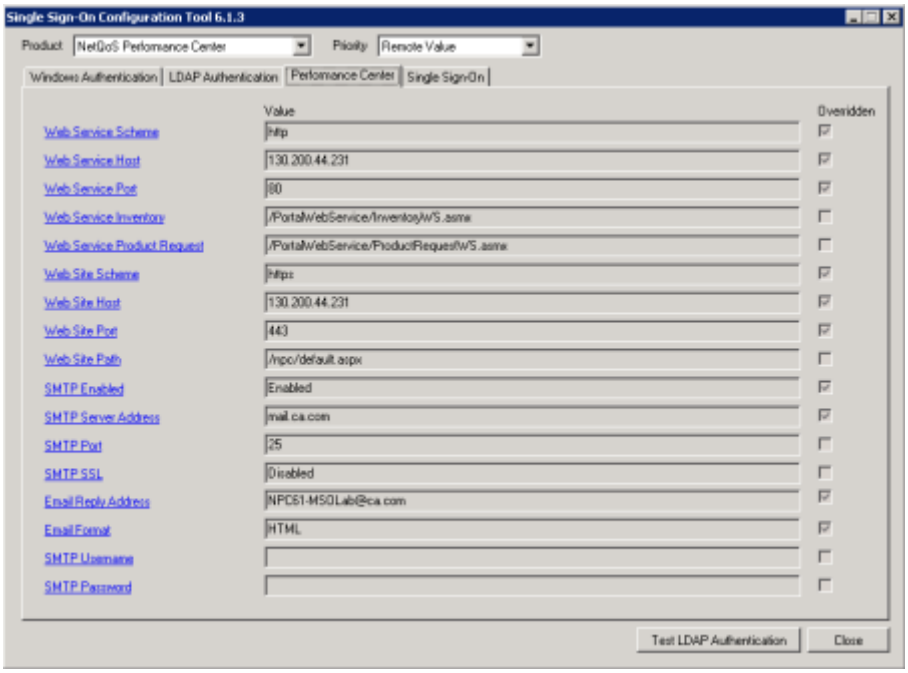
Enable HTTPS Through Single Sign-On

Use the Single Sign-On (SSO) Configuration tool to enable HTTPS. Your changes are propagated to data sources during synchronization.

Perform the procedure on the CA NetQoS Performance Center server and the data source server.

Follow these steps:

1. On the desktop of the CA NetQoS Performance Center server, double-click the SSO icon to open the tool.
2. Click the Performance Center tab. The field names are clickable links.



3. Click the following field names to make the indicated overrides:
   - Web Site Scheme: Change to **https**.

     Important: Although you are changing the scheme, web services continue to run on HTTP.
   - Web Site Host (for SSO version 6.1.3 only): Change to the name of the certificate you created or imported in Create or Import the Certificate (see page 7).
   - Web Site Port: Change to **443**.

4. Click the Single Sign-On tab. The field names here are also clickable.
5. Click the following field names to make the indicated overrides:
   - Scheme: Change to **https**.
   - Port: Change to **443**.

   Note: These fields control the SSO login pages for CA NetQoS Performance Center and the data sources.

Modify the Single Sign-On XML Files

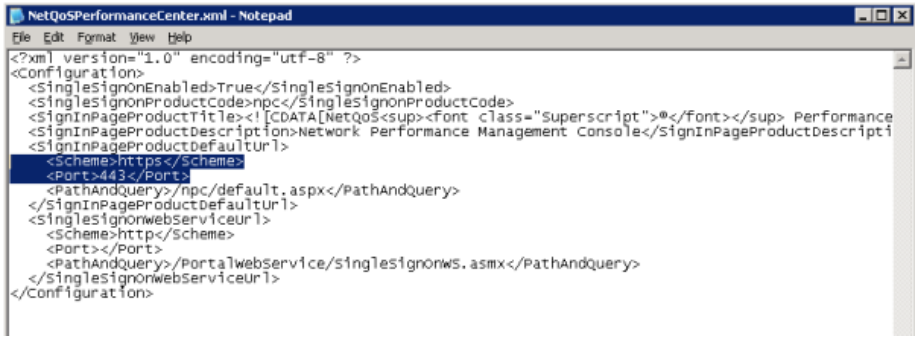
The SSO configuration XML file controls the SSO settings.

Perform this procedure only on the CA NetQoS Performance Center server.

Follow these steps:

1. Navigate to the following directory:

   `D:\NETQOS\SingleSignOn\Configuration.`
2. Open the NetQoSPerformanceCenter.xml file in a text editing tool.
3. Under <SignInPageProductDefaultURL>, change the Scheme and Port fields as shown in the following picture:



   - Scheme: Change to **https**.
   - Port: Change to **443**.

     Important: Do not change any other field.
4. Save your changes and close the file.
5. In a command-line window, run the following command:

   `iisreset`

   This command forces the website to reload and enables HTTPS access to the website.

Modify the Data Source Connection Method

Perform this procedure *only* if you want to seamlessly (using SSO) drill-down from CA NetQoS Performance Center into a data source.

This procedure enables the drill-down links to use HTTPS.

Follow these steps:

1. In the CA NetQoS Performance Center console, click Admin, Data Sources in the menu bar.
2. Right-click the name of the data source you want to configure and click Edit.
3. In the Edit Data Source dialog, disable the 'Same as above' check box in the Web Console area. Because the web services still run on HTTP, they do not use the same configuration as the data source.
4. Complete the new Host Name, Protocol, and Port fields as follows:
   - Host Name: Provide the same host name that you provided when you created or imported the certificate (see page 7).
   - Protocol: Select 'https'.
   - Port: Enter **443**.
5. Click Save.
6. Repeat steps 2 through 5 for each data source you want to configure.

Verify Database Settings

The final task in the process is to verify several database settings. You want to ensure that CA NetQoS Performance Center uses the same host name or FQDN that is listed on the certificate.

Follow these steps:

1. From a command prompt, connect to the CA NetQoS Performance Center database:

   ```
   mysql netqosportal
   ```

2. From a command prompt, list all the settings for SSO:

   ```
   "select * from performance_center_properties;"
   ```

   The list of settings includes the following fields, which are listed as Priority 1:

   - NpcWebSiteHost: set to the FQDN or hostname
   - NpcWebSiteScheme: set to https
   - NpcWebSitePort: set to 443
   - SsoScheme: set to https
   - SsoPort: set to 443

3. From a command prompt, change the performance_center_properties value that updates the FQDN or host name in the data_sources2 table:

   ```
   REPLACE INTO performance_center_properties VALUES ('NpcWebSiteHost', 2,
   'NPC.fqdn.com', 'N', UNIX_TIMESTAMP());
   ```

   NPC.fqdn.com

   Provide the actual FQDN or host name from the certificate.

4. Restart the NetQoS Device Manager Service on the CA NetQoS Performance Center server.

   After the restart, you will have three entries for NpcWebSiteHost. Each entry has a value of 0, 1, and 2, respectively. The entry with a priority of 2 is the entry for the data_sources2 table.

   Note: The underlying data sources do not have priority 2 in the performance_center_properties table.

5. Repeat step 1, and then run the following command to display the console settings that CA NetQoS Performance Center uses when generating a PDF:

   ```
   "select * from data_sources2;"
   ```

   The list of settings includes the following fields:

   - ConsoleHost (for SourceID 0, which is CA NetQoS Performance Center): set to the priority 2 NpcWebSiteHost value in performance_center_properties
   - ConsolePort: set to 443 as updated by the NpcWebSitePort value in performance_center_properties
   - ConsoleProtocol: set to https as updated by the NpcWebSiteScheme in performance_center_properties.

6. For the CA NetQoS Performance Center and data source servers, add the DNS suffix to the computer name if you are using FQDN.

   a. Right-click My Computer and select Properties.

   b. On the Computer Name tab, click Change.

      The Computer Name/Domain Changes dialog opens.

c. Ensure the 'Computer name' and 'Domain' or 'Workgroup' fields are accurate.

d. Click More.

   The DNS Suffix dialog opens.

e. In the 'Primary DNS suffix of this computer' field, provide the DNS suffix to make the full computer name match the certificate.

f. Click OK in the DNS Suffix dialog.

g. Click OK in the Computer Name/Domain Changes dialog.

h. Click OK in the Properties dialog.

i. Reboot the server.

7. Ensure that the URL for accessing CA NetQoS Performance Center matches the FQDN or host name from the certificate and the database settings.

Known Issues

This topic presents known issues and their workarounds.

Images Do Not Appear in a PDF

For CA NetQoS Performance Center 6.1.158 and 6.1.194 SP1, images in PDFs sent in scheduled email do not appear when you use SSL.

Workaround: Apply the patch to 6.1.158 or 6.1.194 SP1, or install version 6.1.205 SP2, which includes the patch. You can obtain the patch from the following locations:

- ftp://ftp.ca.com/pub/netqos/product_patches/NPC/6.1/26034-NPC.6.1.158.SSL.SchedEmailPatch.zip
- ftp://ftp.ca.com/pub/netqos/product_patches/NPC/6.1.194%20%28SP1%29/26034-NPC.6.1.194.SSL.SchedEmailPatch.zip

Note: If you upgrade from 6.1.158 to 6.1.194 SP1, reapply the patch after upgrading. You do not need to reapply the patch when upgrading to 6.1.205 SP2 from either of the earlier versions.