NetQoS
Performance First

NetQoS Single Sign-On 6.1
User Guide

CA NetQoS Single Sign-On User Guide

DSSO61UG-1

Contents

PREFACE

About This Document

The purpose of this document is to give a brief explanation of the Single Sign-On feature and its architecture. This document provides administrators with instructions on how to modify settings in individual instances of a single sign-on website if they would like to change their default configuration.

Single Sign-On is the term used to describe the authentication scheme used by all NetQoS products. Aside from providing a **Sign In** screen, the Single Sign-On feature provides LDAP and Windows Authentication support for every NetQoS product and the ability for a user to only have to sign in once when changing between NetQoS products. For example, if a user signed into the NetQoS Performance Center and then drilled into a view that took them to Reporter Analyzer they would not have to sign in again.

Note: Changes made in the Single Sign-On configuration tool only affect newly created Windows Authentication and LDAP users. They do not apply to existing Windows Authentication or LDAP users registered within NetQoS Performance Center.

Note: Administrators should be aware that their updates to the Single Sign-On website only affect those NetQoS products that are running on the same server because of the distributed architecture.

Chapter	Description
"Setting Up Single Sign-On" on page 7.	This chapter provides an overview of Single Sign-On and how to set up Single Sign-On.
"Single Sign-On Configuration Tool" on page 21	This chapter provides a detailed description of how to configure Single Sign-On using the Configuration Tool.
"Properties in the Configuration Tool" on page 27	This chapter provides detailed descriptions of the fields used in the Configuration Tool.

Conventions

The following conventions are used in this book:

- In instructions, **boldface** type highlights information that you enter or GUI elements that you select.
- All syntax and literal examples are presented in this typeface.
- In syntax, path names, or system messages, text enclosed in angle brackets (<>) represents a variable as shown in the following example:

  net time/setsntp: <*ntpserver*>

Providing Documentation Feedback

We want to help you use our products effectively so that you can work quickly and efficiently. By telling us about your experience with this document, you can help us achieve that goal. Send an email message with your feedback to our technical publications team at the following address: docfeedback@netqos.com

CHAPTER 1

Setting Up Single Sign-On

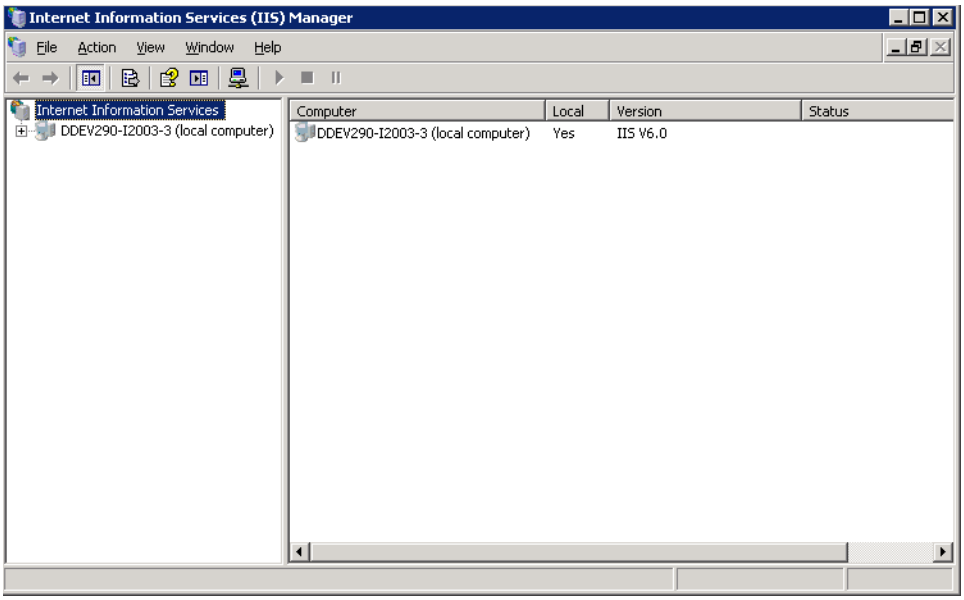
This chapter describes how to install and set up Single Sign-On. You will need to refer to Chapter 2, "Single Sign-On Configuration Tool" on page 21 for information on how to configure Single Sign-On once it is installed.

This chapter contains the following topics:

Determining Which Version of IIS You Are Running

By default, each Single Sign-On website resides in an Internet Information Services (IIS) Virtual Directory named **SingleSignOn**. This website does not use SSL. If you would like to change the Virtual Directory for the Single Sign-On website and/or make this Virtual Directory use SSL, you are going to need to know the version of IIS you are working with. If you already know your version of IIS, or if you do not want to make any changes to the default IIS configuration, then you can skip this section of the document. Otherwise, below are the steps you can follow to determine your version of IIS:

1. Click **Start**>**Programs**>**Administrative Tool**s>**Internet Information Services (IIS) Manager**
2. The **Internet Information Services (IIS) Manager** window will pop up. Select **Internet Information Services** in the left pane and look at the information under the column titled **Version** in the right pane. This will give you the version we're looking for. In this example, we're running IIS 6.0.



3. Go to the **File** menu and select **Exit** to close the Internet Information Services (IIS) Manager window.

Note: Administrators should be aware that their updates to the Single Sign-On website only affect those NetQoS products that are on the same server because of the distributed architecture.

Confirming Single Sign-On Functionality

After setting up Single Sign-On, open each NetQoS product on the modified server the way you normally would. If you are automatically signed into a product, sign out and then verify that the Sign In page URL has the updated Virtual Directory that you added. The URL should look something like `http://<Host>/<VirtualDirectory>/SignIn.aspx?SsoProductCode=...` where <*Host*> is the host name of the server and **<***VirtualDirectory***>** is the name of the Virtual Directory you created. Make sure to sign in and sign out of each NetQoS product on the modified server and verify that your change occurred.

Note: Administrators should be aware that their updates to the Single Sign-On website only affect those NetQoS products that are on the same server because of the distributed architecture.

Single Sign-On and Secure Sockets Layer and Certificates

By default, the Single Sign-On website uses the HTTP protocol. For most customers, this setup will suffice. However, some administrators may choose to have more enhanced security. This section gives pointers for those who wish to use Secure Sockets Layer (SSL) and certificates in IIS.

Although HTTP is the primary protocol for most websites on the Internet, it does have its drawbacks. In particular, all of the traffic between the client and the server is done in clear text. This means that there is the potential for someone to view data being transferred back and forth. That said, you can encrypt the information being transmitted by configuring the Single Sign-On website to use SSL. In order to successfully use SSL though, you need to obtain a server certificate. These can be obtained locally or via a trusted third party. Some administrators may also choose to use client certificates for further security.

Configuring a website in IIS to use SSL, server certificates, and client certificates is outside the scope of this document. However, the following Microsoft article gives an in-depth discussion of the use of these IIS website security features. Likewise, it provides links to other technical documents that give instructions for setting up SSL and obtaining and installing server and client certificates in IIS 6.0.

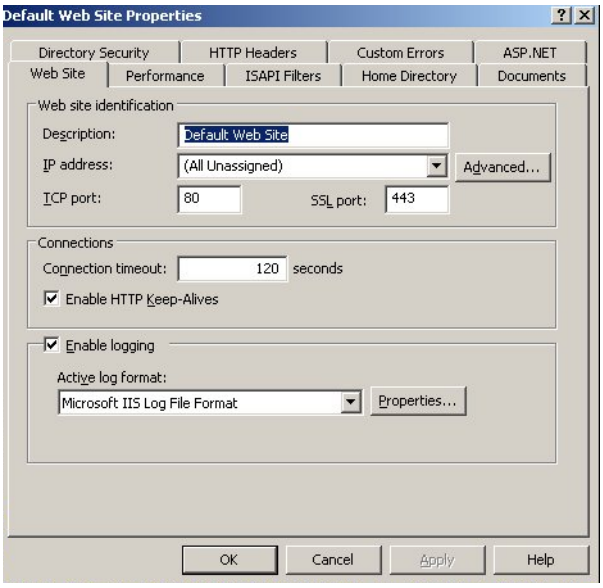
`SSL and Certificates (IIS 6.0):` `http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/559bb9d5-0515-4397-83e0-c403c5ed86fe.mspx?mfr=true`

Please note, if you do choose to use SSL and certificates with the Single Sign-On website, you will need to update the various NetQoS products on the same server with your new Single Sign-On website URL scheme (ie: https) and port (ie: 443). Each product needs this information so that they can redirect a user if they are not authenticated. This step can be done using the Single Sign-On Configuration Tool. You will need to override the **Scheme** and **Port** values under the **Single Sign-On** tab for each product in the Single Sign-On Configuration Tool. For more details on this step, please see "Single Sign-On Configuration Tool" on page 21.

Note: Administrators should be aware that their updates to the Single Sign-On website only affect those NetQoS products that are on the same server because of the distributed architecture.

Using SSL Certificates

1. On the NetQoS product server, open IIS, click start->programs->administrative tools->IIS
2. Select the Website tab.

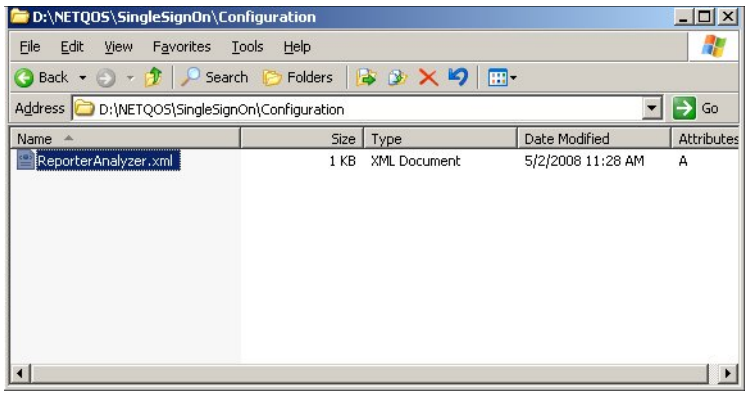


3. In the SSL port field, enter 443.
4. Open the Single Sign On Configuration Tool.

```
D:\NETQOS\SingleSignOnConfigurationTool\SsoConfig.exe
```

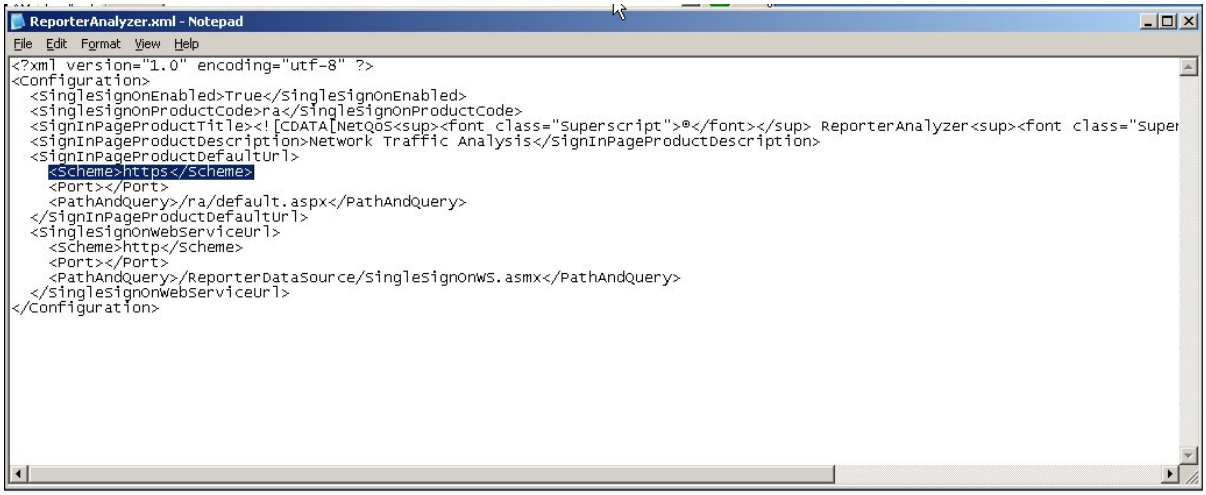
5. Select the Single-Sign On tab.
6. Change the **Scheme** to `https`.
7. Change the **Port** to `443`.
8. Navigate to D:\NETQOS\SingleSignOn\Configuration
9. In Notepad, open the *productname*.xml file for the appropriate product in .

Note: You will need to perform this step for each NetQoS appliance.



10. Change the <*scheme*> **https**.

Note: The web service will not be impacted by this change. Only data delivered to the web browser will be encrypted.



11. From the **Start** button, go to **Control Panel**/**Administration Tools**/**Internet Information Services (IIS) Manager**.

12. Open the NPC folder.

13. Right-click the `config.xml file` in the right hand window to and select **Properties**.

14. Click the **HTTP Headers** tab and set the Website content to Expire after 1 Day(s).

15. Click **OK** to close the window.

16. Right-click the **Flex_bin** folder in the right hand window and select **Properties**.

17. Click the **HTTP Headers** tab and set the website content to Expire after 1 Day(s).

18. Click **OK** to save the settings.

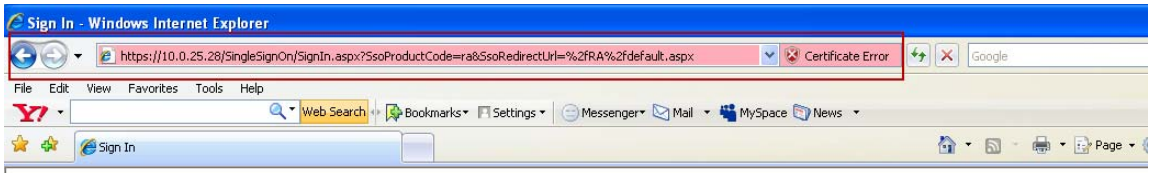
19. Perform a command prompt IIS reset.

Note: Users must clear their cache to see the changes.

20. Open the product.

21. Click **Continue to this Website (not recommended)** when you receive the *There is a problem with this website's security certificate message*.

22. In the browser address bar, the address should be an https:// address.



Note: To change the port, repeat the steps using a different port and perform an iisreset.

Using SSL Certificates with NetQoS NetVoyant

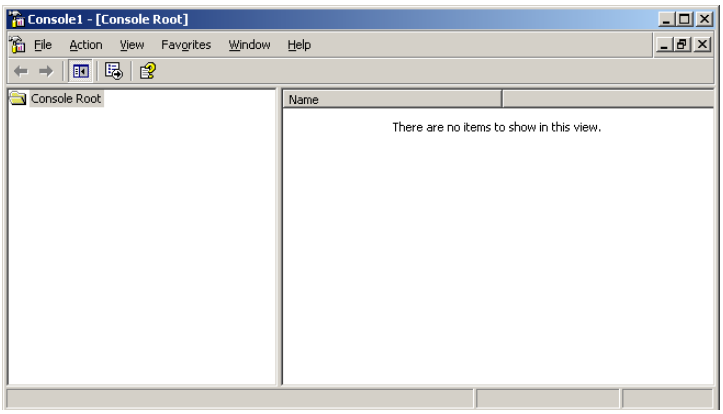
The NetVoyant Console is a Java application that requires some configuration changes to work with SSL certificates. This document describes the configuration changes and how to get the Console to recognize the certificate. Perform the following steps to configure SSL certificates to work with the NetVoyant Console.

Find or Export the SSL Certificate

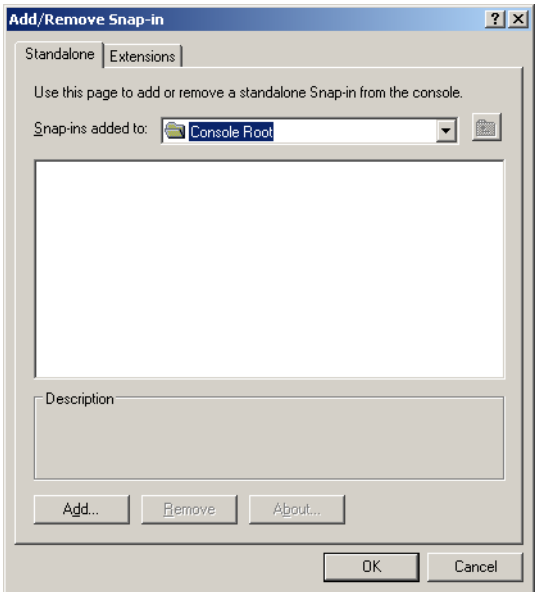
Copy the SSL certificate to the NetVoyant directory. For this example, we will use the file name `iis.cer`. this can be the original certificate file received from the organization that signed the certificate or it can be exported using the Microsoft Management Console.

If you want to export a certificate, here are the basic steps:

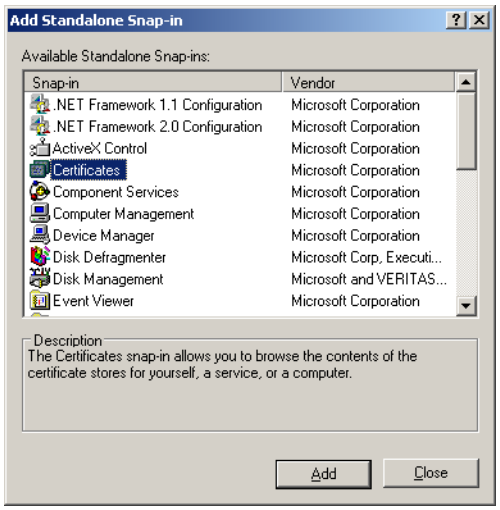
1. Click **Start** > **Run**.
2. Type `mmc`. A new console will open:



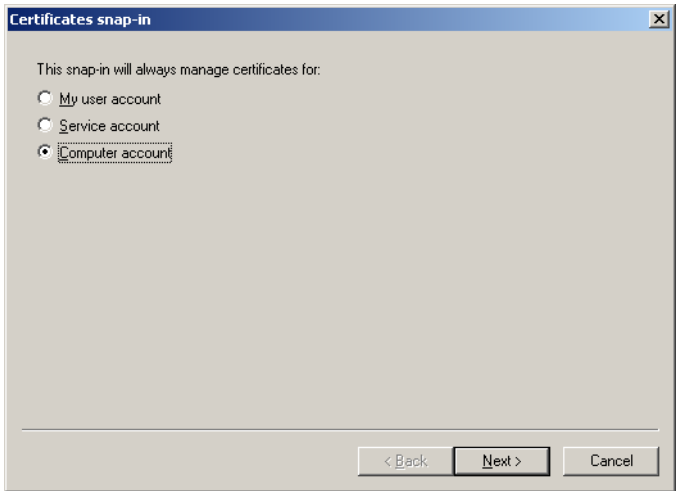
3. Go to **File** > **Add/Remove Snap-In**.



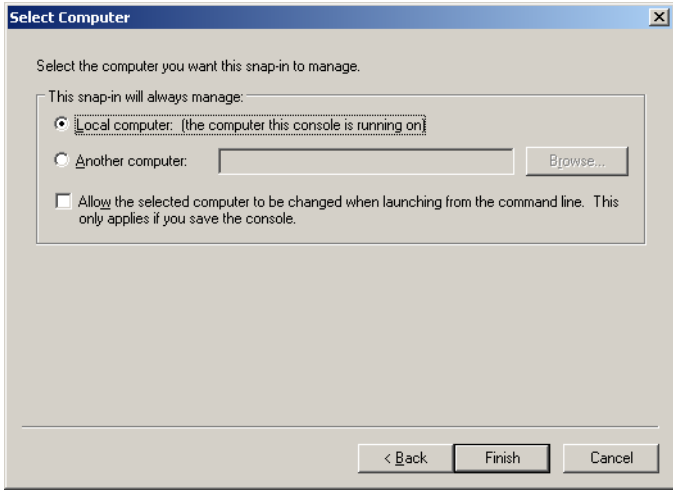
4. Click **Add.**



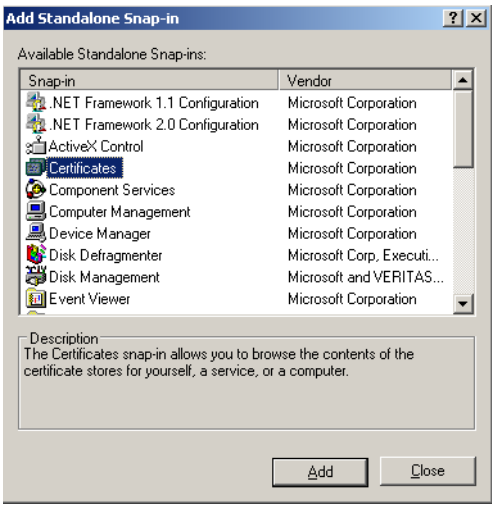
5. Select **Certificates** and click **Add.**



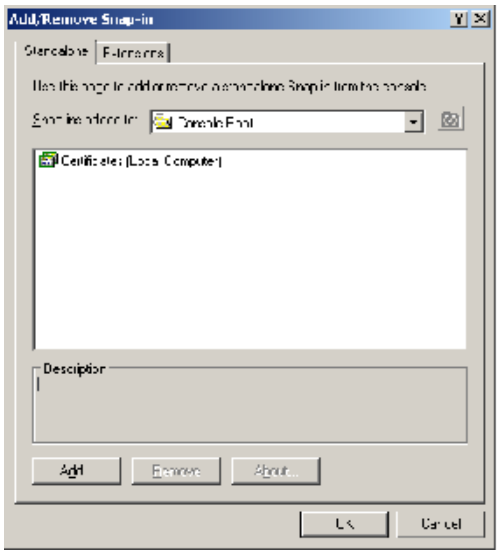
6. Select the **Computer account** and click **Next**.



7. Select **Local Computer** (the default) and click **Finish.**

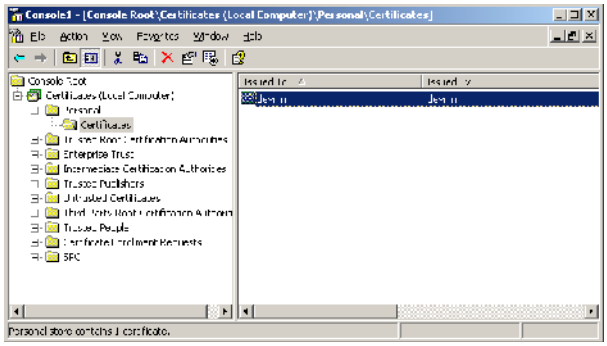


8. Click **Close.**

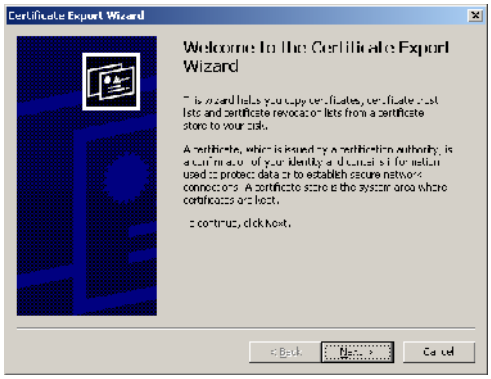


9. Click **OK**.

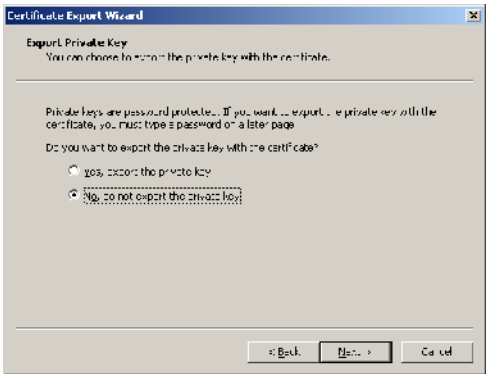
10. Expand **Personal** and then **Certificates**. Select the certificate (there may be more than one).



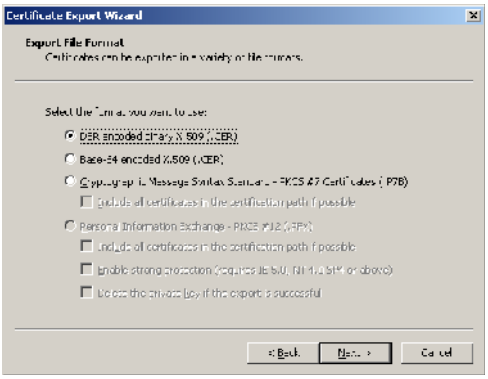
11. Right click on the certificate and select **All Tasks**, then **Export**. The export wizard will start.



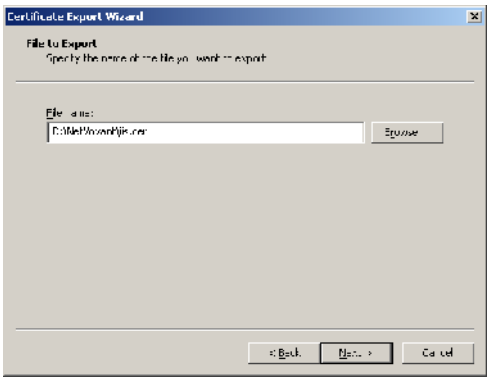
12. Click **Next.**



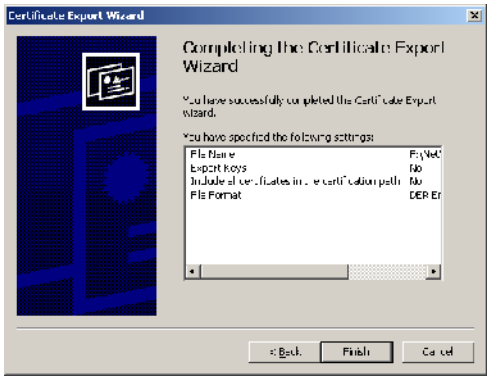
13. Select **No, do not export the private key** and click **Next**.



14. Select **DER encoded binary X.509 (.CER)** and click **Next**.



15. Browse to the `D:NetVoyant` directory and enter a filename such as `iis.cer`. Click **Next**.



16. Click **Finish**.

You should see this message:

Import the certificate into the Java certificate store

From the command prompt, enter the following commands. This assumes the default installation of the NetVoyant software. Some of the information will be different based on the server's actual name. The bold text indicates the text the user will type:

```
D:
D:\> cd \NetVoyant\jre\lib\security
D:\NetVoyant\jre\lib\security>..\..\bin\keytool -import -v -trustcacerts -file D:\NetVoyant\iis.cer -keystore cacerts
Picked up _JAVA_OPTIONS: -Dsun.java2d.d3d=false
Enter keystore password:  changeit
Owner: CN=devmn
Issuer: CN=devmn
Serial number: -196c8fe3bc87c68b03563230125923e
Valid from: Fri Oct 03 10:28:34 CDT 2008 until: Fri Oct 10 10:28:34 CDT 2008
Certificate fingerprints:
   MD5:  6C:B4:A4:58:95:85:9E:B9:3C:1A:48:F1:2B:AB:1A:F9
   SHA1: 67:6F:C6:2F:82:76:CE:DC:1D:D0:DD:B1:21:6E:40:A0:3C:F9:FE:7A
Trust this certificate? [no]:  yes
Certificate was added to keystore
[Saving cacerts]
```

Modify the Console Command Line

The following option needs to be added to the Console command line arguments:

```
-Djavax.net.ssl.trustStore=F:/NetVoyant/jre/lib/security/cacerts
```

It's also possible to create a different key storage file. See the documentation on the Java keystore tool for further information.

Other Configuration Notes

The preceding steps will resolve problems when the SSO or NetQoS Performance Center website is using an SSL certificate. Make sure to make the proper adjustments to the SSO configuration using the SSO Configuration Utility. Note that it's possible that you may need to import more than one certificate in the certificate file (cacerts) depending upon the server configuration. For example, if you have an NetQoS Performance Center using SSL on a different system and are also planning on using SSL on the NetQoS NetVoyant server, you would have two certificates that need to be imported.

The NetQoS NetVoyant reporting website defaults to the following URL:

`http://<servername>/`

Where `<servername>` is the hostname of the NetVoyant Server. If the NetQoS NetVoyant website will be using SSL, then you will need to manually add a property denoting the correct URL. This is done using the MySQL command line utility on the NetQoS NetVoyant server and entering the following command:

```
mysql> insert into properties values(1, 'webServer', 18, 'https://devmn.netqos.com/
',2,2);
```

Change the URL above to one to match your system and restart the Console. If you are using a non-standard port, you will need to adjust the URL accordingly:

```
mysql> insert into properties values(1, 'webServer', 18, 'http://
devmn.netqos.com:8080/',2,2);
```

Windows Authentication Configuration Notes

The Windows Authentication feature of Single Sign-On requires adding NetQoS Performance Center server to the Local Intranet site list that is found within Internet Explorer's internet options on each client. Both the http and https protocols should be added using either the IP address or hostname of the NetQoS Performance Center server. This change can be automatically pushed to client machines which are joined to a domain by use of group policy. Any client machine on the domain which does not have the NetQoS Performance Center server added to this list will display domain authentication prompts prior to accessing the NetQoS Performance Center user interface.

If you are using Windows Authentication and you have existing NetQoS Performance Center user accounts with corresponding Windows Domain accounts, then you need to change the Authentication Type to **External** for the user account in NetQoS Performance Center. For additional information about configuring user accounts, see the *NetQoS Performance Center User and Administrator Guide*. Users will not be able to log in to NetQoS Performance Center until this change is made.

Configuring Firefox for Single Sign-On Windows Authentication

The following changes need to be made in FireFox to support the Single Sign-On Windows Authentication feature:

1. Open Firefox and type `about:config` in the address bar.
2. Type `network.automatic-ntlm-auth.trusted-uris` in the filter field.
3. Double click the name of the preference that you just searched for.
4. Enter the URLs of the sites you wish to pass Windows Authentication info to. This would generally include both http and https instances of each of the NetQoS products you will be accessing. These values are separated by commas. For example, you could enter the following:

   ```
   http://192.168.8.45,https://192.168.8.45
   ```

Troubleshooting User Account Log In Issues

If you use Windows Authentication to access a NetQoS product, there have been rare cases where the user account that is logged in is not the correct account. If this occurs, you must clear the stored user names and passwords for the host where SSO resides. For instance, if SSO is located on 192.168.1.2 then you would remove the stored user names and password for that IP address.

To clear stored user names and passwords

1. Click **Start** on your desktop.
2. Click **Control Panel**.
3. Double-click **User Accounts**.
4. Click the *Advanced* tab, then click **Manage Passwords**.
5. Select the entry you want to delete, then click **Remove**.

CHAPTER 2

Single Sign-On Configuration Tool

The Single Sign-On Configuration Tool is a Windows application that gives administrators the ability to adjust the settings used by the Single Sign-On website and its associated NetQoS products.

The Single Sign-on configuration tool does the following:

- Configures various NetQoS products located on the same server as the tool to use LDAP and Windows authentication. All of the LDAP and Windows Authentication settings for each product are setup using this tool. An administrator can test their configuration by simply entering the appropriate settings. This particular feature is useful when trying to troubleshoot issues with particular settings.
- Updates the Single Sign-On Virtual Directory that each product references. If you added a new Single Sign-On Virtual Directory, as discussed in the above sections, then you will need to use this tool to sync up each of the NetQoS products on the modified server to know where to redirect users when they do not authenticate.

You will also need this tool if you updated the Single Sign-On website to use SSL. Both the Single Sign-On scheme and port will be affected by this change. The Single Sign-On Configuration Tool gives administrators the ability to easily update these values in all of the necessary products.

Note: Changes made in the Single Sign-On configuration tool only affect newly created LDAP and Windows Authentication users. They do not apply to existing LDAP and Windows Authentication users registered within NetQoS Performance Center.

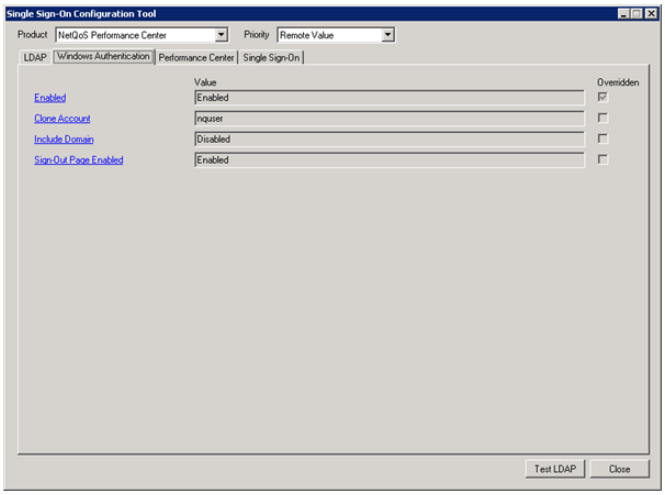
Using the Single Sign-On Configuration Tool

To access the tool, click the shortcut titled **Single Sign-On Configuration Tool** on the **Desktop** of each server that hosts a Single Sign-On website. If you can't find this shortcut on the **Desktop**, then you can get to it using the following path:

```
D:\NETQOS\SingleSignOnConfigurationTool\SsoConfig.exe
```

If you still can't find the file, then search for **SsoConfig.exe** using Windows file search.

Once you open the Single Sign-On Configuration Tool, you should see the main dialog window.



The main dialog window contains the following drop down lists:

- **Product** drop down list: This drop down list is automatically populated with every NetQoS product on the server that uses the Single Sign-On website. The administrator has the ability to modify the settings for each of these products.

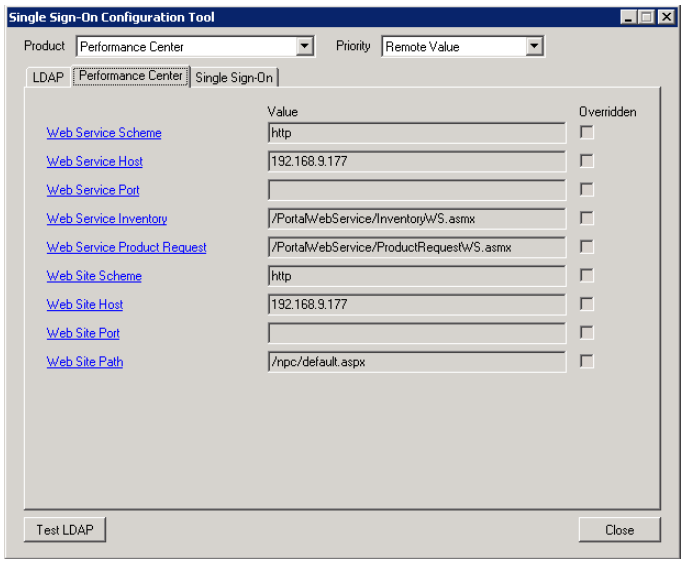
The combination of the selected product and priority determine which values will be shown in the tool and which values can be updated.

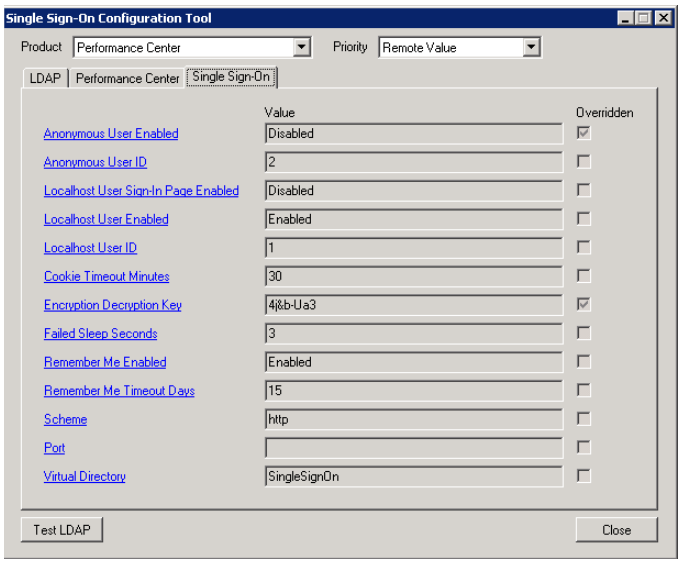
The Priority order is as follows:

- **Local Override** settings can be changed for all products. If a **Local Override** value exists, that will always take precedence over both the **Remote Value** and **Default Value** settings.
- **Remote Value** settings have the next highest precedence. **Remote Value** settings can only be changed by Administrators if the product they are modifying is the **Performance Center**. The **Remote Value** settings are propagated down to every other NetQoS product. If an administrator changes a **Remote Value** setting then that value will end up in each and every NetQoS product. So, if a **Remote Value** setting exists and a **Local Override** does not, then the **Remote Value** setting will be used.
- **Default Value** settings are the settings that are shipped with each product. Administrators do not have the ability to change the **Default Value** settings. They effectively act as a baseline. And, if both the **Local Override** and **Remote Value** settings are not present then the **Default Value** will be used.

Note: The main dialog window also has four tabs: **LDAP**, **Windows Authentication**, **Performance Center**, and **Single Sign-on**. Each tab shows the possible values that can be updated for that category.

The following graphics show the **Performance Center** and **Single Sign-On** values.



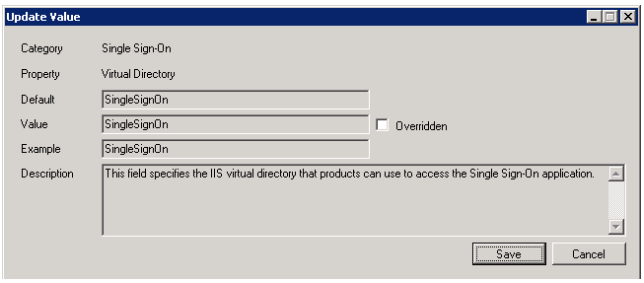


Notice in the preceding view that one of the overridden checkboxes is checked and the others are not. The one that is checked overrides the **Default Value**. The ones that are not checked do not have a **Remote Value** and therefore use the **Default Value** instead.

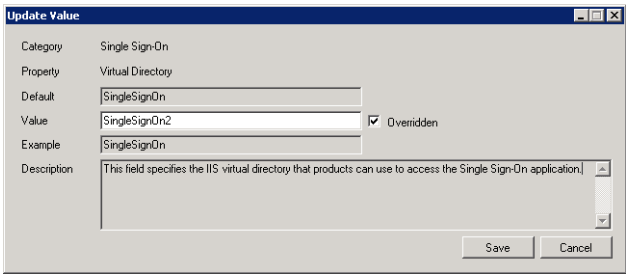
If **Local Override** was selected as the priority then the checked values would override both the **Default Value** and the **Remote Value**, if it existed. Unchecked items would either use the **Remote Value**, if it existed, or the **Default Value** if it did not.

The Single Sign-On Configuration Tool displays the value of the setting with the highest priority relative to what is selected in the priority drop down list. If **Remote Value** was selected in the priority drop down list and an overridden checkbox was not checked, we could guarantee that the value we saw was the **Default Value**. If the overridden checkbox was checked, then we would be looking at the **Remote Value**.

As an example, let's update the Virtual Directory setting under the **Single Sign-On** tab. Currently, it has a value of **SingleSignOn**. Let's change it to have a **Local Override** of **SingleSignOn2**. To do this, we will click on the **Virtual Directory** link. The following window will be displayed.

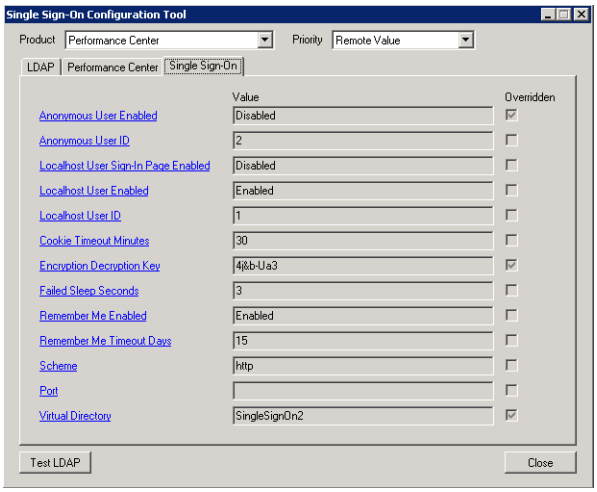


Notice the category and property at the top. Next, there is a default value. This cannot be changed. It is there to show what value was shipped for this particular setting. Next, we have the actual value of **SingleSignOn**. If we check the **Overridden** checkbox then the value textbox will not be disabled and we can update its value. After that, we have an example value and a description of the setting.



By checking the **Overridden** checkbox, we can change the value of this setting to be **SingleSignOn2**. If we uncheck the **Overridden** checkbox, then the value will go back to what it was before and the textbox will be disabled again. The **Overridden** checkbox tells the Single Sign-On Configuration Tool that you want to update the value. Click **Save** and the window will close.

Notice in the following view that the **Overridden** checkbox is now checked and the value is **SingleSignOn2**. This tells an administrator that the Virtual Directory value is actually a **Local Override**. The Performance Center will now direct all unauthenticated users to the Single Sign-On website with a Virtual Directory of **SingleSignOn2**.

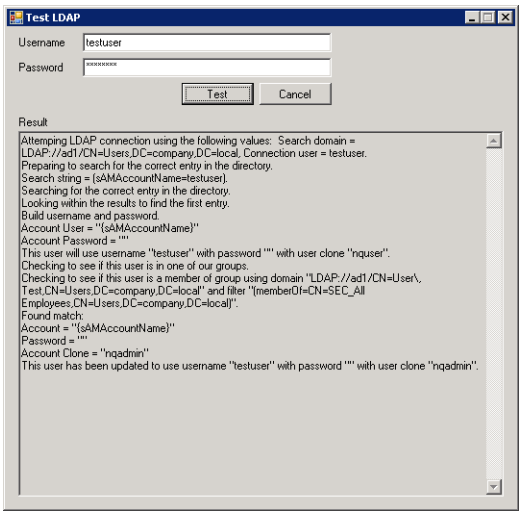


Testing the LDAP Configuration Settings

Aside from updating values, another important feature of the Single Sign-On Configuration Tool is the ability to test the LDAP configuration settings. Click the **Test LDAP** button in the bottom left-hand corner of the main dialog to access the main LDAP testing window. The main LDAP test window has a textbox for a username and a password. After entering the username and password, click **Test** and see the results. The settings under the LDAP tab on the main dialog window will be used in this test.

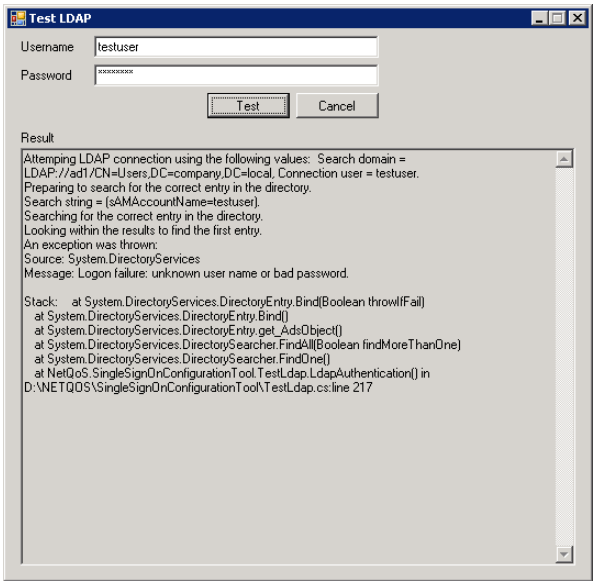
1. Enter a username and a password that you know will authenticate using LDAP. After clicking the Test button, assuming that you have the proper LDAP settings, you will see this message:

2. Click **OK** and the message will close. The results of the LDAP authentication process will be displayed for the administrator. During the LDAP authentication process there are numerous steps that are recorded. These help administrators to troubleshoot issues when they arise. This example worked properly.



3. To demonstrate what happens when there is an issue, enter an incorrect password. The following message will appear.

4. Click the OK button to close this pop up and to get more details about the error. After parsing through the results, there is a line that states **Logon failure:unknown user name or bad password.** This is consistent with the test since the password was incorrect for testuser.



The LDAP testing feature can be used for more than just testing user accounts. A real world example would be using this tool to troubleshoot LDAP settings during an initial configuration. Using the tracing feature in the results log, this tool will hopefully make that task much easier.

CHAPTER 3

Properties in the Configuration Tool

This section contains a list of all of the fields, with descriptions, that can be modified using the Single Sign-On Configuration Tool:

LDAP Fields

Connection User

This field defines the user ID that the login server uses to connect to the LDAP server. This LDAP user name will be used to bind to the server. For example, if the login server uses a fixed account, you would enter text like the following:

```
CN=The User, cn=Users, dc=domain, dc=com
```

If the login server uses the user ID entered on the login form, you would enter:

```
{0}
```

Complex configurations need to have the user principle name in order to identify the user. To do this, simply put `{0}@domain.com` where their email is the domain name. For example:

```
{0}@domain.com
```

If the LDAP server requires a full Dn, you could also enter the following:

```
CN={0}, Cn=Users, dc=domain, dc=com
```

In this case, the user would log in with their log in names such as John Doe.

Note: For security reasons, you should not make the connection user a static account. The LDAP authentication only checks the password when binding to the server. If you use a static account, any user that exists in the LDAP tree will be able to log in with any password.

Connection Password

This field defines the password that the login server uses to connect to the LDAP server. For example, if the login server uses a fixed account, you would enter text like the following:

```
SomePassword
```

If the login server uses the password entered on the login form, you would enter:

```
{1}
```

Search Domain

This field indicates the LDAP protocol, server, and initial search domain. It also identifies where searching starts when verifying account credentials. Typical entries would look like the following:

```
LDAP://localhost/dc=companydoman,dc=com
LDAP://svr/CN=Users,DC=company,DC=local
```

If you have an Active Directory setup as `QASG.local`, your search domain string will be:

```
LDAP://qasg.local/dc=qas,dc=local
```

Search String

This field and the Search Scope field specify the criteria used to locate the correct record for the user. If only a subset of LDAP users is allowed to log in, the search string can be used to look for multiple properties within the record. This field can contain any valid LDAP search criteria. The following is an example of a valid entry for this field:

```
(SamAccountname={0})
```

Search Scope

This field and the Search String field specify the criteria used to locate the correct record for the user. This field determines whether the LDAP server should search in the current directory (**OneLevel**), all subdirectories (**Subtree**), or limit the search to the base object (**Base**). Most installations should use **Subtree**. **OneLevel** matches objects in the current directory and prevents unexpected matches deeper in the LDAP directory.

Encryption

If this flag is set to true, it attaches a cryptographic signature to the message that both identifies the sender and ensures that the message has not been modified in transit. If the LDAP server you are connecting to is configured for encryption, select this checkbox.

SSL

If this flag is set to true, it attaches a cryptographic signature to the message that both identifies the sender and ensures that the message has not been modified in transit. Active Directory requires the Certificate Server be installed to support Secure Sockets Layer (SSL) encryption. If the LDAP server you are connecting to is configured for SSL, select this checkbox.

You must install your client certificate in the following directory if you would like to enable SSL communcation with your LDAP server:

```
Console Root\Certificates (Local Computer)\Trusted Root Certification
Authorities\Certificates
```

Secure

When this option is set, the authentication API tries to authenticate via Kerberos first and then attempts to use NTLM if Kerberos fails. In general, this should be enabled.

Server Bind

Enable this by default. If you encounter problems, you can disable this option.

User Bind

This field specifies whether or not to do an additional bind using the user's DN and password to validate their credentials.

Account User

This field and the **Account Password** field specify the NetQoS Performance Center default account to which to map validated LDAP users who do not have a group membership. If a valid user does not match any group definitions, the user is logged in with the default user ID specified in this field.

If you want the default account to have minimal privileges, you can enter:

```
nquser
nq
```

If you want to allow all the users to log in with their user name, this field should be:

```
{SAMAccountname}
{SAMAccountname} or {CN}
```

Note: The account user field should be a field from the user entry. Typically, this will match your search filter.

Account User Default Clone

This field enables you to specify a user account to clone if validated LDAP users are members of a group other than the ones specified in the Groups field. If you want such users to have minimal privileges, you can clone the nquser account by entering:

```
nquser
```

Note: The account that you specify in this field must be a preexisting account.

Groups

This field enables you to set up default account handling for selected accounts or groups of accounts. For example, to enable all members of a group to log in using an admin account, you could enter:

```
<LDAPGroups><Group searchTag="memberOf" searchString="CN=SEC_All
Employees,CN=Users,DC=company,DC=local" user="{sAMAccountName}" passwd=""
userClone="admin"/></LDAPGroups>
```

Windows Authentication

Note: If you are using Windows Authentication and you have existing NetQoS Performance Center user accounts with corresponding Windows Domain accounts, then you need to change the Authentication Type to **External** for the user account in NetQoS Performance Center. For additional information about configuring user accounts, see the NetQoS Performance Center User and Administrator Guide. Users will not be able to log in to NetQoS Performance Center until this change is made.

Enabled

This field specifies whether or not Windows Authentication is enabled.

Clone Account (*Optional*)

This field enables you to specify a user account to clone if the Windows user name does not already exist in the product. If you want such users to have minimal privileges, you can clone the nquser account by entering `nquser`. A permanent account will be created for the user with the permissions from the cloned account.

Note: The account that you specify in this field must be a preexisting account.

Note: The Anonymous User login will take precedence over Windows Authentication.

Include Domain

This field specifies whether or not the Windows domain will be included as part of the product user name. For example, let's assume your domain name is "NetQoS" and your Windows user name is "JSmith". If this option were enabled then your product user name would become `JSmith@NetQoS`. Note, the format will always be `<User Name>@<Domain Name>`. If this option were disabled then your product user name would be `JSmith`.

Sign-Out Page Enabled

This field specifies whether or not Windows Authentication users will see a sign-out page after manually logging out of the product. If the user that signed out has a domain account, this sign-out page gives users the ability to sign in with a different account or sign in again with the same account. If this field is disabled then the users will simply be redirected to the regular sign-in page.

Performance Center

Important: These settings should be set in the NetQoS Performance Center user interface. The changes made in NetQoS Performance Center will automatically be propagated to Single Sign-On. The option to change these settings are made available to help troubleshoot issues or for special situations. Please consult with CA Support when you are considering changing these settings.

Web Service Scheme

This field specifies the URL scheme that the Single Sign-On application can use to access the Performance Center web service.

Web Service Host

This field specifies the URL host that the Single Sign-On application can use to access the Performance Center web service.

Web Service Port

This field specifies the URL port that the Single Sign-On application can use to access the Performance Center web service.

Web Service Inventory

This field specifies the URL path that the Single Sign-On application can use to access the Performance Center Inventory web service.

Web Service Product Request

This field specifies the URL path that the Single Sign-On application can use to access the Performance Center Product Request web service.

Web Site Scheme

This field specifies the URL scheme that the Single Sign-On application can use to access the Performance Center.

Web Site Host

This field specifies the URL host that the Single Sign-On application can use to access the Performance Center.

Web Site Port

This field specifies the URL port that the Single Sign-On application can use to access the Performance Center.

Web Site Path

This field specifies the URL path that the Single Sign-On application can use to access the Performance Center.

SMTP Enabled

This field specifies whether SMTP is enabled or disabled.

SMTP Server Address

Enter the IP address or domain name of the server to use to send pages or reports by email from the NetQoS Performance Center.

SMTP Port

This field specifies the SMTP Port.

SMTP SSL

This field specifies whether or not SMTP SSL is enabled.

Email Reply Address

Enter the email address from which the NetQoS Performance Center sends reports.

Email Format

Select either HTML or Text format for the email messages generated by the NetQoS Performance Center.

Note: If you are using email to automatically send event notifications, this should be set to HTML to help ensure proper formatting.

SMTP Username

(Optional) Enter the username.

SMTP Password

(Optional) Enter the password.

SINGLE SIGN-ON

Anonymous User Enabled

This field specifies whether or not the sign-in page will appear when users attempt to enter a product. The **Anonymous User ID** field is required if this field is checked. In this scenario, the user will not see the sign-in screen when they attempt to enter a product and they'll be signed in as the user associated with the **Anonymous User ID** field.

If the user is on the Single Sign-On application server and both the **Localhost User Enabled** and **Anonymous User Enabled** fields are checked, then the **Localhost User Enabled** field takes precedence.

Note: The Anonymous User login will take precedence over Windows Authentication.

Anonymous User ID

This field is used only if the **Anonymous User Enabled** field is checked. It specifies the User ID that will be used to automatically authenticate the user and bypass the sign-in screen. The value **1** is the User ID for **nqadmin**. The value **2** is the User ID for **nquser**.

Localhost User Sign-In Page Enabled

This field specifies whether or not the sign-in page will show up if the user is on the Single Sign-On application server. If it is not checked, then the **Localhost User Enabled** field is required to be checked and the **Localhost User ID** field is required to have a valid product User ID. In this scenario, these fields will be used to automatically sign in the user to the product and bypass the sign-in screen. If the **Localhost User Sign-In Page Enabled** field is checked, then the sign-in page will show up despite the fact that the user is on the Single Sign-On application server.

Localhost User Enabled

This field specifies whether or not a user will automatically be signed in if they are on the Single Sign-On application server. The **Localhost User ID** field is required if this field is checked.

Also, if the **Localhost User Sign-In Page Enabled** field is checked, then this field will only come into play if the user does not enter a username or password and clicks the sign-in button. In this scenario, the user will enter the product as the user that is associated with the **Localhost User ID** field. If they do enter a username and password then those credentials will be used to authenticate them. If the **Localhost User Sign-In Page Enabled** field is not checked, and this field is checked, then the user will bypass the sign-in page and will enter the product as the user associated with the **Localhost User ID** field.

If the user is on the Single Sign-On application server and both the **Localhost User Enabled** and **Anonymous User Enabled** fields are checked, then the **Localhost User Enabled** field takes precedence.

Localhost User ID

This field is used only if the **Localhost User Enabled** field is checked. It specifies the User ID that will be used to automatically authenticate the user and bypass the sign-in screen when they are on the Single Sign-On application server. The value **1** is the User ID for **nqadmin**. The value **2** is the User ID for **nquser**.

Cookie Timeout Minutes

This field specifies the number of minutes that pass before a Single Sign-On cookie expires. Each time a user does something in a NetQoS product the cookie timeout starts over. However, if the cookie does timeout then the user is required to reauthenticate.

If NetQoS ReporterAnalyzer is integrated with the NetQoS Performance Center, the ReporterAnalyzer value will default to the NetQoS Performance Center value and ReporterAnalyzer will no longer honor the time-out value configured in IIS.

Note: If you override the default cookie timeout value of 20 minutes, log into the NetQoS Performance Center server and modify the file web.config in the path D:\netqos\portal\website\ using a text editor such as Notepad. Search for the string "InProc" and move to the end of this line. Modify the timeout value to equal your new cookie timeout value that was saved in the SSO tool. Save the changes and close the file

Encryption Decryption Key

This field specifies the key that is used to encrypt and decrypt the cookie that is used in conjunction with the Single Sign-On application.

Failed Sleep Seconds

This field specifies the number of seconds the Single Sign-On application will wait after a failed sign-in attempt.

Remember Me Enabled

This field specifies whether or not the **Remember Me** checkbox will show up on the sign-in page.

Remember Me Timeout Days

This field is used only if the **Remember Me Enabled** field is checked. It specifies the number of days that will pass before a user that checked **Remember Me** on the sign-in page has to reauthenticate. If this field is set to **0** then the **Remember Me** setting will not expire until the user clicks the **Sign Out** link in a NetQoS product.

Scheme

This field specifies the URL scheme that NetQoS products can use to access the Single Sign-On application.

Port

This field specifies the URL port that NetQoS products can use to access the Single Sign-On application.

Virtual Directory

This field specifies the IIS virtual directory that NetQoS products can use to access the Single Sign-On application.

Note: Administrators should be aware that their updates to the Single Sign-On website only affect those NetQoS products that are on the same server because of the distributed architecture.

CA NetQoS Main Office
5001 Plaza on the Lake
Austin, TX 78746
tel: 512.776.0042
800.225.5224
fax: 512.776.0010

www.ca.com