Configuring LDAP and SSL

Integrating CA NetQoS Products with LDAP and SSL

Configuring LDAP (Lightweight Directory Access Protocol) for CA NetQoS products allows organizations to use the usernames and passwords that are already configured on their networks to access CA NetQoS data sources and CA NetQoS Performance Center. This document describes Single Sign-On support for LDAP authentication, describes the required and optional fields on the LDAP tab of the Single Sign-On Configuration Tool, and provides some example configurations for different LDAP deployments. It also addresses how to configure CA NetQoS products when it is necessary to enable SSL through the LDAP server. These procedures are specific to versions 6.0 and 6.1 of CA Single Sign-On for NetQoS.

This document has been reviewed for compatibility with the following product versions and all product versions that are compatible data sources for the following product versions:

NetQoS Performance Center 5.1

NetQoS Performance Center 6.0

CA NetQoS Performance Center 6.1

Introduction

Single Sign-On is the authentication scheme for CA NetQoS Performance Center and all supported data sources. Once they are authenticated to CA NetQoS Performance Center, users can navigate among the console and registered data sources without signing in a second time.
By enabling navigation among separate product interfaces, Single Sign-On helps ensure a seamless drilldown experience for operators who are analyzing performance and status data. For example, if a user logs in to CA Performance Center and then follows a drilldown path to the data source interface, that user does not log in again.

CA Performance Center uses a distributed architecture. An instance of the Single Sign-On website is automatically installed on every server where a supported data source or CA NetQoS Performance Center is installed. If two data source products are installed on the same server, they use the same instance of the Single Sign-On website. The distributed architecture lets users log in to individual CA data source products by logging in to the servers where these products are running.

LDAP is an acronym for Lightweight Directory Access Protocol. It is an application protocol for querying and modifying directory services running over TCP/IP. Single Sign-On provides LDAP integration, allowing operators to authenticate to an LDAP server running in your environment. This prevents administrators from having to create dozens of separate user accounts for CA NetQoS operators. They can instead use their existing login information to access CA NetQoS data source products.

If LDAP integration is successfully configured on a CA NetQoS system, a user will be able to enter his or her login credentials on a CA NetQoS data source Login page. The data source then sends the request through Single Sign-On to the LDAP server and verifies: 1) Whether the user exists in the LDAP directory; 2) Whether the user has permission to access the CA NetQoS data source; and 3) The privileges the user has for each data source and for CA Performance Center.

Further customization is available to create special privileges for different groups of users based on LDAP membership settings. It can also be configured to require SSL (Secure Socket Layer) encryption. This document explains how to configure the various fields required for setting up LDAP in the Single Sign-On Configuration Tool, discusses examples of Active Directory, Global Catalog, and OpenLDAP configurations, and outlines requirements for setting up SSL encryption to the LDAP server.

Single Sign-On Configuration Tool

To get started configuring CA NetQoS products to use LDAP authentication, the CA Administrator needs to launch the Single Sign On Configuration Tool. This utility is located on the server where CA NetQoS Performance Center is running, most commonly the ReporterAnalyzer master console.

All settings required for LDAP integration are located on the LDAP tab in this utility.

Binding

The first step in the LDAP authentication process is a bind to the LDAP server. When a user supplies login credentials, the CA NetQoS data source product attempts to bind to the LDAP server through Single Sign-On. This ensures that the user has permission to access the LDAP server. The credentials that are used for this first binding are supplied in the Connection User and Connection Password fields in the Single Sign-On Configuration tool.

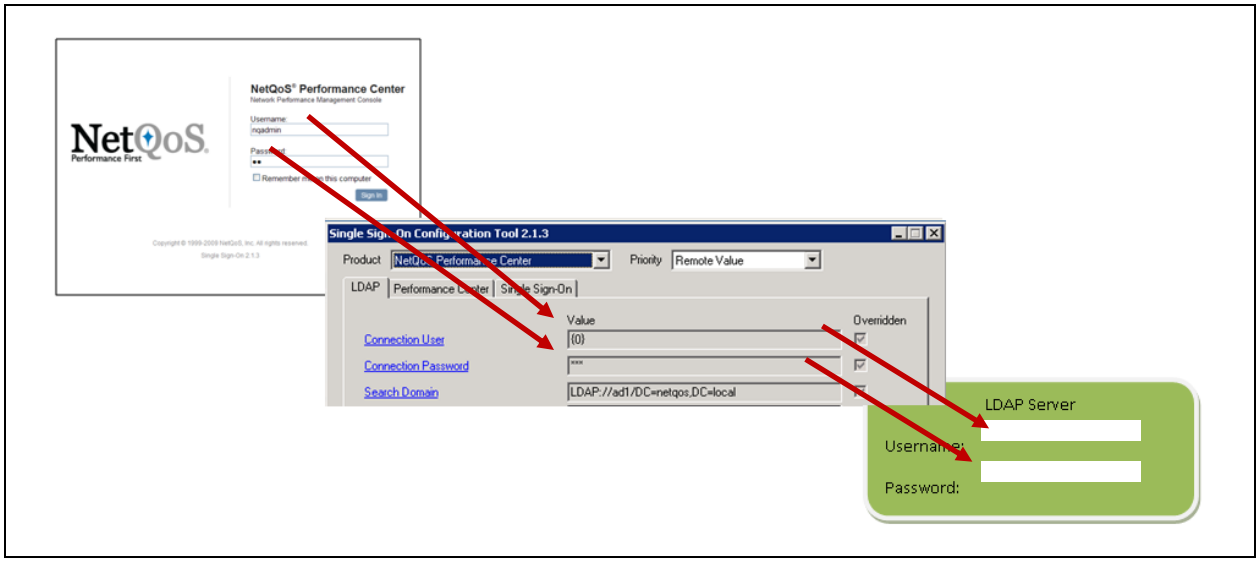

Figure 1. Initial Bind Process to LDAP Server

Figure 1 illustrates the bind process to the LDAP server. The user enters login credentials on the CA NetQoS Performance Center Login page. Because the Connection User and Connection Password fields are configured to use the login credentials that the user entered on the Login page, these credentials are forwarded to the LDAP server to attempt authentication. (For more information, see the "Connection User" and "Connection Password" sections of this document.) If the credentials are authenticated, the bind to the LDAP server is successful, and the user can access the LDAP directory.

Once this first bind to the LDAP server is complete, Single Sign-On tries to find the username that the user entered on the CA NetQoS Performance Center Login page using the Search String configured in the Single Sign-On Configuration Tool. In the example depicted in Figure 2, the LDAP directory specified in the Search Domain field is searched for a sAMAccountName equal to User2, which is the username entered on the CA NetQoS Performance Center Login page. If the username is found and User Bind is *not* enabled, Single Sign-On authenticates the user automatically and does not attempt to compare the password. Note that User Bind is another field that can be enabled or disabled in the Single Sign-On Configuration Tool.

If User Bind is enabled, a second bind is attempted. The second bind verifies that the password entered on the Login page corresponds to the username found in the LDAP directory. If the password matches, the user is successfully authenticated.

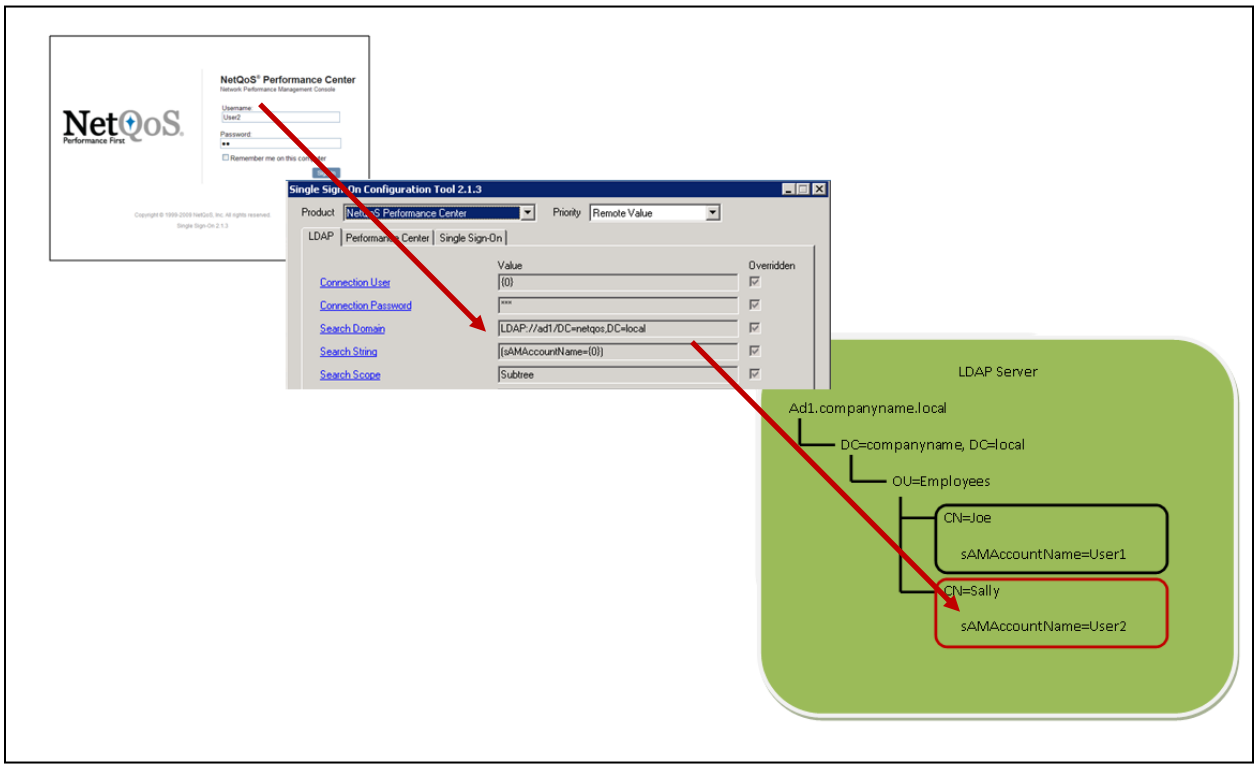

Figure 2. Authenticating User

Connection User and Connection Password

CA Single Sign-On uses the Connection User and Connection Password fields to contact the LDAP server and verify that the user has permission to log in to the LDAP server.

These fields may be hardcoded in the Single Sign-On Configuration Tool by entering an actual username and password for an account that has access to the LDAP server. Take this step if not all LDAP users are able to log in to the LDAP server, even if they exist in the LDAP directory.

If these fields are hardcoded in the Single Sign-On Configuration Tool, Single Sign-On will *not* automatically verify that the user's account exists within the LDAP configuration, that the user's password is correct, or that the user has permission to access the CA NetQoS data sources . The user's credentials are only verified if the Server Bind field is also set to Enabled when these fields are hardcoded.

Generally the Connection User and Connection Password fields are completed as follows:

Connection User: {0}

Connection Password: {1}

If you supply {0} and {1} in these fields, the credentials sent to the LDAP server are those that the user enters at the login screen.

If {0} and {1} are used, the user account must exist, and the password must be correct.

Search Domain

The Search Domain is often the trickiest part of LDAP configuration. It identifies where in the directory tree to begin to search for the user's account credentials. Contact the LDAP administrator to determine the correct Search Domain. The LDAP protocol, server, and initial search domain are required in this field.

Typical entries use the following format:

LDAP://adserver.domain/dc=companydomain,dc=com

Example:

LDAP://ad1.netqos.local/OU=Employees,DC=netqos,DC=local

Figure 3 illustrates the example given above using Active Directory Explorer. Notice how the Path field corresponds to the example. In this example, all of the DNs contained in the OU of Employees will be included in the search.

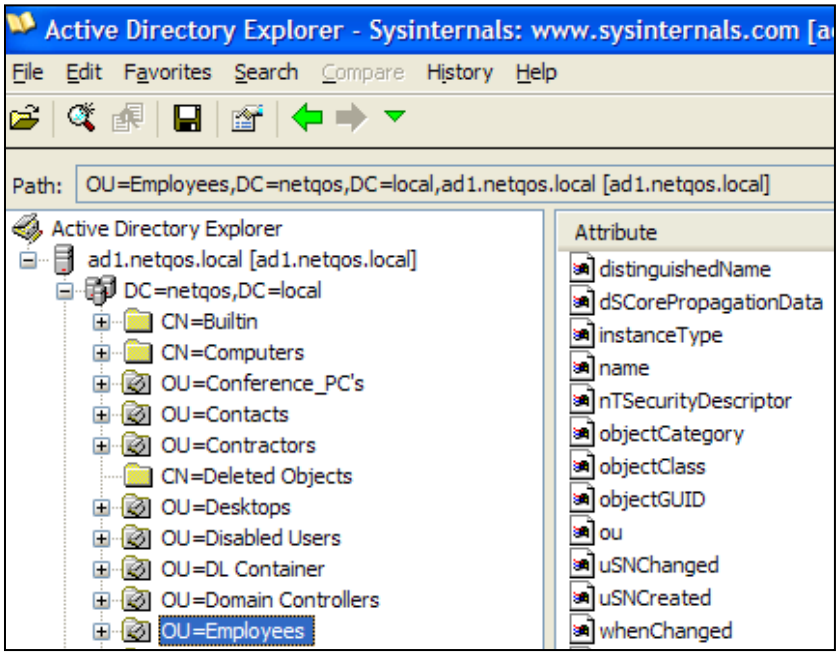

Figure 3. Search Domain

Search String

The Search String is the parameter used to match what the user entered on the Login page of the CA NetQoS data source or CA NetQoS Performance Center with an entry in the LDAP directory. The format of this string should be (<Field in directory>={0}). The <Field in directory> depends on the type of LDAP implementation you have. Table 1 contains some configurations for common LDAP implementations:

LDAP Implementation	Search String
Active Directory	(sAMAccountName={0})
Active Directory connecting to Global Catalog	(userPrincipalName={0})
OpenLDAP	(uid={0})

Table 1. Search String Examples

Search Scope

The Search Scope field, along with the Search String field, specifies the criteria used to locate the correct record for the user who is attempting to authenticate. This field determines whether the LDAP server should search in the current directory, in all subdirectories, or should limit the search to the base object. Most installations will use Subtree, but using OneLevel prevents any unexpected matches deeper in the LDAP directory.

Extent of Search	Search Scope
Searches the directory specified in the Search String field only	OneLevel
Searches the directory specified in the Search String field as well as all sub directories	Subtree
Searches only the base object	Base

Table 2. Search Scope Examples

Encryption

If the Encryption field is enabled, a cryptographic signature is attached to the message that both identifies it to the sender and ensures that the message has not been modified in transit. Set this field to Enabled if the LDAP server to which you are connecting is configured for encryption. Otherwise leave this Disabled.

SSL

Like the Encryption field, if this is enabled, a cryptographic signature is attached to the message that both identifies it to the sender and ensures that the message has not been modified in transit. When using an Active Directory implementation, the Certificate Server must be installed to support SSL encryption. If the LDAP server is configured for SSL, this field should be set to Enabled. See the "SSL" section below for more information about using SSL.

Secure

When the Secure field is set, the authentication API tries to authenticate via Kerberos first. If Kerberos fails, it will then attempt to use NTLM. Enable this field as a best practice.

Server Bind

This field should be enabled by default. But if problems occur, this parameter can be disabled.

User Bind

User Bind is only for situations where the connection user and password are hardcoded. If you use {0} and {1} for the connection user and connection password, you do not need to enable User Bind. Unless User Bind is set to Enabled, the password that the user enters at the login screen will not be verified. If you set this field to Disabled, the password entered by the user is ignored, and the LDAP directory is only checked to verify that the username entered is in the directory.

Account User

Set this field to the username that the administrator would like the CA NetQoS product to use. This can be set to a default user (for example: nquser), to a user that has been created directly in the product (for example: mycompanyuser), or to the LDAP account username (for example: {sAMAccountname}).

We recommend setting the Account User field to a field from the user entry. To do this, set this field to match the search filter—{sAMAccountname} or {CN}. If you hardcode this field, which is not recommended, all users that log in to the product are logged in under the same username.

Account User Default Clone

The Account User Default Clone field allows an administrator to specify a user account to clone if the validated LDAP users are members of a group other than the ones specified in the Groups field (see below).

If you want these users to have minimal privileges, you can clone the default user account for CA NetQoS Performance Center (nquser) by simply entering *nquser* in this field. If the user should have more extensive privileges, *nqadmin* could be entered into this field. Note that the account specified in this field must be a preexisting account.

Groups

This field is optional and, like the Search Domain field, is also one of the trickier fields to configure. It specifies default account handling for selected accounts or groups of accounts. Below are two common examples of how to use this field.

***Example 1**: Give one group access, deny all other users*

Assume, as an example, that you would like to give administrator privileges to all users in the IT group and deny all other LDAP users access to the CA NetQoS data sources.

In this case, you could set the Groups field to the following:

<LDAPGroups><Group searchTag="memberOf" searchString="CN=ITGroup,OU=DL Container,DC=companyname,DC=local" user="{sAMAccountName}" passwd="" userClone="nqadmin"/></LDAPGroups>

This would grant administrator privileges to all members of the IT group.

Table 3 explains each component of the <LDAPGroups> string above.

Component	Explanation	Example
searchTag	The field in the LDAP directory that identifies how the group should be filtered	memberOf
searchString	The exact string from the LDAP directory that identifies the group in question	CN=ITGroup,OU=DL Container,DC=companyname,DC=local
User	The field in the LDAP directory that identifies the username	{sAMAccountName}
passwd	This field is left blank because the password has already been verified earlier in the LDAP authentication process.	
userClone	The user account that should be cloned to give the desired permissions. Note that the account specified in this field must be a preexisting account.	nqadmin

Table 3. Fields for LDAP Groups

To deny access to CA NetQoS products to all users who are *not* in the IT group, create a user account within the data source called something like *denieduser.* Set the product privilege for all products to None for this user. (See Figure 4)

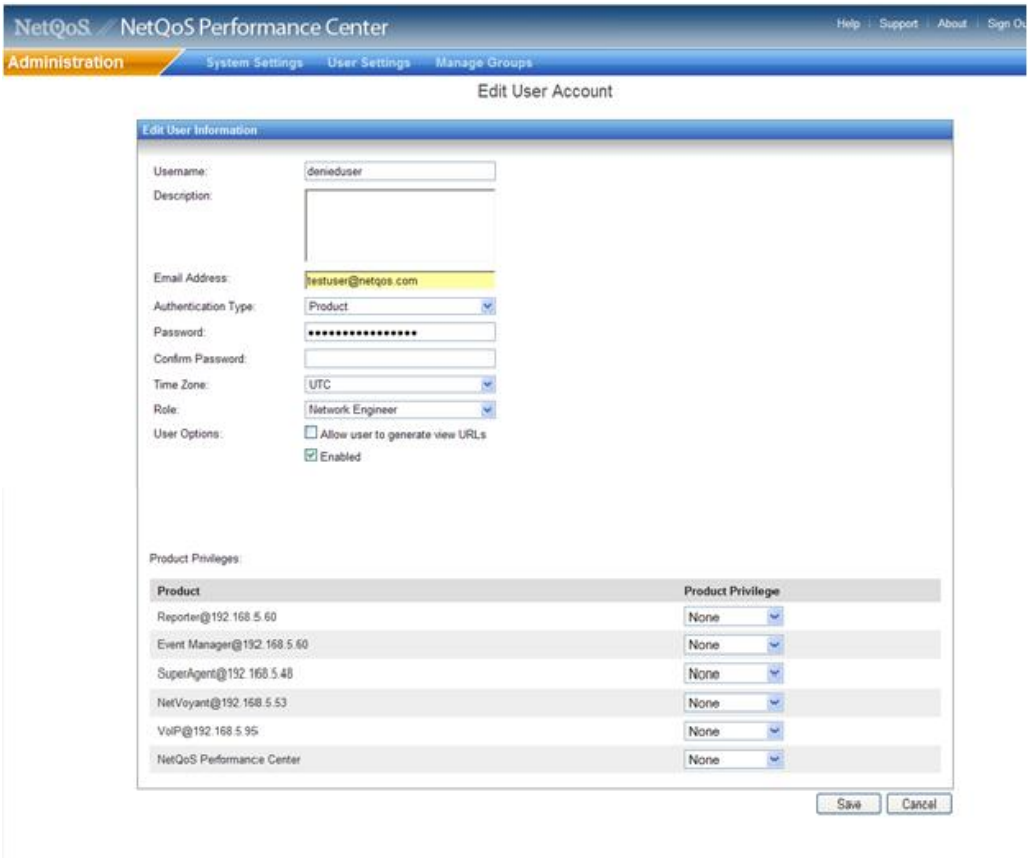

Figure 4. Creating a Denied User Account

You must also set the Account User Default Clone field in the Single Sign-On Configuration Tool to the name of this newly created user, *denieduser*.

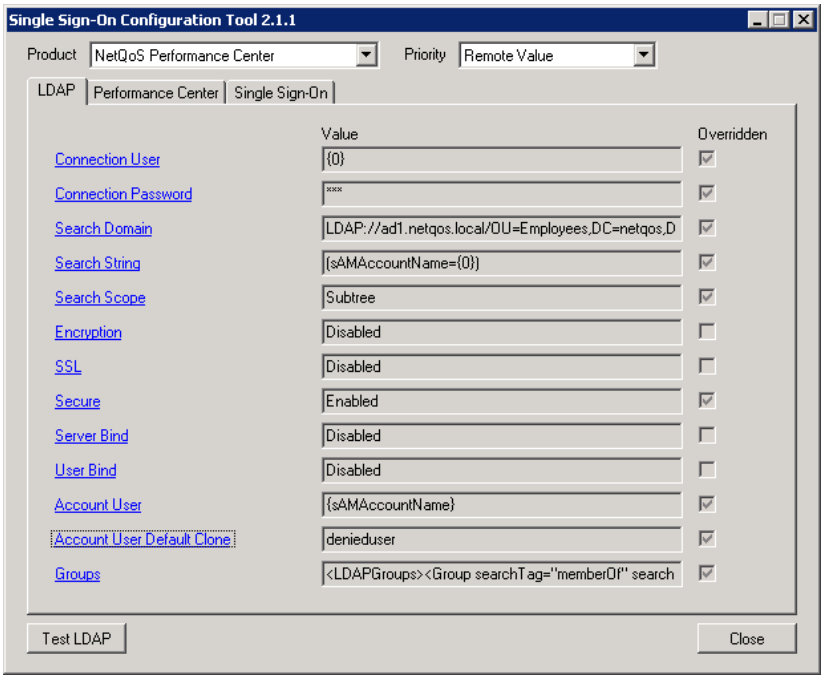

Figure 5. SSO Tool Setup using Groups and a Denied User

With this configuration, if a user tries to log in and is a member of the IT Group, that user will be granted *nqadmin* privileges. If a user tries to log in but is NOT a member of the IT group, that user sees an "Unable to authenticate user" error message.

Note that this example can be modified to allow all users not in the IT group to have another set of privileges (*nquser* privileges, for example) instead of just seeing an "access denied" error. To do this, set the Account User Default Clone field to nquser or to another user that had already been configured in the CA NetQoS data source.

***Example 2**: Set up Multiple Types of Group Permissions*

Assume, for example, that you would like to give administrator privileges to all users in the IT group, power user privileges to all users in the Management group, and user privileges to all other LDAP users.

In this case, you could set the Groups field in the Single Sign-On Configuration Too lto the following:

<LDAPGroups><Group searchTag="memberOf" searchString="CN=ITGroup,OU=DL Container,DC=companyname,DC=local" user="{sAMAccountName}" passwd="" userClone="nqadmin"/> <Group searchTag="memberOf" searchString="CN=Management,OU=DL Container,DC=companyname,DC=local" user="{sAMAccountName}" passwd="" userClone="poweruser"/> </LDAPGroups>

Note that the format of this string is as follows:

<LDAPGroups><Group Definitions1/><Group Definitions2/></LDAPGroups>

You can supply as many groups as desired between the <LDAPGroups> and </LDAPGroups> tags as long as they are in the same format as the group definitions.

Make sure that the userClone values that are assigned correspond to actual user accounts already created in the CA NetQoS product.

After you complete the Group field to assign administrator privileges to the IT Group and power user privileges to the Management Group, set the Account User Default Clone field to *nquser*. This grants user permissions for the products to all other LDAP users.

LDAP Authentication Troubleshooting

The Single Sign-On Configuration Tool lets you test the LDAP settings that you have supplied and verify that LDAP authentication is set up correctly. An LDAP test script prompts you to specify a username and password combination to test, using the current settings for LDAP authentication. If the LDAP test is failing, take one or more of the following steps:

1. Verify the correct LDAP binding credentials. The best way to do this is check with the administrator for your LDAP implementation.
2. Try enabling/disabling the various options such as Secure, Server Bind, etc. Often, the "Secure" setting must be enabled, but the message returned by the test client upon failure simply says, "Unknown username or password."
3. Check to see if the system needs to be on the domain in order to authenticate via LDAP (NOTE: This is not a CA requirement)

If the LDAP test is successful, but attempting to log into the CA NetQoS product produces an error, take one or more of the following steps:

1. Verify that the user account does not exist in the product already. If it does, delete it.
2. Verify that the setting "Account User Default Clone" is set to a user that exists in the product. For example, if you have the account specified as "nquser", verify that the "nquser" account exists inside the CA NetQoS product.
3. Clear out the configuration for "Groups" to verify that these settings are not causing any issues.

SSL

Secure Socket Layer (SSL) is a protocol that provides security and data integrity for communication over a network. If SSL is required for communication between the CA NetQoS product and the LDAP server, you must take the following steps to ensure successful configuration.

1. Generate an SSL certificate on the LDAP server and copy it onto the CA NetQoS server where Single Sign-On is installed.

   Note: This certificate must be a Trusted Certificate Authority.

2. On the same CA server, select Start, Run, and enter *mmc*.

3. From the File menu, click Add/Remove Snap-In, Add.
4. Select Certificates, and click Add.
5. Select Computer Account, and click Next.
6. Select Local Computer, and click Finish.
7. Click OK.
8. Return to the main Console Root window.
9. Expand Certificates (LocalComputer).
10. Expand Trusted Root Certification Authorities.
11. Right-click Certificates, and select All Tasks, Import.
12. Click Next, and then Browse for the certificate from Step 1.
13. Complete the Certificate Import Wizard and close out the Console1 application. Make sure to save.
14. Launch the Single Sign-On Configuration Tool. On the LDAP tab, verify that SSL is set to Enabled.
15. Select on the SSO tab. Verify that the Scheme is set to https and the Port is set to 443.

After you complete these steps, SSL encryption should be successful.

SSL Troubleshooting Tips

If an error message is displayed stating “Service not operational”, it indicates one of the following three problems:

1. No certificate has been installed.
2. Something in the certificate is incorrect. A common problem in this scenario is that the search domain configured in the LDAP tab of the Single Sign-On Configuration Tool lists the IP address of the server, while the certificate was generated for the server name, or vice versa. Try changing the Search Domain field to the server name (if the IP address is currently configured) or to the IP address (if the server name is currently configured).
3. The CA NetQoS product is attempting to connect via SSL, but the LDAP server is not listening on TCP port 636. Make sure that SSL is set up correctly.

Conclusion

CA NetQoS products can leverage the LDAP directories of users’ systems to allow for authentication through their existing user accounts. The Single Sign-On Configuration Tool provides flexibility and customization opportunities to address a variety of implementations.

Appendix A. Example LDAP Configurations

Active Directory

Customers using Active Directory for their LDAP implementation can refer to Figure 6 for an example of how to configure the Single Sign-On Configuration Tool.

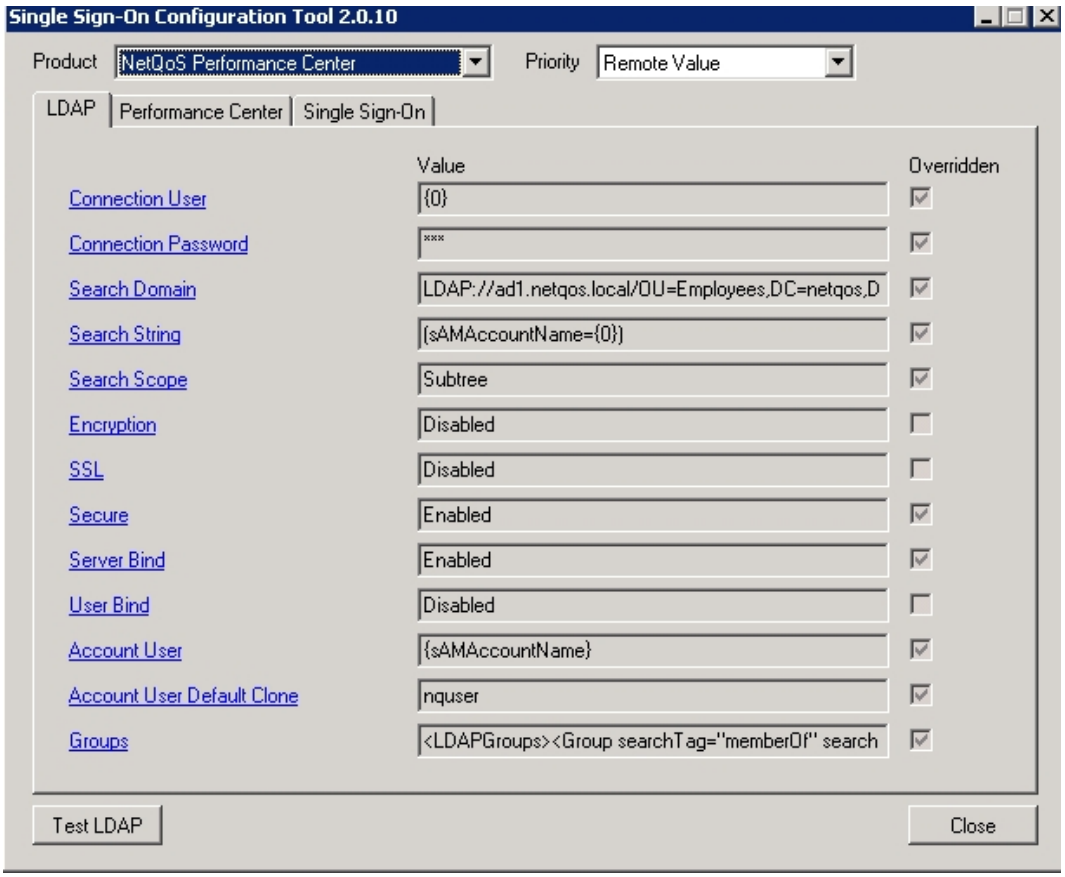

Figure 6. Sample Active Directory Configuration

Items to note from this example:

- The Connection User and Connection Password are not hardcoded. In this configuration, the username and password entered by the user at the CA NetQoS product Login page are used to access the LDAP server.
- The format of the Search Doman uses the following format:

  LDAP://< *server name or IP address*>/OU=<*X*>,DC=<*Y*>,DC=<Z>
- Note that there are no spaces between the commas and the next variable.

- The Search String, sAMAccountName={0}, means that once in the LDAP directory, the username entered on the CA NetQoS Login page must match the sAMAccountName field in the LDAP directory to authenticate successfully.

Active Directory Connecting to Global Catalog

If you are using Active Directory connecting to the Global Catalog for their LDAP implementation, refer to Figure 7 for an example of how to configure the Single Sign-On Configuration Tool.

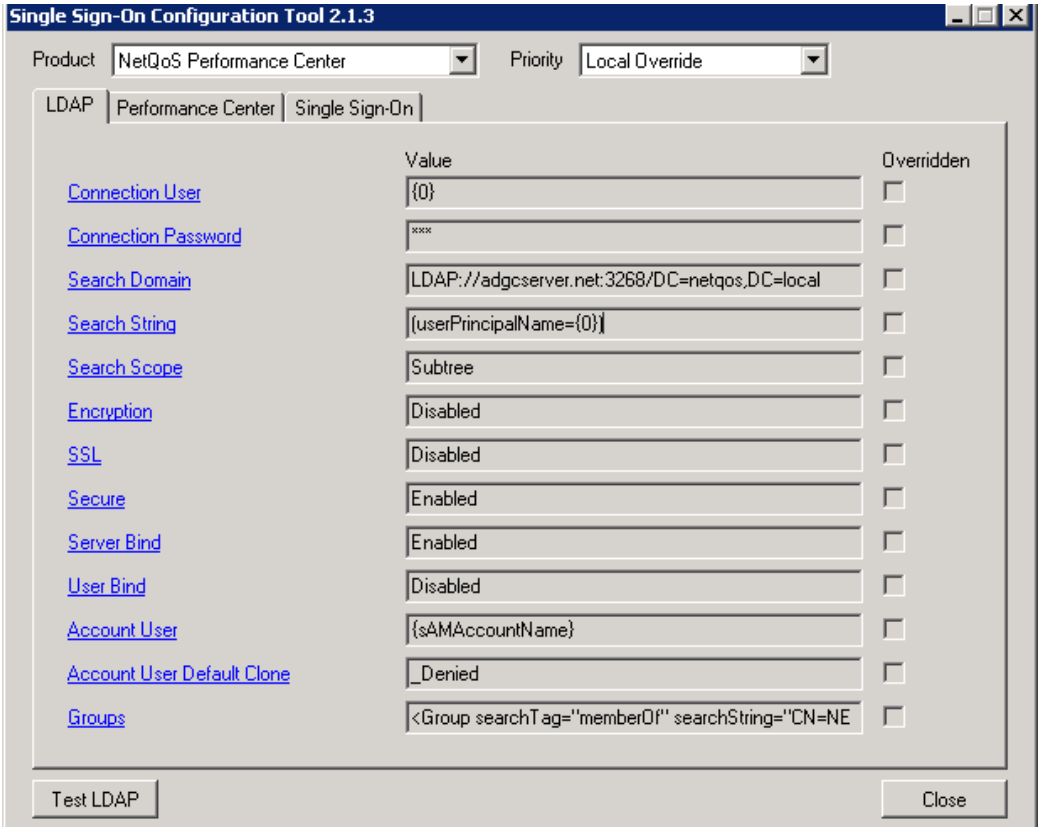

Figure 7. Sample Active Directory Connecting to Global Catalog Configuration

Items to note from this example:

- The Connection User and Connection Password are not hardcoded. In this configuration, the username and password entered by the user on the CA NetQoS product Login page are used to access the LDAP server.
- The format of the Search Doman uses the following format:

  LDAP://< *server name or IP address* >:<port number>/DC=<*X*>,DC=<*Y*>
- Note that there are no spaces between the commas and the next variable.

The Search String, userPrincipalName={0}, means that once in the LDAP directory, the username entered on the CA NetQoS Login page must match the userPrincipalName field in the LDAP directory to authenticate successfully.

OpenLDAP

If you are using OpenLDAP for your LDAP implementation, refer to Figure 8 for an example of how to configure the Single Sign-On Configuration Tool.

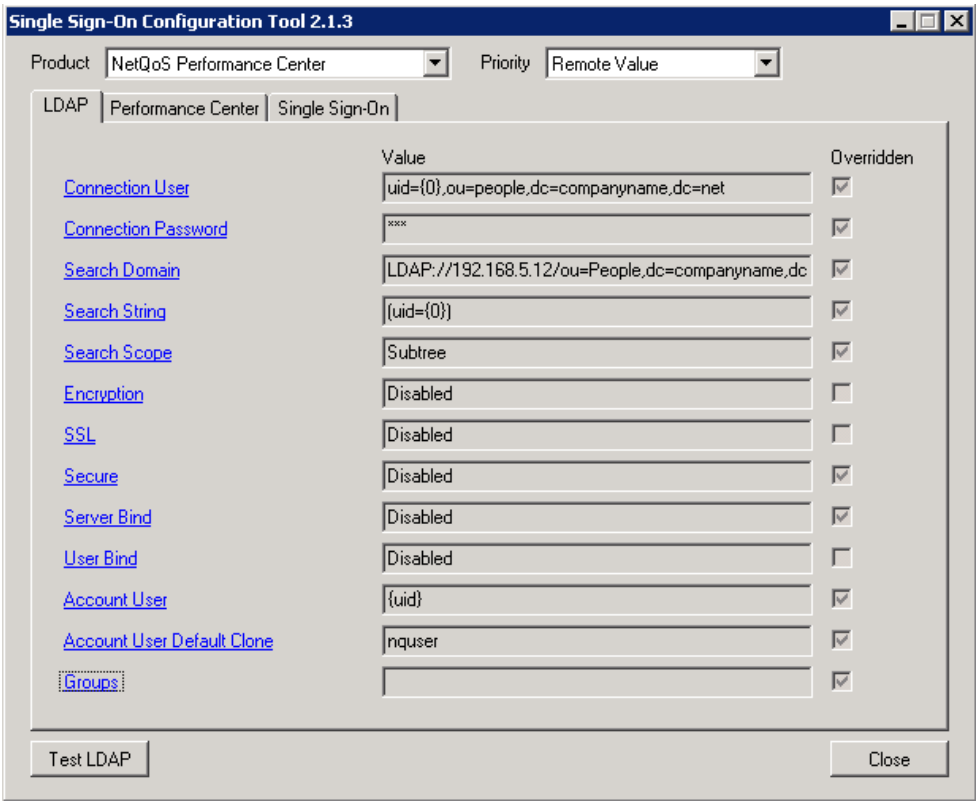

Figure 8. Sample OpenLDAP Configuration

Items to note from this example:

- The Connection User and Connection Password are not hardcoded. In this configuration, the username and password entered by the user on the CA NetQoS Login page are used to access the LDAP server. The format of the Connection User field uses the following format: uid=<*username*>,ou=<x>,dc=<y>,dc=<z>

  Note that there are no spaces between the commas and the next variable.

- The format of the Search Doman uses the following format:

  LDAP://<*server name or IP address*>/ou=<*x*>,dc=<*y*>,dc=<*z*>

  Note that there are no spaces between the commas and the next variable.

- The Search String, uid={0}, means that once in the LDAP directory, the username entered on the CA NetQoS Login page must match the uid field in the LDAP directory to authenticate successfully.