crystal decisions™

Crystal Enterprise

LDAP Features and Functionality in Crystal Enterprise 8.5

Overview

Crystal Enterprise (CE) supports various implementations of Lightweight Directory Access Protocol (LDAP) authentication. With CE 8.5, LDAP support is provided out-of-the-box. The CE 8.5 LDAP provider builds on the features delivered with the CE 8 LDAP provider update with broader support for LDAP servers, customizable LDAP server schema, and improved performance when communicating with an LDAP server.

The information in this document applies to CE 8.5. It is intended for CE administrators and LDAP administrators.

Contents

Introduction

This document includes information on the following topics:

- What LDAP platforms are supported by CE
- Configuration of CE for LDAP authentication
- LDAP Server Specifics
- Troubleshooting Tips

Server Type

The LDAP Authorization page in the Crystal Management Console (CMC) has an **LDAP Server type** list box, which allows the CE administrator to load a set of preset attributes to the page for a particular LDAP server.

NOTE	**LDAP Server Type** is only used for selecting common default attributes for a specific LDAP server. Any modifications made to the attribute mappings (exposed by clicking the **Show Attributes** button) changes the server type to **Custom**. This server type label change is cosmetic only and does not change how CE interacts with the LDAP server. It is the set of individual attribute mappings that define the communication between CE and the LDAP server.

Supported LDAP Servers

CE supports the following LDAP servers:

- IBM SecureWay
- Lotus Domino
- Novell Directory Server (NDS)
- iPlanet Directory Server

Customizable Attribute Mappings

Because each LDAP server implements its own version of the LDAP schema, CE allows the LDAP configuration to be customized. CE also provides the ability to modify the attributes used when searching for LDAP users and groups. This allows the LDAP Provider to integrate with almost any LDAP server or to allow interaction with standard LDAP servers with extended schemas. The list of configurable attributes is accessible by clicking the **Show Attribute Mappings** button on the LDAP authorization page of the CMC.

The ability to specify the object class of LDAP users and groups improves query to the LDAP server's performance as the LDAP server can quickly determine which objects are of the proper type for a query. If the object class attribute is indexed on the LDAP server the query can be even better optimized for prompt results.

How CE Recognizes LDAP Users & Groups

LDAP groups are identified by explicitly mapping them on the LDAP Authorization page of the CMC.

Once an LDAP group is mapped into CE, two things occur:

- The LDAP group gains an identity in the CE system
- All the LDAP users that are members of the LDAP group are mapped into CE.

The LDAP users have an identity similar to the LDAP groups. The LDAP users and groups are considered native to CE security. That is, an administrator can set security on info objects using the LDAP groups and/or users.

User Name Account Mapping

Many LDAP applications allow user to specify a symbolic name for an account name instead of the relative distinguished name (dn) when they log on.

For example:

The dn is cn=JCarmack, ou=People, o=CrystalDecisions and the administrator wants the user to be able to specify “John Carmack” when logging on This is possible because CE allows the **Default user search attribute** to be customized to refer to any attribute available on the LDAP entry.

User Log on Process

When a user logs on using LDAP authentication, CE goes through the following three steps before the user is granted access to the system:

1. CE queries to the LDAP server on the specified base dn to find the entry associated with the logon name entered.
2. When the entry is found, CE retrieves the dn of the user and does a bind operation (log on) to the LDAP server with the password.
3. After binding to the LDAP server, CE queries the LDAP server to determine if the user is a member of one of the mapped LDAP groups. If the user is a member of one of the mapped LDAP groups, they are granted access to CE.

If any of these steps fail and the user is not allowed to log on, refer to the Troubleshooting section of this document.

User List Management

CE provides static and dynamic LDAP user management.

Batch Loading Users (Static)

If many users have been added to the LDAP server or if it is the first time an LDAP user is used in CE, the administrator may choose to map the users in bulk into CE. This is automatically done when the LDAP Authorization page is updated. That is, the administrator clicks the **Update** button on the LDAP Authorization page. Clicking the **Update** button causes CE to iterate through the list of mapped LDAP groups, map the LDAP users in from each LDAP group, and create accounts for them if necessary or map them to existing accounts if that option is selected.

The ability to update is available via the Software Developer's Kit (SDK), thus applications that wish to ensure the user list is up to date could call the SDK on a scheduled basis.

To obtain the SDK, contact a Crystal Decisions sales representative for your area. For contact information go to:

http://www.crystaldecisions.com/contact/contactus/north_america/default.asp

Dynamically Adding New Users

After a CE administrator has mapped an LDAP group to CE, new users may be added to that group inside the LDAP server. Because CE has not been manually updated, these users do not have accounts inside CE. However, if a user is successfully authenticated as an LDAP user, CE dynamically creates a user account for them.

If the user already exists in CE, they are added as an alias to the original user. This only occurs if the CE administrator has chosen the **Assign each added LDAP alias to an account with the same name** option is selected on the LDAP authentication tab of the CMC.

If the administrator wants the user to become a new user instead of being aliased, they can select the **Create a new account for every added LDAP alias** option on the LDAP authentication page. When a user is added and they already exist in the CE environment, CE creates a new name.

For example:

If the account **Claire** already exists, the new account is called **Claire1**.

Deleting users (Static)

To statically remove an LDAP user from CE, the user must first be removed from all LDAP groups that have been mapped into CE. Then the user must be removed on the LDAP server. To remove the user from CE, the LDAP Authorization page must be updated.

Dynamically Disabling Users

When CE checks the LDAP user's membership in LDAP group dynamically at logon, the user is refused access if they have been removed from all LDAP groups on the LDAP server that have been mapped into CE.

Group to Group Membership

CE maintains LDAP group membership for all LDAP groups mapped into CE. LDAP group membership is maintained even if parts of the hierarchy between two LDAP groups have not mapped into CE.

For example:

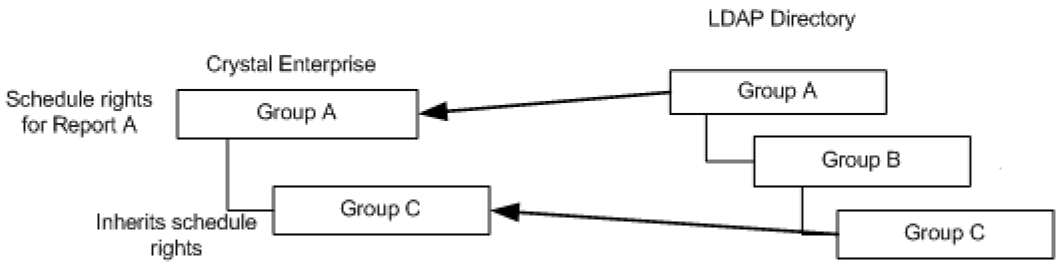


Figure 1

Bob belongs to Group C in the LDAP directory. Group A and Group C belong to the CE environment. Therefore, Bob inherits the rights of Group A even though CE did not bring across Group B. CE maintains the group relationship of the LDAP directory even if some of the groups are not brought into CE.

Group Maintenance for an Active User

When an LDAP user logs on to CE, the set of LDAP groups they belong to is cached in CE to increase performance for queries on object access (Authorization). This list is cached for a non-configurable ten minutes at which time it is refreshed.

LDAP Related Authentication Mechanisms

Authentication is the act of identifying a user and then confirming their identity. CE uses Simple Authentication.

Simple Authentication

The simple authentication option provides minimal authentication facilities, with the contents of the authentication field consisting only of a clear text password as specified in the LDAP V3 specifications.

An LDAP account name and password are required at CE logon. The information is sent to the LDAP server for authentication.

LDAP Referrals

CE supports LDAP referrals, which allow an LDAP server to refer to another LDAP server for queries, LDAP users, or LDAP groups. Therefore, it is possible to split LDAP users between many servers.

LDAP Single Sign On (SSO)

CE requires the LDAP username and password for the user to log on. SSO solutions must be able to forward these user credentials to CE.

LDAP Server Fail Over

CE can be configured to fail over to other LDAP servers if the primary server becomes unavailable. This can be done by adding the server name and port number of the alternative LDAP servers to the **LDAP Hosts** dialog box on the LDAP Authorization page of the CMC. The order of the servers in the list box dictates in what order the servers will be failed over in.

Getting Started

To provide a connectivity test to get a CE deployment started quickly, this section has been created. Included is a list of the basic requirements for configuring CE with LDAP followed by specifics about each LDAP server.

The following section is not a guide to install each LDAP server. Installation of the LDAP server is left to the LDAP server documentation.

Minimum requirements for an LDAP server to operate with CE

CE requires three things to begin recognizing LDAP users and allowing users to log on:

- Hostname and port number of the LDAP server (<**hostname**>,<**port**>)

The hostname is the server name of the LDAP Server. The default LDAP port is 389, which most directory servers default to.

- Base dn (<**base dn**>)

From a CE perspective, this is the root LDAP node from which CE begins all queries.

- At least one LDAP group mapped to CE (ensure the LDAP group has LDAP users in it)

  (<**group name**>)

The users mapped into the LDAP server group will be the users who are mapped into CE and allowed to log on. This assumes the LDAP server will allow anonymous queries. If not, you may need to set the admin username and password in the “LDAP Server Administration Credentials” box on the LDAP Authorization page.

These three requirements can be specified on the LDAP Authorization page in the CMC.

How to configure CE with minimum requirements

To configure CE with the minimum LDAP requirements, complete the following steps:

1. In the CMC, click **Manage Authorization** and then click the **LDAP** tab.
2. Select the **LDAP Authentication is enabled** check box.
3. Click your LDAP server type in the **LDAP Server Type** list.
4. In the **LDAP Hosts** field, type the host name and port number. If the LDAP server is listening on the default port 389, the port number may be left off. The format of this entry is as follows:

   hostname:port

5. In the **Base LDAP Distinguished Name** field, type the base dn in the following format:

   o=base dn

6. Click the **Update** button at the bottom of the page. This tests connectivity to the LDAP server.
7. In the **Add LDAP group (by cn or dn)** field, type an LDAP group name.
8. Click the **Update** button.

If you return to the CMC home page and click **Manage Users**, the LDAP users appear.

LDAP Server Specifics

This section contains a brief introduction to each LDAP server, considerations, and suggestions for each when using with CE.

IBM SecureWay

IBM SecureWay is the LDAP server included with IBM's application server suite. IBM SecureWay has a web based and a thick client administration interface.

The following points outline how to retrieve the port, base dn, and group values needed for CE.

- Port: The IBM SecureWay server defaults to port 389. In the **Directory Management Tool**, the port number is listed on the folder tree tab in the left pane. This is shown in Figure 2.
- base dn: The base dn is the "suffix" in IBM SecureWay. In the **Management Tool,** go to **directory server** > **settings** > **suffixes** to configure suffixes.
- group: Groups are available anywhere under a "suffix". Ensure that the group is created with the Entry Type of Access **group** or it will not be recognized in CE.

Secure Bind

IBM SecureWay returns partial information when making queries from an anonymous bind. The information returned is not enough for CE to determine user and group membership. The admin credentials must be configured in the LDAP authentication tab to return the full set of query information.

IBM (Tivoli) Policy Server

IBM Policy Server is also part of the IBM suite of products. It performs access management on objects and uses IBM SecureWay as its repository for maintaining users and groups. The users and groups that are created using IBM Policy Server are simultaneously created in IBM SecureWay. IBM Policy Server creates extra entries and an additional master security user for its own use.

CE ignores these extra entries but may bring in the extra security user. No additional configuration is required in CE when using an IBM SecureWay server managed by IBM Policy Server if the APS hot fix is applied.

To get this update, go to http://support.crystaldecisions.com/downloads and search for the file ce85apswin_en.zip

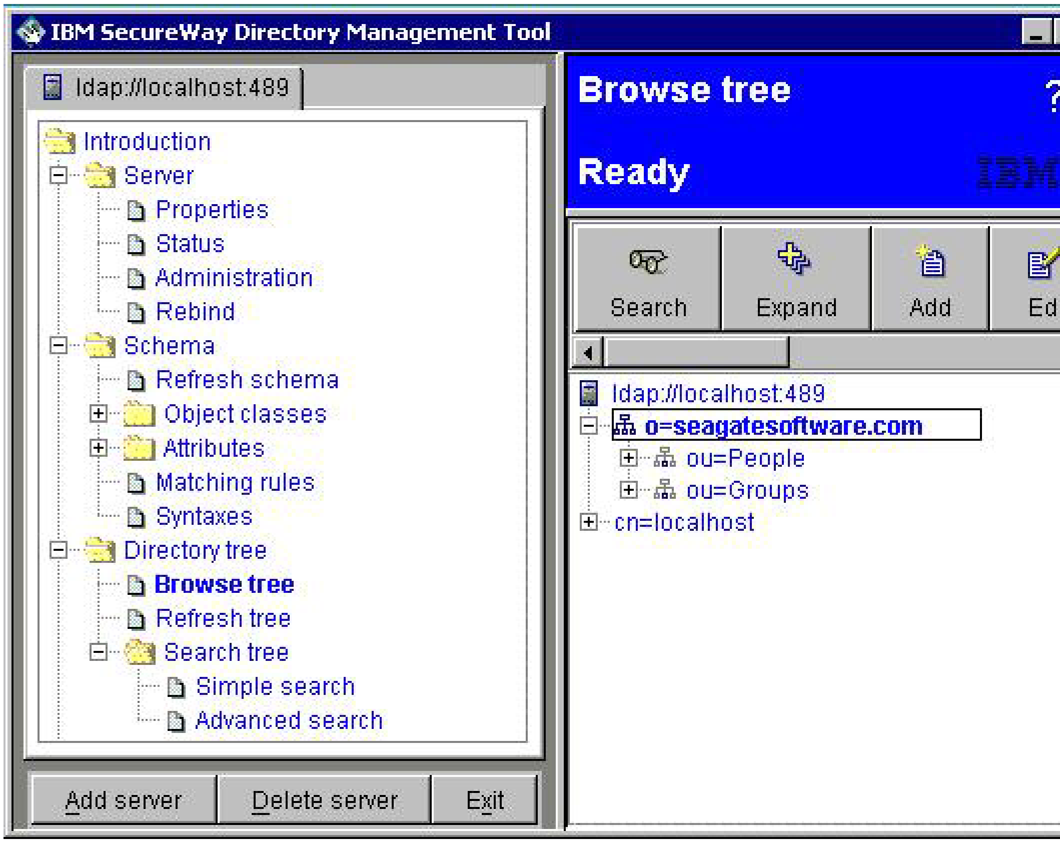


Figure 2

Lotus Domino

Domino is a directory server that provides the ability to expose an LDAP interface. Because Domino supports functionality that is not standard in a basic LDAP directory server, it is suggested that an experienced Domino administrator assist in configuring Domino for LDAP support.

First, the Domino server must be configured to provide an LDAP interface. If, it is not, consult with your Domino administrator.

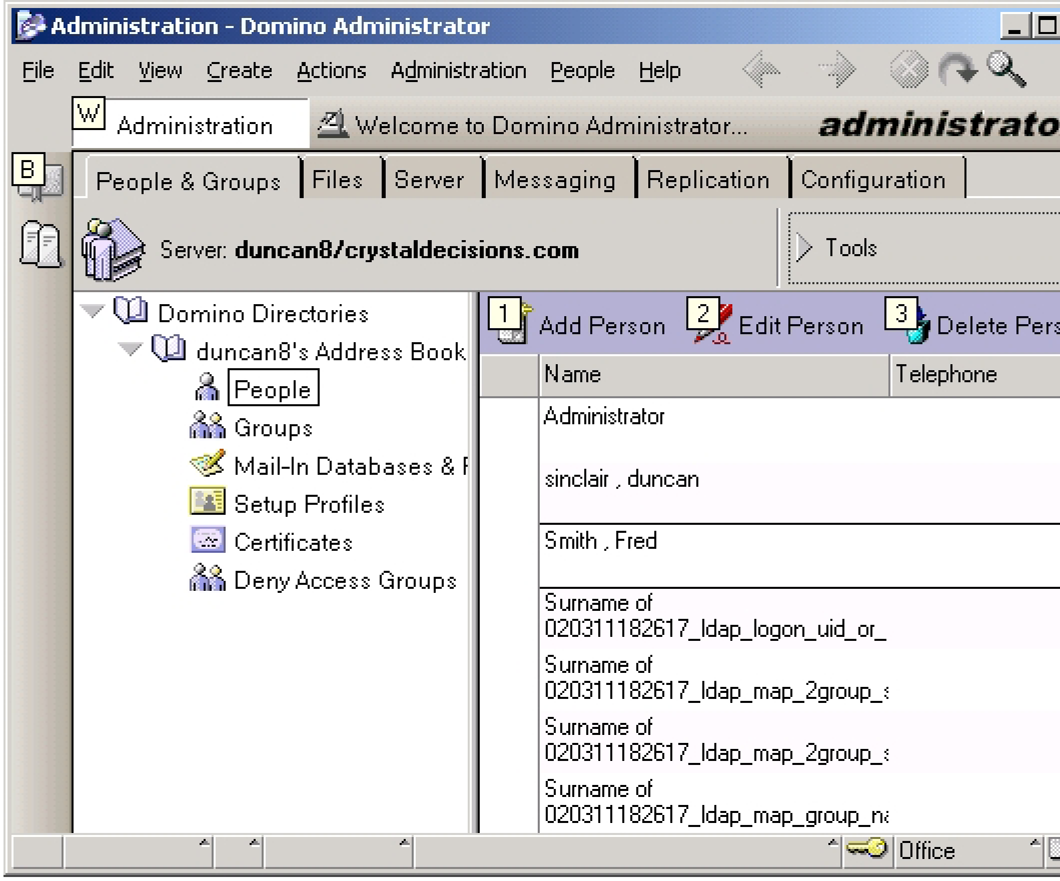
The following points outline how to retrieve the port, base dn, and group values needed for CE.

- port: The Domino server port defaults to 389. The port can be configured under the **server properties** on the LDAP page in Domino.
- base dn: When configuring the LDAP portion of Domino during the setup, the admin would have been prompted for a **certifier's name**. This is the

base dn. The certifier's name is displayed with the Domino server name, once LDAP has been installed.

- group: All you need is the group name.

These values are for the default Domino configuration, if a hierarchy has been set up then some of the values may have to be changed. In such a case, the Domino administrator should be consulted for these values. As retrieving LDAP information from Domino can be challenging, it is suggested that the Domino administrator is available to assist during the CE configuration process.



Name	Telephone
Administrator	
sinclair , duncan	
Smith , Fred	
Surname of 020311182617_ldap_logon_uid_or_	
Surname of 020311182617_ldap_map_2group_s	
Surname of 020311182617_ldap_map_2group_s	
Surname of 020311182617_ldap_map_group_na	

Figure 2

Novell Directory Server (NDS)

NDS, or eDirectory, is Novell's LDAP server. The NDS interface can be challenging and it is recommended that the NDS administrator assist in configuring NDS for CE.

The default installation of NDS does not allow clear text authentication or anonymous queries. Both of these features are required before CE can communicate with NDS.

The following points outline how to retrieve the port, base dn, and group values needed for CE.

- port: Under the CE context, open the properties of the server. The port is displayed on this page.
- base dn: The base dn is the context displayed under the tree.
- group: Under the context, find a group. The group name is the string to use in CE.

Clear Text Authentication

For CE to work with NDS, the **clear text authentication** option must be enabled. To enable NDS for clear text authentication go to the NDS context that CE will be using, activate the properties for the **LDAP Group** icon and select the **Allow Clear Text Passwords** check box.

Anonymous Queries

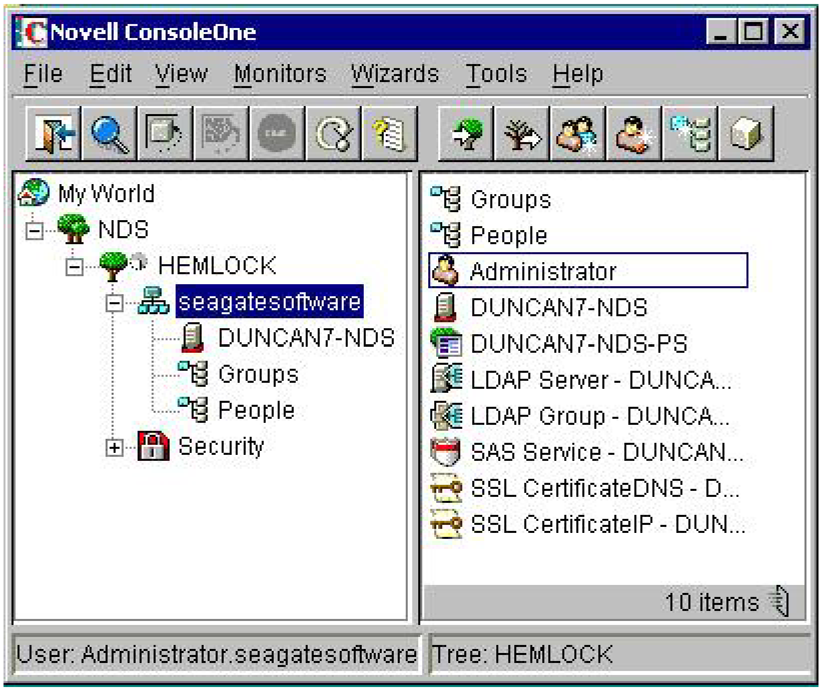
For CE to work with NDS, anonymous queries must be enabled or administrative credentials must be set in CE.

To enable NDS for anonymous queries, go to the tree above the context that CE will be using, activate the properties for the tree and click the **NDS Rights** tab.

The following rights must be assigned to **[Public]:**

- **supervisor**
- **browse**

To set administrative credentials in CE, type the NDS administrative username and password in the **LDAP Server Administration Credentials** box on the LDAP Authorization page.



User: Administrator.seagatesoftware

Tree: HEMLOCK

Figure 4

iPlanet Directory Server

iPlanet ships with a Java based administrative interface for its administrative server and directory server.

iPlanet Directory Server requires a static IP and needs to be used for production systems.

To activate the administrative interface for the directory server, open the iPlanet Administrator and expand the tree to the directory server. Double-click the directory server.

The following points outline how to retrieve the port, base dn, and group values needed for CE.

- port: This is the port number of the directory server, not the administration server. To obtain the port of the administration server, open the administrative server, expand the tree and click the **directory server** icon. In the right pane there is a list of the directory server's properties. The port is listed there.
- base dn: the base dn is the name in the entry that is children of the root node.
- group: Under the **Groups** icon is a list of groups. The group name is the one to use in CE.

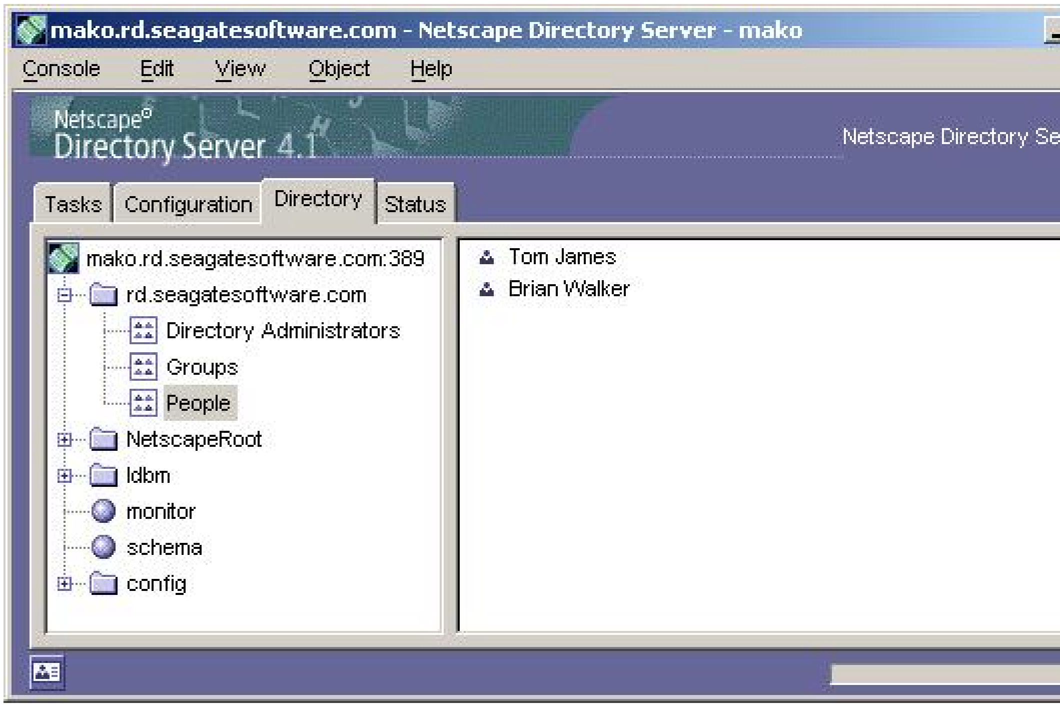


Figure 5

How to recognize Active Directory users with CE

If you want to recognize LDAP users and LDAP groups from Active Directory, this is possible through NT4 support. However, the LDAP users and LDAP groups are mapped in as NT users and NT groups. The NT Authentication mechanism can be used because Microsoft has designed Active Directory to be backward compatible for older operating systems such as NT4.

It should be noted that CE only supports Active Directory servers running in Mixed Mode. Active Directory Native Mode operation is currently not supported.

Troubleshooting Tips and Frequently Asked Questions

When troubleshooting issues with LDAP authentication, the first place to look for answers is the LDAP server log file. When an LDAP related error occurs in CE, the process CE is attempting to achieve on the LDAP server likely produces the error.

I can see my LDAP users in CE but they cannot log on

Besides the obvious errors like incorrect password, these are several reasons why a user may not be able to log on.

User name Mapping

When a user attempts to log on to CE, CE queries the LDAP server for the user by searching for the “user search attribute” that matches the name used to log on to CE with.

Ensure the LDAP “user search attribute” matches the attribute that the LDAP administrator wants users to log on with. For example:

- <First Name><space><Last Name> will require a search attribute of “cn” (e.g. John Smith)
- <First initial of First Name><Last Name> will require a search attribute of “uid” (e.g. jsmith)

Additionally, try using the dn as the account name.

Blank Password

CE requires a password to be present, irrelevant if the LDAP server has one or not. If there is no password in CE, the user will not be allowed to log on.

Group Membership

A user must belong to a group that exists in the CE environment. If they belong to an LDAP group that has not been brought across to CE they will not be able to log on to CE.

I can see my user but when I log on I get the message: “account information not recognized” Why?

This probably happens because simple authentication is not enabled on the LDAP server. Ensure that it is enabled.

When I try to connect to the directory server why do I get the error message stating my credentials are incorrect?

This can occur for two reasons:

- The machine name is invalid. Try the Fully Qualified Distinguished Name or the IP address. Ensure the directory server machine is accessible over the network.
- The port number is incorrect. The default is 389 but when multiple LDAP servers are running on the same machine it is common to have other values in use. Check the directory server properties.

If this fails, try connectivity by using an external LDAP tool to ensure the machine name and port are correct.

Can my users log on with different LDAP attributes? e.g. “jsmith” or “John Smith”

No, only one user search attribute can be specified when looking up a user’s account.

Is Open LDAP Supported in CE?

Currently Open LDAP is not supported. It is being considered for future releases of CE.

If you disable LDAP, how do you clean out the user ids and groups from the CMC?

Delete the group from the LDAP Authorization page and click update. This will remove all users that were only mapped into CE via that deleted group.

If a user password expires will CE prompt the user to change it?

CE does not handle changing passwords from the 3rd party system. This is managed in the front-end application.

Can an LDAP administrator manage CE Rights and Objects (Folders, Report, CAPro objects, instances) from the LDAP server interface?

It is possible to customize the csp pages of the CE administration to do the following:

- read the users' rights on specific objects within LDAP
- write and/or enable these rights on objects within CE
- send information of new published objects, folders, or instances to the LDAP server

Important information regarding this functionality:

- **Modifying CSP admin pages**

CE does not expose the admin CSP pages you must create your own. The CSP must synchronize the LDAP server with the CE server. This process is not recommended.

- **The common solution to this problem**

To do what is being asked of CE would need to store info objects in the LDAP server. This has been looked into and there are three concerns:

- LDAP servers are designed primarily for reads, with the expected ratio being one write to tens of thousands of queries. CE does more reads that writes however, the ratio is much greater than LDAP servers are designed for.
- CE would have to either create its own instance tree in the LDAP server to match it's internal structure, basically turning the LDAP server into the APS database, or expand the customers' existing data scheme. The first option can greatly increase the footprint of the LDAP server, especially if other applications have their own tree instances. The second option can become challenging to manage when many other applications are modifying the schema as well.
- CE has an out-of-the-box User Interface (UI) to ease the management of security in CE. An LDAP server would only be able to provide rudimentary UI for configuring CE security and would be more time consuming to configure and maintain.
- **Current Alternative**

CE's LDAP plug-in allows user membership in groups to be maintained from the LDAP server. If the admin initially set up security in CE using mapped LDAP groups on infoobjects, they could control what infoobjects users could see by adding or removing them from groups on the LDAP server.

What authentication mechanisms can scheduled jobs use to log on to a database?

There are two mechanisms:

- Store the username and password in CE with the object and use them when logging on to the database
- Have the account the process is running under be used to access the database.

  This method is dependant on the Operating System and the database to support it. This method can be a security risk and is commonly avoided.

Contacting Crystal Decisions for Technical Support

We recommend that you refer to the product documentation and that you visit our Technical Support web site for more resources.

Self-serve Support:

http://support.crystaldecisions.com/

Email Support:

http://support.crystaldecisions.com/support/answers.asp

Telephone Support:

http://www.crystaldecisions.com/contact/support.asp