ZENworks 2020 Update 2

User Source and Authentication Reference

August 2021

Legal Notice

About This Guide

This *ZENworks User Sources Reference* explains how to connect your ZENworks system to one or more LDAP directories to provide authoritative user sources in ZENworks. Adding a user source lets you associate ZENworks administrator accounts with LDAP user accounts, assign content to users, associate devices with the users who primarily use them, and run asset inventory and management reports that include users. The guide includes the following sections:

Audience

This guide is intended for ZENworks administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation.

Additional Documentation

ZENworks is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. For additional documentation, see the Documentation Web site.

Contents

1 Prerequisites

- **Minimum directory version:** eDirectory 8.7.3, Microsoft Active Directory on Windows 2000 SP4, Domain Services for Windows (DSfW) on OES 2 SP2.
- **Minimum LDAP version:** LDAPv3
- **Minimum user account rights:** Read rights.

  For Active Directory, you can use a basic user account. This provides sufficient read access to the directory.

  For eDirectory, you need inheritable read rights to the following attributes: CN, O, OU, C, DC, GUID, WM:NAME DNS, and Object Class. You can assign the rights at the directory's root context or at another context you designate as the ZENworks root context.

  The username and password used to access the user source directory are stored in clear-text format on the ZENworks Linux Primary servers in the `/etc/CASA/authtoken/svc/iaRealms.xml` file. By default, the access to this file is limited because of security reasons.

  If you are an eDirectory user the required access rights that are provided by default are: Read, Write, Create, Erase, Modify, File Scan, and Access Control. These rights are sufficient to access a Roaming profile.
- **DNS name resolution:** With Active Directory, your ZENworks Servers (in particular, the DNS clients on the ZENworks Server) must be able to resolve the DNS name of each Active Directory domain defined as a user source. Otherwise, users from the Active Directory domain cannot log in to the ZENworks Management Zone.

2 Managing User Sources

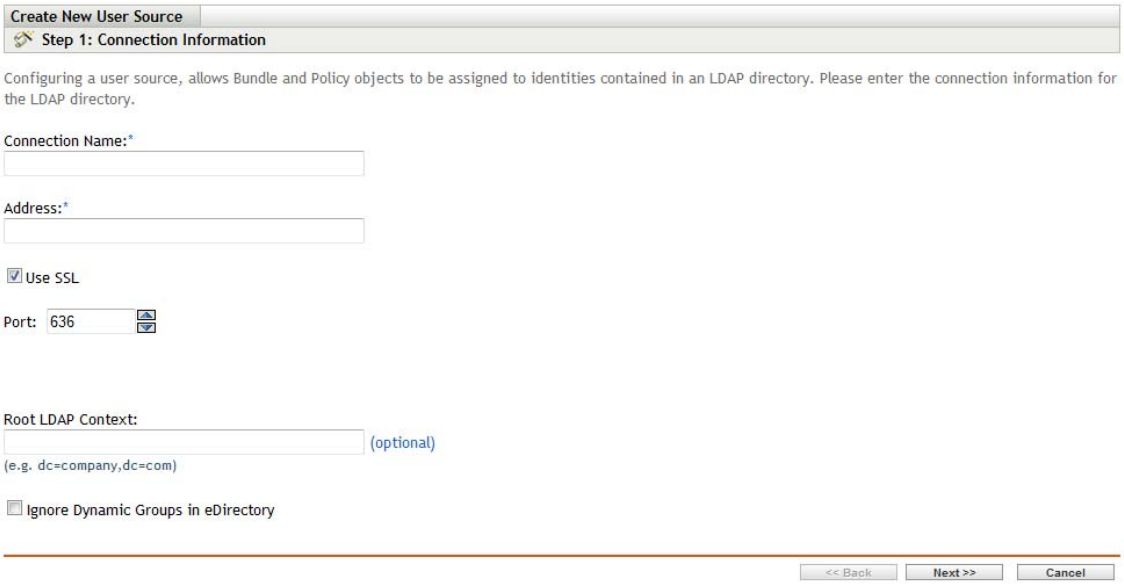
The following sections contain more information:

2.1 Adding User Sources

After you define a user source, the ZENworks Agent automatically prompts device users to log in to the ZENworks Management Zone. If you do not want users to receive this prompt, you can uninstall or disable the User Management module at the ZENworks Agent level. For more information, see “Configuring ZENworks Agent Settings after Deployment” in the *ZENworks Agent Reference*.

1 In ZENworks Control Center, click the **Configuration** tab.

2 In the User Sources panel, click **New** to launch the Create New User Source Wizard.



3 Follow the prompts to create the connection to the user source.

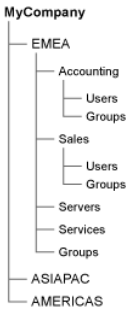
For information about each of the wizard pages, click the **Help** button or refer to the following table:

Wizard Page	Details
Connection Information page	Specify the information required to create a connection to the LDAP directory: ◆ **Connection Name:** Specify a descriptive name for the connection to the LDAP directory. ◆ **Address:** Specify the IP address or DNS hostname of the server where the LDAP directory resides. ◆ **Use SSL:** This option is applicable for a user source and is displayed only if you are creating a new user source. However, this option is not displayed if you are adding a new connection for an existing user source. By default, this option is enabled. Disable the option if the LDAP server is not using the SSL (Secure Socket Layer) protocol. **NOTE:** If the Active Directory servers have the LDAP channel bind fixes from Microsoft, then ZENworks user authentication will break for all the LDAP Servers for which SSL is not enabled. For more information, see "Troubleshooting User Authentication" on page 57 ◆ **Port:** This field defaults to the standard SSL port (636) or non-SSL port (389) depending on whether the **Use SSL** option is enabled or disabled. If your LDAP server is listening on a different port, select that port number. ◆ **Root LDAP Context:** Displays the root context for the LDAP directory. This option is available only when you are creating a new user source. The root context establishes the point in the directory where you can begin to browse for user containers. Specifying a root context can enable you to browse less of the directory, but it is optional. If you don't specify a root context, the directory's root container becomes the entry point. ◆ **Ignore Dynamic Groups in eDirectory:** This option allows you to select whether or not to display the dynamic groups in a Users page. If you choose to select **Ignore Dynamic Groups in eDirectory**, then users cannot assign a policy or a bundle to a dynamic user group and the dynamic group membership will not be computed while calculating the effective assignments for any user.
Certificate Page	(Conditional) If you selected Use SSL on the previous Wizard page (Connection Information), the Certificate page displays as the next. step in the Wizard. Ensure that the Certificate is correct.

Wizard Page	Details

Credentials page	Specify a username and password for accessing the directory:
	◆ **Username:** Specify the username for a user that has read-only access to the directory. The user can have more than read-only access, but read-only access is all that is required and recommended.
	For Novell eDirectory access, use standard LDAP notation. For example:
	`cn=admin_read_only,ou=users,o=mycompany`
	For Microsoft Active Directory, use standard domain notation. For example:
	`AdminReadOnly@mycompany.com`
	For DSfW, use standard LDAP notation. For example:
	`cn=admin_read_only,ou=users,dc=mycompany,dc=com`
	◆ **Password:** Specify the password for the user you specified in the **Username** field.
	NOTE: Ensure that the password does not contain the special characters ~ and \.

Wizard Page	Details
Authentication Mechanisms page	Select the mechanism used to authenticate users to the ZENworks Management Zone. The available mechanisms depend on whether you are configuring a Novell eDirectory or a Microsoft Active Directory user source. ◆ **Kerberos:** Active Directory or Domain Services for Windows (DSfW). Enables Kerberos authentication in which the Active Directory server generates a Kerberos ticket that Novell Common Authentication Services Adapter (CASA) uses to authenticate the user, instead of using a username and password. Kerberos authentication is often used with smart cards. ◆ **Username/Password:** eDirectory, Active Directory, or Domain Services for Windows (DSfW). Enables simple authentication using a username and password. ◆ **Shared Secret:** eDirectory only. Enables a user to automatically log in to ZENworks when a smart card is used to log in to eDirectory. This option is enabled only if the schema of the eDirectory specified in the Connection Information page is extended using the microfocus-zenworks-configure tool. If **Shared Secret** is not selected as an authentication mechanism, a ZENworks login dialog box is displayed when the user on the managed device attempts to log in to eDirectory using a smart card. After the user specifies the eDirectory username and password, that password is stored in Novell SecretStore. The next time the user uses a smart card to log in to eDirectory, the password is retrieved from SecretStore and the user is logged in to the ZENworks without having to specify the password. If you select both available mechanisms (**Kerberos** and **Username/Password** for Active Directory or **Username/Password** and **Shared Secret** for eDirectory), ZENworks Configuration Management attempts to use the first mechanism for authentication. If authentication fails, the next mechanism is used. For example, if you select **Kerberos** and **Username/Password** for Active Directory, ZENworks Configuration Management first attempts to use Kerberos authentication. If Kerberos authentication fails, simple Username/Password authentication is used.

Wizard Page	Details
User Containers page	After you connect to an LDAP directory as a user source, you can define the containers within the directory that you want exposed. The number of user containers you define is determined by how much of the directory you want to expose. Consider the following example:  Assume that you want to enable all users in the Accounting and Sales containers to receive ZENworks content. In addition, you want to be able to access the user groups located in the Accounting, Sales, and Groups containers in order to distribute content based on those groups. To gain access to the users and groups, you have two options: ◆ You can add MyCompany/EMEA as a user container, so all containers located below EMEA are visible in ZENworks Control Center, including the Servers and Services containers. Only users and user groups located in the EMEA containers are visible (servers and services are not), but the structure is still exposed. ◆ You can add MyCompany/EMEA/Accounting as one user container, MyCompany/EMEA/Sales as a second container, and MyCompany/EMEA/Groups as a third container. Only these containers become visible as folders beneath the MyCompany directory reference in ZENworks Control Center. To add the containers where users reside: 1. Click **Add** to display the Add User Container dialog box. 2. In the **Context** field, click to browse for and select the desired container. 3. In the **Display Name** field, specify the name you want used for the user container when it is displayed in ZENworks Control Center. 4. Click **OK** to add the container to the list.

2.2 Deleting User Sources

When you delete a source, all assignments and messages for the source's users are removed. You cannot undo a source deletion.

1. In ZENworks Control Center, click the **Configuration** tab.
2. In the User Sources panel, select the check box next to the user source, then click **Delete**.
3. Click **OK** to confirm the deletion.

2.3 Editing User Sources (Active Directory or eDirectory)

1. In ZENworks Control Center, click the **Configuration** tab.
2. In the User Sources panel, click the underlined link for a user source.
3. You can edit the following settings:

   Username and Password: Click **Edit**, edit the fields, then click **OK**.

   The ZENworks system uses the username to access the LDAP directory. The username must provide read-only access to the directory. You can specify a username that provides more than read-only access, but read-only access is all that is required and recommended.

   For Novell eDirectory access, use standard LDAP notation when specifying the username. For example:

   ```
   cn=admin_read_only,ou=users,o=mycompany
   ```

   For Microsoft Active Directory, use standard domain notation. For example:

   ```
   AdminReadOnly@mycompany.com
   ```

   Authentication Mechanisms: Click **Edit**, select the desired mechanisms, then click **OK**.

   For more information, see Section 7.1, "Authentication Mechanisms," on page 37.

   Use SSL: By default, this option is enabled. Click **No** to disable the option if the LDAP server is not using the SSL (Secure Socket Layer) protocol.

   If you edit this option, you must do the following for every connection that is listed in the connections panel:

   - **Update the certificate:** For more information on updating the certificate see, Section 3.4, "Updating a Certificate for a User Source," on page 25
   - **Update the port:** If your LDAP server is listening on a different port, select that port number.

   NOTE: If you edit the user source either to enable or disable the **Use SSL** option, you must restart the ZENworks services on the server or the authentication to the user source fails.

   Root LDAP Context: Displays the root context for the LDAP directory. This option is available only when you are creating a new user source.

   The root context establishes the point in the directory where you can begin to browse for user containers. Specifying a root context can enable you to browse less of the directory, but it is completely optional. If you don't specify a root context, the directory's root container becomes the entry point. Click **Edit** to modify the root context.

Ignore Dynamic Groups in eDirectory: This option allows you to select whether or not to display the dynamic groups in a Users page. If you choose to select **Ignore Dynamic Groups in eDirectory**, then users cannot assign a policy or a bundle to a dynamic user group and the dynamic group membership will not be computed while calculating the effective assignments for any user.

Description: Click **Edit**, to modify the optional information about the user source, then click **OK**.

User Containers: For more information, see Section 2.4, “Adding a Container from a User Source,” on page 16. You can also remove or rename a user container.

Connections: For more information, see Section 3.2, “Editing User Source Connections,” on page 24.

Authentication Servers: For more information, see Section 5, “Managing Authentication Server Connections for User Sources,” on page 29.

2.4 Adding a Container from a User Source

After you have defined a user source in your Management Zone, you can add containers from that source at any time.

1. In ZENworks Control Center, click the **Configuration** tab.
2. In the User Sources panel, click the user source.
3. In the User Containers panel, click **Add** to display the Add User Container dialog box, then fill in the following fields:

   Context: Click  to browse for and select the container you want to add.

   Display Name: Specify the name you want used for the user container when it is displayed in ZENworks Control Center. The name cannot be the same as the name of any other user containers.
4. Click **OK** to add the user container.

   The container, and its users and user groups, is now available on the **Users** page.

2.5 Enabling User Source for Mobile Device Enrollment

For more information, see Enabling a User Source for Mobile Device Enrollment.

2.6 Configure Azure AD as a User Source

To configure Azure AD as a User Source, you need to perform the following steps:

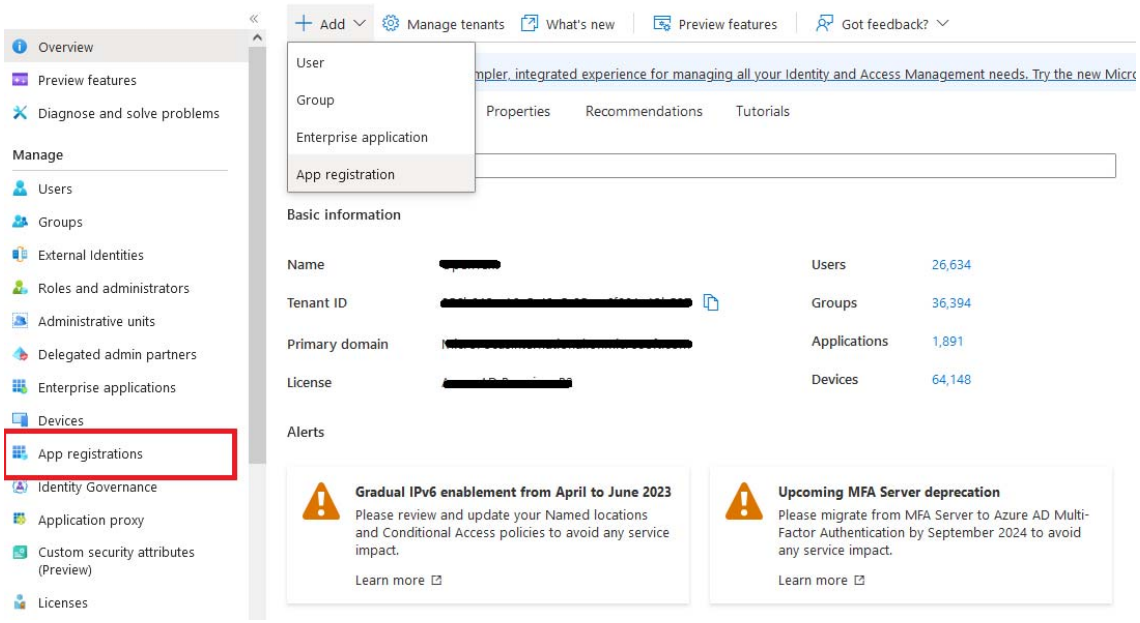
- Step 1: Create Azure AD Application
- Step 2: Adding Azure Application in ZENworks
- Step 3: Configuring Azure AD User Source in ZENworks
- Editing Azure Active Directory User Sources

2.6.1 Step 1: Create Azure AD Application

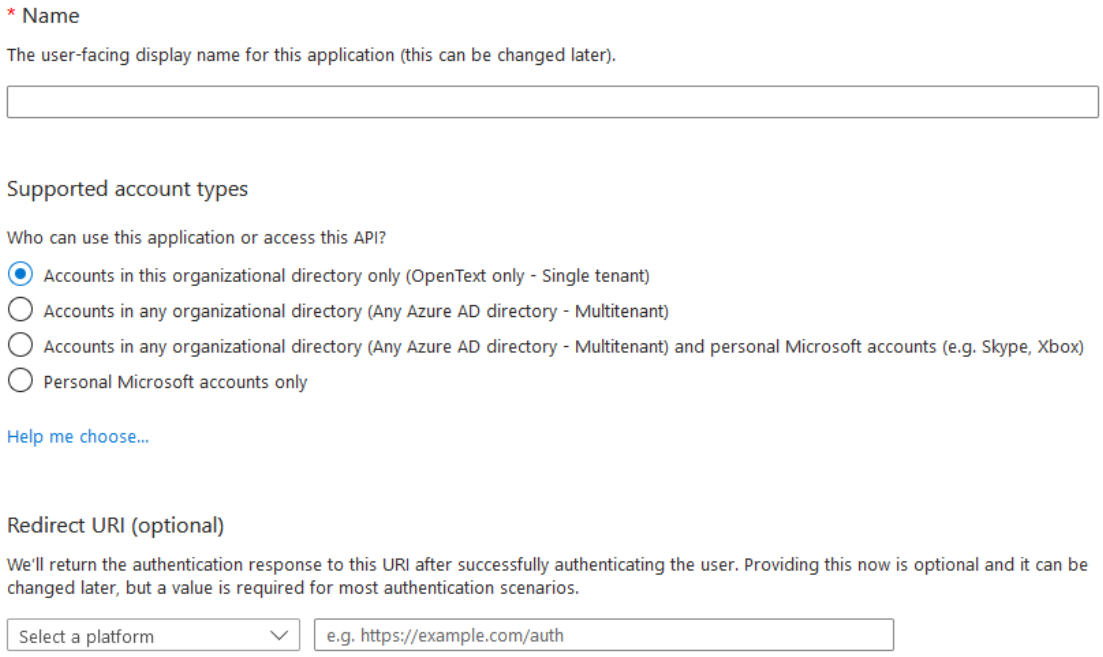
1. Log into the Azure portal.

   https://portal.azure.com/.

2. On the welcome page, Click **Azure Active Directory**.
3. In the left pane, select **App Registrations**.

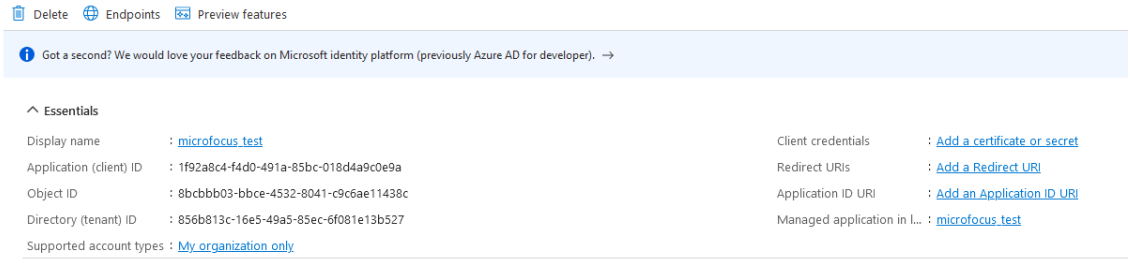


4. Select the **New Registration** link.
5. Specify the registration name.
6. Select **Accounts in this organizational directory only**. Leave Redirect URI blank, which can be updated later.



7. On the **Registration** page, for the new registration created, copy the Application (client) ID.
8. To add the redirect URI, In the left pane, click **Authentication**.

   Redirect URI is a location where the server redirects users after successful authorization.



   Click **Add a platform**, and select **Mobile and desktop applications**.

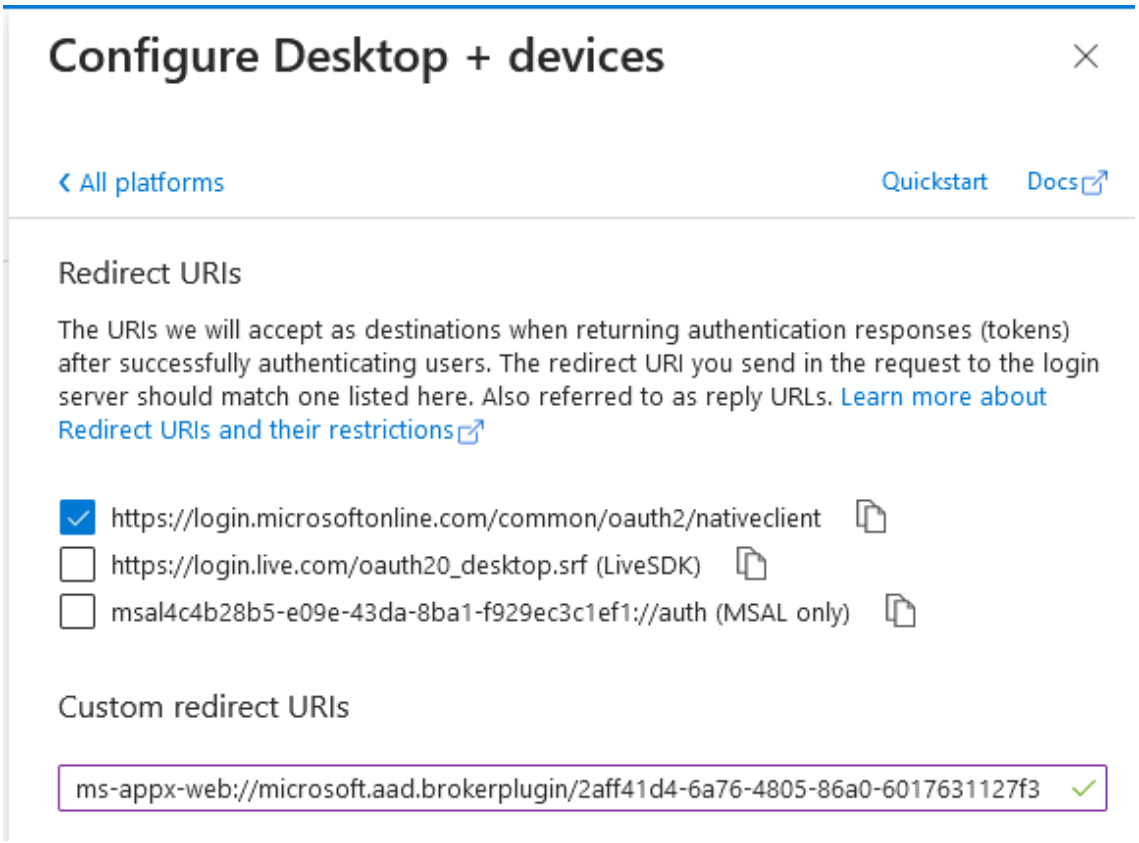
   Select *https://login.microsoftonline.com/common/oauth2/nativeclient* and add a custom URI as shown below:

   ms-appx-web://microsoft.aad.brokerplugin/{client_id}

   Replace {client_id} with the application ID copied in Step 7.

   Example: *ms-appx-web://microsoft.aad.brokerplugin/2aff41d4-6a76-4805-86a0-6017631127f3*

   In this example, *2aff41d4-6a76-4805-86a0-6017631127f3* is the client-id



9. In the left pane, Click **Client credentials**, click **New client secret**, specify the description and select expiry duration, and then click **Add**.
10. Copy the Secret Value (Client Secret).

    The client secret is displayed only once. Hence, it is recommended that you copy the value, so that this can be used later while configuring the user source in ZENworks.
11. On the left menu, Click **Authentication**.
12. In the **Platform configurations**, click **Add a platform**, and then select **Mobile and desktop applications**.
13. On the left menu, Click **API permissions**, click **Add a permission**, and then click **Microsoft Graph Application**.
14. Add the required permissions, click **Application permissions** and select the following:
    - User.Read.All
    - Group.Read.All

    Select **Delegated permissions** and select **openid**.

    After adding the required permission, ensure that all the configured permissions of type **Application** are granted Admin Consent by clicking the button next to **Add a permission**.
15. After successfully completing all the above-steps, the app is configuration is complete.

    Ensure that you have the following details from the Azure portal:

    These details will be used to configure user source in ZENworks.
    - Application (client) ID

- Directory (tenant) ID
- Secret Value (Client Secret)

2.6.2 Step 2: Adding Azure Application in ZENworks

After creating an application and collecting the required details in the Azure portal, switch to ZENworks to add the application, which enables ZENworks to communicate with Azure.

Perform the following steps to add the Azure application in ZENworks:

1. In ZENworks Control Center, click **Configuration** > **Management Zone Settings** > **Infrastructure Management** > **Azure Applications**.
2. In the **Azure Applications** page, click **Add Application**.
3. In the **Add Application** pop-up, select an MDM server.
4. Select the purpose for which the Azure application will be used.

   By default, the User Source Application is selected as the application will be used to configure the Azure AD user source.
5. Click **Add Application**.
6. In the Specify Application Details page, specify the details that were gathered in the Azure portal while creating an application:
   - Application ID
   - Tenant ID
   - Client Secret
7. Click OK.

   The specified application will be validated with the Azure portal.

   After successful validation, the following application details will be retrieved from the Azure portal and displayed in the page:
   - Tenant Name
   - Tenant ID
   - Application Name
   - Application ID
   - Permissions

   If valid details are not provided, then the status will be displayed as failed.

   If required, you can click Edit Application to make changes to the existing application details or click Test Application to validate the application details with Azure.
8. Click OK.

   The Azure Applications page will be populated with the application details.

2.6.3 Step 3: Configuring Azure AD User Source in ZENworks

After adding an application in ZENworks, perform the following steps in ZENworks to configure the Azure AD user source.

1. In ZENworks Control Center, click **Configurations**.
2. In the **User Sources** panel, click **New**.
3. In the **Create New User Source** page, select **Azure Active Directory**, and click **Next**.
4. In the Select Azure Application page, select the Azure application.
   - Ensure that the application you are selecting is not used by another user source.
   - After selecting the Azure application, the Tenant ID and Tenant Name fields will be displayed.
   - By default, the tenant name will be populated as the User Source Name. If required, you can edit the user source name.

   NOTE: The drop-down displays only the applications for which User Source Application was selected while configuring the application.
5. Click **Next**.
6. In the Summary page, review the displayed information, and then click **Finish**.

   After clicking Finish, ZENworks syncs all users and user groups into ZENworks database.

   To view the sync status, go to Configuration > User Sources panel, and then click the Azure Active Directory user source that was added.

NOTE: Following are some of the important points to remember:

- After successful sync, the Last Sync Details field is updated only if you make any modifications to the group name, or description, or add/remove groups. The fields might not be updated if modifications are made to group members, or if members are added/deleted from the group in the Azure portal.
- Bundles that are assigned to Azure AD groups might not be displayed in the Bundle User assignment dashlet.

2.6.4 Editing Azure Active Directory User Sources

If you are using Azure Active Directory as your user source, then refer to the following steps to edit user sources:

1. In ZENworks Control Center, click the **Configuration** tab.
2. In the User Sources panel, click the underlined link for a user source.
3. In this page, you can modify the settings that were configured while creating the user source:
   - Name: Displays the name of the user source.
   - Directory Type: Displays the directory type.
   - Tenant Name: Displays the name of the tenant.

- Application Name: Displays the name of the application that is used to configure the user source. Application Name is the only setting that can be modified in this page.
  - If more than one application is associated with the tenant, only then the Change Application option will be enabled. Click Change Application to view all the associated applications and select the required application. If only one application is associated with the tenant, then the option will not be displayed.
  - If the application associated with the tenant was removed, then Application Removed is displayed. In such a case, the user sync will not be successful until an application is set. If an application is associated with the tenant, then you will be able to set it using the Set Application option. However, if no application is associated with the tenant, then the option is disabled.
  - To view all the Azure applications added in the zone, click View All Applications.
- Application Status: Displays the status of the application. If the status displays  , then the application might be deleted from the zone.
- User Sync Status: Displays the status of the synchronization between Azure Active Directory and ZENworks.

  NOTE: Groups of type Security will be synced with ZENworks. However, groups of type Microsoft 365 will not be synced with ZENworks.
- Last Sync: Displays the last synchronization time. To trigger the synchronization of users, click Sync Now.

  NOTE: To re-enable the Sync Now option, click the  to refresh the page.
- Last Sync Details: After completing the sync, this field displays the sync details such as the number of users added or modified, and the number of users deleted.

3 Managing User Source Connections

You can use Primary Servers and Satellite devices that have the Authentication role to authenticate users to the ZENworks Management Zone. To improve performance, you can create multiple connections to local replicas of Novell eDirectory or Active Directory trees so that Satellites do not have to authenticate users over a WAN or slow link. Creating connections to local LDAP user sources also provides fault tolerance by providing failover to other user source connection in the event that one connection does not work.

For example, if you use Novell eDirectory in your ZENworks environment, you can use multiple authentication servers in your system so that Satellites with the Authentication role can contact local authentication servers for authentication purposes rather than contacting remote servers.

If a user source connection cannot connect, there is more than a one-minute delay for each subsequent user source connection that is tried. This results from CASA having an internal delay that is not currently configurable.

The following sections contain more information.

3.1 Creating User Source Connections

1. In ZENworks Control Center, click the **Configuration** tab, then click a user source in the User Sources panel.
2. In the Connections panel, click **Add** to launch the Create New Connection Wizard.
3. Fill in the fields:

   Connection Name: Specify a descriptive name for the connection to the LDAP directory.

   Address: Specify the IP address or DNS hostname of the server where the LDAP directory resides.

   Port: This field defaults to the standard SSL port (636) or non-SSL port (389) depending on whether the user source uses SSL. If your LDAP server is listening on a different port, select that port number.

   Add Connection to all Primary Servers: Adds the connection you are creating to all ZENworks Primary Servers in the Management Zone.
4. (Conditional) If the user source uses the Secure Socket Layer (SSL) protocol, click **Next** to display the Certificate page, ensure that the certificate is correct, then click **Next** to advance to the Summary page.

   or

If the user source does not use SSL, click **Next** to advance to the Summary page.

5 Review the information and, if necessary, use the **Back** button to make changes to the information, then click **Finish**.

For more information about configuring Satellites with the Authentication role, see "Understanding the Authentication Role" in the *ZENworks Primary Server and Satellite Reference*.

3.2 Editing User Source Connections

1 In ZENworks Control Center, click the **Configuration** tab, then click a user source in the User Sources panel.

2 In the Connections panel, click the name of a connection to display the Edit Connection Details dialog box.

3 Edit the fields, as necessary:

Connection Name: Displays a descriptive name for the connection to the LDAP directory. You cannot edit this field.

Address: Specify the IP address or DNS hostname of the server where the LDAP directory resides.

Use SSL: Displays **Yes** or **No**, depending on whether the user source uses SSL. You cannot edit this field.

Port: This field defaults to the standard SSL port (636) or non-SSL port (389) depending on whether the user source uses SSL. If your LDAP server is listening on a different port, select that port number.

Certificate: If the user source uses SSL, displays the certificate for the user source. You cannot edit the certificate.

Update: If the user source uses SSL, click the **Update** button to update the certificate, if a new certificate exists.

4 Click **OK**.

3.3 Removing User Source Connections

1 In ZENworks Control Center, click the **Configuration** tab.

2 In the User Sources panel, click the underlined link for a user source.

3 In the Connections panel, select a connection's check box.

4 Click **Remove**.

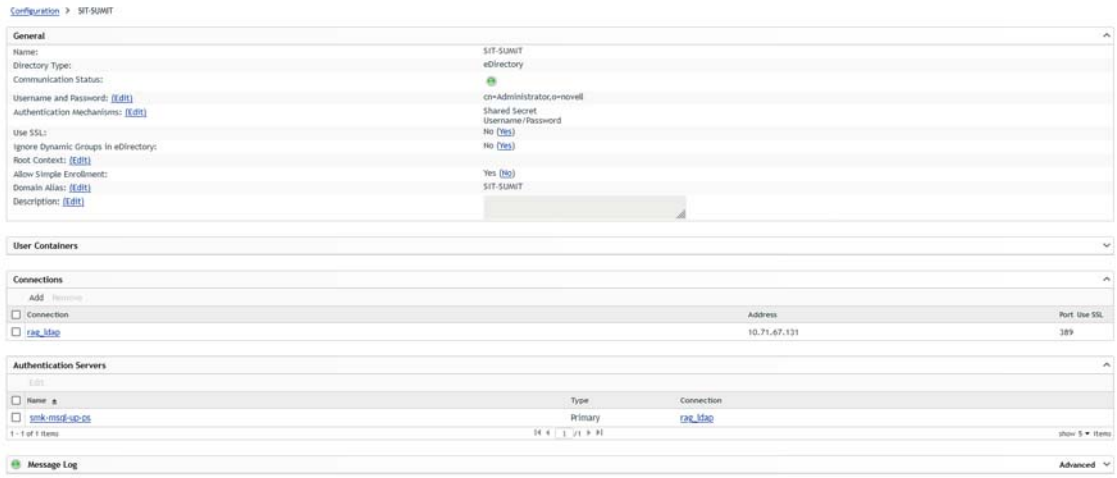
NOTE: When you remove the user source, you need to remove the existing connections and add the new connections.

3.4 Updating a Certificate for a User Source

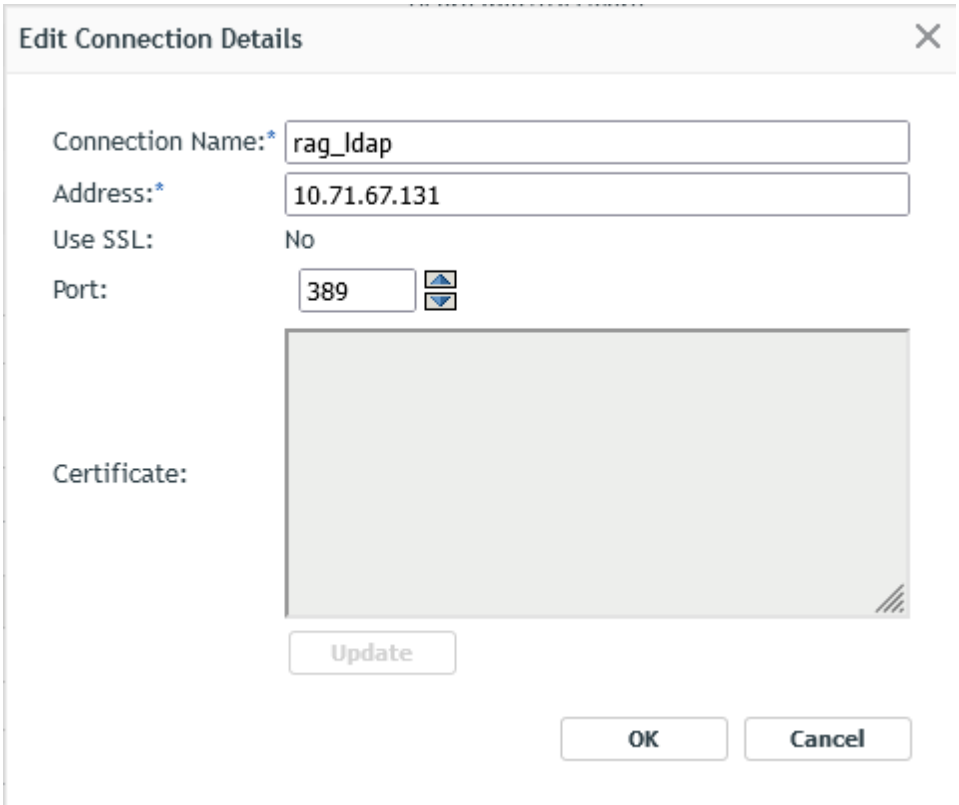
A certificate is used to allow secure communication between devices and user sources. If your certificate expires or you want to change the certificate, you need to update the certificate.

1 In ZENworks Control Center, click the **Configuration** tab.

2 In the User Sources panel, click the user source.



3 In the Connections panel, click a connection to display the Edit Connection Details dialog box.



4 Click **Update**.

4 Managing Primary Server Connections for User Sources

1. In ZENworks Control Center, click the **Configuration** tab.
2. In the Server Hierarchy panel, select the check box next to the Primary Server for which you want to configure authentication connections.
3. Click **Action** > **Configure Primary Authentication Connections**.
4. Select a user source from the drop-down list.
5. (Conditional) To add a user source connection, click Add to display the Add User Source Connections dialog box.
    1. (Optional) In the Connection Name field, specify all or part of the name for the connection to the LDAP directory, then click **Filter** to display the list of connections that match the search criteria.
    2. (Optional) In the Connection Address field, specify part of the IP address or DNS hostname of the connection to the LDAP directory, then click **Filter** to display all connections with that IP address.
    3. Select the check box next to the connection you want to add, then click **OK** to return to the Configure Primary Authentication Connections dialog box.
6. (Conditional) To remove a connection, select a connect, then click **Remove**.
7. (Conditional) To reorder the list of connections, select a connection, then click **Move Up** or **Move Down**.
8. Click **OK**.

5 Managing Authentication Server Connections for User Sources

The Authentication Servers panel on a user source's details page lets you edit authentication server connections, including adding, removing or reordering connections.

The Authentication Servers panel displays information about the user source's ZENworks Primary Servers and Satellite devices that have been configured with the Authentication role. You can also edit the user source settings for each device.

When users logged in to previous versions of ZENworks, they were authenticated to the Management Zone by contacting the ZENworks Primary Server, which in turn contacted the user source that contains the users.

Satellite devices with the Authentication role can now speed the authentication process by spreading the workload among various devices and by performing authentication locally to managed devices. You can have multiple Satellite devices with the Authentication role. In addition, each Satellite with the Authentication role can have multiple user sources configured and each Satellite can have multiple connections to each user source to provide failover.

On the managed device, the Authentication module is inactive until you promote the managed device to be a Satellite with the Authentication role or until the Authentication role is added to an existing Satellite.

The following sections contain more information:

5.1 Assigning a Connection to an Authentication Server

1. In ZENworks Control Center, click the **Configuration** tab.
2. In the User Sources panel, click the name of a user source to display its details.
3. In the Authentication Servers panel, select the check box next to the server's name, then click **Edit** to display the Edit Authentication Server Connections dialog box.
4. Click **Add** to display the Add User Source Connections dialog box.

   By default, the **Add** link is disabled because all connections to the user source display. If a connection is removed, the **Add** link is enabled.
5. (Optional) Use the **Connection Name** field to filter the list of connections.

   Specify all or part of the name for the connection to the LDAP directory, then click **Filter** to display the list of connections that match the criteria.

If you have many connections in your ZENworks Management Zone, you can use the **Connection Name** field to display only those connections that match the criteria. For example, to display all connections that contain the word “London,” type London in the **Connection Name** field, then click **Filter**.

6 (Optional) Use the **Connection Address** field to filter the list of connections.

Specify part of the IP address or DNS hostname of the connection to the LDAP directory, then click **Filter** to display all connections with that IP address.

If you have many connections in your ZENworks Management Zone, you can use the **Connection Address** field to display only those connections that match the criteria. For example, to search for and display all connections that have an IP address starting with 172, type 172 in the **Connection Address** field, then click **Filter**.

7 In the User Source Connections list, select the check box next to the desired connection.

8 Click **OK**.

5.2 Removing a Connection

1 In ZENworks Control Center, click the **Configuration** tab.

2 In the User Sources panel, click the name of a user source to display its details.

3 In the Authentication Servers panel, select the check box next to the server’s name, then click **Edit** to display the Edit Authentication Server Connections dialog box.

4 In the User Source Connections list, select the check box next to the desired connection, then click **Remove**.

5 Click **OK**.

5.3 Reordering Connections

1 In ZENworks Control Center, click the **Configuration** tab.

2 In the User Sources panel, click the name of a user source to display its details.

3 In the Authentication Servers panel, select the check box next to the server’s name, then click **Edit** to display the Edit Authentication Server Connections dialog box.

4 In the User Source Connections list, select the check box next to the desired connection, then click **Move Up** or **Move Down**.

The authentication server uses the connections in the order they are listed to authenticate the device to the ZENworks Management Zone.

5 Click **OK**.

6 Providing LDAP Load Balancing and Fault Tolerance

If you have multiple LDAP servers for access to your user source (directory), you can configure your ZENworks Servers to recognize each of the LDAP servers. This provides both load balancing and fault tolerance.

For example, if you have multiple ZENworks Servers, you can configure each one to access the user source through a different LDAP server. This distributes the workload more evenly among the LDAP servers.

Likewise, for each ZENworks Server, you can list multiple LDAP servers through which it can connect to the user source. If one of the LDAP servers becomes unavailable, the ZENworks Server uses another LDAP server.

In versions prior to ZENworks 11 SP3, you need to specify the additional LDAP servers for a ZENworks Server in the `alt-servers.properties` configuration file located in the following directory on the ZENworks Server:

- Windows: `c:\program files\novell\zenworks\conf\datamodel\authsource`
- Linux: `/etc/opt/novell/zenworks/datamodel/authsource`

However, you can now specify additional LDAP servers by using ZENworks Control Center or the zman command line utility.

- Section 6.1, “Using ZENworks Control Center to Define Additional LDAP Servers for a ZENworks Server,” on page 31
- Section 6.2, “Using the zman Command Line Utility to Define Additional LDAP Servers for a ZENworks Server,” on page 32

6.1 Using ZENworks Control Center to Define Additional LDAP Servers for a ZENworks Server

1. In ZENworks Control Center, click the **Configuration** tab, then click a user source in the User Sources panel.
2. In the Connections panel, click **Add** to launch the Create New Connection Wizard.
3. Fill in the fields:

   Connection Name: Specify a descriptive name for the connection to the LDAP directory.

   Address: Specify the IP address or DNS hostname of the server where the LDAP directory resides.

   Port: This field defaults to the standard SSL port (636) or non-SSL port (389), depending on whether the user source uses SSL. If your LDAP server is listening on a different port, select that port number.

Add Connection to all Primary Servers: Adds the connection you are creating to all ZENworks Primary Servers in the Management Zone.

4 (Conditional) If the user source uses the Secure Socket Layer (SSL) protocol, click **Next** to display the Certificate page, ensure that the certificate is correct, then click **Next** to advance to the Summary page.

or

If the user source does not use SSL, click **Next** to advance to the Summary page.

5 Review the information and, if necessary, use the **Back** button to make changes to the information, then click **Finish**.

6.2 Using the zman Command Line Utility to Define Additional LDAP Servers for a ZENworks Server

To define additional LDAP servers for a ZENworks Server, run the `user-source-add-connection (usac)` command on the server. For more information on using the zman command, see "User Commands" in the *ZENworks Command Line Utilities Reference*.

7 User Source Authentication

By default, a user is automatically authenticated to the Management Zone when he or she logs in to an LDAP directory (Novell eDirectory or Microsoft Active Directory) that has been defined as a user source in the Management Zone. User authentication to ZENworks can occur only if the user's LDAP directory (or the user's LDAP directory context) is defined as a user source in ZENworks.

The ZENworks Agent integrates with the Windows Login or ZENworks Login client to provide a single login experience for users. When users enter their eDirectory or Active Directory credentials in the Windows or Novell client, they are logged in to the Management Zone if the credentials match the ones in a ZENworks user source. Otherwise, a separate ZENworks login screen prompts the user for the correct credentials.

For example, assume that a user has accounts in two eDirectory trees: Tree1 and Tree2. Tree1 is defined as a user source in the Management Zone, but Tree2 is not. If the user logs in to Tree1, he or she is automatically logged in to the Management Zone. However, if the user logs in to Tree2, the ZENworks Agent login screen appears and prompts the user for the Tree1 credentials.

Review the following sections:

Enabling Seamless Authentication on a Device

The first time a user logs in to a device that has more than one user source enabled, the user is prompted to select the user source and specify the user source credentials. During subsequent logins, the user is automatically logged in to the user source selected during the first login. However, if you do not want the user to be prompted to select the user source during the first login, perform the following steps to enable seamless login on the device:

1. Open the Registry Editor.
2. Go to `HKLM/Software/Novell/ZCM/ZenLgn/`.
3. Create a DWORD called EnableSeamlessLogin and set the value to 1.

If seamless login is enabled, a user's first login to a device might be slow. This is because all the existing user sources are searched and the user is logged in to the first user source that matches the user account. If many users use the same device, subsequent logins might also be slow because the user information might not be cached on the device.

Reducing Device Login Time by Specifying the Default User Source

To reduce the login time, specify the default user source for the user to seamlessly log in to the device:

1. Open the Registry Editor.
2. Go to HKLM/Software/Novell/ZCM/ZenLgn/.
3. Create a String called DefaultRealm and set its value to the desired user source. The DefaultRealm value is case sensitive since the realm name is case sensitive.

   For example, if all the users should log in to a user source named POLICY-TREE, create a String called DefaultRealm and set its value to POLICY-TREE.

If the login to the specified default user source fails, the other existing user sources are searched, then the user is logged in to the user source that matches the user account.

For successive logins, the cached user source takes precedence over the DefaultRealm setting. If you want to change the DefaultRealm setting and want it to take precedence over other user sources:

1. Open the Registry Editor
2. Go to HKLM/Software/Novell/ZCM/ZenLgn/History
3. Delete CachedUserZenNames and RealmName registry keys.

NOTE

- The DefaultRealm setting applies only if the EnableSeamlessLogin setting is enabled.
- The DefaultRealm registry key does not work if you log in by using the ZENworks icon on to a Windows 7 device with UAC enabled.

Disabling the Login Status Messages Display on the Device Screen

During the process of logging in to ZENworks, the user can view the status of the login. By default, the login messages are displayed on the screen.

To disable the login messages:

On a Windows XP, Windows 2000, or Windows Server 2003 device:

1. Open the Registry Editor.
2. Go to HKLM\Software\Novell\NWGINA.
3. Create a DWORD called EnableStatusMessages and set its value to 0.

On a Windows 7, Windows Vista, or Windows Server 2008 device:

1. Open the Registry Editor.
2. Go to HKLM\Software\Novell\Authentication.
3. Create a DWORD called EnableStatusMessages and set its value to 0.

Identifying the LDAP Directory That the User Has Logged In To

If the Novell Client is installed on a device, the HKLM\Software\Novell\ZCM\ZenLgn registry key that has DWORDS, DomainLogin and eDIRLogin is added by default on the device. The value of DomainLogin and eDIRLogin helps you identify whether a logged-in user has logged into Novell eDirectory or Microsoft Active Directory.

For example:

- If DomainLogin is set to 1, the user has logged in to Microsoft Active Directory.
- If eDIRLogin is set to 1, the user has logged in to Novell eDirectory.
- If both DomainLogin and eDIRLogin are set to 1, the user has logged in to both Microsoft Active Directory and Novell eDirectory.

This login information might be useful in the following scenarios:

Scenario 1: If a user has logged in to Microsoft Active Directory, a DLU policy does not need to be enforced on a device. Even if you choose to enforce a DLU policy on the device, the policy is not effective on the device. Consequently, you can add a system requirement that the DLU policy must be effective on the device only when the user has logged in to Novell eDirectory.

Scenario 2: If a user has not logged in to Novell eDirectory, any bundle that must access content from a Netware shared location fails. Consequently, you can add a system requirement that the bundle must be effective on the device only when the user has logged in to Novell eDirectory.

Logging Directly in to a Workstation That has Both Novell Client and ZENworks Agent Installed

If you log into a device that has both Novell Client and ZENworks Agent installed, you are automatically logged in to ZENworks eDirectory, even if you have chosen to log in to the workstation only.

In the Novell Client dialog box, if you choose to log in to workstation only, then you must perform the following steps on the managed device to directly log in to the workstation:

On Windows XP device:

1. Open the Registry Editor.
2. Go to HKLM\Software\Novell\ZCM\ZenLgn\.
3. Create a DWORD called HonorClient32WorkstationOnlyCheckbox and set its value to 1.

On Windows Vista/Windows 7/Windows 8 device:

1. Open the Registry Editor.
2. Go to HKLM\Software\Novell\ZCM.
3. Create a DWORD called HonorWorkstationOnlyLogin and set its value to 1.

Authenticating in to a ZENworks Server That Has Novell SecretStore Configured

If you choose to log into a ZENworks Server that has Novell SecretStore configured, perform the following steps on the managed device:

1. Open the Registry Editor.
2. Go to `HKLM/Software/Novell/ZCM/ZenLgn/`.
3. Create a DWORD called EnableSecretStore and set its value to 1. However, if the DWORD already exists, then ensure that its value is set to 1.

Enabling SecretStore on the device might increase the time to authenticate to the ZENworks Server, depending on the number of eDirectory servers that have been added to the Management Zone. For more information on SecretStore operations, see TID 10091039 in the Technical Support Knowledgebase (http://support.novell.com/search/kb_index.jsp).

Authenticating in to a ZENworks Managed Device in a VDI environment

1. Refresh the ZENworks managed device on the master image of the VDI environment.
2. Right-click the ZENworks icon and ensure that the Login option is listed in the menu. You might have to refresh the device until the Login option is listed in the menu.
3. Create the master image. For more information, see the "Agent Deployment in VDI environment" in the*ZENworks Discovery, Deployment, and Retirement Reference* Guide.
4. Shutdown the master image device.
5. The master image of the VDI environment with ZENworks agent is ready. You can use the master image to create multiple virtual machine (VM) images. For information on how to create the VM images, refer to the vendor-specific documentation.
6. Start the VM image.
7. Log in to the VM by specifying the correct credentials.

Enabling debug logging on the micasad SecretStore

1. Use a text editor to create a file named `micasad.exe.config` with the following content:

```
<configuration>
 <system.diagnostics>
   <switches>
     <add name="TraceLevelSwitch" value="4" />
   </switches>
    <trace autoflush="true" indentsize="4">
     <listeners>
        <add name="myListener"
type="System.Diagnostics.TextWriterTraceListener"
initializeData="c:\logs\micasad.log" />
     </listeners>
    </trace>
```

```
    </system.diagnostics>
</configuration>
```

2 (Optional) Edit the value of `TraceLevelSwitch`. to change the log level.

3 (Optional) Edit the value of `initializeData` to change the log level.

4 Save `micasad.exe.config` in the same location where `micasad.exe` file is saved. By default, `micasad.exe` is saved in the following locations:

- **On 32-bit device:** *`Windows_Install_Drive`*`:\Program Files\Novell\CASA\bin`
- **On 64-bit device:** *`Windows_Install_Drive`*`:\Program Files (x86)\Novell\CASA\bin`

Using Domain Alias to Authenticate Users

The **Domain Alias** setting is meant for authenticating mobile device users only. Using these alternate domain alias names, workstation users will fail to authenticate to ZENworks, unless the Kerberos mechanism for authentication is enabled. For more information on the Kerberos authentication mechanism, see Kerberos (Active Directory or Domain Services for Windows). For more information on editing the Domain Alias setting for mobile devices, see Enabling a User Source for Mobile Device Enrollment.

For information on the various authentication mechanisms, credential storage, and disabling user authentication, review the following sections:

- Section 7.1, “Authentication Mechanisms,” on page 37
- Section 7.2, “Credential Storage,” on page 48
- Section 7.3, “Network Credential Manager,” on page 49
- Section 7.4, “Disabling ZENworks User Authentication,” on page 49
- Section 7.5, “Using a DLU in a Domain Environment,” on page 50
- Section 7.6, “Configuring Attribute for ActiveSync Server Authentication,” on page 50

7.1 Authentication Mechanisms

The following mechanisms can be used to authenticate managed devices to the ZENworks Management Zone:

- Section 7.1.1, “Kerberos (Active Directory or Domain Services for Windows),” on page 37
- Section 7.1.2, “Shared Secret,” on page 45
- Section 7.1.3, “Username/Password (eDirectory, Active Directory, Domain Service for Windows),” on page 47

7.1.1 Kerberos (Active Directory or Domain Services for Windows)

Kerberos, an authentication protocol developed at MIT, requires entities (for example, a user and a network service) that need to communicate over an insecure network to prove their identity to one another so that secure authentication can take place.

Kerberos functionality is included natively in a Windows Active Directory environment.

Kerberos requires the use of a Key Distribution Center (KDC) to act as a trusted third party between these entities. All Kerberos server machines need a keytab file to authenticate to the Key Distribution Center (KDC). The keytab file is an encrypted, local, on-disk copy of the host's key.

IMPORTANT: When attempting Kerberos authentication using smart card, ZENworks login process is attempted through ZENworks Credential Manager. Hence, the following capabilities are not available:

- Dynamic Local User
- Windows Roaming Profile Policies
- Windows Group Policies

When using Kerberos authentication, the Active Directory server generates a Kerberos ticket that Novell Common Authentication Services Adapter (CASA) uses to authenticate the user, rather than using a username and password for authentication.

- "Setting Up Kerberos in your ZENworks Environment" on page 38
- "Enabling Kerberos Authentication While Adding a User Source" on page 39
- "Enabling Kerberos Authentication on an Existing User Source" on page 39
- "Understanding How Kerberos Authentication and the ZENworks Login Dialog Box Interact" on page 39
- "Configuring ZENworks for Performing Kerberos Authentication with Domain Services for Windows (DSfW) Server" on page 40

Setting Up Kerberos in your ZENworks Environment

IMPORTANT: If the Active Directory or Domain Services for Windows user source is configured to use only Kerberos authentication mechanism, ensure that the managed device is added to the user source domain.

---

1. Create a new user account and set it as the Kerberos service principal account using the following command on the domain controller:

   For example, if you created a user called atsserver in your domain, you would run the following command from the command prompt

   ```
   setspn -A HOST/atsserver.myserver.com atsserver
   ```

2. Generate a keytab file for that account.

   Microsoft recommends that you use the `crypto` option. Before generating the key tab file for the ZENworks server, you need to enable the `crypto` key for the key tab user in the account settings.

   For more information, see the Microsoft TechNet Web site (https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ktpass).

   For example, since the user account atsserver is set as the service principal account, you would run the following command from the command prompt:

   ```
   ktpass /princ HOST/atsserver.myserver.com@MYSERVER.COM -pass
   atsserver_password -mapuser domain\atsserver -out atsserver.keytab -
   mapOp set -ptype KRB5_NT_PRINCIPAL
   ```

This command creates a keytab file and modifies the user atsserver to be a Kerberos principal. However, if the keytab, generated using the above mentioned command, does not work, then run the following command:

```
ktpass /princ atsserver/myserver.com@MYSERVER.COM -pass
atsserver_password -mapuser domain\atsserver -out atsserver.keytab -
mapOp set -ptype KRB5_NT_PRINCIPAL
```

3 Import the keytab file into ZENworks Control Center.

3a In ZENworks Control Center, click the **Configuration** tab, click **Infrastructure Management**, then click **User Source Settings**.

3b Click  to browse to and select the keytab file.

3c Click OK to import the file.

4 Restart the ZENserver service.

NOTE: Kerberos cannot be configured for Active Directory with multiple domains, since this would require multiple keytab files and ZENworks only supports a single keytab file.

Enabling Kerberos Authentication While Adding a User Source

You can enable Kerberos authentication while adding a user source. For more information see Section 2.1, “Adding User Sources,” on page 9.

Enabling Kerberos Authentication on an Existing User Source

You can enable Kerberos authentication on an existing user source.

1 In ZENworks Control Center, click the **Configuration** tab.

2 In the User Sources panel, click the user source, then click **Edit** next to **Authentication Mechanisms** in the General section.

3 Select the **Kerberos** check box, then click **OK**.

Understanding How Kerberos Authentication and the ZENworks Login Dialog Box Interact

The following table illustrates the ZENworks user experience using Kerberos authentication with Active Directory:

Table 7-1 *ZENworks Kerberos Authentication with Active Directory*

Windows login matches user source login?	ZENworks also uses Username/ Password authentication ?	Member of same domain?	Member of different domain?	Windows and ZENworks credentials match?	Can log in to Management Zone?	ZENworks login dialog box appears?
✓	✓	✓		✓	Yes	No

Windows login matches user source login?	ZENworks also uses Username/ Password authentication ?	Member of same domain?	Member of different domain?	Windows and ZENworks credentials match?	Can log in to Management Zone?	ZENworks login dialog box appears?
✓		✓		✓	Yes	No
	✓		✓		Yes	Yes
			✓		No	No
			✓	✓	No	No
					No	No
				✓	No	No
✓	✓			✓	Yes	No
	✓		✓	✓	Yes	No
	✓				Yes	Yes

For example, in the second row, the user's initial login, user source, and ZENworks login credentials match. As a result, the user can log in to the ZENworks Management Zone and the ZENworks login dialog box does not appear.

As another example, in the third row, the user's initial login credentials are using credentials from a different domain and are different than the ZENworks login credentials. As a result, the user can log in to the ZENworks Management Zone, but the ZENworks login dialog box appears.

Configuring ZENworks for Performing Kerberos Authentication with Domain Services for Windows (DSfW) Server

This section provides information about the tasks that need to be performed on DSfW and ZENworks Servers to configure Kerberos authentication for ZENworks login. It also includes information about additional settings and workarounds that need to be performed on the DSfW Server to ensure smooth Kerberos authentication for all users.

Pre-requisites

- Ensure that the installation and configuration of the DSfW Server is done on the OES machine. For detailed information, see (http://www.novell.com/documentation/oes11/acc_dsfw_lx/?page=/documentation/oes11/acc_dsfw_lx/data/bookinfo.html#bookinfo).
- Verify the functionality of the DSfW Server. For more information refer to TID 7001884 in the Technical Support Knowledgebase (http://www.novell.com/support/viewContent.do?externalId=7001884).
- Verify and test the features provided in this document, by using:
  - ZENworks Server : ZEN . server
  - OES 11 Server : DSfW services installed and configured

- Windows Workstation : Windows XP SP3
- Windows Support Tools : 5.2.*x*

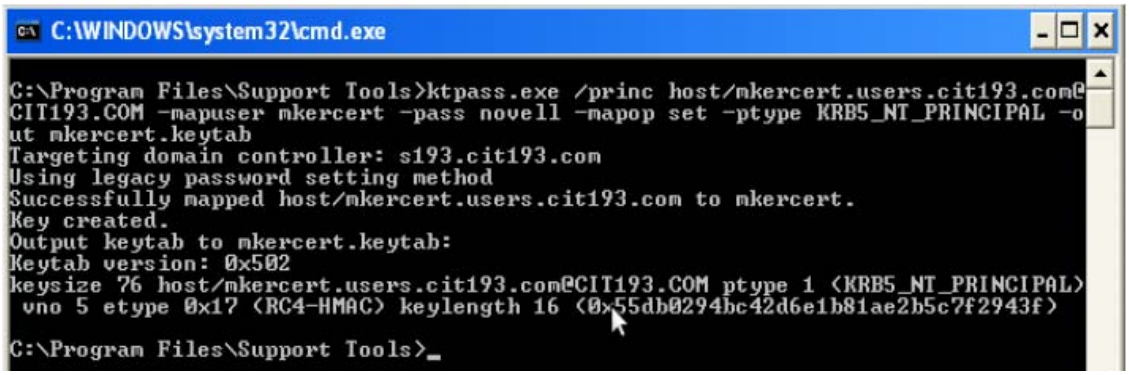
Configuring DSfW Server and Windows Workstation

For example, you can use the credentials provided below to configure the DSfW Server and Windows Workstation.

- Domain name : cit193.com
- User name for creating key tab file : mcertuser
- Users for verifying the setup : muser1, muser2

To configure DSfW Server and Windows Workstation, you need to first add the Windows Workstation to the DSfW domain:

1. Add the DSfW Server as the DNS Server.
2. Select My Computer > Properties, then change the domain for the workstation to the DSfW server's domain.
3. Provide the required credentials to add the workstation to the domain.
4. Restart the client.
5. Install Admin tools and Support tools on the client machine.
6. These tools facilitate the DSfW Server management to create the keytab file. You can find the download details at (http://www.microsoft.com/download/en/details.aspx?id=6315).
7. Install the ZENworks client on the same client by downloading the appropriate ZENworks client set-up from the *http://<ZEN server>/zenworks-setup* server.
8. Create a user in DSfW server by using Microsoft Management Console (MMC), which can be associated to the DSfW service by creating a keytab file. In this case, the user for creating the keytab file is `mcertuser`. The expected result is as shown in figure below.



ZENworks Server Configuration

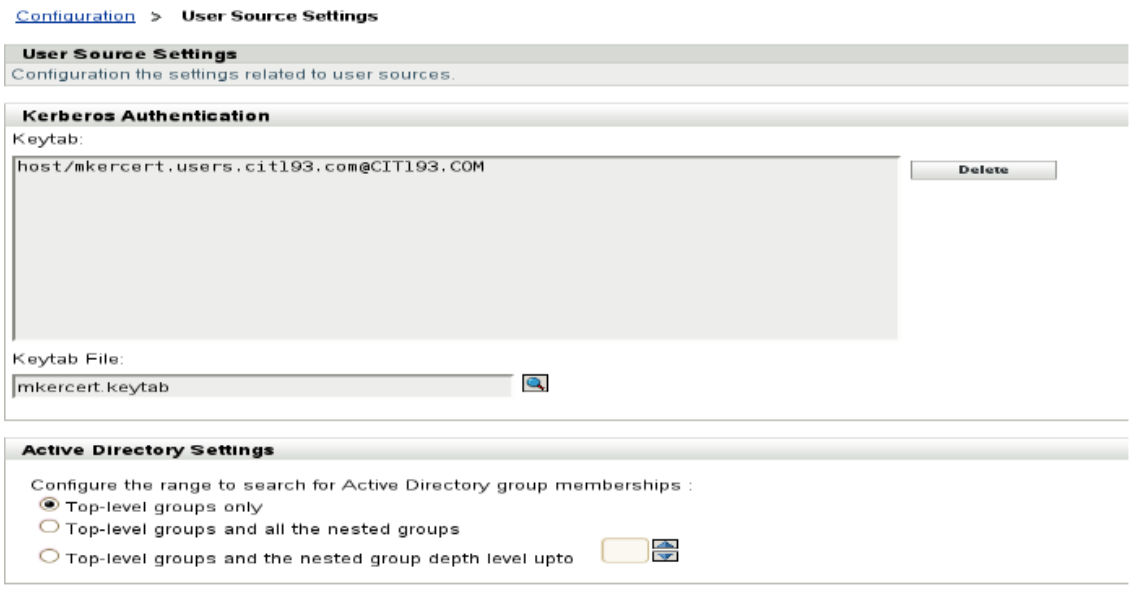
Adding DSfW as a User Source in ZENworks

To add a user source and choose Kerberos as the authentication mechanism, see (http://www.novell.com/documentation/zenworks11/zen11_system_admin/?page=/documentation/zenworks11/zen11_system_admin/data/bafywtr.html).

To verify the result, click the user source enabled with Kerberos.

Adding a Kerberos Keytab file

1. Log in to ZENworks Control Center.
2. In **Infrastructure Management**, select **Configuration** > **User Source Settings**.
3. Add the Kerberos keytab file. After the keytab file is you can view the details as shown in the figure.



Kerberos Authentication for Windows Workstation

To verify the settings and to ensure the working of Kerberos authentication on the client machine, login to Windows as any user. For example, you can log in as either muser1 or muser2 created using MMC.

The same login credentials are passed on to the ZENworks client and login happens seamlessly to the Windows workstation with the same user.

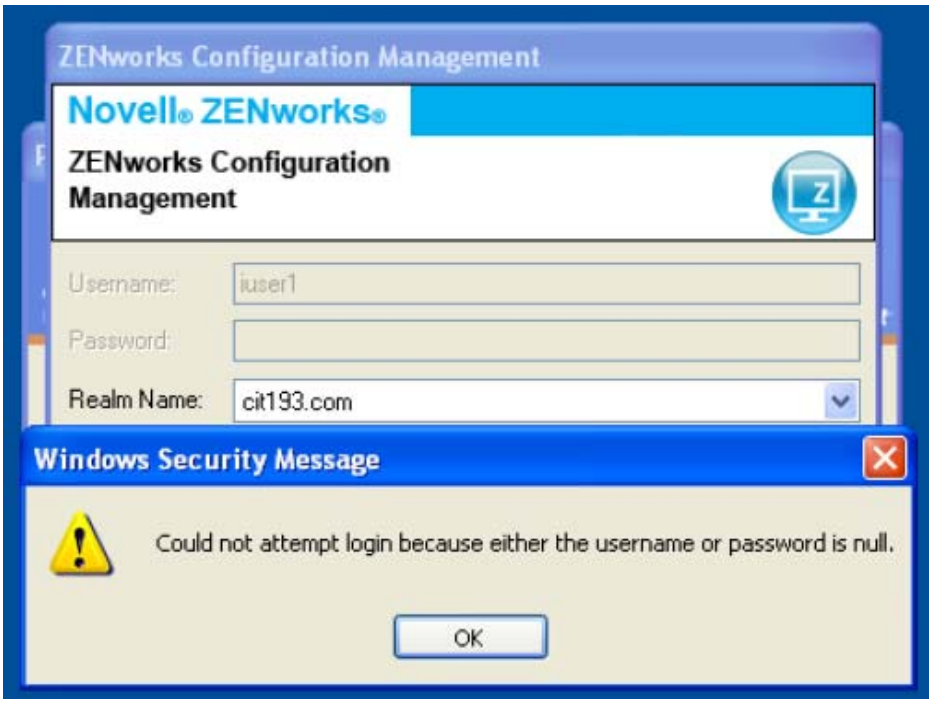
NOTE

- The user used for creating the keytab file cannot login using ZENworks client as this user is associated with a Service Principal Name (SPN) rather than a User Principal Name (UPN).
- The UPN attribute is mandatory for a successful ZENworks Configuration Management and DSfW integration. The UPN attribute is created when the user is created by using the MMC.
- In case of ConsoleOne and iManager tools, the user created will not have the UPN attribute.
- While logging into ZENworks application (ZAPP) by using the ZENworks icon in the system tray, do not append the domain name (@xyz.com) with the username, if the UPN attribute is used.

Troubleshooting Tips

Issue: A user created by using iManager cannot login seamlessly using the ZENworks client.

The login fails with the error message "`Could not attempt login because either username or password is null`" as shown in the figure.

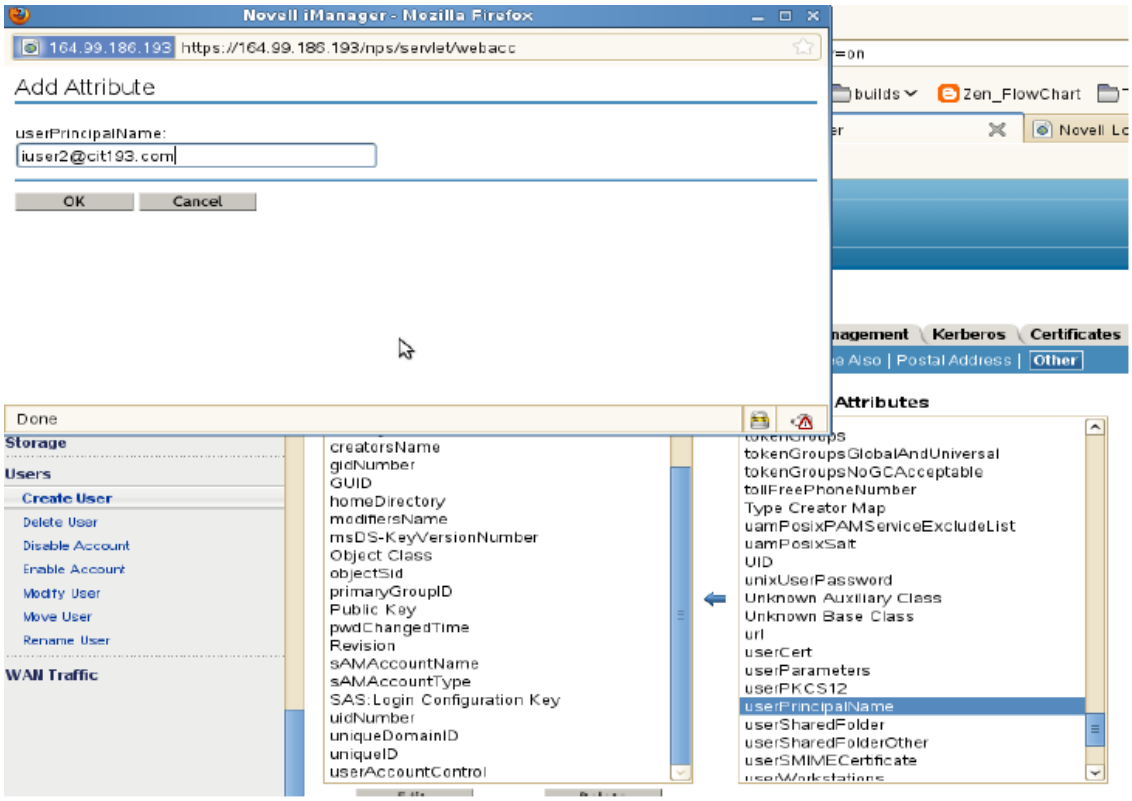


Possible Cause 1: The User Principal Name (UPN) attribute is not set for the users created using iManager.

Workaround: Set the UPN attribute by selecting the user to be supported for Kerberos authentication.

To set the UPN attribute:

1. Log in to iManager.
2. Select **Directory Administration** > **Modify object.** Also, set this attribute in the **Others** tab as shown in the figure.



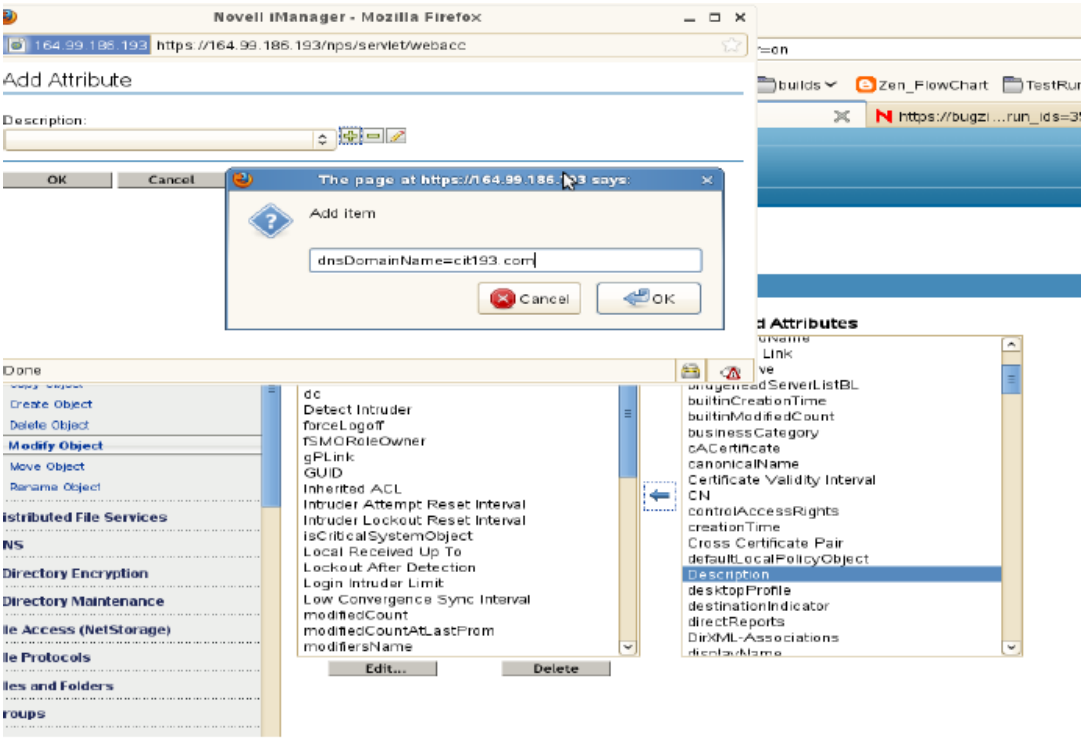
Possible Cause 2: The dnsDomainName attribute is not set at the root level in the DSfW domain.

Workaround: Set the dnsDomainName attribute at the root level of the DSfW domain so that reflects at the user's level.

To set the dnsDomainName attribute:

1. Log in to iManager and select the domain root object. For example you can select cit193.com.
2. Modify the object and add the **Description** field.
3. Add the attribute dnsDomainName=cit193.com.
4. Restart the ndsd (Novell Directory) services on the DSfW server.

   The existing user once modified and any user objects that you create in future will automatically gets the UserPrincipalName attribute. For more information, see TID 7009221 from the Technical Support Knowledgebase (http://www.novell.com/support/documentLink.do?externalID=7009221).



Useful Links

- For enabling CASA logs, see (http://www.novell.com/support/viewContent.do?externalId=3418069)
- For setting the DNS domain name attribute, see (http://www.novell.com/support/documentLink.do?externalID=7009221).
- For verifying the functionality of the DSfW server, see (http://www.novell.com/support/viewContent.do?externalId=7001884).

7.1.2 Shared Secret

When using Shared Secret authentication, you must install and configure the Novell Identity Assurance Solution Client. For more information, and for a list of supported smart card readers and smart cards, see the Identity Assurance Solution Client documentation on the Documentation Web site (http://www.novell.com/documentation/).

When a user uses a smart card to log in to eDirectory, the user is automatically logged in to ZENworks provided the schema of the eDirectory specified when the user source is added has been extended using microfocus-zenworks-configure tool.

Logging in to a workstation with a smart card in the network disconnected mode by selecting the Computer Only Logon option and by using the NMAS for Windows logon method allows local workstation user to login, but the ZENworks user login fails.

For more information on adding the user source, see Section 2.1, “Adding User Sources,” on page 9.

For more information on extending the eDirectory schema, see “Extending the eDirectory Schema to enable Shared Secret Authentication” on page 46.

If the eDirectory schema is not extended, then **Shared Secret** is not available as an authentication mechanism. Consequently, a ZENworks login dialog box is displayed when the user on the managed device attempts to log in to eDirectory using a smart card. After the user specifies the eDirectory username and password, that password is stored in Novell SecretStore. The next time the user uses a smart card to log in to eDirectory, the password is retrieved from SecretStore and the user is logged in to the ZENworks without having to specify the password.

Extending the eDirectory Schema to enable Shared Secret Authentication

To authenticate in to ZENworks by using Shared Secret authentication mechanism, the schema of the eDirectory specified when the user source is added must have been extended using microfocus-zenworks-configure tool.

Perform the following steps to extend the eDirectory schema:

1. Run the microfocus-zenworks-configure utility on a ZENworks Server:

   On Windows: At the command prompt, change to `ZENworks_installation_path\bin` and enter the following command:

   ```
   microfocus-zenworks-configure.bat -c ExtendSchemaForSmartCard
   ```

   On Linux: At the console prompt, change to `/opt/microfocus/zenworks/bin` and enter the following command:

   ```
   ./microfocus-zenworks-configure -c ExtendSchemaForSmartCard
   ```

2. You are prompted to continue with the action of extending the Novell eDirectory schema and adding an optional zcmSharedSecret attribute to the user class. By default, 1 is selected. Press Enter.
3. Enter the DNS name or IP address of the Novell eDirectory server to extend the schema.
4. You are prompted to select Secure Socket Layer (SSL) or Clear Text communication for communicating with the eDirectory server. Enter 1 for SSL communication or 2 for Clear Text Communication, then press **Enter** again.
5. Enter the port for communicating with the eDirectory server.

   The default port for SSL communication is 636 and for Clear Text communication is 389.
6. Enter the fully distinguished name (FDN) of the Administrative User.

   For example, cn=admin,o=organization
7. Enter the password for the Administrative User specified in Step 6.
8. (Optional) Enter the fully distinguished name for the ZENworks user source admin for whom the ACL would be applied.

   The ZENworks user source admin is configured as a user in the ZENworks user source configuration for reading users from the user source and need not be the Administrative User specified in Step 6. If you specify the fully distinguished name of this user, the program sets ACLs at the specified containers to provide read access to zcmSharedSecret attribute for this user.
9. Enter the user containers for which you want to extend the schema.

   Multiple containers can be given separated by + sign. For example, o=sales or o=sales + o=marketing.

10 Press **Enter** to generate random secret for all the users within the above containers.

11 (Conditional) If you have chosen SSL communication for communicating with the eDirectory server, the server presents a certificate. Enter **y** to accept the certificate.

7.1.3 Username/Password (eDirectory, Active Directory, Domain Service for Windows)

When using Username/Password authentication with a Novell eDirectory, Microsoft Active Directory, or Domain Service for Windows user source, if the credentials the user specifies to log in to the workstation or to the domain match the ZENworks login credentials, the ZENworks login dialog box does not display and the user is authenticated to the ZENworks Management Zone.

The username and password are also stored in Secret Store. If a user later logs in to ZENworks where no username or password is available (for example, the user logged in using a smart card), the stored credentials are used and the ZENworks login dialog box is bypassed.

Enabling Username/Password Authentication While Adding a User Source

You can enable Username/Password authentication while adding a user source. For more information see Section 2.1, “Adding User Sources,” on page 9.

Enabling Username/Password Authentication on an Existing User Source

You can enable Username/Password authentication on an existing user source.

1 In ZENworks Control Center, click the **Configuration** tab, click the user source, then click **Edit** next to **Authentication Mechanisms** in the General section.

2 In the User Sources panel, click the user source, then click **Edit** next to **Authentication Mechanisms** in the General section.

3 Select the **Username/Password** check box, then click **OK**.

Understanding How Username/Password Authentication and the ZENworks Login Dialog Box Interact

The following table illustrates the ZENworks user experience using Username/Password authentication with Active Directory:

Table 7-2 *ZENworks Username/Password Authentication with Active Directory*

Windows login matches user source login?	ZENworks also uses Kerberos authentication ?	Member of same domain?	Member of different domain?	Windows and ZENworks credentials match?	Can log in to Management Zone?	ZENworks login dialog box appears?
✓	✓			✓	Yes	No

Windows login matches user source login?	ZENworks also uses Kerberos authentication ?	Member of same domain?	Member of different domain?	Windows and ZENworks credentials match?	Can log in to Management Zone?	ZENworks login dialog box appears?
	✓		✓	✓	Yes	No
	✓				Yes	Yes
✓		✓		✓	Yes	No
			✓	✓	Yes	No
				✓	Yes	No
					Yes	Yes
✓		✓			Yes	Yes
✓			✓		Yes	Yes

For example, in the first row, the user's initial login, user source, and ZENworks login credentials match. As a result, the user can log in to the ZENworks Management Zone and the ZENworks login dialog box does not appear.

As another example, in the second row, the user's initial login credentials are using credentials from a different domain but match the ZENworks login credentials. As a result, the user can log in to the ZENworks Management Zone, and the ZENworks login dialog box does not appear.

7.2 Credential Storage

ZENworks uses Novell CASA (Common Authentication Services Adapter) to enable single sign-on. When the ZENworks Agent authenticates a user to the Management Zone via the credentials entered in the Microsoft client, Novell client, or ZENworks login screen, the username and password is stored in the secure CASA vault on the user's device.

CASA is installed with the ZENworks Agent. It includes the CASA Manager, which is an interface used to manage the credentials in the storage vault. The CASA Manager is available from the **Start** > **Program Files** > **Novell CASA** menu. Generally, you or the device's user should not need to use the CASA Manager. When a user's credentials change in the LDAP directory, they are updated in the CASA storage vault the next time the user logs in. If you run the CASA Manager, you are prompted to install the GTK# Library. If you choose to install the library (which is necessary to run the CASA Manager), you are directed to a Novell Web site. However, the GTK# Library is currently unavailable at this site. You can choose to install the GTK# Library by downloading and installing the `gtksharp-runtime-2.8.3-win32-0.0.exe` file from the Google Code (https://code.google.com/archive/p/casa-auth/) site.

The newly added CASA storage component handles the credential storage by default. For information about disabling newly added CASA storage, see EnableTraditionalCasa in the ZENworks Registry Keys Reference.

Do not remove CASA from the managed device. If you do not want the CASA Manager displayed to users, you can remove the Novell CASA folder from the **Start** > **Program Files** menu.

7.3 Network Credential Manager

ZENworks AgentZENworks Agent includes a Network Credential Manager that supplements ZENworks Credential Provider wrapper. Network Credential Manager facilitates passive mode authentication when users login with any third party credential provider.

Network Credential Manager works with many third party credential providers including Citrix XenDesktop and VMware View credential providers.

When you use an alternate credential provider, the login process is owned by this credential provider and Windows notifies the ZENworks Credential Manager of the user's credentials. So, the following capabilities are not available while using a third party credential manager:

- Dynamic Local User
- Windows Roaming Profile Policies
- Windows Group Policies

NOTE: It is recommended that the Network Credential Manager is used in Windows Active Directory or Domain services.

7.4 Disabling ZENworks User Authentication

By default, if a user source is defined in the ZENworks Management Zone, the ZENworks Agent attempts to authenticate a user to the zone whenever he or she logs in through the Microsoft or Novell client.

If necessary, you can disable user authentication to the zone. For example, you might have some users that only receive device-assigned content, so you don't want the overhead of having them logged in to the zone.

To disable user authentication to the zone:

1. Locate the following key in the registry on the user's device:

   `HKLM\SOFTWARE\Novell\ZCM\ZenLgn`

2. (Conditional) If you want to disable login, add the following DWORD value:

   Value name: DisablePassiveModeLogin

   Value data: Any non-zero value (for example, 1, 2, 3, 100)

   With login disabled, no attempt is made to authenticate to the Management Zone when the user logs in through the Microsoft or Novell client.

3. (Conditional) If you want to disable the ZENworks login prompt that appears if login through the Microsoft client or Novell client fails, add the following DWORD value:

   Value name: DisablePassiveModeLoginPrompt

   Value data: Any non-zero value (for example, 1, 2, 3, 100)

   Normally, the ZENworks Agent attempts to authenticate the user to the zone by using the credentials entered in the Microsoft or Novell client. If login fails, the ZENworks login prompt is displayed in order to give the user an opportunity to authenticate with different credentials. This value setting disables the ZENworks login prompt.

7.5 Using a DLU in a Domain Environment

Domain authentication is not possible when you do a local login based on the eDirectory credentials and not the domain credentials. Enabling a DLU policy forces the creation and use of a local account that does not have access to domain resources, even if you are logged in to the domain.

When a DLU policy is enforced on devices joined to a domain, it forces a local log in instead of a domain log in. Using a DLU is not supported on a domain controller, because the domain controller has no local Security Accounts Manager (SAM) to provide a local login.

You might want to use a DLU for certain reasons, even when the device is in a domain:

- When only devices are in domain and not the users, users need a DLU to ease access to their computers or if the domain trust is broken
- When the users are in the middle of a migration and do not want to flip a switch
- When users require access to local personal computers while accessing certain devices versus their normal domain rights

To manage Windows user accounts in an eDirectory environment:

- Use an NT or AD domain and then use Account Management or Identity Manager to synchronize AD and eDirectory accounts and passwords
- Use a DLU policy to automatically create and manage the Windows account upon eDirectory login

Using a DLU in a domain environment might cause problems in some of the following circumstances:

- When the user assigned to a DLU policy attempts to log in to eDirectory, the Windows authentication is done with a local user and not a domain user. This is because the Windows authentication settings to log in to the domain are ignored, when the DLU policy is in effect.
- When the user is authenticated to Windows with a local account, domain access appears to be working if the local Windows account and the domain Windows account have the same username and password. The DLU user, although it is based on eDirectory credentials has the same username and password as the user in the Active Directory domain. However, account access depends on where the authentication request originates:
  - When you use a local Windows account to access a resource from a domain controller, the authentication attempts work and access is granted because the domain user account exists in the local Security Accounts Manager (SAM) of the domain controller.
  - When you use a local Windows account to access a resource from a member server using a local Windows account, the authentication attempt fails and access is not granted because it is a member server and the domain user account does not exist in its local SAM. The member server cannot access a domain controller to obtain authentication.

7.6 Configuring Attribute for ActiveSync Server Authentication

This feature is applicable for mobile device only. For more information, see Configuring the Attribute for ActiveSync Server Authentication.

8 User Source Settings

You can use the User Source Settings panel to perform the following tasks on the ZENworks Server.

8.1 Kerberos Authentication

The User Source Settings panel lets you search for and select a keytab file used for Kerberos authentication. All Kerberos server machines need a keytab file to authenticate to the Key Distribution Center (KDC). The keytab file is an encrypted, local, on-disk copy of the host's key.

Before you can import the keytab file, you must set up a Kerberos service principal account and generate a keytab file for that account. For more information, see “Kerberos (Active Directory or Domain Services for Windows)” on page 37.

To import the keytab file, click  to search for the file, then click **OK**.

After importing the keytab file, you can enable Kerberos authentication while adding a user source. To do so, click the **Configuration** tab, then click **New** in the User Sources panel to launch the Create New User Source Wizard. You can also enable Kerberos authentication on an existing user source. To do so, click the **Configuration** tab, click the user source, then click **Edit** next to Authentication Mechanisms in the General section.

8.2 Active Directory Settings

The Active Directory Settings panel lets you configure the range to search for Active Directory group memberships within a user container.

For example, assume that you have a user container named BLR that has the A, B, and C top-level groups and the following nested groups:

- Group A has a nested group A1, A1 has a nested group A2, and A2 has a nested group A3.
- Group B has a nested group B1, B1 has a nested group B2, and B2 has a nested group B3.
- Group C has a nested group C1 and C1 has a nested group C2.

Select one of the following options:

- **Top-level groups only:** Limits the search to within the top-level groups of the user container. For example, select this option if you want the search to be performed only in the A, B, and C top-level groups and not in the nested groups (A1, A2, A3, B1, B2, B3,C1, C2).
- **Top-level groups and all the nested groups:** Searches within all the top-level groups and all the nested groups of the user container. For example, select this option if you want the search to be performed in the top-level groups (A, B, and C) and in all the nested groups (A1, A2, A3, B1, B2, B3,C1, C2).
- **Top-level groups and the nested group depth level upto:** Lets you specify the nested group level to search. For example:
  - For the nested group depth level specified as1, the search is performed in all the top-level groups (A, B, and C) and in the A1, B1, and C1 nested groups.
  - For the nested group depth level specified as 2, the search is performed in all the top-level groups (A, B, and C) and in the A1, A2, B1, B2, C1, and C2 nested groups.
  - For the nested group depth level specified as 3, the search is performed in all the top-level groups (A, B, and C) and in the A1, A2, A3, B1, B2, B3, C1, and C2 nested groups.

9 Troubleshooting User Sources

This section contains explanation on some of the user source problems.

User source context is not displayed when User Source is down and loader service is restarted on Primary Servers

Source: ZENworks LDAP User Source

Explanation: In ZENworks Control Center, the user source contexts might not be displayed when the user source is down or not reachable, and the loader service or Primary Server is restarted. This might cause the ZENworks user login on the Managed devices to fail as the user content is missing

Possible Cause: The User source is not reachable or down, and when the loader or Primary Server is restarted. On every loader restart, the iaRealms.xml file will be recreated and if the user source is down, the file will be created without user context information. This causes the ZENworks user login to fail on the managed devices.

Action: Ensure that the user source is up and running, or reachable from Primary Servers, and then restart the loader service on the Primary Servers.

A user group of a Domain Services for Windows user source does not list the members of the group

Explanation: In ZENworks Control Center, a user group of a Domain Services for Windows (DSfW) user source might not list its members even though users have been added as members of this group.

Possible Cause: Objects such as users and user groups listed within the OESSystemObjects container might not have the objectSid attribute defined.

To determine whether an object has the objectSid attribute defined or not, perform the following steps:

1. Log in to ConsoleOne.
2. Right-click the object.
3. Click **Properties**.
4. Click the **Other** tab.
5. Select the Show read only option and check if the objectSid attribute exists.

Action: In ConsoleOne, edit the description of such objects to generate the `objectSid` attribute for the objects.

Possible Cause: ZENworks Control Center throws an unknown host exception when you choose to list the members of the group:

Example:

```
Root exception is java.net.UnknownHostException:
srmdsfw.com
```

Action: Edit the *%WINDIR%*`\system32\drivers\etc\hosts` on the Windows server or the */etc/hosts* file on the Linux server to add the following entry for the unknown host:

`ip` *`hostname`*`.com` *`hostname`*

Example:

```
ip srmdsfw.com srmdsfw
```

Logging in to the user source on a ZENworks Server from a managed device might be slow if Trend Micro AntiVirus Plus AntiSpyware is installed on the device

Explanation: During installation of the ZENworks agent on a device, an executable file named `NalView.exe`, which is configured to run at user login, is added to the Run registry key. This addition enables the bundle icon to be placed on the Start menu, desktop, notification area, and the Quick Launch area of the Windows taskbar.

During the user login, `NalView.exe` runs on the device, resulting in a delay in the overall login time.

Action: To speed up the login process, do one of the following:

- Disable `NalView.exe` at login time:

NOTE: If you choose to disable `Nalview.exe` at login time, the bundle icon is not placed on the device Start menu, desktop, notification area, and the Quick Launch area of the Windows taskbar. However, the bundle icon is placed in the application window of the device.

1. Open the Registry Editor.
2. Go to `HKLM\SOFTWARE\Netware\Nal\1.0\NalView\`.
3. Create a DWORD called `Disabled` and set its value to `1`.
4. Log in to the device again.

- Launch `NalView.exe` after a delay of *x* seconds from the login time:
  1. Open the Registry Editor.
  2. Go to `HKLM\SOFTWARE\Netware\Nal\1.0\NalView\`.
  3. Create a DWORD called `Delay` and set its value to the time (in seconds) by which you want to delay the launch of `NalView.exe`.
  4. Log in to the device again.

An error occurs after adding an administrator group from Active Directory, when the AD is linked to the AD Root Domain

Explanation: While you configure a User Source, if you use Active Directory as the LDAP server and then add the root domain into the **Context** field, an error occurs. To resolve this problem, make sure you also add the AD Server to your `hosts` file.

Action: On a Windows managed device:

1. Open `%SystemRoot%\system32\drivers\etc\hosts` in a text editor.
2. Add the `<IP-Address-of-the-AD-Server> <Domain-Name>` entry to the file.

   For example, you could add the `164.99.165.51 example.com` entry to `C:\WINDOWS\system32\drivers\etc\hosts`, where `164.99.165.51` is the IP address of the AD server and *example.com* is the domain name.

Action: On a Linux managed device:

1. Open `/etc/hosts` in a text editor.
2. Add the `<IP-Address-of-the-AD-Server> <Domain-Name> <Short-Hostname>` entry to the above file.

   For example, you could add the `164.99.165.51 example.com example` entry to `/etc/hosts`, where `164.99.165.51` is the IP address of the AD server, *example.com* is the domain name, and *example* is the short hostname.

Queries sent from ZENworks Control Center to the user source are slow

Explanation: LDAP queries sent from ZENworks Control Center to the eDirectory user source trigger server-side sorts that cause a delay in receiving search results.

Action: To remove the sorting order and to receive results faster:

1. Stop the ZENserver service.
2. Change the `disableSorting` value to `True` in the following file:

   On Windows:

   `<%ZENWORKS_HOME%>conf\datamodel\authsource\edirectory.zls.xml`

   On Linux: `/etc/opt/novell/zenworks/datamodel/authsource/edirectory.zls.xml`
3. Restart the ZENserver service.

eDirectory User groups of Domain Services for a Windows user source do not show up in ZCC when switching from the LDAP port 389 to 1389

Explanation: In ZENworks Control Center, the eDirectory user groups of Domain Services for a Windows (DSfW) user source might not be displayed when switching from the eDirectory LDAP port 389 to the Domain Services for Windows LDAP port 1389.

Possible Cause: For an LDAP Group object on an eDirectory server, the eDir Class `Group` is mapped to the Primary LDAP class `groupOfNames`. This is different for Domain Services for Windows (DSfW). For an LDAP Group object on a DSfW server, the eDir Class `Group` is mapped to the Primary LDAP class `group`.

Action: Use separate eDirectory servers when there are eDirectory user groups.

Browsing while configuring the Active Directory user source takes longer than expected

Explanation: Browsing for containers while trying to configure the Active Directory user source might take more time than expected, if ZENworks is configured to follow referral references.

Action: If there are no referrals in Active Directory, you can set the `IgnoreADReferrals` value to `True` in the `authsourceconfig.xml` file. This file can be accessed from the following location: `%ZENWORKS_HOME%\conf\datamodel\authsource\authsourceconfig.xml`

NOTE: The IgnoreADReferrals parameter is applicable only for the ZCC Browsing and Configuration information. It does not apply to Authentication.

10 Troubleshooting User Authentication

This section contains explanation on some of the user authentication related problems. To troubleshoot other problems you might encounter during authentication, see TID 3273870 in the Novell Support Knowledgebase (http://support.novell.com/search/kb_index.jsp).

ZCC Login Failure Events are not Audited

Explanation: From ZENworks Update 2 onwards, the ZCC login failure events are not audited.

Action: None

The login failure events are logged in:

- on Windows: %ZENWORKS_HOME%\logs\osp-zenworks-${date}.log
- On Linux: /var/opt/microfocus/log/zenworks/osp-zenworks-${date}.log

Incorrect username displayed in the ZENworks Login screen

Explanation: The **Username** option in the ZENworks Login screen displays the Windows local username by default.

Possible Cause: If you changed only the full name of the user (**My Computer** > **Manage** > **System Tools** > **Local Users and Groups** > **Full Name**), the ZENworks login screen displays the old username and not the new full name.

Action: To change the local user account details, you must change both the username and the full name of the user:

1. Click the desktop **Start** menu > **Run**.
2. In the Run window, specify **control userpasswords2**, then click **OK**.
3. Double-click the username and edit both the **User Name** and **Full Name** of the user.
4. Click **OK**.

Unable to log in to the ZENworks Server

Possible Cause: A user with an account in the eDirectory that is installed on an OES 2.0 server tries to log into a non-OES 2.0 ZENworks Server.

Action: To log in to a non-OES 2.0 ZENworks Server, the user must be a Linux User Management (LUM) user. For more information on LUM users, see the *Novell Linux User Management Technology Guide (http://www.novell.com/documentation/oes2/acc_linux_svcs_lx/index.html?page=/documentation/oes2/acc_linux_svcs_lx/data/fbdecbed.html)*

Large number of concurrent client logins might result in login failures

Explanation: The maximum number of concurrent client connections that a server can support depends on the configured `Connector acceptCount`. If the number of concurrent client requests exceeds the value of `Connector acceptCount`, the client connect requests might fail because the server is not able to accept these connections.

Action: Increase the number of client connect requests that the server can support.

On a Windows server:

1. Log in as an administrator.
2. Open the *`ZENworks_Install_path`*`\share\ats\catalinabase\conf\server.xml` file.

3 In the `Define a SSL Coyote HTTP/1.1 Connector on port 2645` section, change the value of the `Connector acceptCount` to the desired value. A value of 300 is optimal.

4 Restart the Authentication Token Service:

4a On the desktop, click **Start** > **Run**.

4b In the Run window, specify **services.msc**, then click **OK**.

4c Restart **CasaAuthTokenSvc**.

On a Linux server:

1 Log in as `root`.

2 Open the `/srv/www/casaats/conf/server.xml` file.

3 In the `Define a SSL Coyote HTTP/1.1 Connector on port 2645` section, change the value of the `Connector acceptCount` to the desired value. A value of 300 is optimal.

4 Restart the Authentication Token Service:

4a At the server prompt, go to `/etc/init.d/`.

4b Run the `casa_atsd restart` command.

How do I enable debug logs on Windows 2003, Windows XP, and Windows Vista devices?

Action: To enable the logs, see TID 3418069 in the Novell Support Knowledgebase (http://support.novell.com/search/kb_index.jsp).

How do I enable the CASA debug logs?

Action: To enable the logs, see TID 3418069 in the Novell Support Knowledgebase (http://support.novell.com/search/kb_index.jsp).

Unable to log into the ZENworks Server when logging in to a Windows Vista device

Explanation: If you log into a Windows Vista device that has Novell SecureLogin installed and Active Directory configured as the user source, you are not automatically logged in to the ZENworks server.

Action: Do the following:

1 Open the Registry Editor.

2 Go to `HKLM\Software\Protocom\SecureLogin\`.

3 Create a DWORD called ForceHKLMandNoDPAPI, and set the value to 1.

4 Restart the device.

The settings assigned to an eDirectory user are not applied on the device where the user has logged in

Possible Cause: Two or more eDirectory users with the same username and password might exist in different contexts of the eDirectory tree.

Explanation: When an eDirectory user specifies the username and password to log in to a device, a user with the same username and password but located in a different context of the eDirectory tree might be logged in to the device and the settings of this user are applied on the device. This is because the login GINA is contextless.

For example: Assume that user1 and user2 have the same username and password:

User1: `CN = bob, OU = org1, O = Company1 (bob.org1.company1)`

User2: `CN = bob, OU = org2, O = Company1 (bob.org2.company1)`

When user2 specifies the username and password to log in to a device, user1 is logged in to the device instead of user2 because user1 appears first in the search performed by Novell CASA. The settings assigned to user1 are applied on the device.

Action: No two eDirectory users should have the same username and password. Even if the usernames are same, ensure that the passwords are different.

The ZENworks login screen is not displayed on a device if Novell Client has been uninstalled from the device

Explanation: If you uninstall the Novell Client 2 for Windows Vista/2008 (IR1a) from a device, the ZENworks login screen is not displayed on the device when you log in to the device.

Action: To log in to ZENworks Configuration Management, right-click the ZENworks icon on the device, then click **Login**.

A DSfW user is unable to use Kerberos authentication to log into a device

Explanation: If an iManager or ConsoleOne created DSfW user chooses to use Kerberos authentication to log in to a device, the authentication fails.

Action: Modify the user to set the value of the `UserPrincipalName` attribute in the standard domain username format (for example, *`user@domain`*`.com`) and then log in to the device again.

or

Use Microsoft Management Console (MMC) for creating DSfW users because the value of the user's `UserPrincipalName` attribute is set by default.

Unable to create a keytab file for a DSfW server

Explanation: During the creation of a keytab file for DSfW server, you might encounter the following error:

```
Unable to find the user in the specified domain
```

Action: Do the following:

1. Run the following command to ensure that the DSfW services are running properly:

   ```
   xadcntrl status
   ```

2. (Conditional) If the DSfW services are not running properly, run the following command to restart the DSfW services:

   ```
   xadcntrl reload
   ```

3. Run the following command to create the keytab file again:

   ```
   ktpass /princ host/atsserver.myserver.com@MYSERVER.COM -
   pass atsserver_password -mapuser domain\atsserver -out
   atsserver.keytab -mapOp set -ptype KRB5_NT_PRINCIPAL
   ```

Seamless Authentication fails on a Windows XP virtual device

Explanation: If you install the ZENworks Agent on a Windows XP virtual device that is provisioned in a VMWare View Persona Management (VDI environment), then seamless login to ZENworks fails on the device.

Action: Use the ZENworks icon to log in to ZENworks.

Unable to seamlessly log in to Novell SecureLogin on a device that has Novell ZENworks installed

Explanation: Novell SecureLogin starts seamlessly after a device desktop opens only if you have used the LDAP Credential Manager mode during the installation of Novell SecureLogin on the device. For more information about the LDAP Server options available during the installation of Novell Secure Login, see the *Novell SecureLogin Installation Guide* at the Novell Documentation site (http://www.novell.com/documentation/securelogin70/installation_guide/data/).

On a device that has ZENworks installed, if Novell SecureLogin does not start seamlessly after the device desktop opens, the authentication registry keys might not be properly set on the device.

Action: Do the following to set the authentication registry keys on the device:

1. Open the Registry Editor.
2. Go to `HKLM\SOFTWARE\Novell\NWGINA\`.
3. Create a DWORD called `PassiveMode` and set its value to 1.
4. Ensure that `HKLM\Software\Novell\Login\LDAP\GinaLoginDone` is set to 0.
5. Log in to the device again.

ZENworks login fails for eDirectory users having simple passwords

Explanation: If there are two passwords, an NDS and a Simple password for an eDirectory user, on changing the password, only the NDS password changes, and the login fails.

Action: Do not configure simple passwords while creating users.

Disabling the ZENworks Credential Provider on a Device

Explanation: The ZENworks Credential Provider filters the Windows Password Credential Provider. When you install the ZENworks Agent on the Windows Vista or later versions and Windows 2008 Server or later versions device that has third-party products with Credential Providers installed, multiple user tiles are displayed.

Action: To suppress multiple user tiles, create the following registry key on the agent:

1. Open the Registry Editor.
2. Go to `HKLM\SOFTWARE\Novell\ZCM\ZenLgn`.
3. Create a DWORD called `DisableZENCredentialProvider` and set its value to 1.
4. Restart the device and log in.

IMPORTANT: If you enable the `HKLM\SOFTWARE\Novell\ZCM\ZenLgn` registry key, you can not manage Dynamic Local User, Roaming Profile and Windows Group policies through ZENworks. ![Removing this line as a part of bug 1171400]

Unable to login to ZENworks

Explanation: Commands from the Network Credential Manager are handled by the Windows Multiple Provider Notification application. If this application is replaced with a Third-Party Notification application that cannot process these commands, the Networks Credential Manager fails to function and you will be unable to login to ZENworks.

DLU with smart card uses PIN for Windows user account

Source: ZENworks Configuration Management; Policy Management; Windows Configuration Policy.

Explanation: The DLU policy with user source credentials and ZENworks smart card login uses the smart card PIN for the Windows Local user account. In this case password complexity may not meet for the Windows password.

Action: Configure Universal Password policy for the eDir user and create universal password for the user. This universal password will be used for the DLU account.

Passive login not working on Windows 10 1803 or later with ZENworks Credential Manager

Explanation: When any third-party credential provider has been installed along with ZENworks Agent on Windows 10 version 1803 or later devices, the ZENworks passive login does not work.This issue occurs even for scenarios in which the ZENworks Credential provider is disabled using the registry key and the ZENworks user login is enabled through ZENworks Credential Manager. Microsoft has confirmed that this issue exists on Windows 10 version 1803 or later devices.

Action: Until you apply the Microsoft fix you can use the `EnableCredManForceLogin` For more information on this registry key, refer to EnableCredManForceLogin in the ZENworks Registry Keys Reference.

The following links include the fixes provided by Microsoft:

- Windows 10 1803: https://support.microsoft.com/en-us/help/4537795
- Windows 10 1809: https://support.microsoft.com/en-us/help/4537818
- Windows 10 1903/1909: https://support.microsoft.com/en-us/help/4535996

NOTE: After the devices are updated with the Microsoft fix, it is recommended to delete the `EnableCredManForceLogin` registry key or set the value to `False` to prevent duplicate user login attempts into ZENworks.

User Authentication fails when LDAP is not configured with SSL

Explanation: When Active Directory servers have the LDAP channel bind fixes from Microsoft, then ZENworks user authentication will fail for all LDAP Servers that are not configured with SSL within ZENworks. For more information, see 2020 LDAP channel binding and LDAP signing requirements for Windows.

Action: You need to enable SSL for LDAP, within ZENworks. For information on how to enable SSL, see Section 2.1, “Adding User Sources,” on page 9.