

### Objective 3 Integrate SUSE Linux Enterprise Desktop 10 into a Novell eDirectory Environment

You can use Novell Linux User Management (LUM) to configure SUSE Linux Enterprise Desktop 10 workstations on your network so that users can log in to them using their Novell eDirectory user names and passwords instead of their local Linux workstation user names and passwords.

Using LUM and eDirectory to manage user login information eliminates the need to create local users in the `/etc/passwd` and `/etc/shadow` files on each SUSE Linux Enterprise Desktop 10 workstation. It also simplifies user account management by consolidating user accounts in a central point of administration.

You can use eDirectory tools and technologies to manage access to Linux resources on the network. After authenticating, users have the rights and privileges specified in eDirectory.

These are the same rights and privileges that are typically stored in a local account or redirected to other authentication methods, such as NIS (Network Information Service).

The user account information stored in eDirectory lets users access file and printer resources on your network.

A user can log in to SUSE Linux Enterprise Desktop 10 workstations using access methods such as `login`, `ftp`, `ssh`, `su`, `rsh`, `rlogin`, `xdm` (KDE), and `gdm` (GNOME).

The user only needs to enter his or her familiar eDirectory user name and password. The user does not have to remember the full context—LUM searches out the correct user in eDirectory.

In this objective, you learn the steps required to set up a SUSE Linux Enterprise Desktop 10 workstation to use eDirectory authentication, including configuring the SUSE Linux Enterprise Desktop workstation for eDirectory authentication and enabling users on the eDirectory server.



For more detailed information on LUM and on configuring your eDirectory 8.6.x, 8.7.x, or 8.8.x server to use LUM, see the *Novell Linux User Management Technology Guide* <http://www.novell.com/documentation/oes/lumadgd/data/bookinfo.html>.

---

This objective covers the following:

- [Set Up eDirectory Authentication](#)
- [Turn Off eDirectory Authentication](#)

## Set Up eDirectory Authentication

The use of eDirectory authentication requires you to configure the workstations to use eDirectory for authentication purposes and to enable Linux User Management within eDirectory:

- [Activate Linux User Management on Workstations](#)
- [Use Novell iManager to Enable Users for eDirectory Authentication](#)

### Activate Linux User Management on Workstations

Before users can use their eDirectory user names and passwords to log in, you must configure the SUSE Linux Enterprise Desktop workstation with Linux User Management components.

You can set up eDirectory Authentication during the SUSE Linux Enterprise Desktop installation, or you can use YaST to set it up anytime after installation.

To install and configure LUM during the SUSE Linux Enterprise Desktop installation, do the following:

1. From the User Authentication Method page shown below, select **eDirectory LDAP**.

Figure 13-16



2. (Conditional) If it is not already installed, you will be prompted to install the **yast2-linux-user-mgmt** package.

To install and configure LUM on an already running workstation, perform the following steps:

1. From the workstation, launch the YaST Control Center:
  - a. GNOME: Select **Computer > More Applications > System > YaST**.
  - b. KDE: Select the **K Menu** button; then select **System > YaST (Administrator Settings)**.
2. Select **Security and Users > Linux User Management**.  
If this module is missing, install the `yast2-linux-user-mgmt` package using the YaST Software Management module. Then close YaST and start it again.
3. Specify whether eDirectory is running on the computer itself (Local System) or on another computer on the network (Remote System).
4. If eDirectory is running on a remote system, specify the remote system's **IP\_address**.
5. (Optional) Specify the eDirectory **admin name**, **context**, and **password**; then select **Next**.

The admin name and context must be entered in LDAP syntax, which uses a comma instead of a period (for example, **cn=admin,o=novell**).



If you do not have rights to create objects in the eDirectory tree, leave these fields blank. You will need to contact your eDirectory administrator, give the administrator the host name of your client, and ask him or her to create a LUM Workstation object with your host name.

You should also ask the administrator where you can get a copy of the CA certificate for the LDAP server. You will need to place this certificate in the `/var/lib/novell-lum/` directory.

The name of the CA certificate matches the name of the preferred-server entry in the `/etc/nam.conf` file and has a `.der` extension. You can type **namconfig get preferred-server** to get the name.

6. Specify the **location** of the Linux/UNIX Config object.

The Linux/UNIX Config object stores a list of the locations (contexts) where Linux/UNIX Workstation objects reside on the network. It also controls the range of numbers to be assigned as UIDs and GIDs when User and Group objects are created.

This object is created when LUM is configured on the eDirectory server and is usually located in an upper container of the eDirectory tree (for example, **o=novell**). Contact your eDirectory administrator for the context.



For more information, see “Understanding eDirectory Objects and Linux” in the *Novell Linux User Management Technology Guide* <http://www.novell.com/documentation/oes/lumadgd/data/bx3sbv9.html>. It is also included on the 3086 Course DVD 2 in the directory OESDocs.

7. (Optional) Specify the **location** of the LUM Workstation object.

The LUM Workstation object represents the actual computer a user logs in to.

If you have rights to create objects in the eDirectory tree, this object is automatically created as part of the workstation configuration and is usually placed in an Organization (O) or Organizational Unit (OU) container in the eDirectory tree.

You can also create a LUM Workstation object by selecting **Linux User Management > Create Linux Workstation Object** in Novell iManager.

8. (Optional) If you have disabled anonymous binds to the LDAP server, specify a *proxy user name, context*, and *password* for a user that has rights to the LDAP tree.
9. Select **Next**.
10. Select which *login access methods* should use eDirectory for authentication.
11. Select **Finish**.

Installing and configuring LUM technology sets up the SUSE Linux Enterprise Desktop workstation to validate login requests against user account information stored in eDirectory.

Before users can log in, they must have eDirectory user accounts created with Novell iManager and extended for LUM, and their User objects must be associated with the workstations they will log in to.

### **Use Novell iManager to Enable Users for eDirectory Authentication**

When Linux User Management components are properly installed, you can use eDirectory and Novell iManager to specify which users can access SUSE Linux Enterprise Desktop computers on the network.

Novell iManager is the browser-based utility for managing eDirectory objects. It runs in a network browser such as Mozilla Firefox, Netscape Navigator, or Internet Explorer.

When you create user or group accounts in Novell iManager, you are prompted to “LUM enable” the User object or Group object. You can also use Novell iManager to enable existing User or Group objects for Linux.

Each time you configure a SUSE Linux Enterprise Desktop workstation for eDirectory authentication, eDirectory users that are LUM enabled must be associated with a workstation before they can log in from that workstation.

To use Novell iManager to enable users for eDirectory Authentication, do the following:

1. Launch Novell iManager:
  - a. In the Address field of a network browser, enter the following:  
**`http://target_server/nps/iManager`**
  - b. Log in using the full context of the *admin user* and *password*.
2. Make sure you are in the Roles and Tasks view by clicking on the top button bar, then, from the left pane, select **Linux User Management**.
3. Select **Enable Users for Linux**.
4. Select the *User object* you want to enable, then select **Next**.

When an eDirectory User object is extended to hold Linux user-login properties, it is said to be LUM enabled or enabled for Linux.

When enabled for Linux, a user can simply access the Linux computer using Telnet, SSH, or other supported methods and enter his or her user name and password.

The access request is redirected to find the appropriate user name and login information stored in eDirectory.

When extended for Linux, the eDirectory User object holds Linux-related properties, such as user ID, primary group ID, primary group name, location of home directory, and preferred shell.

5. Assign the user to a group; then select **Next**.

The group and its corresponding group ID (GID) are assigned as the user's primary GID. If the selected user account already has a primary GID, this group's GID is assigned to the user as secondary.

You can choose any of the following ways to assign the user to a group:

- **An Existing eDirectory Group.** If the Group object has not yet been enabled for Linux, its properties are extended to include Linux login attributes. You can click the Object Selector icon to browse the tree for an existing group.
- **An Existing Linux-Enabled Group.** This option lets you select an existing eDirectory Group object. If you use the Object Selector to browse, you can view and select only those Group objects already extended with Linux login attributes.
- **Create a New Linux-Enabled Group.** This option lets you create a new eDirectory Group object. When created, the Group object is extended to include Linux login attributes.

6. Select the *workstations* to which the users in the group should have access; then select **Next**.
7. Apply the changes and continue by selecting **Finish**; then select **OK**.

Users should now be able to use their eDirectory user login credentials to log in to their SUSE Linux Enterprise Desktop workstations.

### ***Turn Off eDirectory Authentication***

There might be times when you want to turn off a workstation's ability to accept logins from eDirectory. You can permanently turn off this ability by removing the LUM software from the workstation. You can temporarily disable eDirectory authentication by stopping the named daemon.

To stop named, open a shell window and enter **rcnamed stop**.

To turn on eDirectory authentication and LUM, open a shell window and enter **rcnamed start**.