Contents

Chapter 1: How to Register a UNIX Host in a One-Way Trust Domain Environment

Introduction

Scenario for: UNAB®

Release: r12.6.02

OS: UNIX, Linux

This scenario explains how a system administrator registers a UNIX host in a one-way trust domain environment.

This Knowledge Base Article constitutes a portion of the official CA product documentation for this CA product. This Knowledge Base Article is subject to the following notices (see page 20), terms and conditions.

How to Register a UNIX Host in a One-Way Trust Domain Environment

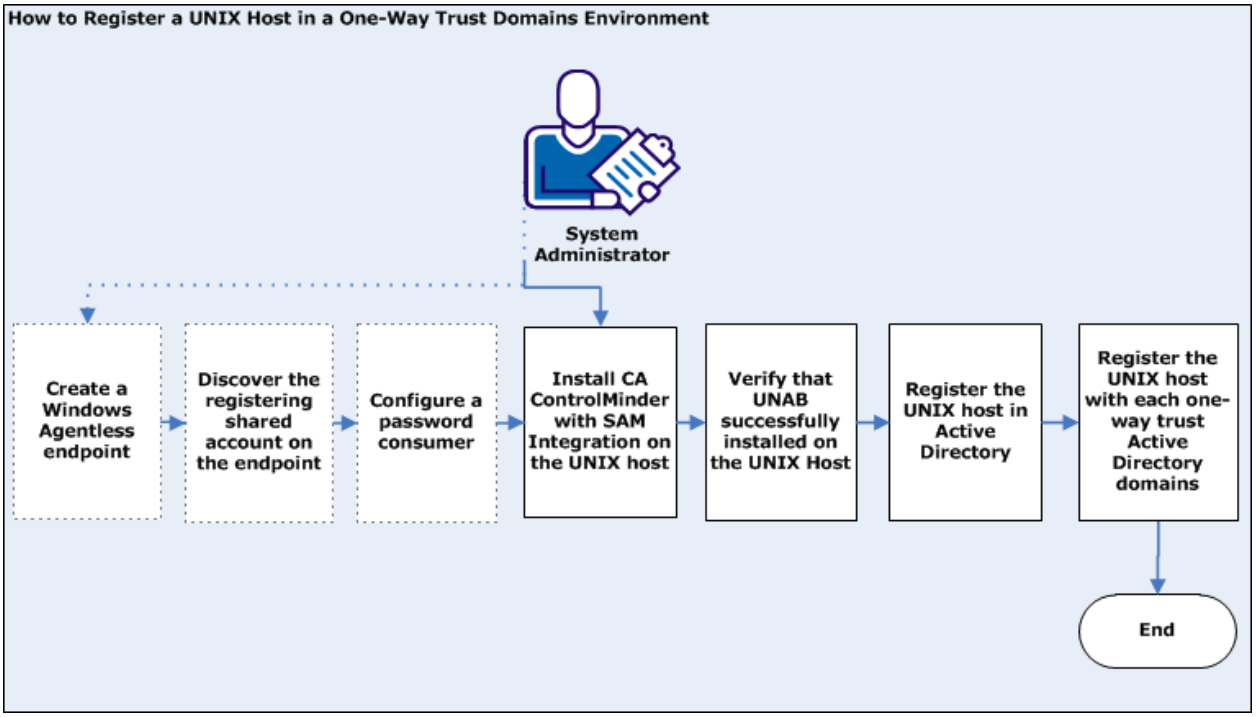
When you register the UNIX host in Active Directory, you use a user account with privileges to retrieve users and groups details from Active Directory. If you register the UNIX host in a two-way trust domains environment, you can use a single user account to retrieve users and groups from every Active Directory domain.

In a one-way trust domain environment the Active Directory account that you use to register a UNIX host cannot retrieve data from other Active Directory domains. In a one way trust domains environment, you register the UNIX host with a regular user account from each Active Directory domain.

Further, you can register a UNIX host with an Active Directory shared account and use Shared Accounts Management to manage the account. The user account must have sufficient permissions to retrieve the user and groups attributes from all every Active Directory domain.

To register a UNIX using a domain account, you use Shared Accounts Management integration. Integrating with Shared Accounts Management enables you to manage the registering user account, for example, apply the domain security policy, change the account password automatically and more.

The following diagram illustrates how to register a UNIX host in a one-way trust domain environment:



Note: Dotted lines indicate optional steps.

Follow these steps:

1. (Optional) To use a shared account to register the UNIX host, follow these steps:
    a. Create a Windows Agentless endpoint (see page 7).

       You specify the connection details of the Active Directory domain that you use to register each UNIX host.

    b. Discover the registering shared account on the endpoin (see page 8)t.

       You run the account discovery wizard on the Windows Agentless endpoint that you created.

    c. Define a password consumer (see page 10).

       You specify the UNAB endpoint as an SDK password consumer to enable the endpoint to obtain the registering user account password.

2. Install CA ControlMinder with Shared Accounts Management integration on each UNIX host that has UNAB installed (see page 13).

   The Shared Accounts Management integration configures the local computer for Shared Accounts Management (SAM). Set the INSTALL_PUPM option to yes to install Shared Accounts Management on the endpoint. For more information about Shared Accounts Management, see the *Enterprise Administration Guide*.

3. Verify that UNAB installation successfully completed. Do the following:
    a. Locate the accommon.ini file. By default, the file is located in the following directory:

       ```
       /opt/CA/AccessControlShared
       ```

    b. Locate the Distribution_Server token under the communication section.

    c. Define the Distribution Server URL. For example:

       ```
       ssl://ds_dr.comp.com:7243
       ```

       Note: For more information about the accommon.ini file, see the *Reference Guide*.

    d. Use the sechkey utility to set the communication password.

    e. Open a selang command-prompt window and enter the following commands:

       ```
       er ACVAR unab value("/opt/CA/uxauth/bin/uxauthd")
       er ACVAR unab value+("opt/CA/uxauth/bin/uxconsole")
       ```

4. Do *one* of the following:

   - To use a regular account to register the UNIX host, follow these steps:

     a. Start CA ControlMinder (see page 15).

     b. Register the UNIX host in each Active Directory domain (see page 16).

     c. Activate UNAB (see page 18).

     d. Register the UNIX host with each Active Directory in the one-way trust domain environment using the uxconsole -register- ows command.

     e. Start UNAB (see page 19).

   - To use a shared account to register the UNIX host, follow these steps:

     a. Start CA ControlMinder (see page 15).

     b. Register a UNIX host in Active Directory (see page 16).

     c. Activate UNAB (see page 18).

     d. Register the UNIX host with each Active Directory in the one-way trust domain environment using the uxconsole -register- ows command..

     e. Start UNAB (see page 19).

     Note: For more information about the uxconsole utility, see the *Reference Guide*

Creating a Windows Agentless Endpoint

Shared Accounts Management can manage domain users on the Active Directory. To manage the Active Directory accounts, define a Windows Agentless Endpoint and provide the following information:

User Login

Defines the name of an administrative user who manages the endpoint. Shared Accounts Management uses this account to perform administrative tasks on the endpoint, for example, to connect to the endpoint, discover accounts, and change passwords.

Specify the *user name* in this field. Do not use the *computer name/user name* format or the *domain name/user name* format.

Example: Administrator.

Note: If you specify the Advanced option, Shared Accounts Management does not use the User Login account to perform administrative tasks. Instead, Shared Accounts Management uses the account that is specified under the Advanced option to perform administrative tasks on the endpoint.

Password

Defines the password of the administrative user of the endpoint.

Note: If you use the Advanced option, do not supply a password.

Host

Defines the Active Directory DNS domain name.

Example: company.com

Note: Shared Accounts Management attempts to resolve the Active Directory domain controller from the domain name. If Shared Accounts Management fails to resolve this name, specify the Active Directory Domain Controller (DC) DNS name or IP address.

Host Domain

Specifies the domain name (NETBIOS name).

Example: domain1

Note: Do not use the DNS name (domain1.ca.com), use the NETBIOS name (domain1).

Is Active Directory

Select this option to specify the Active Directory.

User Domain

Specifies the domain name (NETBIOS domain name) of the user specified in the User Login field or in the Advanced field (in case Advanced is used).

Example: domain1

Note: Do not use the DNS name (domain1.ca.com), use the NETBIOS name (domain1).

Advanced

Specifies whether to use a previously defined privileged administrative account, to perform administrative tasks on the endpoint. For example, Shared Accounts Management uses the account defined in the Advanced field to manage this endpoint instead of using the account specified in the User Login field. This option is useful when using the same privilege account to manage multiple endpoints.

Note: If you specify this option, Shared Accounts Management does not use the User Login account to perform administrative tasks.

Disable Exclusive Sessions

This option specifies whether to disable the exclusive sessions check on this endpoint. When selected, Shared Accounts Management does not check for open sessions on the endpoint.

Discover Privileged Accounts

We recommend that you run the privileged accounts discovery process at fixed intervals to scan for new privileged accounts on the endpoints. Discovering privileged accounts lets you create multiple privileged accounts at the same time. CA ControlMinder Enterprise Management presents the accounts that it discovers in a table, so that you can easily tell which accounts you already manage with Shared Accounts Management.

The first time that you discover privileged accounts on an endpoint type, CA ControlMinder Enterprise Management automatically creates an endpoint privileged access role for using privileged accounts on that endpoint type. For example, the first time you discover privileged accounts on a Windows Agentless endpoint, CA ControlMinder Enterprise Management automatically creates the Windows Agentless Connection endpoint privileged access role.

Follow these steps:

1. In CA ControlMinder Enterprise Management, click Privileged Accounts, Accounts, Discover Privileged Accounts Wizard.

   The Discover Privileged Accounts Wizard: Select Privileged Accounts page appears.

2. Select the Endpoint Type from the list.

3. Select an attribute for the search, type in the filter value, and click Search.

   A list of endpoints that match the filter criteria appears.

4. Select the privileged accounts that you want to manage.

   The following table column headings are not self-explanatory:

   Discovered Account

   Specifies whether the account is already known to CA ControlMinder Enterprise Management. Known accounts include ones that CA ControlMinder Enterprise Management already manages and the administrator account CA ControlMinder Enterprise Management uses to manage the endpoint.

   Is Endpoint Administrator

   Specifies whether CA ControlMinder Enterprise Management uses the account to manage the endpoint.

   Important! Be cautious when selecting the endpoint administrator account. CA ControlMinder Enterprise Management can automatically change the password of privileged accounts it manages. If you select the endpoint administrator account, you may lose the ability to log in and manage privileged accounts on the endpoint.

   Click Next.

   The Discover Privileged Accounts Wizard: General Account Details page appears.

5. Complete the fields in the dialog. The following fields are not self-explanatory:

   Disconnected System

   Specifies whether the account originates from a disconnected system.

   If you select this option, Shared Accounts Management does not manage the account. Instead, it acts only as a password vault for privileged accounts of the disconnected system. Every time you change the password, you also need to manually change the account password on the managed endpoint.

   Password Policy

   Specifies the password policy you want to apply to the privileged or service account.

   Check out Expiration

   Defines the duration, in minutes, before the checked out account expires.

   Exclusive Account

   Specifies whether only a single user can use the account at any one time. An *exclusive account* is a restriction imposed on a privileged account that limits use of the account to a single user at a time.

   Exclusive Session specifies that only a single user can use the account, if no open sessions are currently running on the endpoint.

Change Password on Check Out

Specifies whether you want CA ControlMinder Enterprise Management to change the password of the privileged account every time it is checked out.

Note: This option does not apply to service accounts.

Change Password on Check In

Specifies whether you want CA ControlMinder Enterprise Management to change the password of the privileged account every time it is checked in by a user or a program, or when the checkout period expires.

Note: If the account is not exclusive, CA ControlMinder Enterprise Management generates a new privileged account password only when *all* users have checked in the account.

Note: This option does not apply to service accounts.

Service Account

Specifies whether the discovered account is a service account.

Note: You can also use the Discover Service Accounts Wizard to discover service accounts.

Click Finish.

CA ControlMinder Enterprise Management submit the task and creates the selected privileged accounts if there are no errors.

Create a Password Consumer

Password consumers are applications, Windows services, and Windows scheduled tasks that use privileged accounts and service accounts to execute a script, connect to a database, or manage a Windows service, scheduled task, or RunAs command.

There are two groups of password consumers:

- Password consumers that get passwords on demand—Software development kit, database, Windows Run As

  Note: You must install CA ControlMinder on the Shared Accounts Management endpoint with the Shared Accounts Management Integration feature enabled to use password consumers that get passwords on demand.

- Password consumers that get passwords on password change—Windows Scheduled Task, Windows Service

You provide different information to create password consumers from each group. By default, you must have the System Manager role to create a password consumer.

Note: Complete this task if you create a password consumer of types software development kit, database, and Windows Run As. We recommend that you use the Discover Service Accounts Wizard to create Windows Scheduled Task or Windows Service password consumers.

Follow these steps:

1. In CA ControlMinder Enterprise Management, click Privileged Accounts, Password Consumers, Create Password Consumer.

   The Create Password Consumer: Password Consumer Search screen page appears.

2. (Optional) Select an existing password consumer to create the password consumer as a copy of it, as follows:

   a. Select Create a copy of an object of type Password Consumer.

   b. Select an attribute for the search, type in the filter value, and click Search.

      A list of password consumers that match the filter criteria appears.

   c. Select the object you want to use as a basis for the new password consumer.

3. Click OK.

   The Create Password Consumer task page appears. If you created the password consumer from an existing object, the dialog fields are pre-populated with the values from the existing object.

4. Complete the following fields in the General tab:

   Name

   Defines the name you want to refer to this password consumer by.

   Description

   (Optional) Defines the information you want to record for this password consumer (free text).

   Consumer Type

   Specifies the type of the password consumer.

   Application Path

   (Software development kit, database, Windows Run As, Windows Scheduled Task) Defines the full pathname of the password consumer on the endpoint.

   - For software development kit password consumers, specify the pathname of the application that performs the password request.
   - For database password consumers, specify the pathname of the application that connects to the database.
   - For Windows Run As password consumers, specify the pathname of the application that the user executes.
   - For Windows Scheduled Task password consumers, specify the pathname of the scheduled task.

   Note: You can use wildcards (*) and CA ControlMinder variables in the pathname, for example, <!AC_ROOT_PATH>\bin\acpwd.exe.

Service Name

(Windows Service) Defines the pathname of the Windows service. Specify the pathname exactly as it appears in the Windows service properties page.

Enabled

Specifies that the password consumer is enabled, that is, that Shared Accounts Management accepts requests from this consumer or enforces password change on this consumer.

Status

(Windows Scheduled Task or Windows Service) Indicates whether the last password change succeeded or failed.

Last Synchronized Date

(Windows Scheduled Task or Windows Service) Displays the last successful password synchronization.

Restart

(Windows Service) Specifies whether to restart the Windows service after a password change.

5. Click the Privileged Accounts tab and specify the privileged accounts that are associated with the password consumer.

   If you create a software development kit, database, or Windows Run As password consumer, the password consumer can get the passwords for the privileged accounts that you specify.

   If you create a Windows Scheduled Task or Windows Service password consumer, Shared Accounts Management forces a password change for the password consumer when the passwords for these privileged accounts are changed.

6. Specify the entities that can use the password consumer. Do *one* of the following:

   - To create a software development kit, database, or Windows Run As password consumer, do the following:

     a. Click the Hosts tab and select All Hosts to grant all hosts or host groups access to the privileged account password.

        Note: You can type the name of the host or host group in the Name field, or click "..." to search for a CA ControlMinder host or host group (HNODE or GHNODE object).

b. Click the Users tab and specify the users or groups who can request the privileged account password, or select All Users to let every user request the privileged account password.

   Specify the name of the user or group as it appears on the endpoint, for example, DOMAIN\user1. Do not specify a CA ControlMinder Enterprise Management user or group.

- To create a Windows Scheduled Task or Windows Service password consumer, click the Endpoints tab and specify the endpoints on which you want to create the password consumer.

7. Click Submit.

   CA ControlMinder Enterprise Management creates the password consumer.

Install CA ControlMinder RPM Packages

To manage the CA ControlMinder installation with all your other software installations, install the customized CA ControlMinder RPM package.

Important! You must customize the package to specify that you accept the license agreement using a keyword you can find inside the license agreement.

Note: The actual command you use varies depending on many variables, including whether you are upgrading or installing for the first-time, or whether you want to install to the default directory. Some command examples are available in this topic.

Follow these steps:

1. Use the rpm command to install the ca-lic package.

   The license program installs.

2. Customize the CAeAC package.

   You must customize the package to specify that you accept the license agreement using a keyword that you can find inside the license agreement. You can also customize the package to specify custom installation settings.

   Note: If you are upgrading CA ControlMinder, you do not need to customize the package to specify that you accept the license agreement.

3. Use the rpm command to install the CAeAC package.

   CA ControlMinder installs.

   Note: The UNAB package also installs the CAWIN shared component.

   Important! If you are upgrading an existing CA ControlMinder package, unload SEOS syscall before you try to install the new package. Otherwise, the installation fails.

Customize the CA ControlMinder RPM Package

Before you can install CA ControlMinder using a native package, you must customize the CA ControlMinder package to specify that you accept the license agreement. You can also specify custom installation settings when you customize a package.

You customize a package by extracting the installation parameters file from the package, modifying it as required, and then loading it back into the package. Some commands are available in the customization script so that you do not have to modify the parameters file.

Note: We recommend that you *do not* modify the package manually. Instead, use the script as described in the following procedure to customize the CA ControlMinder package.

You can find the RPM packages for each of the supported Linux operating systems in the NativePackages/RPMPackages directory of the CA ControlMinder Endpoint Components for UNIX DVD.

To customize the CA ControlMinder RPM package

1. Copy the package you want to customize to a temporary location on your file system.

   OS is the appropriate subdirectory name of your operating system.

   In the read/write location on the file system, the package can be customized as required.

2. Copy the customize_eac_rpm script file and the pre.tar file to a temporary location on your file system.

   The pre.tar file is compressed tar file containing installation messages and the CA ControlMinder license agreement.

   Note: You can find the customize_eac_rpm script file and the pre.tar file in the same location where the native packages are.

3. Display the license agreement:

   `customize_eac_rpm -a [-d pkg_location] pkg_filename`

4. Take note of the keyword that appears at the end of the license agreement inside square brackets.

   You specify this keyword in the next step.

5. Customize the CA ControlMinder package to specify that you accept the license agreement:

   `customize_eac_rpm -w keyword [-d pkg_location] pkg_filename`

6. (Optional) Set the language of the installation parameters file:

   `customize_eac_rpm -r -l lang [-d pkg_location] pkg_filename`

7. (Optional) Upgrade from an eTrust Access Control r8 SP1 package:

   `customize_eac_rpm -u install_prefix [-d pkg_location] pkg_filename`

8. (Optional) Change the default encryption files:

   `customize_eac_rpm -s -c certfile -k keyfile [-d pkg_location] pkg_filename`

9. (Optional) Get the installation parameters file:

   `customize_eac_rpm -g -f tmp_params [-d pkg_location] pkg_filename`

10. (Optional) Edit the installation parameters file to suit your installation requirements.

    This file lets you set the installation defaults for the package. For example, activate the POSTEXIT setting (remove the preceding # character) and point it to a post-installation script file you want to run.

11. (Optional) Set the installation parameters in your customized package:

    `customize_eac_rpm -s -f tmp_params [-d pkg_location] pkg_filename`

    You can now use the package to install CA ControlMinder with the customized defaults.

Example: Specify That You Accept the License Agreement

To accept the license agreement when installing a native package, you customize the package. The following example shows you how you do customize the x86 CA ControlMinder RPM package that you can find on the CA ControlMinder Endpoint Components for UNIX DVD (mounted to /mnt/AC_DVD) to accept the license agreement:

```
cp /mnt/AC_DVD/NativePackages/RPMPackages/LINUX/CAeAC*i386.rpm /tmp
cp /mnt/AC_DVD/NativePackages/RPMPackages/pre.tar /tmp
chmod 777 /tmp/CAeAC*i386.rpm
/mnt/AC_DVD/NativePackages/RPMPackages/customize_eac_rpm -w keyword -d /tmp
CAeAC*i386.rpm
```

You can now use the customized package in the /tmp directory to install CA ControlMinder.

Start CA ControlMinder

Assuming you are working in an X Windows environment, invoke CA ControlMinder, verify that it is correctly installed on your system, and perform the following steps to initiate important protection:

1. Open two windows under root (superuser) authority.

2. In either window, enter the command:

   ```
   seload
   ```

   Wait while the seload command starts three CA ControlMinder daemons: Engine, Agent, and Watchdog.

3. After you have started the daemons, go to the other window and enter the command:

   ```
   secons -t+ -tv
   ```

   CA ControlMinder accumulates a file of messages reporting operating system events. The secons -tv command displays the messages on the screen as well.

4. In the first window, where you gave the seload command, enter the following command:

   ```
   who
   ```

   Watch the second window, where CA ControlMinder is writing the trace messages, to see whether CA ControlMinder intercepts the execution of the who command and reports on it. CA ControlMinder is correctly installed on your system if it reports interception of the who command.

5. If you want, enter more commands to see how CA ControlMinder reacts to them.

   The database does not yet contain any rules for blocking access attempts. Nevertheless, CA ControlMinder monitors the system so that you can see how the system behaves with CA ControlMinder installed and running, and which events CA ControlMinder intercepts.

6. Shut down the seosd daemon, by entering the following command:

   ```
   secons -s
   ```

   The following message displays on the screen:

   ```
   CA ControlMinder is now DOWN !
   ```

Register a UNIX Host in Active Directory

To let users defined in Active Directory log in to UNIX computers, register on the Active Directory server each UNIX computer on which you installed UNAB.

Note: You can configure the UNAB installation parameters file to specify that the installation process registers the UNIX endpoint on Active Directory during UNAB installation.

Follow these steps:

1. Verify that the time on the UNIX host and Active Directory server is synchronized.
2. Log in to the UNIX computer as a superuser.

   Note: You must activate UNAB before Active Directory users can log on to the UNIX computer.

3. If you use Microsoft Services for UNIX (SFU), specify the attribute names in the map section of the uxauth.ini file.

   If you do not specify the attribute names in the uxauth.ini file, users that are defined only in SFU cannot log in to UNAB hosts.

   Note: For more information about the uxauth.ini file, see the *Reference Guide*.

4. Navigate to the UNAB bin directory. By default the directory is:

   `/opt/CA/uxauth/bin`

5. Run the uxconsole -register utility.

   UNAB registers the UNIX computer in Active Directory and starts the uxauthd daemon.

   Note: For more information about uxconsole -register, see the *Reference Guide.*

Example: Register a UNIX Host in Active Directory

This example shows you how to register a UNIX computer in Active Directory. You type in the user name (-a administrator) and password (-w admin), define the Active Directory host name (-d Active_Directory_Host), set the verbosity level (-v 3), specify that the UNAB agent does not run at the end of the installation (-n), and define the name of the container in Active Directory (-o OU=COMPUTERS). The container must exist before you register the UNIX computer in Active Directory:

```
./uxconsole -register -a administrator -w admin -d Active_Directory_Host –v 3 -n -o
OU=COMPUTERS
```

Example: Delegating an Active Directory User the Privileges to Register a UNIX Host

If you do not want to specify an administrator user name and password when you run the uxconsole -register command, you can specify the user name and password of a user with delegated privileges for registering the UNIX host in Active Directory. The following example shows you how to delegate the privileges for registering a UNIX host in Active Directory to an Active Directory user.

1. On the Active Directory computer, click Start, Programs, Administrative Tools, Active Directory Users and Computers.

   The Active Directory Users and Computers management console opens.

2. Right-click the Computers folder and select Delegate Control.

   The Delegation Control Wizard opens.

3. Click Next.

   The wizard starts.

4. Complete the installation wizard using the following table, and click Finish:

Information	Action
Users and Groups	Specifies the user to which you want to delegate control to. Select Add and search for the user you want to delegate control to.
Tasks to Delegate	Defines the tasks to delegate to the selected users or groups. Select "Create a custom task to delegate"
Active Directory Object Type	Defines the scope of the task to delegate. Do the following: ■ Select "This folder, existing objects in this folder, and creation of new objects in this folder". ■ Select "Create Computer objects permission from the list".
Permissions	Defines the permissions to delegate to the user. Select "Creation/delegation of specific child objects ".

The wizard closes.You have delegated permission to create computer objects in Active Directory to the user. The user now has sufficient privileges to register a UNIX host in Active Directory.

Activate UNAB

After you have registered the UNIX host in Active Directory, you need to activate UNAB. Activation is the final step in the implementation process of UNAB. Once UNAB is activated it authenticates users based on their Active Directory password.

Follow these steps:

1. Log in to the UNIX computer as a superuser.
2. Navigate to the UNAB bin directory. By default the directory is:

   `/opt/CA/uxauth/bin`

3. Run the following command:

   ```
   ./uxconsole -activate
   ```

   -activate

   Specifies that login is activated for Active Directory users

   UNAB is activated

Note: Activating UNAB lets local users that have an Active Directory account to continue logging into the UNIX host.

Note: For more information about the uxconsole utility, see the *Reference Guide*.

Example: Login to UNAB after activation

The following example shows you how you can log in to a UNIX computer using an Active Directory account after you installed UNAB in partial mode and registered it.

1. Open a terminal window.
2. Connect to the UNIX host:

   ```
   telnet computer.com
   ```

   You are connected to the UNIX computer and a UNIX shell opens.
3. Enter the user name and password of an Active Directory account.

   If successful, a message is displayed, informing you of your last login details.

Start UNAB

For users from Active Directory log into the UNIX computer, start up UNAB.

Follow these steps:

1. Log in to the UNIX computer as a superuser.
2. Locate the UNAB lbin directory.
3. Enter the following command:

   ```
   ./uxauthd.sh start
   ```

   The UNAB daemon starts.

Copyright