Configuring Primary Authentication

This section includes the following topics:

Primary Authentication

Prime Network Services Controller supports three methods to authenticate user logins:

- Local to Prime Network Services Controller
- Remote through LDAP
- Remote through TACACS+

The role and locale assignments for a local user can be changed on Prime Network Services Controllername-network-controller. The role and locale for a remote user can be changed on LDAP. If any of the following information assigned to a user is modified, the administrator must delete all existing sessions of that user so that the new privileges take effect:

- Role
- Privilege for a role
- Locale
- Organization in a locale

Note For the Cisco PNSC, Release 3.4.2c, only the **admin** and **read-only** roles are supported.

Remote Authentication Providers

If a system is configured for a supported remote authentication service, you must create a provider for that service to ensure that Prime Network Services Controller and the system configured with the service can communicate.

User Accounts in Remote Authentication Services

You can create user accounts in Prime Network Services Controller or in the remote authentication server.

The temporary sessions for users who log in through remote authentication services can be viewed through the Prime Network Services Controller GUI.

User Roles and Locales in Remote Authentication Services

If you create user accounts in the remote authentication server, you must ensure that the accounts include the roles and locales those users require for working in Prime Network Services Controller and that the names of those roles and locales match the names used in Prime Network Services Controller. If an account does not have the required roles and locales, the user is granted only read-only privileges.

LDAP Attribute for User

In Prime Network Services Controller, the LDAP attribute that holds the LDAP user roles and locales is preset. This attribute is always a name-value pair. For example, by default CiscoAvPair specifies the role and locale information for the user, and if the filter is specified, the LDAP search is restricted to those values that match the defined filter. By default, the filter is sAMAccountName=$userid. The user can change these values to match the setting on the LDAP server. When a user logs in, Prime Network Services Controller checks for the value of the attribute when it queries the remote authentication service and validates the user. The value should be identical to the username.

An example of LDAP property settings is as follows:

- Timeout—30
- Retries—1
- Attribute—CiscoAvPair
- Filter—sAMAccountName=$userid
- Base DN—DC=cisco, DC=com (The specific location in the LDAP hierarchy where Prime Network Services Controller starts the query for the LDAP user.)

TACACS+ Attribute for User

In TACACS+ Server, while defining a user, to specify Authorization Level following Attribute-Value pair can be defined for the group the user belongs to:

Role—Attribute with name "role" and value should have one of the roles defined in PNSC

Note For 3.4.2c release we support "admin" and "read-only" roles.

For example:

- In ACS server Custom Attributes can be defined in Shell Profiles and it should be linked to the Group for the user under the Authorization rules for Default Device Admin.
- In a Linux based server it would require an attribute value pair to be defined in the Group assigned to the user in the config file.

```
group = GRP1 {
service = PNSC {
role = "admin"
}
}
```

Note TACACS+ support is available from PNSC 3.4.2c onwards.

Creating an LDAP Provider

Before you begin

Configure users with the attribute that holds the user role and locale information for . You can use an existing LDAP attribute that is mapped to the user roles and locales, or you can create a custom attribute, such as the CiscoAVPair attribute, which has an attribute ID of 1.3.6.1.4.1.9.287247.1. When you add the LDAP user to the LDAP server, specify the role and locale in the attribute (for example, shell:roles=network,aaa shell:locale=sanjose,dallas).

SUMMARY STEPS

1. Choose **Administration > Access Control > LDAP**.
2. In the content pane, click **Create LDAP Provider**.
3. In the Create LDAP Provider dialog box, provide the following information: then click **OK** and **Save**.

DETAILED STEPS

Step 1 Choose **Administration > Access Control > LDAP**.

Step 2 In the content pane, click **Create LDAP Provider**.

Step 3 In the Create LDAP Provider dialog box, provide the following information: then click **OK** and **Save**.

Field	Description
Hostname/IP Address	Hostname or IP address of the LDAP provider. If SSL is enabled, this field must match a Common Name (CN) in the security certificate of the LDAP database. **Note** If you use a hostname instead of an IP address, you must configure a DNS server in the server.
Key	Password for the LDAP database account specified in the Root DN field. The maximum is 32 characters.

Field	Description
Root DN	Distinguished Name (DN) for an LDAP database account that has read and search permissions for all objects under the base DN. The maximum supported string length is 127 characters.
Port	Port through which communicates with the LDAP database. The default port number is 389.
Enable SSL	Check to enable SSL.

Example

Following is an example of creating an LDAP provider:

- **Hostname/IP Address**—Provider-blr-sam-aaa-10.cisco.com
- **Key**—xxxxxx (The password of the LDAP database account specified in the **Root DN** field.)
- **Root DN**— CN=bob,DC=cisco,DC=com (The value of CN is the name of a user with query privileges. DC refers to the location in the LDAP directory where a user is created.)
- **Port**—389
- **Enable SSL**—check box

What to do next

Select LDAP as the primary authentication service. For more information, see Selecting a Primary Authentication Service, on page 8.

Editing an LDAP Provider

SUMMARY STEPS

1. Choose **Administration > Access Control > LDAP** > *ldap-adapter*, then click **Edit**.
2. In the Edit dialog box, modify the settings as as described in the following table, then click **OK** and **Save**.

DETAILED STEPS

Step 1 Choose **Administration > Access Control > LDAP** > *ldap-adapter*, then click **Edit**.

Step 2 In the Edit dialog box, modify the settings as as described in the following table, then click **OK** and **Save**.

Field	Description
Name	Hostname or IP address of the LDAP provider (read-only). If SSL is enabled, this field must match a Common Name (CN) in the security certificate of the LDAP database. **Note** Ensure proper DNS resolution is configured for the host name and DNS server configured in the PNSC.
Key	Password for the LDAP database account specified in the Root DN field. The maximum is 32 characters.
Set	Whether or not the preshared key has been set and is properly configured (read-only). If the Set value is Yes, and the Key field is empty, it indicates that a key was provided previously.
Root DN	Distinguished Name (DN) for an LDAP database account that has read and search permissions for all objects under the base DN. The maximum supported string length is 127 characters.
Port	Port through which communicates with the LDAP database. The default port number is 389.
Enable SSL	Check to enable SSL.

Deleting an LDAP Provider

SUMMARY STEPS

1. Choose **Administration > Access Control > LDAP >***ldap-provider*, then click **Delete**.
2. Confirm the deletion, then click **Save**.

DETAILED STEPS

Step 1 Choose **Administration > Access Control > LDAP >***ldap-provider*, then click **Delete**.

Step 2 Confirm the deletion, then click **Save**.

Creating a TACACS+ Provider

Before you begin

Configure users with the Group and attribute-value pairs that holds the user role information. You can use an existing TACACS+ Group that is mapped to the user roles or you can create a custom attribute-value pair. Make sure that you have configured the TACACs+ services on your AAA server and have a shared secret key. Some AAA servers such as Cisco ACS require PNSC added as a device in the AAA client configuration section.

Step 1 Choose **Administration > Access Control > TACACS+**.

Step 2 In the content pane, click **Create TACACS+ Provider**.

Step 3 In the Create TACACS+ Provider dialog box, provide the following information, click **OK** and **Save**.

Field	Description
Hostname/IP Address	Hostname or IP address of the TACACS+ provider. **Note** Ensure proper DNS resolution for the host name and DNS server configured in PNSC.
Key	Password for the TACACS+ database account.
Port	Port through which communicates with the TACACS+ server. The default port number is 49.

Example

Following is an example of creating an TACACs+ provider:

- **Hostname/IP Address**—X.X.X.X
- **Key**—xxxxxx (The shared secret password of the TACACS+ server account specified in the **Hostname/IP Address** field.)
- **Port**—49

What to do next

Select TACACS+ as the primary authentication service. For more information, see Selecting a Primary Authentication Service, on page 8.

Editing a TACACS+ Provider

SUMMARY STEPS

1. Choose **Administration > Access Control > TACACS+** > *tacacsPlusProvider*, then click **Edit**.
2. In the Edit dialog box, modify the settings as as described in the following table, then click **OK** and **Save**.

DETAILED STEPS

Step 1 Choose **Administration > Access Control > TACACS+** > *tacacsPlusProvider*, then click **Edit**.

Step 2 In the Edit dialog box, modify the settings as as described in the following table, then click **OK** and **Save**.

Field	Description
Name	Hostname or IP address of the TACACS+ provider (read-only). **Note** If you use a hostname instead of an IP address, you must configure a DNS server in the server.
Key	Password for the TACAS+ database.
Set	Whether or not the preshared key has been set and is properly configured (read-only). If the Set value is Yes, and the Key field is empty, it indicates that a key was provided previously.
Port	Port through which communicates with the TACACS+ database. The default port number is 49.

Deleting an TACACS+ Provider

SUMMARY STEPS

1. Choose **Administration > Access Control > TACACS+ >***tacacsPlusProvider*, then click **Delete**.
2. Confirm the deletion, then click **Save**.

DETAILED STEPS

Step 1 Choose **Administration > Access Control > TACACS+ >***tacacsPlusProvider*, then click **Delete**.

Step 2 Confirm the deletion, then click **Save**.

Selecting a Primary Authentication Service

Note If the default authentication is set to LDAP, and the LDAP servers are not operating or are unreachable, the local admin user can log in at any time and make changes to the authentication, authorization, and accounting (AAA) system.

Step 1 Choose **Administration > Access Control > Authentication**.

Step 2 In the Properties tab, specify the information as described in the following table, then click **OK**.

Field	Description
Default Authentication	Default method by which a user is authenticated during remote login: • LDAP—The user must be defined on the LDAP server specified for this Prime Network Services Controller instance. • Local—The user must be defined locally in this Prime Network Services Controller instance. • None—A password is not required when the user logs in remotely. • TACACS+ - The user must be defined on the TACACS+ server specified for this instance
Role Policy to Remote Users	Action taken when a user attempts to log in and the LDAP server does not supply a user role with the authentication information: • assign-default-role—The user can log in with a read-only user role. • no-login—The user cannot log into the system, even if the user name and password are correct.