



CHAPTER 6

User Management: Configuring User Roles and Local Users

This chapter describes the following topics:

- [Overview, page 6-1](#)
- [Create User Roles, page 6-1](#)
- [Create Local User Accounts, page 6-14](#)

For details on configuring authentication servers, see [Chapter 7, “User Management: Configuring Auth Servers.”](#)

For details on creating and configuring the web user login page and guest users, see [Chapter 5, “Configuring User Login Page and Guest Access.”](#)

For details on configuring traffic policies for user roles, see [Chapter 8, “User Management: Traffic Control, Bandwidth, Schedule.”](#)

Overview

This chapter describes the user role concept in Cisco NAC Appliance. It describes how user roles are assigned and how to create and configure them. It also describes how to create local users that are authenticated internally by the CAM (used primarily for testing).

Create User Roles

Roles are integral to the functioning of Cisco NAC Appliance and can be thought of in the following ways:

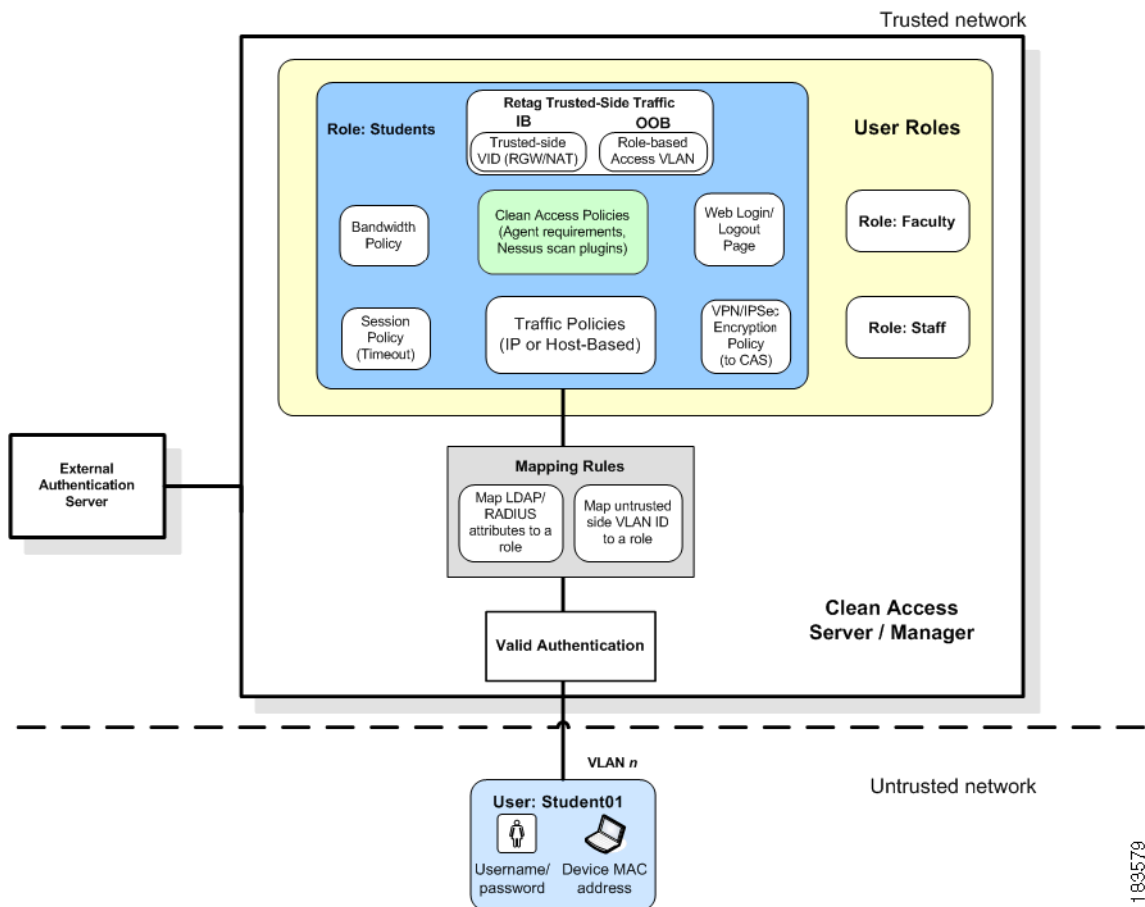
- As a classification scheme for users that persists for the duration of a user session.
- As a mechanism that determines traffic policies, bandwidth restrictions, session duration, Clean Access vulnerability assessment, and other policies within Cisco NAC Appliance for particular groups of users.

In general, roles should be set up to reflect the shared needs of distinct groups of users in your network. Before creating roles, you should consider how you want to allocate privileges in your network, apply traffic control policies, or group types of client devices. Roles can frequently be based on existing groups

within your organization (for example, students/faculty/staff, or engineering/sales/HR). Roles can also be assigned to groups of client machines (for example, gaming boxes). As shown in Figure 6-1, roles aggregate a variety of user policies including:

- Traffic policies
- Bandwidth policies
- VLAN ID retagging
- Clean Access network port scanning plugins
- Clean Access Agent client system requirements

Figure 6-1 Normal Login User Roles



189579

User Role Types

The system puts a user in a role when the user attempts to log in. There are four default user role types in the system: Unauthenticated Role, Normal Login Role, Clean Access Agent Temporary Role, and Clean Access Quarantine Role.

Unauthenticated Role

There is only one Unauthenticated Role and it is the system default role. If a configured normal login role is deleted, users in that role are reassigned to the Unauthenticated Role (see [Delete Role, page 6-14](#)). You can configure traffic and other policies for the Unauthenticated Role, but the role itself cannot be edited or removed from the system.

Users on the untrusted (managed) side of the Clean Access Server are in the Unauthenticated role prior to the initial web login or Clean Access Agent login. When using web login/network scanning only, users remain in the Unauthenticated role until clients pass scanning (and are transferred to a normal login role), or fail scanning (and are either blocked or transferred to the quarantine role).

Normal Login Role

There can be multiple normal login roles in the system. A user is put into a normal login role after a successful login. You can configure normal login roles to associate users with the following:

- Network access traffic control policies — what parts of the network and which application ports can users access while in the role.
- VLAN ID:
 - For in-band users, retag traffic (to/from users in the role) destined to the trusted network to differentiate priority to the upstream router
 - For out-of-band (OOB) users, set the Access VLAN ID for users in the role if using role-based configuration.
- Clean Access network scanning plugins—the Nessus port scanning to perform, if any
- Clean Access Agent requirements—the software package requirements client systems must have.
- End-user HTML page(s) displayed after successful or unsuccessful web logins —the pages and information to show to web login users in various subnets/VLANs/roles. See [Chapter 5, “Configuring User Login Page and Guest Access”](#) for further details.

Typically, there are a number of normal login roles in a deployment, for example roles for Students, Faculty, and Staff (or Engineering, HR, Sales). You can assign normal login roles to users in several ways:

- By the MAC address or subnet of a client device.
You can assign a role to a device or subnet through **Device Management > Filters**. See [Global Device and Subnet Filtering, page 3-7](#) for details.
- By local user attributes. Local users are primarily used for testing and are authenticated internally by the Clean Access Manager rather than an external authentication server. You can assign a role to a local user through **User Roles > Local Users**. See [Create Local User Accounts, page 6-14](#).
- By external authentication server attributes. For users validated by an external authentication server, the role assigned can be based on:
 - The untrusted network VLAN ID of the user.
This allows you to use untrusted network information to map users into a user role.
 - The authentication attributes passed from LDAP and RADIUS authentication servers.
This allows you to use authentication attributes to map different users to different roles within Cisco NAC Appliance. If no mapping rules are specified, users are assigned the default role specified for the authentication server, after login. VLAN mapping and attribute mapping is done through **User Management > Auth Servers > Mapping Rules**.

For details, see [Adding an Authentication Provider, page 7-3](#) and [Map Users to Roles Using Attributes or VLAN IDs, page 7-16](#).

Role Assignment Priority

Note that the order of priority for role assignment is as follows:

1. MAC address
2. Subnet / IP Address
3. Login information (login ID, user attributes from auth server, VLAN ID of user machine, etc.)

Therefore, if a MAC address associates the client with “Role A”, but the user’s login ID associates him or her to “Role B”, “Role A” is used.

For additional details, see also [Global Device and Subnet Filtering, page 3-7](#) and [Device Filters for Out-of-Band Deployment, page 3-11](#).

Clean Access Roles

The Clean Access process can be implemented on your network as network scanning only (see [Figure 9-4 on page 9-5](#)), Clean Access Agent only, or Clean Access Agent with network scanning (see [Figure 9-3 on page 9-4](#)). With Clean Access enabled, two types of roles are used specifically for Clean Access:

- **Clean Access Agent Temporary Role**

When the Clean Access Agent is used, the Clean Access Agent Temporary role is assigned to users after authentication to allow the user limited network access to download and install required packages that will prevent the user’s system from becoming vulnerable. The user is prevented from normal login role access to the network until the Clean Access Agent requirements are met.

There is only one Clean Access Agent Temporary role in the system. This role is only in effect when the user is required to use Clean Access Agent to login and pass Clean Access requirements.

The Clean Access Agent Temporary role is assigned to users for the following time periods:

- a. From the login attempt until successful network access. The client system meets Clean Access Agent requirements and is not found with vulnerabilities after network scanning. The user transfers from the Clean Access Agent Temporary role into the user’s normal login role.
- b. From the login attempt until Clean Access Agent requirements are met. The user has the amount of time configured in the Session Timer for the role to download and install required packages. If the user cancels or times out, the user is removed from the Clean Access Agent Temporary role and must restart the login process. If the user downloads requirements within the time allotted, the user stays in the Clean Access Agent Temporary role and proceeds to network scanning (if enabled).
- c. From the login attempt until network scanning finds vulnerabilities on the user system. If the client system meets Clean Access Agent requirements, but is found to have vulnerabilities during network scanning, the user is transferred from the Clean Access Agent Temporary role into the quarantine role.

- **Quarantine Role**

With network scanning enabled, the purpose of the Clean Access quarantine role is to allow the user limited network access to resources needed to fix vulnerabilities that already exist on the user system. The user is prevented from normal login role access to the network until the vulnerabilities are fixed.

There can be one or multiple quarantine roles in the system. A user is put into a quarantine role if:

- The user attempts to log in using the web login page, and Clean Access network scanning finds a vulnerability on the user system.
- The user logs in using Clean Access Agent and meets Clean Access Agent requirements but Clean Access network scanning finds a vulnerability on the user system.

The user has the amount of time configured in the Session Timer for the role to access resources to fix vulnerabilities. If the user cancels or times out, the user is logged out of the quarantine role and must restart the login process. At the next login attempt, the client again goes through the Clean Access process.

When the user fixes vulnerabilities within the time allotted, if Clean Access Agent is used to log in, the user can go through network scanning again during the same session. If web login is used, the user must log out or time out then login again for the second network scanning to occur.



Note

When using web login, the user should be careful not to close the Logout page (see [Figure 5-11 on page 5-15](#)). If the user cannot not log out but reattempts to login before the session times out, the user is still considered to be in the original quarantine role and is not redirected to the login page.

Only when the user has met requirements and fixed vulnerabilities is the user allowed network access in the corresponding normal login role. You can map all normal login roles to a single quarantine role, or you can create and customize different quarantine roles. For example, multiple quarantine roles can be used if different resources are required to fix vulnerabilities for particular operating systems. In either case, a normal login role can only be mapped to one quarantine role. After the roles are created, the association between the normal role and quarantine role is set up in the **Device Management > Clean Access > General Setup** form. See [General Setup Overview, page 9-16](#) for details.

Session Timeouts

You can limit network access for Clean Access roles with brief session timeouts and restricted traffic policy privileges. The session timeout period is intended to allow users only a minimum amount of time to complete Clean Access checks and get required software packages. A minimal timeout period for Clean Access-related roles:

- Limits the exposure of vulnerable users to the network.
- Prevents users from full network access in the Temporary role
This is to limit users from circumventing rechecks if they fail a particular check, install the required package, restart their computers, but do not manually log out.

Factors in determining the timeout period appropriate for your environment include the network connection speed available to users and the download size of packages you will require.

You can additionally configure a Heartbeat Timer to log off all users if the CAS cannot connect to the clients after a configurable number of minutes. See [Configure User Session and Heartbeat Timeouts, page 8-15](#) for further details.

You can configure **Max Sessions per User Account** for a user role. This allows administrators to limit the number of concurrent machines that can use the same user credentials. The feature allows you to restrict the number of login sessions per user to a configured number. If the online login sessions for a username exceed the value specified (1 – 255; 0 for unlimited), the web login page or the Clean Access Agent will prompt the user to end all sessions or end the oldest session at the next login attempt. See [Role Properties, page 6-8](#) for details.

Default Login Page

A default login page must be added and present in the system in order for both the web login and Clean Access Agent users to authenticate.

The login page is generated by Cisco NAC Appliance and is shown to end users by role. When users first try to access the network from a web browser, an HTML login page appears prompting the users for a user name and password. Cisco NAC Appliance submits these credentials to the selected authentication provider and uses them to determine the role in which to put the user. You can customize this web login page to target the page to particular users based on a user's VLAN ID, subnet, and operating system.



Caution

If a default login page is not present, Clean Access Agent users will see an error dialog when attempting login (“Clean Access Server is not properly configured, please report to your administrator.”).



Note

For L3 OOB deployments, you must also [Enable Web Client for Login Page, page 5-5](#).

For details on creating and configuring the web user login page, see [Chapter 5, “Configuring User Login Page and Guest Access.”](#) To quickly add a default login page, see [Add Default Login Page, page 5-3](#).

Traffic Policies for Roles

When you first create a role, it has a default traffic filtering policy of “deny all” for traffic moving from the untrusted side to the trusted side, and “allow all” for traffic from the trusted side to the untrusted side. Therefore, after creating the role, you need to create policies to permit the appropriate traffic. See [Chapter 8, “User Management: Traffic Control, Bandwidth, Schedule”](#) for details on how to configure IP-based and host-based traffic policies for user roles.

In addition, traffic policies need to be configured for the Clean Access Agent Temporary Role and the quarantine role to prevent general access to the network but allow access to web resources or remediation sites necessary for the user to meet requirements or fix vulnerabilities. See [Configure Policies for Agent Temporary and Quarantine Roles, page 8-18](#) for details.

Add New Role

The Clean Access Agent Temporary role and a Quarantine role already exist in the system and only need to be configured. However, normal login roles (or any additional quarantine roles) must first be added. Once a new role is created, it can then be associated to the traffic policies and other properties you customize in the web console for your environment.



Note

For new roles, traffic policies must be added to allow traffic from the untrusted to the trusted network. See [Chapter 8, “User Management: Traffic Control, Bandwidth, Schedule”](#) next for details.

1. Go to **User Management > User Roles > New Role** ([Figure 6-2](#)).

Figure 6-2 Add New User Role

User Management > User Roles

List of Roles | **New Role** | Traffic Control | Bandwidth | Schedule

Disable this role

Role Name:

Role Description:

Role Type: Normal Login Role

*VPN Policy: Deny

*Dynamic IPsec Key: Enable Disable

*Max Sessions per User Account (Case-Insensitive): (1 - 255; 0 for unlimited)

Retag Trusted-side Egress Traffic with VLAN (In-Band): (0 - 4095, or leave it blank)

*Out-of-Band User Role VLAN: VLAN ID (if left blank, it will default to the default access vlan settings in the Port Profile)

*Bounce Switch Port After Login (OOB): Enable Disable (This option is effective only when port profile is set to use it)

*Refresh IP After Login (OOB): Enable Disable (This option only applies to L2 OOB Virtual Gateway with Role VLAN as Access VLAN and switch port is NOT bounced after VLAN change)

*After Successful Login Redirect to: previously requested URL this URL: (e.g. http://www.cisco.com/)

Redirect Blocked Requests to: default access blocked page this URL or HTML message:

*Roam Policy: Deny Allow

*Show Logged-on Users: IPsec info PPP info User info Logout button

(*only applies to normal login role)

2. If you want the role to be active right away, leave **Disable this role** cleared.
3. Type a unique name for the role in the **Role Name** field.
4. Type an optional **Role Description**.
5. For the role type, choose either:
 - **Normal Login Role** – Assigned to users after a successful login. When configuring mapping rules for authentication servers, the attributes passed from the auth server are used to map users into normal login roles. Network scan plugins and Clean Access Agent requirements are also associated to a normal login role. When users log in, they are scanned for plugins and/or requirements met (while in the unauthenticated/Temporary role). If users meet requirements and have no vulnerabilities, they gain access to the network in the normal login role.



Note Form fields that only apply to normal login roles are marked with an asterisk (*).

- **Quarantine Role** – Assigned to users to quarantine them when Clean Access network scanning finds a vulnerability on the user system. Note that a system Quarantine role already exists and can be configured. However, the New Role form allows you to add additional quarantine roles if needed.

6. See [Role Properties](#), page 6-8 for configuration details on each role setting.



Note If planning to use role-based profiles with an OOB deployment, you must specify the Access VLAN in the **Out-of-Band User Role VLAN** field when you create the user role. For further details see [Out-of-Band User Role VLAN](#), page 6-10 and [Add Port Profile](#), page 4-25.

7. When finished, click **Create Role**. To restore default properties on the form click **Reset**.
8. The role now appears in the **List of Roles** tab.
9. If creating a role for testing purposes, the next step is to create a local user to associate to the role. See [Create Local User Accounts](#), page 6-14 next.

Role Properties

[Table 6-1](#) details all the settings in the **New Role** ([Figure 6-2](#)) and **Edit Role** ([Figure 6-4](#)) forms.

Table 6-1 *Role Properties*

Control	Description
Disable this role	Stops the role from being assigned to new users.
Role Name	A unique name for the role.
Role Description	An optional description for the role.
Role Type	Whether the role is a Normal Login Role or a Clean Access-related role: Quarantine Role or Clean Access Agent Temporary Role . See User Role Types , page 6-2 for details, and Chapter 9, “Clean Access Implementation Overview” for further information.

Table 6-1 Role Properties (continued)

Control	Description
VPN Policy	<p>Note IPsec/L2TP/PPTP and roaming are deprecated and will be removed in future releases.</p> <p>Whether users in the role and authenticated by the provider are required to use IPsec/L2TP/PPTP encryption for connection to the CAS. Options are:</p> <ul style="list-style-type: none"> • Deny (default)– Encryption is not permitted. If this level of security is not required for your environment, you can deny IPsec/L2TP/PPTP encryption to avoid burdening the network infrastructure with traffic. • Optional – Encryption may be used at the client’s choice. • Enforce – The client must use IPsec/L2TP/PPTP encryption. <p>Note The IPsec/L2TP/PPTP encryption policy must also be enabled (Optional or Enforce) on the CAS (Device Management > CCA Servers > Manage [CAS_IP] > Network > IPsec). The CAS policy setting takes precedence over the role policy setting. This allows you to control encryption use based on which CAS (or subnet) the user accessed. See the Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(1) for details.</p> <p>Note If an Optional or Enforce VPN Policy is enabled for both CAS and user role, the Clean Access Agent displays VPN information as a link from the login success dialog (see Figure 11-72 on page 11-65). For web login users, you must configure the logout page to display VPN information fields (see Show Logged-on Users, page 6-12).</p>
Dynamic IPsec Key	<p>If enabled, each user is assigned a distinct, one-time preshared key upon logging in. The user should use this key as the preshared key in their IPsec client to create the IPsec connection. If disabled, the user will need to use the default key (shared by all users) for the IPsec connection. Web login users are given the key in the logout page if you select IPsec info in Show Logged-on Users, page 6-12.</p>
Max Sessions per User Account (Case-Insensitive)	<p>The Max Sessions per User Account option allows administrators to limit the number of concurrent machines that can use the same user credentials. The feature allows you to restrict the number of login sessions per user to a configured number. If the online login sessions for a username exceed the value specified (1 – 255; 0 for unlimited), the web login page or the Clean Access Agent will prompt the user to end all sessions or end the oldest session at the next login attempt.</p> <p>The Case-Insensitive checkbox allows the administrator to allow/disallow case-sensitive user names towards the max session count. For example, if the administrator chooses to allow case-sensitivity (box unchecked; default), then jdoe, Jdoe, and jDoe are all treated as different users. If the administrator chooses to disable case-sensitivity (box checked), then jdoe, Jdoe, and jDoe are treated as the same user.</p>

Table 6-1 Role Properties (continued)

Control	Description
Retag Trusted-side Egress Traffic with VLAN (In-Band)	<p>Note This feature is deprecated and will be removed in future releases.</p> <p>In-Band Configuration—Retag Trusted-side Traffic with VLAN ID</p> <p>When the CAS is deployed inline with traffic, the value entered in this field is used to retag user traffic as it exits the trusted side of the CAS. For example, if two users connect to the same Access Point with the same SSID, depending on their roles, their traffic can be tagged with different VLAN IDs as their traffic flows through the CAS to the trusted side of the network (see Figure 6-1 on page 6-2).</p> <p>Type a value in this field to assign a VLAN ID to outgoing traffic from users in the role. Incoming traffic with the VLAN ID value is reassigned the value originally used by the role, if any. For in-band configuration, trusted-side VLAN retagging is only performed in Real-IP and NAT Gateway modes. In-band Virtual Gateways do not perform VLAN retagging based on role assignment.</p>
Out-of-Band User Role VLAN	<p>Out-of-Band (OOB) Configuration —Retag Trusted-side Traffic with Role VLAN</p> <p>Once a user has finished posture assessment and remediation, if needed, and the client device is deemed to be “certified,” the switch port to which the client is connected can be assigned to a different Access VLAN based on the value specified in the Out-of-Band User Role VLAN field. Hence, users connecting to the same port (at different times) can be assigned to different Access VLANs based on this setting in their user role.</p> <p>For OOB deployment, if configuring role-based VLAN switching for a controlled port, you must specify an Access VLAN ID when you create the user role. When an out-of-band user logs in from a managed switch port, the CAM will:</p> <ul style="list-style-type: none"> • Determine the role of the user based on the user's login credentials. • Check if role-based VLAN switching is specified for the port in the Port Profile. • Switch the user to the Access VLAN, once the client is certified, according to the value specified in the Out-of-Band User Role VLAN field for the user's role. <p>Admins can specify VLAN Name or VLAN ID on the New/Edit User Role form. VLAN Name is case-sensitive. If specifying wildcards for VLAN Name, you can use: abc, *abc, abc*, *abc*. The switch will use the first match for wildcard VLAN Name.</p> <p>You can only specify numbers for VLAN ID</p> <p>If the switch cannot find the VLAN specified (e.g. VLAN Name is mistyped), the error will appear on the perfigo.log (not the Event Log).</p> <p>For additional details, see Global Device and Subnet Filtering, page 3-7 and Chapter 4, “Switch Management: Configuring Out-of-Band (OOB) Deployment.”</p>
Bounce Switch Port After Login (OOB)	<p>If you have first enabled the “Bounce the port based on role settings after VLAN is changed” option on the Switch Management > Profiles > Port > New/Edit page, the Agent does <i>not</i> renew the IP address on the client machine after login and posture assessment.</p> <p>Note This option only applies when a port profile is configured to use it.</p>

Table 6-1 Role Properties (continued)

Control	Description
Refresh IP After Login (OOB)	<p>If you have first enabled the “Bounce the port based on role settings after VLAN is changed” option on the Switch Management > Profiles > Port > New/Edit page, the switch port through which the user is accessing the network is not bounced when the VLAN changes from authentication to access VLAN. Instead, if you have enabled this feature, the Agent renews/refreshes the IP address on the client machine following login and posture assessment.</p> <p>Note This option only applies to a Virtual Gateway CAS operating in Layer 2 OOB mode.</p>
After Successful Login Redirect to	<p>When successfully logged in, the user is forwarded to the web page indicated by this field. You can have the user forwarded to:</p> <ul style="list-style-type: none"> • previously requested URL – (default) The URL requested by the user before being redirected to the login page. • this URL– To redirect the user to another page, type “http://” and the desired URL in the text field. Note that “http://” must be included in the URL. <p>Note Typically, a new browser is opened when a redirect page is specified. If pop-up blockers are enabled, Cisco NAC Appliance will use the main browser window as the Logout page in order to show login status, logout information and VPN information (if any). See also Redirect the Login Success Page, page 5-14.</p>
Redirect Blocked Requests to	<p>If the user is blocked from accessing a resource by a “Block” IP traffic policy for the role, users are redirected when they request the blocked page. You can have the user forwarded to:</p> <ul style="list-style-type: none"> • default access blocked page – The default page for blocked access. • this URL or HTML message– A particular URL or HTML message you specify in the text field. <p>See also Adding Traffic Policies for Default Roles, page 8-26.</p>

Table 6-1 Role Properties (continued)

Control	Description
Roam Policy	<p>Note IPsec/L2TP/PPTP and roaming are deprecated and will be removed in future releases.</p> <p>With roaming support enabled, determines whether users in this role are allowed to roam. See Chapter 16, “Device Management: Roaming (Deprecated)” for details.</p>
Show Logged-on Users	<p>The information that should be displayed to web users in the Logout page. After the web user successfully logs in, the Logout page pops up in its own browser and displays user status based on the combination of options you select:</p> <ul style="list-style-type: none"> • IPsec info – The IPsec key assigned to the user. If the dynamic IPsec key option is enabled, this is the one-time, 128-bit key. If disabled, this is the default preshared key. • PPP info – The password for PPP access on the network. • User info – Information about the user, such as the user name. • Logout button – A button for logging the user off the network (web Logout page only). <p>See Specify Logout Page Information, page 5-15 for an example of a Logout page.</p> <p>Note For Agent users, a link to a VPN Info dialog is provided in the success login and taskbar menu if an Optional or Enforce VPN Policy is enabled for both the CAS and user role. See Figure 11-72 on page 11-65.</p>

Modify Role

From the **List of Roles** tab ([Figure 6-3](#)), you can configure traffic and bandwidth policies for any user role. You can also edit the Clean Access Agent Temporary role, Quarantine role, and any normal login role you have created.

Figure 6-3 List of Roles

Role Name	IPsec	Roam	VLAN	Description	Policies	BW	Edit	Del
Unauthenticated Role	deny	deny		Role for unauthenticated users				
Temporary Role	deny	deny		Role for users to download requirements				
Quarantine Role	deny	deny		Role for quarantined users				
role1	deny	deny	:500					

Operations you can perform from the **List of Roles** tab are as follows:

- The **Policies** button links to the **Traffic Control** tab and lets you set traffic filter policies for the role. For details, see [Chapter 8, “User Management: Traffic Control, Bandwidth, Schedule.”](#)

- The **BW** button links to the **Bandwidth** tab and lets you set upstream and downstream bandwidth restrictions by role. For details, see [Control Bandwidth Usage, page 8-13](#).
- The **Edit** button links to the **Edit Role** tab and lets you modify role properties. See [Edit a Role, page 6-13](#) below.
- The **Delete** button removes the role and all associated polices from the system and assigns users to the Unauthenticated role. See [Delete Role, page 6-14](#).
- Specify a network access schedule for the role. For details, see [Configure User Session and Heartbeat Timeouts, page 8-15](#).

Edit a Role

1. Go to **User Management > User Roles > List of Roles**.
2. Roles listed will include the following:
 - **Clean Access Agent Temporary Role** – Assigned to users to force them to meet Clean Access Agent packages or requirements when Clean Access Agent is required to be used for login and Clean Access vulnerability assessment. There is only one Clean Access Agent Temporary Role which is already present in the system. This role can be edited but not added.
 - **Quarantine Role** – Assigned to users to quarantine them when Clean Access network scanning finds a vulnerability on the user system. You can configure the system Quarantine role only or add additional quarantine roles if needed.
 - **User-defined role** – The user roles you have created.



Note You can configure traffic and bandwidth policies for the **Unauthenticated Role**, but otherwise this system default role cannot be edited or removed.

3. Click the **Edit** button next to a role to bring up the **Edit Role** form

Figure 6-4 Edit Role

User Management > User Roles

List of Roles Edit Role Traffic Control Bandwidth Schedule

Disable this role

Role Name

Role Description

Role Type

*VPN Policy

*Dynamic IPSec Key Enable Disable

*Max Sessions per User (1 - 255; 0 for unlimited)

Account Case-Insensitive

Retag Trusted-side Egress Traffic with VLAN (In-Band)

*Out-of-Band User Role VLAN (if left blank, it will default to the default access vlan settings in the Port Profile)

*Bounce Switch Port After Login (OOB) Enable Disable (This option is effective only when port profile is set to use it)

*Refresh IP After Login (OOB) Enable Disable (This option only applies to L2 OOB Virtual Gateway with Role VLAN as Access VLAN and switch port is NOT bounced after VLAN change)

*After Successful Login Redirect to previously requested URL

this URL: (e.g. http://www.cisco.com/)

Redirect Blocked Requests to default access blocked page

this URL or HTML message:

*Roam Policy Deny Allow

*Show Logged-on Users IPSec info PPP info

User info Logout button

(*only applies to normal login role)

183863

4. Modify role settings as desired. See [Role Properties](#), page 6-8 for details.
5. Click **Save Role**.

Delete Role

To delete a role, click the **Delete** button next to the role in the **List of Roles** tab of the **User Management > User Roles** page. This removes the role and associated polices from the system and assigns users to the Unauthenticated role.

Users actively connected to the network in the deleted role will be unable to use the network. However, their connection will remain active. Such users should be logged off the network manually, by clicking the **Kick User** button next to the user in the **Monitoring > Online Users > View Online Users** page. The users are indicated in the online user page by a value of **Invalid** in the **Role** column.

Create Local User Accounts

A local user is one who is validated by the Clean Access Manager itself, not by an external authentication server. Local user accounts are not intended for general use (the users cannot change their password outside of the administrator web console). Local user accounts are primarily intended for testing or for guest user accounts. For testing purposes, a user should be created immediately after creating a user role.

Create a Local User

1. Go to **User Management > Local Users > New Local User**.

Figure 6-5 New Local User

User Management > Local Users

List of Local Users | **New Local User**

Disable this account

User Name

Password

Confirm Password

Description

Role

163860

2. If you want the user account to be active immediately, be sure to leave the **Disable this account** check box cleared.
3. Type a unique **User Name** for the user. This is the login name by which the user is identified in the system.
4. Type a password in the **Password** field and retype it in the **Confirm Password** field. The password value is case-sensitive.
5. Optionally, type a **Description** for the user.
6. Choose the default role for the user from the **Role** list. All configured roles appear in the list. If the role you want to assign the user does not exist yet, create the role in the **User Roles** page and modify the user profile with the new role.
7. When finished, click **Create User**.

The user now appears in the **List of Local Users** tab. From there, you can view user information, edit user settings such as the name, password, role, or remove the user.

