User Management: Configuring User Roles and Local Users

This chapter describes the following topics:

- Overview, page 6-1
- Create User Roles, page 6-2
- Create Local User Accounts, page 6-15

For details on configuring authentication servers, see Chapter 7, “User Management: Configuring Authentication 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).

Cisco NAC Appliance network protection features are configured for users by role and operating system. The following roles are employed when users are in the Cisco NAC Appliance network (i.e. during the time they are In-Band) and must be configured with traffic policies and session timeout:

- **Unauthenticated Role**—Default system role for unauthenticated users (Agent or web login) behind a Clean Access Server. Web login users are in the unauthenticated role while network scanning is performed.

- **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.

- **Client Posture Assessment Roles** (Agent Temporary Role and Quarantine Role)—Agent users are in the Temporary role while Agent Requirements are checked on their systems. Both web login and Agent users are put in the Quarantine role when network scanning determines that the client machine has vulnerabilities.

Note that the Temporary and Quarantine roles are intended to have limited session time and network access in order for users to fix their systems.
When a user authenticates, either through the web login page or Agent, Cisco NAC Appliance determines the normal login role of the user and the requirements and/or network scans to be performed for the role. Cisco NAC Appliance then performs requirement checking and/or network scanning as configured for the role and operating system.

Note that while the role of the user is determined immediately after the initial login (in order to determine the scans or system requirements associated with the user), a user is not actually put into a normal login role until requirements are met, scanning has occurred and no vulnerabilities are found. If the client has not met requirements, the user stays in the Agent Temporary role until requirements are met or the session times out, including when the user reboots his/her client machine as part of a remediation step (if the required application installation process requires you to restart your machine, for example) and the Logoff NAC Agent users from network on their machine logoff or shutdown after <x> secs option in the CAM Device Management > Clean Access > General Setup > Agent Login web console page has not been enabled. If the user has met requirements but is found with network scanning vulnerabilities, the user can be assigned to a quarantine role or simply blocked, depending on the configuration.

**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, posture 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
- Cisco NAC Appliance network port scanning plugins
- Agent client machine requirements
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, Agent Temporary role, and 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 6-15). 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 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 (including “restricted access” 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.
- Cisco NAC Appliance network scanning plugins—the Nessus port scanning to perform, if any.
- 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 2-10 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 6-15.
- 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 7-4 and Map Users to Roles Using Attributes or VLAN IDs, page 7-30.

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.)
Chapter 6      User Management: Configuring User Roles and Local Users

Create User Roles

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 2-10 and Device Filters for Out-of-Band Deployment, page 2-14.

Client Posture Assessment Roles

You can implement client posture assessment in Cisco NAC Appliance as network scanning only (see Figure 12-1 on page 12-2), Agent only, or Agent with network scanning. With posture assessment configured, two types of roles are used specifically for Cisco NAC Appliance:

- **Agent Temporary Role**

  When the Agent is used, the 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 Agent requirements are met.

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

  The 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 Agent requirements and is not found with vulnerabilities after network scanning. The user transfers from the Agent Temporary role into the user’s normal login role.

  b. From the login attempt until 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 Agent Temporary role and must restart the login process. If the user downloads Agent requirements within the time allotted, the user stays in the Agent Temporary role and proceeds to network scanning (if enabled).

  If the user reboots his/her client machine as part of a remediation step (if the required application installation process requires you to restart your machine, for example), and the Logoff NAC Agent users from network on their machine logoff or shutdown after \( <x> \) secs option in the CAM Device Management > Clean Access > General Setup > Agent Login web console page has not been enabled, the client machine remains in the Temporary role until the Session Timer expires and the user is given the opportunity to perform login/remediation again.

  c. From the login attempt until network scanning finds vulnerabilities on the user system. If the client system meets Agent requirements, but is found to have vulnerabilities during network scanning, the user is transferred from the Agent Temporary role into the quarantine role.

- **Quarantine Role**

  With network scanning enabled, the purpose of the Agent 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 network scanning finds a vulnerability on the user system.
Create User Roles

- The user logs in using the Agent and meets requirements but 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 posture assessment.

When the user fixes vulnerabilities within the time allotted, if the 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 5-16). 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 Client Login Overview, page 1-7 for details.

**Session Timeouts**

You can also limit network access 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 posture assessment and remediation. A minimal timeout period for client posture assessment-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 Agent will prompt the user to end all sessions or end the oldest session at the next login attempt. See Role Properties, page 6-9 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 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 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, 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 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 8-19 for details.

Adding a New User Role

The Agent Temporary role and a Quarantine role already exist in the Cisco NAC Appliance system and only need to be configured to meet your specific network needs. 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” for details.

Step 1

Go to User Management > User Roles > New Role (Figure 6-2).
Create User Roles

**Figure 6-2** Add New User Role

<table>
<thead>
<tr>
<th>User Management &gt; User Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>List of Roles</td>
</tr>
</tbody>
</table>

- **Disable this role**
- **Role Name**
- **Role Description**
- **Role Type**
  - Normal Login Role
- **Max Sessions per User Account**
  - Off-Campus Users: **0** (0 - 255; 0 for unlimited)
- **Mac Address Egress Traffic with VLAN (In-Band)**
  - (0 - 4095; or leave it blank)
- **Out-of-Band User Role VLAN**
  - VLAN ID: **0** (If left blank, it will default to the default access VLAN settings in the Port Profile)
- **Bounce Switch Port After Login (OOB)**
  - **Enable**
- **Refresh IP After Login (OOB)**
  - **Enable**
- **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:
- **Show Logged-on Users**
  - **User info**
  - **Logout button**
- **Enable Passive Re-assessment**
  - To enable Passive Re-assessment for OOB Agent connections, you must also enable the OOB Logoff option in Device Management > Clean Access > General Setup > Agent Login.
- **Re-assessment Interval**
  - **10** (Minimum of 1 hour and maximum of 24 hours. Specified in minutes)
- **Grace Timer**
  - **5** (Minimum of 5 minutes and maximum of 60 minutes)
- **Default action on failure**
  - **Continue**

**Step 2** If you want the role to be active right away, leave **Disable this role** cleared.

**Step 3** Type a unique name for the role in the **Role Name** field.

**Step 4** Type an optional **Role Description**.

**Step 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 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 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.

**Step 6**

See Role Properties, page 6-9 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 3-34.

**Step 7**

When finished, click **Create Role**. To restore default properties on the form click **Reset**.

**Step 8**

The role now appears in the **List of Roles** tab.

**Step 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 6-15 next.

---

### Role Properties

Table 6-1 details all the settings in the **New/Edit Role** (Figure 6-2) form.

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable this role</td>
<td>Stops the role from being assigned to new users.</td>
</tr>
<tr>
<td>Role Name</td>
<td>A unique name for the role.</td>
</tr>
<tr>
<td>Role Description</td>
<td>An optional description for the role.</td>
</tr>
<tr>
<td>Role Type</td>
<td>Whether the role is a <strong>Normal Login Role</strong> or a client posture assessment-related role: <strong>Quarantine Role</strong> or <strong>Agent Temporary Role</strong>. See User Role Types, page 6-3 for details.</td>
</tr>
<tr>
<td>Max Sessions per User Account (Case-Insensitive)</td>
<td>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 Agent will prompt the user to end all sessions or end the oldest session at the next login attempt. 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.</td>
</tr>
<tr>
<td>Retag Trusted-side Egress Traffic with VLAN (In-Band)</td>
<td><strong>Note</strong> This feature is deprecated and will be removed in future releases.</td>
</tr>
</tbody>
</table>
### Table 6-1  Role Properties (continued)

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Out-of-Band User Role VLAN</strong></td>
<td><strong>Out-of-Band (OOB) Configuration — Retag Trusted-side Traffic with Role VLAN</strong></td>
</tr>
<tr>
<td></td>
<td>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 <strong>Out-of-Band User Role VLAN</strong> 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. 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:</td>
</tr>
<tr>
<td></td>
<td>• Determine the role of the user based on the user’s login credentials.</td>
</tr>
<tr>
<td></td>
<td>• Check if role-based VLAN switching is specified for the port in the Port Profile.</td>
</tr>
<tr>
<td></td>
<td>• Switch the user to the Access VLAN, once the client is certified, according to the value specified in the <strong>Out-of-Band User Role VLAN</strong> field for the user’s role.</td>
</tr>
<tr>
<td></td>
<td>Admins can specify <strong>VLAN Name</strong> or <strong>VLAN ID</strong> on the New/Edit User Role form. <strong>VLAN Name</strong> is case-sensitive. If specifying wildcards for VLAN Name, you can use: abc, <em>abc, abc</em>, <em>abc</em>. The switch will use the first match for wildcard VLAN Name. You can only specify numbers for <strong>VLAN ID</strong>. 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). For additional details, see Global Device and Subnet Filtering, page 2-10 and Chapter 3, “Switch Management: Configuring Out-of-Band Deployment.”</td>
</tr>
<tr>
<td><strong>Bounce Switch Port After Login (OOB)</strong></td>
<td>If you have first enabled the <strong>Bounce the port based on role settings after VLAN is changed</strong> option on the OOB Management &gt; Profiles &gt; Port &gt; New/Edit page, the Agent does not renew the IP address on the client machine after login and posture assessment.</td>
</tr>
<tr>
<td><strong>Refresh IP After Login (OOB)</strong></td>
<td>When enabled, the switch port through which the user is accessing the network is not bounced when the VLAN changes from the Authentication VLAN to the Access VLAN. Instead, the Agent renews/refreshes the IP address on the client machine following login and posture assessment. This option only applies when the Port profile is configured to <strong>Bounce the port based on role settings after VLAN is changed</strong> under OOB Management &gt; Profiles &gt; Port &gt; New/Edit (see Add Port Profile, page 3-34). See DHCP Release/Renew with Agent/ActiveX/Java Applet, page 5-6 for additional information on configuring client IP refresh/renew.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This option only applies when a port profile is configured to use it.</td>
</tr>
<tr>
<td></td>
<td>For information on Access to Authentication VLAN change detection for an OOB client machine, see Configure Access to Authentication VLAN Change Detection, page 3-69.</td>
</tr>
</tbody>
</table>
### Table 6-1  Role Properties (continued)

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>After Successful Login Redirect to</td>
<td>When successfully logged in, the user is forwarded to the web page indicated by this field. You can have the user forwarded to:</td>
</tr>
<tr>
<td></td>
<td>• <strong>previously requested URL</strong> – (default) The URL requested by the user before being redirected to the login page.</td>
</tr>
<tr>
<td></td>
<td>• <strong>this URL</strong> – 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.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>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).</td>
</tr>
<tr>
<td></td>
<td>See also <a href="#">Redirect the Login Success Page, page 5-15</a>.</td>
</tr>
<tr>
<td>Redirect Blocked Requests to</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• <strong>default access blocked page</strong>—The default page for blocked access.</td>
</tr>
<tr>
<td></td>
<td>• <strong>this URL or HTML message</strong>—A particular URL or HTML message you specify in the text field.</td>
</tr>
<tr>
<td></td>
<td>See also <a href="#">Adding Traffic Policies for Default Roles, page 8-27</a>.</td>
</tr>
</tbody>
</table>
### Table 6-1 Role Properties (continued)

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
</table>
| Show Logged-on Users     | 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:  
  - **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).  
  See [Specify Logout Page Information, page 5-16](#) for an example of a Logout page. |
|                          | **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. |
Enable Passive Re-assessment

This option allows periodic re-assessment on client systems that are online to ensure continuous compliance of the current network policies. This option is disabled by default.

Passive Re-assessment enables the persistent Agent (Cisco NAC Agent) on the client machine to periodically verify that the client machine is still compliant with imposed network security policies without requiring the user to log out of Cisco NAC Appliance and go through posture assessment to “regain” network access.

Note For OOB deployment, you must enable the Out-of-Band Logoff function in order to enforce Passive Re-assessment. See Configure Out-of-Band Logoff, page 9-6 for details.

Note Passive Re-assessment is available for NAC Agent 4.8.0.32 or later only.

Note While using Passive Re-assessment, the client should communicate with the same CAS that authenticated the user.

- **Re-assessment Interval**—The time interval in minutes between the completion of login process and the first re-assessment, and between consecutive re-assessment attempts on the client machine. The timer starts once the login is completed successfully. The time can vary from 60 minutes (1 hour) to 1440 minutes (24 hours). The default value is 240 minutes (4 hours).

- **Grace Timer**—The time in minutes for which the Agent waits for the users to remediate any failed posture checks, when the Default action on failure option has been set to Allow user to remediate. The time can vary from 5 minutes to 30 minutes. The default value is 5 minutes.

- **Default action on failure**—Select the default action to be performed if the re-assessment fails:
  - **Continue**—The user can continue using the network. No interaction is required by the user with the agent. This is the selected by default.
  - **Allow user to remediate**—The user is prompted for remediation when there is a failure in any of the optional or mandatory requirements. If the user cancels the remediation, then the CAM receives a failed requirement report from the client machine performing Passive Re-Assessment.
  - **Logoff user immediately**—The user is logged out immediately when any of the mandatory requirements fails, and placed back to the unauthenticated network.

The CAM/CAS keep track of the Passive Re-assessment reports and save failed reports, which can be viewed using the Clean Access Agent Report Viewer. If the servers do not receive any report from the Agent within a time interval, then the user is removed from the on-line user list. The maximum time interval for which the server waits is **Re-assessment Interval + 2 x Grace Timer**.
Modifying an Existing Temporary, Quarantine, or Login 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 Agent Temporary role, Quarantine role, and any normal login role you have created.

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

- The Policies icon 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 icon 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 icon links to the Edit Role tab and lets you modify role properties. See Editing an Existing Role, page 6-14 below.

- The Delete icon removes the role and all associated policies from the system and assigns users to the Unauthenticated role. See Delete Role, page 6-15.

- Specify a network access schedule for the role. For details, see Configure User Session and Heartbeat Timeouts, page 8-15.

Editing an Existing Role

Step 1  Go to User Management > User Roles > List of Roles.

Step 2  Roles listed will include the following:

- **Temporary Role**—Assigned to users to force them to meet Agent packages or requirements when Agent is required to be used for login and posture assessment. There is only one 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 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.
Step 3  Click the **Edit** icon next to a role to bring up the **Edit Role** form. An Edit Role window similar to that in Figure 6-2 appears.

Step 4  Modify role settings as desired. See **Role Properties, page 6-9** for details.

Step 5  Click **Save Role**.

---

**Delete Role**

To delete a role, click the **Delete** icon 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 or Edit a Local User**

Step 1  Go to **User Management > Local Users > Local Users** and:

- Choose the **New** subtab option.
- Choose the **List** subtab option and click the **Edit** icon for the user you want to update.
Create Local User Accounts

Chapter 6  User Management: Configuring User Roles and Local Users

Create Local User Accounts

Figure 6-4  New Local User

Step 2 If you want the user account to be active immediately, be sure to leave the Disable this account check box cleared.

Step 3 Type a unique User Name for the user. This is the login name by which the user is identified in the system.

Step 4 Type a password in the Password field and retype it in the Confirm Password field. The password value is case-sensitive.

Step 5 Optionally, type a Description for the user.

Step 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.

Step 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.