



CHAPTER 13

Configuring Network Scanning



Note

Nessus-based network scanning capabilities only apply to web login users and Clean Access Agent users for whom a combination of client network scanning and Agent login functionality has been configured. The Cisco NAC Agent does not support Nessus-based network scanning.

This chapter describes how to set up network scanning for Cisco NAC Appliance. Topics include:

- [Overview, page 13-1](#)
- [User Page Summary, page 13-4](#)
- [Configure the Quarantine Role, page 13-6](#)
- [Load Nessus Plugins into the Clean Access Manager Repository, page 13-6](#)
- [Configure General Setup, page 13-9](#)
- [Apply Plugins, page 13-10](#)
- [Configure Plugin Options, page 13-12](#)
- [Configure Vulnerability Handling, page 13-13](#)
- [Test Scanning, page 13-16](#)
- [Customize the User Agreement Page, page 13-19](#)
- [View Scan Reports, page 13-17](#)

Overview

The Cisco NAC Appliance network scanner uses Nessus plugins to check for security vulnerabilities. With Cisco NAC Appliance, you can define automatic, immediate responses to scan results. For example, if a vulnerability is found, you can have the user notified, blocked from the network, or assigned to a quarantine role.

Nessus (<http://www.nessus.org>), an open source project for security-related software, provides plugins designed to test for specific vulnerabilities on a network. In addition to plugins for remotely detecting the presence of particular worms, plugins exist for detecting peer-to-peer software activity or web servers. The following description defines Nessus plugins:

Nessus plugins are very much like virus signatures in a common virus scanner application. Each plugin is written to test for a specific vulnerability. These can be written to actually exploit the vulnerability or just test for known vulnerable software versions. Plugins can be written in most any

language but usually are written in the Nessus Attack Scripting Language (NASL). NASL is Nessus' own language, specifically designed for vulnerability test writing. Each plugin is written to test for a specific known vulnerability and/or industry best practices. NASL plugins typically test by sending very specific code to the target and comparing the results against stored vulnerable values.

— Anderson, Harry. “Introduction to Nessus” October 28, 2003

<http://www.securityfocus.com/infocus/1741> (10/29/04).

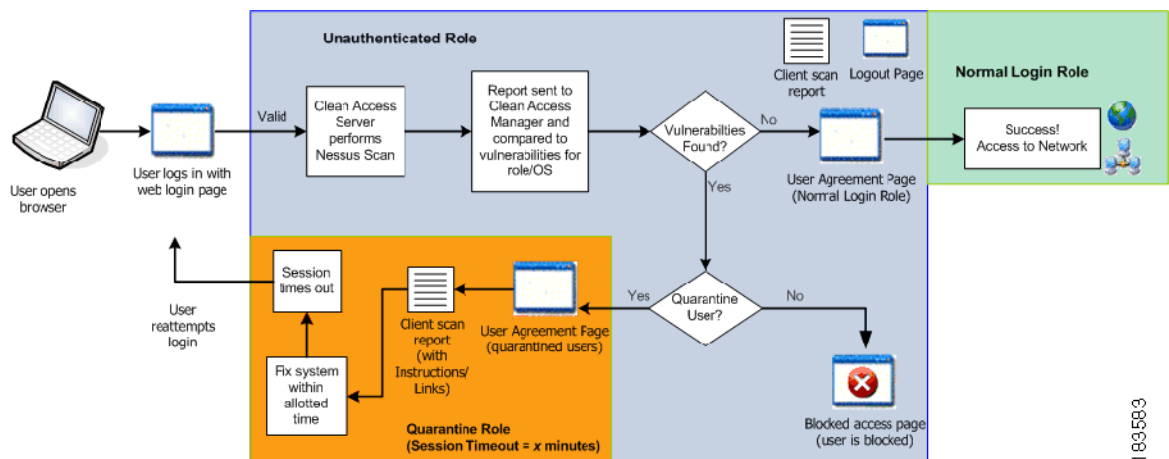
You can use most standard Nessus plugins with Cisco NAC Appliance. You can also customize plugins or create your own using NASL. Refer to the Nessus website for information on how to create plugins using NASL.

When scanning is performed, the network scanner scans the client system according to the plugins you selected and generates a standard report to the Clean Access Manager containing the results of the scan. Network scanning reports will indicate whether the plugin resulted in a security hole, warning, or system information (according to how the Nessus plugin was written). The Clean Access Manager then interprets the report by comparing the result of the plugin to the vulnerability definition you have configured for it. If the report result matches the result you have configured as a vulnerability, the event is logged under **Monitoring > Event Logs > View Logs**, and you can also configure the following options:

- Show the result of the scan to the user.
- Block the user from the network
- Put the user in the quarantine role for limited access until the client system is fixed.
- Warn the user of the vulnerability (with the User Agreement Page).

Figure 13-1 illustrates the general network scanning client assessment process when a user authenticates via web login. If both the Agent and network scanning are enabled for a user role, the user follows the sequence shown in Figure 11-37 on page 11-26 then in Figure 13-1 for the network scanning portion. In this case, the Agent dialogs provide the user information where applicable.

Figure 13-1 Network Scanning Client Assessment



Network Scanning Implementation Steps

The following sections describe the steps required to set up network scanning:

Step 1 [Configure the Quarantine Role, page 13-6](#)

- Step 2** [Load Nessus Plugins into the Clean Access Manager Repository, page 13-6](#)
 - Step 3** [Configure General Setup, page 13-9](#)
 - Step 4** [Apply Plugins, page 13-10](#)
 - Step 5** [Configure Plugin Options, page 13-12](#)
 - Step 6** [Configure Vulnerability Handling, page 13-13](#)
 - Step 7** [Test Scanning, page 13-16](#)
 - Step 8** [Customize the User Agreement Page, page 13-19](#)
 - Step 9** [View Scan Reports, page 13-17](#)
-

User Page Summary

Table 13-1 summarizes the web pages that appear to users during the course of login and perform Nessus Scanning, and lists where they are configured in the web admin console.

Table 13-1 User Page Summary

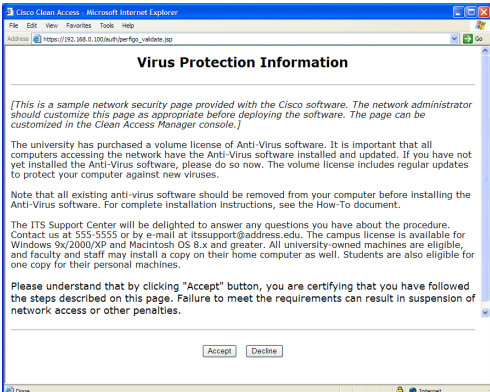
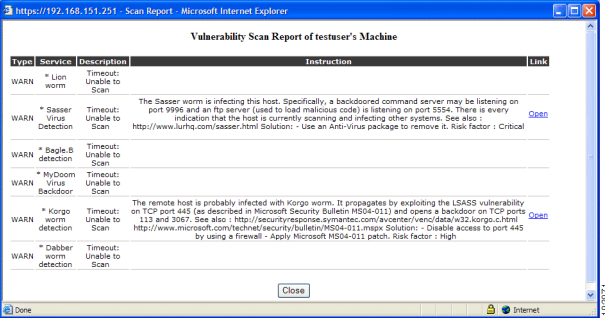
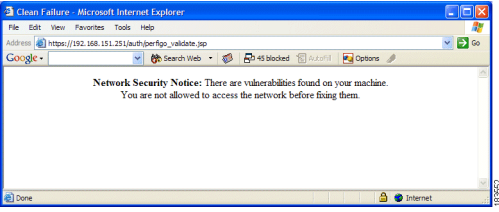
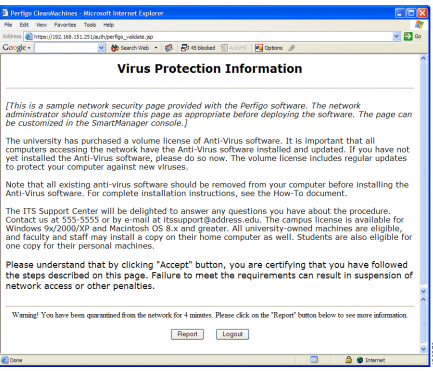
Page	Configured in:	Purpose
Web Login /Network Scanner User Pages		
Network Scanning User Agreement Page	Enable in: Device Management > Clean Access > General Setup > Web Login Configure page in: Device Management > Clean Access > Network Scanner > Scan Setup > User Agreement See Customize the User Agreement Page, page 13-19	If enabled, this page appears after a web login user authenticates and passes network scanning. The user must click Accept to access the network. 
Scan Vulnerability Report	Enable in: Device Management > Clean Access > General Setup > Web Login Configure page in: Device Management > Clean Access > Network Scanner > Scan Setup > Vulnerabilities See Configure Vulnerability Handling, page 13-13	If enabled, this client report appears to web login users after network scanning results in vulnerabilities. It can also be accessed as a link from the Logout page. Administrators can view the admin version of the client report from Device Management > Clean Access > Network Scanner > Reports . Agent users with network scanning vulnerabilities see this information in the context of Agent dialogs. The report appears as follows: 

Table 13-1 User Page Summary (continued)

Page	Configured in:	Purpose
Block Access Page	<p>Device Management > Clean Access > General Setup > Web Login</p> <p>See Customize the User Agreement Page, page 13-19.</p>	<p>If enabled, a web login user sees this page if blocked from the network when vulnerabilities are found on the client system after network scanning,</p> 
User Agreement Page: quarantined user, original role	<p>Enable in:</p> <p>Device Management > Clean Access > General Setup > Web Login</p> <p>Configure page in:</p> <p>Network Scanner > Scan Setup > User Agreement</p> <p>Select normal login role.</p> <p>See Customize the User Agreement Page, page 13-19.</p>	<p>If enabled, this page appears to a web login user if quarantined when vulnerabilities are found on the client system after network scanning.</p>  <p>This page has the same Information Page Message (or URL) contents (“Virus Protection Information”) as the User Agreement Page for the normal login role. However, the Acknowledgment Instructions are hardcoded to include the Session Timeout for the original role, and button labels are hardcoded as “Report” and “Logout”.</p>
User Agreement Page: quarantined user, quarantine role	<p>Enable in: Device Management > Clean Access > General Setup > Web Login</p> <p>Configure page in: Network Scanner > Scan Setup > User Agreement</p> <p>Select appropriate quarantine role.</p> <p>See Customize the User Agreement Page, page 13-19.</p>	<p>If enabled, this page appears to a web login user if quarantined when vulnerabilities are found on the client system after network scanning.</p> <p>This page allows you to specify a User Agreement Page just for the quarantine role, (as opposed to using the quarantine version of the User Agreement Page for the normal login role, as described above). The Acknowledgment Instructions are hardcoded to include the Session Timeout for the quarantine role, and the button labels are also hardcoded as “Report” and “Logout”.</p>

For additional information on redirecting users by role to specific pages or URLs (outside of Cisco NAC Appliance), see [Create Local User Accounts](#), page 7-13.

For additional Cisco NAC Appliance configuration information, see [Configure General Setup](#), page 13-9.

For additional details on configuring Agent Requirements, see [Configuring Agent-Based Posture Assessment](#), page 10-33.

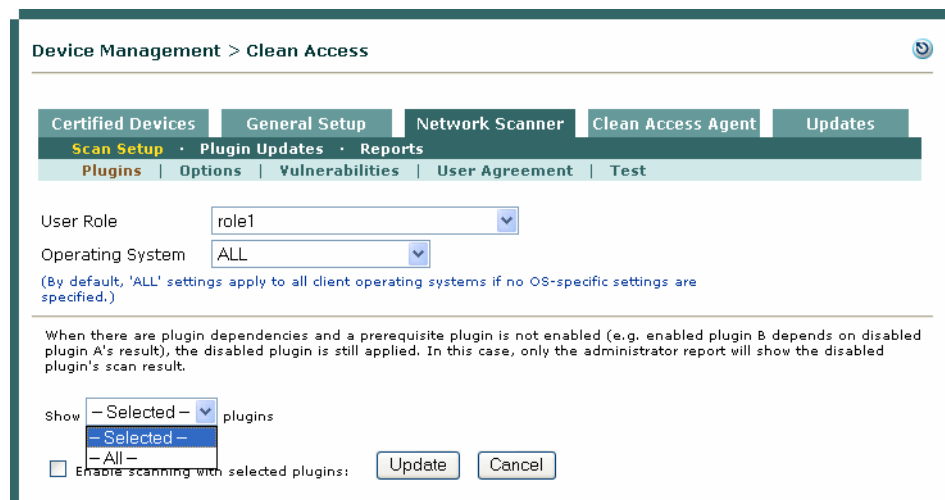
Configure the Quarantine Role

See [Configure Network Scanning Quarantine Role](#), page 9-21 for details.

Load Nessus Plugins into the Clean Access Manager Repository

When the Clean Access Manager is first installed, its Nessus scan plugin repository is empty ([Figure 13-2](#)). Plugins in the repository are listed under **Device Management > Clean Access > Network Scanner > Scan Setup > Plugins**. You can manually load plugins you have downloaded from the Nessus website—as a combined **plugins.tar.gz** file or as individual **.nasl** files—to the Clean Access Manager's plugin repository. You can also load **.nasl** plugins that you have created yourself.

Figure 13-2 Network Scanner Plugins Page



Note

Due to a licensing requirement by Tenable, Cisco is not able to bundle pre-tested Nessus plugins or automated plugin updates to Cisco NAC Appliance, effective Release 3.3.6/3.4.1. Customers can still download Nessus plugins selectively and manually through <http://www.nessus.org>. For details on Nessus plugin feeds, see <http://www.nessus.org/plugins/index.php?view=feed>. To facilitate the debugging of manually uploaded plugins, see [Show Log](#), page 13-17.



Note

Most Nessus 2.2 plugins are supported and can be uploaded to the Clean Access Manager. You must register for Nessus 2.2 plugins from <http://www.nessus.org/plugins/index.php?view=register>. Once you register, you will be able to download the free plugins. Nessus version 2.2.7 has a NASL_LEVEL value of less than 3004. Cisco NAC appliance does not support Nessus plugins which require the NASL_LEVEL to be equal to or greater than 3004. Cisco NAC Appliance currently does not support Nessus version 3 plugins due to vendor licensing restrictions.

If a plugin you want to add has dependent plugins, you must load those dependencies or the plugin is not applied. When customizing a plugin, Cisco recommends giving the plugin a unique name, so that it is not overwritten later by a plugin in a Nessus update set.

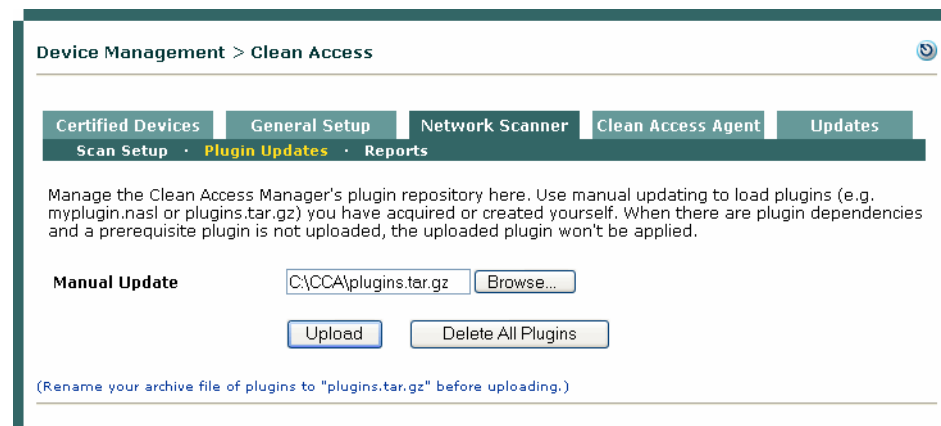
The plugin's description appears in the **Plugins** form of the **Scan Setup** submenu (Figure 13-4 on page 13-8). By customizing the plugin's description, you enable admin console users to distinguish the plugin from others in the plugin set.

Plugins that you have loaded are automatically published from the Clean Access Manager repository to the Clean Access Servers, which perform the actual scanning. The CAM distributes the plugin set to the Clean Access Servers as they start up, if the CAS version of the plugin set differs from the CAM version.

Uploading Plugins

1. Go to **Device Management > Clean Access > Network Scanner > Plugin Updates**.

Figure 13-3 Plugin Updates



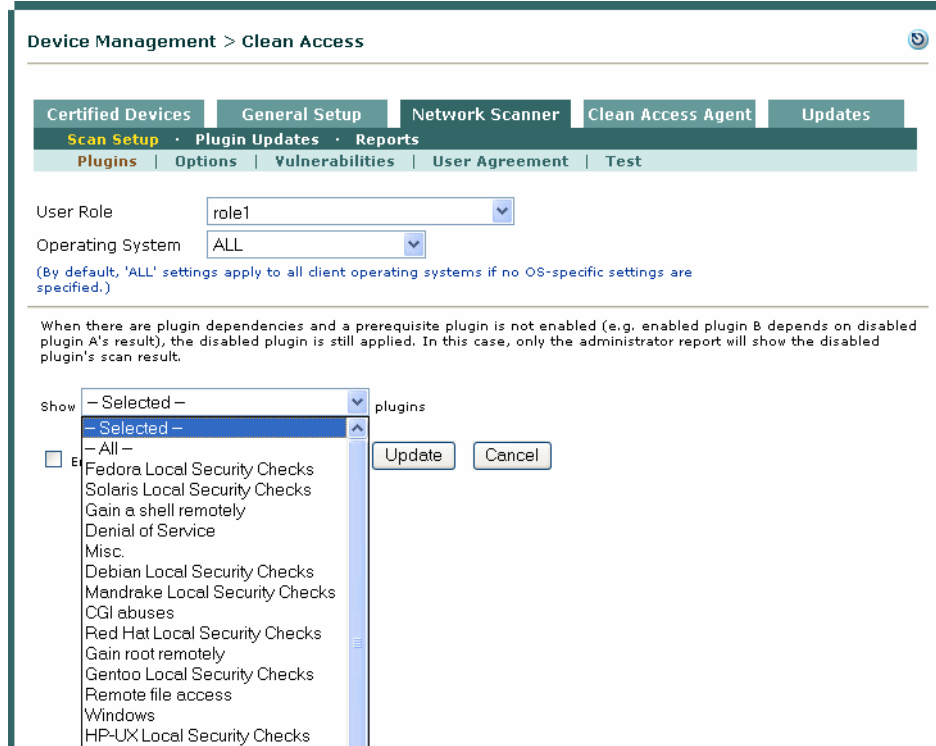
2. With the plugin file in a location accessible to the computer on which you are working, click the **Browse** button next to the **Manual Update** field and navigate to the plugin archive file (**plugins.tar.gz**) or individual plugin file (**myplugin.nasl**).



Note The filename of the uploaded nessus plugin archive must be **plugins.tar.gz**. Most Nessus 2.2 plugins are supported. Nessus version 2.2.7 has a NASL_LEVEL value of less than 3004. Cisco NAC appliance does not support Nessus plugins which require the NASL_LEVEL to be equal to or greater than 3004. Cisco NAC Appliance currently does not support Nessus version 3 plugins due to vendor licensing restrictions.

3. Click **Upload**.
4. The list of plugins loaded to the repository displays under **Network Scanner > Scan Setup > Plugins** (Figure 13-4).

Figure 13-4 Plugins Page After Upload

**Note**

The default view on the **Plugins** page is “Selected.” If Nessus plugins have not yet been checked and updated for the user role, the default view (i.e. Selected Plugins) shows no plugins. To view the plugins you have uploaded, choose one of the other views (for example, “All,” “Backdoors,” etc.) from the “Show...Plugins” dropdown.

5. If the plugins do not immediately display after **Upload**, click **Delete All Plugins**, then perform the upload again.
6. Apply the plugin and configure its parameters as described in the following sections:
 - [Apply Plugins, page 13-10](#)
 - [Configure Vulnerability Handling, page 13-13.](#)

**Note**

When there are plugin dependencies and a prerequisite plugin is not uploaded, the uploaded plugin will not be applied.

Deleting Plugins

1. Go to **Device Management > Clean Access > Network Scanner > Plugin Updates**.
2. Click the **Delete All Plugins** button to remove all plugins from the repository. The **Network Scanner > Scan Setup > Plugins** page will no longer be populated.

Configure General Setup

After loading the scan plugins, you can configure scanning by user role and operating system. Before starting, make sure user roles appropriate for your environment are created.

The General Setup page provides general controls to configure user roles and operating systems for network scanning, including whether user agreement or scan report pages pop up, and whether a client is blocked or quarantined if found with vulnerabilities.

To configure network scanning user page options:

1. Go to **Device Management > Clean Access > General Setup > Web Login**.

Figure 13-5 General Setup—Web Login

Device Management > Clean Access

Certified Devices | **General Setup** | Network Scanner | Clean Access Agent | Updates

Web Login · Agent Login

User Role: Role2

Operating System: ALL

(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)

Show **Network Scanner User Agreement page** to web login users Link to User Agreement Page Configuration Form

Enable pop-up scan vulnerability reports from User Agreement page

Require users to be certified at every web login

Exempt certified devices from web login requirement by adding to MAC filters

Block/Quarantine users with [vulnerabilities](#) in role: Quarantine Role (4 minutes)

Show quarantined users User Agreement Page of: quarantine role

Update Cancel

183648

2. Choose the role for which you want to configure scanning from the **User Role** dropdown.
3. Similarly, choose the user operating system to which the configuration applies from the **Operating System** dropdown. You can apply settings to all versions of an OS platform (such as WINDOWS_ALL), or to a specific operating system version (such as WINDOWS_XP). ALL settings will apply to a client system if a configuration for the specific version of that user's operating system does not exist.

If providing specialized settings, select the operating system and clear the checkbox for the ALL setting (for example, deselect “Use 'ALL' settings for the WINDOWS OS family if no version-specific settings are specified”).

4. Enable the network scanning options:
 - **Show Network Scanner User Agreement page to web login users**
 - **Enable pop-up scan vulnerability reports from User Agreement page**
 - **Require users to be certified at every web login**—this forces clients to go through network scanning at each login (otherwise, clients go through scanning only the first time they log in.)

- **Exempt certified devices from web login requirement by adding to MAC filters**—(Optional) this allows users that have met network scanning requirements to bypass web login altogether by adding the MAC address of their machines to the device filters list.
 - **Block/Quarantine users with vulnerabilities in role**—either:
 - Select the quarantine role in which to quarantine the user, or
 - Select block access to block the user from the network and modify the contents (if desired) of the blocked access page that will appear.
5. When finished, click **Update** to save your changes to the user role.

For additional details, see [Client Login Overview, page 1-6](#) and [Customize the User Agreement Page, page 13-19](#).

Apply Plugins

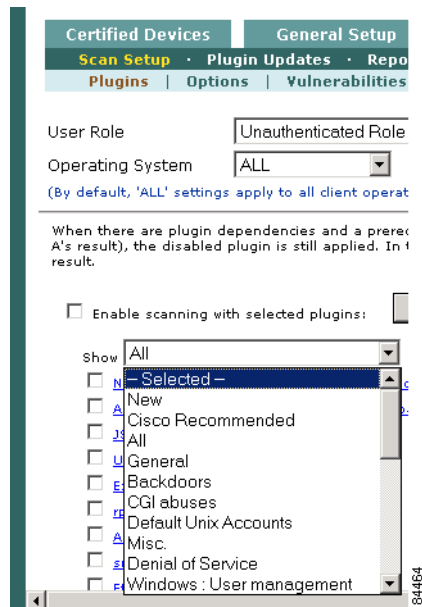
Select the Nessus plugins to be used to determine client vulnerabilities from the **Plugins** page. Select the user role and operating system and choose the plugins that participate in scanning.

To apply scanning plugins:

1. Go **Network Scanner > Scan Setup > Plugins**.

Figure 13-6 *Plugins*

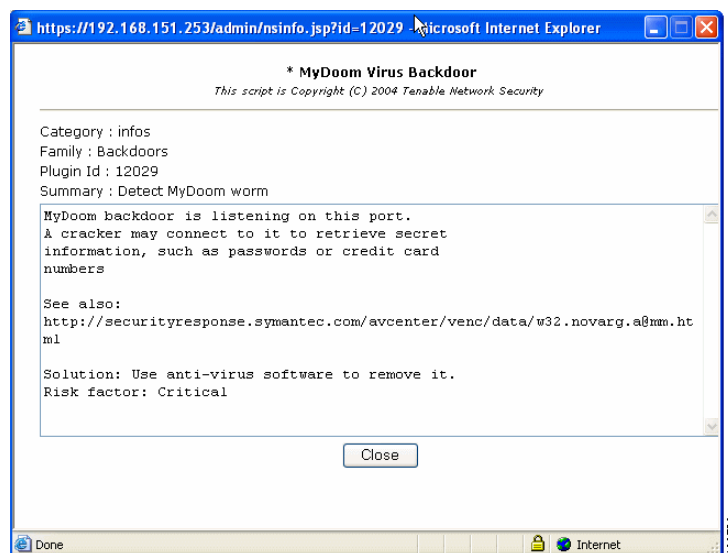
2. In the form, select a **User Role** and **Operating System**, and check the **Enable scanning with selected plugins** check box.
3. If you have many plugins in the repository, you can filter which are displayed at a time by choosing a plugin family from the plugins list, as shown below.
 - Selecting **All** displays all plugins in the repository.
 - Choosing **- Selected-** displays only the plugins you already chose and enabled for the role.

**Note**

The default view on the Nessus plugin page (**Device Management > Clean Access > Network Scanner > Scan Setup > Plugins**) is “Selected.” Note that if Nessus plugins have not yet been checked and updated for the user role, the default view (i.e. Selected Plugins) shows no plugins. To select plugins, the administrator must choose one of the other views (for example, “All,” “Backdoors,” etc.) from the “Show...Plugins” dropdown.

4. Click the plugin name for details. An information dialog appears for each plugin (Figure 13-7).

Figure 13-7 Nessus Plugin Description



5. Select the check box for each plugin that you want to participate in the scan for that role.

**Note**

If the plugin is dependent on other plugins in the repository, those plugins are enabled automatically.

- When finished, click **Update**. This transfers the selected plugins to the **Vulnerabilities** page so that you can configure how these vulnerabilities are handled if discovered on a client system.

If the plugin has configurable parameters, you can now use the **Options** form to configure them, as described in the following procedures. Otherwise you can continue to [Configure Vulnerability Handling, page 13-13](#).

Configure Plugin Options

For plugins that support input parameters, you can configure parameters in the **Options** form. Before starting, the plugin must be enabled in the **Plugins** form, as described in [Apply Plugins, page 13-10](#).

To configure plugin options:

- In the **Network Scanner** tab, click the **Scan Setup** submenu link, then open the **Options** form.
- With the appropriate role and operating system selected, choose the plugin you want to configure from the **Plugin** list. All plugins enabled for the role appear in the list.
- Choose the option you want to configure for the plugin from the options list. When you select a configurable option, **Category**, **Preference Name**, and **Preference Value** dropdowns and/or text boxes will display, as applicable for the option. Parameters that cannot be configured are indicated by a “Not supported” message.

Figure 13-8 Options

Device Management > Clean Access

Certified Devices | General Setup | Network Scanner | Clean Access Agent | Updates

Scan Setup | Plugin Updates | Reports

Plugins | Options | Vulnerabilities | User Agreement | Test

User Role: role1

Operating System: ALL

(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)

Category: Services

Preference Name: Network connection timeout:

Preference Value: 5

Update Cancel

183851

- From the dropdown menus, select the **Category** and **Preference Name**, type the **Preference Value** (if applicable), and click **Update**. Note that you need to click **Update** for each parameter you configure.

**Note**

Cisco recommends using the Agent for host registry checks. In order to use Nessus Windows registry checks, you will need to have a common account (with access to the registry) on all the machines you want to check. This can be configured under **Device Management > Clean Access > Network Scanner > Scan Setup > Options** | Category: **Login configurations** | Preference Name: **[SMB account/domain/password]**. For details on Nessus 2.2 Windows registry checks (requiring credentials), refer to http://www.nessus.org/documentation/nessus_credential_checks.pdf.

Configure Vulnerability Handling

If scanning uncovers a vulnerability on the user's system, the user can be blocked from the network, quarantined, or only warned about the vulnerability.

Network scan reports are listed by user logon attempt under **Device Management > Clean Access > Network Scanner > Reports**. Client scan reports can be enabled by selecting the **Enable pop-up scan vulnerability reports from User Agreement page** option from **Device Management > Clean Access > General Setup**.

If enabled, a client scan report will appear in a popup window to notify users if a vulnerability result was found. This client report is a subset of the scan report and lists only vulnerability results along with instruction steps or a URL link that guide the user through remediation for the vulnerability. If browser popups are blocked on the user's system, the user can click the **Scan Report** link on the logout page to view the report. The warning text that appears to users for each vulnerability is configurable, as described in the following procedures.

Note that typically, plugins do not return results when no issue is found. If a client goes through network scanning and no vulnerability results are found, no scan report popup is displayed.

To configure how vulnerabilities are handled:

1. Open the **Network Scanner > Scan Setup > Vulnerabilities** form.
2. Select a **User Role** and **Operating System**. Note that plugins selected apply to the User Role:OS pair. The same set of plugins appears for all operating systems in the role. However, you can customize which plugins are considered vulnerabilities per operating system.

Figure 13-9 Vulnerabilities

Device Management > Clean Access

Certified Devices | General Setup | Network Scanner | Clean Access Agent | Updates

Scan Setup | Plugin Updates | Reports

Plugins | Options | **Vulnerabilities** | User Agreement | Test

User Role: role1

Operating System: ALL

(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)

Enabled Plugins:

ID	Name	Vulnerable if ...	Instruction	Link	Edit
10970	GSR ACL pub	HOLE			
10973	CSCdi34061	HOLE,WARN			
10561	cisco_675 http DoS	HOLE,WARN,INFO			

183725

- For Enabled Plugins (plugins that have been enabled through the Plugins menu) select the following:

ID: This is the number of the plugin that will be listed on the scan report.

Name: Name of the plugin.

Vulnerable if: These dropdown controls configure how the Clean Access Manager interprets the scan result for the plugin. If the client is scanned and the result returned for a plugin matches the vulnerability configuration, the client will be put in the quarantine role (or blocked). You can increase or decrease the level of result that triggers a vulnerability and assigns users to the quarantine role.

- NEVER**—Ignore the report for the plugin. Even if a HOLE, WARN, or INFO result appears on the report, this plugin is never treated as vulnerability and will never cause the user to be put in the quarantine role.
- HOLE**—If HOLE is the result for this plugin, the client has this vulnerability and will be put in the quarantine role. A result of WARN or INFO on the report is not considered a vulnerability for this plugin. In most cases, administrators should select “HOLE” to configure vulnerabilities. “HOLE” will ignore the other types of information (if any) reported by plugins.
- HOLE, WARN (Timeout)**—This setting means the following:

A HOLE result for this plugin is considered a vulnerability and the client will be put in the quarantine role.

A WARN result for this plugin is considered a vulnerability and the client will be put in the quarantine role. A WARN result means the plugin scan timed out (due to personal firewalls or other software) and could not be performed on the machine. Choosing WARN as a vulnerability will quarantine any client that has a firewall enabled. However, it can also be used as a precautionary measure to quarantine clients when the results of the scan are not known.

An INFO result on the report is not considered a vulnerability for this plugin.

- HOLE, WARN, INFO**—This setting means the following:

A HOLE result for this plugin means the client has this vulnerability and will be put in the quarantine role.

A WARN result for this plugin is considered a vulnerability and the client will be put in the quarantine role. An INFO result usually indicates a client that has a firewall enabled.

An INFO result on the report is considered a vulnerability and the client will be put in the quarantine role. An INFO result indicates status information such as what services (e.g. Windows) may running on a port, or NetBIOS information for the machine. Choosing this level of vulnerability will quarantine any client that returns status information.



Note If the plugin does not return INFO results (and there are no HOLE or WARN results), the client will not be quarantined.

5. To edit a plugin, click the **Edit** button next to the plugin that you want to configure.
6. The **Edit Vulnerabilities** form appears.

Figure 13-10 Edit Vulnerability

Device Management > Clean Access

Certified Devices | General Setup | Network Scanner | Clean Access Agent | Updates

Scan Setup | Plugin Updates | Reports

Plugins | Options | Vulnerability | User Agreement | Test

User Role: role1

Operating System: ALL

Plugin ID: 10973

Plugin Name: CSCdi34061

Vulnerability if report result is: HOLE,WARN
(A plugin will generate a 'WARN' report if the scan times out before a result.)

Instruction: Type instructions describing what action to take in case this vulnerability is found.

Link: <http://www.cisco-remediation-site.com>

Update Cancel

184483

7. From the **Vulnerability if report result is:** option menu, you can increase or decrease the level of vulnerability reported by this plugin that assigns users to the quarantine role.
8. In the **Instruction** text field, type the informational message that appears in the popup window to users if the plugin discovers a vulnerability.
9. In the **Link** field, type the URL where users can go to fix their systems. The URL appears as a link in the scan report. Make sure to enable traffic policies for the quarantine role to allow users HTTP access to the URL.
10. When finished, click **Update**.

Test Scanning

The **Test** form lets you try out your scanning configuration. You can target any machine for the scan, and specify the user role to be assumed by the target client for the purpose of the test. For this type of testing, the test is actually performed against copies of the scan plugins that are kept in the Clean Access Manager. In a production environment, the Clean Access Servers get copies of scan plugins automatically from the Clean Access Manager and perform the scanning,

To perform a test scan:

1. Go to **Device Management > Clean Access > Network Scanner > Scan Setup > Test**.
2. Choose the **User Role** and **Operating System** for which you want to test the user.
3. Enter the IP address of the machine that you want to scan (the address of the current machine appears by default) in the **Target Computer** field.
4. Click **Test**. The scan result appears at the bottom of the page.

Figure 13-11 Network Scanning Test Page

Device Management > Clean Access

Certified Devices | General Setup | Network Scanner | Clean Access Agent | Updates

Scan Setup | Plugin Updates | Reports

Plugins | Options | Vulnerabilities | User Agreement | Test

User Role: role1

Operating System: ALL

Target Computer: 171.69.106.72 [Test from Manager]

Scan Report:

Type	Plugin	Service	Description
INFO	11011	microsoft-ds (445/tcp)	A CIFS server is running on this port
INFO	11011	netbios-ssn (139/tcp)	An SMB server is running on this port
INFO	10150	netbios-ns (137/tcp)	Synopsis : It is possible to obtain the network name of the remote host. Description : The remote host listens on udp port 137 and replies to NetBIOS nbtscan requests. By sending a wildcard request it is possible to obtain the name of the remote system and the name of its domain. Risk factor : None Plugin output : The following 4 NetBIOS names have been gathered : BBAKER-WXP01 = Computer name CISCO = Workgroup / Domain name BBAKER-WXP01 = NetDDE Service BBAKER-WXP01 = File Server Service The remote host has the following MAC address on its adapter : 00:15:58:32:c2:e2 CVE : CVE-1999-0621
INFO	10785	microsoft-ds (445/tcp)	Synopsis : It is possible to obtain information about the remote os. Description : It is possible to get the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445. Risk factor : None Plugin output : The remote Operating System is : Windows 5.1 The remote native lan manager is : Windows 2000 LAN Manager The remote SMB Domain Name is : CISCO
INFO	10884	ntp (123/udp)	A NTP (Network Time Protocol) server is listening on this port. Risk factor : Low
WARN	10394	SMB log in	Timeout: Unable to Scan
WARN	11936	OS Identification	Timeout: Unable to Scan

(Note: The report shown here is the full administrator report. The report shown to end users contains only the vulnerability results for the enabled plugins.)

Show the last 50 lines of the test log. [Show Scan Log] [Show Other Log]

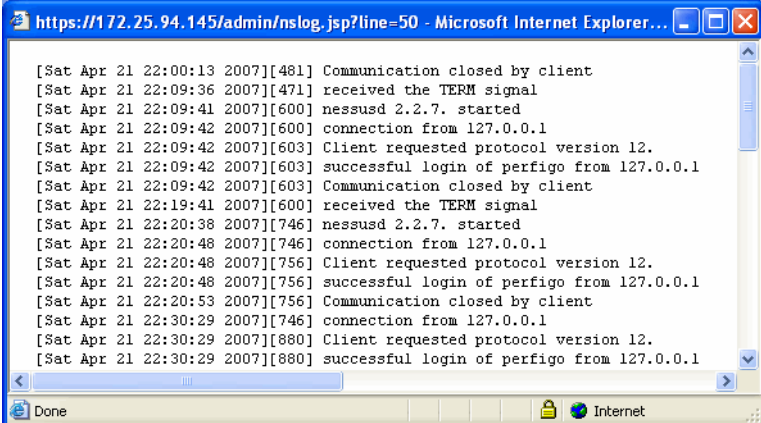
(Use "show other log" to check the plugin dependencies.)

183655

Show Log

Clicking the **Show Log** button on the **Device Management > Network Scanner > Scan Setup > Test** page brings up a debug log (Figure 13-12) for the target computer tested (sourced from `/var/nessus/logs/nessusd.messages`). The log shows which plugins were executed, the results of the execution, which plugins were skipped and the reason (dependency, timeout, etc). Administrators can check this log to debug why a scan result is not as expected.

Figure 13-12 Network Scanning Show Log

A screenshot of a Microsoft Internet Explorer browser window displaying a network scanning log. The address bar shows the URL `https://172.25.94.145/admin/nslog.jsp?line=50`. The log content is as follows:

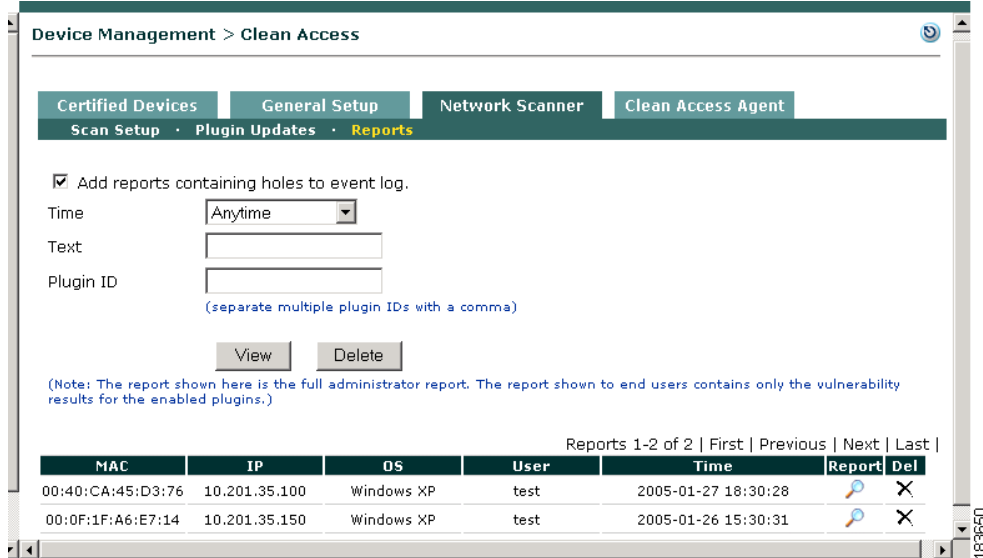
```
[Sat Apr 21 22:00:13 2007][481] Communication closed by client
[Sat Apr 21 22:09:36 2007][471] received the TERM signal
[Sat Apr 21 22:09:41 2007][600] nessusd 2.2.7. started
[Sat Apr 21 22:09:42 2007][600] connection from 127.0.0.1
[Sat Apr 21 22:09:42 2007][603] Client requested protocol version 12.
[Sat Apr 21 22:09:42 2007][603] successful login of perfigo from 127.0.0.1
[Sat Apr 21 22:09:42 2007][603] Communication closed by client
[Sat Apr 21 22:19:41 2007][600] received the TERM signal
[Sat Apr 21 22:20:38 2007][746] nessusd 2.2.7. started
[Sat Apr 21 22:20:48 2007][746] connection from 127.0.0.1
[Sat Apr 21 22:20:48 2007][756] Client requested protocol version 12.
[Sat Apr 21 22:20:48 2007][756] successful login of perfigo from 127.0.0.1
[Sat Apr 21 22:20:53 2007][756] Communication closed by client
[Sat Apr 21 22:30:29 2007][746] connection from 127.0.0.1
[Sat Apr 21 22:30:29 2007][880] Client requested protocol version 12.
[Sat Apr 21 22:30:29 2007][880] successful login of perfigo from 127.0.0.1
```

The browser status bar at the bottom shows "Done" and "Internet".

View Scan Reports

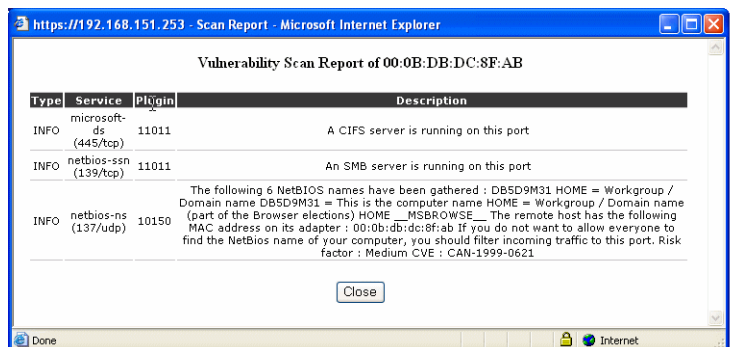
After enabling network scanning, you can view individual scan reports from **Device Management > Clean Access > Network Scanner > Reports**. The report shown here is the full administrator report (Figure 13-14). The report shown to end users contains only the vulnerability results for the enabled plugins. (Users can access their version of the scan report by clicking the **Scan Report** link in their Logout page.)

Figure 13-13 Network Scanner Reports



- Choose **Anytime** from the **Time** dropdown menu to view all reports.
- To view only selected reports, choose a different **Time**, or enter search **Text** or **Plugin ID**, and click **View**. If choosing a “**User Defined**” Time interval, type the “begin” year-month-day and time in the first text box (e.g. 2006-03-22 13:10:00) and the “end” year-month-day and time in the second text box (e.g. 2006-03-23 11:25:00), then click **View**.
- To delete reports displayed according to the selected criteria, click **Delete**.
- Click the **Report** icon to open the detailed scan report, as shown in Figure 13-15.

Figure 13-14 Network Scanner Administrator Report Example

**Note**

When there are dependencies between plugins, for example plugin B is enabled and the scan result of plugin A is the prerequisite of plugin B, the network scanner automatically applies plugin A whether or not plugin A is enabled. However, since plugin A is not explicitly enabled, the scan result reported from plugin A will only be shown in the administrator reports.

- To add reports to the Event log (**Monitoring > Event Logs > View Logs**), check the “**Add reports containing holes to event log**” option. CleanAccess category reports will be generated as shown in Figure 13-15.

Figure 13-15 CleanAccess Network Scanning Event Log

Type	Category	Time	Event
Red Flag	CleanAccess	2005-04-13 18:19:54	[00:0F:1F:A6:E7:14 ## 10.201.35.200] test- Holes reported by plugin #11835:loc-srv (135/tcp)
Green Flag	Administration	2005-04-13 18:19:54	00:0F:1F:A6:E7:14 added to certified device list
Green Flag	Authentication	2005-04-13 18:19:54	[00:0F:1F:A6:E7:14 ## 10.201.35.200] test - Successfully logged in, Provider: Local DB, Access point: N/A, Network: N/A
Green Flag	Administration	2005-04-13 18:18:41	00:0F:1F:A6:E7:14 removed from the certified device list
Green Flag	Authentication	2005-04-13 18:18:41	[00:0F:1F:A6:E7:14 ## 10.201.35.200] test - Forcefully logged out by administrator
Green Flag	Administration	2005-04-13 18:16:59	Admin user session is created, login succeeded. Name:admin, Group:Full-Control Admin, IP:171.69.134.149, Login time:04/13/05 18:16:59, Last access time:04/13/05 18:16:59
Green Flag	Administration	2005-04-13 18:13:47	Admin user session is created, login succeeded. Name:admin, Group:Full-Control Admin, IP:171.69.134.149, Login

Customize the User Agreement Page

You can enable a User Agreement Page (“Virus Protection Page”) for web login users to provide network usage policy information, virus warnings and/or links to software patches or updates after login and successful network scanning.

Only uncertified users will see the User Agreement Page. Once a user device is on the Certified Devices List, the User Agreement Page is not presented again until the device is cleared from the Certified Devices List. Note that the **Certified Devices List** only records the first user that logs in with the device and in this way tracks which user accepted the User Agreement Page at login. To ensure that the User Agreement Page is presented to users at each login, enable the **Require users to be certified at every web login** option for the role/OS on the **General Setup** page.

Configuration settings for this page are located in two places:

- The page target (whether the page is shown to users in a user role) is configured from **Device Management > Clean Access > General Setup** (Figure 13-16).

Figure 13-16 General Setup Tab

Device Management > Clean Access

Certified Devices | **General Setup** | Network Scanner | Clean Access Agent | Updates

Web Login · Agent Login

User Role: Role2

Operating System: ALL

(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)

Show **Network Scanner User Agreement page** to web login users Link to User Agreement Page Configuration Form

Enable pop-up scan vulnerability reports from User Agreement page

Require users to be certified at every web login

Exempt certified devices from web login requirement by adding to MAC filters

Block/Quarantine users with [vulnerabilities](#) in role: Quarantine Role (4 minutes)

Show quarantined users User Agreement Page of: quarantine role

Update Cancel

183648

- The page contents for a user role are configured under **Device Management Clean Access > Network Scanner > Scan Setup > User Agreement Page** (Figure 13-17).

Figure 13-17 User Agreement Page Content Configuration Form

Device Management > Clean Access

Certified Devices | General Setup | Network Scanner | Clean Access Agent | Updates

Scan Setup | Plugin Updates | Reports

Plugins | Options | Vulnerabilities | **User Agreement** | Test

User Role:

Operating System:

(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)

The User Agreement page contains user agreement text, security information, or any information you want users to acknowledge to be certified for network access. Use the Information Page configured below to include information in the User Agreement page specifically for users with the selected role and operating system in your network.

Information Page Message (or URL):

(the web server hosting this page must be accessible to the user role by traffic control policy)

Acknowledgement Instructions:

(this text appears next to the Accept(Continue) and Decline(Logout) buttons at the bottom of the User Agreement page. The variable #time# will be replaced with the quarantine time.)

Accept(Continue) Button Label: (use "HIDDEN" to hide this button)

Decline(Logout) Button Label: (use "HIDDEN" to hide this button)

183654

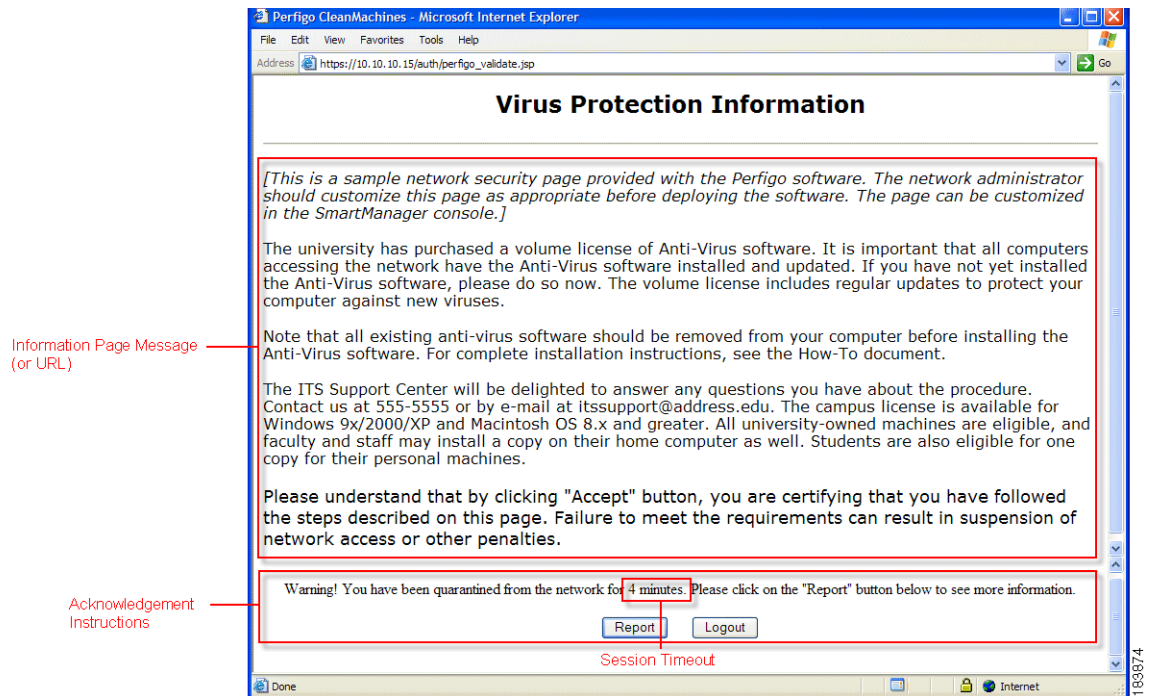
Figure 13-18 illustrates what the default generated page looks like to an end user. The User Agreement Page is not a popup but an HTML frame-based page made up of several components:

- The **Information Page Message (or URL)** component, which contains the contents you specify.
- The **Acknowledgement Instructions** frame component. This contains text and buttons (Accept, Decline) for acknowledging the agreement information.



Note

For quarantine role pages, the buttons are hardcoded to read “Report” and “Logout”.

Figure 13-18 User Agreement Page (Quarantine Role Example)**Note**

The page content (“Virus Protection Information”) shown in [Figure 13-18](#) is the default content shown to the end user, if no other information message or URL is specified for the User Agreement Page. Note that this default content is not displayed in the **Information Page Message (or URL)** text area of the configuration form.

The configuration form (shown in [Figure 13-17](#)) can be used to set up the following types of pages for a web login user:

- After network scanning with no system vulnerabilities found—Users see the User Agreement Page configured for the normal login role (Accept and Decline buttons).
- After web login and network scanning with client system vulnerabilities found—
 - Users are put in a quarantine role and see the User Agreement Page of the quarantine role (Report and Logout buttons).
 - Users are put in a quarantine role but see the User Agreement Page of their normal login role (Report and Logout buttons).

Before starting, create the HTML page that you want to use for the **Information Page Message (or URL)** component. Cisco NAC Appliance lets you present a specific information page to users with a particular role or operating system. The customized page should be on a web server accessible to Cisco NAC Appliance elements.

After configuring the User Agreement Page, you will need to create a traffic policy to enable users in the role access to the web resources of the page. Note that the role must grant access to port 80 of the CAM. See [Chapter 9, “User Management: Traffic Control, Bandwidth, Schedule”](#) for details.

To customize the User Agreement Page:

1. Go to **Device Management > Clean Access > Network Scanner > Scan Setup > User Agreement Page**. The configuration form for the User Agreement Page appears as shown in [Figure 13-19](#).

Figure 13-19 User Agreement Page Configuration Form

Device Management > Clean Access

Certified Devices | General Setup | Network Scanner | Clean Access Agent | Updates

Scan Setup | Plugin Updates | Reports

Plugins | Options | Vulnerabilities | User Agreement | Test

User Role:

Operating System:

(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)

The User Agreement page contains user agreement text, security information, or any information you want users to acknowledge to be certified for network access. Use the Information Page configured below to include information in the User Agreement page specifically for users with the selected role and operating system in your network.

Information Page Message (or URL):

(the web server hosting this page must be accessible to the user role by traffic control policy)

Acknowledgement Instructions:

(this text appears next to the Accept(Continue) and Decline(Logout) buttons at the bottom of the User Agreement page. The variable #time# will be replaced with the quarantine time.)

Accept(Continue) Button Label: (use "HIDDEN" to hide this button)

Decline(Logout) Button Label: (use "HIDDEN" to hide this button)

188654

2. Choose the **User Role** and **Operating System** for which the page applies. The Clean Access Manager determines the operating system of the user's system at login time and serves the page you have specified for that operating system. If selecting a quarantine role, the **Acknowledgement Instructions** and button fields will be disabled.
3. Type HTML content or the URL of the page that you want to appear in the **Information Page Message (or URL)** field of the User Agreement page. If using a file you uploaded to the CAM or CAS, you can reference the file as described below:
 - a. **Enter URLs:** (for a single webpage to appear)

For an external URL, use the format `http://www.webpage.com`.

For a URL on the CAM use the format:

`https://<CAM_IP>/upload/file_name.htm`

where `<CAM_IP>` is the domain name or IP listed on the certificate.



Note

If you enter an external URL or CAM URL, make sure you have created a traffic policy for the Unauthenticated role that allows the user HTTP access only to the CAM or external server.

- b. **Enter HTML:** (to add a combination of resource files, such as logos and HTML links)

Type HTML content directly into the text field.

To reference an uploaded resource file as part of the HTML content, use the following formats:

- To reference a link to an uploaded HTML file:

```
<a href="file_name.html"> file_name.html </a>
```

- To reference an image file (such as a JPEG file) enter:

```

```

See [Upload a Resource File, page 6-13](#) for additional details.

4. If desired, type the text that you want to appear above the accept and decline buttons in the **Acknowledgement Instructions** field.
5. Type the labels that should appear on the accept and decline buttons in their respective fields.
6. Click the **Save** button to save your changes.

The User Agreement Page is now generated with the changes you made for users logging into the network.

**Note**

For details on the web user login page, see [Chapter 6, "Configuring User Login Page and Guest Access."](#)
For traffic policy details, see [Configure Policies for Agent Temporary and Quarantine Roles, page 9-18.](#)
