



CHAPTER 3

System Setup

The system can be configured through the web interface to provide the networking configuration for the appliance and other system settings that are important such as time and SSL certificate. The Cisco NAC Guest Server is administered entirely using a web interface over either HTTP or HTTPS.

This chapter includes the following sections:

- [Accessing the Administration Interface](#)
- [Configuring Network Settings](#)
- [Date and Time Settings](#)
- [SSL Certificate](#)
- [Configuring Administrator Authentication](#)

Accessing the Administration Interface

Upon first accessing the web administration interface of the Cisco NAC Guest Server, you will need to install a product license. You can obtain a license using the instructions in the PAK shipped with the appliance or by registering for a evaluation license at <https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet?FormId=146>.



Note

For additional details on evaluation licenses refer to *Cisco NAC Appliance Service Contract / Licensing Support*.

This section describes the following:

- [Obtain and Install Cisco NAC Guest Server License](#)
- [Access Cisco NAC Guest Server Administration Interface](#)

Obtain and Install Cisco NAC Guest Server License

Use the following steps to obtain and install your FlexLM product license files for Cisco NAC Guest Server.

- Step 1** With FlexLM licensing, you will receive a Product Authorization Key (PAK) for each Guest Server that you purchase. The PAK is affixed as a sticky label on the Software License Claim Certificate card that is included in your package.



Warning

The PAK is NOT the Cisco NAC Guest Server license. The PAK is used to obtain the Cisco NAC Guest Server license, as described below.

- Step 2** Log in as a registered CCO user and fill out the Customer Registration form found at the PAK Cisco Technical Support site: <http://www.cisco.com/go/license>. During customer registration, submit each PAK you receive and the eth0 MAC address of your Cisco NAC Guest Server.



Warning

The eth0 MAC address entered for the Guest Server must be in UPPER CASE (i.e. hexadecimal letters must be capitalized). Do not enter colons (":") in between characters.

Please follow the instructions on the license web pages carefully to ensure that the correct MAC addresses are entered.

- Step 3** For each PAK that you submit, a license file is generated and sent to you via email.
- Step 4** Save each license file you receive to disk.
- Step 5** Open a web browser to the Cisco NAC Guest Server admin interface by entering the IP address that you configured through the command line as the URL.
- For HTTP access, open **`http://<guest_server_ip_address>/admin`**
 - For HTTPS access, open **`https://<guest_server_ip_address>/admin`**
- Step 6** In the Guest Server License Form([Figure 3-1](#)), click the **Browse** button and locate the license file.

Figure 3-1 Guest Server License Form (example)

Guest Server License Form

The product license for this installation (MAC Address: 00:0C:29:AC:4E:63) is either invalid, expired, or not yet set.

Reason for failure: **The license appears to be corrupted**

Please install the correct license.

Product Evaluation:

If you are evaluating the Guest Server product, please visit the [Cisco Technical Support](#) site to register and obtain an evaluation product license. Once this is complete you will receive a license key via email which must be saved to a text file. Enter the license file name in the input box below (use the Browse button to navigate to the text file) and hit the Install License button.

Product Authorization Key (PAK):

If you have received a Product Authorization Key (PAK) with your purchase, please visit the [Cisco Technical Support](#) site to register and obtain the proper product license. Note: During the registration process, you will be asked for the MAC address above, please have this information ready. Once this is complete, you will receive a license key via email which must be saved to a text file. Enter the license file name in the input box below (use the Browse button to navigate to the text file) and hit the Install License button:

185507

Step 7 Click **Submit** to install the license.

Access Cisco NAC Guest Server Administration Interface

- Step 8** The Cisco NAC Guest Server Administration interface ([Figure 3-2](#)) displays. This is the administrator interface to the appliance.
- Step 9** Login as the admin user. The default user name/password is **admin/admin**.

Figure 3-2 Admin Login

Cisco NAC Guest Server Administration

Please enter your administrator username and password to access the administration interface.

Username:

Password:

© Cisco 2007

185642

**Note**

Cisco recommends setting up SSL access and change the default admin user password for security. Refer to [SSL Certificate](#), page 3-7 and [Edit Existing Admin Account](#), page 3-11 for details.

Step 10 After the license is installed, the administrator interface is brought up in web browser as follows:

- For HTTP access, open **http://<guest_server_ip_address>/admin**
- For HTTPS access, open **https://<guest_server_ip_address>/admin**



Note

Entering the Guest Server IP address without the “/admin” as the URL brings up the sponsor interface. See [Chapter 4, “Configuring Sponsor Authentication”](#) for details.

Configuring Network Settings

Configure remaining network settings before performing any other operation. This minimizes the need to restart the appliance later on.

Step 1 From the administration home page select **Server > Network Settings** from the left hand menu ([Figure 3-3](#)).

Figure 3-3 Administration Home Page

Cisco NAC Guest Server Administration

What would you like to do:

- Add/Edit Local User Accounts
- Add/Edit Administrator Accounts
- Configure Sponsor Authentication
- Configure NAC Appliance Settings
- Configure your Email Server Settings
- Select the User Interface Template to use
- Edit the User Interface Templates

© Cisco 2008 Version 1.1.1

187696

Step 2 The Network Settings page provides all the network settings that can be changed on the appliance ([Figure 3-4](#)).

Figure 3-4 Network Settings

You can change the following Network Settings:

- Domain Name—Enter the domain name for your organization (e.g. cisco.com)
- Hostname—Enter the name of the appliance as defined in DNS (without DNS suffix)
- IP Address—Enter the IP address of the eth0 interface on the appliance
- Subnet Mask—Enter the corresponding subnet mask
- Default Gateway—The default gateway for the network to which the appliance is connected
- Nameserver 1—IP address of the primary DNS server
- Nameserver 2—IP address of the secondary DNS server

Step 3 Click the **Save Settings** button to save the changes that you made.

Step 4 Once changes are saved, you need to restart the Guest Server to ensure all processes use the correct IP address. Click the **Restart** button, and the restart process will begin on the Guest Server within 60 seconds.

Date and Time Settings

Correct date and time are critical to the Cisco NAC Guest Server. The Guest Server authenticates guest users based upon the time their accounts are valid. It is important for the time to be correct so guest accounts are created and removed at the correct time. If possible, Cisco recommends using a Network Time Protocol (NTP) server to synchronize the time and date.

Step 1 From the administration interface select **Server > Date/Time Settings** from the left hand menu (Figure 3-5).

Figure 3-5 Date/Time Settings

Date and Time Settings

Date: 15 May 2008

Time: 05 : 30

Note: to set the system time, the timezone below must be set to the correct value.

Set System Date and Time

Timezone settings

Locale: America/Los_Angeles

Set System Timezone

Network Time Protocol settings

NTP Server: 192.168.1.25

NTP Server: 10.24.66.43

Set NTP Server

187698

- Step 2** Select the correct **Date** and **Time** for the location of the Guest Server.
- Step 3** Click the **Set System Date and Time** button to apply the time and date.
- Step 4** Select the correct **Timezone** for the location of the Guest Server.
- Step 5** Apply the settings by clicking the **Set System Timezone** button.



Note If you change the time zone, this action automatically adjusts the date and time on the server.

- Step 6** If you have one or two NTP servers available on the network, enter the addresses of the NTP servers.
- Step 7** Click the **Set NTP Server** button. This saves the settings and restarts the NTP process so the new settings take effect.



Note When setting the NTP server it may take some time for synchronization to occur. Synchronization occurs much faster if the time is set to be close to the NTP server (and saved with the **Set** button) before clicking the **Set NTP Server** button.

SSL Certificate

Both sponsors and administrators can access the Cisco NAC Guest Server using either HTTP or HTTPS. For more secure access Cisco recommends using HTTPS access.

This section describes the following

- [Accessing the Guest Server using HTTP or HTTPS](#)
- [Generating Temporary Certificates/ CSRs/ Private Key](#)
- [Downloading Certificate Files](#)
- [Upload Certificate Files](#)

Accessing the Guest Server using HTTP or HTTPS

You can configure whether sponsors and administrators access the portal using HTTP, both HTTP and HTTPS, or HTTPS only.

- Step 1** From the administration interface, select **Server > SSL Settings** from the left hand menu ([Figure 3-6](#)).

Figure 3-6 *SSL Settings Main Page*

- Step 2** The Main SSL Settings page provides the following options:
- **Redirect http to https**—When enabled, any sponsor or administrator accessing the Guest Server using HTTP is automatically redirected to the HTTPS interface. If this setting is not enabled, then no redirection occurs.
 - **Allow http access**—When enabled, allows sponsors and administrators to access the portal with standard HTTP. If this is not enabled, sponsors and administrators are redirected if the first option is set, or if not set, are shown a web page explaining that HTTP access is not available.
- Step 3** When you have made your changes, click the **Save Settings** button.

**Note**

The Main SSL Settings page also provides the **Restart Web Server** button. You need to restart the Web Server component of the appliance when new certificates are generated or uploaded to the appliance. Clicking the **Restart** button makes the Guest Server use the new certificates.

Generating Temporary Certificates/ CSRs/ Private Key

Cisco NAC Guest Server ships with a default certificate installed. If you are planning on using HTTPS, Cisco highly recommends generating a new temporary certificate/private key. When doing this, a certificate signing request (CSR) is also generated that can be used to obtain a CA signed certificate.

The whole process of generating a temporary certificate, CSR and private key is performed on the Create page. Entering the correct details on the Create page automatically generates the required files.

- Step 1** From the administration interface, select **Server > SSL Settings** from the left hand menu, then select **Create** from the menu at the top of the page (Figure 3-7).

Figure 3-7 Create SSL Page

- Step 2** Enter the details on the screen to provide the details for the temporary certificate and CSR.
- **Common Name**—This is either the IP address of the Cisco NAC Guest Server, or the fully qualified domain name (FQDN) for the Guest Server. The FQDN must resolve correctly in DNS.
 - **Organization**—The name of your organization or company.
 - **Organizational Unit**—The name of the department or business unit that owns the device.
 - **City**—The city where the server is located.
 - **State**—The state where the server is located.
 - **2 Letter Country Code**—The 2 letter ISO abbreviation for the country where the Guest Server is located, such as US for United States, GB for Great Britain or United Kingdom.
- Step 3** Click **Create Certificate**. This creates a temporary self-signed certificate, a new private key and also the corresponding CSR which can be used for obtaining a certificate from a Certificate Authority (CA).

- Step 4** To use the new temporary certificate you must restart the web server process. Click the Main tab from the top of the screen, then click the **Restart Web Server** button (Figure 3-6).



- Note** If you want the CSR, you can download it from the download page as described in [Downloading Certificate Files](#), page 3-9.

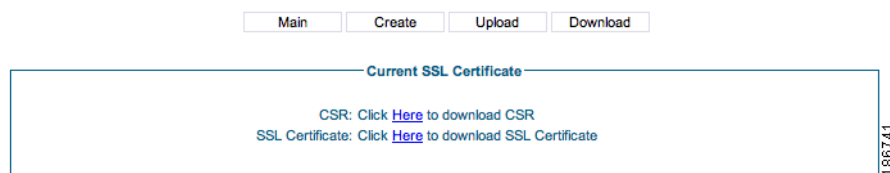
Downloading Certificate Files

Downloading the CSR and Certificate

You will need to download the CSR from the appliance so that it can be sent to a Certificate Authority to obtain a certificate. Cisco strongly recommends backing up the certificate and private key.

- Step 1** From the administration interface select **Server > SSL Settings** from the left hand menu.
- Step 2** Select **Download** from the menu at the top of the page (Figure 3-8).

Figure 3-8 Download Certificate Files



- Step 3** Click the relevant link to download the CSR or SSL Certificate.
- Step 4** Save the SSL Certificate to a secure backup location.

Downloading the Private Key

The private key can only be obtained through an SFTP connection to the Guest Server. For windows platforms, you can get a free SFTP client from <http://winscp.net>.

- Step 1** Open an SFTP connection to the Cisco NAC Guest Server, the authentication credentials are the same as for the command line. This is the username of root and the password you have assigned for this account. The default password is cisco, Cisco recommends you change this as detailed in [Command Line Configuration](#), page 2-3.
- Step 2** Download the `/etc/pki/tls/private/localhost.key` file and store it in a secure backup location.

Upload Certificate Files

The Cisco NAC Guest Server provides a method of importing/uploading certificate files to the appliance. The Upload SSL Certificate pages is used to install a CA-signed certificate or to restore files previously backed up.



Note

The certificate files are not backed up as part of any backup process. You must manually back them up as described in [Downloading Certificate Files, page 3-9](#).

Step 1 From the administration interface select **Server > SSL Settings** from the left hand menu.

Step 2 Select **Upload** from the menu at the top of the page ([Figure 3-9](#)).

Figure 3-9 Upload Certificate Files

Step 3 In the Upload SSL Certificate page, click the **Browse** button to locate the SSL Certificate file, Root CA Certificate or Private Key file you want to upload and click the **Upload** button.

Configuring Administrator Authentication

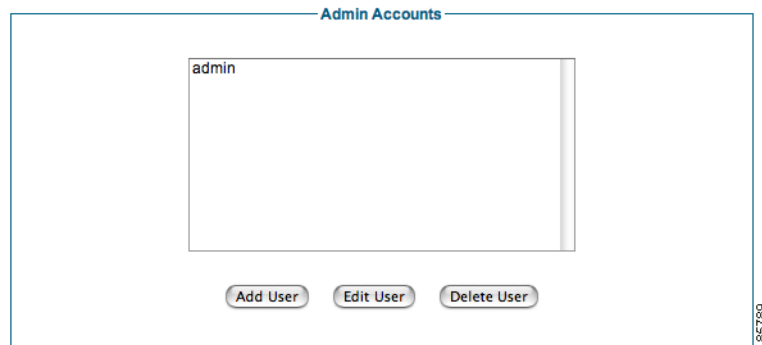
Cisco NAC Guest Server has a single default administrator account, called “admin.” The Admin Accounts pages under the Authentication menu allow you to create, edit and delete additional administrator accounts.

This section describes the following

- [Add New Admin Account](#)
- [Edit Existing Admin Account](#)
- [Delete Existing Admin Account](#)

Add New Admin Account

Step 1 From the administration interface select **Authentication > Administrators** from the left hand menu.

Figure 3-10 Admin Accounts

Step 2 In the Admin Accounts page (Figure 3-10), click the **Add User** button.

Figure 3-11 Add Admin User

Step 3 In the Add Administrator page (Figure 3-11), enter all the admin user credentials.

- First Name—Type the first name of the admin user
- Surname—Type the last name of the admin user.
- Email Address—Type the email address of the admin user
- Username—Type the user name for the admin account.
- Password—Type the password for the admin account.
- Repeat Password—Retype the password for the admin account

Step 4 Click the **Add Administrator** button.

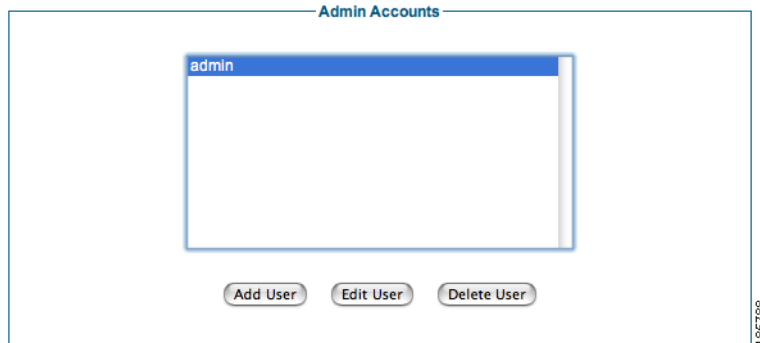
- If there are any errors, the account is not added and an error message displays at the top of the page.
- If successfully added, a success message displays at the top of the page and you can add additional admin accounts.

Edit Existing Admin Account

You can modify the settings of admin accounts that are already created.

Step 1 From the administration interface select **Authentication > Administrators** from the left hand menu.

Figure 3-12 Admin Users to Edit



Step 2 In the Admin Accounts page (Figure 3-12), select the user from the list and click the **Edit User** button.

Step 3 In the Edit Administrator page (Figure 3-13), edit the user credentials.

Figure 3-13 Edit Admin Account

 A screenshot of the 'Edit the administrator user account details' web form. The form contains the following fields: 'Username: admin', 'First Name: admin', 'Surname: admin', 'Email Address: admin@localhost', 'Password:', and 'Repeat Password:'. Below the password fields is a note: 'If you don't wish to change the password please keep the entry empty.' At the bottom are two buttons: 'Save Settings' and 'Reset Form'. A vertical number '185787' is on the right side of the image.

- First Name—Edit the first name of the admin user
- Surname—Edit the last name of the admin user.
- Email Address—Edit the email address of the admin user
- Username—Edit the user name for the admin account.



Note Leaving the Password and Repeat Password fields empty keeps the existing password.

- Password—Edit the password for the admin account.
- Repeat Password—Edit the password for the admin account.

Step 4 Click the **Save Settings** button.

- If there are any errors, the account is not changed and an error message displays at the top of the page.

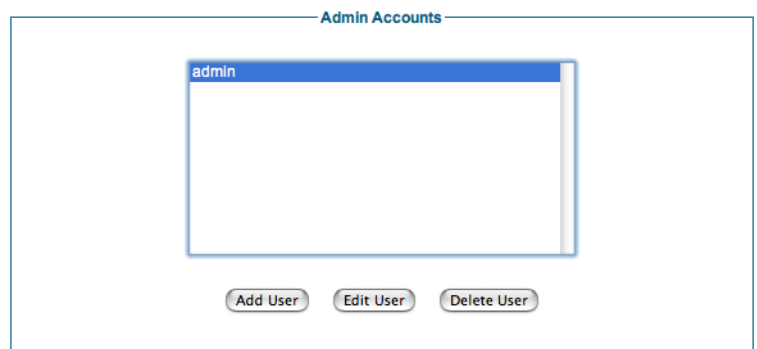
- If successfully changed, a success message displays at the top of the page and you can make additional changes to the same admin account.

Delete Existing Admin Account

You can remove existing admin accounts from the administration interface.

- Step 1** From the administration interface select **Authentication > Administrators** from the left hand menu.

Figure 3-14 Select Admin Account to Delete



- Step 2** In the Admin Accounts page (Figure 3-14), select the user from the list and click the **Delete User** button.
- Step 3** At the prompt “Are you sure you want to delete the user”, click OK to delete the user or Cancel to cancel the deletion.

If successfully deleted, a success message displays at the top of the page and you can perform additional admin account operations.

