



## CHAPTER 3

# System Setup

---

The Cisco NAC Guest Server is administered entirely using a web interface over either HTTP or HTTPS. After initial installation, 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 the SSL certificate.

This chapter includes the following sections:

- [Installing the Product License and Accessing the Administration Interface](#)
- [Configuring Network Settings](#)
- [Date and Time Settings](#)
- [Configuring SSL Certificates](#)
- [Configuring Administrator Authentication](#)

## Installing the Product License and Accessing the Administration Interface

Before accessing the web administration interface of the Cisco NAC Guest Server, you 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 an 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 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 received and the eth0 MAC address of your Cisco NAC Guest Server.



**Note**

For convenience, the top part of the Cisco NAC Guest Server License Form as shown in [Figure 3-1](#), lists the MAC address of the Guest Server appliance.



**Warning**

**The eth0 MAC address entered in the customer registration form 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 by email.
- Step 4** Save each license file you receive to disk.
- Step 5** Open a web browser to the Cisco NAC Guest Server Administration interface by entering the IP address that you configured through the command line as the URL, followed by /admin:
- For HTTP access, open **`http://<guest_server_ip_address>/admin`**
  - For HTTPS access, open **`https://<guest_server_ip_address>/admin`**
- Step 6** In the Cisco NAC Guest Server License Form as shown in [Figure 3-1](#), click the **Browse** button and locate the license file.

Figure 3-1 Cisco NAC Guest Server License Form (example)

**Cisco NAC Guest Server Administration**  
Version: 2.0.0

The product license for this installation (MAC Address: **00:0C:29:35:0D:47**) is either invalid, expired, or not yet set.  
**(No license file found)**

Please install the correct license.

License File:

**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 above (use the Browse button to navigate to the text file) and hit the Upload 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 above (use the Browse button to navigate to the text file) and hit the Upload License button.

© 2007-2009 Cisco Systems, Inc. All rights reserved.  
Cisco, the Cisco logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

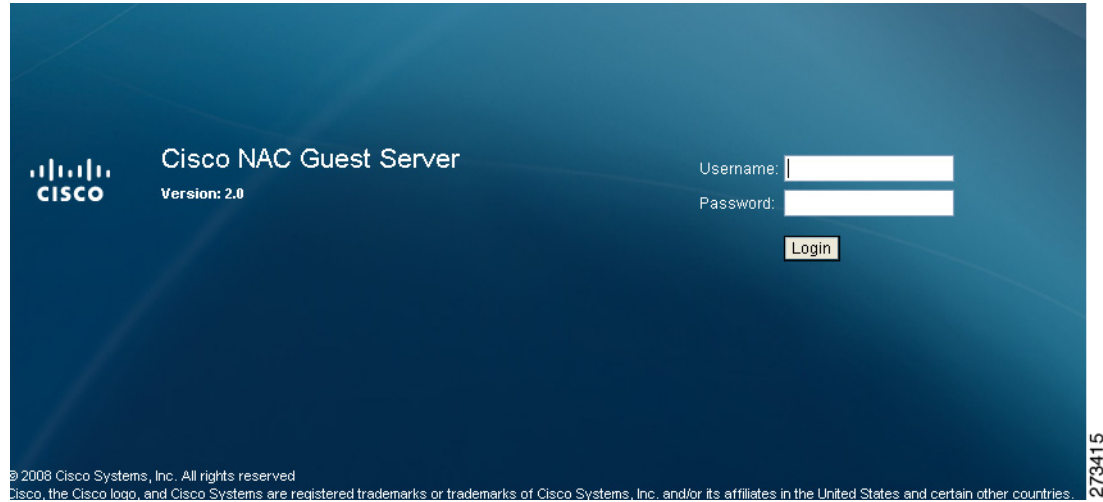
192658

**Step 7** Click **Upload License** to install the license.

## Access Cisco NAC Guest Server Administration Interface

- Step 1** If you have installed a license, the admin login is automatically displayed. Otherwise, open a web browser to the Cisco NAC Guest Server Administration interface by entering the IP address that you configured through the command line as the URL, followed by /admin:
- For HTTP access, open **http://<guest\_server\_ip\_address>/admin**
  - For HTTPS access, open **https://<guest\_server\_ip\_address>/admin**
- Step 2** The Cisco NAC Guest Server Administration interface is displayed as shown in [Figure 3-2](#). This is the administrator interface to the appliance.
- Step 3** Log in as the admin user. The default user name/password for the admin console is **admin/admin**.

Figure 3-2 Admin Login

**Note**

Cisco recommends setting up SSL access and change the default admin user password for security. Refer to [Configuring SSL Certificates, page 3-9](#) and [Edit Existing Admin Account, page 3-17](#) for details.

**Note**

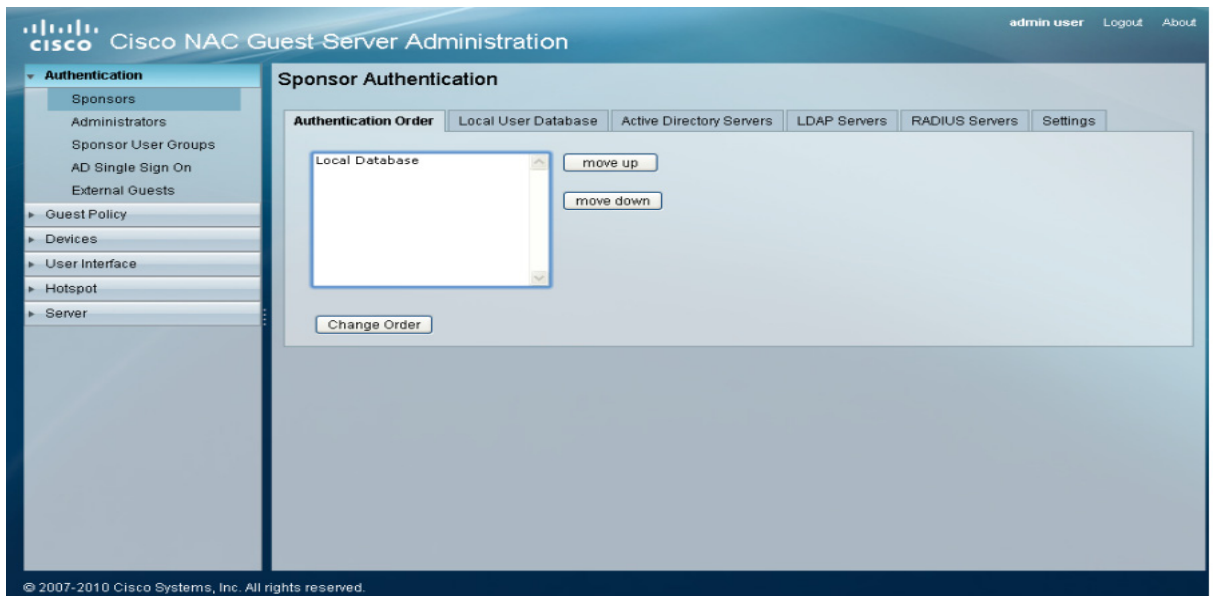
Entering the Guest Server IP address without the "/admin" as the URL brings up the sponsor interface. See [Chapter 4, "Configuring Sponsor Authentication"](#) for details.

## Configuring Network Settings

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

- Step 1** Upon logging into the administration interface, by default, the home page displays the **Authentication > Sponsors > Authentication Order** page as shown in [Figure 3-3](#).

Figure 3-3 Administration Home Page



- Step 2** From the administration home page, select **Server > Network Settings** from the left panel to go to the Network Settings page. This page provides all the network settings that can be changed on the Cisco NAC Guest Server appliance as shown in Figure 3-4.

Figure 3-4 Network Settings

You can change the following Network Settings:

- Hostname—Assign the name of the appliance as defined in DNS (without DNS suffix).
- IP Address—Modify the IP address of the eth0 interface on the appliance.
- Subnet Mask—Enter the corresponding subnet mask.
- Gateway—Modify the default gateway for the network to which the appliance is connected.
- Domain—Enter the domain name for your organization (e.g. cisco.com).
- Primary DNS—Enter the IP address of the primary DNS server.
- Secondary DNS—Enter the 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 **Reboot Server** button, and the restart process will begin on the Guest Server within 60 seconds.



**Note** Modifications to **Server** settings require a reboot. You can modify and save multiple **Server** settings at a time before a reboot, but you must click **Reboot Server** for the changes to be applied.

## 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 that 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** to display the Date/Time Settings page as shown in [Figure 3-5](#).

**Figure 3-5** Date/Time Settings

- Step 2** Select the correct **System Date** and **System Time** for the location of the Guest Server.
- Step 3** Select the correct **System Timezone** for the location of the Guest Server.
- Step 4** Click the **Save Settings** button to apply the System Timezone.



**Note** Changing the System Timezone automatically adjusts the date and time on the server.

- Step 5** If you have one, two or three NTP servers available on the network, click the **Use NTP to set System Date & Time** checkbox.
- Step 6** Enter the IP address of each NTP server available into the fields provided.
- Step 7** Click the **Save Settings** button to apply the changes.



---

**Note** When setting the NTP server it may take some time for synchronization. Synchronization occurs much faster if the time is set close to the NTP server (and saved by clicking the **Save Settings** button) before saving the NTP Server settings.

---

- Step 8** Click the **Reboot Server** button to restart the NTP process so the new settings take effect.



---

**Note** If you modify the Server settings, you need to reboot the system. You can modify and save multiple **Server** settings at a time, but you must click **Reboot Server** for the changes to be applied.

---

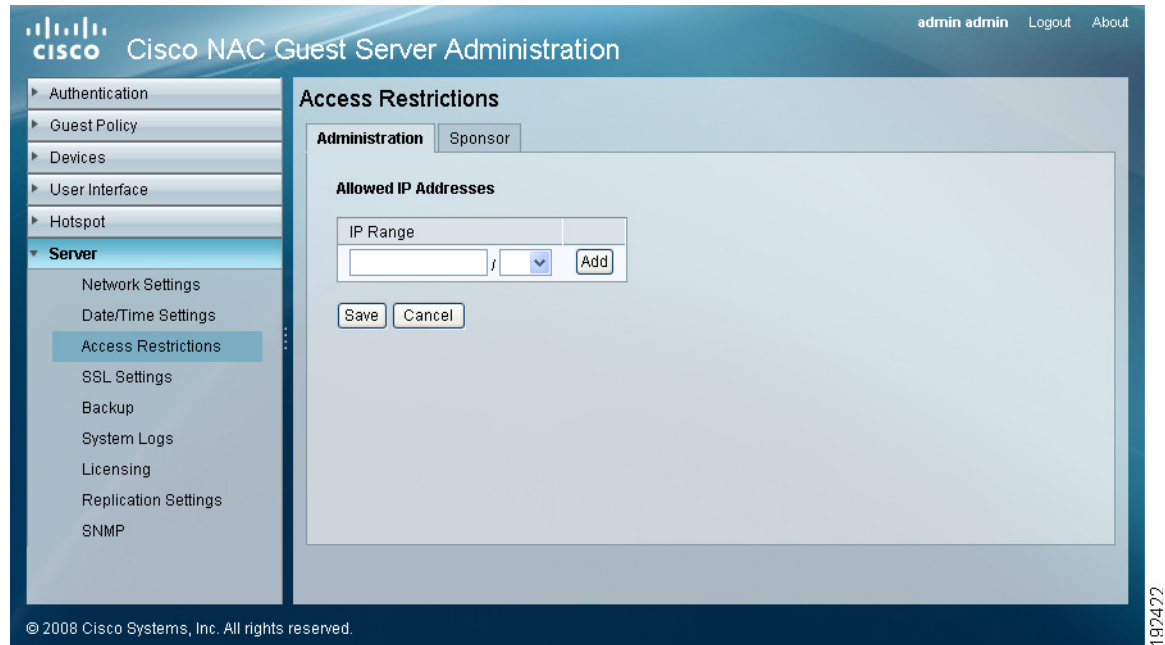
## Access Restrictions

You can configure Cisco NAC Guest Server to restrict access to only certain IP address ranges for the administration interface and the sponsor interface at any one time.

### Administration Access

- 
- Step 1** From the administration interface, select **Server > Access Restrictions** and click the **Administration** tab as shown in [Figure 3-6](#).

Figure 3-6 Access Restrictions Admin



- Step 2** In the Allowed IP Addresses field, type a range of IP addresses that are allowed access to the Guest Server Administration interface, and apply a CIDR subnet range using the dropdown menu.
- Step 3** Click **Add** to add addresses to the list.
- Step 4** Click **Save** to make the changes permanent.

**Note**

Leaving the IP Range field blank allows all IP addresses to access the Administration interface, if users have the required admin account permissions.

## Sponsor Access

- Step 1** From the administration interface, select **Server > Access Restrictions** and click the **Sponsor** tab as shown in [Figure 3-7](#).

Figure 3-7 Access Restrictions Sponsor

**Step 2** Type the range of IP addresses that are allowed to access the Sponsor interface, and apply a CIDR subnet range using the dropdown menu.

**Step 3** Click **Save** to continue.



**Note** Leaving the IP Range field blank allows all IP addresses to access the Sponsor interface, if users have the required sponsor account permissions.



**Note** If you modify the Server settings, you need to reboot the system. You can modify and save multiple **Server** settings at a time, but you must click **Reboot Server** for the changes to be applied.

## Configuring SSL Certificates

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

This section describes the following:

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

## Accessing the Guest Server Using HTTP or HTTPS

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

**Step 1** From the administration interface, select **Server > SSL Settings** from the left panel to display the SSL Settings page as shown in [Figure 3-8](#).

Figure 3-8 SSL Settings Main Page



**Step 2** The main SSL Settings page provides the following options:

- **Allow Only HTTPS**—When selected, only allows HTTPS access to the sponsor or administration interfaces of the Guest Server.
- **Allow Only HTTP**—When selected, only allows HTTP access to the sponsor or administration interfaces of the Guest Server.
- **Allow HTTPS and HTTP**—When selected, allows both HTTPS and HTTP access to the sponsor or administration interfaces of the Guest Server.
- **Allow Only HTTPS (with HTTP Redirected to HTTPS)**—When selected, allows sponsors and administrators to access the portal with HTTPS and standard HTTP; however, sponsors and administrators are redirected via HTTPS if using a standard HTTP connection.



**Note** HTTP to HTTPS redirection is not supported for API access.

**Step 3** When you have made your selection, click the **Save Settings** button.



**Note** Modifications to **Server** settings require a reboot. You can modify and save multiple **Server** settings at a time before a reboot, but you must click **Reboot Server** for the changes to be applied.

## Generating Temporary Certificates/ CSRs/ Private Key

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

- Step 1** From the administration interface, select **Server > SSL Settings** from the left hand menu and click the **Create CSR** link from the center section of the page as shown in [Figure 3-9](#) to bring up the Create CSR form as shown in [Figure 3-10](#).

**Figure 3-9 Certificate Signing Request**

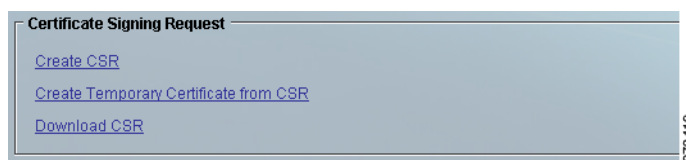


**Figure 3-10 Create a CSR**

- Step 2** Provide the details for the temporary certificate and CSR in the Create CSR form:
- **Common Name (FQDN or IP Address)**—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 (Section)**—The name of the department or business unit that owns the device.
  - **Locality (e.g. City)**—The city where the server is located.
  - **State or Province**—The state where the server is located.
  - **Country**—Select the relevant country from the dropdown menu.

- Step 3** The **Regenerate Private Key** checkbox is optional and should be used if you think your existing private key has been compromised. If you regenerate your private key, the current certificate is invalidated and a new self-signed temporary certificate is generated using the new private key and CSR. Select this option to regenerate a private key.
- Step 4** Click **Create**.
- Step 5** The **Certificate Signing Request** page is again displayed as shown in [Figure 3-9](#). If you chose to regenerate the private key, you will be prompted to restart the server. You need to restart the server to use the new certificate and private key.
- Step 6** The **Create Temporary Certificate from CSR** and **Download CSR** options are now available as shown in [Figure 3-11](#).

**Figure 3-11** Create CSR and Download CSR



- Step 7** Selecting **Create Temporary Certificate from CSR** generates a temporary certificate from the previously requested Certificate Signing Request that you created in Steps 1 to 4.
- Step 8** You can download the CSR by clicking the **Download CSR** option in [Figure 3-11](#). Once you have sent the CSR to a Certificate Authority and obtained the CA-signed certificate in return, you can upload it by following the instructions in the [Uploading Certificate Files](#), page 3-14.
- Step 9** To use the new temporary certificate you must restart the web server process. Click the **Reboot Server** button as shown in [Figure 3-8](#).



**Note**

Modifications to **Server** settings require a reboot. You can modify and save multiple **Server** settings at a time before a reboot, but you must click **Reboot Server** for the changes to be applied.



**Tip**

If you want to install SSL certificates issued by an intermediate CA, you need to perform a CLI procedure. Contact [Cisco TAC](#) to receive guidance about this procedure.

## Generating Self-Signed SSL Certificates Through CLI

When the administrator tries to install an SSL Certificate that is not relevant in the NAC Guest Server, the following error message is displayed: "The Current Private Key does not Correspond to the Current Certificate".

If the user clicks the **Reboot Server** option, the invalid certificate is uploaded and the GUI becomes inaccessible. The workaround is to generate and install a self-signed SSL Certificate using CLI. This enables the user to access the GUI.

Perform the following steps to generate self-signed SSL Certificate using the CLI:

---

**Step 1** Generate key and certificate file by entering the following command:

```
openssl req -new -key /etc/pki/tls/private/localhost.key -nodes -x509 -days 365 -out
/etc/pki/tls/certs/localhost.crt
```

**Step 2** Enter the appropriate information to be incorporated into your certificate request, as follows:

```
Country Name (2 letter code) [GB]:
State or Province Name (full name) [Berkshire]:
Locality Name (eg, city) [Newbury]:
Organization Name (eg, company) [My Company Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:
Email Address []:
```

**Step 3** Provide a copy of the certificate and key to the postgres by entering the following commands:

```
cp /etc/pki/tls/certs/localhost.crt /var/lib/pgsql/data/server.crt
chmod 600 /var/lib/pgsql/data/server.crt
chown postgres:postgres /var/lib/pgsql/data/server.crt

cp /etc/pki/tls/private/localhost.key /var/lib/pgsql/data/server.key
chmod 600 /var/lib/pgsql/data/server.key
chown postgres:postgres /var/lib/pgsql/data/server.key
```

**Step 4** Reboot the server.

---

You can access the GUI after rebooting the server.

## Downloading Certificate Files

### Downloading the Certificate

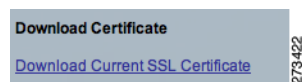
Cisco strongly recommends backing up the certificate and private key. The certificate can be downloaded from the administration interface for manual backup to a secure location.

---

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

**Step 2** Select **Download Current SSL Certificate** from the **Download Certificate** section of the page as shown in [Figure 3-12](#).

**Figure 3-12** Download Certificate File



**Step 3** 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. Login with the root username and password you assigned for this account in the initial setup.
- Step 2** Download the `/etc/pki/tls/private/localhost.key` file and store it in a secure backup location.
- 

## Uploading Certificate Files

The Cisco NAC Guest Server provides a method of importing/uploading certificate files to the Guest Server appliance. The **Upload Certificates** option is used to install a CA-signed certificate or to restore Base 64 PEM format certificate files previously backed up.



### Note

You must upload certificate files in Base 64 PEM format.

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 3-13](#).

Wildcard certificates are not supported.

---

- Step 1** From the administration interface, select **Server > SSL Settings** from the left hand menu.
- Step 2** View the **Upload Certificates** section at the bottom of the page as shown in [Figure 3-13](#).

**Figure 3-13** Upload Certificate Files

- Step 3** Click the **Browse** button to locate the SSL Certificate file or Root CA Certificate file you want to upload and click the **Upload** button.



### Warning

**When uploading a certificate, it must match the private key installed.**

---

- Step 4** If uploading a new Server SSL Certificate, you are prompted to restart the server for the certificate to take effect.



### Note

Modifications to **Server** settings require a reboot. You can modify and save multiple **Server** settings at a time before a reboot, but you must click **Reboot Server** for the changes to be applied.

---

## Uploading a Private Key

The private key can be uploaded only 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. Login with the root username and password you have assigned for this account in the initial setup.
- Step 2** Upload the key to `/etc/pki/tls/private/localhost.key` file.
- Step 3** Change the ownership and file permissions, so that it is owned by root and has permissions of 644.
- ```
chown root:root /etc/pki/tls/private/localhost.key
chmod 644 /etc/pki/tls/private/localhost.key
```
- Step 4** Copy the new key to `/var/lib/pgsql/data/server.key`.
- ```
cp /etc/pki/tls/private/localhost.key /var/lib/pgsql/data/server.key
```
- Step 5** Change the ownership and file permissions, so that it is owned by postgres and has permissions of 700.
- ```
chown postgres:postgres /var/lib/pgsql/data/server.key
chmod 700 /var/lib/pgsql/data/server.key
```

**Warning**

**As it is possible to disable a server or invalidate a server certificate, Cisco strongly recommends that you have a strong knowledge of PKI before working with the server private key directly as described in the method.**

---

## Configuring Administrator Authentication

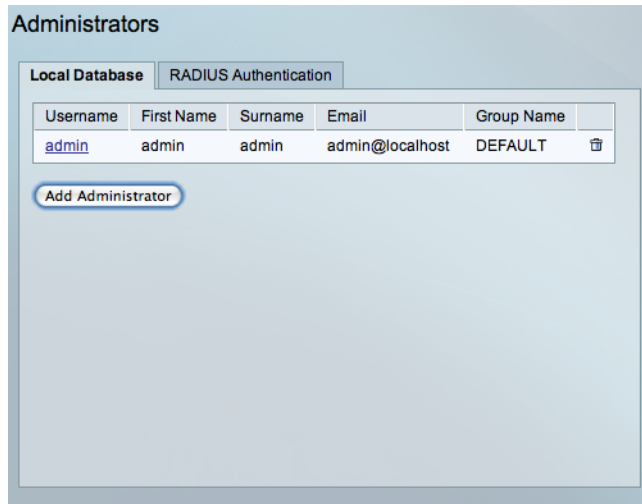
Cisco NAC Guest Server has a single default administrator account, called “admin.” You can additionally configure the Cisco NAC Guest Server to authenticate administrators against an external RADIUS server. The Admin Accounts pages under the Authentication menu allow you to create, edit and delete additional administrator accounts.

This section describes the following:

- [Add New Admin Account](#)
- [Edit Existing Admin Account](#)
- [Delete Existing Admin Account](#)
- [Admin Session Timeout](#)
- [Configuring RADIUS for Administrator Authentication](#)

### Add New Admin Account

- 
- Step 1** From the administration interface, select **Authentication > Administrators** from the left hand menu.
- Step 2** In the Local Database tab of the Administrators page as shown in [Figure 3-14](#), click the **Add Administrator** button.

**Figure 3-14 Administrator Accounts**

**Step 3** In the Add Administrator page as shown in [Figure 3-15](#), enter all the admin user credentials.

**Figure 3-15 Add Admin User**

The screenshot shows the 'Add An Administrator Account' page with the 'Local Database' tab selected. The page contains the following text and form fields:

Administrator Accounts can change the settings of the Guest Access Portal

First Name:

Surname:

Email:

Username:

Password:  Confirm:

Buttons: Add Administrator, Cancel

- 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.
- Confirm—Retype the password for the admin account

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

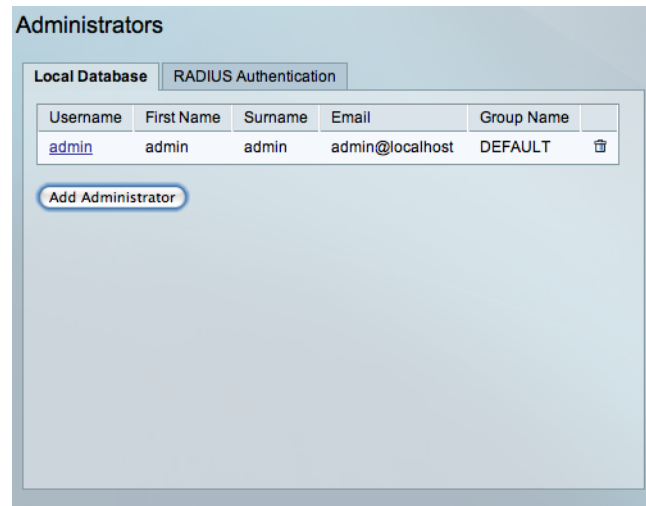
- If there are any errors, the account is not added and an error message is displayed at the top of the page.
- If successfully added, a success message is displayed at the top of the page and you can add additional admin accounts.

## 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.
- Step 2** In the Local Database tab of the Administrators page as shown in [Figure 3-16](#), click the username from the list.

**Figure 3-16** Admin Users to Edit



- Step 3** In the Edit Administrator page as shown in [Figure 3-17](#), edit the user credentials.

Figure 3-17 Edit Admin Account

**Edit An Administrator Account**

**Local Database**

Administrator Accounts can change the settings of the Guest Access Portal

Username: admin

First Name:

Surname:

Email:

Password:  Confirm:

If you don't wish to change the password please keep the entry empty.

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



**Note** Cisco recommends using a strong password that is not based on a dictionary word, has a minimum of 6 characters, and contains at least 5 different characters.



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

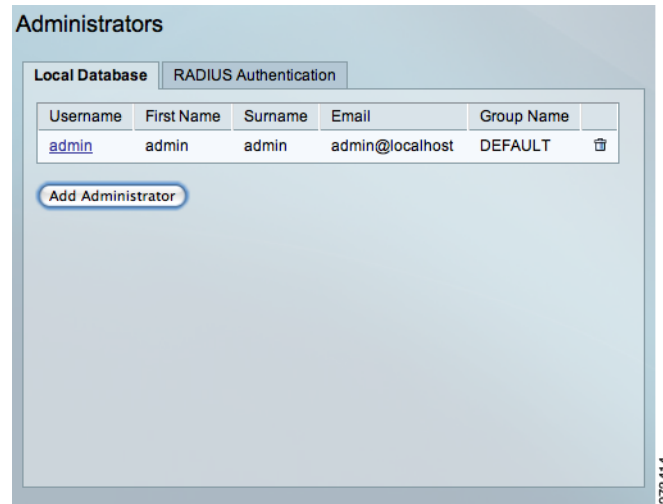
**Step 4** Click the **Save Settings** button.

- If there are any errors, the account is not changed and an error message is displayed at the top of the page.
- If successfully changed, a success message is displayed 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 3-18** Select Admin Account to Delete

- Step 2** In the Admin Accounts page as shown in [Figure 3-18](#), click the bin icon at the end of the user entry that you want to delete.
- Step 3** When prompted, click **OK** to delete the user or click **Cancel** to cancel the deletion. If successfully deleted, a success message is displayed at the top of the page.

## Admin Session Timeout

The Session Timeout defined for the Sponsor interface also applies to the Administration interface. See [Session Timeouts, page 4-20](#) for details.

## Configuring RADIUS for Administrator Authentication



### Note

Cisco NAC Guest Server only allows access to admin users who are successfully authenticated. The RADIUS server must return the IETF Service-Type attribute set to 6 (administrative).

As an alternative to configuring local administrator accounts, you can configure admin users to be authenticated over RADIUS to a RADIUS server. To configure RADIUS authentication for Administrator Authentication, perform the following steps:

- Step 1** From the administration interface, select **Authentication > Administrators**.
- Step 2** Click the **RADIUS Authentication** tab as shown in [Figure 3-19](#).

Figure 3-19 Administrator RADIUS Authentication

**Administrator Accounts**

Local Database | **RADIUS Authentication**

**Primary Server**

Server IP Address:

Port:

RADIUS Secret:  Confirm:

---

**Secondary Server**

Server IP Address:

Port:

RADIUS Secret:  Confirm:

---

**Authentication Mode**

Only allow local user authentication if both RADIUS servers cannot be contacted:

192562

- Step 3** Type the **Server IP Address** for the Primary RADIUS Server.
- Step 4** Type the **Port** that RADIUS authentication is running on for that server (default is 1645 or 1812).
- Step 5** In the **RADIUS Secret** field, type the shared secret to be used between the RADIUS Server and the NAC Guest Server.
- Step 6** Confirm the secret to make sure that it is set correctly.
- Step 7** Enter details for a Secondary RADIUS Server. These details are used when the NAC Guest Server does not receive response from the Primary RADIUS Server. These fields are optional.
- Step 8** Check the **Authentication Mode** checkbox so that Local Admin account is allowed if both the RADIUS Servers cannot be contacted. If this option is unchecked, Local Admin account is allowed if authentication is denied for any one of the RADIUS Servers.
- Step 9** Click the **Save** button to save the Administrator RADIUS settings.