



Administering the CiscoWorks Server

The CiscoWorks Server includes administrative tools to ensure that the server is performing properly:

- [Using Basic Administrative Tools](#)
- [Managing Secure Connections](#)
- [Maintaining Log Files](#)
- [Performing Data Management Tasks](#)
- [Managing Back-End Processes](#)
- [Managing Jobs and Resources](#)
- [Managing Network Events](#)
- [Exporting and Importing User Information](#)

Using Basic Administrative Tools

You can use these basic administrative tools to perform tasks described in [Table 4-1](#).

Table 4-1 Basic Administrative Tasks

Task	Purpose	Action
View installed software packages.	Lists installed software packages.	Select Server Configuration > Administration > Package Options
View log file status.	Displays log file size and utilization.	Select Server Configuration > Administration > Log File Status
View SSL compliance	Displays whether the installed applications are SSL compliant.	Select Server Configuration > About the Server > Applications and Versions

Managing Secure Connections

CiscoWorks Server provides secure access between the client browser and management server and also between the management server and devices. It uses Secure Socket Layer (SSL) encryption to provide secure access between the client browser and management server, and Secure Shell (SSH) to provide secure access between the management server and devices.

Based on whether you want to use secure access between the client browser and the management server, you can enable or disable SSL from the CiscoWorks desktop.

**Note**

If your CiscoWorks Server is integrated with any Network Management Station (NMS) in your network using the Network Management Integration Utility (NMIM), you must perform the integration every time you enable or disable SSL in the CiscoWorks Server. This is required to update the application registration in the NMS. For more information, see the Integrating with Third-Party Vendors section in CiscoView online help.

To use the secure access features provided in CiscoWorks Server, you must have the security certificate files on your system. You can either generate self-signed certificates from CiscoWorks Server desktop or obtain certificates from other agencies and use them to enable SSL in CiscoWorks Server. For more information, see [“Creating Self-Signed Security Certificates” section on page 4-15](#).

You cannot enable SSL if there is a non-SSL compliant application installed on the CiscoWorks server.

**Note**

You must have administrative privileges in CiscoWorks to enable and disable SSL and to manage the security certificates.

Enabling SSL

CiscoWorks Server uses security certificates for authenticating secure access between the client browser and the management server. To enable SSL from the client browser, you must have the necessary security certificates on your system. For details on security certificates, see [“Managing Security Certificates” section on page 4-14](#).

CiscoWorks Server allows you to enable SSL:

- From the CiscoWorks desktop. For more information, see [“Enabling SSL From the CiscoWorks Desktop” section on page 4-4](#).

- Using the Command Line Interface (CLI). For more information, see [“Enabling SSL From the Command Line Interface \(CLI\)”](#) section on page 4-5.

**Note**

If you have non-SSL compliant applications installed on the server, SSL cannot be enabled in CiscoWorks Server.

Enabling SSL From the CiscoWorks Desktop

To enable SSL from the CiscoWorks desktop:

-
- Step 1** In the CiscoWorks desktop, select **Server Configuration > Administration > Security Management > Enable/Disable SSL**.

The Configure SSL window appears in the right frame.

- Step 2** Click the Enable button.
-

If you have the required security certificates available on the server, CiscoWorks enables SSL. If you do not have the security certificates on the server, CiscoWorks prompts you to create your own self-signed certificate. For more information, see [“Creating Self-Signed Security Certificates”](#) section on page 4-15.

To complete the task of enabling SSL:

-
- Step 1** Log out from your CiscoWorks session and close all browser sessions.

- Step 2** Restart the daemon manager from the CiscoWorks Server CLI:

On Windows:

- Enter `net stop crmdmgtd`
- Enter `net start crmdmgtd`

On Solaris:

- Enter `/etc/init.d/dmgtd stop`
- Enter `/etc/init.d/dmgtd start`

Step 3 Restart the browser and the CiscoWorks session.

When you restart the CiscoWorks session after enabling SSL, you must enter the URL with the following changes:

- The URL should begin with *https* instead of *http* to indicate secure connection. CiscoWorks will automatically redirect you to https mode if SSL is enabled.
- The port number suffix should be changed from *1741* to *1742*

**Note**

If you do not make the above changes, CiscoWorks Server will automatically redirect you to *http*s mode with port number *1742*. The port numbers mentioned above are applicable for CiscoWorks Server running on Windows.

On Solaris, if the default port (*1741*) is used by another application, you can select a different port during CiscoWorks Server installation. For details, see *Installation and Setup Guide for CiscoWorks Common Services on Solaris*.

Enabling SSL From the Command Line Interface (CLI)

To enable SSL from a Windows CLI:

Step 1 Go to the command prompt.

Step 2 Navigate to the directory `NMSROOT\lib\web`.

Step 3 Enter `<NMSROOT>\bin\perl ConfigSSL.pl -enable`

Step 4 Press **Enter**.

If you have the required security certificates available on the server, CiscoWorks enables SSL.

If you do not have the security certificates on the server, CiscoWorks prompts you to create your own self-signed certificate. It also prompts you to enter the details needed to create a self-signed certificate.

Step 5 Enter the values required for the fields described in the table below:

Field	Description	Usage Notes
Country Name	Name of country	Use two character country code
State or Province	Name of state or province	Use two character state or province code or the complete name of the state or province
Locality	Name of city or town	Use two character city or town code or the complete name of the city or town
Organization Name	Name of your organization	Use complete name of your organization or an abbreviation
Organization Unit Name	Name of department or section	Use complete name of your department or an abbreviation
Host Name	Name of server where CiscoWorks Server is installed	Use exact DNS name of the server or the IP address of the server

CiscoWorks Server creates the security certificate. The process generates the following files:

- server.key—Server private key
- server.crt—Server self-signed certificate
- server.pk8—Server private key in PKCS#8 format
- server.csr—Certificate Signing Request (CSR) file. You can use this file to request a security certificate, if you want to use third party issued security certificates. For more information, see [“Obtaining Security Certificates for CiscoWorks” section on page 4-19.](#)



Note Back up the files and store them in a safe location; you need these files to enable secure connections in CiscoWorks.

The `server.key` file is particularly important, as this file holds the private key information for the server. If you lose the `server.key` file, you will not be able to use the self-signed certificate or upload a certificate (corresponding to the private key) you received from the Certificate Authority (CA).

These files are available at `NMSROOT\lib\web\conf`

This security certificate will be valid for a year, from the date of creation. You can use this certificate to enable SSL in CiscoWorks Server from your client browser.

To complete the task of enabling SSL:

Step 1 Log out from your CiscoWorks session and close all browser sessions.

Step 2 Restart the daemon manager from the CiscoWorks Server CLI:

- a. Enter `net stop crmdmgt`.
- b. Enter `net start crmdmgt`.

Step 3 Restart the browser and CiscoWorks session.

When you restart the CiscoWorks session after enabling SSL, you must enter the URL with the following changes:

- The URL should begin with `https` instead of `http` to indicate secure connection. CiscoWorks will automatically redirect you to https mode if SSL is enabled.
- The port number succeeding the server name should be changed from `1741` to `1742`



Note The port numbers mentioned above are applicable for CiscoWorks Server running on Windows.

On Solaris, if the default port (1741) is used by another application, you can select a different port during CiscoWorks Server installation. For details, see *Installation and Setup Guide for CiscoWorks Common Services on Solaris*.

To enable SSL from a Solaris CLI:

Step 1 Using a terminal window, navigate to the directory `$NMSROOT/objects/web/bin`.

Step 2 Enter `./ConfigSSL.pl -enable`

Step 3 Press **Enter**.

If you have the required security certificates available on the server, CiscoWorks enables SSL.

If you do not have the security certificates on the server, CiscoWorks prompts you to create your own self-signed certificate and for the details required for creating a self-signed certificate.

Step 4 Enter the values required for the fields described in the table below:

Field	Description	Usage Notes
Country Name	Name of country	Use two character country code
State or Province	Name of state or province	Use two character state or province code or complete name of state or province
Locality	Name of city or town	Use two character city or town code or complete name of the city or town
Organization Name	Name of your organization	Use complete name of your organization or an abbreviation
Organization Unit Name	Name of department or section	Use complete name of your department or an abbreviation

Field	Description	Usage Notes
Host Name	Name of server where CiscoWorks Server is installed	Use exact DNS name of the server or the IP address of the server
Country Name	Name of country	Use two character country code

CiscoWorks Server creates the security certificate. The process generates the following files:

- server.key—Server private key
- server.crt—Server self-signed certificate
- server.pk8—Server private key in PKCS#8 format
- server.csr—Certificate Signing Request (CSR) file. You can use this file to request a security certificate, if you want to use third party issued security certificates. For more information, see the [“Obtaining Security Certificates for CiscoWorks”](#) section on page 4-19.



Note Back up these files and store them in a safe location, as you need these files to enable secure connections in CiscoWorks. The server.key file is particularly important, as this file holds the private key information for the server. If you lose the server.key file, you will not be able to use the self-signed certificate or upload a certificate (corresponding to the private key) you received from the CA.

- These files are available at `$NMSROOT/objects/web/conf`

This security certificate is valid for one year from the date of creation. You can use this certificate to enable SSL in CiscoWorks Server from your client browser.

To complete the task of enabling SSL:

Step 1 Log out from your CiscoWorks session and close all browser sessions.

Step 2 Restart the daemon manager from the CiscoWorks Server CLI:

- a. Enter `/etc/init.d/dmgtm stop`.
- b. Enter `/etc/init.d/dmgtm start`.

Step 3 Restart the browser and CiscoWorks session.

When you restart the CiscoWorks session after enabling SSL, you must enter the URL with the following changes:

- The URL should begin with *https* instead of *http* to indicate secure connection. CiscoWorks will automatically redirect you to https mode if SSL is enabled.
- The port number succeeding the server name should be changed from *1741* to *1742*



Note

The port numbers mentioned above are applicable for CiscoWorks Server running on Windows. On Solaris, if the default port (1741) is used by another application, you can select a different port during CiscoWorks Server installation. For more information, see *Installation and Setup Guide for CiscoWorks Common Services on Solaris*.

Disabling SSL

CiscoWorks Server does not allow SSL-compliant applications to co-exist with non-SSL compliant applications on the same server. When you need to install a non-SSL compliant application after enabling SSL on the server, you must disable SSL in CiscoWorks Server before you proceed with the installation.

You may want to disable SSL in cases where improved performance takes precedence over secure connections.

CiscoWorks Server provides the following ways to disable SSL:

- Disabling SSL from the CiscoWorks desktop—for details, see the [“Disabling SSL from the CiscoWorks Desktop”](#) section on page 4-11.
- Disabling SSL using the Command Line Interface (CLI)—for details, see the [“Disabling SSL From CLI”](#) section on page 4-12.

Disabling SSL from the CiscoWorks Desktop

To disable SSL from CiscoWorks desktop:

-
- Step 1** In the CiscoWorks desktop, select **Server Configuration > Administration > Security Management > Enable/Disable SSL**.
The Configure SSL window appears in the right frame.
- Step 2** Click the Disable button.
-

To complete the task of disabling SSL from desktop:

-
- Step 1** Log out from your CiscoWorks session and close all browser sessions.
- Step 2** Restart the daemon manager from the CiscoWorks Server CLI:
- On Windows:
- a. Enter `net stop crmdmgtd`
 - b. Enter `net start crmdmgtd`
- On Solaris:
- a. Enter `/etc/init.d/dmgtd stop`
 - b. Enter `/etc/init.d/dmgtd start`

Step 3 Restart the browser and CiscoWorks session.

When you restart the CiscoWorks session after enabling SSL, you must enter the URL with the following changes:

- The URL should begin with *http* instead of *https* to indicate that the connection is not secure
- The port number succeeding the server name should be changed from *1742* to *1741*



Note The port numbers mentioned above are applicable for CiscoWorks Server running on Windows.

On Solaris, if the default port (1741) is used by another application, you can select a different port during CiscoWorks Server installation. For more information, see *Installation and Setup Guide for CiscoWorks Common Services on Solaris*.

Disabling SSL From CLI

You can disable SSL using the CLI from the server where CiscoWorks is installed.

To disable SSL from Windows CLI:

Step 1 Go to the command prompt.

Step 2 Navigate to the directory *NMSROOT\lib\web*.

Step 3 Enter `<NMSROOT>\bin\perl ConfigSSL.pl -disable`

Step 4 Press **Enter**.

To complete the task of disabling SSL from CLI:

Step 1 Log out from your CiscoWorks session and close all browser sessions.

Step 2 Restart the daemon manager from the CiscoWorks Server CLI:

a. Enter `net stop crmdmgt`

b. Enter `net start crmdmgt`

Step 3 Restart the browser and CiscoWorks session.

When you restart the CiscoWorks session after enabling SSL, you must enter the URL with the following changes:

- The URL should begin with *http* instead of *https* to indicate that the connection is not secure
- The port number succeeding the server name should be changed from *1742* to *1741*



Note The port numbers mentioned above are applicable for CiscoWorks Server running on Windows.

On Solaris, if the default port (1741) is used by another application, you can select a different port during CiscoWorks Server installation. For more information, see *Installation and Setup Guide for CiscoWorks Common Services on Solaris*.

To disable SSL from Solaris CLI:

Step 1 In the terminal window, navigate to the directory `$NMSROOT/objects/web/bin`.

Step 2 Enter `./ConfigSSL.pl -disable`

Step 3 Press **Enter**.

To complete the task of disabling SSL from CLI:

Step 1 Log out from your CiscoWorks session and close all browser sessions.

Step 2 Restart the daemon manager from the CiscoWorks Server CLI:

a. Enter `/etc/init.d/dmgttd stop`

b. Enter `/etc/init.d/dmgttd start`

Step 3 Restart the browser and CiscoWorks session.

When you restart the CiscoWorks session after enabling SSL, you must enter the URL with the following changes:

- The URL should begin with *http* instead of *https* to indicate that the connection is not secure
- The port number succeeding the server name should be changed from *1742* to *1741*



Note

The port numbers mentioned above are applicable for CiscoWorks Server running on Windows.

On Solaris, if the default port (1741) is used by another application, you can select a different port during CiscoWorks Server installation. For more information, see *Installation and Setup Guide for CiscoWorks Common Services on Solaris*.

Managing Security Certificates

CiscoWorks Server uses security certificates for authenticating secure access between client browser and management server. You must have the security certificate files on the server to use the secure access features provided in CiscoWorks Server.

CiscoWorks Server allows you to generate self-signed certificates. However, you can obtain certificates from third party Certificate Authorities (CAs) and use them to enable SSL in CiscoWorks Server.

Creating Self-Signed Security Certificates

CiscoWorks allows you to create self-signed security certificates, which can be used to enable SSL connections between your client browser and management server. These security certificates are valid for a year. When the certificate expires, the browser prompts you to renew the certificate.

When you enable SSL for the first time, CiscoWorks Server prompts you to create a self-signed security certificate or upload an existing certificate. You can create self-signed security certificate and enable SSL.

CiscoWorks Server also provides an option to create self-signed security certificates, which can be used when required. You can create self-signed security certificates:

- From the CiscoWorks Server desktop. You can use this option from the client browser and from a browser session on the server where CiscoWorks Server is installed. For details, see the [“Creating Self-Signed Security Certificates From CiscoWorks Server Desktop”](#) section on page 4-15.
- From the CLI. You can create self-signed certificates from CLI when you enable SSL from the CLI. For more information, see the [“Enabling SSL From the Command Line Interface \(CLI\)”](#) section on page 4-5.

Creating Self-Signed Security Certificates From CiscoWorks Server Desktop

To create your own self-signed security certificates from the CiscoWorks desktop:

Step 1 In the CiscoWorks desktop, select **Server Configuration > Administration > Security Management > Create Self Signed Certificates**.

The Create Certificates window appears in the right frame.

Step 2 Enter the values required for the fields described in the table below:

Field	Description	Usage Notes
Country Name	Name of country	Use two character country code
State or Province	Name of state or province	Use two character state or province code or complete name of state or province

Field	Description	Usage Notes (continued)
Locality	Name of city or town	Use two character city or town code or complete name of city or town
Organization Name	Name of your organization	Use complete name of your organization or an abbreviation
Organization Unit Name	Name of department or section	Use complete name of your department or an abbreviation
Host Name	Name of server where CiscoWorks Server is installed	Use the exact DNS name of server or IP address of the server
Email Address	Your email address	None

Step 3 Click **Finish**.

CiscoWorks Server creates the security certificate. The process generates the following files:

- server.key—Server private key
- server.crt—Server self-signed certificate
- server.pk8—Server private key in PKCS#8 format
- server.csr—Certificate Signing Request (CSR) file. You can use this file to request a security certificate, if you want to use third party issued security certificates. For more information, see the [“Obtaining Security Certificates for CiscoWorks”](#) section on page 4-19.

**Note**

Back up these files and store them in a safe location, as you need these files to enable secure connections in CiscoWorks. The server.key file is particularly important, as this file holds the private key information for the server. If you lose the server.key file, you will not be able to use the self-signed certificate or upload a certificate (corresponding to the private key) you received from the CA.

You can find these files at:

- On Windows: *NMSROOT\lib\web\conf*
- On Solaris: *\$NMSROOT/objects/web/conf*

This security certificate will be valid for one year from the date of creation. You can use this certificate to enable SSL in CiscoWorks Server from your client browser.

Modifying Security Certificates

CiscoWorks Server allows you to modify the self-signed security certificates using the Create Self Signed Certificates option. If you have valid self-signed security certificates on the server, the Create Self Signed Certificates option in the CiscoWorks desktop brings up the details of the existing self-signed certificate in the Create Certificates window.

To modify self-signed certificates:

-
- Step 1** In the CiscoWorks desktop, select **Server Configuration > Administration > Security Management > Create Self Signed Certificates**.

The Create Self Signed Certificates window displays the details of the existing certificate.

- Step 2** Modify the values as required.

- Step 3** Click **Submit**.

For more information, see the [“Creating Self-Signed Security Certificates From CiscoWorks Server Desktop”](#) section on page 4-15.



Note

When you modify the certificate, the validity period is calculated from the day you last modified the certificate.

You cannot modify third party CA certificates from the CiscoWorks desktop.

Working with Third Party Security Certificates

CiscoWorks Server provides an option to use security certificates issued by third party Certificate Authorities (CAs). You may want to use this option in cases where your organizational policy prevents you from using CiscoWorks self-signed certificates or requires you to use security certificates obtained from a particular CA.

The option to upload third party certificates allows you to obtain security certificates from your preferred CA and use them instead of the CiscoWorks self-signed certificates. You can use these certificates to enable SSL when you need secure access between CiscoWorks Server and your client browser.

Requirements for Third Party Certificates

CiscoWorks requires the certificates (both self-signed and those issued by a certificate authority) used for establishing secure connections to meet the following criteria:

- The certificates should be in [Base64- Encoded X.509 Certificate Format](#)
- The certificates should not be encrypted, or password protected

Note the following before you upload certificates issued by a CA:

- CiscoWorks requires you to follow specific procedures for obtaining and uploading the certificate to the CiscoWorks Server. You must follow these instructions, and should not go by the instructions given by the Certificate Authority (CA) who issued the certificate. For more information, see the [“Obtaining Security Certificates for CiscoWorks” section on page 4-19](#).
- You cannot upload any existing certificate on the server or elsewhere into CiscoWorks Server. You must request the Certificate Authority to create a certificate explicitly for CiscoWorks, and upload it. For more information, see the [“Obtaining Security Certificates for CiscoWorks” section on page 4-19](#).
- You can obtain a certificate from a CA of choice, based on your organization’s preferences and policies. However, you must verify if the CA will issue the certificates that meet the criteria specified for CiscoWorks. You must complete the legal obligations, if any, are involved in obtaining the certificate.

- Before you request for the security certificate for CiscoWorks, you must confirm if the CA can issue certificates for Apache Web Servers.
- CiscoWorks allows you to upload:
 - Single certificate (signed directly by the root CA)
 - or
 - Certificate chains (server certificate with intermediate certificates)
- While uploading the Server Certificate, you have to upload the intermediate certificates (if required). If the server certificate is not issued by a prominent CA, you must upload the root CA certificate also, as part of the chain.
- When you upload a certificate chain, ensure that CiscoWorks recognizes the input certificates as valid certificates or valid certificate chains. To ensure this, you must upload the root CA certificate or intermediate certificates as part of the certificate chain.
- All the certificates should be in Base64 Encoded X.509 Certificate format.

Obtaining Security Certificates for CiscoWorks

After you receive the confirmation from the CA, you can initiate the process of obtaining a security certificate.

Obtaining security certificates for CiscoWorks from a CA involves:

1. [Creating the Certificate Signing Request \(CSR\) File](#) in CiscoWorks
2. [Applying for Security Certificates from the CA](#), using the CSR file

Creating the Certificate Signing Request (CSR) File

To create the Certificate Signing Request (CSR) file in CiscoWorks, you must enable SSL. You can enable SSL either from the CiscoWorks desktop or using the CLI.

If you are enabling SSL for the first time in CiscoWorks, you will be prompted for the details to create a self-signed certificate and the server.csr file.

For more information, see the [“Creating Self-Signed Security Certificates” section on page 4-15](#). If you have already enabled SSL and created self-signed certificates, the `server.csr` will be in the server already. You can find this file:

- On Windows: `NMSROOT\lib\web\conf`
- On Solaris: `$NMSROOT/objects/web/conf`

**Note**

The details required for the certificates should be entered correctly, especially the Host Name with proper domain name. The details you provide at this stage will be displayed in the server certificate (both self-signed or third party issued).

When you submit the details, CiscoWorks creates the following files:

- `server.key`—Server Private Key
- `server.crt`—Server self-signed Certificate
- `server.pk8`—Server private key in PKCS#8 format
- `server.csr`—Certificate Signing Request (CSR) file

You can find these files:

- On Windows: `NMSROOT\lib\web\conf`
- On Solaris: `$NMSROOT/objects/web/conf`

**Note**

Back up these files and store them in a safe location, as you need these files to enable secure connections in CiscoWorks. The `server.key` file is particularly important, as this file holds the private key information for the server. If you lose the `server.key` file, you will not be able to use the self-signed certificate or upload a certificate (corresponding to the private key) you received from the CA.

Applying for Security Certificates from the CA

After you generate the `server.csr` file from CiscoWorks, you can request the security certificate from the CA. You can obtain the certificate from a CA of choice, based on your organization's preferences and policies. If the CA is not one of repute, it is recommended that you request for a Root CA certificate, used for signing the CiscoWorks security certificates, also from the CA.

**Note**

You can verify if the Root CA certificate of the CA is already available in CiscoWorks Server by running the SSL Utility Script (`SSLUtil.pl`). For more information, see the [“About the SSL Utility Script” section on page 4-23](#).

When you apply for the security certificate, ensure that:

- The CA issues the certificates meeting the criteria specified for CiscoWorks. For more information, see the [“Requirements for Third Party Certificates” section on page 4-18](#).
- All the legal requirements for obtaining the certificate, if any, are met.
- The `server.csr` file generated from CiscoWorks is used to obtain the certificate. Typically, you can send the `server.csr` file to the certificate authority, or copy the contents of the file and paste it in the appropriate field, if you are using an online form to submit the request.

**Note**

To copy the contents of the `server.csr` file, you must open this file in a plain text editor such as Vi or Notepad. Do not open this file in editors such as Microsoft Word, which may add special characters to the contents of the file.

Certificate authorities request a host of information when you apply for security certificates. In addition to the `server.csr` file, you may need to provide the following details specific to the CiscoWorks Server:

- Web Server—select Apache MODSSL, Apache SSL or Apache (from the list of available web servers, in the order)
- Web Server version—1.3.27

Uploading Third Party Security Certificates to CiscoWorks Server

You may receive the security certificates from the CA in the form of files or mail attachments. If you have received these as files, copy these files to a directory in the CiscoWorks Server. If you received the certificates in the form of a mail, copy the contents and create separate files for each of the certificates (server certificate and intermediate certificates).

**Note**

While copying the contents of the certificate files, you must use a plain text editor such as Vi or Notepad. Do not open this file in editors such as Microsoft Word, which may add special characters to the contents of the file.

If the certificates are in a different format, contact the CA and request for the certificates to be sent in the required format. You can also get the procedure to change the existing format to the format required for CiscoWorks Server.

The instruction you receive from the CA to change the format may require you to run some commands using OpenSSL. OpenSSL is provided as part of the CiscoWorks Server package. You can find OpenSSL:

- On Windows: *NMSROOT\lib\web*
- On Solaris: *\$NMSROOT/objects/web/bin*

**Tip**

Windows recognizes most of the certificate formats and has the options to convert from one format to another. Therefore, if you received the security certificates in a format other than what is required by CiscoWorks Server, you can copy the Certificate to a Windows machine and use these options to convert them to the required format.

After you have the server certificate and the required intermediate certificates in the required format, you must run the SSL Utility script to verify the certificate or certificate chain, and then to upload them to the CiscoWorks Server.

You must do the following while uploading third party certificates to CiscoWorks Server:

- Stop the daemon manager in CiscoWorks Server
- Use SSL Utility script only to upload the certificate to the CiscoWorks server

- Follow the instructions provided in [“Using the SSL Utility Script to Upload Third Party Security Certificates”](#) section on page 4-28 to upload the certificates. Do not use the CA’s Instructions to install the certificate in the CiscoWorks Server.
- Do not copy the certificates manually to any of the directories in the CiscoWorks Server
- Do not edit the httpd.conf file manually

About the SSL Utility Script

The SSL Utility script (SSLUtil.pl) is provided to upload the security certificates you obtain from the CAs to the CiscoWorks Server. You can find the SSL Utility script:

- On Windows: *NMSROOT\lib\web*
- On Solaris: *\$NMSROOT/objects/web/bin*

This utility has the following options:

Number	Option	What it Does...
1	Display CiscoWorks Server certificate information	<ul style="list-style-type: none"> • Displays the Certificate details of the CiscoWorks Server. In the case of third party issued certificates, this option displays the details of the server certificate, the intermediate certificates, if any, and the Root CA certificate. • Verifies if the certificate is valid
2	Display the input certificate information	<p>This option accepts a certificate as an input and:</p> <ul style="list-style-type: none"> • Verifies if the certificate is in Base64 Encoded X.509 certificate format • Displays subject and issuer details of the certificate • Verifies if the certificate is valid on the server

Number	Option	What it Does... (continued)
3	Display Root CA certificates trusted by CiscoWorks Server	<p>Generates a list of all Root CA Certificates, and stores it in the SSL.log file.</p> <p>You can find the SSL.log at:</p> <ul style="list-style-type: none"> • On Windows: <i>NMSROOT\log</i> • On Solaris: <i>/var/adm/CSCOPx/log</i>
4	Verify the input certificate or certificate chain	<p>Verifies whether the server certificate issued by third party CAs, can be uploaded.</p> <p>When you choose this option, the utility:</p> <ul style="list-style-type: none"> • Verifies if the certificate is in Base64 Encoded X.509Certificate format • Verifies if the certificate is valid on the Server • Verifies if the server private key and input server certificate match • Verifies if the server certificate can be traced to the required Root CA certificate using which it was signed • Constructs the certificate chain, if the intermediate chains are also given, and verifies if the chain ends with the proper Root CA certificate <p>After the verification is successfully completed, you are prompted to upload the certificates to CiscoWorks Server.</p> <p>The utility displays an error:</p> <ul style="list-style-type: none"> • If the input certificates are not in required format • If the certificate date is not valid or if the certificate has already expired • If the server certificate could not be verified or traced to a root CA certificate

Number	Option	What it Does... (continued)
4 (continued)		<ul style="list-style-type: none"> • If any of the intermediate Certificates were not given as input. • If the server's private key is missing or if the server certificate that is being uploaded could not be verified with the server's private key. <p>You must contact the CA who issued the certificates to correct these problems before you upload the certificates to CiscoWorks.</p>
5	Upload single server certificate to CiscoWorks Server	<p>You must verify the certificates using option 4 before you select this option.</p> <p>Select this option, only if there are no intermediate certificates and there is only the server certificate signed by a prominent Root CA certificate.</p> <p>If the Root CA is not one trusted by CiscoWorks, do not select this option.</p> <p>In such cases, you must obtain a Root CA certificate used for signing the certificate from the CA and upload both the certificates using option 6.</p> <p>When you select this option, and provide the location of the certificate, the utility:</p> <ul style="list-style-type: none"> • Verifies if the certificate is in Base64 Encoded X.509 certificate format • Displays subject and issuer details of the certificate • Verifies if the certificate is valid on the server

Number	Option	What it Does... (continued)
5 (continued)		<ul style="list-style-type: none"> • Verifies if the server private key and input server certificate match • Verifies if the server certificate can be traced to the required Root CA certificate using which it was signed <p>After the verification is successfully completed, the utility uploads the certificate to CiscoWorks Server. For more information, see “Uploading Third Party Security Certificates to CiscoWorks Server” section on page 4-22.</p> <p>The utility displays an error:</p> <ul style="list-style-type: none"> • If the input certificates are not in required format • If the certificate date is not valid or if the certificate has already expired • If the server certificate could not be verified or traced to a root CA certificate • If the server's private key is missing or if the server certificate that is being uploaded could not be verified with the server's private key <p>You must contact the CA who issued the certificates to correct these problems before you upload the certificates in CiscoWorks again.</p>
6	Upload a certificate chain to CiscoWorks Server	<p>You must verify the certificates using option 4 before you select this option.</p> <p>Select this option, if you are uploading a certificate chain. If you are uploading the root CA certificate also, you must include it as one of the certificates in the chain.</p>

Number	Option	What it Does... (continued)
6 (continued)		<p>When you select this option, and provide the location of the certificates, the utility:</p> <ul style="list-style-type: none"> • Verifies if the certificate is in Base64 Encoded X.509Certificate format • Displays subject and issuer details of the certificate • Verifies if the certificate is valid on the Server • Verifies if server private key and the server certificate match • Verifies if the server certificate can be traced to the root CA certificate using which it was signed • Constructs the certificate chain, if intermediate chains are given and verifies if the chain ends with the proper root CA certificate <p>After the verification is successfully completed, the server certificate is uploaded to CiscoWorks Server. All the intermediate certificates and the Root CA certificate are uploaded and copied to the CiscoWorks TrustStore.</p> <p>The utility displays an error:</p> <ul style="list-style-type: none"> • If the input certificates are not in required format • If the certificate date is not valid or if the certificate has already expired • If the server certificate could not be verified or traced to a root CA certificate

Number	Option	What it Does... (continued)
6 (continued)		<ul style="list-style-type: none"> If any of the intermediate certificates were not given as input. If the server's private key is missing or if the server certificate that is being uploaded could not be verified with the server's private key <p>You must contact the CA who issued the certificates to correct these problems before you upload the certificates in CiscoWorks again.</p>
7	Modify Common Services Certificate	<p>This option allows you to modify the Host Name entry in the Common Services Certificate.</p> <p>You can enter an alternate Hostname if you wish to change the existing Host Name entry.</p>

Using the SSL Utility Script to Upload Third Party Security Certificates

To upload the certificates:

-
- Step 1** Stop the daemon manager from the CiscoWorks Server CLI:
- On Windows:
- Enter `net stop crmdmgt`
- On Solaris:
- Enter `/etc/init.d/dmgt stop`
- Step 2** Navigate to the directory where the SSL Utility script is located.
- On Windows:
- Go to `NMSROOT\lib\web`.
 - Enter `NMSROOT\bin\perl SSLUtil.pl`.
- On Solaris:
- Go to `$NMSROOT/objects/web/bin`.
 - Enter `./SSLUtil.pl`.

Step 3 Select option **4**, Verify the input Certificate/Certificate Chain.

Step 4 Enter the location of the certificates (server certificate and intermediate certificate).

The script verifies if the server certificate is valid. After the verification is complete, the utility displays the options described in [About the SSL Utility Script, page 4-23](#).



Note If the script reports errors during validation and verification, the SSL Utility displays instructions to correct these errors. Follow the instructions to correct those errors.

Step 5 Select option **5**, if you have only one certificate to upload, that is if you have a server certificate signed by a Root CA certificate.

Select option **6**, if you have a certificate chain to upload, that is if you have a server certificate and intermediate certificates.



Note CiscoWorks Server does not allow you to proceed with the upload if you have not stopped the CiscoWorks daemon manager.

Step 6 Enter the required details—location of the certificate, if there are intermediate certificates, and location of intermediate certificates, if any.

SSL Utility uploads the certificates, if all the details are correct and the certificates meet CiscoWorks requirements for security certificates.

Step 7 Restart the daemon manager for the new security certificate take effect.



Note The utility displays a warning message if there are hostname mismatches detected in the server certificate being uploaded, but you can continue to upload the certificate.

Maintaining Log Files

Log files can grow and fill up disk space. CiscoWorks includes a script that enables you to control this growth.

Files maintained by this script include the following log files:

- Daemon manager
- JRUN
- Web server log files

Most log files are located in directories in the PX_LOGDIR directory. On UNIX systems, this directory is `/var/adm/CSCOpX/log` and on Windows, it is `NMSROOT\log`.

JRUN files are not located here. On UNIX machines they are located under `$NMSROOT/objects/jrun/jsm-cw2000/logs` and on Windows, they are located in `NMSROOT\lib\jrun\jsm-cw2000\logs`.



Caution

As part of the file back-up procedure, CiscoWorks daemon manager is shut down and restarted. To prevent loss of data, make sure you are not running any critical tasks.

Maintaining Log Files on UNIX

To maintain log files on UNIX:

-
- Step 1** Make sure the new location has sufficient disk space.
 - Step 2** Log in as the superuser and enter the root password.
 - Step 3** Stop all processes and enter `/etc/init.d/dmgtD stop`
 - Step 4** Perform log maintenance by entering:

```
$NMSROOT/bin/perl $NMSROOT/cgi-bin/admin/logBackup.pl
[-force] [-dir destination directory]
```

where `$NMSROOT` is the CiscoWorks installation directory, `-force` allows backup regardless of log file size, and `-dir` specifies the full path of the destination directory.



Note The target directory must be owned by user casuser and group casusers. The user must have read, write, and execute permissions, and the group must have at least read permission. Otherwise, the program will terminate with an error message and the log files will not be updated.

Without any options, the script backs up the log files to the default directory, PX_LOGDIR/backup.

Step 5 Verify the procedure was successful by examining the contents of the log files in this location:

`/var/adm/CSCOpX/log/*.log`

Only log files that reach 90% of their size limits are backed up and the original log file is emptied.

Step 6 Restart the system and enter `/etc/init.d/dmgtD start`

Step 7 Select **Server Configuration > Administration > Log File Status** to view your log changes.

Maintaining Log Files on Windows

To maintain log files on Windows:

Step 1 Make sure the new location has sufficient disk space.

Step 2 At the command line, make sure you have the correct permissions.

Step 3 Stop all processes by entering:

```
net stop crmdmgtD
```

Step 4 Perform log maintenance by entering:

```
NMSROOT\bin\perl NMSROOT\cgi-bin\admin\logBackup.pl  
[-force][-dir destination directory]
```

where *NMSROOT* is the CiscoWorks installation directory, *-force* allows backup regardless of log file size, and *-dir* specifies the full path of the destination directory.



Note If there is a problem, the program will terminate with an error message and the log files will not be updated.

Step 5 Verify the procedure was successful by examining the contents of the log files in the following location:

NMSROOT\log

Only log files that reach 90% of their size limits are backed up and the original log file is emptied.

Step 6 Restart the system by entering:

```
net start crmdmgt
```

Step 7 Select **Server Configuration > Administration > Log File Status** to view your log changes.

Performing Data Management Tasks

Regularly perform storage management tasks (see [Table 4-3](#)) to ensure that you have a set of database backups in case your current database becomes corrupted or otherwise unusable. When setting up your database backup strategy, consider these guidelines:

- Check the size of the files stored in the backup directory. Some files stored in the backup directory might require additional disk space.
- The backup directory must be writeable by the user casuser on UNIX systems.
- Database files are stored using the backup directory structure described in [Table 4-2](#):
 - Format—*/generation_number/suite/directory/filename*
 - Example—*/1/cmf/database/cmf.db*

Table 4-2 Backup Directory Structure

Variable	Description	Usage Notes
generation_number	Indicates number of backups	For example, 1, 2, and 3, with 3 being the latest database backup.
suite	Describes application or suite	The CiscoWorks Server suite is <i>cmf</i> . Other optional suites are supported, such as <i>rme</i> or <i>ani</i> .
directory	Describes what is being stored	Directories include database and any suite applications.
filename	Name of file that has been backed up	Files include database (.db), log (.log), version (DbVersion.txt), manifest (.tx), tar (.tar), and data files (datafiles.txt).

The suite name used for the CiscoWorks Server database files is *cmf*. The *cmf* database includes data backup for the CiscoWorks Server applications. Data management tasks (see [Table 4-3](#)) for other suites are also supported.

For example, if a suite is installed that uses the ANI Server, the suite name for the ANI Server database files is *ani*. For more information, see the appropriate user guide for suite-specific details.

Table 4-3 Data Management Tasks

Task	Purpose	Action
Backup database	Performs a database backup now to ensure you have backups if current database becomes corrupted or otherwise unusable	Select Server Configuration>Administration>Database Management>Back Up Data Now
Schedule regular backups	Performs database backups on a regular schedule to ensure you have most-recent set of backups if current database becomes corrupted or otherwise unusable	Select Server Configuration>Administration>Database Management>Schedule Backup
Restore a database	Replaces damaged or corrupted database with a previously backed up copy	Run script from a command prompt. Refer to the Database Management online help for instructions.
Change the database password	Changes the database password to ensure security	Must be done as a superuser from a command prompt. Refer to the Database Management online help for instructions.

Backing Up Data

You can back up data on demand instead of waiting for the next scheduled backup by using the Backup Data option. It is recommended that your target location be on a different hard disk or partition than where CiscoWorks is installed. Database options work within the current version only and do not support other versions.

The Backup Data Now option is used to backup database for applications in the Lan Management Solution bundle like Essentials, Campus and so on.



Note

Backup requires enough storage space on the target location for the backup to start.

To backup the data:

-
- Step 1** Select **Server Configuration > Administration > Database Management > Back Up Data Now**.
- The Back Up Data Now dialog box appears.
- Step 2** Enter the pathname of the target directory.
- Step 3** To begin the backup, click **Finish**. This process could take some time to complete.
-

Scheduling a Backup

You can schedule automatic database backups using this option. Database options work within the current version only and do not support other versions. Follow the upgrade procedures for your platform to save your database information.

To schedule a backup:

-
- Step 1** Select **Server Configuration > Administration > Database Management > Schedule Backup**.
- The Set Backup Schedule dialog box appears.
- Step 2** Enter the following:
- a. Backup Directory—Location of the backup directory. It is recommended that your target location be on a different partition than where CiscoWorks is installed.
 - b. Generations—Number of database backup copies to retain. The system keeps only the number of copies you specify.
 - c. Time—From the drop-down lists, select the time for the backup to occur. Use a 24-hour format.
 - d. Frequency—Select the backup schedule (daily, weekly or monthly)
- Step 3** Click **Finish**. The Schedule Backup message verifies your schedule and provides the location of backup log files.
-

Restoring Data

You can restore your database by running a script from the command line. Database options work only within the current version. They do not support other versions. To save your database information, follow the upgrade procedures for your platform.

While restoring data, CiscoWorks is shut down and restarted. Ensure that you do not run any critical tasks during data restoration. Otherwise, you may lose the data for such tasks.



Note

If you restore the database when CiscoWorks server is SSL enabled, the backed up Server Certificate and Private Key will also be restored. Your existing Certificate and Private Key will be overwritten.



Caution

Restoring the database from a backup permanently replaces your database with the backed up version.

To restore the data on UNIX:

Step 1 Log in as the superuser and enter the root password.

Step 2 Stop all processes by entering:

```
/etc/init.d/dmgttd stop
```

Step 3 Restore the database by entering:

```
$NMSROOT/bin/perl $NMSROOT/bin/restorebackup.pl [-force] [-s suite] [-gen generationNumber] -d backup directory
```

where *\$NMSROOT* is the CiscoWorks installation directory and

- a. [-force]—Optional. Forces restoration of an old schema. For example, if the backup has several generations, there may be 1 through 5. If generation 2 is a much older schema than 5, the restorebackup complains that the schema is too old. The restorebackup process aborts. If a restorebackup -force is used, then restorebackup prompts for confirmation and the old schema will be restored.

- b. [-s suite]—Optional. By default, this option restores all suite's data. You can also specify a particular suite by this option. Refer to the appropriate user guide for suite-specific details.
- c. [-gen generationNumber]—Optional. By default, it is the latest generation. If generations 1 through 5 exist, then 5 will be the latest .
- d. -d backup directory—Required. Which backup directory to use.
- e. -h—Provides help when used with -d <backup directory> syntax. Shows correct syntax along with available suites and generations.

Step 4 To restore the most recent version, enter:

```
$NMSROOT/bin/perl $NMSROOT/bin/restorebackup.pl -d /var/backup
```

Step 5 Examine the log file in the following location to verify that the database was restored:

```
/var/adm/CSCOpX/log/restorebackup.log
```

Step 6 Restart the system:

```
/etc/init.d/dmgttd start
```

To restore the data on Windows:

At the command line (make sure you have the correct permissions):

Step 1 Stop all processes by entering:

```
net stop crmdmgttd
```

Step 2 Restore the database by entering:

```
NMSROOT\bin\perl NMSROOT\bin\restorebackup.pl [-force] [-s suite][-gen generationNumber] -d backup directory
```

where *NMSROOT* is the CiscoWorks installation directory. Refer to previous section for command option descriptions.

Step 3 To restore the most recent version, enter the following command:

```
NMSROOT\bin\restorebackup.pl -d drive:\var\backup\
```

Step 4 Examine the log file in the following location to verify that the database was restored by entering:

```
NMSROOT\log\restorebackup.log
```

Step 5 Restart the system by entering:

```
net start crmdmgtd
```

Managing Back-End Processes

CiscoWorks applications use back-end processes to manage application-specific activities or jobs. The process management tools enable you to manage these back-end processes to optimize or troubleshoot the CiscoWorks Server (see [Table 4-4](#)).

For a description of the CiscoWorks Server processes, see the process description table in the online help. For suite-specific processes, see the appropriate user guide.

Table 4-4 Process Management Tasks

Task	Purpose	Action
Start process.	Restarts specific processes and displays a message: <i>Running normally</i>	Select Server Configuration > Administration > Process Management > Start Process
Stop process.	Stops process and displays a message: <i>Administrator has shut down this server</i>	Select Server Configuration > Administration > Process Management > Stop Process
View processes.	Displays process information including state, ID, and other data	Select Server Configuration > Administration > Process Management > Process Status
View process failures.	Displays the failed process, failure information, and time failure occurred	Select Server Configuration > Diagnostics > Process Failures

Managing Jobs and Resources

Job Management provides job, resource, and event notification services to CiscoWorks. Use Job Management to browse jobs, release resources and stop and remove jobs (see [Table 4-5](#)).

Table 4-5 Job Management Tasks

Task	Purpose	Action
Cancel a scheduled job.	Stops job from running, but keeps it in the Job Management	Select Server Configuration > Administration > Job Management, then select Stop Job
Remove a job.	Removes job from the Job Management	Select Server Configuration > Administration > Job Management, then select Remove Job
Unlock an orphaned resource.	Frees resources inadvertently locked due to a system failure Use Free Resource only if there are no other options.	Select Server Configuration > Administration > Job Management, then select Free Resource

Managing Network Events

Two CiscoWorks services exist that allow you to manage events; some applications use one service, and some use the other. They are:

- [Event Distribution Service \(EDS\)](#)
- [Event Services Software \(ESS\)](#)
- [Creating Filters](#)

Event Distribution Service (EDS)

EDS allows you to manage event sources and event consumers. Event sources create network events and event consumers are the recipients of the events (see [Table 4-6](#)).

Table 4-6 Event Distribution Service Tasks

Task	Purpose	Action
Enable or disable debugging or trace message generation.	Diagnosis problems.	Select Server Configuration > Administration > Event Management > Event Channel Admin, then select Debug
Configure individual services.	Enables setup and configuration of event source or event consumer services, such as queue parameters.	Select Server Configuration > Administration > Event Management > Event Channel Admin, then select Configure
Associate event filters with a generic consumer.	Enables you to use a filter to specify which events should be passed to each generic consumer.	Select Server Configuration > Administration > Event Management > Event Consumer Admin
View performance statistics for all internal data queues for the event sources and event consumers.	Displays the work being done by EDS. From these statistics, you can determine whether events are being lost and the high-water mark for setting queue capacity.	Select Server Configuration > Administration > Event Management > Event Channel Admin, then select Performance
View events received from EDS and the event logger.	Monitors or troubleshoots your network.	As a superuser, enter: On Solaris: <code>/opt/CSCOpX/bin/eds -display</code> On Windows: <code>NMSROOT\bin\eds -display</code>

Creating Filters

You can create persistent event filters using the Named Filter window. These filters are used by Event Distribution Service consumers to determine which events the EventToTrap service receives. After the events have been converted into traps, the traps are then forwarded to a network management station via a destination hostname and port. Use this feature to make sure CiscoWorks passes critical events to an NMS, such as HP OpenView.

To create filters on UNIX:

Step 1 Log in as superuser and enter the root password.

Step 2 Start the Named Filter dialog box:

```
/opt/CSCOpX/bin/eds -filter
```

If you did not use the default install directory ($\$NMSROOT/CSCOpX/bin/eds$ -filter, where $\$NMSROOT$ is the default installation directory and $CSCOpX$ is the target directory), the Named Filter window appears. The Named Filter window menu selections follow.



Note

You should enter the complete executable of Netscape in the file: $\$NMSROOT/www/classpath/com/cisco/nm/cm/eds/ui/helpSupport.properties$. Edit the line “webBrowser=netscape” with the path where Netscape is installed on your server.

Step 3 You can:

- a. Add a Filter
- b. Delete a Filter
- c. Change an existing Filter

Step 4 Complete the tasks desired and exit the Named Filter Window.

To create filters on Windows:

Step 1 Make sure you have the correct permissions.

Step 2 Start the Named Filter dialog box:

```
NMSROOT\CSCOpX\bin\eds -filter
```

where *NMSROOT* is the default installation directory and **CSCOpX** is the target directory. The Named Filter window appears.

Step 3 You can:

- a. Add a Filter
- b. Delete a Filter
- c. Change an existing Filter

Step 4 Complete the tasks desired and exit the Named Filter Window.

Adding an Event Filter

To add an Event filter:

Step 1 Start the Named Filter window.

Step 2 Select **File > New** in the Named Filter window.

The New Filter window opens.

Step 3 Enter the filter name and filter description.

Step 4 Select filter options:

- a. Add generic events
The events are added to the list in the New Filter window.
- b. Add registered events
The Add Registered Events window opens.

- c. Select the event category, problem description, and severity, then select matching events to add to this filter.
 - d. Click **OK**.
-

Deleting an Event Filter

To delete an Event filter:

- Step 1** Start the Named Filter window.
 - Step 2** Select a filter name from list.
 - Step 3** Select **Edit > Delete** in the Named Filter window. The selected filter is deleted.
-

Changing an Event Filter

To change an Event filter:

- Step 1** Start the Named Filter window.
 - Step 2** Select a filter name from list.
 - Step 3** Select **File > Open** in the Named Filter window. The Open Filter window opens.
 - Step 4** Change the filter as needed.
 - Step 5** Click **OK** to save filter changes.
-

Event Services Software (ESS)

Event Services Software (ESS) provides a means for various CiscoWorks processes to broadcast messages to other processes in a networked and distributed environment. ESS uses a publish and subscribe model, where each process broadcast messages, and other processes selectively subscribe to the messages.

In this model each process subscribe to a host of topics, and other processes, when they need the process to get a message, publish their messages to any of those topics. For example, if process 1 is subscribed to topics a, b and c, other processes will publish messages intended for process 1 on topics a, b or c.

Exporting and Importing User Information

The current version of CiscoWorks Server allows you to import or export user information (containing user IDs and passwords) from one CiscoWorks Server to another. You can do this only if the servers are running on the same operating system.

For example, you can export user information from one CiscoWorks server running on Windows to another running on Windows.

To export user information from the CiscoWorks server:

-
- Step 1** Make sure that the Cisco Works Common Services CD-ROM is in the CD-ROM drive of the machine running CiscoWorks.
 - Step 2** Navigate to the root directory in the Cisco Works Common Services CD-ROM.
 - Step 3** From the root directory, run the script `export_userinfo.pl`.
 - Step 4** Copy the directories `NMSROOT\rigel\user_info` and `NMSROOT\rigel\manifest\user_info` from the machine running Cisco Works Common Services into the corresponding directories on the other system to which you want to export the user information.
 - Step 5** In the system to which you have exported the user information, navigate to the directory `NMSROOT\rigel\scripts`.
 - Step 6** Execute the script `import_userinfo.pl`.
-

This completes the import process, and all the user information data are exported from the first Cisco Works Common Services server to the other.