



System Administration

The system administration utilities enable you to modify the settings of the CiscoWorks Common Services server. These utilities are available only if you have Management Center (MC) applications installed on your server. With these utilities you can:

- [Updating Licensing Information](#)
- [Specifying Administrative Preferences](#)
- [Configuring Authentication and Authorization](#)
- [Changing the SSL Certificate](#)
- [Editing User Information](#)
- [Collecting Troubleshooting Information](#)

Updating Licensing Information

You can view details of your current software license or update to a new license on the License Information dialog box.

To retrieve or validate licensing information:

- Step 1** Select **VPN/Security Management Solution > Administration > Common Services > Licensing Information**.

The License Information dialog box appears. The license type, number of devices supported by the license, and the expiration date of the license appear under License Information.



Note The **VPN/Security Management Solution** drawer is available only if Management Center (MC) applications are installed on your server.

- Step 2** To update your license, follow these steps:
- a. Enter the path to the new license file in the Filename field, or click **Select** to locate the new file.
 - b. Click **Update**.
After the system verifies the license file, a message indicates the status of the license update.
 - c. To close the message box, click **OK**.
The updated licensing information appears under License Information.

Specifying Administrative Preferences

You can specify default preferences for managing log files, e-mail notifications, and database backup and restores. If you set these preferences, you do not need to supply the information each time you access the related management pages.

To configure the administration preferences:

-
- Step 1** Select **VPN/Security Management Solution > Administration > Common Services > Preferences**.
- To specify the number of days to keep log files, enter a value in the Delete the log data if older than field.
 - To specify the default mail server, enter server name in the Mail Server field.
 - To specify the default recipient of e-mail notifications, enter the recipient's e-mail address in the Mail To field. You can enter more than one e-mail address in this field by separating the addresses with a comma and a space (for example: bob@example.com, alice@example.com).

The e-mail addresses entered in this field appear in the Email field on the CiscoWorks Common Services administration pages.
 - To specify the default sender of e-mail notifications, enter the e-mail address in the Mail From field.

The e-mail address in this field appears in the From field of each e-mail sent by CiscoWorks Common Services.
 - To specify the default directory where backup files are stored, enter the path in the Backup Directory field. If the directory does not exist, you are prompted to create the directory when you save your changes.
 - The directory specified in this field appears in the Backup Directory field on the Backup VMS Data page and the Backed-up Archive field on the Restore VMS Data page.
- Step 2** To save your changes, click **Apply**.
If the directory specified as the default backup directory does not exist, CiscoWorks Common Services asks if you want to create the directory.
- Step 3** Click **OK** to create the specified directory.
Or
Click **Cancel** to return to the Administrative Preferences dialog box and change the directory.

A message alerts you to the changed preferences.
- Step 4** Click **OK** to close the message box.
-

Configuring Authentication and Authorization

CiscoWorks Common Services supports two modes of user authentication and authorization:

- Local - The default mode when you install CiscoWorks Common Services.
- Cisco Secure ACS - To use this mode, you must have a Cisco Secure ACS server installed on your network.

About Common Services Authentication

By default, CiscoWorks Common Services uses CiscoWorks Server authentication to authenticate users and authorize them to access CiscoWorks Common Services applications. The CiscoWorks Server authentication scheme has five roles, listed here from least privileged to most privileged:

- Help Desk
- Approver
- Network Operator
- Network Administrator
- System Administrator.

You cannot change these roles, or the privileges assigned to those roles.

You can also use Cisco Secure ACS to provide user authentication and authorization. Cisco Secure ACS allows you to create custom roles and privileges so that you can customize CiscoWorks Common Services client applications to best suit your business workflow and needs.

However, CiscoWorks Common Services itself cannot use Cisco Secure ACS for authorization. If you configure CiscoWorks Common Services to use Cisco Secure ACS for authentication, authorization services are provided by CiscoWorks Server. And, unless that user is also defined in CiscoWorks Server, the user is given the role with the fewest privileges—Help Desk.

If you use Cisco Secure ACS for authentication, and you have a user that needs higher-level privileges in both CiscoWorks Common Services and in a client application, you can do one of two things.

You can create accounts for that user in both CiscoWorks Server and Cisco Secure ACS, using the same user name and password, assigning the appropriate role to each user account.

Or you can create two user accounts;

- In Cisco Secure ACS for the user to use when accessing client applications.
- In CiscoWorks Common Services for the user to use when accessing CiscoWorks Common Services functions, such as database backup.

Cisco Secure ACS Support for Common Services Client Applications

Cisco Secure ACS supports Common Services client applications by providing command authorization for network users who use the management application to configure managed network devices. Command authorization for client application users is supported by using unique command authorization set types for each client application, configured to use Cisco Secure ACS for authorization.

Cisco Secure ACS uses TACACS+ to communicate with client applications. For a client application to communicate with Cisco Secure ACS, you must configure in Cisco Secure ACS as a AAA client that uses TACACS+. Also, you must provide the client application with a valid administrator name and password. When a client application initially communicates with Cisco Secure ACS, these requirements ensure the validity of the communication.

Additionally, the administrator used by the client application must have the Create New Device Command Set Type privilege enabled. When a client application initially communicates with Cisco Secure ACS, it makes the Cisco Secure ACS, create a new device command set type.

This new device command set type appears in the Shared Profile Components section of the HTML interface. It also dictates a custom service to be authorized by TACACS+. The custom service appears on the TACACS+ page in the Interface Configuration section of the HTML interface.

After the client application has dictated the custom TACACS+ service and device command set type to Cisco Secure ACS, you can configure command authorization sets for each role supported by the client application. You can then apply those sets to user groups that contain network administrators or to individual users who are network administrators.

For more information about configuring Cisco Secure ACS administrators, users, and command authorization sets, refer to the *Cisco Secure ACS 3.1 for Windows/NT Servers User Guide*. Although the basic procedures for configuring Cisco Secure ACS are provided in this manual, more detailed information about the various configuration options appear in the Cisco Secure ACS documentation.

Configuring CiscoWorks Common Services to use Local Authentication and Authorization

Local authentication and authorization is the default when you install CiscoWorks Common Services. Follow this procedure only if you have changed the authentication and authorization mode and want to change it back to local.

-
- Step 1** Set the Login Module to CiscoWorks Local.
For more information, see [“Setting the Login Module to CiscoWorks Local” section on page 8-6](#).
- Step 2** Synchronize the authentication server.
For more information, see [“Synchronizing the Authentication Server for Local Authentication” section on page 8-7](#).
-

Setting the Login Module to CiscoWorks Local

The Login Module defines how authorization and authentication are performed. Changing the Login Module to CiscoWorks Local causes the system to use local authentication and authorization services. After changing the Login Module, you need define the authentication and authorization server that will process the request.

To set the Login Module to CiscoWorks Local, follow these steps:

-
- Step 1** Select **Server Configuration > Setup > Security > Select Login Module**
The Select Login Module dialog box appears.
- Step 2** Select **CiscoWorks Local** from the Available Login Modules list.

Step 3 Click **Next**.

The Login Module Options dialog box appears.

Step 4 Select the **False** radio button next to Debug.



Note Setting Debug to True creates additional log files. Use this option only if you experience authentication failures. The TAC may request these logs when troubleshooting your problem.

Step 5 Click **Finish**.

The next time a user logs in, CiscoWorks authentication will be used. However, to complete the change, you must specify the server that will process the request.

Synchronizing the Authentication Server for Local Authentication

After changing the Login Module, you need to specify the authentication server that will process authentication requests. In CiscoWorks Common Services, this is called synchronization, because you are synchronizing the server with the selected Login Module.

To synchronize the authentication server, follow these steps:

Step 1 Select **VPN/Security Management Solution > Administration > Configuration > AAA Server**.

The AAA Server Information dialog box appears. It displays information for the current authentication server.

Step 2 Click **Synchronize**.



Note The Synchronize button is active only if you changed the Login Module.

The Cisco Secure ACS information is cleared from the dialog box, and the CiscoWorks Local option is selected. This indicates that the CiscoWorks server is providing authentication request processing.

Configuring CiscoWorks Common Services to use Cisco Secure ACS Authorization and Authentication

When you install CiscoWorks Common Services as a standalone server, CiscoWorks Common Services uses the local authentication and authorization method.

You can change this method to use a Cisco Secure ACS server for authentication and authorization. Using Cisco Secure ACS allows you to define custom roles and privileges for the client application users.

**Note**

Even if you change to Cisco Secure ACS authentication, CiscoWorks Common Services uses local authorization for CiscoWorks Common Services-specific utilities, such as backup and restore. To perform these actions, the user must also be defined locally and be given the appropriate privilege level.

Before You Begin

Verify that your Cisco Secure ACS server is running version 3.1 or later. CiscoWorks Common Services is not compatible with earlier versions of Cisco Secure ACS. If your Cisco Secure ACS server is running a software version earlier than 3.1, upgrade your Cisco Secure ACS server before continuing.

-
- Step 1** Create an administrator account on the Cisco Secure ACS server for CiscoWorks Common Services.

This is the administrator account that CiscoWorks Common Services uses to update Cisco Secure ACS settings for each client application. You can view the audit data for this administrator account to see what actions CiscoWorks Common Services is performing on the Cisco Secure ACS server.

For more information, see [“Adding an Administrator Account” section on page 8-9](#).

- Step 2** Configure the CiscoWorks Common Services server as a AAA client on the ACS server.

The CiscoWorks Common Services server must be configured as a client of the ACS server for authentication and authorization to occur.

For more information, see [“Adding a AAA Client” section on page 8-11](#).

- Step 3** Set the CiscoWorks Common Services Login Module to TACACS+.
For more information, see [“Setting the Login Module to TACACS+” section on page 8-13.](#)
- Step 4** Synchronize the authentication server.
For more information, see [“Selecting the Cisco Secure ACS Authentication Server” section on page 8-14.](#)
- Step 5** Add users to Cisco Secure ACS.
You must add each CiscoWorks Common Services and client application user to your Cisco Secure ACS server.
For more information, see [“Adding a Cisco Secure ACS User Account” section on page 8-16.](#)
-

Adding an Administrator Account

Use this procedure to add an administrator account to Cisco Secure ACS. This is the administrator account that CiscoWorks Common Services uses to register the client application roles and privileges.

To add a Cisco Secure ACS administrator account, follow these steps:

-
- Step 1** Log in to Cisco Secure ACS.
- Step 2** In the navigation bar, click **Administration Control**.
- Step 3** Click **Add Administrator**.
The Add Administrator dialog box appears.
- Step 4** Complete the fields in the Administrator Details table:
- In the **Administrator Name** field, enter the login name for the new Cisco Secure ACS administrator account.

**Note**

The Administrator Name can contain up to 32 characters, including special characters and spaces.

- b. In the **Password** field, enter the password for the new Cisco Secure ACS administrator account.



Note The password can contain up to 32 characters.

- c. In the **Confirm Password** field, enter the password a second time.
- To select all privileges, including user group editing privileges for all user groups, click **Grant All**.

All privileges options are selected. All user groups move to the Editable groups list.



Tip

To clear all privileges, including user group editing privileges for all user groups, click **Revoke All**.

- To grant user and user group editing privileges, follow these steps:
Select the desired check boxes under User & Group Setup.
 - To move a user group to the Editable groups list, select the group in the Available groups list, and then click --> (right arrow button).
The selected group moves to the Editable groups list.
 - To remove a user group from the Editable groups list, select the group in the Editable groups list, and then click <-- (left arrow button).
The selected group moves to the Available groups list.
 - To move all user groups to the Editable groups list, click >>.
The user groups in the Available groups list move to the Editable groups list.
 - To remove all user groups from the Editable groups list, click <<.
The user groups in the Editable groups list move to the Available groups list.
- To grant any of the remaining privilege options, in the Administrator Privileges table, select the applicable check boxes.

Step 5 Click **Submit**.

Cisco Secure ACS saves the new administrator account. The new account appears in the list of administrator accounts on the Administration Control dialog box.

Adding a AAA Client

Use this procedure to add CiscoWorks Common Services as a AAA client to Cisco Secure ACS. You must be logged into Cisco Secure ACS to perform this procedure.

Before You Begin

For Cisco Secure ACS to provide AAA services to a AAA client, you must ensure that gateway devices between AAA clients and Cisco Secure ACS allow communication over the ports needed to support the applicable AAA protocol (RADIUS or TACACS+).

To add a AAA client:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration section opens.

Step 2 Do one of the following:

- If you are using NDGs, click the name of the NDG to which the AAA client is to be assigned. Then, click **Add Entry** below the AAA Clients table.
- To add a AAA client when you have not enabled NDGs, click **Add Entry** below the AAA Clients table.

The Add AAA Client dialog box appears.

Step 3 In the AAA Client Hostname field, enter the name assigned to this AAA client (up to 32 characters).

Step 4 In the AAA Client IP Address field, enter the AAA client IP address or addresses.

Step 5 In the Key field, enter the shared secret that the AAA client and Cisco Secure ACS use to encrypt the data (up to 32 characters).



Note For correct operation, the identical key must be configured on the AAA client and Cisco Secure ACS. Keys are case sensitive.

If you are using NDGs, from the Network Device Group list, select the name of the NDG to which this AAA client should belong, or select **Not Assigned** to set this AAA client to be independent of NDGs.



Note To enable NDGs, click **Interface Configuration**, click **Advanced Options**, and then select the **Network Device Groups** check box.

Step 6 From the Authenticate Using list, select **TACACS+**.

- To enable single connection from a AAA client, rather than a new one for every TACACS+ request, select the **Single Connect TACACS+ AAA Client (Record stop in accounting on failure)** check box.



Note If TCP connections between Cisco Secure ACS and the AAA client are unreliable, do not use this feature.

- To log watchdog packets, select the **Log Update/Watchdog Packets from this AAA Client** check box.

Step 7 To save your changes and apply them immediately, click **Submit + Restart**.



Note Restarting the service clears the Logged-in User report and temporarily interrupts all Cisco Secure ACS services. This affects the Max Sessions counter.



Tip To save your changes and apply them later, click **Submit**. When you are ready to implement the changes, click **System Configuration**, click **Service Control**, and then click **Restart**.

Setting the Login Module to TACACS+

The Login Module determines the type of authentication and authorization CiscoWorks Common Services uses. By default, the Login Module is set to local authentication and authorization. You can change this default value to use Cisco Secure ACS for user authentication and authorization.

Before You Begin you should:

-
- Step 1** Install your Cisco Secure ACS server.
 - Step 2** Configure CiscoWorks Common Services as an Cisco Secure ACS client in Cisco Secure ACS.
 - Step 3** Create an Cisco Secure ACS administrative account for CiscoWorks Common Services.
-

To select set the login module to TACACS+:

-
- Step 1** Select **Server Configuration > Setup > Security > Select Login Module** from the navigation tree.
The Select Login Module dialog box appears.
 - Step 2** Click **TACACS+** in the Available Login Modules field.
 - Step 3** Click **Next**.
The Login Module Options dialog box appears.
 - Step 4** In the Server field, enter the server name of your ACS server.
 - Step 5** In the Port field, enter the ACS service port number.
 - Step 6** In the Key field, enter the shared secret established when you configured ACS to accept CiscoWorks Common Services as a client.
 - Step 7** Select the **False** radio button next to Debug.



Note If you cannot connect to your ACS server from within CiscoWorks Common Services, select the **True** radio button. Selecting True causes additional logs to be created. These logs are useful for Cisco TAC personnel when providing assistance.

Step 8 Select a login fallback option:

Fallback Option	Description
Allow all CiscoWorks local users to fallback to the CiscoWorks Local login	If the user cannot be authenticated against ACS, the system attempts to authenticate the user against the local user database. This requires a local account with the same name and password as the ACS user account.
Only allow the following user(s) to fallback to the CiscoWorks Local login if preceding login fails:	This is the default setting. You can specify a list of users that will fall back to local authentication if ACS authentication fails. By default, the “admin” user appears in this field. You can add additional user names by separating them with a commas. This requires a local account with the same name and password as the ACS user account.
Allow no fallbacks to the CiscoWorks Local login	If the user cannot be authenticated against ACS, the login attempt fails.



Note

When using the fallback option, you need to make sure that the users that are allowed to fall back exist as users in CiscoWorks Server. Additionally, they need to be given the appropriate role in CiscoWorks Server to access and use the desired functions.

Step 9 Click **Finish**.

The Login Module is changed to your selection.

Selecting the Cisco Secure ACS Authentication Server

Before you can use Cisco Secure ACS for authentication and authorization service, you must select the Cisco Secure ACS authentication server and register the client applications with that server.

Before you begin make sure you have configured your Cisco Secure ACS server to work with CiscoWorks Common Services. You cannot register client application roles and privileges with Cisco Secure ACS until you have added an

administrative account for CiscoWorks Common Services to Cisco Secure ACS. Additionally, you cannot log back in to CiscoWorks Common Services until you have added the CiscoWorks Common Services users to Cisco Secure ACS.

To specify the ACS Server information, follow these steps:

-
- Step 1** Select **VPN/Security Management Solution > Administration > Configuration > AAA Server**.

The AAA Server Information dialog box appears. The current authentication and authorization server, CiscoWorks Local or ACS, is selected.



Note If you changed the Login Module, the Synchronize button is active. If you did not change the Login Module, you cannot perform any actions on this dialog box.

- Step 2** Click **Synchronize**.

The selected authentication and authorization server changes to match your selection on the Available Login Modules dialog box. If your new authentication and authorization server is ACS, the Server Details section is populated with the ACS server information that you entered on the Login Modules Options dialog box and the Login and Register/Unregister Applications sections becomes available for input.

- Step 3** In the **User Name** field, enter the name of the administrative account that you set up in ACS for use by CiscoWorks Common Services.

- Step 4** In the **Password** field, enter the password for the administrative account.

- Step 5** In the **ACS Shared Secret** field, enter the shared secret that you created when specifying CiscoWorks Common Services as an ACS client.

- Step 6** Click **Register**.

The Select Applications to Register with ACS Server dialog box appears.

- Step 7** Select the client applications names in the Available Applications field that you want to register with Cisco Secure ACS, and then click **Add**.

The client application names move to the Selected Applications field.

Step 8 Click **OK**.

The installed client applications register their roles and privileges with the ACS server. When the roles and privileges have been registered, a status message appears.

Step 9 Click **OK** to close the status message.

Step 10 Click **Finish**.

The Cisco Secure ACS username, password, and shared secret are saved. A status message appears.

Step 11 Click **OK** to close the status message.

Adding a Cisco Secure ACS User Account

Use this procedure to add a new user account to Cisco Secure ACS and to specify the device management command authorization set parameters for a user. Device management command authorization sets support the authorization of tasks in Cisco device management applications that are configured to use Cisco Secure ACS for authorization. You can choose one of four options:

- **None**—No authorization is performed for commands issued in the applicable Cisco device management application.
- **Group**—For this user, the group-level command authorization set applies for the applicable device management application.
- **Assign a device management application** for any network device—For the applicable device management application, one command authorization set is assigned, and it applies to management tasks on all network devices.
- **Assign a device management application** on a per Network Device Group Basis—For the applicable device management application, this option enables you to apply command authorization sets to specific Network Device Groups (NDGs), so that a set affects all management tasks on the network devices belonging to the NDG.

Before you add a new user account:

- Ensure that a AAA client has been configured to use TACACS+ as the security control protocol.
- In the Advanced Options section of Interface Configuration, ensure that the Per-user TACACS+/RADIUS Attributes check box is selected.
- In the TACACS+ (Cisco) section of Interface Configuration, ensure that, under New Services, the new TACACS+ service corresponding to the applicable device management application is selected in the User column.
- If you intend to apply command authorization sets, ensure that you have previously configured one or more device management command authorization sets.

To add a user account:

Step 1 Log in to Cisco Secure ACS using an account with privileges for adding user accounts.

Step 2 In the navigation bar, click **User Setup**.

The User Setup Select dialog box opens.

Step 3 Type a name in the User box.



Note The username can contain up to 32 characters. Names cannot contain the following special characters:
? " * > <
Leading and trailing spaces are not allowed.

Step 4 Click **Add/Edit**.

The User Setup Edit dialog box opens. The username being added appears at the top of the dialog box.

Step 5 Ensure that the Account Disabled check box is *not* selected.



Note Alternatively, you can select the Account Disabled check box to create a user account that is disabled, and enable the account at another time.

- Step 6** Scroll down to the TACACS+ Settings table and to the applicable device management command authorization feature area within it.
- To prevent the application of any command authorization for actions performed in the applicable device management application, select (or accept the default of) the **None** option.
 - To assign command authorization for the applicable device management application at the group level, select the **As Group** option.
 - To assign a particular command authorization set that affects device management application actions on any network device, follow these steps:
 - a. Select the **Assign a device management application** for any network device option.
 - b. Then, from the list directly below that option, select the command authorization set you want applied to this user.
 - To create associations that assign a particular command authorization set that affects device management application actions on a particular NDG, for each association, follow these steps:
 - a. Select the **Assign a device management application** on a per Network Device Group Basis option.
 - b. Select a **Device Group** and an associated *device management application*.
 - c. Click **Add Association**.

The associated NDG and command authorization set appear in the table.
- Step 7** Click **Submit** to record the options.
-

Changing the SSL Certificate

CiscoWorks Common Services uses a self-signed certificate to secure communication between your web browser and the CiscoWorks Common Services server.

This certificate is different from the certificate used by CiscoWorks Server to secure web communications to the CiscoWorks Server components. CiscoWorks Server also uses a self-signed certificate when SSL is enabled. However, you can replace the CiscoWorks Server certificate with a third-party, signed certificate.

You can configure CiscoWorks Common Services to use the CiscoWorks Server certificate. The benefits of using the CiscoWorks Server certificate are:

- You can regenerate self-signed CiscoWorks Server certificates.
- You can replace the CiscoWorks Server certificate with a third-party certificate.

Refer to the CiscoWorks Server online help for information about regenerating self-signed certificates or replacing the self-signed certificate with a third-party certificate.

**Note**

The CiscoWorks Server certificate options are available when CiscoWorks Common Services is installed as a standalone server or integrated with CiscoWorks Server.

Before You Begin

If you are switching from the CiscoWorks Common Services certificate to the CiscoWorks Server certificate, you must create an SSL certificate for the CiscoWorks Server components. If you have not created the SSL certificate for the CiscoWorks Server components, you will receive an error that the selected certificate could not be found.

To change the SSL certificate used by CiscoWorks Common Services:

Step 1 Select **VPN/Security Management Solution > Administration > Configuration > Certificate**.

The Certificate Configuration dialog box appears. The certificate that is used by CiscoWorks Common Services to secure the SSL connection is selected.

Step 2 To change the selection, click the desired certificate.

Step 3 Click **Finish**.

Step 4 Click **OK**.

Step 5 Shut down and restart Common Services web server. This restarts your session using the selected certificate.

Editing User Information

The CiscoWorks Common Services Edit User link takes you to either the CiscoWorks Modify/Delete User dialog box or the Cisco Secure ACS login dialog box, depending upon the type of authorization you use with CiscoWorks Common Services. If you are using Cisco Secure ACS authentication, you need to log in to Cisco Secure ACS server to access the user modification dialog box.

**Note**

You cannot modify the default CiscoWorks Server admin account from this link. To modify the admin account, you must log in as “admin” and select **Server Configuration > Setup > Security > Modify My Profile** from the navigation tree.

To edit a user account, Select **VPN/Security Management Solution > Administration > Edit User**.

- If you use Cisco Secure ACS as the user authentication mechanism, the Cisco Secure ACS login dialog box appears. If you use CiscoWorks authentication, the CiscoWorks Modify/Delete User dialog box appears.
 - If the Cisco Secure ACS login dialog box appears, refer to the Cisco Secure ACS user guide or online help for information about modifying Cisco Secure ACS user accounts.
 - If the CiscoWorks Modify/Delete User dialog box appears, refer to the CiscoWorks documentation or online help for information about modifying CiscoWorks user accounts.
-

Collecting Troubleshooting Information

Cisco support personnel may ask you to submit system configuration information when you submit a problem report. This information assists the support staff with diagnosing the reported problem.

CiscoWorks Common Services includes a command-line utility, MDCSupport.exe for Windows and mdcsupport for Solaris, that collects this troubleshooting information.

The MDCSupport.exe utility collects configuration and system information in a .zip file, called MDCSupportInformation.zip, and the mdcsupport utility collects configuration and system information in a .tar file called MDCSupportInformation.tar.Z, that you can send to the Cisco Technical Assistance Center (TAC) support staff.

By default, the MDCSupportInformation.zip file and MDCSupportInformation.tar.Z files are placed in the `<installation_location>/CSCSpX/MDC/etc` directory, where `<installation_location>` is the drive and directory where you installed CiscoWorks Common Services.

Each time you run the executable, the previous MDCSupportInformation files are overwritten. You can change the output location for the MDCSupportInformation files by supplying the drive and path that you need as an argument to the MDCSupport.exe and mdcsupport utilities.

**Note**

You only need to run MDCSupport.exe when requested to by Cisco support personnel. You do not need to submit this information when you first submit a problem report.

The MDCSupportInformation.zip files includes the following information:

- Database files
- Configuration files and MDCSupport log file
- Apache configuration and log files
- Tomcat configuration and log files
- Installation, audit, and operation log files
- The CiscoWorks Common Services Registry subtree ([HKEY_LOCAL_MACHINE][SOFTWARE][Cisco][MDC])
- Windows System Event and Application Event log files
- Host environment information (operating system version and installed service packs, amount of RAM, disk space on all volumes, computer name, and virtual memory size)
- Process Information

The MDCSupportInformation.tar.Z file includes the following information:

- Database files
- Configuration files and MDCSupport log file
- Apache configuration and log files
- Tomcat configuration and log files
- Installation, audit, and operation log files
- Host environment information (operating system version and installed service packs, amount of RAM, disk space on all volumes, computer name, and virtual memory size)
- Process Information

Additionally, MDCSupport executables run any support utilities that were installed and registered by client applications. The output from the client application support utilities is included in the MDCSupportInformation.zip file for Windows and MDCSupportInformation.tar.Z for Solaris.

You can provide the details for Windows and Solaris platforms separately.

On Windows

To collect troubleshooting data:

Step 1 Open an MS-DOS command prompt on the CiscoWorks Common Services server. On Windows, the command prompt is typically available from the Start menu

Step 2 Enter **MDCSupport** at the DOS prompt.

To change the location where the MDCSupportInformation.zip file is created, enter **MDCSupport drive:\path** at the DOS prompt.

The MDCSupport utility creates a .zip file that contains your CiscoWorks Common Services configuration data and log files.

Step 3 Submit the resulting .zip file to TAC.

The TAC representative provides the method and location for submitting the support file.

On Solaris

To collect troubleshooting data:

Step 1 Go to `$NMSROOT/MDC/bin` directory.

Step 2 Enter `MDCSupport` at the prompt.

To change the location where the `MDCSupportInformation.tar.Z` file is created, enter `./mdcsupport` at the prompt or `./mdcsupport /path`

The `MDCSupport` utility creates a compressed `.tar` file that contains your CiscoWorks Common Services configuration data and log files.

Step 3 Uncompress it to get the normal tar file.

Step 4 Submit the resulting `.tar` file to TAC. The TAC representative provides the method and location for submitting the support file.
