



## CHAPTER 2

# Common Problems

---

**Revised: November 13, 2009, OL-12555-02**

This chapter describes common problems associated with the Cisco Secure Access Control Server, hereafter referred to as ACS.

This chapter contains:

- [Administration, page 2-1](#)
- [Authentication and Authorization, page 2-4](#)
- [Browser, page 2-8](#)
- [Cisco Network Admission Control \(NAC\), page 2-10](#)
- [Databases, page 2-13](#)
- [Dial-In Connections, page 2-19](#)
- [EAP Protocols, page 2-22](#)
- [GAME Protocol, page 2-23](#)
- [Installations and Upgrades, page 2-25](#)
- [Interoperability, page 2-28](#)
- [Logging, page 2-29](#)
- [MAC Authentication Bypass Problems, page 2-30](#)
- [Remote Agent \(ACS Solution Engine\), page 2-30](#)
- [Reports, page 2-31](#)
- [User Group Management, page 2-33](#)

## Administration

This section contains:

- [Unauthorized Users Logging In, page 2-2](#)
- [Restart Services Does Not Work, page 2-2](#)
- [Event Notification E-Mail Not Received, page 2-3](#)
- [Remote Administrator Cannot Access Browser, page 2-3](#)
- [Remote Administrators Cannot Log In, page 2-3](#)

- [Remote Administrator Receives Logon Failed... Message, page 2-4](#)
- [Remote Administrator Cannot Access ACS, page 2-4](#)

**Note**

For information on using the command line interface (CLI) to execute administrative commands, see the “Administering Cisco Secure ACS Solution Engine” chapter of the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.1*.

## Administrator Locked Out

**Condition**

ACS has locked out an administrator.

**Action**

- For ACS for Windows:
  - Option 1—Re-enable Local Login, then reset accounts through the GUI.
  - Option 2—Use:

```
csutil -s a unlock <Admin> <Password>
```

- For the ACS Solution Engine, use the CLI **unlock** command:

```
unlock-guiadmin <Admin> <Password>
```

**Tip**

If compliance permits, enable the **Account Never Expires** option for one account in order to prevent lockout.

## Unauthorized Users Logging In

**Condition**

Unauthorized users can log in.

**Action**

List start and end IP addresses for the **Reject listed IP addresses** option. Choose **Administrator Control > Access Policy**, and specify the **Start IP Address** and **End IP Address**.

## Restart Services Does Not Work

**Condition**

The Restart Services option in the web interface does not restart the services.

**Action (ACS for Windows)**

The system is not responding. To manually restart services:

1. From the Windows **Start** menu, choose **Settings > Control Panel > Administrative Tools > Services**.

2. Choose *service\_name* > **Stop** > **Start.**, where *service\_name* can be **CSAdmin**, **CSAuth**, **CSDBSync**, **CSLog**, **CSMon**, **CSRADIUS**, **CSTacacs**.

If the services do not respond when manually restarted, reboot the server.

#### Action (ACS Solution Engine)

The system is not responding to the **restart** command on the System Configuration > Service Control page. Open a console and use the **show** command to determine server status. If necessary, use the CLI to stop the service. See [Chapter 1, “The Remote Agent CLI \(Solution Engine Only\).”](#)

To manually restart services, log in to the ACS console and enter the **restart** command, followed by a single space and the name of the ACS service that you want to restart.

## Event Notification E-Mail Not Received

#### Condition

The administrator is configured for event notification but is not receiving event notification e-mails.

#### Action

Be certain that the SMTP server name is correct. If the name is correct, be certain that the computer that runs ACS can **ping** the SMTP server or can send e-mail using a third-party e-mail software package.

Be certain that the e-mail address does not contain underscores (\_).

## Remote Administrator Cannot Access Browser

#### Condition

A remote administrator cannot bring up the ACS web interface in a browser, or receives a warning that access is not permitted.

#### Action

To recover from this condition:

1. Verify that you are using a supported browser. Refer to the *Release Notes for Cisco Secure ACS Release 4.1* for a list of supported browsers.
2. Use the **show** command with the Remote Agent console.
3. Verify that the remote administrator is using a valid administrator name and password that have previously been added in Administration Control.
4. Verify that Java functionality is enabled in the browser.
5. Determine whether the remote administrator is trying to administer ACS through a firewall, through a device performing Network Address Translation, or from a browser configured to use an HTTP proxy server.

## Remote Administrators Cannot Log In

#### Condition

Remote administrators cannot log in.

**Action**

List no start or end IP addresses for the Allow only listed IP addresses to connect option. Choose **Administrator Control > Access Policy**, and specify the **Start IP Address** and **End IP Address**.

## Remote Administrator Receives Logon Failed... Message

**Condition**

When browsing, a remote administrator receives the `Logon failed . . . protocol error message`.

**Action (ACS for Windows)**

Restart the **CSAdmin** service. To restart the **CSAdmin** service:

1. From the Windows **Start** menu, choose **Control Panel > Services**.
2. Choose **CSAdmin > Stop > Start**.

If necessary, restart the server.

**Action (ACS Solution Engine)**

Restart the **CSAdmin** service. To restart the **CSAdmin** service, from the CLI enter the **restart** command with **CSAdmin** as the argument. If necessary, reboot the appliance.

## Remote Administrator Cannot Access ACS

**Condition**

A remote administrator cannot bring up ACS from the browser, or receives a warning that access is not permitted.

**Action**

If Network Address Translation (NAT) is enabled on the Project Information Exchange (PIX) Firewall, administration through the firewall cannot work. To administer ACS through a firewall, you must configure an HTTP port range. Choose **Administrator Control > Access Policy**. You must configure the PIX Firewall to permit HTTP traffic over all ports in the range specified in ACS.

## Authentication and Authorization

This section contains:

- [Windows Authentication Problems, page 2-5](#)
- [Dial-in Not Disabled, page 2-5](#)
- [Settings Not Inherited, page 2-5](#)
- [Retry Interval Too Short, page 2-5](#)
- [AAA Client Times Out, page 2-6](#)
- [Unknown NAS Error, page 2-6](#)
- [Key Mismatch Error, page 2-6](#)
- [Unexpected Authorizations, page 2-7](#)

- [RADIUS Extension DLL Rejected User Error, page 2-7](#)
- [Request Does Not Appear in an External Database, page 2-7](#)

## Windows Authentication Problems

### Condition

Problems diagnosing Windows authentications.

### Action

Log in to the ACS server (by using the normal interactive Login field) with the same user credentials that you want ACS to validate. If the logon does not work, then ACS cannot authenticate. This condition indicates an Active Directory (AD) configuration issue.

If the login works, but ACS does not authenticate, this condition indicates permission problems. Check Auth.log for the username, and look for errors. Review the permission requirements and be certain that ACS is running with proper privileges.

## Dial-in Not Disabled

### Condition

After the administrator disables the Dialin Permission setting, Windows database users can still dial in and apply the Callback string that is configured under the Windows user database. (To locate the Dialin Permission check box, choose **External User Databases > Database Configuration > Windows Database > Configure.**)

### Action

Restart the ACS services.

## Settings Not Inherited

### Condition

Users moved to a new group inherit new group settings, but they keep their existing user settings. Users did not inherit settings from the new group.

### Action

Manually change the settings in the User Setup section.

## Retry Interval Too Short

### Condition

The retry interval is too short, and authentication fails.

### Action

Check the Failed Attempts report.

The retry interval may be too short. (The default is 5 seconds.) Increase the retry interval (`tacacs-server timeout 20`) on the AAA client to 20 or greater.

## AAA Client Times Out

### Condition

The AAA client times out when authenticating against a Windows user database.

### Action

Increase the TACACS+ or RADIUS timeout interval from the default (5) to 20 by entering these Cisco IOS commands:

```
tacacs-server timeout 20
radius-server timeout 20
```

## Unknown NAS Error

### Condition

Authentication fails; the error `Unknown NAS` appears in the Failed Attempts log.

### Action

To be certain that the NAS is recognized:

- 
- Step 1** Verify that the AAA client is configured under the Network Configuration section.
  - Step 2** If you have RADIUS/TACACS+ source-interface command configured on the AAA client, ensure that the client on ACS is configured by using the IP address of the specified interface.
- 

## Key Mismatch Error

### Condition

Authentication fails; the error `Key mismatch` appears in the Failed Attempts log.

### Action

To be certain that the keys match:

- 
- Step 1** Verify that the TACACS+ or RADIUS keys are identical in the AAA client and ACS (case sensitive).
  - Step 2** Re-enter the keys to confirm that they are identical.
-

## Unexpected Authorizations

### Condition

The user can authenticate, but authorizations do not match expectations.

### Action

Different vendors use different AV pairs. One vendor protocol may ignore the AV pairs used in another protocol, for example. Be certain that the user settings reflect the correct vendor protocol; for example, RADIUS (Cisco IOS/PIX).

## RADIUS Extension DLL Rejected User Error

### Condition

LEAP authentication fails. The error `Radius extension DLL rejected user` appears in the Failed Attempts log.

### Action

To verify configured authentication type:

- 
- Step 1** Verify that the correct authentication type has been set on the Access Point. Be certain that, at a minimum, you checked the Network-EAP check box.
- Step 2** If you are using an external user database for authentication, verify that ACS supports the database. For information on the external databases that ACS supports, see *User Databases*, in the *User Guide for Cisco Secure Access Control Server*.
- 

## Request Does Not Appear in an External Database

### Condition

An authentication request does not appear in an external database.

### Action

To verify that the authentication request is being forwarded:

- 
- Step 1** Set logging to Full. Choose **System Configuration > Service Control** to set the logging.
- Step 2** Check `auth.log` for confirmation that the authentication request is being forwarded to the third-party server. If the authentication request is not being forwarded, confirm that the external database configuration is correct, as well as the unknown user policy settings.
-

## TACACS+ Authentication is Failing

**Condition**

TACACS+ authentication is failing.

**Action**

Examine the Failed Attempts log. If you observe unusual strings in place of the username, then check for configuration error in the TACACS+ client NAS, and correct the configuration of the device.

## Browser

This section contains:

- [Cannot Access the Web Interface, page 2-8](#)
- [Pages Do Not Appear Properly, page 2-8](#)
- [Browser crash when trying to open ACS, page 2-9](#)
- [Session Connection Lost, page 2-9](#)
- [Administrator Database Corruption \(Netscape\), page 2-9](#)
- [Remote Administrator Cannot Browse, page 2-9](#)

## Cannot Access the Web Interface

**Condition**

The browser cannot display the ACS web interface.

**Action**

To fix the display:

- 
- Step 1** Open Internet Explorer or Netscape Navigator. Choose **Help > About**, and determine the version of the browser. See the *Installation Guide for Cisco Secure ACS for Windows Release 4.1* and the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.1* for a list of supported browsers, and the *Release Notes for Cisco Secure ACS Release 4.1* for known issues with a particular browser version.
- Step 2** Check that **CSAdmin** service is running.
- 

## Pages Do Not Appear Properly

**Condition**

Parts of pages do not appear properly, parts of the page are missing, or the page is corrupted.

**Action**

Perform these steps:

- 
- Step 1** Check that the Java Runtime Environment (JRE) is installed on the client machine.
- Step 2** Check for the correct JRE for applets in the browser advance option. See installation guide for web client requirements.
- 

## Browser crash when trying to open ACS

### Condition

When opening ACS, the browser crashes.

### Action

If you are using the JRE 1.5.0\_00, upgrade to the current version of the JRE at the Java website.

## Session Connection Lost

### Condition

1. The browser displays a Java message indicating that your session connection is lost.
2. You cannot use the browser.

### Action

Check the **Session idle timeout** value for remote administrators. Choose **Administration Control Session Policy Setup**, and increase the timeout value as needed.

## Administrator Database Corruption (Netscape)

### Condition

The administrator database appears to be corrupted when using Netscape.

### Action

The remote Netscape client is caching the password. If you specify an incorrect password, it is still cached. When you attempt to reauthenticate with the correct password, Netscape sends the incorrect password. Clear the cache before attempting to re-authenticate, or close the browser and open a new session.

## Remote Administrator Cannot Browse

### Condition

Remote administrator intermittently cannot browse in the ACS web interface.

### Action

Confirm that the client browser does not contain a proxy server configuration. ACS does not support the HTTP proxy for remote administrative sessions. Disable the proxy server settings.

# Cisco Network Admission Control (NAC)

This section contains:

- [Posture Problems, page 2-10](#)
- [Cisco IOS Commands Not Denied, page 2-11](#)
- [EAP Request Has Invalid Signature, page 2-11](#)
- [Administrator Locked Out of Client, page 2-11](#)
- [Cannot Enter Enable Mode, page 2-12](#)
- [Nonresponsive Endpoint Limit Reached, page 2-12](#)
- [NAC Posture Problem, page 2-13](#)
- [NAC Posture Problem, page 2-13](#)

## Posture Problems

### Condition

The results of `show eou all` or `show eou ip address` include postures that do not match the actual result of posture validation or display a line of hyphens (-----) instead of a posture.

### Action

If you see a line of hyphens (-----), the AAA client is not receiving the posture-token attribute-value (AV) pair within a Cisco IOS/PIX RADIUS `cisco-av-pair` vendor-specific attribute (VSA). If the posture that appears does not correspond to the actual result of posture validation, the AAA client is receiving an incorrect value in the posture-token AV pair.

Check group mappings for Network Admission Control (NAC) databases to verify that the correct user groups are associated with each system posture token (SPT). In the user groups that are configured for use with NAC, be certain that the Cisco IOS/PIX `cisco-av-pair` VSA is correctly configured. For example, in a group configured to authorize NAC clients receiving a healthy System Posture Token (SPT), be certain that the `[009\001] cisco-av-pair` check box is checked and that the SPT string appears in the `[009\001] cisco-av-pair` text box:

```
posture-token=Healthy
```



### Caution

The posture-token AV pair is the only way that ACS notifies the AAA client of the SPT that the posture validation returns. Because you manually configure the posture-token AV pair, errors in configuring the posture-token can send the incorrect SPT to the AAA client; or, if the AV pair name is mistyped, the AAA client is not receiving the SPT at all.



### Note

AV pair names are case sensitive.

For more information about the Cisco IOS/PIX `cisco-av-pair` VSA, see the *User Guide for Cisco Secure Access Control Server*.

## Cisco IOS Commands Not Denied

### Condition

Under EXEC Commands, ACS is not denying Cisco IOS commands when checked.

### Action

Examine the Cisco IOS configuration at the AAA client. If necessary, enter this Cisco IOS command into the AAA client configuration:

```
aaa authorization command <0-15> default group TACACS+
```

The correct syntax for the arguments in the text box is **permit** *argument* or **deny** *argument*.

## EAP Request Has Invalid Signature

### Condition

ACS receives traffic from an EAP-enabled device that has the wrong shared secret, and ACS logs the error.

### Action

Check for these conditions:

- The wrong signature is being used.
- A RADIUS packet was corrupted in transit.
- ACS is being attacked.

Check the EAP-enabled device and make changes, if necessary.

## Administrator Locked Out of Client

### Condition

An administrator has been locked out of the AAA client because of an incorrect configuration setup in the AAA client.

### Action

Perform these steps:

- 
- Step 1** If you have a fallback method configured on your AAA client, disable connectivity to the AAA server and log in with the local or line username and password.
  - Step 2** Try to connect directly to the AAA client at the console port.
  - Step 3** If the direct connection is not successful, see your AAA client documentation or see the [Password Recovery Procedures](#) page on Cisco.com for information regarding your particular AAA client.
-

## Cannot Enter Enable Mode

### Condition

Unable to enter Enable Mode after performing `aaa authentication enable default tacacs+`. The system returns the error message: `Error in authentication on the router.`

### Action

Check the Failed Attempts log. If the log reads `CS password invalid`, it may be that the user has no enable password set up. If you do not see the Advanced TACACS+ Settings section among the user setup options:

- 
- Step 1** Choose **Interface Configuration > Advanced Configuration Options > Advanced TACACS+ Features**.
  - Step 2** Select the option that configures the TACACS+ settings to appear in the user settings.
  - Step 3** Choose **Max privilege for any AAA Client** (this will typically be 15).
  - Step 4** Enter the **TACACS+ Enable Password** for the user.
- 

## Nonresponsive Endpoint Limit Reached

### Condition

The system reaches the NAC Nonresponsive Endpoint (NRE) Guest Access Limit of 100 Endpoints.

### Action

A feature in the EAPoUDP state table prevents denial of service (DoS) attacks on the ACS server by limiting RADIUS requests.

When the system reaches the maximum limit of 100 unauthorized nonresponsive endpoints per Network Access Device (NAD), a warning message appears on the router console:

```
*Jan 19 09:51:04.855: %AP-4-POSTURE_EXCEED_MAX_INIT: Exceeded maximum limit (100).
```

The router stops processing RADIUS requests for NAC. This mechanism will leave legitimate users, with or without the Cisco Trust Agent, with default network access. The default access is whatever the router interface Access Control List (ACL) allows.

This message appears because 100 (or more) EAPoUDP sessions are in the INIT state. Normally, when receiving a RADIUS Accept-Accept from the ACS, the session will transition out of this state. However, the EAPoUDP session will stay in this state if the:

- NAD has more than 100 concurrently unauthorized endpoints.
- Router receives an Access-Reject from ACS.
- Router fails to receive a response from ACS.

Based on this behavior, your options are:

- Properly configure ACS for NAC to minimize unintentional Access-Rejects.
- When passively deploying NAC (monitor-only mode), configure ACS to accept all NREs by using a MAC or IP address wildcard with network access restrictions (NARs) in ACS.

- You should never have more than 100 unauthorized endpoints behind a single NAC-enabled router because they will prevent access for Cisco Trust Agent-enabled endpoints.
- Set the default hold period to a low value.

## NAC Posture Problem

In ACS Release 4.1, the SPT is no longer configured in **Group Mapping for NAC Databases**. The posture result automatically sends the in the `cisco-av-pair`.

## Authorization Policy

When you configure an authorization policy and select *any* in the user group or the posture token, you may want to configure *none*. For a group, *any* refers to cases of posture only (no authentication). For a posture token, *any* refers to cases of authentication only (no posture).

## Databases

This section contains:

- [RDBMS Synchronization Not Properly Operating, page 2-13](#)
- [Database Replication Not Properly Operating, page 2-14](#)
- [External User Database Not Available, page 2-14](#)
- [Unknown Users Not Authenticated, page 2-14](#)
- [User Problems, page 2-15](#)
- [Cannot Implement the RSA Token Server, page 2-15](#)
- [ACE SDI Server Does Not See Incoming Request, page 2-16](#)
- [External Databases Not Properly Operating \(ACS Solution Engine\), page 2-16](#)
- [Group Mapping \(ACS Solution Engine\), page 2-16](#)
- [Configuration of Active Directory, page 2-17](#)
- [NTLMv2 Does Not Work, page 2-18](#)

## RDBMS Synchronization Not Properly Operating

### Condition

RDBMS synchronization is not properly operating.

### Action

Be certain that the correct server appears in the Partners list.

## Database Replication Not Properly Operating

### Condition

Database replication is not properly operating.

### Action

- Be certain that you have correctly set the server as Send or Receive.
- On the sending server, be certain that the receiving server is in the Replication list.
- On the receiving server, be certain that the sending server is chosen in the Accept Replication from list. Also, be certain that the sending server is not in the replication partner list.
- Be certain that no ACS server is associated with a master server (in the right column) in order to avoid loops.
- Be certain that the replication schedule on the sending ACS is not conflicting with the replication schedule on the receiving ACS.
- If the receiving server has dual network cards, on the sending server add a AAA server to the AAA Servers table in the Network Configuration section for every IP address of the receiving server. If the sending server has dual network cards, on the receiving server add an AAA server to the AAA Servers table in the Network Configuration for every IP address of the receiving server.

## External User Database Not Available

### Condition

The external user database is not available in the Group Mapping section.

### Action

The external database has not been configured in the External User Databases section; or, the username and password have been incorrectly typed. Click the applicable external database. Be certain that the username and password are correct.

## Unknown Users Not Authenticated

### Condition

Unknown users are not authenticated.

### Action



#### Note

---

If you are using the ACS Unknown User feature, external databases can only authenticate by using Password Authentication Protocol (PAP).

---

To authenticate unknown users:

- 
- Step 1** Choose **External User Databases > Unknown User Policy**.
  - Step 2** Click the **Check the following external user databases** option.
  - Step 3** From the External Databases list, choose the database(s) against which to authenticate unknown users.

- Step 4** Click the **right arrow** button to add the database to the Selected Databases list.
- Step 5** Click **Up** or **Down** to move the selected database into the correct position in the authentication hierarchy.
- 

## User Problems

### Condition

The same user appears in multiple groups or duplicate users exist in the ACS internal database. You cannot delete the user from the database.

### Action

To clean up the database, you use **CSUtil.exe** from the command line:

```
CSUtil -q -d -n -l dump.txt
```

This command causes the database to be unloaded and reloaded to clear the counters.



### Tip

When you install ACS in the default location, **CSUtil.exe** is located in:  
C:\Program Files\CiscoSecure ACS vX.X\bin.

---

For more information on using the **CSUtil.exe** command, see the *User Guide for Cisco Secure Access Control Server*.

## Cannot Implement the RSA Token Server

### Condition

You cannot successfully implement the RSA token server.

### Action

To recover from this problem:

---

- Step 1** Log in to the computer that is running ACS. (Be certain that your login account has administrative privileges.)
- Step 2** Be certain that the RSA Client software is installed on the same computer as ACS.
- Step 3** Follow the setup instructions. Do not restart at the end of the installation.
- Step 4** Get the file named `sdconf.rec` from the `\data` directory of the RSA ACE server.
- Step 5** Place `sdconf.rec` in the `%SystemRoot%\system32` directory.
- Step 6** Be certain that you can **ping** the machine that is running the ACE server by hostname. (You might need to add the machine in the `lmhosts` file.)
- Step 7** Verify that support for RSA is enabled in the External User Database > Database Configuration in the ACS.
- Step 8** Run **Test Authentication** from the Windows control panel for the ACE client application.

**Step 9** From ACS, add the token server to the external database list.

---

## ACE SDI Server Does Not See Incoming Request

### Condition

On the Active Collaboration Engine (ACE) Systems Development and Integration (SDI) server, no incoming request is seen from ACS, although the RSA agent authentication works.

### Action (ACS for Windows, ACS Solution Engine)

For dial-up users, be certain that you are using PAP and not MS-CHAP or CHAP. RSA SDI does not support CHAP and ACS does not send the request to the RSA server; rather, ACS will log an error for external database failure.

## External Databases Not Properly Operating (ACS Solution Engine)

### Condition

External databases are not properly operating.

### Action

Run **cssupport.exe** to generate a package.cab file in order to collect logging information for the SE.

Be certain that the Remote Agent is properly installed and configured. See the *Installation and Configuration Guide for Cisco Secure Remote Agents 4.1*.

Be certain that a two-way trust (for dial-in check) is established between the ACS domain and the other domains. Check CSAuth.log for any debug messages beginning with [External DB].

## Group Mapping (ACS Solution Engine)



### Note

---

On some servers, you should configure ACS services with the Local System account. On other servers, it will be necessary to configure a domain account (for example, create an account called ACS in the AD domain and assign appropriate privileges). In some extreme cases, it may be necessary to make this account a member of Domain Administrators.

---

### Condition

During configuration of group mapping, the user sees a failure message in a popup window:

```
Failed to enumerate Windows groups. If you are using AD consult the installation guide for information
```

### Action

This problem may occur if:

- ACS services do not have privileges to execute the **NetGroupEnum** function. For information go to MSDN on Microsoft.com.
- NetBIOS over TCP is not enabled.
- DNS is not correctly working. You can try reregistering by using **ipconfig /flushdns** and then **ipconfig /registerdns** from a DOS prompt. Otherwise, go to the Microsoft website for more information.
- RPC is not correctly working (for example, after Blaster Update). Go to support.microsoft.com and check for these hot fixes:
  - kb822831
  - kb823980
  - kb824105
  - kb824146
- The domain controllers are not synchronized. To synchronize, use the **net time** command from a DOS prompt: **net time /Domain: <DomainName>**.
- Different SPs are running on different domain controllers.
- The **NetLogon** service is not up and running on all domain controllers.
- Check that packet filters are installed.
- Choose **yes** on the DNS properties to **Allow Dynamic Updates**.

## Configuration of Active Directory



### Note

On some servers, ACS services should be configured with the Local System account. On other servers, it will be necessary to configure a domain account (for example, create an account called ACS in the AD domain and assign appropriate privileges). In some extreme cases, you might have to make this account a member of Domain Administrators.

### Condition

You must configure Active Directory for ACS.

### Action

On the domain controller serving the ACS server:

- 
- Step 1** Create a user and provide a strong password.
  - Step 2** Make the user a member of Domain Admins group.
  - Step 3** Make the user a member of the Administrators group.
  - Step 4** On the Windows 2000 server that is running ACS:
    - a. Add a new user to the local group.
    - b. Choose **Administrative Tools** from the Windows control panel.
    - c. Choose **Computer Management > Local Users and Groups > Groups**.
    - d. Double-click the **Administrators** group, and then click **Add**.

- e. Choose the domain from the **Look in** box.
  - f. Double-click the user created earlier to add the user, and then click **OK**.
- Step 5** Give the new user special rights on ACS server:
- a. Choose **Administrative Tools** from the control panel.
  - b. Choose **Local Security Policy > Local Policies**.
  - c. Open **User Rights Assignment**.
  - d. Double-click on **Act as part of the operating system** and click **Add**.
  - e. Choose the domain from the **Look in** box.
  - f. Double-click the user that you created earlier to add it and click **OK**.
  - g. Double-click on **Log on as a service**, and click **Add**.
  - h. Choose the domain from the **Look in** box.
  - i. Double-click the user created earlier to add the user, and click **OK**.
- Step 6** Set the ACS services to run as the created user:
- a. Choose **Open Administrative Tools** from the control panel.
  - b. Choose **Services**.
  - c. Double-click the **CSAdmin** entry.
  - d. Click the **Log On** tab, and then click **This Account** and **Browse**.
  - e. Choose the domain, double-click the user created earlier. Click **OK**.
- Step 7** Repeat the steps for the rest of the CS services.
- Step 8** Wait for Windows to apply the security policy changes, or reboot the server. If you rebooted the server, skip the rest of these instructions.
- Step 9** Stop and then start the **CSAdmin** service.
- Step 10** Open the ACS web interface.
- Step 11** Choose **System Config > Service Control > Restart**.
- Step 12** If the **Domain Security Policy** is set to override settings for the **Act as part of the operating system** and **Log on as a service** rights, you must also make the user rights changes listed previously to the policy.
- 

## NTLMv2 Does Not Work

### Condition

NTLMv2 does not work.

### Action

You must have the appropriate version of Windows installed (or a certain service pack) *and* configure the domain controllers registry to request NTLMv2. For additional information, see Microsoft article #239869.

# Dial-In Connections

This section contains:

- [Cannot Connect to AAA Client \(No Report\)](#), page 2-19
- [Cannot Connect to the AAA Client \(Windows External Database\)](#), page 2-20
- [Cannot Connect to AAA Client \(ACS Internal Database\)](#), page 2-20
- [Cannot Connect to AAA Client \(Telnet Connection Authenticated\)](#), page 2-21
- [Cannot Connect to AAA Client \(Telnet Connection Not Authenticated\)](#), page 2-21
- [Callback Not Working](#), page 2-22
- [Authentication Fails When Using PAP](#), page 2-22

## Cannot Connect to AAA Client (No Report)

### Condition

A dial-in user cannot connect to the AAA client.

No record of the attempt appears in the TACACS+ or RADIUS Accounting Report. From the navigation bar, choose **Reports and Activity**, then choose **TACACS+ Accounting** or **RADIUS Accounting** or **Failed Attempts** to check for the record.

### Action

Examine the ACS Reports or AAA client Debug output to narrow the problem to a system error or a user error. Confirm that the:

- Dial-in user was able to establish a connection and **ping** the computer *before* ACS was installed. If the dial-in user could not, the problem is related to modem configuration on an AAA client, not ACS.
- LAN connections for the AAA client and the computer that is running ACS are physically connected.
- IP address of the AAA client in the ACS configuration is correct.
- IP address of ACS in AAA client configuration is correct.
- TACACS+ or RADIUS keys in the AAA client and ACS are identical (case sensitive).
- Command **ppp authentication pap** is entered for each interface, if you are using a Windows user database.
- Command **ppp authentication chap pap** is entered for each interface, if you are using the ACS internal database.
- AAA and TACACS+ or RADIUS commands are correct in the AAA client. The necessary commands reside in:  
Program Files\CiscoSecure ACS vx.x\TacConfig.txt  
Program Files\CiscoSecure ACS vx.x\RadConfig.txt
- ACS Services (**CSAdmin**, **CSAuth**, **CSDBSync**, **CSLog**, **CSRADIUS**, **CSTacacs**) are running on the computer that is running ACS.

## Cannot Connect to the AAA Client (Windows External Database)

### Condition

A dial-in user cannot connect to the AAA client, and you configured the Windows user database for authentication.

ACS creates a record of a failed attempt in the Failed Attempts Report in the Reports and Activity section.

### Action

Create a local user in the ACS internal database and test whether authentication is successful. If it is successful, the issue is user information that is not correctly configured for authentication in Windows or ACS.

From Windows User Manager or Active Directory Users and Computers, confirm that the:

- Username and password are configured in the Windows User Manager or Active Directory Users and Computers.
- User can log in to the domain by authenticating through a workstation.
- User Properties window does not have User Must Change Password at Login enabled.
- User Properties window does not disable the account.
- User Properties for the dial-in window does not disable dial-in permission, if ACS is using this option for authentication.

From within ACS confirm that:

- If the username is already entered into ACS, a Windows user database configuration is selected for the user in the Password Authentication list on the User Setup page.
- If the username is already entered into ACS, the ACS group to which the user is assigned has the correct authorization enabled (such as IP and PPP, IPX and PPP or Exec and Telnet). Click **Submit + Restart** if you make a change.
- The user expiration information in the Windows user database has not caused a failed authentication. For troubleshooting purposes, disable password expiry for the user in the Windows user database.

Then:

- Click **External User Databases > Database Configuration**; then click **List All Databases Configured**, and then be certain that the database configuration for Windows is listed.
- Click **External User Databases > Unknown User Policy** to be certain that the Fail the attempt option is not chosen. And be certain that the Selected Databases list reflects the necessary database.
- Verify that the Windows group to which the user belongs has not been mapped to No Access.

## Cannot Connect to AAA Client (ACS Internal Database)

### Condition

A dial-in user cannot connect to the AAA client, and the ACS internal database is being used for authentication.

A record of a failed attempt appears in the Failed Attempts Report (choose **Reports and Activity**, then click **Failed Attempts**).

**Action**

From within ACS confirm that the:

- Username is entered into ACS.
- ACS internal database is chosen from the Password Authentication list and a password has been entered in User Setup for the user.
- ACS group to which the user is assigned has the correct authorization protocols enabled (such as IP and PPP, IPX and PPP or Exec and Telnet). Click **Submit + Restart** if you made a change.
- Expiration information has not caused a failed authentication. Change the option to **Expiration: Never** for troubleshooting.

## Cannot Connect to AAA Client (Telnet Connection Authenticated)

**Condition**

A dial-in user cannot connect to the AAA client; however, a Telnet connection can be authenticated across the LAN.

**Action**

Isolate the problem area. The possibilities are:

- Line or modem configuration problem. Review the documentation that came with your modem and verify that the modem is properly configured.
- The user is not assigned to a group that has the correct authorization rights. You can modify authorization rights under Group Setup or User Setup. User settings override group settings.
- The ACS or TACACS+ or RADIUS configuration is not correct in the AAA client.

Additionally, you can verify ACS connectivity by attempting to Telnet to the access server from a workstation connected to the LAN. A successful authentication for Telnet confirms that ACS is working with the AAA client.

## Cannot Connect to AAA Client (Telnet Connection Not Authenticated)

**Condition**

A dial-in user cannot connect to the AAA client, and a Telnet connection cannot be authenticated across the LAN.

**Action**

Determine whether the ACS is receiving the request by viewing the ACS reports. Based on what does not appear in the reports and which database is being used, look for:

- Line or modem configuration problem. Review the documentation that came with your modem and verify that the modem is properly configured.
- The user does not exist in the Windows user database or the ACS internal database, and might not have the correct password. Authentication parameters can be modified under User Setup.
- The ACS or TACACS+ or RADIUS configuration is not correct in the AAA client.

## Callback Not Working

**Condition**

Callback is not working.

**Action**

Be certain that callback works on the AAA client when using local authentication; then, add AAA authentication.

## Authentication Fails When Using PAP

**Condition**

User authentication fails when using PAP.

**Action**

Outbound PAP is not enabled. If the Failed Attempts report shows that you are using outbound PAP:

- 
- Step 1** Go to the Interface Configuration section and check the **Per-User Advanced TACACS+ Features** check box.
  - Step 2** Choose the **TACACS+ Outbound Password** section of the **Advanced TACACS+ Settings** table on the **User Setup** page.
  - Step 3** Enter and confirm the password in the boxes.
- 

## EAP Protocols

**Condition**

Problems with EAP protocols.

**Action**

The general troubleshooting strategy is the same for all EAP methods:

- 
- Step 1** Examine the ACS Auth.log.
  - Step 2** Enable debug logging on the NAD and examine the output.
  - Step 3** Use a sniffer to get a protocol wire trace.
  - Step 4** Examine any trace information that the client may provide.
  - Step 5** Verify configurations throughout the network.
  - Step 6** Confirm that credentials (certificates) are valid and installed.
-

**Note**

You can use the Microsoft Management Console (MMC) to examine user-based and machine-based certificates. For information on using the MMC, go to the Microsoft website.

## GAME Protocol

This section contains:

- [GAME Configuration Problem](#), page 2-23
- [GAME Troubleshooting Setup](#), page 2-23
- [Expected Device-Type is Not Matched](#), page 2-24
- [Device-type Attribute is Not Returned by the Audit Server](#), page 2-24
- [Failure Returned by the Audit Server](#), page 2-25

## GAME Configuration Problem

**Condition**

The Generic Authorization Message Exchange (GAME) configuration is incorrect.

**Action**

To check the configuration, choose:

- **Network Access Profiles > Protocols** to be certain that you have checked **Allow Agentless Request Processing**.
- **Network Access Profiles > Posture Validation > Select Audit** to be certain that you checked an Audit Server to set up the appropriate device-type rules.
- **Posture Validation > External Posture Validation Audit Setup**, and verify that:
  - The Audit Server is configured with the correct URL.
  - The group and host are configured in Which Groups and Hosts are Audited.
  - Game Group Feedback is configured and Request Device Type from Audit Server is checked. The device-type attribute must be added to the ACS dictionary. If the attribute is not in the ACS dictionary, the Request Device Type from Audit Server check box is unchecked.

## GAME Troubleshooting Setup

**Condition**

You need to troubleshoot the GAME feature.

**Action**

Assign policies and groups:

---

**Step 1** Be certain that the host to audit is configured or that Audit All Hosts is chosen.

**Step 2** Choose Audit all user groups.

- Step 3** Configure these unique groups:
- a. Configure a group for Assign this Group if Audit Server Did not Return a Device-Type.
  - b. Configure a Match-all rule and assign a group for all device-type strings that the audit server returns.
  - c. Choose **Network Access Profiles > Authentication** and configure a group for If Agentless Request was not Assigned.

---

Configure these logs:

- Passed and Failed Attempts
- Audit Device-Type (as a column to log)

## Expected Device-Type is Not Matched

### Condition

ACS cannot match a device-type.

### Action

Check these configuration items:

- Configure the Game Troubleshooting Setup. See [GAME Troubleshooting Setup, page 2-23](#).
- After audit, the Group configured for **Match -all** is assigned.
- Audit Device-Type column shows the device type.
- Device-type as seen by ACS is reported in the Pass Authen log.

Device-type as seen by ACS is also reported in the CSAuth log and the output from the debugging mode of CSAuth: **DZAuth -p -z -v**.

```
[PDE]: PdeAttributeSet::addAttribute: Unix:Audit:Device-Type=IP Phone
[PDE]: AuditAction::Received device-type=IP Phone
[PDE]: PdeAttributeSet::addAttribute: PDE-Audit-Req-Device-Type-34=TRUE
```

## Device-type Attribute is Not Returned by the Audit Server

### Condition

The audit server does not return a device-type attribute.

Auth.log indicates Audit Server did not Return Device Type.

```
[PDE]: PdeAttributeSet::addAttribute: PDE-Audit-Req-Device-Type-34=TRUE
[PDE]: Device type requested but Audit Server did not return device type
[PDE]: AuditAction::Invoking GAMEGroupMappingPolicy
```

### Action

Verify configuration items and logging:

- Configure the GAME Troubleshooting setup. See [GAME Troubleshooting Setup, page 2-23](#).
- Be certain that the Audit Device-Type column is . . . (empty) in Pass Authen Report.
- Be certain that, after audit, the Group configured for Assign this Group if AuditServer Did not Return a Device-Type is assigned.

- Check for a device type for a known device.

## Failure Returned by the Audit Server

### Condition

The audit server returns a failure.

AUTH.log indicates Audit Server return zero length device type or an error parsing GAME response.

```
[PDE]: PdeAttributeSet::addAttribute:Unix:Audit:Device-Type=  
[PDE]: Audit Server return zero length device type ...  
[PDE]: PolicyMgr::Process: last action result=-2147 Audit policy failed (-2147),  
attempting fail open  
[PDE]: Error parsing GAME response: Could not find element AttributeValue under element  
saml:Attribute  
[PDE]: PolicyMgr::Process: last action result=-2165 Audit policy failed (-2165),  
attempting fail open
```

### Action

Verify these configuration items:

- GAME Troubleshooting setup. See [GAME Troubleshooting Setup, page 2-23](#).
- Audit Device-Type column is ... (empty) in the Pass Authen Report.
- The Group configured for If agentless request was not assigned a user-group is assigned, after audit.
- Audit Server is accessible and functional (that is, posture audit works with the same server).

## Installations and Upgrades

This section contains:

- [rad\\_mon.dll and tac\\_mon.dll In Use Condition, page 2-26](#)
- [During Upgrade the ACS Folder is Locked, page 2-26](#)
- [During Uninstall the ACS Folder is Locked, page 2-26](#)
- [After Restart ACS Cannot Start Services, page 2-26](#)
- [Upgrade or Uninstall Cannot Complete, page 2-27](#)
- [Invalid File or Data, page 2-27](#)
- [Accounting Logs Missing, page 2-28](#)
- [Upgrade Command Does Not Work \(ACS Solution Engine\), page 2-28](#)
- [On Solaris, autorun.sh Does Not Execute \(ACS Solution Engine\), page 2-28](#)

## System Requirements

Be certain that you have installed your release according to the requirements in the Installation Guide and Release Notes that accompany the release.

## rad\_mon.dll and tac\_mon.dll In Use Condition

### Condition

The rad\_mon.dll and tac\_mon.dll files remain in use after uninstall and **clean.exe**. The in-use condition then prevents a new installation of ACS.

### Action

Restart the computer in order to clear the in-use condition, or stop any service that is using the .dll files, such as **AgentSrv.exe**. You can use third-party tools, such as the Process Explorer, to find the processes that are using the .dlls.

## During Upgrade the ACS Folder is Locked

### Condition

When upgrading ACS, **setup.exe** hangs and displays an error message: The CiscoSecure ACS folder appears to be locked by another application... . Please close any applications that are using any files or directories and re-run Uninstall.

### Action

Remove excess log files. ACS stores log files in \CiscoSecure ACS v.x.x\Logs. If any log file folder gets too large, and you cannot upgrade, you must first delete all but the last three log files from the folder. When ACS starts up, choose **System Configuration > Service Control**. In the Services Log File Configuration, check **Manage Directory**, and choose **Keep only the last <n> files**. Set <n> to 3.

If **PNLogAgent** is running, stop that service to release any locks that it might have on the folder.

## During Uninstall the ACS Folder is Locked

### Condition

When uninstalling, the ACS folder is locked.

### Action

Check for these conditions:

- A **CSUtil.exe** process from an aborted restore is still in a created but not started state. Solution: Restart.
- Another application such as **Notepad** has a file open. Solution: Close the application.
- An explorer has a subfolder of ACS install open. Solution: Close the explorer.

## After Restart ACS Cannot Start Services

### Condition

When the Windows Firewall Internet Connection Sharing (ICS) service has started on Windows 2003, SP1, ACS cannot start these services:

- CSAuth
- CSRadius

- CSTacacs
- CSAdmin

**Action**

Manually start the services, or disable the ICS service.

To disable the ICS service:

- 
- Step 1** Locate the Windows Firewall and Internet Connection Sharing (ICS) service.
- Step 2** Right-click on the service and choose **Properties**.
- Step 3** Change the **Startup Type** to **Disabled**.
- 

## Upgrade or Uninstall Cannot Complete

**Condition**

Upgrade or uninstall cannot complete.

**Action**

Close:

- 
- Step 1** All ACS files.
- Step 2** All log files, for example, *auth.log*.
- Step 3** All programs,
- Step 4** Programs such as **Radtest**, and close any binaries that are running.
- Step 5** Microsoft Management Console (MMC) tools such as the **Performance Monitor**. For information on how to use the MMC, go to the Microsoft website.
- 

## Invalid File or Data

**Condition**

An error message appears when you try to upgrade or uninstall ACS: The following file is invalid or the data is corrupted "DelsL1.isu".

**Action**

From the Windows Registry, delete the following Registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\CiscoSecure
```

## Accounting Logs Missing

**Condition**

All previous accounting logs are missing.

**Action**

When reinstalling or upgrading the ACS software, these files are deleted; unless they have been moved to an alternative directory location.

## Upgrade Command Does Not Work (ACS Solution Engine)

**Condition**

From the serial console, the **upgrade** command has no effect.

**Action**

You must first obtain an appliance upgrade. Choose **System Configuration > Appliance Upgrade**.

## On Solaris, autorun.sh Does Not Execute (ACS Solution Engine)

**Condition**

While performing an upgrade when using a Solaris distribution server, **autorun.sh** cannot be executed.

**Action**

Use the command **chmod +x autorun.sh** to grant execution permissions to **autorun.sh**.

## Interoperability

This section contains:

- [Interoperation Between Builds, page 2-28](#)
- [Proxy Requests Fail, page 2-29](#)

## Interoperation Between Builds

**Condition**

Interoperation between different builds of ACS does not work.

**Action**

Interoperation between different builds is not supported. The builds must match.

## Proxy Requests Fail

### Condition

Proxy requests to another server fail.

### Action

Be certain that the:

- Direction on the remote server is set to Incoming and Outgoing or Incoming, and that the direction on the authentication forwarding server is set to Incoming and Outgoing or Outgoing.
- Shared secret (key) matches the shared secret of one or both ACSs.
- Character string and delimiter match the stripping information configured in the Proxy Distribution table, and the position is set correctly to Prefix or Suffix.

If the previous conditions are met, one or more servers is probably down; or, no fallback server is configured. Click **Network Configuration** from the navigation bar and configure a fallback server. Fallback servers are used only when:

- The remote ACS is down.
- One or more services (**CSTacacs**, **CSRADIUS**, or **CSAuth**) are down.
- The secret key is misconfigured.
- Inbound or outbound messaging is misconfigured.

## Logging

This section describes troubleshooting procedures for log files. For related information, see [Reports](#), page 2-31.

## Too Many Log Files

### Condition

When upgrading ACS, **setup.exe** hangs and displays an error message: `The CiscoSecure ACS folder appears to be locked by another application ... . Please close any applications that are using any files or directories and re-run Uninstall.`

### Action

If the problem still exists after closing applications and re-running the uninstall program, it could be that the folder is locked because of large number of log files.

Remove excess log files. ACS stores log files in `\CiscoSecure ACS v.4.\Logs`. If a log file folder becomes too large, and you cannot upgrade, you must first delete all but a small number of files from the folder (for example, 3). When ACS starts up, choose **System Configuration > Service Control**. In the Services Log File Configuration, check Manage Directory, and check Keep only the last <n> files. Set <n> to a small number (for example, 3).

# MAC Authentication Bypass Problems

This section contains:

- [The MAC Address Exists in LDAP but Always Maps to the Default User Group, page 2-30](#)
- [The MAC Exists in the Internal Database but is Mapped to the Wrong User Group, page 2-30](#)
- [Request is Rejected, page 2-30](#)

## The MAC Address Exists in LDAP but Always Maps to the Default User Group

### Condition

MAC exists in LDAP but always maps to the default user-group.

### Action

- Check the LDAP configuration.
- Check the LDAP Group Mapping settings.
- Verify that the MAC address format stored in the LDAP server is one of the supported formats.
- Check that the LDAP server is reachable.

## The MAC Exists in the Internal Database but is Mapped to the Wrong User Group

### Condition

The MAC exists in the internal database but is mapped to the wrong user-group.

### Action

Check that the MAC address or a prefix of the address does not exist in a previous mapping.

## Request is Rejected

### Condition

Request is rejected.

### Action

- Be certain that the Agentless Request Processing in the Protocols page is enabled.
- Check that the User-Group mapped by the MAC address is not disabled.
- Check the NAP authorization rules.

## Remote Agent (ACS Solution Engine)

This section describes troubleshooting for the Remote Agent.

## RPC Timeouts

When the appliance sends requests to the Remote Agent, it will wait no more than 60 seconds for a reply.

## Reports

This section contains:

- [Blank Reports, page 2-31](#)
- [Unknown User Information Missing, page 2-31](#)
- [Two Entries Logged for One User Session, page 2-32](#)
- [Old Format Dates Persist, page 2-32](#)
- [Logging Halted, page 2-32](#)
- [Logged in Users Report Works Only with Certain Devices, page 2-32](#)

For related information, see [Logging, page 2-29](#).

## Blank Reports

### Condition

A report is blank.

### Action

Be certain that you have selected **Log to <reportname> Report** under **System Configuration > Logging > Log Target <reportname>**. You must also set **Network Configuration <servername> Access Server Type to ACS for Windows NT**.

### Condition

The *lognameactive.csv* report is blank.

### Action

You changed protocol configurations recently.

Whenever protocol configurations change, the existing *lognameactive.csv* report file is renamed to *lognameyyyy-mm-dd.csv*, and a new, blank *lognameactive.csv* report is generated.

## Unknown User Information Missing

### Condition

No Unknown User information is included in reports.

### Action

The Unknown User database was changed. Accounting reports will still contain unknown user information.

## Two Entries Logged for One User Session

### Condition

Two entries are logged for one user session.

### Action

Be certain that the remote logging function is not configured to send accounting packets to the same location as the Send Accounting Information fields in the proxy distribution table.

## Old Format Dates Persist

### Condition

After you have changed the date format, the Logged-In User list and the **CSAdmin** log still display old format dates.

### Action

To see the changes made, you must restart the **CSAdmin** services and log on again.

## Logging Halted

### Condition

Effect of logging unavailability on authentication functionality.

### Action

When local or remote logging normal operation is halted, authentication functionality will stop after a very short time because all worker threads are busy with logging assignments. Fixing the logging functionality will restore authentication; thus, troubleshooting the logging service logs is necessary.

## Logged in Users Report Works Only with Certain Devices

### Condition

The Logged in Users report works with some devices, but not with others.

### Action

For the Logged in Users report to work (and this also applies to most other features involving sessions), packets should include:

- **Authentication Request packet**
  - `nas-ip-address`
  - `nas-port`
- **Accounting Start packet**
  - `nas-ip-address`
  - `nas-port`
  - `session-id`

- framed-ip-address
- **Accounting Stop packet**
  - nas-ip-address
  - nas-port
  - session-id
  - framed-ip-address

Also, if a connection is so brief that there is limited time between the start and stop packets (for example, HTTP through the PIX Firewall), the `Logged in Users` report may fail.

## User Group Management

This section contains:

- [MaxSessions Not Working Over VPDN, page 2-33](#)
- [MaxSessions Fluctuates, page 2-33](#)
- [MaxSessions Does Not Take Effect, page 2-33](#)
- [TACACS+ and RADIUS Attributes Missing, page 2-34](#)

### MaxSessions Not Working Over VPDN

#### Condition

MaxSessions over a Virtual Private Dialup Network (VPDN) is not working.

#### Action

The use of MaxSessions over VPDN is not supported.

### MaxSessions Fluctuates

#### Condition

User MaxSessions fluctuates or is unreliable.

#### Action

Services were restarted, possibly because the connection between the ACS and the AAA client is unstable. Uncheck the **Single Connect TACACS+ AAA Client** check box.

### MaxSessions Does Not Take Effect

#### Condition

User MaxSessions not taking effect.

**Action**

Be certain that you have accounting configured on the AAA client, and that you are receiving accounting start or stop records.

## TACACS+ and RADIUS Attributes Missing

**Condition**

TACACS+ and RADIUS attributes do not appear on the Group Setup page.

**Action**

Be certain that you have configured at least one RADIUS or TACACS+ AAA client in the Network Configuration. Be certain that you have enabled the appropriate attributes in the Interface Configuration.

**Note**

---

Some attributes are not customer-configurable; instead, ACS sets their values.

---