



Troubleshooting

This appendix provides information about certain basic problems and describes how to resolve them.

Scan the column on the left to identify the condition that you are trying to resolve, and then carefully go through each corresponding recovery action offered in the column on the right.

This chapter contains the following topics:

- [Administration Issues, page A-1](#)
- [Browser Issues, page A-3](#)
- [Cisco NAC Issues, page A-4](#)
- [Database Issues, page A-6](#)
- [Dial-in Connection Issues, page A-7](#)
- [Proxy Issues, page A-10](#)
- [Installation and Upgrade Issues, page A-10](#)
- [MaxSessions Issues, page A-11](#)
- [Report Issues, page A-11](#)
- [Third-Party Server Issues, page A-12](#)
- [User Authentication Issues, page A-13](#)
- [TACACS+ and RADIUS Attribute Issues, page A-14](#)

Administration Issues



Note

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

The following table provides troubleshooting information for administration issues.

Condition	Recovery Action
Remote administrator cannot bring up the ACS web interface in a browser or receives a warning that access is not permitted.	<p>To recover from this condition:</p> <ol style="list-style-type: none"> 1. Verify that you are using a supported browser. Refer to the <i>Release Notes for Cisco Secure ACS Solution Engine 4.0</i> for a list of supported browsers. 2. Verify that the remote administrator is using a valid administrator name and password that have previously been added in Administration Control. 3. Verify that Java functionality is enabled in the browser. 4. 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.
No remote administrators can log in.	The Allow only listed IP addresses to connect option is selected, but no start or stop IP addresses are listed. Choose Administrator Control > Access Policy , and specify the Start IP Address and End IP Address .
Unauthorized users can log in.	The Reject listed IP addresses option is selected, but no start or stop IP addresses are listed. Choose Administrator Control > Access Policy , and specify the Start IP Address and Stop IP Address .
The Restart Services function does not work.	<p>The system is not responding to the Restart command on the System Configuration > Service Control page. Ping Cisco Secure ACS to confirm connectivity.</p> <p>To manually restart services, log in to the Cisco Secure ACS console and type the restart command followed by a single space and the name of the ACS service you want to restart.</p>
Administrator configured for event notification is not receiving e-mail.	Ensure that the SMTP server name is correct. If the name is correct, ensure that the computer running ACS can ping the SMTP server or can send e-mail via a third-party e-mail software package. Ensure that you have not used underscores (_) in the e-mail address.
Remote Administrator receives Logon failed . . . protocol error message, when browsing.	Restart the CSAdmin service. To restart the CSAdmin service, from the CLI type the restart command with CSAdmin as the argument. If necessary, reboot the appliance.
Remote administrator cannot bring up ACS from his or her browser, or receives a warning that access is not permitted.	<p>If Network Address Translation is enabled on the PIX Firewall, administration through the firewall cannot work.</p> <p>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. For more information, see Access Policy, page 12-8.</p>


Browser Issues

The following table provides troubleshooting information for browser issues.

Condition	Recovery Action
The browser cannot bring up the ACS web interface.	Open Internet Explorer or Netscape Navigator. Choose Help > About to determine the version of the browser. See <i>Installation and Setup Guide for Cisco Secure ACS Solution Engine</i> for a list of browsers that ACS supports, and the release notes for known issues with a particular browser version.
The browser displays the Java message that your session connection is lost.	Check the Session idle timeout value for remote administrators. This value appears on the Session Policy Setup page of the Administration Control section. Increase the value as needed.
Administrator database appears corrupted.	The remote Netscape client is caching the password. If you specify an incorrect password, it is cached. When you attempt to re-authenticate with the correct password, the incorrect password is sent. Clear the cache before attempting to re-authenticate, or close the browser and open a new session.
Remote administrator intermittently can't browse the ACS web interface.	Ensure that the client browser does not have proxy server configured. ACS does not support HTTP proxy for remote administrative sessions. Disable proxy server settings.

Cisco NAC Issues

The following table provides troubleshooting information for Cisco NAC issues.

Condition	Recovery Action
The results of <code>show eou all</code> or <code>show eou ip address</code> include postures that do not match the actual result of posture validation or display “-----” instead of a posture.	<p>If you see “-----”, the AAA client is not receiving the posture-token attribute-value (AV) pair within a Cisco IOS/PIX RADIUS <code>cisco-av-pair</code> 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.</p> <p>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, ensure that the Cisco IOS/PIX <code>cisco-av-pair</code> VSA is configured correctly. For example, in a group configured to authorize NAC clients receiving a Healthy SPT, be sure the <code>[009\001] cisco-av-pair</code> check box is checked and that the following string appears in the <code>[009\001] cisco-av-pair</code> text box:</p> <pre>posture-token=Healthy</pre> <p> 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 posture-token can result in the incorrect SPT being sent to the AAA client; or, if the AV pair name is mistyped, the AAA client not receiving the SPT at all.</p> <p>Note AV pair names are case sensitive.</p> <p>For more information about the Cisco IOS/PIX <code>cisco-av-pair</code> VSA, see About the cisco-av-pair RADIUS Attribute, page C-5.</p>
Under EXEC Commands, Cisco IOS commands are not being denied when checked.	<p>Examine the Cisco IOS configuration at the AAA client. If it is not already present, add the following Cisco IOS command to the AAA client configuration:</p> <pre>aaa authorization command <0-15> default group TACACS+</pre> <p>The correct syntax for the arguments in the text box is permit <i>argument</i> or deny <i>argument</i>.</p>
EAP request has invalid signature. Error message appears in log.	<p>If ACS receives traffic from any EAP-enabled device that has the wrong shared secret, this error message appears in the log. Three conditions that might cause this to occur are:</p> <ul style="list-style-type: none"> • The wrong signature is being used. • A RADIUS packet was corrupted in transit. • ACS is being attacked. <p>Check the EAP-enabled device and make changes if necessary.</p>
Administrator has been locked out of the AAA client because of an incorrect configuration setup in the AAA client.	<p>If you have a fallback method configured on your AAA client, disable connectivity to the AAA server and log in using local or line username and password.</p> <p>Try to connect directly to the AAA client at the console port. If that is not successful, consult your AAA client documentation or see the Password Recovery Procedures page on Cisco.com for information regarding your particular AAA client.</p>

Condition	Recovery Action
<p>Unable to enter Enable Mode after doing <code>aaa authentication enable default tacacs+</code>. Getting error message: Error in authentication on the router.</p>	<p>Check the failed attempts log in the ACS. If the log reads <code>CS password invalid</code>, it may be that the user has no enable password set up. Set the TACACS+ Enable Password in the Advanced TACACS+ Settings section.</p> <p>If you do not see the Advanced TACACS+ Settings section among the user setup options, choose Interface Configuration > Advanced Configuration Options > Advanced TACACS+ Features and select that option to have the TACACS+ settings appear in the user settings. Then select Max privilege for any AAA Client (this will typically be 15) and enter the TACACS+ Enable Password that you want the user to have for enable.</p>
<p>NAC NRE/Guest Access Limit of 100 Endpoints.</p>	<p>A feature in the EAPoUDP state table that prevents denial of service (DoS) attacks on the ACS server by throttling RADIUS requests.</p> <p>When the maximum limit of 100 unauthorized nonresponsive endpoints per NAD is reached, the following message appears on the router console:</p> <pre>*Jan 19 09:51:04.855: %AP-4-POSTURE_EXCEED_MAX_INIT: Exceeded maximum limit (100).</pre> <p>The router stops processing RADIUS requests for NAC. This mechanism will leave legitimate users—with or without CTA—with default network access (whatever the router's interface ACL allows).</p> <p>This message appears because 100 (or more) EAPoUDP sessions are in the INIT state. Normally, upon 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 during any of the following situations. The:</p> <ul style="list-style-type: none"> • NAD has over 100 concurrently unauthorized endpoints. • Router receives an Access-Reject from ACS. • Router fails to receive a response from ACS. <p>Based on this behavior, remember the following recommendations:</p> <ul style="list-style-type: none"> • Properly configure ACS for NAC to minimize unintentional Access-Rejects. • When deploying NAC passively (monitor-only mode), configure ACS to accept all nonresponsive endpoints (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 or they will prevent access for CTA-enabled endpoints. • Set the default hold period to a low value. <p>A new command will be added to the IOS to allow this limit to be increased or decreased as needed for a given deployment.</p>

Database Issues

The following table provides troubleshooting information for database issues.

Condition	Recovery Action
RDBMS Synchronization is not operating properly.	Make sure that the correct server appears in the Partners list.
Database Replication not operating properly.	<ul style="list-style-type: none"> • Make sure you have set the server correctly as Send or Receive. • On the sending server, ensure that the receiving server is in the Replication list. • On the receiving server, ensure that the sending server is selected in the Accept Replication from list. Also, ensure that the sending server is not in the replication partner list. • Make sure 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 a AAA server to the AAA Servers table in Network Configuration for every IP address of the receiving server.
The external user database is not available in the Group Mapping section.	The external database has not been configured in the External User Databases section; or, the username and password have been typed incorrectly. Click the applicable external database to configure. Make sure that the username and password are correct.
External databases not operating properly.	Make sure that a two-way trust (for dial-in check) has been established between the ACS domain and the other domains. Check the <i>csauth</i> service log file for any debug messages beginning with [External DB].
Unknown users are not authenticated.	<p>To remedy this situation:</p> <ol style="list-style-type: none"> 1. Choose External User Databases > Unknown User Policy. 2. Select the Check the following external user databases option. 3. From the External Databases list, select the database(s) against which to authenticate unknown users. 4. Click —> (right arrow button) to add the database to the Selected Databases list. 5. Click Up or Down to move the selected database into the correct position in the authentication hierarchy. <p>If you are using the ACS Unknown User feature, external databases can only authenticate by using PAP.</p>

Dial-in Connection Issues

The following table provides troubleshooting information for dial-in connection issues.

Condition	Recovery Action
<p>A dial-in user cannot connect to the AAA client.</p> <p>No record of the attempt appears in the TACACS+ or RADIUS Accounting Report (in the Reports & Activity section, click TACACS+ Accounting or RADIUS Accounting or Failed Attempts).</p>	<p>Examine the ACS Reports or AAA client Debug output to narrow the problem to a system error or a user error. Confirm that:</p> <ul style="list-style-type: none"> • The dial-in user was able to establish a connection and ping the computer <i>before</i> ACS was installed. If the dial-in user could not, the problem is related to a AAA client/modem configuration, not ACS. • LAN connections for both the AAA client and the computer 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 key in both AAA client and ACS are identical (case sensitive). • The command ppp authentication pap is entered for each interface, if you are using a Windows user database. • The command ppp authentication chap pap is entered for each interface, if you are using the ACS database. • The AAA and TACACS+ or RADIUS commands are correct in the AAA client. The necessary commands reside in: <ul style="list-style-type: none"> <i>Program Files\CiscoSecure ACS vx.x\TacConfig.txt</i> <i>Program Files\CiscoSecure ACS vx.x\RadConfig.txt</i> • The ACS Services are running (CSAdmin, CSAAuth, CSDBSync CSLog, CSRADIUS, CSTacacs) on the computer running ACS.

Condition	Recovery Action
<p>A dial-in user cannot connect to the AAA client.</p> <p>The Windows user database is being used for authentication.</p> <p>A record of a failed attempt appears in the Failed Attempts Report (in the Reports & Activity section, click Failed Attempts).</p>	<p>Create a local user in the ACS internal database and test whether authentication is successful. If it is successful, the issue is that the user information is not correctly configured for authentication in Windows or ACS.</p> <p>From the Windows User Manager or Active Directory Users and Computers, confirm that the:</p> <ul style="list-style-type: none"> • 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 have Account Disabled selected. • User Properties for the dial-in window does not have Grant dial-in permission to user disabled, if ACS is using this option for authenticating. <p>From within ACS confirm that:</p> <ul style="list-style-type: none"> • If the username has already been entered into ACS, a Windows user database configuration is selected in the Password Authentication list on the User Setup page for the user. • If the username has already been entered into ACS, the ACS group to which the user is assigned has the correct authorization enabled (such as IP/PPP, IPX/PPP or Exec/Telnet). Click Submit + Restart if a change has been made. • The user expiration information in the Windows user database has not caused failed authentication. For troubleshooting purposes, disable password expiry for the user in the Windows user database. <p>Click External User Databases, click List All Databases Configured, and then ensure that the database configuration for Windows is listed.</p> <p>In the Configure Unknown User Policy table of the External User Databases section ensure that the Fail the attempt option is not selected. And ensure that the Selected Databases list reflects the necessary database.</p> <p>Verify that the Windows group that the user belongs to has not been mapped to No Access.</p>
<p>A dial-in user cannot connect to the AAA client.</p> <p>The ACS internal database is being used for authentication.</p> <p>A record of a failed attempt appears in the Failed Attempts Report (in the Reports & Activity section, click Failed Attempts).</p>	<p>From within ACS confirm that:</p> <ul style="list-style-type: none"> • The username has been entered into ACS. • ACS internal database is selected from the Password Authentication list and a password has been entered in User Setup for the user. • The ACS group to which the user is assigned has the correct authorization enabled (such as IP/PPP, IPX/PPP or Exec/Telnet). Click Submit + Restart if a change has been made. • Expiration information has not caused failed authentication. Set to Expiration: Never for troubleshooting.

Condition	Recovery Action
A dial-in user cannot connect to the AAA client; however, a Telnet connection can be authenticated across the LAN.	<p>The problem is isolated to one of three areas:</p> <ul style="list-style-type: none"> • 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. Authorization rights can be modified 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. <p>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.</p>
A dial-in user cannot connect to the AAA client, and a Telnet connection cannot be authenticated across the LAN.	<p>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, troubleshoot the problem based on:</p> <ul style="list-style-type: none"> • 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 is not working.	Ensure that callback works on the AAA client when using local authentication. Then add AAA authentication.
User authentication fails when using PAP.	Outbound PAP is not enabled. If the Failed Attempts report shows that you are using outbound PAP, go to the Interface Configuration section and check the Per-User Advanced TACACS+ Features check box. Then, choose the TACACS+ Outbound Password section of the Advanced TACACS+ Settings table on the User Setup page and type and confirm the password in the boxes provided.

Proxy Issues

The following table provides troubleshooting information for proxy issues.

Condition	Recovery Action
Proxying requests to another server fail.	<p>Ensure that the:</p> <ul style="list-style-type: none"> • Direction on the remote server is set to Incoming/Outgoing or Incoming, and that the direction on the authentication forwarding server is set to Incoming/Outgoing or Outgoing. • Shared secret (key) matches the shared secret of one or both ACSes. • Character string and delimiter match the stripping information configured in the Proxy Distribution Table, and the position is set correctly to either Prefix or Suffix. <p>If the previous conditions are met, one or more servers is probably down, or no fallback server is configured. Choose the Network Configuration section and configure a fallback server. Fallback servers are used only when:</p> <ul style="list-style-type: none"> • 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.

Installation and Upgrade Issues

The following table provides troubleshooting information for installation and upgrade issues.

Condition	Recovery Action
Installation difficulties	Refer to your <i>Installation and Setup Guide for Cisco Secure ACS Solution Engine</i> .
From the serial console, the upgrade command has no effect.	You must first obtain an appliance upgrade (when available, obtained from the Appliance Upgrade page of System Configuration).
While performing an upgrade using a Solaris distribution server, <code>autorun.sh</code> cannot be executed.	Use the command chmod +x autorun.sh to grant execution permissions to autorun.sh .

MaxSessions Issues

The following table provides troubleshooting information for MaxSessions issues.

Condition	Recovery Action
MaxSessions over VPDN is not working.	The use of MaxSessions over VPDN is not supported.
User MaxSessions fluctuates or is unreliable.	Services were restarted, possibly because the connection between the ACS and the AAA client is unstable. Click to clear the Single Connect TACACS+ AAA Client check box.
User MaxSessions not taking affect.	Ensure that you have accounting configured on the AAA client, and you are receiving accounting start or stop records.

Report Issues

The following table provides troubleshooting information for report issues.

Condition	Recovery Action
The <i>lognameactive.csv</i> report is blank.	You changed protocol configurations recently. Whenever protocol configurations change, the existing <i>lognameactive.csv</i> report file is renamed to <i>lognameyyy-mm-dd.csv</i> , and a new, blank <i>lognameactive.csv</i> report is generated.
A report is blank.	Ensure that you have selected Log to <i>reportname</i> Report under System Configuration: Logging: Log Target: <i>reportname</i> . You must also set Network Configuration: <i>servername</i> : Access Server Type to ACS for Windows NT.
No Unknown User information is included in reports.	The Unknown User database was changed. Accounting reports will still contain unknown user information.
Two entries are logged for one user session.	Make sure 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.
After you have changed the date format, the Logged-In User list and the <i>CSAdmin</i> log still display old format dates.	To see the changes made, you must restart the <i>CSAdmin</i> services and log on again.
Effect of logging unavailability on authentication functionality.	When local or remote logging normal operation is halted, authentication functionality will stop after a very short time as all worker threads are busy with logging assignments. Fixing the logging functionality will restore authentication; thus, troubleshooting the logging service logs is necessary.

Condition	Recovery Action
The Logged in Users report works with some devices, but not with others	<p>For the Logged in Users report to work (and this also applies to most other features involving sessions), packets should include at least the following fields:</p> <ul style="list-style-type: none"> • Authentication Request packet <ul style="list-style-type: none"> – nas-ip-address – nas-port • Accounting Start packet <ul style="list-style-type: none"> – nas-ip-address – nas-port – session-id – framed-ip-address • Accounting Stop packet <ul style="list-style-type: none"> – nas-ip-address – nas-port – session-id – framed-ip-address <p>Also, if a connection is so brief that there is little time between the start and stop packets (for example, HTTP through the PIX Firewall), the Logged in Users report may fail.</p>

Third-Party Server Issues

The following table provides troubleshooting information for third-party server issues.

Condition	Recovery Action
Authentication request does not hit the external database.	<p>Set logging to full. Choose System Configuration > Service Control.</p> <p>Check <i>auth.log</i> for confirmation that the authentication request is being forwarded to the third-party server. If it is not being forwarded, confirm that the external database configuration is correct, as well as the unknown user policy settings.</p>
On ACE/SDI server no incoming request is seen from ACS, although RSA/agent authentication works.	<p>For dial-up users, ensure that you are using PAP and not MS-CHAP or CHAP. RSA/SDI does not support CHAP and ACS will not send the request to the RSA server; rather, it will log an error with external database failure.</p>

User Authentication Issues

The following table provides troubleshooting information for user authentication issues.

Condition	Recovery Action
After the administrator disables the Dialin Permission setting, Windows database users can still dial in and apply the Callback string configured under the Windows user database. (To locate the Dialin Permission check box, choose External User Databases > Database Configuration > Windows Database > Configure.)	Restart ACS services. For steps, see Stopping, Starting, or Restarting Services, page 8-2 .
User did not inherit settings from new group.	Users moved to a new group inherit new group settings; but they keep their existing user settings. Manually change the settings in the User Setup section.
Authentication fails.	Check the Failed Attempts report. The retry interval may be too short. (The default is 5 seconds.) Increase the retry interval (<code>tacacs-server timeout 20</code>) on the AAA client to 20 or greater.
The AAA client times out when authenticating against a Windows user database.	Increase the TACACS+/RADIUS timeout interval from the default, 5, to 20. Set the Cisco IOS command as: <code>tacacs-server timeout 20</code> <code>radius-server timeout 20</code>
Authentication fails; the error <code>Unknown NAS</code> appears in the Failed Attempts log.	Verify the following: <ul style="list-style-type: none"> • AAA client is configured under the Network Configuration section. • 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 interface specified.
Authentication fails; the error <code>key mismatch</code> appears in the Failed Attempts log.	Verify that the TACACS+ or RADIUS keys, in AAA client and ACS, are identical (case sensitive). Re-enter the keys to confirm they are identical.
User can authenticate, but authorizations are not what is expected.	Different vendors use different AV pairs. AV pairs used in one vendor protocol may be ignored by another vendor protocol. Ensure that the user settings reflect the correct vendor protocol; for example, RADIUS (Cisco IOS/PIX).
LEAP authentication fails; the error <code>Radius extension DLL rejected user</code> appears in the Failed Attempts log.	Verify the correct authentication type has been set on the Access Point. Ensure that, at a minimum, the Network-EAP check box is selected. If you are using an external user database for authentication, verify that it is supported. For more information, see Authentication Protocol-Database Compatibility, page 1-7 .

TACACS+ and RADIUS Attribute Issues

The following table provides troubleshooting information for TACACS+ and RADIUS attribute issues.

Condition	Recovery Action
TACACS+ and RADIUS attributes do not appear on the Group Setup page.	<p data-bbox="667 426 1442 548">Ensure that you have at least one RADIUS or TACACS+ AAA client configured in the Network Configuration section and that, in the Interface Configuration section, you have enabled the attributes you need to configure.</p> <p data-bbox="667 562 1463 625">Note Some attributes are not customer-configurable in ACS; instead, their values are set by ACS.</p>