



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-2](#)
- [Browser Issues, page A-4](#)
- [Cisco IOS Issues, page A-5](#)
- [Database Issues, page A-7](#)
- [Dial-in Connection Issues, page A-10](#)
- [Debug Issues, page A-14](#)
- [Proxy Issues, page A-15](#)
- [Installation and Upgrade Issues, page A-16](#)
- [MaxSessions Issues, page A-16](#)
- [Report Issues, page A-17](#)
- [Third-Party Server Issues, page A-19](#)
- [User Authentication Issues, page A-20](#)
- [TACACS+ and RADIUS Attribute Issues, page A-22](#)

Administration Issues


Condition	Recovery Action
<p>Remote administrator cannot bring up the Cisco Secure ACS HTML interface in a browser or receives a warning that access is not permitted.</p>	<ul style="list-style-type: none"> • Verify that you are using a supported browser. Refer to the <i>Release Notes for Cisco Secure Access Control Server for Windows Server Version 3.3</i> for a list of supported browsers. • Ping Cisco Secure ACS to confirm connectivity. • Verify that the remote administrator is using a valid administrator name and password that have previously been added in Administration Control. • Verify that Java functionality is enabled in the browser. • Determine whether the remote administrator is trying to administer Cisco Secure ACS through a firewall, through a device performing Network Address Translation, or from a browser configured to use an HTTP proxy server. For more information about accessing the HTML interface in these networking scenarios, see Network Environments and Administrative Sessions, page 1-30.
<p>No remote administrators can log in.</p>	<p>The option Allow only listed IP addresses to connect is selected, but no start or stop IP addresses are listed. Go to Administrator Control > Access Policy and specify the Start IP Address and End IP Address.</p>
<p>Unauthorized users can log in.</p>	<p>The option Reject listed IP addresses is selected, but no start or stop IP addresses are listed. Go to Administrator Control > Access Policy and specify the Start IP Address and Stop IP Address.</p>
<p>The Restart Services function does not work.</p>	<p>This may occur if the system is not responding. To manually restart services, from the Windows Start menu, choose Settings > Control Panel > Administrative Tools > Services. Click CSAdmin, and then Stop, and then Start.</p> <p>If the services do not respond when manually restarted, reboot the server.</p>

Condition	Recovery Action
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 Cisco Secure ACS can ping the SMTP server or can send e-mail via a third-party e-mail software package. Make sure 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 Windows Start menu choose Control Panel > Services . Click CSAdmin , and then Stop , and then Start . If necessary, restart the server.
Remote administrator cannot bring up Cisco Secure ACS from his or her browser, or receives a warning that access is not permitted.	If Network Address Translation is enabled on the PIX Firewall, administration through the firewall cannot work. To administer Cisco Secure ACS through a firewall, you must configure an HTTP port range in Administrator Control > Access Policy . The PIX Firewall must be configured to permit HTTP traffic over all ports included in the range specified in Cisco Secure ACS. For more information, see Access Policy, page 12-11 .
Unable to log in on Cisco Secure ACS. Authentication fails.	Back up the NT Registry. Use the regedit command and remove the users in the following: <code>HKEY_LOCAL_MACHINE\SOFTWARE\Cisco\CiscoAAA#\CSAdmin\Administrators</code> Under the Administrators key you will see all administrators that you have created. Delete the users and exit the Registry. Upon accessing Cisco Secure ACS, you will not be prompted for a username and password. After you have brought up the Cisco Secure ACS HTML interface, you can re-add administrators.

Browser Issues

Condition	Recovery Action
The browser cannot bring up the Cisco Secure ACS HTML interface.	<p>Open Internet Explorer or Netscape Navigator and choose Help > About to determine the version of the browser. See System Requirements, page 2-2, for a list of browsers supported by Cisco Secure ACS and the release notes for known issues with a particular browser version.</p> <p>For information about various network scenarios that affect remote administrative sessions, see Network Environments and Administrative Sessions, page 1-30.</p>
The browser displays the Java message that your session connection is lost.	Check the Session idle timeout value for remote administrators. This is 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 Cisco Secure ACS HTML interface.	Make sure that the client browser does not have proxy server configured. Cisco Secure ACS does not support HTTP proxy for remote administrative sessions. Disable proxy server settings.

Cisco IOS Issues

Condition	Recovery Action
<p>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>	<p>If the posture displayed is “-----”, 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 displayed 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 configured for use with NAC, be sure 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 [009\001] cisco-av-pair check box is selected and that the following string appears in the [009\001] cisco-av-pair text box:</p> <pre>posture-token=Healthy</pre> <hr/> <p> Caution The posture-token AV pair is the only way that Cisco Secure ACS notifies the AAA client of the SPT returned by posture validation. 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> <hr/> <p>Note AV pair names are case sensitive.</p> <p>For information about group mapping for NAC databases, see NAC Group Mapping, page 17-13. For more information about the Cisco IOS/PIX <code>cisco-av-pair</code> VSA, see About the cisco-av-pair RADIUS Attribute, page C-7.</p>

Condition	Recovery Action
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 argument or deny argument.</p>
Administrator has been locked out of the AAA client because of an incorrect configuration set up 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/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>
IETF RADIUS attributes not supported in Cisco IOS 12.0.5.T	<p>Cisco incorporated RADIUS (IETF) attributes in Cisco IOS Release 11.1. However, there are a few attributes that are not yet supported or that require a later version of the Cisco IOS software. For more information, see the RADIUS Attributes page on Cisco.com.</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>Check the failed attempts log in the ACS. If the log reads “CS password invalid,” it may be that the user has no enable password set up. Set the TACACS+ Enable Password within the Advanced TACACS+ Settings section.</p> <p>If you do not see the Advanced TACACS+ Settings section among the user setup options, go to 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>

Database Issues

Condition	Recovery Action
RDBMS Synchronization is not operating properly.	Make sure that the correct server is listed in the Partners list.
Database Replication not operating properly.	<ul style="list-style-type: none"> • Make sure you have set the server correctly as either Send or Receive. • On the sending server, make sure the receiving server is in the Replication list. • On the receiving server, make sure the sending server is selected in the Accept Replication from list. Also, make sure that the sending server is not in the replication partner list. • Make sure that the replication schedule on the sending Cisco Secure ACS is not conflicting with the replication schedule on the receiving Cisco Secure 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.

Condition	Recovery Action
External databases not operating properly.	<p>Make sure that a two-way trust (for dial-in check) has been established between the Cisco Secure ACS domain and the other domains.</p> <p>If Cisco Secure ACS is installed on a Member Server and is authenticating to a Domain Controller, see the “Authentication Failures When ACS/NT 3.0 Is Authenticating to Active Directory” Field Notice at the following URL:</p> <p>http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_field_notice09186a00800b1583.shtml</p>
Cannot install Novell NDS database authentication.	Make sure Novell Requestor is installed on the same Windows server as the Cisco Secure ACS.
Unknown users are not authenticated.	<p>Go to External User Databases > Unknown User Policy. Select the Check the following external user databases option. From the External Databases list, select the database(s) against which to authenticate unknown users. Click → (right arrow button) to add the database to the Selected Databases list. Click Up or Down to move the selected database into the desired position in the authentication hierarchy.</p> <p>If you are using the Cisco Secure ACS Unknown User feature, external databases can only authenticate using PAP.</p>
Novell NDS or Generic LDAP Group Mapping not working correctly.	<p>Make sure that you have correctly configured Group Mapping for the applicable database.</p> <p>For more information, see Chapter 17, “User Group Mapping and Specification”.</p>

Condition	Recovery Action
Unable to authenticate against the Novell NDS database.	<p>Make sure that the tree name, context name, and container name are all specified correctly. Start with one container where users are present; then you can add more containers later, if needed.</p> <p>If you are successful, check on the AAA client to see if you can authenticate the shell user (Telnet user). Also make sure that for PPP you have PAP authentication configured on the asynchronous interface.</p>
Same user appears in multiple groups or duplicate users exist in the Cisco Secure ACS database. Unable to delete user from database.	<p>Clean up the database typing the following command from the command line:</p> <pre>csutil -q -d -n -l dump.txt</pre> <p>This command causes the database to be unloaded and reloaded to clear up the counters.</p> <p>Tip When you install Cisco Secure ACS in the default location, CSUtil.exe is located in the following directory: C:\Program Files\CiscoSecure ACS vX.X\Utils.</p> <p>For more information on using the csutil command see Appendix D, “CSUtil Database Utility”.</p>

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 either the TACACS+ or RADIUS Accounting Report (in the Reports & Activity section, click TACACS+ Accounting or RADIUS Accounting or Failed Attempts).</p>	<p>Examine the Cisco Secure ACS Reports or AAA client Debug output to narrow the problem to a system error or a user error. Confirm the following:</p> <ul style="list-style-type: none"> • The dial-in user was able to establish a connection and ping the computer <i>before Cisco Secure ACS</i> was installed. If the dial-in user could not, the problem is related to a AAA client/modem configuration, not Cisco Secure ACS. • LAN connections for both the AAA client and the computer running Cisco Secure ACS are physically connected. • IP address of the AAA client in the Cisco Secure ACS configuration is correct. • IP address of Cisco Secure ACS in AAA client configuration is correct. • TACACS+ or RADIUS key in both AAA client and Cisco Secure 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 Cisco Secure ACS database. • The AAA and TACACS+ or RADIUS commands are correct in the AAA client. The necessary commands are listed in the following: <ul style="list-style-type: none"> Program Files\CiscoSecure ACS vx.x\TacConfig.txt Program Files\CiscoSecure ACS vx.x\RadConfig.txt • The Cisco Secure ACS Services are running (CSAdmin, CSAuth, CSDBSync CSLog, CSRADIUS, CSTacacs) on the computer running Cisco Secure 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 CiscoSecure user 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 Cisco Secure ACS.</p> <p>From the Windows User Manager or Active Directory Users and Computers, confirm the following:</p> <ul style="list-style-type: none"> • The username and password are configured in the Windows User Manager or Active Directory Users and Computers. • The user can log in to the domain by authenticating through a workstation. • The User Properties window does not have User Must Change Password at Login enabled. • The User Properties window does not have Account Disabled selected. • The User Properties for the dial-in window does not have Grant dial-in permission to user disabled, if Cisco Secure ACS is using this option for authenticating. <p>From within Cisco Secure ACS confirm the following:</p> <ul style="list-style-type: none"> • If the username has already been entered into Cisco Secure 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 Cisco Secure ACS, the Cisco Secure ACS group to which the user is assigned has the correct authorization enabled (such as IP/PPP, IPX/PPP or Exec/Telnet). Be sure to 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, and click List All Databases Configured, and then make sure 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 Fail the attempt 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>

Condition	Recovery Action
<p>A dial-in user cannot connect to the AAA client.</p> <p>The CiscoSecure user database is being used for authentication.</p> <p>A record of a failed attempt is displayed in the Failed Attempts Report (in the Reports & Activity section, click Failed Attempts).</p>	<p>From within Cisco Secure ACS confirm the following:</p> <ul style="list-style-type: none"> • The username has been entered into Cisco Secure ACS. • CiscoSecure user database is selected from the Password Authentication list and a password has been entered in User Setup for the user. • The Cisco Secure ACS group to which the user is assigned has the correct authorization enabled (such as IP/PPP, IPX/PPP or Exec/Telnet). Be sure to click Submit + Restart if a change has been made. • Expiration information has not caused failed authentication. Set to Expiration: Never for troubleshooting.
<p>A dial-in user cannot connect to the AAA client; however, a Telnet connection can be authenticated across the LAN.</p>	<p>The problem is isolated to one of three areas:</p> <ul style="list-style-type: none"> • Line/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 Cisco Secure ACS or TACACS+ or RADIUS configuration is not correct in the AAA client. <p>Additionally, you can verify Cisco Secure ACS connectivity by attempting to Telnet to the access server from a workstation connected to the LAN. A successful authentication for Telnet confirms that Cisco Secure ACS is working with the AAA client.</p>

Condition	Recovery Action
A dial-in user cannot connect to the AAA client, and a Telnet connection cannot be authenticated across the LAN.	<p>Determine whether the Cisco Secure ACS is receiving the request. This can be done by viewing the Cisco Secure ACS reports. Based on what does not appear in the reports and which database is being used, troubleshoot the problem based on one of the following:</p> <ul style="list-style-type: none">• Line/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 CiscoSecure user database and might not have the correct password. Authentication parameters can be modified under User Setup.• The Cisco Secure 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 select the Per-User Advanced TACACS+ Features check box. Then, go to 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.

Debug Issues

Condition	Recovery Action
<p>When you run debug aaa authentication on the AAA client, Cisco Secure ACS returns a failure message.</p>	<p>The configurations of the AAA client or Cisco Secure ACS are likely to be at fault.</p> <p>From within Cisco Secure ACS confirm the following:</p> <p>Cisco Secure ACS is receiving the request. This can be done by viewing the Cisco Secure ACS reports. What does or does not appear in the reports may provide indications that your Cisco Secure ACS is misconfigured.</p> <p>From the AAA client, confirm the following:</p> <ul style="list-style-type: none"> • The command ppp authentication pap is entered for each interface if authentication against the Windows user database is being used. • The command ppp authentication chap pap is entered for each interface if authentication against the CiscoSecure user database is being used. • The AAA and TACACS+ or RADIUS configuration is correct in the AAA client.
<p>When you run debug aaa authentication and debug aaa authorization on the AAA client, Cisco Secure ACS returns a <code>PASS</code> for authentication, but returns a <code>FAIL</code> for authorization.</p>	<p>This problem occurs because authorization rights are not correctly assigned.</p> <p>Examine the following:</p> <ul style="list-style-type: none"> • Check failed attempts reports under Reports and Activities to see if any services/protocols are being denied for the user. • From User Setup, confirm that the user is 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. • If a specific attribute for TACACS+ or RADIUS is not displayed within the Group Setup section, this may indicate that it has not been enabled in Interface Configuration: TACACS+ (Cisco IOS) or RADIUS.

Proxy Issues

Condition	Recovery Action
Proxying requests to another server fail	<p>Make sure that the following conditions are met:</p> <ul style="list-style-type: none"> • The 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. • The shared secret (key) matches the shared secret of one or both Cisco Secure ACSes. • The 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 conditions above are met, one or more servers is probably down, or no fallback server is configured. Go to the Network Configuration section and configure a fallback server. Fallback servers are used only under the following circumstances:</p> <ul style="list-style-type: none"> • The remote Cisco Secure ACS is down. • One or more services (CSTacacs, CSRADIUS, or CSAUTH) are down. • The secret key is misconfigured. • Inbound/Outbound messaging is misconfigured.

Installation and Upgrade Issues

Condition	Recovery Action
<p>The following error message appears when you try to upgrade or uninstall Cisco Secure ACS:</p> <p>The following file is invalid or the data is corrupted</p> <p>"DelsL1.isu"</p>	<p>From the Windows Registry, delete the following Registry key:</p> <pre>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion\Uninstall\CiscoSecure</pre>
<p>All previous accounting logs are missing.</p>	<p>When reinstalling or upgrading the Cisco Secure ACS software, these files are deleted unless they have been moved to an alternative directory location.</p>

MaxSessions Issues

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

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>lognameyyyy-mm-dd.csv</i> , and a new, blank <i>lognameactive.csv</i> report is generated
A report is blank.	Make sure 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 Cisco Secure 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.

Condition	Recovery Action
The <code>Logged in Users</code> report works with some devices, but not with others	<p>For the <code>Logged in Users</code> 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 <code>Logged in Users</code> report may fail.</p>

Third-Party Server Issues

Condition	Recovery Action
You cannot successfully implement the RSA token server.	<ol style="list-style-type: none"> 1. Log in to the computer running Cisco Secure ACS. (Make sure your login account has administrative privileges.) 2. Make sure the RSA Client software is installed on the same computer as Cisco Secure ACS. 3. Follow the setup instructions. Do not restart at the end of the installation. 4. Get the file named <code>sdconf.rec</code> located in the <code>/data</code> directory of the RSA ACE server. 5. Place <code>sdconf.rec</code> in the <code>%SystemRoot%\system32</code> directory. 6. Make you can ping the machine that is running the ACE server by hostname. (You might need to add the machine in the <code>lmhosts</code> file.) 7. Verify that support for RSA is enabled in External User Database: Database Configuration in the Cisco Secure ACS. 8. Run Test Authentication from the Windows control panel for the ACE/Client application. 9. From Cisco Secure ACS, install the token server.
Authentication request does not hit the external database.	<p>Set logging to full in System Configuration > Service Control</p> <p>Check <code>csauth.log</code> 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 Cisco Secure ACS, although RSA/agent authentication works.	<p>For dial-up users, make sure you are using PAP and not MS-CHAP or CHAP; RSA/SDI does not support CHAP, and Cisco Secure ACS will not send the request to the RSA server, but rather it will log an error with external database failure.</p>

User Authentication Issues

Condition	Recovery Action
<p>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. (You can locate the Dialin Permission check box by clicking External User Databases, clicking Database Configuration, clicking Windows Database, and clicking Configure.)</p>	<p>Restart Cisco Secure ACS services. For steps, see Stopping, Starting, or Restarting Services, page 8-2.</p>
<p>User did not inherit settings from new group.</p>	<p>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.</p>
<p>Authentication fails.</p>	<p>Check the Failed Attempts report.</p> <p>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.</p>
<p>The AAA client times out when authenticating against a Windows user database.</p>	<p>Increase the TACACS+/RADIUS timeout interval from the default, 5, to 20. Set the Cisco IOS command as follows:</p> <p>tacacs-server timeout 20 radius-server timeout 20</p>

Condition	Recovery Action
Authentication fails; the error “Unknown NAS” appears in the Failed Attempts log.	<p>Verify the following:</p> <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, make sure the client on ACS is configured using the IP address of the interface specified. <p>Alternatively, you can configure a default NAS in the NAS configuration area by leaving the hostname and IP address blank and entering only the key.</p>
Authentication fails; the error “key mismatch” appears in the Failed Attempts log.	<p>Verify that the TACACS+ or RADIUS keys, in both AAA client and Cisco Secure ACS, are identical (case sensitive).</p> <p>Re-enter the keys to confirm they are identical.</p>
User can authenticate, but authorizations are not what is expected.	<p>Different vendors use different AV pairs. AV pairs used in one vendor protocol may be ignored by another vendor protocol. Make sure that the user settings reflect the correct vendor protocol; for example, RADIUS (Cisco IOS/PIX).</p>
LEAP authentication fails; the error “Radius extension DLL rejected user” appears in the Failed Attempts log.	<p>Verify the correct authentication type has been set on the Access Point. Make sure that, at a minimum, the Network-EAP check box is selected</p> <p>If you are using an external user database for authentication, verify that it is supported. For more information, see Authentication Protocol-Database Compatibility, page 1-10.</p>

TACACS+ and RADIUS Attribute Issues

Condition	Recovery Action
TACACS+ and RADIUS attributes do not appear on the Group Setup page.	<p data-bbox="674 319 1245 475">Make sure 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="674 492 1245 623">Note Some attributes are not customer-configurable in Cisco Secure ACS; instead, their values are set by Cisco Secure ACS.</p>