



CHAPTER 10

Logs and Reports

The Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS, produces a variety of logs. You can download many of these logs, or view them in the ACS web interface as HTML reports.

These topics describe how to configure and view ACS logs and reports:

- [About ACS Logs and Reports, page 10-1](#)
- [Configuring ACS Logs, page 10-22](#)
- [Viewing and Downloading Reports, page 10-30](#)
- [Update Packets in Accounting Logs, page 10-37](#)
- [Logging Configuration Pages Reference, page 10-37](#)
- [Service Control Page Reference, page 10-43](#)
- [Reports Page Reference, page 10-44](#)

About ACS Logs and Reports

ACS logs a variety of user and system activities to different formats and targets. These topics describe the information that you can log:

- [AAA-Related Logs, page 10-1](#)
- [ACS Audit Logs, page 10-5](#)
- [ACS Logging Formats and Targets, page 10-5](#)
- [Dynamic Administration Reports, page 10-11](#)
- [Entitlement Reports, page 10-11](#)
- [Service Logs, page 10-12](#)

AAA-Related Logs

AAA-related logs contain information about the use of remote access services by users. [Table 10-1](#) describes all AAA-related logs.

In the web interface, you can enable, configure, and view AAA-related logs, if you have the appropriate permissions.

Table 10-1 AAA-Related Log Descriptions

Log	Description
TACACS+ Accounting	<p>Contains:</p> <ul style="list-style-type: none"> • User sessions stop and start times • AAA client messages with username • Caller line identification (CLID) • Session duration
TACACS+ Administration	<p>Lists configuration commands entered on a AAA client by using TACACS+ (Cisco IOS). Particularly if you use ACS to perform command authorization, we recommend that you use this log.</p> <p>Note To use the TACACS+ Administration log, you must configure TACACS+ AAA clients to perform command accounting with ACS. The following line must appear in the access server or router configuration file:</p> <pre>aaa accounting commands start-stop tacacs+</pre>
RADIUS Accounting	<p>Contains:</p> <ul style="list-style-type: none"> • User sessions stop and start times • AAA client messages with username • Caller line identification information • Session duration <p>You can configure ACS to include accounting for Voice-over-IP (VoIP) in the RADIUS Accounting log, in a separate VoIP accounting log, or in both places.</p>
VoIP Accounting	<p>Contains:</p> <ul style="list-style-type: none"> • VoIP session stop and start times • AAA client messages with username • CLID information • VoIP session duration • cisco-av-pair attribute information <p>You can configure ACS to include accounting for VoIP in this separate VoIP accounting log, in the RADIUS Accounting log, or in both places.</p>
Failed Attempts	<p>Lists authentication and authorization failures with an indication of the cause. For posture-validation requests, this log records the results of any posture validation that returns a posture token other than <code>Healthy</code>.</p> <p>You can use these reports to find out who disabled the account if a given number of failed attempts has been enabled under the expiration information. This can also provide some insight into intrusion attempts and is a valuable tool for troubleshooting.</p>
Passed Authentications	<p>Lists successful authentication requests. This log does not depend on accounting packets from your AAA clients, so it is available; even if your AAA clients do not support RADIUS accounting or if you have disabled accounting on your AAA clients. For posture-validation requests, this log records the results of all posture-validation requests resulting in an SPT.</p>

Logging Attributes

Information is logged as a set of logging attributes. These attributes can be:

- Cisco generic.
- RADIUS generic—See [Appendix B, “RADIUS Attributes”](#) for information about these attributes.
- TACACS generic—See [Appendix A, “TACACS+ Attribute-Value Pairs”](#) for information about these attributes.
- ACS specific.— See [Table 10-17](#) for additional Audit Log Attributes specific to ACS.

Among the many attributes that ACS can record in its logs, a few are of special importance. The following list explains the special logging attributes that ACS provides.

- **User Attributes**—These logging attributes appear in the Attributes list for any log configuration page. ACS lists them by using their default names: Real Name, Description, User Field 3, User Field 4, and User Field 5. If you change the name of a user-defined attribute, the default name, rather than the new name, still appears in the Attributes list.

The values that you enter in the corresponding fields in the user account determine the content of these attributes. For more information about user attributes, see [Customizing User Data, page 2-5](#).

- **ExtDB Info**—If the user is authenticated with an external user database, this attribute contains a value that the database returns. In the case of a Windows user database, this attribute contains the name of the domain that authenticated the user.

In entries in the Failed Attempts log, this attribute contains the database that last successfully authenticated the user. It does not list the database that failed the user-authentication attempt.

- **Access Device**—The name of the AAA client that is sending the logging data to ACS.
- **Network Device Group**—The network device group to which the access device (AAA client) belongs.
- **Filter Information**—The result of network access restrictions (NARs) applied to the user, if any. The message in this field indicates whether all applicable NARs permitted the user access, all applicable NARs denied the user access, or more specific information about which NAR denied the user access. If no NARs apply to the user, this logging attribute notes that no NARs were applied.

The Filter Information attribute is available for Passed Authentication and Failed Attempts logs.

- **Device Command Set**—The name of the device command set, if any, that was used to satisfy a command authorization request.

The Device Command Set attribute is available for Failed Attempts logs.

- **Bypass info**—Information about the MAC authentication bypass feature. The message in this field indicates whether the MAC address was found or not found.

The Bypass info attribute is available for Failed Attempts and Passed Authentications logs.

- **Remote Logging Result**—Whether a remote logging service successfully processes a forwarded accounting packet. This attribute is useful for determining which accounting packets, if any, a central logging service did not log. It depends on the receipt of an acknowledgment message from the remote logging service. The acknowledgment message indicates that the remote logging service properly processed the accounting packet according to its configuration. A value of `Remote-logging-successful` indicates that the remote logging service successfully processed the accounting packet. A value of `Remote-logging-failed` indicates that the remote logging service did not process the accounting packet successfully.



Note ACS cannot determine how a remote logging service is configured to process accounting packets that it forwarded. For example, if a remote logging service is configured to discard accounting packets, it discards a forwarded accounting packet and responds to ACS with an acknowledgment message. This message causes ACS to write a value of `Remote-logging-successful` in the Remote Logging Result attribute in the local log that records the account packet.

- **Posture-Validation Logging Attributes:**

- **Application-Posture-Token**—The application posture token (APT) that a particular policy returns during a posture-validation request. This attribute is available only in the Passed Authentications and Failed Attempts logs.
- **System-Posture-Token**—The system posture token (SPT) that a particular policy returns during a posture-validation request. This attribute is available only in the Passed Authentications and Failed Attempts logs.
- **Other Posture-Validation Attributes**—Attributes that a NAC client sends to ACS during a posture-validation request. The attributes are uniquely identified by the vendor name, application name, and attribute name. For example, the `NAI:AV:DAT-Date` attribute is an attribute containing information about the date of the DAT file on the NAC client for the antivirus application by Network Associates, Inc. These attributes are available only in the Passed Authentications and Failed Attempts logs.

You can choose to log posture-validation attributes in the Passed Authentications and Failed Attempts logs. All inbound attributes are available for logging. The only two outbound attributes that you can record in logs are `Application-Posture-Assessment` and `System-Posture-Assessment`.

All posture-validation requests resulting in a system posture token (SPT), also known as a system posture assessment, are logged in the Passed Authentications log. Posture-validation requests resulting in an SPT of anything other than `Healthy` are logged in the Failed Attempts log. For more information about posture tokens, see [Posture Tokens, page 13-3](#).

- **Authen-Failure-Code attribute for HCAP errors:**

When Host Credentials Authentication Protocol (HCAP) fails, the `Authen-Failure-Code` attribute entry in the Failed Attempts report may display one of the following errors:

- `Version failure - Could not communicate with external policy server - wrong HCAP version`
- `Connection failure - Could not open a connection to external policy server`
- `Authentication failure - Could not communicate with external policy server - authentication failure`
- `Timeout error - Could not connect to external policy server - timeout error`
- `Other - Posture Validation Failure on External Policy`

Related Topics

- [Configuring ACS Logs, page 10-22](#)
- [Viewing and Downloading CSV Reports, page 10-31](#)

ACS Audit Logs

Audit logs contain information about the ACS system and activities and, therefore, record system-related events. These logs are useful for troubleshooting or audits. Comma-separated value (CSV) audit logs are always enabled, and you can enable or disable audit logs to other loggers. You cannot configure the audit log content.

Audit logs can display the actual changes administrators made for each user. ACS audit logs list all the attributes that were changed for a given user. For the list of the 95 attributes audit log attributes, see [Audit Log Attributes, page 10-46](#).

[Table 10-2](#) provides information about each audit log.

Table 10-2 **Audit Log Descriptions**

Log	Description and Related Topics
ACS Backup and Restore	Lists dates and times that the ACS system information was backed up and restored, and whether the action was successful. For information about changing the schedule or the location of the backup and restore files, see ACS Backup, page 7-8 and ACS System Restore, page 7-14 .
RDBMS Synchronization	Lists the times the RDBMS database was synchronized and whether the synchronization was manual or scheduled. For information about changing the RDBMS synchronization schedule, see RDBMS Synchronization, page 8-17 .
Database Replication	Lists the times the ACS Internal Database was replicated to the backup server and whether the replication was manual or scheduled. For information about changing the database replication schedule, see ACS Internal Database Replication, page 8-1 .
Administration Audit	Lists actions taken by each system administrator, such as adding users, editing groups, configuring a AAA client, or viewing reports.
User Password Changes	Lists user password changes that users initiate, regardless of which password-change mechanism was used to change the password. Thus, this log contains records of password changes that the ACS Authentication Agent, the User Changeable Password web interface, or the Telnet session made on a network device that is using TACACS+. This log does not list password changes that an administrator makes in the ACS web interface.
ACS Service Monitoring	Lists when ACS services start and stop.
Appliance Administration Audit	Lists administrator activity on the serial console, including logins, logouts, and commands executed.

Related Topics

- [Configuring ACS Logs, page 10-22](#)
- [Viewing and Downloading CSV Reports, page 10-31](#)

ACS Logging Formats and Targets

ACS *loggers* provide logging interfaces to record AAA-related logs and audit logs in different formats, and to different targets. You can use:

- [CSV Logger, page 10-6](#)
- [Syslog Logger, page 10-7](#)
- [ODBC Logger \(ACS for Windows only\), page 10-9](#)
- [Remote Logging for ACS for Windows, page 10-10](#)
- [Remote Logging for ACS SE with ACS Remote Agents, page 10-10](#)

You can configure ACS to log information to more than one logger. For information about configuring logs, see [Configuring ACS Logs, page 10-22](#).

You can configure a *critical logger* for accounting logs to guarantee delivery of these logs to at least one logger. For more information, see [Configuring Critical Loggers, page 10-23](#).

CSV Logger

The CSV logger records data for logging attributes in columns separated by commas (.). You can import this format into a variety of third-party applications, such as Microsoft Excel or Microsoft Access. After you import data from a CSV file into such applications, you can prepare charts or perform queries, such as determining how many hours a user was logged in to the network during a given period. For information about how to use a CSV file in a third-party application such as Microsoft Excel, see the documentation from the third-party vendor.



Tip

Using a CSV file may not work well for every language or locale; for example, when imported into programs such as Word or Excel. You may need to replace the commas (,) with semicolons (;), if necessary.

You can access the CSV files on the ACS server hard drive or you can download the CSV file from the web interface.

CSV Log File Locations

By default, ACS keeps log files in directories that are unique to the log. You can configure the log file location of CSV logs. The default directories for all logs reside in `sysdrive:\Program Files\CiscoSecure ACS vx.x`. For the subdirectory of this location for a specific log, see [Table 10-3](#).

Table 10-3 Default CSV Log File Locations

Log	Default Location
TACACS+ Accounting	<i>Logs\TACACS+Accounting</i>
CSV TACACS+ Administration	<i>Logs\TACACS+Administration</i>
CSV RADIUS Accounting	<i>Logs\RADIUS Accounting</i>
CSV VoIP Accounting	<i>Logs\VoIP Accounting</i>
CSV Failed Attempts	<i>Logs\Failed Attempts</i>
Passed Authentications	<i>Logs\Passed Authentications</i>
ACS Backup and Restore	<i>Logs\Backup and Restore</i>
RDBMS Synchronization	<i>Logs\DbSync</i>
RDBMS Synchronization	<i>Logs\DBReplicate</i>
Administration Audit	<i>Logs\AdminAudit</i>

Table 10-3 Default CSV Log File Locations (continued)

Log	Default Location
User Password Changes	<i>CSAuth\PasswordLogs</i>
ACS Active Service Monitoring	<i>Logs\ServiceMonitoring</i>

CSV Log Size and Retention

For each CSV log, ACS writes a separate log file. When a log file size reaches 10 MB, ACS starts a new log file. ACS retains the seven most recent log files for each CSV log.

Related Topics

- [Configuring a CSV Log, page 10-24](#)
- [Viewing and Downloading CSV Reports, page 10-31](#)

Syslog Logger

The ACS syslog logger supports the standard syslog format. You can send log data for any report to up to two syslog servers. You configure the syslog servers for each report individually. You can use syslog to centralize the data from multiple ACSs.

ACS syslog logging follows the standard syslog protocol (RFC 3164). Messages are sent connectionless to syslog servers by using an unsecured UDP port without data encryption.

**Note**

The syslog protocol contains no mechanism to ensure delivery, and since the underlying transport is UDP, message delivery is not guaranteed.

Syslog Message Format

The format of the ACS syslog message content is:

```
<n> mmm dd hh:mm:ss XX:XX:XX:XX TAG msg_id total_seg seg# A1=V1
```

where:

- **<n>**—The Priority value of the message; it is a combination of the facility and severity of the syslog message. The Priority value is calculated according to RFC 3164, by first multiplying the *facility* value by 8 and then adding the *severity* value.

ACS syslog messages use the following facility values:

- 4 (Auth)—Security and authorization messages. This value is used for all AAA-related messages (failed attempts, passed attempts, accounting, and so on).
- 13 (System3)—Log audit. This value is used for all other ACS report messages.

All ACS syslog messages use a severity value of 6 (Info).

For example, if the facility value is 13 and the severity value is 6, the Priority value is 110 ((8 x 13) + 6). The Priority value appears according to the syslog server setup, and might appear as one of:

- **System3.Info**
- **<110>**



Note You cannot configure the format of the syslog facility and severity on ACS.

- **mmm dd hh:mm:ss**—Date and time of the message.
- **XX:XX:XX:XX**—IP Address of the machine generating this syslog message.
- **TAG**—A value representing the ACS report name:
 - CisACS_01_PassedAuth—Cisco ACS Passed Authentications
 - CisACS_02_FailedAuth—Cisco ACS Failed Attempts
 - CisACS_03_RADIUSAcc—Cisco ACS RADIUS Accounting
 - CisACS_04_TACACSAdmin—Cisco ACS TACACS+ Accounting
 - CisACS_05_TACACSAdmin—Cisco ACS TACACS+ Administration
 - CisACS_06_VoIPAcc—Cisco ACS VoIP Accounting
 - CisACS_11_BackRestore—Cisco ACS Backup and Restore log messages
 - CisACS_12_Replication—Cisco ACS Database Replication log messages
 - CisACS_13_AdminAudit —Cisco ACS Administration Audit log messages
 - CisACS_14_PassChanges—Cisco ACS User Password Changes log messages
 - CisACS_15_ServiceMon—Cisco ACS Service Monitoring log messages
 - CisACS_16_RDBMSSync—Cisco ACS RDBMS Synchronization Audit log messages
 - CisACS_17_ApplAdmin—Cisco ACS Appliance Administration Audit log messages
- **msg_id**—Unique message ID. All segments of one message share the same message ID.
- **total_seg**—Total number of segments in this message. For more details, see [Syslog Message Length Limitations, page 10-8](#).
- **seg#**—Segment sequence number within this message segmentation. For more details, see [Syslog Message Length Limitations, page 10-8](#).
- **A1=V1**—Attribute value pairs delimited by a comma (,) for Cisco ACS log messages and the message itself.

Syslog Message Length Limitations

You can configure the maximum length for ACS syslog messages. We recommend a maximum message length of 1,024 bytes for messages to a standard syslog server; however, the configuration should correspond to the target server specifications.

When an ACS message, including header and data, exceeds the syslog standard length limitation or target length limitation, the message content is split into several segments:

- The message is split between attribute value pairs keeping an attribute value pair complete within the segment, if possible. Each segment ends with the comma (,) delimiter; the next segment starts with the header and then the next attribute value pair.
- All segments of the same message have the same header. The **<msg_id>** and **<total_seg>** values are shared between all segments. The **<seg#>** is set according to the sequence of the segments.

For information about enabling and configuring syslog logs, see [Configuring Syslog Logging, page 10-24](#).

Related Topics

[Configuring Syslog Logging, page 10-24](#)

ODBC Logger (ACS for Windows only)

These topics describe ODBC logging and what to do before you configure ODBC logs in ACS:

- [About ODBC Logging, page 10-9](#)
- [Preparing for ODBC Logging, page 10-9](#)

About ODBC Logging

You can use Open DataBase Connectivity (ODBC) loggers to log directly in an ODBC-compliant relational database, where the logs are stored in tables, one table per log. After the data is exported to the relational database, you can use the data however you need. For more information about querying the data in your relational database, refer to the documentation from the relational database vendor.

Preparing for ODBC Logging

Before you can configure ODBC logs in ACS, you must:

1. Set up the relational database to which you want to export logging data. For more information, refer to your relational database documentation.
2. On the computer that is running ACS, set up a system data source name (DSN) for ACS to communicate with the relational database that will store your logging data.

To set up a system DSN for use with ODBC logging:

-
- Step 1** In the Windows Control Panel, double-click **ODBC Data Sources**.
- Step 2** In the ODBC Data Source Administrator page, click the **System DSN** tab.
- Step 3** Click **Add**.
- Step 4** Select the driver to use with your new DSN, and then click **Finish**.
- A dialog box displays fields requiring information that is specific to the selected ODBC driver.
- Step 5** Type a descriptive name for the DSN in the Data Source Name box.
- Step 6** Complete the other fields that are required by the selected ODBC driver. These fields may include information such as the IP address of the server on which the ODBC-compliant relational database runs.
- Step 7** Click **OK**.
- Step 8** Close the ODBC window and Windows Control Panel.

The System DSN that ACS uses for communicating with the relational database is created on the computer running ACS. The name you assigned to the DSN appears in the Data Source list on each ODBC log configuration page.

Related Topics

[Configuring an ODBC Log \(ACS for Windows only\), page 10-25](#)

Remote Logging for ACS for Windows

You can use Remote Loggers to centralize AAA-related and audit logs that multiple ACSs generate. You can configure each ACS to point to one or more ACSs to use as a remote logging server. The remote logging ACS still performs AAA functions, but it also is the repository for the logs that it receives.

The Remote Logging feature enables ACS to send data directly to the CSLog service on the remote logging server, where the data is written to the logs. The remote logging server generates the logs in the formats that it is configured to use regardless of the local logging configuration on the ACSs that are sending the data.

ACS listens on TCP port 2001 for remote logging communication. A 128-bit proprietary algorithm encrypts remote logging data.



Note

The Remote Logging feature does not affect the forwarding of data for proxied authentication requests. ACS only applies Remote Logging settings to data for sessions that the proxy authenticates when data for sessions that the proxy authenticates is logged locally. For more information about proxied authentication requests and data for sessions that the proxy authenticates, see [Configuring Proxy Distribution Tables, page 3-28](#).



Note

Do not configure bidirectional remote logging for ACS. For example, you should not have ACS_SERVER_1 refer to ACS_SERVER_2 as a remote logger, and then have ACS_SERVER_2 refer to ACS_SERVER_1 as a remote logger.

Related Topics

[Configuring and Enabling Remote Logging \(ACS for Windows only\), page 10-26](#)

Remote Logging for ACS SE with ACS Remote Agents

The Remote Logging feature enables ACS to send data to one or more ACS Remote Agents. The remote agent runs on a computer on your network. It writes the data that ACS sends to it into CSV files. You can configure many ACS SEs to point to a single remote agent, thus making the computer that runs the remote agent a central logging server.

For more information about installing and configuring an ACS Remote Agent, see *Installation and Configuration Guide for Cisco Secure ACS Remote Agents Release 4.2*.



Note

The Remote Logging feature does not affect the forwarding of data for proxied authentication requests. ACS only applies Remote Logging settings to data for sessions authenticated by proxy when accounting data for sessions authenticated by proxy is logged locally. For more information about proxied authentication requests and data for sessions authenticated by proxy, see [Configuring Proxy Distribution Tables, page 3-28](#).

Regardless of how many ACS SEs send their accounting data to the remote agent server, the remote agent receives its configuration from a single ACS SE. That ACS is the configuration provider for the remote agent. You determine:

- What logs the remote agent keeps.
- What data is recorded for each log kept.
- How the remote agent manages the log files.

Related Topics

[Configuring Logging to Remote Agents \(ACS SE only\), page 10-27](#)

Dynamic Administration Reports

These reports show the status of user accounts when you access them in the ACS web interface. They are available only in the web interface, are always enabled, and require no configuration.

[Table 10-4](#) contains descriptions of ACS administration reports.

Table 10-4 **Dynamic Administration Report Descriptions**

Report	Description and Related Topics
Logged-In Users	<p>Lists all users receiving services for a single AAA client or all AAA clients. You can delete logged-in users from specific AAA clients or from all AAA clients.</p> <p>Users accessing the network with Cisco Aironet equipment appear on the list for the access point that they are currently associated with, provided that the firmware image on the Cisco Aironet Access Point supports sending the RADIUS Service-Type attribute for rekey authentications.</p> <p>On a computer configured to perform machine authentication, machine authentication occurs when the computer starts. When a computer is started and before a user logs in on that computer, the computer appears on the Logged-In Users List in the Reports and Activity section of the ACS web interface. Once user authentication begins, the computer no longer appears on the Logged-In Users List. For more information about machine authentication, see EAP and Windows Authentication, page 12-10.</p> <p>Note To use the logged-in user list feature, you must configure AAA clients to perform authentication and accounting by using the same protocol—TACACS+ or RADIUS.</p> <p>For information about viewing the Logged-in User report in the web interface and deleting logged-in users, see Viewing the Logged-in Users Report, page 10-34.</p>
Disabled Accounts	<p>Lists all user accounts that are disabled and the reason they were disabled. They might have been manually disabled or disabled automatically based on the aging information defined under User Setup.</p> <p>For information about viewing the Disabled Accounts report in the web interface, see Viewing the Disabled Accounts Report, page 10-35.</p>
Appliance Status	<p>Lists information about resource utilization on the ACS SE. Also displays information about the IP configuration for the ACS SE and the MAC address of its network interface card.</p> <p>For information about viewing the Appliance Status report in the web interface, see Viewing the Appliance Status Report, page 10-35.</p>

Related Topics

- [Viewing Dynamic Administration Reports, page 10-34](#)

Entitlement Reports

These reports provide information about administrator privileges and user mappings to groups. All these reports can be downloaded as text files in CSV format. You can display the reports for individual administrators in the ACS web interface. Entitlement reports are always enabled and require no configuration.

[Table 10-5](#) contains descriptions of ACS entitlement reports.

Table 10-5 Entitlement Report Descriptions

Report	Description and Related Topics
User Entitlements	The user entitlement report provides mappings of users to group. This report lists all users with their group, Network Access Profile (NAP) if relevant, and the mapping type (static or dynamic). You can download this report in CSV format; however, you cannot display it in the ACS web interface because of its potential size.
Administrator Entitlements	The two types of Administrator Entitlement Reports are: <ul style="list-style-type: none"> • Privilege report for all administrators—Lists the privileges of each administrator. You can download this report in CSV format; however, you cannot display it in the ACS web interface because of its potential size. • Privilege reports for individual administrators—Lists privileges for the selected administrator. You can display reports for individual administrators in the ACS web interface, and you can download them as text files in CSV format.

Related Topics

- [Viewing and Downloading Entitlement Reports, page 10-36](#)

Service Logs

Service logs are considered diagnostic logs, which you use for troubleshooting or debugging purposes only. These logs are not intended for general use by ACS administrators; instead, they are mainly sources of information for Cisco support personnel. Service logs contain a record of all ACS service actions and activities. When service logging is enabled, each service generates a log whenever the service is running, regardless of whether you are using the service. For example, RADIUS service logs are created even if you are not using the RADIUS protocol in your network. For more information about ACS services, see [Chapter 1, “Overview.”](#)

Service log files reside in the `\Logs` subdirectory of the applicable service directory. For example, the following is the default directory for the ACS authentication service:

```
c:\Program Files\CiscoSecure ACS vx.x\CSAuth\Logs
```

Services Logged

ACS generates logs for the following services:

- CSAdmin
- CSAuth
- CSDBSync
- CSLog
- CSMon
- CSRADIUS
- CSTacacs

The most recent debug log is named:

```
SERVICE.log
```

where *SERVICE* is the name that represents the applicable service, for example *auth* represents the **CSAuth** service.

Older debug logs are named with the year, month, and date on which they were created. For example, a file that was created on July 13, 1999, would be named:

SERVICE 1999-07-13.log

where *SERVICE* is the name that represents the applicable service.

If you selected the Day/Month/Year format, the file would be named:

SERVICE 13-07-1999.log

For information about changing the date format, see [Date and Time Format Control](#), page 7-3.

Related Topics

[Configuring Service Logs](#), page 10-29

Adding Session IDs to the CSAuth Diagnostic Log

ACS supports a session ID parameter for the **CSAuth** diagnostic log. The **CSAuth** diagnostic log tracks each active authentication session by using a session data structure. The ACS services refer to these structures by session ID. You can use a unique session ID to differentiate log threads in the **CSAuth** diagnostic logs.

[Example 10-1](#) shows the session ID **1000** is processed by two different threads (2560, 2548) in the network model thread. You can filter the logs by session ID to restrict the output for each session.

Example 10-1 CSAuth Diagnostic Log with session ID

```
AUTH 09/08/2006 18:29:57 I 5081 2560 1000 Start RQ1040, client 1 (127.0.0.1)
AUTH 09/08/2006 18:30:13 I 5094 2548 Worker 1 processing message 17.
AUTH 09/08/2006 18:30:14 I 0991 2368 0000 pvNASMonitorThreadMain: start NM
update ...
AUTH 09/08/2006 18:30:14 I 1006 2368 0000 pvNASMonitorThreadMain: commit NM
update ...
AUTH 09/08/2006 18:30:14 I 5081 2560 1000 Done RQ1040, client 1, status 0
AUTH 09/08/2006 18:30:14 I 1011 2368 0000 pvNASMonitorThreadMain: succeeded
to commit NM update
AUTH 09/08/2006 18:30:28 I 5081 2548 1000 Start RQ1012, client 2 (127.0.0.1)
AUTH 09/08/2006 18:30:28 I 5081 2548 1000 Done RQ1012, client 2, status 0
```



Note

The additional session ID field in the ACS diagnostic log involves minimal overhead: eight bytes per line for each authentication session.

You use the same session ID for different authentication sessions. This means that the same session ID can appear in the diagnostic logs for more than one session. Cisco recommends that you use unique session IDs for each authentication session. Session IDs are maintained up to a limit of 120 seconds.

Description of Error Codes in the CSAuth Diagnostic Log

CSAuth diagnostic logs display a description of client requests and responses. Previous versions of ACS used a numeric code for client requests and responses. The description is useful for locating client requests and responses in the **CSAuth** diagnostic logs.

Two examples of **CSAuth** diagnostic log entries follow. [Example 10-2](#) represents an entry from previous versions of the **CSAuth** diagnostic log. [Example 10-3](#) represents how this entry for the **CSAuth** diagnostic log appears in this release.

[Example 10-3](#) shows that in the **CSAuth** diagnostic log:

- UDB_AUTHENTICATE_USER replaces the RQ1026 request code in the first example.
- UDB_CHALLENGE_REQUIRED replaces the 2046 status code in the first example.

Example 10-2 CSAuth Diagnostic Log Entry

```
AUTH 09/11/2006 09:55:27 I 5081 2512 Done RQ1026, client 50, status -2046
```

Example 10-3 CSAuth Diagnostic Log Entry (with Descriptive text)

```
AUTH 09/11/2006 09:55:27 I 5081 2512 Done UDB_AUTHENTICATE_USER, client 50, status UDB_CHALLENGE_REQUIRED
```

Descriptive Request Text in the CSAuth Diagnostic Logs

[Table 10-6](#) and [Table 10-7](#) list the descriptive text for requests and status that appear in the **CSAuth** diagnostic logs.

[Table 10-6](#) lists the descriptive text in the **CSAuth** diagnostic logs and the corresponding request code.

Table 10-6 Descriptive Request Text and Request Code

Request Text	Request Code
UDB_BASE_CMD	1000
UDB_HAIL	1001
UDB_OPEN	1002
UDB_CLOSE	1003
UDB_GOODBYE	1004
UDB_PING	1005
UDB_REFRESH	1006
UDB_REFRESH_EX	1007
UDB_RESET_HOST_CACHE	1008
UDB_USER_ADD	1010
UDB_USER_REMOVE	1011
UDB_VALID_USER	1012
UDB_USER_ENUM_BY_GROUP	1013
UDB_CHANGE_PASSWORD	1014
UDB_SET_PASS_STATUS	1015
UDB_GET_PASS_STATUS	1016
UDB_USER_ENUM	1017
UDB_USER_GET_INFO	1018
UDB_USER_PAP_CHECK	1019

Table 10-6 Descriptive Request Text and Request Code (continued)

Request Text	Request Code
UDB_USER_PROF_ASSIGN	1020
UDB_USER_PROF_COUNT	1021
UDB_USER_PROF_GET	1022
UDB_USER_CHAP_CHECK	1023
UDB_USER_CHECK_EXPIRY	1024
UDB_USER_SET_INFO	1025
UDB_AUTHENTICATE_USER	1026
UDB_SEND_RESPONSE	1027
UDB_SET_PASSWORD	1028
UDB_USER_LOCN_CHECK	1029
UDB_SET_VALUE	1030
UDB_GET_VALUE	1031
UDB_GET_NEXT_VALUE	1032
UDB_DEL_VALUE	1033
UDB_FIND_VALUE	1034
UDB_GET_VALUE_BY_NAME	1035
UDB_LOG	1040
UDB_SET_APPDATA	1041
UDB_GET_APPDATA	1042
UDB_DEL_DB	1043
UDB_AVERT_LOG	1044
UDB_DIR_CREATE	1050
UDB_FILE_CREATE	1051
UDB_FILE_WRITE	1052
UDB_FILE_READ	1053
UDB_FILE_CLOSE	1054
UDB_FILE_EXISTS	1055
UDB_FILE_APPEND	1056
UDB_FILE_SET_PTR	1057
UDB_USER_LIST_ADD	1070
UDB_USER_LIST_DEL	1071
UDB_USER_LIST_GET	1072
UDB_USER_LIST_COUNT	1073
UDB_USER_LIST_UPDATE	1074
UDB_USER_ALIAS_SET	1080
UDB_USER_ALIAS_DEL	1081

Table 10-6 Descriptive Request Text and Request Code (continued)

Request Text	Request Code
UDB_USER_ALIAS_VALID	1082
UDB_START_TRANSACTION	1090
UDB_END_TRANSACTION	1091
UDB_KICK_SYNC_TX	1092
UDB_KICK_SYNC_RX	1093
UDB_EXCHANGE_SYNC_INFO	1094
UDB_AQUIRE_IP_ADDRESS	1095
UDB_VALIDATE_PASSWORD	1096
UDB_EXTRACT_AGING_DATA	1097
UDB_AUTH_FAILED	1098
UDB_RESET_USER_PASSWORD_AGING_DATA	1099
UDB_GET_AGING_INFO	1100
UDB_DO_BACKUP_NOW	1101
UDB_AQUIRE_CALLBACK	1102
UDB_GET_AGING_LIMIT	1103
UDB_PURGE_NAS	1104
UDB_SEND_FAKE_STOPS	1105
UDB_SERVICE_CONTROL	1106
UDB_RESET_GROUP	1107
UDB_SET_ENABLE_PASS_STATUS	1108
UDB_UPDATE_AGING_POLICY	1109
UDB_ADD_HOST	1110
UDB_DEL_HOST	1111
UDB_GET_HOST	1112
UDB_UPDATE_HOST	1113
UDB_ADD_PROXY	1114
UDB_DEL_PROXY	1115
UDB_ADD_PROXY_TARGET	1116
UDB_ADD_NDG	1117
UDB_DEL_NDG	1118
UDB_GET_NDG_ID	1119
UDB_SET_USER_FEATURE_FLAG	1120
UDB_GET_USER_COUNTER	1121
UDB_RESET_USER_COUNTER	1122
UDB_RESET_GROUP_USERS_COUNTER	1123
UDB_GET_FIRST_QUOTA_TYPE	1124

Table 10-6 Descriptive Request Text and Request Code (continued)

Request Text	Request Code
UDB_GET_NEXT_QUOTA_TYPE	1125
UDB_SET_QUOTA	1126
UDB_HAS_USER_QUOTA_EXHAUSTED	1127
UDB_SHARED_PROFILE	1128
UDB_ADD_UDV	1140
UDB_DEL_UDV	1141
UDB_GET_VID_FROM_IETF	1142
UDB_ADD_UDV_VSA	1143
UDB_ADD_UDV_VSA_ENUM	1144
UDB_ADD_UDV_VSA_PROFILE	1145
UDB_SET_REP_DIRTY_FLAG	1150
UDB_USER_COMMIT_NOW	1151
UDB_POLICY_CREATE_CONTEXT	1152
UDB_USER_REMOVE_DYNAMIC	1153

Table 10-7 lists the descriptive text in the **CSAuth** diagnostic logs and the corresponding status code.

Table 10-7 Descriptive Status Text and Request Code

Status Description	Status Code
UDB_BASE_ERR	1000
UDB_DB_NOT_OPEN	1001
UDB_INVALID_ENTRY	1002
UDB_CANT_CREATE_MAP	1003
UDB_CANT_CREATE_VIEW	1004
UDB_CANT_OPEN_INDEX	1005
UDB_DB_IS_OPEN	1006
UDB_SIZE_MISMATCH	1007
UDB_CANT_OPEN_FILE	1008
UDB_CRC_FAILED	1009
UDB_CANT_INIT_INDEX	1010
UDB_INVALID_DATA	2011
UDB_CANT_GROW_FILE	1012
UDB_USER_INVALID	2013
UDB_DUPLICATE_NAME	1014
UDB_INVALID_PASSWORD	2015
UDB_IPC_DATA_INVALID	1016
UDB_FEATURE_NOT_READY	1017

Table 10-7 Descriptive Status Text and Request Code (continued)

Status Description	Status Code
UDB_SERVER_BUSY	1018
UDB_REGISTRY_READ_FAIL	1019
UDB_UNKNOWN_VARIABLE	2020
UDB_NO_FILE_HANDLES	1021
UDB_DIR_CREATE_FAILED	1022
UDB_FILE_WRITE_FAILED	1023
UDB_FILE_READ_FAILED	1024
UDB_INVALID_DIR_NAME	1025
UDB_INVALID_FILE_NAME	1026
UDB_MALLOC_FAIL	1027
UDB_INVALID_HANDLE	1028
UDB_USER_NOT_OWNER	1029
UDB_CANT_REBUILD_INDEX	1030
UDB_CANT_REMOVE_OLD_DB	1031
UDB_USER_REMOVED	2032
UDB_NO_VARIABLE	1033
UDB_PASSWORD_DISABLED	2034
UDB_FILE_SET_PTR_FAILED	1035
UDB_USER_LICENCE_LIMIT	1036
UDB_APP_NOT_LICENSED	1037
UDB_BAD_SECRET	1038
UDB_DB_VERSION_MISMATCH	1039
UDB_DIR_REMOVE_FAILED	1040
UDB_CANT_ASSIGN_PROFILE	1041
UDB_LOGGER_OFFLINE	1042
UDB_CANT_ACCESS_USERLIST	1043
UDB_SESSION_COUNT_EXCEEDED	2044
UDB_PASSWORD_REQUIRED	2045
UDB_CHALLENGE_REQUIRED	2046
UDB_NO_SESSION	1047
UDB_INTERNAL_ERROR	1048
UDB_BAD_TODDOW	2049
UDB_CANT_LOCK_RECORD	1050
UDB_NT_DIALIN_REQUIRED	2051
UDB_NT_PW_WRONG	2052
UDB_NT_AC_RESTRICTED	2053

Table 10-7 Descriptive Status Text and Request Code (continued)

Status Description	Status Code
UDB_NT_TOD_DOW	2054
UDB_NT_PW_EXPIRED	2055
UDB_NT_AC_DISABLED	2056
UDB_NT_BAD_WORKSTATION	2057
UDB_NT_UNKNOWN_ERR	1058
UDB_NT_PASS_CHANGE	2059
UDB_NT_NO_DOMAIN	2060
UDB_NT_AC_LOCKED	2061
UDB_NT_NO_BROWSER	2062
UDB_INVALID_CHAP_PW	2063
UDB_INVALID_ARAP_PW	2064
UDB_INVALID_TOKEN_PW	2065
UDB_INVALID_UNIX_PW	2066
UDB_TOKEN_SERVER_DOWN	1067
UDB_USER_CLI_FILTERED	2068
UDB_NO_SENDAUTH_PW	1069
UDB_NO_TOKENSRV	1070
UDB_NT_NO_LOGON_NOT_GRANTED	2071
UDB_CANT_START_TRANSACTION	1072
UDB_VARDB_NOT_OPEN	1073
UDB_NOT_IN_CACHE	1074
UDB_CANT_OPEN_ODBC_DB	1075
UDB_DLL_MISMATCH	1076
UDB_NOT_INSTALLED	1077
UDB_CHAP_ENFORCED	2078
UDB_ACCESS_DENIED	2079
UDB_REPLICATION_DENIED	1080
UDB_FAILED_TO_AQUIRE_IP_ADDR	1081
UDB_PASSWORD_DEAD	2082
UDB_PASSWORD_STATE_NOT_ACCESSIBLE	1083
UDB_PASSWORD_AGE_CHECK_FAILED	1084
UDB_NEW_PASSWORD_NOT_GOOD	2085
UDB_FAILED_TO_EXTRACT_DATA	1086
UDB_EXTERN_DB_ERROR	2087
UDB_BACKUP_FAILED_TO_START	1088
UDB_FAILED_TO_AQUIRE_CALLBACK	1089

Table 10-7 Descriptive Status Text and Request Code (continued)

Status Description	Status Code
UDB_FAILED_TO_PERFORM_SERVICE_OP	1090
UDB_TIME_OUT_WAITING_TO_START_AUTH	1091
UDB_AUTH_NOT_SUPPORTED_BY_EXT_DB	2092
UDB_CACHED_TOKEN_REJECTED	2093
UDB_TOKEN_PIN_CHANGED	2094
UDB_INVALID_MSCHAP_PW	2095
UDB_INVALID_EXT_CHAP_PW	2096
UDB_INVALID_EXT_ARAP_PW	2097
UDB_INVALID_EXT_MSCHAP_PW	2098
UDB_INVALID_EXT_USER	2099
UDB_NT_AC_EXPIRED	2100
UDB_AUTH_DENIED_DUE_TO_VOIP	2101
UDB_MALFORMED_USERNAME	2102
UDB_CANT_OPEN_HOST_DB	1103
UDB_CANT_OPEN_PROXY_DB	1104
UDB_CANT_OPEN_NDG_DB	1105
UDB_HOST_DB_FAILURE	1106
UDB_PROXY_DB_FAILURE	1107
UDB_NDG_DB_FAILURE	1108
UDB_INVALID_COUNTER_TYPE	1109
UDB_EXTERN_DB_TRANSIENT_ERROR	1110
UDB_INVALID_QUOTA_INDEX	1111
UDB_USAGE_QUOTA_EXCEEDED	2112
UDB_NT_CHANGE_PASS_FAILED	2113
UDB_CANT_LOAD_DLL	1114
UDB_EXTN_DLL_REJECTED	2115
UDB_INVALID_EXT_EAP_PW	2116
UDB_EAP_METHOD_NOT_SUPPORTED	2117
UDB_EAP_TLS_PASS_HS_USER_NOT_FOUND	2118
UDB_EAP_NO_MATCH_NAME_IN_CERT	2119
UDB_EAP_TLS_HANDSHAKE_FAILED	2120
UDB_EAP_IGNORE	2121
UDB_SUPPLIER_NOT_CONFIGURED	2122
UDB_UDV_CONFIG_ERROR	1123
UDB_USER_FOUND	2124
UDB_USER_NOT_FOUND	2125

Table 10-7 Descriptive Status Text and Request Code (continued)

Status Description	Status Code
UDB_EAP_FAILED	1126
UDB_MISSING_MPPE_DATA	2127
UDB_EAP_MACHINE_AUTH_DISABLED	2128
UDB_NT_NO_REMOTE_AGENT	2129
UDB_EAP_FAST_PAC_PROVISIONING	2130
UDB_EAP_FAST_USER_AND_IID_NOT_MATCH	2131
UDB_EAP_FAST_PAC_INVALID	2132
UDB_EAP_FAST_INBAND_NOT_ALLOWED	2133
UDB_EAP_FAST_INVALID_MASTER_KEY	2134
UDB_GROUP_DISABLED	2135
UDB_AVERT_NO_MAPPING	2136
UDB_EAP_PASSWORD_CHANGE_DISABLED	2137
UDB_AVERT_PROCEED_TO_UUP	2138
UDB_AVERT_LOCAL_POLICY_FAILED	2139
UDB_AVERT_EX_POLICY_FAILED	2140
UDB_AVERT_GENERAL_FAILURE	2141
UDB_ACCESS_DENIED_FAST_REC_NO_USER	2142
UDB_ACCESS_DENIED_MAR_RESTRICTION	2143
UDB_AVERT_UNKNOWN_ATTRIBUTE	2144
UDB_AUTH_PROTOCOL_NOT_ALLOWED	2145
UDB_EAP_FAST_ANON_INBAND_NOT_ALLOWED	2146
UDB_AUDIT_BAD_RESPONSE	2147
UDB_AUDIT_TOO_MANY_ROUND_TRIPS	2148
UDB_POSTURE_VALIDATION_FAILED	2149
UDB_MAC_AUTH_BYPASS_NOT_ALLOWED	2150
UDB_ACCESS_DENIED_NO_SERVICE	2151
UDB_AUTHORIZATION_REJECT	2152
UDB_PV_FAILED_NO_SERVICE	2153
UDB_LOCAL_USER_HAS_EXT_DB_AUTH	2154
UDB_SERVICE_EXT_DB_NOT_ALLOWED	2155
UDB_NT_LOGON_FAILURE	2156
UDB_MAC_AUTH_BYPASS_GROUP_DISABLE	2157
UDB_BADLY_FORMED_DACL_RQ	2158
UDB_INTERNAL_DACL_ERROR	2159
UDB_DACL_ASSIGN_ERROR	2160
UDB_INTERNAL_RAC_ERROR	2161

Table 10-7 Descriptive Status Text and Request Code (continued)

Status Description	Status Code
UDB_RAC_MISSING_ERROR	2162
UDB_AUDIT_RECIEVED_ERROR	2163
UDB_AUDIT_SERVER_UNREACHEABLE	2164
UDB_AUDIT_PARSE_ERROR	2165
UDB_EXT_POLICY_VER_ERROR	2166
UDB_EXT_POLICY_CONN_ERROR	2167
UDB_EXT_POLICY_AUTH_ERROR	2168
UDB_EXT_POLICY_TIMEOUT_ERROR	2169
UDB_ERR_PROFILE_TOO_BIG	1170
UDB_EXT_POLICY_CONN_ERROR_CA_UNKNOWN	2171
UDB_BASE_WARN	1000
UDB_ALREADY_OPEN	1001
UDB_PASSWORD_EXPIRED	1002
UDB_UNKNOWN_PASS_STATUS	1003
UDB_UDB_VALUE_OVERWRITE	1004
UDB_BUFFER_TOO_SMALL	1005
UDB_SIZE_SMALLER	1006
UDB_USER_NOT_ALIAS	1007
UDB_NO_MORE_QUOTA_TYPES	1008

Line Numbers in Diagnostic Logs

The ACS diagnostic log files contain the correct line number of the source code that generated the error. In previous versions of ACS, the **dzlog** function contained the hard-coded source code line number, which was populated to the ACS diagnostic log.

Generic EAP Code Debug Messages

ACS reports all EAP debug messages to the **CSAuth** diagnostic log.

Configuring ACS Logs

You can enable and configure logging for individual logs. ACS can log information to multiple loggers simultaneously.

The starting point for enabling and configuring service logs is the Service Control page, which you access by choosing **System Configuration > Service Control**. The starting point for enabling and configuring all other logs and loggers is the Logging Configuration page, which you access by choosing **System Configuration > Logging**. The Logging Configuration page also displays which ACS logs are currently enabled.

These topics describe how to configure and enable ACS logs:

- [Configuring Critical Loggers](#), page 10-23
- [Configuring a CSV Log](#), page 10-24
- [Configuring Syslog Logging](#), page 10-24
- [Configuring an ODBC Log \(ACS for Windows only\)](#), page 10-25
- [Configuring and Enabling Remote Logging \(ACS for Windows only\)](#), page 10-26
- [Configuring Logging to Remote Agents \(ACS SE only\)](#), page 10-27
- [Configuring Service Logs](#), page 10-29
- [Providing Service Logs for Customer Support](#), page 10-29

Configuring Critical Loggers

You can configure a critical logger for accounting logs to guarantee delivery of these logs to at least one logger.

When you configure a critical logger, the reply that ACS sends to an authenticating device depends on the success or failure of logging the relevant message to the critical logger only. ACS sends the message to other loggers off-stream, (best effort but not guaranteed), which does not affect the authentication result. (For all other AAA-related reports, such as failed attempts, passed authentications and TACACS+ administration, logging is done off-stream, and does not affect the authentication attempt result.)

You can configure a different critical logger for each accounting report; the default critical logger for each report is the local CSV log. If you do not select a critical logger, delivery of accounting messages is not guaranteed.

**Note**

We do not recommend that you configure a syslog logger as a critical logger; because, according to syslog standards, syslog message logging is not guaranteed.

To configure a critical logger for accounting reports:

-
- Step 1** In the navigation bar, click **System Configuration**.
 - Step 2** Click **Logging**.
The Logging Configuration page appears.
 - Step 3** Click **Critical Loggers Configuration**.
The Critical Loggers Configuration page appears.
 - Step 4** Select a critical logger for each accounting report. For more information about the options for selecting critical loggers, see [Critical Loggers Configuration Page](#), page 10-38.
 - Step 5** Click **Submit**.
ACS implements the specified critical loggers configuration.
-

**Note**

If a critical logger is chosen but the specified log is disabled, ACS will not implement critical logging for the specific report.

Configuring a CSV Log

You can configure ACS to record AAA-related logs and audit logs to a CSV logger.

To configure a CSV log:

-
- Step 1** In the navigation bar, click **System Configuration**.
 - Step 2** Click **Logging**. The Logging Configuration page appears.
 - Step 3** In the ACS Reports table, click **Configure** for the CSV log that you want to configure.
The CSV *log* File Configuration page appears, where *log* is the name of the CSV log that you selected.
 - Step 4** To enable or disable the log, under Enable Logging, check or uncheck the **Log to *log* report** check box, where *log* is the name of the selected log.
 - Step 5** For AAA-related reports, configure the attributes that you want ACS to log. For more information about the options for configuring attributes, see [CSV log File Configuration Page, page 10-40](#).
 - Step 6** (ACS for Windows only) Specify file management options for the CSV files. For more information about the file management options, see [CSV log File Configuration Page, page 10-40](#).
 - Step 7** Click **Submit**.
ACS implements the specified CSV log configuration.
-

Related Topics

[Viewing and Downloading CSV Reports, page 10-31](#)

Configuring Syslog Logging

You can configure ACS to record AAA-related logs and audit logs to a syslog logger.

To configure a syslog log:

-
- Step 1** In the navigation bar, click **System Configuration**.
 - Step 2** Click **Logging**. The Logging Configuration page appears.
 - Step 3** In the ACS Reports table, click **Configure** for the syslog log that you want to configure.
The *log* Configuration page appears, where *log* is the name of the syslog log that you selected.
 - Step 4** To enable or disable the log, under Enable Logging, check or uncheck the **Log to *log* report** check box, where *log* is the name of the selected log.
 - Step 5** For AAA-related reports, configure the attributes that you want ACS to log. For more information about the options for configuring attributes, see [Syslog log Configuration Page, page 10-41](#).
 - Step 6** Configure the syslog servers to which you want to send the syslog messages. For more information about the options for configuring syslog servers, see [Syslog log Configuration Page, page 10-41](#).
 - Step 7** Click **Submit**.
ACS implements the specified syslog log configuration.
-

Configuring an ODBC Log (ACS for Windows only)

You can configure ACS to record AAA-related logs and audit logs to an ODBC logger. You can configure the SQL create table statement before or after configuring the ODBC log in ACS.

**Note**

Before you can configure an ODBC log, you must prepare for ODBC logging. For more information, see [Preparing for ODBC Logging, page 10-9](#).

To configure an ODBC log:

- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **Logging**. The Logging Configuration page appears.
- Step 3** In the ACS Reports table, click **Configure** for the ODBC log that you want to configure.
The ODBC *log* Configuration page appears, where *log* is the name of the ODBC log you selected.
- Step 4** To enable or disable the log, under Enable Logging, check or uncheck the **Log to *log* report** check box, where *log* is the name of the selected log.
- Step 5** For AAA-related reports, configure the attributes that you want ACS to send to the relational database. For more information about the options for configuring attributes, see [ODBC log Configuration Page \(ACS for Windows only\), page 10-42](#).
- Step 6** Configure ACS to communicate with the ODBC database. For more information about Connection Settings options, see [ODBC log Configuration Page \(ACS for Windows only\), page 10-42](#).
- Step 7** Click **Submit**.
ACS saves the log configuration. The Logging Configuration page appears.

To configure an SQL create table statement:

- Step 1** In the Logging Configuration page, click **Configure** for the ODBC log that you are configuring.
The ODBC log configuration page appears.
- Step 2** To display a SQL create table statement, click **Show Create Table**.
A SQL create table statement for Microsoft SQL Server appears in the right panel of the ACS window. The table name is the name that is specified in the Table Name field. The column names are the attributes that are specified in the Logged Attributes list.

**Note**

The generated SQL is valid for Microsoft SQL Server only. If you are using another relational database, refer to your relational database documentation for information about writing a command to create a table.

- Step 3** Using the information provided in the generated SQL, create a table in your relational database for this ODBC log. For ODBC logging to work, the table name and the column names must exactly match the names in the generated SQL.

When you enable the log, ACS begins sending logging data to the relational database table that you created by using the system DSN that you configured.

Configuring and Enabling Remote Logging (ACS for Windows only)

You can configure remote logging for AAA-related logs and audit logs. You must first configure the remote logging server, and then configure remote logging on each ACS that will send information to the remote logging server.

These topics describe how to set up remote logging:

- [Configuring the Remote Logging Server, page 10-26](#)
- [Configuring ACS to Send Data to a Remote Logger, page 10-27](#)

Configuring the Remote Logging Server

Before You Begin

- On a computer that you want to use as a remote logging server to store all logging data, install ACS. For information about installing ACS, see the *Installation Guide for Cisco Secure ACS for Windows Release 4.2*.
- Ensure that gateway devices between the ACSs that are sending data and the remote logging ACS server permit the remote logging ACS server to receive data on TCP port 2001.

To configure the remote logging server:

-
- Step 1** Configure and enable the individual logs as needed. All data that is sent to the remote logging server will be recorded in the way that you configure logs on this ACS. For information about:
- Configuring CSV logs, see [Configuring a CSV Log, page 10-24](#).
 - Configuring syslog logs, see [Configuring Syslog Logging, page 10-24](#).
 - Configuring ODBC logs, see [Configuring an ODBC Log \(ACS for Windows only\), page 10-25](#).



Note You can configure Remote Logging on the remote logging server so that it will send all data to another remote logging server. However, you must use this option with caution; otherwise, you might create an endless logging loop.

- Step 2** To the AAA Servers table, add each ACS from which the remote logging server will receive logging data. For more information, see [Configuring AAA Servers, page 3-15](#).



Note If the remote logging server logs watchdog and update packets for an ACS, you must check the Log Update/Watchdog Packets from this remote AAA Server check box for that ACS in the AAA Servers table.

If you want to implement remote logging on other remote logging servers for use as secondary servers or as mirrored logging servers, repeat this procedure for each additional remote logging server.

Related Topics

[Configuring ACS to Send Data to a Remote Logger, page 10-27](#)

Configuring ACS to Send Data to a Remote Logger

**Note**

Before configuring the Remote Logging feature on each ACS server that will send data to the remote logging server, ensure that you have configured your remote logging ACS server. For more information, see [Configuring the Remote Logging Server, page 10-26](#).

On each ACS that will send data to the remote logging server:

-
- Step 1** Add the remote logging server to the AAA Servers table. For more information, see [Configuring AAA Servers, page 3-15](#). If you have created multiple remote logging servers, repeat this step for each remote logging server.
- Step 2** In the navigation bar, click **System Configuration**.
- Step 3** Click **Logging**.
The Logging Configuration page appears.
- Step 4** Click **Remote Logging Servers Configuration**.
The Remote Logging Setup page appears.
- Step 5** Set the applicable Remote Logging Services Configuration options. For information about these options, see [Remote Logging Setup Page, page 10-39](#).
- Step 6** Click **Submit**.
ACS saves and implements the remote logging configuration that you specified.
-

Related Topics

- [Configuring the Remote Logging Server, page 10-26](#)

Configuring Logging to Remote Agents (ACS SE only)

You can configure remote logging of AAA-related logs and audit logs to installed ACS remote agents. For more information about installing and configuring an ACS Remote Agent, see *Installation and Configuration Guide for Cisco Secure ACS Remote Agents Release 4.2*.

The following steps are required to set up remote logging:

1. On each ACS SE, add the remote agent. For more information, see [Configuring Remote Agents \(ACS SE Only\), page 3-19](#).
2. Configure each ACS SE to send logs to the remote agent. For more information, see [Configuring ACS SE to Send Data to the Remote Agent, page 10-28](#).
3. On the ACS SE that the remote agent is configured to use as its configuration provider, configure log content and log-file management for all logs recorded on the remote agent. For more information, see [Configuring Remote Agent Logs on the Configuration Provider, page 10-28](#).

You can set up remote logging to another remote agent, for use as a secondary server or as a mirror server by repeating these steps.

Configuring ACS SE to Send Data to the Remote Agent

You configure each local ACS SE to send data to the remote agent. Local configuration of remote logging does not affect the types of logs sent to remote agents or the configuration of the data included in logs sent to remote agents. For information about configuring which logs are sent to remote agents and the data the logs contain, see [Configuring Remote Agent Logs on the Configuration Provider, page 10-28](#).

Before You Begin

Install and configure the remote agent before configuring the Remote Logging feature on each ACS SE that will send data to the remote agent.

On each ACS SE that will send data to the remote agent:

-
- Step 1** Add the remote agent on ACS SE. For more information, see [Configuring Remote Agents \(ACS SE Only\), page 3-19](#).
 - Step 2** In the navigation bar, click **System Configuration**.
 - Step 3** Click **Logging**.
The Logging Configuration page appears.
 - Step 4** Click **Remote Logging Servers Configuration**.
The Remote Logging Setup page appears.
 - Step 5** Set the applicable Remote Logging Services Configuration options. For information about these options, see [Remote Logging Setup Page, page 10-39](#).
 - Step 6** Click **Submit**.
ACS saves and implements the remote logging configuration that you specified.
-

Related Topics

[Configuring Remote Agent Logs on the Configuration Provider, page 10-28](#)

Configuring Remote Agent Logs on the Configuration Provider

On the configuration provider, you configure which logs will be stored on the remote agent, the log content, and how the remote agent will manage the log files.

For information about specifying to which remote agents ACS sends log data, see [Configuring ACS SE to Send Data to the Remote Agent, page 10-28](#).

To configure a CSV log for a remote agent:

-
- Step 1** In the navigation bar, click **System Configuration**.
 - Step 2** Click **Logging**.
The Logging Configuration page appears.
 - Step 3** Click **Remote Agent Reports Configuration**.

The Remote Agent Reports Configuration page appears.

Step 4 Click **Configure** for the remote logging report that you want to configure.

The CSV *log* File Configuration page appears, where *log* is the name of the remote agent log that you selected.

Step 5 To enable or disable the log, check or uncheck the **Log to CSV *log* name report** check box, where *log* is the name of the remote agent log that you selected.

Step 6 For AAA-related reports, configure the attributes that you want ACS to log. For more information about the options for configuring attributes, see [CSV log File Configuration Page, page 10-40](#).

Step 7 Specify file management options for the CSV files. For more information about the file management options, see [CSV log File Configuration Page, page 10-40](#).

Step 8 Click **Submit**.

ACS implements the remote agent log configuration that you specified.

Related Topics

[Configuring ACS SE to Send Data to the Remote Agent, page 10-28](#)

Configuring Service Logs

To configure how ACS generates and manages the service log file:

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

Step 2 Click **Service Control**.

The status of the services appears in ACS on *hostname* table, where *hostname* is the name of the computer that is running ACS.

Step 3 Set service log options in the Services Log File Configuration page. For information about the options in this page, see [Service Control Page Reference, page 10-43](#).

To disable the service log file, under Level of Detail, select the **None** option.

Step 4 Click **Restart**.

ACS restarts its services and implements the service log settings that you specified.

Related Topics

[Providing Service Logs for Customer Support, page 10-29](#)

Providing Service Logs for Customer Support

To provide customer support with enough data to research potential issues, set the Level of Detail to Full in the Services Log File Configuration page. See [Service Control Page Reference, page 10-43](#) for more details. Ensure that you have sufficient disk space to handle your log entries.

If a problem exists on your ACS, customer support will ask you to create a *package.cab* file. The *package.cab* file contains various files including:

- **Certificate files**—The ACS server certificate, as well as the certificate's CA.
- *Admin.txt*—Contains information regarding ACS administrators.
- *Host.txt* and *HostServices.txt*—Contain information regarding hosts and hosts configuration.
- *NDG.txt*—Contains configured network device groups.
- *DictionaryKey.txt* and *DictionaryValue.txt*—Contains ACS dictionary files.

To create a *package.cab* file:

-
- Step 1** At the command prompt, type **drwtsn32**.
- Check the Dr. Watson settings to be sure the **Dump Symbol Table** and **Dump All Thread Contents** options are selected in addition to the default options.
- Step 2** Go to the *bin* subdirectory in the directory in which ACS was installed.
- Step 3** Type **CSSupport.exe**.
- Run the executable with all default options. The program will collect all the necessary information including Dr. Watson logs and place them in a file called *package.cab*. The location of the file appears when the executable is finished.
-

The Support feature in the System Configuration section of the ACS web interface includes service logs in the *package.cab* file that it generates if you click Run Support Now. For information about this feature, see [Support Page, page 7-25](#).



Note

When creating a *package.cab* file that is larger than 2GB, additional *.cab* files are created due to the size limit of the packer. The first package name is *package.cab*, the second is *package1.cab*, and so on, until the N package, *packageN.cab*, where N is the number of packages minus one. The files are saved in the same location that is specified before the packing begins. These files are not standalone and all of them must be sent to package. Problems with the packed file (*package.cab*) may arise if there is not enough hard-disk space.

Related Topics

[Configuring Service Logs, page 10-29](#)

Viewing and Downloading Reports

The starting point for viewing and downloading reports is the Reports page, which you access from **Reports and Activity in the navigation bar**. See [Reports Page Reference, page 10-44](#) for a list of all the reports that can be accessed from this page.



Note

The RDBMS Synchronization report and the Database Replication report are available only if those options are enabled in **Interface Configuration > Advanced Options**.

These topics describe how to view reports in the ACS web interface, and how to download reports:

- [Viewing and Downloading CSV Reports, page 10-31](#)
- [Viewing Dynamic Administration Reports, page 10-34](#)

- [Viewing and Downloading Entitlement Reports, page 10-36](#)

Viewing and Downloading CSV Reports

These topics describe how to view and download ACS CSV reports:

- [CSV Log File Names, page 10-31](#)
- [Viewing a CSV Report, page 10-31](#)
- [Downloading a CSV Report, page 10-33](#)

CSV Log File Names

When you access a report in Reports and Activity, ACS lists the CSV files in chronological order, with the current CSV file at the top of the list. The current file is named *log.csv*, where *log* is the name of the log.

Older files are named as:

logyyyy-mm-dd.csv

where:

log is the name of the log.

yyyy is the year that the CSV file was started.

mm is the month that the CSV file was started, in numeric characters.

dd is the date that the CSV file was started.

For example, a Database Replication log file that was generated on October 13, 2002, would be named *Database Replication 2002-10-13.csv*.

Related Topics

- [Viewing a CSV Report, page 10-31](#)
- [Downloading a CSV Report, page 10-33](#)

Viewing a CSV Report

You can view the contents of CSV reports in the ACS web interface. You can sort the table by entries in the column, and you can filter CSV log reports.

Filtering criteria includes a regular expression, a time range, or both:

- Regular expression-based filtering checks that at least one of each column's value, per row, matches the provided regular expression. When you use regular-expression filtering, ACS traverses each column and displays only the rows that match the filtering criteria.
- You can use time-based filtering by specifying values for a Start Date & Time and an End Date & Time. Rows dated within the specified time range appear.

When you enter a regular expression and use time-based filtering as well, the report will include only the rows that match both criteria.

To view a CSV report:

-
- Step 1** In the navigation bar, click **Reports and Activity**.
- Step 2** Click the name of the CSV report that you want to view.
On the right side of the browser, ACS lists the current CSV report filename and the filenames of any old CSV report files.
- Step 3** Click the CSV report filename whose contents you want to view.
If the CSV report file contains information, the information appears in the display area.
- Step 4** To check for newer information in the current CSV report, click **Refresh**.
- Step 5** Use the **Next** and **Previous** buttons to navigate forward and backward through the report pages.
- Step 6** To sort the table by entries in the column, in ascending or descending order. Click a column title once to sort the table by that column's entries in ascending order. Click the column a second time to sort the table by that column's entries in descending order.
- Step 7** To specify filtering criteria and apply the filter to the log file's content:
- In the **Regular Expression** text box enter a string value. The expression can be up to 100 characters long. See [Table 10-8](#) for Regular Expression characters and their syntax definitions.
 - In the **Start Date & Time** and **End Date & Time** text boxes, enter string values. The date and time format is *dd/mm/yyyy, hh:mm:ss* or *mm/dd/yyyy, hh:mm:ss* as defined in the ACS system configuration for the date format.
 - In the **Rows per Page** box choose the number of rows to display per page. (The default is 50.)
 - Click **Apply Filter**. The ACS web server will apply the specified filtering criteria to the report file and display the filtered results in the report's table.
 - Click **Clear Filter** to reset filtering parameters to their default values. Use this option to display the entire report unfiltered.
-

Table 10-8 Regular Expression Syntax Definitions

Character	Regular Expression Use
^	A caret (^) matches to the beginning of the string. Referred to as “begins with.” For example, ^A will match ABc , A123 , but not 1A234 . See the last table entry for another caret usage.
\$	The dollar sign (\$) matches the end of the string. Referred to as “ends with.” For example, yz\$ will match strings ending with xyz , 0123yz , but not 12yzA .
\	The backslash (\) matches a given string at any location. Referred to as “contains.” A backslash is also used for expressing 'special characters' in a given regular expression (For example, \+ will match against the plus sign (+), to differentiate from the plus sign (+) usage in regular expressions.
.	The dot (.) matches any character.
*	The asterisk (*) indicates that the character to the left of the asterisk in the expression should match for any number of instances (that is, 0 or more times).
+	The plus sign (+) is similar to the asterisk (*) but at least one match of the character should appear to the left of the plus sign (+) in the expression.

Table 10-8 Regular Expression Syntax Definitions

Character	Regular Expression Use
?	The question mark (?) matches the expression or character to its left 0 or 1 times.
	The pipe () allows the expression on either side of it to match the target string. For example, A a matches against A as well as a .
-	The hyphen (-) indicates a range of values. For example, a-z.
()	The parentheses are used for grouping of expressions and affect the order of pattern evaluation.
[]	Brackets ([]) enclosing a set of characters indicate that any of the enclosed characters may match the target character. Values in brackets can be one or more characters, or ranges. For example, [02468], [0-9].
[^	When a caret (^) immediately follows a left bracket ([), it excludes the remaining characters within brackets from matching the target string. For example, [^0-9] indicates that the target character is alpha rather than numeric.

Related Topics

- [CSV Log File Names, page 10-31](#)
- [Downloading a CSV Report, page 10-33](#)

Downloading a CSV Report

You can download the CSV file for any CSV report that you view in ACS.

After downloading a CSV log file, you can import it into spreadsheets by using most popular spreadsheet application software. Refer to your spreadsheet software documentation for instructions. You can also use a third-party reporting tool to manage report data. For example, aaa-reports! by Extraxi supports ACS.

To download a CSV report:

-
- Step 1** In the navigation bar, click **Reports and Activity**.
 - Step 2** Click the name of the required CSV report.
On the right side of the browser, ACS lists the current CSV report filename and the filenames of any old CSV report files.
 - Step 3** Click the CSV report filename that you want to download.
If the CSV report file contains information, the information appears in the display area in the right pane.
 - Step 4** In the right pane of the browser, click **Download**.
The browser displays a dialog box for accepting and saving the CSV file.
 - Step 5** Choose a location where you want to save the CSV file, and click **Save** to save the file.
-

Related Topics

- [CSV Log File Names, page 10-31](#)
- [Viewing a CSV Report, page 10-31](#)

Viewing Dynamic Administration Reports

These topics describe how to view and use dynamic administration reports:

- [Viewing the Logged-in Users Report, page 10-34](#)
- [Viewing the Disabled Accounts Report, page 10-35](#)
- [Viewing the Appliance Status Report, page 10-35](#)

Viewing the Logged-in Users Report


Note

The Logged-In Users report might take up to 20 seconds to open. Specific user information might take up to several minutes to appear.

You can view the Logged-in Users report in the ACS web interface.


Note

This list of users is cleared and restarted anytime ACS services are restarted. This list contains the names of users who logged in since the last time ACS was started; unless the list has been purged manually.

From this report, you can instruct ACS to delete users who are logged in to a specific AAA client. When a user session terminates without a AAA client sending an accounting stop packet to ACS, the Logged-in Users Report continues to show the user. Deleting logged-in users from a AAA client ends the accounting for those user sessions.


Note

Deleting logged-in users terminates only the ACS accounting record of users who are logged in to a particular AAA client. It does not terminate active user sessions, nor does it affect user records.

To view the Logged-in Users report:

Step 1 In the navigation bar, click **Reports and Activity**.

Step 2 Click **Logged-in Users**.

The Select a AAA Client page displays the name of each AAA client, its IP address, and the number of users who are logged in through the AAA client. At the bottom of the table, the **All AAA Clients** entry shows the total number of users who are logged in.

Step 3 To see a list of all users who are logged in, click **All AAA Clients**.

Step 4 To see a list of users who are logged in through a particular AAA client, click the name of the AAA client.

For each list of users, ACS displays tabular information on all users who are logged in, including:

- Date and Time
- User
- Group
- Assigned IP
- Port
- Source AAA Client



Tip To print this list, click anywhere in the right window and print the window from your browser.

Step 5 To sort the table by any column's entries, in ascending or descending order. Click a column title once to sort the table by the entries in that column in ascending order. Click the column a second time to sort the table by the entries in that column in descending order.

Step 6 To purge users who are logged in through a particular AAA client:

- a. Click the name of the AAA client.

ACS displays a table of all users who are logged in through the AAA client. The Purge Logged in Users button appears below the table.

- b. Click **Purge Logged in Users**.

ACS displays a message, which shows the number of users who are purged from the report and the IP address of the AAA client.

Viewing the Disabled Accounts Report

To view the Disabled Accounts report:

Step 1 In the navigation bar, click **Reports and Activity**.

Step 2 Click **Disabled Accounts**.

The Select a user account to edit page displays disabled user accounts, the account status, and the group to which the user account is assigned.



Tip To print this list, click anywhere in the right window and print the window from your browser.

Step 3 To edit a user account listed, in the User column, click the username.

ACS opens the user account for editing.

For more information about editing a user account, see [Basic User Setup Options, page 6-2](#).

Viewing the Appliance Status Report

To view the Appliance Status report:

Step 1 In the navigation bar, click **Reports and Activity**.

Step 2 Click **Appliance Status Page**.

The Appliance Status report appears in the right pane of the browser.



Tip To print this list, click anywhere in the right window and print the window from your browser.

Viewing and Downloading Entitlement Reports

You can download the CSV User Entitlement report file of mappings of users to groups. You can download a report of all administrators and their privileges as well as reports or privileges for each individual administrator. You can also view the reports for individual administrators in the ACS web interface.

To view and download entitlement reports:

-
- Step 1** In the navigation bar, click **Reports and Activity**.
- Step 2** Click **Entitlement Reports**.
The Entitlement Reports page appears.
- Step 3** To download the User Entitlement report:
- a. Click **Download report for mappings of users to groups**.
The browser displays a dialog box for accepting and saving the CSV file.
 - b. Choose a location where you want to save the CSV file, and click **Save**.
- Step 4** To download the privilege report for all administrators:
- a. Click **Download Privilege Report for All Administrators**.
The browser displays a dialog box for accepting and saving the CSV file.
 - b. Choose a location where you want to save the CSV file, and click **Save**.
- Step 5** To view and download the privilege report for an individual administrator:
- a. Click **Privilege Report for Admin**, where *Admin* is the name of the administrator account.
The report appears in the right pane of the browser.



Tip To print this list, click anywhere in the right pane and print the window from your browser.

- b. To download the CSV log file, click **Download** in the right pane of the browser.
The browser displays a dialog box for accepting and saving the CSV file.
 - c. Choose a location where you want to save the CSV file, and click **Save**.
-

Update Packets in Accounting Logs

Whenever you configure ACS to record accounting data for user sessions, ACS records start and stop packets. If you want, you can configure ACS to record update packets, too. In addition to providing interim accounting information during a user session, update packets drive password-expiry messages via the ACS Authentication Agent. In this use, the update packets are called watchdog packets.

**Note**

To record update packets in ACS accounting logs, you must configure your AAA clients to send the update packets. For more information about configuring your AAA client to send update packets, refer to the documentation for your AAA clients.

- **Logging Update Packets Locally**—To log update packets according to the local ACS logging configuration, enable the Log Update/Watchdog Packets from this Access Server option for each AAA client in Network Configuration.

For more information on setting this option for a AAA client, see [Adding AAA Clients, page 3-12](#).

- **Logging Update Packets Remotely**—To log update packets on a remote logging server, enable the Log Update/Watchdog Packets from this remote AAA Server option for the remote server AAA Server table entry on the local ACS.

For more information on setting this option for a AAA server, see [Adding AAA Servers, page 3-17](#).

Logging Configuration Pages Reference

The following topics describe the logging configuration pages.

- [Logging Configuration Page, page 10-37](#)
- [Critical Loggers Configuration Page, page 10-38](#)
- [Remote Logging Setup Page, page 10-39](#)
- [Remote Agents Reports Configuration Page \(ACS SE only\), page 10-39](#)
- [CSV log File Configuration Page, page 10-40](#)
- [Syslog log Configuration Page, page 10-41](#)
- [ODBC log Configuration Page \(ACS for Windows only\), page 10-42](#)

Logging Configuration Page

The Logging Configuration page is the starting point for configuring loggers and individual logs.

To open this page, choose **System Configuration > Logging**.

Table 10-9 Logging Configuration Page

Option	Description
Critical Loggers Configuration	Opens the Critical Loggers Configuration Page, page 10-38 , in which you can configure <i>critical loggers</i> when ACS records accounting messages to multiple loggers.
Remote Logging Services Configuration	Opens the Remote Logging Setup Page, page 10-39 , to configure remote loggers.
Remote Agent Reports Configuration (ACS SE only)	Opens the Remote Agents Reports Configuration Page (ACS SE only), page 10-39 , to configure the log content and file management of logs on the remote agent.
ACS Reports table	Displays which logs are enabled. The Configure links open the individual configuration page for each log: <ul style="list-style-type: none"> • CSV log File Configuration Page, page 10-40 • Syslog log Configuration Page, page 10-41 • ODBC log Configuration Page (ACS for Windows only), page 10-42

Related Topics

- [Configuring ACS Logs, page 10-22](#)
- [Remote Logging for ACS for Windows, page 10-10](#)
- [Remote Logging for ACS SE with ACS Remote Agents, page 10-10](#)

Critical Loggers Configuration Page

Use the Critical Loggers Configuration page to configure *critical loggers* for accounting logs to guarantee delivery of these logs to at least one logger.

To open this page, choose **System Configuration > Logging**. In the Logging Configuration Page, click the **Critical Loggers Configuration** link.

Table 10-10 Critical Loggers Configuration Page

Option	Description
RADIUS accounting critical logger	Specifies the critical logger for RADIUS accounting logs.
TACACS+ accounting critical logger	Specifies the critical logger for TACACS+ accounting logs.
VoIP accounting critical logger	Specifies the critical logger for VoIP accounting logs.

**Note**

We do not recommend that you configure a syslog logger as a critical logger; because, according to syslog standards, syslog message logging is not guaranteed.

Related Topics

[Configuring Critical Loggers, page 10-23](#)

Remote Logging Setup Page

Use the Remote Logging Setup page to configure to which remote loggers to send logs from the local ACS.

To open this page, choose **System Configuration > Logging**. In the Logging Configuration Page, click the Remote Logging Servers Configuration link.

Table 10-11 Remote Logging Setup Page

Option	Description
Do not log remotely	Disables logging to remote loggers.
Log to all selected remote log services	Sends logging data to all remote loggers in the Selected Log Services list.
Log to subsequent remote log services on failure	Sends logging information for this ACS server to one remote logger. ACS logs to the first accessible remote logger in the Selected Log Services list. Use this option when you want to configure ACS to send logging data to the next remote logger in the Selected Log Services list only if the first remote logger fails.
Log Services lists	These lists contain the ACS servers that are configured in the AAA Services table. The right (->) and left (<-) arrow buttons add and remove logging services to and from the Selected Log Services list. The Up and Down buttons order the logging services in the Selected Log Services list.

Related Topics

- [Remote Logging for ACS for Windows, page 10-10](#)
- [Remote Logging for ACS SE with ACS Remote Agents, page 10-10](#)

Remote Agents Reports Configuration Page (ACS SE only)

Use the Remote Agent Reports Configuration page on the ACS SE that the remote agent is configured to use as its configuration provider, to configure log content and log file management for all logs recorded on the remote agent.

To open this page, choose **System Configuration > Logging**. In the Logging Configuration Page, click the Remote Agent Reports Configuration link.

Table 10-12 Logging Configuration Page

Option	Description
Remote Logging Reports table	Displays which logs are enabled for the remote agent. The Configure links open the individual configuration page for each log.

Related Topics

[Configuring Remote Agent Logs on the Configuration Provider, page 10-28](#)

CSV log File Configuration Page

Use the CSV *log* File Configuration page to enable logging to an individual local or remote CSV logger, and configure the content and file management of that log.

To open this page, choose **System Configuration > Logging**. In the Reports Configurations tables, click **Configure** for a log in the CSV column.

For an ACS SE configuration provider, to enable remote logging to a remote agent, click **Remote Agent Reports Configuration**, then click **Configure** for a log.


Note

For ACS SE, there are no configurable options for local CSV Audit logs.

Table 10-13 CSV log File Configuration Page

Option	Description
Enable Logging	Contains the option to enable or disable the log.
Log to CSV <i>log</i> report check box	Enables or disables logging to the selected logger. Note This check box is grayed out for CSV Audit logs, which are always enabled.
Configure Log Content (AAA-related reports only)	Contains the options to specify which attributes will be logged.
Select Columns to Log	The Attribute list contain attributes that have not been selected for logging. The Logged Attributes list contains attributes that have been selected for logging. The right (->) and left (<-) arrow buttons add and remove attributes to and from the Logged Attributes list. The Up and down buttons order the attributes in the Logged Attributes list.
Reset Columns button	Sets the attributes in the Logged Attributes list back to the default selections.
Log File Management (ACS for Windows and Remote Agent Reports configuration only)	Contains log file management options.
Generate New File	Specifies when ACS or the remote agent should generate a new CSV file: <ul style="list-style-type: none"> • Every day—At 12:01 A.M. local time every day. • Every week—At 12:01 A.M. local time every Sunday. • Every month—At 12:01 A.M. on the first day of every month. • When size is greater than <i>x</i> KB—When the current file reaches the size, which you enter in kilobytes, in the <i>X</i> box.
Directory	The directory to which ACS or the remote agent writes the CSV log file. We recommend that you specify the full path including drive letter, otherwise the file location will be relative to the installation directory. If the remote agent server uses Sun Solaris, the path must begin at the root directory, such as <i>/usr/data/acs-logs</i> .
Manage Directory	Manages which CSV files are retained.

Table 10-13 CSV log File Configuration Page (continued)

Option	Description
Keep only the last X files	Limits the number of CSV files that are retained. Enter the maximum number of files you want to retain in the X box.
Delete files older than X days	Limits the age of the CSV files that are retained. Enter the number of days to retain a CSV file before deleting it.

Related Topics

- [Configuring a CSV Log, page 10-24](#)
- [Configuring the Remote Logging Server, page 10-26](#)
- [Configuring Remote Agent Logs on the Configuration Provider, page 10-28](#)

Syslog log Configuration Page

Use the Syslog *log* File Configuration page to enable logging to up to two syslog loggers, and configure the content of those logs.

To open this page, choose **System Configuration > Logging**. In the Reports Configurations tables, click **Configure** for a log in the Syslog column.

Table 10-14 Syslog log File Configuration Page

Option	Description
Enable Logging	Contains the option to enable or disable the log.
Log to syslog <i>log</i> report check box	Enables or disables logging to the selected logger. The default is disabled.
Configure Log Content (AAA-related reports only)	Contains the options to specify which attributes will be logged.
Select Columns to Log	The Attribute list contain attributes that have not been selected for logging. The Logged Attributes list contains attributes that have been selected for logging. The right (->) and left (<-) arrow buttons add and remove attributes to and from the Logged Attributes list. The Up and down buttons order the attributes in the Logged Attributes list.
Reset Columns button	Sets the attributes in the Logged Attributes list back to the default selections.
Syslog Servers	Contains options to configure up to two syslog logging servers.
IP	Specifies the IP addresses of the syslog servers.
Port	Specifies the ports of the syslog servers to which log messages will be sent.
Max message length (bytes)	Specifies the maximum message length of syslog messages, in bytes. The default length, which is the recommended length for a standard syslog server, is 1024 bytes. If the syslog is used as a proxy you can reduce the message length to allow some room for the proxy headers. The minimum value allowed is 200 bytes.

Related Topics

- [Configuring Syslog Logging, page 10-24](#)
- [Configuring the Remote Logging Server, page 10-26](#)

ODBC *log* Configuration Page (ACS for Windows only)

Use the ODBC *log* Configuration page to enable logging to an individual ODBC logger, and configure the content and connection settings for ACS to the ODBC database.

To open this page, choose **System Configuration > Logging**. In the Reports Configurations tables, click the icon by the name of a log in the ODBC column.

Table 10-15 ODBC *log* Configuration Page

Option	Description
Enable Logging	Contains the option to enable or disable the log.
Log to ODBC <i>log</i> report check box	Enables or disables logging to the selected logger. The default is disabled.
Configure Log Content (AAA-related reports only)	Contains the options to specify which attributes will be logged.
Select Columns to Log	The Attribute list contain attributes that have not been selected for logging. The Logged Attributes list contains attributes that have been selected for logging. The right (->) and left (<-) arrow buttons add and remove attributes to and from the Logged Attributes list. The Up and down buttons order the attributes in the Logged Attributes list.
Reset Columns button	Sets the attributes in the Logged Attributes list back to the default selections,
ODBC Connection Settings	Contains options for ACS to communicate with the ODBC database.
Data Source list	The system DSN that you created to allow ACS to send ODBC logging data to your relational database.
Username	The username of a user account in your relational database (up to 80 characters). Note The user must have sufficient privileges in the relational database to write the ODBC logging data to the appropriate table.
Password	The password (up to 80 characters) for the specified relational database user account
Table Name	The name (up to 80 characters) of the table to which you want ODBC logging data appended.

Table 10-15 ODBC log Configuration Page (continued)

Option	Description
Create Table Statement	Contains the option to display a SQL create table statement.
Show Create Table button	<p>Displays a SQL create table statement for Microsoft SQL Server. The statement appears in the right panel of the ACS window.</p> <p>The table name is the name that is specified in the Table Name field. The column names are the attributes that are specified in the Logged Attributes list.</p> <p>Note The generated SQL is valid for Microsoft SQL Server only. If you are using another relational database, refer to your relational database documentation for information about writing a command to create a table.</p>

Related Topics

- [Configuring an ODBC Log \(ACS for Windows only\), page 10-25](#)
- [Configuring the Remote Logging Server, page 10-26](#)

Service Control Page Reference

Use the Services Log File Configuration page to enable or disable logging of services logs, and configure the detail and file management of that log.

To open this page, choose **System Configuration > Service Control**.

You must click the Restart button for these options to take effect.

Table 10-16 Services Log File Configuration Page

Option	Description
Cisco Secure ACS on <server>	Displays whether ACS services are running or stopped.
Services Log File Configuration	Contains options to enable, disable, and configure logging of services.
Level of Detail	<p>Disables logging, or sets the level of logging:</p> <ul style="list-style-type: none"> • None—No log file is generated. • Low—Only start and stop actions are logged. This is the default setting. • Full—All services actions are logged. Use this option when collecting data for customer support. This option provides customer support with enough data to research potential issues. Ensure that you have sufficient disk space to handle your log entries.
Log File Management (ACS for Windows only)	Contains log file management options.

Table 10-16 Services Log File Configuration Page (continued)

Option	Description
Generate New File	Select when ACS or the remote agent should generate a new CSV file: <ul style="list-style-type: none"> • Every day—At 12:01 A.M. local time every day. • Every week—At 12:01 A.M. local time every Sunday. • Every month—At 12:01 A.M. on the first day of every month. • When size is greater than <i>x</i> KB—When the current file reaches the size, that you enter, in kilobytes, in the <i>X</i> box.
Manage Directory	Check to manage which CSV files are retained.
Keep only the last <i>X</i> files	Select to limit the number of CSV files that are retained. Enter the maximum number of files to retain in the <i>X</i> box.
Delete files older than <i>X</i> days	Select to limit the age of the CSV files that are retained. Enter the number of days to retain a CSV file before deleting it.

Related Topics

[Configuring Service Logs, page 10-29](#)

Reports Page Reference

Use this page to access and download ACS CSV reports.

To open this page, click **Reports and Activity** in the navigation bar.

Table 10-17 Reports Page

Option	Description
TACACS+ Accounting Reports	Displays TACACS+ accounting reports, which contain a record of all successful authentications for the applicable item during the period that the report covers.
TACACS+ Administration Reports	Displays TACACS+ Administration reports, which contain all TACACS+ commands requested during the period that the report covers. This information is typically used when you use ACS to manage access to routers.
RADIUS Accounting Report	Displays RADIUS accounting reports, which contain a record of all successful authentications for the applicable item during the period that the report covers.
VoIP Accounting Reports	Displays VoIP accounting reports, which contain a record of all successful authentications for the applicable item during the period that the report covers.
Passed Authentications	Displays Passed Authentications reports, which list successful authentications during the period that the report covers.
Failed Attempts	Displays the Failed Attempts reports, which contain a record of all unsuccessful authentications during the period that the report covers for TACACS+ and RADIUS. The reports capture the username attempted, time and date, and cause of failure.

Table 10-17 Reports Page (continued)

Option	Description
Logged-in Users	Displays all users currently logged in, grouped by AAA client. You can delete logged-in users from specific AAA clients or from all AAA clients.
Disabled Accounts	Displays accounts that have been disabled.
ACS Backup and Restore	Displays ACS Backup and Restore reports, which list dates and times that the ACS system information was backed up and restored and whether the action was successful.
RDBMS Synchronization	Displays RDBMS Synchronization reports, which contain the times the RDBMS database was synchronized and whether synchronization was manual or scheduled. This report is available only if you enable this option in the Interface Configuration > Advanced Options page.
Database Replication	Displays Database Replication reports, which contain the times the ACS Internal Database was replicated to the backup server and whether replication was manual or scheduled. This report is available only if you enable this option in the Interface Configuration > Advanced Options page.
Administration Audit	Displays Administration Audit reports, which contain a list of the administrators who accessed ACS on the applicable date, the actions they made or attempted to make, and the time of the action. Examples of actions logged include starting and stopping the administration session, editing user and group data, and changing the network configuration.
User Password Changes	Displays User Password Changes reports, which contain information about user-initiated changes to passwords stored in the ACS internal database.
ACS Service Monitoring	Displays ACS Service Monitoring reports, which contain a log of the events that ACS encounters when it attempts to monitor services, such as CSAdmin. This information includes events for the Active Service Monitor, CSMon, which is a service.
Entitlement Reports	Lists the available user and administrator entitlement reports. The user entitlement report lists all users with their group, Network Access Profile (NAP) if relevant, and the mapping type (static or dynamic). the administrator entitlement reports lists privileges of administrators.
Appliance Status Page (ACS SE only)	Displays current statistics about hardware resource usage with information about the IP network configuration and network interface card of the ACS appliance.
Appliance Administration Audit (ACS SE only)	Displays Appliance Administration Audit reports, which contain a list of activity on the serial console of the ACS appliance. It records when the appliance administrator account is used to log in, the commands issued during the serial console session, and when the administrator logs out, ending the session.

Related Topics

- [About ACS Logs and Reports, page 10-1](#)
- [Viewing and Downloading Reports, page 10-30](#)

Audit Log Attributes

Table 10-18 lists the attributes that are monitored in ACS and specify administrative user actions for editing fields in the user page.

Table 10-18 *Audit Log Attributes*

Code	Editing Field
1	Account_Disabled
2	Real_Name
3	Description
4	Password_Authentication
5	PAP_Passowrd
6	Separate_PWD_For_CHAP
7	CHAP_Password
8	User_Group
9	Callback_setting
10	Client_IP_ADDR_Assignment
11	Selected_Pools
12	Shared_NAR
13	Selected_NARs
14	PerUser_NAR
15	Per_User_Def_Net_Access_Restriction_Table
16	CLI/DNIS-based_Access_Restrictions
17	CLI/DNIS-based_Access_Restrictions_Table
18	MAX_Sessions
19	User_Usage_Quotas
20	reset_Usage_Counters
21	Advanced_Account_Disable_options
22	Time_Bound_Alternate_Group
23	DownloadableACL
24	Tacacs+Enable_Control
25	AssociationTable
26	Tacacs+Enable_Passwd_settings
27	Tacacs+Passwd
28	Tacacs+OutBoundPasswd
29	Tacacs+Settings_PPP_IP
30	Tacacs+Settings_Custom_Attr_PPP_IP
31	Tacacs+Settings_PPP_IPX
32	Tacacs+Settings_Custom_Attr_PPP_IPX

Table 10-18 *Audit Log Attributes*

33	Tacacs+Settings_PPP_Multilink
34	Tacacs+Settings_Custom_Attr_PPP_MultiLink
35	Tacacs+Settings_PPP_Apple_Talk
36	Tacacs+Settings_Custom_Attr_PPP_Apple_Talk
37	Tacacs+Settings_PPP_VPDN
38	Tacacs+Settings_Custom_Attr_PPP_VPDN
39	Tacacs+Settings_PPP_LCP
40	Tacacs+Settings_Custom_Attr_PPP_LCP
41	Tacacs+Settings_ARAP
42	Tacacs+Settings_Custom_Attr_ARAP
43	Tacacs+Settings_Shell_exec
44	Tacacs+Settings_Custom_shell_exec
45	Tacacs+Settings_PIXShell
46	Tacacs+Settings_PIXShell_Custom_Attributes
47	Tacacs+Settings_Slip
48	Tacacs+Settings_Slip_Custom_Attributes
49	Tacacs+Settings_shell_cmd_Auth_Set
50	Shell_Cmd_Auth_Set_Table
51	Per_User_Command_Authorization
52	PIX/ASA_Command_Authorization
53	PIX/ASA_Command_Authorization_Table
54	Tacacs+UnknownServices
55	IETF_RADIUS_Attributes_Service_Type
56	IETF_RADIUS_Attributes_Framed_Protocol
57	IETF_RADIUS_Attributes_Framed-IP-Netmask
58	IETF_RADIUS_Attributes_Framed-Routing
59	IETF_RADIUS_Attributes_Filter-ID
60	IETF_RADIUS_Attributes_Framed-MTU
61	IETF_RADIUS_Attributes_Framed-Compression
62	IETF_RADIUS_Attributes_Login-IP-Host
63	IETF_RADIUS_Attributes_Login-Service
64	IETF_Radius_Attributes_Login-TCP-Port
65	IETF_RADIUS_Attributes_Reply-Message
66	IETF_RADIUS_Attributes_CallBack-ID
67	IETF_RADIUS_Attributes_Framed-Route
68	IETF_RADIUS_Attributes_Framed-IPX-Network
69	IETF_RADIUS_Attributes_State

Table 10-18 *Audit Log Attributes*

70	IETF_RADIUS_Attributes_Class
71	IETF_RADIUS_Attributes_Session-Timeout
72	IETF_RADIUS_Attributes_Termination-Action
73	IETF_RADIUS_Attributes_Proxy-State
74	IETF_RADIUS_Attributes_Login-LAT-Service
75	IETF_RADIUS_Attributes_Login-LAT-Node
76	IETF_RADIUS_Attributes_Login-LAT-Group
77	IETF_RADIUS_Attributes_Framed-AppleTalk-Link
78	IETF_RADIUS_Attributes_Framed-AppleTalk-Network
79	IETF_RADIUS_Attributes_Framed-AppleTalk-Zone
80	IETF_RADIUS_Attributes_Port-Limit
81	IETF_RADIUS_Attributes_Login-LAT-Port
82	IETF_RADIUS_Attributes_Tunnel-Type
83	IETF_RADIUS_Attributes_Tunnel-Medium-Type
84	IETF_RADIUS_Attributes_Tunnel-Client-Endpoint
85	IETF_RADIUS_Attributes_Tunnel-Server-Endpoint
86	IETF_RADIUS_Attributes_Tunnel-Password
87	IETF_RADIUS_Attributes_ARAP-Features
88	IETF_RADIUS_Attributes_ARAP-Zone-Access
89	IETF_RADIUS_Attributes_Configuration-Token
90	IETF_RADIUS_Attributes_Tunnel-Private-Group-ID
91	IETF_RADIUS_Attributes_Tunnel-Assignment-ID
92	IETF_RADIUS_Attributes_Tunnel-Preference
93	IETF_RADIUS_Attributes_Acct-Interim-Interval
94	IETF_RADIUS_Attributes_Tunnel-Client-Auth-ID
95	IETF_RADIUS_Attributes_Tunnel-Server-Auth-ID