ACS View 4.0

Deployment Guide

Contents

Introduction

This document discusses planning, design, and implementation practices for deploying Cisco® Secure Access Control Server (ACS) View 4.0. It describes:

- Deployment of ACS View with ACS
- ACS View performance
- Network topology
- Access requirements
- Installation procedure and the basic features
- Integration with Cisco Wireless Control System (WCS)

This document also provides you an overview of ACS logs. The information in this document is based on Cisco Secure ACS View version 4.0, which provides reporting capabilities for ACS 4.1.4 and 4.2 deployments.

ACS Logs and Logging

Cisco Secure Access Control Server generates a variety of logs. You can download many of these logs to your local drive or view them as HTML reports in the ACS web interface.

ACS logs a variety of user and system activities to different formats and targets. These logs are used for troubleshooting and diagnostics, compliance and auditing, building reports, and billing.

The ACS logs are:

Network

- TACACS+ Accounting
- TACACS+ Administration
- RADIUS Accounting
- VoIP Accounting
- Passed Authentications
- Failed Attempts
- Logged-in users

Configuration Reports

- Disabled Accounts
- Entitlement Reports
- User Entitlement Reports
- Administrator Entitlement Reports

Configuration Audit

- Administration Audit
- User Password Changes

System Logs

- ACS Backup and Restore
- RDBMS Synchronization
- Database Replication
- ACS Service Monitoring
- Appliance Status Page

You can activate and configure logging for individual logs. ACS can log information to multiple loggers simultaneously. In ACS, you can configure:

- **Critical loggers:** Critical logger for accounting logs guarantees delivery of these logs to at least one logger. It is recommended that you configure a syslog logger as a critical logger, because according to syslog standards, you cannot guarantee syslog messages.
- **Comma-separated value (CSV) log:** The standard internal log storage, viewed by the Cisco Secure ACS log viewer. Windows allows rollover based on frequency or size, specification of log directory, and optional purging of files based on age or number. The Cisco Secure ACS Solution Engine (ACS-SE) has a fixed log file rollover at 10 MB and retains the seven most recent log files.

- **Syslog logging:** To record authentication, authorization, and accounting (AAA)–related logs and audit logs to a syslog logger. You can configure each log to go to a separate syslog server. You can configure up to two servers per log file.
- **Open Database Connectivity (ODBC) log (Cisco Secure ACS for Windows):** 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 Cisco Secure ACS.
- **Remote logging (Cisco Secure ACS for Windows):** Remote logging for AAA-related logs and audit logs. You must first configure the remote logging server and then configure remote logging on each Cisco Secure ACS that will send information to the remote logging server.
- **Logging to Cisco Secure ACS remote agents (Cisco Secure ACS Solution Engine):** For remote logging of AAA-related logs and audit logs to installed Cisco Secure ACS remote agents. You can configure multiple remote agent destinations. You can log to all destinations, or use as a failover list.
- **Service logs:** Contain a log of the events when Cisco Secure ACS attempts to monitor services such as CSAdmin. This includes events for the Active Service Monitor, CSMon, which is itself a service. This report is on by default.
- **Providing service logs for customer support:** To create a *package.cab* file for debugging. Cisco Secure ACS has a number of debugging logs including CSAdmin, CSAuth, CSDBSync, CSLog, CSMon, CSRadius, and CSTacacs. You can set the log level to None, Low, or Full. You must set the log level to Full for diagnostics. Starting with Cisco Secure ACS 4.1.3, Cisco Secure ACS provides a session key to correlate various logs. The diagnostic log is only for local logging. The **Support** command on Cisco Secure ACS Solution Engine allows debugging log download.

Choosing the Correct Log Format

It is recommended to use an internal CSV file for a small deployment that consists of one or two Cisco Secure ACS systems. You can use the remote logging option to consolidate logs on one system in Cisco Secure ACS for Windows.

For medium to large deployments, the syslog option for offloading logs to a remote server is recommended. This has several advantages including the ability to ”steer” different logs to different servers and allowing the use of a dedicated log server for log consolidation.

For more information on ACS logging, see:

- The User Guide for Cisco Secure Access Control Server: http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_user_guide_list.html.
- The complete product documentation: http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs41/index.htm .
- Additional white papers: http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_white_papers_list.html,
- Additional configuration guides: http://www.cisco.com/en/US/partner/products/sw/secursw/ps2086/prod_configuration_examples_list.html,

An Overview of ACS View

The ACS View product represents a major evolutionary change for the reporting, monitoring, and troubleshooting capabilities of Cisco Secure ACS. The goal of ACS View is to provide administrators a consolidated product that helps enable them to extract the core logging information from ACS and correlate that data to provide advanced reporting, diagnostics, and troubleshooting capabilities for single or multiple ACS(s) deployed in the field.

ACS View 4.0 is a web-based application that addresses the reporting needs for ACS 4.x deployments. The ACS View server collects the log and configuration data from the ACS registered with it, using the available supported mechanisms in ACS such as syslog and *package.cab* downloaded over HTTP/HTTPS.

Using the data collected from the ACS, ACS View provides:

- Different set of rich and interactive reports for an administrator to analyze and correlate the data retrieved from ACS. Provides predefined and system reports like session traffic, authentication summary, and so on. The reports are in tabular or charts/graphic format or both, depending on the report category, and allow the user to view the details wherever possible. The reports can be filtered on, exported to CSV/HTML/PDF format, emailed, and printed. You can also schedule the reports and view the reports generated offline in the Report Inbox of the users.
- The capability to create custom reports by querying against the available attributes in various log data collected from one or more ACS(s) in the network.
- Configurable alerts (triggers): Administrators can configure alerts by defining thresholds and rules on the data retrieved from ACS.
- A user dashboard to view the user's favorite queries, alerts, and reports.

System Specifications

ACS View server is a standalone server running Linux operating system, with an easy-to-use management interface. ACS View makes use of the command-line interface (CLI) infrastructure for its administrative tasks such as security (AAA), backup, restore, packaging, and installation.

ACS View uses a variant of the Application Deployment Engine (ADE) 2120 appliance with:

- Intel Core2 Duo (2.13 GHz)
- 4 GB RAM
- Two 250 GB hard disk drives
- Two 10/100/1000 network interface cards (NICs)

The appliance runs on Linux Operating System Kernel version 2.6. The file system as such is not available for access. Only the CLI is available when you log in to an ACS View appliance.

Besides, only a minimal set of ports is opened in the ACS View appliance. The ports and protocols include:

- 80 HTTP/443 HTTPS
- 21 FTP/69 TFTP/115 SFTP
- 514 SYSLOG
- 2049 NFS

- 22 SSH
- 25 SMTP Simple Mail Transfer Protocol
- 53 DNS Domain Name Service

Note: If a firewall is located between ACS and ACS View, you need to enable the ports for syslog, HTTP/HTTPS transport access protocol for *package.cab* file download from Cisco Secure ACS, and the other protocols based on the external server placement.

ACS View Log Retrieval

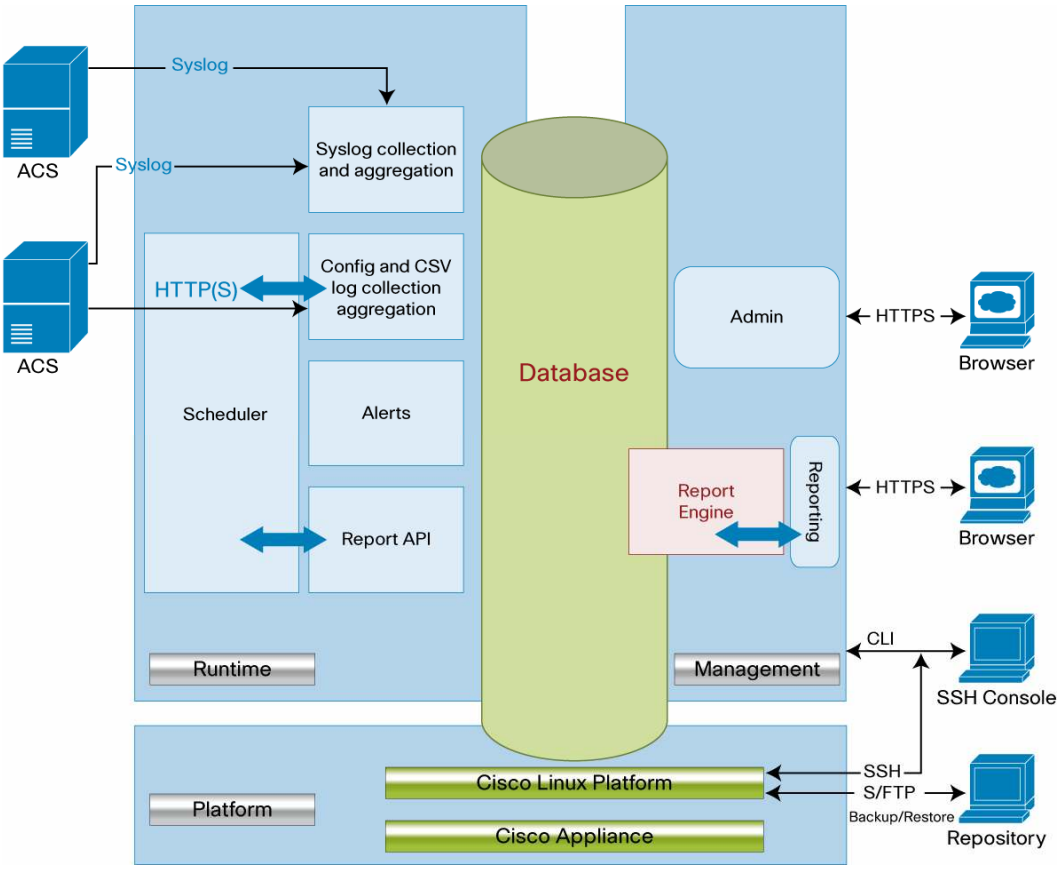
ACS View 4.0 uses the following approach to retrieve the log data from ACS:

- Push from ACS: Syslog pushes the data from ACS to ACS View. This is the primary mechanism of collecting data from ACS.
- Pull from ACS: ACS View pulls the *package.cab* files using HTTP/HTTPS, as an alternate or fallback mechanism to plug in any gaps in the data retrieval through syslog.

To generate reports, ACS View retrieves ACS logs (referred to as ACS log data in this document) such as TACACS+ accounting, RADIUS accounting, failed attempts, which are available as CSV files for downloading or viewing in the Reports and Activity page of ACS. This does not include the service logs.

Figure 1 provides a very high level overview of various components of ACS View.

Figure 1. ACS View Components



Note: For ACS View to receive syslog from ACS, you must configure each log in ACS to send syslog data to ACS View. You can do this by using the ACS web interface as detailed in the *User Guide for Cisco Secure Access Control Server 4.1*. You must configure ACS View in ACS as the syslog server, by providing the hostname or the IP address of the ACS View server.

Syslog Collector

In ACS View, the syslog collector receives the log data from ACS. The syslog collector processes only the logs retrieved from the registered and licensed ACS. Syslog data received from an unregistered ACS is dropped, and the information is not logged. ACS View can collect the syslog from the standalone ACS or from the remote logging server. This is applicable only for ACS Windows. ACS View does not support collecting logs from remote agent and ODBC loggers for ACS Windows.

Configuration and CSV Collector over HTTP/HTTPS

The ACS logs are primarily collected by ACS View using syslog. The logs retrieved through *package.cab* download serve as a backup for syslog data lost because of network issues or when ACS View is down or not reachable.

ACS View downloads the *package.cab* file periodically from the configured ACS(s) and retrieves the required information. It acts like a filter, checking the missing log information and adding it to the ACS View database.

ACS provides the option to download the CSV files and ACS configuration data as part of *package.cab* through the HTTP/HTTPS URL call.

- **Csvlog collector:** Download the *package.cab* files; extract the CSV files.
- **Config collector:** Download the *package.cab* files; extract the TXT files and parse them.

You can download *package.cab* from the configured ACS on demand or on a periodic daily schedule.

Alternately, you can upload any *package.cab* file that you have generated from these ACS to ACS View.

Note: ACS View does not support receiving logs from the remote agent and ODBC loggers.

ACS View Deployment Planning

This section describes various aspects of Cisco Secure ACS View server that influence its deployment in the network. These include:

- **ACS logging:** Types of ACS logging and how they affect the ACS View deployment decisions
- **ACS View server sizing and scaling:** How to decide the number of Cisco Secure ACS View servers to deploy; a predeployment scenario in which a customer wants to estimate the number of ACS View servers that are required in the network, and a postdeployment scenario for which an additional ACS View server is required.

ACS Logging

ACS logging is categorized into:

- ACS syslog logging (ACS Windows/ACS-SE)
- ODBC logging for ACS Windows
- Remote logging for ACS Windows
- Remote logging for ACS-SE with remote agent

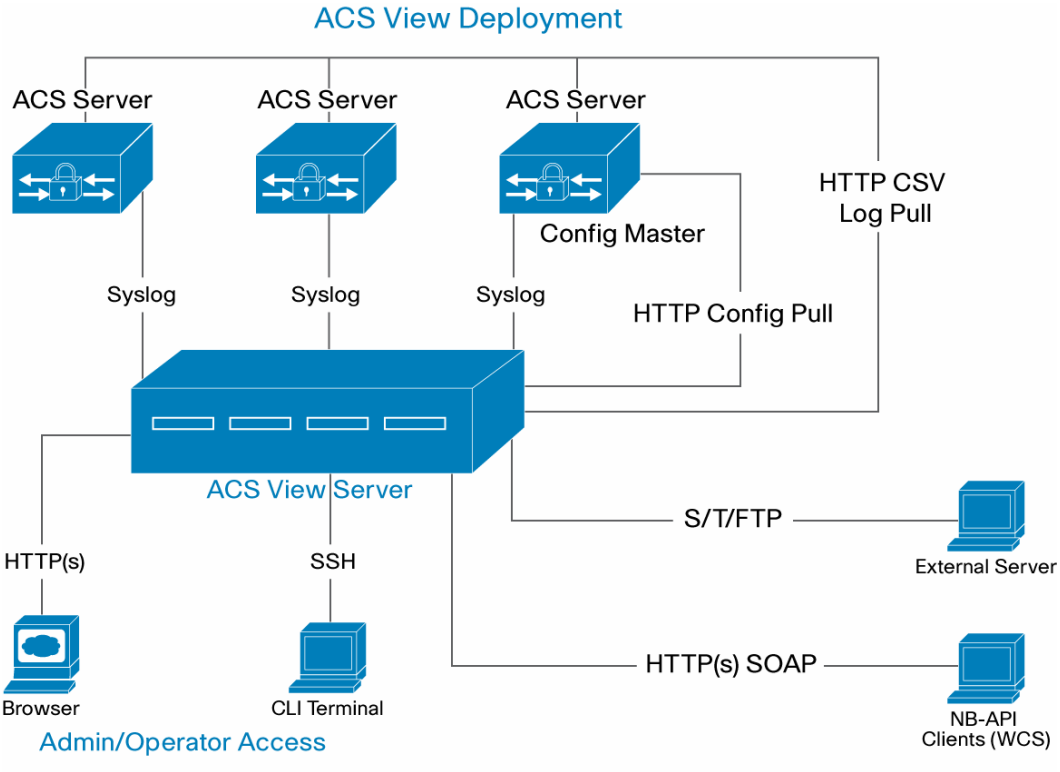
The ACS View server can be deployed in an ACS syslog logging environment, irrespective of the version of ACS (ACS Windows/ACS-SE), which is actually the primary deployment model. Also, ACS View supports collecting logs from the remote logging server, which is applicable only for ACS Windows. ACS View does not support collecting logs from the remote agent and ODBC logger; thus, remote logging for ACS-SE with remote agent and ODBC logging for ACS Windows are not supported. In such scenarios, it is recommended to enable syslog and configure the ACS View server as the syslog server individually.

I. Deploying ACS View in ACS Syslog Logging (ACS for Windows/ACS-SE)

This is the primary deployment model, in which all the ACS are enabled with syslog and the ACS View server is configured as the syslog server. 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 ACS. ACS syslog logging follows the standard syslog protocol (RFC 3164). Messages are sent connectionless to syslog servers by using an unsecured User Datagram Protocol (UDP) port without data encryption.

Figure 2 provides you an overview of the deployment of ACS View with ACS syslog logging (ACS Windows/ACS-SE).

Figure 2. Deploying ACS View with ACS Syslog Logging (ACS Windows/ACS-SE)



Syslogs are instant log messages produced by ACS whenever an activity occurs in ACS. Configuring ACS with ACS View as their syslog destination is the primary deployment, and this is independent of ACS versions. Each ACS is configured with ACS View as its logging destination.

You can redirect the syslog message from ACS to ACS View by configuring ACS View as the syslog server. ACS View receives syslog messages and computes the data to generate various reports. For more information, see the *User Guide for Cisco Secure Access Control Server ACS*.

ACS View processes the syslog only from a registered ACS. The syslog messages from registered ACSs are dropped when:

- The message violates any syslog RFC pattern
- An AAA server attribute is missing in the original message part
- The AAA server attribute value is empty

The syslog collector component in ACS View retrieves instant log data from the registered ACS. The ACS logs are primarily collected by ACS View using syslog. The logs retrieved through *package.cab* download or upload serve as a backup for syslog data lost because of network issues or when ACS View is down or not reachable. By default, ACS View downloads *package.cab* from ACS at 12:01 a.m.

Note: ACS services or processes are not restarted while creating the *package.cab* file; this is applicable for ACS 4.1.4 and later versions.

Choosing the Configuration Master

ACS(s) managed by ACS View server are expected to be in a single configuration domain, which means that the configuration data is common and shared across the ACS(s).

ACS View pulls the configuration data from only one ACS added to it. This server is the configuration master. You can specify the configuration master while adding the ACS to ACS View. The configuration master can be any ACS; it does not have to be the ACS replication master.

ACS View requires a few mandatory attributes as part of ACS syslog and CSV messages to generate effective reports and accurate data collection. For a list of the mandatory attributes for each log and how to configure them, see the *User Guide for Cisco Secure Access Control Server View 4.0*.

Adding ACS Syslog Server to ACS View

1. Log in to ACS View 4.0.
2. Choose **System Administration > ACS Servers Configuration > Server List**, and click **Add**.
3. In the ACS Server Settings area, enter:
   - **Server Name**: Enter the name of the ACS.
   - **IP Address**: Enter the IP address of the ACS.
   - **Admin Username**: Enter a valid username of an ACS administrator. ACS View uses this admin username and the admin user password to collect data from ACS over HTTP or HTTPS. Make sure that this administrator has support operations enabled in the ACS.
   - **Admin User Password**: Enter the password of the specified administrator user.
   - **ACS Time Zone**: Choose the appropriate time zone from the list. This is the time zone configured in ACS.
   - **ACS Platform**: Specify whether you are using ACS Solution Engine or ACS Windows.
   - **Transport for Administration Access**: Choose the web access mode (HTTP or HTTPS) as configured in ACS.
   - **Configuration Master**: Click **Yes** if you want this ACS to be the master ACS configuration server; otherwise click **No**.
4. In the ACS Log Settings area, enter:
   - **Remote Logging Configuration**: Specify whether the ACS stores the logs in a remote server.
   - Choose the **Does not log remotely** option.
   - **Date Format for CSV log**: Click the appropriate date format as configured in ACS.
   - **Time Zone for Syslog**: Click **GMT Time** or **Local Time** for syslog depending on the time zone as configured in ACS at **System Configuration > Date Format Control > Time Zone Selection For Syslog**. This option is available only from ACS 4.2 onwards. For earlier ACS versions, choose **GMT**.
5. Click **Save**.

ACS View will start collecting the syslog messages from the registered ACS.

II. Deploying ACS View with ACS Remote Logging for ACS Windows

Remote logging allows the ACS to send the log data directly to the centralized remote logging server, where the data is written to the logs. ACS listens to TCP port 2001 for remote logging communication. A 128-bit proprietary algorithm encrypts remote logging data. The remote logging server needs to be configured in a remote logging–enabled ACS.

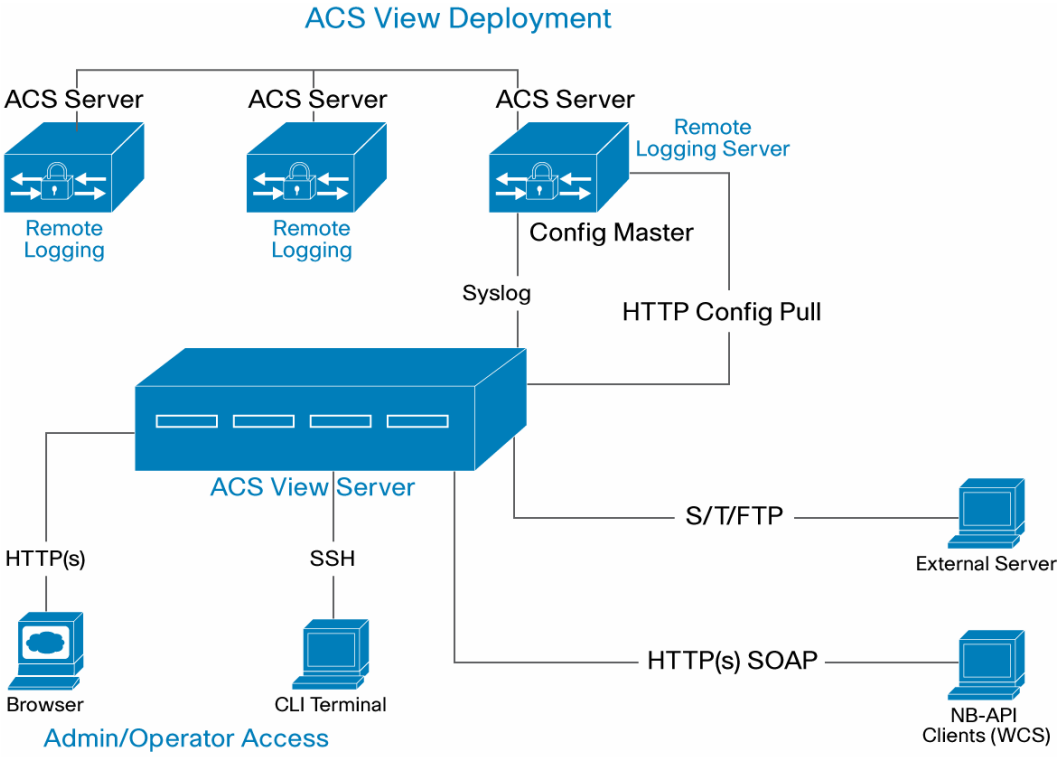
Refer the ACS user guide for configuring ACS to send data to a remote logger.

Note: Before configuring the remote logging feature on each ACS that sends data to the remote logging server, make sure that you have configured your remote logging ACS.

For more information, see the "Configuring the Remote Logging Server" section in the *User Guide for Cisco Secure Access Control Server 4.2*.

Figure 3 provides you an overview of the deployment of ACS View with ACS remote logging for ACS Windows.

Figure 3. ACS View with ACS Remote Logging for ACS Windows



The remote logger or the remote logging server acts as the centralized log collection server that collects the log files from the remote logging–enabled ACS. The remote logging server still performs AAA functions and acts as the repository for the logs that it receives from other ACS(s).

This remote logging server is enabled with syslog logging, and the logs are redirected to ACS View. ACS View collects the syslog messages and the CSV files from the remote logging server for all the remote logging–enabled ACS.

The logs retrieved through *package.cab* download or upload serve as a backup for syslog data lost because of network issues or when ACS View is down or not reachable. By default the *package.cab* file download is schedule at 12:01 a.m.

Note: ACS services/processes are not restarted while creating the *package.cab* file; this is applicable from ACS 4.1.4.

Choosing the Configuration Master

ACS(s) managed by the ACS View server are expected to be in a single configuration domain, which means that the configuration data is common and shared across the ACS(s).

ACS View pulls the configuration data from only one ACS added to it. This server is the configuration master. You can specify the configuration master while adding the ACSs to ACS View. The configuration master can be any ACS; it does not have to be the ACS replication master or a remote logging server.

ACS View requires a few mandatory attributes as part of ACS syslog and CSV messages to generate effective reports and accurate data collection. For a list of the mandatory attributes for each log and how to configure them, see the *User Guide for Cisco Secure Access Control Server View 4.0*.

Adding a Remote Logging ACS to ACS View

Add the remote logging server to the ACS View server list:

1. Log in to ACS View 4.0.
2. Choose **System Administration > ACS Servers Configuration > Server List**, and click **Add**.
3. In the ACS Server Settings area, enter:
   - **Server Name**: Enter the name of the ACS.
   - **IP Address**: Enter the IP address of the ACS.
   - **Admin Username**: Enter the valid username of an ACS administrator. ACS View will use this admin username and the admin user password to collect data from ACS over HTTP or HTTPS. Make sure that this administrator has support operations enabled in the ACS.
   - **Admin User Password**: Enter the password of the specified administrator user.
   - **ACS Time Zone**: Choose the appropriate time zone from the list. This is the time zone configured in ACS.
   - **ACS Platform**: Click **ACS Windows**.
   - **Transport for Administration Access**: Choose the web access mode (HTTP or HTTPS) as configured in the ACS.
   - **Configuration Master:** Click **Yes** if you want this ACS to be the master ACS configuration server; otherwise click **No**.
4. In the ACS Log Settings area, enter:
   - **Remote Logging Configuration**: Specify whether the ACS stores the logs on a remote server. Choose the **Does not log remotely** option.
   - **Date Format for CSV log**: Click the appropriate date format as configured in ACS.

- **Time Zone for Syslog**: Click **GMT Time** or **Local Time** for syslog depending on the time zone as configured in ACS at **System Configuration > Date Format Control > Time Zone Selection For Syslog**. This version is available only from ACS 4.2 onwards. For earlier ACS versions, choose **GMT**.

5. Click **Save**.

Adding a Remote Logging–Enabled ACS to ACS View

1. Log in to ACS View 4.0.
2. Choose **System Administration > ACS Servers Configuration > Server List**, and click **Add**.
3. In the ACS Server Settings area, enter:
   - **Server Name**: Enter the name of the ACS.
   - **IP Address**: Enter the IP address of the ACS.
   - **Admin Username**: Enter the valid username of an ACS administrator. ACS View uses this admin username and the admin user password to collect data from ACS over HTTP or HTTPS. Make sure that this administrator has support operations enabled in the ACS.
   - **Admin User Password**: Enter the password of the specified administrator user.
   - **ACS Time Zone**: Choose the appropriate time zone from the list. This is the time zone configured in ACS—the time zone of the Windows application on which ACS runs.
   - **ACS Platform**: Specify ACS Windows.
   - **Transport for Administration Access**: Choose the web access mode (HTTP or HTTPS) as configured in the ACS.
   - **Configuration Master**: Click **Yes** if you want this ACS to be the master ACS configuration server; otherwise click **No**.
4. In the ACS Log Settings area, enter:
   - **Remote Logging Configuration**: Specify whether the ACS stores the logs in a remote server.
   - Choose **Log remotely to ACS** and choose the corresponding remote logging server from the drop-down list.
   - **Date Format for CSV log**: Click the appropriate date format as configured in ACS.
   - **Time Zone for Syslog**: Click **GMT Time** or **Local Time** for syslog depending on the time zone as configured in ACS at **System Configuration > Date Format Control > Time Zone Selection For Syslog**. This version is available only from ACS 4.2 onwards. For earlier ACS versions, choose **GMT**.
5. Click **Save**.

Now, ACS View will collect the syslog and CSV files from only the remote logging server. The remote logging enabled–ACS must be configured with remote logging server, syslog, and CSV with mandatory attributes enabled. ACS View will start collecting the log data from the registered ACS.

ACS View Sizing and Scaling

This section describes the sizing element for ACS View 4.0 in an ACS deployment. The sizing fits into two scenarios:

- A predeployment scenario wherein a customer wants to estimate the number of ACS View servers that are required in the network
- A postdeployment period when an additional ACS View server is required

Basically, the sizing depends on the:

- Amount of traffic that is received from the ACS per second
- Online storage space
- Number of ACS
- Configuration master

A customer can ideally use:

- **One ACS View server:**
  - When the ACS is distributed across multiple sites and the cost of transferring the log data between these sites is lower and assuming the ACS(s) are in a single configuration domain.
- **Two or more ACS View servers:**
  - When the ACS is distributed across multiple sites and the cost of transferring the log data between these sites is higher.
  - If ACS(s) generate a great deal of traffic over many hours to ACS View, and the number of active ACS(s) is expected to grow.
  - If the customer has independent ACS deployments, then the customer may need to consider an individual ACS View server for each deployment.

The Predeployment Scenario

ACS View 4.0 supports 1.5 to 2 million events a day, with 0.5 million authentication and 1 million accounting records.

Table 1 shows the performance benchmarking under normal and burst traffic.

Table 1. Performance Benchmarking

Traffic	Events per Second*	Maximum Number of Events per Day	Database Size	Number of ACS
Normal traffic	25	~ 1.5-2 million	0.5-1 GB	10-12
Burst traffic	100-200	~ 1.5-2.5 million	1-1.5 GB	10-12

* Events per second = Syslog messages per second; for example, each successful authentication creates 1 syslog event and 2 accounting syslog events.

The Amount of Traffic

The recommended ACS View performance benchmark for normal traffic is a maximum of 25 events per second at a constant rate for 24 hours for stable performance.

To calculate total events per day, apply this formula:

```
Events per second * Number of seconds per day (86400)
```

The recommended events per day, thus, is 25 * 86,400 ~=2 million events a day.

To calculate the estimated number of events per second, apply this formula:

```
Number of events per day / Number of seconds per day (86400)
```

For example, if there are 2,500,000 events per day, the event per second amounts to 2,500,000 / 86,400 ~= 29 events per second.

Burst Traffic and Events per Second

The recommended burst traffic per second during peak time is 100 to 200 events for any 3 to 5 hours from multiple ACS. The performance benchmark with 100 to 200 events per second in burst traffic for 3 to 5 hours is found to be stable with very minimal syslog drops.

Note: If there is continuous traffic for more than the maximum recommended events for hours, say over 200 events per second for more than 3 to 5 hours continuously, a considerable number of syslog messages may be dropped.

To summarize, ACS View can handle anywhere betwen100 and 200 events per second during peak hour for any 3 to 5 hours with very minimal syslog messages being dropped. You can download *package.cab* from the configured ACS on demand or to a daily schedule as a backup for lost syslog data.

In order to calculate the events per second for busy periods, calculate the events per hour (EPH). To calculate EPH, apply the following formula; assume that 80 percent of the events occur over a 10-hour period during the day.

```
Number of events per day * .8 (80%) / by 10 (number of hours in the
period)
```

After calculating the EPH, divide that figure by the number of seconds per hour (3600) to know the events per second for the busy period.

For example, assuming 5,000,000 events per day, the EPH for a busy period is 5,000,000 * 0.8 / 10 hrs = 400,000.

To calculate EPS, 400,000 / 3600 sec ~=111.

Online Storage Space

The ACS View appliance is bundled with a 500-GB hard disk and bundled with Sybase version 10 as a built-in database. The database size can grow anywhere between 0.5 GB to 1.5 GB per day based on the incoming events per second and the size of the packets.

The default length of syslog messages (1024) is the recommended length for a standard syslog server. The minimum value allowed is 200 bytes.

The performance benchmarking report has an average of 512 bytes of data with all mandatory attributes enabled.

For example, to calculate the disk size consumed per day:

```
512 bytes per message
25 messages per second * 512 bytes = 12800 bytes per sec / 12. 5
kilobytes per second
```

To calculate per day, apply:

```
12800 bytes per sec * 86,400 seconds per day = 1.03 GB per day
```

The /opt directory can hold around 70 GB of data, which accounts for 2 to 3 months of data to generate reports. This is based on the incoming record rate and the packet size. Data purging kicks in when the /opt directory reaches 70 GB of data.

The data purging feature deletes older entries to make room for incoming data without running into disk-space crunches. You can define the limit for database purging.

Note: When data purging is done, you must rebuild the database from the CLI by using the database **rebuild** command. This command reflects the exact free and used space in the database after purging old data. This command rebuilds the database and is recommended for better performance.

Upload or Download package.cab

The ACS logs are collected by ACS View primarily by using syslog. The logs retrieved through a *package.cab* download serve as a backup for syslog data lost because of network issues or when ACS View is down or not reachable. You can download *package.cab* from the configured ACS on demand or on a daily schedule. You can also upload any *package.cab* file that you have generated from the registered ACS to ACS View.

Table 2 shows the performance numbers for a package.cab file upload and download.

Table 2. Performance Numbers for package.cab Download or Upload

.cab Size (in MB)	Database Size (in GB)	Time Taken for Upload/Download	Number of Records in .cab File
50	15	12 minutes	2,59,000
40	15	10 minutes	1,64,000
30	15	7 minutes	1,52,000

By default, ACS View downloads *package.cab* at 12:01 a.m. from all registered ACS(s). The recommended *package.cab* upload and download values to ACS View are 50 MB per instance.

When generating *package.cab*, make sure that you:

- Exclude service logs
- Restrict the log data collection date to range for a fewer days

Note: If the *package.cab* file is large, the upload and extraction time will be longer. ACS View pulls configuration data only from the ACS configured as the configuration master in ACS View.

The Number of ACS

ACS View generates dynamic and customizable reports from the data collected from the ACS(s) by using syslog and *package.cab*, which you can download over HTTP. ACS View supports collecting logs from multiple ACS(s) and configuration data from only one server that is configured as the configuration master. This feature provides maximum flexibility to add as many ACS(s) as needed based on your requirements.

The number of ACS(s) that ACS View supports is mutually aligned with the events per second. ACS View does not limit the number of servers that you can add. ACS View must have valid licenses to add these ACS(s). You can add any number of ACS to ACS View, but the incoming events must not exceed 25 events per second at a constant rate.

The performance benchmark is tested with a maximum of 12 ACS with 25 events per second in normal traffic. ACS View can handle 100 to 200 events per second in peak hour traffic for any 3 to 5 hours, but there will be a very minimal amount of syslog messages being dropped, and *package.cab* file download serves as a backup for dropped syslog messages.

Configuration Master

ACS(s) managed by the ACS View server are expected to be in a single configuration domain, which means that the configuration data is common and shared across the ACS(s).

ACS View pulls the configuration data from only one ACS added to it. This server is the configuration master from which ACS View pulls the configuration data. You can specify this while adding the ACS to ACS View. If you have independent ACS deployments, you may need to deploy an individual ACS View server for each deployment.

The Postdeployment Scenario

You can add more ACS View servers to your network when the number of ACS increases and the syslog events per second grow over the recommended burst figures.

The guidelines and performance analysis show that each ACS View server can handle 25 events per second in normal traffic conditions and 100 to 200 events per second in burst traffic conditions for any 3 to 5 hours from multiple servers. If the event per second continues to grow over the recommended figures continuously, it is recommended that you deploy an additional ACS View server.

If the number of ACS increases in the network and the number of events per second also grows at a rapid rate beyond recommended figures, you can get an additional ACS View server and add a few ACS to the second ACS View server.

You can go for an additional ACS View server if:

- The number of records that get into the database is high
- The online storage grows beyond the limit
- You want to store more data online to generate reports (more than 70 GB of data)

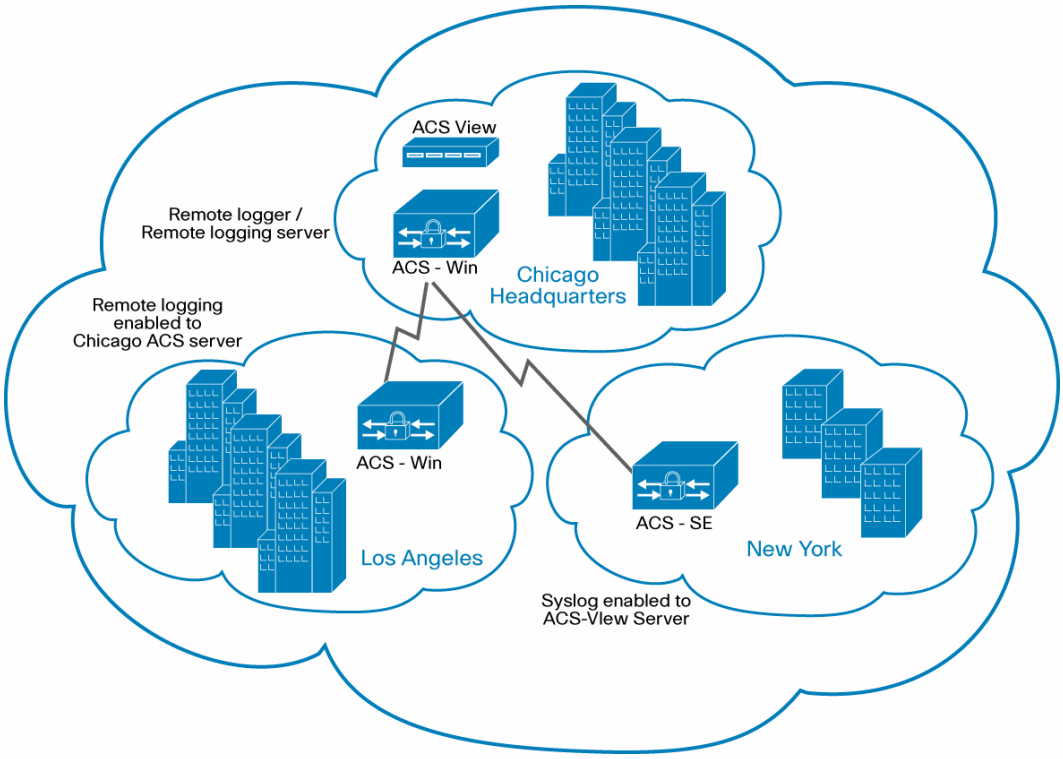
Note: The additional ACS View server will be an individual setup, managing data from a different set of ACS, and the ACS View servers will not interact or share data with each other. ACS View will download the configuration from only one server that is configured as the configuration master.

Deployment Scenario

Flop International corporate sites are in Los Angeles, Chicago, and New York. The design team has decided to deploy wireless and remote-access capabilities throughout the network. The ACS(s) are placed in each location and in different time zones, and the configuration is replicated across the servers from the ACS in Chicago to each location. The ACS View server is placed in the corporate head office, that is, Chicago. ACS View retrieves log data from ACS using syslog and downloads the *package.cab* file using HTTP/HTTPS.

Figure 4 shows the Flop International network diagram.

Figure 4. Flop International Network Diagram



The ACS in Chicago and LA are ACS for Windows. The ACS in Chicago headquarters is acting as the remote logging server for the ACS in LA. The ACS in NY is an ACS-SE standalone appliance. It is syslog enabled and configured ACS View server as the syslog logging server. Chicago headquarters ACS is acting as the configuration master.

Note: ACS View collects the log from the remote logging server; this is applicable only for ACS Windows. ACS View does not support collecting logs from remote agents or from ODBC logger; therefore, remote logging for ACS-SE and ODBC logger for ACS Windows are not supported. In such cases, you must activate syslog and configure the ACS View server as the syslog server.

Caution: ACS(s) managed by ACS View server are expected to be in a single configuration domain, which means that the configuration data is common and shared across the ACS(s). ACS View pulls the configuration data from only one ACS added to it. This server is the configuration master. You can specify this while adding the ACS to ACS View. If you have independent ACS deployments, you may need to consider an individual ACS View server for each deployment.

ACS Requirements

This release of ACS View 4.0 provides reporting capabilities for ACS 4.1.4 and 4.2 deployments; therefore, make sure all ACS are 4.1.4 or 4.2. ACS View is not tested with any older version of ACS, and therefore is it not recommended and not supported. Contact your local Cisco account representative for information about the upgrade process.

ACS 1: Chicago HQ – Remote logging server/remote logger

- ACS name: ACSCHC (AAA server attribute name)
- IP-address: 10.77.155.180
- ACS edition: Software
- ACS time zone: CDT
- Admin username and password (Make sure that the ACS administrator user has Administrator privileges for Support Operations enabled in ACS.)
- Activate syslog and the CSV log
- Mandatory attributes to be selected for logging in ACS (Refer to the *User Guide for Cisco Secure Access Control Server View* for mandatory attributes.)
- Configure the ACS View server as the syslog logging server.
- Date format and syslog time zone: MM/DD/YYYY, Local Time
- Transport Access mode HTTP/HTTPS: HTTP

ACS 2: LA – Remote logging enabled to ACS 1 (ACSCHC)

- ACS name: ACSLA (AAA server attribute name)
- IP-address: 10.77.155.196
- ACS edition: Software
- ACS time zone : PDT
- Admin username and password (Make sure that the ACS administrator user has Administrator privileges for Support Operations enabled in ACS.)
- Activate remote logging to ACS – 1 (ASCCHC)
- Date format and syslog time zone: MM/DD/YYYY, local time
- Transport access mode HTTP/HTTPS: HTTP

ACS 3: NY

- ACS name: ACSNY (AAA server attribute name)
- IP-address: 10.77.155.155
- ACS edition: Appliance
- ACS time zone: EDT
- Admin username and password (enabled with Support Operations in ACS)
- Mandatory attributes to be selected for logging in ACS (Refer to *Cisco Secure Access Control Server View User Guide for* the list of mandatory attributes.)
- Enable syslog and the CSV log.
- Configure the ACS View server as the syslog logging server.
- Date format and syslog Time zone: MM/DD/YYYY, local time

Installing ACS View

The setup process is a one-time configuration task. You must power up the appliance before you configure ACS View.

The following is a sample output of the **setup** command:

```
localhost login: setup
Enter hostname[]: acs-view-1
Enter IP address[]: 209.165.200.225
Enter IP default netmask[]: 255.255.255.0
Enter IP default gateway[]: 209.165.200.1
Enter IP default DNS domain[]: yourcompany.com
Enter Primary nameserver[]: 209.165.200.254
Add/Edit another nameserver? Y/N : n
Enter username [admin]: admin
Enter password:
Enter password again:
Pinging the gateway...
Pinging the primary nameserver...
Do not use `Ctrl-C' from this point on...
Appliance is configured
Installing applications...
Installing acsview...
Generating configuration...
Rebooting...
```

After you execute the **setup** command successfully, the ACS View server reboots, and the settings take effect. You can now log in to ACS View with your username and the password that you entered during setup.

You can check the status of the ACS View processes using the process status command, now. For more information, see the *User Guide for Cisco Secure Access Control Server View 4.0*.

Accessing the ACS View GUI

Launch a web browser and in the address bar, enter:

```
https://{servername.domain | ip_address}
```

`Example: https://10.77.155.138`

Licenses and Certificates

ACS View follows the node-locked licensing mechanism. Node-locked licenses tie a single software application to a single machine. Node-locked licensing is based on the unique device identifier (UDI). This UDI is a combination of product and serial number and provides inventory identification. By default, ACS View appliance supports two ACS(s). An additional license is needed for each extra ACS server.

For licenses, visit the Cisco licenses page at http://www.cisco.com/go/license.

You must provide the UDI information and the number of ACS(s) that you plan to register with ACS View.

To obtain the UDI, enter **`show udi`** in the CLI.

For example,

```
acsview-cars/admin# show udi
```

SPID: ADE-1010
VPID: V01
Serial: 123455

Provide the SPID (serial product ID) and the serial number to the license provider to obtain the node-locked license.

As there are three ACS(s) to register with ACS View, we need to get an additional license for the third ACS to increase the default, which is two ACS(s).

INCREMENT ACSCOUNT cisco 4.0 31-may-2008 uncounted \

VENDOR_STRING="<COUNT>3</COUNT> <UDI>*******</UDI>" HOSTID=ANY \

NOTICE="<LicFileID>Eval_15</LicFileID><LicLineID>0</LicLineID> \

<PAK>dummyPak</PAK>" SIGN="0059 E534 CBFF A6AC F1C0 7F48 A8F4 \

024A 7DA9 83CE EC3E C807 480E 83F0 4E81 0403 20F5 DB68 D50A \

74C6 8AD8 CB4D 9988 ED15 218D E90C 49DA 0C2A 9E46 5615"

Note: ACS View processes the syslog messages collected only from the ACS that are registered with ACS View with valid licenses. If the central logging server also acts as an ACS (that is, if there are accounting and authentication logs from this server as well), it will be counted as one license. To upload a new license, click **Browse** and choose the .lic file and click **Upload** in the Licenses page.

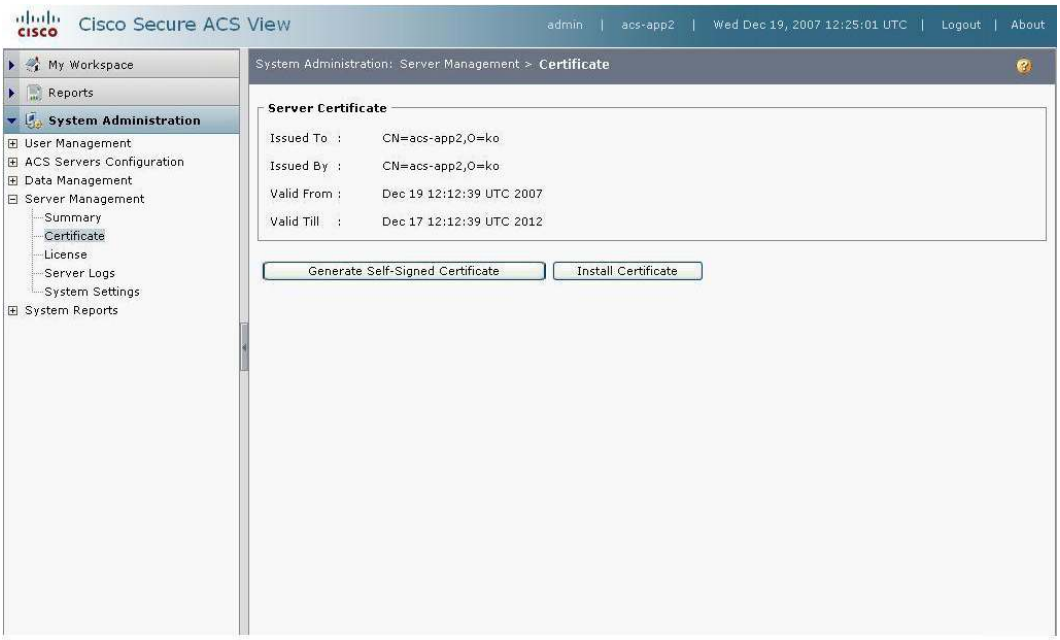
ACS View installation and initial setup also creates a self-signed certificate, which will be used by the ACS View web server for secure browser-server communication (in SSL mode).

During the initial setup, only the hostname will be populated in the certificate. Updating the self-signed certificate requires a restart of the web server.

Note: The certificate generated will be valid for five years.

Figure 5 shows the Certificates page in ACS View.

Figure 5. Certificates



To install an external certificate, click **Install Certificate** and choose the certificate file and specify the private key. To generate a self-signed certificate, click **Generate self-signed certificate** and specify the organization name, output, and challenge password.

Adding ACS to ACS View

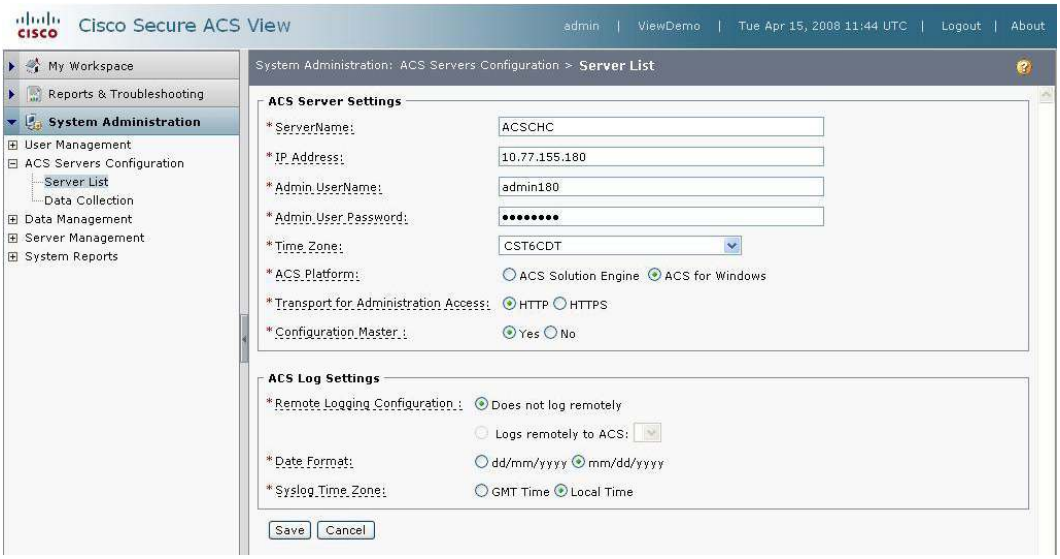
To start with, first add the ACS remote logging server to the ACS View server list and followed by the remote logging enabled ACS to the list.

Adding the remote logging server to the server list – ACSCHC – ACS 1

To add an ACS, go to **System Administration > ACS Servers Configuration > Server List**, and click **Add**.

Figure 6 shows adding a remote logging server to ACS View.

Figure 6. Adding Remote Logging Server



Enter the following:

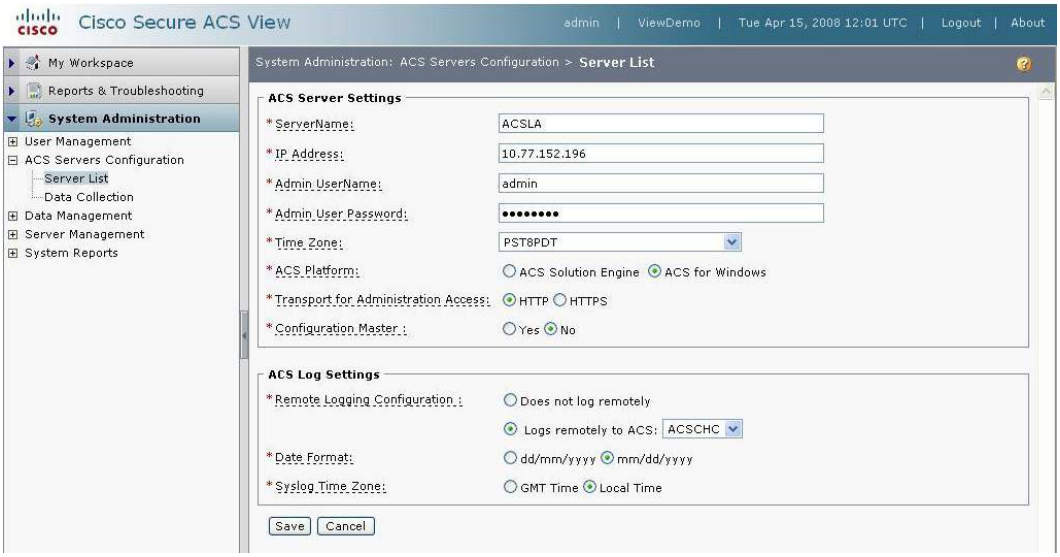
- **Server Name**: Enter the name of the server.
- **IP Address**: Enter a valid IP address.
- **Admin Username**: Enter the valid username.
- **Admin User Password**: Enter the valid credentials.
- **Time Zone**: Based on ACS geographical location, you must enter the appropriate time zone of the ACS.
- **ACS platform**: Specify **ACS Appliance** or **ACS Software** edition.
- **Transport Access mode**: HTTP/HTTPS.
- **Configuration Master**: Click **Yes**. ACS View pulls configuration data only from the ACS configured as the configuration master in ACS View.
- **Remote Logging Configuration**: Choose **Does not log remotely**, if the logs are stored locally.
- **Date Format**: Specify the date format of the ACS.
- **Syslog Time Zone**: **Local** or **GMT**.

Click **Save** to finish adding the server.

Similarly, add the ACS located in LA; remote logging is enabled for this server to ACS 1 (ACSCHC).

Figure 7 shows adding the ACS in LA to ACS View.

Figure 7. Adding the LA Server to ACS View



Enter the following:

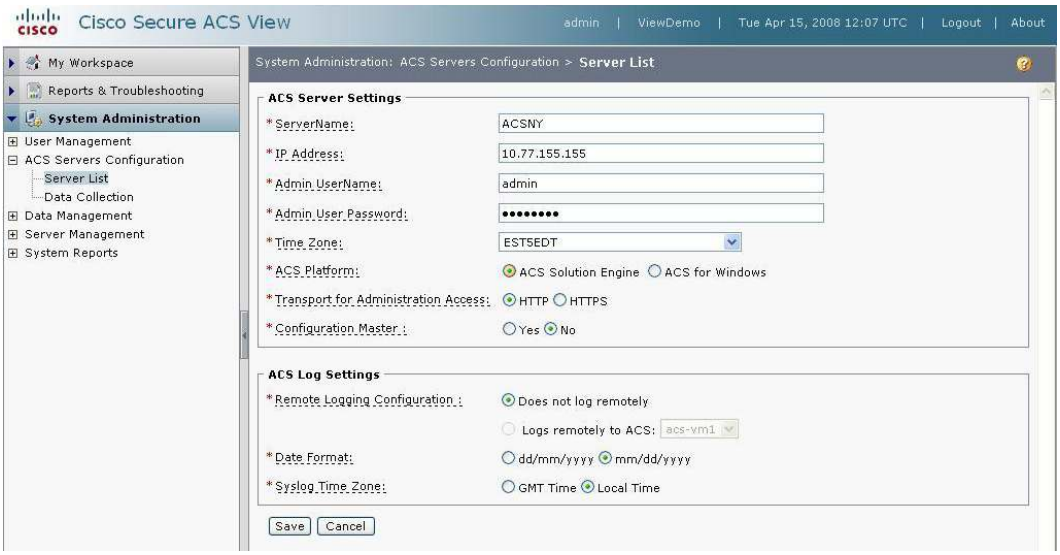
- **Server Name**: Enter the name of the server.
- **IP Address**: Enter a valid IP address.
- **Admin Username**: Enter the valid username.
- **Admin User Password**: Enter the valid credentials.
- **Time Zone**: Based on the ACS geographical location, you must enter the appropriate time zone of the ACS.
- **ACS platform**: Specify **ACS Appliance** or **ACS Software** edition.
- **Transport Access mode**: HTTP/HTTPS
- **Configuration Master**: Click **No**, because this server is not the configuration master. ACS View pulls configuration data only from the ACS configured as the configuration master in ACS View.
- **Remote Logging Configuration**: Choose **Logs Remotely to ACS** and choose the remote logging server from the drop-down list (ACSCHC If the logs are redirected to a remote logging server).
- **Date Format**: Specify the date format of the ACS.
- **Syslog Time Zone**: **Local** or **GMT**.

Click **Save** to finish adding the server.

Similarly, add the ACS in New York to the server list. This server is an ACS-SE enabled with syslog logging to the ACS View server.

Figure 8 shows how to add the NY server to ACS View.

Figure 8. Adding the NY Server to ACS View



Enter the following:

- **Server Name**: Enter the name of the server.
- **IP Address**: Enter a valid IP address.
- **Admin Username**: Enter the valid username.
- **Admin User Password**: Enter the valid credentials.
- **Time Zone**: Based on ACS geographical location, you must enter the appropriate time zone of the ACS.
- **ACS platform**: Specify **ACS Appliance**.
- **Transport Access mode**: HTTP/HTTPS
- **Configuration Master**: Click **No**, because this server is not the configuration master. ACS View pulls configuration data only from the ACS configured as the configuration master in ACS View.
- **Remote Logging Configuration**: Choose **Does not log remotely** if the logs are stored locally.
- **Date Format**: Specify the date format of the ACS.
- **Syslog Time Zone**: **Local** or **GMT**.

Enabling and Scheduling Data Collection

ACS View collects the syslog messages from ACS that you register with it. ACS View collects the following data from ACS:

- Log data by using syslog, which is the primary mechanism for data retrieval.
- Log and configuration data through *package.cab* downloads, which occur over HTTP/HTTPS.

Log data refers to information related to the functioning of ACS, such as starting or stopping of the server, requests to the server, and internal events. Some of the events that the ACS logs capture are failed attempts, passed authentication, RADIUS accounting, and TACACS+ accounting.

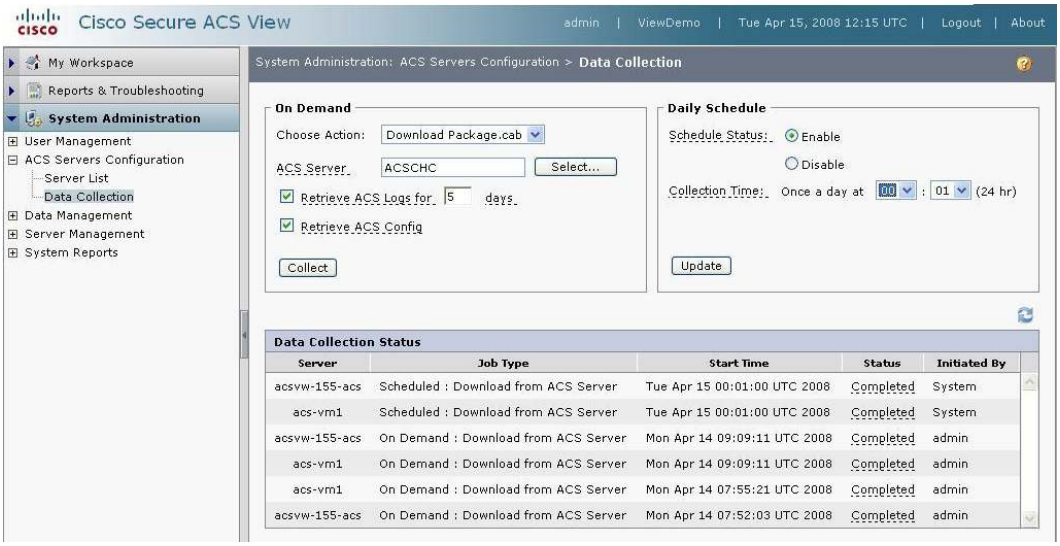
Configuration data refers to the information about ACS configuration that ACS View retrieves from the ACS that you configure as the configuration master. Configuration data includes Network Access Profile (NAP), Network Access Device (NAD), Network Device Group (NDG), and information about ACS users and administrators.

You can redirect syslog messages from ACS to ACS View by configuring the syslog server in ACS. After you configure the syslog server on ACS, ACS View receives syslog messages and processes the data to generate various reports.

Note: ACS View accepts and processes syslog messages only from registered ACS(s). When you use the remote logging setup in ACS, ACS View processes syslog messages from the remote logging server alone. ACS View supports remote logging only in ACS Windows. Collecting logs from the remote agents is not supported.

Figure 9 shows the Data Collection page in ACS View.

Figure 9. Data Collection in ACS View



Note: For ACS View to receive syslog data from ACS, you must configure each log in the ACS to send syslog data to ACS View. To do this, provide the hostname or IP address of ACS View in the ACS web interface, as detailed in the *User Guide for Cisco Secure Access Control Server 4.1*.

ACS View retrieves missing log and configuration data through a *package.cab* download. ACS View downloads the *package.cab* file periodically from ACS and compiles all the required information. When you download *package.cab*, ACS View detects missing log messages and then synchronizes the data.

The *package.cab* download serves as a backup for syslog data in the event of loss of data because of a network outage or when ACS View is inactive.

To download *package.cab*:

1. Log in to ACS View.
2. Choose **System Administration > ACS Servers Configuration > Data Collection**.
   - Choose **Download package.cab**.

- Choose the appropriate ACS name.
- Choose ACS Logs and ACS Config if you want both log and configuration data from ACS, and choose the number of days.
- Click **Collect**.

You can schedule the *package.cab* file download; by default this is scheduled at 12:01 a.m.

ACS View syslog collector processes the logs retrieved from the registered and licensed ACS list. Syslog data received from any other ACS will be dropped, and the information will be logged.

Note: ACS View will poll the ACS server every day to retrieve the *package.cab* file and parse it to retrieve the needed configuration data. From ACS 4.1.3, the ACS processes are brought down during the creation of the *package.cab*, since the *package.cab* also includes service logs. ACS 4.1.4 provides an option to exclude the inclusion of the service logs in *package.cab*, which will avoid the ACS processes restart.

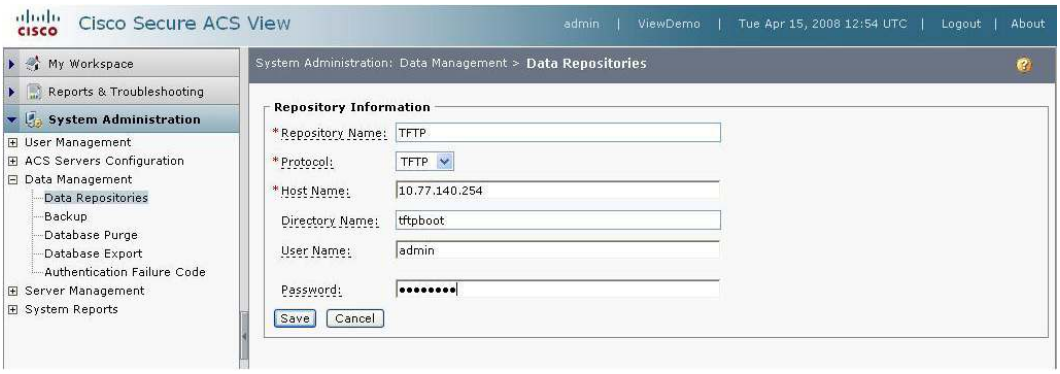
Backup and Restore

The Backup and Restore page in ACS View allows you to schedule ACS data backup to an external repository. ACS View backup and restore options are available as part of the CLI utilities. ACS View provides an option to administrators to schedule this backup through the UI. The default schedule will be daily at 12:00 a.m. The configurable options are daily, weekly, and monthly, along with other details like time, day, and date to run, as appropriate.

ACS View backup data includes the database files, log files related to the database and configuration files, scheduled reports, related data, and so on. You can configure a repository using the UI or the CLI.

Figure 10 shows the Data Repositories page in ACS View.

Figure 10. Data Repositories



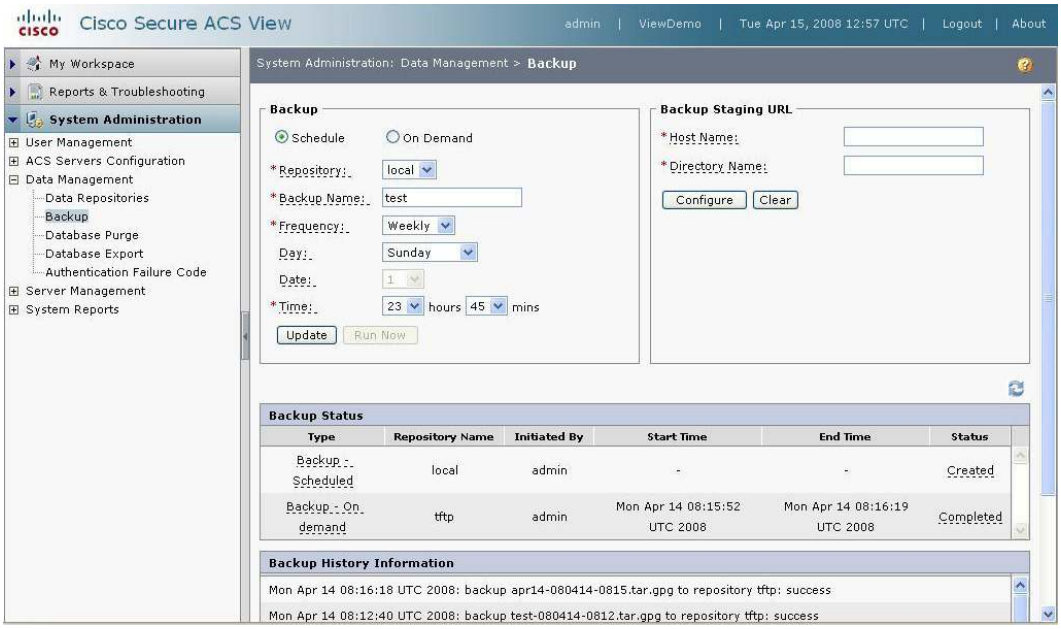
The data repository is a location where you can back up your files as well as from where you can restore your files. For application/patch installation as well as backup processes, you must create:

- **Local repository:** Use a local disk or insert the CD-Rom in your machine and then get the required information from the media or the CD-ROM directory.
- **Remote repository:** Using FTP, SFTP, TFTP, or NFS protocols.

ACS View administrators can schedule this backup through the GUI. The configurable options are daily, weekly, and monthly, including other details like time, day and date. You can initiate a backup either through the GUI or the CLI and restore only through the CLI. You can schedule a backup only from the GUI.

Figure 11 shows the data backup page in ACS View.

Figure 11. Data Backup



Note: You can initiate backup either through the GUI or the CLI and restore only through the CLI. You can schedule a backup only from the GUI. Restore is a manual operation, and it overwrites the existing data with the backed up data. Restore can be done to the same server or a different server, but you must change the system configuration using the CLI if it is restored to a different server.

Handling Different Time Zones

ACS View generates reports based on data collected from multiple ACSs in different time zones. The time zone information of each ACS will also be obtained as a user input, while adding the ACS to the server list.

ACS View automatically converts the time stamp of the data received from different ACS(s) to GMT and stores it to the database. All the data used to generate reports and alerts is based on the GMT time stamp.

Operations based on ACS data like reports and alerts are in GMT time zone.

Operations based on ACS View system jobs, such as system reports, are in ACS View server local time zone.

ACS View Server Performance

When all the ACS View components are running at peak, the average CPU usage of ACS View should be within 60 percent. The average memory usage at any point of time should be within 40 percent to 60 percent.

The guidelines and performance analysis show that each ACS View server can handle 25 events per second in normal traffic conditions and 100 to 200 events per second in burst traffic conditions for any 3 to 5 hours from multiple servers with very minimal syslog drops.

Online Storage Space

The ACS View appliance is bundled with a 500-GB hard disk and with Sybase version 10 as a built-in database. The database size can grow anywhere between 0.5 GB to 1.5 GB per day based on the incoming events per second and the size of the packet.

The recommended *package.cab* file upload or download values to ACS View are 50 MB per instance.

While generating *package.cab*, make sure to:

- Exclude service logs
- Restrict the log data collection date range to fewer days

Note: If the *package.cab* file is large, the upload and extraction time will be longer. ACS View pulls configuration data only from the ACS that is configured as the configuration master in ACS View.

The number of ACS(s) supported is aligned with the number of events per second. The performance benchmarking is done with 10 to 12 ACS(s) in place, and it is the recommended number of ACS(s) against one ACS View server.

You must get separate ACS View appliances to support a higher number of ACS(s) than this number. These ACS View servers will manage data from a different set of ACS. They will not interact or share data with each other in the current release of ACS View 4.0.

Redundancy

- The logs retrieved through *package.cab* download serve as a backup for syslog data lost because of network issues or when ACS View is down or not reachable.
- Automatically synchronize servers for missing data. When ACS View restarts after a downtime, a startup job automatically retrieves the missing data from one or more ACS(s) and updates the ACS View database.
- Backup Restore function. Restore can be done to the same server or a different server but requires change in the system configuration, such as the IP address, in the CLI.

Integrating ACS View with WCS

The Cisco Wireless Control System is a Cisco Unified Wireless Network Solution management tool that adds to the capabilities of the web user interface and CLI, moving from individual controllers to a network of controllers. WCS includes the same configuration, performance monitoring, security, fault management, and accounting options used at the controller level and adds a graphical view of multiple controllers and managed access points.

WCS runs on Windows 2003 and Red Hat Enterprise Linux ES 5.1. On both Windows and Linux, WCS can run as a normal application or as a service, which runs continuously and resumes running after a reboot.

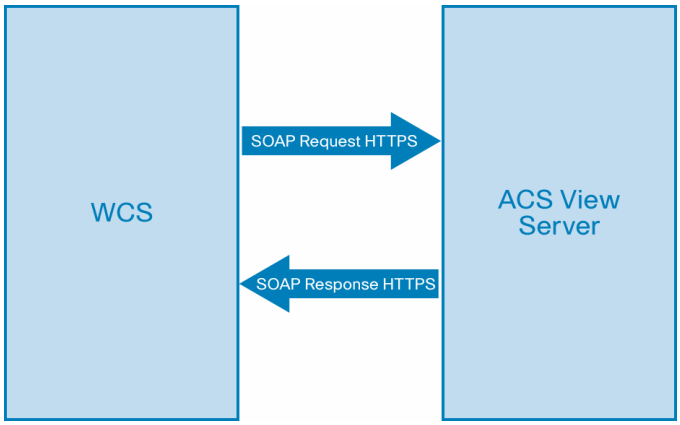
The WCS user interface helps enable operators to control all permitted Cisco Unified Wireless Network Solution configuration, monitoring, and control functions through Internet Explorer 6.0 or later.

Operator permissions are defined by the administrator using the WCS user interface Administration menu, which lets the administrator manage user accounts and schedule periodic maintenance tasks. WCS simplifies controller configuration and monitoring while reducing data entry errors. WCS uses the industry-standard Simple Network Management Protocol (SNMP) to communicate with the controllers.

WCS 5.1 is integrated with ACS View to retrieve the ACS data stored in ACS View. It uses secure HTTPS transport to transfer the data in XML with Simple Object Access Protocol (SOAP) encoding between WCS and ACS View. The ACS View server provides WCS with aggregated client status information from multiple ACS. The client status information allows you to further troubleshoot client issues and determine whether they are related to authentication or authorization.

Figure 12 shows ACS View with WCS integration.

Figure 12. WCS Integration



Configuring ACS View Server in WCS

To facilitate communication between WCS and the ACS View server and to access the ACS View Server tab, you must add an ACS View server to WCS, with credentials. Follow these steps to configure the ACS View server credentials.

1. Choose **Configure > ACS View Server**.
2. Enter the port number of the ACS View server you are adding. (Some ACS View servers do not allow you to change the port on which HTTPS runs.)
3. Enter the password that was established on the ACS View server.
4. Confirm the password.
5. Specify the time in seconds after which the authentication request times out and a retransmission is attempted by the controller.
6. Specify the number of retries that will be attempted.
7. Click **Submit**.

An example for the message flow:

- WCS sends MAC address of client, along with the date and time ranges.
- ACS View server will respond back with all the authentication and authorization status it has for that client, within the specified range.

Refer to the *WCS Configuration Guide* for more information.

More Information about ACS View

Detailed information about ACS View 4.0 is available on Cisco.com.

For product information, go to: http://www.cisco.com/en/US/products/ps9302/index.html.

For the *User Guide for Cisco Secure Access Control Server View 4.0*, go to: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_view/4.0/user/guide/UserGuide40.html.

ACS View support alias: cs-ciscosecure@cisco.com.

Appendix

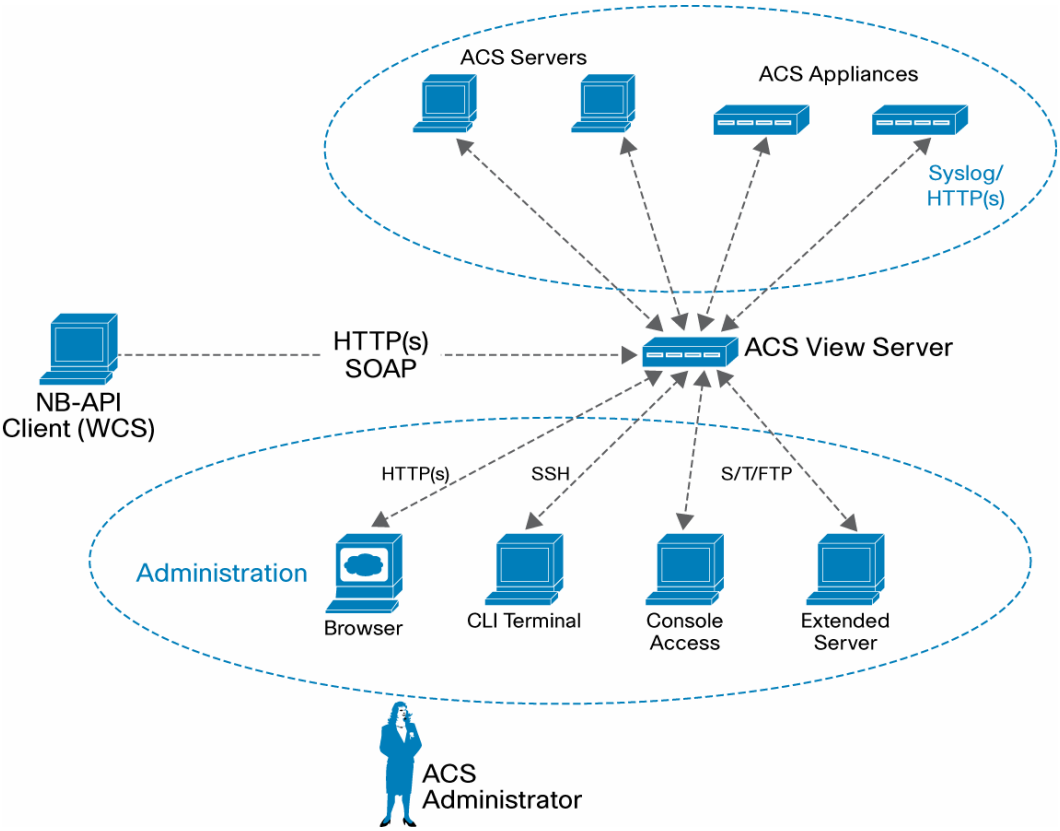
ACS View GUI

ACS View provides a web interface to generate or schedule reports, configure alerts, and perform various administrative tasks. Access to the ACS View server through the browser session will only be over HTTPS. HTTP access will be disabled. Administration and configuration of ACS View can also be done remotely over HTTPS using a web browser.

ACS View uses a self-signed certificate for SSL communication between the client and the ACS View server.

Figure 13 shows the ACS View external interface.

Figure 13. ACS View External Interface



You can do the following administrative tasks in ACS View using the GUI:

- Add users and configure password policies
- Add licenses and ACS
- Generate reports
- Configure data purging
- Configure data collection and backup schedule
- Update the self-signed certificate information using the Certificate Setup page
- Perform debugging and troubleshooting

CLI Operations

- Backup, restore, and repository configurations
- Option to view the processes status and stop/start ACS View processes/system
- Patch Installation: Allows the administrator to download the patches for ACS View and install the same in the ACS View server. You must restart the server from the CLI after the patch installation.

Table 3 lists the tasks that you can do using the GUI or CLI of ACS View.

Table 3. Tasks in ACS View

Feature	UI	CLI
Repository configuration	X	X
Backup – schedulable	X	
Backup – on demand	X	X
Restore		X
Data Purging – on demand	X	
Data Purging – automatic	X	
Database Export	X	
Import – ACS log/config data	X	
Licensing – add licenses	X	
ACS Server List	X	
Certificates – generate/update self-signed certs	X	
Application restart	X	X
Application status: CPU, memory, process status, etc.	X	X
User Management	X	X
User Preferences	X	
Password Policies	X	X
Application logging	X	
Patch Management		X
Export – ACS log/config data	X	
Data Collection	X	
ACS Reports	X	
ACS View Reports	X	
Report Inbox, report scheduling, favorite queries	X	
Dashboard	X	
Alerts	X	
System Settings	X	

Reports in ACS View

Reports form the core part of the ACS View functionality. ACS View identifies the report categories as system and custom reports. Based on the type of report, it categorizes the reports appropriately under each category.

This section provides you an overview of the various types of reports available in ACS View.

System Reports

ACS View has a set of predefined system reports for the following categories:

- Authentication reports
  - **Authentication Summary and Authentication Detail reports:** Analyze the passed, failed, and total attempts in terms of count and percentage for the ACS, users, user groups, NAD, NDG, or NAP. Also, average and peak response time of authentication is available for each record in the report. Details are available on the failed authentication's count and percentage, and failure of authentication generates a Failed Authentication report.
  - **Failed Authentication:** Analyzes the root cause for the increased number of failed authentications, with the help of message types, and the issues with the device. This report is displayed as a pie chart with a specific amount of data for users, user groups, NADs, NDGs, NAPs, message types, and failure codes.
- Session traffic reports
  - **RADIUS Session Summary:** Analyzes the session information (duration and throughput) in a device or in one or more ACS for a specific duration for RADIUS protocol–based traffic. The report can be viewed based on the Report On parameters such as the user, user group, ACSs, NAP, device, NDGs, and NAPs.
  - **TACACS+ Session Summary:** Analyzes the session information (duration and throughput) in a device or in one or more ACS for a specific duration for TACACS+ protocol–based traffic.
  - **Abnormal Activity Summary:** Lists all the abnormal activities that occurred within the time that you specify. This report provides tabular representations of sessions during off hours.
  - **Inactivity Summary:** Identifies the inactive entities (user, user group, NAD, NDG, or AAA server) of the deployment, based on the Report On query parameter. It displays information such as the user, user group, NAD, NDG, or ACS with the number of inactive days that is equal to the threshold value that you entered.
- Device administration reports
  - **User Summary:** Displays your device administration activities. This tabular report contains the list of commands the user has executed to administer the device and the time stamp to audit activities.
  - **Failed Commands:** Shows the list of failed commands that you executed in the device and the reasons for failure. It is used to analyze the reason and the commands with respect to your privilege levels.
- ACS configuration reports
  - **User Status:** Displays the user account status, such as Active, Expire, or Disabled, the last password change, and the activity time stamp for the user. It appears as a tabular report based on the query parameters such as ACS, user group, and user and account status.
  - **User Entitlement:** Displays the user access rights and your profile information like NAP, NAR, DCS, and network access permission.
  - **Network Client Summary:** Shows the list of AAA clients and NDGs and their respective

configurations in a tabular format based on the ACS.

- **Password Changes:** Analyzes the password change command that you executed on the device with a time stamp for the devices.
- **NAP Summary:** Lists all the NAPs available in the ACS, and each record would contain the NAP profile information such as selection rules, protocol settings, authentication and authorization rules, and their respective status.

- ACS administration reports
  - **Administrator Status:** Lists the administrators available for the ACS, the status (active or locked), the last password change, and the activity time stamp for the user.
  - **Administrator Entitlement:** Summarizes the access rights for the administrators available for the ACS. It is a tabular report that contains the administrator name and status and the rights to access network resources such as group permissions, shared profile components, network configuration, and system configuration.
  - **Administrative Audit:** Identifies the actions or configurations performed on the ACS by the administrator. If the ACS performance or functionality is affected, the administrator can use this tabular report to identify the reason and can revert to the configuration as well as the action performed.
  - **Backup and Restore:** Identifies the status of the backup and restore, such as Manual or Scheduled, and its status (Success or Failed).
  - **Replication:** Identifies the status of the database replication, such as Manual or Scheduled, with respect to the ACS.
  - **Service Status:** Shows the status of the system that has the ACS running and the status of each service associated with this ACS. It contains the memory usage, CPU usage, thread, and handle count for each process of an ACS with the corresponding time stamp.
- Troubleshooting reports
  - **Authentication Query:** Searches the user authentication status by using the query options available. You can get the authentication status from the displayed user list, or you can directly enter the user name and get the authentication status of the particular user.
  - **Connect to ACS:** This troubleshooting report is required to check the connectivity to the ACS and to download the *package.cab* file to the client machine. ACS View offers connectivity tests to check the ping, traceroute, and NFS lookup status.

Custom Reports

Custom reports, which are also called the ad hoc reports, are reports you design dynamically, to suit your needs. You can save a custom report in the My Reports folder. The reports saved in the My Reports folder are available only to the user who created them. You can also save these reports in the public folder, and these are available for all users.

ACS View provides tabular, graphical, and chart type reports.

The tabular reports allow you to do pagination, filter one or more columns, navigate between pages, sort data in multiple columns, view more details on the report output, and group the records based on the column value. You can also export these reports in both PDF and CSV formats.

Apart from the above-mentioned advantages, the graph options or types are available to the reports or report category to allow inclusion of charts or graphs. Using the interactive viewer, you

can change chart titles as well as axis titles in these charts.

Alerts in ACS View

Alerts are critical conditions or rules that you define to monitor, based on a threshold configuration, on a set of data collected from ACS. Alerts are checked by performance of periodic polling mechanisms based on the type of alert.

ACS View alerts are classified into two categories:

- **Alerts based on ACS data:** These are the alerts defined on the logs collected from ACS. Threshold conditions for the triggers are defined on the data set that is retrieved from ACS through syslog. When the threshold condition is met, an alert is triggered, and it appears in the Alert Inbox.

  There are various trigger conditions set for each alert category.

  - Time-based (passed or failed authentications, authentication inactivity)
  - Content-based (TACACS+ command audit, ACS administration audit)
  - Action-based (ACS backup or restore, replication, service stopped or restarted)
- **ACS View System Alerts:** ACS View system alerts are immediate and trigger-based. They contain information on the ACS View system. Triggers are the user-defined threshold conditions that serve as the basis on which alerts are generated.

The various parameters required for defining threshold conditions are provided in the GUI. The parameters vary for different types of alerts:

- For ACS data-based alerts, the threshold conditions can be defined by the administrators by modifying or updating the values of the predefined trigger condition list.
- ACS View system alerts will be generated based on the built-in threshold or error conditions. When the trigger condition is met, the ACS View alert engine generates an alert. You are notified through:
  - **Alert Inbox:** When an alert is generated, it appears in the inbox of all the users (both administrators and operators). When the user deletes an alert from the inbox, it will be deleted only from that user's inbox and still remains in other users' inboxes.
  - **Dashboard:** Lists a summary of the most recent five alerts in the user's inbox.
  - **E-mail:** If you specify your email address when you define a threshold in ACS View, ACS View sends an email notification when it generates an alert. It contains a comma-separated list. For ACS View system alerts, you can specify email addresses in the System Settings page. Alert triggers can be created, edited, and modified only by an administrator. An operator can only view the triggers defined and generated in the Alerts Inbox.

ACS View system alerts include data on:

- CPU, RAM utilization, and disk space
- The *package.cab* download issues
- Missing log fields in ACS logs, syslogs received from unregistered ACS

ACS View supports syslog-based alerts and not CSV-based alerts.

ACS View Database

Sybase is the internal database for ACS View server. The data retrieved from multiple ACS are processed and stored in the ACS View internal database.

Note: ACS View with external database is currently not supported; support for the same is in the roadmap.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C07-484555-00 07/08