# Configuring System Operations

You can configure and deploy ACS instances so that one ACS instance becomes the *primary instance* and the other ACS instances can be registered to the primary as *secondary instances*. An ACS instance represents ACS software that runs on a network.

An ACS deployment may consist of a single instance, or multiple instances deployed in a distributed manner, where all instances in a system are managed centrally. All instances in a system will have an identical configuration.

Use the Distributed System Management page **(System Administration > Operations > Distributed System Management)** to manage all the instances in a deployment. You can only manage instances from the primary instance. You can invoke the Deployment Operations page from any instance in the deployment, but it only controls the operations on the local server.

**Note** You can register any primary instance or any secondary instance to another primary instance; however, the primary instance you wish to register cannot have any secondary instances registered to it.

The primary instance, created as part of the installation process, centralizes the configuration of the registered secondary instances. Configuration changes made in the primary instance are automatically replicated to the secondary instance. You can force a *full replication* to the secondary instance if configuration changes do not replicate to the secondary instance.

This chapter contains:


- Understanding Distributed Deployment, page 17-2
- Scheduled Backups, page 17-6
- Synchronizing Primary and Secondary Instances After Backup and Restore, page 17-9
- Editing Instances, page 17-10
- Activating a Secondary Instance, page 17-15
- Registering a Secondary Instance to a Primary Instance, page 17-16
- Deregistering Secondary Instances from the Distributed System Management Page, page 17-19
- Deregistering a Secondary Instance from the Deployment Operations Page, page 17-19
- Changing the IP address of a Primary Instance from the Primary Server, page 17-23
- Failover, page 17-23
- Promoting a Secondary Instance from the Distributed System Management Page, page 17-20
- Replicating a Secondary Instance from a Primary Instance, page 17-21

- Creating, Duplicating, Editing, and Deleting Software Repositories, page 17-25
- Managing Software Repositories from the Web Interface and CLI, page 17-26
- Configuring RSA Public Key for Authentication against SFTP Repositories, page 17-27
- Exporting Policies from ACS Web Interface, page 17-30
- Trust Communication in a Distributed Deployment, page 17-31


# Understanding Distributed Deployment

You can configure multiple ACS servers in a deployment. Within any deployment, you designate one server as the *primary* server and all the other servers are *secondary* servers.

In general, you make configuration changes on the primary server only, and the changes are propagated to all secondary servers, which can then view the configuration data as read-only data. A small number of configuration changes can be performed on a secondary server, including configuration of the server certificate, and these changes remain local to the server.

There is no communication between the secondary servers. Communication happens only between the primary server and the secondary servers. The secondary servers do not know the status of the other secondaries in their deployment.

ACS allows you to deploy an ACS instance behind a firewall. Table 17-1 lists the ports that must be open on the firewall for you to access ACS through the various management interfaces.

***Table 17-1 Ports to Open in Firewalls***

| Process | Port |
|---|---|
| ACS Web Interface/Web Service | 443 |
| Database replication | TCP 2638 |
| RADIUS server | • 1812 and 1645 (RADIUS authentication and authorization)<br>• 1813 and 1646 (RADIUS accounting)<br>• 3799 (RADIUS COA and POD listen for proxy purpose)<br>If your RADIUS server uses port 1812, ensure that your PIX firewall software is version 6.0 or later. Then, run the following command to use port 1812:<br>**aaa-server radius-authport** *1812* |
| Replication over the Message Bus | TCP 61616 |
| RMI | TCP 2020 (for RMI registry service) |
| | TCP 2030 (for incoming calls) |
| SNMP (for request) | UDP 161 |
| SNMP (for notifications) | UDP 162 |
| SSH | 22 |
| TACACS+ server | TCP 49 or the port numbers that are configured on TACACS+ Port to listen (1024 to 65535). |

*Table 17-1 Ports to Open in Firewalls*

| Process | Port |
|---|---|
| ACS View Collector | UDP 20514 |
| ACS View net flow syslog processing | UDP 9993 |

The ports that are displayed as a listening port on 127.0.0.1 are not listed in the above table. These ports are not accessible outside ACS instance.

The Distributed System Management page can be used to monitor the status of the servers in a deployment and perform operations on the servers.

ACS 5.8.1 supports one primary and twenty one secondary ACS instances in a large ACS deployment. You can make one secondary instance as a dedicated hot standby secondary instance which can be promoted as a primary instance when the actual primary instance goes down. The medium ACS deployment consists of one primary and thirteen secondary ACS instances. Similarly, you can make one secondary instance as a dedicated hot standby secondary instance which can be promoted as a primary instance when the actual primary instance goes down. Also, all ACS 5.8.1 deployments supports 150,000 AAA clients, 10,350 network device groups, 400,000 users, and 200,000 hosts. ACS 5.8.1 log collector server can handle 2 million records per day and 750 messages per second for stress that are sent from various ACS nodes in the deployment to the log collector server.For more information on ACS server deployments, see *Installation and Upgrade Guide for Cisco Secure Access Control System 5.8.1*.

In a distributed deployment, if you want to use an administrator account whose password hashing option is enabled to add an ACS instance as a secondary instance to the deployment, then you must enable trust communication between ACS instances in the deployment. For information on Trust Communication, see Trust Communication in a Distributed Deployment, page 17-31.

**Note** ACS 5.8.1 does not support the large deployment with more than twenty two ACS instances.

**Related Topics**

- Activating Secondary Servers, page 17-3
- Removing Secondary Servers, page 17-4
- Promoting a Secondary Server, page 17-4
- Understanding Local Mode, page 17-4
- Understanding Full Replication, page 17-5
- Specifying a Hardware Replacement, page 17-6

# Activating Secondary Servers

To add a server to a deployment:

**Step 1** From the secondary server, issue a request to register on the primary server by selecting the Deployment Operations option.

**Step 2** Activate the secondary instance on the primary server.

You must activate the secondary instance on the primary instance in order for the secondary instance to receive configuration information; this provides a mechanism of admission control.

However, there is an option to automatically activate newly added secondary instances, rather than performing a manual activation request.

**Related Topics**

- Removing Secondary Servers, page 17-4
- Promoting a Secondary Server, page 17-4
- Understanding Local Mode, page 17-4
- Understanding Full Replication, page 17-5
- Specifying a Hardware Replacement, page 17-6

# Removing Secondary Servers

To permanently remove a secondary server from a deployment, you must first deregister the secondary server and then delete it from the primary. You can make the request to deregister a server from either the secondary server to be deregistered or from the primary server.

**Related Topics**

- Activating Secondary Servers, page 17-3
- Understanding Distributed Deployment, page 17-2

# Promoting a Secondary Server

There can be one server only that is functioning as the primary server. However, you can promote a secondary server so that is assumes the primary role for all servers in the deployment. The promotion operation is performed either on the secondary server that is to assume the primary role or on the primary server.

**Note** When the primary server is down, do not simultaneously promote two secondary servers.

**Related Topics**

- Activating Secondary Servers, page 17-3
- Removing Secondary Servers, page 17-4
- Understanding Local Mode, page 17-4
- Understanding Full Replication, page 17-5

# Understanding Local Mode

You can use the local mode option:

- If the primary server is unreachable from a secondary server (for example, there is a network disconnection) and a configuration change must be made to a secondary server, you can specify that the secondary server go into *Local Mode*.
- If you want to perform some configuration changes on a trial basis that would apply to only one server and not impact all the servers in your deployment, you can specify that one of your secondary servers go into *Local Mode*.

In Local Mode, you can make changes to a single ACS instance through the local web interface, and the changes take effect on that instance only. The Configuration Audit Report available in the Monitoring and Report Viewer has an option to report only those configuration changes that were made in the local mode.

You can generate this report to record the changes that you made to the secondary server in Local Mode. For more information on reports and how to generate them from ACS, see Managing Reports, page 13-1.

When the connection to the primary server resumes, you can reconnect the disconnected secondary instance in Local Mode to the primary server. From the secondary instance in Local Mode, you specify the Admin username and password to reconnect to the primary instance. All configuration changes made while the secondary server was in Local Mode are lost.

**Related Topics**

- Activating Secondary Servers, page 17-3
- Understanding Full Replication, page 17-5

# Understanding Full Replication

Under normal circumstances, each configuration change is propagated to all secondary instances. Unlike ACS 4.x where full replication was performed, in ACS 5.8.1, only the specific changes are propagated. As configuration changes are performed, the administrator can monitor (on the Distributed System Management page) the status of the replication and the last replication ID to ensure the secondary server is up to date.

If configuration changes are not being replicated as expected, the administrator can request a full replication to the server. When you request full replication, the full set of configuration data is transferred to the secondary server to ensure the configuration data on the secondary server is re synchronized.

**Note** Replication on the Message Bus happens over TCP port 61616. Full replication happens over the Sybase DB TCP port 2638.

**Warning** **ACS management services are started even when a warning message is displayed as connection failed. The services do not get stuck in the initialization stage.**

**Related Topics**

- Activating Secondary Servers, page 17-3
- Promoting a Secondary Server, page 17-4
- Understanding Local Mode, page 17-4

## Specifying a Hardware Replacement

You can perform a hardware replacement to allow new or existing ACS instance hardware to re-register to a primary server and take over an existing configuration already present in the primary server. This is useful when an ACS instance fails and needs physical replacement.

To perform the hardware replacement

**Step 1** From the web interface of the primary instance, you must mark the server to be replaced as deregistered.

**Step 2** From the secondary server, register to the primary server.

In addition to the standard administrator credentials for connecting to the primary server (username/password), you must specify the replacement keyword used to identify the configuration in the primary server. The keyword is the hostname of the instance that is to be replaced.

**Step 3** You must activate the secondary server on the primary, either automatically or by issuing a manual request.

**Related Topics**


- Viewing and Editing a Primary Instance, page 17-10
- Viewing and Editing a Secondary Instance, page 17-14
- Activating a Secondary Instance, page 17-15
- Registering a Secondary Instance to a Primary Instance, page 17-16
- Deregistering Secondary Instances from the Distributed System Management Page, page 17-19
- Promoting a Secondary Instance from the Distributed System Management Page, page 17-20
- Using the Deployment Operations Page to Create a Local Mode Instance, page 17-24


# Scheduled Backups

You can schedule backups to be run at periodic intervals. You can schedule backups from the primary web interface. The Scheduled Backups feature backs up ACS configuration data. You can back up data from an earlier version of ACS and restore it to a later version.

Refer to the *Installation and Setup Guide for Cisco Secure Access Control System 5.8.1* for more information on upgrading ACS to later versions.

### ACS Backup Encryption

ACS backup is encrypted using a dynamic encryption password. The user is prompted for an encryption password while performing a backup operation. ACS encrypts only the ACS data using a dynamic encryption key. The CARS and ACS view data are encrypted using a static key. Therefore ACS prompts for an encryption password when you run a backup that contains ACS data. The user is prompted for a decryption password while restoring a backup that contains ACS data.

When you run a full backup in ACS, ACS uses the static key to encrypt the CARS and ACS data and makes a .gpg file; whereas the ACS backup data is saved inside this .gpg file as a separate .gpg file using the dynamic encryption password. When you restore the full backup, ACS prompts for the decryption password to decrypt the ACS backup data. ACS decrypts the CARS data and ACS view data using the static key.

The encryption password should have:

- A minimum of 8 characters
- Not more than 32 characters
- At least one upper case letter.
- At least one lower case letter.

Special characters are allowed except:

- `
- $
- (
- )

ACS displays the password policy if the entered password does not meet the password requirements.

**Note** ACS 5.8.1 does not support scheduled backups through the CLI.

**Related Topic**

Creating, Duplicating, and Editing Scheduled Backups, page 17-7

# Creating, Duplicating, and Editing Scheduled Backups

You can create a scheduled backup only for the primary instance. To create, duplicate, or edit a scheduled backup:

**Step 1** Choose **System Administration > Operations > Scheduled Backups**.

The Scheduled Backups page appears. Table 17-2 describes the fields listed in the Scheduled Backups page.

*Table 17-2 Scheduled Backups Page*

| Option | Description |
|---|---|
| **Backup Data** | |
| Filename created by backup includes a time stamp and file type information appended to the prefix entered | |
| Filename Prefix | Enter a filename prefix to which ACS appends the backup time stamp. For example, if you enter ACSBackup as the filename prefix and backup is run on June 05, 2009 at 20:37 hours, then ACS creates the backup file ACSBackup-090506-2037.tar.gpg.<br>**Note** In ACS web interface, you cannot configure utf-8 characters for a backup filename and a repository name. |
| Encryption Password | Enter a password to encrypt the ACS backup files. |
| Confirm Encryption Password | Re-enter the encryption password. |
| Repository | Click **Select** to open the Software Update and Backup Repositories dialog box, from which you can select the appropriate repository in which to store the backup file. |

*Table 17-2 Scheduled Backups Page (continued)*

| Option | Description |
|---|---|
| **Schedule Options** | |
| Time of Day | Choose the time of the day at which you want ACS to back up the ACS configuration data. Backups can be scheduled on a daily, weekly, or monthly basis.<br>• Daily—Choose this option for ACS to back up the ACS configuration data at the specified time every day.<br>• Weekly—Choose this option and specify the day of the week on which you want ACS to back up the ACS configuration data every week.<br>• Monthly—Choose this option and specify the day of the month on which you want ACS to back up the ACS configuration data every month. |

**Step 2** Click **Submit** to schedule the backup.

**Related Topic**

Backing Up Primary and Secondary Instances, page 17-8

# Backing Up Primary and Secondary Instances

ACS allows you to encrypt the backup with a password. The backup file encryption is available only for ACS configuration backup. The password-based encryption is not applicable if you choose to obtain only the ADE-OS configuration data backup from secondary ACS instances.

ACS provides you the option to back up the primary and secondary instances at any time apart from the regular scheduled backups. For a primary instance, you can back up the following:

- ACS configuration data only
- ACS configuration data and ADE-OS configuration data

For secondary instances, ACS only backs up the ADE-OS configuration data. In this case, ACS does not prompt for an encryption password.

To run an immediate backup from Distributed System Management page:

**Step 1** Choose **System Administration > Operations > Distributed System Management**.

The Distributed System Management page appears.

**Step 2** From the Primary Instance table or the Secondary Instances table, select the instance that you want to back up.

You can select only one primary instance, but many secondary instances for a backup.

**Step 3** Click **Backup**.

The Distributed System Management - Backup page appears with the fields described in Table 17-3.

*Table 17-3 Distributed System Management - Backup Page*

| Option | Description |
|---|---|
| **Backup Data** | |
| Filename created by backup includes a time stamp and file type information appended to the prefix entered | |
| Filename Prefix | Enter a filename prefix to which ACS appends the backup time stamp. For example, if you enter ACSBackup as the filename prefix and backup is run on June 05, 2009 at 20:37 hours, then ACS creates the backup file ACSBackup-090506-2037.tar.gpg.<br>**Note** In ACS web interface, you cannot configure utf-8 characters for a backup filename and a repository name. |
| Encryption Password | Enter the encryption password to encrypt the ACS backup files. |
| Confirm Encryption Password | Re-enter the encryption password which must match the encryption password exactly. |
| Repository | Click **Select** to open the Software Update and Backup Repositories dialog box, from which you can select the appropriate repository in which to store the backup file. |
| **Backup Options (only applicable for primary instances)** | |
| ACS Configuration Backup | Click this option if you want to back up only the ACS configuration data. |
| ACS Configuration and ADE-OS Backup | Click this option if you want to back up both the ACS configuration data and the ADE-OS configuration data. |

**Step 4** Click **Submit** to run the backup immediately.

To run an immediate backup from Deployment Operations page:

**Step 1** Choose **System Administration > Operations > Local Operations > Deployment Operations**.

The Deployment Operations page appears.

**Step 2** Click **Backup**.

The Deployment Operations - Backup page appears with the fields described in Table 17-3.

**Step 3** Modify the fields in Table 17-3 and click **Submit** to run the backup immediately.

**Related Topic**

Scheduled Backups, page 17-6

# Synchronizing Primary and Secondary Instances After Backup and Restore

When you specify that a system backup is restored on a primary instance, the secondary instance is not updated to the newly restored database that is present on the primary instance.

To make sure the secondary instance is updated, from the secondary instance, you need to request a hardware replacement to rejoin the restored primary instance. To do this:

**Step 1** Deregister the secondary instance from the primary instance.

**Step 2** From the web interface of the secondary instance, choose **Systems Administration > Operations > Local Operations > Deployment Operations**, then click **Deregister from Primary**.

**Step 3** Choose **Systems Administration > Operations > Local Operations > Deployment Operations**.

This allows you to perform the hardware replacement of the secondary instance to the primary instance again.

**Step 4** Specify the primary hostname or IP address and the administrator credential.

**Step 5** Select **Hardware Replacement** and specify the hostname of the secondary instance.

**Step 6** Click **Register to Primary**.

# Editing Instances

When you Choose **System Administration > Operations > Distributed System Management**, you can edit either the primary or secondary instance. You can take a backup of primary and secondary instances. The Distributed System Management page allows you to do the following:

- Viewing and Editing a Primary Instance, page 17-10
- Viewing and Editing a Secondary Instance, page 17-14
- Backing Up Primary and Secondary Instances, page 17-8
- Synchronizing Primary and Secondary Instances After Backup and Restore, page 17-9

# Viewing and Editing a Primary Instance

To edit a primary instance:

**Step 1** Choose **System Administration > Operations > Distributed System Management**.

The Distributed System Management page appears with two tables:

- Primary Instance table—Shows the primary instance.

  The primary instance is created as part of the installation process.

- Secondary Instances table—Shows a listing and the status of the secondary instances. See Viewing and Editing a Secondary Instance, page 17-14 for more information.

  The Distributed System Management Page displays the information described in Table 17-4:

*Table 17-4 Distributed System Management Page*

| Option | Description |
|---|---|
| **Primary Instance** | |
| Name | Hostname of the primary instance. |

*Table 17-4 Distributed System Management Page (continued)*

| Option | Description |
|---|---|
| IP Address | IP address of the primary instance. |
| Online Status | Indicates if the primary instance is online or offline. A check mark indicates that the primary instance is online; **x** indicates that the primary instance is offline. |
| Replication ID | The transaction ID that identifies the last configuration change on the primary instance. This value increases by 1 for every configuration change. Valid values are 1 to infinity. |
| Role | Displays the role of the primary instance. If a primary ACS instance is set as a log collector server, the role is displayed as Primary: Log Collector. |
| Last Update | Time stamp of the last database configuration change. The time stamp is in the form *hh:mm dd:mm:yyyy*. |
| Version | Current version of the ACS software running on the primary ACS instance. Valid values can be the version string or, if a software upgrade is initiated, *Upgrade in progress*. |
| Description | Description of the primary instance. |
| Edit | Select the primary instance and click this button to edit the primary instance. |
| Backup | Select the primary instance and click this button to back up the primary instance. See Backing Up Primary and Secondary Instances, page 17-8 for more information. |
| **Secondary Instances** | |
| Name | Hostname of the secondary instance. |
| IP Address | IP address of the secondary instance. |
| Online Status | Indicates if the secondary instance is online or offline. A check mark indicates that the secondary instance is online; **x** indicates that the secondary instance is offline. |
| Replication ID | The transaction ID that identifies the last configuration change which is received on a secondary instance from a primary instance. This value increases by 1 for every configuration change. Valid values are 1 to infinity. This number must be the same as the Replication ID in the Primary Instance for the primary and secondary ACS servers to be in sync. |
| Role | Displays the role of the secondary instance. If a secondary ACS instance is set as a log collector server, the role is displayed as Secondary: Log Collector. |
| Replication Status | Replication status values are:<br>• UPDATED—Replication is complete on the secondary instance. Both Management and Runtime services are current with configuration changes from the primary instance.<br>• PENDING—Request for full replication has been initiated or the configuration changes made on the primary have not yet been propagated to the secondary.<br>• REPLICATING—Replication from the primary to the secondary is processing.<br>• LOCAL MODE—The secondary instance does not receive replication updates from the deployment and maintains its own local configuration.<br>• DEREGISTERED—The secondary instance is deregistered from the primary instance and is not part of the deployment.<br>• INACTIVE—The secondary instance is inactive. You must select this instance and click **Activate** to activate this instance.<br>• **—The communication between the primary instance and the secondary instance is not available now. You need to log in to the specific ACS instance to view the required information. |
| Replication Time | Time stamp of the last replication. The time stamp is in the form *hh:mm dd:mm:yyyy*. |

*Table 17-4 Distributed System Management Page (continued)*

| Option | Description |
|---|---|
| Version | Current version of the ACS software running on the secondary ACS instance. Valid values can be the version string or, if a software upgrade is initiated, *Upgrade in progress*. |
| Description | Description of the secondary instance. |
| Edit | Select the secondary instance that you want to edit and click this button to edit it. |
| Delete | Select the secondary instance that you want to delete and click this button to delete it. |
| Activate | If the option to auto-activate the newly registered secondary instance is disabled, the secondary is initially placed in the inactive state. Click **Activate** to activate these inactive secondary instances. |
| Deregister[1] | Disconnects the secondary instance from the primary instance. Stops the secondary instance from receiving configuration updates from the primary instance. Deregistration restarts the deregistered node.<br>When full replication is in progress on an instance, do not attempt to deregister that instance. Wait until the full replication is complete and the secondary instance is restarted before you deregister the secondary instance. |
| Promote | Requests to promote a secondary instance to the primary instance. All updates to the current primary instance are stopped so that all replication updates can complete. The secondary instance gets primary control of the configuration when the replication updates complete.<br>The secondary instance must be active before you can promote it to the primary instance. |
| Full Replication | Replicates the primary instance's database configuration for the secondary instance. ACS is restarted.<br>When full replication is in progress on an instance, do not attempt to deregister that instance. Wait until the full replication is complete and the secondary instance is restarted before you deregister the secondary instance. |
| Backup | Select the secondary instance that you want to back up and click this button to take a backup. See Backing Up Primary and Secondary Instances, page 17-8 for more information. |
| Refresh | Click to refresh the Distributed System Management page manually. |
| Refresh Interval | Select the time interval in seconds for the Distributed System Management page to be refreshed automatically. The default value is 30 seconds. The available options are No Refresh, 15 seconds, 30 seconds, and 60 seconds.<br>If you select:<br>• No Refresh—ACS does not refresh the Distributed System Management page automatically. You must click **Refresh** to refresh the page manually.<br>• 15 seconds—ACS refreshes the Distributed System Management page for every 15 seconds.<br>• 30 seconds—ACS refreshes the Distributed System Management page every for 30 seconds.<br>• 60 seconds—ACS refreshes the Distributed System Management page every for 60 seconds.<br>The selected interval works only when you are in the Distributed System Management page. If you navigate to any other page, ACS resets the refresh interval to its default value.<br>**Note** The refresh interval does not work when you delete a deregistered secondary instance or instances from the Distributed System Management page. |

1. Deregistration restarts the deregistered node, but does not restart ACS. Registration and Full Replication restart ACS because the database is replaced.

**Note** ACS displays two asterisks "**" in a column when that particular ACS instance information is unavailable. The two asterisks indicate that the communication is not available and you need to log in to that particular ACS instance to view the required information.

**Note** You will not have session time-outs if you are on the Distributed System Management Page as the page is refreshed automatically at regular intervals.

**Step 1** From the Primary Instance table, click the primary instance that you want to modify, or check the **Name** check box and click **Edit**.

**Step 2** Complete the fields in the Distributed System Management Properties page as described in Table 17-5:

*Table 17-5 Distributed System Management Properties Page*

| Option | Description |
|---|---|
| **Instance Data** | |
| Hostname | Name of the ACS host machine. |
| Launch Session for Local GUI | Click this button to launch a new instance of the selected ACS machine. You are required to log in to the primary or secondary instance.<br>This option appears only when you view or edit another instance. |
| Role | Specifies a primary or secondary instance or Local. |
| IP Address | IP address of the primary or secondary instance. |
| Port | Port for Management service. |
| MAC Address | MAC address for the instance. |
| Description | Description of the primary or secondary instance. |
| Check Secondary Every (only applies for primary instance) | Rate at which the primary instance sends a heartbeat status request to the secondary instance. The default value is 60 seconds. The minimum value is 30 seconds and the maximum value is 30 minutes. |
| Statistics Polling Period (only applies for primary instance) | Rate at which the primary instance polls the secondary instance for statistical and logging information. During each polling period, the primary server does not send any query to all the secondary servers, but, all ACS servers send their health information to the log collector server. The minimum value is 60 seconds and the maximum value is 30 minutes. However, you can specify a value of 0 which indicates to turn off polling and logging. As a result, the log collector server does not show any health status. The default value is 60 seconds. |
| Enable Auto Activation for Newly Registered Instances (only applies for primary instance) | Check this check box to automatically activate the registered secondary instance. |
| **Instance Status** | |
| Status | Indicates if the primary instance or secondary instance is online or offline. |
| Version | The current version of the ACS software. |

*Table 17-5 Distributed System Management Properties Page (continued)*

| Option | Description |
|---|---|
| Replication Status (only applies for secondary instances) | Replication status values are:<br>• UPDATED—Replication is complete on ACS instance. Both management and runtime services are current with configuration changes from the primary instance.<br>• PENDING—Request for full replication has been initiated.<br>• REPLICATING—Replication from the primary to the secondary is processing.<br>• DEREGISTERED—Deregistered the secondary instance from the primary.<br>• N/A—No replication on primary instance. |
| Last Update Time (only applies for primary instance) | Time stamp of the last database configuration change. The time stamp is in the form *hh:mm dd:mm:yyyy*. |
| Last Replication Time (only applies for secondary instances) | Time stamp of the last replication. The time stamp is in the form *hh:mm dd:mm:yyyy*. |
| Last Replication ID (only applies for primary instance) | Transaction ID that identifies the last configuration change on the secondary instances. This value increases by 1 for every configuration change. Valid values are 1 to infinity. |
| Primary Replication ID (only applies for secondary instances) | Transaction ID that identifies the last configuration change on the primary instance. This value increases by 1 for every configuration change. Valid values are 1 to infinity. |

**Step 3** Click **Submit**.

The Primary Instance table on the Distributed System Management page appears with the edited primary instance.

**Related Topics**

- Replicating a Secondary Instance from a Primary Instance, page 17-21
- Viewing and Editing a Secondary Instance, page 17-14

# Viewing and Editing a Secondary Instance

To edit a secondary instance:

**Step 1** Choose **System Administration > Operations > Distributed System Management**.

The Distributed System Management page appears with two tables:

- Primary Instance table—Shows the primary instance.
- Secondary Instances table—Shows a listing and the status of the secondary instances registered to the primary instance.

See Table 17-4 to view column definitions.

**Step 2** From the Secondary Instances table, click the secondary instances that you want to modify, or check the check box near the secondary instances and click **Edit**.

**Step 3** Complete the fields in the Distributed System Management Properties page as described in Table 17-5.

**Step 4** Click **Submit**.

The Secondary Instances table on the Distributed System Management page appears with the edited secondary instance.

**Related Topics**

- Editing Instances, page 17-10
- Viewing and Editing a Primary Instance, page 17-10

## Deleting a Secondary Instance

To delete a secondary instance:

**Step 1** Choose **System Administration > Operations > Distributed System Management**.

The Secondary Instances table on the Distributed System Management page appears with a list of secondary instances.

**Step 2** Deregister the secondary instance you wish to delete. Refer to Deregistering Secondary Instances from the Distributed System Management Page, page 17-19.

**Step 3** Check one or more check boxes near the secondary instances that you want to delete.

**Step 4** Click **Delete**.

The following warning message appears:

```
Are you sure you want to continue deleting the selected instance(s)?
Please note that auto Refresh will be disabled during this operation.
```

**Step 5** Click **OK**.

The Secondary Instances table on the Distributed System Management page appears without the deleted secondary instances.

# Activating a Secondary Instance

To activate a secondary instance:

**Step 1** Choose **System Administration > Operations > Distributed System Management**.

The Distributed System Management page appears with two tables:

- Primary Instance table—Shows the primary instance.
- Secondary Instances table—Shows a listing and the status of the secondary instances registered to the primary instance.

See the Table 17-4 to view column descriptions.

**Step 2** From the Secondary Instances table, check the check box near the secondary instances that you want to activate.

**Step 3** Click **Activate**.

**Step 4** The Secondary Instances table on the Distributed System Management page appears with the activated secondary instance. See the Table 17-5 for valid field options.

**Related Topics**

- Viewing and Editing a Secondary Instance, page 17-14
- Deleting a Secondary Instance, page 17-15
- Replicating a Secondary Instance from a Primary Instance, page 17-21
- Registering a Secondary Instance to a Primary Instance, page 17-16
- Deregistering a Secondary Instance from the Deployment Operations Page, page 17-19
- Promoting a Secondary Instance from the Distributed System Management Page, page 17-20
- Using the Deployment Operations Page to Create a Local Mode Instance, page 17-24

# Registering a Secondary Instance to a Primary Instance

To register a secondary instance to a primary instance:

**Step 1** Log into the machine that will be used as a secondary Instance for another ACS server.

**Step 2** Choose **System Administration > Operations > Local Operations > Deployment Operations**.

The Deployment Operations page appears, displaying the information described in Table 17-6:

*Table 17-6 System Operations: Deployment Operations Page*

| Option | Description |
|---|---|
| **Instance Status** | |
| Current Status | Identifies the instance of the node you log into as primary or secondary, and identifies whether you are running in local mode. |
| Primary Instance | Hostname of the primary instance. |
| Primary IP | IP address of the primary instance. |
| **Registration (only active for an instance not running in Local Mode)** | |
| Primary Instance | Hostname of the primary server that you wish to register with the secondary instance. |
| Admin Username | Username of an administrator account. |
| Admin Password | Password for the administrator's account. |
| Hardware Replacement | Check to enable a new or existing ACS instance hardware to re-register to a primary instance and acquire the existing configuration already present in the primary instance. This is useful when an instance fails and needs physical replacement. |

*Table 17-6 System Operations: Deployment Operations Page (continued)*

| Option | Description |
|---|---|
| Recovery Keyword | Name of the instance that is to be replaced. This value is the hostname of the system that is being replaced. After you submit this information, this instance connects to the primary instance.<br>The primary instance finds the associated ACS instance records based on the keyword, and marks each record as registered. |
| Register to Primary | Connects to the remote primary and registers the secondary instance to the primary instance. |
| **Backup** | |
| Backup | Backs up the current instance. |
| **Local Mode** | |
| Admin Username | Username of an administrator account. |
| Admin Password | Password for the administrators account. |
| Reconnect<br>This option appears only on the local mode node and prompts you for credentials. | Click **Reconnect** to reconnect to the primary instance.<br>Once you reconnect to the primary instance, you lose the configuration changes that you have made to the local secondary instance.<br>If you want to retain the configuration changes that you have made to the local secondary instance, you must:<br>1. Deregister the local secondary instance (this instance would become your new primary)<br>2. Deregister all the instances from the deployment.<br>3. Register all the instances to the new primary, whose configuration changes you want to retain. |
| Request Local Mode<br>This option appears only on a registered secondary page. | Request to place the secondary instance in local mode. This enables administrators to make configuration changes only to this instance. Any changes made to the secondary instance are not automatically updated when you reconnect to the primary instance. You must manually enter your changes for the secondary instance. |

*Table 17-6 System Operations: Deployment Operations Page (continued)*

| Option | Description |
|---|---|
| **Deregistration** | |
| Deregister from Primary | Deregisters the secondary from the primary instance. The secondary instance retains the database configuration from when it was deregistered. All nodes are marked as deregistered and inactive, and the secondary instance becomes the primary instance.<br>When full replication is in progress on an instance, do not attempt to deregister that instance. Wait until the full replication is complete and the secondary instance is restarted before you deregister the secondary instance. |
| **Promotion** | |
| Promote to Primary | Request to promote a secondary instance to primary instance. All updates to the current primary instance are stopped so that all replication updates can complete. The secondary instance gets primary control of the configuration when the replication updates complete. |
| **Replication** | |
| Force Full Replication | Replicates the primary instance's database configuration for the secondary instance.<br>When full replication is in progress on an instance, do not attempt to deregister that instance. Wait until the full replication is complete and the secondary instance is restarted before you deregister the secondary instance. |

**Note** To join a secondary instance to a primary instance, the SuperAdmin account must be local to ACS. You cannot create a deployment using the Admin accounts in the external DB such as AD, LDAP or RSA.

**Step 3** Specify the appropriate values in the Registration Section.

**Step 4** Click **Register to Primary**.

The following warning message is displayed.

```
This operation will register this ACS Instance as a secondary to the specified Primary
Instance. ACS will be restarted. You will be required to login again. Do you wish to
continue?
```

**Step 5** Click **OK**.

The Secondary Instance is restarted automatically.

The credentials and the configurations that you create on the primary instance are applied to the secondary instance.

**Step 6** Register another ACS machine as secondary to the same deployment after the first secondary instance is up and running, successfully. Follow the same procedure to register all the secondary machines on the deployment.

**Note** Memory utilization of 90% is considered normal in the secondary instance if the log collector is running and the server is under heavy load. If Memory utilization increases beyond 90% and keeps increasing, it may be abnormal and needs to be analyzed.

# Deregistering Secondary Instances from the Distributed System Management Page

To deregister secondary instances from the Distributed System Management page:

**Step 1** Choose **System Administration > Operations > Distributed System Management**.

The Distributed System Management page appears.

**Step 2** From the Secondary Instances table, check one of check boxes the secondary instances that you want to deregister.

**Step 3** Click **Deregister**.

The system displays the following warning message:

```
This operation will deregister this server as a secondary with the primary server. ACS
will be restarted. You will be required to login again. Do you wish to continue?
```

**Step 4** Click **OK**.

**Step 5** Log into the ACS machine.

**Step 6** Choose **System Administration > Operations > Distributed System Management**.

The Distributed System Management page appears with the secondary instance deregistered from the primary instance.

**Related Topics**

- Viewing and Editing a Secondary Instance, page 17-14
- Deleting a Secondary Instance, page 17-15
- Activating a Secondary Instance, page 17-15
- Deregistering a Secondary Instance from the Deployment Operations Page, page 17-19
- Promoting a Secondary Instance from the Distributed System Management Page, page 17-20
- Using the Deployment Operations Page to Create a Local Mode Instance, page 17-24

# Deregistering a Secondary Instance from the Deployment Operations Page

**Note** In this case, the secondary instance is the local machine you are logged in to.

To deregister a secondary instance from the Deployment Operations page:

**Step 1** Choose **System Administration > Operations > Local Operations > Deployment Operations**.

The Deployment Operations page appears with the secondary instance that you are logged in to. See Table 17-6 for valid field options.

**Step 2** Click **Deregister from Primary**.

The system displays the following warning message:

```
This operation will deregister this server as a secondary with the primary server. ACS
will be restarted. You will be required to login again. Do you wish to continue?
```

**Step 3** Click **OK**.

**Step 4** Log into the ACS machine.

**Step 5** Choose **System Administration > Operations > Local Operations > Deployment Operations**.

The Deployment Operations page appears with the secondary instance you were logged in to deregistered from the primary instance.

---

**Related Topics**

- Viewing and Editing a Secondary Instance, page 17-14
- Deleting a Secondary Instance, page 17-15
- Activating a Secondary Instance, page 17-15
- Deregistering Secondary Instances from the Distributed System Management Page, page 17-19
- Promoting a Secondary Instance from the Distributed System Management Page, page 17-20
- Using the Deployment Operations Page to Create a Local Mode Instance, page 17-24

# Promoting a Secondary Instance from the Distributed System Management Page

To promote a secondary instance to a primary instance from the Distributed System Management page:

---

**Step 1** Choose **System Administration > Operations > Distributed System Management**.

The Distributed System Management page appears. See Table 17-4 for valid field options.

**Step 2** From the Secondary Instances table, check the box the secondary instance that you want to promote to a primary instance.

**Step 3** Click **Promote**.

The Distributed System Management page appears with the promoted instance.

---

**Related Topics**

- Viewing and Editing a Secondary Instance, page 17-14
- Deleting a Secondary Instance, page 17-15
- Activating a Secondary Instance, page 17-15
- Deregistering Secondary Instances from the Distributed System Management Page, page 17-19
- Using the Deployment Operations Page to Create a Local Mode Instance, page 17-24

# Promoting a Secondary Instance from the Deployment Operations Page

To promote a secondary instance to a primary instance from the Deployment Operations page:

**Step 1** Choose **System Administration > Operations > Distributed System Management**.

The Deployment Operations page appears. See the Table 17-6 for valid field options.

**Step 2** Register the secondary instance to the primary instance. See Registering a Secondary Instance to a Primary Instance, page 17-16.

**Step 3** Choose **System Administration > Operations > Distributed System Management**.

The Deployment Operations page appears.

**Step 4** Check the box the secondary instance that you want to promote to a primary instance.

**Step 5** Click **Promote to Primary**.

The Distributed System Management page appears with the promoted instance.

**Related Topics**

- Viewing and Editing a Secondary Instance, page 17-14
- Deleting a Secondary Instance, page 17-15
- Replicating a Secondary Instance from a Primary Instance, page 17-21
- Activating a Secondary Instance, page 17-15
- Deregistering Secondary Instances from the Distributed System Management Page, page 17-19
- Promoting a Secondary Instance from the Distributed System Management Page, page 17-20
- Using the Deployment Operations Page to Create a Local Mode Instance, page 17-24

# Replicating a Secondary Instance from a Primary Instance

You can use two different pages to replicate a secondary instance:

- Replicating a Secondary Instance from the Distributed System Management Page, page 17-21
- Replicating a Secondary Instance from the Deployment Operations Page, page 17-22

**Note** For more information on replication, see ACS 4.x and 5.8.1 Replication, page 1-2.

## Replicating a Secondary Instance from the Distributed System Management Page

**Note** All ACS appliances must be in sync with the AD domain clock.

To replicate a secondary instance:

**Step 1** Choose **System Administration > Operations > Distributed System Management.**

The Distributed System Management page appears.

**Step 2** From the Secondary Instances table, check one of check boxes the secondary instances that you want to replicate.

**Step 3** Click **Full Replication**.

The system displays the following warning message:

```
This operation will force a full replication for this secondary server. ACS will be
restarted. You will be required to login again. Do you wish to continue?
```

**Step 4** Click **OK**.

**Step 5** Log into the ACS machine.

**Step 6** Choose **System Administration > Operations > Distributed System Management.**

The Distributed System Management page appears. On the Secondary Instance table, the Replication Status column shows **UPDATED**. Replication is complete on the secondary instance. Management and runtime services are current with configuration changes from the primary instance.

# Replicating a Secondary Instance from the Deployment Operations Page

**Note** All ACS appliances must be in sync with the AD domain clock.

To replicate a secondary instance:

**Step 1** Choose **System Administration > Operations > Local Operations > Deployment Operations**.

The Deployment Operations page appears. See the Table 17-6 for valid field options.

**Step 2** Click **Force Full Replication**.

The system displays the following warning message:

```
This operation will force a full replication for this secondary server. ACS will be
restarted. You will be required to login again. Do you wish to continue?
```

**Step 3** Click **OK**.

**Step 4** Log into the ACS machine.

**Step 5** Choose **System Administration > Operations > Distributed System Management.**

The Distributed System Management page appears. On the Secondary Instance table, the Replication Status column shows **UPDATED**. Replication is complete on the secondary instance. Management and runtime services are current with configuration changes from the primary instance.

# Changing the IP address of a Primary Instance from the Primary Server

To change the IP address of a primary ACS server:

**Step 1** Log into the ACS primary web interface and Choose **System Administration > Operations > Distributed System Management** to deregister all the secondary ACS instances from the primary ACS server.

The Distributed System Management page is displayed.

**Step 2** Check the check box near the secondary ACS instance one by one and click **Deregister.**

Make sure that the log collector is running in the primary ACS server before deregistering all secondary ACS instances. If the log collector is running in any one of the secondary ACS server, change the log collector to the primary ACS server.

To change the log collector, see Configuring the Log Collector, page 18-36.

**Step 3** Check the check boxes near the deregistered secondary ACS instances to delete all deregistered secondary ACS instances.

The deregistered secondary ACS instances are deleted.

**Step 4** Log into the ACS server in Admin mode by entering:

```
acs-5-2-a/admin# conf t
```

**Step 5** Enter the following commands:

```
int g 0
ip address old ip address new ip address
```

**Step 6** Press **Ctrl z**.

The following warning message is displayed.

```
Changing the hostname or IP may result in undesired side effects, such as installed
application(s) being restarted.Are you sure you want to proceed? [y/n]
```

**Step 7** Press **y**

**Step 8** Access the primary ACS server using the administrator mode and the new IP address.

**Step 9** Use the command **show application status acs** to check if all process are running properly.

**Step 10** Register the secondary instances to the primary ACS server. See Registering a Secondary Instance to a Primary Instance, page 17-16

# Failover

ACS 5.8.1 allows you to configure multiple ACS instances for a deployment scenario. Each deployment can have one primary and multiple secondary ACS servers.

Scenario: Primary ACS goes down in a Distributed deployment

Consider we have three ACS instances ACS1, ACS2, and ACS3.

ACS1 is the primary, and ACS2 and ACS3 are secondaries. You cannot make any configuration changes on the secondary servers when the primary server ACS1 is down. If all other secondary ACS servers are active, we can make any secondary server as a primary server.

**Step 1** Promote the ACS2 to the primary for the time being and use it to make configuration changes.

See Promoting a Secondary Instance from the Distributed System Management Page, page 17-20 and Promoting a Secondary Instance from the Deployment Operations Page, page 17-21 to promote a secondary ACS server as a primary server.

Now, ACS2 is the new primary instance. So, we can make the configuration changes on ACS2 and it will be instantly replicated to ACS3 and on all secondary servers.

Now, consider the ACS1 is back Online. If you need to retain the changes made on ACS2 and the rest of the deployment so that ACS1 is the standalone, do not replicate the changes anymore.

**Step 2** Delete ACS2 and ACS3 from the secondary server list of ACS1.

**Step 3** Delete ACS1 from ACS2, the current primary server to register ACS1 as secondary.

Now, ACS2 is the primary server and ACS1 is the secondary server. The deployment is now completely back Online.

If you want ACS1 to be the primary server, then you need to promote ACS1 as a primary server.

# Using the Deployment Operations Page to Create a Local Mode Instance

When the secondary instance is in local mode it does not receive any configuration changes from the primary instance. The configuration changes you make to the secondary instance are local and do not propagate to the primary instance.

To use the Deployment Operations page to create a local mode instance:

**Step 1** Choose **System Operations > Operations > Local Operations > Deployment Operations**.

The Deployment Operations page appears. See the Table 17-4 on page 10 for valid field options.

**Step 2** Specify the appropriate values in the Registration section for the secondary instance you want to register.

**Step 3** Click **Register to Primary**.

The system displays the following warning message:

```
This operation will register this ACS Instance as a secondary to the specified Primary
Instance. ACS will be restarted. You will be required to login again. Do you wish to
continue?
```

**Step 4** Click **OK**.

**Step 5** Log into the ACS local machine.

**Step 6** Choose **System Administration > Operations > Local Operations > Deployment Operations**.

The Deployment Operations page appears.

4. Click **Request Local Mode.**

The secondary instance is now in local mode.

After you reconnect the secondary instance to a primary instance you will lose the configuration changes you made to the local secondary instance. You must manually restore the configuration information for the primary instance.

You can use the configuration information on the ACS Configuration Audit report to manually restore the configuration information for this instance.

# Creating, Duplicating, Editing, and Deleting Software Repositories

To create, duplicate, edit, or delete a software repository:

**Step 1** Choose **System Administration > Operations > Software Repositories**.

The Software Repositories page appears with the information described in Table 17-7:

*Table 17-7 Software Repositories Page*

| Option | Description |
|---|---|
| Name | Name of the software repository.<br>**Note** In ACS web interface, you cannot configure utf-8 characters for a backup filename and a repository name. |
| Protocol | Name of the protocol (DISK, FTP, SFTP, TFTP, NFS) you want to use to transfer the upgrade file. |
| Server Name | Name of the server. |
| Path | Name of the path for the directory containing the upgrade file. You must specify the protocol and the location of the upgrade file; for example, ftp://acs-home/updates. |
| Description | Description of the software repository. |
| Download RSA Key | Click this option to download the generated RSA public authentication key. |
| Generate RSA Key | Click this option to generate RSA public authentication key for SFTP repositories. |

**Step 2** Perform one of these actions:

- Click **Create**.
- Check the check box the software repository that you want to duplicate and click **Duplicate**.
- Click the software repository that you want to modify; or, check the check box for the name and click **Edit**.
- Check one or more check boxes the software repository that you want to delete and click **Delete**.

The Software Update Repositories Properties Page page appears.

**Step 3** Complete the fields in the Software Repositories Properties Page as described in Table 17-8:

*Table 17-8 Software Update Repositories Properties Page*

| Option | Description |
|---|---|
| **General** | |
| Name | Name of the software repository.<br>**Note** In ACS web interface, you cannot configure utf-8 characters for a backup filename and a repository name. |
| Description | Description of the software repository. |

*Table 17-8 Software Update Repositories Properties Page (continued)*

| Option | Description |
|---|---|
| **Repository Information** | |
| Protocol | The name of the protocol that you want to use to transfer the upgrade file. Valid options are:<br>• DISK—If you choose this protocol, you must provide the path.<br>• FTP—If you choose this protocol, you must provide the server name, path, and credentials.<br>• SFTP—If you choose this protocol, you must provide the server name, path, and credentials.<br>• TFTP—If you choose this protocol, you must enter the name of the TFTP server. You can optionally provide the path.<br>• NFS—If you choose this protocol, you must provide the server name and path. You can optionally provide the credentials. If you choose this protocol, make sure that ACS has full access to the NFS file system. You must have read-write and allow root access permission on the NFS file system. |
| Server Name | Name of the FTP, SFTP, TFTP, or NFS server. |
| **Note** The actual location that the repository points to is /localdisk/*pathname* | |
| Path | Name of the path for the upgrade file. You must specify the protocol and the location of the upgrade file; for example, ftp://acs-home/updates. |
| Enable RSA public key authentication | Check this check box if you want to use RSA public key for authentication against SFTP repositories. If you enable this option, you have to generate the RSA key from Software Repositories page and ACS uses the generated RSA key to connect to the SFTP server. |
| **User Credentials** | |
| Username | Administrator name. |
| Password | Administrator password. |

**Step 4** Click **Submit**.

The new software repository is saved. The Software Repository page appears, with the new software repository that you created, duplicated, or edited.

**Related Topics**

- Managing Software Repositories from the Web Interface and CLI, page 17-26

# Managing Software Repositories from the Web Interface and CLI

You can manage repositories from the web interface or the CLI. Keep in mind the rules for creating or deleting repositories from the web interface or CLI:

- If you create a repository from the CLI, that repository is not visible from the web interface, and can only be deleted from the CLI.
- If you create a repository from the web interface, it can be deleted from the CLI; however, that repository still exists in the web interface. If you use the web interface to create a repository for a software update, the repository is automatically created again in the CLI.
- If you delete a repository using the web interface, it is also deleted in the CLI.

# Configuring RSA Public Key for Authentication against SFTP Repositories

In general, when you want to configure an SFTP repository in ACS, you need to configure it with a username and password. The password of SFTP users are changing frequently according to the system requirement. Every time when there is a change in the user password, user needs to update the password in ACS repository configuration which is troublesome. To overcome this problem, ACS allows you to configure SFTP repository with RSA public key based authentication. In ACS 5.8.1, you can configure an SFTP repository with a username and RSA public key using which you can authenticate the users.

To configure SFTP repository with RSA Public key authentication, complete the following steps:

**Step 1** Login to ACS CLI.

**Step 2** Configure an SFTP Repository with RSA public key authentication. For more information, see Configuring SFTP Repository in ACS CLI, page 17-27.

**Step 3** Generate RSA Public key. You can generate RSA public key from ACS CLI and ACS web interface. For more information on generating RSA public key from ACS CLI, see Generating RSA Public Key, page 17-28.

**Step 4** Export the generated RSA public key to a remote repository. For more information on exporting RSA public key, see Exporting RSA Public Key to a remote Repository, page 17-28.

**Step 5** Enable the RSA public key authentication in the SFTP server. For more information, see Enabling RSA Public Key Authentication in SFTP Repository, page 17-29.

**Step 6** Add the exported RSA public key to the authorized keys list on the SFTP server. For more information on adding the public key to the authorized keys list, see Adding the Exported RSA Public Key to the Authorized Key List in SFTP Repository, page 17-29.

## Configuring SFTP Repository in ACS CLI

To configure SFTP repository in ACS CLI, complete the following steps.

**Step 1** Login to ACS CLI.

**Step 2** Enter **configure terminal** to enter the configuration mode.

**Step 3** Enter the **repository sftp** command to enter the configure repository mode.

**Step 4** Enter the **url sftp: <repository IP address> /<path>** command where “repository IP address” is the IP address of the SFTP repository and the “path” is the path in which you are going to store the data in the SFTP repository.

**Step 5** Perform one of the following actions:

- Enter the **user <username> Password {hash \ plain} <password>** command to configure the repository password with username and password.
- Enter the **user <username> rsa-public-key** command to configure the SFTP repository with username and RSA public key authentication.

**Step 6** Enter the **exit** command to come out of the repository configuration mode.

ACS CLI displays the following warning message.

```
% Warning: Host key of the server must be added using "crypto host_key add" exec command
before sftp repository can be used.
```

**Step 7** Enter the **exit** command to come out of the configuration mode.

**Step 8** Enter **show running-config** to see the configured RSA public key for sftp repository.

## Generating RSA Public Key

You can generate RSA public key from both ACS CLI and ACS web interface.

### Generating RSA Public Key using ACS CLI

To generate RSA public key from ACS CLI, complete the following steps.

**Step 1** Login to ACS CLI.

**Step 2** Enter the **crypto key generate rsa passphrase <passphrase key>** command.

**Step 3** Press **Enter**.

The following message is displayed.

```
RSA key pair for user admin generated.
```

### Generating RSA Public Key using ACS web interface

To generate RSA public key from ACS web interface, complete the following steps.

**Step 1** Login to ACS web interface.

**Step 2** Choose **System Administration > Operations > Software Repositories**.

**Step 3** Click **Generate RSA Key**.

**Step 4** Enter the **Passphrase**.

**Step 5** Enter the same Passphrase again in the **Confirm Passphrase** field.

**Step 6** Click **OK**.

The RSA key is now generated.

**Note** If you generate RSA public key from ACS web interface, then you need to download it using the **Download RSA Key** to add it to the authorized_keys file in SFTP repository.

## Exporting RSA Public Key to a remote Repository

The SFTP repository is not functional yet. Therefore, you need to export the RSA public key file to a remote repository, copy the key file contents from the remote repository and add it to the SFTP repository authorized key file.

To export the RSA public key to a remote repository, complete the following steps.

**Step 1** Login to ACS CLI.

**Step 2** Enter the **crypto key export <key_file_name> repository <repository_name>** to export the generated RSA key to a remote repository.

You can now open the remote repository to which the RSA public key is exported, copy it, and add it to the SFTP repository authorized_keys file.

## Enabling RSA Public Key Authentication in SFTP Repository

To enable RSA public key authentication in SFTP repository, complete the following steps.

**Step 1** Login to SFTP server with required permission to edit the /etc/ssh/sshd_config file.

**Step 2** Enter the **vi /etc/ssh/sshd_config** command.

SFTP server lists the contents of the sshd_config file.

**Step 3** Remove the "#" symbol from the following three lines to enable the RSA public key authentication.

- RSAAuthentication yes
- PubkeyAuthentication yes
- AuthorizedKeysFile ~/.ssh/authorized_keys

RSA public key authentication is now enabled in this SFTP server.

## Adding the Exported RSA Public Key to the Authorized Key List in SFTP Repository

To add the exported RSA public key to authorized keys file in SFTP repository, complete the following steps.

**Step 1** Login to SFTP server with required permission to edit the */etc/ssh/sshd_config* file.

**Step 2** Enter the **vi /home/<SFTP-username>/.ssh/authorized_keys** command.

This command opens the authorized_keys file from the home repository. If the authorized_keys file is not available, then SFTP repository creates a file on the same name.

**Step 3** Copy the contents from RSA public key file that you have exported to a remote repository and paste it in the authorized_keys file.

**Step 4** Enter "**wq!**" to save the authorized_keys file.

The generated RSA public key is now added to the authorized_keys file in SFTP repository.

**Related Topics**

- Creating, Duplicating, Editing, and Deleting Software Repositories, page 17-25

# Exporting Policies from ACS Web Interface

ACS allows you to export the following policies and policy elements from the ACS web interface as an XML file to a remote repository or to email ids that you have configured:

- Service Selection Rules
- Access Services (Default Device Admin and Default Network Access)
- Group Mapping
- Authorization Policies
- Authorization Profiles
- Command Sets
- Shell Profiles
- Downloadable Access Lists

You can configure remote repositories in ACS from the Software Repositories page in ACS web interface. You can perform an instant export or schedule it for a future day and time from the ACS web interface. ACS exports the above mentioned policies and policy elements as an XML file and encrypts it with a password. ACS stores the exported XML file in the remote repository or sends an email to the recipients configured in the ACS web interface. You can decrypt the exported XML file using the encryption password to perform a quick analysis of the ACS configuration and identify any errors. You must have an administrator account with SuperAdmin role to export policies from the ACS web interface. ACS does not export Access Service policies of type Security Group Access and External Proxy.

**Before you Begin**

Ensure that you have an administrator account with SuperAdmin role.

To export policies from the ACS web interface:

**Step 1** Choose System **Administration > Operation > Scheduled Policy Export**.

The Scheduled Policy Export properties page appears.

**Step 2** Complete the fields in the Scheduled Policy Export page as described in Table 17-9:

*Table 17-9 Scheduled Policy Export Page Properties*

| Option | Description |
|---|---|
| **Export Policy Configuration Data** | |
| Encryption Password | Enter the password that ACS uses to encrypt the policies file that is being exported. You need to use this password to decrypt the exported XML file. |
| Confirm Encryption Password | Enter the password again which must match the encryption password entry exactly. |
| Repository | Click **Select** to open the Software Update and Backup Repositories dialog box, from which you can select the appropriate repository in which you can store the exported policy file. You need to configure the remote repository in Software Repositories page on the ACS web interface. |
| Email file to | Enter the email address to which an email notification should be sent with the exported XML file. You can add multiple email addresses separating them with a comma. |

*Table 17-9 Scheduled Policy Export Page Properties (continued)*

| Option | Description |
|---|---|
| Mail Server | Enter a valid IPv4 or IPv6 email host server. You will not receive an email if you do not configure the email server. |
| **Schedule Options** | |
| On Demand Export | Select if you want ACS to export the policies immediately after submitting the request (instant export). |
| Schedule Export | Select if you want ACS to schedule the export operation for a future day and time. |
| Time of Day | Choose the time of the day at which you want ACS to export the policies. The export operation can be scheduled on a daily, weekly, or monthly basis.<br>• **Daily**—Choose this option to export the policies at the specified time every day.<br>• **Weekly**—Choose this option and specify the day of the week to export policies every week on the specified day.<br>• **Monthly**—Choose this option and specify the day of the month to export policies every month on the specified day. |

**Step 3** Click **Submit**.

ACS exports the policies and policy elements:

- Immediately after submitting the request if you select the On Demand Export option.
- Saves the schedule and performs the export operation on the scheduled date and time if you select the Scheduled Export option.

**Related Topics**

Creating, Duplicating, Editing, and Deleting Software Repositories, page 17-25

# Trust Communication in a Distributed Deployment

ACS introduces the Trust Communication feature, which provides additional security for communication between the ACS instances in your deployment. You can use this feature to establish a secure tunnel for communication between the primary and secondary ACS instances in a deployment. You can enable Trust Communication on both the primary and secondary ACS instances or on either instance. However, for increased security, Cisco recommends that you enable Trust Communication on all nodes in your deployment. After the deployment is ready, you cannot edit the Enable Nodes Trust Communication settings on secondary ACS instances. The changes that you make in the Trust Communication settings of the primary ACS instance will be replicated to all secondary ACS instances.

In ACS 5.8.1, when you register a secondary instance to a primary instance, both the primary and secondary instances verify each other's certificates before establishing a secure tunnel for communication. All subsequent transactions between these two nodes happen through the established secure tunnel.

By default, Trust Communication is enabled on a fresh ACS instance. If you do not need this type of security, you can uncheck the **Enable Nodes Trust Communication** check box in the Trust Communication Settings page.

- When you enable Trust Communication on your primary and secondary ACS instance, and you register the secondary instance with the primary, both the primary and secondary instance check the CA and server certificates of each other. After the certificates are verified:
  - If the certificates in both the primary and secondary ACS instances are valid certificates, the instances establish a secure tunnel between them and register the secondary instance to the primary.
  - If any of the certificates in the primary instance are invalid, the secondary ACS instance stops the registration process.
  - If any of the certificates in the secondary instance are invalid, the primary ACS instance rejects the register request from the secondary ACS instance.
- When you enable Trust Communication only in the primary ACS instance and register a secondary to this primary, then this primary instance verifies the secondary's certificates. If the certificates are valid, the primary registers the new ACS instance as a secondary instance. The secondary does not verify the primary's certificates.
- When you enable Trust Communication only in the secondary ACS instance and register this instance to the primary instance, then this secondary instance verifies the primary's certificates during registration. If the certificates are valid, the secondary instance proceeds with the registration process. The primary instance does not verify the secondary's certificates.

**Note** If the certificates that you have used for ACS instances in a deployment are invalid (such as expired certificates, revoked certificates, and not yet valid certificates), then the primary and secondary ACS instances cannot communicate and the system will not work as expected.

# Configuring Trust Communication in a Distributed Deployment

**Before You Begin**

Before enabling Trust Communication between nodes in a distributed deployment, you need to make sure that you have done the following:

- Add a trusted Certificate Authority (CA) certificate in your Primary ACS instance. For more information, see Adding a Certificate Authority, page 8-95.
- Add a management server certificate duly signed by a valid CA to the primary ACS instance. For more information, see Configuring Local Server Certificates, page 18-16.
- Add a trusted CA to the ACS instance which is going to be registered as a secondary ACS instance. For more information, see Adding a Certificate Authority, page 8-95.
- Add a management server certificate duly signed by a valid CA to the ACS instance that is going to be registered as a secondary ACS instance. For more information, see Configuring Local Server Certificates, page 18-16.
- Make sure that the CA that issued the server certificate of the secondary instance is present in the primary instance and that the CA that issued the server certificate of the primary instance is present in the secondary instance.

To configure Trust Communication between nodes in a distributed deployment.

**Step 1** Choose **System Administration > Configuration > Global System Options > Trust Communication Settings**.

**Step 2** Check the **Enable Nodes Trust Communication** check box.

**Step 3** Click **Submit**.

Trust Communication between the nodes is enabled now. You can now register a secondary instance to the primary. For more information, see Registering a Secondary Instance to a Primary Instance, page 17-16.