CHAPTER 18

# Managing System Administration Configurations

After you install Cisco Secure ACS, you must configure and administer it to manage your network efficiently. The ACS web interface allows you to easily configure ACS to perform various operations. For a list of post-installation configuration tasks to get started with ACS, see Chapter 6, "Post-Installation Configuration Tasks".

When you select **System Administration > Configuration** you can access pages that allow you do the following:

- Configure global system options, including settings for TACACS+, EAP-TTLS, PEAP, and EAP-FAST. See Configuring Global System Options, page 18-1.
- Configure protocol dictionaries. See Managing Dictionaries, page 18-5.
- Manage local sever certificates. See Configuring Local Server Certificates, page 18-14.
- Manage log configurations. See Configuring Logs, page 18-21.
- Manage licensing. See Licensing Overview, page 18-34.

# Configuring Global System Options

From the **System Administration > Configuration > Global System Options** pages, you can view these options:

- Configuring TACACS+ Settings, page 18-1
- Configuring EAP-TLS Settings, page 18-2
- Configuring PEAP Settings, page 18-3
- Configuring EAP-FAST Settings
- Generating EAP-FAST PAC

## Configuring TACACS+ Settings

Use the TACACS+ Settings page to configure TACACS+ runtime characteristics.

Select **System Administration > Configuration > Global System Options > TACACS+ Settings.**

The TACACS+ Settings page appears as described in Table 18-1:

*Table 18-1 TACACS+ Settings*

| Option | Description |
|---|---|
| Port to Listen | Port number on which to listen. By default, the port number is displayed as 49 and you cannot edit this field. |
| Connection Timeout | Number of minutes before the connection times out. |
| Session Timeout | Number of minutes before the session times out. |
| Maximum Packet Size | Maximum packet size (in bytes). |
| Single Connect Support | Check to enable single connect support. |
| **Login Prompts** | |
| Username Prompt | Text string to use as the username prompt. |
| Password Prompt | Text string to use as the password prompt. |
| **Password Change Control** | |
| Enable TELNET Change Password | Choose this option if you want to provide an option to change password during a TELNET session. |
| Prompt for Old Password: | Text string to use as the old password prompt. |
| Prompt for New Password | Text string to use as the new password prompt. |
| Prompt for Confirm Password | Text string to use as the confirm password prompt. |
| Disable TELNET Change Password | Choose this option if you do not want change password during a TELNET session. |
| Message when Disabled | Message that is displayed when you choose the Disable TELNET Change Password option. |

# Configuring EAP-TLS Settings

Use the EAP-TLS Settings page to configure EAP-TLS runtime characteristics.

Select **System Administration > Configuration > Global System Options > EAP-TLS Settings.**

The EAP-TLS Settings page appears as described in Table 18-2:

*Table 18-2 EAP-TLS Settings*

| Option | Description |
|---|---|
| Enable EAP-TLS Session Resume | Check this box to support abbreviated reauthentication of a user who has passed full EAP-TLS authentication.<br>This feature provides reauthentication of the user with only an SSL handshake and without the application of certificates. EAP-TLS session resume works only within the EAP-TLS session timeout value. |
| EAP-TLS session timeout | Enter the number of seconds before the EAP-TLS session times out. |

# Configuring PEAP Settings

Use the PEAP Settings page to configure PEAP runtime characteristics.

Select **System Administration > Configuration > Global System Options > PEAP Settings.**

The PEAP Settings page appears as described in Table 18-3:

*Table 18-3 PEAP Settings*

| Option | Description |
|---|---|
| Enable PEAP Session Resume | When checked, ACS caches the TLS session that is created during phase one of PEAP authentication, provided the user successfully authenticates in phase two of PEAP. If a user needs to reconnect and the original PEAP session has not timed out, ACS uses the cached TLS session, resulting in faster PEAP performance and a lessened AAA server load.<br>You must specify a PEAP session timeout value for the PEAP session resume features to work. |
| PEAP Session Timeout | Enter the number of seconds before the PEAP session times out. The default value is 7200 seconds. |
| Enable Fast Reconnect | Check to allow a PEAP session to resume in ACS without checking user credentials when the session resume feature is enabled. |

**Related Topic**

- Generating EAP-FAST PAC, page 18-4

# Configuring EAP-FAST Settings

Use the EAP-FAST Settings page to configure EAP-FAST runtime characteristics.

Select **System Administration > Configuration > Global System Options > EAP-FAST > Settings.**

The EAP-FAST Settings page appears as described in Table 18-4:

*Table 18-4 EAP-FAST Settings*

| Option | Description |
|---|---|
| **General** | |
| Authority Identity Info Description | User-friendly string that describes the ACS server that sends credentials to a client. The client can discover this string in the Protected Access Credentials Information (PAC-Info) Type-Length-Value (TLV). The default value is Cisco Secure ACS. |
| Master Key Generation Period | The value is used to encrypt or decrypt and sign or authenticate PACs. The default is one week. |
| **Revoke** | |
| Revoke | Click **Revoke** to revoke all previous master keys and PACs. This operation should be used with caution.<br>If the ACS node is a secondary node, the Revoke option is disabled. |

# Generating EAP-FAST PAC

Use the EAP-FAST Generate PAC page to generate a user or machine PAC.

**Step 1** Select **System Administration > Configuration > Global System Options > EAP-FAST > Generate PAC.**

The Generate PAC page appears as described in Table 18-5:

*Table 18-5 Generate PAC*

| Option | Description |
|---|---|
| Tunnel PAC | Select to generate a tunnel PAC. |
| Machine PAC | Select to generate a machine PAC. |
| Identity | Specifies the username or machine name presented as the "inner username" by the EAP-FAST protocol. If the Identity string does not match that username, authentication will fail. |
| PAC Time To Live | Enter the equivalent maximum value in days, weeks, months and years, and enter a positive integer. |
| Password | Enter the password. |

**Step 2** Click **Generate PAC**.

# Configuring RSA SecurID Prompts

You can configure RSA prompts for an ACS deployment. The set of RSA prompts that you configure is used for all RSA realms and ACS instances in a deployment. To configure RSA SecurID Prompts:

**Step 1** Choose **System Administration > Configuration > Global System Options > RSA SecurID Prompts**.

The RSA SecurID Prompts page appears.

**Step 2** Modify the fields described in Table 18-6.

*Table 18-6 RSA SecurID Prompts Page*

| Option | Description |
|---|---|
| Next Token Prompt | Text string to request for the next token. The default value is "Enter Next TOKENCODE:". |
| Choose PIN Type Prompt | Text string to request the PIN type. The default value is "Do you want to enter your own pin?". |

*Table 18-6 RSA SecurID Prompts Page*

| Option | Description |
|---|---|
| Accept System PIN Prompt | Text string to accept the system-generated PIN. The default value is "ARE YOU PREPARED TO ACCEPT A SYSTEM-GENERATED PIN?".<br>For the two PIN entry prompts below, if the prompt contains the following strings, they will be substituted as follows:<br>• {MIN_LENGTH}- will be replaced by the minimum PIN length configured for the RSA Realm.<br>• {MAX_LENGTH}- will be replaced by the maximum PIN length configured for the RSA Realm. |
| Alphanumeric PIN Prompt | Text string for requesting an alphanumeric PIN. |
| Numeric PIN Prompt | Text string for requesting a numeric PIN. |
| Re-Enter PIN Prompt | Text string to request the user to re-enter the PIN. The default value is "Reenter PIN:". |

**Step 3** Click **Submit** to configure the RSA SecurID Prompts.

# Managing Dictionaries

The following tasks are available when you select **System Administration > Configuration > Dictionaries**:

- Viewing RADIUS and TACACS+ Attributes, page 18-5
- Configuring Identity Dictionaries, page 18-10

## Viewing RADIUS and TACACS+ Attributes

The RADIUS and TACACS+ Dictionary pages display the available protocol attributes in these dictionaries:

- RADIUS (IETF)
- RADIUS (Cisco)
- RADIUS (Microsoft)
- RADIUS (Ascend)
- RADIUS (Cisco Airespace)
- RADIUS (Cisco Aironet)
- RADIUS (Cisco BBSM)
- RADIUS (Cisco VPN 3000)
- RADIUS (Cisco VPN 5000)
- RADIUS (Juniper)
- RADIUS (Nortel [Bay Networks])

- RADIUS (RedCreek)
- RADIUS (US Robotics)
- TACACS+

To view and choose attributes from a protocol dictionary, select **System Administration > Configuration > Dictionaries > Protocols;** then choose a dictionary.

The Dictionary page appears with a list of available attributes as shown in Table 18-7:

***Table 18-7 Protocols Dictionary Page***

| Option | Description |
|---|---|
| Attribute | Name of the attribute. |
| ID | (RADIUS only) The VSA ID. |
| Type | Data type of the attribute. |
| Direction | (RADIUS only) Specifies where the attribute is in use: in the request, in the response, or both. Single or bidirectional authentication. |
| Multiple Allowed | (RADIUS only) Multiple attributes are allowed. Attributes that specify *multiple allowed* can be used more than once in one request or response. |

Use the arrows to scroll through the attribute list.

ACS 5.3 also supports RADIUS vendor-specific attributes (VSAs). A set of predefined RADIUS VSAs are available. You can define additional vendors and attributes from the ACS web interface. You can create, edit, or delete RADIUS VSAs.

After you have defined new VSAs, you can use them in policies, authorization profiles, and RADIUS token servers in the same way as predefined VSAs. For more information, see:

- RADIUS VSAs, page A-6.
- Creating, Duplicating, and Editing RADIUS Vendor-Specific Attributes, page 18-6

# Creating, Duplicating, and Editing RADIUS Vendor-Specific Attributes

Vendor-Specific Attributes (VSAs) allow vendors to create extension to the RADIUS attributes. The vendors have a specific vendor number assigned to them. VSAs are attributes that contain subattributes. ACS 5.3 allows you to create, duplicate, or edit RADIUS VSA (VSAs). To do this:

Some of the internally used attributes cannot be modified.

You cannot modify an attribute's type if the attribute is used by any policy or policy element.

**Step 1** Choose **System Administration > Configuration > Dictionaries > Protocols > RADIUS VSA**.

**Step 2** Do one of the following:

- Click **Create**.
- Check the check box next to the RADIUS VSA that you want to duplicate, then click **Duplicate**.
- Check the check box next to the RADIUS VSA that you want to edit, then click **Edit**.

The Create RADIUS VSA page appears. Modify the fields as described in Table 18-8.

*Table 18-8 RADIUS VSA - Create, Duplicate, Edit Page*

| Option | Description |
|---|---|
| Attribute | Name of the RADIUS VSA. |
| Description | (Optional) A brief description of the RADIUS VSA. |
| Vendor ID | ID of the RADIUS vendor. |
| Attribute Prefix | (Optional) Prefix that you want to prepend to the RADIUS attribute so that all attributes for the vendor start with the same prefix. |
| **Use Advanced Vendor Options** | |
| Vendor Length Field Size | Vendor length field of 8 bits for specifying the length of the VSA. Choose the vendor length of the VSA. Valid options are 0 and 1. The default value is 1. |
| Vendor Type Field Size | Vendor type field of 8 bits. Choose the vendor type of the VSA. Valid options are 1, 2, and 4. The default value is 1. |

**Step 3** Click **Submit** to save the changes.

**Related Topics**

Viewing RADIUS and TACACS+ Attributes, page 18-5

# Creating, Duplicating, and Editing RADIUS Vendor-Specific Subattributes

To create, duplicate, and edit RADIUS vendor-specific subattributes:

**Step 1** Choose **System Administration > Configuration > Dictionaries > Protocols > RADIUS > RADIUS VSA**.

You can alternatively choose the RADIUS VSA from the navigation pane.

**Step 2** Do one of the following:

- Click **Create** to create a subattribute for this RADIUS VSA.
- Check the check box next to the RADIUS VSA that you want to duplicate, then click **Duplicate**.
- Check the check box next to the RADIUS VSA that you want to edit, then click **Edit**.

The RADIUS VSA subattribute create page appears.

**Step 3** Complete the fields described in Table 18-9.

*Table 18-9 Creating, Duplicating, and Editing RADIUS Subattributes*

| Option | Description |
|---|---|
| **General** | |
| Attribute | Name of the subattribute. The name must be unique. |
| Description | (Optional) A brief description of the subattribute. |
| **RADIUS Configuration** | |
| Vendor Attribute ID | Enter the vendor ID field for the subattribute. This value must be unique for this vendor. |
| Direction | Specifies where the attribute is in use: in the request, in the response, or both. Single or bidirectional authentication. |
| Multiple Allowed | Multiple attributes are allowed. Attributes that specify *multiple allowed* can be used more than once in one request or response. |
| Include attribute in the log | Check this check box to include the subattribute in the log. For sensitive attributes, you can uncheck this check box so to they are not logged. |
| **Attribute Type** | |
| Attribute Type | Type of the attribute. Valid options are:<br>• String<br>• Unsigned Integer 32<br>• IPv4 Address<br>• HEX String<br>• Enumeration—If you choose this option, you must enter the ID-Value pair<br>You cannot use attributes of type HEX String in policy conditions. |

*Table 18-9 Creating, Duplicating, and Editing RADIUS Subattributes*

| Option | Description |
|---|---|
| ID-Value | (Optional) *For the Enumeration attribute type only.*<br>• ID—Enter a number from 0 to 999.<br>• Value—Enter a value for the ID.<br>• Click **Add** to add this ID-Value pair to the ID-Value table.<br>To edit, replace, and delete ID-Value pairs:<br>• Select the ID-Value pair from the ID-Value table.<br>• Click **Edit** to edit the ID and Value fields. Edit the fields as required.<br>• Click **Add** to add a new entry after you modify the fields.<br>• Click **Replace** to replace the same entry with different values.<br>• Click **Delete** to delete the entry from the ID-Value table. |
| **Attribute Configuration** | |
| Add Policy Condition | Check this check box to enter a policy condition in which this subattribute will be used. |
| Policy Condition Display Name | Enter the name of the policy condition that will use this subattribute. |

**Step 4** Click **Submit** to save the subattribute.

# Viewing RADIUS Vendor-Specific Subattributes

To view the attributes that are supported by a particular RADIUS vendor:

**Step 1** Choose **System Administration > Configuration > Dictionaries > Protocols > RADIUS > RADIUS VSA**.

The RADIUS VSA page appears.

**Step 2** Check the check box next to the vendor whose attribute you want to view, then click **Show Vendor Attributes**.

The vendor-specific attributes and the fields listed in Table 18-7 are displayed. You can create additional VSAs, and duplicate or edit these attributes. For more information, see Creating, Duplicating, and Editing RADIUS Vendor-Specific Subattributes, page 18-7.

### Related Topic

Creating, Duplicating, and Editing RADIUS Vendor-Specific Attributes, page 18-6

# Configuring Identity Dictionaries

This section contains the following topics:



# Creating, Duplicating, and Editing an Internal User Identity Attribute

To create, duplicate, and edit an internal user identity attribute:

**Step 1** Select **System Administration > Configuration > Dictionaries > Identity > Internal Users**.

The Attributes list for the Internal Users page appears.

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

- Click **Create**.
- Check the check box next to the attribute that you want to duplicate and click **Duplicate**.
- Click the attribute name that you want to modify; or, check the check box for the name and click **Edit**.

The Identity Attribute Properties page appears.

**Step 3** Modify the fields in the Identity Attributes Properties page as required. See Configuring Internal Identity Attributes, page 18-11 for field descriptions.

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

The internal user attribute configuration is saved. The Attributes list for the Internal Users page appears with the new attribute configuration.

### Related Topics

- Deleting an Internal User Identity Attribute, page 18-12
- Creating, Duplicating, and Editing an Internal Host Identity Attribute, page 18-13
- Policies and Identity Attributes, page 3-17

# Configuring Internal Identity Attributes

Table 18-10 describes the fields in the internal <*users* | *hosts*> identity attributes.

***Table 18-10 Identity Attribute Properties Page***

| Option | Description |
|---|---|
| **General** | |
| Attribute | Name of the attribute. |
| Description | Description of the attribute. |
| **Attribute Type** | |
| Attribute Type | (Optional) Use the drop-down list box to choose an attribute type. Valid options are:<br>• String—Populates the Maximum Length and Default Value fields in the page. When you select String as attribute type and enter a non-null value for a user, the user is authenticated against the ID store with the name that matches with the already set value, for the attribute on the user details (ACS-RESERVED-Authen-ID-Store).<br>• Unsigned Integer 32—Populates the Valid Range From and To fields in the page.<br>• IPv4 Address—Populates the Default Value field in the page.<br>• Boolean—Populates the Default Value check box in the page.When you set the value of the Boolean attribute as true, it overrides the global settings for password expiration policy and deactivate the policy (ACS-RESERVED-Never-Expired).<br>• Date—Populates the Default Value field and calendar icon in the page.<br>• Enumeration—Populates the ID and Value fields and the Add, Edit, Replace, and Delete buttons. |
| Maximum Length | (Optional) *For the String attribute type only.* Enter the maximum length of your attribute. The valid range is from 1 to 256. (Default = 32) |
| Value Range | (Optional) *For the Unsigned Integer attribute type only.*<br>• From—Enter the lowest acceptable integer value. The valid range is from 0 to 2^31-1 (2147483647). This value must be smaller than the Valid Range To value.<br>• To—Enter the highest acceptable integer value. The valid range is from 0 to 2^31-1 (2147483647). This value must be larger than the Valid Range From value. |
| Default Value | Enter the default value for the appropriate attribute:<br>• String—Up to the maximum length. (Follow the UTF-8 standard.) You can use the letters a to z, A to Z, and the digits 0 to 9.<br>• Unsigned Integer 32—An integer in the range from 0 to 2^31-1 (2147483647).<br>• IPv4 Address—Enter IP address you want to associate with this attribute, in the format: *x.x.x.x*, where *x.x.x.x* is the IP address (no subnet mask).<br>• Date—Click the calendar icon to display the calendar popup and select a date.<br>• Boolean Value—Select True or False. |

*Table 18-10 Identity Attribute Properties Page (continued)*

| Option | Description |
|---|---|
| ID-Value | (Optional) *For the Enumeration attribute type only.*<br>• ID—Enter a number from 0 to 999.<br>• Value—Enter a value for the ID.<br>• Click **Add** to add this ID-Value pair to the ID-Value table.<br>To edit, replace, and delete ID-Value pairs:<br>• Select the ID-Value pair from the ID-Value table.<br>• Click **Edit** to edit the ID and Value fields. Edit the fields as required.<br>• Click **Add** to add a new entry after you modify the fields.<br>• Click **Replace** to replace the same entry with different values.<br>• Click **Delete** to delete the entry from the ID-Value table. |
| Attribute Configuration | |
| Mandatory Fields | Check the check box to make this attribute a requirement in the User Properties page. |
| Add Policy Condition | Check the check box to create a custom condition from this attribute. When you check this option, you must enter a name in the Policy Condition Display Name field. |
| Policy Condition Display Name | Enter a name for the policy condition. After you submit this page, the condition appears in the **Policy Elements > Session Conditions > Custom** page. |

# Deleting an Internal User Identity Attribute

To delete an internal user identity attribute:

**Step 1** Select **System Administration > Configuration > Dictionaries > Identity > Internal Users**.

The Attributes list for the internal user page appears.

**Step 2** Check the check box next to the attribute you want to delete.

Because deleting an identity attribute can take a long time to process, you can delete only one attribute at a time.

**Step 3** Click **Delete**.

**Step 4** For confirmation, click **OK** or **Cancel**.

The Attributes list for the internal user page appears without the deleted attribute.

### Related Topics

- Creating, Duplicating, and Editing an Internal User Identity Attribute, page 18-10
- Policies and Identity Attributes, page 3-17

# Creating, Duplicating, and Editing an Internal Host Identity Attribute

To create, duplicate, and edit an internal host identity attribute:

**Step 1** Select **System Administration > Configuration > Dictionaries > Identity > Internal Hosts**.

The Attributes list for the Internal Hosts page appears.

**Step 2** Do one of the following:

- Click **Create**.
- Check the check box next to the attribute that you want to duplicate and click **Duplicate**.
- Click the attribute name that you want to modify; or, check the check box for the name and click **Edit**.

The Identity Attribute Properties page appears.

**Step 3** Modify the fields in the Identity Attributes Properties page as required. See Table 18-10 for field descriptions.

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

The internal host attribute configuration is saved. The Attributes list for the Internal Hosts page appears with the new attribute configuration.

### Related Topics

- Deleting an Internal Host Identity Attribute, page 18-13
- Policies and Identity Attributes, page 3-17

# Deleting an Internal Host Identity Attribute

To delete an internal host identity attribute:

**Step 1** Select **System Administration > Configuration > Dictionaries > Identity > Internal User**.

The Attributes list for the Internal Hosts page appears.

**Step 2** Check the check box next to the attribute you want to delete.

Because deleting an attribute can take a long time to process, you can delete only one attribute at a time.

**Step 3** Click **Delete**.

**Step 4** For confirmation, click **OK** or **Cancel**.

The Attributes list for the Internal Hosts page appears without the deleted attribute.

### Related Topics

- Creating, Duplicating, and Editing an Internal Host Identity Attribute, page 18-13
- Policies and Identity Attributes, page 3-17

## Adding Static IP address to Users in Internal Identity Store

To add static IP address to a user in Internal Identity Store:

**Step 1** Add a static IP attribute to internal user attribute dictionary:

**Step 2** Select **System Administration > Configuration > Dictionaries > Identity > Internal Users**.

**Step 3** Click **Create**.

**Step 4** Add static IP attribute.

**Step 5** Select **Users and Identity Stores > Internal Identity Stores > Users**.

**Step 6** Click **Create**.

**Step 7** Edit the static IP attribute of the user.

# Configuring Local Server Certificates

Local server certificates are also known as ACS server certificates. ACS uses the local server certificates to identify itself to the clients. The local server certificates are used by:

- EAP protocols that use SSL/TLS tunneling.
- Management interface to authenticate the web interface (GUI).

This section contains the following topics:



# Adding Local Server Certificates

You can add a local server certificate, also known as an ACS server certificate, to identify the ACS server to clients.

**Step 1** Select **System Administration > Configuration > Local Server Certificates > Local Certificates**.

The Local Certificates page appears displaying the information in Table 18-11:

*Table 18-11 Local Certificates Page*

| Option | Description |
|---|---|
| Friendly Name | Name that is associated with the certificate. |
| Issued To | Entity to which the certificate is issued. The name that appears is from the certificate subject. |
| Issued By | Trusted party that issued the certificate. |
| Valid From | Date the certificate is valid from. |
| Valid To (Expiration) | Date the certificate is valid to. |
| Protocol | Protocol associated with the certificate. |

**Step 2** Click **Add**.

**Step 3** Enter the information in the Local Certificate Store Properties page as described in Table 18-12:

*Table 18-12 Local Certificate Store Properties Page*

| Option | Description |
|---|---|
| Import Server Certificate | Select to browse the client machine for the Local Certificate file and import the private key and private key password. See Importing Server Certificates and Associating Certificates to Protocols, page 18-15.<br>Supported certificate formats include, DER, PEM, or Microsoft private key proprietary format. |
| Generate Self Signed Certificate | Select to generate a self-signed certificate. See Generating Self-Signed Certificates, page 18-16. |
| Generate Certificate Signing Request | Select to generate a certificate signing request. See Generating a Certificate Signing Request, page 18-17. |
| Bind CA Signed Certificate | Select to bind the CA certificate. After the RA signs the request, you can install the returned signed certificate on ACS and bind the certificate with its corresponding private key. See Binding CA Signed Certificates, page 18-17. |

# Importing Server Certificates and Associating Certificates to Protocols

The supported certificate formats are either DER or PEM.

**Step 1** Select **System Administration > Configuration > Local Server Certificates > Local Certificates > Add**.

**Step 2** Select **Import Server Certificate > Next**.

**Step 3** Enter the information in the ACS Import Server Certificate as described in Table 18-13:

*Table 18-13 Import Server Certificate Page*

| Option | Description |
|---|---|
| Certificate File | Select to browse the client machine for the local certificate file. |
| Private Key File | Select to browse to the location of the private key. |
| Private Key Password | Enter the private key password. The value may be minimum length = 0 and maximum length = 256. |
| **Protocol** | |
| EAP | Check to associate the certificate with EAP protocols that use SSL/TLS tunneling: EAP-TLS, EAP-FAST, and PEAP. |
| Management Interface | Check to associate the certificate with the management interface. |
| Allow Duplicate Certificates | Allows to add certificate with same CN and same SKI with different Valid From, Valid To, and Serial number. |
| **Override Policy** | |
| Replace Certificate | Check to replace the content of an existing certificate with the one that you import, but retain the existing protocol selections. |

**Step 4** Click **Finish.**

The new certificate is saved. The Local Certificate Store page appears with the new certificate.

# Generating Self-Signed Certificates

**Step 1** Select **System Administration > Configurations > Local Server Certificates > Local Certificates > Add.**

**Step 2** Select **Generate Self Signed Certificate> Next**.

**Step 3** Enter the information in the ACS Import Server Certificate as described in Table 18-14:

*Table 18-14 Generate Self Signed Certificate Step 2*

| Option | Description |
|---|---|
| Certificate Subject | Certificate subject entered during generation of this request. The Certificate Subject field may contain alphanumeric characters. The maximum number of characters is 1024. This field is prefixed with “cn=”. |
| Key Length | Key length entered during generation of this request.Values may be 512, 1024, 2048, or 4096. |
| Digest to Sign with | Select either SHA1 or SHA256 as management certificates, from the dropdown list. |
| Expiration TTL | Select the maximum value in days, weeks, months, and years, and enter a positive integer. |
| **Protocol** | |
| EAP | Check to associate the certificate with EAP protocols that use SSL/TLS tunneling: EAP-TLS, EAP-FAST, and PEAP. |

*Table 18-14 Generate Self Signed Certificate Step 2*

| Option | Description |
|---|---|
| Management Interface | Check to associate the certificate with the management interface. |
| **Override Policy** | |
| Replace Certificate | Check to replace the content of an existing certificate with the one that you import, but retain the existing protocol selections. |

**Step 4** Click **Finish.**

The new certificate is saved. The Local Certificate Store page appears with the new certificate.

# Generating a Certificate Signing Request

**Step 1** Select **System Administration > Configurations > Local Server Certificates > Local Certificates > Add.**

**Step 2** Select **Generate Certificate Signing Request** > **Next**.

**Step 3** Enter the information in the ACS Import Server Certificate as described in Table 18-15:

*Table 18-15 Generate Signing Requests Step 2*

| Option | Description |
|---|---|
| Certificate Subject | Certificate subject entered during generation of this request. The Certificate Subject field may contain alphanumeric characters. The maximum number of characters is 1024. This field is prefixed with “cn=”. |
| Key Length | Key length entered during generation of this request.Values may be 512, 1024, 2048, or 4096. |
| Digest to Sign with | Select either SHA1 or SHA256 as management certificates, from the dropdown list. |

**Step 4** Click **Finish.**

The following message is displayed:

```
A server certificate signing request has been generated and can be viewed in the
“Outstanding Signing Requests" list.
```

The new certificate is saved. The Local Certificate Store page appears with the new certificate.

# Binding CA Signed Certificates

Use this page to bind a CA signed certificate to the request that was used to obtain the certificate from the CA.

**Step 1** Select **System Administration > Configurations > Local Server Certificates > Local Certificates > Add.**

**Step 2** Select **Bind CA Signed Certificate** > **Next**.

**Step 3** Enter the information in the ACS Import Server Certificate as described in Table 18-16:

*Table 18-16 Bind CA Signed Certificate Step 2*

| Option | Description |
|---|---|
| Certificate File | Browse to the client machine and select the certificate file to be imported. |
| **Protocol** | |
| EAP | Check to associate the certificate with EAP protocols that use SSL/TLS tunneling: EAP-TLS, EAP-FAST, and PEAP. |
| Management Interface | Check to associate the certificate with the management interface. |
| **Override Policy** | |
| Replace Certificate | Check to replace the content of an existing certificate with the one that you import, but retain the existing protocol selections. |

**Step 4** Click **Finish.**

The new certificate is saved. The Local Certificate Store page appears with the new certificate.

**Related Topics**

- Configuring Local Server Certificates, page 18-14
- Certificate-Based Network Access for EAP-TLS, page 4-10

# Editing and Renewing Certificates

You can renew an existing self-signed certificate without having to remove it and adding a new certificate. This ensures that any service that uses the local certificate continues without any interruption. To renew or extend a local server certificate:

**Step 1** Select **System Administration > Configuration > Local Server Certificates > Local Certificates**.

**Step 2** Click the name that you want to modify; or, check the check box for the Name, and click **Edit**.

**Step 3** Enter the certificate properties as described in Table 18-17:

*Table 18-17 Edit Certificate Store Properties Page*

| Option | Description |
|---|---|
| **Issuer** | |
| Friendly Name | Name that is associated with the certificate. |
| **Description** | Description of the certificate. |
| Issued To | *Display only.* The entity to which the certificate is issued. The name that appears is from the certificate subject. |

*Table 18-17 Edit Certificate Store Properties Page (continued)*

| Option | Description |
|---|---|
| Issued By | *Display only.* The certification authority that issued the certificate. |
| Valid From | *Display only.* The start date of the certificate's validity. An X509 certificate is valid only from the start date to the end date (inclusive). |
| Valid To (Expiration) | *Display only.* The last date of the certificate's validity. |
| Serial Number | *Display only.* The serial number of the certificate. |
| **Protocol** | |
| EAP | Check for ACS to use the local certificate with EAP protocols that use SSL/TLS tunneling: EAP-TLS, EAP-FAST, and PEAP. |
| Management Interface | Check for ACS to use the local certificate for SSL client authentication. |
| **Renew Self Signed Certificate** | |
| Certificate Expires On | *Display only.* Date the certificate expires. |
| Renew Self Signed Certificate | Check to allow the renewal of a self signed certificate that expired. |
| Expiration TTL | Expiration TTL is the number of days, months, weeks, or years that you want to extend the existing certificate for. Valid options are: one day, one month, one week, and one year.<br>At a maximum, you can extend the certificate for a period of one year. |

**Step 4** Click **Submit** to extend the existing certificate's validity.

The Local Certificate Store page appears with the edited certificate.

**Related Topic**

- Configuring Local Server Certificates, page 18-14

# Deleting Certificates

To delete a certificate:

**Step 1** Select **System Administration > Configuration > Local Server Certificates > Local Certificates**.

**Step 2** Check one or more check boxes next to the certificates that you want to delete.

**Step 3** Click **Delete**.

**Step 4** For confirmation, click **Yes** or **Cancel**.

The Certificate Store page appears without the deleted certificate(s).

**Related Topic**

- Configuring Local Server Certificates, page 18-14

# Exporting Certificates

To export a certificate:

**Step 1** Select **System Administration > Configuration > Local Server Certificates > Local Certificates**.

**Step 2** Check the box next to the certificates that you want to export, then click **Export**.

The Export Certificate dialog box appears.

**Step 3** Select one of the following options:

- Export Certificate Only
- Export Certificate and Private Key

**Step 4** Enter your private key password in the Private Key Password field.

**Step 5** Enter the same password in the Confirm Password field.

**Note** Exporting the private key is not a secure operation and could lead to possible exposure of the private key.

**Step 6** Click **OK** or **Cancel**.

### Related Topic

- Configuring Local Server Certificates, page 18-14

# Viewing Outstanding Signing Requests

**Step 1** Select **System Administration > Configurations > Local Server Certificates > Outstanding Signing Request**.

The Certificate Signing Request page appears displaying the information described in Table 18-18:

***Table 18-18 Certificate Signing Request Page***

| Option | Description |
|---|---|
| Name | Name of the certificate. |
| Certificate Subject | Certificate subject entered during generation of this request. The Certificate Subject field may contain alphanumeric characters. The maximum number of characters is 1024. This field should automatically prefixed with “cn=”. |
| Key Length | Key length entered during generation of this request.Values may be 512, 1024, 2048, or 4096. |
| Timestamp | Date certificate was created. |
| Friendly Name | Name that is associated with the certificate. |

**Step 2** Click **Export** to export the local certificate to a client machine.

# Configuring Logs

Log records are generated for:

- Accounting messages
- AAA audit and diagnostics messages
- System diagnostics messages
- Administrative and operational audit messages

The messages are arranged in tree hierarchy structure within the logging categories (see Configuring Logging Categories, page 18-24 for more information).

You can store log messages locally or remotely, based on the logging categories and maintenance parameters.

This section contains the following topics:



See Chapter 19, "Understanding Logging" for a description of the preconfigured global ACS logging categories and the messages that each contains.

## Configuring Remote Log Targets

You can configure specific remote log targets (on a syslog server only) to receive the logging messages for a specific logging category. See Chapter 19, "Understanding Logging" for more information on remote log targets. See Configuring Logging Categories, page 18-24 for more information on the preconfigured ACS logging categories.

To create a new remote log target:

**Step 1** Select **System Administration > Configuration > Log Configuration > Remote Log Targets**.

The Remote Log Targets page appears.

**Step 2** Do one of the following:

- Click **Create**.
- Check the check box next to the remote log target that you want to duplicate and click **Duplicate**.
- Click the name of the remote log target that you want to modify; or check the check box next to the name of the remote log target that you want to modify and click **Edit**.

One of these pages appears:

- Remote Log Targets > Create, if you are creating a new remote log target.

- Remote Log Targets > Duplicate: "*log_target*", where *log_target* is the name of the remote log target you selected in Step 2, if you are duplicating a remote log target.
- Remote Log Targets > Edit: "*log_target*", where *log_target* is the name of the remote log target you selected in Step 2, if you are modifying a remote log target.

**Step 3** Complete the required fields as described in Table 18-19:

***Table 18-19 Remote Log Targets Configuration Page***

| Option | Description |
|---|---|
| **General** | |
| Name | Name of the remote log target. Maximum name length is 32 characters. |
| Description | Description of the remote log target. Maximum description length is 1024 characters. |
| Type | Type of remove log target—Syslog (the only option). |
| **Target Configuration** | |
| IP Address | IP address of the remote log target, in the format *x.x.x.x*. |
| Use Advanced Syslog Options | Click to enable the advanced syslog options—port number, facility code, and maximum length. |
| Port | Port number of the remote log target used as the communication channel between the ACS and the remote log target (default = 514). This option is only visible if you click Use Syslog Options. |
| Facility Code | Facility code. Valid options are:<br>• LOCAL0 (Code = 16)<br>• LOCAL1 (Code = 17)<br>• LOCAL2 (Code = 18)<br>• LOCAL3 (Code = 19)<br>• LOCAL4 (Code = 20)<br>• LOCAL5 (Code = 21)<br>• LOCAL6 (Code = 22; default)<br>• LOCAL7 (Code = 23)<br>This option is only visible if you click Use Advanced Syslog Options. |
| Maximum Length | Maximum length of the remote log target messages. Valid options are from 200 to 1024. This option is only visible if you click Use Advanced Syslog Options. |

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

The remote log target configuration is saved. The Remote Log Targets page appears with the new remote log target configuration.

### Related Topic

- Deleting a Remote Log Target, page 18-23

# Deleting a Remote Log Target

To delete a remote log target:

**Step 1** Select **System Administration > Configuration > Log Configuration > Remote Log Targets**.

The Remote Log Targets page appears, with a list of configured remote log targets.

**Step 2** Check one or more check boxes next to the remote log targets you want to delete.

**Step 3** Click **Delete**.

The following error message appears:

```
Are you sure you want to delete the selected item/items?
```

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

The Remote Log Targets page appears without the deleted remote log targets.

### Related Topic

- Configuring Remote Log Targets, page 18-21

# Configuring the Local Log

Use the Local Configuration page to configure the maximum days to retain your local log data.

**Step 1** Select **System Administration > Configuration > Log Configuration > Local Log Target**.

The Local Configuration page appears.

**Step 2** In the Maximum log retention period box, enter the number of days for which you want to store local log message files, where <*num*> is the number of days you enter. Valid options are 1 to 365. (Default = 7.)

**Note** If you reduce the number of days for which to store the local log message files, the log message files older than the number of days you specify are deleted automatically.

You can click **Delete Logs Now** to delete the local logs, including all non-active log files, immediately. See Deleting Local Log Data, page 18-23 for more information on deleting log data.

**Step 3** Click **Submit** to save your changes.

Your configuration is saved and the Local Configuration page is refreshed.

# Deleting Local Log Data

Use the Local Configuration page to manually delete your local log data. You can use this option to free up space when the local store is full. See Local Store Target, page 19-5 for more information about the local store.

**Step 1** Select **System Administration > Configuration > Log Configuration > Local Log Target**.

The Local Configuration page appears.

**Step 2** Click **Delete Logs Now** to immediately delete all local log data files, except the log data in the currently active log data file.

The Local Configuration page is refreshed.

# Configuring Logging Categories

This section contains the following topics:



All configuration performed for a parent logging category affects the children within the logging category. You can select a child of a parent logging category to configure it separately, and it does not affect the parent logging category or the other children.

## Configuring Global Logging Categories

To view and configure global logging categories:

**Step 1** Select **System Administration > Configuration > Log Configuration > Logging Categories > Global**.

The Logging Categories page appears; from here, you can view the logging categories.

**Step 2** Click the name of the logging category you want to configure; or, click the radio button next to the name of the logging category you want to configure and click **Edit**.

**Step 3** Complete the fields as described in Table 18-20.

*Table 18-20 Global: General Page*

| Option | Descriptions |
|---|---|
| **Configure Log Category** | |
| Log Severity | For diagnostic logging categories, use the drop-down list box to select the severity level. (For audit and accounting categories, there is only one severity, NOTICE, which cannot be modified.) Valid options are:<br>• FATAL—Emergency. ACS is not usable and you must take action immediately.<br>• ERROR—Critical or error condition.<br>• WARN—Normal, but significant condition. (Default)<br>• INFO—Informational message.<br>• DEBUG—Diagnostic bug message. |

*Table 18-20 Global: General Page (continued)*

| Option | Descriptions |
|---|---|
| **Configure Local Setting for Category** | |
| Log to Local Target | Check to enable logging to the local target.<br>For administrative and operational audit logging category types, logging to local target is enabled by default and cannot be disabled. |
| Local Target is Critical | *Usable for accounting and for AAA audit (passed authentication) logging category types only.* Check the check box to make this local target the critical target.<br>For administrative and operational audit logging category types, the check box is checked by default and cannot be unchecked; the local target is the critical target.<br>If you make local target as the critical target and the logging operation fails, authentication request will be rejected and accounting response will not be sent to the device. |
| **Configure Logged Attributes** | |
| — | *Display only.* All attributes are logged to the local target. |

If you have completed your configuration, proceed to Step 6.

**Step 4** To configure a remote syslog target, click the **Remote Syslog Target** and proceed to Step 5.

**Step 5** Complete the Remote Syslog Target fields as described in Table 18-21:

*Table 18-21 Global: Remote Syslog Target Page*

| Option | Description |
|---|---|
| **Configure Syslog Targets** | |
| Available targets | List of available targets. You can select a target from this list and move it to the Selected Targets list. |
| Selected targets | List of selected targets. You can select a target from this list and move it to the Available Targets list to remove it from your configuration. |

**Step 6** Click **Submit**.

The Logging Categories page appears, with your configured logging category.

---

Administrative and operational audit messages include audit messages of the following types:

- Configuration changes
- Internal user change password
- Administrator access
- Operational audit

Some of the operational audit messages are not logged in the local log target. See Table 18-22 for a list of administrative and operational logs that are not logged in the local target. See Viewing ADE-OS Logs, page 18-28 for information on how you can view these logs from the ACS CLI.

Table 18-22 lists a set of administrative and operational logs under various categories that are not logged to the local target.

***Table 18-22 Administrative and Operational Logs Not Logged in the Local Target***

| Category | Log and Description |
|---|---|
| Process-Management | • ACS_START_PROCESS—ACS process started<br>• ACS_STOP_PROCESS—ACS process stopped<br>• ACS_START—All ACS processes started<br>• ACS_STOP—All ACS processes stopped<br>• WD_RESTART_PROCESS—ACS process restarted by watchdog<br>• WD_CONFIG_CHANGE—Watchdog configuration reloaded<br>• ACS_START_STOP_ERROR—ACS process reported start/stop error |
| DB-Management | • CARS_BACKUP—CARS backup complete<br>• CARS_RESTORE—CARS restore complete<br>• ACS_BACKUP—ACS DB backup complete<br>• ACS_RESTORE—ACS DB restore complete<br>• ACS_SUPPORT—ACS support bundle collected<br>• ACS_RESET—ACS DB reset |
| File-Management | • ACS_DELETE_CORE—ACS core files deleted<br>• ACS_DELETE_LOG—ACS log files deleted |

*Table 18-22 Administrative and Operational Logs Not Logged in the Local Target (continued)*

| Category | Log and Description |
|---|---|
| Software-Management | • ACS_UPGRADE—ACS upgraded<br>• ACS_PATCH—ACS patch installed<br>• UPGRADE_SCHEMA_CHANGE—ACS schema upgrade complete<br>• UPGRADE_DICTIONARY—ACS dictionary upgrade complete<br>• UPGRADE_DATA_MANIPULATION—ACS upgrade - data manipulation stage complete<br>• UPGRADE_AAC—ACS AAC upgrade complete<br>• UPGRADE_PKI—ACS PKI upgrade complete<br>• UPGRADE_VIEW—ACS View upgrade complete<br>• CLI_ACS_UPGRADE—ACS upgrade started<br>• CLI_ACS_INSTALL—ACS install started |
| System-Management | • ACS_MIGRATION_INTERFACE—ACS migration interface enabled/disabled<br>• ACS_ADMIN_PSWD_RESET—ACS administrator password reset<br>• CLI_CLOCK_SET—Clock set<br>• CLI_TZ_SET—Time zone set<br>• CLI_NTP_SET—NTP Server set<br>• CLI_HOSTNAME_SET—Hostname set<br>• CLI_IPADDRESS_SET—IP address set<br>• CLI_IPADDRESS_STATE—IP address state<br>• CLI_DEFAULT_GATEWAY—Default gateway set<br>• CLI_NAME_SERVER—Name server set<br>• ADEOS_XFER_LIBERROR—ADE OS Xfer library error<br>• ADEOS_INSTALL_LIBERROR—ADE OS install library error<br>• AD_JOIN_ERROR—AD agent failed to join AD domain<br>• AD_JOIN_DOMAIN—AD agent joined AD domain<br>• AD_LEAVE_DOMAIN—AD agent left AD domain<br>• IMPORT_EXPORT_PROCESS_ABORTED—Import/Export process aborted<br>• IMPORT_EXPORT_PROCESS_STARTED—Import/Export process started<br>• IMPORT_EXPORT_PROCESS_COMPLETED—Import/Export process completed<br>• IMPORT_EXPORT_PROCESS_ERROR—Error while Import/Export process |

**Related Topic**

- Configuring Per-Instance Logging Categories, page 18-29
- Viewing ADE-OS Logs, page 18-28

## Viewing ADE-OS Logs

The logs listed in Table 18-22 are written to the ADE-OS logs. From the ACS CLI, you can use the following command to view the ADE-OS logs:

**show logging system**

This command lists all the ADE-OS logs and your output would be similar to the following example.

```
Sep 29 23:24:15 cd-acs5-13-179 sshd(pam_unix)[20013]: 1 more authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=10.77.137.95
user=admin
Sep 29 23:24:34 cd-acs5-13-179 sshd(pam_unix)[20017]: authentication failure; logname=
uid=0 euid=0 tty=ssh ruser= rhost=10.77.137.95 user=ad
min
Sep 29 23:24:36 cd-acs5-13-179 sshd[20017]: Failed password for admin from 10.77.137.95
port 3635 ssh2
Sep 30 00:47:44 cd-acs5-13-179 sshd(pam_unix)[20946]: authentication failure; logname=
uid=0 euid=0 tty=ssh ruser= rhost=10.77.137.95 user=ad
min
Sep 30 00:47:46 cd-acs5-13-179 sshd[20946]: Failed password for admin from 10.77.137.95
port 3953 ssh2
Sep 30 00:54:59 cd-acs5-13-179 sshd(pam_unix)[21028]: authentication failure; logname=
uid=0 euid=0 tty=ssh ruser= rhost=10.77.137.95 user=ad
min
Sep 30 00:55:01 cd-acs5-13-179 sshd[21028]: Failed password for admin from 10.77.137.95
port 3962 ssh2
Sep 30 00:55:35 cd-acs5-13-179 last message repeated 5 times
Sep 30 00:55:39 cd-acs5-13-179 sshd[21028]: Accepted password for admin from 10.77.137.95
port 3962 ssh2
Sep 30 00:55:39 cd-acs5-13-179 sshd(pam_unix)[21038]: session opened for user admin by
(uid=0)
Sep 30 00:55:40 cd-acs5-13-179 debugd[2597]: hangup signal caught, configuration read
Sep 30 00:55:40 cd-acs5-13-179 debugd[2597]: successfully loaded debug config
Sep 30 00:55:40 cd-acs5-13-179 debugd[2597]: [21043]: utils: cars_shellcfg.c[118] [admin]:
Invoked carsGetConsoleConfig
Sep 30 00:55:40 cd-acs5-13-179 debugd[2597]: [21043]: utils: cars_shellcfg.c[135] [admin]:
No Config file, returning defaults
Sep 30 01:22:20 cd-acs5-13-179 sshd[21038]: Received disconnect from 10.77.137.95: 11:
Connection discarded by broker
Sep 30 01:22:20 cd-acs5-13-179 sshd(pam_unix)[21038]: session closed for user admin
Sep 30 01:22:22 cd-acs5-13-179 debugd[2597]: hangup signal caught, configuration read
Sep 30 01:22:22 cd-acs5-13-179 debugd[2597]: successfully loaded debug config
Sep 30 02:48:54 cd-acs5-13-179 sshd[22500]: Accepted password for admin from 10.77.137.58
port 4527 ssh2
Sep 30 02:48:54 cd-acs5-13-179 sshd(pam_unix)[22504]: session opened for user admin by
(uid=0)
Sep 30 02:48:55 cd-acs5-13-179 debugd[2597]: hangup signal caught, configuration read
Sep 30 02:48:55 cd-acs5-13-179 debugd[2597]: successfully loaded debug config
```

You can view the logs grouped by the module that they belong to. For example, the monitoring and troubleshooting logs contain the string **MSGCAT** and the debug logs contain the string **debug**.

From the ACS CLI, you can enter the following two commands to view the monitoring and troubleshooting logs and the administrative logs respectively:

- **show logging system | include MSGCAT**
- **show logging system | include debug**

The output of the **show logging system | include MSGCAT** would be similar to:

```
Sep 27 13:00:02 cd-acs5-13-103 MSGCAT58010/root: info:[ACS backup] ACS backup completed
Sep 28 13:00:03 cd-acs5-13-103 MSGCAT58010/root: info:[ACS backup] ACS backup completed
Sep 29 06:28:17 cd-acs5-13-103 MSGCAT58007: Killing Tomcat 8363
```

```
Sep 29 06:28:28 cd-acs5-13-103 MSGCAT58004/admin: ACS Stopped
Sep 29 06:31:41 cd-acs5-13-103 MSGCAT58037/admin: Installing ACS
Sep 29 09:52:35 cd-acs5-13-103 MSGCAT58007: Killing Tomcat 32729
Sep 29 09:52:46 cd-acs5-13-103 MSGCAT58004/admin: ACS Stopped
Sep 29 09:53:29 cd-acs5-13-103 MSGCAT58004/admin: ACS Starting
Sep 29 10:37:45 cd-acs5-13-103 MSGCAT58018/admin: [ACS-modify-migration-state] completed
successfully - interface migration enable
Sep 29 13:00:02 cd-acs5-13-103 MSGCAT58010/root: info:[ACS backup] ACS backup completed
Sep 29 13:56:36 cd-acs5-13-103 MSGCAT58018/admin: [ACS-modify-migration-state] completed
successfully - interface migration disable
Sep 29 13:57:02 cd-acs5-13-103 MSGCAT58018/admin: [ACS-modify-migration-state] completed
successfully - interface migration disable
Sep 29 13:57:25 cd-acs5-13-103 MSGCAT58018/admin: [ACS-modify-migration-state] completed
successfully - interface migration enable
Sep 30 10:57:10 cd-acs5-13-103 MSGCAT58010/admin: info:[ACS backup] ACS backup completed
```

For more information on the **show logging** command, refer to

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.3/command/reference/cli_app_a.html#wp1917127.

## Configuring Per-Instance Logging Categories

You can define a custom logging category configuration for specific, overridden ACS instances, or return all instances to the default global logging category configuration.

To view and configure per-instance logging categories:

**Step 1** Select **System Administration > Configuration > Log Configuration > Logging Categories > Per-Instance**.

The Per-Instance page appears; from here, you can view the individual ACS instances of your deployment.

**Step 2** Click the radio button associated with the name of the ACS instance you want to configure, and choose one of these options:

- Click **Override** to override the current logging category configuration for selected ACS instances.
- Click **Configure** to display the Logging Categories page associated with the ACS instance. You can then edit the logging categories for the ACS instance. See Displaying Logging Categories, page 18-32 for field descriptions.
- Click **Restore to Global** to restore selected ACS instances to the default global logging category configuration.

Your configuration is saved and the Per-Instance page is refreshed.

### Related Topic

- Configuring Per-Instance Security and Log Settings, page 18-30

## Configuring Per-Instance Security and Log Settings

You can configure the severity level and local log settings in a logging category configuration for a specific overridden or custom ACS instance. Use this page to:

- View a tree of configured logging categories for a specific ACS instance.
- Open a page to configure a logging category's severity level, log target, and logged attributes for a specific ACS instance.

**Step 1** Select **System Administration > Configuration > Log Configuration > Logging Categories > Per-Instance**, then click **Configure**.

The Per-Instance: Configuration page appears as described in Table 18-23:

*Table 18-23 Per-Instance: Configuration Page*

| Option | Description |
|---|---|
| Name | Expandable tree structure of AAA service logging categories. |
| Edit | Click to display a selected Logging Categories > Edit: "*lc_name*" page, where *lc_name* is the name of the logging category. |

**Step 2** Do one of the following:

- Click the name of the logging category you want to configure.
- Select the radio button associated with the name of the logging category you want to configure, and click **Edit**.

The Per-Instance: General page appears.

From here, you can configure the security level and local log settings in a logging category configuration for a specific ACS instance. See Table 18-24:

*Table 18-24 Per-Instance: General Page*

| Option | Description |
|---|---|
| **Configure Log Category** | |
| Log Severity | Use the list box to select the severity level for diagnostic logging categories. (For audit and accounting categories, there is only one severity, NOTICE, which cannot be modified.) Valid options are:<br>• FATAL—Emergency. The ACS is not usable and you must take action immediately.<br>• ERROR—Critical or error condition.<br>• WARN—Normal, but significant condition. (Default)<br>• INFO—Informational message.<br>• DEBUG—Diagnostic bug message. |
| **Configure Local Setting for Category** | |
| Log to Local Target | Check to enable logging to the local target.<br>For administrative and operational audit logging category types, logging to local target is enabled by default and cannot be disabled. |
| Local Target is Critical | *Usable for accounting and for passed authentication logging category types only.* Check the check box to make this local target the critical target.<br>For administrative and operational audit logging category types, the check box is checked by default and cannot be unchecked; the local target is the critical target.<br>If you make local target as the critical target and the logging operation fails, the authentication request will be rejected and accounting response will not be sent to the device. |
| **Configure Logged Attributes** | |
| — | *Display only.* All attributes are logged to the local target. |

## Configuring Per-Instance Remote Syslog Targets

Use this page to configure remote syslog targets for logging categories.

**Step 1** Select **System Administration > Configuration > Log Configuration > Logging Categories > Per-Instance**, then click **Configure**.

The Per-Instance: Configuration page appears as described in Table 18-23.

**Step 2** Do one of the following actions:

- Click the name of the logging category you want to configure.
- Select the radio button associated with the name of the logging category you want to configure, and click **Edit**.

**Step 3** Click the **Remote Syslog Target** tab.

The Per-Instance: Remote Syslog Targets page appears as described in Table 18-25:

*Table 18-25 Per-Instance: Remote Syslog Targets Page*

| Option | Description |
|---|---|
| **Configure Syslog Targets** | |
| Available targets | List of available targets. You can select a target from this list and move it to the Selected Targets list. |
| Selected targets | List of selected targets. You can select a target from this list and move it to the Available Targets list to remove it from your configuration. |

# Displaying Logging Categories

You can view a tree of configured logging categories for a specific ACS instance. In addition, you can configure a logging category's severity level, log target, and logged attributes for a specific ACS instance.

**Step 1** Select **System Administration > Configuration > Log Configuration > Logging Categories > Per-Instance**, then click **Configure**.

**Step 2** Complete the fields as described in Table 18-26:

*Table 18-26 Per-Instance: Configuration Page*

| Option | Description |
|---|---|
| Name | Expandable tree structure of AAA services logging categories. |
| Edit | Click to display a selected Logging Categories > Edit: "*lc_name*" page, where *lc_name* is the name of the logging category. |

# Configuring the Log Collector

Use the Log Collector page to select a log data collector and suspend or resume log data transmission.

**Step 1** Select **System Administration > Configuration > Log Configuration > Log Collector**.

The Log Collector page appears.

**Step 2** Complete the Log Collector fields as described in Table 18-27:

*Table 18-27 Log Collector Page*

| Option | Description |
|---|---|
| **Log Data Collector** | |
| Current Log Collector | *Display only.* Identifies the machine on which the local log messages are sent. |
| Select Log Collector | Use the drop-down list box to select the machine on which you want local log messages sent. |
| Set Log Collector | Click to configure the log collector according to the selection you make in the Select Log Collector option. |

**Step 3** Do one of the following:

- Click **Suspend** to suspend the log data transmission to the configured log collector.
- Click **Resume** to resume the log data transmission to the configured log collector.

Your configuration is saved and the Log Collector page is refreshed.

# Viewing the Log Message Catalog

Use the Log Message Catalog page to view all possible log messages.

Select **System Administration > Configuration > Log Configuration > Log Message Catalog**.

The Log Message Catalog page appears, with the fields described in Table 18-28, from which you can view all possible log messages that can appear in your log files.

*Table 18-28 Log Messages Page*

| Option | Description |
|---|---|
| Message Code | *Display only.* A unique message code identification number associated with a message. |
| Severity | *Display only.* The severity level associated with a message. |
| Category | *Display only.* The logging category to which a message belongs. |
| Message Class | *Display only.* The group to which a message belongs. |
| Message Text | *Display only.* English language message text (name of the message). |
| Description | Display only. English language text that describes the associated message. |

# Licensing Overview

To operate ACS, you must install a valid license. ACS prompts you to install a valid base license when you first access the web interface. Each ACS instance (primary or secondary) in a distributed deployment requires a unique base license.

**Note** Each server requires a unique base license in a distributed deployment.

## Types of Licenses

Table 18-29 shows the ACS 5.3 license support:

*Table 18-29 ACS License Support*

| License | Description |
|---|---|
| Base License | Required for all software instances deployed, as well as for all appliances. The base license enables you to use all the ACS functionality except license controlled features, and it enables all reporting features. Base license is:<br>• Required for each ACS instance, primary and secondary.<br>• Required for all appliances.<br>• Supports deployments with up to 500 managed devices.<br>Base licenses are of three types:<br>• Permanent—Supports up to 500 devices.<br>• Eval—Supports up to 50 devices and expires in 90 days.<br>The number of devices is determined by the number of unique IP addresses that you configure. This includes the subnet masks that you configure. For example, a subnet mask of 255.255.255.0 implies 256 unique IP addresses and hence the number of devices is 256.<br>If your evaluation license expires or is about to expire, you cannot use another evaluation license or extend your current license. Before your evaluation license expires, you must upgrade to a Permanent license. |
| Add-on Licenses | Supports an unlimited number of managed devices. Requires an existing ACS permanent base license. There are also evaluation-type licenses for add-on licenses.<br>The Security Group Access feature licenses are of three types: Permanent, Eval, and NFR. However, the permanent Security Group Access feature license can be used only with a permanent base license.<br>Also, the large deployment license can only be used only with a permanent base license. |
| Evaluation License (standard) | Enables standard centralized reporting features.<br>• Cannot be reused on the same platform.<br>• You can only install one evaluation license per platform. You cannot install additional evaluation licenses.<br>• Supports 50 managed devices.<br>• Expires 90 days from the time the license is installed. |

**Related Topics**

- Licensing Overview, page 18-34
- Installing a License File, page 18-35
- Viewing the Base License, page 18-36
- Adding Deployment License Files, page 18-39
- Deleting Deployment License Files, page 18-40

# Installing a License File

You can obtain a valid license file using the Product Activation Key (PAK) supplied with the product. To install a license file:

**Step 1** Log into the ACS web interface.

The Initial Licenses page appears when you log in to the ACS machine for the first time.

**Step 2** Click **Cisco Secure ACS License Registration.**

This link directs you to Cisco.com to purchase a valid license file from a Cisco representative.

**Step 3** Click **Install** to install the license file that you purchased.

The ACS web interface log in page reappears. You can now work with the ACS application.

**Note** You cannot upgrade a base permanent license. You can only upgrade a base evaluation license.

**Related Topics**

- Licensing Overview, page 18-34
- Viewing the Base License, page 18-36
- Adding Deployment License Files, page 18-39
- Deleting Deployment License Files, page 18-40

# Viewing the Base License

To upgrade the base license:

**Step 1** Select **System Administration > Configuration > Licensing > Base Server License**.

The Base Server License page appears with a description of the ACS deployment configuration and a list of the available deployment licenses. See Types of Licenses for a list of deployment licenses.

Table 18-30 describes the fields in the Base Server License page.

***Table 18-30 Base Server License Page***

| Option | Description |
|---|---|
| **ACS Deployment Configuration** | |
| Primary ACS Instance | Name of the primary instance created when you logged into the ACS 5.3 web interface. |
| Number of Instances | Current number of ACS instances (primary or secondary) in the ACS database. |
| Current Number of Configured IP Addresses in Network Devices | Total number of IP addresses in all the subnetworks that you have configured as part of network device configuration.<br>The number of devices is determined by the number of unique IP addresses that you configure. This includes the subnet masks that you configure. For example, a subnet mask of 255.255.255.0 implies 256 unique IP addresses and hence the number of devices is 256. |
| Maximum Number of IP Addresses in Network Devices | Maximum number of IP addresses that your license supports:<br>• Base License—Supports 500 IP addresses.<br>The number of devices is determined by the number of unique IP addresses that you configure. This includes the subnet masks that you configure. For example, a subnet mask of 255.255.255.0 implies 256 unique IP addresses and hence the number of devices is 256.<br>• Large Deployment—Supports an unlimited number of IP addresses. |
| Use this link to obtain a valid License File | Directs you to Cisco.com to generate a valid license file using the Product Activation Key (PAK) |
| **Base License Configuration** | |
| ACS Instance | Name of the ACS instance, either primary or secondary. |
| Identifier | Name of the base license. |
| License Type | Specifies the base license type (permanent, evaluation). |
| Expiration | Specifies the expiration date for evaluation licenses. For permanent licenses, the expiration field indicates *permanent*. |
| Licensed to | Name of the company that this product is licensed to. |
| PAK | Name of the Product Activation Key (PAK) received from Cisco. |
| Version | Current version of the ACS software. |

You can select one or more radio buttons next to the instance whose license you want to upgrade.

**Step 2** Click **Upgrade**. See Upgrading the Base Server License, page 18-37 for valid field options.

### Related Topic

- Upgrading the Base Server License, page 18-37

# Upgrading the Base Server License

You can upgrade the base server license.

**Step 1** Select **System Administration > Configuration > Licensing > Base Server License**.

The Base Server License page appears with a description of the ACS deployment configuration and a list of the available deployment licenses. See Types of Licenses for a list of deployment licenses.

**Step 2** Select a license, then click **Upgrade**.

The Base Server License Edit page appears.

**Step 3** Complete the fields as described in Table 18-31:

*Table 18-31 Base Server License Edit Page*

| Option | Description |
|---|---|
| **ACS Instance License Configuration** | |
| Version | Displays the current version of the ACS software. |
| ACS Instance | Displays the name of the ACS instance, either primary or secondary. |
| License Type | Specifies the license type. |
| Use this link to obtain a valid License File | Directs you to Cisco.com to purchase a valid license file from a Cisco representative. |
| **License Location** | |
| License File | Click **Browse** to navigate to the directory that contains the license file and select it. |

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

### Related Topics

- Licensing Overview, page 18-34
- Types of Licenses, page 18-34
- Installing a License File, page 18-35
- Adding Deployment License Files, page 18-39
- Deleting Deployment License Files, page 18-40

# Viewing License Feature Options

You can add, upgrade, or delete existing deployment licenses. The configuration pane at the top of the page shows the deployment information.

Select **System Administration > Configuration > Licensing > Feature Options**.

The Feature Options Page appears as described in Table 18-32:

*Table 18-32 Feature Options Page*

| Option | Description |
|---|---|
| **ACS Deployment Configuration** | |
| Primary ACS Instance | Name of the primary instance created when you login into the ACS 5.3 web interface. |
| Number of Instances | Current number of ACS instances (primary or secondary) in the ACS database. |
| Current Number of Configured IP Addresses in Network Devices | Total number of IP addresses in all the subnetworks that you have configured as part of network device configuration.<br>The number of devices is determined by the number of unique IP addresses that you configure. This includes the subnet masks that you configure. For example, a subnet mask of 255.255.255.0 implies 256 unique IP addresses and hence the number of devices is 256. |
| Maximum Number of IP Addresses in Network Devices | Maximum number of IP addresses that your license supports:<br>• Base License—Supports 500 IP addresses.<br>The number of devices is determined by the number of unique IP addresses that you configure. This includes the subnet masks that you configure. For example, a subnet mask of 255.255.255.0 implies 256 unique IP addresses and hence the number of devices is 256.<br>• Large Deployment—Supports an unlimited number of IP addresses. |
| Use this link to obtain a valid License File | Directs you to Cisco.com to purchase a valid license file from a Cisco representative. |
| **Installed Deployment License Options** | |
| Feature | • Large Deployment—Supports an unlimited number of managed devices.<br>• Security Group Access Control—Enables Cisco Trusted Server (SGA) management functionality. This requires an existing ACS base license. |
| Licensed to | Name of the company that this product is licensed to. |
| License Type | Specifies the license type (permanent, evaluation). |
| Expiration | Expiration date for the following features:<br>• Large Deployment<br>• SGA |
| Add/Upgrade | Click **Add/Upgrade** to access the Viewing License Feature Options and add a license file. |
| Delete | Select the radio button next to the license feature you wish to delete and click **Delete**. |

# Adding Deployment License Files

To add a new base deployment license file:

**Step 1** Select **System Administration > Configuration > Licensing > Feature Options**.

The Feature Options page appears with a description of the ACS deployment configuration and a list of the available deployment licenses and their configurations. See Add-on Licenses in Types of Licenses for a list of deployment licenses. See Viewing License Feature Options, page 18-38 for field descriptions.

**Step 2** Click **Add.**

The Feature Options Create page appears.

**Step 3** Complete the fields as described in Table 18-33 to add a license:

*Table 18-33 Feature Options Create Page*

| Option | Description |
|---|---|
| **ACS Deployment Configuration** | |
| Primary ACS Instance | Name of the primary instance created when you login into the ACS 5.3 web interface. |
| Number of Instances | Current number of ACS instances (primary or secondary) in the ACS database. |
| Current Number of Configured IP Addresses in Network Devices | Total number of IP addresses in all the subnetworks that you have configured as part of network device configuration.<br>The number of devices is determined by the number of unique IP addresses that you configure. This includes the subnet masks that you configure. For example, a subnet mask of 255.255.255.0 implies 256 unique IP addresses and hence the number of devices is 256. |
| Maximum Number of IP Addresses in Network Devices | Maximum number of IP addresses that your license supports:<br>• Base License—Supports 500 IP addresses.<br>The number of devices is determined by the number of unique IP addresses that you configure. This includes the subnet masks that you configure. For example, a subnet mask of 255.255.255.0 implies 256 unique IP addresses and hence the number of devices is 256.<br>• Large Deployment—Supports an unlimited number of IP addresses. |
| Use this link to obtain a valid License File | Directs you to Cisco.com to purchase a valid license file from a Cisco representative. |
| **License Location** | |
| License File | Click **Browse** to browse to the location of the purchased license file you wish to install and select it. |

**Step 4** Click **Submit** to download the license file.

The Feature Options page appears with the additional license.

**Related Topics**

- Licensing Overview, page 18-34
- Types of Licenses, page 18-34
- Installing a License File, page 18-35
- Viewing the Base License, page 18-36
- Deleting Deployment License Files, page 18-40

# Deleting Deployment License Files

To delete deployment license files:

**Step 1** Select **System Administration > Configuration > Licensing > Feature Options**.

The Feature Options page appears with a description of the ACS deployment configuration and a list of the available deployment licenses and their configurations. See Add-on Licenses in Types of Licenses for a list of deployment licenses. See the Table 18-32 for field descriptions.

**Step 2** Select the radio button next to the deployment you wish to delete.

**Step 3** Click **Delete to delete the license file.**

**Related Topics**

- Licensing Overview, page 18-34
- Types of Licenses, page 18-34
- Installing a License File, page 18-35
- Viewing the Base License, page 18-36
- Adding Deployment License Files, page 18-39

# Available Downloads

This section contains information about the utilities and files that are available for download from the ACS web interface:

- Downloading Migration Utility Files, page 18-41
- Downloading UCP Web Service Files, page 18-41
- Downloading Sample Python Scripts, page 18-41
- Downloading Rest Services, page 18-42

# Downloading Migration Utility Files

To download migration application files and the migration guide for ACS 5.3:

**Step 1** Choose **System Administration > Downloads > Migration Utility**.

The Migration from 4.x page appears.

**Step 2** Click **Migration application files**, to download the application file you want to use to run the migration utility.

**Step 3** Click **Migration Guide**, to download *Migration Guide for the Cisco Secure Access Control System 5.3*.

# Downloading UCP Web Service Files

You can download the WSDL file from this page to integrate ACS with your in-house portals and allow ACS users configured in the ACS internal identity store to change their own passwords. The UCP web service allows only the users to change their passwords. They can do so on the primary or secondary ACS servers.

The UCP web service compares the new password that you provide with the password policy that is configured in ACS for users. If the new password conforms to the defined criteria, your new password takes effect. After your password is changed on the primary ACS server, ACS replicates it to all the secondary ACS servers.

To download the UCP WSDL Files:

**Step 1** Choose **System Administration > Downloads > User Change Password**.

The User Change Password (UCP) web service page appears.

**Step 2** Click one of the following:

- **UCP WSDL** to download the WSDL file.
- **UCP Web application example** to download the application file.
- **Python Script for Using the User Change Password Web Service** to download a sample Python script.

For more information on how to use the UCP web service, refer to

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.3/sdk/ucp.html.

# Downloading Sample Python Scripts

The Scripts page contains sample Python scripts for:

- Using the UCP web service.
- Automating the bulk import and export operations.

To download these sample scripts:

**Step 1** Choose **System Administration > Downloads > Sample Python Scripts**.

The Sample Python Scripts page appears.

**Step 2** Click one of the following:

- **Python Script for Using the User Change Password Web Service**—To download the sample script for the UCP web service.
- **Python Script for Performing CRUD Operations on ACS Objects**—To download the sample script for the import and export process.

**Step 3** Save the script to your local hard drive.

The scripts come with installation instructions. For more information on how to use the scripts, refer to

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.3/sdk/acs_sdk.html.

**Note** The Cisco Technical Assistance Center (TAC) supports only the default Python Script. TAC does not offer any support for modified scripts.

# Downloading Rest Services

ACS Rest Service allows to create, update, delete and retrieve objects from ACS Database.

**Note** You must enable the Rest Service using the command line for reading the WADL files.

To download ACS Rest Service WADL files:

**Step 1** Choose **System Administration > Downloads > Rest Service**.

The Rest Service Page appears.

**Step 2** Click one of the following:

- **Common or Identity**—To download XSD files that describe the structure of the objects supported on ACS 5.3 Rest interfaces.
- **Schema files**—To download the Schema files.
- **SDK Samples**—To download the SDK Samples.

For more information on how to use the Rest Services, refer to

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.3/sdk/rest.html.