Managing Access Policies

In ACS 5.8, policy drives all activities. Policies consist mainly of rules that determine the action of the policy. You create access services to define authentication and authorization policies for requests. A global service selection policy contains rules that determine which access service processes an incoming request.

For a basic work flow for configuring policies and all their elements, see Flows for Configuring Services and Policies, page 3-19. In general, before you can configure policy rules, you must configure all the elements that you will need, such as identities, conditions, and authorizations and permissions.

For information about:

- Managing identities, see Managing Users and Identity Stores, page 8-1
- Configuring conditions, see Managing Policy Elements, page 9-1.
- Configuring authorizations and permissions, see 17, page 17-1.

This section contains the following topics:

For information about creating Egress and NDAC policies for Cisco Security Group Access, see Configuring an NDAC Policy, page 4-24.

Policy Creation Flow

Policy creation depends on your network configuration and the degree of refinement that you want to bring to individual policies. The endpoint of policy creation is the access service that runs as the result of the service selection policy. Each policy is rule driven.

In short, you must determine the:

- Details of your network configuration.
- Access services that implement your policies.
- Rules that define the conditions under which an access service can run.

This section contains the following topics:

Network Definition and Policy Goals

The first step in creating a policy is to determine the devices and users for which the policy should apply. Then you can start to configure your policy elements.

For basic policy creation, you can rely on the order of the drawers in the left navigation pane of the web interface. The order of the drawers is helpful because some policy elements are dependent on other policy elements. If you use the policy drawers in order, you initially avoid having to go backward to define elements that your current drawer requires.

For example, you might want to create a simple device administration policy from these elements in your network configuration:

- Devices—Routers and switches.
- Users—Network engineers.
- Device Groups—Group devices by location and separately by device type.
- Identity groups—Group network engineers by location and separately by access level.

The results of the policy apply to the administrative staff at each site:

- Full access to devices at their site.
- Read-only access to all other devices.
- Full access to everything for a supervisor.

The policy itself applies to network operations and the administrators who will have privileges within the device administration policy. The users (network engineers) are stored in the internal identity store.

The policy results are the authorizations and permissions applied in response to the access request. These authorizations and permissions are also configured as policy elements.

Policy Creation Flow—Next Steps

- Policy Elements in the Policy Creation Flow, page 10-2
- Access Service Policy Creation, page 10-4
- Service Selection Policy Creation, page 10-4

Policy Elements in the Policy Creation Flow

The web interface provides these defaults for defining device groups and identity groups:

- All Locations

- All Device Types
- All Groups

The locations, device types, and identity groups that you create are children of these defaults.

To create the building blocks for a basic device administration policy:

Step 1 Create network resources. In the Network Resources drawer, create:

- Device groups for Locations, such as All Locations > East, West, HQ.
- Device groups for device types, such as All Device Types > Router, Switch.
- AAA clients (clients for AAA switches and routers, address for each, and protocol for each), such as EAST-ACCESS-SWITCH, HQ-CORE-SWITCH, or WEST-WAN-ROUTER.

Step 2 Create users and identity stores. In the Users and Identity Stores drawer, create:

- Identity groups (Network Operations and Supervisor).
- Specific users and association to identity groups (Names, Identity Group, Password, and more).

Step 3 Create authorizations and permissions for device administration. In the Policy Elements drawer, create:

- Specific privileges (in Shell Profiles), such as full access or read only.
- Command Sets that allow or deny access (in Command Sets).

For this policy, you now have the following building blocks:

- Network Device Groups (NDGs), such as:
  - Locations—East, HQ, West.
  - Device Types—Router, Switch.
- Identity groups, such as:
  - Network Operations Sites—East, HQ, West.
  - Access levels—Full Access.
- Devices—Routers and switches that have been assigned to network device groups.
- Users—Network engineers in the internal identity store that have been assigned to identity groups.
- Shell Profiles—Privileges that can apply to each administrator, such as:
  - Full privileges.
  - Read only privileges.
- Command Sets—Allow or deny authorization to each administrator.

Policy Creation Flow—Previous Step

- Network Definition and Policy Goals, page 10-2

Policy Creation Flow—Next Steps

- Access Service Policy Creation, page 10-4
- Service Selection Policy Creation, page 10-4

Access Service Policy Creation

After you create the basic elements, you can create an access policy that includes identity groups and privileges. For example, you can create an access service for device administration, called NetOps, which contains authorization and authentication policies that use this data:

- Users in the Supervisor identity group—Full privileges to all devices at all locations.
- User in the East, HQ, West identity groups—Full privileges to devices in the corresponding East, HQ, West device groups.
- If no match—Deny access.

Policy Creation Flow—Previous Steps

- Network Definition and Policy Goals, page 10-2
- Policy Elements in the Policy Creation Flow, page 10-2

Policy Creation Flow—Next Step

- Service Selection Policy Creation, page 10-4

Service Selection Policy Creation

ACS provides support for various access use cases; for example, device administration, wireless access, network access control, and so on. You can create access policies for each of these use cases. Your service selection policy determines which access policy applies to an incoming request.

For example, you can create a service selection rule to apply the NetOps access service to any access request that uses the TACAC+ protocol.

Policy Creation Flow—Previous Steps

- Network Definition and Policy Goals, page 10-2
- Policy Elements in the Policy Creation Flow, page 10-2
- Access Service Policy Creation, page 10-4

Customizing a Policy

ACS policy rules contain conditions and results. Before you begin to define rules for a policy, you must configure which types of conditions that policy will contain. This step is called customizing your policy. The condition types that you choose appear on the Policy page. You can apply only those types of conditions that appear on the Policy page. For information about policy conditions, see Managing Policy Conditions, page 9-1.

By default, a Policy page displays a single condition column for compound expressions. For information on compound conditions, see Configuring Compound Conditions, page 10-41.

If you have implemented Security Group Access functionality, you can also customize results for authorization policies.

Caution If you have already defined rules, be certain that a rule is not using any condition that you remove when customizing conditions. Removing a condition column removes all configured conditions that exist for that column.

To customize a policy:

Step 1 Open the Policy page that you want to customize. For:

- The service selection policy, choose **Access Policies > Service Selection Policy**.
- An access service policy, choose **Access Policies > Access Services > *service* > *policy***, where *service* is the name of the access service, and *policy* is the name of the policy that you want to customize.

Step 2 In the Policy page, click **Customize**.

A list of conditions appears. This list includes identity attributes, system conditions, and custom conditions.

Note Identity-related attributes are not available as conditions in a service selection policy.

Step 3 Move conditions between the Available and Selected list boxes.

Step 4 Click **OK**

The selected conditions now appear under the Conditions column.

Step 5 Click **Save Changes**.

Configuring a Policy—Next Steps

- Configuring the Service Selection Policy, page 10-5
- Configuring Access Service Policies, page 10-23

Configuring the Service Selection Policy

The service selection policy determines which access service processes incoming requests. You can configure a simple policy, which applies the same access service to all requests; or, you can configure a rule-based service selection policy.

In the rule-based policy, each service selection rule contains one or more conditions and a result, which is the access service to apply to an incoming request. You can create, duplicate, edit, and delete rules within the service selection policy, and you can enable and disable them.

This section contains the following topics:

- Configuring a Simple Service Selection Policy, page 10-6
- Creating, Duplicating, and Editing Service Selection Rules, page 10-8

Note If you create and save a simple policy, and then change to a rule-based policy, the simple policy becomes the default rule of the rule-based policy. If you have saved a rule-based policy and then change to a simple policy, you will lose all your rules except for the default rule. ACS automatically uses the default rule as the simple policy.

Configuring a Simple Service Selection Policy

A simple service selection policy applies the same access service to all requests.

To configure a simple service selection policy:

Step 1 Select **Access Policies > Service Selection Policy**.

By default, the Simple Service Selection Policy page appears.

Step 2 Select an access service to apply; or, choose **Deny Access**.

Step 3 Click **Save Changes** to save the policy.

Service Selection Policy Page

Use this page to configure a simple or rule-based policy to determine which service to apply to incoming requests.

To display this page, choose **Access Policies > Service Selection**.

If you have already configured the service selection policy, the corresponding Simple Policy page (see Table 10-1) or Rule-based Policy page (see Table 10-2) opens; otherwise, the Simple Policy page opens by default.

Table 10-1 Simple Service Selection Policy Page

Option	Description
Policy type	Defines the type of policy: • Select one result—The results apply to all requests. Rule-based result selection—Configuration rules apply different results depending on the request.
Service Selection Policy	Access service to apply to all requests. The default is Deny Access.

Table 10-2 Rule-based Service Selection Policy Page

Option	Description
Policy type	Defines the type of policy to configure: • Select one result—Results apply to all requests. • Rule-based result selection—Configuration rules apply different results depending on the request.
Status	Current status of the rule that drives service selection. The rule statuses are: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor Only—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Name	Rule name.
Conditions	Conditions that determine the scope of the service. This column displays all current conditions in subcolumns. You cannot use identity-based conditions in a service selection rule.
Results	Service that runs as a result of the evaluation of the rule.
Hit Count	Number of times that the rule is matched. Click **Hit Count** to refresh and reset this column.
Default Rule	ACS applies the Default rule when: • Enabled rules are not matched. • No other rules are defined. Click the link to edit the Default Rule. You can edit only the results of the Default Rule; you cannot delete, disable, or duplicate it.
Customize button	Opens the Customize page in which you choose the types of conditions to use in policy rules. A new Conditions column appears in the Policy page for each condition that you add. **Caution** If you remove a condition type after defining rules, you will lose any conditions that you configured for that condition type.
Hit Count button	Opens a window that enables you to reset and refresh the Hit Count display in the Policy page. See Displaying Hit Counts, page 10-10.

To configure a rule-based service selection policy, see these topics:

- Creating, Duplicating, and Editing Service Selection Rules, page 10-8
- Deleting Service Selection Rules, page 10-10

After you configure your service selection policy, you can continue to configure your access service policies. See Configuring Access Service Policies, page 10-23.

Creating, Duplicating, and Editing Service Selection Rules

Create service selection rules to determine which access service processes incoming requests. The Default Rule provides a default access service in cases where no rules are matched or defined.

When you create rules, remember that the order of the rules is important. When ACS encounters a match as it processes the request of a client that tries to access the ACS network, all further processing stops and the associated result of that match is found. No further rules are considered after a match is found.

You can duplicate a service selection rule to create a new rule that is the same, or very similar to, an existing rule. The duplicate rule name is based on the original rule with parentheses to indicate duplication; for example, Rule-1(1). After duplication is complete, you access each rule (original and duplicated) separately. You cannot duplicate the Default rule.

You can edit all values of service selection rules; you can edit the specified access service in the Default rule.

Note To configure a simple policy to apply the same access service to all requests, see Configuring a Simple Service Selection Policy, page 10-6.

Before You Begin

- Configure the conditions that you want to use in the service selection policy. See Managing Policy Conditions, page 9-1.

Note Identity-related attributes are not available as conditions in a service selection policy.

- Create the access services that you want to use in the service selection policy. See Creating, Duplicating, and Editing Access Services, page 10-12. You do not need to configure policies in the access service before configuring the service selection policy.
- Configure the types of conditions to use in the policy rules. See Customizing a Policy, page 10-4, for more information.

To create, duplicate, or edit a service selection policy rule:

Step 1 Select **Access Policies > Service Selection Policy**. If you:

- Previously created a rule-based policy, the Rule-Based Service Selection Policy page appears with a list of configured rules.
- Have not created a rule-based policy, the Simple Service Selection Policy page appears. Click **Rule-Based**.

Step 2 Do one of the following:

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

The Rule page appears.

Step 3 Enter or modify values:

- User-defined rules—You can edit any value. Ensure that you include at least one condition. If you are duplicating a rule, you must change the rule name.

- The Default Rule—You can change only the access service.

See Table 10-3 for field descriptions:

Table 10-3 Service Selection Rule Properties Page

Option	Description
General	
Name	Name of the rule. If you are duplicating a rule, you must enter a unique name as a minimum configuration; all other fields are optional.
Status	Rule statuses are: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor Only—The rule is active but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The Monitor option is especially useful for watching the results of a new rule.
Conditions	
conditions	Conditions that you can configure for the rule. By default, the compound condition appears. Click **Customize** in the Policy page to change the conditions that appear. The default value for each condition is *ANY*. To change the value for a condition, check the condition check box, then specify the value. If you check **Compound Condition**, an expression builder appears in the conditions frame. For more information, see Configuring Compound Conditions, page 10-41. **Note** The service selection policy, which contains a compound condition with TACACS+ username, does not work consistently. The policy works only when the first TACACS+ authentication request contains a username. If the first packet does not have the username and when ACS requests NAS for the username, the TACACS+ username condition is not matched. Therefore, the request meets the default deny access condition and fails to meet the proper access service. It is recommended to use the other TACACS+ attributes such as remote address, existing in the first request, to the rule condition.
Results	
Service	Name of the access service that runs as a result of the evaluation of the rule.

Step 4 Click **OK.**

The Service Selection Policy page appears with the rule that you configured.

Step 5 Click **Save Changes**.

Related Topics

- Configuring Access Services, page 10-11
- Deleting Service Selection Rules, page 10-10

Displaying Hit Counts

Use this page to reset and refresh the Hit Count display on the Rule-based Policy page.

To display this page, click **Hit Count** on the Rule-based Policy page.

Table 10-4 Hit Count Page

Option	Description
Hit Counts Reset	
Last time hit counts were reset for this policy	Displays the date and time of the last hit count reset for this policy.
Reset hit counts display for this policy	Click **Reset** to reset the hit counts display to zero (0) for all rules on the Policy page.
Hit Counts Collection	
Hit counts are collected every:	Displays the interval between hit count collections.
Last time hit counts were collected for this policy:	Displays the date and time of the last hit count update for this policy.
Refresh hit counts display for this policy	Click **Refresh** to refresh the hit count display in the Policy page with updated hit counts for all rules. The previous hit counts are deleted. When a TACACS+ authentication request succeeds, the hit counts of the corresponding identity policy rule and authorization policy rule both increase by 1.

Deleting Service Selection Rules

Note You cannot delete the Default service selection rule.

To delete a service selection rule:

Step 1 Select **Access Policies > Service Selection Policy**.

The Service Selection Policy page appears, with a list of configured rules.

Step 2 Check one or more check boxes the rules that you want to delete.

Step 3 Click **Delete**.

The Service Selection Rules page appears without the deleted rule(s).

Step 4 Click **Save Changes** to save the new configuration.

Configuring Access Services

Access services contain the authentication and authorization policies for requests. You can create separate access services for different use cases; for example, device administration, wireless network access, and so on.

When you create an access service, you define the type of policies and policy structures that it contains; for example, policies for device administration or network access.

Note You must create access services before you define service selection rules, although you do not need to define the policies in the services.

This section contains the following topics:

- Creating, Duplicating, and Editing Access Services, page 10-12
- Deleting an Access Service, page 10-22

After you create an access service, you can use it in the service selection policy. See Configuring the Service Selection Policy, page 10-5.

You can customize and modify the policies in the access service. See Configuring Access Service Policies, page 10-23.

Related Topic

- Creating, Duplicating, and Editing Access Services, page 10-12

Editing Default Access Services

ACS 5.8 is preconfigured with two default access services, one for device administration and another for network access. You can edit these access services.

To edit the default access service:

Step 1 Choose one of the following:

- **Access Policies > Access Services > Default Device Admin**
- **Access Policies > Access Services > Default Network Access**

The Default *Service* Access Service Edit page appears.

Step 2 Edit the fields in the Default *Service* Access Service page.

Table 10-5 describes the fields in the General tab.

Table 10-5 Default Access Service - General Page

Option	Description
General	
Name	Name of the access service.
Description	Description of the access service.
Service Type	(Display only) Type of service, device administration, or network access.
Policy Structure	

Table 10-5 Default Access Service - General Page

Option	Description
Identity	Check to include an identity policy in the access service, to define the identity store or stores that ACS uses for authentication and attribute retrieval.
Group Mapping	Check to include a group mapping policy in the access service, to map groups and attributes that are retrieved from external identity stores to the identity groups in ACS.
Authorization	Check to include an authorization policy in the access service, to apply: • Authorization profiles for network access services. • Shell profiles and command sets for device administration services.

Step 3 Edit the fields in the Allowed Protocols tab as described in Table 10-7.

Step 4 Click **Submit** to save the changes you have made to the default access service.

Creating, Duplicating, and Editing Access Services

Access services contain the authentication and authorization policies for requests.

When you create an access service, you define:

- Policy structure—The types of policies the service will contain. You can define these according to a service template, an existing service, or a use case.

  A service can contain:

  - An Identity policy—Defines which identity store to use for authentication.
  - A group mapping policy—Defines the identity group to which to map.
  - An Authorization policy—For network access, this policy defines which session authorization profile to apply; for device administration, it defines which shell profile or command set to apply.
- Allowed protocols—Specifies which authentication protocols are allowed for this access service, and provides additional information about how ACS uses them for authentication.

Use a service template to define an access service with policies that are customized to use specific condition types. See Configuring Access Services Templates, page 10-21 for information about the service templates.

Duplicate an access service to create a new access service with rules that are the same, or very similar to, an existing access service. After duplication is complete, you access each service (original and duplicated) separately.

To replicate a service policy structure without duplicating the source service's rules, create a new access service based on an existing service.

To create, duplicate, or edit an access service:

Step 1 Select **Access Policies > Access Services**.

The Access Services page appears with a list of configured services.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box the access service that you want to duplicate; then click **Duplicate**.
- Click the access service name that you want to modify; or, check the check box the name and click **Edit**.
- Click the access service name in the left navigation tab.

The Access Service Properties General page appears.

- If you are creating a new access service:
  - Define the name and policy structure of the access service.
  - Click **Next** to proceed to the Allowed Protocols page.
  - Click **Finish** to save the new access service.
- If you are duplicating or editing an access service:
  - Modify fields in the Properties page tabs as required. You can add policies, but you cannot remove existing policies.
  - Click **Submit** to save changes.

For information about valid field options, see:

- Configuring General Access Service Properties, page 10-13
- Configuring Access Service Allowed Protocols, page 10-16
- Configuring Access Services Templates, page 10-21

The access service configuration is saved. The Access Services page appears with the new configuration.

Related Topics

- Deleting an Access Service, page 10-22
- Configuring Access Service Policies, page 10-23
- Configuring the Service Selection Policy, page 10-5

Configuring General Access Service Properties

Access service definitions contain general and allowed protocol information. When you duplicate and edit services, the Access Service properties page contains tabs.

Step 1 Select **Access Policies > Access Services**, then click **Create**, **Duplicate**, or **Edit**.

Step 2 Complete the fields as described in Table 10-6:

Table 10-6 Access Service Properties—General Page

Option	Description
General	
Name	Name of the access service. If you are duplicating a service, you must enter a unique name as a minimum configuration; all other fields are optional.

Table 10-6 Access Service Properties—General Page (continued)

Option	Description
Description	Description of the access service.
Access Service Policy Structure	
Based on service template	Creates an access service containing policies based on a predefined template. This option is available only for service creation.
Based on existing service	Creates an access service containing policies based on an existing access service. The new access service does not include the existing service's policy rules. This option is available only for service creation.To replicate a service, including its policy rules, duplicate an existing access service.
User selected service type	Provides you the option to select the access service type. The available options are Network Access, Device Administration, and External Proxy. The list of policies you can configure depends on your choice of access service type.
User Selected Service Type—Network Access and Device Administration	
Policy Structure	
Identity	Check to include an identity policy in the access service to define the identity store or stores that ACS uses for authentication and attribute retrieval.
Group Mapping	Check to include a group mapping policy in the access service to map groups and attributes that are retrieved from external identity stores to ACS identity groups.
Authorization	Check to include an authorization policy in the access service to apply: • Authorization profiles for network access services. • Shell profiles and command sets for device administration services.
User Selected Service Type—External Proxy	
External Proxy Servers—Select the set of external servers to be used for proxies. You can also determine the order in which these servers are used.	
Available External Proxy Servers	List of available external RADIUS and TACACS+ servers. Select the external servers to be used for proxy and move them to the Selected External Proxy Servers list.
Selected External Proxy Servers	List of selected external proxy servers.
Advanced Options	
Accounting	
Remote Accounting	Check to enable remote accounting.
Local Accounting	Check to enable local accounting.
Username Prefix\Suffix Stripping	
Strip start of subject name up to the first occurrence of the separator	Check to strip the username from the prefix. For example, if the subject name is acme\smith and the separator is \, the username becomes smith. The default separator is \.
Strip end of subject name from the last occurrence of the separator	Check to strip the username from the suffix. For example, if the subject name is smith@acme.com and the separator is @, the username becomes smith. The default separator is @.
RADIUS INBOUND Attributes Injection—The RADIUS INBOUND attributes section is used for manipulating the incoming attributes before sending them to the proxy server.	

Table 10-6 Access Service Properties—General Page (continued)

Option	Description
Add	After you define a RADIUS incoming attribute, click **ADD** to add it to the RADIUS attributes list.
Edit	To edit the listed RADIUS incoming attribute, select the attribute in the list and click **Edit**. The attribute properties appear in the fields. Modify the properties as required, then click **Replace**.
Replace	Click **Replace** to replace the selected RADIUS incoming attribute with the value that is currently defined in this field.
Delete	Click **Delete** to delete the selected RADIUS incoming attribute from the list.
Dictionary Type	Choose the dictionary that contains the RADIUS incoming attribute you want to use.
RADIUS Attribute	Name of the RADIUS attribute. Click **Select** to choose a RADIUS attribute from the specified dictionary.
Attribute Type	Type of the selected RADIUS attribute. Client vendor type of the attribute, from which ACS allows access requests. For a description of the attribute types, refer to Cisco IOS documentation for the Cisco IOS Software release that is running on your AAA clients.
Operation	You can perform the following three operations: • Choose **ADD** to add a new attribute value for the selected RADIUS attribute: – If Multiple not allowed—adds the new value for the selected attribute only if this attribute does not exists on the request. – If Multiple allowed—always adds the attribute with a new value. • Choose **UPDATE** to update the existing value of a selected RADIUS attribute: – If Multiple not allowed—updates the attribute value with the new value if the attribute exists on the request. – If Multiple allowed—removes all occurrences of this attribute and adds one attribute with the new value. – If the attribute is a cisco-avpair (pair of key=value), the update is done according to the key. • Choose **DELETE** to delete the value of the selected RADIUS attribute. The attribute operations statements are ordered. The administrator can change the statement's order at the time of configuration. ACS performs the operation on the attributes according to the configured order. For more information on this, see RADIUS Attribute Rewrite Operation, page 4-29.
Attribute New Value	Enter a new value for the selected RADIUS incoming attribute. This option is not available if you choose the delete operation.
RADIUS OUTBOUND Attributes Injection—The RADIUS OUTBOUND attributes section is used for manipulating the outgoing attributes before sending them from the proxy server.	
Add	After you define a RADIUS outgoing attribute, click **ADD** to add it to the RADIUS attributes list.
Edit	To edit the listed RADIUS outgoing attribute, select the attribute in the list and click **Edit**. The attribute properties appear in the fields. Modify the properties as required, then click **Replace**.
Replace	Click **Replace** to replace the selected RADIUS attribute with the value that is currently defined in this field.
Delete	Click **Delete** to delete the selected RADIUS outgoing attribute from the list.
Dictionary Type	Choose the dictionary that contains the RADIUS outgoing attribute you want to use.

Table 10-6 Access Service Properties—General Page (continued)

Option	Description
RADIUS Attribute	Name of the RADIUS attribute. Click **Select** to choose a RADIUS attribute from the specified dictionary.
Attribute Type	Type of the selected RADIUS attribute. Client vendor type of the attribute, from which ACS allows access requests. For a description of the attribute types, refer to Cisco IOS documentation for the Cisco IOS Software release that is running on your AAA clients.
Operation	You can perform the following three operations: • Choose **ADD** to add a new attribute value for the selected RADIUS attribute: – If Multiple not allowed—adds the new value for the selected attribute only if this attribute does not exists on the request. – If Multiple allowed—always adds the attribute with a new value. • Choose **UPDATE** to update the existing value of a selected RADIUS attribute: – If Multiple not allowed—updates the attribute value with the new value if the attribute exists on the request. – If Multiple allowed—removes all occurrences of this attribute and adds one attribute with the new value. – If the attribute is a cisco-avpair (pair of key=value), the update is done according to the key. • Choose **DELETE** to delete the value of the selected RADIUS attribute. The attribute operations statements are ordered. The administrator can change the statement's order at the time of configuration. ACS performs the operation on the attributes according to the configured order. For more information on this, see RADIUS Attribute Rewrite Operation, page 4-29.
Attribute New Value	Enter a new value for the selected RADIUS outgoing attribute. This option is not available if you choose the delete operation.

Step 3 Click **Next** to configure the allowed protocols. See Configuring Access Service Allowed Protocols, page 10-16.

Related Topic

- Configuring Access Service Allowed Protocols, page 10-16
- Configuring Access Services Templates, page 10-21

Configuring Access Service Allowed Protocols

The allowed protocols are the second part of access service creation. Access service definitions contain general and allowed protocol information. When you duplicate and edit services, the Access Service properties page contains tabs.

Step 1 Select **Access Policies > Access Services**, and then click:

- **Create** to create a new access service, and then click **Next** to go to the Allowed Protocols screen.

- **Duplicate** to duplicate an access service, then click **Next** to go to the Allowed Protocols screen.
- **Edit** to edit an access service, then click **Next** to go to the Allowed Protocols screen.

Step 2 Complete the fields as shown in Table 10-7:

Table 10-7 Access Service Properties—Allowed Protocols Page

Option	Description
Process Host Lookup	Check to configure ACS to process the Host Lookup field (for example, when the RADIUS Service-Type equals 10) and use the System UserName attribute from the RADIUS Calling-Station-ID attribute. Uncheck for ACS to ignore the Host Lookup request and use the original value of the system UserName attribute for authentication and authorization. When unchecked, message processing is according to the protocol (for example, PAP).
Authentication Protocols	
Allow PAP/ASCII	Enables PAP/ASCII. PAP uses clear-text passwords (that is, unencrypted passwords) and is the least secure authentication protocol. When you check **Allow PAP/ASCII**, you can check **Detect PAP as Host Lookup** to configure ACS to detect this type of request as a Host Lookup (instead of PAP) request in the network access service.
Allow CHAP	Enables CHAP authentication. CHAP uses a challenge-response mechanism with password encryption. CHAP does not work with the Windows Active Directory.
Allow MS-CHAPv1	Enables MS-CHAPv1.
Allow MSCHAPv2	Enables MSCHAPv2.
Allow EAP-MD5	Enables EAP-based Message Digest 5 hashed authentication. When you check **Allow EAP-MD5**, you can check **Detect EAP-MD5 as Host Lookup** to configure ACS to detect this type of request as a Host Lookup (instead of EAP-MD5) request in the network access service.
Allow EAP-TLS	Enables the EAP-TLS Authentication protocol and configures EAP-TLS settings. You can specify how ACS verifies user identity as presented in the EAP Identity response from the end-user client. User identity is verified against information in the certificate that the end-user client presents. This comparison occurs after an EAP-TLS tunnel is established between ACS and the end-user client. If you choose Allow EAP-TLS, you can configure the following: • **Enable Stateless Session resume**—Check this check box to enable the Stateless Session Resume feature per Access service. This feature enables you to configure the following options: – **Proactive Session Ticket update**—Enter the value as a percentage to indicate how much of the Time to Live must elapse before the session ticket is updated. For example, the session ticket update occurs after 10 percent of the Time to Live has expired, if you enter the value 10. – **Session ticket Time to Live**—Enter the equivalent maximum value in days, weeks, months, and years, using a positive integer. EAP-TLS is a certificate-based authentication protocol. EAP-TLS authentication can occur only after you have completed the required steps to configure certificates. See Configuring Local Server Certificates, page 18-16 for more information.
Allow LEAP	Enables LEAP authentication.

Table 10-7 Access Service Properties—Allowed Protocols Page (continued)

Option	Description
Allow PEAP	Enables the PEAP authentication protocol and PEAP settings. The default inner method is MSCHAPv2. When you check **Allow PEAP**, you can configure the following PEAP inner methods: • Allow EAP-TLS—Check to use EAP-TLS as the inner method. • Allow EAP-MSCHAPv2—Check to use EAP-MSCHAPv2 as the inner method. – Allow Password Change—Check for ACS to support password changes. – Retry Attempts—Specifies how many times ACS requests user credentials before returning login failure. Valid values are 1 to 3. • Allow EAP-GTC—Check to use EAP-GTC as the inner method. – Allow Password Change—Check for ACS to support password changes. – Retry Attempts—Specifies how many times ACS requests user credentials before returning login failure. Valid values are 1 to 3. • Allow PEAP Cryptobinding TLV—Check to use the PEAP cryptobinding TLV support. • Allow PEAPv0 only for legacy clients—Check this option to allow PEAP supplicants to negotiate PEAPv0 only. **Note** A few legacy clients do not confirm the PEAPv1 protocol standard. As a result, the EAP conversations are dropped with an `Invalid EAP payload` error message.

Table 10-7 Access Service Properties—Allowed Protocols Page (continued)

Option	Description
Allow EAP-FAST	Enables the EAP-FAST authentication protocol and EAP-FAST settings. The EAP-FAST protocol can support multiple internal protocols on the same server. The default inner method is MSCHAPv2. When you check **Allow EAP-FAST**, you can configure EAP-FAST inner methods: • Allow EAP-MSCHAPv2 – Allow Password Change—Check for ACS to support password changes in phase zero and phase two of EAP-FAST. – Retry Attempts—Specifies how many times ACS requests user credentials before returning login failure. Valid values are 1-3. • Allow EAP-GTC – Allow Password Change—Check for ACS to support password changes in phase zero and phase two of EAP-FAST. – Retry Attempts—Specifies how many times ACS requests user credentials before returning login failure. Valid values are 1-3. • Allow TLS-Renegotiation—Check for ACS to support TLS-Renegotiation. This option allows an anonymous TLS handshake between the end-user client and ACS. EAP-MS-CHAP will be used as the only inner method in phase zero. • Use PACs—Choose to configure ACS to provision authorization PACs for EAP-FAST clients. Additional PAC Options, page 10-20 appear. • Don't use PACs—Choose to configure ACS to use EAP-FAST without issuing or accepting any tunnel or machine PACs. All requests for PACs are ignored and ACS responds with a Success-TLV without a PAC. – Allow Machine Authentication—Check this option to configure ACS to perform machine authentication. – Accept Client Certificate—Check this option to configure ACS to accept client certificates when you use Cisco IP phones.

Table 10-7 Access Service Properties—Allowed Protocols Page (continued)

Option	Description
Allow EAP-FAST (continued)	**PAC Options** • Tunnel PAC Time To Live—The Time To Live (TTL) value restricts the lifetime of the PAC. Specify the lifetime value and units. The default is one (1) day. • Proactive PAC Update When: <*n*%> of PAC TTL is Left—The Update value ensures that the client has a valid PAC. ACS initiates update after the first successful authentication but before the expiration time that is set by the TTL. The Update value is a percentage of the remaining time in the TTL. (Default: 10%) • Allow Anonymous In-band PAC Provisioning—Check for ACS to establish a secure anonymous TLS handshake with the client and provision it with a so-called PAC by using phase zero of EAP-FAST with EAP-MSCHAPv2. **Note** To enable Anonymous PAC Provisioning, you must choose both the inner methods, EAP-MSCHAPv2 and EAP-GTC. • Allow Authenticated In-band PAC Provisioning—ACS uses Secure Socket Layer (SSL) server-side authentication to provision the client with a PAC during phase zero of EAP-FAST. This option is more secure than anonymous provisioning but requires that a server certificate and a trusted root CA be installed on ACS. – Server Returns Access Accept After Authenticated Provisioning—Check this option to configure ACS to return an Access-Accept message to the client after successful authenticated PAC provisioning. – Accept Client Certificate For Provisioning—Check this option to configure ACS to accept client certificates for PAC provisioning when you use Cisco IP phones. • Allow Machine Authentication—Check for ACS to provision an end-user client with a machine PAC and perform machine authentication (for end-user clients who do not have the machine credentials). The machine PAC can be provisioned to the client by request (in-band) or by administrator (out-of-band). When ACS receives a valid machine PAC from the end-user client, the machine identity details are extracted from the PAC and verified in the ACS external identity store. After these details are correctly verified, no further authentication is performed. **Note** ACS 5.8 only supports Active Directory as an external identity store for machine authentication. When you check this option, you can enter a value for the amount of time that a machine PAC is acceptable for use. When ACS receives an expired machine PAC, it automatically reprovisions the end-user client with a new machine PAC (without waiting for a new machine PAC request from the end-user client). • Enable Stateless Session Resume—Check for ACS to provision authorization PACs for EAP-FAST clients and always perform phase two of EAP-FAST (default = enabled). Uncheck this option: – If you do not want ACS to provision authorization PACs for EAP-FAST clients. – To always perform phase two of EAP-FAST. When you check this option, you can enter the authorization period of the user authorization PAC. After this period the PAC expires. When ACS receives an expired authorization PAC, it performs phase two EAP-FAST authentication.

Table 10-7 Access Service Properties—Allowed Protocols Page (continued)

Option	Description
Preferred EAP protocol	Select the preferred EAP protocol from the following options available: • EAP-FAST • PEAP • LEAP • EAP-TLS • EAP-MD5 This option helps ACS to be flexible to work with old supplicants (end devices) which are not capable of sending No-Acknowledgment, when a particular protocol is not implemented. You can use this option to place a particular protocol first in list of protocols that is being negotiated with device so that the negotiation is successful.
EAP-TLS L-bit	Enables the L (length included) flag in access policies. When you perform EAP-TLS authentication against Terminal Wireless Local Area Network Unit (TWLU) client in ACS 5.x, the TWLU is expecting a L Flag (length included flag) set in change cipher specifications and the encrypted handshake message. If you are using the Honeywell TWLU unit, then it is recommended to create a group of all TWLU units and create an access policy with L flag included in it and use that access policy for all the TWLU units so that it will not disturb the other clients. The EAP-TLS L-bit is available at **Access Policies > Access Services > Default Network Access > Edit: "Default Network Access"** page in ACS web interface.
Allow weak ciphers for EAP	**Note** This option is available from ACS 5.8 patch 4. Enables weak ciphers for EAP protocol. If this option is enabled, legacy clients are allowed to negotiate using weak ciphers. We recommend that you enable this option only if your legacy clients support only weak ciphers. This option is disabled by default. **Note** If FIPS is enabled, ACS will not allow you to enable this option and vice-versa.
Send as User-Name in RADIUS Access-Accept	
RADIUS Access-Request User-Name	Select this option if you want ACS to send the username that was received in the RADIUS access request in the RADIUS access accept response.
Principal User Name	Select this option if you want ACS to send the principal name of the certificate that is used to authenticate the user in the RADIUS access accept response.

Step 3 Click **Finish** to save your changes to the access service.

To enable an access service, you must add it to the service selection policy.

Configuring Access Services Templates

Use a service template to define an access service with policies that are customized to use specific condition types.

Step 1 In the Configuring General Access Service Properties, page 10-13, choose **Based on service template** and click **Select**.

Step 2 Complete the fields as described in Table 10-8:

Table 10-8 Access Services Templates

Template Name	Access Service Type	Protocols	Policies	Conditions	Results
Device Admin - Simple	Device Administration	PAP/ASCII	Identity	None - Simple	Internal users
			Authorization	Identity group, NDG:Location, NDG:Device Type, Time and Date	Shell profile
Device Admin - Command Auth	Device Administration	PAP/ASCII	Identity	None - Simple	Internal users
			Authorization	Identity group, NDG:Location, NDG: Time and Date	Command sets
Network Access - Simple	Network Access	PEAP, EAP-FAST	Identity	None - Simple	Internal users
			Authorization	NDG:Location, Time and date	Authorization profiles
Network Access - MAC Authentication Bypass	Network Access	Process Host Lookup, PAP/ASCII (detect PAP as host lookup) and EAP-MD5 (detect EAP-MD5 as host lookup)	Identity	None - Simple	Internal users
			Authorization	Use case	Authorization profiles

Deleting an Access Service

To delete an access service:

Step 1 Select **Access Policies > Access Services**.

The Access Services page appears with a list of configured services.

Step 2 Check one or more check boxes the access services that you want to delete.

Step 3 Click **Delete**; then click **OK** in the confirmation message.

The Access Policies page appears without the deleted access service(s).

Related Topic

- Creating, Duplicating, and Editing Access Services, page 10-12

Configuring Access Service Policies

You configure access service policies after you create the access service:

- Viewing Identity Policies, page 10-23
- Configuring Identity Policy Rule Properties, page 10-26
- Configuring a Group Mapping Policy, page 10-28
- Configuring a Session Authorization Policy for Network Access, page 10-31
- Configuring a Session Authorization Policy for Network Access, page 10-31
- Configuring Shell/Command Authorization Policies for Device Administration, page 10-36

You can configure simple policies to apply to the same result to all incoming requests; or, you can create rule-based policies.

Note If you create and save a simple policy, and then change to a rule-based policy, the simple policy becomes the default rule of the rule-based policy. If you have saved a rule-based policy and then change to a simple policy, you will lose all your rules except for the default rule. ACS automatically uses the default rule as the simple policy.

Before you begin to configure policy rules, you must:

- Configure the policy conditions and results. See Managing Policy Conditions, page 9-1.
- Select the types of conditions and results that the policy rules apply. See Customizing a Policy, page 10-4.

For information about configuring policy rules, see:

- Creating Policy Rules, page 10-39
- Duplicating a Rule, page 10-40
- Editing Policy Rules, page 10-40
- Deleting Policy Rules, page 10-41

Viewing Identity Policies

The identity policy in an access service defines the identity source that ACS uses for authentication and attribute retrieval. ACS can use the retrieved attributes in subsequent policies.

The identity source for:

- Password-based authentication can be a single identity store, or an identity store sequence.
- Certificate-based authentication can be a certificate authentication profile, or an identity store sequence.

An identity store sequence defines the sequence that is used for authentication and an optional additional sequence to retrieve attributes. See Configuring Identity Store Sequences, page 8-102.

If you created an access service that includes an identity policy, you can configure and modify this policy. You can configure a simple policy, which applies the same identity source for authentication of all requests; or, you can configure a rule-based identity policy.

In the rule-based policy, each rule contains one or more conditions and a result, which is the identity source to use for authentication. You can create, duplicate, edit, and delete rules within the identity policy; and you can enable and disable them.

Caution If you switch between the simple policy and the rule-based policy pages, you will lose your previously saved policy.

To configure a simple identity policy:

Step 1 Select **Access Policies > Access Services > *service* > Identity**, where *service* is the name of the access service.

By default, the Simple Identity Policy page appears with the fields described in Table 10-9:

Table 10-9 Simple Identity Policy Page

Option	Description
Policy type	Defines the type of policy to configure: • Simple—Specifies the result to apply to all requests. • Rule-based—Configure rules to apply different results, depending on the request. If you switch between policy types, you will lose your previously saved policy configuration.
Identity Source	Identity source to apply to all requests. The default is Deny Access. For: • Password-based authentication, choose a single identity store, or an identity store sequence. • Certificate-based authentication, choose a certificate authentication profile, or an identity store sequence. The identity store sequence defines the sequence that is used for authentication and an optional additional sequence to retrieve attributes. See Configuring Identity Store Sequences, page 8-102.
Advanced options	Specifies whether to reject or drop the request, or continue with authentication for these options: • If authentication failed—Default is reject. • If user not found—Default is reject. • If process failed—Default is drop. Owing to restrictions on the underlying protocol, ACS cannot always continue processing when the Continue option is chosen. ACS can continue when authentication fails for PAP/ASCII, EAP-TLS, or Host Lookup. For all other authentication protocols, the request will be dropped even if you choose the Continue option.

Step 2 Select an identity source for authentication; or, choose **Deny Access**.

You can configure additional advanced options. See Configuring Identity Policy Rule Properties, page 10-26.

Step 3 Click **Save Changes** to save the policy.

Viewing Rules-Based Identity Policies

Select **Access Policies > Access Services > *service* > Identity**, where <*service*> is the name of the access service.

By default, the Simple Identity Policy page appears with the fields described in Table 10-9. If configured, the Rules-Based Identity Policy page appears with the fields described in Table 10-10:

Table 10-10 Rule-based Identity Policy Page

Option	Description
Policy type	Defines the type of policy to configure: • Simple—Specifies the results to apply to all requests. • Rule-based—Configure rules to apply different results depending on the request. **Caution** If you switch between policy types, you will lose your previously saved policy configuration.
Status	The current status of the rule. The rule statuses are: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The Monitor option is especially useful for watching the results of a new rule.
Name	Rule name.
Conditions	Conditions that determine the scope of the policy. This column displays all current conditions in subcolumns.
Results	Identity source that is used for authentication as a result of the evaluation of the rule.
Hit Count	Number of times that the rule is matched. Click the Hit Count button to refresh and reset this column.
Default Rule	ACS applies the Default rule when: • Enabled rules are not matched. • No other rules are defined. Click the link to edit the Default Rule. You can edit only the results of the Default Rule; you cannot delete, disable, or duplicate it.
Customize button	Opens the Customize page in which you choose the types of conditions to use in policy rules. A new Conditions column appears in the Policy page for each condition that you add. **Caution** If you remove a condition type after defining rules, you will lose any conditions that you configured for that condition type.
Hit Count button	Opens a window that enables you to reset and refresh the Hit Count display in the Policy page. See Displaying Hit Counts, page 10-10.

To configure a rule-based policy, see these topics:

- Creating Policy Rules, page 10-39
- Duplicating a Rule, page 10-40
- Editing Policy Rules, page 10-40
- Deleting Policy Rules, page 10-41

For information about configuring an identity policy for Host Lookup requests, see Configuring an Authorization Policy for Host Lookup Requests, page 4-19.

Related Topics

- Configuring a Group Mapping Policy, page 10-28
- Configuring a Session Authorization Policy for Network Access, page 10-31
- Configuring a Session Authorization Policy for Network Access, page 10-31
- Configuring Shell/Command Authorization Policies for Device Administration, page 10-36

Configuring Identity Policy Rule Properties

You can create, duplicate, or edit an identity policy rule to determine the identity databases that are used to authenticate the client and retrieve attributes for the client.

To display this page:

Step 1 Choose **Access Policies > Access Services >** ***service*** **> Identity, then do one of the following:**

- **Click Create**.
- Check a rule check box, and click **Duplicate**.
- Click a rule name or check a rule check box, then click **Edit**.

Step 2 Complete the fields as shown in the Identity Rule Properties page described in Table 10-11:

Table 10-11 Identity Rule Properties Page

Option	Description
General	
Rule Name	Name of the rule. If you are duplicating a rule, you must enter a unique name as a minimum configuration; all other fields are optional.
Rule Status	Rule statuses are: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The Monitor option is especially useful for watching the results of a new rule.
Conditions	
conditions	Conditions that you can configure for the rule. By default the compound condition appears. You can change the conditions that appear by using the Customize button in the Policy page. The default value for each condition is *ANY*. To change the value for a condition, check the condition check box, then specify the value. If you check **Compound Condition**, an expression builder appears in the conditions frame. For more information, see Configuring Compound Conditions, page 10-41.
Results	
Identity Source	Identity source to apply to requests. The default is Deny Access. For: • Password-based authentication, choose a single identity store, or an identity store sequence. • Certificate-based authentication, choose a certificate authentication profile, or an identity store sequence. The identity store sequence defines the sequence that is used for authentication and attribute retrieval and an optional sequence to retrieve additional attributes. See Configuring Identity Store Sequences, page 8-102.
Advanced options	Specifies whether to reject or drop the request, or continue with authentication for these options: • If authentication failed—Default is reject. • If user not found—Default is reject. • If process failed—Default is drop. Owing to restrictions on the underlying protocol, ACS cannot always continue processing when the Continue option is chosen. ACS can continue when authentication fails for PAP/ASCII, EAP-TLS or Host Lookup. For all other authentication protocols, the request is dropped even if you choose the Continue option.

Configuring a Group Mapping Policy

Configure a group mapping policy to map groups and attributes that are retrieved from external identity stores to ACS identity groups. When ACS processes a request for a user or host, this policy retrieves the relevant identity group which can be used in authorization policy rules.

If you created an access service that includes a group mapping policy, you can configure and modify this policy. You can configure a simple policy, which applies the same identity group to all requests; or, you can configure a rule-based policy.

In the rule-based policy, each rule contains one or more conditions and a result. The conditions can be based only on attributes or groups retrieved from external attribute stores, and the result is an identity group within the identity group hierarchy. You can create, duplicate, edit, and delete rules within the policy; and you can enable and disable them.

Caution If you switch between the simple policy and the rule-based policy pages, you will lose your previously saved policy.

To configure a simple group mapping policy:

Step 1 Select **Access Policies > Access Services > *service* > Group Mapping**, where *service* is the name of the access service.

By default, the Simple Group Mapping Policy page appears. See Table 10-12 for field descriptions.

See Table 10-13 for Rule-Based Group Mapping Policy page field descriptions.

Table 10-12 Simple Group Mapping Policy Page

Option	Description
Policy type	Defines the type of policy to configure: • Simple—Specifies the results to apply to all requests. • Rule-based—Configure rules to apply different results depending on the request. **Caution** If you switch between policy types, you will lose your previously saved policy configuration.
Identity Group	Identity group to which attributes and groups from all requests are mapped.

Table 10-13 Rule-based Group Mapping Policy Page

Option	Description
Policy type	Defines the type of policy to configure: • Simple—Specifies the results to apply to all requests. • Rule-based—Configure rules to apply different results depending on the request. **Caution** If you switch between policy types, you will lose your previously saved policy configuration.
Status	Current status of the rule. The rule statuses are: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Name	Rule name.
Conditions	Conditions that determine the scope of the policy. This column displays all current conditions in subcolumns.
Results	Identity group that is used as a result of the evaluation of the rule.
Hit Count	Number of times that the rule is matched. Click the Hit Count button to refresh and reset this column.
Default Rule	ACS applies the Default rule when: • Enabled rules are not matched. • No other rules are defined. Click the link to edit the Default Rule. You can edit only the results of the Default Rule; you cannot delete, disable, or duplicate it.
Customize button	Opens the Customize page in which you choose the types of conditions to use in policy rules. A new Conditions column appears in the Policy page for each condition that you add. **Caution** If you remove a condition type after defining rules, you will lose any conditions that you configured for that condition type.
Hit Count button	Opens a window that enables you to reset and refresh the Hit Count display in the Policy page. See Displaying Hit Counts, page 10-10.

Step 2 Select an identity group.

Step 3 Click **Save Changes** to save the policy.

To configure a rule-based policy, see these topics:

- Creating Policy Rules, page 10-39
- Duplicating a Rule, page 10-40
- Editing Policy Rules, page 10-40

- Deleting Policy Rules, page 10-41

Related Topics

- Viewing Identity Policies, page 10-23
- Configuring a Session Authorization Policy for Network Access, page 10-31
- Configuring a Session Authorization Policy for Network Access, page 10-31
- Configuring Shell/Command Authorization Policies for Device Administration, page 10-36

Configuring Group Mapping Policy Rule Properties

Use this page to create, duplicate, or edit a group mapping policy rule to define the mapping of attributes and groups that are retrieved from external databases to ACS identity groups.

Step 1 Select **Access Policies > Access Services > *service* > Group Mapping,** then do one of the following:

- Click **Create**.
- Check a rule check box, and click **Duplicate**.
- Click a rule name or check a rule check box, then click **Edit**.

Step 2 Complete the fields as described in Table 10-14:

Table 10-14 Group Mapping Rule Properties Page

Option	Description
General	
Rule Name	Name of the rule. If you are duplicating a rule, you must enter a unique name as a minimum configuration; all other fields are optional.
Rule Status	Rule statuses are: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Conditions	
conditions	Conditions that you can configure for the rule. By default, the compound condition appears. You can change the conditions that appear by using the Customize button in the Policy page. The default value for each condition is ANY. To change the value for a condition, check the condition check box, then specify the value. If you check **Compound Condition**, an expression builder appears in the conditions frame. For more information, see Configuring Compound Conditions, page 10-41.
Results	
Identity Group	Identity group to which attributes and groups from requests are mapped.

Configuring a Session Authorization Policy for Network Access

When you create an access service for network access authorization, it creates a Session Authorization policy. You can then add and modify rules to this policy to determine the access permissions for the client session.

You can create a standalone authorization policy for an access service, which is a standard first-match rule table. You can also create an authorization policy with an exception policy. See Configuring Authorization Exception Policies, page 10-37. When a request matches an exception rule, the policy exception rule result is always applied.

The rules can contain any conditions and multiple results:

- Authorization profile—Defines the user-defined attributes and, optionally, the downloadable ACL that the Access-Accept message should return.
- Security Group Tag (SGT)—If you have installed Cisco Security Group Access, the authorization rules can define which SGT to apply to the request.

For information about how ACS processes rules with multiple authorization profiles, see Processing Rules with Multiple Authorization Profiles, page 3-16.

To configure an authorization policy, see these topics:

- Creating Policy Rules, page 10-39
- Duplicating a Rule, page 10-40
- Editing Policy Rules, page 10-40
- Deleting Policy Rules, page 10-41

For information about creating an authorization policy for:

- Host Lookup requests, see ACS and Cisco Security Group Access, page 4-22.
- Security Group Access support, see Creating an Endpoint Admission Control Policy, page 4-25.

Step 1 Select **Access Policies > Access Services > *service* > Authorization**.

Step 2 Complete the fields as described in Table 10-15:

Table 10-15 Network Access Authorization Policy Page

Option	Description
Status	Rule statuses are: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Name	Name of the rule.
Conditions	
Identity Group	Name of the internal identity group to which this is matching against.
NDG:*name*	Network device group. The two predefined NDGs are Location and Device Type.
conditions	Conditions that define the scope of the rule. To change the types of conditions that the rule uses, click the Customize button. You must have previously defined the conditions that you want to use.
Results	
Authorization Profile	Displays the authorization profile that will be applied when the corresponding rule is matched. When you enable the Security Group Access feature, you can customize rule results; a rule can determine the access permission of an endpoint, the security group of that endpoint, or both. The columns that appear reflect the customization settings.
Hit Count	The number of times that the rule is matched. Click the Hit Count button to refresh and reset this column.
Default Rule	ACS applies the Default rule when: • Enabled rules are not matched. • No other rules are defined. Click the link to edit the Default Rule. You can edit only the results of the Default Rule; you cannot delete, disable, or duplicate it.
Customize button	Opens the Customize page in which you choose the types of conditions to use in policy rules. A new Conditions column appears in the Policy page for each condition that you add. When you enable the Security Group Access feature, you can also choose the set of rule results; only session authorization profiles, only security groups, or both. **Caution** If you remove a condition type after defining rules, you will lose any conditions that you configured for that condition type.
Hit Count button	Opens a window that enables you to reset and refresh the Hit Count display in the Policy page. See Displaying Hit Counts, page 10-10.

Configuring Network Access Authorization Rule Properties

Use this page to create, duplicate, and edit the rules to determine access permissions in a network access service.

Step 1 Select **Access Policies > Access Services > <*service*> > Authorization**, and click **Create, Edit,** or **Duplicate**.

Step 2 Complete the fields as described in Table 10-16:

Table 10-16 Network Access Authorization Rule Properties Page

Option	Description
General	
Name	Name of the rule. If you are duplicating a rule, you must enter a unique name as a minimum configuration; all other fields are optional.
Status	Rule statuses are: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Conditions	
conditions	Conditions that you can configure for the rule. By default the compound condition appears. You can change the conditions that appear by using the Customize button in the Policy page. The default value for each condition is ANY. To change the value for a condition, check the condition check box, then specify the value. If you check **Compound Condition**, an expression builder appears in the conditions frame. For more information, see Configuring Compound Conditions, page 10-41.
Results	
Authorization Profiles	List of available and selected profiles. You can choose multiple authorization profiles to apply to a request. See Processing Rules with Multiple Authorization Profiles, page 3-16 for information about the importance of authorization profile order when resolving conflicts.
Security Group	(Security Group Access only) The security group to apply. When you enable Security Group Access, you can customize the results options to display only session authorization profiles, only security groups, or both.

Note ACS allows you to create an internal user account using the identity string attribute to match a particular NDG:location only by configuring the detailed path of the NDG.

Configuring Device Administration Authorization Policies

A device administration authorization policy determines the authorizations and permissions for network administrators.

You create an authorization policy during access service creation. See Configuring General Access Service Properties, page 10-13 for details of the Access Service Create page.

Use this page to:

- View rules.
- Delete rules.
- Open pages that enable you to create, duplicate, edit, and customize rules.

Select **Access Policies > Access Services > *service* > Authorization**.

The Device Administration Authorization Policy page appears as described in Table 10-17.

Table 10-17 Device Administration Authorization Policy Page

Option	Description
Status	Rule statuses are: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Name	Name of the rule.
Conditions	Conditions that define the scope of the rule. To change the types of conditions that the rule uses, click the Customize button. You must have previously defined the conditions that you want to use.
Results	Displays the shell profiles and command sets that will be applied when the corresponding rule is matched. You can customize rule results; a rule can apply shell profiles, or command sets, or both. The columns that appear reflect the customization settings.
Hit Count	Number of times that the rule is matched. Click the Hit Count button to refresh and reset this column.
Default Rule	ACS applies the Default rule when: • Enabled rules are not matched. • No other rules are defined. Click the link to edit the Default Rule. You can edit only the results of the Default Rule; you cannot delete, disable, or duplicate it.
Customize button	Opens the Customize page in which you choose the types of conditions and results to use in policy rules. The Conditions and Results columns reflect your customized settings. **Caution** If you remove a condition type after defining rules, you will lose any conditions that you configured for that condition type.
Hit Count button	Opens a window that enables you to reset and refresh the Hit Count display in the Policy page. See Displaying Hit Counts, page 10-10.

Configuring Device Administration Authorization Rule Properties

Use this page to create, duplicate, and edit the rules to determine authorizations and permissions in a device administration access service.

Select **Access Policies > Access Services > *service* > Authorization**, and click **Create, Edit,** or **Duplicate**.

The Device Administration Authorization Rule Properties page appears as described in Table 10-18.

Table 10-18 Device Administration Authorization Rule Properties Page

Option	Description
General	
Name	Name of the rule. If you are duplicating a rule, you must enter a unique name as a minimum configuration; all other fields are optional.
Status	Rule statuses are: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Conditions	
conditions	Conditions that you can configure for the rule. By default the compound condition appears. You can change the conditions that appear by using the Customize button in the Policy page. The default value for each condition is ANY. To change the value for a condition, check the condition check box, then specify the value. If you check **Compound Condition**, an expression builder appears in the conditions frame. For more information, see Configuring Compound Conditions, page 10-41.
Results	
Shell Profiles	Shell profile to apply for the rule.
Command Sets	List of available and selected command sets. You can choose multiple command sets to apply.

Configuring Device Administration Authorization Exception Policies

You can create a device administration authorization exception policy for a defined authorization policy. Results from the exception rules always override authorization policy rules.

Use this page to:

- View exception rules.
- Delete exception rules.
- Open pages that create, duplicate, edit, and customize exception rules.

Select **Access Policies > Access Services > *service* > Authorization,** and click **Device Administration Authorization Exception Policy**.

The Device Administration Authorization Exception Policy page appears as described in Table 10-19.

Table 10-19 Device Administration Authorization Exception Policy Page

Option	Description
Status	Rule statuses are: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Name	Name of the rule.
Conditions	
Identity Group	Name of the internal identity group to which this is matching against.
NDG:*name*	Network device group. The two predefined NDGs are Location and Device Type.
Condition	Conditions that define the scope of the rule. To change the types of conditions that the rule uses, click the Customize button. You must have previously defined the conditions that you want to use.
Results	Displays the shell profile and command sets that will be applied when the corresponding rule is matched. You can customize rule results; a rule can determine the shell profile, the command sets, or both. The columns that appear reflect the customization settings.
Hit Count	Number of times that the rule is matched. Click the Hit Count button to refresh and reset this column.
Customize button	Opens the Customize page in which you choose the types of conditions to use in policy rules. A new Conditions column appears in the Policy page for each condition that you add. You do not need to use the same set of conditions and results as in the corresponding authorization policy. **Caution** If you remove a condition type after defining rules, you will lose any conditions that you configured for that condition type.
Hit Count button	Opens a window that enables you to reset and refresh the Hit Count display in the Policy page. See Displaying Hit Counts, page 10-10.

Configuring Shell/Command Authorization Policies for Device Administration

When you create an access service and select a service policy structure for Device Administration, ACS automatically creates a shell/command authorization policy. You can then create and modify policy rules.

The web interface supports the creation of multiple command sets for device administration. With this capability, you can maintain a smaller number of basic command sets. You can then choose the command sets in combination as rule results, rather than maintaining all the combinations themselves in individual command sets.

You can also create an authorization policy with an exception policy, which can override the standard policy results. See Configuring Authorization Exception Policies, page 10-37.

For information about how ACS processes rules with multiple command sets, see Processing Rules with Multiple Command Sets, page 3-11.

To configure rules, see:

Configuring Authorization Exception Policies

An authorization policy can include exception policies. In general, exceptions are temporary policies; for example, to grant provisional access to visitors or increase the level of access to specific users. Use exception policies to react efficiently to changing circumstances and events.

The results from the exception rules always override the standard authorization policy rules.

You create exception policies in a separate rule table from the main authorization policy table. You do not need to use the same policy conditions in the exception policy as you used in the corresponding standard authorization policy.

To access the exception policy rules page:

Step 1 Select **Access Policies > Service Selection Policy** ***service* > *authorization policy***, where *service* is the name of the access service, and *authorization policy* is the session authorization or shell/command set authorization policy.

Step 2 In the Rule-Based Policy page, click the **Exception Policy** link above the rules table.

The Exception Policy table appears with the fields described in Table 10-20:

Table 10-20 Network Access Authorization Exception Policy Page

Option	Description
Status	Rule statuses are: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Name	Name of the rule.
Conditions	
Identity Group	Name of the internal identity group to which this is matching against.
NDG:*name*	Network device group. The two predefined NDGs are Location and Device Type.
Condition Name	Conditions that define the scope of the rule. To change the types of conditions that the rule uses, click the Customize button. You must have previously defined the conditions that you want to use.
Results	Displays the authorization profile that will be applied when the corresponding rule is matched. When you enable the Security Group Access feature, you can customize rule results; a rule can determine the access permission of an endpoint, the security group of that endpoint, or both. The columns that appear reflect the customization settings.
Hit Count	Number of times that the rule is matched. Click the Hit Count button to refresh and reset this column.
Customize button	Opens the Customize page in which you choose the types of conditions to use in policy rules. A new Conditions column appears in the Policy page for each condition that you add. You do not need to use the same set of conditions as in the corresponding authorization policy. When you enable the Security Group Access feature, you can also choose the set of rule results; only session authorization profiles, only security groups, or both. **Caution** If you remove a condition type after defining rules, you will lose any conditions that you configured for that condition type.
Hit Count button	Opens a window that enables you to reset and refresh the Hit Count display in the Policy page. See Displaying Hit Counts, page 10-10.

To configure rules, see:

- Creating Policy Rules, page 10-39
- Duplicating a Rule, page 10-40
- Editing Policy Rules, page 10-40
- Deleting Policy Rules, page 10-41

Related Topics

- Configuring a Session Authorization Policy for Network Access, page 10-31
- Configuring Shell/Command Authorization Policies for Device Administration, page 10-36

Creating Policy Rules

When you create rules, remember that the order of the rules is important. When ACS encounters a match as it processes the request of a client that tries to access the ACS network, all further processing stops and the associated result of that match is found. No further rules are considered after a match is found.

The Default Rule provides a default policy in cases where no rules are matched or defined. You can edit the result of a default rule.

Before You Begin

- Configure the policy conditions and results. See Managing Policy Conditions, page 9-1.
- Select the types of conditions and results that the policy rules apply. See Customizing a Policy, page 10-4.

To create a new policy rule:

Step 1 Select **Access Policies > Service Selection Policy *service* > *policy***, where *service* is the name of the access service, and *policy* is the type of policy. If you:

- Previously created a rule-based policy, the Rule-Based Policy page appears, with a list of configured rules.
- Have not created a rule-based policy, the Simple Policy page appears. Click **Rule-Based**.

Step 2 In the Rule-Based Policy page, click **Create**.

The Rule page appears.

Step 3 Define the rule.

Step 4 Click **OK**

The Policy page appears with the new rule.

Step 5 Click **Save Changes** to save the new rule.

To configure a simple policy to use the same result for all requests that an access service processes, see:

- Viewing Identity Policies, page 10-23
- Configuring a Group Mapping Policy, page 10-28
- Configuring a Session Authorization Policy for Network Access, page 10-31
- Configuring a Session Authorization Policy for Network Access, page 10-31
- Configuring Shell/Command Authorization Policies for Device Administration, page 10-36

Related Topics

- Duplicating a Rule, page 10-40
- Editing Policy Rules, page 10-40
- Deleting Policy Rules, page 10-41

Note ACS 5.8 displays a detailed audit reports on ACS configuration audit reports page for creating, editing, or re-ordering access service policies from the ACS web interface.

Duplicating a Rule

You can duplicate a rule if you want to create a new rule that is the same, or very similar to, an existing rule. The duplicate rule name is based on the original rule with parentheses to indicate duplication; for example, Rule-1(1).

After duplication is complete, you access each rule (original and duplicated) separately.

Note You cannot duplicate the Default rule.

To duplicate a rule:

Step 1 Select **Access Policies > Service Selection Policy > *service* > *policy***, where *service* is the name of the access service, and *policy* is the type of policy.

The Policy page appears with a list of configured rules.

Step 2 Check the check box the rule that you want to duplicate. You cannot duplicate the Default Rule.

Step 3 Click **Duplicate**.

The Rule page appears.

Step 4 Change the name of the rule and complete the other applicable field options.

Step 5 Click **OK**.

The Policy page appears with the new rule.

Step 6 Click **Save Changes** to save the new rule.

Step 7 Click **Discard Changes** to cancel the duplicate rule.

Related Topics

- Creating Policy Rules, page 10-39
- Editing Policy Rules, page 10-40
- Deleting Policy Rules, page 10-41

Editing Policy Rules

You can edit all values of policy rules; you can also edit the result in the Default rule.

To edit a rule:

Step 1 Select **Access Policies > Service Selection Policy > *service* > *policy***, where *service* is the name of the access service, and *policy* is the type of policy.

The Policy page appears, with a list of configured rules.

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

The Rule page appears.

Step 3 Edit the appropriate values.

Step 4 Click **OK**.

The Policy page appears with the edited rule.

Step 5 Click **Save Changes** to save the new configuration.

Step 6 Click **Discard Changes** to cancel the edited information.

Related Topics

- Creating Policy Rules, page 10-39
- Duplicating a Rule, page 10-40
- Deleting Policy Rules, page 10-41

Deleting Policy Rules

Note You cannot delete the Default rule.

To delete a policy rule:

Step 1 Select **Access Policies > Service Selection Policy > *service* > *policy***, where *service* is the name of the access service, and *policy* is the type of policy.

The Policy page appears, with a list of configured rules.

Step 2 Check one or more check boxes the rules that you want to delete.

Step 3 Click **Delete**.

The Policy page appears without the deleted rule(s).

Step 4 Click **Save Changes** to save the new configuration.

Step 5 Click **Discard Changes** to retain the deleted information.

Related Topics

- Creating Policy Rules, page 10-39
- Duplicating a Rule, page 10-40
- Editing Policy Rules, page 10-40

Configuring Compound Conditions

Use compound conditions to define a set of conditions based on any attributes allowed in simple policy conditions. You define compound conditions in a policy rule page; you cannot define them as separate condition objects.

This section contains the following topics:

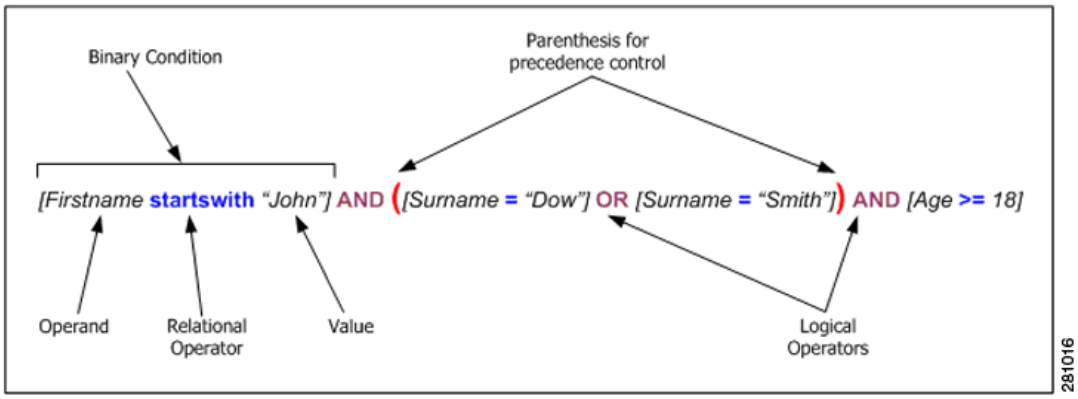
- Compound Condition Building Blocks, page 10-42
- Types of Compound Conditions, page 10-43

- Using the Compound Expression Builder, page 10-46

Compound Condition Building Blocks

Figure 10-1 shows the building blocks of a compound condition.

Figure 10-1 Building Blocks of a Compound Condition



- **Operands**—Any attribute or condition type, such as Protocol/Request Attributes, Identity Attributes, Identity Groups, Network Device Groups (NDGs), Date/Time, and Custom or Standard Conditions.
- **Relational Operators**—Operators that specify the relation between an operand and a value; for example, equals (=), or does not match. The operators that you can use in any condition vary according to the type of operand.
- **Binary condition**—A binary condition defines the relation between a specified operand and value; for example, [username = "Smith"].
- **Logical Operators**—The logical operators operate on or between binary conditions. The supported logical operators are AND and OR.
- **Precedence Control**—You can alter the precedence of logical operators by using parentheses. Nested parentheses provide administrator control of precedence. The natural precedence of logical operators, that is, without parenthesis intervention, is NOT, AND, OR, where NOT has the highest precedence and OR the lowest.

Table 10-21 summarizes the supported dynamic attribute mapping while building Compound Conditions.

Table 10-21 Supported Dynamic Attribute Mapping in Policy Compound Condition

Operand1	Operand2	Example
String attribute	String attribute	—
Integer attribute	Integer attribute	—
Enumeration attribute	Enumeration attribute	—
Boolean attribute	Boolean attribute	—
IP address attribute	IP address attribute	—
Special cases		

Table 10-21 Supported Dynamic Attribute Mapping in Policy Compound Condition

Operand1	Operand2	Example
Hierarchical attribute	String attribute	NDG:Customer vs. 'Internal Users' string attribute
String attribute	Hierarchical attribute	—

Note Dynamic attribute mapping is not applicable for ExternalGroups attribute of Type "String Enum" and "Time And Date" attribute of type "Date Time Period".

For hierarchical attribute, the value is appended with attribute name so while configuring any string attribute to compare with hierarchical attribute the value of the string attribute has to start with hierarchical attribute name.

For example:

- When you define a new string attribute named *UrsAttr* to compare against *DeviceGroup* attribute created under NDG, then the value of the *UsrAttr* has to be configured as follows:

  DeviceGroup: *Value*

- When you want to compare a string attribute with *UserIdentityGroup* which is a hierarchy type attribute within each internal users, then the string attribute has to be configured as follows:

  IdentityGroup:All Groups:"Identity Group Name"

Related Topics

- Types of Compound Conditions, page 10-43
- Using the Compound Expression Builder, page 10-46

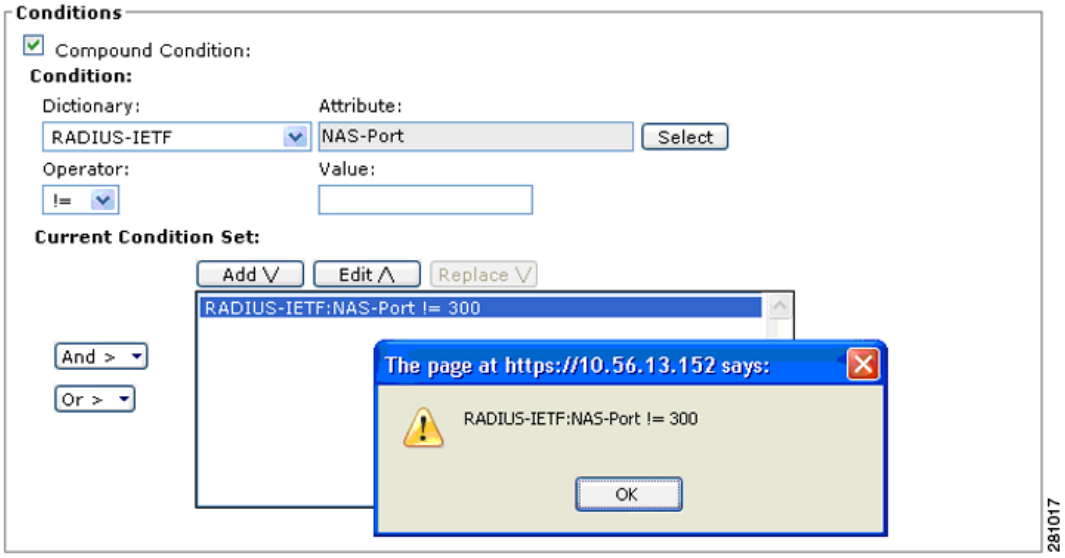
Types of Compound Conditions

You can create three types of compound conditions:

Atomic Condition

Consists of a single predicate and is the only entry in the list. Because all simple conditions in a rule table, except for NDGs, assume the equals (=) operation between the attribute and value, the atomic condition is used to choose an operator other than equals (=). See Figure 10-2 for an example.

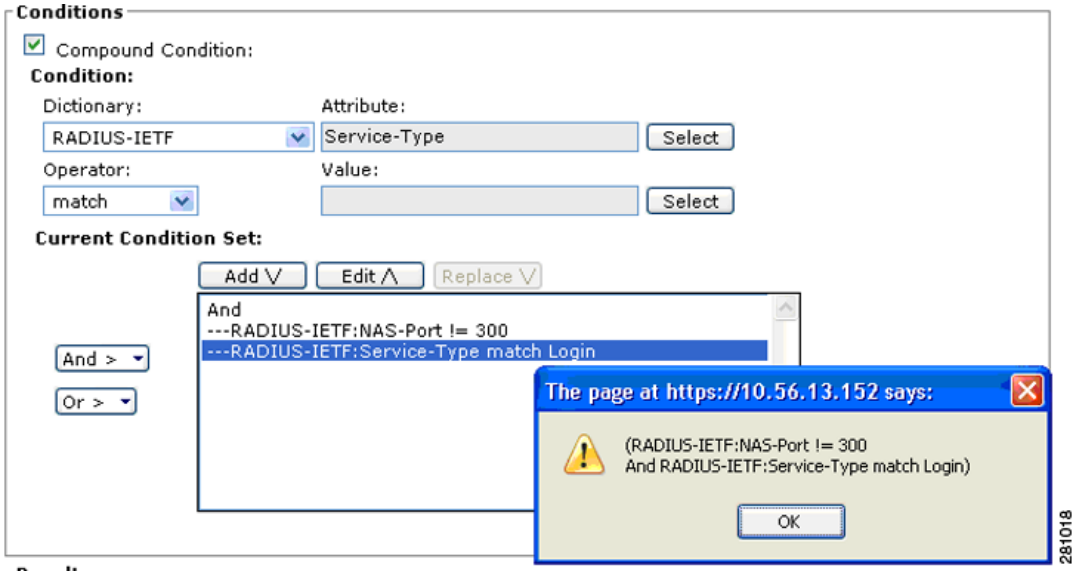
Figure 10-2 Compound Expression - Atomic Condition



Single Nested Compound Condition

Consists of a single operator followed by a set of predicates (>=2). The operator is applied between each of the predicates. See Figure 10-3 for an example. The preview window displays parentheses [()] to indicate precedence of logical operators.

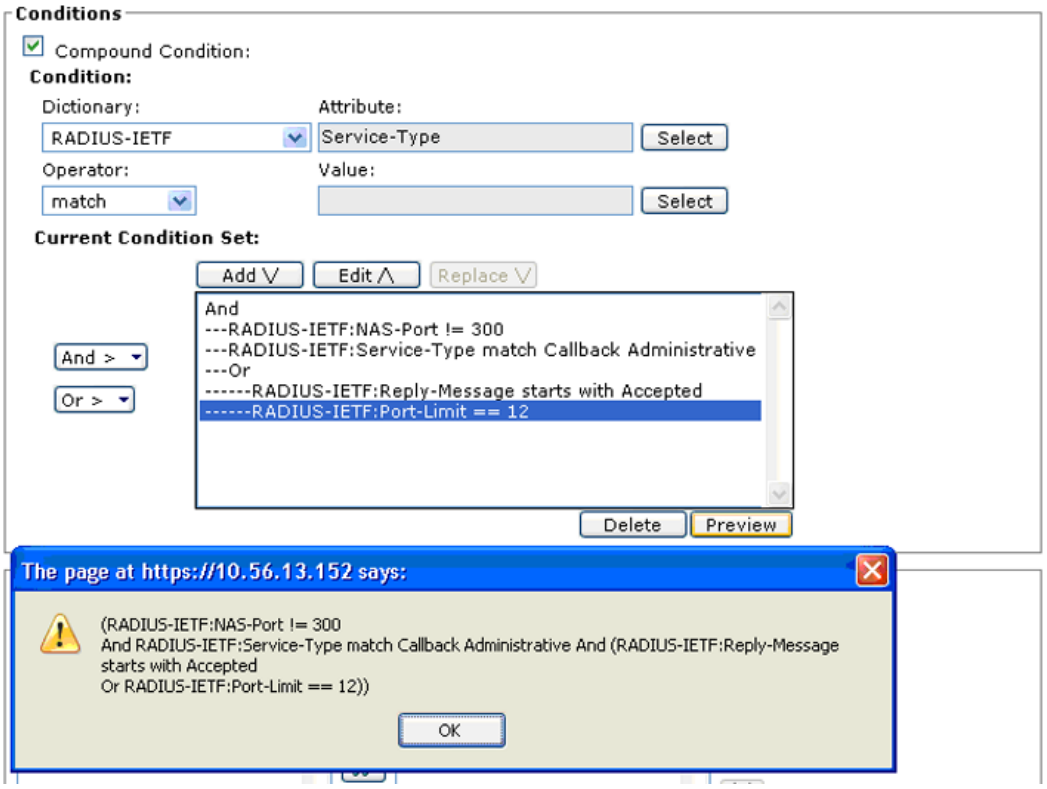
Figure 10-3 Single Nested Compound Expression



Multiple Nested Compound Condition

You can extend the simple nested compound condition by replacing any predicate in the condition with another simple nested compound condition. See Figure 10-4 for an example. The preview window displays parentheses [()] to indicate precedence of logical operators.

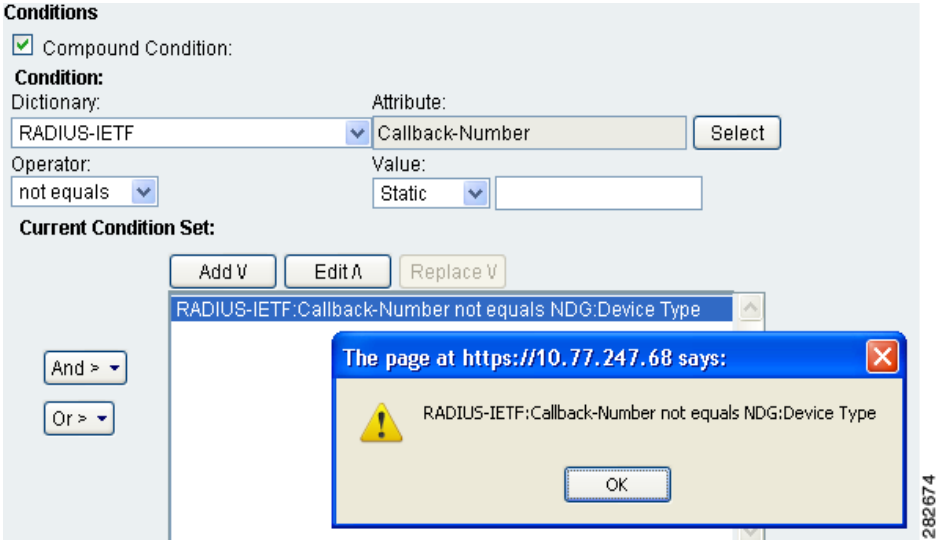
Figure 10-4 Multiple Nested Compound Expression



Compound Expression with Dynamic value

You can select dynamic value to select another dictionary attribute to compare against the dictionary attribute selected as operand. See Figure 10-5 for an example.

Figure 10-5 Compound Expression Builder with Dynamic Value



Related Topics

- Compound Condition Building Blocks, page 10-42
- Using the Compound Expression Builder, page 10-46

Using the Compound Expression Builder

You construct compound conditions by using the expression builder in Rule Properties pages. The expression builder contains two sections: a predicate builder to create primary conditions and controls for managing the expression.

In the first section, you define the primary conditions. Choose the dictionary and attribute to define the operand, then choose the operator, and specify a value for the condition. Use the second section to organize the order of conditions and the logical operators that operate on or between binary conditions.

Table 10-22 describes the fields in the compound expression builder.

Table 10-22 Expression Builder Fields

Field	Description
Condition	Use this section to define the primary conditions.
Dictionary	Specifies the dictionary from which to take the operand. These available options depend on the policy that you are defining. For example, when you define a service selection policy, the Identity dictionaries are not available.
Attribute	Specifies the attribute that is the operand of the condition. The available attributes depend on the dictionary that you chose.
Operator	The relational operator content is dynamically determined according to the choice in the preceding operand field.
Value	The condition value. The type of this field depends on the type of condition or attribute. Select one of the following two options: • Static—If selected, you have to enter or select the static value depending on attribute type. • Dynamic—If selected, you can select another dictionary attribute to compare against the dictionary attribute selected as operand.
Current Condition Set	Use this section to organize the order of conditions and the logical operators that operate on or between binary conditions.
Condition list	Displays a list of defined binary conditions for the compound conditions and their associated logical operators.
Add	After you define a binary condition, click Add to add it to the Condition list.
Edit	To edit a binary condition, select the condition in the Condition list and click Edit. The condition properties appear in the Condition fields. Modify the condition as required, then click Replace.
Replace	Click to replace the selected condition with the condition currently defined in the Condition fields.
And Or	Specifies the logical operator on a selected condition, or between the selected condition and the one above it. Click the appropriate operator, and click Insert to add the operator as a separate line; click the operator and click Replace, to replace the selected line.
Delete	Click to delete the selected binary condition or operator from the condition list.
Preview	Click to display the current expression in corresponding parenthesis representation. The rule table displays the parenthesis representation after the compound expression is created.

Related Topics

- Compound Condition Building Blocks, page 10-42
- Types of Compound Conditions, page 10-43

Security Group Access Control Pages

This section contains the following topics:

Egress Policy Matrix Page

The Egress policy, also known as an SGACL policy, determines which SGACLs to apply at the Egress points of the network, based on the source and destination SGTs. ACS presents the Egress policy as a matrix; it displays all the security groups in the source and destination axes. Each cell in the matrix can contain a set of ACLs to apply to the corresponding source and destination SGTs.

The network devices add the default policy to the specific policies that you defined for the cells. For empty cells, only the default policy applies.

Use the Egress policy matrix to view, define, and edit the sets of ACLs to apply to the corresponding source and destination SGTs.

To display this page, choose **Access Policies > Security Group Access Control > Egress Policy**.

Table 10-23 Egress Policy Matrix Page

Option	Description
Destination Security Group	Column header displaying all destination security groups.
Source Security Group	Row header displaying all source security groups.
Cells	Contain the SGACLs to apply to the corresponding source and destination security group.
Edit	Click a cell, then click Edit to open the Edit dialog box for that cell. See Editing a Cell in the Egress Policy Matrix, page 10-48.
Default Policy	Click to open a dialog box to define the default Egress policy. See Defining a Default Policy for Egress Policy Page, page 10-48.
Set Matrix View	To change the Egress policy matrix display, choose an option, then click **Go**: • All—Clears all the rows and columns in the Egress policy matrix. • Customize View—Launches a window where you can customize source and destination security groups corresponding to the selected cell.

Related Topic

- Creating an Egress Policy, page 4-26

Editing a Cell in the Egress Policy Matrix

Use this page to configure the policy for the selected cell. You can configure the SGACLs to apply to the corresponding source and destination security group.

To display this page, choose **Access Policies > Security Group Access Control > Egress Policy**, select a cell, then click **Edit**.

Table 10-24 Edit Cell Page

Option	Description
Configure Security Groups	*Display only.* Displays the source and destination security group name for the selected cell.
General	Description for the cell policy.
ACLs	Move the SGACLs that you want to apply to the corresponding source and destination security group from the Available list to the Selected list. To specify the order of the list of SGACLs, use the Up (^) and Down (v) arrows.

Related Topic

- Creating an Egress Policy, page 4-26

Defining a Default Policy for Egress Policy Page

Use this page to define the default Egress policy. The network devices add the default policy to the specific policies defined for the cells. For empty cells, only the default policy applies.

To display this page, choose **Access Policies > Security Group Access Control > Egress Policy**, then click **Default Policy**.

Table 10-25 Default Policy Page

Option	Description
ACLs	Move the SGACLs that you want to apply to the corresponding source and destination security group from the Available list to the Selected list. To specify the order of the list of SGACLs, use the Up (^) and Down (v) arrows. Select **Permit All** or **Deny All** as a final catch-all rule.

Related Topics

- Creating an Egress Policy, page 4-26
- Creating a Default Policy, page 4-27

NDAC Policy Page

The Network Device Admission Control (NDAC) policy determines the SGT for network devices in a Security Group Access environment. The NDAC policy handles:

- Peer authorization requests from one device about its neighbor.
- Environment requests (a device is collecting information about itself).

The policy returns the same SGT for a specific device, regardless of the request type.

Note You do not add an NDAC policy to an access service; it is implemented by default. However, for endpoint admission control, you must define an access service and session authorization policy. See Configuring Network Access Authorization Rule Properties, page 10-33, for information about creating a session authorization policy.

Use this page to configure a simple policy that assigns the same security group to all devices, or configure a rule-based policy.

To display this page, choose **Access Policies > Security Group Access Control > Network Device Access > Authentication Policy**.

If you have already configured an NDAC policy, the corresponding Simple Policy page or Rule-based Policy page opens; otherwise, the Simple Policy page opens by default.

Simple Policy Page

Use this page to define a simple NDAC policy.

Table 10-26 Simple NDAC Policy Page

Option	Description
Policy type	Defines the type of policy to configure: • Simple—Specifies that the result applies to all requests. • Rule-based—Configure rules to apply different results depending on the request. If you switch between policy types, you will lose your previously saved policy configuration.
Security Group	Select the security group to assign to devices. The default is Unknown.

Rule-Based Policy Page

Use this page for a rule-based policy to:

- View rules.
- Delete rules.
- Open pages that create, duplicate, edit, and customize rules.

Table 10-27 Rule-Based NDAC Policy Page

Option	Description
Policy type	Defines the type of policy to configure: • Simple—Specifies the result to apply to all requests. • Rule-based—Configure rules to apply different results depending on the request. If you switch between policy types, you will lose your previously saved policy configuration.
Status	Rule statuses are: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Name	Name of the rule. The Default Rule is available for conditions for which: • Enabled rules are not matched. • Rules are not defined. Click a link to edit or duplicate a rule. You can edit the Default Rule but you cannot delete, disable, or duplicate it.
Conditions	Conditions that you can use to define policy rules. To change the display of rule conditions, click the Customize button. You must have previously defined the conditions that you want to use.
Results	Displays the security group assigned to the device when it matches the corresponding condition.
Hit Count	Number of times that the rule is matched. Click the Hit Count button to refresh and reset this column.
Customize button	Opens the Customize page in which you choose the types of conditions to use in policy rules. A new Conditions column appears in the Policy page for each condition that you add. You do not need to use the same set of conditions as in the corresponding authorization policy. ⚠ **Caution** If you remove a condition type after defining rules, you will lose any conditions that you configured for that condition type.
Hit Count button	Opens a window that enables you to reset and refresh the Hit Count display in the Policy page. See Displaying Hit Counts, page 10-10.

Related Topics:

- Configuring an NDAC Policy, page 4-24
- NDAC Policy Properties Page, page 10-50

NDAC Policy Properties Page

Use this page to create, duplicate, and edit rules to determine the SGT for a device.

To display this page, choose **Access Policies > Security Group Access Control > Network Device Access > Authentication Policy**, then click **Create, Edit,** or **Duplicate**.

Note For endpoint admission control, you must define an access service and session authorization policy. See Configuring Network Access Authorization Rule Properties, page 10-33 for information about creating a session authorization policy.

Table 10-28 NDAC Policy Properties Page

Option	Description
General	
Name	Name of the rule. If you are duplicating a rule, you must enter a unique name as a minimum configuration; all other fields are optional.
Status	Rule statuses are: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Conditions	
conditions	Conditions that you can configure for the rule. The default value for each condition is ANY. To change the value for a condition, check the condition check box, then enter the value. If compound expression conditions are available, when you check Compound Expression, an expression builder appears. For more information, see Configuring Compound Conditions, page 10-41. To change the list of conditions for the policy, click the Customize button in the NDAC Policy Page, page 10-49.
Results	
Security Group	Select the security group to assign to the device when it matches the corresponding conditions.

Related Topics:

- Configuring an NDAC Policy, page 4-24
- NDAC Policy Page, page 10-49

Network Device Access EAP-FAST Settings Page

Use this page to configure parameters for the EAP-FAST protocol that the NDAC policy uses.

To display this page, choose **Access Policies > Security Group Access Control > Network Device Access.**

Table 10-29 Network Device Access EAP-FAST Settings Page

Option	Description
EAP-FAST Settings	

Table 10-29 Network Device Access EAP-FAST Settings Page (continued)

Option	Description
Tunnel PAC Time To Live	Time to live (TTL), or duration, of a PAC before it expires and requires replacing.
Proactive PAC Update When % of PAC TTL is Left	Percentage of PAC TTL remaining when you should update the PAC.

Related Topics:

- Configuring an NDAC Policy, page 4-24
- Configuring EAP-FAST Settings for Security Group Access, page 4-25
- NDAC Policy Page, page 10-49

Maximum User Sessions

For optimal performance, you can limit the number of concurrent users accessing network resources. ACS 5.8 imposes limits on the number of concurrent service sessions per user.

The limits are set in several different ways. You can set the limits at the user level or at the group level. Depending upon the maximum user session configurations, the session count is applied to the user.

Note To make the maximum sessions work for user access, the administrator should configure RADIUS accounting.

Note To make the maximum sessions work for device management, the administrator should configure TACACS+ session authorization and accounting.

This section contains the following topics:

- Maximum Session User Settings, page 10-52
- Maximum Session Group Settings, page 10-53
- Maximum Session Global Settings, page 10-55
- Purging User Sessions, page 10-55
- Maximum User Session in Distributed Environment, page 10-56
- Maximum User Session in Proxy Scenario, page 10-57

Maximum Session User Settings

You can configure maximum user sessions for each user globally.

To configure maximum user sessions:

Step 1 Choose **Access Policies > Max User Session Policy > Max Session User Settings**.

Step 2 Specify a **Max User Session Value**, for the maximum number of concurrent sessions permitted.

Step 3 Check the **Unlimited Sessions** check box if you want users to have unlimited sessions.

Step 4 Click **Submit**.

Note If the maximum number of sessions is configured at both the user and group level, the smaller value will have precedence.

For example:

Given a user Bob in the group America:US:West with a maximum session value of 5 sessions for the group and a maximum session value of 10 for the user. In this case, user Bob can have a maximum of 5 sessions only.

Related Topics

- Maximum Session Group Settings, page 10-53
- Maximum Session Global Settings, page 10-55
- Purging User Sessions, page 10-55
- Maximum User Session in Distributed Environment, page 10-56
- Maximum User Session in Proxy Scenario, page 10-57

Maximum Session Group Settings

You can configure the maximum number of sessions for the identity groups. All the sessions can sometimes be used by a few users in the group. Requests from other users to create a new session are rejected because the number of sessions has already reached the maximum configured value.

ACS 5.8 allows you to configure a maximum session limit for any user in the group; for example, each user belonging to a specific Identity Group may open not more than the session limit, no matter how many sessions other users from the same group have opened. There is no option to set up a session limit for a particular user.

From the ACS web interface, you can configure the Maximum Sessions limit for a user belonging to an identity group from the ACS web interface.

The ACS 4.x migration utility includes migrating the maximum session configuration.

When calculating the session limit for a particular user, the lowest configuration value takes the precedence—whether the global session limit per user, the session limit per identity group that the user belongs to, or the session limit per user in the group.

To configure maximum sessions for a group:

Step 1 Choose **Access Policies > Max User Session Policy > Max Session Group Settings**.

All the configured identity groups are listed.

Step 2 Check the check box the group for which you want to configure a maximum number of sessions.

Step 3 Click **Edit**.

Step 4 Complete the fields as described in Table 10-30.

Table 10-30 Max User Session Global Settings Page

Option	Description
General	
Name	Name of the Identity Group.
Description	Description of the Identity Group.
Max Session Group Settings	
Unlimited Session	Check this check box if you want to provide unlimited sessions to the group.
Max Session for Group	Specify a value for the maximum number of concurrent sessions permitted for the group.
Unlimited Sessions for Users in Group	Check this check box if you want to provide unlimited sessions for each user in a group.
Max Session for User in Group	Specify a value for the maximum number of concurrent sessions permitted for each user in a group. This option overrides the maximum number of sessions for a group.

Step 5 Click **Submit**.

Unlimited is selected by default. Group-level session limits are applied based on the hierarchy. For example:

The group hierarchy is *America:US:West:CA* and the maximum sessions are as follows:

- America: 100 max sessions
- US: 80 max sessions
- West: 75 max sessions
- CA: 50 max sessions

If "Max Session for User in Group X" is set to N, each user belonging to the group X may open not more than N sessions.

If the user belongs to *America/US/West,* ACS checks that the number of sessions does not exceed the limit that is specified for the parent groups *America/US/West*, *America/US*, *America*. When you set the maximum number of sessions of a user group to 100, the total count of all sessions established by all members of that group cannot exceed 100. Once the session is allowed, the Number of Active Sessions Availed counter for the three nodes is increased by one. The ACS runtime component takes care of this validation during authentication.

Note If the maximum number of sessions is configured at the group level, at the user level within a group level, and at the user level globally, then ACS considers the least value among them.

Related Topics

- Maximum Session User Settings, page 10-52
- Maximum Session Global Settings, page 10-55
- Purging User Sessions, page 10-55
- Maximum User Session in Distributed Environment, page 10-56
- Maximum User Session in Proxy Scenario, page 10-57

Maximum Session Global Settings

You can assign session keys for RADIUS and TACACS+ requests. A session key is provided with a set of attributes for RADIUS and TACACS+. You can customize the session key attributes according to your environment. If you do not assign a session key, ACS uses the default session key values.

A session key is a unique key that is used to track user sessions. The session key helps ACS differentiate between a user re-authenticating to the same session and a user starting a new session. The session key attributes for a single session should be the same in the access request and in the accounting start packet. The Session key helps ACS to identity the session properly. When ACS re-authenticates the same session again, the same key is retained.

To configure the global settings for maximum user sessions, choose **System Administration > Users > Max User Session Global Settings.**

Table 10-31 Max User Session Global Settings Page

Option	Description
RADIUS Session Key Assignment	
Available Session Keys	RADIUS sessions keys available for assignment. **Note** To use the RADIUS Acct-Session-Id (attribute #44) in the RADIUS session key, you should configure the Acct-Session-Id to be sent in the access request: `Router(config)# radius-server attribute 44 include-in-access-req`
Assigned Session Keys	RADIUS session key assigned. The default session keys for RADIUS are: UserName:NAS-Identifier:NAS-Port:Calling-Station-ID
TACACS+ Session Key Assignment	
Available Session Keys	TACACS+ sessions keys available for assignment.
Assigned Session Keys	TACACS+ session key that have been assigned. The default session keys for TACACS+ are: User:NAS-Address:Port:Remote-Address
Max User Session Timeout Settings	
Unlimited Session Timeout	No timeout.
Max User Session Timeout	Once the session timeout is reached, ACS sends a fake STOP packet to close the respective session and updates the session count. **Note** The user is not forced to log out of the device.

Related Topics

- Maximum Session User Settings, page 10-52
- Maximum Session Group Settings, page 10-53
- Purging User Sessions, page 10-55
- Maximum User Session in Distributed Environment, page 10-56
- Maximum User Session in Proxy Scenario, page 10-57

Purging User Sessions

You can use the Purge option only when users are listed as Logged-in but connection to the AAA client has been lost and the users are no longer actually logged in.

Purging will not log off the user from the AAA client, however it will decrease the session count by one. While the count is zero, any interim updates or STOP packet that arrives from the device will be discarded. Due to this purging, if a user logged in with the same user name and password in another AAA client, this session will not be affected.

Note A fake accounting stop is sent irrespective of the session count value.

To purge the User session:

Step 1 Go to **System Administration > Users > Purge User Sessions.**

The Purge User Session page appears with a list of all AAA clients.

Step 2 Select the AAA client for which you want to purge the user sessions.

Step 3 Click **Get Logged-in User List.**

A list of all the logged in users is displayed.

Step 4 Click **Purge All Sessions** to purge all the user session logged in to the particular AAA client.

Related Topics

- Maximum Session User Settings, page 10-52
- Maximum Session Group Settings, page 10-53
- Maximum Session Global Settings, page 10-55
- Maximum User Session in Distributed Environment, page 10-56
- Maximum User Session in Proxy Scenario, page 10-57

Maximum User Session in Distributed Environment

In distributed environment, all the user and identity group configurations are replicated to the secondaries except the session cache related information with respect to maximum user session maintained by runtime. Hence, each server has its own session established details in the runtime. Also, the maximum session count gets applied based on which ACS server the authentication/accounting request is received on.

Related Topics

- Maximum Session User Settings, page 10-52
- Maximum Session Group Settings, page 10-53
- Maximum Session Global Settings, page 10-55
- Purging User Sessions, page 10-55
- Maximum User Session in Proxy Scenario, page 10-57

Maximum User Session in Proxy Scenario

Authentication and accounting requests should be sent to the same ACS server; else the Maximum Session feature will not work as desired.

Related Topics

- Maximum User Sessions, page 10-52
- Maximum Session User Settings, page 10-52
- Maximum Session Group Settings, page 10-53
- Maximum Session Global Settings, page 10-55
- Purging User Sessions, page 10-55
- Maximum User Session in Distributed Environment, page 10-56

Maximum Login Failed Attempts Policy

ACS 5.8 allows the administrator to disable the user accounts after n successive failed attempts. You can configure the maximum login failed attempts count from ACS web interface. This feature is applicable only for internal users. You can configure this feature at user level, identity group level, and globally. ACS 5.8 introduces the maximum login failed attempt count configuration at user level and identity groups level. The global maximum login failed attempt count configuration is already available in ACS.

Note ACS counts the failed attempts until you reach the maximum failed attempts count or make a successful login attempt. ACS does not have a specific time range (such as within 15 minutes, 30 minutes, 1 hour and so on) configured for consecutive failed attempts count calculation.

Note If a user is configured with less number of maximum login failed attempt count and the user group is configured with more number of maximum login failed attempt count, then ACS considers the maximum login failed attempt count at the user level even though it is less.

When a user enters an incorrect login credentials, ACS executes the following maximum login failed attempts policy algorithm:

Step 1 If the maximum login failed attempt count is configured at user level:

- ACS disables the user account if the maximum login failed attempts count is reached.
- ACS allows the user to enter the credentials and try logging in again if the maximum login failed attempts count is not reached.

If the maximum login failed attempt count is not configured at user level, then ACS proceeds to identity group level check.

Step 2 If the maximum login failed attempt count is configured at the identity group that is associated with the user:

- ACS disables the user account if the maximum login failed attempts count is reached.
- ACS allows the user to enter the credentials and try logging in again if the maximum login failed attempts count is not reached.

If the maximum login failed attempt count is not configured at the immediate group that is associated with the user, then ACS proceeds to the parent identity group level.

Step 3 If the maximum login failed attempt count is configured at the parent identity group:

- ACS disables the user account if the maximum login failed attempts count is reached.
- ACS allows the user to enter the credentials and try logging in again if the maximum login failed attempts count is not reached.

If the maximum login failed attempt count is not configured at the parent group, then ACS proceeds to the next level in the hierarchy until it reaches the root of the hierarchical groups. If the maximum login failed attempt count is not configured at any group including the root, then ACS proceeds to the global maximum login failed attempt count check.

Step 4 If the maximum login failed attempts count is configured globally:

- ACS disables the user account if the maximum login failed attempts count is reached.
- ACS allows the user to enter the credentials and try logging in again if the maximum login failed attempts count is not reached.

If the global maximum login failed attempts count configuration is not available, then ACS never disables the user account and allows the user to enter the login credentials and try logging in again and again.

This section describes the following:

- Configuring Maximum Login Failed Attempts Count for Users, page 10-58.
- Configuring Maximum Login Failed Attempts Count for Identity Groups, page 10-59.
- Configuring Maximum Login Failed Attempts Count for Users Globally, page 10-59

Configuring Maximum Login Failed Attempts Count for Users

To configure maximum login failed attempt count for internal users:

Step 1 Choose **Users and Identity Stores > Internal Identity Store > Users**.

The Internal Users page appears.

Step 2 Perform one of the following actions:

- Click **Create**.
- Click the username to whom you want to configure the maximum login failed attempts count, or check the check box next to the name and click **Edit**.

Step 3 Check the **Disable account after *n* successive failed attempts** check box and enter the maximum login failed attempts count in the text box provided.

Step 4 Click **Submit**.

The maximum login failed attempt count for the selected user is configured. The Internal Users page appears with the new configuration.

Configuring Maximum Login Failed Attempts Count for Identity Groups

To configure failed attempts count for identity groups:

Step 1 Choose **Access Policies > Max Login Failed Attempts Policy > Max Login Failed Attempts Group Settings**.

All the configured identity groups are listed.

Step 2 Check the check box next to the group name for which you want to configure the maximum login failed attempts count.

Step 3 Click **Edit**.

The Edit Identity Groups page appears with the identity group name and the description.

Step 4 Check the **Disable account after n successive failed attempts** check box and enter the failed attempts count in the text box provided under **Max Login Failed Attempts Group Settings** area.

Step 5 Click **Submit**.

The maximum login failed attempt count for the selected identity group is configured.

Configuring Maximum Login Failed Attempts Count for Users Globally

To configure failed attempts count for users globally:

Step 1 Choose **System Administration > Users > Authentication Settings > Advanced.**

The User Authentication Settings page appears with the Advanced tab.

Step 2 Check the **Disable account if** check box.

Step 3 Check the **Failed Attempts Exceed** check box and enter the maximum login failed attempts count in the text box provided.

Step 4 Click **Submit**.

The maximum login failed attempt count for internal users is configured globally.

Note If the authentication points of the primary and secondary instances are in different geographical locations, you can expect a delay in Distributed Deployment update across the Wide Area Network, thereby leading to a delayed update from the secondary instance to the primary instance. In this case, if you authenticate a user against a secondary instance in a deployment which is in a geographical location other than where the primary instance is located, the feature “Disable User after N failed attempt count” will not work properly.