Cisco APE User Model

This chapter describes the following sections:

Object Attributes

You can configure and operate Cisco APE through a set of data classified as objects that are arranged in a hierarchy. Each object contains attributes that define the behavior of each object.

This chapter describes the attributes of the following objects:

- Users
- Resources
- Authorization Devices
- Roles
- Resource Types
- Locations
- Policies

About Users

Users represent both the Cisco APE system administrators and the operators.

Table 2-1 lists user attributes, which you can set or change.

Note When a field is listed as required, you must supply a value. If a default is set, you can use the default, or change it to something else, but you cannot remove the default. You must supply values to all required fields when there are no default values given.

Table 2-1 User Attributes

Attribute	Description
User ID	Required. Usernames must be unique. Can be a string up to 128 printable characters
Description	Optional. Can be a string up to 255 printable characters.
Password	A required attribute. Can be a string up to 64 characters. Must be stored securely and be able to be retrieved in original format to support Challenge Handshake Authentication Protocol (CHAP) and MS-CHAP.
Level 0 enable password	Optional. Can be a string up to 64 characters.
First name	Optional. Can be a string up to 128 printable characters.
Last name	Optional. Can be a string up to 128 printable characters.
ID number	Optional. Can be a string up to 128 printable characters.
Phone number	Optional. Can be a string up to 128 printable characters.
Supervisor's name	Optional. Can be a string up to 128 printable characters.

About Resources

Resources are provided by various devices to which you must control access. Resources can be offered by any kind of device (Telco device, IOS devices, and so on). Any resource that can be accessed through an IP address, or Domain Name System (DNS) and an optional network port is a resource. The term, resource also represents objects that you can authorize access to by using Cisco APE.

Operators can browse and connect to a resource. Also, the TACACS+ server can process authorization requests against resources.

Table 2-2 lists resource attributes which you can set or change.

Table 2-2 Resource Attributes

Attribute	Description
Name	Required. Must be unique within the resource location. Can be a string up to 128 printable characters
Description	Optional. Can be a string up to 255 printable characters.

Table 2-2 Resource Attributes (continued)

Attribute	Description
IP address	Optional. Must be in the IP address format. Cisco IOS allows you to create an alias for line IDs and Hunt groups on a given Cisco IOS device to an IP address, and attempts to connect to the alias are routed through the Cisco IOS device to the line or Hunt group. You can use this IP address in the URL provided in the operators' UI. **Note** If you do not enter this attribute, the IP address of the authorization device and the network port for this resource will be used to build the URL for the resources in the operators' UI.
Network port	Required. Must be an integer. An operator can Telnet to this port to access the resource. In the case of devices hanging off a serial line, this information can be used to determine the line ID that the resource is attached to. This is necessary for authorization.
Enabled or disabled flag	Required. The default value is Enabled. This is a toggle setting on a device. When you set the switch to Disable it will not accept any authorization requests, and the Resource does not appear on the operators' UI.
DNS Name	This is an optional value and must be in the standard DNS name format. You can provide this name when you use the IP address alias feature. The DNS name then maps to the alias IP address. (See IP address attribute)

Note A single device can provide zero or more resources in the Cisco APE user model.

About Hunt Group Resources

A Hunt group is a collection of devices. These devices are associated together such that incoming calls to the Hunt group are automatically distributed across the set of lines by an algorithm. When an operator connects to a Hunt group, the T+ device routes the connection to one of the lines making up the Hunt group. The lines can all go to one physical device or to multiple devices.

A Hunt group resource represents a Hunt group on a Cisco IOS device. You can use the resource to control access to that Hunt group. You can add a Hunt group resource to a role instead of adding each resource in that Hunt group to a Role.

Table 2-3 lists Hunt group resource attributes that you can set or change.

Table 2-3 Hunt Group Resource Attributes

Attribute	Description
Name	Required. Must be unique within the resource location. Can be a string up to 128 printable characters
Description	Optional. Can be a string up to 255 printable characters.

Table 2-3 Hunt Group Resource Attributes (continued)

Attribute	Description
IP address	Optional if you have entered the network port attribute; required if you have not entered the network port. **Note** You can enter both the IP address and the network port. Cisco IOS allows you to create an alias for line IDs and Hunt groups on a given Cisco IOS device to an IP address, and attempts to connect to the alias are routed through the Cisco IOS device to the Hunt group. You can use this alias IP address in the URL provided in the operators' UI. **Note** If you do not enter this attribute, the IP address of the authorization device and the network port for this resource will be used to build the URL for the resources in the operators' UI.
Network Port	The port to which an operator Telnets to access the resource. In the case of devices hanging off a serial line, you can use this information to determine the line ID. Optional if you have entered the IP address; required if you have not entered the IP address. Must be an integer. You can enter both the IP address and the network port.
Enabled or Disabled Flag	Required. The default value is Enabled. This is a toggle setting on a device. When you set it to Disable, the resource does not appear on the operators' UI.
DNS Name	Optional. Must be in the standard DNS name format. Enter this name when you use the IP address alias feature. The DNS name then maps to the alias IP address. (See IP address.)

About Authorization Devices

An authorization device represents a TACACS+ device or client in the system. The authorization device enforces access control to resources.

Specifying and defining Authorization devices in this system serves two functions:

- Defines valid internal TACACS+ server clients.
- Provides a point of access for resources that do not have IP addresses.

Note Any resource in the system must refer to an authorization device, so authorization devices are a required part of a working configuration. Defining an authorization device itself does not define any resources. If an authorization device offers one or more resources (like a command or configuration shell), you must separately define those resources.

Table 2-4 lists authorization device attributes which you can set or change.

Table 2-4 Authorization Device Attributes

Attribute	Description
Name	Required. Must be unique within the location of the authorization device. Can be a string up to 128 characters.
Description	Optional. Can be a string up to 255 characters.
TACACS+ Key	Required. Can be a string up to 128 characters. This is a shared secret used to authenticate the TACACS+ client (the authorization device) and the Cisco APE TACACS+ server.
IP address	Required. Must be in the IP address format. This is the address that a TACACS+ request from the authorization device originates from. You can use this address in the Telnet URLs provided in the operators' UI to see resources accessible when you use the authorization device.

About Roles

Roles are relationships of permissions, resources, policies, and users. Use roles to:

- Control user access to resources.
- Assign roles and access rights that are associated with each role.

Roles are defined based on unique positions in an organizational structure. Associate access rights with these roles based on the tasks that you assign to a user in a role.

Table 2-5 lists role attributes that you can set or change.

Table 2-5 Role Attributes

Attribute	Description
Name	Required. Must be unique among role names. Can be a string up to 128 printable characters long.
Description	Optional. Can be a string up to 255 printable characters long.
Permissions	Optional. You can create a set of zero or more permissions for a Role. Each permission can be one or more of the following fixed permissions: • Cisco APE Administrative Access • Change Password • Resource Access or • CLI matching expressions

About Resource Types

Resource types are a classification and navigation mechanism for resources.

Table 2-6 lists resource type attributes that you can set or change.

Table 2-6 Resource Type Attributes

Attribute	Description
Name	Required. Must be a unique name under the parent for this resource type. Can be a string up to 128 printable characters long.
Description	Optional. Can be a string up to 255 printable characters long.

About Locations

Locations are a classification and navigation mechanism for resources. Locations refer to a geographical region of a device or an operator.

Note Each user or device must belong to a location.

Table 2-7 lists location attributes that you can set or change.

Table 2-7 Location Attributes

Attribute	Description
Name	Required. Must be unique under the parent of this location. Can be a string up to 128 printable characters long.
Description	Optional, and can be a string up to 255 printable characters long.
User-defined fields	Optional. Can be a string up to 255 printable characters long. You can specify labels for each field. These labels would appear on the Operations UI or the Management UI any time this information is displayed or entered.
Attribute	**Description**
Name	Required. Must be unique under the parent of this location. Can be a string up to 128 printable characters long.
Description	Optional, and can be a string up to 255 printable characters long.

About Policies

Policies are rules that apply to roles for access control. Policies allow you to attach business logic to roles. This logic ensures that certain conditions are true before allowing a role to be used in satisfying an authorization request.

Table 2-8 lists policy attributes that you can set or change.

Table 2-8 Policy Attributes

Attribute	Description
Name	Required. Must be unique among policies. Can be a string up to 128 printable characters long.

Table 2-8 Policy Attributes (continued)

Attribute	Description
Description	Optional. Can be a string up to 255 printable characters long.
Conditions	Policies can have one or more conditions up to a maximum of five. For a Policy to be successfully applied, all the conditions must evaluate to "true". In other words, all the conditions in a Policy are logically "ANDed" together.

About Conditions Governing Policies

Resource in Location *X*

This condition evaluates to true if the location of the resource specified in the authorization request is equal to or under the location specified by you (X). When configuring this condition, you must provide a valid location.

Example:

Resource in /US/MA/Middlesex

This condition evaluates to true for any resource with a location of /US/MA/Middlesex or a location under /US/MA/Middlesex.

User in Location *Y*

This condition evaluates to true if the location of the user specified in the authorization request is equal to or under the location specified by you (*Y*). When configuring this condition, you must provide a valid location.

Example:

User in /US/MA/Middlesex

This condition evaluates to true for any user with a location of /US/MA/Middlesex or a location under /US/MA/Middlesex.

Resource in User's Location

This condition evaluates to true if the location of the resource specified in the authorization request is equal to or under the location of the user specified in the authorization request. When selecting this condition, you do not need to provide any other input.

Resource is a Resource Type *Z*

This condition evaluates to true if the resource type of the resource specified in the authorization request is equal to or under the resource type specified by you (*Z*). When configuring this condition, you must provide a valid resource type.

Example:

Resource is a Cisco/IOS/Switch

This condition evaluate to true for any resource with a resource type of Cisco/IOS/Switch or a resource type under Cisco/IOS/Switch.

Remote Address is A.B.C.D

This condition evaluates to true if the RemoteAddress specified in the authorization request is equal to the one specified by the administrator (A.B.C.D).

Example:

Remote Address is 10.1.1.19

Relationships of Objects

This section describes the data model of Cisco APE and how all the objects work together.

Relationship Between Users and Roles

A user may or may not belong to a role. You can establish this relationship when you are configuring Cisco APE and define which users are members of a particular role. When roles refer to users, it is an indication that a user is a member of that role. A user can be a member of zero or more roles, and roles can refer to zero or more users.

When a role refers to a user, the role can refer to different sets of users:

- Any user. You can add any user to a role.
- Any authenticated user. A role applies to any authenticated user in the system.
- An entire set of users. A role applies to an entire set of users.

Relationship Between Users and Locations

- A user may or may not have a location.
- You can establish this relationship at the time of configuring Cisco APE.
- A user can have only one location.
- You can use this attribute with policies to grant access based upon the user's location.
- Zero or more users can have the same location.

Relationship Between Users and Policies

A user and a policy may or may not be related. This is a dynamic relationship, and is established during an authorization request after you have configured the system. When users request access to a device, a policy can evaluate attributes of users, such as their location to assist in access control.

Relationship Between Resources and Roles

- You can assign resources to roles when configuring Cisco APE.
- Resources indicate which users in a role can have permissions to the resources.
- A role may refer to zero or more resources, and a resource may have zero or more roles.

A role can also refer to a predefined resource group. You can create a role which applies to all resources, or create roles which use policies to choose the resources for which the roles apply.

Relationship Between Resources and Resource Types

A resource may have one resource type. Zero or more resources can have the same resource type.

By using policies, you can grant access to a resource based on the resource type. You can also use policies to present resources in the resource type hierarchy in the operators' UI.

Relationship Between Resources and Locations

A resource may or may not have a location. Zero or more resources can have the same location.

By using policies, you can grant access to a resource based on the location of the resource. You can also use policies to present resources in the locations hierarchy in the operators' UI.

Relationship Between Resources and Hunt Group Resources

Hunt groups are logical groups of resources. You can add zero or more resources to a Hunt group resource during configuration.

Relationship Between Resources and Policies

The relationship between resources and policies is established at run time when a user requests authorization to access a resource. Policies examine the attributes of a resource, such as location, or resource type.

Relationship Between Roles

Roles can relate to other roles as parents. A role can be a "child" of another role. When you establish a parent-child relationship between two roles, the child role picks up the following attributes from the parent role:

- Permissions
- Policies
- Resources

You can have zero or one parent role. A role may have zero or more "childrens'" roles.

Relationship Between Roles and Policies

You can use policies in roles to enforce rules. A role may have zero or more policies. A policy can refer to zero or more roles.

Relationship Between Resource Types

A resource type:

- May have a parent-child relationship with another resource type. The parent-child relationship allows you to define a hierarchy of resource types.
- Must have one parent.
- May have zero or more "children" resource types.
- Can refer to a predefined root node as a parent.

Relationship Between Resource Types and Policies

The relationship between resource types and policies is established both when you specify a resource type in a policy, or when an authorization request is processed. When a user makes an authorization request, a policy examines the specified resource type to control access.

Relationship Between Locations

You must establish a parent-child relationship between locations and define a location hierarchy. A location:

- May have a predefined root as the parent location, so that the root appears in the top-level of the location hierarchy.
- Must have a parent location.

- May have zero or more “child” locations.

When you define a location to location relationship, the parent locations will appear as trees consisting of branches or “children” locations.

Relationship Between Locations and Policies

A relationship between locations and policies is established when you specify a location in a policy and during an authorization request. When a user makes an authorization request, policies check the specified location attribute of a resource and a user to assist in access control.

Relationship Between Authorization Devices and Resources

An authorization device may have zero or more resources.

Note A resource can have only one authorization device.

You can establish a relationship between an authorization device and a resource when you add the resource to the system. Access to the resource is enforced by the specified authorization device.