Device Administration with Cisco Secure Access Control System 5.x

Q. What are network device groups in ACS?

A. In Cisco Secure Access Control System 5, you can define network device groups (NDGs), which are sets of devices. These NDGs provide logical grouping of devices (for example, by Device Location or Device Type) that you can use in policy conditions.

Q. How does Cisco Secure Access Control System use NDGs?

A. When the Cisco Secure Access Control System receives a request for a device, the network device groups associated with that device are retrieved and compared against those in the policy table. With this method, you can group multiple devices and assign them the same policies. For example, you can group all devices in a specific location together and assign to them the same policy.

Q. What is the maximum number of NDGs can I create?

A. Twelve (12) including the default (predefined) device groups: Device Type and Device Location.

Q. What are NDG hierarchies?

A. The device group hierarchy is the hierarchical structure that contains the network device groups. Two of these, Device Location and Device Type, are predefined; you cannot change their names or delete them.

Q. How do NDGs relate to device group hierarchy?

A. An NDG relates to any node in the hierarchy and is the entity with which devices are associated. These nodes can be any node within the hierarchy, not just leaf nodes.

Q. How many NDG levels (nodes) can be added to each hierarchy?

A. You can have a maximum of six nodes in the NDG hierarchy, including the root node.

Q. How can I create, duplicate, or edit a network device group?

A. See http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.2/user/guide/net_resources.html#wp1052534

Q. How do I delete a network device group?

A. See http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.2/user/guide/net_resources.html#wp1090910

Q. How do I create, duplicate, or edit a network device group node within a NDG hierarchy?

A. See http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.2/user/guide/net_resources.html#wp1052576

Q. How do I delete a network device group from within a hierarchy?

A. See http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.2/user/guide/net_resources.html#wp1052610

Q. How are network devices that are defined in Cisco Secure Access Control System permitted access to the network?

A. They may be permitted with a specific IP address or a subnet mask, where all IP addresses within the subnet can access the network. The device definition includes the association of the device with network device groups (NDGs).

Q. What authentication, authorization, and accounting (AAA) protocols does Cisco Secure Access Control System support for network device administration?

A. Terminal Access Controller Access-Control System Plus (TACACS+) or RADIUS, and Cisco TrustSec®, if it is a Cisco TrustSec device. You must install the Cisco TrustSec license to enable Cisco TrustSec options. The Cisco TrustSec options only appear if you have installed the Cisco TrustSec license.

Q. How many devices can be added with Cisco Secure Access Control System Base license?

A. Up to 500.

Q. How are the devices counted based on their IP address and mask?

A. When you use subnet masks, the number of unique IP addresses depends on the number of IP addresses available through the subnet mask. For example, a subnet mask of 255.255.255.0 means you have 256 unique IP addresses.

Q. How many devices are supported with a large deployment license?

A. There is no enforced limit, but Cisco has tested up to 50,000 devices.

Q. How can I view and import network devices?

A. See http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.2/user/guide/net_resources.html#wp1094156

Q. How do I export a list of network devices?

A. See http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.2/user/guide/net_resources.html#wp1093668

Q. What protocols are supported for device administration?

A. RADIUS and TACACS+.

Q. How can I define authorization profiles for device administration roles and permissions?

A. You can configure Cisco IOS® Software shell profiles and command sets for user authorization. Shell profiles and command sets are combined for authorization purposes.

Q. What are shell profiles?

A. Shell profile authorization provides decisions for the following capabilities for the user requesting authorization and is enforced for the duration of a user's session:

- Privilege level
- General capabilities, such as device administration and network access

Q. How can I use shell profile definitions for authorization and access privilege decisions on the Cisco Secure Access Control System?

A. Shell profile definitions are split into two components:

- Common tasks
- Custom attributes

The Common Tasks tab allows you to select and configure the frequently used attributes for the profile. The attributes that are included here are those defined by the TACACS+ protocol draft specification that is specifically relevant to the shell service. However, the values can be used in the authorization of requests from other services. The Custom Attributes tab allows you to configure additional attributes. Each definition consists of attribute name, an indication of whether the attribute is mandatory or optional, and the value for the attribute. Custom attributes can be defined for nonshell services.

After you create shell profiles and command sets, you can use them in authorization and permissions within rule tables.

Q. How do I create, duplicate, or edit a shell profile?

A. See http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.2/user/guide/pol_elem.html#wp1053110

Q. How can I define Common Tasks to configure privilege levels for a shell profile?

A. See http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.2/user/guide/pol_elem.html#wp1053199

Q. How can I define custom attributes for the shell profile?

A. See http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.2/user/guide/pol_elem.html#wp1053259

Q. What are command sets and how can I use them to define device administration role restrictions?

A. Command sets provide decisions for allowed commands and arguments for device administration. You can specify command sets as results in a device configuration authorization policy. After you create command sets, you can use them in authorizations and permissions within rule tables. A rule can contain multiple command sets.

Q. Can I create or duplicate similar command sets from an existing command set?

A. Yes. You can duplicate a command set if you want to create a new command set that is the same, or similar to, an existing command set. After duplication is complete, you access each command set (original and duplicated) separately to edit or delete them.

Q. What protocol attributes do command sets support?

A. Command sets support TACACS+ protocol attributes only.

Q. How do I create, duplicate, or edit a new command set?

A. See http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.2/user/guide/pol_elem.html#wp1077595

Q. What are downloadable access control lists (ACLs) and how can I use them for device administration?

A. You can define downloadable ACLs for the Access-Accept message to return. Use ACLs to prevent unwanted traffic from entering the network. ACLs can filter source and destination IP addresses, transport protocols, and more by using the RADIUS protocol. After you create downloadable ACLs as named permission objects, you can add them to authorization profiles, which you can then specify as the result of an authorization policy.

Q. How can I create, duplicate, or edit downloadable ACLs for device administration?

A. See http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.2/user/guide/pol_elem.html#wp1053438

Q. What is a device administration authorization policy and when can I create such a policy?

A. A device administration authorization policy determines the authorizations and permissions for network administrators. You can create an authorization policy during access service creation.

Q. How can I use device administration authorization policies?

A. Using Device *Administration Authorization Policy* page in Cisco Secure Access Control System GUI, you can:

View policy rules.

- Delete policy rules.

Open pages that enable you to create, duplicate, edit, and customize device administration policy rules.

Q. What are the different the *statuses* of a device administration authorization policy rule?

A. The rule statuses are:

- Enabled - The rule is active.
- Disabled - The Cisco Secure Access Control System does not apply the results of the rule.
- Monitor - The rule is active, but Cisco Secure Access Control System does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.

Q. What are the *conditions* of a device administration authorization policy rule?

A. Rule 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.

Q. What are the *results* of a device administration authorization policy rule?

A. The rule results are 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 to shell profiles, or command sets, or both. The columns that appear reflect the customization settings.

Q. What is a default device administration authorization policy rule?

A. Cisco Secure Access Control System applies the default rule when:

- Enabled rules are not matched.
- No other rules are defined.

Click the Default Rule link to edit the default rule. You can edit only the results of the default rule; you cannot delete, disable, or duplicate it.

Q. How can I customize the conditions and results of a device administration authorization policy rule?

A. Click the Customize button at the right side of the bottom of the page displaying Authorization Policy rules. This 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.

Warning: If you remove a condition type after defining rules, you will lose any conditions that you configured for that condition type.

Q. How can I configure device administration authorization rule properties?

A. See http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.2/user/guide/access_policies.html#wp1054484

Q. How can I configure shell/command authorization policies for device administration?

A. When you create an access service and select a service policy structure for Device Administration, Cisco Secure Access Control System 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.

For more details, see
http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.2/user/guide/access_policies.html#wp1054600

Q. What is an authorization exception policy?

A. 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.

Q. How do I configure authorization exception policies?

A. See http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.2/user/guide/access_policies.html#wp1054630

Q. How can I create, duplicate, edit and delete access service policy rules?

A. See http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.2/user/guide/access_policies.html#wp1054721

Q. What are compound conditions?

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

Q. How can I configure compound conditions for access service policy rules?

A. See http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.2/user/guide/access_policies.html#wp1054918

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

Printed in USA

C67-649357-00 02/11