



CVD



# Device Management Using ACS

## TECHNOLOGY DESIGN GUIDE

August 2013



# Table of Contents

---

- Preface.....1
- CVD Navigator .....2
  - Use Cases ..... 2
  - Scope ..... 2
  - Proficiency ..... 2
- Introduction .....3
  - Technology Use Case ..... 3
    - Use Case: Controlling Change to the Network Configuration ..... 3
  - Design Overview..... 3
- Deployment Details.....5
  - Deploying Authentication and Authorization ..... 5
  - Limiting Access to Devices Based on the User Role ..... 22
- Appendix A: Product List .....28

# Preface

Cisco Validated Designs (CVDs) provide the framework for systems design based on common use cases or current engineering system priorities. They incorporate a broad set of technologies, features, and applications to address customer needs. Cisco engineers have comprehensively tested and documented each CVD in order to ensure faster, more reliable, and fully predictable deployment.

CVDs include two guide types that provide tested and validated design and deployment details:

- **Technology design guides** provide deployment details, information about validated products and software, and best practices for specific types of technology.
- **Solution design guides** integrate or reference existing CVDs, but also include product features and functionality across Cisco products and may include information about third-party integration.

Both CVD types provide a tested starting point for Cisco partners or customers to begin designing and deploying systems using their own setup and configuration.

## How to Read Commands

Many CVD guides tell you how to use a command-line interface (CLI) to configure network devices. This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

Commands at a CLI or script prompt appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
police rate 10000 pps burst 10000 packets conform-action set-discard-class-  
transmit 48 exceed-action transmit
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

```
interface Vlan64  
  ip address 10.5.204.5 255.255.255.0
```

## Comments and Questions

If you would like to comment on a guide or ask questions, please use the [feedback form](#).

For the most recent CVD guides, see the following site:

<http://www.cisco.com/go/cvd>

# CVD Navigator

---

The CVD Navigator helps you determine the applicability of this guide by summarizing its key elements: the use cases, the scope or breadth of the technology covered, the proficiency or experience recommended, and CVDs related to this guide. This section is a quick reference only. For more details, see the Introduction.

## Use Cases

This guide addresses the following technology use cases:

- **Controlling Change to the Network Configuration**—Without a centralized access and identity policy enforcement point, it's difficult to ensure the reliability of a network as the number of network devices and administrators increases.

For more information, see the “Use Cases” section in this guide.

## Scope

This guide covers the following areas of technology and products:

- Integration of Cisco Secure Access Control System and Microsoft Active Directory provides differentiated management access based on user and device.

For more information, see the “Design Overview” section in this guide.

## Proficiency

This guide is for people with the following technical proficiencies—or equivalent experience:

- **CCNA Security**—1 to 3 years installing, monitoring, and troubleshooting network devices to maintain integrity, confidentiality, and availability of data and devices
- **VCP VMware**—At least 6 months installing, deploying, scaling, and managing VMware vSphere environments

# Introduction

---

## Technology Use Case

The ongoing explosion of different types of IP data, along with the perennial increase in the sheer volume of data, has necessitated a commensurate growth in the supporting network infrastructure—routers, switches, firewalls, wireless LAN controllers, and so on. Enterprise network infrastructures can comprise hundreds, even thousands, of network devices.

Controlling and monitoring change to the network configuration are essential parts of meeting the availability requirements of the critical services the network provides. However, when you control and monitor change to the network configuration separately on each device, the difficulty and complexity increase as the number of devices increase.

As the number of network devices in a typical network has grown, the number of administrators required to keep the network operating has likewise increased. These administrators are inevitably spread across the organization, and they may be employed by different departments. The larger and more complex the network and organization, the more complex the resulting system administration structure becomes. Without a mechanism to control which administrators can perform which commands upon which devices, problems with the security and reliability of the network infrastructure become unavoidable.

### Use Case: Controlling Change to the Network Configuration

Without a centralized access and identity policy enforcement point, it's difficult to ensure the reliability of a network as the number of network devices and administrators increases.

This design guide enables the following capabilities:

- Control of administrator authentication and authorization to the network devices from a central location
- Control of who can manage the network, based on AD user group and network device type
- Control of what level of management access an administrator has, based on AD user group and network device type

## Design Overview

Cisco Secure Access Control System (ACS) is the centralized identity and access policy solution that ties together an organization's network access policy and identity strategy. Cisco Secure ACS operates as a centralized authentication, authorization, and accounting (AAA) server that combines user authentication, user and administrator access control, and policy control in a single solution.

Cisco Secure ACS 5.3 uses a rule-based policy model, which allows for security policies that grant access privileges based on many different attributes and conditions in addition to a user's identity.

The capabilities of Cisco Secure ACS coupled with an AAA configuration on the network devices reduce the administrative issues that surround having static local account information on each device. Cisco Secure ACS can provide centralized control of authentication, which allows the organization to quickly grant or revoke access for a user on any network device.

Rule-based mapping of users to identity groups can be based on information available in an external directory or an identity store such as Microsoft Active Directory. Network devices can be categorized in multiple device groups, which can function as a hierarchy based on attributes such as location, manufacturer, or role in the network. The combination of identity and device groups allows you to easily create authorization rules that define which network administrators can authenticate against which devices.

These same authorization rules allow for privilege-level authorization. Privilege-level authorization can be used to give limited access to the commands on a device. Cisco IOS® Software has 16 privilege levels: 0 to 15. By default, upon the first connection to a device command line, a user's privilege level is set to 1. Privilege level 1 includes all user-level commands at the device > prompt. To change the privilege level, the user must run the enable command and provide the enable password. If the password is correct, privilege level 15 is granted, which includes all enable-level commands at the device # prompt. Authorization rules can assign minimum and maximum privilege levels. For example, a rule can give network administrators enable-level (that is, Level 15) access as soon as they log in, or limit helpdesk users so they can issue user-level (Level 1) commands only.



# Deployment Details

## PROCESS

### Deploying Authentication and Authorization

1. Register the software license certificate
2. Set up the Cisco Secure ACS platform
3. Enable the default network device
4. Create internal identity store groups
5. Create internal identity store users
6. Create an external identity store
7. Create an identity store sequence
8. Create shell profiles
9. Map external groups to internal groups
10. Create authorization policy rules

The following process outlines the procedures for deploying Cisco Secure ACS for network device administration. They provide instructions for setting up two policies that apply different privileges to helpdesk users and network administrators. The procedures explain how to configure Cisco Secure ACS to authenticate users against Microsoft Active Directory and then against its local identity store, as well as how to pull group membership information from the Active Directory service.

#### Procedure 1 Register the software license certificate

A product authorization key (PAK) for each Cisco Secure ACS 5.3 license that you purchase is affixed as a sticky label to the bottom of the Software License Claim Certificate card included in your package. You must submit the PAK that you received to obtain valid license files for your system. For each PAK that you submit, you receive a license file via email. You should save the license file to disk. You must install these license files when you set up Cisco Secure ACS.

**Step 1:** Carefully follow the instructions on the Software License Claim Certificate card.

## Procedure 2 Set up the Cisco Secure ACS platform

**Step 1:** Power on the Cisco Secure ACS. At the login prompt, type **setup**, and then press **Enter**.

```
*****
Please type 'setup' to configure the appliance
*****
localhost login: setup

Enter the platform login parameters.
Press 'Ctrl-C' to abort setup
Enter hostname[: acs
Enter IP address [: 10.4.48.15
Enter IP default netmask[: 255.255.255.0
Enter IP default gateway[: 10.4.48.1
Enter default DNS domain[: cisco.local
Enter Primary nameserver[: 10.4.48.10
Add/Edit another nameserver? Y/N : N
Enter username[admin]:
Enter password: *****
Enter password again: *****
Bringing up network interface...
Pinging the gateway...
Pinging the primary nameserver ...
Do not use 'Ctrl-C' from this point on...
Appliance is configured Installing applications...
Installing acs ...
Generating configuration...
Rebooting...
```

The system reboots automatically and displays the Cisco Secure ACS login prompt. Now, you can use this username and password to log in.

**Step 2:** Configure the synchronized clock.

```
acs/admin(config)# ntp server 10.4.48.17
The NTP server was modified.
If this action resulted in a clock modification, you must restart ACS.
acs/admin(config)# clock timezone US/Pacific
```

**Step 3:** Log in to Cisco Secure ACS via the GUI (<https://acs.cisco.local>). The GUI login is a different account than the platform login you created in Step 2. Enter the default credentials: **acsadmin/default**. You will be prompted to change the password.

**Step 4:** Browse to the license file, and then click **Install**. The license is installed.



### Procedure 3 Enable the default network device

**Step 1:** Navigate to **Network Resources > Default Network Device**.

**Step 2:** In the **Default Network Device Status** list, choose **Enabled**.

Next, you must show the TACACS+ configuration.

**Step 3:** Under Authentication Options, click the arrow next to **TACACS+**.

**Step 4:** In the Shared Secret box, type the secret key that is configured on the organization's network infrastructure devices. (Example: SecretKey)

**Step 5:** Clear the **RADIUS** check box, and then click **Submit**.

**Default Network Device**  
The default device definition can optionally be used in cases where no specific device definition is found that matches a device IP address.

Default Network Device Status: **Enabled**

**Network Device Groups**

Location:

Device Type:

**Authentication Options**

▼ TACACS+ ☒

Shared Secret:

☐ Single Connect Device

☒ Legacy TACACS+ Single Connect Support

☐ TACACS+ Draft Compliant Single Connect Support

► RADIUS ☐

= Required fields

### Procedure 4 Create internal identity store groups

Create groups in the Cisco Secure ACS internal identity store for network device administrators and helpdesk users. Users in the network device administrator group have enable-level EXEC access to the network devices when they log in, while helpdesk users must type in the enable password on the device in order to get enable-level access.

Table 1 - Internal identity group

Group name	Description
Helpdesk	Users who are allowed to log in to a device but not make changes
Network Admins	Users who are allowed to log in to a device and make changes

**Step 1:** Navigate to **Users and Identity Stores > Identity Groups**.

**Step 2:** Click **Create**.

**Step 3:** In the **Name** box, enter **Network Admins**, and then enter a description for the group.

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

The screenshot shows a 'General' configuration form. It has three main fields: 'Name' with the value 'Network Admins', 'Description' which is empty, and 'Parent' with the value 'All Groups'. There is a 'Select' button next to the 'Parent' field. A legend at the bottom left indicates that an orange asterisk icon represents 'Required fields'.

**Step 5:** Repeat Step 2 through Step 4 for the Helpdesk group, using the values from Table 1.

The screenshot shows the 'Identity Groups' management page. At the top, there is a breadcrumb trail 'Users and Identity Stores > Identity Groups'. Below this is a search bar with 'Filter:', 'Match if:', and a 'Go' button. A table lists the identity groups:

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	▼ All Groups	Identity Group Root
<input type="checkbox"/>	Helpdesk	
<input type="checkbox"/>	Network Admins	

At the bottom of the page, there are buttons for 'Create', 'Duplicate', 'Edit', 'Delete', 'File Operations', and 'Export'.

## Procedure 5 Create internal identity store users

The Cisco Secure ACS internal identity store can contain all the network administrator accounts or just accounts that require a policy exception if an external identity store (such as Microsoft Active Directory) is available. A common example of an account that requires an exception is one associated with a network management system that allows the account to perform automated configuration and monitoring.

**Step 1:** Navigate to **Users and Identity Stores > Internal Identity Stores > Users**.

**Step 2:** Click **Create**.

**Step 3:** Enter a name, description, and password for the user account.

The screenshot shows the 'Create' user account form. The breadcrumb trail is 'Users and Identity Stores > Internal Identity Stores > Users > Create'. The form is divided into several sections: 'General' with fields for Name (admin), Status (Enabled), Description (Example Network Device Manager), and Identity Group (All Groups); 'Password Information' with fields for Password Type (Internal Users), Password, and Confirm Password; 'Enable Password Information' with fields for Enable Password and Confirm Password; and 'User Information' with a note that there are no additional identity attributes defined for user records. A legend indicates that orange asterisks denote required fields. At the bottom are 'Submit' and 'Cancel' buttons.

**Step 4:** To the right of Identity Group, click **Select**.

**Step 5:** Select the option button next to the group with which you want to associate the user account.

The screenshot shows the 'Identity Groups' selection dialog. It has a search bar with 'Filter' and 'Match if' dropdowns. Below is a table with two columns: 'Name' and 'Description'. The table lists three groups: 'All Groups' (Identity Group Root), 'Helpdesk' (Users who are allowed to login to a device but not make changes), and 'Network Admins' (Users who are allowed to login to a device and make changes). The 'Network Admins' group is selected. At the bottom are 'Create', 'Duplicate', 'File Operations', 'Export', 'OK', 'Cancel', and 'Help' buttons.

Name	Description
All Groups	Identity Group Root
Helpdesk	Users who are allowed to login to a device but not make changes
Network Admins	Users who are allowed to login to a device and make changes

**Step 6:** Click **OK**, and then click **Submit**.

**Step 7:** Repeat Step 2 through Step 6 for each user account you want to create.

## Procedure 6 Create an external identity store

An *external identity store* allows designated users to authenticate against a network device by using their pre-existing credentials. You can also use attributes (such as group membership) in the external store when defining authorization policy rules.

**Step 1:** Navigate to **Users and Identity Stores > External Identity Stores > Active Directory**.

**Step 2:** Enter the Microsoft Active Directory domain name and user credentials.

Users and Identity Stores > External Identity Stores > Active Directory

**General**

**Connection Details**

Active Directory Domain Name:

Please specify the credentials used to join this machine to the Active Directory Domain:

Username:

Password:

You may use the Test Connection Button to ensure credentials are correct and Active Directory Domain is reachable.

Click on 'Save Changes' to connect to the Active Directory Domain and save this configuration. Once you have successfully connected to the Domain, you can select the Directory Groups and Directory Attributes to be available for use in policy rules.

**End User Authentication Settings**

☒ Enable password change

☒ Enable machine authentication

☐ Enable Machine Access Restrictions

Aging time (hours):

**Connectivity Status**

Joined to Domain: Connectivity Status:

\* = Required fields

**Step 3:** Click **Save Changes**.

Connectivity Status changes to **CONNECTED**.

<b>Connectivity Status</b>
Joined to Domain: cisco.local    Connectivity Status: <b>CONNECTED</b>

**Step 4:** Click the **Directory Groups** tab, and then click **Select**.

The screenshot shows the 'Directory Groups' tab in the Cisco Secure ACS configuration interface. At the top, there are three tabs: 'General', 'Directory Groups' (which is selected), and 'Directory Attributes'. Below the tabs, a text box states: 'Directory groups must be selected on this page to be available as options in group mapping conditions in policy rules. Click 'Select' to launch a dialog to select groups from the directory.'

Under the heading 'Selected Directory Groups:', there is a large, empty rectangular box with a vertical scrollbar on the right side, intended for listing selected groups. Below this box are five buttons: 'Add A', 'Edit V', 'Replace A', 'Deselect', and 'Select'. The 'Select' button is the one to be clicked according to the instructions.

Below the buttons is a 'Group Name' text input field. Underneath the input field, an example for group format is provided: 'cisco.com/Users/Domain Users'. At the bottom left, a legend indicates that an orange asterisk icon represents 'Required fields'.

**Step 5:** Select the check box next to each Microsoft Active Directory group that you want to use during the definition of the Cisco Secure ACS authentication policies, and then click **OK**.

The screenshot shows the 'External User Groups' dialog box. At the top, there is a 'Search Base DN' field containing 'DC=cisco,DC=local' and a 'Search Filter' field. A 'Go' button is located to the right of the 'Search Filter' field. Below these fields is a table with two columns: 'Group Name' and 'Group Type'. The table lists various Microsoft Active Directory groups. Two groups are selected, indicated by checked checkboxes and green background shading: 'cisco.local/Builtin/Helpdesk' (GLOBAL) and 'cisco.local/Builtin/Network Device Admins' (GLOBAL). Other groups listed include 'cisco.local/Builtin/Account Operators', 'cisco.local/Builtin/Administrators', 'cisco.local/Builtin/Backup Operators', 'cisco.local/Builtin/Distributed COM Users', 'cisco.local/Builtin/Guests', 'cisco.local/Builtin/Incoming Forest Trust Builders', 'cisco.local/Builtin/Network Configuration Operators', 'cisco.local/Builtin/Performance Log Users', 'cisco.local/Builtin/Performance Monitor Users', and 'cisco.local/Builtin/Pre-Windows 2000 Compatible Access'. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Group Name	Group Type
<input type="checkbox"/> cisco.local/Builtin/Account Operators	LOCAL
<input type="checkbox"/> cisco.local/Builtin/Administrators	LOCAL
<input type="checkbox"/> cisco.local/Builtin/Backup Operators	LOCAL
<input type="checkbox"/> cisco.local/Builtin/Distributed COM Users	LOCAL
<input type="checkbox"/> cisco.local/Builtin/Guests	LOCAL
<input checked="" type="checkbox"/> cisco.local/Builtin/Helpdesk	GLOBAL
<input type="checkbox"/> cisco.local/Builtin/Incoming Forest Trust Builders	LOCAL
<input type="checkbox"/> cisco.local/Builtin/Network Configuration Operators	LOCAL
<input checked="" type="checkbox"/> cisco.local/Builtin/Network Device Admins	GLOBAL
<input type="checkbox"/> cisco.local/Builtin/Performance Log Users	LOCAL
<input type="checkbox"/> cisco.local/Builtin/Performance Monitor Users	LOCAL
<input type="checkbox"/> cisco.local/Builtin/Pre-Windows 2000 Compatible Access	LOCAL

### Step 6: Click Save Changes.

Users and Identity Stores > External Identity Stores > Active Directory

General | **Directory Groups** | Directory Attributes

Directory groups must be selected on this page to be available as options in group mapping conditions in policy rules. Click "Select" to launch a dialog to select groups from the directory.

Selected Directory Groups:

Group Name
cisco.local/BuiltIn/Network Device Admins
cisco.local/BuiltIn/Helpdesk

Add A Edit V Replace A Deselect **Select**

Group Name

Example for group format :  
cisco.com/Users/Domain Users

Required fields

Save Changes Discard Changes Clear Configuration

## Procedure 7 Create an identity store sequence

An *identity store sequence* allows Cisco Secure ACS to try to authenticate a user against one identity store (such as Microsoft Active Directory) before trying another identity store (such as the internal identity store). This capability allows you to build simple authentication rules regardless of which identity store contains the user.

**Step 1:** Navigate to **Users and Identity Stores > Identity Store Sequences**.

**Step 2:** Click **Create**.

**Step 3:** In the **Name** box, enter **AD then Local DB**.

**Step 4:** Select **Password Based**.

**Step 5:** Use the arrow buttons to move the AD1 and Internal Users identity stores from the **Available** list to the **Selected** list.

**Step 6:** Use the up and down arrow buttons to promote the AD1 identity store so it is the first item in the **Selected** list.

**Step 7:** Click the arrow next to **Advanced Options**.

**Step 8:** Select **Continue to next identity store in the sequence.**

Users and Identity Stores > Identity Store Sequences > Edit: "AD then Local DB"

**General**

Name: AD then Local DB

Description:

**Authentication Method List**

☐ Certificate Based

☒ Password Based

**Authentication and Attribute Retrieval Search List**

A set of identity stores that will be accessed in sequence until first authentication succeeds

Available: Internal Hosts, NAC Profiler

Selected: AD1, Internal Users

**Additional Attribute Retrieval Search List**

An optional set of additional identity stores from which attributes will be retrieved

Available: AD1, Internal Hosts, Internal Users, NAC Profiler

Selected:

**Advanced Options**

If access to the current identity store failed:

☐ Break Sequence

☒ Continue to next identity store in the sequence

For Attribute Retrieval only:

☐ If internal user/host not found or disabled then exit sequence and treat as "User Not Found"

\* = Required fields

Submit Cancel

**Step 9:** Click **Submit**.

## Procedure 8 Create shell profiles

Shell profiles allow you to define the level of access granted to users when they manage a device. The following procedure creates two profiles: one that grants enable-level access upon login (Level 15), and another that allows a user to log in but requires a separate device-level password for enable-level access (Level 1).

Table 2 - Shell profiles

Profile name	Default privilege	Maximum privilege
Level1	1	15
Level15	15	15

**Step 1:** Navigate to **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles**.

**Step 2:** Click **Create**.



**Step 3:** Enter a name and description for the shell profile, and then click the **Common Tasks** tab.

The screenshot shows the 'Create' dialog for a shell profile. The breadcrumb path is 'Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Create'. The 'General' tab is selected. The 'Name' field contains 'Level15' and the 'Description' field contains 'Drop to Enable Prompt at Login'. A legend indicates that orange asterisks denote required fields. At the bottom are 'Submit' and 'Cancel' buttons.

**Step 4:** In the Default Privilege and Maximum Privilege drop-down lists, choose **Static**.

The screenshot shows the 'Common Tasks' tab of the shell profile configuration. Under 'Privilege Level', 'Default Privilege' and 'Maximum Privilege' are both set to 'Static', with a 'Value' of '15' for each. Under 'Shell Attributes', several options are listed with 'Not in Use' selected: 'Access Control List', 'Auto Command', 'No Callback Verify', 'No Escape', 'No Hang Up', 'Timeout', and 'Idle Time'. 'Submit' and 'Cancel' buttons are at the bottom.

**Step 5:** Define the privilege level according to the preceding table by choosing a value from the Value drop-down lists, and then click the **Custom Attributes** tab.

**Step 6:** Under Manually Entered, in the **Attribute** box, enter **waas\_rbac\_groups**. This enables network administrators to log in to Cisco Wide Area Application Services (WAAS) devices as well as Cisco IOS Software devices.

**Step 7:** In the **Requirement** list, choose **Optional**.

**Step 8:** In the **Value** box, enter **Network Admins**, and then click **Add**.

**Step 9:** Click **Submit**.

**Step 10:** Repeat Step 2 through Step 9 for the Level1 shell profile, using the values from Table 2.

Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Edit "Level 15"

General Common Tasks Custom Attributes

Common Tasks Attributes

Attribute	Requirement	Value
Assigned Privilege Level	Mandatory	15
Max Privilege Level	Mandatory	15

Manually Entered

Attribute	Requirement	Value
waas_rbac_groups	Optional	Network Admins

Add A Edit V Replace A Delete

Attribute: waas\_rbac\_groups

Requirement: Optional

Value: Network Admins

Required fields

Submit Cancel

## Procedure 9 Map external groups to internal groups

In order to reduce the number of authorization rules, you can map attributes (such as group membership) in the external identity store to attributes in the internal identity store. Mapping allows the authorization rules to be defined using only the internal attributes, and rules that use the external attributes are not required.

**Step 1:** Navigate to **Access Policies > Access Services > Default Device Admin > Identity**.

**Step 2:** Click **Select**.

**Step 3:** In the Identity Source list, choose **AD then Local DB**, and then click **OK**.

Access Policies > Access Services > Default Device Admin > Identity

☒ Single result selection ☐ Rule based result selection

Identity Source: AD then Local DB **Select**

Advanced Options

**Step 4:** Click **Save Changes**.

**Step 5:** Navigate to **Access Policies > Access Services > Default Device Admin**.

## Step 6: Select Group Mapping.

Access Policies > Access Services > Default Device Admin > Edit: "Default Device Admin"

**General** Allowed Protocols

Name: Default Device Admin

Description: Default Device Administration Access Service

Service Type: Device Administration

Policy Structure

- ☒ Identity
- ☒ Group Mapping
- ☒ Authorization

## Step 7: Click Submit.

## Step 8: Navigate to Access Policies > Access Services > Default Device Admin > Group Mapping.

## Step 9: Select Rule based result selection.

Access Policies > Access Services > Default Device Admin > Group Mapping

☐ Single result selection ☒ Rule based result selection

## Step 10: On the message that appears, click OK.

Windows Internet Explorer

You switched from single to rule-based result selection. Any settings saved in the single mode will be lost when you Submit. Click OK to continue.

OK Cancel

## Step 11: Click Create.

## Step 12: Select Compound Condition.

## Step 13: To the right of Attribute, click Select.

**Conditions**

☒ Compound Condition:

**Condition:**

Dictionary: AD-AD1 Attribute: [Select]

## Step 14: In the Attribute list, select ExternalGroups, and then click OK.

External Identity Store Dictionary Showing 1-2 of 2 50 per page Go

Filter: Match it: Go

Attribute	Type
<input checked="" type="radio"/> ExternalGroups	String Enumeration
<input type="radio"/> IdentityAccessRestricted	Boolean

Page 1 of 1

OK Cancel Help

**Step 15:** Under Value, click **Select**.

Operator: contains any

Value:

Select Deselect Clear

**Step 16:** Choose a Microsoft Active Directory group, and then click **OK**.

String Enum Definition Showing 1-2 of 2 50 per page Go

Filter: Match if: Go

☐ Enum Name

☐ cisco.local/Builtin/Helpdesk

☒ cisco.local/Builtin/Network Device Admins

Page 1 of 1

OK Cancel

**Step 17:** Click **Add V**.

Operator: contains any

Value: cisco.local/Builtin/Network Device Admins

Select Deselect Clear

Current Condition Set:

Add V Edit Replace V

**Step 18:** To the right of Identity Group, click **Select**. This is the identity group to which the Microsoft Active Directory group will map.

Results

Identity Group: Select

**Step 19:** Select **Network Admins**.

Identity Groups

Filter: Match if: Go

Name	Description
All Groups	Identity Group Root
Helpdesk	Users who are allowed to login to a device but not make changes
Network Admins	Users who are allowed to login to a device and make changes

Create Duplicate Edit Delete File Operations Export

OK Cancel Help

Step 20: Click **OK**, and then click **OK** again.

Step 21: Click **Save Changes**.

	Status	Name	Conditions	Results
1	<input checked="" type="checkbox"/>	<a href="#">Rule-1</a>	AD-AD1:ExternalGroups contains any cisco.local/BuiltIn/Network Device Admins	All Groups:Network Admins
**	<input type="checkbox"/>	<a href="#">Default</a>	If no rules defined or no enabled rule matches.	All Groups

Step 22: Repeat Step 11 through Step 21 for the helpdesk group.

## Procedure 10 Create authorization policy rules

Cisco Secure ACS is preconfigured with two access services: Default Device Admin and Default Network Access (for TACACS+ and RADIUS authentications, respectively). This procedure modifies the Default Device Admin authorization policy to allow logins to network devices only for Network Admins and Helpdesk group members. You use the same policy rules to assign appropriate privilege levels.

Table 3 - Access policy rules

Name	In identity group	Shell profile
Helpdesk	All Groups:Helpdesk	Level1
Network Admins	All Groups: Network Admins	Level15

**Step 1:** Navigate to **Access Policies > Access Services > Default Device Admin > Authorization**, and then click **Create**.

**Step 2:** Enter a name for the rule.

**General**  
Name:  Status:

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

**Conditions**

☒ Identity Group:

☐ NDG:Location:

☐ NDG:Device Type:

☐ Time And Date:

**Results**

Shell Profile:

**Step 3:** To the right of Identity Group, click **Select**.

**Step 4:** Select **Network Admins**, and then click **OK**.

**Identity Groups**

Filter:  Match if:

Name	Description
▼ All Groups	Identity Group Root
Helpdesk	Users who are allowed to login to a device but not make changes
<b>Network Admins</b>	<b>Users who are allowed to login to a device and make changes</b>

|

**Step 5:** To the right of Shell Profile, click **Select**.

**General**

Name:  Status:

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

**Conditions**

☒ Identity Group:

☐ NDG:Location:

☐ NDG:Device Type:

☐ Time And Date:

**Results**

Shell Profile:

**Step 6:** Select **Level15** , and then click **OK**.

**Shell Profiles** Showing 1-5 of 5 50 per page

Filter:  Match if:

Name	Description
DenyAccess	
Level1 - 15	Login at Level 1 but allow Enable prompt
<b>Level15</b>	<b>Drop to Enable Prompt at Login</b>
Permit Access	



**Step 7:** Click **OK** again. This saves the rule you just created.

**General**  
Name:  Status:

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

**Conditions**  
☒ Identity Group:     
☐ NDG:Location:   
☐ NDG:Device Type:   
☐ Time And Date:

**Results**  
Shell Profile:

Next, edit the default rule,

**Step 8:** Click **Default**.

**Default** If no rules defined or no enabled rule matches. DenyAccess 0

**Step 9:** To the right of Shell Profile, click **Select**.

**Results**  
Shell Profile:

**Step 10:** Select **DenyAccess**, and then click **OK**.

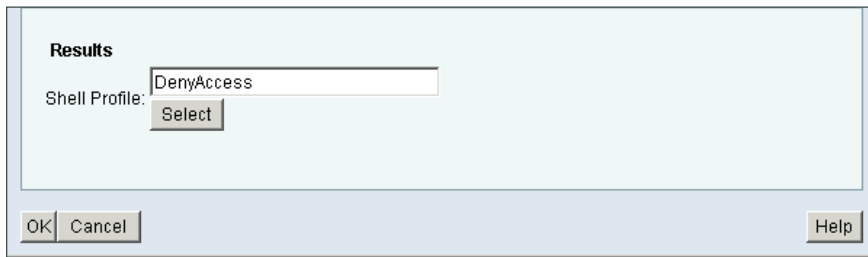
**Shell Profiles** Showing 1-5 of 5 50 per page Go

Filter:  Match if:  Go

Name	Description
<input checked="" type="radio"/> DenyAccess	
<input type="radio"/> Level1	Login Only
<input type="radio"/> Level15	Drop to Enable Prompt at Login
<input type="radio"/> Permit Access	

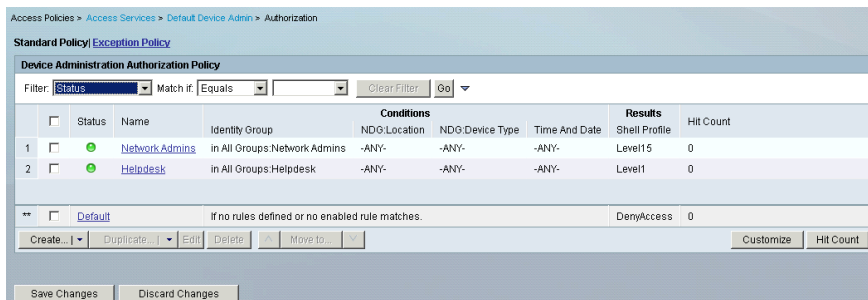
Page 1 of 1

Step 11: Click OK again.



Step 12: Repeat Step 1 through Step 7 for the helpdesk access policy rule.

Step 13: Click Save Changes.



## PROCESS

### Limiting Access to Devices Based on the User Role

1. Create a network device type group
2. Create a network device
3. Exclude users from Security Devices group

This process configures Cisco Secure ACS to allow only network administrators to log in to devices that you want to limit access to (also called security devices).

#### Procedure 1 Create a network device type group

This procedure creates a network device type group to contain all the devices to which you want to limit access.

Step 1: Navigate to **Network Resources > Network Device Groups > Device Type**.

Step 2: Click **Create**.

Network Resources > Network Device Groups > Device Type

**Network Device Groups**

Filter:  Match if:

<input type="checkbox"/> Name	Description
<input type="checkbox"/> <a href="#">All Device Types</a>	All Device Types

Step 3: Enter a name and description for the device type group.

**Device Group - General**

☐ Name:

Description:

☐ Parent:

☐ = Required fields

Step 4: Click **Submit**.

## Procedure 2 Create a network device

This procedure defines a network device entry for each device that you want to limit access to and assigns it to the network device type group.

Step 1: Navigate to **Network Resources > Network Devices and AAA Clients**.

**Step 2:** Click **Create**.

Network Resources > Network Devices and AAA Clients

**Network Devices** Showing 0-0 of 0 50 per page Go

Filter: Match if: Go

<input type="checkbox"/>	Name	IP / Mask	NDG:Location	NDG:Device Type	Description
No data to display					

Create Duplicate Edit Delete File Operations Export Page 1 of 1

**Step 3:** Enter a name and description for the network device entry.

Network Resources > Network Devices and AAA Clients > Create

Name: ASA 5540

Description: Internet Edge Firewall

**Network Device Groups**

Location All Locations Select

Device Type All Device Types Select

**Step 4:** To the right of Device Type, click **Select**.

**Step 5:** Click the radio button next to the device type group that you created in Procedure 1.

**Network Device Groups**

Filter: Match if: Go

Name	Description
<input type="radio"/> All Device Types	All Device Types
<input checked="" type="radio"/> Security Devices	

Create Duplicate Edit Delete File Operations Export

OK Cancel Help

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

**Step 7:** In the **IP** field, enter the IP address.

**Step 8:** Select the **TACACS+** check box.

**Step 9:** In the **Shared Secret** field, enter a shared secret.

Step 10: Click Submit.

The screenshot shows the 'Create' form for a Network Device. The breadcrumb path is 'Network Resources > Network Devices and AAA Clients > Create'. The form includes fields for 'Name' (ASA 5540) and 'Description' (Internet Edge Firewall). Under 'Network Device Groups', there are dropdowns for 'Location' (All Locations) and 'Device Type' (All Device Types: Security Devices). The 'IP Address' section has radio buttons for 'Single IP Address' (selected) and 'IP Range(s)', with an 'IP' field containing '10.4.24.30'. The 'Authentication Options' section has a checked 'TACACS+' checkbox, a 'Shared Secret' field (SecretKey), and unchecked checkboxes for 'Single Connect Device', 'Legacy TACACS+ Single Connect Support', and 'TACACS+ Draft Compliant Single Connect Support'. There is also an unchecked 'RADIUS' checkbox. A legend indicates that an orange asterisk denotes required fields. At the bottom are 'Submit' and 'Cancel' buttons.

Step 11: Repeat this procedure for every security device that you want to limit access to.

### Procedure 3 Exclude users from Security Devices group

This procedure edits the existing authorization rule to prohibit Helpdesk users from logging in to security devices.

Step 1: Navigate to **Access Policies > Access Services > Default Device Admin > Authorization**.

Step 2: In the list of rules, select the **Helpdesk** check box.

The screenshot shows the 'Authorization' page under 'Access Policies > Access Services > Default Device Admin'. It features a 'Standard Policy' and an 'Exception Policy' link. Below is a 'Device Administration Authorization Policy' section with a filter bar (Status, Match if, Equals, Clear Filter, Go). A table lists two rules:

	Status	Name	Identity Group	Conditions	NDG:Location	NDG:Device Type	Time And Date	Re
1	<input type="checkbox"/>	Network Admins	in All Groups:Network Admins	-ANY-	-ANY-	-ANY-	-ANY-	Levi
2	<input checked="" type="checkbox"/>	Helpdesk	in All Groups:Helpdesk	-ANY-	-ANY-	-ANY-	-ANY-	Levi

Below the table is a 'Default' rule with a status checkbox and a description: 'If no rules defined or no enabled rule matches.' At the bottom are buttons for 'Create...', 'Duplicate...', 'Edit', 'Delete', 'Move to...', 'Customize', 'Hit Count', 'Save Changes', and 'Discard Changes'.

Step 3: Click Edit.

#### Step 4: Select NDG:Device Type.

**General**  
Name: Helpdesk Status: Enabled

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

**Conditions**  
☒ Identity Group: in All Groups: Helpdesk   
☐ NDG:Location: -ANY-  
☒ NDG:Device Type: not in   
☐ Time And Date: -ANY-

**Results**  
Shell Profile: Level1

OK Cancel Help

Step 5: From the drop-down list, choose **Not In**.

Step 6: To the right of NDG:Device Type, click **Select**.

Step 7: Select **Security Devices**, and then click **OK**.

**Network Device Groups**  
Filter: Match if:

Name	Description
All Device Types	All Device Types
Security Devices	

Create Duplicate Edit Delete File Operations Export

OK Cancel Help

Step 8: Click **OK** again.

**General**  
Name: Helpdesk Status: Enabled

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

**Conditions**  
☒ Identity Group: in All Groups: Helpdesk   
☐ NDG:Location: -ANY-  
☒ NDG:Device Type: not in All Device Types: Security Devices   
☐ Time And Date: -ANY-

**Results**  
Shell Profile: Level1

OK Cancel Help

## Step 9: Click Save Changes.

Access Policies > Access Services > Default Device Admin > Authorization

Standard Policy | [Exception Policy](#)

**Device Administration Authorization Policy**

Filter:  Match if:

	<input type="checkbox"/>	Status	Name	Identity Group	NDG:Location	NDG:Device Type
1	<input type="checkbox"/>	●	<a href="#">Network Admins</a>	in All Groups:Network Admins	-ANY-	-ANY-
2	<input type="checkbox"/>	●	<a href="#">Helpdesk</a>	in All Groups:Helpdesk	-ANY-	not in All Device Types:Security Devices

Conditions

\*\* ☐ [Default](#) If no rules defined or no enabled rule matches.



# Appendix A: Product List

---

## Access Control

Functional Area	Product Description	Part Numbers	Software
Authentication Services	ACS 5.3 VMware Software and Base License	CSACS-5.3-VM-K9	5.3

## Feedback

Please use the [feedback form](#) to send comments and suggestions about this guide.



**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](http://www.cisco.com/go/offices).

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2013 Cisco Systems, Inc. All rights reserved.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)