Device Management Using ACS

Technology Design Guide

August 2014 Series

Table of Contents

Preface

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

CVDs include two guide types that provide tested design 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 existing CVDs but also include product features and functionality across Cisco products and sometimes 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.

CVD Foundation Series

This CVD Foundation guide is a part of the *August 2014 Series*. As Cisco develops a CVD Foundation series, the guides themselves are tested together, in the same network lab. This approach assures that the guides in a series are fully compatible with one another. Each series describes a lab-validated, complete system.

The CVD Foundation series incorporates wired and wireless LAN, WAN, data center, security, and network management technologies. Using the CVD Foundation simplifies system integration, allowing you to select solutions that solve an organization's problems—without worrying about the technical complexity.

To ensure the compatibility of designs in the CVD Foundation, you should use guides that belong to the same release. For the most recent CVD Foundation guides, please visit the CVD Foundation web site.

Comments and Questions

If you would like to comment on a guide or ask questions, please use the feedback form.

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**—As the number of network devices increases and as network administrators change over time, deploying a centralized access and identity policy enforcement point lowers the administrative burden of ensuring the reliability of a network.

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 to provide 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 number of different IP data types is constantly increasing. So is the sheer volume of data. This growth requires comparable scaling of the supporting network infrastructure—routers, switches, firewalls, wireless LAN controllers, and so on. Enterprise network infrastructures can be composed of 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 who can perform specified commands upon specified 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 Active Directory (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 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

How to Read Commands

This guide uses the following conventions for commands that you enter at the command-line interface (CLI).

Commands to enter at a CLI prompt:

```
configure terminal
```

Commands that specify a value for a variable:

```
ntp server 10.10.48.17
```

Commands with variables that you must define:

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

Commands at a CLI or script prompt:

```
Router# enable
```

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

```
police rate 10000 pps burst 10000
packets conform-action
```

Noteworthy parts of system output (or of device configuration files) are highlighted:

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

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. It assumes you have already loaded the Cisco Secure ACS software on a server. The procedures provide instructions for setting up two policies that apply different privileges to helpdesk users and network administrators. The procedures also 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 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 in order 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 secondary nameserver? Y/N [N]: N
Enter NTP server[time.nist.gov]: 10.4.48.17
Add another NTP server? Y/N [N]: N
Enter system timezone[UTC]: US/Pacific
Enable SSH service? Y/N [N]: Y
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...
Generating configuration...
Installing Applications...
Installing ACS ...
Unbundling Application Package...
Initiating Application Install...
Rebooting...
```

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

Step 2: Verify the Cisco Secure ACS installation.

```
acs/admin# show application version acs
Cisco ACS VERSION INFORMATION
-----------------------------
Version : 5.5.0.46
Internal Build ID : B.723
acs/admin# show application status acs
ACS role: PRIMARY
Process ‘database’                    running
Process ‘management’                  running
Process ‘runtime’                     running
Process ‘ntpd’                        running
Process ‘view-database’               running
Process ‘view-jobmanager’             running
Process ‘view-alertmanager’           running
Process ‘view-collector’              running
Process ‘view-logprocessor’           running
```

Step 3: Using a web browser, 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 1. Enter the default credentials: **acsadmin/default**. You are prompted to change the password.

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

Tech Tip

After you install the software, check the release notes and apply any recommended patches, following the release note guidance. Applying patches may be done from the CLI and can affect ACS service.

Procedure 3 Enable the default network device

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

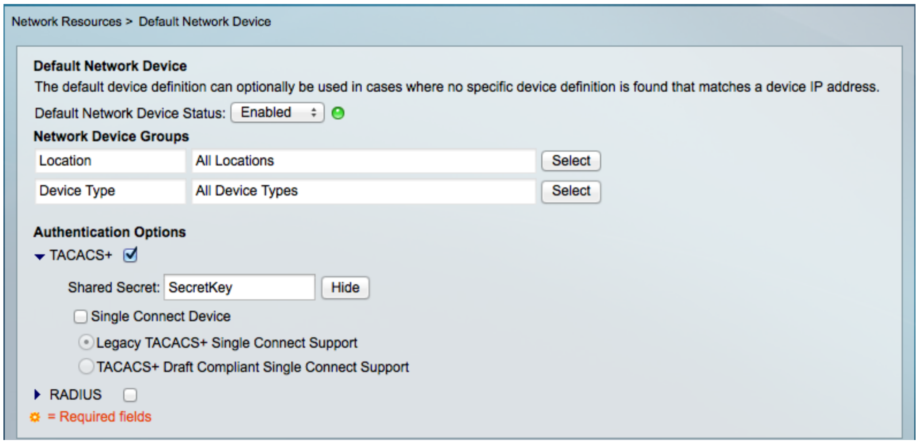
Step 2: In the **Default Network Device Status** list, choose **Enabled**.

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**.



Network Resources > Default Network Device

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	All Locations	Select
Device Type	All Device Types	Select

Authentication Options

TACACS+ ☑

Shared Secret: SecretKey Hide

□ 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

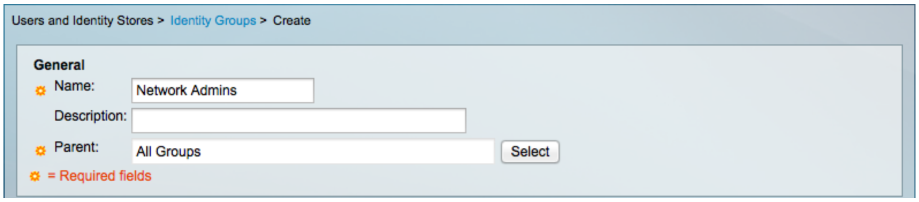
Group name	Description
Helpdesk	Users who are allowed to log in to a device but not make changes
Network Admins	Users who are allowed to log in to a device and make changes

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**.



Users and Identity Stores > Identity Groups > Create

General

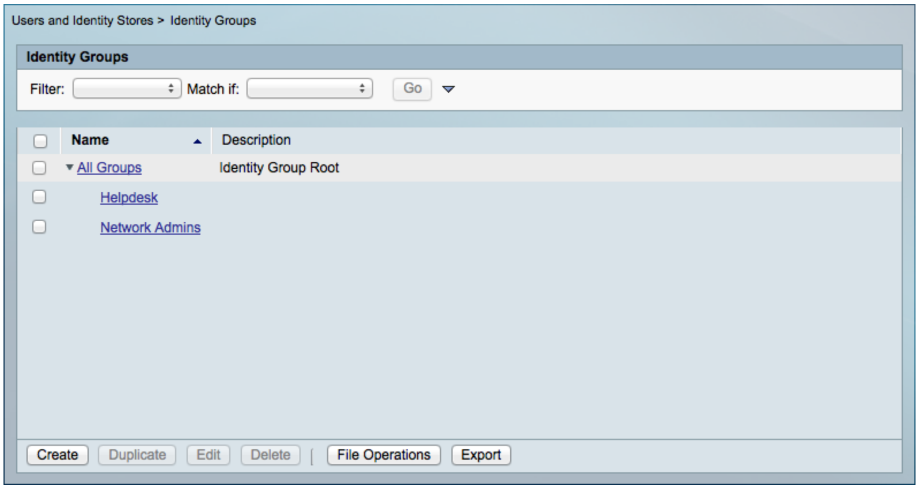
Name: Network Admins

Description:

Parent: All Groups Select

= Required fields

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



□	Name	Description
□	All Groups	Identity Group Root
□	Helpdesk	
□	Network Admins	

Caution

When you use centralized authentication for network infrastructure device management, enable an additional method to authenticate locally to the devices. The local authentication method is used during situations where management connectivity between the device and the ACS server is lost.

For example, with Catalyst switches, you configure a local username and password, and then you use the following AAA command:

```
aaa authentication login default group TACACS-SERVERS local
```

This command first references a user-defined **TACACS-SERVERS** group configuration as the default choice for authentication. When the switch cannot connect to the servers in the **TACACS-SERVERS** group, then the switch authenticates the user against the locally stored username and password instead.

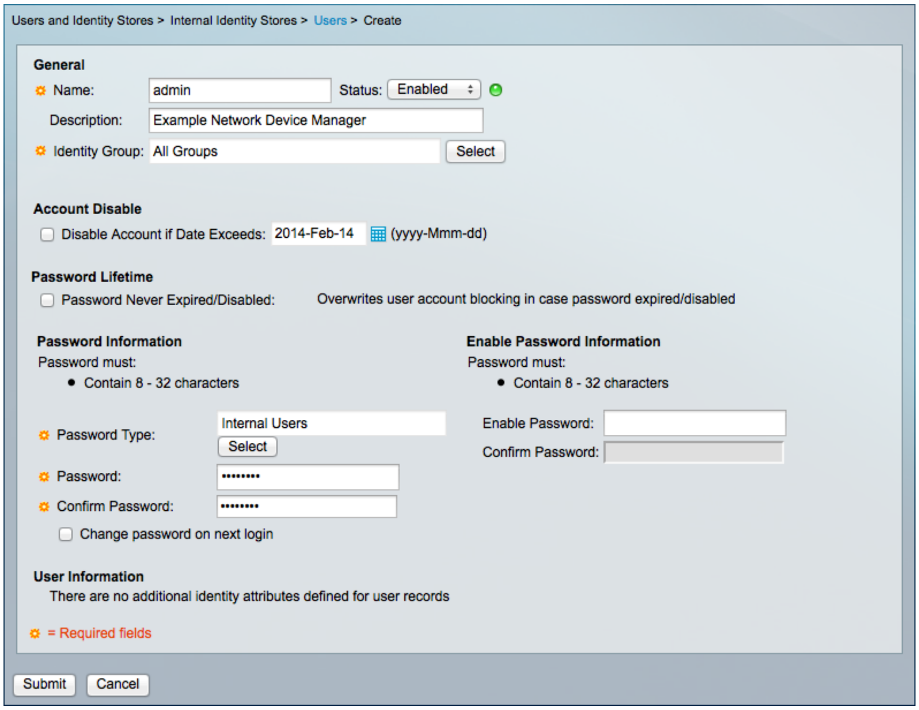
Procedure 5 Create internal identity store users

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.



Users and Identity Stores > Internal Identity Stores > Users > Create

General

Name: admin Status: Enabled

Description: Example Network Device Manager

Identity Group: All Groups Select

Account Disable

□ Disable Account if Date Exceeds: 2014-Feb-14 (yyyy-Mmm-dd)

Password Lifetime

□ Password Never Expired/Disabled: Overwrites user account blocking in case password expired/disabled

Password Information

Password must:

- Contain 8 - 32 characters

Password Type: Internal Users Select

Password: ••••••••

Confirm Password: ••••••••

□ Change password on next login

Enable Password Information

Password must:

- Contain 8 - 32 characters

Enable Password:

Confirm Password:

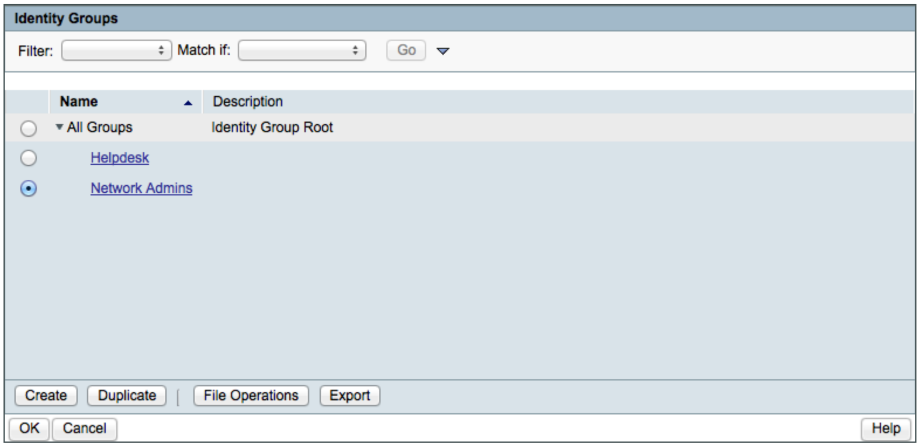
User Information

There are no additional identity attributes defined for user records

= Required fields

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.



Identity Groups

Filter: Match if: Go

	Name	Description
○	All Groups	Identity Group Root
○	Helpdesk	
●	Network Admins	

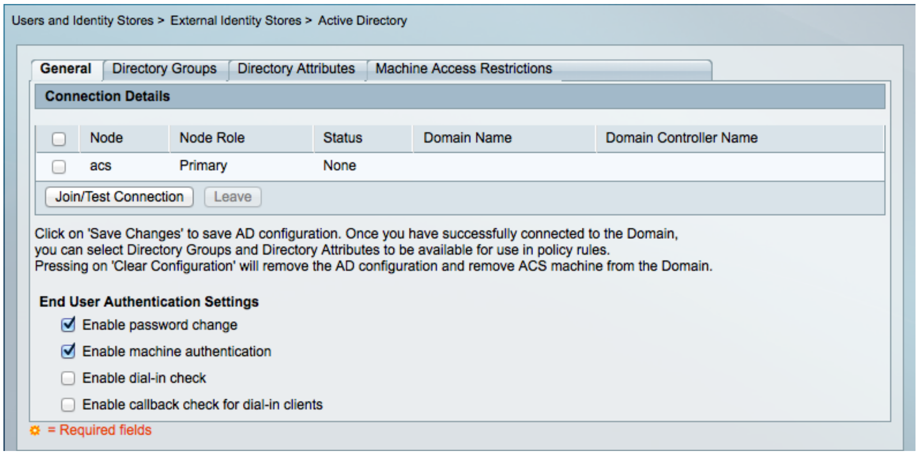
Step 6: Click **OK**, and then click **Submit**.

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**, and then click **Join/Test Connection**.


Users and Identity Stores > External Identity Stores > Active Directory
General
Directory Groups
Directory Attributes
Machine Access Restrictions

Connection Details

□	Node	Node Role	Status	Domain Name	Domain Controller Name
□	acs	Primary	None		

Join/Test Connection
Leave

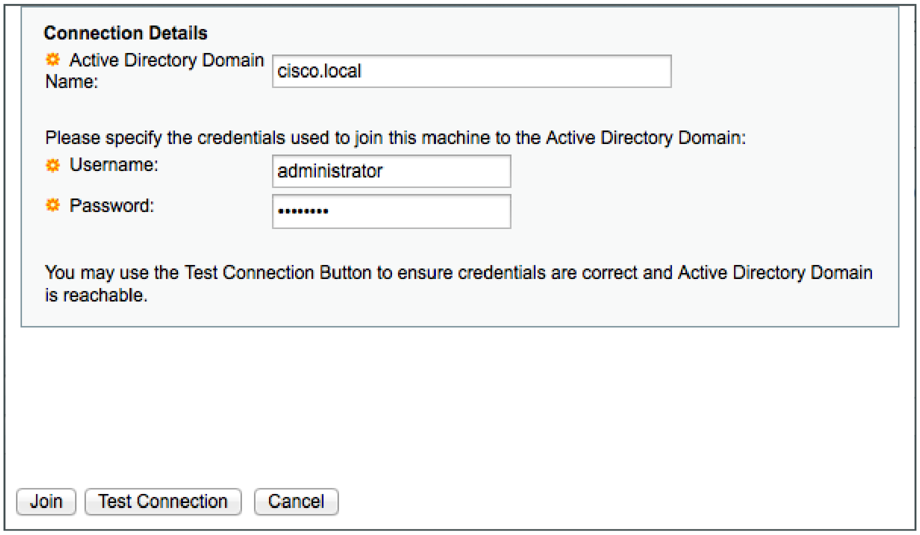
Click on 'Save Changes' to save AD configuration. Once you have successfully connected to the Domain, you can select Directory Groups and Directory Attributes to be available for use in policy rules.
Pressing on 'Clear Configuration' will remove the AD configuration and remove ACS machine from the Domain.

End User Authentication Settings

- ☑ Enable password change
- ☑ Enable machine authentication
- □ Enable dial-in check
- □ Enable callback check for dial-in clients

✱ = Required fields

Step 2: Enter the Microsoft Active Directory domain name and user credentials, and then click **Join**.



Connection Details

✱ Active Directory Domain Name: cisco.local

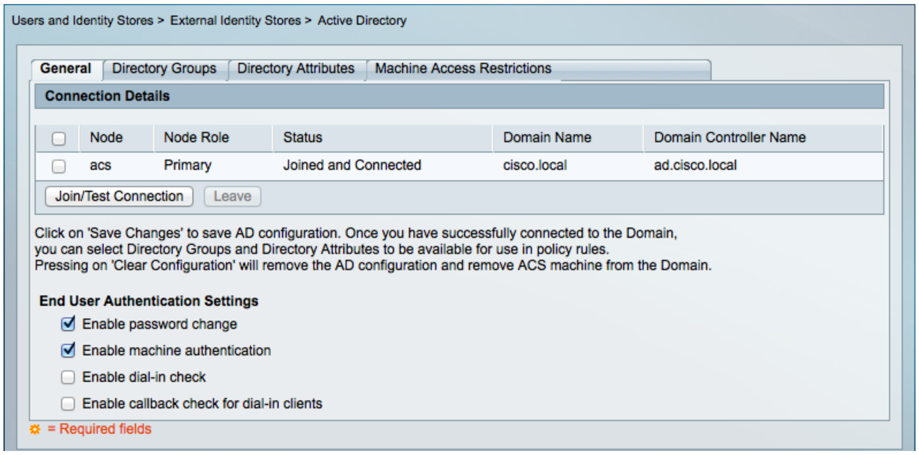
Please specify the credentials used to join this machine to the Active Directory Domain:

✱ Username: administrator

✱ Password: ••••••••

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

The status changes to Joined and Connected.



Users and Identity Stores > External Identity Stores > Active Directory

Connection Details

☐	Node	Node Role	Status	Domain Name	Domain Controller Name
☐	acs	Primary	Joined and Connected	cisco.local	ad.cisco.local

Click on 'Save Changes' to save AD configuration. Once you have successfully connected to the Domain, you can select Directory Groups and Directory Attributes to be available for use in policy rules.
Pressing on 'Clear Configuration' will remove the AD configuration and remove ACS machine from the Domain.

End User Authentication Settings

☑ Enable password change

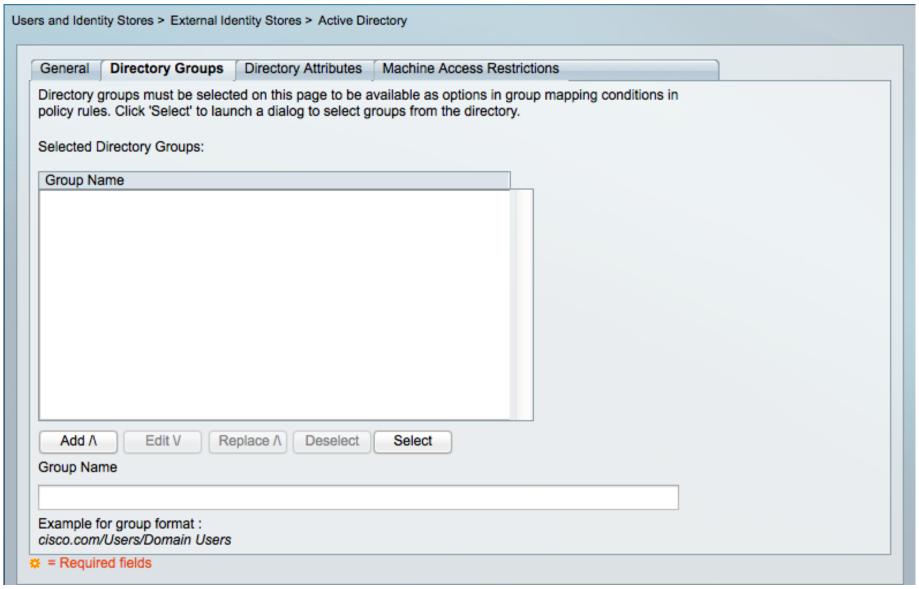
☑ Enable machine authentication

☐ Enable dial-in check

☐ Enable callback check for dial-in clients

✱ = Required fields

Step 3: Click the **Directory Groups** tab, and then click **Select**.



Users and Identity Stores > External Identity Stores > Active Directory

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.

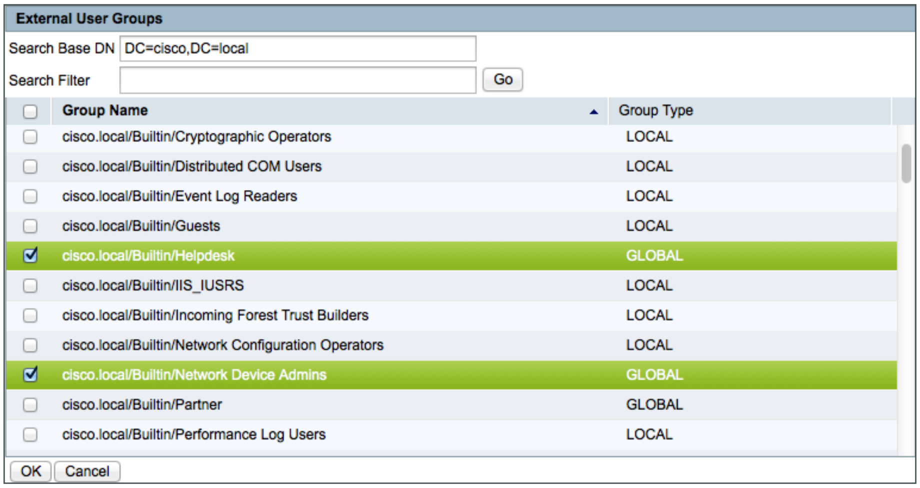
Selected Directory Groups:

Group Name

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

✱ = Required fields

Step 4: 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**.



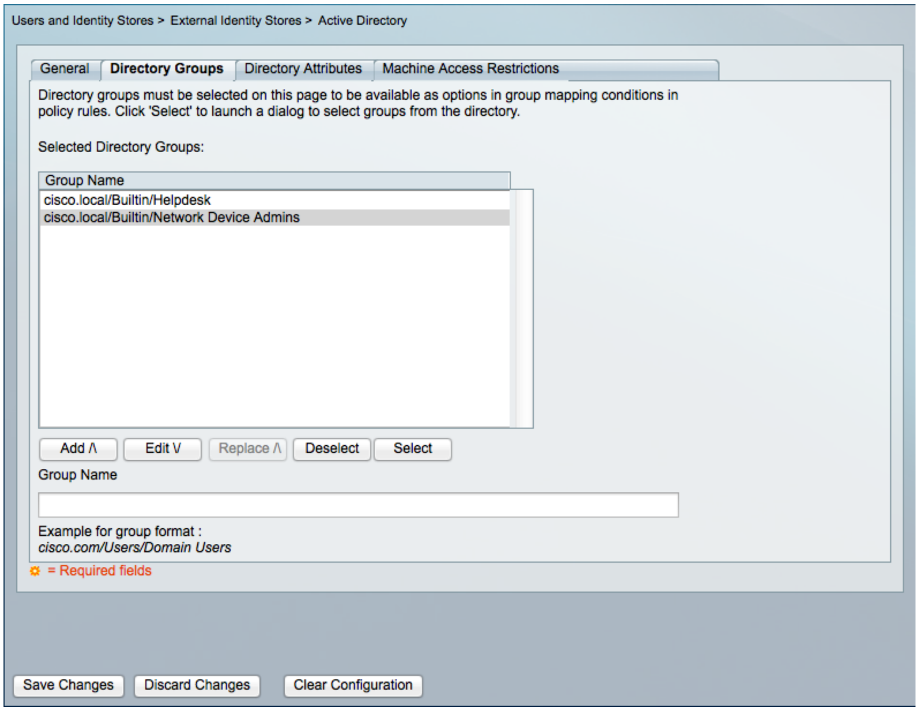
External User Groups

Search Base DN: DC=cisco,DC=local

Search Filter:

□	Group Name	Group Type
□	cisco.local/Builtin/Cryptographic Operators	LOCAL
□	cisco.local/Builtin/Distributed COM Users	LOCAL
□	cisco.local/Builtin/Event Log Readers	LOCAL
□	cisco.local/Builtin/Guests	LOCAL
☑	cisco.local/Builtin/Helpdesk	GLOBAL
□	cisco.local/Builtin/IIS_IUSRS	LOCAL
□	cisco.local/Builtin/Incoming Forest Trust Builders	LOCAL
□	cisco.local/Builtin/Network Configuration Operators	LOCAL
☑	cisco.local/Builtin/Network Device Admins	GLOBAL
□	cisco.local/Builtin/Partner	GLOBAL
□	cisco.local/Builtin/Performance Log Users	LOCAL

Step 5: Click **Save Changes**.



Users and Identity Stores > External Identity Stores > Active Directory

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/Helpdesk
cisco.local/Builtin/Network Device Admins

Group Name

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

✲ = Required fields

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**.

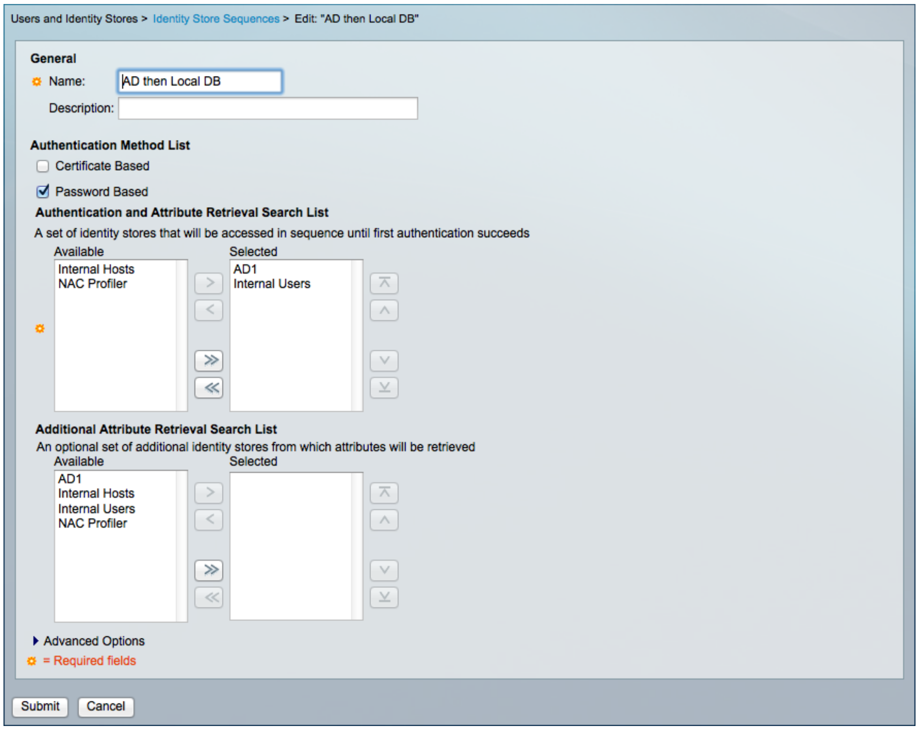
Step 4: Select **Password Based**.

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	Selected
Internal Hosts NAC Profiler	AD1 Internal Users

Additional Attribute Retrieval Search List

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

Available	Selected
AD1 Internal Hosts Internal Users NAC Profiler	

Advanced Options

= Required fields

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 (Level15), and another that allows a user to log in but requires a separate device-level password for enable-level access (Level1).

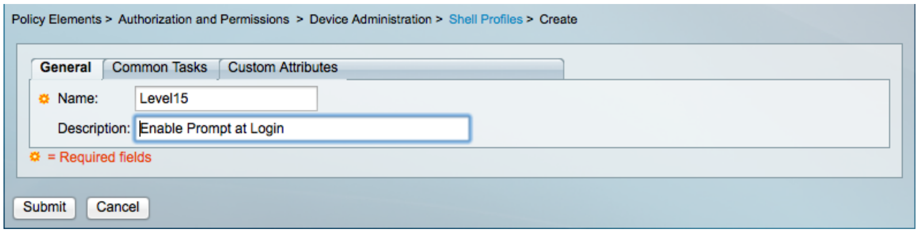
Table 2 - Shell profiles

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**.

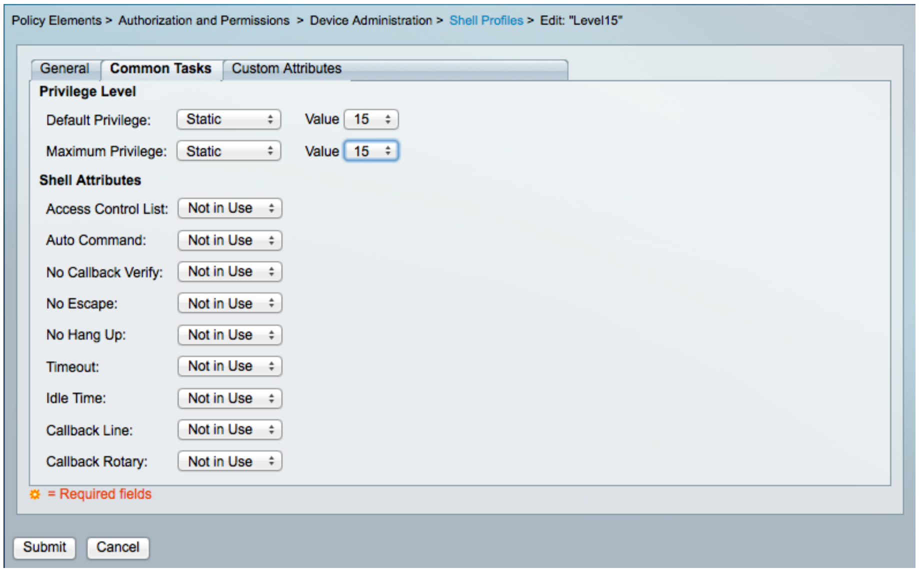
Step 3: Enter a name and description for the shell profile, and then click the **Common Tasks** tab.


Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Create
General
Common Tasks
Custom Attributes
= Required fields
Submit
Cancel

Name: Level15
Description: Enable Prompt at Login

Step 4: Select the Shell Profile just created (Example: Level15), and then click the **Common Tasks** tab.

Step 5: In the **Default Privilege** and **Maximum Privilege** drop-down lists, choose **Static**.


Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Edit: "Level15"
General
Common Tasks
Custom Attributes
= Required fields
Submit
Cancel

Privilege Level
Default Privilege: Static Value 15
Maximum Privilege: Static Value 15

Shell Attributes
Access Control List: Not in Use
Auto Command: Not in Use
No Callback Verify: Not in Use
No Escape: Not in Use
No Hang Up: Not in Use
Timeout: Not in Use
Idle Time: Not in Use
Callback Line: Not in Use
Callback Rotary: Not in Use

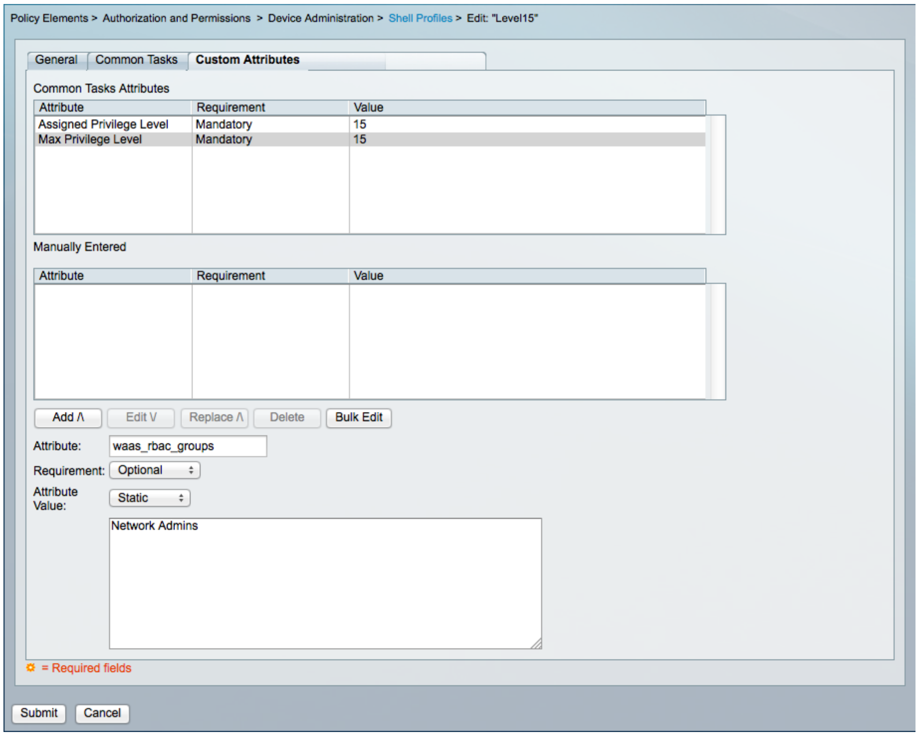
Step 6: Define the privilege level according to the preceding table by choosing a value from both of the **Value** drop-down lists, and then click the **Custom Attributes** tab.

Step 7: 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 8: In the **Requirement** list, choose **Optional**.

Step 9: In the **Attribute Value** list, choose **Static**.

Step 10: In the text box for **Attribute Value**, enter **Network Admins**, and then click **Add /\**.



Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Edit: "Level15"

Common Tasks Attributes

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

Manually Entered

Attribute	Requirement	Value

Attribute: waas_rbac_groups

Requirement: Optional

Attribute Value: Static

Network Admins

Step 11: Click **Submit**.

Step 12: Repeat Step 2 through Step 11 for the Level1 shell profile, using the values from Table 2.

Tech Tip

If you have Cisco AireOS-based wireless LAN controllers, you will need to create a specific shell profile for the WLC in order to allow authorization for this additional shell type. For more information, see the Campus Wireless LAN Technology Design Guide.

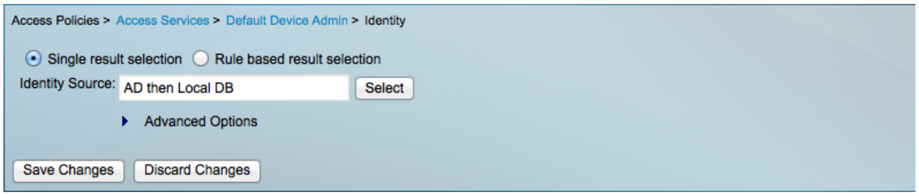
Procedure 9 Map external groups to internal groups

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 Store** 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

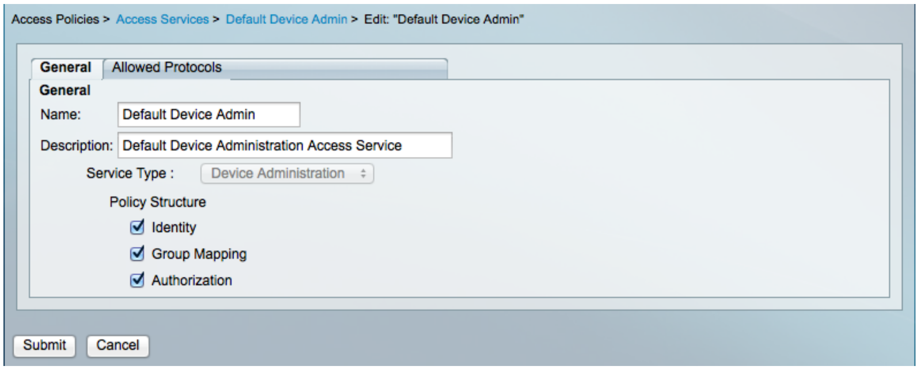
Identity Source: AD then Local DB

The Identity Source field is populated with the selection.

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

Name: Default Device Admin

Description: Default Device Administration Access Service

Service Type : Device Administration

Policy Structure

☑ Identity

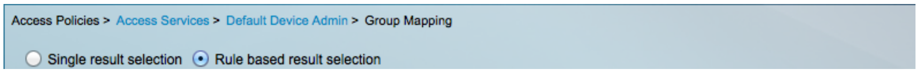
☑ Group Mapping

☑ Authorization

Step 7: Click **Submit**.

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

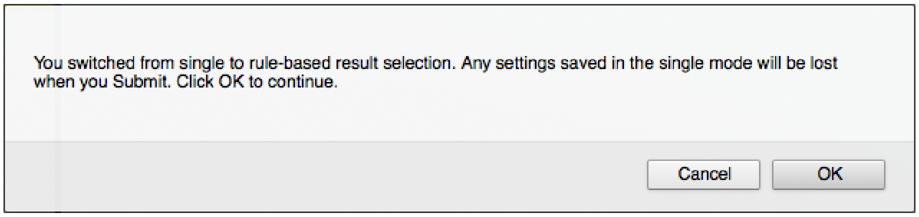
Step 9: Select **Rule based result selection**.



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**.

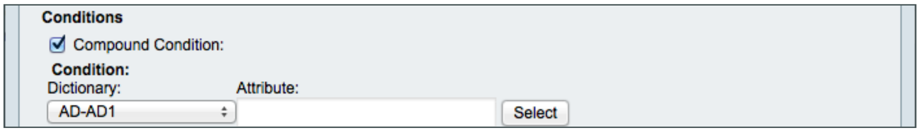


You switched from single to rule-based result selection. Any settings saved in the single mode will be lost when you Submit. Click OK to continue.

Step 11: Click **Create**.

Step 12: Select **Compound Condition**.

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



Conditions

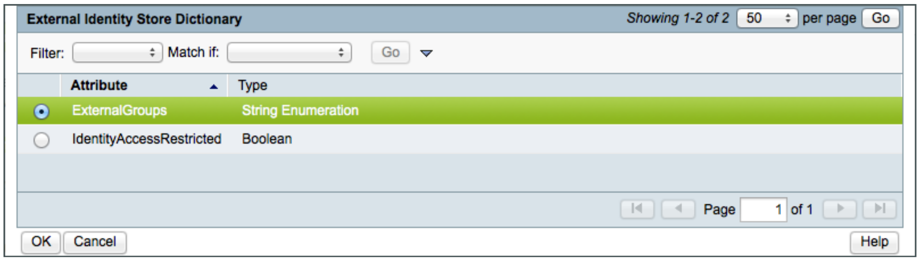
☑ Compound Condition:

Condition:

Dictionary: AD-AD1

Attribute:

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



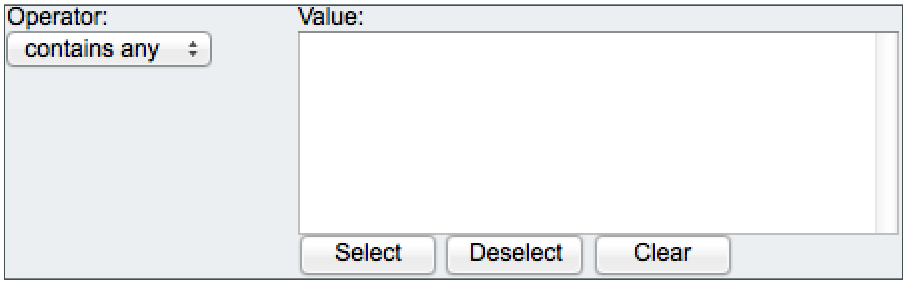
External Identity Store Dictionary — *Showing 1-2 of 2* 50 per page

Filter: Match if:

	Attribute	Type
●	ExternalGroups	String Enumeration
○	IdentityAccessRestricted	Boolean

Page 1 of 1

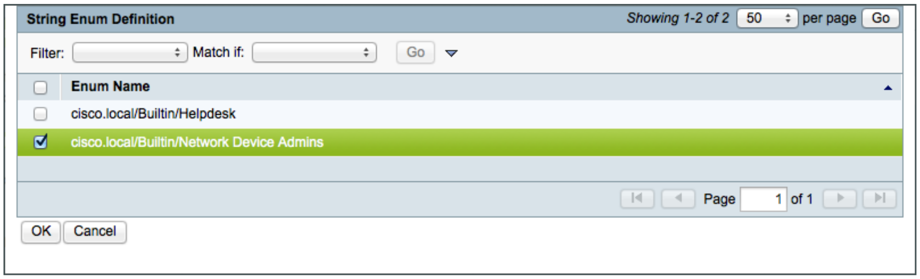
Step 15: Under Value, click **Select**.



Operator: contains any

Value:

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



String Enum Definition

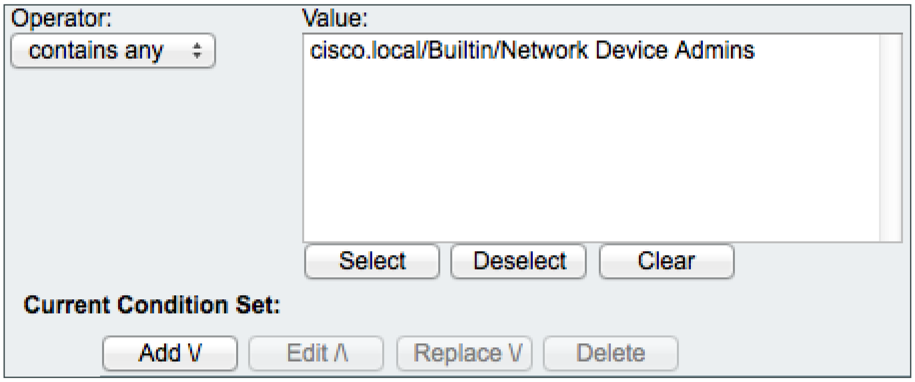
Showing 1-2 of 2 | 50 per page

Filter: Match if:

	Enum Name
☐	cisco.local/Builtin/Helpdesk
☑	cisco.local/Builtin/Network Device Admins

Page 1 of 1

Step 17: Click **Add V**.

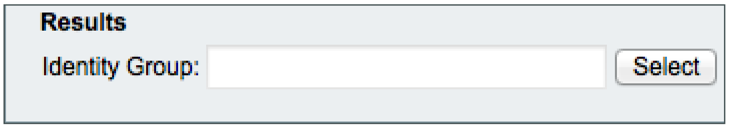


Operator: contains any

Value: cisco.local/Builtin/Network Device Admins

Current Condition Set:

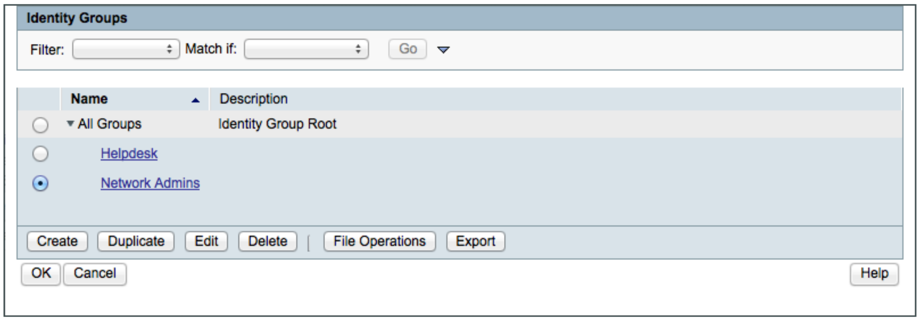
Step 18: To the right of Identity Group, click **Select**. This is the identity group to which the Microsoft Active Directory group will map.



Results

Identity Group:

Step 19: Select **Network Admins**.

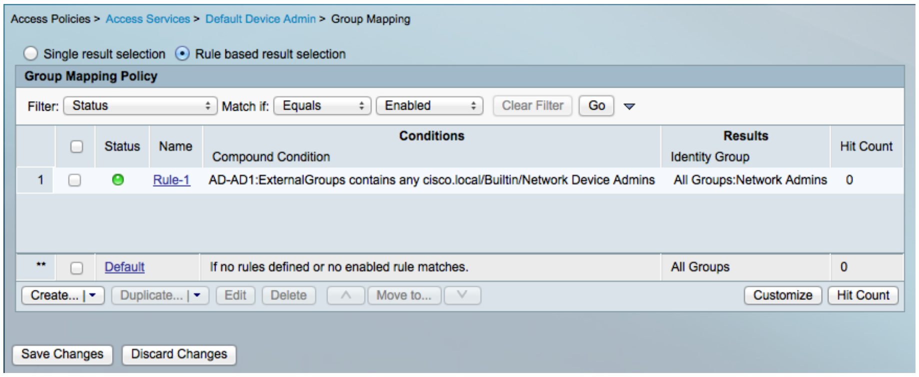


Identity Groups

Filter: Match if:

	Name	Description
○	▾ All Groups	Identity Group Root
○	Helpdesk	
●	Network Admins	

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



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

○ Single result selection ● Rule based result selection

Group Mapping Policy

Filter: Status Match if: Equals Enabled

		Status	Name	Conditions Compound Condition	Results Identity Group	Hit Count
1	□	●	Rule-1	AD-AD1:ExternalGroups contains any cisco.local/Builtin/Network Device Admins	All Groups:Network Admins	0
**	□		Default	If no rules defined or no enabled rule matches.	All Groups	0

Step 21: Repeat Step 11 through Step 20 for the Helpdesk group.

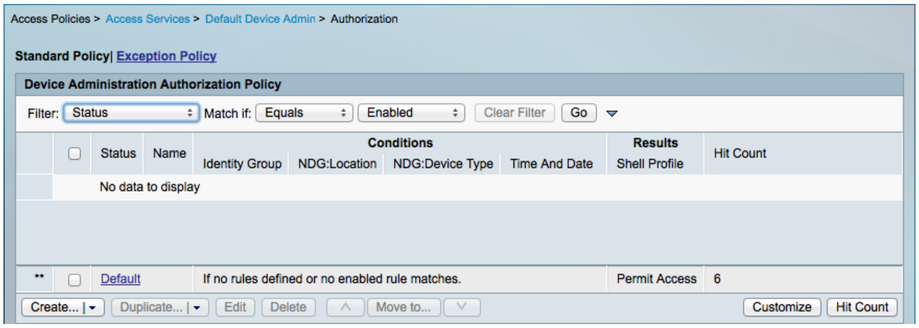
Procedure 10 Create authorization policy rules

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**.



Access Policies > Access Services > Default Device Admin > Authorization

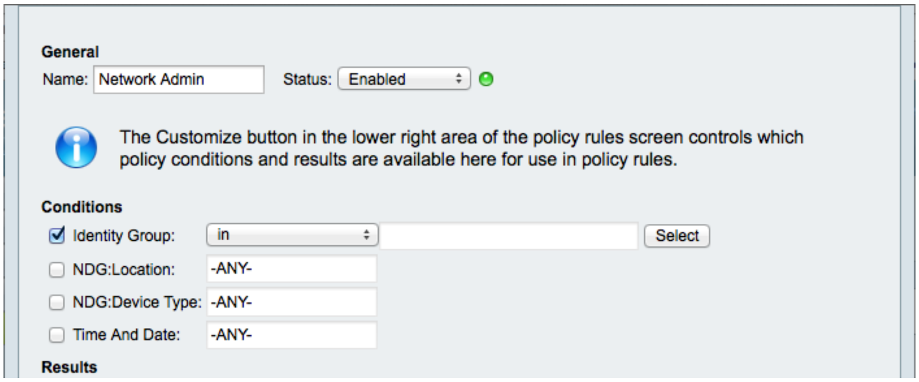
Standard Policy| Exception Policy

Device Administration Authorization Policy

Filter: Status Match if: Equals Enabled

		Status	Name	Conditions Identity Group	NDG:Location	NDG:Device Type	Time And Date	Results Shell Profile	Hit Count
		No data to display							
**	□		Default	If no rules defined or no enabled rule matches.				Permit Access	6

Step 2: Enter a name for the rule, and then select **Identity Group**.



General

Name: Network Admin 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 [Select]

□ NDG:Location: -ANY-

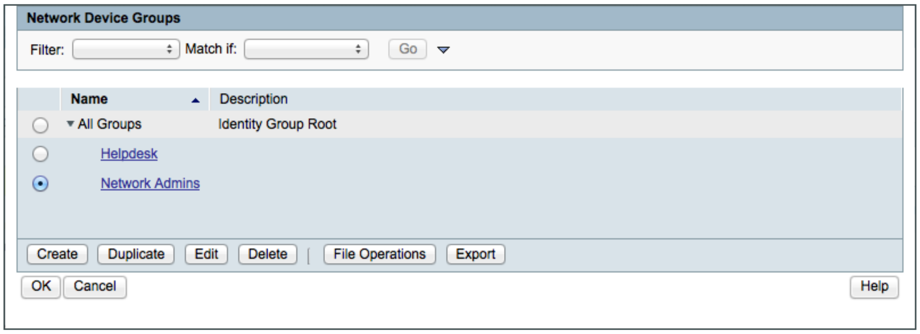
□ NDG:Device Type: -ANY-

□ Time And Date: -ANY-

Results

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

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

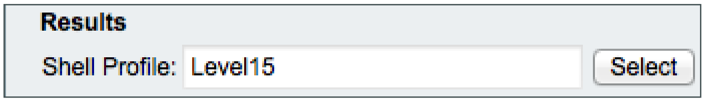


Network Device Groups

Filter: Match if: Go

	Name	Description
○	▾ All Groups	Identity Group Root
○	Helpdesk	
●	Network Admins	

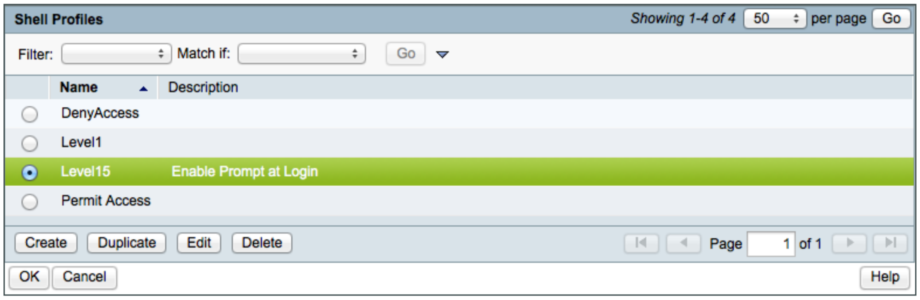
Step 5: To the right of Shell Profile, click **Select**.



Results

Shell Profile: Level15 [Select]

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



Shell Profiles *Showing 1-4 of 4* 50 per page Go

Filter: Match if: Go

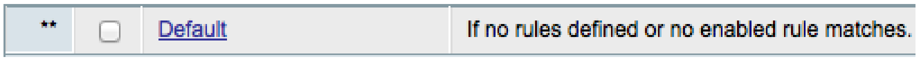
	Name	Description
○	DenyAccess	
○	Level1	
●	Level15	Enable Prompt at Login
○	Permit Access	

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

Step 8: Repeat Step 1 through Step 7 for the helpdesk access policy rule, using the values in Table 3.

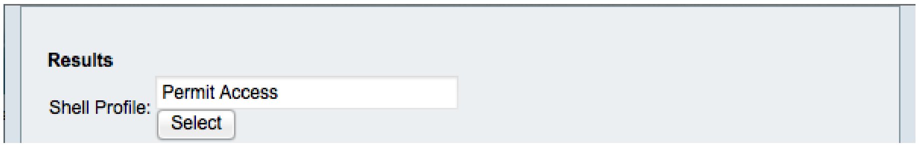
Next, edit the default rule.

Step 9: Click **Default** link.



**	□	Default	If no rules defined or no enabled rule matches.

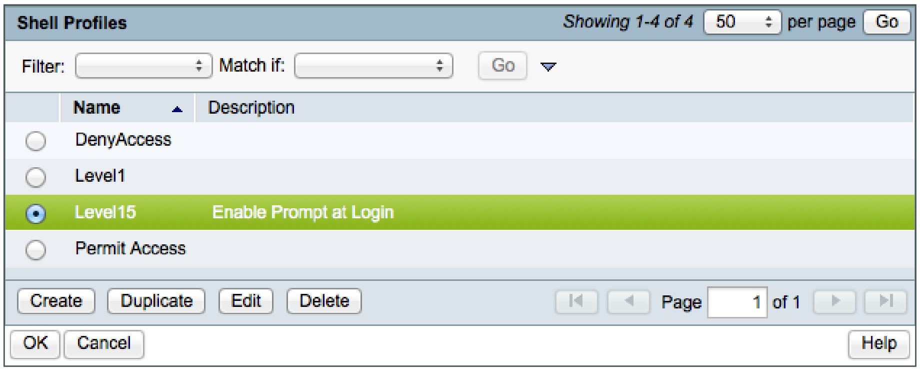
Step 10: To the right of Shell Profile, click **Select**.



Results

Shell Profile: Permit Access

Step 11: Select **DenyAccess**, and then click **OK**.

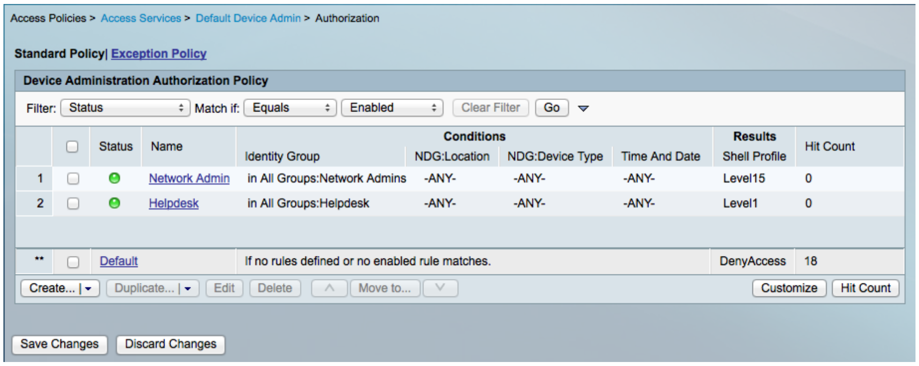


Shell Profiles — Showing 1-4 of 4 — 50 per page

	Name	Description
○	DenyAccess	
○	Level1	
●	Level15	Enable Prompt at Login
○	Permit Access	

Step 12: Click **OK** again.

Step 13: Click **Save Changes**.



Access Policies > Access Services > Default Device Admin > Authorization

Standard Policy| Exception Policy

Device Administration Authorization Policy

Filter: Status Match if: Equals Enabled

				Conditions				Results	
	□	Status	Name	Identity Group	NDG:Location	NDG:Device Type	Time And Date	Shell Profile	Hit Count
1	□	●	Network Admin	in All Groups:Network Admins	-ANY-	-ANY-	-ANY-	Level15	0
2	□	●	Helpdesk	in All Groups:Helpdesk	-ANY-	-ANY-	-ANY-	Level1	0
**	□		Default	If no rules defined or no enabled rule matches.				DenyAccess	18

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

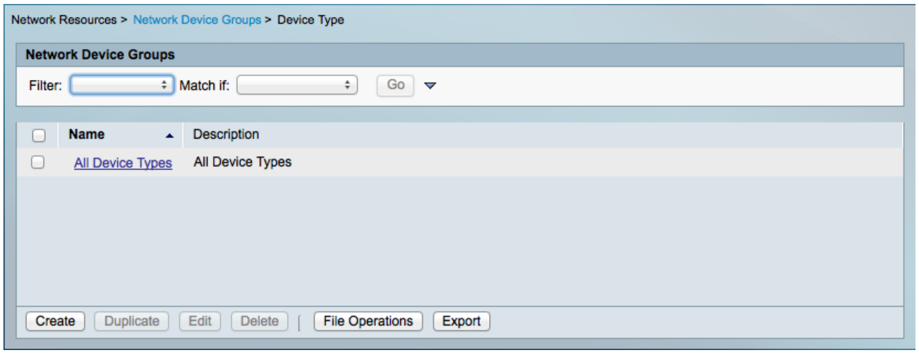
This process configures Cisco Secure ACS to allow only network administrators to log in to devices that you want to limit access to (also called security devices).

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.

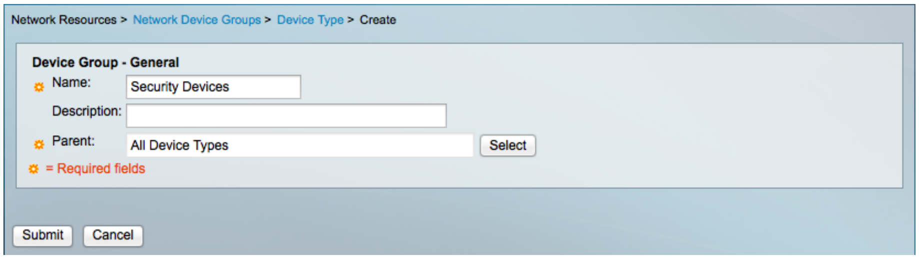
Step 1: Navigate to **Network Resources > Network Device Groups > Device Type**.

Step 2: Click **Create**.



Name	Description
All Device Types	All Device Types

Step 3: Enter a name and description for the device type group, and then click **Submit**.


Network Resources > Network Device Groups > Device Type > Create
Device Group - General
Select
= Required fields
Submit
Cancel

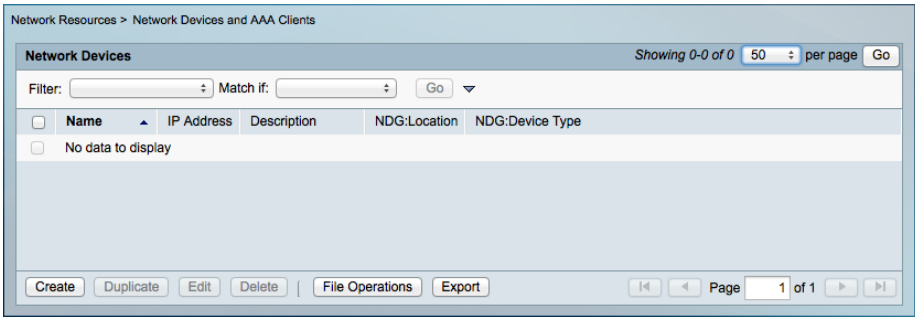
Name: Security Devices
Description:
Parent: All Device Types

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.

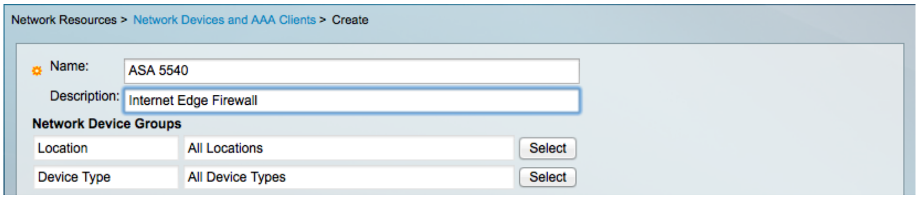
Step 1: Navigate to **Network Resources > Network Devices and AAA Clients**.

Step 2: Click **Create**.



□	Name	IP Address	Description	NDG:Location	NDG:Device Type
□	No data to display				

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


Network Resources > Network Devices and AAA Clients > Create
Select
Select

Name: ASA 5540

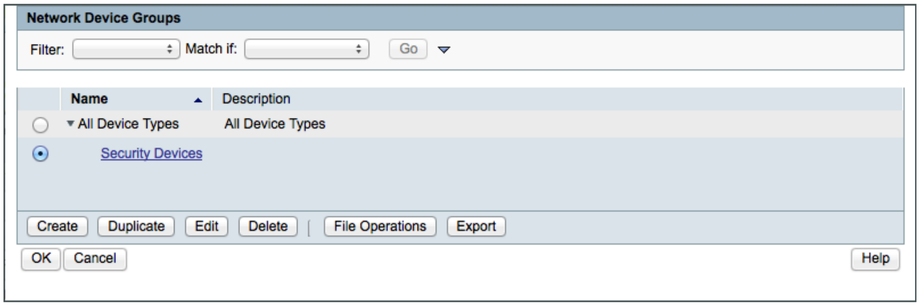
Description: Internet Edge Firewall

Network Device Groups

Location	All Locations
Device Type	All Device Types

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

Step 5: Click the option button next to the device type group that you created in Procedure 1, “Create a network device type group,” and then click **OK**.

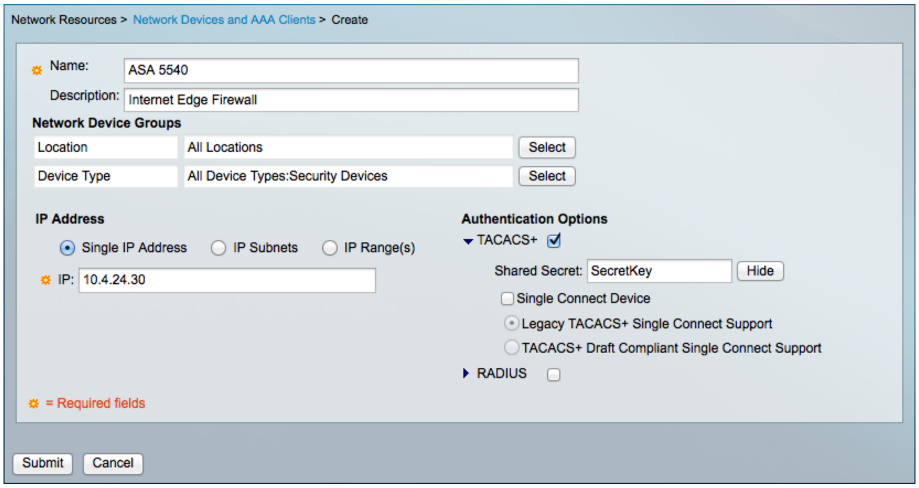


	Name	Description
○	▾ All Device Types	All Device Types
●	Security Devices	

Step 6: In the **IP** field, enter the IP address.

Step 7: Select the **TACACS+** check box.

Step 8: In the **Shared Secret** field, enter a shared secret, and then click **Submit**.



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:Security Devices	Select

IP Address

● Single IP Address ○ IP Subnets ○ IP Range(s)

IP: 10.4.24.30

Authentication Options

TACACS+ ☑

Shared Secret: SecretKey Hide

□ Single Connect Device

● Legacy TACACS+ Single Connect Support

○ TACACS+ Draft Compliant Single Connect Support

RADIUS □

= Required fields

Submit Cancel

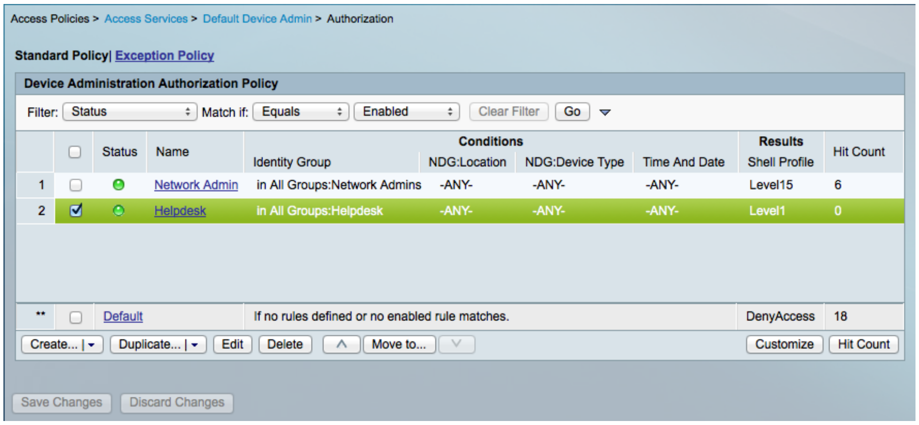
Step 9: Repeat this procedure for every security device that you want to limit access to.

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.



Access Policies > Access Services > Default Device Admin > Authorization

Standard Policy| Exception Policy

Device Administration Authorization Policy

Filter: Status Match if: Equals Enabled Clear Filter Go

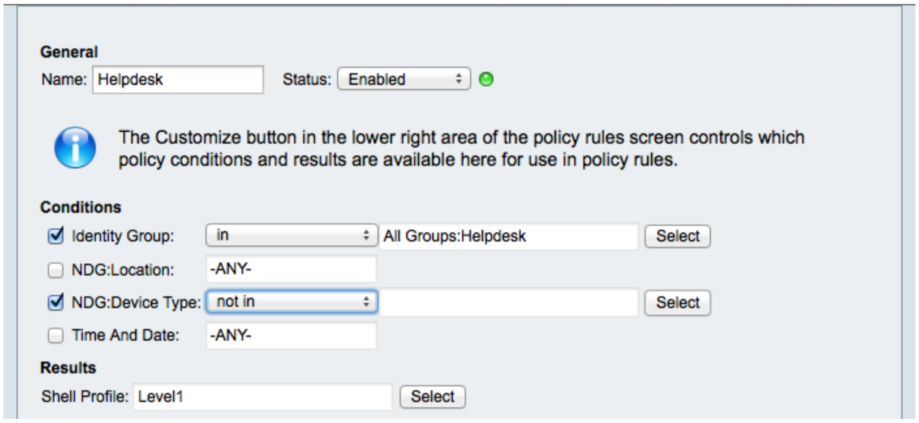
				Conditions				Results	
	□	Status	Name	Identity Group	NDG:Location	NDG:Device Type	Time And Date	Shell Profile	Hit Count
1	□	●	Network Admin	in All Groups:Network Admins	-ANY-	-ANY-	-ANY-	Level15	6
2	☑	●	Helpdesk	in All Groups:Helpdesk	-ANY-	-ANY-	-ANY-	Level1	0
**	□		Default	If no rules defined or no enabled rule matches.				DenyAccess	18

Create... | Duplicate... | Edit Delete Move to... Customize Hit Count

Save Changes 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-

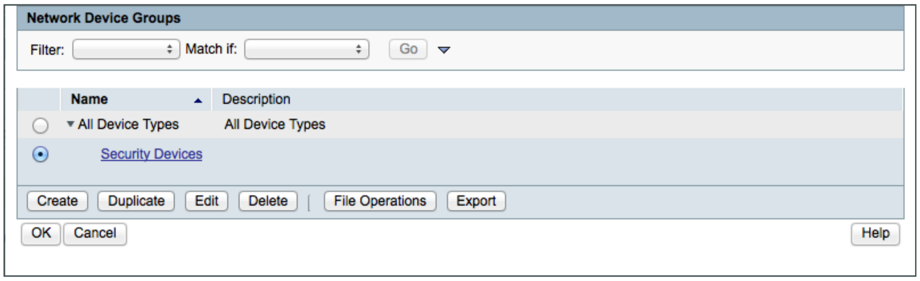
Results

Shell Profile: Level1

Step 5: In the **NDG:Device Type** list, choose **not In**.

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

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

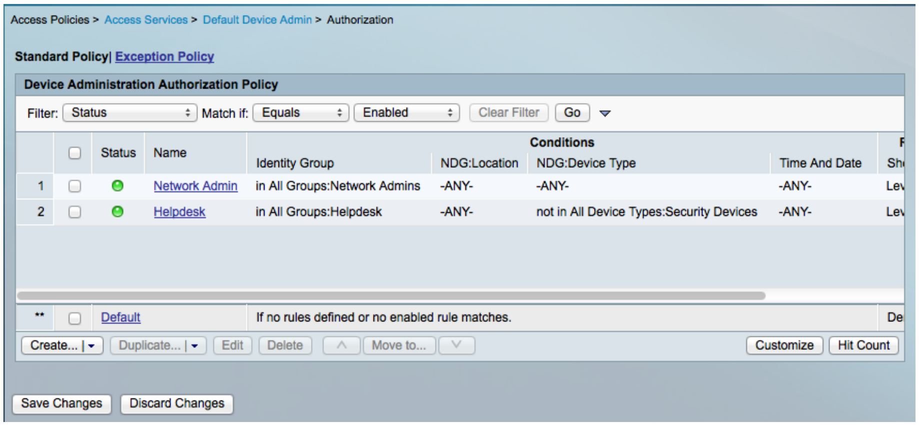


Network Device Groups

Filter: Match if:

	Name	Description
○	▾ All Device Types	All Device Types
●	Security Devices	

Step 8: Click **OK** again, and then click **Save Changes**.



Access Policies > Access Services > Default Device Admin > Authorization

Standard Policy| Exception Policy

Device Administration Authorization Policy

Filter: Status Match if: Equals Enabled

	☐	Status	Name	Conditions				
				Identity Group	NDG:Location	NDG:Device Type	Time And Date	Sh
1	☐	●	Network Admin	in All Groups:Network Admins	-ANY-	-ANY-	-ANY-	Lev
2	☐	●	Helpdesk	in All Groups:Helpdesk	-ANY-	not in All Device Types:Security Devices	-ANY-	Lev
**	☐		Default	If no rules defined or no enabled rule matches.				De

Appendix A: Product List

Access Control

Functional Area	Product Description	Part Numbers	Software
Authentication Services	ACS 5.5 VMware Software And Base License	CSACS-5.5-VM-K9	5.5 with Cumulative Patch 5.5.0.46.2

Appendix B: Changes

This appendix summarizes the changes Cisco made to this guide since its last edition.

- We updated the version of Cisco Secure ACS to the version listed in Appendix A: Product List.

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.

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.

B-0000160-1 08/14