Newer Cisco SBA Guides Available

This guide is part of an older series of Cisco Smart Business Architecture designs. To access the latest Cisco SBA Guides, go to http://www.cisco.com/go/sba

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

SBA

SBA

BORDERLESS NETWORKS

DEPLOYMENT GUIDE

Device Management Using ACS Deployment Guide

SMART BUSINESS ARCHITECTURE

August 2012 Series

Preface

Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

Release Series

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

The Release Notes for a series provides a summary of additions and changes made in the series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

month year Series

For example, the series of guides that we released in August 2012 are the "August 2012 Series".

You can find the most recent series of SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). 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 shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

```
Router# enable
```

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

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100
100 100 100
```

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 SBA feedback form.

If you would like to be notified when new comments are posted, an RSS feed is available from the SBA customer and partner pages.

Table of Contents

What's In This SBA Guide

Cisco SBA Borderless Networks

Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

Cisco SBA Borderless Networks is a comprehensive network design targeted at organizations with up to 10,000 connected users. The SBA Borderless Network architecture incorporates wired and wireless local area network (LAN) access, wide-area network (WAN) connectivity, WAN application optimization, and Internet edge security infrastructure.

Route to Success

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.

About This Guide

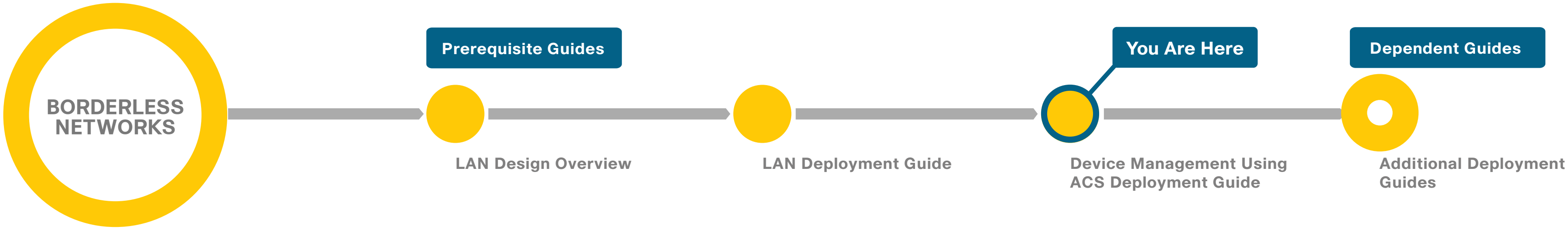
This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- Business Overview—Describes the business use case for the design. Business decision makers may find this section especially useful.
- Technology Overview—Describes the technical design for the business use case, including an introduction to the Cisco products that make up the design. Technical decision makers can use this section to understand how the design works.
- Deployment Details—Provides step-by-step instructions for deploying and configuring the design. Systems engineers can use this section to get the design up and running quickly and reliably.

You can find the most recent series of Cisco SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel



Introduction

Business Overview

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.

Technology 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
```

Step 2: 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 3: 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 4: 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 5: 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**.

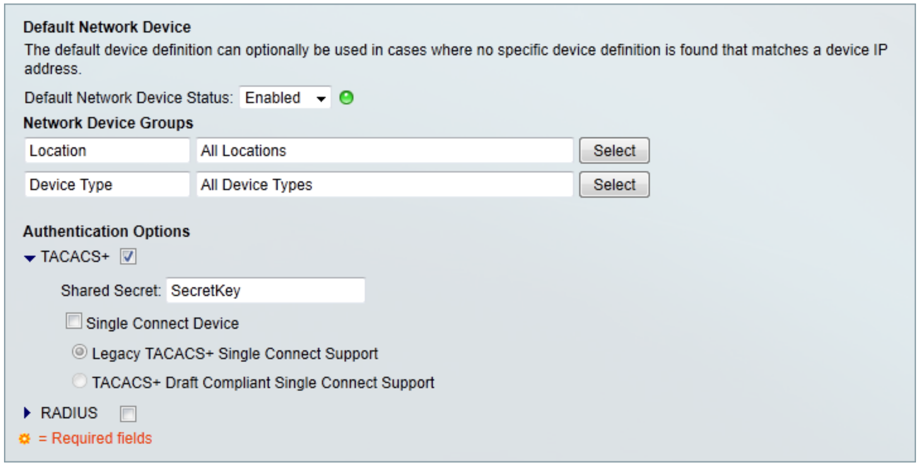
Step 2: In the Default Network Device Status list, choose **Enabled**.

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	All Locations	Select
Device Type	All Device Types	Select

Authentication Options

▾ TACACS+ ☑

Shared Secret: SecretKey

□ 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

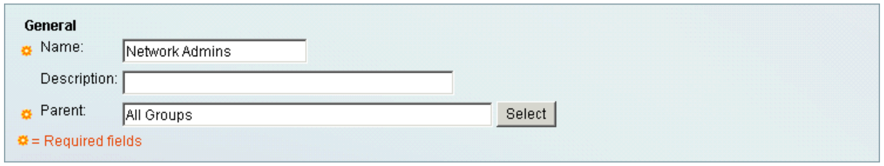
Group name	Description
Helpdesk	Users who are allowed to log in to a device but not make changes
Network Admins	Users who are allowed to log in to a device and make changes

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.

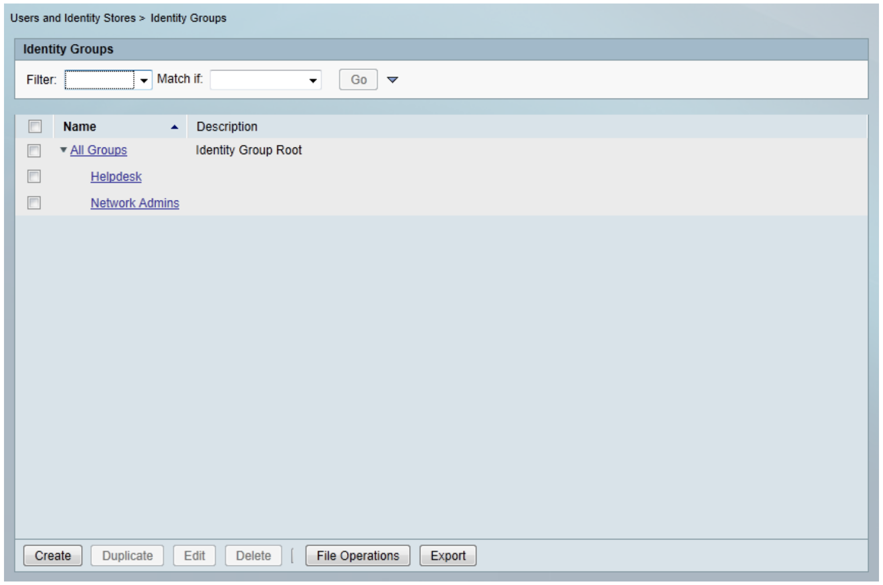
Step 4: Click **Submit**.



General

Name:	Network Admins
Description:	
Parent:	All Groups

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



Users and Identity Stores > Identity Groups

Identity Groups

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

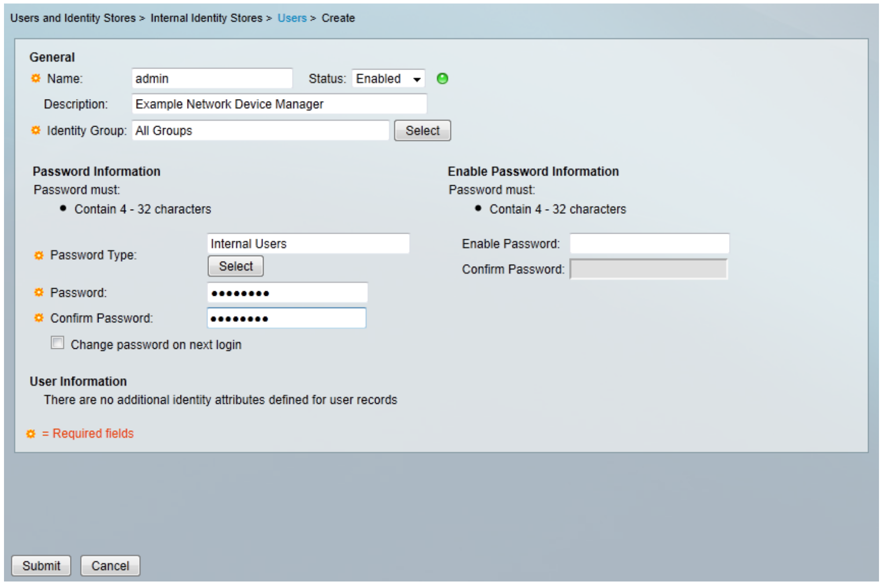
Procedure 5 Create internal identity store users

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

Password Information
Password must:
- Contain 4 - 32 characters

Password Type:	Internal Users
Password:	••••••••
Confirm Password:	••••••••

□ Change password on next login

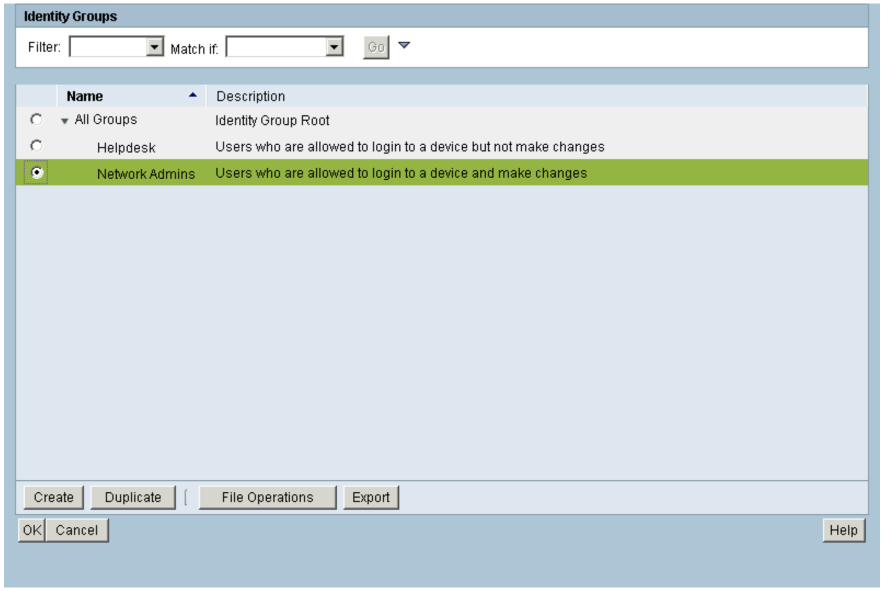
Enable Password Information
Password must:
- Contain 4 - 32 characters

Enable Password:	
Confirm Password:	

User Information
There are no additional identity attributes defined for user records

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	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**.

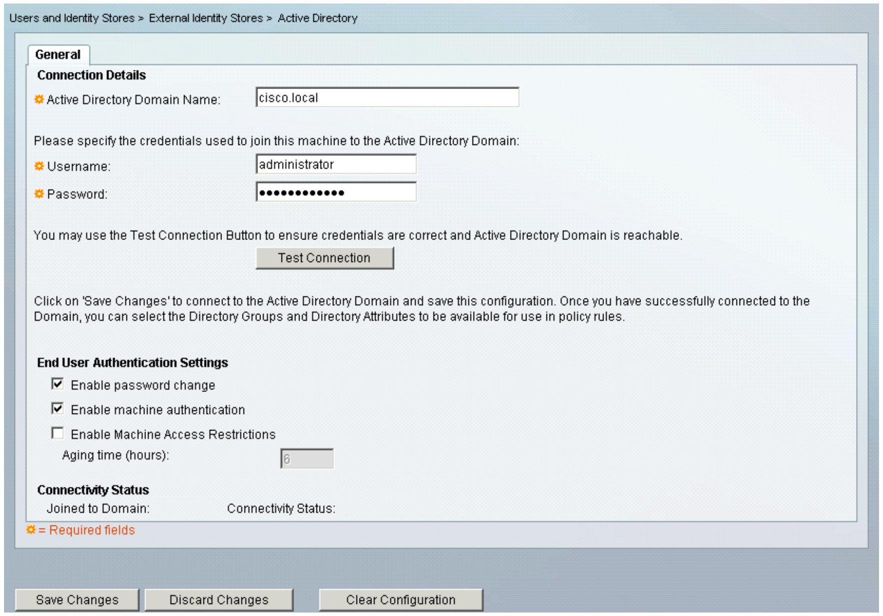
Step 7: Repeat Step 1 through Step 6 for each user account you want to create.

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: 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.

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): 6

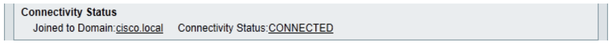
Connectivity Status

Joined to Domain: Connectivity Status:

= Required fields

Step 3: Click **Save Changes**.

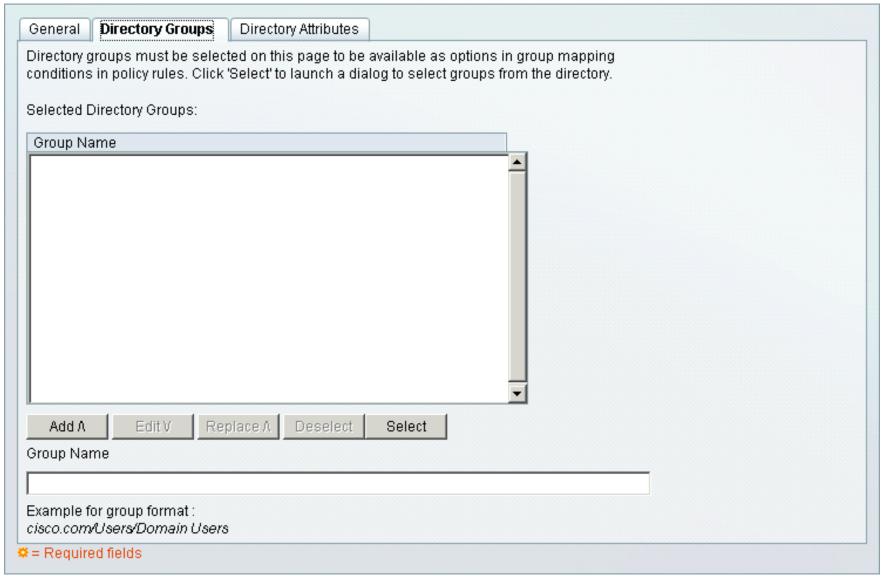
Connectivity Status changes to CONNECTED.



Connectivity Status

Joined to Domain: cisco.local Connectivity Status: CONNECTED

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



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:

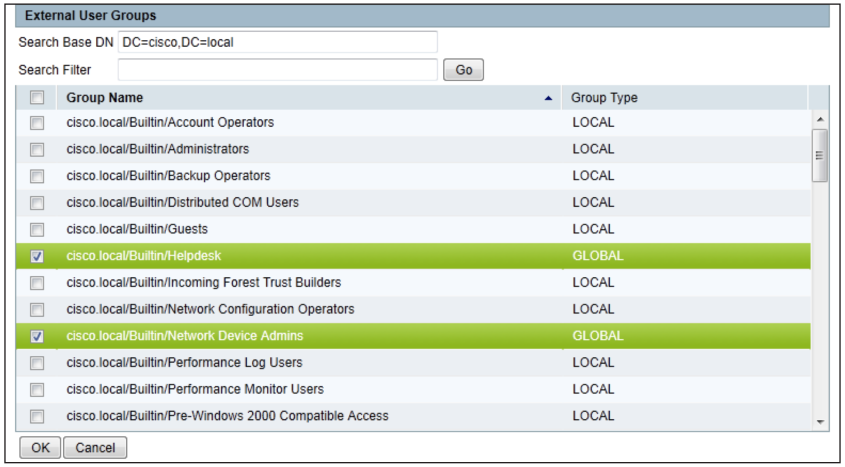
Group Name

Group Name

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

✱ = 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**.



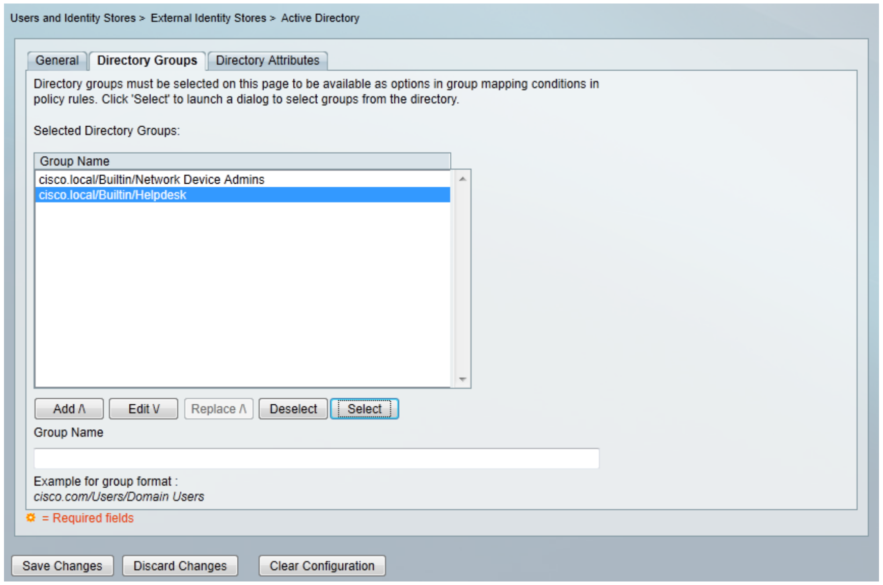
External User Groups

Search Base DN: DC=cisco,DC=local

Search Filter:

□	Group Name ▲	Group Type
□	cisco.local/Builtin/Account Operators	LOCAL
□	cisco.local/Builtin/Administrators	LOCAL
□	cisco.local/Builtin/Backup Operators	LOCAL
□	cisco.local/Builtin/Distributed COM Users	LOCAL
□	cisco.local/Builtin/Guests	LOCAL
☑	cisco.local/Builtin/Helpdesk	GLOBAL
□	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/Performance Log Users	LOCAL
□	cisco.local/Builtin/Performance Monitor Users	LOCAL
□	cisco.local/Builtin/Pre-Windows 2000 Compatible Access	LOCAL

Step 6: 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/Network Device Admins
cisco.local/Builtin/Helpdesk

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**.

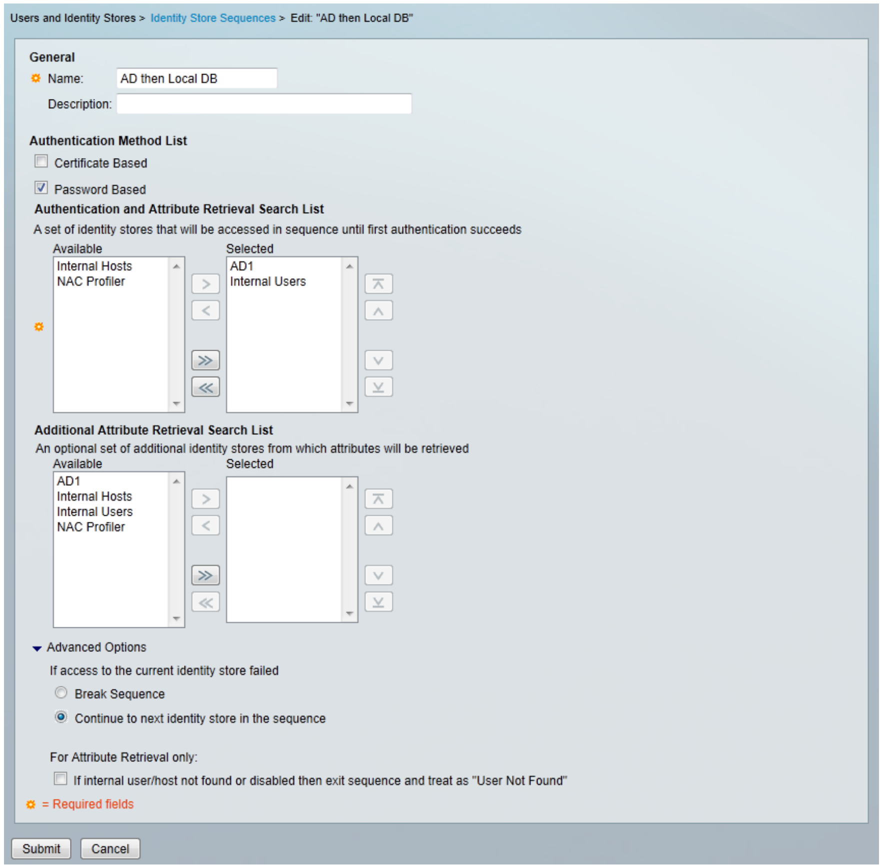
Step 4: Select **Password Based**.

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

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

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).

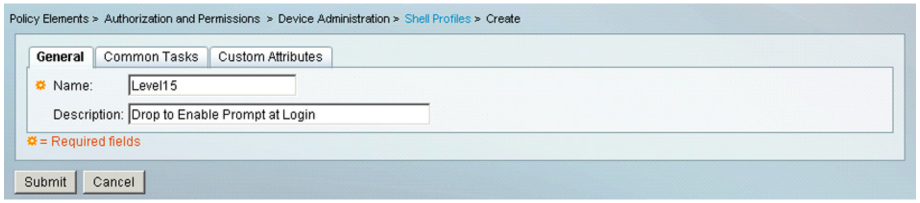
Table 2 - Shell profiles

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.



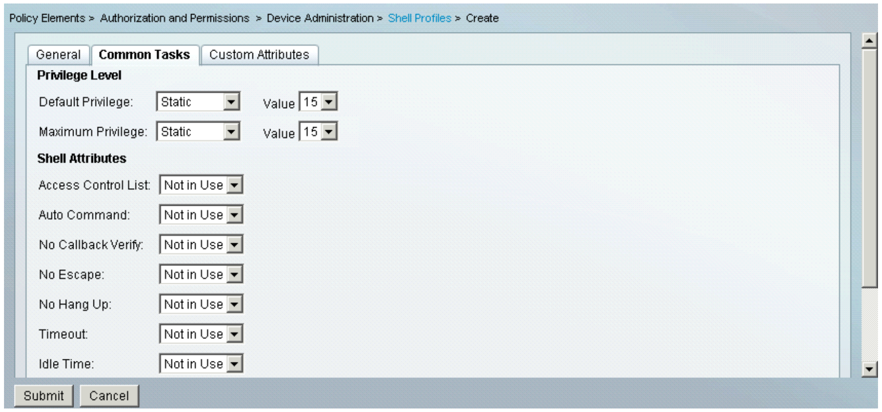
Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Create

Name: Level15

Description: Drop to Enable Prompt at Login

= Required fields

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



Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Create

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

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.

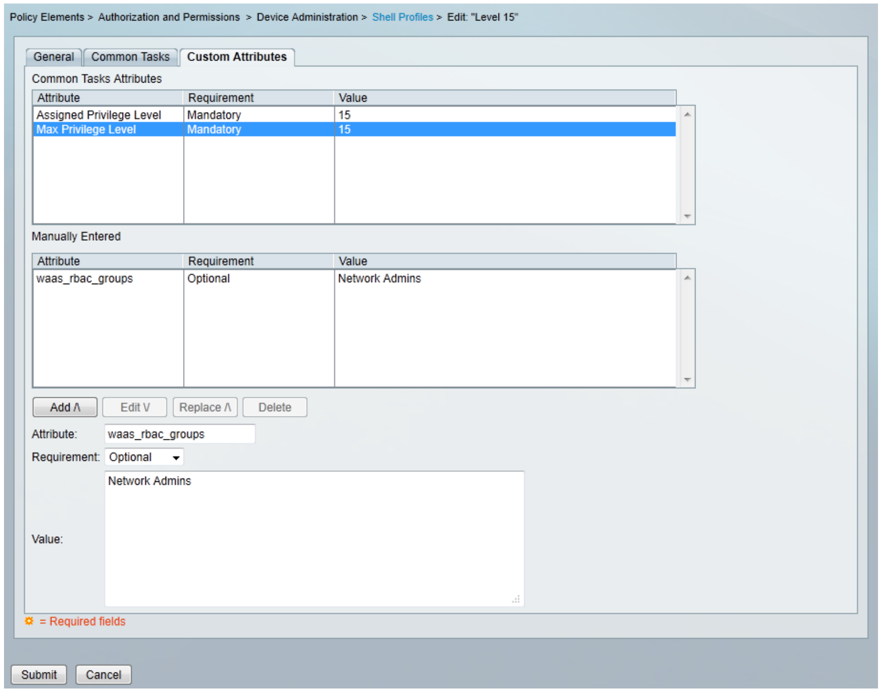
Step 6: Under Manually Entered, in the **Attribute** box, enter **waas_rbac_groups**. This enables network administrators to log in to Cisco Wide Area Application Services (WAAS) devices as well as Cisco IOS Software devices.

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 1 through Step 10 for the Level1 shell profile, using the values from Table 2.



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

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

Attribute: waas_rbac_groups

Requirement: Optional

Value: Network Admins

☼ = Required fields

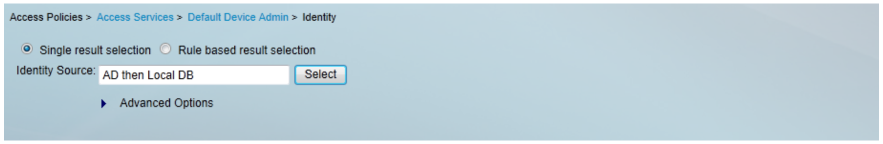
Procedure 9 Map external groups to internal groups

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

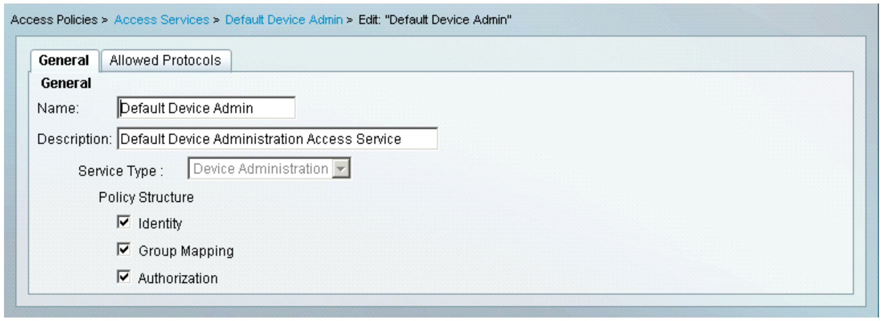
○ Single result selection ○ Rule based result selection

Identity Source: AD then Local DB

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

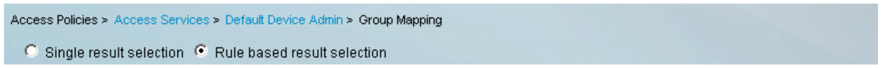
☑ Group Mapping

☑ Authorization

Step 7: Click **Submit**.

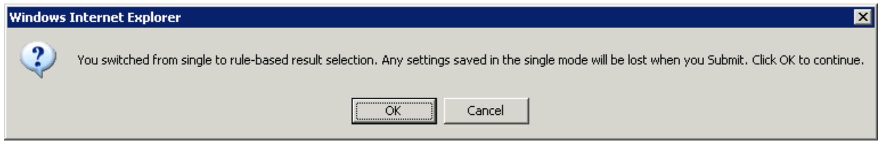
Step 8: Navigate to **Access Policies > Access Services > Default Device Admin > Group Mapping**.

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**.

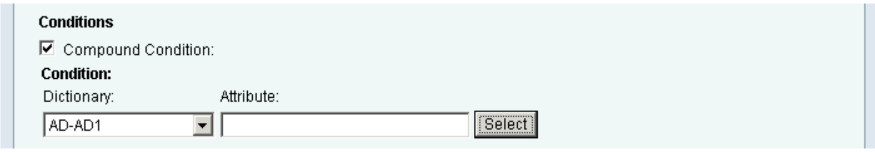

Windows Internet Explorer

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.

Step 11: Click **Create**.

Step 12: Select **Compound Condition**.

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


Conditions

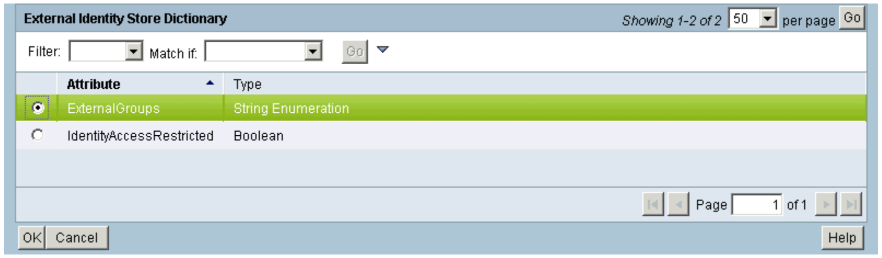
☑ Compound Condition:

Condition:

Dictionary: AD-AD1

Attribute:

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

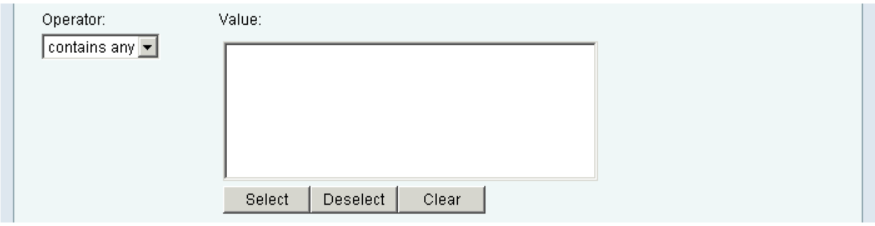

External Identity Store Dictionary

Showing 1-2 of 2 50 per page

	Attribute	Type
●	ExternalGroups	String Enumeration
○	IdentityAccessRestricted	Boolean

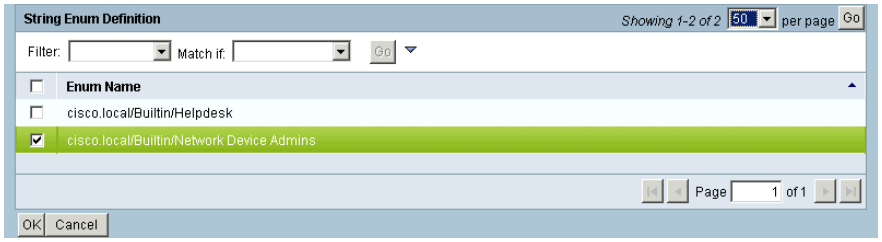
Page 1 of 1

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


Operator: contains any

Value:

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

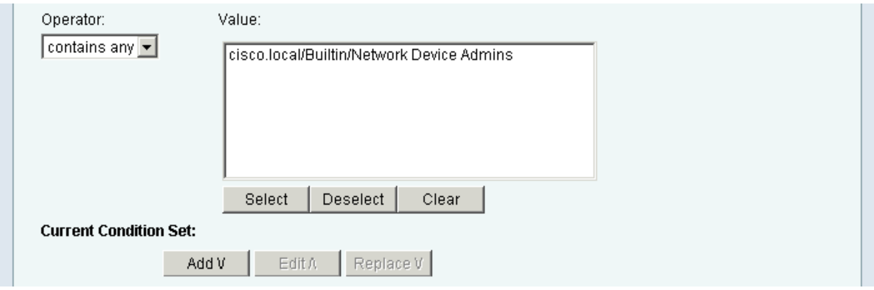

String Enum Definition

Showing 1-2 of 2 | 50 per page

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

Page 1 of 1

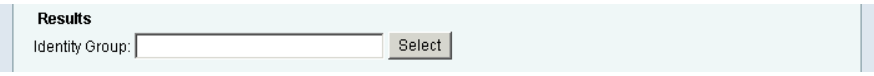
Step 17: Click **Add V**.


Operator: contains any

Value: cisco.local/Builtin/Network Device Admins

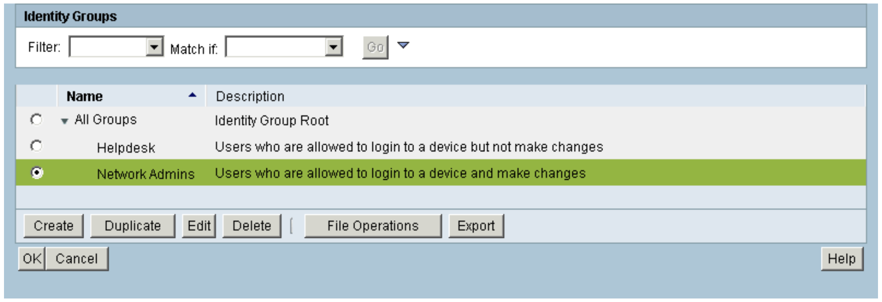
Current Condition Set:

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

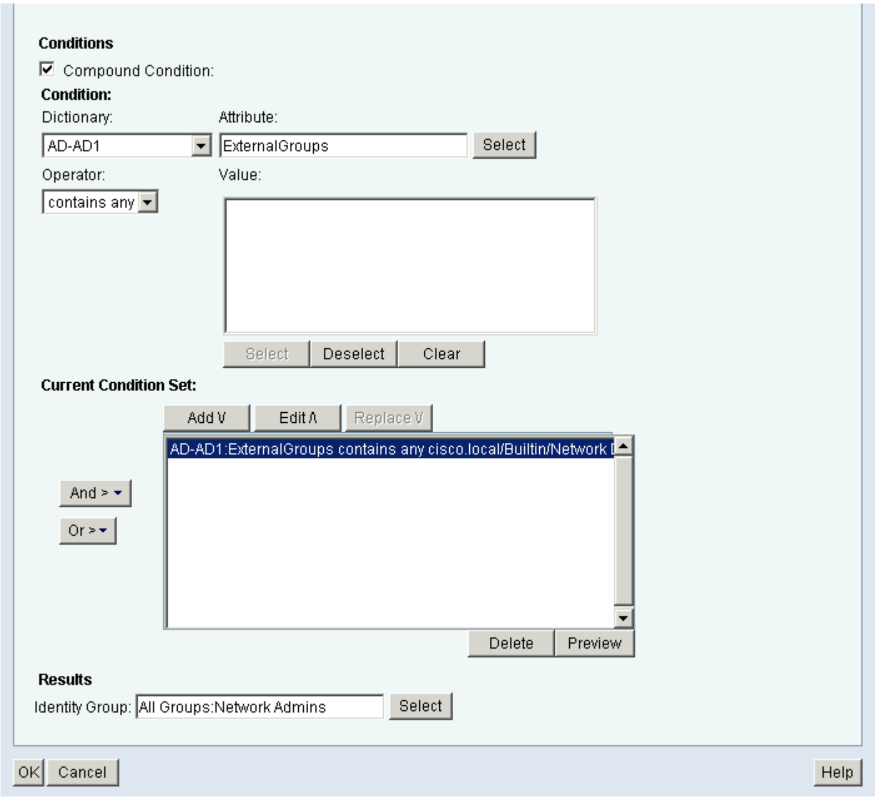
Identity Group:

Step 19: Select **Network Admins**.


Identity Groups

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


Conditions

☑ Compound Condition:

Condition:

Dictionary: AD-AD1

Attribute: ExternalGroups

Operator: contains any

Value:

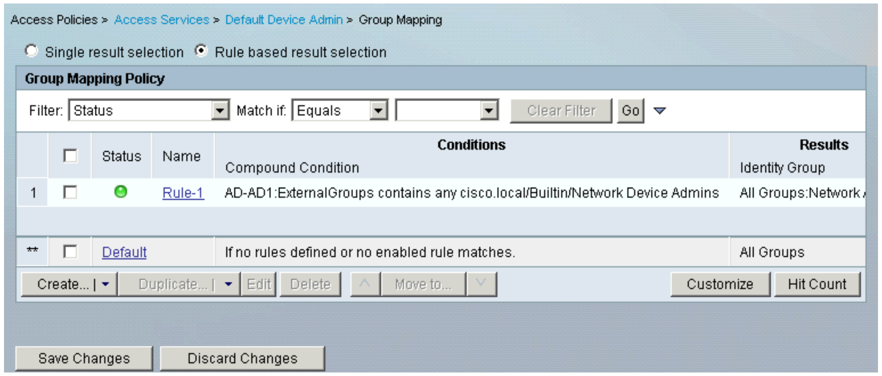
Current Condition Set:

AD-AD1:ExternalGroups contains any cisco.local/Builtin/Network

Results

Identity Group: All Groups:Network Admins

Step 21: 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

	☐	Status	Name	Conditions Compound Condition	Results Identity Group
1	☐	●	Rule-1	AD-AD1:ExternalGroups contains any cisco.local/Builtin/Network Device Admins	All Groups:Network
**	☐		Default	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

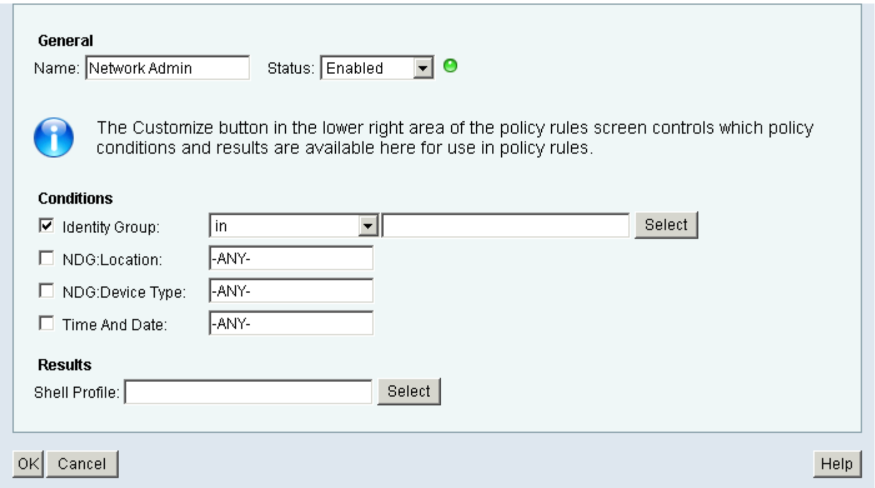
Cisco Secure ACS is preconfigured with two access services: Default Device Admin and Default Network Access (for TACACS+ and RADIUS authentications, respectively). This procedure modifies the Default Device Admin authorization policy to allow logins to network devices only for Network Admins and Helpdesk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

☐ NDG:Location: -ANY-

☐ NDG:Device Type: -ANY-

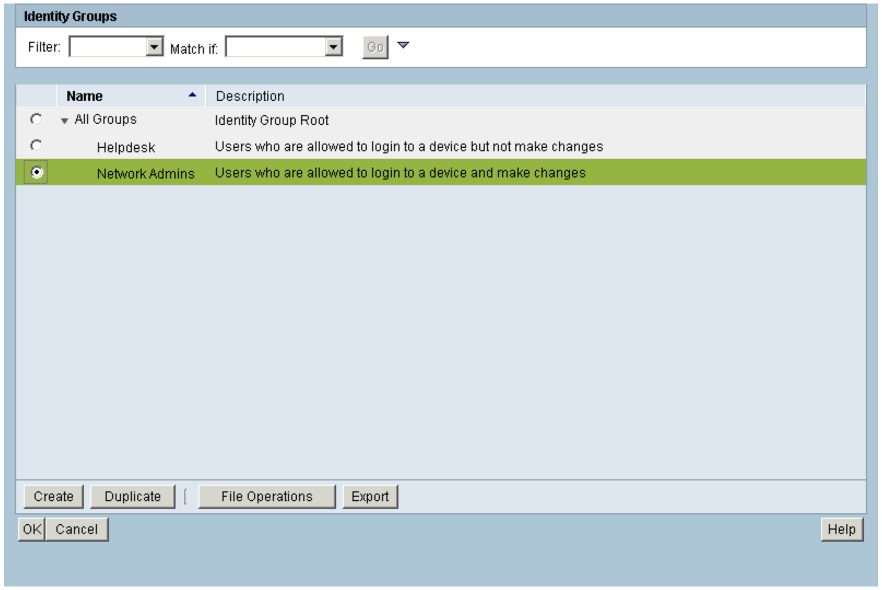
☐ Time And Date: -ANY-

Results

Shell Profile:

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

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

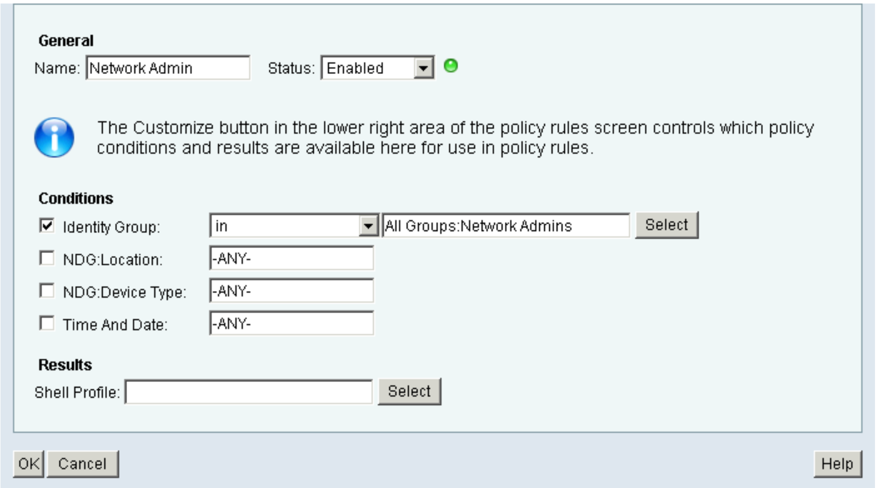


Identity Groups

Filter: Match if:

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

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



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 All Groups:Network Admins

☐ NDG:Location: -ANY-

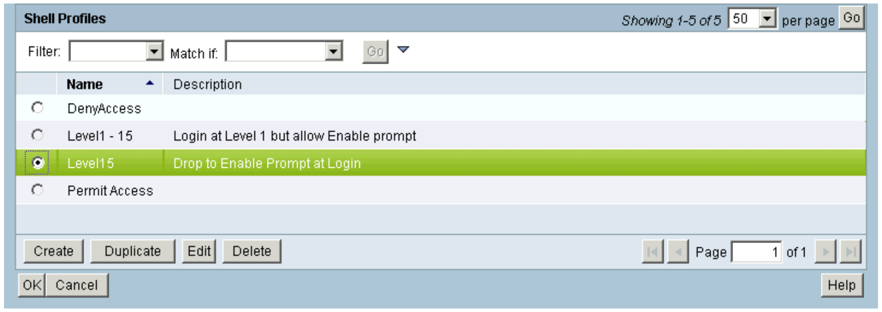
☐ NDG:Device Type: -ANY-

☐ Time And Date: -ANY-

Results

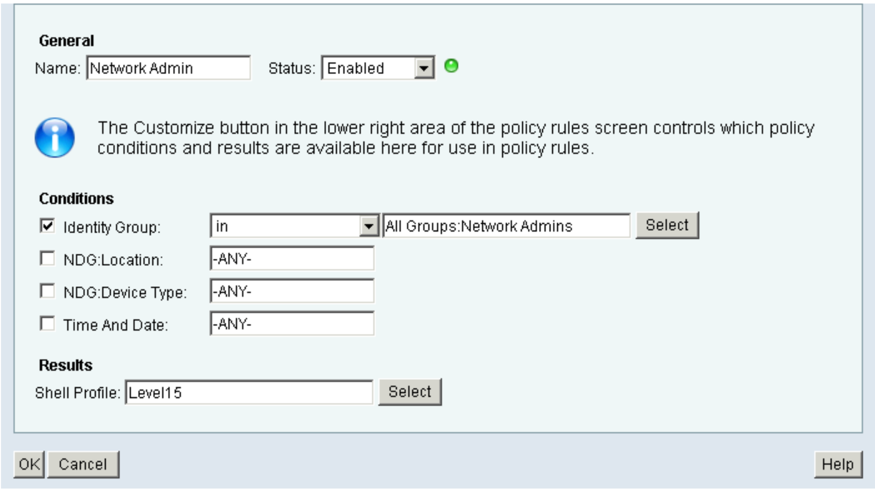
Shell Profile:

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



	Name	Description
○	DenyAccess	
○	Level1 - 15	Login at Level 1 but allow Enable prompt
●	Level15	Drop to Enable Prompt at Login
○	Permit Access	

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


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 All Groups:Network Admins Select

☐ NDG:Location: -ANY-

☐ NDG:Device Type: -ANY-

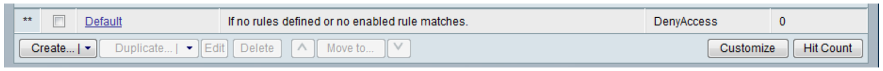
☐ Time And Date: -ANY-

Results

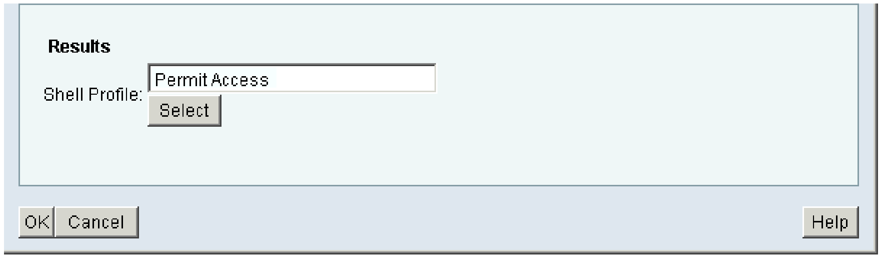
Shell Profile: Level15 Select

Next, edit the default rule,

Step 8: Click **Default**.

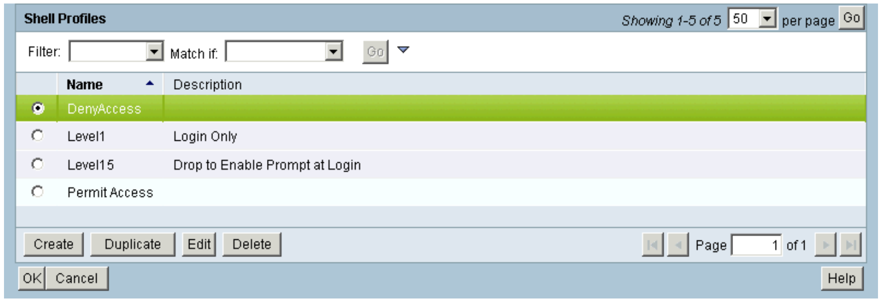

**	☐	Default	If no rules defined or no enabled rule matches.	DenyAccess	0

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


Results

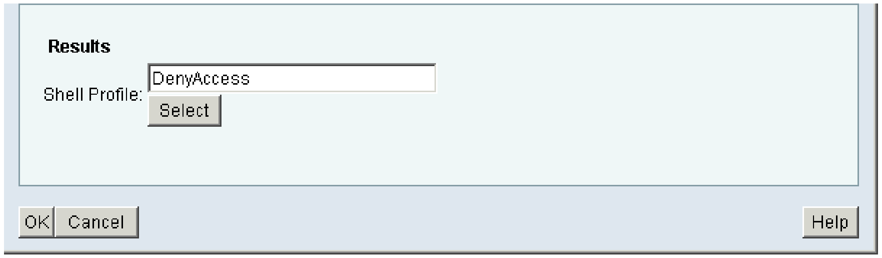
Shell Profile: Permit Access Select

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



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

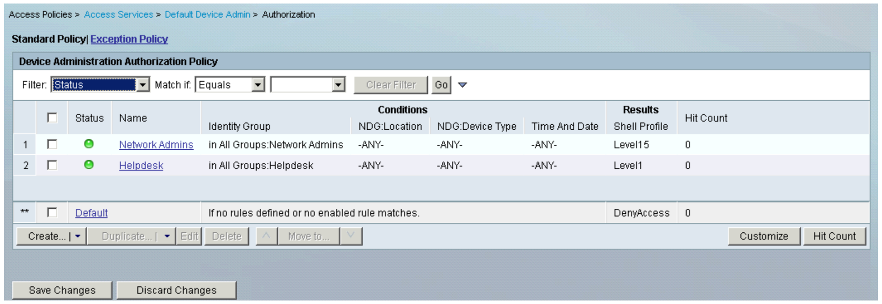
Step 11: Click **OK** again.


Results

Shell Profile: DenyAccess Select

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

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

				Conditions				Results	
	□	Status	Name	Identity Group	NDG:Location	NDG:Device Type	Time And Date	Shell Profile	Hit Count
1	□	●	Network Admins	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	0

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

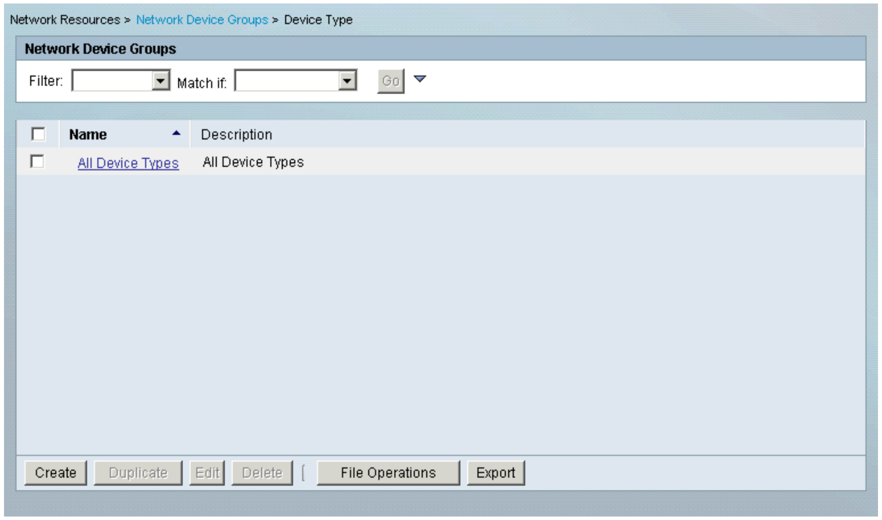
This process configures Cisco Secure ACS to allow only network administrators to log in to devices that you want to limit access to (also called *security devices*).

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**.



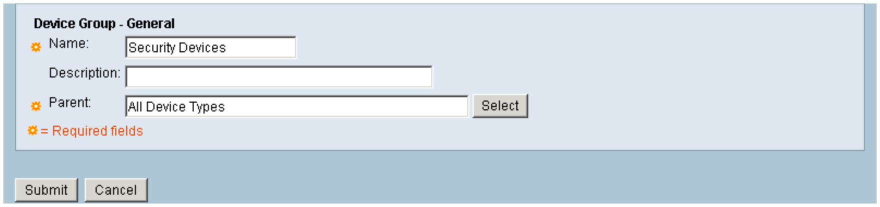
Network Resources > Network Device Groups > Device Type

Network Device Groups

Filter: Match if:

□	Name	Description
□	All Device Types	All Device Types

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



Device Group - General

Name: Security Devices

Description:

Parent: All Device Types

= Required fields

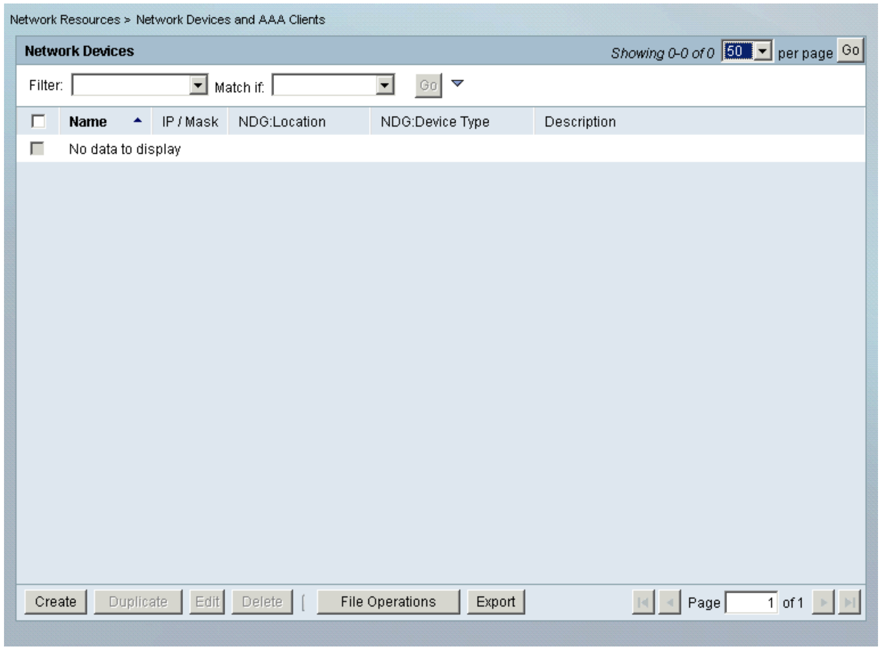
Step 4: Click **Submit**.

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**.



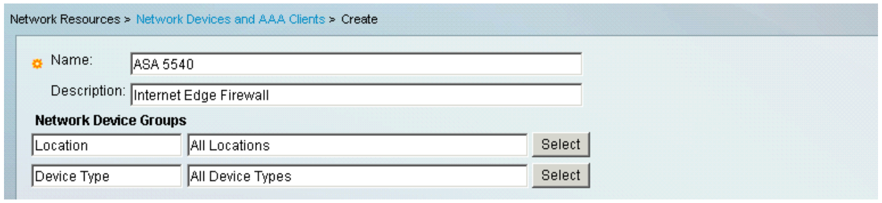
Network Resources > Network Devices and AAA Clients

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

Filter: Match if: Go

□	**Name** ▲	IP / Mask	NDG:Location	NDG:Device Type	Description
□	No data to display				

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



Network Resources > Network Devices and AAA Clients > Create

Name: ASA 5540

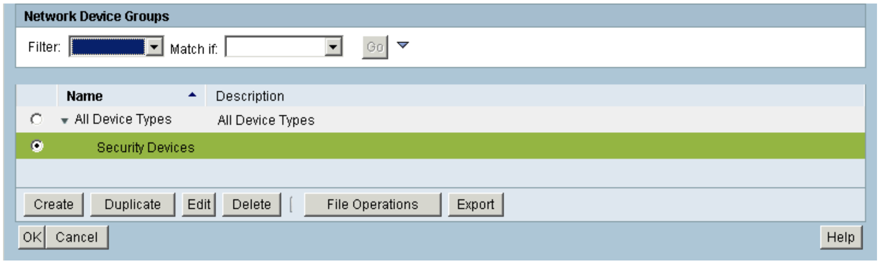
Description: Internet Edge Firewall

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
○	▾ All Device Types	All Device Types
●	Security Devices	

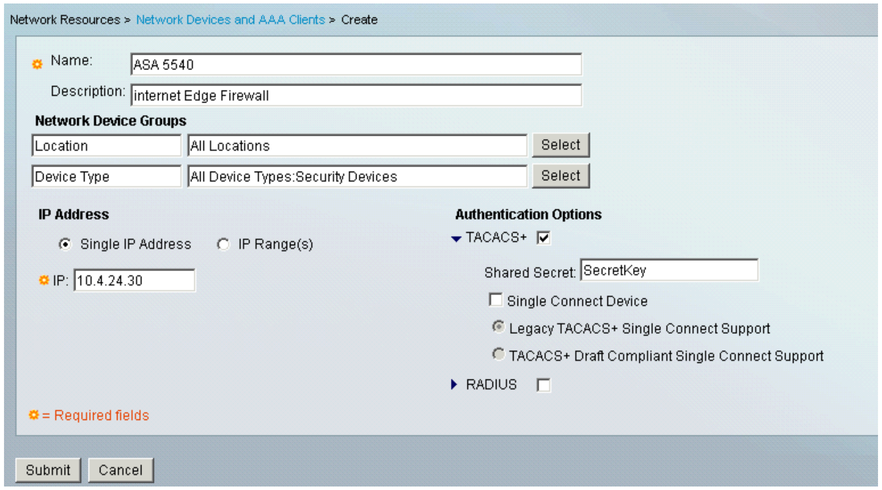
Step 6: Click **OK**.

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**.



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 Range(s)

IP: 10.4.24.30

Authentication Options

▾ TACACS+ ☑

Shared Secret: SecretKey

□ Single Connect Device

● Legacy TACACS+ Single Connect Support

○ TACACS+ Draft Compliant Single Connect Support

▸ RADIUS □

= Required fields

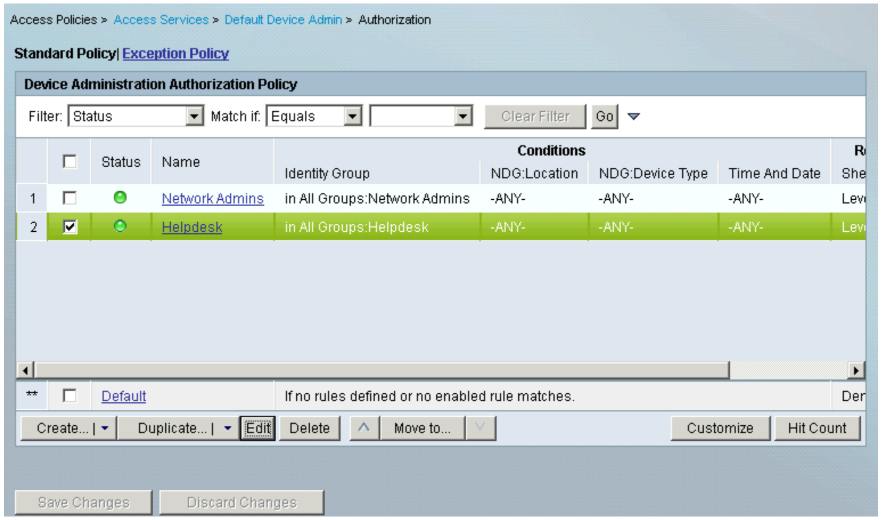
Step 11: Repeat this procedure for every security device that you want to limit access to.

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.



Access Policies > Access Services > Default Device Admin > Authorization

Standard Policy | Exception Policy

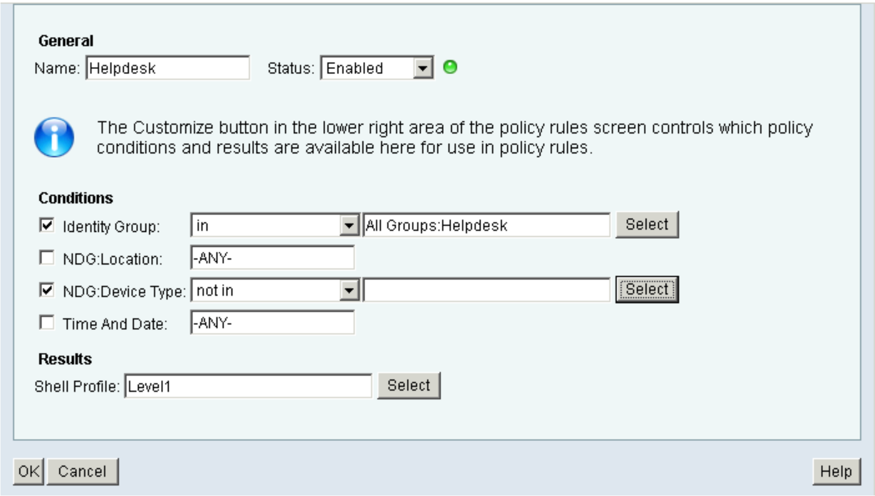
Device Administration Authorization Policy

Filter: Status Match if: Equals

	☐	Status	Name	Conditions Identity Group	NDG:Location	NDG:Device Type	Time And Date	R She
1	☐	●	Network Admins	in All Groups:Network Admins	-ANY-	-ANY-	-ANY-	Lev
2	☑	●	Helpdesk	in All Groups:Helpdesk	-ANY-	-ANY-	-ANY-	Lev
**	☐		Default	If no rules defined or no enabled rule matches.				Der

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-

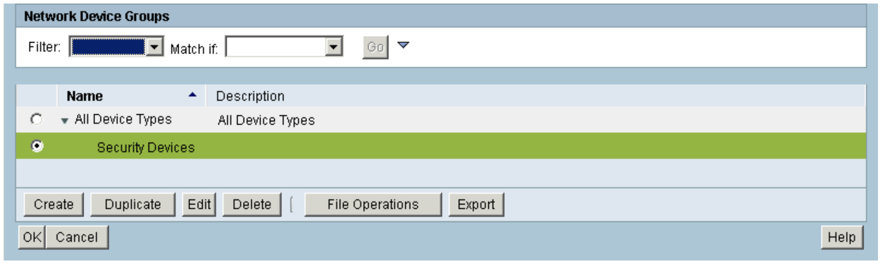
Results

Shell Profile: Level1

Step 5: 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**.

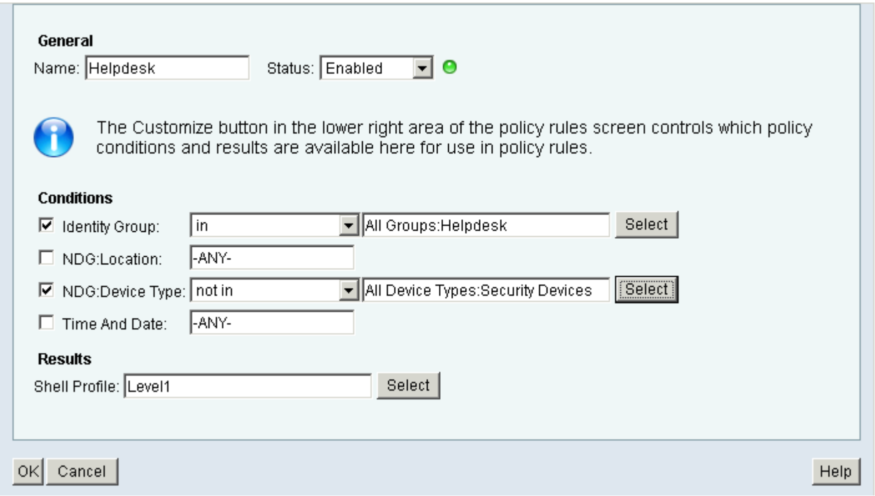


Network Device Groups

Filter: Match if:

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

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.

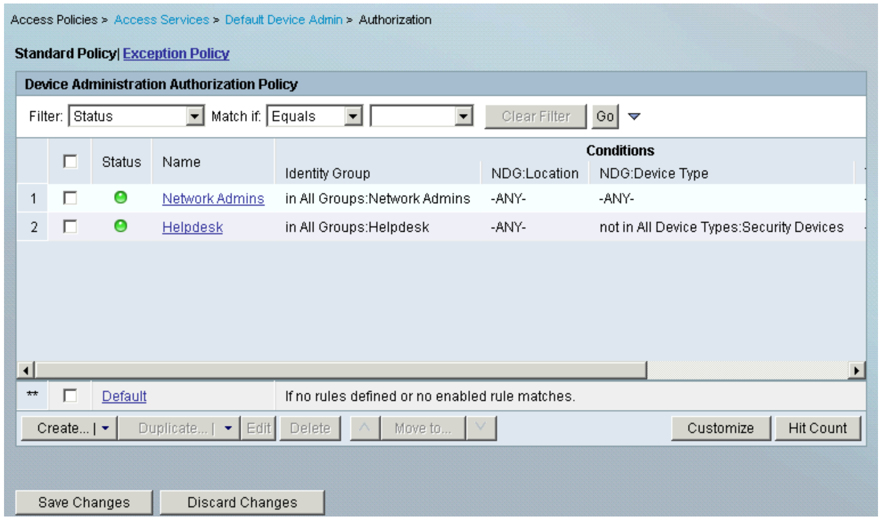
Conditions

☑ Identity Group:	in	All Groups:Helpdesk	Select
□ NDG:Location:	-ANY-		
☑ NDG:Device Type:	not in	All Device Types:Security Devices	Select
□ Time And Date:	-ANY-		

Results

Shell Profile: Level1

Step 9: Click **Save Changes**.



Access Policies > Access Services > Default Device Admin > Authorization

Standard Policy| Exception Policy

Device Administration Authorization Policy

Filter: Status Match if: Equals

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

Notes

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

Appendix B: Changes

This appendix summarizes the changes to this guide since the previous Cisco SBA series.

- We upgraded Cisco Secure ACS to version 5.3.
- We made minor changes to improve the readability of this guide.

Notes

Feedback

Click here to provide feedback to Cisco SBA.

SMART BUSINESS ARCHITECTURE

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.

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.