

ACS 5.x: TACACS+ Authentication and Command Authorization based on AD group membership Configuration Example

Document ID: 113590

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configuration

- Configure ACS 5.x for Authentication and Authorization
- Configure the Cisco IOS device for Authentication and Authorization

Verify

Related Information

Introduction

This document provides an example of configuring TACACS+ Authentication and Command Authorization based on AD group membership of a user with Cisco Secure Access Control System (ACS) 5.x and later. ACS uses Microsoft Active Directory (AD) as an external identity store to store resources such as users, machines, groups, and attributes.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- ACS 5.x is fully integrated to the desired AD Domain. If the ACS is not integrated with the desired AD Domain, refer to ACS 5.x and later: Integration with Microsoft Active Directory Configuration Example for more information in order to perform the integration task.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure ACS 5.3
- Cisco IOS[®] Software Release 12.2(44)SE6.

Note: This configuration can be done on all the Cisco IOS devices.

- Microsoft Windows Server 2003 Domain

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configuration

Configure ACS 5.x for Authentication and Authorization

Before you begin the configuration of the ACS 5.x for Authentication and Authorization, ACS should have been integrated successfully with Microsoft AD. If the ACS is not integrated with the desired AD Domain, refer to ACS 5.x and later: Integration with Microsoft Active Directory Configuration Example for more information in order to perform the integration task.

In this section, you map two AD groups to two different command sets and two Shell profiles, one with full-access and the other with limited-access on the Cisco IOS devices.

1. Log into the ACS GUI using Admin credentials.
2. Choose **Users and Identity Stores > External Identity Stores > Active Directory** and verify that the ACS has joined the desired domain and also that the **connectivity status** is shown as **connected**.

Click on **Directory Groups** Tab.

Users and Identity Stores > External Identity Stores > Active Directory

General Directory Groups Directory Attributes

Connection Details

Active Directory Domain Name: MCS55.com

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

Username: training

Password:

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

Test Connection

Click on 'Save Changes' to connect to the Active Directory Domain and save this configuration. Once you have success 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

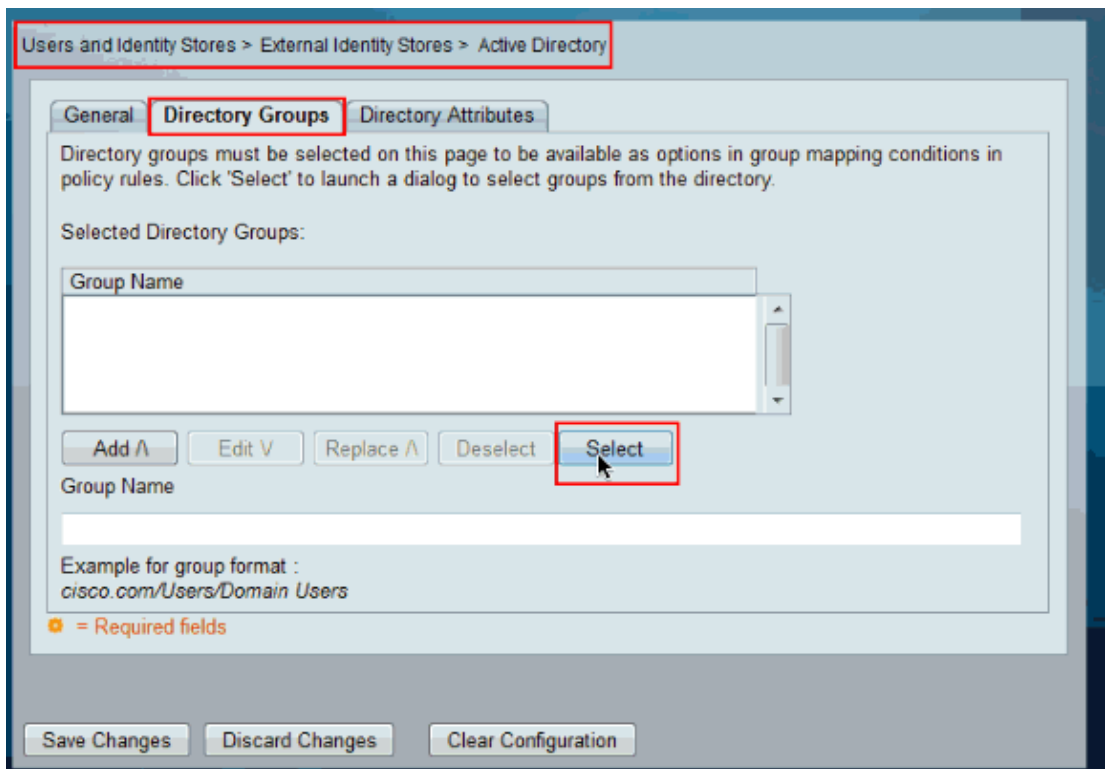
Connectivity Status

Joined to Domain: mcs55.com Connectivity Status: CONNECTED

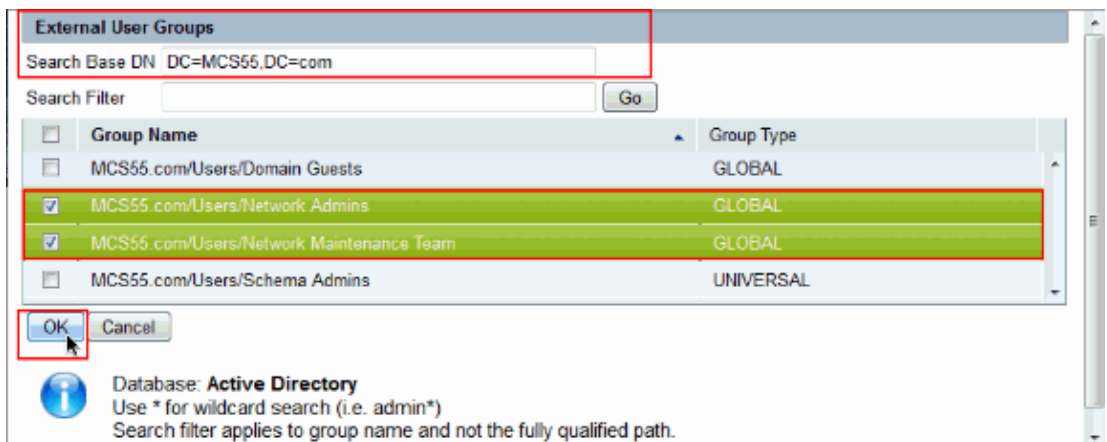
= Required fields

Save Changes Discard Changes Clear Configuration

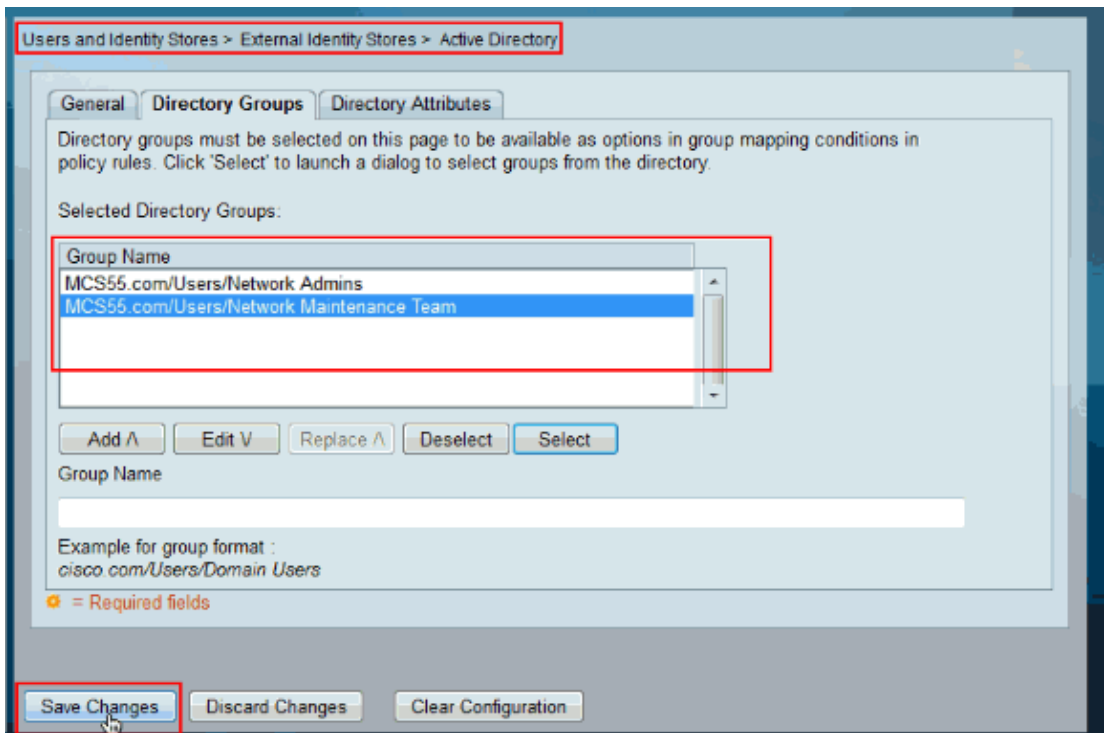
3. Click **Select**.



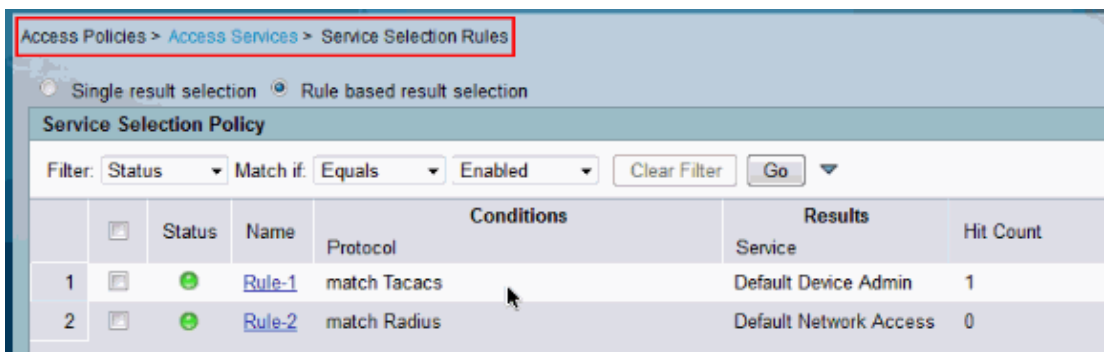
4. Choose the groups that need to be mapped to the Shell profiles and command sets in the later part of the configuration. Click **OK**.



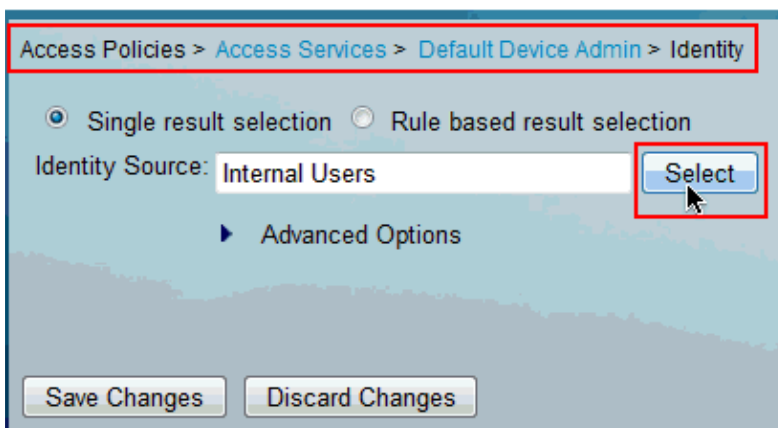
5. Click **Save Changes**.



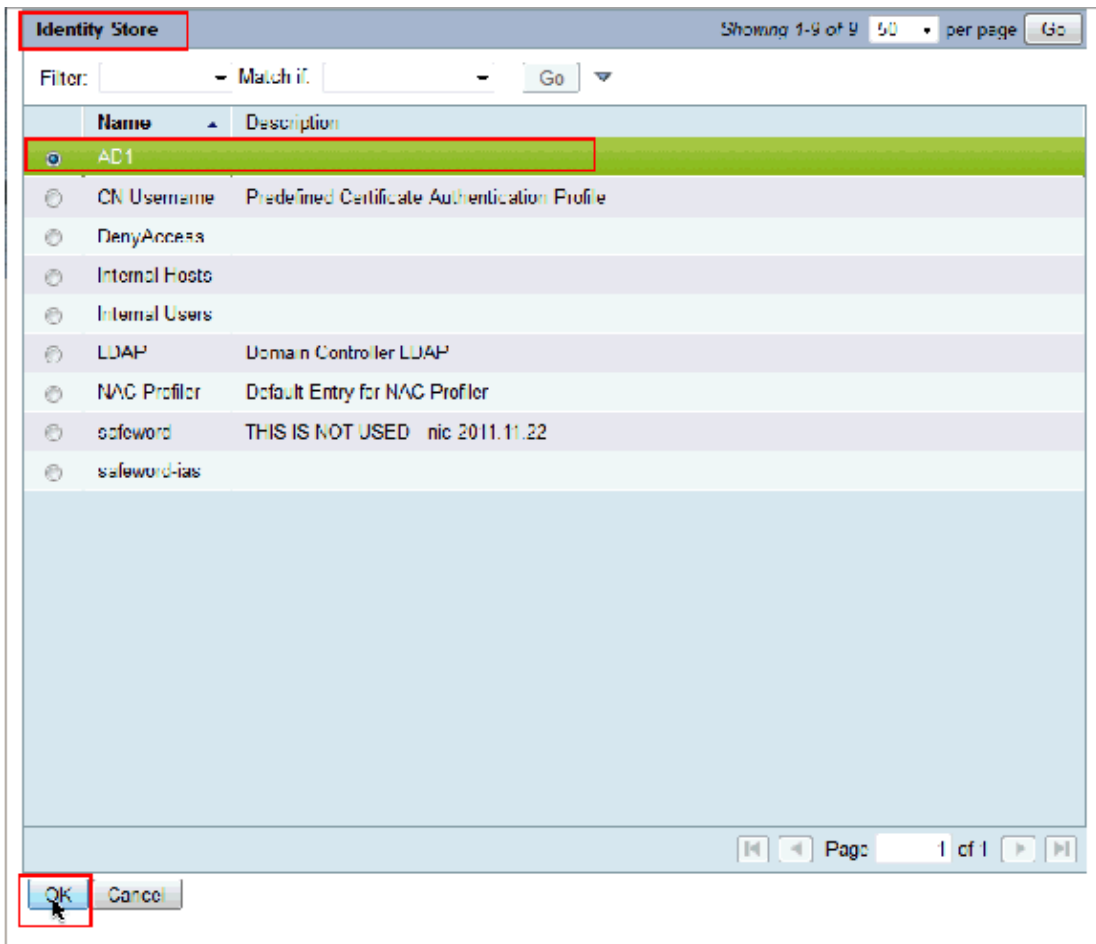
6. Choose **Access Policies > Access Services > Service Selection Rules** and identify the access service, which processes the TACACS+ Authentication. In this example, it is **Default Device Admin**.



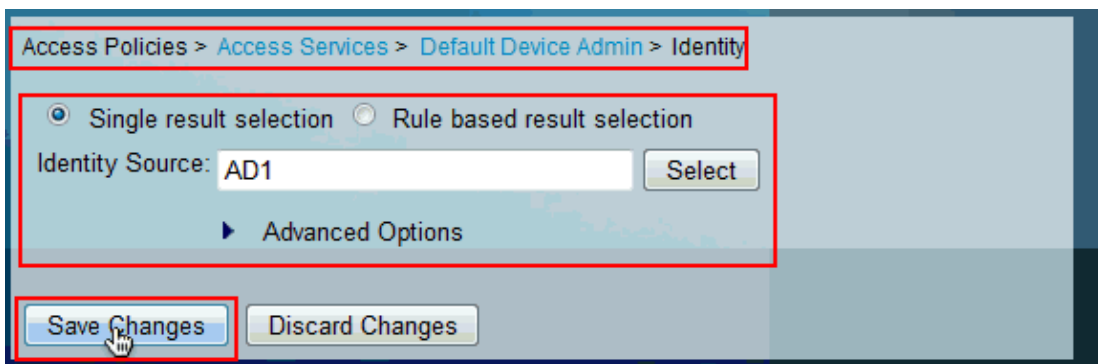
7. Choose **Access Policies > Access Services > Default Device Admin > Identity** and click **Select** next to **Identity Source**.



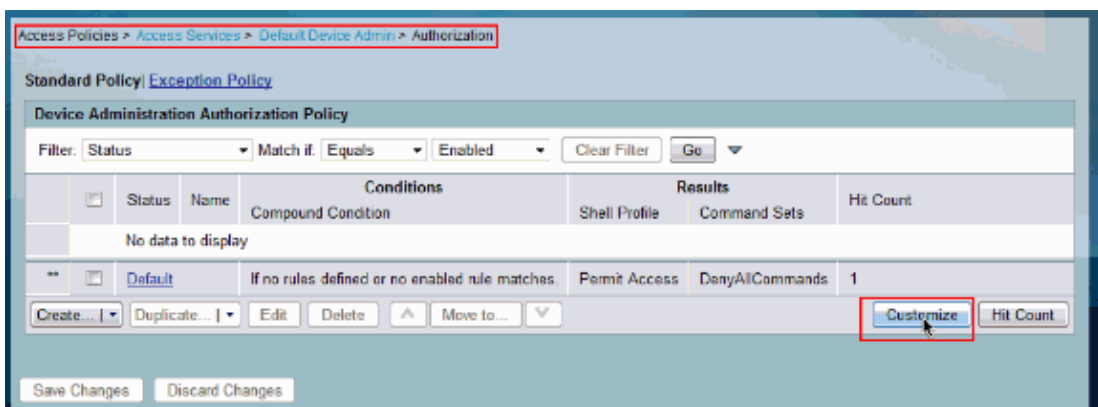
8. Choose **AD1** and click **OK**.



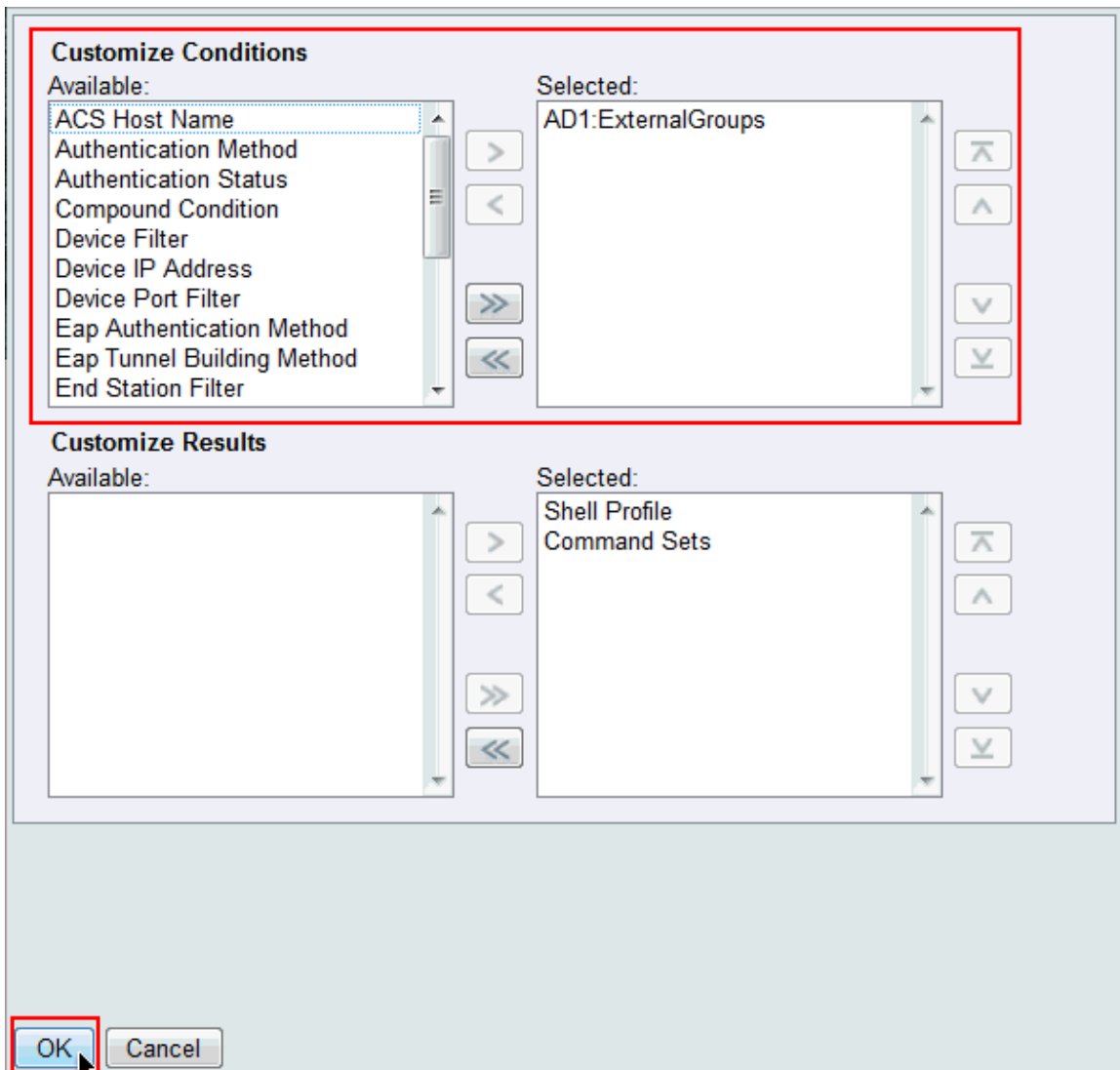
9. Click **Save Changes**.



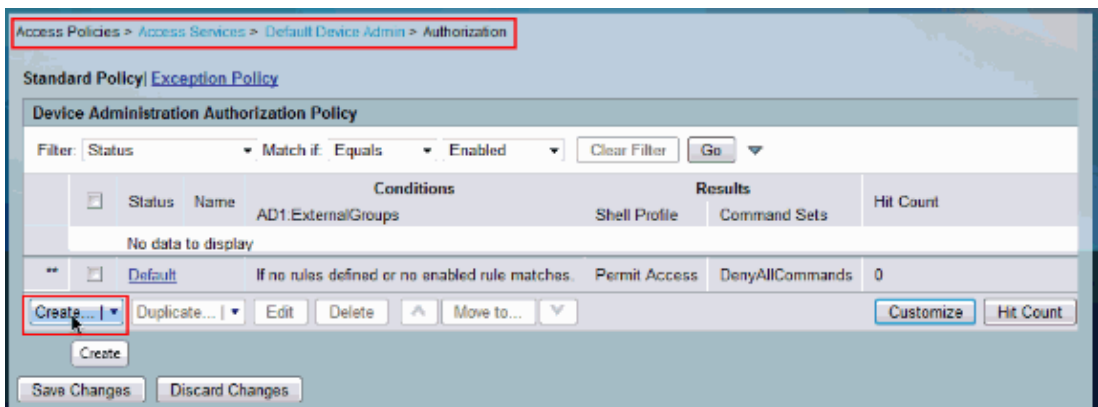
10. Choose **Access Policies > Access Services > Default Device Admin > Authorization** and click on **Customize**.



11. Copy **AD1:ExternalGroups** from **Available** to **Selected** section of **Customize Conditions** and then move **Shell Profile** and **Command Sets** from **Available** to **Selected** section of **Customize Results**. Now click **OK**.



12. Click **Create** in order to create a new Rule.



13. Click **Select** in the **AD1:ExternalGroups** Condition.

General
 Name: Status:

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

Conditions
 AD1:ExternalGroups:

Results
 Shell Profile:

Command Sets:

14. Choose the group that you want to provide full access on the Cisco IOS device. Click **OK**.

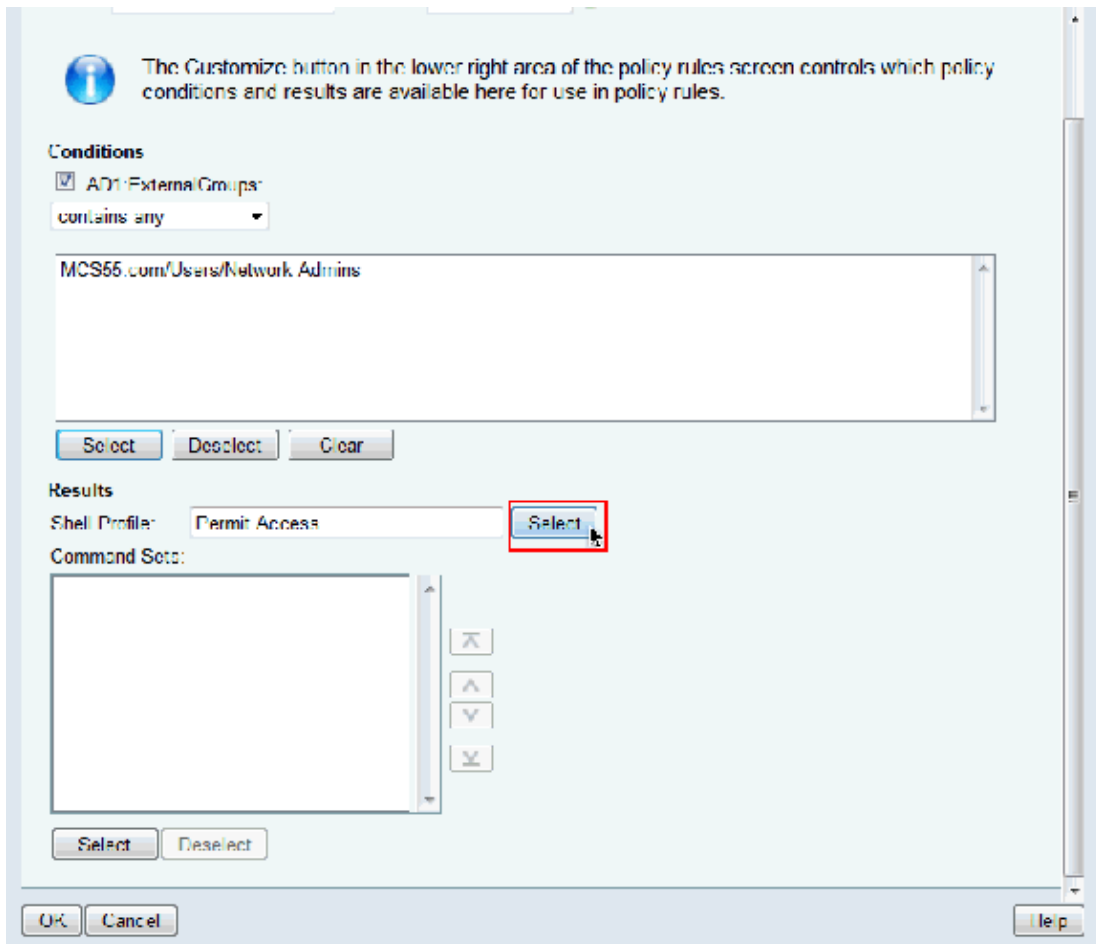
String Enum Definition Showing 1-2 of 2 50 per page Go

Filter: Match if: Go

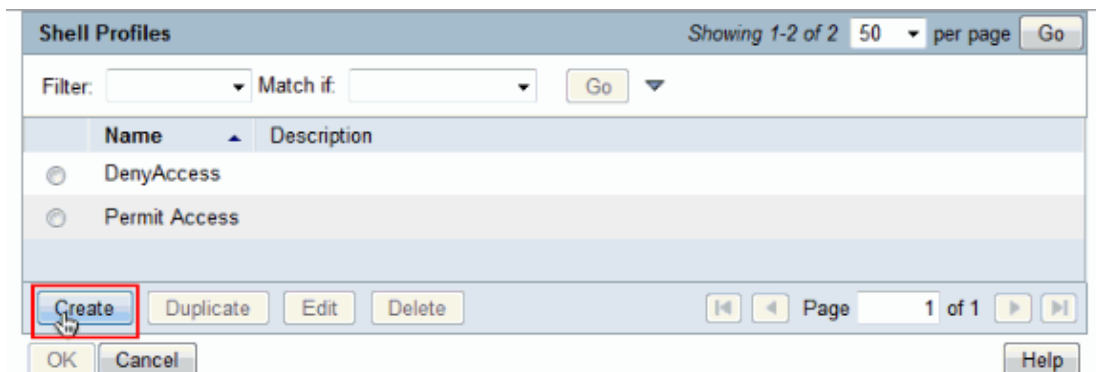
<input type="checkbox"/>	Enum Name
<input checked="" type="checkbox"/>	MCS55.com/Users/Network Admins
<input type="checkbox"/>	MCS55.com/Users/Network Maintenance Team

Page 1 of 1

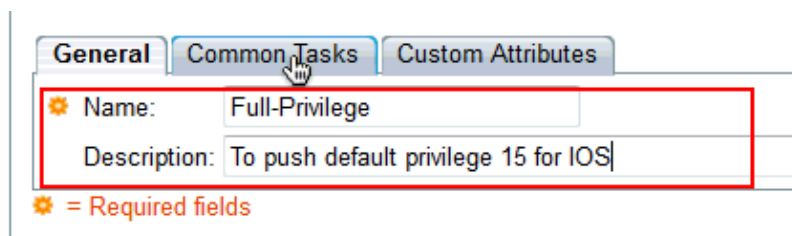
15. Click **Select** in the Shell Profile field.



16. Click **Create** in order to create a new **Shell Profile** for full access users.



17. Provide a **Name** and **Description**(optional) in the **General tab** and click on **Common Tasks** tab.



18. Change the **Default Privilege** and **Maximum Privilege** to **Static** with **Value 15**. Click **Submit**.

General **Common Tasks** Custom Attributes

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

⚙ = Required fields

Submit Cancel

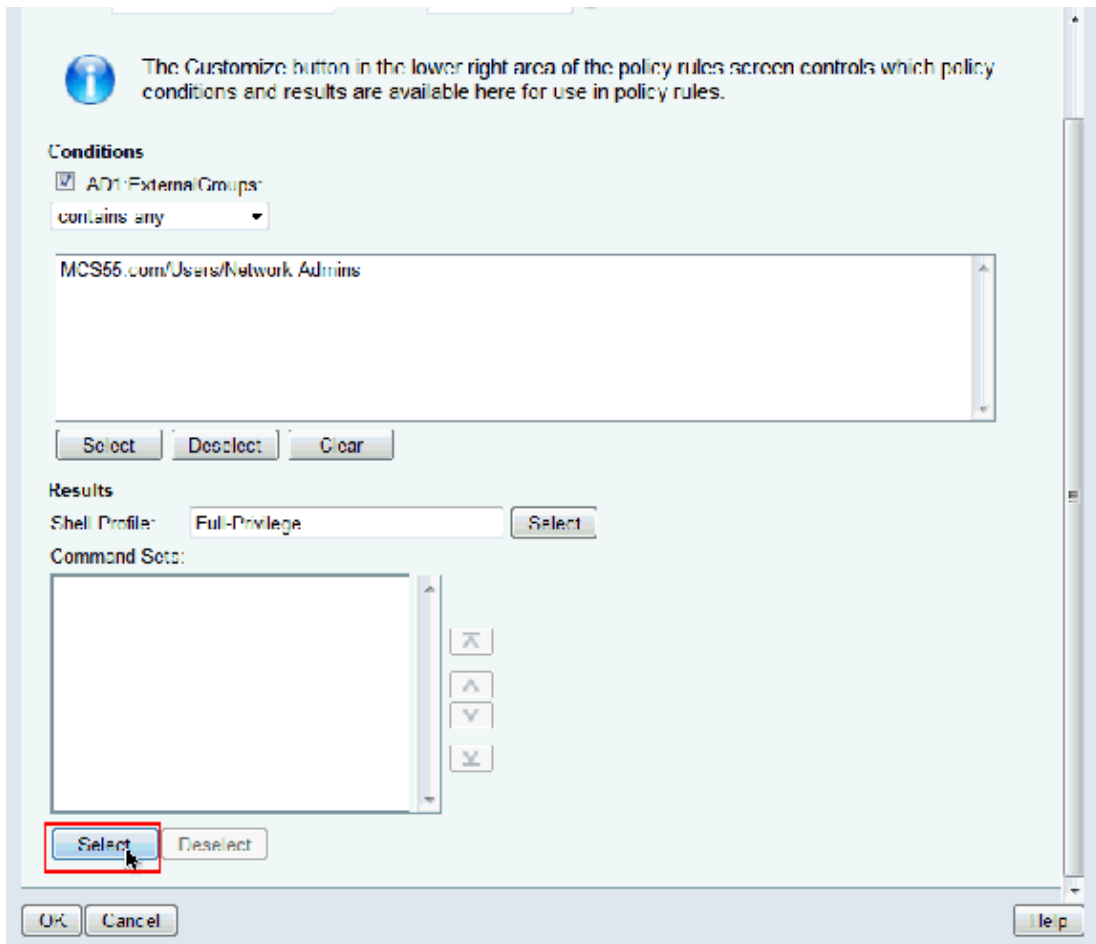
19. Now choose the newly created full access **Shell Profile** (Full-Privilege in this example) and click **OK**.

Shell Profiles

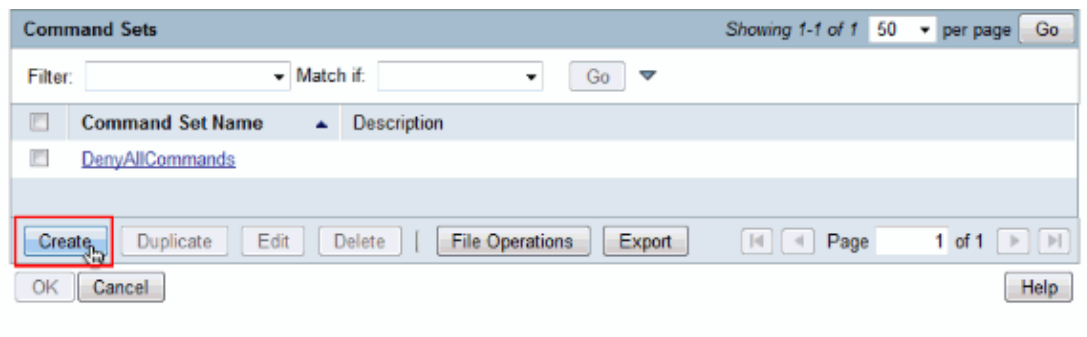
Filter: Match if:

Name	Description
<input type="radio"/> DenyAccess	
<input checked="" type="radio"/> Full-Privilege	To push default privilege 15 for IOS
<input type="radio"/> Permit Access	

20. Click **Select** in the Command Sets field.



21. Click **Create** in order to create a new **Command Set** for **Full-Access** users.



22. Provide a **Name** and ensure that the check box next to **Permit any command that is not in the table below** is checked. Click **Submit**.

Note: Refer to Creating, Duplicating, and Editing Command Sets for Device Administration for more information on Command Sets.

General

Name:

Description:

Permit any command that is not in the table below

Grant	Command	Arguments

Grant:
Command:
Arguments:

Select Command/Arguments from Command Set:

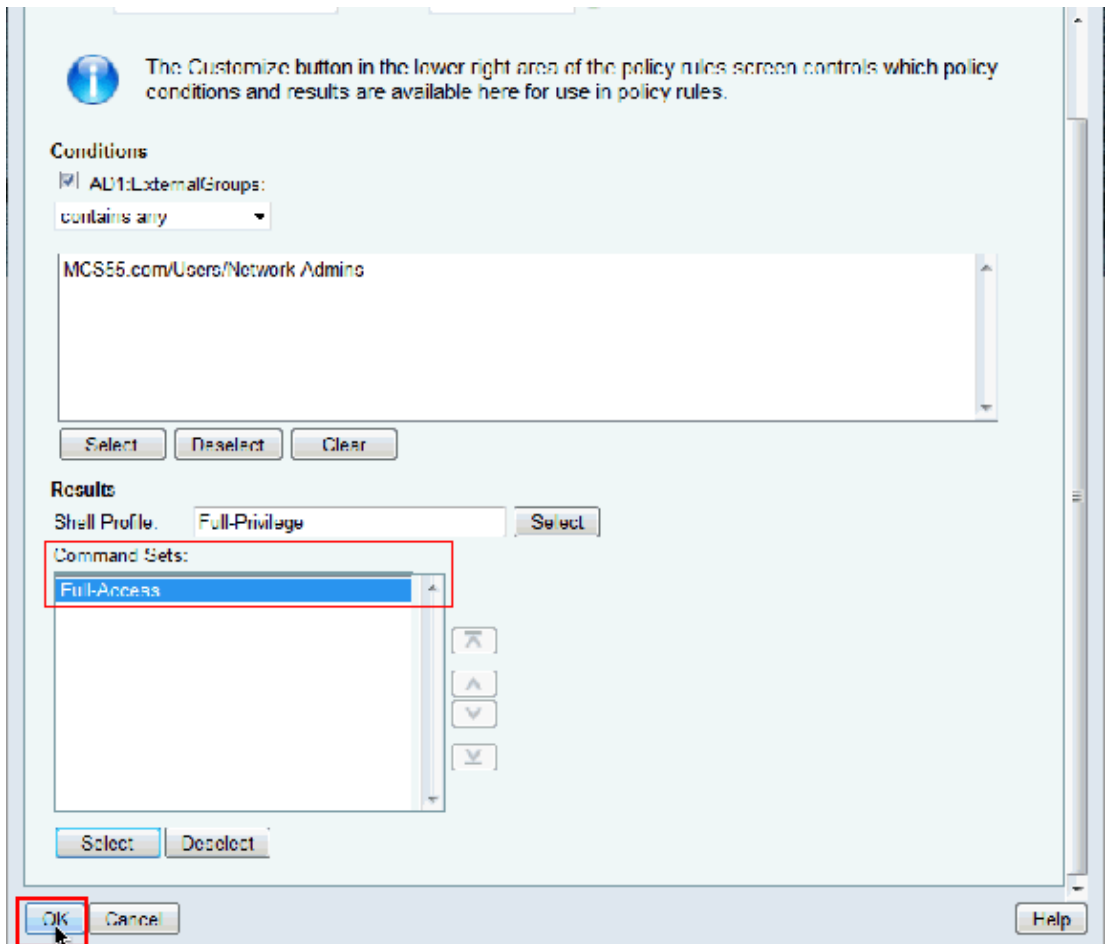
23. Click **OK**.

Command Sets

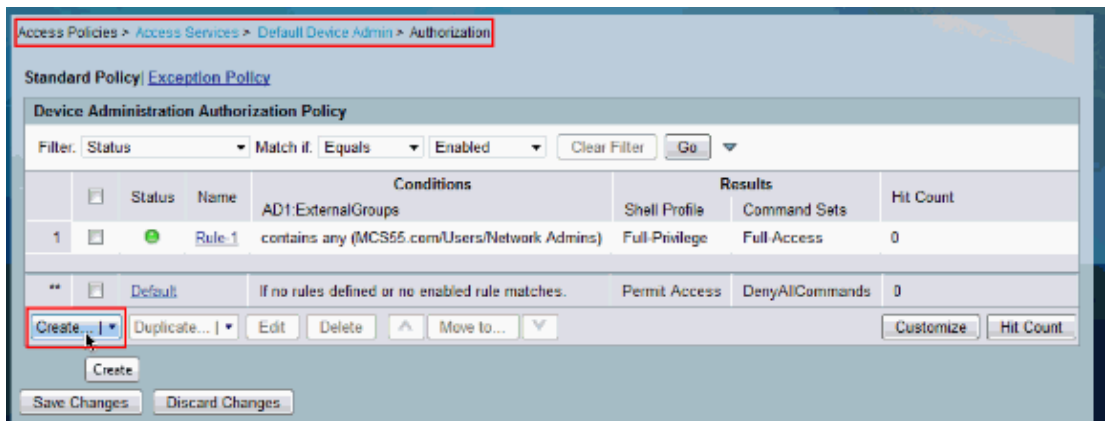
Filter: Match if:

<input type="checkbox"/>	Command Set Name	Description
<input type="checkbox"/>	DenyAllCommands	
<input checked="" type="checkbox"/>	Full-Access	

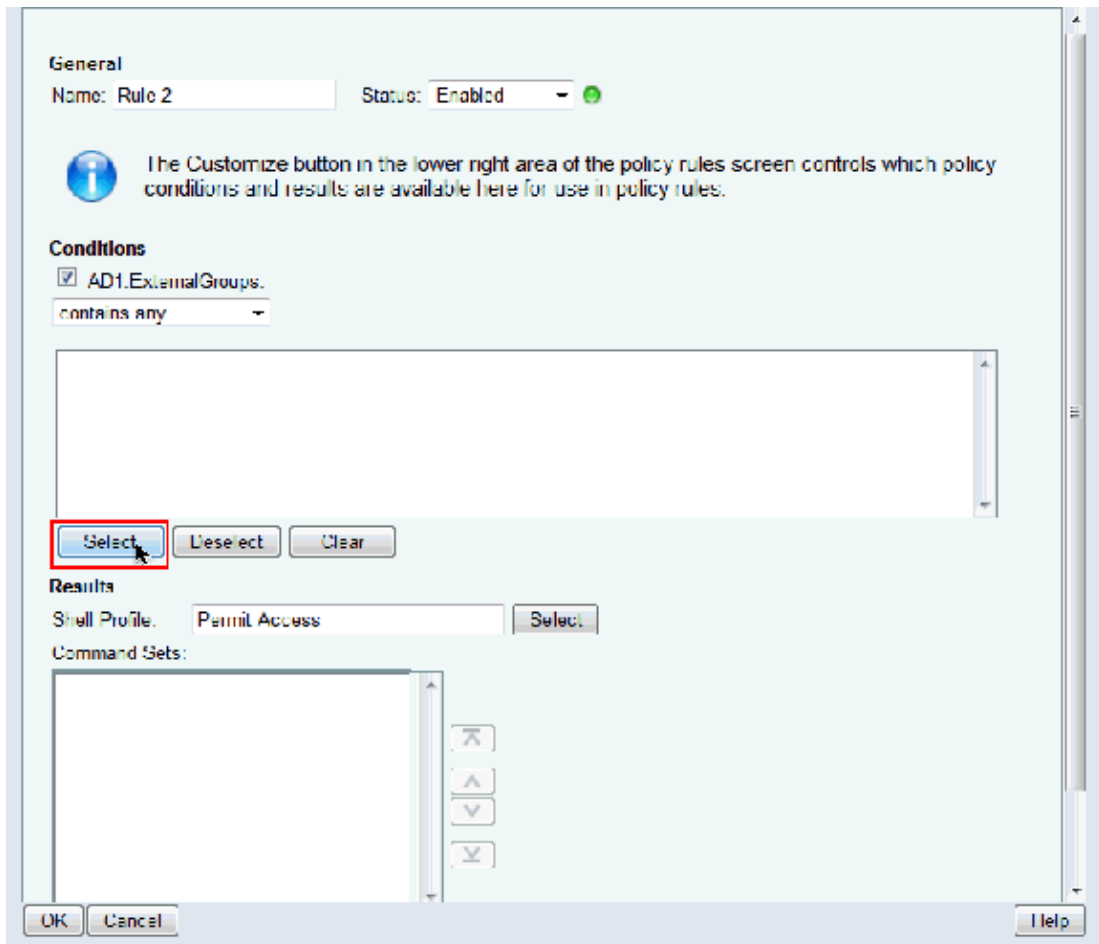
24. Click **OK**. This completes the configuration of **Rule-1**.



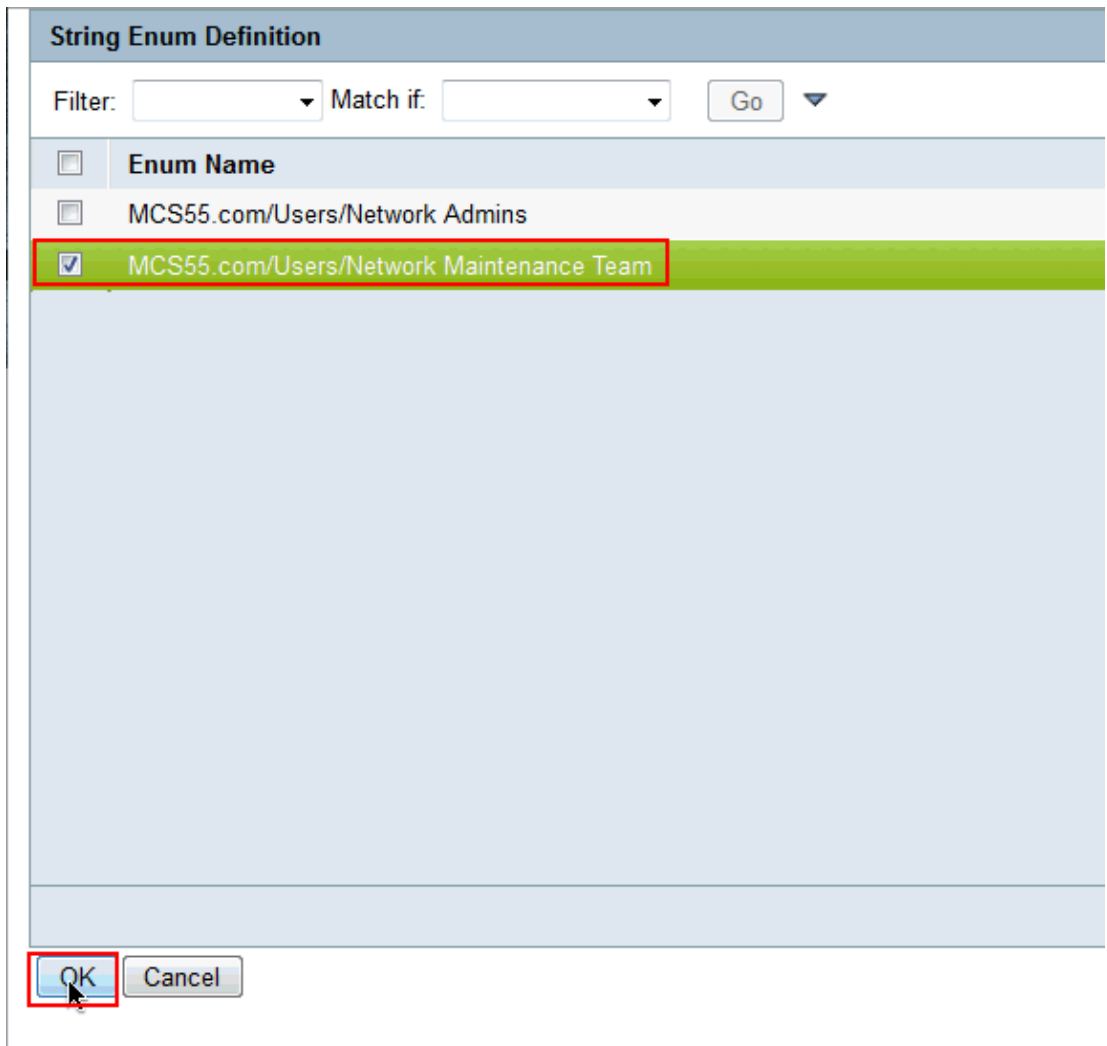
25. Click **Create** in order to create a new Rule for **limited** access users.



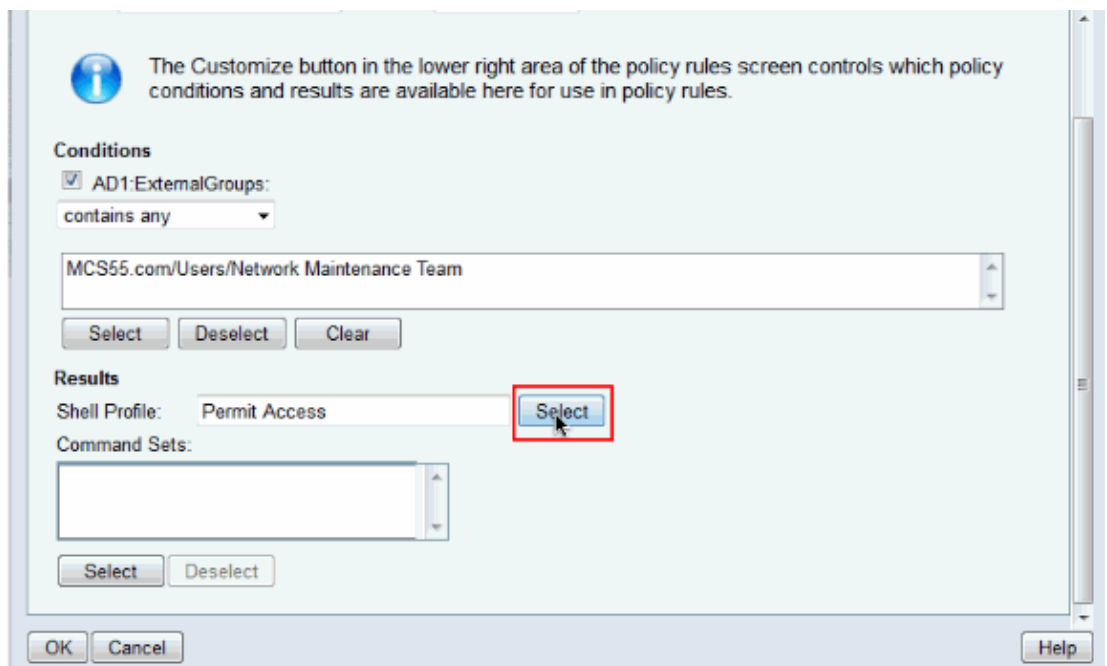
26. Choose **AD1:ExternalGroups** and click **Select**.



27. Choose the group (or) groups that you want to provide limited access to and click **OK**.



28. Click **Select** in the Shell Profile field.



29. Click **Create** in order to create a new **Shell Profile** for limited access.

Shell Profiles

Filter: Match if: ▼

	Name ▲	Description
<input type="radio"/>	DenyAccess	
<input type="radio"/>	Full-Privilege	To push default privilege 15 for IOS
<input type="radio"/>	Permit Access	

30. Provide a **Name** and **Description**(optional) in the **General** tab and click on **Common Tasks** tab.

General **Common Tasks** **Custom Attributes**

⚙ Name:

Description:

⚙ = Required fields

31. Change the **Default Privilege** and **Maximum Privilege** to **Static** with Values **1** and **15** respectively. Click **Submit**.

General **Common Tasks** Custom Attributes

Privilege Level

Default Privilege: Static Value 1

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

 = Required fields

Submit Cancel


32. Click **OK**.

Shell Profiles

Filter: Match if:

	Name	Description
<input type="radio"/>	DenyAccess	
<input type="radio"/>	Full-Privilege	To push default privilege 15 for IOS
<input checked="" type="radio"/>	Limited-Privilege	To push default privilege 1 for IOS
<input type="radio"/>	Permit Access	

33. Click **Select** in the Command Sets field.

 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

AD1:ExternalGroups:
contains any

MCS55.com/Users/Network Maintenance Team

Results

Shell Profile: Limited-Privilege

Command Sets:

34. Click **Create** to create a new **Command Set** for the limited access group.

Command Sets

Filter: Match if: Go

<input type="checkbox"/>	Command Set Name	Description
<input type="checkbox"/>	DenyAllCommands	
<input type="checkbox"/>	Full-Access	

|

35. Provide a **Name** and ensure that the checkbox next to **Permit any command that is not in the table below** is not selected. Click **Add** after typing **show** in the space provided in the **command** section and choose **Permit** in the **Grant** section so that only the show commands are permitted for the users in the limited access group.

General

Name:

Description:

Permit any command that is not in the table below

Grant	Command	Arguments

Grant:
Command:
Arguments:

Select Command/Arguments from Command Set:

36. Similarly add any other commands to be permitted for the users in limited access group with the use of **Add**. Click **Submit**.

Note: Refer to Creating, Duplicating, and Editing Command Sets for Device Administration for more information on Command Sets.

General

Name:

Description:

Permit any command that is not in the table below

Grant	Command	Arguments
Permit	show	
Permit	enable	
Permit	exit	

Grant: Command: Arguments:

Select Command/Arguments from Command Set:

37. Click **OK**.


Command Sets

Filter: Match if:

<input type="checkbox"/>	Command Set Name	Description
<input type="checkbox"/>	DenyAllCommands	
<input type="checkbox"/>	Full-Access	
<input checked="" type="checkbox"/>	Show-Access	

|

38. Click **OK**.

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

Conditions

AD1:ExternalGroups:
contains any

MCS55.com/Users/Network Maintenance Team

Select Deselect Clear

Results

Shell Profile: Limited-Privilege Select

Command Sets:
Show-Access

Select Deselect

OK Cancel

39. Click **Save Changes**.

Access Policies > Access Services > Default Device Admin > Authorization

Standard Policy | [Exception Policy](#)

Device Administration Authorization Policy

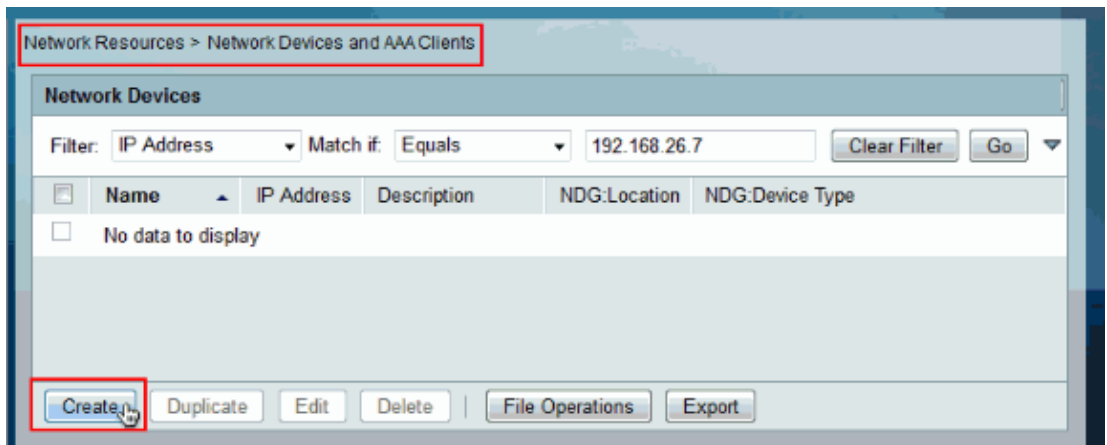
Filter: Status Match if: Equals Enabled Clear Filter Go

	Status	Name	Conditions	Shell Profile	Command Sets	Hit Count
1	<input checked="" type="checkbox"/>	Rule-1	contains any (MCS55.com/Users/Network Admins)	Full-Privilege	Full-Access	0
2	<input checked="" type="checkbox"/>	Rule-2	contains any (MCS55.com/Users/Network Maintenance Team)	Limited-Privilege	Show-Access	0
**	<input type="checkbox"/>	Default	If no rules defined or no enabled rule matches	Permit Access	DenyAllCommands	0

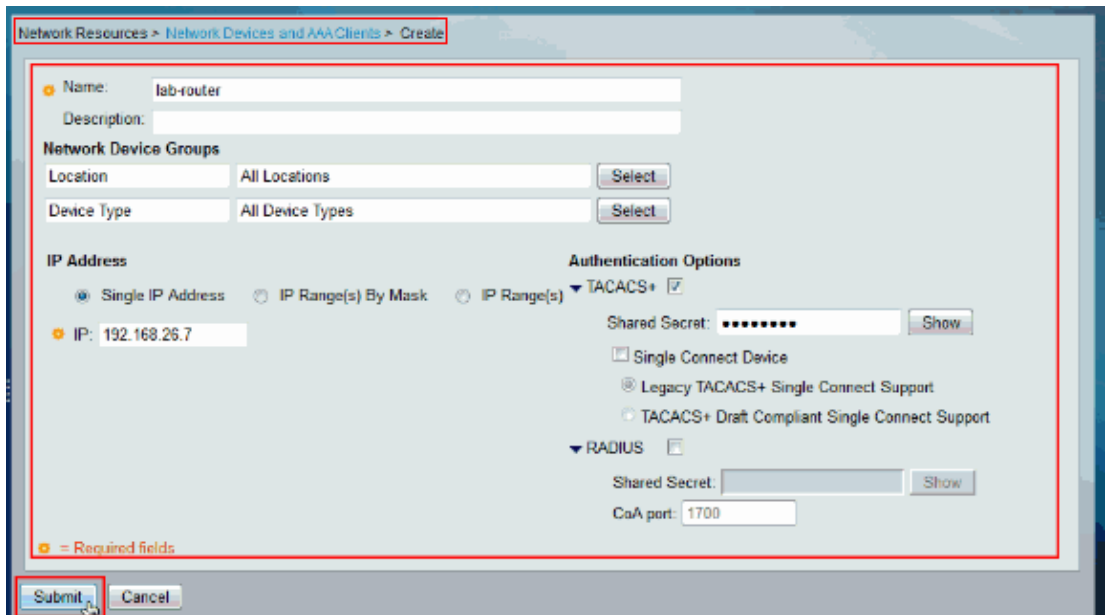
Create... Duplicate... Edit Delete Move to... Customize Hit Count

Save Changes Discard Changes

40. Click **Create** in order to add the **Cisco IOS** device as a **AAA Client** on the ACS.



41. Provide a **Name**, **IP Address**, **Shared Secret** for **TACACS+** and click **Submit**.



Configure the Cisco IOS device for Authentication and Authorization

Complete these steps in order to configure Cisco IOS device and ACS for Authentication and Authorization.

1. Create a local user with full privilege for fallback with the **username** command as shown here:

```
username admin privilege 15 password 0 cisco123!
```

2. Provide the IP address of the ACS in order to enable AAA and add ACS 5.x as TACACS server.

```
aaa new-model
tacacs-server host 192.168.26.51 key cisco123
```

- Note:** The key should match with the Shared-Secret provided on the ACS for this Cisco IOS device.
3. Test the TACACS server reachability with the **test aaa** command as shown.

```
test aaa group tacacs+ user1 xxxxx legacy
Attempting authentication test to server-group tacacs+ using tacacs+
User was successfully authenticated.
```

The output of the previous command shows that the TACACS server is reachable and the user has been successfully authenticated.

Note: User1 and password xxx belong to AD. If the test fails please ensure that the Shared–Secret provided in the previous step is correct.

4. Configure login and enable authentications and then use the Exec and command authorizations as shown here:

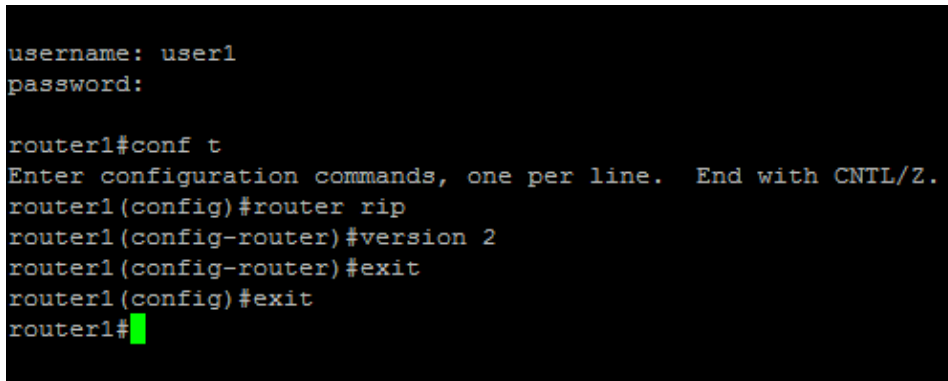
```
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authentication exec default group tacacs+ local
aaa authorization commands 0 default group tacacs+ local
aaa authorization commands 1 default group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
aaa authorization config-commands
```

Note: The Local and Enable keywords are used for fallback to the Cisco IOS local user and enable secret respectively if the TACACS server is unreachable.

Verify

In order to verify authentication and authorization login to the Cisco IOS device through Telnet.

1. Telnet to the Cisco IOS device as user1 who belongs to the full–access group in AD. Network Admins group is the group in AD which is mapped to Full–Privilege Shell Profile and Full–Access Command set on the ACS. Try to run any command to ensure that you have full access.



```
username: user1
password:

router1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
router1(config)#router rip
router1(config-router)#version 2
router1(config-router)#exit
router1(config)#exit
router1#
```

2. Telnet to the Cisco IOS device as user2 who belongs to the limited–access group in AD. (**Network Maintenance Team** group is the group in AD which is mapped to **Limited–Privilege Shell Profile** and **Show–Access Command set** on the ACS). If you try to run any command other than the ones mentioned in the Show–Access command set, you should get a Command Authorization Failed error, which shows that the user2 has limited access.

```

username: user2
password:

router1>enable
password:
router1#
router1#
router1#show version
Cisco IOS Software, C3550 Software (C3550-IPBASEK9-M), version 12.2(44)SE6, RELEASE S
OFTWARE (r6)
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Mon 09-Mar-09 20:26 by gereddy
Image text base: 0x00003000, data base: 0x00EAS3E8

ROM: Bootstrap program is C3550 boot loader

router1 uptime is 16 hours, 45 minutes
System returned to ROM by power-on
System image file is "flash:c3550-ipbasek9-mz.122-44.SEC.bin"

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/ww1/export/crypto/total/stiprg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

router1#conf t
Command authorization failed.

router1#wr mem
Command authorization failed.

router1#

```

3. Login to the ACS GUI and launch **Monitoring and Reports viewer**. Choose **AAA Protocol > TACACS+ Authorization** in order to verify the activities performed by user1 and user2.

ACS View Timestamp	ACS Timestamp	Status	Details	Failure Reason	User Name	Command Set	Shell Profile	Network Device
Jun 8 12 6 21 19:410 AM	Jun 8 12 6 21 19:393 AM	✓			user2	[Cisco]enable		lab-csr201
Jun 8 12 6 20 59:800 AM	Jun 8 12 6 20 59 799 AM	✗		11021 Command failed to match a Permit rule	user2	[Cisco]enable memory		lab-csr201
Jun 8 12 6 20 58:088 AM	Jun 8 12 6 20 58 893 AM	✗		11021 Command failed to match a Permit rule	user2	[Cisco]enable ipconfig terminal		lab-csr201
Jun 8 12 6 20 50:036 AM	Jun 8 12 6 20 50 036 AM	✓			user2	[Cisco]show version		lab-csr201
Jun 8 12 6 20 38:508 AM	Jun 8 12 6 20 38 490 AM	✓		Commands run by user 2	user2	[Cisco]enable		lab-csr201
Jun 8 12 6 20 34:425 AM	Jun 8 12 6 20 34 406 AM	✓			user2	[Cisco]=	Limited-Privilege	lab-csr201
Jun 8 12 6 20 02:616 AM	Jun 8 12 6 20 02 596 AM	✓			user1	[Cisco]enable		lab-csr201
Jun 8 12 6 20 00:269 AM	Jun 8 12 6 20 00 246 AM	✓		Commands run by user1	user1	[Cisco]enable 2		lab-csr201
Jun 8 12 6 19 57:203 AM	Jun 8 12 6 19 57 200 AM	✓			user1	[Cisco]router ip		lab-csr201
Jun 8 12 6 19 55:109 AM	Jun 8 12 6 19 55 076 AM	✓			user1	[Cisco]configure terminal		lab-csr201
Jun 8 12 6 19 42:745 AM	Jun 8 12 6 19 42 746 AM	✓			user1	[Cisco]=	Full-Privilege	lab-csr201

Related Information

- [Cisco Secure Access Control System](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jun 29, 2012

Document ID: 113590
