# Table of Contents

Preface ........................................................................................................................................1  

CVD Navigator .............................................................................................................................2  
  Use Cases .................................................................................................................................. 2  
  Scope ......................................................................................................................................... 2  
  Proficiency .................................................................................................................................. 2  

Introduction .................................................................................................................................3  
  Technology Use Case ................................................................................................................. 3  
    Use Case: Controlling Change to the Network Configuration ................................................ 3  
    Design Overview ....................................................................................................................... 3  

Deployment Details ......................................................................................................................5  
  Deploying Authentication and Authorization ............................................................................. 5  
  Limiting Access to Devices Based on the User Role ............................................................... 23  

Appendix A: Product List ...........................................................................................................27  

Appendix B: Changes ..................................................................................................................28
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](#).
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
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.
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

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.

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

<table>
<thead>
<tr>
<th>Group name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Helpdesk</td>
<td>Users who are allowed to log in to a device but not make changes</td>
</tr>
<tr>
<td>Network Admins</td>
<td>Users who are allowed to log in to a device and make changes</td>
</tr>
</tbody>
</table>

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

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, the switch authenticates the user against the locally stored username and password instead.

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.

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.

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.

Step 2: Enter the Microsoft Active Directory domain name and user credentials, and then click Join.
The status changes to Joined and Connected.

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

Step 5: Click Save Changes.

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.

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

<table>
<thead>
<tr>
<th>Profile name</th>
<th>Default privilege</th>
<th>Maximum privilege</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level1</td>
<td>1</td>
<td>15</td>
</tr>
<tr>
<td>Level15</td>
<td>15</td>
<td>15</td>
</tr>
</tbody>
</table>

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.

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.

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 /\**.

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.

![Identity Store Selection](image)

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.

![Group Mapping Selection](image)

**Step 7:** Click Submit.

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

**Step 9:** Select Rule based result selection.
Step 10: On the message that appears, click OK.

![Message dialog](image)

Step 11: Click Create.

Step 12: Select Compound Condition.

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

![Select attribute](image)

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

![External Groups](image)

Step 15: Under Value, click Select.

![Select value](image)
Step 16: Choose a Microsoft Active Directory group, and then click OK.

Step 17: Click Add V.

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

Step 19: Select Network Admins.
Step 20: Click OK, click OK again, and then click Save Changes.

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

<table>
<thead>
<tr>
<th>Name</th>
<th>In identity group</th>
<th>Shell profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Helpdesk</td>
<td>All Groups:Helpdesk</td>
<td>Level1</td>
</tr>
<tr>
<td>Network Admins</td>
<td>All Groups:Network Admins</td>
<td>Level15</td>
</tr>
</tbody>
</table>

Step 1: Navigate to Access Policies > Access Services > Default Device Admin > Authorization, and then click Create.
Step 2: Enter a name for the rule, and then select **Identity Group**.

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

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

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

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

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.

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

Step 11: Select DenyAccess, and then click OK.

Step 12: Click OK again.

Step 13: Click Save Changes.
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.

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

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

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.

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**.

![Image of Network Resources screen]

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.

![Image of Authorization screen]

**Step 3:** Click **Edit**.
Step 4: Select NDG:Device Type.

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.

Step 8: Click OK again, and then click Save Changes.
## Access Control

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Product Description</th>
<th>Part Numbers</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Services</td>
<td>ACS 5.5 VMware Software And Base License</td>
<td>CSACS-5.5-VM-K9</td>
<td>5.5 with Cumulative Patch 5.5.0.46.2</td>
</tr>
</tbody>
</table>
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.