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.
Network Device Authentication and Authorization Deployment Guide

SMART BUSINESS ARCHITECTURE

February 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 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.

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 2011 are the “August 2011 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 forum at the bottom of one of the following sites:

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

An RSS feed is available if you would like to be notified when new comments are posted.
Table of Contents

What’s In This SBA Guide .......................................................... 1
   About SBA ........................................................................ 1
   About This Guide ................................................................. 1

Introduction ................................................................. 2
   Business Overview ............................................................. 2
   Technology Overview .......................................................... 2

Deployment Details ............................................................ 3
   Deploying Authentication and Authorization .................. 3
   Limiting Access to Devices Based on the User Role ......... 19

Appendix A:
   Network Device Authentication and Authorization
   Deployment Guide Product List ........................................ 23

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.

© 2012 Cisco Systems, Inc. All rights reserved.
What’s In This SBA Guide

About SBA
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.

For more information, see the How to Get Started with Cisco SBA document:

About This Guide
This additional deployment guide includes the following sections:

- Business Overview—The challenge that your organization faces. Business decision makers can use this section to understand the relevance of the solution to their organizations’ operations.
- Technology Overview—How Cisco solves the challenge. Technical decision makers can use this section to understand how the solution works.
- Deployment Details—Step-by-step instructions for implementing the solution. Systems engineers can use this section to get the solution up and running quickly and reliably.

This guide presumes that you have read the prerequisites guides, as shown on the Route to Success below.

Route to Success
To ensure your success when implementing the designs in this guide, you should read any guides that this guide depends upon—shown to the left of this guide on the route above. Any guides that depend upon this guide are shown to the right of this guide.

For customer access to all SBA guides: http://www.cisco.com/go/sba
For 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. When the control and monitoring of change to the network configuration are done separately on each device, the number of devices can compound the difficulty and complexity.

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 are 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 5.2 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 repository 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 for the easy creation of 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, the rules can give network administrators enable-level access as soon as they log in and to limit helpdesk users to user-level commands only.
The following procedures outline the steps 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 5.2 license that you purchase is affixed as a sticky label to the bottom of the Software License Claim Certificate card included in your package.

Step 1: Carefully follow the instructions on this card to perform customer registration via the Internet. You must submit the PAK that you received to obtain valid license files for your system. For each PAK that you submit, a license file is generated and sent to you via email. You should save the license file to disk. You must install these license files when you set up Cisco Secure ACS.
Procedure 2  Set Up the Cisco Secure ACS Platform

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

```
**********************************************
Please type 'setup' to configure the appliance
**********************************************
```

localhost login: setup

Next, Setup takes you through a series of steps.

Step 2: Enter the platform login parameters as shown in the example below:

- Press ‘Ctrl-C’ to abort setup
- Enter hostname[]: acs
- Enter IP address []: 10.4.48.17
- 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. In the future, you can use these setup credentials to log in to the Cisco Secure ACS platform either via the console or SSH.

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
```

Time zone was modified. You must restart ACS.

Do you want to restart ACS now? (yes/no) YES

Step 4: Log in to Cisco Secure ACS via the GUI (https://<ACS_hostname>). The GUI login is a different account than the platform login you created during setup. Enter the default credentials: acsadmin/default. You will be prompted to change the password.

Step 5: Browse to the license file and click Install. The license installs.
**Procedure 3**  
**Enable 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**.

*Figure 1 - Example of configured default network device*

---

**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 will have enable-level EXEC access to the network devices when they log in, and helpdesk users will be required to type in the enable password on the device for that level of access.

<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>

Table 1 - Internal Groups

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

Step 2: Click **Create**.

*Figure 2 - Create internal identity store groups*
Step 3: Enter a name and description for the group (example: Network Admins).

Step 4: Click Submit.

Step 5: Repeat Steps 1 through 4 for each group you want to create.

**Figure 2 - Example identity groups**

---

**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 would require an exception is one associated to 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: Click Select.

Step 5: Select the radio 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 Steps 1 through 6 for each user account you want to create.
Procedure 6  Create an External Identity Store

Defining an external identity store allows designated users to authenticate against a network device by using their pre-existing credentials. You can also use attributes in the external store, such as group membership, 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.

Step 3: Click Save Changes. The Connectivity Status is CONNECTED.

Step 4: Click the Directory Groups tab.

Step 5: Click Select.

Step 6: 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.
Step 7: Click OK.

Step 8: Click Save Changes.

*Figure 4 - Example directory group configuration*
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 Sequence.

Step 2: Click Create.

Step 3: Enter a name and description for the identity store sequence. (Example: AD then Local DB)

Step 4: Select Password Based.

Step 5: Use the arrow buttons to move the AD1 and Internal Users identity store to the selected set for authentication and attribute retrieval.

Step 6: Use the arrow buttons to promote the AD1 identity store to the first item in the sequence.

Step 7: 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 log in, the other allows a user to log in but requires a separate device-level password for enable-level access.

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.

Step 4: Click the Common Tasks tab.

Step 5: From 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 the Value drop-down lists.

Next, you enable network administrators to login to WAAS devices as well as IOS devices.

Step 7: On the Level15 profile, click the Custom Attributes tab.

Step 8: In the Attribute box, enter waas_rbac_groups.

Step 9: In the Requirement list, choose Optional.

Step 10: In the Value box, enter Network Admins, and then click Add.

Step 11: Click Submit.

Step 12: Repeat Steps 1 through 5 for each shell profile in Table 2.
Figure 6 - Example shell profiles
Procedure 9  Map External Groups to Internal Groups

Mapping attributes (such as group membership) in the external identity store to attributes in the internal identity store reduces the number of authorization rules that are required. 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: Select AD then Local DB, and then click OK.

Step 4: Click Save Changes.


Step 6: Select Group Mapping.

Step 7: Click Submit.


Step 9: Select Rule based result selection.

Step 10: Review the warning message, and then click OK.
Step 11: Click Create.

Step 12: Select Compound Condition.

Step 13: Click Select.

Step 14: Select the condition attribute ExternalGroups.

Step 15: Click OK.

Step 16: Click Select.

Step 17: Choose a Microsoft Active Directory group.

Step 18: Click OK.
Step 19: Click Add V.

Step 20: To choose the internal identity group to which the Microsoft Active Directory group will map, click Select.

Step 21: Click the option button next to the internal identity group.

Step 22: Click OK, and then click OK again.

Step 23: Click Save Changes.

Step 24: Repeat Step 5 – 23 for the helpdesk group.
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 admin and helpdesk group members. Appropriate privilege levels are assigned via the same policy rules.

**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 > Device Default Admin > Authorization.

**Step 2:** Click Create.

**Step 3:** Enter a name for the rule.

**Step 4:** Select the Identity Group condition.

**Step 5:** Click Select.

**Step 6:** Click the option button next to the internal identity group.

**Step 7:** Click OK.
Step 8: Click the **Select** button next to Shell Profile to use if a user is part of the Internal Identity Group.

Step 9: Click the radio button next to the shell profile.

Step 10: Click **OK**.

Step 11: To save the rule, click **OK**.

Next, edit the default rule,

Step 12: Click **Default**.

Step 13: Click **Select**.
Step 14: Select DenyAccess.

Step 15: Click OK, and then click OK again.

Step 16: Repeat Steps 1 through 10 for each access policy rule.

Step 17: Click Save Changes.

Figure 7 - Example authorization policy rules
Limiting Access to Devices Based on the User Role

1. Create Network Device Type Groups
2. Create a Network Device
3. Modify Authorization Rules

This process configures Cisco Secure ACS to allow only network administrators to log in to security devices.

Procedure 1  Create Network Device Type Groups

This procedure creates a network device type group that will 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.

Step 4: Click Submit.

Procedure 2  Create a Network Device

This procedure defines a network device entry for each device that requires limited access 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: Click Select.

Step 5: Click the radio button next to the device type group.

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.
Procedure 3  Modify Authorization Rules

This procedure edits the existing authorization rule for helpdesk users. In this example, the rule prohibits logins to security devices.


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

Step 3: Click Edit.

Step 4: Select the NDG:Device Type check box.

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

Step 6: Click Select.

Step 7: Click the radio button next to the device type group.
Step 8: Click OK, and then click OK again.

Step 9: Click Save Changes.

Figure 9 - Example authorization rules
## Appendix A: Network Device Authentication and Authorization Deployment Guide Product List

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Product</th>
<th>Part Numbers</th>
<th>Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Management</td>
<td>Cisco Access Control System</td>
<td>CSACS-5.2-VM-K9</td>
<td>5.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ACS 5.2 VMWare Software and Base License</td>
<td></td>
</tr>
</tbody>
</table>