ılıılı cısco

Deployment Guide

Cisco Virtual Office—AAA Deployment with Cisco Secure Access Control Server 5

Deployment Guide

August 2011

Contents

Introduction	
Cisco Secure ACS Version 5 Overview	
Standalone Appliance Cisco Secure ACS Version 5 Graphical User Interface	
Cisco Secure ACS Version 5 Configuration for Cisco Virtual Office	
Installing a Certificate	
Migration from Cisco Secure ACS 4.x to 5.x (Optional)	
Setting Up Network Devices	
Adding User Groups	
Adding New Users	
Creating Authorization Policies	
Access Policies	
802.1x Configuration for EAP-TLS (Certificate Authentications)	
Wireless and SDP Profiles	
Resources	

Introduction

This deployment guide provides information on how to set up the Cisco[®] Secure Access Control Server (ACS) Version 5 for the Cisco Virtual Office solution. This guide uses screenshots taken from Cisco Secure ACS 5.2, but steps for deployment, as well as the interface, are similar for any Cisco Secure ACS Version 5.x. This guide will refer to Cisco Secure ACS Version 5 or Cisco Secure ACS 5.x to include all releases within Version 5.

Please refer to the Cisco Virtual Office overview (<u>http://www.cisco.com/go/cvo</u>) for more information about the solution, its architecture, and all the related components. For a more thorough explanation of Cisco Secure ACS 5.x, please refer to the user guide at:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.2/user/guide/acsuserguide.ht ml

Cisco Secure ACS Version 5 Overview

The new Cisco Secure Access Control Server is an improved way to perform authentication, authorization, and accounting (AAA). The Cisco Secure ACS Version 5 is more granular to allow greater flexibility in authentication. Users authenticate against rules created by administrators. These rules contain conditions such as time and date, group the user is in, and even the group the device is in.

Cisco offers two installation options for Cisco Secure ACS Version 5: a dedicated standalone appliance and a VMware ESX image. Their requirements follow:

Standalone Appliance

- ACS 1121 Appliance: Intel Xeon @ 2.66 GHz, (Quad Core), 4-GB memory, 500-GB hard drive (2 x 250 GB)
- VMware Requirements: VMware ESX 3.5 or 4.0; Intel Core 2 @ 2.13 GHz; 4-GB memory, Minimum 512-GB hard drive

Cisco Secure ACS Version 5 Graphical User Interface This section discusses the Cisco Secure ACS Version 5 GUI.

Figure 1 shows the My Workplace tab of Cisco Secure ACS Version 5. This window is displayed after you log into the Cisco Secure ACS GUI. The content of the My Workplace tab is shown in the main window of the ACS GUI. The tabs on the left are for configuration.





Figure 2 shows the Network Resources tab, which includes the Network Device Groups, where devices that are allowed to use the AAA for authentication of users are listed.



Figure 2. Network Resources

Figure 3 shows the Users and Identity Stores tab, where users and devices can be created. Users can also be imported from LDAP or Microsoft Active Directory.

🕹 Cisco Secure ACS - Mozilla Firefox Eile Edit View History Bookmarks Tools Help 🔇 🔊 🔹 😋 📉 🏠 🚺 stealth-acs5 Search Bookmarks and History - Soogle P 🔒 ÷ tisco Secure ACS cisco Cisco Secure ACS acsadmin stealth-acs5 (Primary) Log Out About Help 🕨 😚 My Workspace Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles ▶ 🎲 Network Resources **Authorization Profiles** Showing 1-3 of 3 50 💌 per page 😡 👻 🎒 Users and Id Filter: 🖌 🚺 🗢 👻 Match if: Identity Groups . Internal Identity Stores Name - Description Users IP-Phone-Profile To Authorize IP phone Hosts Permit Access External Identity Stores LDAP Active Directory RSA SecurID Token Servers RADIUS Identity Servers Certificate Authorities Certificate Authentication Profile Identity Store Sequences Solicy Elements Access Policies ▶ 📄 Monitoring and Reports 🕨 🍓 System Administration Create Duplicate Edit Delete 14 🔍 Page 1 of 1 💽 🕅 Done

Figure 3. Users and Identity Store

Figure 4 shows the Policy Elements tab; policy elements are used to create conditions that users have to meet in order to be given privileges.





Figure 5 shows the Access Policies tab; access policies are used to create rules. The rules are created using the condition in the Policy Elements tab.



Figure 5. Access Policies

Figure 6 shows the Monitoring and Reports tab. Click **the Launch Monitoring & Report Viewer** tab to open a new window that has logging and monitoring capabilities.



Figure 6. Monitoring and Reports

Figure 7 shows the Monitoring window, which gives information on alarms, reports, and pass/failed authentication attempts.





Figure 8 shows the System Administration tab. This tab contains configuration options to manage the system, operation configurations, logging configuration, and licensing.



Figure 8. System Administration

Cisco Secure ACS Version 5 Configuration for Cisco Virtual Office

The Cisco Secure Access Control Server (ACS) requires configuration upon installation for proper functioning. The following section details the configuration required to interoperate with Cisco Virtual Office. If ManageExpress Virtual Office (MEVO) software is used, this ACS configuration should be done before configuration of MEVO.

Installing a Certificate

Most of the EAP protocols require the use of a certificate to authenticate the ACS server. In Cisco Virtual Office, 802.1x and wireless authentication use EAP protocols, and installation of a certificate on the ACS is required.

Multiple certificates can be installed in Cisco Secure ACS Version 5. Figure 9 shows where to install the certificate: Go to System Administration \rightarrow Local Server Certificates \rightarrow Local Certificates and click Add.

🥹 Cisco Secure ACS - Mozilla Firefox								
<u>File Edit View History Bookmarks Too</u>	ls <u>H</u> elp							
🔇 🛛 🗸 C 🗙 🏠 🔤 stealt	n-acs5 http	s://stealth-acs5/acsadr	min/				습 - 🚷 -	Google 🔎 🔝
dua Cisco Secure ACS	4							-
cisco Cisco Secure A	CS					acsadmin s	tealth-acs5 (Primary)	Log Out About Help
🕨 🚭 My Workspace	System A	dministration > Configu	ration	> Local Server Ce	ertificates > Local Certific	ates		
Network Resources	Local	Certificates					Showing 1-2 of 2 50	🗸 per page 🛛 🖌
Boliny Elements	Filter:		~	Match if:	Go] ▼		
Control Policy Elements Access Policies		Friendly Name	*	Issued To	Issued By	Valid From	Valid To (Expiration)	Protocol
Monitoring and Reports		stealth-acs5		stealth-acs5	stealth-acs5	12:50 09.01.2010	12:50 09.01.2011	Managemer
🔹 💐 System Administration		stealthacs5		stealthacs5	beta-ca.cisco.com	02:28 05.03.2010	02:38 05.03.2011	EAP
Internal Hosts Local Server Certificates Local Certificates Outstanding Signing Requests Log Configuration Remote Log Targets Local Log Target Logging Categories Global Per-Instance Log Collector Log Message Catalog Licensing Downloads								
Migration Utility	<		~		101			>
User Change Password Sample Python Scripts	Add	Edit Delet	e	Export			Page	1 of 1 🕨 📕
Done								🔒 .a

Figure 9. System Administration Local Certificates

Select Generate a Certificate Signing Request, and click **Next**, as shown in Figure 10.

Figure 10. Generate Certificate Request



Fill in the Certificate Subject box and select the key length, as shown in Figure 11. The Certificate Subject should contain at least the parameter "CN", which is the common name or hostname of the ACS server.

The Key Length should be at least 1024 bits long.

Click Finish.

A window will pop up to download a text file with the certificate request. Use this certificate request to generate a new certificate.

If you are using Microsoft Certificate Authority, go to <u>http://IP_Certificate_Authority/certsrv</u> and go to **Request a Certificate** -> Advanced Certificate Request. Copy and paste the certificate request and click Submit. Then download the certificate.

For other certificate authorities, please refer to the specific documentation for that certificate authority.

Figure 11. Certificate Parameters

🕹 Cisco Secure ACS - Mozilla Firefox		
Eile Edit Yiew History Bookmarks Tools Help		
🚱 🕞 C 🗶 🏠 🚈 steakth-acs5 https://steakth-acs5/acsadmin/	☆ - 🚼 -	Google 🔎 🔒
dens Cisco Secure ACS		-
cisco Secure ACS	nin stealth-acs5 (Primary)	Log Out About Help
F 🖓 My Workspace System Administration > Configuration > Local Server Certificates > Local Certificates > Create		
▶ 😓 Network Resources		
Select server certificate creation method Generate Certificate Signing Requir Select server certificate creation method	est	
Step 2 - Generate Certificate Signing Request		
Construct Continued C		
Fin Monitoring and Reports CN=		
👻 👷 System Administration 🧧 Key Length: 1024 💌		
Internal Hosts Digest to Sign with: SHA1		
▼ Local Server Certificates		
Local Certificates		
Utstanding Signing Requests		
Remote Log Targets		
Local Log Target		
Logging Categories		
Per-Instance		
Log Collector		
Log Message Catalog		
Licensing Downloade		
Migration Utility		
User Change Password	Back	Einish Cancel
Sample Python Scripts	Datk	
Done		∂ ,:

Retrieve the certificate from the certificate authority.

After the certificate is downloaded, go to System Administration \rightarrow Local Certificates \rightarrow Bind CA Signed Certificate, and select Next, as shown in Figure 12.

Figure 12. Bind CA Signed Certificate



Select Browse and choose the certificate that was downloaded.

Check the appropriate protocols in the Protocol section; the certificate will be used for those protocols selected.

As shown in Figure 13, for certificate-based user authentication, select the EAP option.



Figure 13. Upload Certificate

Click **Finish** to complete the certificate installation. Click **Local Certificates** on the left again, and make sure the certificate appears under Local Certificates and is in a valid state.

Migration from Cisco Secure ACS 4.x to 5.x (Optional)

This section discusses the migration from Cisco Secure ACS Version 4 to Cisco Secure ACS Version 5.

Migration can be done **only** if the original Cisco Secure ACS Version 4 is installed on a Microsoft Windows server. If the original ACS is purchased as an appliance, then the database must first be replicated to an ACS running on a Microsoft Windows server. The ACS installed on the Microsoft Windows Server must also match the ACS version installed on the appliance.

To begin migration, you need the migration tool. From the Microsoft Windows server installed with the original Cisco Secure ACS Version 4, open a browser and log into the Cisco Secure ACS Version 5 GUI; e.g., <u>https://acs5</u>.

Go to System Administration \rightarrow Downloads \rightarrow Migration Utility, as shown in Figure 14.

Click Migration application files.

Figure 14. Migration Utility Download



The file will be downloaded as a zip file. After the download, extract the content in the zip file to a local directory.

When the file is unzipped, the folder named Migration will be created. Within the Migration folder are four folders: bin, config, jre, and lib. Inside the folder bin is a file called migration.bat, which is the tool you use for migration from 4.x to 5.x.

Note: Do not use remote desktop. Migration tool will fail.

Use VNC or, while directly using the Windows server, open a Windows command prompt. From the command prompt, change directories to the bin folder. When you are inside the bin folder, type "migration.bat" (without the quotes) and click **Enter** to execute the migration tool.

Following are the steps to use the Migration Utility.

First, export the data from the Cisco Secure ACS 4.0:

```
Copyright (c) 2008-2009 Cisco Systems, Inc.
All rights reserved.
_____
               _____
This utility migrates data from ACS 4.x to ACS 5. You can migrate directly from
the following ACS versions:
- ACS 4.1.1.24
- ACS 4.1.4
- ACS 4.2.0.124
- ACS 4.2.1
Data migration involves the following:
a. The migration utility analyzes the ACS 4.x data, exports any data from ACS 4.x
that can be migrated automatically, and imports the data into ACS 5.
b. Before the import stage, you can manually consolidate and resolve data
according to the analysis report, to maximize the amount of data that the utility
can migrate.
c. After migration, use the imported data to recreate your policies in ACS 5.
   _____
_____
Make sure that the database is running.
Enter ACS 5 IP address or hostname:[nn.nn.nnn]
Enter ACS 5 administrator username: [test]
Enter ACS 5 password:
Change user preferences?[no]
no
Show full report on screen?[yes]
ves
_____
Select the ACS 4.x Configuration groups to be migrated:[1]
1 - ALLObjects
2 - AllUsersObjects
3 - AllDevicesObjects
4 - SharedCommandSet
5 - SharedDACLObject
6 - MasterKeys
7 - SharedRACObjectWithVSA
_____
1
  _____
The following object types will be extracted:
_____
User Attributes
User Attribute Values
Network Device Groups
User Groups
```

```
Groups Shell Exec
Groups Command Set
Users Shell Exec
Users Command Set
Shared Command Sets
Network Device
Users
Shared Downloadable ACL
EAP FAST - Master Keys
MAB
_____
Choose one of the following:
1 - AnalyzeAndExport
2 - Import
3 - CreateReportFiles
4 - Exit
             -----1
```

Do not close the window after this step.

The next step is to import the data into Cisco Secure ACS Version 5.

Continuing from the previous session, choose option 2 to import the data into Cisco Secure ACS Version 5:

```
2
Tue Jul 20 14:57:00 EST 2007 Network Device Group 1 / 3 (33%) complete.
Tue Jul 20 14:57:00 EST 2007 Network Device Group 2 / 3 (66%) complete.
Tue Jul 20 14:57:00 EST 2007 Network Device Group 3 / 3 (100%) complete.
Imported 3 items of type: Network Device Group
Imported 2 items of type: User Group
Tue Jul 20 14:57:02 EST 2007 Group Shell Exec 1 / 1 (100%) complete.
Imported 1 items of type: Group Shell Exec
Tue Jul 20 14:57:03 EST 2007 Group Command Set 1 / 1 (100%) complete.
Imported 1 items of type: Group Command Set
Imported 0 items of type: User Shell Exec
Imported 0 items of type: User Command Set
Tue Jul 20 14:57:06 EST 2007 Shared Command Set 1 / 2 (50%) complete.
Tue Jul 20 14:57:24 EST 2007 Shared Command Set 2 / 2 (100%) complete.
Imported 2 items of type: Shared Command Set
Tue Jul 20 14:57:25 EST 2007 User 1 / 5 (20%) complete.
Tue Jul 20 14:57:25 EST 2007 User 2 / 5 (40%) complete.
Tue Jul 20 14:57:25 EST 2007 User 3 / 5 (60%) complete.
Tue Jul 20 14:57:25 EST 2007 User 4 / 5 (80%) complete.
Tue Jul 20 14:57:26 EST 2007 User 5 / 5 (100%) complete.
Imported 5 items of type: User
Tue Jul 20 14:57:26 EST 2007 Network Device 1 / 6 (16%) complete.
Tue Jul 20 14:57:27 EST 2007 Network Device 2 / 6 (33%) complete.
```

Tue Jul 20 14:57:28 EST 2007 Network Device 3 / 6 (50%) complete. Tue Jul 20 14:57:28 EST 2007 Network Device 4 / 6 (66%) complete. Tue Jul 20 14:57:29 EST 2007 Network Device 5 / 6 (83%) complete. Tue Jul 20 14:57:29 EST 2007 Network Device 6 / 6 (100%) complete.

Then you can create a report to confirm the migration:

```
3
               _____
Import Report
_____
The following User Attributes were not imported:
1. Name: Real Name Comment: Attribute cannot be added.4-37 Migration Guide for
the Cisco Secure Access Control System 5.1 OL-19125-01 Chapter 4 Migrating Data
from ACS 4.x to ACS 5.1 Migrating Multiple Instances
2. Name: Description Comment: Attribute cannot be added.
The following Network Device Groups were not imported:
  _____
1. Name: Not Assigned Comment: Error 1: Failure to add object: Migrated NDGs:All
Migrated NDGs:Not Assigned in function: createGroup
The following User Groups were not imported:
      _____
1. Name: IdentityGroup:All Groups:Migrated Group Comment: Failure to add object:
IdentityGroup:All Groups:Migrated Group in function: createGroup
The following Group Shell Exec were not imported:
_____
1. Name: ACS_Migrate_Priv Comment: customError CRUDex002 Object already exist
exception
The following Group Command Set failed on import:
_____
The following User Shell Exec were not imported:
_____
The following User Command Set were not imported:
_____
The following Shared Command Set were not imported:
_____
The following Network Devices were not imported:
_____
The following Users were not imported:
_____
The following Shared Downloadable ACL were not imported:
_____
The following EAP FAST - Master Keys were not imported:
_____
The following Mab were not imported:
```

After you finish this process, the database should be migrated from Cisco Secure ACS 4.0 to Cisco Secure ACS Version 5.

Setting Up Network Devices

The Network Resources section is used to categorize and group network devices that will be sending authentication, authorization, and accounting (AAA) requests to the ACS.

The Network Resources tab is where network devices and AAA clients are added, as shown in Figure 15. To add a network device or an AAA client, click **Create**.



Figure 15. Network Resources Tab

To add a network device, go to the Network Resources tab and select Network Devices and AAA clients. Figure 16 shows what is required to add a new Network Device. After entering the name of the Device/AAA client, select an option under Authentication options. Cisco Virtual Office is configured for RADIUS; select that option and enter the shared secret.

Cisco Secure ACS - Mozilla Firefox					
Eile Edit View History Bookmarks Tool:	s <u>H</u> elp				
🔇 🕗 📲 C 🗙 🏠 🔤 stealth	-acs5 https://stealth-acs5/acs	admin/		☆ + 🛃 -	Google 🔎 🔝
des Cisco Secure ACS	*				+
🔑 Do you want Firefox to remember the passwo	rd for "acsadmin" on https://ste	ealth-acs5?		Remember Never for This	s Site Now 🛛
cisco Cisco Secure Ad	CS		acsadmin	stealth-acs5 (Primary)	Log Out About Help
🕨 🖟 My Workspace	Network Resources > Netwo	ork Devices and AAA Clients > Create			
Network Resources Network Device Groups Location Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers Soft Device External Identity Stores Soft Device Servers Molicy Elements Access Policies Monitoring and Reports System Administration	Name: Description: Network Device Group: Location Device Type IP Address Single IP Addr P: P: Single IP Addr Single IP Addr Single IP Addr Cancel Submit Cancel	IS All Locations All Device Types ess IP Range(s)	Se Se Authentication Op ✓ TACACS+ Shared Secr Single C LegacyT TACACS ♥ RADIUS ♥ ♥ Shared Secre ▶ TrustSec	elect elect tions ret: ACACS+ Single Connect Sup (+ Draft Compliant Single Con et:	port nect Support
Done					🔒

Figure 16. Adding Network Resources Single IP Address

You can add either a single IP address or IP range(s) as network devices. The IP addresses included under the IP Address section are allowed as originating IP addresses for AAA. Adding an IP range will allow all devices within that IP range to submit an AAA request to the ACS. You can configure multiple subnets; you also can combine a single IP address and multiple subnets. Devices with IP addresses not specified in this section will be denied if they attempt to send an AAA request to the ACS.

You should add the IP address range that Cisco Virtual Office routers use and then click Submit.

Adding User Groups

Groups are logical divisions of Cisco Virtual Office users. Each group carries only three attributes: Name, Description, and Parent group, as shown in Figure 17.

Cisco Virtual Office supports two web authentication methods: Authentication Proxy and User Group Firewall.

First, go to **Users and Identity Stores** → **Identity Groups**.

For example, to create a group for Authentication Proxy, click **Create** and fill in the Name field with Authentication Proxy.

Fill in a Description as desired.

Leave the Parent field as All Groups.

Click Submit.

The name of the group has no effect on the function of the group, although descriptive names do help with monitoring. Repeat the process to create a group for User Group Firewall. Users will be added to the group later.

Figure 17. Creating a Group

🕲 Cisco Secure ACS - Mozilla Firefox	
Eile Edit View Higtory Bookmarks Iools Help	
🕜 🖂 👻 🏠 🔠 stealth-acs5 https://stealth-acs5/acsadmin/	🟠 🗝 🚮 🕶 Google 🛛 🔎 🎧
this Cisco Secure ACS +	
cisco Secure ACS	stealth-acs5 (Primary) Log Out About Help
GM Wy Workspace Users and Identity Stores > Identity Groups > Create	
Iterative Creation Image: Control of the control of	
Submit Cancel	4

Adding New Users

Cisco Secure ACS supports both internal and external databases. In the internal database, user credentials are stored locally on the ACS server. In the external database, user credentials can be stored on other supported servers; e.g., Microsoft Active Directory.

For the authentication mechanism to function properly, each Cisco Virtual Office user must be added to the ACS, either using the internal database or linked from an external database.

To set up an internal user, go to Users and Identity Stores, as shown in Figure 18. Click Create to create a user.

🕹 Cisco Secure ACS - Mozilla Firefox						
Eile Edit View History Bookmarks Ioo	ols <u>H</u> elp					
🔇 🖂 - C 🗙 🏠 📠 stealt	h-acs5 https://	/stealth-acs5	i/acsadmin/	☆ -	Google 🖇	
dire Cisco Secure ACS	÷					+
cisco Cisco Secure A	cs			acsadmin stealth-acs5 (Pri	mary) Log-Out About	Help
🕨 🧬 My Workspace	Users and Id	entity Stores	Internal Identity Stores > Users			
Network Resources	Internal	Users		Showing 1-50 of 151	50 🔽 per page 🛛 Go	1 🔺
Busers and Identity Stores Identity Groups	Filter:		👻 Match if: 🛛 👻 🔽 🐨			
 Internal Identity Stores 	S	tatus	User Name	Identity Group	Description	
Hosts		0	709f303bf3cdf0fdcb75f159454c21ce84e9c328	All Groups:iPhone VPN Pilot	helder	~
		0	881user.cisco.com	All Groups:Test Users	CVO Device	
LDAP Active Directory		Θ	aa19517b1826a23a63f6b450a6a5e560b2a72089	All Groups:iPhone VPN Pilot	michan2	
RSA SecurID Token Servers		Θ	<u>aarunkum</u>	All Groups:iPhone VPN Pilot		-
RADIUS Identity Servers		0	aelberse	All Groups:iPhone VPN Pilot		
Certificate Authorities Certificate Authentication Profile		0	aiith	All Groups:iPhone VPN Pilot		1
Identity Store Sequences		0	aksingha	All Groups:iPhone VPN Pilot		
Policy Elements		0	anuragn	All Groups: Phone VPN Pilot		
Access Policies		Θ	anvuser1	All Groups:802.1Xgroup		
Monitoring and Reports		0	arastogi	All Groups:iPhone VPN Pilot		
🖌 🍓 System Administration		Θ	asawani	All Groups:iPhone VPN Pilot		
		Θ	ауар	All Groups:iPhone VPN Pilot		
		0	b48b63415a1b4a9dd2516b1124838ab16a8e0ed8	All Groups:iPhone VPN Pilot	asawani test iPhone	
	Create	Dupi	cate Edit Delete Change Password	File Operations Expor	t III Page	~
Done						a

Figure 18. Adding a New User

Figure 19 shows the window to add a new user. In the General section are four fields: Name, Status, Description, and Identity Group.

Fill in the Name field as the username of the employee.

Check the Enabled status field to enable this account.

Check the appropriate Identity Group to associate the user with the group desired.

The Password Information section has five fields: Change password on next login, Password and a confirmation, and Enable Password and a confirmation.

Do not check the Change password on login check box; checking this box forces a change of password. The RADIUS/TACACS authentication request will be rejected.

Fill in the Password and Confirm Password fields for authentication.

The Enable Password and Confirm Password fields are used to authenticate the user when logging into a router. Leave these fields blank, because users do not usually have "enable" access to Cisco Virtual Office routers. Filling in an Enable Password field will not automatically allow access to the network device. An access policy will need to be created to specify if any user needs access to a network device.

To add a user as part of the Authentication Proxy group, fill in the username, leave the status as enable, and for Identity Group, click Select and choose Authentication Proxy from the pop-up window. Fill in the Password the user will be using in the authentication proxy. When all appropriate fields are filled in, click **Submit**.

🕘 Cisco Secure ACS - Mozilla Firefox		
Elle Edit View History Bookmarks Iools Help		
🔇 💴 🗸 🔬 🖾 stealth-acs5 https://stealth-acs5/acsadmin/	😭 🔻 😽 🛪 Google	P 🔒
tia Cisco Secure ACS 🔅		÷
cisco Secure ACS	stealth-acs5 (Primary) Log Out	About Help
► 😚 My Workspace Users and identity Stores > Internal identity Stores > Users > Create		
 Network Resources Status: Enabled Name: Status: Enabled Name: Status: Enabled Name: Status: Enabled Status: Enabled Select Description: Identity Stores LDAP Active Directory RADIUS Identity Servers Certificate Authorities Confirm Password: Change password on next login User Information There are no additional identity attributes defined for user records System Administration Submit Cancel 	rmation characters	
Done		🔒:

Figure 19. New User Attributes

You can also link the ACS to an external database for user credentials. LDAP, Active Directory, RSA SecurID Token Servers, and RADIUS Identity Servers are supported. Click each option and configure the connection appropriately to activate the external database.

Note: Only one Active Directory domain can be connected from the ACS.

Figure 20 shows an example of LDAP configuration.

Figure 20. LDAP External Identity Store

🔮 Cisco Secure ACS - Mozilla Firefox	
Eile Edit View Higtory Bookmarks Iools Help	
💽 🕞 🕈 😧 🔂 🚺 steaktr-acs5 🛛 🔶 🖓 - Google 🔎]
Jen: Cisco Secure ACS *	
acsadmin stealth-acs5 (Primary) Log Out About	Help
My WOrkspace Users and Identity Stores > External Identity Stores > LDAP > Edit: "Steath Team"	
 Network Resources Network Resources Sever Connection Directory Organization Directory Groups Directory Attributes Schema Subject Objectclass: Person @ Group Objectclass: GroupOfUniqueNames Subject Objectclass: Person @ Group Map Attribute: UniqueMember Subject Name Attribute: username @ Group Map Attribute: UniqueMember Subject Objects Contain Reference To Groups Subject Objects Contain Reference To Groups Group Objects Contain Reference To Subjects Group Objects Contain Reference To Subjects Subjects In Groups Are Stored In Member Attribute As: Username Subject Search Base: Our active,our employees,our employ	
Monitoring and Reports Group Search Base: ou=active.ou=employees.ou=people.o=cisco.com	
Register Administration	
Username Prefix/Suffix Stripping	
Strip start of subject name up to the last occurrence (e.g. if separator set to 1', subject name 'acme\smith'	
Submit Cancel	
Done	a

Creating Authorization Policies

This step is required if you are using authentication proxy, user group firewall, or PKIAAA.

After creating the user in the group, you must create an authorization profile. This profile ensure proper authorization parameters are passed back to the Cisco Virtual Office routers for the user to obtain proper authorization. Without proper authorization, any of the previously mentioned features will return a rejection.

Figure 21 shows the Policy Elements window. To create a new Authorization Profile, go to **Policy Elements** \rightarrow **Authentication and Permissions** \rightarrow **Network Access** \rightarrow **Authorization Profiles** and click **Create**.

😻 Cisco Secure ACS - Mozilla Firefox		
Eile Edit Yiew History Bookmarks Iool	; <u>H</u> elp	
🔇 🕗 C 🗙 🏠 🛄 stealth	acs5	→ - Google 🔎 🔝
dia Cisco Secure ACS		-
🖉 Do you want Firefox to remember the passwo	rd for "acsadmin" on https://stealth-acs5?	Remember Never for This Site Not Now
cisco Cisco Secure A	acsadmin	stealth-acs5 (Primary) Log Out About Help
🕨 🥳 My Workspace	Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles	
Network Resources	Authorization Profiles	Showing 1-3 of 3 50 💌 per page 😡
Users and Identity Stores	Filter: V Match if: 00 V	
Policy Elements	Name Description	
Date and Time	IP-Phone-Profile To Authorize IP phone	
 Network Conditions 	Permit Access	
End Station Filters Device Filters		
Device Port Filters		
 Authorization and Permissions Network Access 		
Authorization Profiles		
Security Groups Device Administration		
Shell Profiles		
Access Policies		
Monitoring and Reports		
🕞 🍓 System Administration	Create Duplicate Edit Delete	Page 1 of 1 > >
Done		

Figure 21. Policy Elements

Figure 22 shows the Create window. Give an appropriate name to the profile; e.g. authentication proxy, PKIAAA, or user group firewall.



🕹 Cisco Secure ACS - Mozilla Firefox			
<u>File E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> oo	s <u>H</u> elp		
🕜 🛛 🕶 C 🗙 🏠 🚺 stealtr	-acs5 Search Bookmarks and History	+ Google	P 🔒
tion Cisco Secure ACS	*		-
Do you want Firefox to remember the passwork	rd for "acsadmin" on https://stealth-acs5?	Remember Never for This Site	Not Now
cisco Cisco Secure A	acsadmin	stealth-acs5 (Primary) Log C	Dut About Help
🕨 🖓 My Workspace	Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Create	3	
Network Resources	Courset Courses Testes [BADIUC Attributes]		
Users and Identity Stores	General Common rasks Rabios aunoues		
👻 🦻 Policy Elements	Security Sec		
Session Conditions			
Date and Time Custom	🐱 = Requirea fields		
Network Conditions			
End Station Filters			
Device Priters Device Port Filters			
 Authorization and Permissions 			
Network Access			
Security Groups			
Shell Profiles			
Command Sets			Statistics of the
Maplicity and Departs			Statement of the
Monitoring and Reports			
🕨 🤘 System Administration	Submit Cancel		
Done			â

The Common Tasks tab is not important for the Cisco Virtual Office deployment.

For a Cisco Virtual Office deployment, the most relevant tab is the RADIUS Attributes. All the features rely on RADIUS attributes return to function properly.

For PKI-AAA, the RADIUS attribute required is: RADIUS-Cisco; cisco-av-pair; pki:cert-application=all.

The configuration is also shown for PKIAAA in Figure 23.

Figure 23. Authentication Profiles Common Tasks



For authentication proxy, the RADIUS attributes required follow:

- RADIUS-Cisco; cisco-av-pair; auth-proxy:priv-lv15
- RADIUS-Cisco; cisco-av-pair; auth-proxy:proxyacl#1=permit ip any any

For user-based firewall, the RADIUS attributes required follow:

- RADIUS-Cisco; cisco-av-pair; supplicant-group=group-engineer
- RADIUS-Cisco; cisco-av-pair; priv-lvl=15
- RADIUS-Cisco; cisco-av-pair; auth-proxy:priv-lvl=15
- RADIUS-Cisco; cisco-av-pair; auth-proxy:proxyacl#1=permit ip any any

Access Policies

This section ties the previously defined user group to the authorization policies to allow the association between a group of users and a particular authorization policy. The group of users can then be properly authorized for their activity within the boundary of the associated policy (e.g., authentication proxy, etc.)

To achieve authorization an authorization policy must be created for each group of users. Go to Access Policies \rightarrow Access Services \rightarrow Default Network Access \rightarrow Authorization, as shown in Figure 24.

🕙 Cisco Secure ACS - Mozilla Firefox					
Eile Edit View History Bookmarks Tools	Help				
🔇 🗵 🗸 C 🗙 🏠 🖾 stealth-	acs5 https://ste	alth-acs5/acsadmin/	(☆	🔹 🛃 🗝 in proxy radius 🔎 <table-cell></table-cell>
端 Cisco Secure ACS 🛛 🔯	date Cisco Secu	re ACS - Monitoring	and Rep 🔄 🔤 definition Implementing Authentication Proxy	- G 🖂 🛛 🛧	+
cisco Cisco Secure AC	08		acs	admin stealth-acs5 (P	rrimary) Log Out About Help
🕨 🧬 My Workspace	Access Policies	> Access Services	> LDAP test > Authorization		
🕨 🎲 Network Resources	Standard Pol	icyl Excention Dol	icy		
🕞 🍰 Users and Identity Stores	Network Ac	coss Authorizatio	n Policy		
Sp. Policy Elements		CC33 Hutton Zutt			
👻 🕵 Access Policies	Fliter: Estat	us	Match II: Equais 💽 Enabled 📡		
 Access Services ▲ El Service Selection Rules 		Status Name	Conditions Compound Condition	Results Authorization Profiles	Security Group Hit Count
 Ø 802.1x Identity Authorization O Default Device Admin Identity Authorization O Default Network Access Identity Authorization O LDAP test 		No data to displa	ay		
Identity	**	Default	If no rules defined or no enabled rule matches.	Permit Access	Unknown 0
TrustSec Access Control Fire Foress Policy Monitoring and Reports	Create -	Duplicate •	Edit Delete A Move to V		Customize Hit Count
🕨 🍓 System Administration	Save Chang	jes Discard C	hanges		
Done					≙ ,;;

Figure 24. Access Policies

Click **Create** at the bottom left. A pop-up window will appear, as shown in Figure 25.

Create a meaningful name under the section General; e.g. Authentication Proxy.

For the Cisco Virtual Office, check Identity Group under Conditions.

Click **Select** to the right and pick the policy that matches the user group, e.g. Authentication Proxy created earlier in this document. Then click **OK** to confirm.

Under Results, click Select and pick the appropriate Authorization Profiles. Click OK to confirm.

Finally click **OK** to close the pop-up window.

Figure 25. Creating Authorization Rule

🕹 Cisco Secure ACS - Mozilla Firefox			
Elle Edit View History Bookmarks Iools Help	Cisco Secure #CS - Mozilla Firefox		
🔇 🖂 + C 🗙 🏠 📠 stealth-acs5 http	staalth-arc5 https://stealth-arc5/arcadoin/PolicyInutAction.do	<u></u>	
🚓 Cisco Secure ACS 🛛 😹 🕬 Cisco		1	-
cisco Cisco Secure ACS	General Name: Authentication Proxy Status: Enabled 👽 \Theta		alp
Access P	The Customize button in the lower right area of the policy rules screen controls which		
Network Resources Standar			
Bigging Stores Set Stores Set Stores Set Store Set	Conditions		
Policy Elements Eilter	NDG:Location: -ANY-		
V 🛼 Access Policies	Time And Date: -ANY-		
Access Services El Service Selection Rules Ø 802.1x Identity Authorization Ø Default Device Admin Identity Authorization Ø Default Network Access Identity Authorization Ø Default Network Access Identity Authorization Ø LDAP test Identity Authorization TrustSec Access Control Creat	Identity Group: In All Groups Addrenitication Proxy Select Authorization Profiles: Authonization Proxy You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined. Select Deselect		
Erress Policy Monitoring and Reports System Administration	Done		

After the confirmation, you should have a rule that associates the user group to an appropriate authorization profile. Figure 26 shows an example of authentication proxy. The rule named Authentication Proxy associates the Authentication Proxy user group to the Authentication Proxy authorization profile.

Figure 26. Final Access Polices

🥹 Cisco Secure ACS - Mozilla Firefox								
Eile Edit View History Bookmarks Tool	Help							
🔇 💵 🕑 🗶 🏠 🎰 stealth	acs5 https://stealth-acs5/acsadmin/	😭 👻 🚼 🔪 in proxy radius 🔎 <table-cell></table-cell>						
dia Cisco Secure ACS 🛛 🛛 🛛	disco Cisco Secure ACS - Monitoring and Rep	. *						
acsadmin steatth-acs5 (Primary) Log Out About Help								
🕨 🧭 My Workspace	Access Policies > Access Services > Test2 > Authorization							
🕨 🎲 Network Resources	twork Resources Standard Deligni Europation Delign							
Busers and Identity Stores	Network Access Authorization Policy							
Policy Elements	Filter Statue	Filter Go V						
🔹 🛃 Access Policies								
 ✓ Access Services ▲ Service Selection Rules 	Status Name Status Name NDG:Location Time And Date Ide	is Results entity Group Authorization Pr						
▼ ● 802.1x	1 🦳 🥝 Authentication Proxy -ANYANY- in /	All Groups:Authentication Proxy Authentication P						
Authorization								
✓ O LDAP test	<u><</u>	<u> </u>						
Authorization	If no rules defined or no enabled rule r	natches. Permit Access						
TrustSec Access Control	Create Duplicate Edit Delete A Move to	Customize Hit Count						
Monitoring and Reports								
🕨 🍓 System Administration	Save Changes Discard Changes							
Done								

If multiple features are used, create more rules as appropriate. Figure 27 shows the case with both Authentication Proxy and PKIAAA in use. The order of the rules does not matter.

🕹 Cisco Secure ACS - Mozilla Firefox								
Elle Edit Yew Higtory Bookmarks Icols Help								
🌀 🕞 🕈 🖒 🕼 stealth-acs5 https://stealth-acs5/acsadmin/								
📾 Cisco Secure ACS 🛛 🛛	aste Ciso	o Secure	ACS - Mo	nitoring and Rep 🔯 🛛 🚦	ដ Implementing Au	hentication Proxy - (5i 🔝 🛛 🔶	
acsadmin steatth-acs5 (Primary) Log Out About Help CISCO CISCO Secure ACS								
🕨 😽 My Workspace	Ky Workspace Access Policies > Access Services > Test2 > Authorization							
🕨 🎲 Network Resources	Standa	rd Policy	d Excen	tion Policy				
Big Users and Identity Stores	Statual & Poincy <u>Exception Poincy</u>							
Sp. Policy Elements			33 HUU	u u u c				
👻 🛃 Access Policies	Filter:	Status		Match IT: Ec	luais 💌 En	abled 💌 🖸	aear Filter Go V	
 ★ Access Services ▲ Service Selection Rules 			Status	Name	NDG:Location	Con Time And Date	ditions Identity Group	Results Authorization Pr
	1		0	Authentication Proxy	-ANY-	-ANY-	in All Groups:Authentication F	Proxy Authentication P
Authorization	2		0	PKIAAA	-ANY-	-ANY-	in All Groups:PKIAAA	PKIAAA
	K T Creat	E	<u>Default</u> Duplica	te ▼] [Edit][Dele	iii If no rules defin te	ed or no enabled i	rule matches. Cu	Permit Access stornize Hit Count
System Administration	Save (Change		iscard Changes				
Done		-						<u></u>

Figure 27. Final Access Polices

802.1x Configuration for EAP-TLS (Certificate Authentications)

Simple 802.1x implementation produces an authentication request only. Because no authorization is taking place, it is not required for 802.1x users to be part of a specific group, or be assigned to a specific rule if rules and groups are already configured. The server accepts authentication requests by default.

802.1x allows two types of authentication: certificate or username/password.

To allow certificate authentication, first go to **Users and Identity Stores** \rightarrow **Certification Authentication Profile**. Make sure the attribute that stores the username in the X.509 certificate is present in the profile. For example, the common name (CN) is present as the username-storing attribute shown in Figure 28.

Note: This section is required only if you use 802.1x with EAP-TLS (certificate authentications). If you use only 802.1x username/password credentials authentication, skip this section.



Figure 28. Attribute in the X.509 Certificate that Stores the Username

Now add the newly defined authentication profile into the Default Access Service, so that both 802.1x certificatebased authentication and other standard authentication can function at the same time.

Go to Access Policies \rightarrow Access Services \rightarrow Default Network Access \rightarrow Identity. Single result selection should be checked on the right; change it to Rule-based result selection.

Your screen should look like Figure 29 after the change.

Figure 29. Access Policies Identity



You must create two rules in Identity to sufficiently serve both 802.1x certificate authentication and standard authentication methods. The first rule is shown in Figure 30.

The rule is triggered when an EAP-TLS (802.1x certificate) authentication request comes in, and the identity source is set to CN Username (the identity profile created earlier to match the attribute from the certificate to the user credentials store).



Figure 30. Rule to Allow 802.1x Certificate Authentications

Then also create a second rule for the standard authentication (Figure 31).



Figure 31. Rule for Standard Authentication

	• <u>U</u> +#	Cisco Secure ACS - Mozilla Firefox		6
	acs5 https	tealth-acs5 https://stealth-acs5/acsadmin/PolicyInputAction.do		10
Cisco Secure ACS	* CS	General Name: Standard Authentication Status: Enabled 🕜 \Theta	^	4
• 😚 My Workspace	Access Po	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.		
Network Resources	🔘 Sinç			
Wsers and Identity Stores	Identity	Conditions		
Specific Policy Elements	Filter:	Condition:		
▼ ♣ Access Policies		Dictionary: Attribute:		
Access Services Service Selection Rules		NDG Location Select		
 ✓ Ø 802.1x 	1	Operator: Value:		
Identity		in V Select		
O Default Device Admin		Current Condition Set:		
Identity		Add V Edit A Replace V		
Authorization		NDG.Location in All Locations		
Identity		And > -		
Authorization		Or > •		
Identity	**			
Authorization	Create			
✓ / lest Identity	Create	<u>w</u>		
Monitoring and Reports		Delete		
🕨 😼 System Administration	Save C	Results		
Done		Identity Source: Internal Users	-	1
		OK Cancel	Help	
		Done	a	

- **- X**

Your rule table should now look like Figure 32.

Figure 32. Rule-Based Result Selection



You have now finished the configuration for 802.1x with EAP-TLS (certificate authentications).

Wireless and SDP Profiles

Wireless and SDP authentications do not require separate configuration on the Cisco Secure ACS. If wireless EAP-TLS is used, the configuration from 802.1x with EAP-TLS in the previous section would satisfy the configuration requirements.

Please make sure the users are present in the selected identity store.

You have finished the configuration for Cisco Access Control Server Version 5 for Cisco Virtual Office.

Resources

For more information about Authentication Proxy, click here:

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_cfg_authen_prxy_external_docbase_0900e 4b1805afd05_4container_external_docbase_0900e4b1807b01d5.html

For more information about PKI and AAA integration (PKI-AAA), click here:

http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_cfg_auth_rev_cert_external_docbase_0900 e4b1805afd04_4container_external_docbase_0900e4b1807b4277.html

For more information about user-based firewall, click here:

http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_user_fw_supp.html



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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Printed in USA