

TrustSec Phased Deployment Configuration Guide

Last Updated: September 6, 2011



Building Architectures to Solve Business Problems

About Cisco Validated Design (CVD) Program

The CVD program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit http://www.cisco.com/go/designzone.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLEC-TIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUP-PLIERS 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.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

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 http://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)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

TrustSec Phased Deployment Configuration Guide

© 2011 Cisco Systems, Inc. All rights reserved.



TrustSec Phased Deployment Configuration Guide

This document is designed to help focus and streamline Cisco TrustSec deployments. It includes the following sections:

- Phased Deployment Overview, page 3
- Implementing Monitor Mode, page 11
- Implementing Low Impact Mode, page 43
- Implementing High Security Mode, page 91
- Creating a Certificate for a Windows XP Browser, page 104
- References, page 109

Phased Deployment Overview

This section includes the following topics:

- Cisco TrustSec Overview, page 3
- Cisco IOS Software Identity Enhancements, page 4
- Cisco Discovery Protocol Enhancement for Second Port Disconnect, page 5
- Cisco Secure Access Control System 5.x, page 5
- Phased Implementation Strategy, page 6
- Predeployment LAN Requirements, page 8

Cisco TrustSec Overview

Cisco Trusted Security (TrustSec) is an integrated solution comprising several Cisco products that offer authentication, access control, and user policies to secure network connectivity and resources. Cisco TrustSec facilitates greater security and cost-effective management of changes throughout your organization.



Having a secure TrustSec framework in place helps enterprises better manage employee mobility, reduce network access expenses, and boost overall productivity while lowering operating costs.

The Cisco TrustSec solution provides the following benefits:

- Improves business capability without compromising security—Policies are associated with users and not physical ports, which not only gives your users more mobility but also simplifies administration for IT staff. Policy enforcement and dynamic provisioning ease management functions and deliver greater scalability.
- Provides greater flexibility and mobility—Creating user or group profiles with policies that define trust relationships between users and network resources helps easily authenticate, authorize, and account for all wired and wireless network users.
- Increases efficiency and manage costs—Delivering secure network access to partners and vendors though centralized policy-based administration decreases the time, complexity, and effort associated with port security techniques at the media access control level.
- Increases visibility and enforces policy compliance—Tracking users and accounting for user activities help safeguard your network.

Cisco IOS Software Identity Enhancements

This section describes Cisco IOS Software features that accommodate the deployment scenarios described in this guide. It includes the following topics:

- IEEE 802.1X with Multiauth, page 4
- Flexible Authentication Sequencing, page 4
- IEEE 802.1X with Open Access, page 5
- IEEE 802.1X and MAB with Downloadable ACLs, page 5
- IEEE 802.1X and MAB with Downloadable VLAN, page 5
- Multidomain Authentication, page 5

IEEE 802.1X with Multiauth

Multiple authentication allows more than one host to authenticate on an IEEE 802.1X-enabled switch port. With multiauth, each host must authenticate individually before it can gain access to the network resources.



When multiauth is enabled, your dynamic authorization options change. Because an Ethernet port can be assigned to only one VLAN, you cannot have each authenticated session on a different VLAN. Therefore, Cisco recommends that you consider using downloadable access control lists (dACLs) as your authorization method. This is discussed later in this document.

Flexible Authentication Sequencing

Flexible authentication sequencing provides a flexible timeout and fallback mechanism among IEEE 802.1X, MAC authentication bypass (MAB), and web authentication methods. It also allows switch administrators to control the sequence of the authentication methods. This simplifies the Cisco TrustSec configuration by providing a single-set of configuration commands to handle different types of endpoints

connecting to the switch ports. In addition, flexible authentication sequencing allows users to configure any authentication method on a standalone basis; that is, MAB can be configured without requiring IEEE 802.1X configuration.

IEEE 802.1X with Open Access

This feature allows users to have limited network access, such as the Intel Preboot eXecution Environment (PXE) boot server, before IEEE 802.1X authentication. The limited access is optionally controlled by an access control list (ACL) or a virtual LAN (VLAN) that is defined by the switch administrator and applied on the switch port.

IEEE 802.1X and MAB with Downloadable ACLs

This feature allows per-user ACLs to be downloaded from the Cisco Access Control Server (ACS) as policy enforcement after authentication using IEEE 802.1X, MAB, or web authentication.

IEEE 802.1X and MAB with Downloadable VLAN

This feature allows per-port VLAN to be downloaded from the Cisco ACS as policy enforcement after authentication using IEEE 802.1X and MAB.

Multidomain Authentication

This feature allows an IP phone, either Cisco or non-Cisco, and a PC to authenticate on the same switch port while it places them on appropriate voice and data VLANs.

For a full list of the new Cisco IOS Software enhancements and additional information, see the following URLs:

- http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6970/ps6017/ps9673/product_bulleti n_c25-503086.html#wp9000607
- http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.h tml#wp1107452

Cisco Discovery Protocol Enhancement for Second Port Disconnect

Cisco Discovery Protocol (CDP) is enhanced to add a new type-length-value (TLV) for the IP phone to inform the switch in the event of the PC disconnecting from the IP phone. Upon receiving this notification, the switch can clear the authenticated session security record for the PC. This enables end users to move behind phones without validating security policies, and thus eliminating error disabling of ports.

Cisco Secure Access Control System 5.x

Cisco Secure Access Control System 5.x (ACS 5.x) is the Cisco policy management system for supporting comprehensive, identity-based access control and security. Cisco ACS 5.x is focused on enhanced support for 802.1X. The following are the key enhancements for Cisco ACS 5.x:

- Rules-based attribute-driven policy model
- Lightweight web GUI
- · Centralized reporting, monitoring, and troubleshooting
- Linux-based system architecture
- Improved integration with identity and policy databases
- · Available as physical appliance and virtual appliance for VMware

Phased Implementation Strategy

The depth and breadth of Cisco TrustSec accommodates a large number of use cases and deployment scenarios. This section describes the following two aspects of the use cases discussed in this guide:

- Authentication and Authorization Modes, page 6
- Endpoint/User—Use Cases, page 7

Authentication and Authorization Modes

Cisco recommends a phased deployment model that can allow for limited impact on network access while gradually introducing authentication and authorization on the wired network. The phases are as follows:

- Monitor mode
- Low impact mode
- High security mode

Monitor Mode

Monitor mode allows for the deployment of the TrustSec authentication methods IEEE 802.1X, MAB, and/or web authentication (WebAuth) without any effect to user or endpoint access to the network. Monitor mode is basically like placing a security camera at the door to monitor and record port access behavior.

With AAA RADIUS accounting enabled, you can log authentication attempts and gain visibility into who and what is connecting to your network with an audit trail. You can discover the following:

- Which endpoints such as PCs, printers, cameras, and so on, are connecting to your network
- Where these endpoints connected
- Whether they are 802.1X capable or not
- Whether they have valid credentials
- In the event of failed MAB attempts, whether the endpoints have known, valid MAC addresses

Monitor mode is enabled using 802.1X with the open access and multiauth mode Cisco IOS Software features enabled, as follows:

```
sw(config-if) #authentication open
sw(config-if) #authentication host-mode multi-auth
```

The open access feature transforms the normal behavior of blocking traffic on an 802.1X-enabled port until authentication and authorization are successfully performed. The default behavior of 802.1X is still to block all traffic accept Extensible Authentication Protocol over LAN (EAPoL). However, the open access feature allows the customer/administrator the option of providing unrestricted access to all traffic, even though authentication (802.1X, MAB, and/or WebAuth) is enabled.

All of this is accomplished with no impact to end users or network-attached hosts.

Low Impact Mode (also known as Selective Access Mode)

In this mode, you are able to incrementally increase the security by adding an ingress ACL to the 802.1X-enabled switchport that is configured in open mode. This ACL provides the ability to maintain whatever basic connectivity is required for unauthenticated hosts while selectively providing differentiated access for authenticated users.

An example of how this may be used is providing a host attached to a default port the ability to use Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), and perhaps get to the Internet; all while blocking access to internal resources. When a device connected to that switchport authenticates, a dACL is applied to permit all traffic.

High Security Mode

Another option for 802.1X-enabled switch ports is the strict use of the traditional closed mode in conjunction with the use of dynamic VLAN assignment for differentiated access. This is the default behavior of an 802.1X-enabled switch port.

This guide demonstrates how to configure these three identity-enabled modes, allowing you to determine which mode works best for your environment.

Endpoint/User—Use Cases

Most if not all customer environments have a mix of host and users types. These typically fall into the following four primary categories:

- Managed Hosts/Assets
- Managed Users
- Unmanaged Host/Assets
- Unmanaged Users

Managed Hosts/Assets

The host device/asset is managed by the IT department and belongs to one of the following two classes for the purpose of TrustSec:

- 802.1X capable—The device has a supplicant and can authenticate using 802.1X.
- Non-802.1X capable—The device does not have the ability to authenticate using 802.1X; that is, there is no supplicant.

Because the devices are managed, the IT department has knowledge of the device and in most cases can install and configure the prerequisite 802.1X supplicant software if it is available.



This guide uses Active Directory and the Cisco ACS internal database as the identity management (IdM) systems for managed hosts.

Managed Users

The end user has some affiliation with the company, either as an employee or subcontractor, and has been provisioned with an identity (username/password, digital certificate, and so on) in the identity IdM system of the company; typically, Microsoft Active Directory or Lightweight Directory Access Protocol (LDAP). The Cisco TrustSec Policy Management Server (ACS) integrates with common IdM systems to allow seamless authentication of user credentials.



This guide uses Active Directory as the IdM system for managed user identities.

Unmanaged Host/Assets

Endpoints that belong to short-term guests or business partners such as consultants, contractors, and customers. Because of legal or liability concerns, most IT departments cannot or are reluctant to install client software such as 802.1X supplicants on these unmanaged host PCs.

Unmanaged Users

Users that are considered short-term guests or business partners such as consultants, contractors, and customers, which are not or will not be provisioned into the traditional company IdM systems.

The key is to be able to accommodate all of the above endpoint/user use cases with a single switch port configuration. This can be accomplished with Cisco IOS Software enhancements; specifically, flexible authentication (FlexAuth) and flexible authentication sequencing. FlexAuth is used in conjunction with a policy or procedure to register the PC MAC addresses of guests and contractors.

Predeployment LAN Requirements

This section includes the following topics:

- Assumptions and Prerequisites, page 8
- Pre-TrustSec Switchport Interface Configuration, page 9
- Verifying Network Infrastructure Before TrustSec is Deployed, page 11

Assumptions and Prerequisites

The following network services should be installed, configured, and ready for use:

- Microsoft Active Directory (AD)
- Certificate Authority (CA); this document assumes Microsoft CA
- DHCP
- DNS

For this configuration guide, the following have been preconfigured:

- AD domain *demo.local*
- AD users and passwords, as listed in Table 1
- Switch VLANs and DHCP scopes, as listed in Table 2.

Username	Example Passwords	Record Your Passwords Here
Administrator	aPa\$\$word0	
User1	uPa\$\$word1	
User2	uPa\$\$word2	

Table 2Switch VLANs and Scopes

VLAN NAME	VLAN ID	IP	Description
Monitor Mode			
DATA	210	10.200.10.x/24	All non-Voice
VOICE	211	10.200.11.x/24	Voice Only
High Security Mo	de (used later)		
MACHINES	212	10.200.12.x/24	Managed Host/Assets
GUEST	213	10.200.13.x/24	Non-802.1X responsive Host
CONTRACTOR	214	10.200.14.x/24	Reserved for Contractors
AUTHFAIL	215	10.200.15.x/24	Failed 802.1X attempts

Figure 1 shows a diagram of the TrustSec components used in the Cisco testing lab.

Figure 1 TrustSec Lab Components



Pre-TrustSec Switchport Interface Configuration

ſ

The following is a typical switchport configuration before TrustSec implementation:

```
Interface GigabitEthernet 2/1
switchport access vlan 210
switchport voice vlan 211
switchport mode access
spanning-tree portfast
spanning-tree bpduguard enable
ip verify source vlan dhcp-snooping
etc.
end
```

! Comments:

! Your configuration may vary. The main thing to note is that we are only using a DATA

! and VOICE VLAN initially and no TrustSec features are enabled.

The following global switch configuration needs to be applied to the switch to enable DHCP Snooping on the port:

1

```
ip dhcp snooping vlan 210-215 <- your vlans may vary
no ip dhcp snooping information option
ip dhcp snooping
```

Verify that all hosts, except contractors and rogue APs, are online and working:

Cat6K#**show cdp neighbors**

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone, D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID	Loca	al Intrfce	Holdtme	Capability	Platform	Port ID
SEP001BD585391E	Fas	s 2/16	161	НРМ	IP Phone	Port 1
SEP0018BAC7BCEE	Fas	2/12	175	H P	IP Phone	Port 1
SEP0018BAC7BCFA	Fas	2/13	167	H P	IP Phone	Port 1
6506-1.identity.	com	Fas2/48	151	R S I	I WS-C6506	Gig1/43
001DE5EBE5EF		Fas 2/8	136	Н	CIVS-1	IPC- eth0
001DE5EBF900		Fas 2/11	131	Н	CIVS-1	IPC- eth0

Cat6k#show ip dhcp snooping binding

IpAddress	Leas	se(sec) Type		VLAN
10.200.11.202	613050	dhcp-snooping	211	FastEthernet2/16
10.200.10.203	450645	dhcp-snooping	210	FastEthernet2/13
10.200.10.201	358850	dhcp-snooping	210	FastEthernet2/1
10.200.11.201	687677	dhcp-snooping	211	FastEthernet2/13
10.200.11.203	687690	dhcp-snooping	211	FastEthernet2/12
10.200.10.206	687692	dhcp-snooping	210	FastEthernet2/11
10.200.10.206	687692	dhcp-snooping	210	FastEthernet2/11
10.200.10.204	687693	dhcp-snooping	210	FastEthernet2/8
10.200.10.205	444919	dhcp-snooping	210	FastEthernet2/12
	IpAddress 10.200.11.202 10.200.10.203 10.200.10.201 10.200.11.201 10.200.11.203 10.200.10.206 10.200.10.206 10.200.10.204 10.200.10.205	IpAddress Leas 10.200.11.202 613050 10.200.10.203 450645 10.200.10.201 358850 10.200.11.201 687677 10.200.11.203 687690 10.200.10.206 687692 10.200.10.206 687692 10.200.10.204 687693 10.200.10.205 444919	IpAddress Lease(sec) Type 10.200.11.202 613050 dhcp-snooping 10.200.10.203 450645 dhcp-snooping 10.200.10.201 358850 dhcp-snooping 10.200.11.201 687677 dhcp-snooping 10.200.11.203 687690 dhcp-snooping 10.200.10.206 687692 dhcp-snooping 10.200.10.206 687692 dhcp-snooping 10.200.10.206 687693 dhcp-snooping 10.200.10.204 687693 dhcp-snooping 10.200.10.205 444919 dhcp-snooping	IpAddress Lease(sec) Type 10.200.11.202 613050 dhcp-snooping 211 10.200.10.203 450645 dhcp-snooping 210 10.200.10.201 358850 dhcp-snooping 210 10.200.11.201 687677 dhcp-snooping 211 10.200.11.203 687690 dhcp-snooping 211 10.200.10.206 687692 dhcp-snooping 210 10.200.10.206 687692 dhcp-snooping 210 10.200.10.204 687693 dhcp-snooping 210 10.200.10.204 687693 dhcp-snooping 210 10.200.10.205 444919 dhcp-snooping 210

Total number of bindings: 8

Verifying Network Infrastructure Before TrustSec is Deployed

Verify the following before deploying TrustSec:

- DNS and DHCP are working
- Client machines have joined the AD domain
- The access switch can ping the Cisco ACS
- The Cisco ACS can ping the AD domain controller
- IP phones are working; check for dial tone
- All VLANs are configured and routable on the network
- Devices such as IP cameras and printers are working; for example, browse to the IP camera http://10.200.10.206



Do *not* enable TrustSec features such as 802.1X on the switch until you have configured your AAA server, switch-to-AAA/RADIUS configurations, and so on.

Implementing Monitor Mode

This section describes the global configuration necessary to implement monitor mode. This section includes the following topics:

- Monitor Mode Overview, page 11
- Installing Digital Certificates, page 12
- Adding a Certificate Authority, page 20
- Using Policy Elements, page 27
- Configuring the Access Switch, page 34
- Verifying Monitor Mode, page 36

Monitor Mode Overview

This section describes how to enable TrustSec authentication on the access switch ports and configure the infrastructure to support authentication and accounting. Monitor mode does not disrupt any network services for attached hosts, but enables you to account for and monitor network access attempts from the hosts connecting to your network.

Note that configuration of 802.1X supplicants, or clients, is not a concern here because monitor mode does not enforce authentication. However, if there are hosts with 802.1X enabled, you are able to detect them via the RADIUS accounting logs.

Installing Digital Certificates

To install digital certificates, complete the following steps.

Procedure

Step 1 Login to your newly installed Cisco Secure ACS 5.X (see Figure 2).

Unless otherwise configured, use the default username and password: acsadmin/default.

Figure 2	Cisco Secure ACS Login	
 cisco	Cisco Secure ACS	Username:
	Version 5.2.0.26 Hostname: atw-acs02 (Primary) Welcome to Cisco Secure ACS For Authorized Use Only	Password: Log In Reset

Step 2 To create a digital certificate for ACS from your lab, trusted public, or enterprise certificate authority, go to the Cisco Secure ACS System Administration > Configuration > Local Server Certificates > Local Certificates, and select Add (see Figure 3).

<u>P</u> Tip

Best Practice Recommendation—Do not use self-signed certificates. Creating a digital certificate for ACS that is signed by a trusted third-party or enterprise CA is highly recommended. It is the foundation of trust for most browser-based (SSL) and EAP-based (RADIUS) protocols.



Figure 3 Creating a Digital Certificate

Step 3 Check the Generate Certificate Signing Request and click Next (see Figure 4).

Figure 4 Selecting Generate Certificate Signing Request

Generate Certificate Signing Request Use this option to have the ACS server generate a certificate signing request to present to your local Certificate Authority. Once you have generated the signing request, go to the "Outstanding Signing Requests" list, select the signing request, and export a copy of the signing request (save a copy on your client system). Once you receive a certificate from your CA, you will use the "Bind CA Signed Certificate" option below to install it.

- **Step 4** In the Generate Certificate Signing Request screen (see Figure 5), do the following:
 - a. In the Certificate Subject text box, enter the fully qualified domain name of your ACS 5.0 server: cn=acs5.demo.local.
 - b. In the Key Length text field, select 4096
 - c. Click Finish.



Step 5 To access the Certificate Signing Request (CSR), go to System Administration > Configuration > Local Server Certificates > Outstanding Signing Requests (see Figure 6).

Figure 6 Certificate Signing Request

s	ystem A	Administration > Configuration > Lo	cal Server Certificates > Outst	anding Signing Reques	ts		
	Certif	icate Signing Request			Show	<i>ving</i> 1-1 of 1 50 🛟 p	ŧ
	Filter:	: 🚺 Matc	h if:	G0 🔻			
		Name 🔺	Certificate Subject	Key Length	Timestamp	Friendly Name	8
		Certificate Signing Request 2	CN=acs5.demo.local	4096	08:40 27.06.2011	1	2141

I

Step 6 Select the CSR you created, click **Export** and then click **Save** (see Figure 7).

You will need to access this CSR from the CA in a later step.

Figure 7 Saving the Certificate Signing Request

Do you v	want to sa	ve this file?	
	Name: Type: From:	Certificate_Signing_Request1.pem Unknown File Type acs5.idux.local	
		Save	Cancel
	√hile files fi	om the Internet can be useful, some i	files can potentially

Step 7 Open your enterprise or pilot/demo root CA server: http://ad.demo.local/certsrv.

The Welcome screen appears, as shown in Figure 8.

Figure 8 Microsoft Certificate Services—Welcome Screen

Microsoft Certificate Services mcs-17 Hom	<u>e</u>
Welcome	_
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.	
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.	
For more information about Certificate Services, see Certificate Services Documentation.	
Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL	
	-

Step 8 Select Request a Certificate.

The Request a Certificate screen appears, as shown in Figure 9.

Figure 9 Request a Certificate Screen

Microsoft Certificate Services mcs-17	<u>Home</u>
Request a Certificate	
Select the certificate type: User Certificate	
Or, submit an <u>advanced certificate request</u> .	14197

Step 9 Select advanced certificate request.

The Advanced Certificate Request screen appears, as shown in Figure 10.

Figure 10 Advanced Certificate Request Screen

Microsoft Certificate Services -- mcs-17

Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file. Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.

Note: You must have an enrollment agent certificate to submit a request on behalf of another user.

Submit a certificate request by using a base-64-encoded CMC or PKCS#10 file, or submit a renewal request by using a base-64-encoded PKCS#7 file (see Figure 11).

Home

214198

Figure 11 Submitting a Certificate Request

Microsoft Certificate Services mcs-17		<u>Home</u>
Submit a Certificate Request or Renewal Request		
To submit a saved request to the CA, paste a base-64-encode generated by an external source (such as a Web server) in the	ed CMC or PKCS #10 certificate request or PKCS #7 renewal request Saved Request box.	
Saved Request:		
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	×	
Certificate Template:		
Administrator		
Additional Attributes:	_	
Attributes:	l∕s	
Submit >	—	

1

Step 10 Open the CSR you created from ACS in the previous step in a text editor (see Figure 12).



Figure 12 CSR Opened in a Text Editor

- Ensure that word wrap is not enabled and select all of the text. Step 11
- Step 12 Paste the selected text into the CA window and click **Submit** (see Figure 13).

Figure 13 Submitting a Certificate Request (2)

Microsoft Certificate Services mcs-17	<u>Home</u>
Submit a Certificate Request or Renewal Request	
To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal requested by an external source (such as a Web server) in the Saved Request box.	uest
Saved Request:	
Base-64-encoded SM5f++BR2lolzgEUJENBFURy18mAA2/DrecWCV Base-64-encoded RJ032cLliODLuXPordCXBeQYuIBFGGOMfpzKtKcL certificate request 18c540CnCDvsbigsCL7cn2Gq4UHKEmTX620GCSj (CMC or Bqc3jXDNSB3/K4w5yAcXEPPoxnk5AHGL PKCS #IO or END CERTIFICATE REQUEST PKCS #IO: END certificate request Browse for a file to insert.	
Certificate Template:	
Web Server	
Additional Attributes:	
Attributes:	
Submit >	
	-

1

Step 13 Download your certificate on your local computer in DER format for importing into ACS; for example, ca-cert-DER.cer (see Figure 14).

Make a note of the filename and directory in which you saved it.

Figure 14	Certificate Issued	
Microsoft Certificate S	Services mcs-17	Home
Certificate Issued	1	
The certificate you	requested was issued to you.	
© DER Downloa Downloa	t encoded or ⊂ Base 64 encoded <u>ad certificate</u> <u>ad certificate chain</u>	

Step 14To install the new certificate in the Cisco ACS 5.0 interface, go to System Administration >
Configuration > Local Server Certificates > Local Certificates and select Add (see Figure 15).



Figure 15 Adding a New Certificate

Step 15 Select the Bind CA Signed Certificate option and click Next (see Figure 16.)

Figure 16 Bind CA Signed Certificate Screen

O Bind CA Signed Certificate

After using the previous option to generate a certificate signing request, this option is used to bind/install the certificate received from your CA. ACS will automatically match the certificate with the appropriate outstanding signing request.

Step 16 Browse, locate, and select the file you created earlier, and make sure to check both the **EAP** and **Management Interface** checkboxes (see Figure 17).

214205



Figure 17 Step 2 - Bind CA Signed Certificate Screen

Step 17 Click Finish.

You should now see the new digital certificate successfully installed (see Figure 18), and you may delete the old self-signed certificate.

Figure 18 New Digital Certificate Installed

Friendly Name	Issued To	Issued By	Valid From	Valid To (Expiration)	Protocol	
ACS5-2	ACS5-2	ACS5-2	04:59 06.10.2008	04:59 06.10.2009	N/A	207
acs5.idux.local	acs5.idux.local	mcs-17	01:14 15.11.2008	01:14 15.11.2010	EAP: Used for EAP protocols that use SSL/TLS tunneling,HTTPS	214

This completes the ACS certificate enrollment section.

Adding a Certificate Authority

To add a certificate authority, complete the following steps.

Procedure

- **Step 1** Go to User and Identity Stores > External Identity Stores > Certificate Authorities and click Add.
- **Step 2** In the Certificate File to Import screen, click **Browse** and select the .cer file of the root CA created previously.
- Step 3 Click Open and ensure that the Trust for Client with EAP-TLS checkbox is checked (see Figure 19).

Figure 19	Adding a Certificate Authority	
Users and Identity	y Stores: <u>Certificate Authorities</u> > Create	
Certificate File	e To Import	
Add (Import) a	new Trusted CA (Certificate Authority) Certificate.	
* Certificate File:	C:\Documents and Settings\Administrator\Desktop\idi	
Trust for client	with EAP-TLS: 🔽	
Description:		8
*Required fields		2142

Click Submit and the new CA will be displayed in the Trust Certifcate List (Figure 20). Step 4

	Figure 20	Trust Certificate List
--	-----------	------------------------

Trust Certificate list Items 1-1 of 1 Rows per page: 🔂 🔽 GCA									
Filter: Match if: Go 🗸									
	Friendly Name	Expiration	Issued To	Issued By	Description				

Configuring Network Access Devices

To create an RADIUS entry for your access switch, complete the following steps.

Procedure

ſ

- Step 1 Go to Network Resources > Network Devices and AAA Clients.
- Step 2 Create an entry for RADIUS for your access switch (see Figure 21) by doing the following:
 - a. Provide a name and IP address that corresponds to your access switch.
 - **b.** Check the RADIUS box.
 - c. Provide a shared secret; this exercise uses *cisco123*.

Location All Locations Device Type All Device Types IP Address Select IP Address TACACS+ IP: 10.200.1.155 IP: Single Connect Device IP: Single Connect Device IP: Location IP: TACACS+ IP: Single Connect Device IP: Location IP: TACACS+ IP: Single Connect Support IP: TACACS+ IP: Select	* Name: Ca Description: Acc	t6K cess Switch Running IOS 12.2(33)SXI	
Device Type All Device Types Select IP Address	Location	All Locations	Select
IP Address Single IP Address IP Range(s)	Device Type	All Device Types	Select
	© Single IP Ad	ddress () IP Range(s)	Shared Secret: Shared Secret: Legacy TACACS+ Single Connect Support TACACS+ Draft Compliant Single Connect Support RADIUS Shared Secret: cisco123

Figure 21 Creating a RADIUS Entry for the Access Switch

Connecting to the Active Directory Domain

To connect to the Active Directory domain, complete the following steps.

Procedure

- **Step 1** Go to Users and **Identity Stores > External Identity Stores > Active Directory**, and do the following:
 - a. Enter the appropriate domain name; for example, demo.local.
 - **b.** Provide a username and password that allow you to connect to the domain; for example, **administrator**/*yourpassword*.
- Step 2 Click on the Test Connection button to validate joining the domain.
 - If you get an error similar to the one shown in Figure 22, your clocks are not synchronized. In this case, go to the "Setting the Clock for the New Cisco ACS 5.x Appliance" section on page 23.

Figure 22 Connection Failed Message

Microsoft	: Internet Explorer 🛛 🔀	}
1	Connection to idux.local failed. Further information on status: - Clock Skew error.	
	(CK)	214213

• If you were successful, select **Save Changes** and move to the "Creating Identity Groups and Identity Store Sequences" section on page 25.



Clock synchronization is extremely important to Active Directory operations. Always use NTP where possible.

Setting the Clock for the New Cisco ACS 5.x Appliance

To set the clock on a new Cisco ACS 5.x appliance, complete the following steps.

Procedure

Step 1

Access the command-line interface on the ACS appliance and enter the administratively defined login credentials; for example, **admin/password** (see Figure 23).



Figure 23

You configured the password in the setup process of the ACS appliance.

ACS5-2	login:	_			

Login Screen

Step 2 Determine the correct value for your timezone by typing the following command at the base prompt (not in global configuration mode) to display the available options.

ACS5-2/admin# show timezone

- **Step 3** Access global configuration mode by typing **conf t**.
- **Step 4** Type the clock timezone value (for example, **US/Pacific**) and press the **Enter** key.
- **Step 5** Use the following command to set your timezone:

ACS5-2/admin(config)# clock timezone < YOURTIMEZONE>

- **Step 6** At the Do you want to restart now? prompt, type **y**.
- **Step 7** Do one of the following:
 - **a.** To set the NTP server, from global configuration mode use the **ntp server** *<server>* command, as in the following example:

ACS5-2/admin(config) # ntp server time.cisco.com

b. To set the time, use the clock set <month day time year> command, as in the following example: ACS5-2/admin# clock set Jun 24 14:27:00 2011 Your ACS appliance should now have the same timezone, time, and date as your Active Directory domain controller.

Step 8 Go back into the Cisco ACS web interface and finish your Active Directory setup.

If you had to adjust the timezone, date, and time, go back to the previous step and set up your Active Directory as an external identity store. When you are complete, you should now be able to establish a connection with the active directory, as shown in Figure 24.

Figure 24 Successful Connection to the Active Directory

Jeneral		
Connection Details		
* Active Directory Domain Na	me: idux.local	
Please specify the credentials	used to join this machine to the Act	ive Directory Domain:
*Username:	administrator	
* Password:	•••••	
You may use the Test (soft Internet Explorer 🛛 🗙	correct and Active Directory Domain is reachable
	Connection to idux.local succeeded.	correct and Active Directory Domain is reachable.
Click on 'Save Change: connected to the Doma	ОК	and save this configuration. Once you have successfully Directory Attributes to be available for use in policy rules.
End User Authentication	Settings	
🔽 Enable password chang	e	
🔽 Enable machine authent	tication	N
🔲 Enable Machine Access	Restrictions	13
* Aging time (hours):	0	
Connectivity Status		
Joined to Domain: Connec	tivity Status:	

Creating Identity Groups and Identity Store Sequences

This section includes the following topics:

- Creating Identity Groups, page 25
- Creating Identity Store Sequences, page 26

Creating Identity Groups

To create identity groups, complete the following steps.

Procedure

- **Step 1** Go to **Users and Identity Stores > Identity Groups** and select **Create**.
- Step 2 Type in the name and description information and click Submit (see Figure 25).

Figure 25 Creating Identity Groups

Users and Identity Stores > Identity Groups > Create						
	General a Name: IP Phones Description: Corporate Managed IP Phones c Parent: All Groups c = Required fields Select					
Users and Identity Stores > Identity Groups Identity Groups Filter: Attach if: Go						
Name Description						
□ ▼ <u>All Groups</u> Identity Group Root						
IP Phones Corpora	IP Phones Corporate Managed IP Phones					
MACHINES Corporate Managed Machines (Printers, Cameras, etc.)						
and the second s						

Step 3 Repeat for the next group.

ſ

It is not necessary to create any internal identity stores as a host for MAB in monitor mode. These are added in the next phase. which is low impact mode.

Creating Identity Store Sequences

The identity store sequence allows you to add multiple identity stores to an access service. It attempts each identity store in the sequence, which is extremely flexible. This allows having users such as IP phones, temporary users, admin users, and so on, to be internally defined in ACS without having to add them to the corporate Active Directory or other external LDAP database.

To create identity store sequences, complete the follow steps.

Procedure

Step 1 Go to **User and Identity Stores > Identity Store Sequences** and select **Create**.

- **Step 2** In the window shown in Figure 26, do the following:
 - a. Type the name 802.1X-TrustSec.
 - b. Type a description and select Internal Users and AD1.
 - c. Click Submit.

This is used later in the 802.1X access service.

Figure 26 Creating Identity Store Sequences

Seneral					
Name:	802.1X-TrustSec	•			
Description	1:				
Authenticatio	n Method List				
Certificate	Based				
Password	Based				
Authenticati	on and Attribute R	etrieval Search List			
A set of ident	ty stores that will be	e accessed in sequen	ce until first authenti	cation succeeds	
Available		Selected			
Internal H NAC Pro	losts filer	AD1	$\overline{}$		
	6		\frown		
•					
	G	9			
	<u> </u>	2			

Using Policy Elements

This section describes the configuration of policy elements. It includes the following topics:

- Creating Access Policies, page 27
- Defining Identity Sources and Authorization Profiles, page 29
- Creating Service Selection Rules, page 31

Note

You do not need to create any authorization profiles for monitor mode because the port allows *all* traffic to flow, regardless of whether the endpoint successfully authenticates or not. You are only monitoring in this mode.

Creating Access Policies

For this guide, two new access services are created: one for 802.1X, and one for MAC Authentication Bypass (MAB).

Complete the following steps.

Procedure

- Step 1 Go to Access Policies > Access Services and select Create.
- **Step 2** In the window shown in Figure 27, do the following:
 - a. For the Name, type 802.1X.
 - b. For the Description, type IEEE 802.1X.
 - c. Select User Selected Policy Structure.
 - d. Click Next.

Figure 27 Creating Access Services—Step 1



Step 3 Select all of the check boxes shown in Figure 28 and click Finish.



Figure 28 Creating Access Services—Step 2



Decline any messages requesting you create matching Service Selection Rules. This is done in a later step.

Step 4 Select Access Policies > Access Services again.

Repeat the process above to create a new access service for MAB. The MAB service allows you to recognize network access requests, glean the MAC addresses, and record them in the AAA accounting logs. This helps you monitor and determine what devices, via their MAC addresses, are connecting to the network and where.

- Step 5 Select Create.
- **Step 6** In the window shown in Figure 29, do the following:
 - a. For the name, type MAB.
 - b. For the description, type MAC-Auth Bypass.
 - c. Select User Selected Service Type.
 - d. Accept the defaults and click Next.

,	Access Policies > Ac	Cess Services > Create		
	Step 1 - G	eneral		1
l	General			1
l	Name:	MAB		1
l	Description:	MAC-Auth Bypass		
	Access Service	Policy Structure		1
l	Based on s	ervice template		Select
l	Based on e	xisting service		Select
l	User Selection	ed Service Type Netwo	ork Access	
l	User Selected	Service Type		1
l	F OIK	Identity		5
l		Group Mapping		4
l	6	Authorization		1
				100
1	and		and a second second second	Service and the service of the servi

Figure 29 Creating an Access Service for MAB—Step 1

For MAB, select only Process Host Lookup and Allow PAP/ASCII (see Figure 30). Step 7

Figure 30 Creating an Access Service for MAB—Step 2

Access Policies > Access Services > Create	1
✓ General Allowed Protocols	
Step 2 - Allowed Protocols	
Process Host Lookup	5
Authentication Protocols	
Allow PAP/ASCI	





I

Decline any messages requesting you create matching Service Selection Rules. This is done in a later step.

Defining Identity Sources and Authorization Profiles

After creating the 802.1X and MAB Access Services, define their respective identity sources and authorization profiles by completing the following steps.

Procedure

- From within Access Policies > Access Services, select the previously created 802.1X access service. Step 1
- Step 2 Use the drop-down arrow to select **Identity** to set up the Identity Source.

TrustSec Phased Deployment Configuration Guide

Step 3 For 802.1X, specify 802.1X-TrustSec (see Figure 31).

This is the Identity Store Sequence you created previously, which contains both Active Directory and the internal database.

I

My Workspace	Access Policies > Access Services > 802.1X > Identity
Network Resources	Single result selection Rule based result selection
Busers and Identity Stores Store	Identity Source: 802.1X-TrustSec Select
Policy Elements	Advanced Ontions
👻 🌉 Access Policies	
Access Services Service Selection Rules ✓ 802.1X Identity Authorization O Default Device Admin O Default Network Access ✓ MAB TrustSec Access Control Monitoring and Reports System Administration	Save Changes Discard Changes

Figure 31 Setting up the Identity Source

- **Step 4** Accept the defaults and click **Save Changes**.
- **Step 5** Select **Authorization** under the 802.1X Access Service.
- **Step 6** In the window shown in Figure 32, for Monitor Mode, accept the Default Policy Rule for both 802.1X and MAB Access Services, which is **Permit Access**.

Figure 32 Authorization

	Access	Policies	s > Access	Services	> 802.1X > Authorization			
Network Resources	Stand	ard Po	licyl Exce	eption Po	blicy			
Busers and Identity Stores Store	Netv	vork A	ccess Aut	thorizatio	on Policy			
Policy Elements	Filte	e Ste	atue	unonizati	Match if: Equals A Enabled	Clear Eilter Go)	
🔹 🛃 Access Policies	Fille	1. 04	100) •	
Access Services Service Selection Rules			Status	Name	Conditions Compound Condition	Results Authorization Profiles	Security Group	Hit Count
▼ Ø 802.1X			No data	to displa	iy			
O Default Device Admin O Default Network Access Z MAB TrustSec Access Control								
Monitoring and Reports System Administration								
D Monitoring and Reports System Administration		ate	Default	licate	If no rules defined or no enabled rule matches	Permit Access	Unknown Customize)	0 Hit Count

Creating Service Selection Rules

In this section, you create two service selection rules: one for 802.1X and a second for MAB. Service selection is a means for Cisco ACS to identify an access service request and associate it with the proper administratively defined access service such as 802.1X, MAB, TACACS+, and so on. This allows for the specialized handling of different types of service requests, as listed in Table 3.

Table 3Service Selection Rules

Service Selection Rule Name	Compound Expr				
	Dictionary	Attribute	Operator	Value	Result Service
Match-802.1X	RADIUS-IETF	Service-Type	Match	Framed	802.1X
Match-MAB	RADIUS-IETF	Service-Type	Match	Call-Check	MAB

Complete the following steps.

Procedure

- Step 1 Go to Access Policies > Service Selection Rules.
- **Step 2** Select the **Customize** button from the lower right corner and make sure **Compound Condition** is selected (see Figure 33).

Figure 33 Customize Conditions Screen

ACS Host Name Device Filter Device IP Address Device Port Filter End Station Filter	\otimes	Protocol Compound Condition	$\overline{\mathbf{x}}$
NDG:Device Type NDG:Location Time And Date UseCase) (*)		$\overline{\vee}$

- Step 3 Click OK.
- Step 4 Select Create.
- **Step 5** In the windows shown in Figure 34, do the following:
 - a. For the Name, type Match-802.1X.
 - **b.** Select the **Protocol** checkbox.
 - c. Select RADIUS.
 - d. Select the Compound Conditions checkbox.
 - e. Select **RADIUS-IETF** from the dictionary drop-down box.
 - f. Click the Select button to select Service-Type for the Attribute.

g. Click OK.

	2	RADI	US Dictionary				Showing 1-25 of 25 50	per page 🤇
General	F.	Filter	:	Match if: (:	G0 🔻		
Name: Match-802.1X Status: Enabled	3	U	Attribute	ID 19	Type	Direction	Multiple Allowed	
The Customize button in the lower right area of the policy rules screen controls which	1	0	Login-LAT-Group	36	String	BOTH	false	
policy conditions and results are available here for use in policy rules.	1	0	Login-LAT-Node	35	String	BOTH	false	
		0	Login-LAT-Port	63	String	BOTH	false	
A Destance (Selant)	1	0	Login-LAT-Service	34	String	BOTH	false	
Protocol: Match Radius Select	£	0	NAS-Identifier	32	String	INBOUND	false	
Compound Condition: Condition:	1	0	NAS-IP-Address	4	IPv4 Address	INBOUND	false	
Dictionary: Attribute:	1	0	NAS-Port	5	Unsigned Integer 32	INBOUND	false	
RADIUS-IETF Service-Type	1	0	NAS-Port-Id	87	String	INBOUND	false	
Value:	1	0	NAS-Port-Type	61	Enumeration	INBOUND	false	
match 🗘 (Select)	3	0	Port-Limit	62	Unsigned Integer 32	BOTH	false	
Current Condition Set:	5	۲	Service-Type	6	Enumeration	вотн	false	
Add V Edit A Replace V	3	0	State	24	String	BOTH	false	
	è.	0	User-Name	1	String	INBOUND	false	
	1						(III) Page	1 of 1 🕩 🤇
(And > •)	1	OK)	Cancel					(H
(Or > •)	422	, min	and a free states	-	and the second second	والقي العامي	والمحمد والمحمد والمحمد والمستعورة	an a sure
and a second	- ⁶							

1

Figure 34 Creating the Service Selection Rule (1)

Step 6 From the Operator drop-down menu, Select match and Select Framed for the value (see Figure 35).

Figure 35 Creating the Service Selection Rule (2)

	1	Enun	n Definition	Showing 1-17 of 17 50 + per page
General	7		Enum Name	ID
Name: Match-802.1X Status: Enabled)	0	Login	1
		۲	Framed	
The Customize button in the lower right area of the policy rules screen controls which	<u>۱</u>	Θ	Callback Login	3
policy conditions and results are available here for use in policy rules.	ł.	0	Callback Framed	4
Conditions	2	0	Outbound	5
Protocol: match Badius (Select		0	Administrative	6
		0	NAS Prompt	7
Condition:	1	0	Authenticate Only	8
Dictionary: Attribute:	<u>ا</u>	0	Caliback NAS Prompt	9
RADIUS-IETF Service-Type Select	4	0	Call Check	10
Uperator: Value:	1	0	Callback Administrative	11
match Framed Select		0	Voice	12
Current Condition Set:	5	0	Fax	13
Add V Edit A Replace V	5	0	Modem Relay	14
	€	0	IAPP-Register	15
	1.			(4) (4) Page 1 of 1 (>>)
(And > •)	1422	OK	Cancel	
and a second	ćν	سي ا		الم المحصور بالمحصور المحصور بالمحمور ومحمول والمحمور من المحمور عن المحاصر المحمو

Step 7 In the window shown in Figure 36, do the following:

- a. Select Add V.
- **b.** In the Service drop-down menu under Results, select **802.1X**.
- c. Click OK.

policy conditions a	ton in the lower right area of the po nd results are available here for us	blicy rules screen controls which e in policy rules.
Conditions	h A Dadius	(Color)
	Radius	Select
Compound Condition:		
Dictionary:	Attribute:	
RADIUS-IETF	Service-Type	Select
Operator:	Value:	
match	value.	Select
Current Condition Set:		Select
Current Condition Set.		
Add V	Edit N Replace V	
RADIUS-IE	TF:Service-Type match Framed	
And > •		
Or> -		
		× ·
	De	elete (Preview)

Figure 36 Creating the Service Selection Rule (3)

You now see the newly created service selection rule Match-802.1X.

Step 8 Select **Save Changes** to save the changes.

Step 9 To create the MAB service selection rule, select **Create**.

Step 10 In the window shown in Figure 37, do the following:

- a. Give this rule the name of Match-MAB.
- **b.** Select the **RADIUS** protocol.
- c. In the Compound Condition section, select RADIUS-IETF from the Dictionary drop-down menu.
- d. Click the **Select** button to select **Service-Type** for the Attribute value.
- e. Click OK.
- f. Select match from the Operator drop-down menu.
- g. For the value, click the Select button and select Call-Check and then OK.
- h. Select Add V.

ſ

- i. From the Service drop-down menu in the Results section, select MAB.
- j. Click OK and then Save Changes.

The Customize policy condition	button in th	e lower right area of as are available here	the policy rules for use in policy	screen contro rules.	ols which
Conditions					
Protocol:	match	Radius		Sel	ect
Compound Condition: Condition:					
Dictionary:		Attribute:			
RADIUS-IETF		Service-Type		Select	
Operator:		Value:			
match 🗧				Select	
Add RADIU Or> •	V Edit S-IETF:Servic	A Replace V e-Type match Call Chec	k Delete P	Paview	
Service: MAB	•				

Figure 37 Creating the MAB Service Selection Rule

Configuring the Access Switch

This section describes the configuration of the access switch. It includes the following topics:

- Configuring Global Identity Settings, page 34
- Configuring Monitor Mode on the Switch Port, page 35

Configuring Global Identity Settings

Configure the global identity commands on the switch to enable TrustSec by using the following commands as a guide:

• AAA settings:

! Enable AAA aaa new-model ! Create an 802.1X port-based authentication method list aaa authentication dot1x default group radius

! Required for VLAN/dACL assignment aaa authorization network default group radius

! Enables 802.1X Accounting and MAB aaa accounting dot1x default start-stop group radius

• RADIUS settings:

! Define the Radius Server and establish the ports to use. ! The test keyword will proactively check that the RADIUS server (ACS 5) is still responding.

radius-server host [ACS_Server_IP_Address] auth-port 1645 acct-port 1646 test username test-radius

! Define the Shared-Secret to be used between ACS & the Switch. ! This must match what was entered in ACS.

radius-server key [user-defined-shared-key]

! ensure your RADIUS traffic is always sourced from the ip address entered in the RADIUS server. ip radius source-interface [interface_name]

! create the user in Global Config for the RADIUS server Test. username test-radius password 0 cisco123

• Globally enable 802.1X authentication:

dot1x system-auth-control

There are additional features to consider before going into production, such as Inaccessible Authentication Bypass, also known as Critical Auth. For instructions on Inaccessible Authentication Bypass, as well as other identity features, see the following URL: http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/dot1x.ht ml#wp1054805

Configuring Monitor Mode on the Switch Port

To configure monitor mode on the switch, add the following TrustSec settings to the access ports:

```
! Enter the range of interfaces to apply the port configuration to
interface range g2/1-16
! Enable pre-authentication open access (non-restricted)
authentication open
! Enable port-based Authentication on the Interface
authentication port-control auto
! Enable 802.1X Authentication on the Interface
dot1x pae authenticator
! Enable MAC-Auth Bypass on the Interface
mab
! Enable multiauth Mode
authentication host-mode multi-auth
```

! multiauth Allows a single IP phone and one or more data clients to independently authenticate ! on an authorized port. Each host, or MAC Address, is authenticated individually.



This is not an extensive list of the identity feature set, but just those necessary for the enabling of monitor mode for the purposes of this guide.

Verifying Monitor Mode

Now that you have enabled the global settings in Cisco ACS and on the switch, as well as the port-specific configuration to enable TrustSec monitor mode, run the validation steps described in this section to verify proper operation.

This section includes the following topics:

- Verifying Access Switch-to-Cisco ACS Server Communication, page 36
- Verifying Authenticator-to-Authentication Server Communication, page 36
- Verifying that the Cisco ACS Server Can Communicate with the AD Domain Controller, page 38
- Verifying Host Network Connectivity and Network Services, page 38
- Verifying that IP Phones are Working, page 42
- Verifying that Devices such as IP Cameras Work, page 42

Verifying Access Switch-to-Cisco ACS Server Communication

Access the switch console and ping the IP address of your Cisco ACS server.



This is an optional step because you should have already validated communications during the Cisco ACS configuration steps earlier.

Verifying Authenticator-to-Authentication Server Communication

This validation exercise verifies that the switch is sending RADIUS messages for those hosts attempting to authenticate to those ports where you have enabled monitor mode. The easiest way to verify this is to check the accounting logs on the Cisco ACS server. Because you are in monitor mode, you should see failed authentication attempts from hosts.

Complete the following steps.

Procedure

Step 1 From within the Cisco ACS web interface, select Monitoring and Reports (see Figure 38).


Figure 38 Monitoring and Reports Screen

Step 2 Select Launch Monitoring & Report Viewer.

I

Depending on your browser behavior settings, either a new browser window or tab within the existing browser window is launched (see Figure 39).

	Monitoring and Reports: Dashboard		
Dashboard Alarms Inbox Thresholds Reports Favorites Shared Catalog Troubleshooting Connectivity Tests	Monitoring Reporting Authentication Lookup Protocol: RADIUS User: MAC Address: Time Range: Today	Select Clear Select Clear	
⊢ACS Support Bundle	Run White: Enter a value for user or MAC	۵/۲۷۷۷) Address. Both fields cannot be blank.	
	▼ Favorite Reports		
	▼ Favorite Reports Favorite Name	Report Name	Report Type
	Favorite Reports Favorite Name ACS - Configuration Changes - Today	Report Name ACS Instance>ACS_Configuration_Changes	Report Type System Report
	Favorite Reports Favorite Name ACS - Configuration Changes - Today ACS - System Errors - Today	Report Name ACS Instance>ACS_Configuration_Changes ACS Instance>ACS_System_Diagnostics	Report Type System Report System Report
	Favorite Reports Favorite Name ACS - Configuration Changes - Today ACS - System Errors - Today Active Sessions - RADIUS	Report Name ACS Instance>ACS_Configuration_Changes ACS Instance>ACS_System_Diagnostics Session Directory>RADIUS_Active_Sessions	Report Type System Report System Report System Report
		Report Name ACS Instance>ACS_Configuration_Changes ACS Instance>ACS_System_Diagnostics Session Directory>RADIUS_Active_Sessions Session Directory>TACACS_Active_Sessions	Report Type System Report System Report System Report System Report
		Report Name ACS Instance>ACS_Configuration_Changes ACS Instance>ACS_System_Diagnostics Session Directory>RADIUS_Active_Sessions Session Directory>TACACS_Active_Sessions AAA Protocol>RADIUS_Authentication	Report Type System Report System Report System Report System Report System Report
		Report Name ACS Instance > ACS_Configuration_Changes ACS Instance > ACS_System_Diagnostics Session Directory > RADIUS_Active_Sessions Session Directory > TACACS_Active_Sessions AAA Protocol > RADIUS_Authentication AAA Protocol > RADIUS_Authentication	Report Type System Report System Report System Report System Report System Report System Report

Figure 39 Monitoring and Reports Dashboard

Step 3 From within the Monitoring and Report view screen, select **Authentications – RADIUS – Today** from the Favorite Reports section.

You should see failed authentication attempts, as shown in Figure 40. However, remember that because you are in monitor mode and using the Open Access Cisco IOS Software feature, those hosts still have full network access.

💄 📑 🔛 🖻					Launc	h Interactive Viewer 🏻 🖺
Showing P	age	1 of	14 41 4 🕨 🕪	Goto Page:	>	
AAA Protocol >	RAD	IUS Au	thentication			-
Authentication Stat Date :	us:	Pass or January	Fail 8, 2009			
Generated on Janua	ary 8,2	009 11:	17:18 AM PST			
Reload						-
✓=Pass ×=Fail	0	Click for	r details			
Logged At	Status	Details	Failure Reason	User Name	Calling Station ID	Authentication Method
11:17:11.573 AM	×	0	22041 Unknown User	00-1D-E5-EB-F9-00	00-1D-E5-EB-F9-00	Lookup
11:17:11.573 AM	×	9	22041 Unknown User	00-1D-E5-EB-E5-EF	00-1D-E5-EB-E5-EF	Lookup
11:17:10.546 AM	×	0	22041 Unknown User	00-18-BA-C7-BC-FA	00-18-BA-C7-BC-FA	Lookup
11-17-04 403 AM	×	0	22041 Unknown User	00-21-86-58-DB-6B	00-21-86-58-DB-6B	Lookup
11.17.04.405 AM	×	0	12006 EAP-MD5 authentication failed	CP-7961G-SEP001BD585391E	00-1B-D5-85-39-1E	CHAP/MD5
11:16:52.736 AM						
11:16:52.736 AM 11:16:46.986 AM	×	0	22041 Unknown User	00-18-BA-C7-BC-EE	00-18-BA-C7-BC-EE	Lookup
11:16:52.736 AM 11:16:46.986 AM 11:16:46.983 AM	×	୍	22041 Unknown User 22041 Unknown User	00-18-BA-C7-BC-EE 00-18-F8-08-F8-38	00-18-BA-C7-BC-EE 00-18-F8-08-F8-38	Lookup
11:16:52.736 AM 11:16:46.986 AM 11:16:46.983 AM 11:16:45.956 AM	× × ×	୍ ଜ୍ ଜ୍	22041 Unknown User 22041 Unknown User 22041 Unknown User	00-18-BA-C7-BC-EE 00-18-F8-08-F8-38 00-18-F8-09-CF-C6	00-18-BA-C7-BC-EE 00-18-F8-08-F8-38 00-18-F8-09-CF-C6	Lookup Lookup Lookup

Figure 40 Failed Authentication Attempts

Verifying that the Cisco ACS Server Can Communicate with the AD Domain Controller

Access a command-line prompt on the ACS server and ping the IP address of your Microsoft AD Controller.

Note

This is an optional step because you should have already validated communications during the Cisco ACS configuration steps earlier.

Verifying Host Network Connectivity and Network Services

Now that you have enabled 802.1X and MAB in Open Mode, once again verify that the hosts connected to these ports still have network access as they did before enabling these TrustSec features.

I

Complete the following steps.

Procedure

Step 1 Access the switch console perform the following:

```
conf t
int range f2/1-16 (or the range of ports you configured)
shut
no shut
end
```

Notice the console messages on your terminal showing 802.1X and MAB authentication attempts and failures as shown in Figure 41. This is normal output. Depending on the authentication order commands, the switch ports first attempt 802.1X and then MAB, because these are the two TrustSec features you enabled.



*Jan 8 11:53:43.383: %AUTHHGR-5-START: Starting 'dot1x' for client (0018.f809.cfc6) on Interface Fa2/1
id-4503-2#
*Jan 8 11:53:47.547: %AUTHMGR-5-START: Starting 'dot1x' for client (0018.bac7.bcee) on Interface Fa2/12
*Jan 8 11:53:48.323: %AUTHMGR-5-START: Starting 'dot1x' for client (0021.8658.db6b) on Interface Fa2/12
id-4503-2#
*Jan 8 11:53:48.647: %AUTHMGR-5-START: Starting 'dot1x' for client (0018.f808.f838) on Interface Fa2/13
id-4503-2#
*Jan 8 11:53:54.751: XAUTHMGR-5-START: Starting 'dot1x' for client (0018.bac7.bcfa) on Interface Fa2/13
id-4503-2#
*Jan 8 11:53:58.831: %AUTHMGR-5-START: Starting 'dot1x' for client (001b.d585.391e) on Interface Fa2/16
id-4503-2#
*Jan 8 11:54:12.859: %AUTHMGR-5-START: Starting 'dot1x' for client (001d.e5eb.f900) on Interface Fa2/11
*Jan 8 11:54:13.239: %AUTHMGR-5-START: Starting 'dot1x' for client (001d.e5eb.e5ef) on Interface Fa2/8
id-4503-2#
*Jan 8 11:54:31.603: %AUTHMGR-5-START: Starting 'dot1x' for client (001b.d505.391e) on Interface Fa2/16
*Jan 8 11:54:31.619: %DOT1X-5-FAIL: Authentication failed for client (001b.d585.391e) on Interface Fa2/16
id-4503-2#
*Jan 8 11:54:31.619: XAUTHMGR-7-RESULT: Authentication result 'fail' from 'dot1x' for client (001b.d585.391e) on Interface Fa2/16
id-4503-2#
*Jan 8 11:55:00.615: %DOT1X-5-FAIL: Authentication failed for client (0018.f809.cfc6) on Interface Fa2/1
*Jan 8 11:55:00.615: %AUTHMGR-7-RESULT: Authentication result 'no-response' from 'dot1x' for client (0018.f809.cfc6) on Interface Fa2/1
*Jan 8 11:55:00.615: %AUTHMGR-7-FAILOVER: Failing over from 'dot1x' for client (0018.f809.cfc6) on Interface Fa2/1
*Jan 8 11:55:00.615: %AUTHMGR-5-START: Starting mab' for client (0018.f809.cfc6) on Interface Fa2/1
*Jan 8 11:55:00.623: MMAB-5-FAIL: Authentication failed for client (0018.f809.cfc6) on Interface Fa2/1
id-4503-2#
*Jan 8 11:55:00.623: %AUTHMGR-7-RESULT: Authentication result 'fail' from 'mab' for client (0018.f809.cfc6) on Interface Fa2/1
*Jan 8 11:55:00.627: %AUTHMGR-7-FAILOVER: Failing over from 'mab' for client (0018.f809.cfc6) on Interface Fa2/1
*Jan 8 11:55:00.627: XAUTHMGR-7-NOMOREMETHODS: Exhausted all authentication methods for client (0018.f809.cfc6) on Interface Fa2/1
id_4583_2#

However, because you have enabled *open mode*, connectivity should not be affected at all. To verify this, perform the following steps.

Step 2 To check the port authentication status on the switch for a given port, type the **show authentication** session command for a specific interface from your console connection to the switch.

For example, **show auth session int f2/1**. You should notice an output similar to the one shown in Figure 42, indicating that the host failed authentication where the status shows *Authz Failed*. You should also notice that the port attempted 802.1X and then failed over to MAB, both indicating they failed over.

Figure 42 Sample Status Output

id-4503-2>en		
Password:		
id-4503-2#show auth se	ssion int f2/1	
Interface:	FastEthernet2/1	
MAC Address:	0018.f809.cfc6	
IP Address:	10.200.10.201	
Status:	Authz Failed	
Domain:	DATA	
Oper host mode:	multi-auth	
Oper control dir:	both	
Session timeout:	N/A	
Idle timeout:	N/A	
Common Session ID:	0AC8018000000000000990C	
Acct Session ID:	0x0000002	
Hand Le :	0×1A000000	
Runnable methods list:		
Method State		
dot1x Failed	over	
mab Failed	over	
id-4503-2#		214237

- **Step 3** To verify that there has been no disruption of network services for the hosts attached to this monitor mode-enabled switch/network, verify that DNS/DHCP is working using the **ipconfig** and **ping** commands on one of the PCs.
- **Step 4** From one of the PCs connected to the port for which you just verified the failed authentication from the previous exercise, access the command line dialogue.

For example, got to **Start > Run > CMD** and click **OK** (see Figure 43).



Figure 43 Accessing the Command Prompt

Step 5 From the command prompt, type **ipconfig**.

Your output should be similar to that shown in Figure 44. Notice the host has an IP address.

Figure 44 Sample ipconfig Output

📾 Command Prompt	- 🗆 🗙
Microsoft Windows XP [Version 5.1.2600] (C) Copyright 1985-2001 Microsoft Corp.	-
C:\Documents and Settings\Administrator.IDUX>ipconfig	
Windows IP Configuration	
Ethernet adapter Connected to IP Phone 7960 on id-4503-2 F2-1:	
Connection-specific DNS Suffix . : idux.local IP Address : 10.200.10.203 Subnet Mask : 255.255.255.0 Default Gateway : 10.200.10.1	
C:\Documents and Settings\Administrator.IDUX>	
	4230
	5

Step 6 Verify network connectivity by typing **ping** *<ip* address>.

For example, type **ping 10.200.1.117** for the Microsoft AD Server, or use the IP address you assigned your AD server. Your output should be similar to that shown in Figure 45.

Figure 45 Verifying Network Connectivity

📾 Command Prompt	- 🗆 🗙
Windows IP Configuration	▲ I
Ethernet adapter Connected to IP Phone 7960 on id-4503-2 F2-1:	
Connection-specific DNS Suffix . : idux.local IP Address : 10.200.10.203 Subnet Mask : 255.255.255.0 Default Gateway : 10.200.10.1	
C:\Documents and Settings\Administrator.IDUX>ping 10.200.1.117	
Pinging 10.200.1.117 with 32 bytes of data:	
Reply from 10.200.1.117: bytes=32 time<1ms TTL=127 Reply from 10.200.1.117: bytes=32 time<1ms TTL=127 Reply from 10.200.1.117: bytes=32 time<1ms TTL=127 Reply from 10.200.1.117: bytes=32 time<1ms TTL=127	
Ping statistics for 10.200.1.117: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms	
C:\Documents and Settings\Administrator.IDUX>_	- 1420

Step 7 Verify that the client PC can still join the AD domain by logging out and logging back into the Windows PC domain (see Figure 46).

Log On to W	lindows
Copyright © 1985 Microsoft Corporal	2001 2001 Microsoft Professional Microsoft
User name: Password:	Administrator
Log on to:	IDUX Log on using dial-up connection
	OK Cancel Shut Down Options <<

Figure 46 Logging into Windows PC Domain

Step 8 Using the Windows Internet Explorer, verify that you can access the web server hosted on your network (see Figure 47).

This example uses a default page on the Windows AD Server.

ſ



Figure 47 Accessing the Web Server

Verifying that IP Phones are Working

Check to see that the IP phones have obtained IP addresses and verify that they have a dial tone, indicating they have associated with the Cisco Call Manager.

Verifying that Devices such as IP Cameras Work

To verify that your IP cameras work, complete the following steps.

Procedure

- **Step 1** Using Internet Explorer, browse to the IP address of one of your Cisco MediaNet IP Video Cameras; for example, http://10.200.10.202.
- Step 2 When prompted for login credentials, enter admin for the username and Cisco123 for the password.

After you have authenticated, you see whatever your camera is viewing (see Figure 48). You may need to adjust the focus ring to focus the video.

I



Figure 48 Accessing the IP Camera

Implementing Low Impact Mode

This section includes the following topics:

- Low Impact Mode Overview, page 43
- Configuring Cisco ACS, page 44
- Configuring Access Policies, page 55
- Configuring the Switch, page 78
- Verifying Low Impact Mode, page 85

Low Impact Mode Overview

I

Low impact mode enables you to incrementally increase the security level by configuring an ingress port ACL on the Open Access TrustSec-enabled port. This provides basic connectivity for guests, contractors, and unauthenticated hosts while selectively limiting access to introduce a higher level of access security.

Additionally, differentiated access can be accommodated based on successful authentication and authorization by combining downloadable ACLs (dACLs) with the Cisco TrustSec-enabled port, which uses 802.1X, MAB, and/or WebAuth.

Combined with dACLs for successfully authenticated users and hosts, you can create profiles to grant or deny access to network resources based on need and your security policies, as shown in Table 4. This enables differentiated services while still maintaining secure network connectivity for legacy hosts.

Table 4 Profiles

Profile Name	Description	VLAN	dACL
Phone-Authz	Policy to map IP phones to voice VLAN	VOICE	CorpAssetACL
Managed-Asset-Authz	Policy to be applied to managed assets	n/a	CorpAssetACL
MediaNet-Authz	Policy for Cisco MediaNet endpoints	n/a	CorpAssetACL
CorpUser-Authz	Policy for valid AD authenticated Users	n/a	CorpUserACL
Contractor-Authz	Policy for short-term contractors	n/a	ContractorACL

Configuring Cisco ACS

This section includes the following topics:

- Configuring Active Directory Groups, page 44
- Configuring ACS Policy Elements, page 47
- Configuring Authorization Profiles, page 50

Configuring Active Directory Groups

Before configuring policies, you need to select some Active Directory groups so they are available for subsequent steps.

Complete the following steps.

Procedure

Step 1 Go to Users and Identity Store > External Identity Stores > Active Directory (see Figure 49).

	Directory Gr		
Network Resources	General Directory Gr	oups Directory Attributes	Ē
🕶 🎒 Users and Identity Stores	* Active Directory Don	nain lidux local	
Identity Groups	Name:	Journood	
Internal Identity Stores	Please specify the cre	dentials used to join this machine to the Active Directory Domain:	
Hosts	*Username:	administrator	
 External Identity Stores LDAP 	*Password:		
Active Directory Certificate Authorities	You may use the Test	Connection Button to ensure credentials are correct and Active Directory Domain is	
Certificate Authentication Profile	reachable.	Test Connection	
Identity Store Sequences	Click on 'Save Chang have successfully con be available for use in	es' to connect to the Active Directory Domain and save this configuration. Once you nected to the Domain, you can select the Directory Groups and Directory Attributes to 1 policy rules.	
	End User Authentic	cation Settings	
	Enable password	d change	
	🔽 Enable machine	authentication	
Sp Policy Elements	Enable Machine	Access Restrictions	
Access Policies	Aging time (hour	s): 6	_
Monitoring and Reports	Connectivity Status	s	•
System Administration	Save Changes	Discard Changes Clear Configuration	

Figure 49 Active Directory

Step 2 Select the **Directory Groups** tab (see Figure 50).

Figure 50	Active Directory—Directory Groups
-----------	-----------------------------------

Users and Identity Stores: External Identity Stores > Active Directory
General Directory Groups Directory Attributes
Directory groups must be selected on this page to be available as options in group mapping conditions in policy ru 'Select' to launch a dialog to select groups from the directory.
Selected Directory Groups:
Salact [Decelert]
*Required fields

- **Step 3** In this window, do the following:
 - a. Click Select.

Γ

b. Scroll down and select /Users/Domain Computers and /Users/Domain Users (see Figure 51).

earch Base DN DC=idux,DC=local arch Filter Go Group Name ▲ Group Type idux.local/Users/DHCP Users LOCAL idux.local/Users/DnSAdmins LOCAL idux.local/Users/DnsUpdateProxy GLOBAL idux.local/Users/Domain Admins GLOBAL idux.local/Users/Domain Computers GLOBAL idux.local/Users/Domain Controllers GLOBAL idux.local/Users/Domain Guests GLOBAL idux.local/Users/Domain Users GLOBAL idux.local/Users/Domain Users GLOBAL idux.local/Users/Domain Users GLOBAL idux.local/Users/Domain Users GLOBAL idux.local/Users/Enterprise Admins GLOBAL idux.local/Users/Enterprise Admins GLOBAL idux.local/Users/Enterprise Admins GLOBAL idux.local/Users/Enterprise Admins GLOBAL idux.local/Users/Enterprise Admins GLOBAL idux.local/Users/HelpServicesGroup Cereator Owners GLOBAL	External User Groups	
iearch Filter	Search Base DN DC=idux,DC=local	
Group Name ▲ Group Type idux.local/Users/DHCP Users LOCAL idux.local/Users/DnsAdmins LOCAL idux.local/Users/DnsUpdateProxy GLOBAL idux.local/Users/Domain Admins GLOBAL idux.local/Users/Domain Computers GLOBAL idux.local/Users/Domain Computers GLOBAL idux.local/Users/Domain Controllers GLOBAL idux.local/Users/Domain Guests GLOBAL idux.local/Users/Domain Users GLOBAL idux.local/Users/Domain Users GLOBAL idux.local/Users/Domain Users GLOBAL idux.local/Users/Pomain Users GLOBAL idux.local/Users/Pomain Users GLOBAL idux.local/Users/Finterprise Admins GLOBAL idux.local/Users/Finterprise Admins GLOBAL idux.local/Users/HelpServicesGroup GLOBAL	Search Filter	io
idux.local/Users/DHCP Users LOCAL idux.local/Users/DnsAdmins LOCAL idux.local/Users/DnsUpdateProxy GLOBAL idux.local/Users/Domain Admins GLOBAL idux.local/Users/Domain Computers GLOBAL idux.local/Users/Domain Computers GLOBAL idux.local/Users/Domain Computers GLOBAL idux.local/Users/Domain Computers GLOBAL idux.local/Users/Domain Guests GLOBAL idux.local/Users/Domain Users GLOBAL idux.local/Users/Domain Users GLOBAL idux.local/Users/Enterprise Admins GLOBAL idux.local/Users/Feterprise Admins GLOBAL idux.local/Users/HelpServicesGroup GLOBAL	Group Name A	Group Type
idux.local/Users/DnsAdmins LOCAL idux.local/Users/DnsUpdateProxy GLOBAL idux.local/Users/Domain Admins GLOBAL idux.local/Users/Domain Computers GLOBAL idux.local/Users/Domain Computers GLOBAL idux.local/Users/Domain Controllers GLOBAL idux.local/Users/Domain Guests GLOBAL idux.local/Users/Domain Users GLOBAL idux.local/Users/Domain Users GLOBAL idux.local/Users/Enterprise Admins GLOBAL idux.local/Users/Fenterprise Admins GLOBAL idux.local/Users/HelpServicesGroup LOCAL	idux.local/Users/DHCP Users	LOCAL
idux.local/Users/DnsUpdateProxy GLOBAL idux.local/Users/Domain Admins GLOBAL idux.local/Users/Domain Computers GLOBAL idux.local/Users/Domain Controllers GLOBAL idux.local/Users/Domain Controllers GLOBAL idux.local/Users/Domain Controllers GLOBAL idux.local/Users/Domain Controllers GLOBAL idux.local/Users/Domain Guests GLOBAL idux.local/Users/Domain Users GLOBAL idux.local/Users/Enterprise Admins GLOBAL idux.local/Users/Fnterprise Admins GLOBAL idux.local/Users/HelpServicesGroup LOCAL	idux.local/Users/DnsAdmins	LOCAL
idux.local/Users/Domain Admins GLOBAL idux.local/Users/Domain Computers GLOBAL idux.local/Users/Domain Controllers GLOBAL idux.local/Users/Domain Guests GLOBAL idux.local/Users/Domain Guests GLOBAL idux.local/Users/Domain Users GLOBAL idux.local/Users/Domain Users GLOBAL idux.local/Users/Enterprise Admins GLOBAL idux.local/Users/Fenterprise Admins GLOBAL idux.local/Users/HelpServicesGroup GLOBAL	idux.local/Users/DnsUpdateProxy	GLOBAL
idux.local/Users/Domain Computers GLOBAL idux.local/Users/Domain Controllers GLOBAL idux.local/Users/Domain Guests GLOBAL idux.local/Users/Domain Users GLOBAL idux.local/Users/Domain Users GLOBAL idux.local/Users/Enterprise Admins GLOBAL idux.local/Users/Fenterprise Admins GLOBAL idux.local/Users/Fenterprise Admins GLOBAL idux.local/Users/HelpServicesGroup LOCAL	idux.local/Users/Domain Admins	GLOBAL
idux.local/Users/Domain Controllers GLOBAL idux.local/Users/Domain Guests GLOBAL idux.local/Users/Domain Users GLOBAL idux.local/Users/Enterprise Admins GLOBAL idux.local/Users/Group Policy Creator Owners GLOBAL idux.local/Users/HelpServicesGroup LOCAL	idux.local/Users/Domain Computers	GLOBAL
idux.local/Users/Domain Guests GLOBAL idux.local/Users/Domain Users GLOBAL idux.local/Users/Enterprise Admins GLOBAL idux.local/Users/Group Policy Creator Owners GLOBAL idux.local/Users/HelpServicesGroup LOCAL	idux.local/Users/Domain Controllers	GLOBAL
idux.local/Users/Domain Users GLOBAL idux.local/Users/Enterprise Admins GLOBAL idux.local/Users/Group Policy Creator Owners GLOBAL idux.local/Users/HelpServicesGroup LOCAL	idux.local/Users/Domain Guests	GLOBAL
idux.local/Users/Enterprise Admins GLOBAL idux.local/Users/Group Policy Creator Owners GLOBAL idux.local/Users/HelpServicesGroup LOCAL	idux.local/Users/Domain Users	GLOBAL
idux.local/Users/Group Policy Creator Owners GLOBAL idux.local/Users/HelpServicesGroup LOCAL	idux.local/Users/Enterprise Admins	GLOBAL
idux.local/Users/HelpServicesGroup LOCAL	idux.local/Users/Group Policy Creator Owners	GLOBAL
	idux.local/Users/HelpServicesGroup	LOCAL
	Database: Active Directory Use * for wildcard search (i.e. admin*) Search filter applies to group name and not the fully qualified	path.
Database: Active Directory Use * for wildcard search (i.e. admin*) Search filter applies to group name and not the fully qualified path.	(•

1

Figure 51 Selecting Group Names

Note

Your domain name will most likely be different than demo.local; for example, yourcompany.com.

c. Click OK.

The window shown in Figure 52 appears, showing the Directory Groups you selected.

Figure 52 Selected Directory Groups

sers and Identity Stores: External Identity Stores > Active Directory	
General Directory Groups Directory Attributes	
Directory groups must be selected on this page to be available as options in group mapping conditions in policy rules. Clicl Select' to launch a dialog to select groups from the directory.	<
Selected Directory Groups:	
idux.local/Users/Domain Computers idux.local/Users/Domain Users	
Select Deselect	

Step 4 Click Save Changes.

Configuring ACS Policy Elements

This section describes how to create and/or modify the three ACS policy components listed in Table 5, which are linked together for the authorization policies.

ACS Component Type	Section within the ACS GUI	Comments	
Downloadable ACLs (dACL)	Policy Elements > Authorizations and Permission > Named Permission Objects	Named ACLs that can be associated with different authorization profiles	
Authorization profiles	Access Policies > Access Services > Named Access Service	Named profiles that allow you to provide different permission or policies to different groups	
Authorization profiles	Policy Elements > Authorizations and Permission > Network Access	These authorization profiles are created within the access service; for example, 802.1X, MAB, and so on	

Table 5Three ACS Policy Components

This is an extensible approach that allows you to differentiate various types of request per access service, and to create and apply different policy based on groups.

The three dACLs listed in Table 6 will be used in the authorization profiles.



I

These are only sample ACLs. Consult with the InfoSec or Security staff of your organization to determine what is appropriate for your requirements.

Table 6 dACLs

Named dACL	ACE Permissions
CorpAssetACL	permit icmp any any log permit ip any any
CorpUserACL	permit icmp any any log permit ip any any
ContractorACL	remark Allow DHCP permit udp any eq bootpc any eq bootps remark Allow DNS permit udp any any eq domain remark Allow access to internet permit tcp any any eq www permit tcp any any eq 443 remark Allow IPSEC VPN permit udp any any eq 62515 permit udp any any eq isakmp permit udp any any eq 10000 permit udp any any eq 4500 permit esp any any permit ah any any

Complete the following steps.

Procedure

Step 1 To create the *CorpAssetACL* dACL, select **Policy Elements > Authorization and Permissions > Named Permission Objects > Downloadable ACLs** from the ACS web interface (see Figure 53). 1

1

Figure 53 Downloadable Access Control Lists

▶ 🛠 My Workspace	Policy Elements : Authorization and Permissions >	Named Permission Objects > Downloadable ACLs	
Network Resources	Downloadable Access Control Lists	Items 0-0 of 0 Rows per page: 🚺 💌	Go
Busers and Identity Stores Store	Filter: Match if:	🔹 Go 🔻	
 Policy Elements 	Name A	Description	٢
 Session Conditions Date and Time Custom Authorization and Permissions Network Access Authorization Profiles Security Groups Device Administration Named Permission Objects Downloadable ACLs Security Group ACLs 	No data to display		
Access Policies		R	
 Monitoring and Reports System Administration 	Create Duplicate Edit Delete	Page 1 of 1 d	>0
Done		🔒 🎯 Internet	

Step 2 Select Create.

Step 3 In the window shown in Figure 54, enter the name, description, and the ACL permissions from Table 6 for the *CorpAssetACL* dACL.

Policy Elements : Authorization and Permissions > Named Permis	sion Objects > <u>Downloadable ACLs</u> > Create
General	
*Name: CorpAssetACL	
Description: Full Access for Corporate Assets	
Downloadable ACL Content	
permit icmp any any log permit ip any any	<u> </u>
*	
	<u>_</u>
*Required fields	
	R
Submit Cancel	

Figure 54 Creating a dACL

Step 4 Click Submit.

ſ

Step 5 Repeat the above steps to enter the *CorpUserACL* and *ContractorACL* dACLs.

After you have created all three dACLs, you should see the information shown in Figure 55 under the Downloadable ACLs section.

Figure 55 Three dACLs

Policy	Elements : Authorization and Perr	missions > Named Permission Objects > Downloadable ACLs
Dow	nloadable Access Control List	s Items 1-3 of 3 Rows per page: 🚺 🗸 🤆
Filter	• Match if:	Go 🗸
	Name 🔺	Description
	ContractorACL	Restricted Access for Contractors
	CorpAssetACL	Full Access for Corporate Assets
	CorpUserACL	Full Access for Corporate Users

214249

Configuring Authorization Profiles

For low impact mode, create the five authorization profiles listed in Table 7. These profiles will be associated with identity groups and access services.

Profile Name Description V		VLAN	dACL
Phone-Authz	Policy to map IP phones to Voice VLAN	n/a	CorpAssetACL
Managed-Asset-Authz	Policy to be applied to Managed Assets	n/a	CorpAssetACL
MediaNet-Authz	Policy for Cisco MediaNet Endpoints	n/a	CorpAssetACL
CorpUser-Authz Policy for Valid AD Authenticated Users		n/a	CorpUserACL
Contractor-Authz Policy for short term r contractors		n/a	ContractorACL

Table 7Five Authorization Profiles

To create the five authorization profiles, complete the following steps.

Procedure

- Step 1 Go to Policy Elements > Authorizations and Permissions > Network Access > Authorization Profiles and select Create.
- **Step 2** In the screen shown in Figure 56, type **Phone-Authz** in the Name field and enter an appropriate description.

Figure 56 Authorization Profiles—General Tab

Policy Elements : Authorization and Permissions > Network Access > Authorization Profiles > Edit: "Phone-Aut	hz"
General Common Tasks RADIUS Attributes	
General	
* Name: Phone-Authz	
Description: Policy for IP Phones	ត
*Required fields	2142

Step 3 Select the **Common Tasks** tab (see Figure 57).

General Common Tasks	RADIUS Attributes
VLAN ID/Name:	Not in Use 💌
URL for Redirect:	Not in Use 💌
URL Redirect ACL:	Not in Use
ACLS	
Downloadable ACL Name:	Static Value CorpAssetAC -
IOS ACL Filter ID:	Not in Use 💌
Proxy ACL:	Not in Use 💌
QOS	
QOS Profile Name:	Not in Use 🔍
Input Policy Map:	Not in Use 🔍
Output Policy Map:	Not in Use 🔍
Voice VLAN	
Permission to Join:	Static Yes (device-traffic-class=voice)
Reauthentication	
Reauthentication Timer:	Not in Use 🔍
Maintain Connectivity durir Reauthentication:	g

Figure 57 Authorization Profiles—Common Tasks Tab

Step 4 Do the following:

I

- a. For Downloadable ACL Name, select Static.
- **b.** From the Value drop-down menu, select **CorpAssetACL**.
- c. In the Voice VLAN section, select Static from the Permission to Join drop-down menu.
- Step 5 Click the RADIUS Attributes tab.
- **Step 6** In the RADIUS Attributes tab, accept the defaults and click **Submit**.
- **Step 7** Create the *Managed-Asset-Authz* authorization profile by performing the above steps, using the information shown in Figure 58 and Figure 59.

Figure 58 Authorization Profiles—General Tab

General Common Tasks RADIUS Attributes General * Name: Managed-Asset-Authz	l	Policy Elem	nents : Authorizati	on and Permissions	> Network Access > <u>Authorization Profiles</u> > Create
General * Name: Managed-Asset-Authz		General	Common Tasks	RADIUS Attributes	
Description: Policy to be applied to Managed Assets		General * Name: Descrip	Managed-As	set-Authz applied to Managed #	Assets

General Common Tasks	RADIUS Attributes	
VLAN ID/Name:	Not in Use 💌	
URL for Redirect:	Not in Use 💌	
URL Redirect ACL:	Not in Use 👻	
ACLS		
Downloadable ACL Name:	Static 🔹	Value CorpAssetAC -
IOS ACL Filter ID:	Not in Use 💌	
Proxy ACL:	Not in Use 💌	
QOS		
QOS Profile Name:	Not in Use 💌	
Input Policy Map:	Not in Use 💌	
Output Policy Map:	Not in Use 💌	
Voice VLAN		<i>'</i> 0
Permission to Join:	Not in Use 💌	
Reauthentication		
Reauthentication Timer:	Not in Use 💌	
Maintain Connectivity during Reauthentication:	3	

1

Figure 59 Authorization Profiles—Common Tab

- **Step 8** Repeat the above steps to create the *MediaNet-Authz* profile.
- **Step 9** Repeat the above steps to create the *CorpUser-Authz* profile, using the information shown in Figure 60 and Figure 61.

In the Value drop-down menu in the ACLS section, select CorpUserACL.

Figure 60 Authorization Profiles—General Tab

Policy El	ements : Authorizati	ion and Permissions $>$ Network Access $>$ Authorization Profiles $>$ Crea	ite			
Genera	Common Tasks	RADIUS Attributes				
Gene	General					
* Nam	* Name: CorpUser-Authz					
Desc	ription: Policy for V	alid AD Authenticated Users	14255			
*Require	ed fields					

VLAN ID/Name: Not in Use URL for Redirect: Not in Use URL Redirect ACL: Not in Use ACLS Downloadable ACL Name: Static IOS ACL Filter ID: Not in Use Proxy ACL: Not in Use QOS QOS QOS Profile Name: Not in Use Input Policy Map: Not in Use Voice VLAN Permission to Join: Not in Use		RADIUS Attributes	Common Tasks	General
URL for Redirect: Not in Use URL Redirect ACL: Not in Use ACLS Downloadable ACL Name: Static Value CorpUserACL IOS ACL Filter ID: Not in Use Proxy ACL: Not in Use QOS QOS QOS QOS Output Policy Map: Not in Use Voice VLAN Permission to Join: Not in Use Reauthentication		Not in Use 💌	'Name:	VLAN ID/
URL Redirect ACL: Not in Use ACLS Downloadable ACL Name: Static Value CorpUserACL IOS ACL Filter ID: Not in Use Proxy ACL: Not in Use QOS QOS QOS Profile Name: Not in Use Input Policy Map: Not in Use Voice VLAN Permission to Join: Not in Use Reauthentication		Not in Use 💌	tedirect:	URL for R
ACLS Downloadable ACL Name: Static Value CorpUserACL IOS ACL Filter ID: Not in Use Proxy ACL: Not in Use QOS QOS QOS Profile Name: Not in Use Input Policy Map: Not in Use Voice VLAN Permission to Join: Not in Use Reauthentication		Not in Use 💌	rect ACL:	URL Redir
Downloadable ACL Name: Static Value CorpUserACL IOS ACL Filter ID: Not in Use Proxy ACL: Not in Use QOS QOS QOS Profile Name: Not in Use Input Policy Map: Not in Use Output Policy Map: Not in Use Voice VLAN Permission to Join: Not in Use Reauthentication				ACLS
IOS ACL Filter ID: Not in Use Proxy ACL: Not in Use QOS QOS QOS QOS Input Policy Map: Not in Use Voice VLAN Permission to Join: Not in Use Reauthentication	/alue CorpUserACL -	Static 💽	dable ACL Name:	Download
Proxy ACL: Not in Use QOS QOS Profile Name: Not in Use Input Policy Map: Not in Use Voice YLAN Permission to Join: Not in Use Reauthentication		Not in Use 💌	Filter ID:	IOS ACL
QOS QOS Profile Name: Not in Use Input Policy Map: Not in Use Output Policy Map: Not in Use Voice VLAN Permission to Join: Not in Use Reauthentication		Not in Use 💌	CL:	Proxy AC
QOS Profile Name: Not in Use Input Policy Map: Not in Use Output Policy Map: Not in Use Voice VLAN Permission to Join: Not in Use				QOS
Input Policy Map: Not in Use Output Policy Map: Not in Use Voice VLAN Permission to Join: Not in Use Reauthentication		Not in Use 💌	file Name:	QOS Prof
Output Policy Map: Not in Use Voice VLAN Permission to Join: Not in Use Reauthentication		Not in Use 💌	icy Map:	Input Poli
Voice VLAN Permission to Join: Not in Use Reauthentication		Not in Use 💌	olicy Map:	Output Po
Permission to Join: Not in Use 💌			LAN	Voice V
Reauthentication		Not in Use 💌	on to Join:	Permissio
			entication	Reauthe
Reauthentication Timer: Not in Use 💌		Not in Use 💌	ntication Timer:	Reauthen

Figure 61 Authorization Profiles—Common Tasks Tab

Step 10 Repeat the above steps to create the *Contractor Authz* profile, using the information shown in Figure 62 and Figure 63.

In the Value drop-down menu in the ACLS section, select ContractorACL.

Figure 62 Authorization Profiles—General Tab

l	Policy Elem	nents : Authorizati	on and Permissions $>$ Network Access $>$ Authorization Profiles $>$ C	reate		
	General	Common Tasks	RADIUS Attributes			
	General					
	* Name: Contractor-Authz					
	Descrip	otion: Policy for sh	ort term contractors	24257		

*Required fields

ſ

General Common	Tasks	RADIUS Attrib	outes	
VLAN ID/Name:		Not in Use	•	
URL for Redirect:	Ν	Not in Use	•	
URL Redirect ACL:	45	Not in Use	Ψ.	
ACLS				
Downloadable ACL N	lame:	Static	•	Value ContractorAC -
IOS ACL Filter ID:		Not in Use	¥	
Proxy ACL:		Not in Use	-	
QOS				
QOS Profile Name:		Not in Use	-	
Input Policy Map:		Not in Use	-	
Output Policy Map:		Not in Use	-	
Voice VLAN				
Permission to Join:		Not in Use	-	
Reauthentication				
Reauthentication Tim	ner:	Not in Use	-	
Maintain Connectivity Reauthentication:	y durin	3		

I

1

Figure 63 Authorization Profiles—Common Tasks Tab

Step 11 After you have created all the sample profiles, you should see the information shown in Figure 64 in your Authorization Profiles section.

Figure 64 Authorization Profiles

Policy Elements : Authorization and Permissions > Network Access > Authorization Profiles					
Auth	norization Profiles	Items 1-6 of 6 Rows per page: 50 💌			
Filte	r: 💽 Match if:	G0 V			
	Name 🔺	Description			
	Contractor-Authz	Policy for short term contractors			
	CorpUser-Authz	Policy for Valid AD Authenticated Users			
	Managed-Asset-Authz	Policy to be applied to Managed Assets			
	MediaNet-Authz	Policy for Cisco MediaNet Endpoints			
	Permit Access				
	Phone-Authz	Policy to map IP Phones to Voice VLAN			

Configuring Access Policies

This section includes the following topics:

- Configuring User and Identity Stores, page 55
- Adding Authorization Rules for 802.1X Service, page 60
- Adding Authorization Rules for MAB Service, page 68

Configuring User and Identity Stores

Table 8 lists the identity groups used in this section.

Table 8 Identity Groups

Group	Description	Comment
IP phones	Corporate managed IP phones	Added previously in monitor mode
MACHINES	Corporate managed machines such as printers, cameras, and so on	Added previously in monitor mode
Contractor	Contractors	New group to be added

Adding a Contractor Identity Group

To create the *Contractor* identity group, complete the following steps.

Procedure

- Step 1 Go to Users and Identity Stores > Identity Groups and select Create.
- **Step 2** Type in the group and description information listed for the Contractor identity group in Table 8.
- Step 3 Click Submit.

I

Creating Internal Identity Stores—Host for MAB

Next you will create entries for managed host devices and assign them to identity groups. These entries are used to provide authentication and authorization using MAB.

The information listed in Table 9 is provided as an example.

Table 9 Identity Group Information

MAC Address	Description	Identity Group
00-18-BA-C7-BC-EE	Cisco 7960 IP Phone (non-802.1X capable)	IP Phone
00-18-BA-C7-BC-FA	Cisco 7960 IP Phone (non-802.1X capable)	IP Phone
00-1D-E5-EB-E5-EF	Cisco IP Video Camera	MACHINE
00-1D-E5-EB-F9-00	Cisco IP Video Camera	MACHINE
00-21-86-58-DB-6B	Contractor PC (Non-managed host)	Contractor

Note

The Cisco 7961 Phone used in the example described in this guide is 802.1X-capable. Therefore, you do not need to enter it in the host database. It is added in the Users database in the next section.

Use Table 10 to record your own MAC addresses to accommodate the use cases described in this guide.

Table 10 MAC Address Reference List

MAC Address	Description	Identity Group
	Cisco IP Phone	IP Phone
	Cisco IP Phone	IP Phone
	Cisco IP Camera (or other non-dot1x host)	MACHINE
	Cisco IP Camera (or other non-dot1x host)	MACHINE
	Contractor PC	CONTRACTOR

To create entries for managed host devices and assign them to identity groups, complete the following steps.

Procedure

Step 1 Go to User and Identity Stores > Internal Identity Stores > Hosts (see Figure 65).

Figure 65 Users and Identity Stores—Hosts

Users and Identity S	tores: Internal Identity Stores > Hosts > Create	1	Cisco Secure ACS Pre-Release	Web Page Dialog	×
General		1.1	Identity Groups		
MAC address must	t be entered in the standard hyphen-separated format "01-23-45-67-89-ab"		Filter: Match	f: Go 💌	
*MAC Address:	00-18-BA-C7-BC-EE Status: Enabled 💌 😁				
Description:	Cisco 7960 IP Phone		Name *	Description	
* Identity Group:	All Groups Select.		C B All Groups	Identity Group Root	
-MAC Host Inform	ation		C • Contractor	Contractors	
There are no addit	ional identity attributes defined for MAC host records		O • IP Phones	Corporate Managed IP Phones	
* Required fields	,		O * MACHINES	Corporate Managed Machines (Printers, Cameras, etc.)	
					×
			Create Duplicate		
			OK Cancel		Help
	2		4		
Submit Cancel		1426	tps://acs5.idux.local/acsadmin/Identil	:yGroupsLPInputAction.do	Trusted sites

- **Step 2** In the Identity Groups screen, select **Create.**
- **Step 3** In the screen shown in Figure 66, do the following:
 - a. Type the MAC address and description, using the information from Table 9.
 - **b.** Click the **Select** button for Identity Group selection and select the appropriate group.

I

c. Click OK, then click Submit.

General MAC address must	the entered in the standard hyphen-separated format "01-23-45-67-89-ah"	
MAC Address	00-18-BA-C7-BC-EE Status: Enabled	
Description:	Cisco 7960 IP Phone	
Identity Group:	All Groups: IP Phones Select	
MAC Host Inform There are no addit	ation ional identity attributes defined for MAC host records	

Figure 66 Users and Identity Stores—Create

Step 4 Repeat the above steps to enter the other MAC addresses listed in Table 9.

After you have entered all the MAC addresses for your pilot, your host database should look like the screen shown in Figure 67.

Isers and Identity Stores: Internal Identity Stores > Hosts						
Inter	nal Hosts		Items 1-5 of 5 Rows per page: 50 💌 🤇			
Filter		Match if:	G0 ▼			
	Status	MAC Address	Identity Group	Description A		
	0	01-18-ba-c7-bc-ee	All Groups: IP Phones	Cisco 7960 IP Phone		
	0	00-18-ba-c7-bc-fa	All Groups: IP Phones	Cisco 7960 IP Phone		
	0	00-1d-e5-eb-e5-ef	All Groups:MACHINES	Cisco MediaNet IP Video Camera		
	0	00-1d-e5-eb-f9-00	All Groups:MACHINES	Cisco MediaNet IP Video Camera		
	Θ	00-21-86-58-db-6b	All Groups:Contractor	Contractor PC		

Figure 67 Internal Hosts



Cisco offers products that can automate the process of building a database of profiled MAC addresses. The installation and configuration of those products are covered in another document. Additionally, if you already have a database of known valid MAC addresses from an asset management system, those may be imported into the internal database of ACS. Consult the ACS User Guide for more information. For more information on Cisco ACS 5.0, see the following URL:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.0/user/guide/ACS _user_guide.html

Configuring Internal Identity Stores—Users for 802.1X

Next you will create entries for managed host devices and assign them to identity groups. These are used to provide authentication and authorization, using 802.1X for identities that are not maintained in your external identity management (IdM) system.



This internal database can be used to create accounts for 802.1X-capable phones, administration, bootstrapping, troubleshooting, and other uses without having to add a user into your official IdM system; for example, Microsoft AD. Where possible, the use of existing identity repositories such as AD is recommended as a best practice. However, certain use cases may require the use of the internal database within ACS. Follow the security policies of your company in this matter.

The information shown in Table 11 is provided as an example.

Table 11 Managed Host Device Information

Host ID	Description	MD5 Password	Identity Group
CP-7961G-SEP001BD58539 1E	Cisco 7961G 802.1X-capable IP Phone	password	IP Phones

Use Table 12 to record your own MAC addresses to accommodate the use cases described in this guide.

Table 12 Managed Host Reference List

Host ID	Description	MD5 Password	Identity Group

To create entries for managed host devices and assign them to identity groups, complete the following steps.

I

Procedure

Step 1 Go to User and Identity Stores > Internal Identity Stores > Users (see Figure 68).

Image:	Internal Users		Items 0-0 of	0 Rows per page: 50 💌 G
🗸 🎒 Users and Identity Stores	Filter:	Match if:	Go 🔻	
Identity Groups Internal Identity Stores	T Status	User Name 🔺	Identity Group	Description
Hosts	No data to display			
External Identity Stores LDAP				
Active Directory				
Certificate Authorities				
Certificate Authentication Profile	4			
Policy Elements				
Access Policies				
Monitoring and Reports	Create Duplicate	Edit Delete I Import		200 1 of 1 14 4 0 0
System Administration		inport	- P	age _ I OI I II II II II II

Figure 68 Internal Users

Step 2 Select Create.

ſ

Step 3 In the screen shown in Figure 69, do the following:

- a. Type the UserID for example, CP-7961G-SEP001BD585391E
- b. Type an appropriate description; for example, Cisco 7961G 802.1X Capable IP Phone.
- c. Type a password; for example, pa\$\$Word4.

This password must match the one you configured on your host. In this case, *pa\$\$Word4* is used for the password on the Cisco 7961G IP Phone.

Figure 69 Creating an Entry

Users and Ident	tity Stores: Internal Iden	tity Stores > <u>Users</u> > Create	
General			
*Name:	CP-7961G-SEP001BD	58539: Status: Enabled 💌 😁	
Description:	Cisco 7961G 802.1X C	Capable IP Phone	
* Identity Grou	p: All Groups:IP Phones	Select	
Authenticati	on I formation		
🗌 Change p	bassword on next login		
* Password:	•••••	* Confirm Password:	
Enable Passw	ord:	Confirm Password:	
User Inform	ation		
There are no	additional identity attribut	tes defined for user records	
* Required field	s		6

Step 4 For Identity Group, click **Select** and select the appropriate group; for example, **All Groups:IP Phones** (see Figure 70). Then click **OK**.

Identity Groups				
Filter: Match if: Go 🗸				
	Name 🔺	Description		
0	All Groups	Identity Group Root		
0	 Contractor 	Contracted Staff		
۲	IP Phones	Corporate Managed IP Phones		
0	* MACHINES	Corporate Managed Machines (Printers, Cameras, etc.)		

Figure 70 Identity Groups

Step 5 Click Submit.

You should now see your entry in the Internal Users database, as shown in Figure 71.

Figure 71 Internal Users Database

Interna	al User	's		Items 1-1 of 1 Rows per page: 50
Filter:		▼ Match if:	🔹 G0 🗢	
□ s ^r	tatus	User Name 🔺	Identity Group	Description

Adding Authorization Rules for 802.1X Service

For low impact mode, you will now add new authorization rules to allow for differentiated services between the various groups or classes of users and hosts.

Adding an 802.1X-Capable Phones Authorization Rule

Complete the following steps.

Procedure

Step 1 Go to Access Policies > Access Services > 802.1X > Authorization (see Figure 72).

• 🛠 My Workspace	Access Policies: <u>Access Services</u> > 802.1X > Authorization
• 🔄 Network Resources	Standard Policy Exception Policy
Busers and Identity Stores Store	Network Access Authorization Policy
Policy Elements	Filter: Status 🔹 Match if: Equals 🔹 💽 Glear Filter 🛛 Go 🗢
Access Policies	Conditions Results
Service Selection	Status Name Compound Condition Authorization Profiles Security Group
B OC2.1X Identity Authorization Default Device Admin Default Network Access Identity Group Mapping Authorization MAB TrustSec Access Control	No data to display
Monitoring and Reports	

Figure 72 Network Access Authorization Policy

- Step 2 To set up an authorization policy for 802.1X-capable IP phones, click Create.
- **Step 3** In the screen shown in Figure 73, do the following:

ſ

- a. For the Name, enter a new name; for example, Match-1X-Phone-Authz.
- **b.** Select the **Compound Condition** checkbox.
- c. From the Dictionary drop-down menu, select System.

ieneral		- ^
ame: Match-1X-Phone-Auth	z Status: Enabled 💽 \Theta	
The Customize button i conditions and results a	n the lower right area of the policy rules screen controls which policy are available here for use in policy rules.	
onditions		-
Compound Condition:		
C ondition: Dictionary:	Attribute:	
System 💌	IdentityGroup Select	
Operator:	Value:	
in 💌	All Groups: IP Phones Select	
Current Condition Set:		
→ bbA	Edit A Replace V	
System: I	dentityGroup in All Groups: IP Phones	
And > • Or > •		
U	Delete Preview	_
esults		_
uthorization Profiles:		
Cancel	If desired, you can select more than one authorization profile, to define a 'merged' authorization result. Note that the order is significant for resolving any conflicts that	t Help

1

Figure 73 Creating an Authorization Policy

d. For Attribute, click **Select** and select **IdentityGroup** (see Figure 74).

Atti	ibutes List	Items 1-13 of 13 Rows per page: 50 💌 Go
	Attribute	Туре
0	AuthenticationMethod	Enumeration
С	AuthenticationStatus	Enumeration
0	Device IP Address	IPv4 Address
C	HostName	String
۲	Identity Group	Hierarchy
С	NACRadiusPolicyStatus	Enumeration
0	NACRadiusRole	String
С	NACRadiusUserName	String
0	Protocol	Enumeration
С	Time And Date	Date Time Period
0	UseCase	Enumeration
С	UserName	String
0	WasMachineAuthenticated	Boolean
		Page 1 of 1 14 4 D
ок∣	Cancel	Help
:ps://	acs5.idux.local/acsadmin/DictionaryAcsLPInputAction.do	🥥 Internet

Figure 74 Attribute List

e. Click OK.

Γ

- f. In the Operator drop-down menu, make sure that In is selected.
- g. Click Select to select IP Phones from the Network Device Groups list (see Figure 75).

Figure 75 Network Device Groups

etwork Device Groups		
lter: 🗾 Mat	ch if: Go 🔻	
Name 🔺	Description	
🗇 🖃 All Groups	Identity Group Root	
Contractor	Contracted Staff	
• IP Phones	Corporate Managed IP Phones	
* MACHINES	Corporate Managed Machines (Printers, Cameras, etc.)	
(Cancel		Help

Step 4 Select Add.
Step 5 In the Results/Authorization Profiles section, click Select.
Step 6 Select the previously created Phone-Authz profile (see Figure 76).

uthorization Profile	s	Items 1-	-7 of 7 Rows per page:	50 💽 Go
ilter:	Match if:	▼ G0 ▼		
	Name 🔺	Description	ı	
Contractor-Authz		Policy for short term contractors		-
CorpUser-Authz		Policy for Valid AD Authenticated Users		
DenyAccess				
Managed-Asset-A	uthz	Policy to be applied to Managed Assets		
MediaNet-Authz		Policy for Cisco MediaNet Endpoints		
Permit Access	l	\$		
Phone-Authz		Policy to map IP Phones to Voice VLAN		
	1 1 1		Page 1 of 1	

Figure 76 Authorization Profiles List

Step 7 Click **OK** and then click **OK** again.

Click Save Changes.

Adding 802.1X-CorpUserRule

Complete the following steps.

Procedure

- **Step 1** In the screen shown in Figure 72, click **Create**.
- **Step 2** In the screen shown in Figure 77, do the following:
 - a. For the Name, enter a new name; for example, 802.1X-CorpUserRule.
 - **b.** Select the **Compound Condition** checkbox.
 - c. From the Dictionary drop-down menu, select AD-AD1.
 - d. From the attribute list, press Select to select ExternalGroups.
 - e. Click OK.
 - f. In the **Operator** drop-down menu, make sure that **contains any** is selected.

General		_
Name: 802.1X-CorpUserRule	Status: Enabled 🔽 😑	
The Customize button i conditions and results a	in the lower right area of the policy rules screen controls which policy are available here for use in policy rules.	У
Conditions		
Compound Condition:		
Condition:		
Dictionary:	Attribute:	
AD-AD1 💌	ExternalGroups Select	
Operator:	Value:	
contains any 💌		
Current Condition Set:	Select Deselect Clear	
Add 🗸	Edit 🔨 Replace V	
And > T		
HING P		
Or > •		
	_	
	Delete Device	
	Delete Preview	-
K Cancel		Help

Figure 77 Creating an Authorization Policy

Γ

Step 3 Click **Select** and select /Users/Domain Users from the Network Device Groups screen (see Figure 78).

ring Enum Definition	Items 1-2 of 2 Rows per page: 50 💌 G
lter: 💽 Match if: 💽 🔽 Go 🔻	
Enum	Name 🔺
idux.local/Users/Domain Computers	
idux.local/Users/Domain Users	
	Page 1 of 1 🔣 🖉 🕨
Cancel	
Calicer	

1

Figure 78 Network Device Groups

- Step 4 Click OK.
- Step 5 Click Add V (see Figure 79).

Figure 79	Clicking Add V
-----------	----------------

General	A
lame: 802.1X-CorpUserRule	Status: Enabled 💌 😑
The Customize button conditions and results	n the lower right area of the policy rules screen controls which policy are available here for use in policy rules.
Conditions	
Compound Condition:	
Condition:	
Dictionary:	Attribute:
AD-AD1	ExternalGroups Select
Operator:	Value:
contains any 💌	
	Select Deselect Clear
Current Condition Set:	
→ Add	Edit A Replace V
AD-AD1:	ExternalGroups contains any idux.local/Users/Doma 🔺
And > • Or > •	
KCancel	Delete Preview 👻 Help
	- Frank Andrew de

- Step 6 Scroll down to the Results/Authorization Profiles section and click Select.
- Step 7 Select the previously created CorpUser-Authz profile (see Figure 80).

Authorizatio	on Profiles	Items 1-7 of 7 Rows	per page: 50 💌 Go
Filter:	▼ Match if:	Go 🔻	
	Name 🔺	Description	
Contrac	ctor-Authz	Policy for short term contractors	
CorpUs	er-Authz	Policy for Valid AD Authenticated Users	
DenyAc	ccess		
Manage	ed-Asset-Authz	Policy to be applied to Managed Assets	
MediaNe	et-Authz	Policy for Cisco MediaNet Endpoints	
Permit /	Access		
Phone-/	Authz	Policy to map IP Phones to Voice VLAN	
Create	Duplicate Edit Delete	Page 1	of 1 🚺 🚽 🕨 🕅 Help

Figure 80 Authorization Profiles List

Step 8 Click OK and then OK again.

Step 9 Click Save Changes.

Γ

Now you should see both the *Match-1X-Phone-Authz* and the *802.1X-CorpUserRules* as authorizations for 802.1X (see Figure 81).





For now, this is all you will create for 802.1X in low impact mode. If your organization has more types of wired 802.1X devices, you may want to try adding more.

As demonstrated in the previous exercises, you used the previously created dACLs and authorization profiles in creating these specific authorization rules for 802.1X. Next, you will do a similar configuration of authorization rules for MAB.

Adding Authorization Rules for MAB Service

MAB IP Phones Rule

In this section you will set up an identity source and authorization rule to match IP phones in the MAB access service. This ensures that the MAB authenticated phones are put into the voice VLAN for proper access. All successfully authenticated non-802.1X phones obtain the Phone-Authz profile, which allows full access to the voice VLAN with no ACL restrictions; that is, **permit ip any any**.

I

Complete the following steps.

Procedure

- **Step 1** From the MAB Access Service section, select **Identity** (see the left-hand side of Figure 82).
- Step 2 Press Select.
- Step 3 In the screen shown in the right-hand side of Figure 82, do the following:
 - a. Select Internal Hosts.
 - b. Click OK.
 - c. Click Submit.

Figure 82 Selecting Internal Hosts

Access Ballalan	Identi	ty Store		Showing 1-8 of 8 50	🔹 per page 🕜
Access Policies Access Services	Filter	:	Match if: Go 🗢		
Service Selection Rules		Name 🔺	Description		1
- O 802.1X	0	802.1X-TrustSec			1
Identity	0	AD1			4
Authorization	0	All_ID_Stores			
Default Device Admin	0	CN Username	Predefined Certificate Authentication Profile		
O Duluuit Network Access	0	DenyAccess			
	0	Internal Hosts			
Authorization	0	Internal Users			1
Trustoco Aucos Control	0	NAC Profiler	Default Entry for NAC Profiler		

- Step 4 From the MAB Access Service section, select Authorization and click Create.
- **Step 5** In the screen shown in Figure 83, do the following:

I

- a. For the name, enter an appropriate name; for example, MAB-Phone-Authz.
- **b.** Check the **Compound Condition** checkbox.
- c. From the Dictionary drop-down menu, select System and then click Select.

Figure 83 Creating an Authorization Policy

Cisco Secure ACS Pre-F	Release Web Page Dialog	×
General		-
Name: MAB-Phone-Aut	thz Status: Disabled 💌 🖉	
The Customize bu conditions and re	utton in the lower right area of the policy rules screen controls which policy sults are available here for use in policy rules.	
Conditions		1
Compound Conditio	on:	
Condition:		
Dictionary:	Attribute:	
System	✓ IdentityGroup Select	
Operator:	Value:	
in 💌	All Groups: IP Phones Select	
Current Condition S	et:	
Α	Add V Edit ∧ Replace V	
Sx.	stem:IdentityGroup in All Groups: IP Phones	
And > • Or > •	r2	
	Delete Preview	
Results		1
uthorization Profiles:		
Phone-Authz	If desired, you can select more than one authorization profile, to define a 'merged' authorization result. Note that the order is significant for resolving any conflicts that	•
Cancel		Help
s://acs5.idux.local/acsadn	nin/PolicyInputAction.do	
	1 · · · · · · · · · · · · · · · · · · ·	

Step 6 From the Attribute List (see Figure 84), select Identity Group and click OK.

Attr	ibutes List	Items 1-13 of 13 Rows per page: 50 💌 Go
	Attribute	Туре
0	AuthenticationMethod	Enumeration
$^{\circ}$	AuthenticationStatus	Enumeration
0	Device IP Address	IPv4 Address
0	HostName	String
۲	IdentityGroup	Hierarchy
$^{\circ}$	NACRadiusPolicyStatus	Enumeration
$^{\circ}$	NACRadiusRole	String
$^{\circ}$	NACRadiusUserName	String
0	Protocol	Enumeration
0	Time And Date	Date Time Period
0	UseCase	Enumeration
0	UserName	String
0	WasMachineAuthenticated	Boolean
		Page 1 of 1 14 4 D
ок	Cancel	Help

1

Figure 84 Attributes List

- Step 7 In the Operator drop-down menu, make sure that In is selected and click Select.
- **Step 8** From the Network Device Groups list, select **IP Phones** (see Figure 85).

Figure 85 Network Device Groups

letwork Device Groups		
ilter: 🗾 Ma	tch if: Go 🗢	
Name 🔺	Description	
🗅 🖃 All Groups	Identity Group Root	-
Contractor	Contracted Staff	
• IP Phones	Corporate Managed IP Phones	
MACHINES	Corporate Managed Machines (Printers, Cameras, etc.)	
K Cancel		<u>–</u> Help

- Step 9 Click Add.
- **Step 10** In the Results/Authorization Profiles section, click **Select** and select the previously created **Phone-Authz** profile (see Figure 86).

- della	orization Profiles		Items 1-	7 of 7 Rowsperp	age: 50 💽 Go
Filter	r: 🔽 N	1atch if:	▼ G0 ▼		
	N	lame 🔺	Description		
	Contractor-Authz		Policy for short term contractors		A
	CorpUser-Authz		Policy for Valid AD Authenticated Users		
	DenyAccess				
	Managed-Asset-Au	thz	Policy to be applied to Managed Assets		
	MediaNet-Authz		Policy for Cisco MediaNet Endpoints		
	Permit Access				
~	Phone-Authz	2	Policy to map IP Phones to Voice VLAN		
Cre	eate Duplicate	Edit Delete		Page 1 of 1	

Figure 86 Authorization Profiles List

- Step 11 Click OK and then click OK again.
- Step 12 Click Save Changes.

Adding a MAB Contractor Rule

To add a MAB contractor rule, complete the following steps.

Procedure

ſ

- Step 1 From the MAB Access Service section, select Authorization and click Create.
- **Step 2** In the window shown in Figure 87, do the following:
 - a. For the Name, enter an appropriate name; for example, MAB-Contractor-Authz.
 - **b.** Select Compound Condition
 - c. From the Dictionary drop-down menu, select System and then press the Select button.

General		
Name: MAB-Contracto	Authz Status: Enabled 💌 🖲	
The Customize bu conditions and re	tton in the lower right area of the policy rules screen controls which policy sults are available here for use in policy rules.	
Conditions		
Compound Condition	n:	
Condition:		
Dictionary:	Attribute:	
System	✓ IdentityGroup Select	
Operator:	Value:	
in 💌	All Groups:Contractor	
Current Condition S	et:	
4	dd ∨ Edit ∧ Replace ∨	
Sy	tem:IdentityGroup in All Groups:Contractor	
And > • Or > •		
	-	
U	Delete Preview	_
Results		
uthorization Profiles:		
Contractor-Authz	If desired, you can select more than one authorization profile, to define a 'merged' authorization result. Note that	
K Cancel	the order is significant for resolving any conflicts that	.▼ elp

1

Figure 87 Creating an Authorization Policy

Step 3 From the Attribute List (see Figure 88), select **Identity Group** and then click **OK**.
Attributes List Items 1-13 of 13 Rows per page: 50 🔽 G			
	Attribute	Туре	
0	AuthenticationMethod	Enumeration	
С	AuthenticationStatus	Enumeration	
0	Device IP Address	IPv4 Address	
0	HostName	String	
⊙	Identity Group	Hierarchy	
0	NACRadiusPolicyStatus	Enumeration	
0	NACRadiusRole	String	
0	NACRadiusUserName	String	
0	Protocol	Enumeration	
С	Time And Date	Date Time Period	
0	UseCase	Enumeration	
С	UserName	String	
0	WasMachineAuthenticated	Boolean	
		Page 1 of 1 14 4	
к	Cancel	Help	

Figure 88 Attribute List

Step 4 In the Operator drop-down menu, *m*ake sure **In** is selected.

Step 5 From the Network Device Groups list (see Figure 89), click Select to select Contractor.

Figure 89 Network Device Groups

Network Device Groups			
Filter: 🗾 Mate	sh if: Go ▼		
Name 🔺	Description		
🔿 🖃 All Groups	Identity Group Root		^
 Contractor 	Contracted Staff		
• IP Phones	Corporate Managed IP Phones		
MACHINES	Corporate Managed Machines (Printers, Cameras, etc.)		
		L _k	
< Cancel		ß	

Step 6 Click Add.

Γ

Step 7 In the Results/Authorization Profiles section, click **Select** and select the previously created **Contractor-Authz** profile (see Figure 90).

uth	orization Profiles	Items 1-7 of 7 Rows per page: 50 💌 G
ilter	: Match if:	▼ Go ▼
	Name 🔺	Description
2	Contractor-Authz	Policy for short term contractors
	CorpUser-Authz	Policy for Valid AD Authenticated Users
	DenyAccess	
	Managed-Asset-Authz	Policy to be applied to Managed Assets
1	MediaNet-Authz	Policy for Cisco MediaNet Endpoints
	Permit Access	
	Phone-Authz	Policy to map IP Phones to Voice VLAN
		\searrow
Cre	ate Duplicate Edit Delete	Page 1 of 1 🕅 🖉 🕨 🕅
	Cancel	Hel

1

Figure 90 Authorization Profiles List

- Step 8 Click OK and then click OK again.
- Step 9 Click Save Changes.

Adding a MAB MediaNet Rule

To add a MAB MediaNet rule, complete the following steps.

Procedure

- Step 1 From the MAB Access Service section, select Authorization and click Create.
- **Step 2** In the window shown in Figure 91, do the following:
 - a. For the Name, enter an appropriate name; for example, MAB-MediaNet-Authz.
 - **b.** Select Compound Condition.
 - c. From the Dictionary drop-down menu, select System and then press the Select button.

General		- L
lame: MAB-MediaNet-Authz	Status: Enabled 💌 오	
The Customize button in conditions and results a	n the lower right area of the policy rules screen controls which policy re available here for use in policy rules.	
Conditions		-
Compound Condition:		
Condition:		
Dictionary:	Attribute:	
System 🗸	IdentityGroup Select	
Operator: 😽	Value:	
in 💌	All Groups:MACHINES Select	
Current Condition Set:		
Add V	Edit A Replace V	
System: Io	dentityGroup in All Groups:MACHINES	
And > • Or > •		
	· · · · · · · · · · · · · · · · · · ·	
	Delete Preview	_
Results		7
uthorization Profiles:		
MediaNet-Authz K Cancel	If desired, you can select more than one authorization profile, to define a 'merged' authorization result. Note that the order is significant for resolving any conflicts that	Help

Figure 91 Creating an Authorization Policy

d. From the Attribute List (see Figure 92) select Identity Group and click OK.

Γ

Attributes List Items 1-13 of 13 Rows per page: 50 🔽 Go				
	Attribute	Туре		
0	AuthenticationMethod	Enumeration		
0	AuthenticationStatus	Enumeration		
0	Device IP Address	IPv4 Address		
0	HostName	String		
•	IdentityGroup	Hierarchy		
0	NACRadiusPolicyStatus	Enumeration		
0	NACRadiusRole	String		
0	NACRadiusUserName	String		
0	Protocol	Enumeration		
0	Time And Date	Date Time Period		
0	UseCase	Enumeration		
0	UserName	String		
0	WasMachineAuthenticated	Boolean		
		Page 1 of 1 🔣 🖉 🕨		
к	Cancel	Help		

1

Figure 92	Attribute List
-----------	----------------

Step 3 In the Operator drop-down menu, make sure In is selected and click Select.

Step 4 From the Network Device Groups list (see Figure 93), select MACHINES.

Figure 93 Network Device Groups

etwork Device Groups			
Filter: Match if: Go 🗸			
Name 🔺	Description		
🗇 🖃 All Groups	Identity Group Root		
Contractor	Contracted Staff		
• IP Phones	Corporate Managed IP Phones		
MACHINES	Corporate Managed Machines (Printers, Cameras, etc.)		
Cancel		Help	

- Step 5 Click Add.
- **Step 6** In the Results/Authorization Profiles section, click **Select** button and select the previously created **MediaNet-Authz** profile (see Figure 94).

Authorization Profiles Items 1-7 of 7 Rows per pa			-7 of 7 Rows per page: 50	🚽 Go
ilter	: Match if:	🔹 Go 🔻		
	Name 🔺	Description	n	
	Contractor-Authz	Policy for short term contractors		-
	CorpUser-Authz	Policy for Valid AD Authenticated Users		
	DenyAccess			
	Managed-Asset-Authz	Policy to be applied to Managed Assets		
	MediaNet-Authz	Policy for Cisco MediaNet Endpoints		
	Permit Access	Ν		
-	Phone-Authz	V Policy to map IP Phones to Voice VLAN		
Cre	eate Duplicate Edit Delete]	Page 1 of 1 1	
Cre	eate Duplicate Edit Delete]	Page 1 of 1 🕅 🕘	Help

Figure 94 Authorization Profiles List

Step 7 Click OK and then click OK again.

Step 8 Click Save Changes.

ſ

You should have now three authorization rules for MAB, as shown in Figure 95:

- MAB-Phone-Authz
- MAB-Contractor-Authz
- MAB-MediaNet-Authz

These apply differentiated authorization policy per group type.

Network Access Authorization Policy								
Filt	er: S	tatus	Mate	ch if: Equals 🔽 🔍	Clear Filter	Go 🔻		_
		Status	Name	Conditions Compound Condition	Result Authorization Profiles	s Security Group	Hit Count	
1		0	MAB-Phone- Authz	System:IdentityGroup in All Groups:IP Phones	Phone-Authz	Unknown	2	A
2		9	MAB- Contractor-Rule	System:IdentityGroup in All Groups:Contractor	Contractor-Authz	Unknown	0	
3		Θ	<u>MAB-MediaNet-</u> <u>Rule</u>	System:IdentityGroup in All Groups:MACHINES	MediaNet-Authz	Unknown	0	
								-
**		<u>Default</u>		Default Lif no rule is defined in the table or none of the above enabled rules are matched.	Permit Access	Unknown	18	

Figure 95 MAB Authorization Policies

Configuring the Switch

This section includes the following topics:

- Global Switch Default ACLs, page 78
- Switch Port Configuration, page 79

Global Switch Default ACLs

Apply the following pre-authentication ACL to be applied to the TrustSec-enabled ports:

```
ip access-list extended PRE-AUTH
remark Allow DHCP
permit udp any eq bootpc any eq bootps
remark Allow DNS
permit udp any any eq domain
remark Allow Websense
permit tcp any any eq 15871
remark Deny access to HO
deny ip any 10.0.0.0 0.255.255.255
deny ip any 192.168.0.0 0.0.255.255
remark Allow access to internet
permit tcp any any eq www
permit tcp any any eq 443
```

To enable dACLs, you must first configure your access switch to allow communications using the *cisco-av-pair* attribute with the value *aaa:event=acl-download*. To enable this functionality, enter the following command in the global configuration of the switch. Failure to add this command results in failed authentication/authorization requests.

conf t radius-server vsa send end

Switch Port Configuration

Access your switch console and add **ip access-group PRE-AUTH** to the TrustSec-enabled ports you have configured for this exercise:

```
interface range fa2/1-16
  shut
  switchport access vlan 210
  switchport voice vlan 211
  switchport mode access
  ip access-group PRE-AUTH in
  authentication host-mode multi-domain
  authentication open
  authentication port-control auto
  mab
  dot1x pae authenticator
  ip verify source vlan dhcp-snooping
  no shut
```

You are adding only one new line to the configuration (**ip access-group PRE-AUTH in**) and modifying the host-mode from *multiauth* to *multidomain*, which restricts one host in the voice VLAN and one host in the data VLAN. You can use the above configuration as a reference to the other configuration items that should be enabled on the low impact identity-enabled ports.

Configuring the Endpoint Host

For the purposes of this TrustSec phased deployment demonstration, the 802.1X client configuration is limited to Windows XP, the Cisco Secure Services Client (SSC), and PEAP as the authentication protocol.

Before installing Cisco SSC on your Windows XP PC, make sure you do not have any other 802.1X supplicant installed or configured. If you do, remove the supplicant and reboot before starting the next procedure.

To configure the endpoint host, complete the following steps.

Procedure

Step 1 Download the latest version of Cisco's SSC (v5.1.1 or later) from http://tools.cisco.com/support/downloads/ to your desktop on the Windows XP machine.

You need both of the following installation applications:

- Cisco_SSC-XP2K_5.1.1.3.zip—Required to install the supplicant on the host PC.
- Cisco_SSCMgmtUtil_5.1.1.4.zip—Required on by the Administrator to create profiles.
- **Step 2** Unzip the archive, and run the Cisco SSC Installer (see Figure 96).

Figure 96	Cisco SSC Installer	
B Cisco Secure Services	Client - InstallShield Wizard 🛛 🔀	1₽ Cisco Secure Services Client - InstallShield Wizard
alah	Welcome to the InstallShield Wizard for Cisco Secure Services Client	License Agreement Please read the following license agreement carefully.
CISCO.	The InstallShield(R) Wizard will install Cisco Secure Services Client 5.0.2.3 on your computer. To continue, click Next.	End User License Agreement
	WARNING: This program is protected by copyright law and international treaties.	CISCO-SOPPIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT. CISCO IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. BY DOWNLOADING OR INSTAILING THE SOFTWARE OD HENGT THE FOUNDENT THIS
There is a second se	< Back Next > Cancel	I accept the terms in the license agreement I do not accept the terms in the license agreement InstallShield

I

1

Step 3 Accept the terms and default installation directory (see Figure 97) and click Install.

Figure 97 Installation Directory

🛱 Cisco Secure Services Client - InstallShield Wizard 🛛 🔀	🔞 Cisco Secure Services Client - InstallShield Wizard
Destination Folder Click Next to install to this folder, or click Change to install to a different folder. CISCO.	Ready to Install the Program The wizard is ready to begin installation.
Install Cisco Secure Services Client to: C:\Program Files\Cisco\Cisco Secure Services Client\ Change	Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
Instalishield	InstallShield Cancel 80

The two screens shown in Figure 98 show the installation progress

Figure 98 Installation Progress

😼 Cisco Secure Services Client - InstallShield Wizard	🔂 Cisco Secure Services Client - InstallShield Wizard 🛛 🔀
Installing Cisco Secure Services Client The program features you selected are being installed.	InstallShield Wizard Completed
Please wait while the InstallShield Wizard installs Clisco Secure Services Client 5.0.2.3. This may take several minutes.	CISCO Services Client 5.0.2.3. Click Finish to exit the wizard.
InstallShield	
<back next=""> Cancel</back>	< Back Finish Cancel

Step 4 When the installation is complete, click **Finish**.

Step 5 Select Yes to reboot.

You are required to reboot.

Figure 9	9 Reboot Screen	
🔂 Cisco	Secure Services Client Installer Information	×
<u>.</u>	You must restart your system for the configuration changes made to Cisco Secure Services Client to take effects Click Yes to restart now or No if you plan to restart later.	
	Tes No	

- **Step 6** When the Windows XP PC has rebooted, log back in as the Administrator.
- **Step 7** To configure the client for network access, run the *sscManagementUtility.exe* file.
- **Step 8** Click **Create New Configuration Profile** > and select **Cisco SSC 5.0** > (see Figure 100).

Figure 100 Welcome and Select Cisco SSC Version Screens

() Cisco SSC Managem	ient Utility 🛛 💽 🔀	😫 Cisco SSC Manage	ment Utility
ahaha	Welcome to Enterprise Deployment Configuration	ahaha	Select Cisco SSC Version
CISCO	This Enterprise Deployment wizard for Cisco SSC enables network and desktop administrators to centrally configure, deploy, and manage the Secure Services Client in an enterprise environment.	cisco	Please select the Cisco SSC Version for which you would like to create a new Deployment Configuration.
	Gives IT professionals the capability to enforce network security polices on end stations. Provides IT professionals with the flexibility to configure various settings to support existing enterprise standards and reduce support calls. Offers end users a hassle free networking experience.		7
	Create New Configuration Profile > Modify Existing Configuration Profile >		[Esco 55C 5.0 >]
	Process Existing Configuration Profile >		
	Sschanagement/Lility (S. 0. 1. 6229) © 2007_Gisco Systems, Inc.		View Configuration XML while editing (advanced users)
	Quit	142.00	<back quit<="" th=""></back>

214298

- **Step 9** In the Client Policy screen (see Figure 101), do the following:
 - **a**. Paste in your license key.
 - **b.** Select the **Attempt connection before user logon** radial button.
 - c. Check the Allow Wired (802.3) Media checkbox.
 - d. Click Next.

ſ

Step 10 In the Authentication Policy screen (see Figure 101) select all of the Association and Authentication modes and click **Next**.

վերին	Client Policy	111111	Authentication Policy	
cisco	Userse Provide Licence Provid	cisco	Allowed Association Modes	Aloved Authentication Modes EAP MOS EAP MOS HAPV2 EAP TAS EAP Fast EAP Fast Leap EAP EAP EAP EAP EAP TILS

Figure 101 Client Policy and Authentication Policy Screens

Step 11 To create a network profile for each network to which you connect, click Add Network.

Step 12 In the Network Media screen (see Figure 102), accept the default and click Next.

Figure 102 Network Media and Wired Network Settings Screens

😫 Cisco SSC 5.0 C	onfiguration Profile	Cisco SSC 5.0 C	Configuration Profile
cisco	Network Media Choose Your Network Media Wred (802.3) Network Select a wired network if the endstations will be connecting to the network with a traditional ethemet cable.	cisco	Wired Network Settings Network Settings Display Name: [Jdux.local Wired Network Correction Timeout: 30 Security Level Open Network Open Network Open Network Authentication networks have no security, and are open to anybody with physical access. This is the least secure type of network. Authentication networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.
	< Back Next > Cancel		< Back Next > Cancel

- **Step 13** In the Wired Network Settings screen (see Figure 102), do the following:
 - a. Enter a name for this network; for example, Demo.local Wired Network.
 - **b.** Change the Connection Timeout to **30**.
 - c. Select Authenticating Network.
 - d. Click Next.
- Step 14 In the Connection Settings screen (see Figure 103), set the Connection Settings as shown and click Next.

😫 Cisco SSC 5.0 Co	onfiguration Profile		📵 Cisco SSC 5.0 Config	uration Profile	? 🔀
ahaha	Connection Settings		11 111 11 N	etwork Connection Type	
CISCO	B02.1X Settings authPeriod 30 heldPeriod 60 startPeriod 3 maxStart		CISCO	letwork Connection Type Machine Connection Two less used if the and station should be gonto the network before the user kgs in. The is typically used for connecting to domains, to get Gi and other updates from the network before the user has access. User Connection Work to the used when a machine connection is not necessary. A to connection will make the network available after the user has logged on. Machine and User Connection. Machine and Sec Connection. That type of connection will be made automatically when the machine boots. It will be brought down, and back up again with different credentials when the user logged on the user logged on the user logged on the store of the made automatically when the machine boots. It will be brought down, and back up again with different credentials when the user logged on the user l	e o's ser I then s in.
		4			
	< Back Nex	t > Cancel		< Back Next > Car	cel

Figure 103 Connection Settings and Network Connection Type Screens

- **Step 15** In the Network Connection Type screen (see Figure 103), select Machine and User Connection and click Next.
- **Step 16** In the Machine Authentication (EAP) Method screen (see Figure 104), select **EAP PEAP** and click the **Configure** button.

Figure 104	Machine Authentication (EAP) Method and EAP PEAP Settings Scree	ns
------------	---	----

😫 Cisco SSC 5.0 C	onfiguration Profile	EAP PEAP Settings	? 🗙
cisco	Machine Authentication (EAP) Method EAP Methods EAP MSCHAPV2 LEAP EAP GTC	EAP Peap Settings Validate Server Identity Enable Fast Reconnect	
	EAP TLS Con EAP TLS Con EAP TLS Con EAP Fast Con	figure fi	
	< Back Ne		OK Cancel

- Step 17 In the EAP PEAP Settings screen (see Figure 104), for the EAP PEAP setting, check the boxes as shown, click OK, and click Next.
- **Step 18** In the Machine Credentials screen (see Figure 105), select Use Machine Credentials radial box and click Next.

I

Cisco SSC 5.0 C	ionfiguration Profile	? 🔀	Cisco SSC 5.0 Conf	figuration Profile		?
սիսիս	Machine Credentials		սիսիս կ	Jser Authentication	(EAP) Method	
CISCO	Machine Identity Unprotected Identity Pattern: host/[username] Protected Identity Pattern: host/[username] Machine Credentials Use Machine Credentials Password: Password: Password: Password: Password: Password: Password: Password: Password: Password: Password: Password: Password: Password: Password: Password: Password: Password: Password: Password: Passwor	•	CISCO	EAP Methods EAP MDS EAP MSCHAPv2 LEAP EAP GTC EAP TLS EAP TL	Configure Configure Configure Configure	
	< Back Next >	Cancel	8	C EAP Fast	Configure	ancel

Figure 105 Machine Credentials and User Authentication (EAP) Method Screens

- **Step 19** In the User Authentication (EAP) Method screen (see Figure 105), select the EAP PEAP radio box and then click Configure.
- **Step 20** Select the check boxes and radio buttons as shown in Figure 106 for the EAP PEAP settings, click **OK**, and then click **Next**.

Figure 106 EAP PEAP Settings and User Credentials Screens

EAP PEAP Settings	😫 Cisco SSC 5.0 Co	onfiguration Profile	? 🛛
EAP Peap Settings Validate Server Identity Enable Fast Reconnect Disable when using a Smart Card	cisco	User Credentials User Identky Unprotected Identky Pattern: [[username]] Protected Identky Pattern: [[username]] User Credentials	
Inner Methods based on Credentials Source Authenticate using a Password EAP MSCHAPv2 EAP GTC		Use Single Sign On Credentials Prompt for Credentials Remember Forever Remember while the User is Logged On Never Remember	
Authenticate using a Token and EAP GTC EAP TLS, using a Certificate		Use Static Credentials Password:	
OK Cancel		< Back Finish C	Cancel

- Step 21 In the User Credentials screen (see Figure 106), accept Use Single Sign On Credentials and click Finish.
- **Step 22** Click **Next** to validate the configuration (see Figure 107).

😫 Cisco SSC 5.0 Co	nfiguration Profile			? 🗙	📵 Cisco SSC 5.0 C	Configuration Profile
ahaha	Networks				adraha	Validation
cisco	Networks				CISCO	The configuration has been validated.
	Group / Network	Media	Security Level			
	[Networks Available to All Groups] [Idux.local Wired Network Default	Wired (802.3)	Authentication			
				<		
						View Configuration VM
						Save Processed and Simple Configuration Ele
			N			sers(Application Data)Cisco(Cisco Secure Services Client(newContigHies)contiguration.xml Browse
			4			Save Original Configuration File
	Add Group	Add Network	Modify Remove			co Secure Services Client\newConfigFiles\unprocessed_configuration_do_not_deploy.xml Browse
			< Back Next >	Cancel	14810	< Back Finish Cancel

Figure 107 Networks and Validation Screens

Step 23 Click **Finish** and you are finished with this PC.

Repeat the SCC and Management Utility configuration for other PCs that you are using in this demonstration.

Note

There is a way to create an administrative install MSI file with preconfigured settings for a mass deployment. For more information, see the Cisco SSC documentation at the following URL: http://www.cisco.com/en/US/products/ps7034/index.html.

Verifying Low Impact Mode

This section includes the following topics:

- Verifying Host Network Connectivity and Network Services, page 85
- Verifying 802.1X-Capable Managed Assets, page 88
- Verifying Non-802.1X-Capable Managed Assets, page 90



Global AAA/RADIUS configuration verification should not be necessary because this was validated in the previous sections.

Verifying Host Network Connectivity and Network Services

A quick way to gain insight into the IP addresses associated with the ports and MAC addresses is to run the **show ip dhcp snooping binding** Cisco IOS Software CLI switch command (see Figure 108).

MacAddress	IpAddress	Lease(sec)	Туре	VLAN	Interface
00:18:F8:08:F8:38	10.200.10.203	685617	dhcp-snooping	210	FastEthernet2/13
00:18:F8:09:CF:C6	10.200.10.201	685558	dhcp_snooping	210	FastEthernet2/1
00:18:BA:C7:BC:FA	10.200.11.201	691176	dhcp_snooping	211	FastEthernet2/13
00:18:BA:C7:BC:EE	10.200.11.203	691134	dhcp_snooping	211	FastEthernet2/12
00:1D:E5:EB:F9:00	10.200.10.200	685586	dhcp_snooping	210	FastEthernet2/11
00:18:D5:85:39:1E	10.200.11.202	691116	dhcp_snooping	211	FastEthernet2/16
00:1D:E5:EB:E5:EF	10.200.10.202	685583	dhcp_snooping	210	FastEthernet2/8
00:21:86:58:DB:6B	10.200.10.205	685620	dhcp_snooping	210	FastEthernet2/12
Total number of bin	ndings: 8				

Figure 108 s	how ip dhcp snooping	binding Output
--------------	----------------------	----------------

Comparing this with the original lab diagram shown in Figure 1, you can see that all of the devices are connected and have an IP address. You also see which VLAN they are in and their MAC addresses. The only exception is the rogue AP on port f2/14.

Another useful IOS **show** command is **show authentication sessions**. This displays the state of all TrustSec-enabled switch ports on that switch. Figure 109 and Figure 110 show port-specific derivatives of this command.

Figure 109 show authenticated sessions Output

id-4503-2#show authentication sessions					
Interface	MAC Address	Method	Domain	Status	Session ID
Fa2/8	(unknown)	dot1x	UNKNOWN	Running	0AC8018000009D3890DCEED8
Fa2/11	(unknown)	dot1x	UNKNOWN	Running	0AC8018000009D3990DCF2C0
Fa2/1	0018.f809.cfc6	dot1x	DATA	Authz Success	0AC8018000009D3190DC8948
Fa2/16	001b.d585.391e	dot1x	UNKNOWN	Running	0AC8018000009D3590DC9124
Fa2/13	0018.bac7.bcfa	dot1x	UNKNOWN	Running	0AC8018000009D3790DC9510
Fa2/12	0018.bac7.bcee	dot1x	UNKNOWN	Running	0AC8018000009D3690DC9510
Fa2/14	0006.2504.c295	dot1x	UNKNOWN	Running	0AC8018000009D3390DC8D40
Fa2/12	0021.8658.db6b	dot1x	UNKNOWN	Running	0AC8018000009D3A90DD020C
Fa2/13	0018.f808.f838	dot1×	UNKNOWN	Running	0AC8018000009D3B90DD0598

Figure 110 show cdp neighbors Output



Another quick summary view is to look at the Authentication and Authorization logs within ACS Reporting and Monitoring (see Figure 111).

💷 🚔 💽 🕺						Launch Interactive	e Viewer 🛛 🛐
Showing F	Dage	1 of	24 41 4 🕨 🕪	Goto Page: 🗾 🖻			
AAA Protocol	> RAE	DIUS A	uthentication				<u> </u>
Authentication Sta Date :	atus :	Pass Janua	or Fail ary 9, 2009				
Generated on Janu	uary 9,	2009 3:	30:40 PM PST				
Reload							
✓=Pass ×=Fai	il 🍳	=Click f	or details				
Logged At	Status	Details	Failure Reason	User Name	Calling Station ID	Authentication Method	Sele Authorizat
3:29:01.610 PM	1	0		#ACSACL#-IP-ContractorACL-496676a5			
3:29:01.600 PM	1	0		00-21-86-58-DB-6B	00-21-86-58-DB-6B	Lookup	Contracto
3:28:57.503 PM	1	0		00-1D-E5-EB-F9-00	00-1D-E5-EB-F9-00	Lookup	MediaNet-
3:28:56.480 PM	1	9		00-1D-E5-EB-E5-EF	00-1D-E5-EB-E5-EF	Lookup	MediaNet-
3:28:32.913 PM	1	0		00-18-BA-C7-BC-FA	00-18-BA-C7-BC-FA	Lookup	Phone-Aut
3:28:32.910 PM	1	0		00-18-BA-C7-BC-EE	00-18-BA-C7-BC-EE	Lookup	Phone-Aut
3:28:31.886 PM	×	0	22041 Unknown User	00-06-25-04-C2-95	00-06-25-04-C2-95	Lookup	
3:28:21.413 PM	1	0		IMAC-CLIENT-2\Administrator	00-18-F8-08-F8-38	MSCHAPV2	CorpUser-
3:28:02.016 PM	1	0		CP-7961G-SEP001BD585391E	00-1B-D5-85-39-1E	CHAP/MD5	Phone-Aut
3:28:02.013 PM	1	9		#ACSACL#-IP-CorpAssetACL-496675ed			-

Figure 111 Authentication and Authorization Logs (1)

The screenshot in Figure 112 is the same list of hosts, which has been scrolled to the right to show the rest of the data available.

Figure 112 Authentication and Authorization Log	s (2)
---	-------

I

	4 🔒 🔒 🖻							Laun	ch Interactive Viewer	5
	Showing Page	1 of 24	41 4 > 1>	Goto	Page:	>				
										-
D	Authentication Method	Selected	Selected Exception	Network Device	NAS IP Address	NAS Port	Access Service	Identity Store	Identity Group	
		Authorization Profiles	Authorization Profiles	14 4500.0	10.000 1.100					
				10-4503-2	10.200.1.128					
в	Lookup	Contractor-Authz		<u>id-4503-2</u>	10.200.1.128	50212	MAB	Internal Hosts	All Groups:Contractor	r
0	Lookup	MediaNet-Authz		<u>id-4503-2</u>	10.200.1.128	50211	MAB	Internal Hosts	All Groups:MACHINES	\$
E	Lookup	MediaNet-Authz		id-4503-2	10.200.1.128	50208	MAB	Internal Hosts	All Groups:MACHINES	3
FA	Lookup	Phone-Authz		id-4503-2	10.200.1.128	50213	MAB	Internal Hosts	All Groups: IP Phones	
<u>EE</u>	Lookup	Phone-Authz		id-4503-2	10.200.1.128	50212	MAB	Internal Hosts	All Groups: IP Phones	
15	Lookup			id-4503-2	10.200.1.128	50214	AB	Internal Hosts		
3	MSCHAPV2	CorpUser-Authz		id-4503-2	10.200.1.128	50213	802.1X	AD1		
. <u>E</u>	CHAP/MD5	Phone-Authz		id-4503-2	10.200.1.128	50216	802.1X	Internal Users	All Groups: IP Phones	

As shown, all of the administratively allowed devices have successfully authenticated and received the authorization policy as prescribed. Note that the host with the MAC address 00-06-25-04-C2-95 failed authentication. By having this log, we know that someone has plugged in a rogue device on switch id-4503-2 on port 50214 (i.e, F2/14). Per policy in Low Impact mode, this device is allowed to gain an IP address and access limited resources per the PRE-AUTH ACL. However, this allows you to also send someone out to determine what the device is and whether it should be on your network.

Verifying 802.1X-Capable Managed Assets

802.1X Cisco IP Phone

This simple verification step verifies that the phone has an IP address and has connected to the Call Manager. One easy test is to pick up the phone and see whether it has dial tone. If it does, chances are everything is working just fine.

For further verification look at the switch port status, as shown in Figure 113.

Figure 113 Switch Port Status

id 4502 2. on						
10-4503-25en						
Password:						
id-4503-2#show authen s	ession interface f2/16					
Interface:	FastEthernet2/16					
MAC Address:	001b.d585.391e					
IP Address:	10.200.11.202					
User-Name:	CP-7961G-SEP001BD585391E					
Status:	Authz Success					
Domain:	VOICE					
Oper host mode:	multi-auth					
Oper control dir:	both					
Authorized By:	Authentication Server					
Session timeout:	3600s (local), Remaining: 1154s					
Timeout action:	Reauthenticate					
Idle timeout:	N/A					
Common Session ID:	0AC8018000009D30907E4128					
Acct Session ID:	0×00009D3E					
Handle:	0×9A000D6F					
Runnable methods list:						
Method State						
dot1x Authc S	uccess					
mah Not run						
100 101						

Figure 113 shows that the phone successfully authenticated via 802.1X and was placed in the VOICE VLAN.

Windows XP and Cisco SSC 802.1X Supplicant/Client

Complete the following steps.

Procedure

Step 1 From the Windows XP interface, double-click the SSC icon (that is, the round green icon) in the tray bar (see Figure 114).



This loads the SSC dialog window, showing the status of your connection (see Figure 115).

Cisco Secure Services Clien ettings Help	nt - Charles and Charle		
Active Connection Group			
Default		~ C	onfigure Groups
Available Connections			
Configured connections appear in b	oldface		
Connection	Signal	Security	Status
Idux.local Wired Hetwork			Connected
<			>
Connect Edit	Delete	Add SSID Co	onnection Status

Figure 115 Connection Status

- **Step 2** For further verification, look at the switch port status (see Figure 116).
 - Figure 116 Switch Port Status

Γ

id-4503-2#show authenti	cation sessions interface f2/1	
Interface:	FastEthernet2/1	
MAC Address:	0018.f809.cfc6	
IP Address:	10.200.10.201	
User-Name:	administrator	
Status:	Authz Success	
Domain:	DATA	
Oper host mode:	multi-auth	
Oper control dir:	both	
Authorized By:	Authentication Server	
Vian Policy:	N/A	
Session timeout:	3600s (local), Remaining: 2270s	
Timeout action:	Reauthenticate	
Idle timeout:	N/A	
Common Session ID:	0AC8018000009D25907D4E68	
Acct Session ID:	0x00009D33	
Handle:	0×7A000D64	
Runnable methods list:		
Method State		
dot1x Autho S	uccess	
mah Not run		8
ndo rorian		4

Verifying Non-802.1X-Capable Managed Assets

Cisco IP Phone (no 802.1X Supplicant)

Verify that the phone has dial tone and check the authentication status of the switch port. Two non-802.1X phones are on ports F2/12 and F2/13. You can also determine where they are connected by using the following Cisco IOS Software CLI commands:

- show cdp neighbors
- show ip dhcp snooping binding
- show authentication session

You can also check the AAA logs from ACS.

Figure 117 shows the output for show authentication sessions interface f2/12 & f2/13.

id-4503-2#show authentication sessions interface f2/12	id-4503-2#show authentication sessions interface f2/13
Interface: FastEthernet2/12	Interface: FastEthernet2/13
MAC Address: 0018.bac7.bcee	MAC Address: 0018.bac7.bcfa
IP Address: 10.200.11.203	IP Address: 10.200.11.201
User-Name: 00-18-BA-C7-BC-EE	User-Name: 00-18-BA-C7-BC-FA
Status: Authz Success	Status: Authz Success
Domain: VOICE	Domain: VOICE
Oper host mode: multi-auth	Oper host mode: multi-auth
Oper control dir: both	Oper control dir: both
Authorized By: Authentication Server	Authorized By: Authentication Server
Session timeout: N/A	Session timeout: N/A
Idle timeout: N/A	Idle timeout: N/A
Common Session ID: 0AC8018000009D3690DC9510	Common Session ID: 0AC8018000009D3790DC9510
Acct Session ID: 0x00009D47	Acct Session ID: 0x00009D48
Handle: 0x0A000D75	Handle: 0x28000D76
Runnable methods list:	Runnable methods list:
Method State	Method State
dot1× Failed over	dot1× Failed over
mab Authc Success	mab Authc Success
Interface: FastEthernet2/12	
140 AUG1855. 0021.0000.0000	THE AUGTESS. 0010.1000.1000
IP Address: 10.200.10.205	IP Address: 10.200.10.203
User-Name: 00-21-86-58-DB-6B	User-Name: IMAC-CLIENT-2\Administrator
Status: Authz Success	Status: Authz Success
Domain: DATA	Domain: DATA
Oper host mode: multi-auth	Oper host mode: multi-auth
Oper control dir: both	Oper control dir: both
Authorized By: Authentication Server	Authorized By: Authentication Server
Vlan Policy: N/A	Vlan Policy: N/A
Session timeout: N/A	Session timeout: N/A
Idle timeout: N/A	Idle timeout: N/A
Common Session ID: 0AC8018000009D3A90DD020C	Common Session ID: 0AC8018000009D3B90DD0598
Acct Session ID: 0x00009D4B	Acct Session ID: 0x00009D4C
Handle: 0x31000D79	Handle: 0x3A000D7A
Runnable methods list:	Runnable methods list:
Method State	Method State
dot1x Failed over	g dot1x Authc Success
mab Autho Success	😤 mab Notrun

Figure 117 show authentication sessions interface f2/12 & f2/13 Output

As shown in the output from these Cisco IOS show commands, two devices are authenticated on each port: a phone and a PC. The phones are placed in the VOICE VLAN and the PCs in the DATA VLAN.

214324

I

For port F2/12, the phone and the PC are both authenticated via MAB. On port F2/13, the phone is authenticated via MAB and the PC is authenticated via 802.1X. Both ports have the same configuration. This is the power of FlexAuth combined with multiauth.

You can also repeat the validation steps performed in the "Verifying Monitor Mode" section on page 36 for a complete validation.

Implementing High Security Mode

This section includes the following topics:

- High Security Mode Overview, page 91
- Modifying Authorization Profiles, page 91
- Verifying Global Switch VLAN Definition, page 97
- Configuring the Switch Port, page 98
- Verifying High Security Mode, page 98

High Security Mode Overview

Low impact mode may fulfill initial access security requirements for many organizations. For those that need stricter access controls may choose to deploy high security mode.

High security mode returns to the traditional closed mode of 802.1X, in conjunction with dynamic VLAN assignment for differentiated access. Although high security mode represents a more traditional deployment model, the new Cisco IOS FlexAuth feature set can be used to create a flexible, adaptable deployment.

FlexAuth allows you to configure secondary authentication methods to 802.1X, such as MAB and/or Web Authentication for guest access. Additionally, FlexAuth allows you to re-order the sequence of authentication. For example, you can try MAB before 802.1X.

Because you are moving from monitor or low impact mode, the base infrastructure configuration is already in place. Here you need to modify only the authorization profiles and switch port configurations.

Modifying Authorization Profiles

For high security mode, you are going to modify the five existing authorization profiles. The authorization is changed from dACLs to VLANs.

Table 13 lists the authorization profiles for all three modes.

Profile Name	Description	VLAN	dACL		
Monitor Mode					
No Authorization Profile Required	n/a	n/a	n/a		
Low Impact or Selective Access Mode					
Phone-Authz	Policy to map IP phones to Voice VLAN	n/a	CorpAssetACL		
Managed-Asset-Authz	Policy to be applied to managed assets	n/a	CorpAssetACL		
MediaNet-Authz	Policy for Cisco MediaNet endpoints	n/a	CorpAssetACL		

Table 13Authorization Profiles

CorpUser-Authz	Policy for valid AD authenticated users	n/a	CorpUserACL
Contractor-Authz	Policy for short-term contractors	n/a	ContractorACL
High Security Mode			
Phone-Authz	Policy to map IP phones to Voice VLAN	N/A	n/a
Managed-Asset-Authz	Policy to be applied to managed assets	MACHINE	n/a
MediaNet-Authz	Policy for Cisco MediaNet endpoints	MEDIANET	n/a
CorpUser-Authz	Policy for valid AD authenticated users	DATA	n/a
Contractor-Authz	Policy for short-term contractors	CONTRACTOR	n/a

To modify existing authorization profiles, first access the ACS web interface and go to **Policy Elements** > **Authorization and Permissions** > **Network Access** > **Authorization Profiles** (see Figure 118).

Figure 118 Authorization Profiles Screen

Policy Elements : Authorization and Permissions > Network Access > Authorization Profiles						
Auth	orization Profiles	Items 1-6 of 6 Rows per page: 50 💌				
Filter	r: 💽 Match if:	. Go 🗸				
	Name 🔺	Description				
	Contractor-Authz	Policy for short term contractors				
	CorpUser-Authz	Policy for Valid AD Authenticated Users				
	Managed-Asset-Authz	Policy to be applied to Managed Assets				
	MediaNet-Authz	Policy for Cisco MediaNet Endpoints				
	Permit Access					
	Phone-Authz	Policy to map IP Phones to Voice VLAN				

From here, modify the existing profiles by completing the following steps.

Modifying the Phone-Authz Profile

Step 1 Select the **Phone-Authz** profile (see Figure 119).

Figure 119 Modifying the Phone-Authz Profile

olicy Elements : Authorization and Permissions > Network Access > <u>Authorization Profiles</u> > Edit: "Phone-Authz"	
General Common Tasks RADIUS Attributes	
General	
* Name: Phone-Authz	326
Description: Policy for IP Phones	214
Required fields	

Step 2 Select the Common Tasks tab.

Step 3 Under the ACLS section, from the Downloadable ACL Name drop-down menu, change static to Not in Use (see Figure 120).

olicy Elements : Authorizatio	n and Permissions > Network Access > <u>Authorization Profiles</u> > Edit: "Phone-Authz"
General Common Tasks	RADIUS Attributes
VLAN ID/Name:	Not in Use
URL for Redirect:	Not in Use
URL Redirect ACL:	Not in Use
ACLS	
Downloadable ACL Name:	Not in Use 💌
IOS ACL Filter ID:	Not in Use 💌
Proxy ACL:	Not in Use 💌
QOS	
QOS Profile Name:	Not in Use 💌
Input Policy Map:	Not in Use 💌
Output Policy Map:	Not in Use 💌
Voice VLAN	
Permission to Join:	Static Yes (device-traffic-class=voice)
Reauthentication	
Reauthentication Timer:	Not in Use 💌
Maintain Connectivity during Reauthentication:	
Required fields	

Figure 120 Authorization Profiles—Common Tasks Tab

Step 4 Click **Submit** to finish.

ſ

Repeat these steps for the rest of the Authz profiles created, using Table 13 to map the appropriate VLANs to these profiles.

Modifying the Managed-Asset-Authz Profile

Step 1 Select the Managed-Asset-Authz profile (see Figure 121).

Figure 121 Modifying Managed-Asset-Authz Profile

Policy Elements : Authorization and Permissions > Network Access > <u>Authorization Profiles</u> > Edit: "Managed-Asset-Auth	hz"
General Common Tasks RADIUS Attributes	
General Managed-Asset-Authz	a
Description: Policy to be applied to Managed Assets	149.0
* Required fields	

Step 2 Select the **Common Tasks** tab (see Figure 122) and do the following:

- a. For the VLAN ID/Name drop-down option, select static.
- **b.** In the Value input field, type **MACHINE**.
- **c.** Under the ACLS section, from the Downloadable ACL Name drop-down menu, change **static** to **Not in Use**.

General	Common Tasks	RADIUS Attributes	
VLAN ID/	Name:	Static 🔹	Value MACHINE
URL for R	edirect:	Not in Use 💌	
URL Redir	ect ACL:	Not in Use 💌	
ACLS			
Download	lable ACL Name:	Not in Use 💌	
IOS ACL	Filter ID:	Not in Use 💌	
Proxy AC	L:	Not in Use 💌	
QOS			
QOS Prof	ile Name:	Not in Use 💌	
Input Poli	cy Map:	Not in Use 💌	
Output Po	licy Map:	Not in Use 💌	
Voice VI	LAN		
Permissio	n to Join:	Not in Use 💌	
Reauthe	ntication		
Reauthen	tication Timer:	Not in Use 💌	
Maintain (Reauthen	Connectivity during tication:	,	

1

Figure 122 Authorization Profiles—Common Tasks Tab

Step 3 Click Submit.

Modifying the MediaNet-Authz Profile

Step 1 Select the **MediaNet-Authz** profile (see Figure 123).

Figure 123 Modifying the MediaNet-Authz Profile

Policy Elements : Authorization and Permissions > Network Access > <u>Authorization Profiles</u> > Edit: "MediaNet-Authz"	
General Common Tasks RADIUS Attributes	_
General	
* Name: MediaNet-Authz	8
Description: Policy for Cisco MediaNet Endpoints	2143
*Required fields	

- **Step 2** Select the **Common Tasks** tab (see Figure 124) and do the following:
 - a. For the VLAN ID/Name drop-down option, select static.
 - **b.** In the Value input field, type **MEDIANET**.
 - c. Under the ACLS section, from the Downloadable ACL Name drop-down menu, change static to Not in Use.

General	Common Tasks	RADIUS Attributes	
VLAN ID/I	Name:	Static Value MEDIANET	
URL for R	edirect:	Not in Use 💌	
URL Redir	ect ACL:	Not in Use	
ACLS			
Download	lable ACL Name:	Not in Use 🔽	
IOS ACL	Filter ID:	Not in Use 💌	
Proxy AC	L:	Not in Use 💌	
QOS			
QOS Prof	ile Name:	Not in Use 💌	
Input Poli	cy Map:	Not in Use 💌	
Output Po	licy Map:	Not in Use 💌	
Voice VI	LAN		
Permissio	n to Join:	Not in Use 💌	
Reauthe	entication		
Reauthen	tication Timer:	Not in Use 💌	
Maintain (Reauthen	Connectivity during tication:	g	

Figure 124 Authorization Profiles—Common Tasks Tab

Step 3 Click Submit.

I

Modifying the CorpUser-Authz Profile

Step 1 Select the **CorpUser-Authz** profile (see Figure 125).

Figure 125 Modifying the CorpUser-Authz Profile

Policy Ele	ments : Authorizati	on and Permissions	> Network Access > <u>Authorization Profiles</u> > Edit: "CorpUser-Authz"	
General	Common Tasks	RADIUS Attributes		
Gener * Name	al : CorpUser-A	uthz		
Descr	iption: Policy for Va	alid AD Authenticated	Users	214332
* Require	d fields			

- **Step 2** Select the **Common Tasks** tab (see Figure 126) and do the following:
 - a. For the VLAN ID/Name drop-down option, select static.
 - **b.** In the Value input field, type **DATA**.
 - **c.** Under the ACLS section, from the Downloadable ACL Name drop-down menu, change **static** to **Not in Use**.

General Common Tasks	RADIUS Attributes	
VLAN ID/Name:	Static Value DATA	
URL for Redirect:	Not in Use 💌	
URL Redirect ACL:	Not in Use	
ACLS		
Downloadable ACL Name:	Not in Use 💽 🗸	
IOS ACL Filter ID:	Not in Use 💌	
Proxy ACL:	Not in Use 💌	
QOS		_
QOS Profile Name:	Not in Use 💌	
Input Policy Map:	Not in Use 💌	
Output Policy Map:	Not in Use 💌	
Voice VLAN		_
Permission to Join:	Not in Use 💌	
Reauthentication		
Reauthentication Timer:	Not in Use 💌	
Maintain Connectivity durin Reauthentication:	g	

1

Figure 126 Authorization Profiles—Common Tasks Tab

Step 3 Click Submit.

Modifying the Contractor Authorization Profile

Step 1 Select the **Contractor-Authz** profile (see Figure 127).

Figure 127 Modifying the Contractor-Authz Profile

Policy Elem	ents : Authorizati	on and Permissions	> Network Access >	Authorization F	Profiles > Edi	t: "Contracto	r-Authz"	
General	Common Tasks	RADIUS Attributes						
General * Name: Descrip	Contractor-/	Authz						14334
*Required	fields N							- (1

Select the **Common Tasks** tab (see Figure 128) and do the following:

- **a**. For the VLAN ID/Name drop-down option, select **static**.
- **b.** In the Value input field, type **CONTRACTOR**.
- **c.** Under the ACLS section, from the Downloadable ACL Name drop-down menu, change **static** to **Not in Use**.

General	Common Tasks	RADIUS Attributes	
VLAN ID/N	ame:	Static 🔹	Value CONTRACTOR
URL for Re	direct:	Not in Use 💌	
URL Redire	ect ACL:	Not in Use 💌	
ACLS			
Download	able ACL Name:	Not in Use 💌	
IOS ACL F	ilter ID:	Not in Use 💌	
Proxy ACL	.:	Not in Use 💌	
QOS			
QOS Profil	e Name:	Not in Use 💌	
Input Polic	y Map:	Not in Use 💌	
Output Pol	icy Map:	Not in Use 💌	
Voice VL	AN		
Permission	n to Join:	Not in Use 💌	
Reauthe	ntication		
Reauthent	ication Timer:	Not in Use 💌	
Maintain C Reauthent	onnectivity durin ication:	g	

Figure 128 Authorization Profiles—Common Tasks Tab

Step 2 Click Submit.

Table 14

ſ

Verifying Global Switch VLAN Definition

VLANs

Verify that the VLANs listed in Table 14 are enabled on the TrustSec-enabled switch.

	VI AN ID	IP	Description
Monitor Mode	12/1112		Decemption
DATA	210	10.200.10.x/24	All non-Voice
VOICE	211	10.200.11.x/24	Voice Only
High Security Mode	(Above plus those lis	sted below)	
MACHINES	212	10.200.12.x/24	Managed Host/Assets
GUEST	213	10.200.13.x/24	Non-802.1X responsive Host
CONTRACTOR	214	10.200.14.x/24	Reserved for Contractors
AUTHFAIL	215	10.200.15.x/24	Failed 802.1X attempts

Figure 129 shows the output for the show run | begin vlan internal command.

vlan internal allocation policy ascending	
vlan 201	
name MAIN	
vlan 210	
name DATA	
vlan 211	
name VOICE	
vian 212	
name MACHINES	
1 11 an 212	
vian 213	
nume GOEST	
: vlan 214	
name CONTRACTOR	
vlan 215	
name AUTHFAIL	
vlan 250	
name RESTRICTED	
1	433.
	a a

Figure 129 show run | begin vlan internal Output

Configuring the Switch Port

Access your switch console and remove **ip access-group PRE-AUTH in** and **authentication open** on all of the TrustSec-enabled ports you have configured in the previous monitor and low impact modes:

```
interface range fa2/1-16
shut
switchport access vlan 210
switchport voice vlan 211
switchport mode access
ip access-group PRE-AUTH in <- Remove this entry
no ip access group PRE-AUTH in
authentication open <- Remove this entry
no authentication open
authentication host-mode multi-domain
authentication port-control auto
mab
dot1x pae authenticator
ip verify source vlan dhcp-snooping
no shut</pre>
```

When complete, make sure you bounce the affected interfaces by using the **shut** and then the **no shut** commands.

Verifying High Security Mode

This section includes the following topics:

- Verifying Host Network Connectivity and Network Services, page 99
- Verifying 802.1X-Capable Managed Assets, page 100
- Verifying Non-802.1X-Capable Managed Assets, page 102



I

Global AAA/RADIUS configuration verification should not be necessary because this was validated in the previous sections.

Verifying Host Network Connectivity and Network Services

The **show authentication sessions** Cisco IOS command is useful to display the state of all TrustSec-enabled switch ports on that switch. Figure 130 shows a port-specific derivative of this command.

id-4503-2#show authentication sessions								
Interface	MAC Address	Method	Domain	Status	Session ID			
Fa2/8	(unknown)	dot1x	UNKNOWN	Running	0AC8018000009D3890DCEED8			
Fa2/11	(unknown)	dot1x	UNKNOWN	Running	0AC8018000009D3990DCF2C0			
Fa2/1	0018.f809.cfc6	dot1x	DATA	Authz Success	0AC8018000009D3190DC8948			
Fa2/16	001b.d585.391e	dot1x	UNKNOWN	Running	0AC8018000009D3590DC9124			
Fa2/13	0018.bac7.bcfa	dot1x	UNKNOWN	Running	0AC8018000009D3790DC9510			
Fa2/12	0018.bac7.bcee	dot1x	UNKNOWN	Running	0AC8018000009D3690DC9510			
Fa2/14	0006.2504.c295	dot1x	UNKNOWN	Running	0AC8018000009D3390DC8D40			
Fa2/12	0021.8658.db6b	dot1x	UNKNOWN	Running	0AC8018000009D3A90DD020C			
Fa2/13	0018.f808.f838	dot1x	UNKNOWN	Running	0AC8018000009D3B90DD0598			

Figure 130 show authenticated sessions Output

You can also see the authentication status for a specific port; for example, show authentication session int f2/1 (see Figure 131).

id-4503-2#show authentic	cation sessions interface f2/1
Interface:	FastEthernet2/1
MAC Address:	0018.f809.cfc6
IP Address:	10.200.10.201
User-Name:	administrator
Status:	Authz Success
Domain:	DATA
Oper host mode:	multi-domain
Oper control dir:	both
Authorized By:	Authentication Server
Vian Policy:	210
Session timeout:	3600s (local), Remaining: 3233s
Timeout action:	Reauthenticate
Idle timeout:	N/A
Common Session ID:	0AC801800000002403D4FD7C
Acct Session ID:	0×0000002B
Handle:	0x53000024
Runnable methods list:	
Method State	
dot1x Authc S	uccess
mab Not run	

Figure 131 show authentication session int f2/1 Output

For another quick summary view, look at the Authentication and Authorization logs within ACS Reporting and Monitoring (see Figure 132).

Showing F	Dage	1 of	2 🗤 🖌 🕨	Goto Page:	>		
AAA Protocol >	> RAD	IUS AL	Ithentication				
Authentication Stat Date :	tus :	Pass or Februar	Fail 7y 3, 2009				
Senerated on Febr	uary 3,	2009 2:	13:20 PM PST				
Reload							
✓=Pass ×=Fail	0	Click for	r details				
					1		
Logged At	Status	Details	Failure Reason	User Name	Calling Station ID	Authentication Method	Selected Authorization Pr
Logged At 2:12:30.070 PM	Status V	Details	Failure Reason	User Name IMAC-CLIENT-2\Administrator	Calling Station ID 00-18-F8-08-F8-38	Authentication Method MSCHAPV2	Selected Authorization Pr CorpUser-Authz
Logged At 2:12:30.070 PM 2:11:45.026 PM	Status	Details Q Q	Failure Reason	User Name IMAC-CLIENT-2\Administrator 00-18-BA-C7-BC-FA	Calling Station ID 00-18-F8-08-F8-38 00-18-BA-C7-BC-FA	Authentication Method MSCHAPV2 Lookup	Selected Authorization Pr CorpUser-Authz Phone-Authz
Logged At 2:12:30.070 PM 2:11:45.026 PM 2:11:37.863 PM	Status	Q Q Q Q	Failure Reason	User Name IMAC-CLIENT-2\Administrator 00-18-BA-C7-BC-FA 00-18-BA-C7-BC-EE	Calling Station ID 00-18-F8-08-F8-38 00-18-BA-C7-BC-FA 00-18-BA-C7-BC-EE	Authentication Method MSCHAPV2 Lookup Lookup	Selected Authorization Pr CorpUser-Authz Phone-Authz Phone-Authz
Logged At 2:12:30.070 PM 2:11:45.026 PM 2:11:37.863 PM 2:11:22.506 PM	Status v v v	Q Q Q Q Q Q	Failure Reason	User Name IMAC-CLIENT-2\Administrator 00-18-BA-C7-BC-FA 00-18-BA-C7-BC-FE 00-21-86-58-DB-6B	Calling Station ID 00-18-F8-08-F8-38 00-18-BA-C7-BC-FA 00-18-BA-C7-BC-FE 00-21-86-58-DB-6B	Authentication Method MSCHAPV2 Lookup Lookup Lookup	Selected Authorization Pr CorpUser-Authz Phone-Authz Phone-Authz Contractor-Auth
Logged At 2:12:30.070 PM 2:11:45.026 PM 2:11:37.863 PM 2:11:22.506 PM 2:11:22.506 PM	Status V V V X	Details ् ् ् ् ् ् ् ् ् ् ् ्	Failure Reason	User Name IMAC-CLIENT-2\Administrator 00-18-BA-C7-BC-FA 00-18-BA-C7-BC-FE 00-21-86-58-DB-6B 00-18-F8-08-F8-38	Calling Station ID 00-18-F8-08-F8-38 00-18-BA-C7-BC-FA 00-18-BA-C7-BC-EE 00-21-86-58-DB-68 00-18-F8-08-F8-38	Authentication Method MSCHAPV2 Lookup Lookup Lookup Lookup	Selected Authorization Pr CorpUser-Authz Phone-Authz Phone-Authz Contractor-Auth
Logged At 2:12:30.070 PM 2:11:45.026 PM 2:11:27.863 PM 2:11:22.506 PM 2:11:22.506 PM 2:11:22.543 PM	Status V V V X X	Details Q Q Q Q Q Q Q Q Q Q Q Q Q Q Q	Failure Reason 22041 Unknown User 22041 Unknown User	User Name IMAC-CLIENT-2\Administrator 00-18-BA-C7-BC-FA 00-18-BA-C7-BC-FE 00-21-86-58-DB-6B 00-18-F8-08-F8-38 00-06-25-04-C2-95	Calling Station ID 00-18-F8-08-F8-38 00-18-BA-C7-BC-FA 00-18-BA-C7-BC-FE 00-21-86-58-DB-6B 00-18-F8-08-F8-38 00-06-25-04-C2-95	Authentication Method MSCHAPV2 Lookup Lookup Lookup Lookup Lookup	Selected Authorization Pr CorpUser-Authz Phone-Authz Phone-Authz Contractor-Auth
Logged At 2:12:30.070 PM 2:11:45.026 PM 2:11:37.863 PM 2:11:22.506 PM 2:11:22.506 PM 2:11:20.443 PM 2:11:20.443 PM	Status V V V X X V	Details e e e e e e e e e e e e e e e e e e e	Failure Reason 22041 Unknown User 22041 Unknown User	User Name IMAC-CLIENT-2\Administrator 00-18-BA-C7-BC-FA 00-18-BA-C7-BC-FE 00-21-86-58-DB-6B 00-18-F8-08-F8-38 00-06-25-04-C2-95 CP-7961G-SEP001BD585391E	Calling Station ID 00-18-F8-08-F8-38 00-18-BA-C7-BC-FA 00-18-BA-C7-BC-FE 00-21-86-58-DB-6B 00-18-F8-08-F8-38 00-06-25-04-C2-95 00-18-D5-85-39-1E	Authentication Method MSCHAPV2 Lookup Lookup Lookup Lookup CHAP/MD5	Selected Authorization Pr CorpUser-Authz Phone-Authz Phone-Authz Contractor-Auth

Figure 132 Authentication and Authorization Logs (1)

The screenshot shown in Figure 133 is the same list of hosts, which has been scrolled to the right to show the rest of the data available.

Figure 133 Authentication and Authorization Logs (2)

🔔 🚔 💽 🐱							Launch Inte	eractive Viewer
Showing Page	1 of 2	4 4 🕨		Goto I	Page:	•		
Selected Exception ofiles Authorization Profiles	Network Device	NAS IP Address	NAS Port	Access Service	Identity Store	Identity Group	CTS NAC R Security Group	cole ACS Instanc
	id-4503-2	10.200.1.128	50213	802.1X	AD1		· · · ·	ACS5-2
	id-4503-2	10.200.1.128	50213	MAB	Internal Hosts	All Groups: IP Phones		<u>ACS5-2</u>
	id-4503-2	10.200.1.128	50212	MAB	Internal Hosts	All Groups: IP Phones		ACS5-2
ız	id-4503-2	10.200.1.128	50212	MAB	Internal Hosts	All Groups:Contractor		ACS5-2
	id-4503-2	10.200.1.128	50213	MAB	Internal Hosts			ACS5-2
	id-4503-2	10.200.1.128	50214	MAB	Internal Hosts			ACS5-2
	id-4503-2	10.200.1.128	50216	802.1X	Internal Users	All Groups: IP Phones		ACS5-2
	id-4503-2	10.200.1.128	50201	802.1X	AD1			ACS5-2

As shown, all the administratively allowed devices have successfully authenticated and received the authorization policy as prescribed. Note that the host with the MAC address 00-06-25-04-C2-95 failed authentication. By having this log, you know that someone has plugged in a rogue device on switch id-4503-2 on port 50214 (that is, F2/14). Per policy in high security mode, this device is not allowed to gain access to the network.

Verifying 802.1X-Capable Managed Assets

802.1X Cisco IP Phone

In this simple verification step, verify that the phone has an IP address and has connected to the Call Manager. One easy test is to pick up the phone and see whether it has dial tone. If it does, chances are everything is working just fine.

For further verification, you can look at the switch port status (see Figure 134).

Figure 134	Switch Port Status
id-4503-2#show auth	session int f2/16
Interfa	ce: FastEthernet2/16
MAC Addre	ss: 001b.d585.391e
IP Addre	ss: 10.200.11.202
User-Na	me: CP-7961G-SEP001BD585391E
Stat	us: Authz Success
Doma	in: VOICE
Oper host mo	de: multi-domain
Oper control d	ir: both
Authorized	By: Authentication Server
Vlan Poli	cy: 211
Session timeo	ut: 3600s (local), Remaining: 2191s
Timeout acti	on: Reauthenticate
Idle timeo	ut: N/A
Common Session	ID: 0AC801800000002E03D5F924
Acct Session	ID: 0x00000035
Hand	le: 0x4400002E
Runnable methods li	st:
Method Sta	te
dot1x Aut	hc Success
mab Not	run

As shown, the phone successfully authenticated via 802.1X, was placed in the VOICE VLAN, and the host mode is multidomain.

Windows XP and Cisco SSC 802.1X Supplicant/Client

Step 1 From the Windows XP interface, double-click the SSC icon in the tray bar.



ſ

This loads the SSC dialog window showing the status of your connection (see Figure 136).

ctive Connection Gro	up		
Default		v	Configure Groups
vailable Connections			
configured connections ap	pear in boldface Signal	Security	Status
dux.local Wired Netwo	rk 💛 🗠		Connected

1

Figure 136 Connection Status

Step 2 For further verification, look at the switch port status (see Figure 137).

Figure 137 Switch Port Status

id-4503-2#show auth ses	sion int f2/1
Interface:	FastEthernet2/1
MAC Address:	0018.f809.cfc6
IP Address:	10.200.10.201
User-Name:	administrator
Status:	Authz Success
Domain:	DATA
Oper host mode:	multi-domain
Oper control dir:	both
Authorized By:	Authentication Server
Vian Policy:	210
Session timeout:	3600s (local), Remaining: 2043s
Timeout action:	Reauthenticate
Idle timeout:	N/A
Common Session ID:	0AC80180000002403D4FD7C
Acct Session ID:	0×000002B
Handle:	8x53000024
Runnable methods list:	
Method State	
dot1x Authc S	uccess
mab Notrun	Selected and the selection of the select
10.46 (MC 3.260)	

Verifying Non-802.1X-Capable Managed Assets

Cisco IP Phone (no 802.1X Supplicant)

Verify dial tone and look at the authentication status of the switch port. From before, two non-802.1X-capable phones are on ports F2/12 and F2/13. You can also determine where they are connected from the following Cisco IOS commands:

- show cdp neighbors
- show ip dhcp snooping binding

• show authentication session

You can also check the AAA logs from ACS.

Figure 138 shows the output for the show authentication sessions interface f2/12 & f2/13 command.

id-4503-2#show auth session int f2/12	id-4503-2#show auth session int f2/13
Interface: FastEthernet2/12	Interface: FastEthernet2/13
MAC Address: 0018.hoc7.hcee	MAC Address: 0018.bac7.bcfa
IP Address: 10.200.11.203	IP Address: 10.200.11.201
liser_Name: 00_18_B4_07_B0_FF	User-Name: 00-18-BA-C7-BC-FA
Status: Authz Success	Status: Authz Success
Domain: UNICE	Domain: VOICE
Oper host mode: multi domain	Oper host mode: multi-domain
Oper control dir: both	Oper control dir: both
Authorized Rus Authorization Server	Authorized By: Authentication Server
Wan Delieve 244	Vlan Policy: 211
Section timesut: N/A	Session timeout: N/A
Idle timeout: N/A	Idle timeout: N/A
Tute timeout: N/A Common Section ID: 010004000000000054504	Common Session ID: 0AC80180000002803D561A8
Common Session ID: 0AC00100000002A03D54504	Acct Session ID: 0x0000032
ACCT Session ID: 0X00000031	Handle: 0x34000028
Hanale: 0xCB00002A	Nandro. Oxonooodab
Barris I. S.	Punnable methods list:
Runnable methods list:	Method State
nethod State	dot1y Egiled over
dotix Failed over	mah Autho Success
mab Autho Success	mub Hutile Success
Interface: EastEthernet2/12	Interface: FastEthernet2/13
110011000. 1030201011002/12	
MAC Address: 0021_8658_db6b	MAC Address: 0018.f808.f838
TP Address: 10.200.10.205	IP Address: 10.200.10.203
User_Name: 00_21_86_58_DB_68	User-Name: IMAC-CLIENT-2\Administrator
Status: Authz Success	Status: Authz Success
Domain: DATA	Domain: DATA
Oper host mode: multi-domain	Oper host mode: multi-domain
Oper control dir: both	Oper control dir: both
Authorized By: Authentication Server	Authorized By: Authentication Server
Ulan Policy: 214	Vlan Policy: 210
Session timeout: N/A	Session timeout: N/A
Idle timeout: N/A	Idle timeout: N/A
Common Section ID: 04C90190000002903DE0E48	Common Session ID: 04C80180000002903D50554
Acct Session ID: 0x000000000000000000000	Acct Session ID: 0x0000030
Handle: 0v1000002F	Handle: 0x30000029
HUNUTE: 0X19000020	
Punnable methods list.	Runnable methods list:
Method State	Method State
dot1y Egiled over	dot1x Autho Success
mah Autho Success	mah Failed over
mub Autric Success	

Figure 138 show authentication sessions interface f2/12 and f2/13 Output

As shown from the output of these Cisco IOS **show** commands, two devices are authenticated on each port: a phone and a PC. The phones are placed in the VOICE domain and the PCs in the DATA domain.

For port F2/12, the phone and the PC are both authenticated via MAB. On port F2/13, the phone is authenticated via MAB and the PC is authenticated via 802.1X. Both ports have the same configuration. This is the power of FlexAuth and multiauth.

Furthermore, using the **show vlan** command, you can see that interface f2/12 is in both the VOICE and CONTRACTOR VLANs (see Figure 139).

214347

Fig	ure 139	show vlan Outpu	ıt						
id-4	id-4503-2#show vlan								
VLAN	Name	Status	Ports						
1	default	active	611/1, 611/2, Fa2/3, Fa2/4 Fa2/5, Fa2/6, Fa2/7, Fa2/9 Fa2/18, Fa2/17, Fa2/18, Fa2/19 Fa2/28, Fa2/21, Fa2/22, Fa2/23 Fa2/24, Fa2/25, Fa2/36, Fa2/21 Fa2/32, Fa2/29, Fa2/36, Fa2/31 Fa2/32, Fa2/33, Fa2/34, Fa2/39 Fa2/36, Fa2/31, Fa2/38, Fa2/39 Fa2/48, Fa2/41, Fa2/42, Fa2/43						
201	MATN	active	102/44, 102/45, 102/46, 102/47						
210	DATA	active	Fa2/1, Fa2/2, Fa2/8, Fa2/11 Fa2/13, Fa2/14, Fa2/15, Fa2/16						
211	VOICE	active	Fa2/1, Fa2/2, Fa2/8, Fa2/11 Fa2/12, Fa2/13, Fa2/14, Fa2/15 Fa2/16						
212 213 214 215	MACHINES GUEST CONTRACTOR AUTHFAIL	active active active active	Fa2/12						

The phone that is in the VOICE domain has been placed in the VOICE VLAN and the PC that is in the DATA domain is in the CONTRACTOR VLAN.

1

You can also repeat the validation steps performed in the "Verifying Monitor Mode" section on page 36 for a complete validation.

Creating a Certificate for a Windows XP Browser

To create a certificate for your Windows XP browser, complete the following steps.

Procedure

Step 3 Access your CA via your browser; for example, http://demo.local/certsrv/ (see Figure 140).

● ● ● ● imac-mcs-20	
Microsoft Certificate Services - Microsoft Internet Explorer File Edit View Eavorites Tools Help	. 8 ×
O Back ▼ O ~ R 2	
Address 🕘 http://ad.idux.local/certsrv/	Links
Microsoft Certificate Services mcs-17 Hon	ne
Welcome	_
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.	
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.	
For more information about Certificate Services, see Certificate Services Documentation.	
Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL	
Re la companya de la companya	
Done	<u> </u>
🥂 Start 🛛 😰 🙈 🔰 🖉 Cisco Secure ACS Pre-Re 🖉 Microsoft Certificate	N

Figure 140 Microsoft Certificate Services Screen

I

Γ

Step 4 Select **Download a CA Certificate**, **Certificate Chain**, or **CRL** (see Figure 141).

900	imac-mcs-20	
Microsoft Certificate Services - Micros	oft Internet Explorer	_ 8 :
ele Edit View Favorites Tools Hel		~~~
Back • 🕤 • 🗶 💈 🏠 🔑 Search	n 🛠 Favorites 🐇 🔯 🖾	
goress en http://ad.idux.local/certsrv/certc	arc.asp	So Link
Microsoft Certificate Services mc	s-17	Home
Download a CA Certificate, C	ertificate Chain, or CRL	
To trust certificates issued from	this certification authority, install this CA certificate chain.	
Fo download a CA certificate, c	ertificate chain, or CRL, select the certificate and encoding method.	
CA certificate:	_	
Current [mcs-17]	1	
Encoding method:	-	
© DER		
Download CA certificate chain		
Download latest base CRL		
Download latest delta CRL		
	\searrow	
	*	
		<u>.</u>
		rusted sites
Start 🛛 🕼 🕭 👘 🖉 Cisco Secure	ACS Pre-Re 🖉 Microsoft Certificate	9 6

1

Figure 141 Selecting a Certificate to Download

- Step 5 Download a CA Certificate (see Figure 142, Figure 143, Figure 144, Figure 145, and Figure 146).

Note ACS supports only the DER certificate format. Save the certificate (*demo-local-ca-cert.cer*) for installation into your browser or applications.

00				imac-mcs-20		
My Compub	er					
кесусіе ві	n _i ,					
-						
Holding						
MEDIANET CAM1	Т					
- 20						
ACS 5.0 -						
IDUX.LOCA	AL.					
Certificate_						
10000						
idux-loca	Open Install Certificate					
ert.c	Open With					
	Scan for viruses					
ca-cert-D	Cut				N	
	⊆ору				1	
	Create Shortcut Delete					
ca-cert-B	Rename					
者 Start	Properties	Secure ACS Pre-Re	Microsoft Certificate Ser	. Ertificate_Signing_Reg		1435
						N 1/2

Figure 142 Opening the Certificate

Γ

Figure 143 Certificate Import Wizard and Select Certificate Store Screens

Certificate Import Wizard	Select Certificate Store
Certificate Store Certificate stores are system areas where certificates are kept.	Select the certificate store you want to use.
Windows can automatically select a certificate store, or you can specify a location for C Automatically select the certificate store based on the type of certificate Place all certificates in the following store Certificate store: Browse Browse	Personal Trusted Root Certification Authorities Registry Local Computer Trusted Root Certification Authorities Totermediate Certification Authorities Show physical stores OK Cancel
< <u>Back</u> Next > Cancel	14362

214353

Certificate Import Wizard		X
Completing the Certificate Impor Wizard		Certificate Import
	You have successfully compl wizard.	eted the Certificate Import
	You have specified the follow	ving settings:
	Certificate Store Selected Content	Automatically determined by t Certificate
	•	•
	,	
	< <u>B</u> ack	Finish Cancel

Figure 144 Completing the Certificate Import Wizard Screen

1

Figure 145 Warning Message

Security	Warning 🔀	
	You are about to install a certificate from a certification authority (CA) claiming to represent:	
	mcs-17	
	Windows cannot validate that the certificate is actually from "mcs-17". You should confirm its origin by contacting "mcs-17". The following number will assist you in this process:	
	Thumbprint (sha1): D975473D FCBD2FE2 380B9090 82568FDF CC74A125	
	Warning: If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.	
	Do you want to install this certificate?	
	<u>Y</u> es	214.355

Figure 146 Success Message

Certificat	e Import Wizard 🛛 🔀	
•	The import was successful.	
		214356
References

TrustSec 1.99 Documents

- Wired 802.1X Deployment Guide http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_1.99/Dot1X_Deployme nt/Dot1x_Dep_Guide.html
- IP Telephony for 802.1X Design Guide http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_1.99/IP_Tele/IP_Teleph ony_DIG.html
- MAC Authentication Bypass Deployment Guide http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_1.99/MAB/MAB_Dep_ Guide.html
- TrustSec Phased Deployment Configuration Guide http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_1.99/Phased_Deploy/Ph ased_Dep_Guide.html
- Local WebAuth Deployment Guide http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_1.99/WebAuth/WebAut h_Dep_Guide.html
- Scenario-Based TrustSec Deployments Application Note http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_1.99/Scenario_based_A ppNote/Scenario_based_AN.html
- TrustSec 1.99 Deployment Note: FlexAuth Order, Priority, and Failed Authentication http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_1.99/FlexAuthNote/flex auth-note.html
- TrustSec Planning and Deployment Checklist http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_1.99/TrustSec_Checklis t/trustsec-199_checklist.html

Related Documents

- Configuring WebAuth on the Cisco Catalyst 3750 Series Switches http://www.cisco.com/en/US/partner/docs/switches/lan/catalyst3750/software/release/12.2_55_se/ configuration/guide/sw8021x.html
- Configuring WebAuth on the Cisco Catalyst 4500 Series Switches http://www.cisco.com/en/US/partner/docs/switches/lan/catalyst4500/12.2/53SG/configuration/web auth.html
- Configuring WebAuth on the Cisco Catalyst 6500 Series Switches http://www.cisco.com/en/US/partner/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/gui de/webauth.html
- Cisco IOS Firewall authentication proxy http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a0080094eb0. shtml

• WebAuth with Cisco Wireless LAN Controllers http://www.cisco.com/en/US/partner/tech/tk722/tk809/technologies_configuration_example09186 a008076f974.shtml#external-process

1