



Cisco TrustSec How-To Guide: Authenticating to Multiple AD Domains

For Comments, please email: howtoguides@external.cisco.com

Current Document Version: 3.0

August 27, 2012

Table of Contents

Table of Contents.....	2
Introduction	3
What Is the Cisco TrustSec System?.....	3
About the TrustSec How-To Guides.....	3
<i>What does it mean to be "TrustSec Certified"?</i>	4
Solution Overview.....	5
ISE Communication to Active Directory as a LDAP Server	5
<i>Searching Active Directory</i>	5
<i>EAP Authentication Methods</i>	5
Scenario Overview	6
Configuring ISE for TLS authentication	7
<i>Configure an LDAP Server</i>	7
<i>Configuration for EAP-TLS Connections</i>	10
<i>Authentication</i>	12
Appendix A.....	15
Authenticating Users via PEAP-GTC	15
Appendix B: References.....	21
TrustSec System:	21
Device Configuration Guides:	21

Introduction

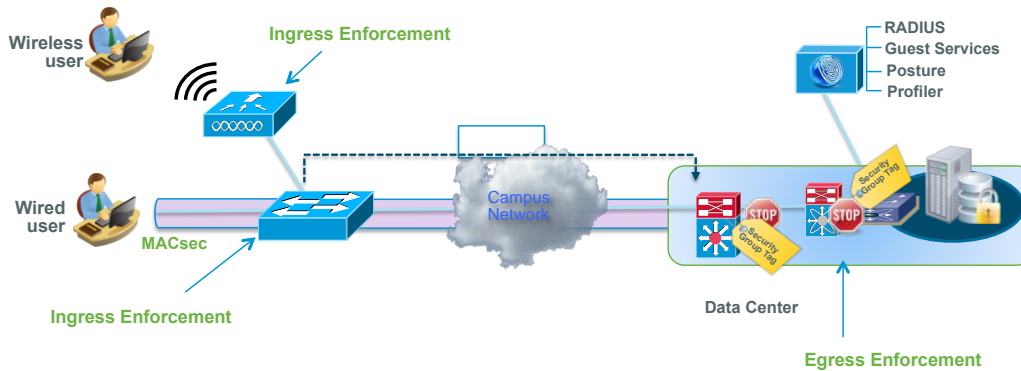
What Is the Cisco TrustSec System?

Cisco TrustSec®, a core component of the Cisco SecureX Architecture™, is an intelligent access control solution. TrustSec mitigates security risks by providing comprehensive visibility into who and what is connecting across the entire network infrastructure, and exceptional control over what and where they can go.

TrustSec builds on your existing identity-aware access layer infrastructure (switches, wireless controllers, and so on). The solution and all the components within the solution are thoroughly vetted and rigorously tested as an integrated system.

In addition to combining standards-based identity and enforcement models, such as IEEE 802.1X and VLAN control, the TrustSec system it also includes advanced identity and enforcement capabilities such as flexible authentication, Downloadable Access Control Lists (dACLs), Security Group Tagging (SGT), device profiling, posture assessments, and more.

Figure 1: TrustSec Architecture Overview

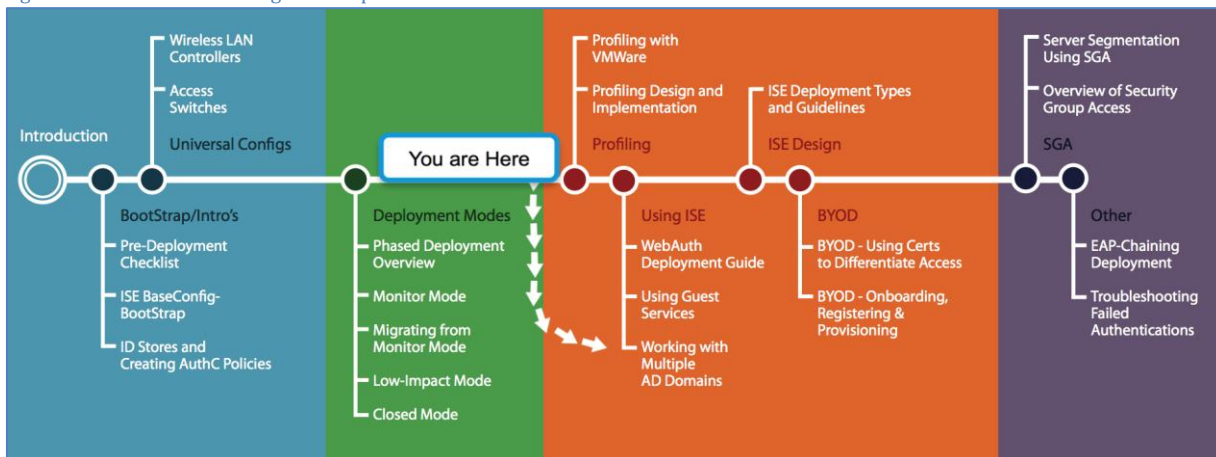


About the TrustSec How-To Guides

The TrustSec team is producing this series of How-To documents to describe best practices for TrustSec deployments. The documents in the series build on one another and guide the reader through a successful implementation of the TrustSec system. You can use these documents to follow the prescribed path to deploy the entire system, or simply pick the single use-case that meets your specific need.

Each guide in this series comes with a subway-style “You Are Here” map to help you identify the stage the document addresses and pinpoint where you are in the TrustSec deployment process (Figure 2).

Figure 2: How-To Guide Navigation Map



What does it mean to be ‘TrustSec Certified’?

Each TrustSec version number (for example, TrustSec Version 2.0, Version 2.1, and so on) is a certified design or architecture. All the technology making up the architecture has undergone thorough architectural design development and lab testing. For a How-To Guide to be marked “TrustSec certified,” all the elements discussed in the document must meet the following criteria:

- Products incorporated in the design must be generally available.
- Deployment, operation, and management of components within the system must exhibit repeatable processes.
- All configurations and products used in the design must have been fully tested as an integrated solution.

Many features may exist that could benefit your deployment, but if they were not part of the tested solution, they will not be marked as “TrustSec “certified”. The TrustSec team strives to provide regular updates to these documents that will include new features as they become available, and are integrated into the TrustSec test plans, pilot deployments, and system revisions. (i.e., TrustSec 2.2 certification).

Additionally, many features and scenarios have been tested, but are not considered a best practice, and therefore are not included in these documents. As an example, certain IEEE 802.1X timers and local web authentication features are not included.

Note: Within this document, we describe the recommended method of deployment, and a few different options depending on the level of security needed in your environment. These methods are examples and step-by-step instructions for TrustSec deployment as prescribed by Cisco best practices to help ensure a successful project deployment.

Solution Overview

The Cisco Identity Services Engine (ISE) integrates with external identity sources to validate credentials in user authentication functions and to retrieve group information and other attributes that are associated with the user for use in authorization policies. ISE supports multiple types of external identity sources such as Active Directory, Lightweight Directory Access Protocol (LDAP), and other RADIUS servers.

Cisco ISE supports integration with a single Active Directory identity source. Cisco ISE uses this Active Directory identity source to join itself to an Active Directory domain. If this Active Directory source has a multidomain forest, trust relationships must exist between its domain and the other domains in order for Cisco ISE to retrieve information from all domains within the forest. This dependency on trust becomes an issue for large-scale deployments that can't have trust relationships between domains due to compliance policies or government regulations.

Active Directory is Microsoft's implementation of LDAPv3 directory services. Thus, directory clients can use LDAP to search for and retrieve information from an Active Directory server. Cisco ISE can function as a directory client and, in that function, can communicate to multiple LDAP servers.

This document explains how Cisco ISE can communicate via LDAP to Active Directory servers in an untrusted domain or forest.

ISE Communication to Active Directory as a LDAP Server

Searching Active Directory

Active Directory supports LDAP-based searches on port 3268 (global catalog) and port 389 (LDAP). The main benefit to searching the global catalog is that the search includes all directory partitions in the forest. Searches using port 389 can only include single domain directory partitions. Configuring Cisco ISE to search the global catalog requires configuration of a single external LDAP identity source rather than multiple identity sources that represent each Active Directory domain.

While a global catalog search minimizes Cisco ISE configuration tasks, it poses an issue when authorization rules are defined by Active Directory groups. (See the Appendix for further details.)

EAP Authentication Methods

Cisco ISE supports all Extensible Authentication Protocol (EAP) versions, including Transport Layer Security (TLS) and Protected EAP-Generic Token Card (PEAP-GTC). However, Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2) is not possible when an LDAP-based authentication server is used. Table 1 shows these authentication and authorization policies (AuthC and AuthZ).

Table 1 EAP Authentication Methods and Authentication Types That Work with LDAP

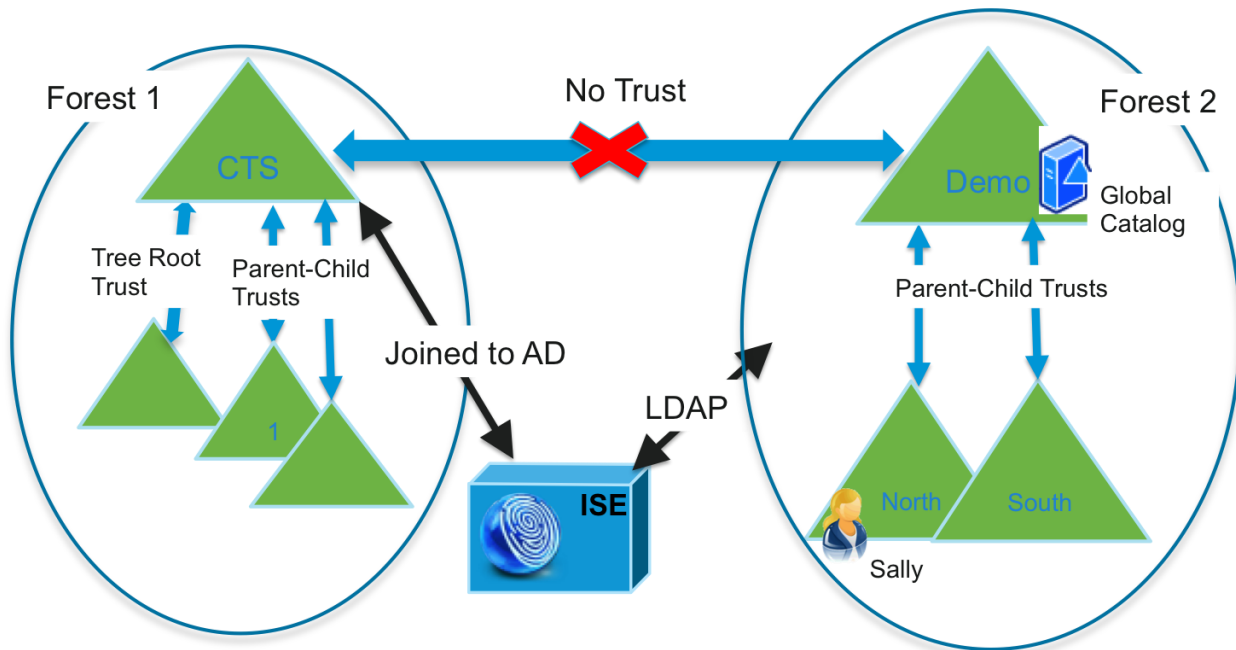
	Machine AuthC	Machine AuthZ	User AuthC	User AuthZ
EAP-TLS (port 389)	Yes	Yes	Yes	Yes
EAP-TLS (port 3268)	Yes	Yes	Yes	Yes; conditions apply*
MSCHAPv2	No	No	No	No
PEAP-GTC (port 389)	No	No	Yes	Yes
PEAP-GTC (port 3268)	No	No	Yes	Yes; conditions apply*

Note: The “memberOf” attribute within the Active Directory schema depicts what Active Directory groups a user belongs to. A global catalog server is a domain controller that, in addition to its full, writable domain directory partition replica, also stores a partial, read-only replica of all other domain directory partitions in the forest. The replica of the child domain does not store the “memberOf” attribute, however, so authorization rule definitions based on groups in child domains will fail. Appendix 2 describes a potential workaround for this exception.

Scenario Overview

Figure 2 shows an example topology.

Figure 3 Active Directory Topology



In this scenario, ISE must authenticate engineers that are in both the CTS and Demo forests. The CTS and Demo forests do not have a cross-forest trust established between them. ISE is already configured to authenticate against the CTS forest via Active Directory. This document details how to configure ISE to authenticate and authorize users and machines in the Demo forest, which comprises the parent domain, Demo.local, and two child domains, North.demo.local and South.demo.local.

The main section of this document details configuration for authentication via EAP-TLS on port 389. Since many of the configuration steps are the same, configuration for authentication via PEAP-GTC is covered in Appendix A.

Configuring ISE for TLS authentication

Note: Creating and deploying user and machine certificates are out of the scope of this document.

Note: Certificates used for this document were generated by a 2008 R2 Microsoft Active Directory Certificate Server.

Configure an LDAP Server

To complete an LDAP search, Cisco ISE must complete the following steps:

- Find a LDAP directory server.
- Establish a connection.
- Authenticate against (bind to) the LDAP directory server.
- Perform a search.

The steps below guide you through configuring Cisco ISE to perform these functions.

Procedure 1 Configure an LDAP Server

Step 1 Navigate to Administration → Identity Management → External Identity Sources → LDAP.

Step 2 Click Add.

Step 3 Configure the name as **Demo**.

Step 4 Select Custom as the schema and set the Subject Name Attribute to **CN**.

Figure 4 General LDAP Configuration

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The navigation pane on the left shows the path: Administration > Identity Management > External Identity Sources > LDAP. The main content area is titled 'LDAP Identity Source' and shows the 'General' tab. The configuration fields are as follows:

- * Name: Demo
- Description: (empty)
- Schema: Custom (indicated by a red arrow)
- * Subject Objectclass: Person
- * Subject Name Attribute: CN (indicated by a red arrow)
- * Group Objectclass: Group
- * Group Map Attribute: memberOf
- Certificate Attribute: userCertificate
- ☒ Subject Objects Contain Reference To Groups
- ☐ Group Objects Contain Reference To Subjects
- Subjects In Groups Are Stored In Member Attribute As: Distinguished Name

Step 5 Click the Connection tab.

Step 6 Enter the hostname/IP.

Step 7 Enter the port number as **389**.

Step 8 Select Authenticated Access.

Step 9 Enter the Admin DN. This is the DN (distinguished name) for a user that is a member of the Schema Admins group within Active Directory. For example: **cn=SchemaAdmin, cn=Users, dc=demo, dc=local**.

Step 10 Enter the Admin DN's password.

Figure 5 LDAP Connection Configuration

The screenshot shows the 'LDAP Identity Source' configuration page with the 'Connection' tab selected. The 'Primary Server' section contains the following fields:

- * Hostname/IP: 10.1.101.100
- * Port: 389
- Access: ☐ Anonymous Access, ☒ Authenticated Access
- Admin DN: * cn=schemaadmin,cn=users,dc=demo,dc=local
- Password: * [masked]
- Secure Authentication: ☐ Enable Secure Authentication
- Root CA: cts-AD-CA#cts-AD-CA#00006
- * Server Timeout: 10 Seconds
- * Max. Admin Connections: 20

A purple callout bubble points to the 'Admin DN' field with the text: 'User must be a member of Schema Admins groups'.

At the bottom are 'Submit' and 'Cancel' buttons.

Step 11 Click the Directory Organization tab.

Step 12 Configure both the Subject Search Base and the Group Search Base as **DC=demo, DC=local**.

Best Practice: Be as specific as possible when defining the search bases. For a standard Active Directory server configuration, the search base to use for subject and group search is CN=Users, <Domain Component>. (CN=Users, DC=demo, DC=local)

Step 13 Check the box titled “Strip start of subject name up to the last occurrence of the separator.” Enter @ as the separator value.

Step 14 Check the box titled “Strip end of subject name from the first occurrence of the separator.” Enter a period as the separator value.

Step 15 Click Submit.

Figure 6 LDAP Identity Source Configuration

LDAP Identity Sources List > **New LDAP Identity Source**

LDAP Identity Source

General Connection **Directory Organization** Groups Attributes

* Subject Search Base ⓘ

* Group Search Base ⓘ

Search for MAC Address in Format ▼

* ☒ Strip start of subject name up to the last occurrence of the separator

* ☒ Strip end of subject name from the first occurrence of the separator

Annotations:

- Necessary for user authentication (points to '@' separator)
- Necessary for machine authentication (points to '.' separator)

[[Note: In the figure, the text box that takes the period also shows a pipe symbol. Is this just an unintentional inclusion of the cursor, or does a pipe need to be typed in as well? Could be confusing to the reader.]]

Notes: In this example, the search bases are defined to start the directory search at the top of the directory tree. You should refine this based on your directory schema.

During user authentication, the username is sent in user@domain format. By enabling the separator, only the username is passed to the LDAP server. During machine authentication, the username is sent in machine.domain format. By enabling the separator, only the machine name is passed to the LDAP server.

Step 16 Navigate to Groups.

Step 17 Click Groups → Add → Select Groups From Directory.

Cisco ISE allows a network administrator to select specific groups and attributes from Active Directory. This scenario enables faster lookup times when authenticating a user. It also ensures that, when building policies related to AD groups, the administrator needs to look through only a small list instead of every group in AD.

Figure 7 LDAP Identity Group Configuration

LDAP Identity Sources List > **New LDAP Identity Source**

LDAP Identity Source

General Connection Directory Organization **Groups** Attributes

▼

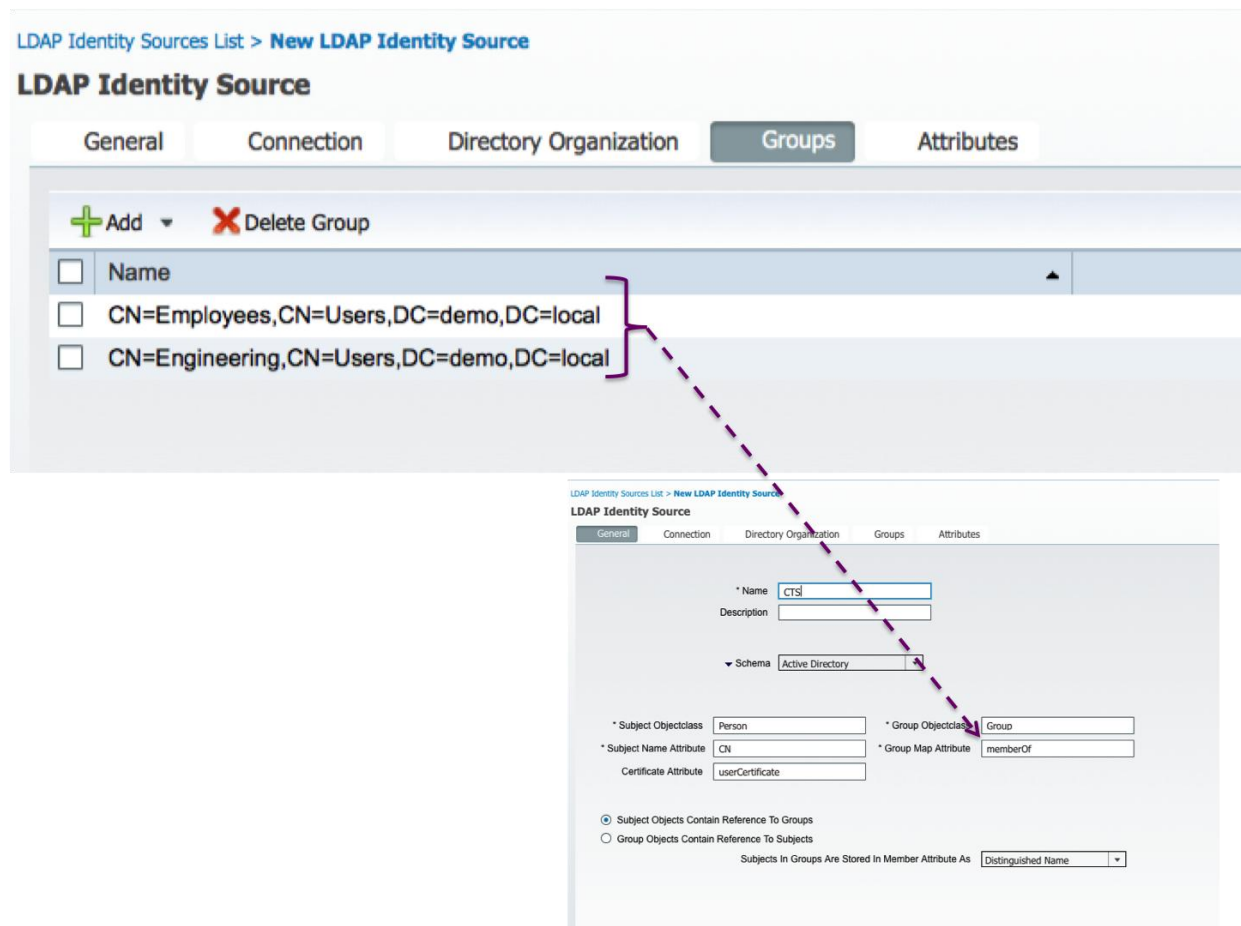
Select Groups From Directory

Add Group

Note: The groups found are the result of the returned values from a search based on the *MemberOf* attribute that was configured on the General screen.

Step 18 Of the groups retrieved, select the specific groups that will be used to define authentication and authorization policies.

Figure 8 LDAP Identity Group List



Step 19 Click Save.

Step 20 Repeat steps 1–20 for the North child domain. Substitute **CN=Users, DC=North, DC=Demo, DC=local** for the subject and group base search values in Step 12.

Configuration for EAP-TLS Connections

Procedure 1 Define a Certificate Authentication Profile

A certificate authentication profile (CAP) is used to designate that authentication is based on certificates rather than a username and password sequence.

Step 1 Navigate to Administration → Identity Management → External Identity Sources → Certificate Authentication Profile

Step 2 Name the profile **Demo_CAP**.

Step 3 Set the Principal Username X509 Attribute to Common Name.

This defines what field within the certificate represents the username. This is directly related to the value selected for the Subject Name Attribute within the general configuration settings for the LDAP server.

Figure 9 CAP Configuration

The image shows two overlapping web forms. The background form is titled "Certificate Authentication Profile" and includes fields for "Name" (set to "Demo_CAP"), "Description", "Principal Username X509 Attribute" (set to "Common Name"), and "LDAP/AD Instance Name". It also has a checkbox for "Perform Binary Certificate Comparison with" and "Submit" and "Cancel" buttons. The foreground form is titled "LDAP Identity Source" and includes tabs for "General", "Connection", "Directory Organization", "Groups", and "Attributes". The "General" tab is active, showing fields for "Name" (set to "CTS"), "Description", "Schema" (set to "Active Directory"), "Subject Objectclass" (set to "Person"), "Subject Name Attribute" (set to "CN"), "Certificate Attribute" (set to "userCertificate"), "Group Objectclass" (set to "Group"), and "Group Map Attribute" (set to "memberOf"). It also has radio buttons for "Subject Objects Contain Reference To Groups" (selected) and "Group Objects Contain Reference To Subjects", and a dropdown for "Subjects In Groups Are Stored In Member Attribute As" (set to "Distinguished Name"). A dashed purple arrow points from the "Common Name" field in the CAP form to the "Subject Name Attribute" field in the LDAP form.

Step 4 Navigate to Administration → Identity Management → Identity Source Sequences.

Step 5 Click Add.

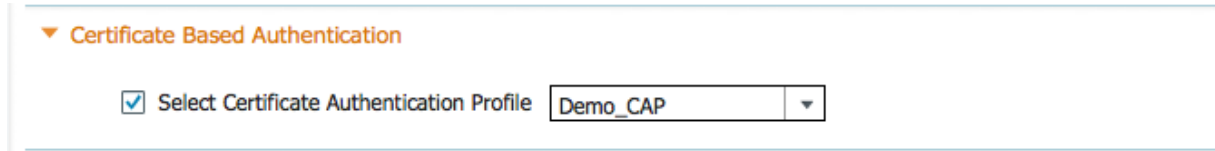
Step 6 Name the Identity Source Sequence **Demo_ID_Seq**.

Figure 10 Identity Source Sequence Configuration

The image shows the "Identity Source Sequence" configuration page in the Cisco Identity Services Engine. The page has a navigation bar with "Home", "Operations", "Policy", and "Administration" tabs, and a sub-navigation bar with "System", "Identity Management", "Network Resources", and "Web Portal Management" tabs. The "Identity Source Sequences" tab is selected. The page title is "Identity Source Sequence" and the breadcrumb is "Identity Source Sequences List > Demo_ID_Seq_for_TLS_and_PEAP". The form includes fields for "Name" (set to "Demo_ID_Seq_for_TLS") and "Description" (set to "Identity Source Sequence To Handle TLS Based Connections").

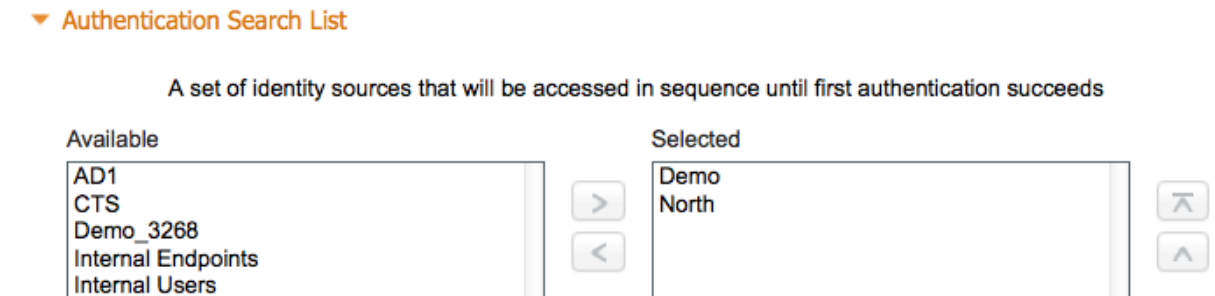
Step 7 Check the box titled “Select Certificate Authentication Profile” and choose Demo_CAP from the pull-down list.

Figure 11 Select the CAP



Step 8 Within the Authentication Search List, add the Demo and North identity source.

Figure 12 Authentication Search List



Step 9 Click Submit.

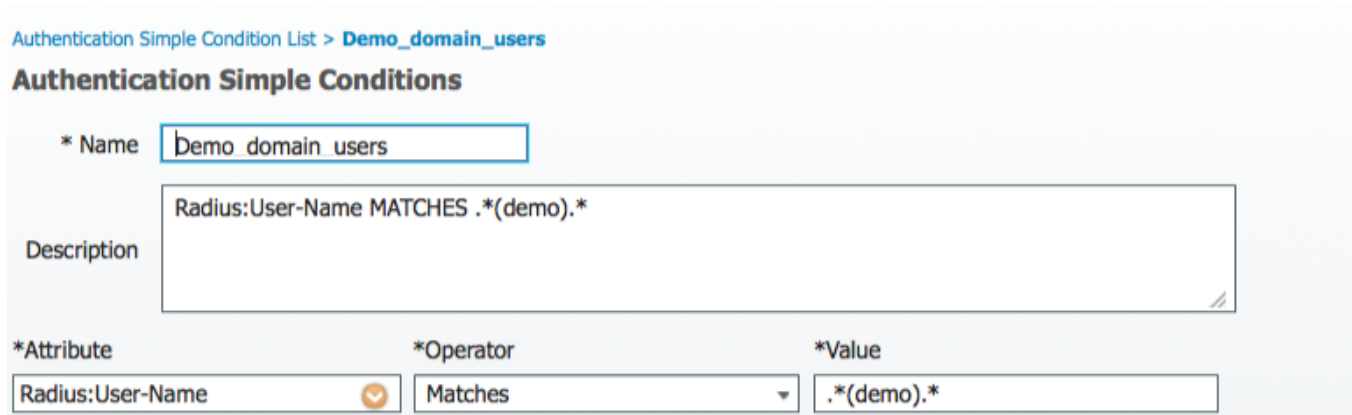
Authentication

Procedure 1 User Authentication

Step 1 Navigate to Policy → Policy Element → Conditions → Authentications → Simple Conditions.

Step 2 Add the condition shown in Figure 12.

Figure 13 Authentication Condition Configuration



Note: Supported regex syntax:

- `Starts with`—for example, using the REGEX value of `^(Acme).*`—this condition is configured as CERTIFICATE:Organization MATCHES `Acme` (any match with a condition that starts with "Acme").
- `Ends with`—for example, using the REGEX value of `.*(mktg)$`—this condition is configured as CERTIFICATE:Organization MATCHES `mktg` (any match with a condition that ends with "mktg").
- `Contains`—for example, using the REGEX value of `.*(1234).*`—this condition is configured as CERTIFICATE:Organization MATCHES `1234` (any match with a condition that contains "1234," such as Eng1234, 1234Dev, and Corp1234Mktg).
- `Does not start with`—for example, using the REGEX value of `^(?!LDAP).*`—this condition is configured as CERTIFICATE:Organization MATCHES `LDAP` (any match with a condition that does not start with "LDAP," such as usLDAP or CorpLDAPmktg).

Step 3 Click Submit.

Step 4 Navigate to Policy → Authentication.

Step 5 Create the rule shown in Figure 14.

Figure 14 Authentication Rule Configuration

Conditions Details

Wired_802.1X AND Demo_domain_users

☒ Demo Users : If Wired_802.1X A... allow protocols Allowed Protocol : Default Network and...

☒ Default : use Demo_ID_Seq_for_TLS

Step 6 Click Submit.

Procedure 2 User Authorization

Step 1 Navigate to Policy → Policy Elements → Results → Authorization → Authorization Profiles.

Step 2 Click Add.

Step 3 Add the profile shown in Figure 15.

Figure 15 Authorization Profile

Authorization Profiles > Demo_Machines

Authorization Profile

* Name: Demo Machines

Description:

* Access Type: ACCESS_ACCEPT

Common Tasks

☒ DACL Name: PERMIT_ALL_TRAFFIC

Step 4 Click Submit.

Step 5 Navigate to Policy → Authorization.

Step 6 Create the rule shown in Figure 16 for user authorization.

Figure 16 Authentication Rule

☒ Engineer_in_Demo_Domain if (North:ExternalGroups EQUALS CN=Engineering,CN=Users,DC=north,DC=demo,DC=local OR Demo:ExternalGroups EQUALS CN=Engineering,CN=Users,DC=demo,DC=local) then Engineer

Step 7 Create the rule shown in Figure 17 to authorize machines.

Figure 17 Authorization Rule

☒ Demo_Machines if (Radius:User-Name STARTS_WITH host/ AND CERTIFICATE:Subject Alternative Name MATCHES .*(demo.local)\$) then Demo_Machines

Procedure 3 Test Machine and User Authentication

Configuration is done! It's time to verify that both machine and user authentication are working correctly.

Step 1 Connect to the network with a Windows or MAC device configured for an EAP-TLS connection.

Note: Native Windows and MAC supplicant configuration is beyond the scope of this document.

Note: If the client certificate is issued by a private certificate authority, you must import the root certificate into ISE

Step 2 View the Cisco ISE Live Authentication Log for the machine session.

Figure 18 Live Authentication Log

WIN7-2	00:10:18:64:E3:DE	10.1.10.101	GigabitEthernet0/1	Demo_Machines	Profiled:Workstation	Authentication succeeded	dot1x	EAP-TLS
--------	-------------------	-------------	--------------------	---------------	----------------------	--------------------------	-------	---------

Figure 19 Authentication Log for Machine

Authentication Summary	
Logged At:	May 30,2012 6:50:18.584 AM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	WIN7-2
MAC/IP Address:	00:10:18:64:E3:DE
Network Device:	3K-X : 10.1.48.2 : GigabitEthernet0/1
Allowed Protocol:	Default Network Access
Identity Store:	
Authorization Profiles:	Demo_Machines
SGA Security Group:	
Authentication Protocol :	EAP-TLS

Step 3 View the Cisco ISE Live Authentication Log for the user session.

Figure 20 Live Authentication Log - User

neng1	00:10:18:64:E3:DE	10.1.10.100	GigabitEthernet0/1	Engineer	Profiled:Workstation	Authentication succeeded
-------	-------------------	-------------	--------------------	----------	----------------------	--------------------------

Figure 21 Authentication Log for User

Authentication Summary	
Logged At:	May 29,2012 11:02:52.363 PM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	neng1
MAC/IP Address:	00:10:18:64:E3:DE
Network Device:	3K-X : 10.1.48.2 : GigabitEthernet0/1
Allowed Protocol:	Default Network Access
Identity Store:	
Authorization Profiles:	Engineer
SGA Security Group:	
Authentication Protocol :	EAP-TLS

Appendix A

Authenticating Users via PEAP-GTC

Authentication via PEAP-GTC does not require the use of certificates. PEAP-GTC is a username- and password-based authentication method. Cisco AnyConnect® Network Access Manager 3.1 is one of the only supplicants that supports EAP-GTC. Cisco AnyConnect Network Access Manager is a module of Cisco AnyConnect Client for Windows 3.x and provides a fully configurable and powerful supplicant option instead of the native supplicant of the Windows OS. The Network Access Manager (NAM) is licensed with no charge, and more information may be found here:

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/data_sheet_c78-527494.html

Below are instructions on how to configure the standalone profile editor. For instructions on how to configure AnyConnect via Cisco Adaptive Security Device Manager (ASDM), please reference the following guide:

http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect20/administrative/guide/adminpre.html

Procedure 1 Cisco AnyConnect NAM Configuration

Step 1 Select Networks, click Add, enter: **wired-peap**.

Step 2 Follow the configuration settings in Figure 22

Figure 22 AnyConnect Configuration for Wired 802.1X Connection

Networks
Profile: Untitled

Name: wired-peap

Group Membership

☐ In group: (auto-generated)

☒ In all groups (Global)

Choose Your Network Media

☒ Wired (802.3) Network

Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.

☐ Wi-Fi (wireless) Network

Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.

SSID (max 32 chars):

☐ Hidden Network

Association Timeout (sec) 5

Common Settings

Script or application on each user's machine to run when connected.

Browse Local Machine

Connection Timeout (sec.) 40

Media Type

Security Level

Next Cancel

Step 3 Click Next.

Step 4 Select Authenticating Network.

Step 5 Set the “startPeriod” to 10

Step 6 Check “EAP fails” under the Port Authentication Exception Policy.

Step 7 Click the checkbox for “Enable port exceptions”

Figure 23 AnyConnect NAM Security Level Configuration

Networks
Profile: Untitled

Security Level

☐ Open Network
Open networks have no security, and are open to anybody within range. This is the least secure type of network.

☒ Authenticating Network
Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.

802.1X Settings

authPeriod (sec.) 30 startPeriod (sec.) 10
heldPeriod (sec.) 60 maxStart 2

Security

Key Management
None

Encryption
None

Port Authentication Exception Policy

☒ Enable port exceptions

☐ Allow data traffic before authentication

☒ Allow data traffic after authentication even if

☒ EAP fails

☐ EAP succeeds but key management fails

Next Cancel

Media Type
Security Level
Connection Type
User Auth
Credentials

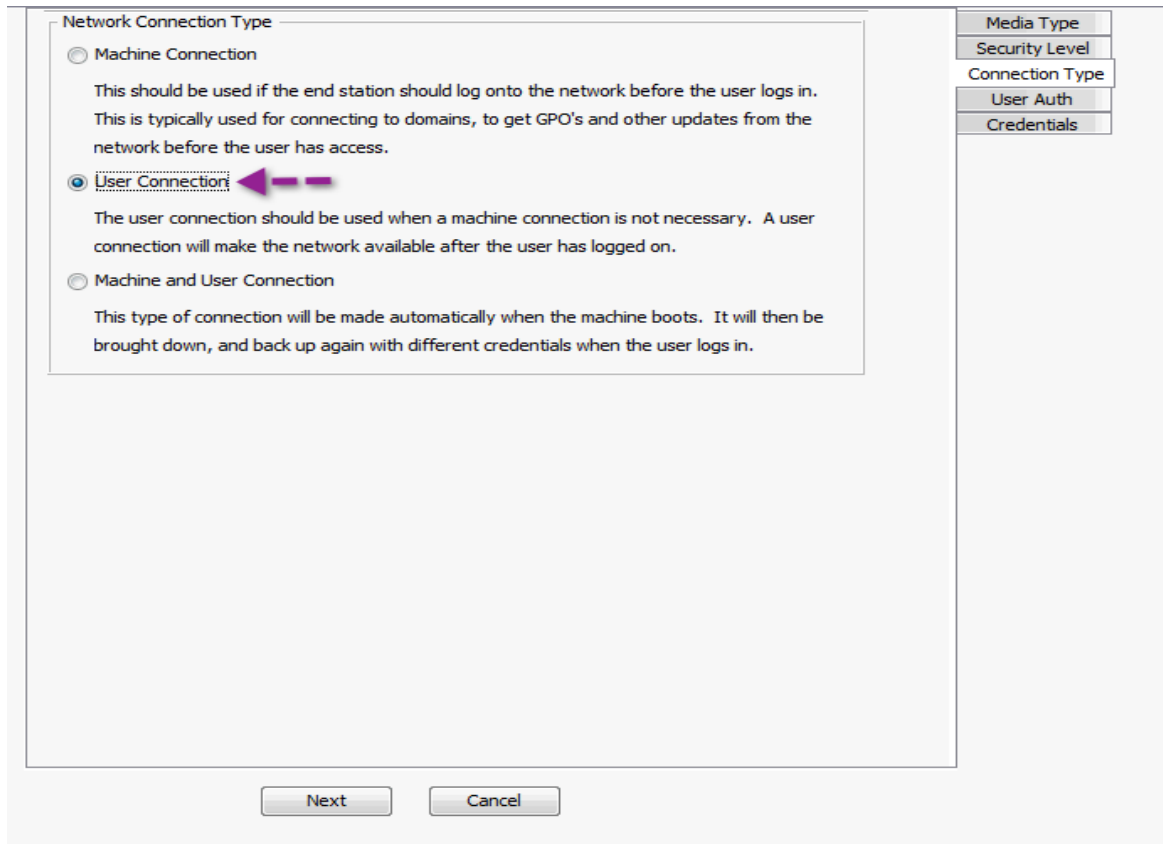
Note: Since the switchport is configured for open mode, the above steps configure NAM to allow traffic to flow even if EAP fails. Otherwise NAM, per IEEE 802.1X specifications, will fail the connection if EAP authentication fails.

Note: The startPeriod is equivalent to tx-period on the switchport. Because it is a best practice to set the tx-period to 10 seconds, NAM's startPeriod value must reflect the same value.


Step 8 Click Next.

Step 9 At upper right, select Connection Type, then select the User Connection radio button.

Figure 24 AnyConnect Connection Type Configuration



The dialog box is titled "Network Connection Type". It contains three radio button options:

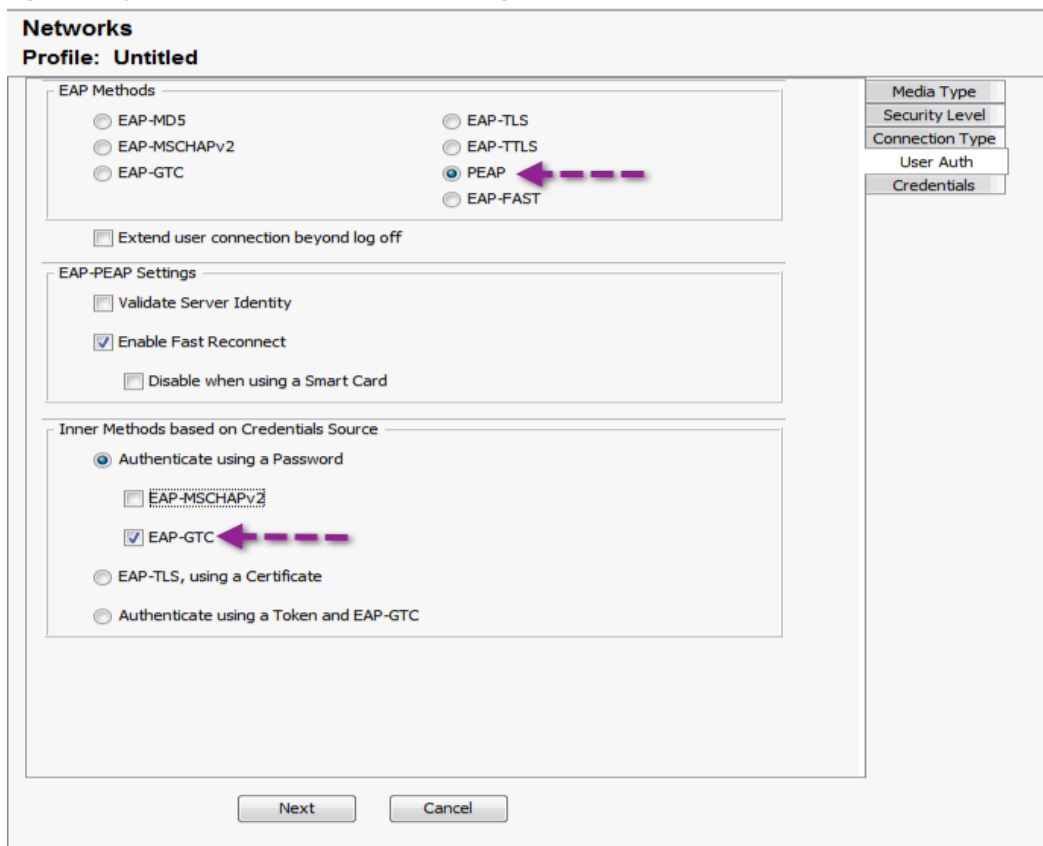
- ☐ Machine Connection
This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access.
- ☒ User Connection 
The user connection should be used when a machine connection is not necessary. A user connection will make the network available after the user has logged on.
- ☐ Machine and User Connection
This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in.

At the bottom are "Next" and "Cancel" buttons. On the right side, there is a vertical stack of tabs: "Media Type", "Security Level", "Connection Type", "User Auth", and "Credentials".



Step 10 At upper right, select User Auth.

Step 11 Set the EAP Methods to PEAP and check EAP-GTC.

Figure 25 AnyConnect NAM User Authentication Configuration



The dialog box is titled "Networks" and "Profile: Untitled". It contains several sections:

- EAP Methods**
 - ☐ EAP-MD5
 - ☐ EAP-MSCHAPv2
 - ☐ EAP-GTC
 - ☒ EAP-TLS
 - ☐ EAP-TTLS
 - ☒ PEAP 
 - ☐ EAP-FAST
- ☐ Extend user connection beyond log off
- EAP-PEAP Settings**
 - ☐ Validate Server Identity
 - ☒ Enable Fast Reconnect
 - ☐ Disable when using a Smart Card
- Inner Methods based on Credentials Source**
 - ☒ Authenticate using a Password
 - ☐ EAP-MSCHAPv2
 - ☒ EAP-GTC 
 - ☐ EAP-TLS, using a Certificate
 - ☐ Authenticate using a Token and EAP-GTC

At the bottom are "Next" and "Cancel" buttons. On the right side, there is a vertical stack of tabs: "Media Type", "Security Level", "Connection Type", "User Auth", and "Credentials".

Step 12 At upper right, select the Credentials tab. Configure Unprotected Identity Pattern as shown in Figure 26.

Note: Single Sign On is selected.

Figure 26 AnyConnect User Credential Configuration

Networks
Profile: Untitled

User Identity

Unprotected Identity Pattern: ←

Protected Identity Pattern:

User Credentials

☒ Use Single Sign On Credentials ←

☐ Prompt for Credentials

- ☐ Remember Forever
- ☒ Remember while User is Logged On
- ☐ Never Remember

☐ Use Static Credentials

Password:

Media Type
Security Level
Connection Type
User Auth
Credentials

Done Cancel

Note: The “Unprotected Identity Pattern” (also known as the outer identity) is the RADIUS username that is sent to Cisco ISE. It is NOT the username that is sent within the EAP tunnel. This outer identity is what is used to match an authentication rule that is defined to match the RADIUS username.


In this step, you’ve appended “@[domain]” to the outer identity, so the resulting identity is anonymous@demo or anonymous@north. This is necessary to designate the domain in which the user belongs. Based on this domain designation, the authentication request can match an authentication rule.

Step 13 Click Done.

Step 14 Select Network Groups. Move the wired-peap connection to the top of the Network Order.

Step 15 From the menu, click File and then Save As to save the configuration with the filename **configuration.xml** in the \ProgramData\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\newConfigFiles directory.

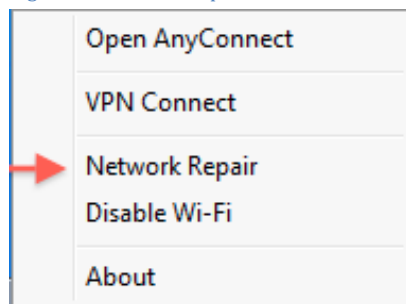
Note: This file name is critical.

Step 16 To apply this new configuration, go to the AnyConnect icon  in the system tray.

Step 17 Right-click to view the options.

Step 18 Select Network Repair. This step forces AnyConnect to restart its services. A service restart causes NAM to search the newConfigFiles directory for a configuration.xml file.

Figure 27 Network Repair



Procedure 2 ISE Configuration

Previously, a simple authentication condition was created to match on usernames that contain the string “demo.” When using EAP-TLS, the username is based on FQDN, which means that all usernames contain “demo” in the string, and only a single condition was configured. When using PEAP-GTC, only the domain name (NetBIOS) is sent (e.g., Demo, North, or South). Thus, additional authentication configuration is necessary.

Step 1 Navigate to Policy → Policy Element → Conditions → Authentications → Simple Conditions.

Step 2 Configure a simple condition to match on the North domain.

Figure 28 Authentication Condition Configuration

Step 3 Click Submit.

Step 4 Navigate to Policy → Authentication.

Step 5 Create a new authentication rule above as follows:

Figure 28 AnyConnect Authentication Rule

Step 6 Click Save.

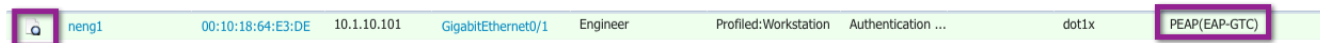
Procedure 3 Test User Authentication

Configuration is done! It's time to verify that user authentication is working correctly.

Step 1 Connect to the network with a Windows or MAC device configured for a PEAP-GTC connection.

Step 2 View Live Log.

Figure 29 Live Log



Step 3 Click the Details button.

Figure 30 AnyConnect User Authentication Log

Authentication Summary	
Logged At:	May 31,2012 6:16:16.043 PM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	<u>neng1</u>
MAC/IP Address:	<u>00:10:18:64:E3:DE</u>
Network Device:	<u>3K-X : 10.1.48.2 : GigabitEthernet0/1</u>
Allowed Protocol:	<u>Default Network Access</u>
Identity Store:	North
Authorization Profiles:	Engineer
SGA Security Group:	
Authentication Protocol : PEAP(EAP-GTC)	
Authentication Details	
Logged At:	May 31,2012 6:16:16.043 PM
Occurred At:	May 31,2012 6:16:16.042 PM
Server:	<u>ise11MR</u>
Authentication Method:	dot1x
EAP Authentication Method :	EAP-GTC
EAP Tunnel Method :	PEAP
Username:	<u>neng1</u>
RADIUS Username :	anonymous@north

Appendix B: References

TrustSec System:

- <http://www.cisco.com/go/trustsec>
- http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

Device Configuration Guides:

Cisco Identity Services Engine User Guides:

http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

For more information about Cisco IOS Software, Cisco IOS XE Software, and Cisco NX-OS Software releases, please refer to following URLs:

- For Cisco Catalyst 2900 series switches:
http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 3000 series switches:
http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 3000-X series switches:
http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 4500 series switches:
http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 6500 series switches:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html
- For Cisco ASR 1000 series routers:
http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html

For Cisco Wireless LAN Controllers: <http://www.cisco.com/en/US/docs/wireless/controller/7.2/configuration/guide/cg.html>