

# Cisco TrustSec How-To Guide: Adding ID Stores and Creating Authentication Policies

For Comments, please email: <u>howtoguides@external.cisco.com</u> 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
What does it mean to be 'TrustSec Certified'?	
Adding Identity Stores and Creating Authentication Policies	5
Overview	5
Understanding EAP Methods and Identity Sources	6
Active Directory Configuration	7
Cisco ISE Configuration and Active Directory Integration	7
LDAP Configuration	
Internal Database/Certificate Authorization Profile (CAP) /RADIUS Token/RADIUS Proxy	13
Identity Source Sequence	13
Adding Identity Source Sequences	14
Creating Authentication Policies	15
Configuring Authentication Policy	15
Appendix A: References	1
Cisco TrustSec System:	21
Device Configuration Guides:	21

# What Is the Cisco TrustSec System?

Cisco TrustSec®, a core component of the Cisco SecureX Architecture<sup>TM</sup>, 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.



# 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 is 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).



# 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.

# Adding Identity Stores and Creating Authentication Policies

# Overview

The Cisco® Identity Services Engine (ISE) provides an internal database for authenticating users and endpoints. Internal databases are typically used to authenticate guest users via web authentication or endpoints through MAC authentication bypass (MAB). However, Cisco ISE can integrate with external identity sources to validate user or endpoint credentials and retrieve security group memberships and other attributes that are associated with the user or device for use in authorization policies. External identity sources are not only used to authenticate and authorize users and endpoints for 802.1x/MAB/web authentication process verifies the validity of endpoint or user's credentials by forwarding it to correct identity sources. Cisco ISE does this by processing RADIUS requests from network access devices (NADs), querying the credentials in an identity database, and forwarding the request to the authorization policy for further processing where different permissions can be assigned. This allows ISE to process different identity requests using different identity databases.

When a NAD sends an authentication request to the Cisco ISE, the request is sent as a RADIUS request (NADs may include VPN concentrators, wireless LAN controllers, and LAN switches). The RADIUS request consists of multiple attributes, including username/password, service type, class attributes, and so on. The authentication policy compares the incoming RADIUS request to the configured authentication conditions, filters out protocols and Extensible Authentication Protocol (EAP) types using filters the protocol allows, selects the assigned identity store, and processes the response sent back by the identity store. Then the authorization (AuthZ) policy takes over.

For instance, when endpoints are authenticating through Protected Extensible Authentication Protocol (PEAP) with Microsoft Challenge Handshake Authentication Protocol Version 2 (PEAP-MSCHAPv2), the ISE authentication policy can direct the request to an Active Directory (AD) identity source using the authentication conditions; however, when ISE receives a MAB request, it can direct the request to internal endpoint database. Another scenario is when VPN requests are forwarded to a one-time password (OTP) server, but WLAN and LAN 802.1X requests are forwarded to AD for authentication.

Note: For ease of reading and distinguishing terminology, we will commonly refer to authentication policies as AuthC policies, and to authorization policies as AuthZ policies.

The ISE graphical user-interface logic separates out the AuthC and AuthZ policies (Figure 3). The AuthC policy dictates what identity store to query based on the incoming authentication request. For example, an authentication request coming from a VPN gateway may be configured to check an OTP server to validate credentials. Meanwhile, using the same ISE installation, an authentication request from a Cisco Wireless LAN Controller (WLC) results in validating the credentials with Active Directory. ISE provides very powerful and flexible authentication policy functionality.

Figure 3 ISE Authentication and Authorization Policy Construct



Before you can configure AuthC policies using external identity sources, you must configure the external identity source that contains your user information in ISE. This How-To Guide provides the basic understanding of EAP methods and demonstrates how to handling identity stores by using Microsoft AD and Lightweight Directory Access Protocol (LDAP).

# Understanding EAP Methods and Identity Sources

Not all identity sources support all EAP methods. When you choose an identity source, be sure to verify that it supports the EAP method you wish to deploy. Conversely, if you have already decided on an identity source to use, be sure to choose an EAP method that is supported by that source. For example, an EAP type that uses MSCHAPv2 as the inner method (such as PEAP-MSCHAPv2) can use Active Directory as a backend database, but cannot use a generic LDAP server. Table 1 shows various identity source platforms and the EAP methods they support.

EAP-Type	Win 7 Native	Vista Native	Win XP Native	AC 3.0	Apple SL (10.6)	Ubuntu	RHL	ACS 5.2	ISE 1.0	AD	LDAP
EAP-TLS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
EAP-TTLS	No	No	No	Yes	Yes	Yes	Yes	No	No	Yes	Yes
PEAP MSCHAPv2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
PEAP EAP-GTC	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PEAP EAP-TLS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
EAP-FAST MSCHAPv2	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
EAP-FAST EAP-GTC	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 1 EAP Types Supported by Major Identity Source Platforms

# Active Directory Configuration

Cisco ISE uses an Active Directory connector so that each Cisco ISE node in a TrustSec deployment joins the AD domain and accesses AD resources just like any other Windows domain member. This scenario allows for tremendous increase in speed, ease of use, and flexibility when using Active Directory with the TrustSec security solution. ISE AD integration supports multiple AD domains provided that there is mutual trust relationship configured among the domains. If you are looking for a way to integrate ISE in an environment where a mutual trust relationship is not possible among the domains, please refer to the TrustSec Multiple Active Directories How-To Guide.

**Cisco Best Practice:** Both time synchronization and Domain Name System (DNS) are critical to a solid integration with Active Directory. Therefore, always use Network Time Protocol (NTP) and always ensure DNS is configured correctly, with reverse-DNS pointers for all Active Directory servers.

### Cisco ISE Configuration and Active Directory Integration

#### Procedure 1 Join the Domain.

Each Cisco ISE node joins the domain separately. The following is a list of ports that must be open between all Cisco ISE nodes and Active Directory:

- SMB (TCP/445)
- KDC (TCP/88)
- Global Catalog (TCP/3268 and 3289)
- KPASS (TCP/464)
- NTP (UDP/123)
- LDAP (TCP and UDP/389)
- LDAPS (TCP/636)

Step 1 In the Cisco ISE GUI select Administration  $\rightarrow$  Identity Management  $\rightarrow$  External Identity Sources  $\rightarrow$  Active Directory

Step 2 Enter the AD Domain Name (in the example, cts.local) and click Save Configuration (Figure 4).

Figure 4 AD External Identity Source: Configuring AD Connector

External Identity Sources	
🔶 🔲 🗐	Connection Advanced Settings Groups Attributes
Certificate Authentication Profile	To configure Active Directory:
2 Active Directory	Eirst enter the required fields: the Domain Name to connect to and the Mentity Store Name to refer to
EDAP (	This enter the required telds, the bolinain name to connect to and the identity store name to refer to the store is the Active Directory configuration to all nodes in the ISE deployment.
RADIUS Token	<ul> <li>After the configuration has been submitted, then Join or Leave operations must be performed.</li> </ul>
RSA SecurID	* Domain Name cts.loca
	* Identity Store Name AD1

Step 3 Click the ISE checkbox and click Join (Figure 5).

* Do	main Name cts.local		]
* Identity	Store Name AD1		]
One or more nodes may be selected for Join or I Connection.	Leave operations. If a n	ode is joined then a leav	e operatio
🚰 Join 😤 Leave 😤 Test Connection 👻			
ISE Node	ISE Node Role	Status	
✓ ISE	STANDALONE	Connected 🗹	

The Join Domain pop-up window appears. Enter a username and password for an AD account that has rights to join a workstation to the domain—for example, **administrator** (Figure 6).

Figure 6 AD Externa	I Identity Source:	Account Information
---------------------	--------------------	---------------------

Join Domain	×
* User Name:	administrator
* Password:	•••••
	OK Cancel

**Note:** The user account used for the preceding operation must have, at a minimum, permission to add and remove computers. **Note:** The credentials used to add the ISE node to the domain are not saved on ISE.

Step 4 Select Administration  $\rightarrow$  Identity Management  $\rightarrow$  External Identity Sources  $\rightarrow$  Active Directory  $\rightarrow$  Groups

Step 5 Select the option Select Groups From Directory (Figure 7).

Figure 7 AD External Identity Source - Groups

Active Directory > AD1			
Active Directory > AD1			
Connection	Advanced Settings	Groups	Attributes
🕂 Add 👻 🗙 De	elete Group	-	
Select Groups Fro	m Directory 🦰		
Add Group	ns		

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

Step 6 Select the groups that you want to use in policy decisions (Figure 8).

Select groups that will be used in your network access policies later. Common groups may include: Domain Computers, Contractors, Employees, Domain Users, and more. You can add and remove groups at any time.

#### Figure 8 AD External Identity Source - Group search

#### Select Directory Groups × This dialog is used to select groups from the Directory. Click Retrieve Groups.. to read directory. Use \* for wildcard search (i.e. admin\*). Search filter applies to group name and not the fully qualified path. Domain: cts.local Filter: Retrieve Groups... Number of Groups Retrieved: 43 (Limit is 100) Name Group Type cts.local/Users/DnsUpdateProxy GLOBAL ✓ cts.local/Users/Domain Admins GLOBAL ✓ cts.local/Users/Domain Computers GLOBAL cts.local/Users/Domain Controllers GLOBAL cts.local/Users/Domain Guests GLOBAL ✓ cts.local/Users/Domain Users GLOBAL ✓ cts.local/Users/Employees GLOBAL Cts.local/Users/Enterprise Admins UNIVERSAL Cts.local/Users/Enterprise Read-only Domain Controllers UNIVERSAL cts.local/Users/Group Policy Creator Owners GLOBAL cts.local/Users/RAS and IAS Servers LOCAL cts.local/Users/Read-only Domain Controllers GLOBAL = cts.local/Users/Schema Admins UNIVERSAL ✓ cts.local/Users/Sponsors GLOBAL ✓ cts.local/Users/Sponsors\_Full GLOBAL ОК Cancel

Step 7 After selecting all necessary groups, click OK (Figure 8).



#### Step 8 Click Save Configuration (Figure 10).

Figure 10 Save Configuration

Save Configuration Delete Configuration

# LDAP Configuration

Cisco ISE supports LDAP v3-compliant LDAP servers for authentication. Although LDAP server is added through the Policy Administration Node (PAN) GUI, each Policy Services Node (PSN) connects directly to the configured LDAP server for the authentication request.

LDAP can also be used during the configuration of AuthZ policies independent of whether endpoint was authenticated via LDAP. In other words you can configure authentication to use the certificate authentication profile (CAP) and do a lookup of endpoint's group membership on the configured LDAP server for further authorization conditions.

For more information on how to configure CAP using LDAP lookup, please refer to TrustSec Multiple Active Directories How-To Guide.

When you set up an LDAP server on the Cisco ISE, you'll notice that there are predefined schema for Microsoft Active Directory, Sun directory server, and Novell eDirectory. For other LDAPv3 compliant servers, you can use the custom option to configure the schema settings. The following section provides an example of configuring the ISE to connect to Microsoft Active Directory server for LDAP authentication.

### Procedure 1 Add a LDAP Server

- Step 1 Navigate to Administration→Identity Management→External Identity Sources→LDAP.
- Step 2 Click Add.
- Step 3 Enter name of the LDAP identity source.
- Step 4 Select Active Directory as the Schema. Click the down-arrow to view the details of the Active Directory Schema (Figure 11).

System	ment Admini	stration V Network Resources 🛛 🍇 Gues	t Management		
entities Groups External Ider	ntity Sources	Identity Source Sequences	Settings		
external Identity Sources	1	LDAP Identity Sources List > LDAP			
<b>≜-≡</b> '≡	. 263	LDAP Identity Source			
Certificate Authentication Profile	• •	General Connection	n Directory Organization	Groups Attribute	s
Active Directory	<u></u>				
	0	100 million 100			
RADIUS Token	۲	* Nar	ne LDAP		
RSA SecurID	()	Descripti	on		
		2.1.			
		<ul> <li>✓ Sche</li> <li>* Subject Objectclass</li> </ul>	ma Active Directory	Group Objectclass	Group
		<ul> <li>Subject Objectclass</li> <li>Subject Name Attribute</li> </ul>	ma Active Directory	Group Objectclass  Group Map Attribute	Group
		Subject Objectclass     Subject Name Attribute     Certificate Attribute	ma Active Directory Person CN userCertificate	Group Objectclass  Group Map Attribute	Group memberOf

Figure 11 LDAP External Identity Source: Schema

- Step 5 Click the Connection tab.
- Step 6 Enter the Hostname/IP (see Figure 12).

- Step 7 Enter the Port number. In the example, this number is 389.
- Step 8 For the Access type, select Authenticated Access.
- Step 9 Enter the Admin DN—in this example, cts\administrator. This is the Distinguished Name for a user who is a member of the Schema Admin Group within Active Directory. For example: cn=SchemaAdmin, cn=Users, dc=demo, dc=local.
- Step 10 Enter the Admin DN's password.

Best Practice: Cisco ISE allows up to two LDAP servers for redundancy. We recommend that you use both servers in case the primary server fails

Best Practice: We recommend that you use SSL by enabling Secure Authentication. The LDAP setting may require different port.

Figure 3 LDAP External Identity Source: Configuration

		-
* Hostname/IP	192.168.1.72	<i>(</i> <b>i</b> )
* Port	389	]
Access	O Anonymous Access	
	<ul> <li>Authenticated Access</li> </ul>	
Admin DN	* cts\administrator	
Password	* •••••	
		_
Secure Authentication	Enable Secure Authentication	
Root CA	server#server#00002	
* Server Timeout	10	() Second
Server Timeout	10	Second
* Max. Admin Connections	20	<i>i</i>
	D	
	Test Bind to Server	

Step 11 Click Test Bind to Server to validate the configuration. You should receive a confirmation as shown in Figure 13.

Figure 4 LDAP External Identity Source: Test Bind Validation

Bind successful to 192.168.	.1.72:389
Result of testing this config Number of Subjects: 14 Number of Groups: 44	uration is as follows:
Response time:43ms	
	ОК

Step 12 Click the Directory Organization tab.

Step 13 Configure the Subject Search Base and the Group Search Base as DC=cts, DC=local (Figure 14).

Best Practice: It is a best practic configuration, the search ba DC=local)	ce to define the search bases as speci ses to use for subject and group searc	ifically as possible th is <b>CN=Users,</b> •	e. For a standard <domain compor<="" th=""><th>Active Directory server nent&gt;. (CN=Users, DC=demo,</th></domain>	Active Directory server nent>. (CN=Users, DC=demo,
Figure 14 LDAP External Identity	Source: Directory Organization			
LDAP Identity Sources List > LDAP				
LDAP Identity Source				
General Conned	tion Directory Organization	Groups	Attributes	
Subject Search Base     Group Search Base     Search for MAC Address     Strip start of subje     Strip end of subje	DC=cts,DC=local DC=cts,DC=local in Format xx-xx-xx-xx-xx-xx ect name up to the last occurrence of ct name from the first occurrence of t	Naming Cont Naming Cont	i exts i	

Step 14 Navigate to the Groups tab.

Step 15 Select Groups  $\rightarrow$  Add  $\rightarrow$  Select Groups From Directory (Figure 15).

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 policy related to AD groups, the administrator needs to look through only a small list instead of every group in AD.

ce.	
ory Organization Gr	oups Attributes
	tory Organization Gr

Note: The groups found are the result of the returned values from a search based on the **memberOf** attribute that you configured back on the general LDAP Identity Source page (Figure 11).

Step 16 Of the groups retrieved, select the specific groups that will be used to define AuthC and AuthZ policies (Figure 16).

#### Figure 16 LDAP External Identity Source: Search Groups

#### Select Directory Groups

This dialog is used to select groups from the Directory. Click Retrieve Groups.. to read directory.

Filte	r: * Retrieve Groups Number of Groups Retrieved: 43 (Limit is 100)	
	Name	
	CN=DHCP Users,CN=Users,DC=cts,DC=local	ń
	CN=Denied RODC Password Replication Group,CN=Users,DC=tocal	
	CN=Distributed COM Users,CN=Builtin,DC=cts,DC=local	
	CN=DnsAdmins,CN=Users,DC=cts,DC=local	_
	CN=DnsUpdateProxy,CN=Users,DC=cts,DC=local	
	CN=Domain Admins,CN=Users,DC=cts,DC=local	
	CN=Domain Computers,CN=Users,DC=cts,DC=local	
	CN=Domain Controllers,CN=Users,DC=cts,DC=local	
	CN=Domain Guests,CN=Users,DC=cts,DC=local	Ē
	CN=Domain Users,CN=Users,DC=tcs,DC=local	
	CN=Engineering,CN=Users,DC=cts,DC=local	
	CN=Enterprise Admins,CN=Users,DC=cts,DC=local	
	CN=Enterprise Read-only Domain Controllers, CN=Users, DC=tcs, DC=local	
	CN=Event Log Readers,CN=Builtin,DC=cts,DC=local	
	CN=Finance,CN=Users,DC=cts,DC=local	× ×
	CN=Group Policy Creator Owners, CN=Users, DC=tcs, DC=local	Ŧ
	OK	ancel

Step 17 Click Save.

# Internal Database/Certificate Authorization Profile (CAP) /RADIUS Token/RADIUS Proxy

In addition to AD and LDAP, Cisco ISE also supports internal database, certificate, RADIUS token servers for OTP, and native integration for RSA SecurID token servers for authentication. ISE provides three types of internal databases: users, endpoints, and guest. The user and guest identity database are typically used for authenticating endpoints when 802.1x or web authentication is used for authentication. The endpoint identity database is used for categorization of endpoints from automated profiling, device registration, and also from manually created white lists or black lists of MAC addresses. Endpoint identity sources can be used to simply MAB endpoints or they can be combined with other conditions during authorizations for corporate BYOD policies.

Note: The guest identity database is visible only when you log into the sponsor portal page.

A certificate authentication profile (CAP) can be used to authenticate endpoints identifying themselves using digital certificates. This is used in an environment where mutual authentication using digital certificates is required. You can select which X.509 field, such as the subject of the CN= field, or the email address of the SAN, will be used for endpoint identity.

For integration with one-time password (OTP) servers, Cisco ISE supports RADIUS token servers and native SecurID integration. RADIUS token servers are used when the OTP server is running RADIUS natively and ISE forwards the RADIUS request to the OTP RADIUS server. SecurID is used where Cisco ISE terminates the RADIUS locally and forwards the OTP request to the SecurID server via the Secure Device Provisioning (SDP) feature.

Configuration of CAP and OTP is beyond the scope of this document. For more information, please refer to the ISE 1.1 User Guide document.

## **Identity Source Sequence**

Identity sequences are used in ISE to provide a single "object" that is actually a sequence of identity stores that only ISE queries when validating credentials. This is useful when there are multiple identity databases and when it is not possible to identify which identity source the user is member of during authentication request processing. In our configuration example, we create an identity sequence that queries the following identity stores in order: Active Directory  $\rightarrow$  Internal Users.

**Best Practice:** Avoid using identity source sequences if possible. Instead, use an authentication condition to forward the authentication request to the correct identity source.

×

## Procedure 1 Create an Identity Sequence

Step 1 Navigate to Administration→Identity Management→Identity Source Sequences.

Step 2 There are two identity source sequences by default (Figure 17).

Figure 17 Adding Identity Source Sequence

Identity Source Sequence					
🖊 Edit 🕂 Add 🕞 Duplicate 🗙 Delete					
Name	Description	Identity Stores			
Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Internal Users			
Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal	Internal Users			

Step 3 Click Add.

Step 4 Name the identity sequence All\_ID\_Stores. Select the identity stores AD1 from left pane and add it to the right pane. Then select and add Internal Users (Figure 18).

* Name	All_ID_Stores			
escription				
Cortificato I	acad Authontication			
Cer unicate i	ased Authentication			
Authentica				
. Generation	tion Search List			
A	tion Search List	at will be accessed in sequ	ence until first authentication	succeeds
Available	tion Search List	at will be accessed in sequ	ence until first authentication s	succeeds
Available	tion Search List	at will be accessed in seques	ence until first authentication s	succeeds
A Available Internal Er LDAP	tion Search List	at will be accessed in sequestion Selection AD1	ence until first authentication s led lal Users	succeeds
A Available Internal Er LDAP	tion Search List	at will be accessed in sequence of the sequence of the second sec	ence until first authentication s ied nal Users	succeeds
A Available Internal Er LDAP	tion Search List	at will be accessed in sequence of the sequence of the second sec	ence until first authentication : ed nal Users	succeeds
A Available Internal Er LDAP	tion Search List	at will be accessed in sequestion of the sequence of the second s	ence until first authentication : ied ial Users	succeeds

Step 5 Scroll to the bottom of the window and click Submit.

## **Creating Authentication Policies**

In our configuration example, we will create an authentication policy that does the following:

- Forward any MAB request to internal endpoint database
- Forward wired and wireless 802.1x requests to AD
- Forward any unknown request to All\_ID\_Store sequence we configured in previous section

**Configuring Authentication Policy** 

#### **Procedure 1** Examine the Default ISE Authentication Policy

Step 1 Navigate to Policy  $\rightarrow$  Authentication.

There are two preconfigured rules in the authentication policy, as well as a default rule. The Policy Rule table behaves like an access list: it is processed from the top down, and the first match is the rule that is used.

**Note:** There is Policy Type option at the top of the page where you can select either simple or rule-based. When Simple option is used, all authentication requests can be forwarded only to single identity source or identity source sequence. For most deployments, it is recommended to use the rule-based option for efficient routing of the authentication request to the proper identity sources.

The way an authentication request is matched to a rule-line is based on the conditions. To explain this further, we will examine the first preconfigured rule, named MAB. This is a rule for MAC authentication bypass from switches.

Cisco ISE policy constructs are built in a logical IF-THEN format. Notice the IF just before the "picker" that says Wired\_MAB. This particular line is stating: "If RADIUS request is Wired\_MAB, then allow the Default Network Protocols to be used."

IF Wired\_MAB THEN Allow the default protocols ELSE Move to next Line in Authentication Policy Table

Figure 7 Authentication Policies

CISCO Identity Services Engine				
🛕 Home Operations 🔻 Policy 🔻	Administration 🔻			
Authentication O Authorization	Refiling Posture	Client Provisioning	Security Group Access	Policy Elements

#### Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication. Policy Type O Simple Rule-Based

	МАВ	: If Wired_MAB < allow protocols Allowed Protocol : Default Networs and	
-	Dot1X	: If Wired_802.1X Wired_802.1X Wired_802.1X	
	Default Rule (If no match)	: allow protocols Allowed Protocol : Default Networ and use identity source : Internal Users	

Step 2 In Figure 19, notice the "and ..." after the Allowed Protocol boxes. Next to the word "and..." is a black drop-down triangle (circled in Figure 19)

Step 3 Click the triangle.

The result is shown in Figure 20. Each rule in the Authentication Policy table has a second part to it. This is the line where the credential store is chosen. By default, this preconfigured rule for MAC authentication bypass is configured to use the Internal Endpoints data store. The Internal Endpoints data store is the database of known devices internal to ISE. This database can be populated manually or dynamically.

Figure 20	Authentication	Policies:	MAB
-----------	----------------	-----------	-----

Rule	e Based	d				-	
	<b>-</b>	MAB	: If Wired_MAB	allow protocols	Allowed Protocol : Default Networ	and .	🙀 Actions 🗸
		▼ Default	: use Internal Endpoir	nts 🔶		_	🍄 Actions 🗸

Note: An example of manual population: The admin exports a list of known Cisco Unified IP Phone MAC addresses from the Cisco Unified Communications Manager interface, and imports that list into ISE.

An example of dynamic population: ISE profiling discovered this device via one or more of the profiling probes, and created the device entry in the Internal Endpoints data store.

So, the IF-THEN statement looks like this:

```
IF Wired_MAB
THEN Allow the default protocols
AND Check Credentials with the Internal Endpoints Data Store
ELSE
Move to next Line in Authentication Policy Table
```

Note: The Wired\_MAB is a prebuilt condition to match RADIUS attributes service-type = call-check, and nas-port-type = ethernet.

### Procedure 2 Enable Wireless Authentication

Step 1 Navigate to Policy  $\rightarrow$  Authentication.

Step 2 Expand the IF conditions for the Dot1X rule and choose to Add Condition from Library (Figure 21).

Figure 8 Authentication Policies: Adding WLAN Condition 1

		to an an an a	De la		
Authentication	orization 🔀 Profiling 🕑 Posture	Dient Provisioning	Security Group Access	Policy Elements	
entication Policy					
the Authentication Policy by s	electing the protocols that ISE should use to	communicate with the network	devices, and the identity source	s that it should use for authentication.	
Type () Simple (•) Rule	-Based				
MAB	: If Wired MAB	allow protocols Allow	ved Protocol : Default Networ	and	
		-			
Dot1X	: If Wired_802.1X O	aliow protocols Allow	ved Protocol : Default Networ	and	
🛛 👻 Dot1X	: If Wired_802.1X O	allow protocols Allow	ved Protocol : Default Networ	] and	
Dot1X     Default Rule (If no r	: If Wired_802.1X O match) : all 💾 Add All Conditi	allow protocols Allow	ved Protocol : Default Networ	] and •	
	If Wired_802.1X O match) : all Add All Condition Nar	allow protocols Allow ons Below to Library me Expression	ved Protocoi : Default Networ	and	
Dot1X  Default Rule (If no r	If Wired_802.1X O match) : all Add All Condition Nai Wired_802.1X	allow protocols Allow ons Below to Library me Expression	ved Protocoi : Default Networ	] and ,	
Dot1X     Default Rule (If no r	i If Wired_802.1X O match) : all Add All Condition Nar Wired_802.1X	allow protocols Allow     ons Below to Library     me Expression	ved Protocol : Default Networ	or e.	Add Attribute/Value

Step 3 From the Select Condition drop-down menu, select: Compound Condition  $\rightarrow$  Wireless\_802.1X (Figure 22).

Figure 9 Authentication Policies: Adding WLAN Condition 2

CISCO Identity Services Engine						
🛕 Home Operations 🔻 Policy 🔻 Administra	ation 🔻					
Authentication 🖉 Authorization 🥂 Prof	iling 🕜 Posture 🔂 Client Provisioning	Security Group Access	nents			
Authentication Policy						
Define the Authentication Policy by selecting the protocols to Policy Type O Simple   Rule-Based	hat ISE should use to communicate with the network	devices, and the identity sources that it should u	use for authentication.			
MAB : If	Wired_MAB 🗇 allow protocols Allow	ed Protocol : Default Networ and				
Dot1X : If	Wired_802.1X O  allow protocols Allow	ed Protocol : Default Networ and				
Default Rule (If no match) : all	Add All Conditions Below to Library					
	Condition Name Expression		OR 🔻			
	Wired_802.1X 📀		OR 🚔₊			
	Select Condition		- ∰.+			
	Compound Condition					
	<b>↔</b> • ■ 1					
	Wired_MAB					
	Wired_802.1X					
	Wireless_802.1X					
	Switch_Local_Web_A	uthentication				
	WLC_Web_Authentica	ation				

Step 4 Ensure that the operator is specified as OR, not AND (Figure 23).

Figure 23 Authentication Policies: Adding WLAN Condition 3

Wired_802.1X O  allo	w protocols Allowed Protocol : Default Networ and		
Add All Conditions Below to	Library		
Condition Name	Expression	OR 👻	
Wired_802.1X 📀		OR	÷
Wireless_802.1X 📀	A condition to match an 802.1X based authentication reques		<b>₩</b> -

Step 5 Save the settings.

So, the IF-THEN statement for Dot1X rule looks like this:

IF Wired_802.1X or Wireless_802.1X			
THEN Allow the default protocols			
AND Check Credentials with the Internal	Users	Data	Store
ELSE			
Move to <b>next</b> Line in Authentication Policy	Table		

Note: Wired\_802.1X is a prebuilt condition to match the following RADIUS attributes: service-type = Framed, and nas-port-type = Ethernet. In contrast, Wireless\_802.1X is a prebuilt condition to match these RADIUS attributes: service-type = call-check, and nas-port-type = Wireless – IEEE 802.11.

### Procedure 3 Change the identity stores.

With the preconfigured rules, MAB will use the Internal Endpoints store to look for the MAC addresses of known devices. If the incoming authentication request is an 802.1X authentication, ISE will use the Internal Users data store to check for username and password validity.

If the authentication is of another type (for example, WebAuth), it will not match either of the preconfigured rules and it will end up with the Default Rule. The default rule is preconfigured to check the Internal Users data store.

Most organizations will not want to use the default, local data stores for user accounts. The vast majority of organizations use Active Directory as their main source of user identity data. Therefore, we will change the default rule to use All\_ID\_Store and the Dot1X Rules to use Active Directory only.

Step 1 In the Default Rule, click the plus sign next to Internal Users.

This opens the Identity Source picker.

Step 2 Select the All\_ID\_Stores identity source sequence that we built earlier (Figure 24).

Figure 10 Authentication Policies: Modifying Default Rule 1



Step 3 Click the minus sign to close the Identity Source picker (Figure 25).

Figure 11 Authentication Policies: Modifying Default Rule 2

Allowed Protocol : Default Networ	All_ID_Stores
	Identity Source All_ID_Stores
	Options
	If authentication failed Reject
	If user not found Reject 💌
	If process failed Drop 🔹
	Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS MSCHAP it is not possible to continue processing when authentication fails or user is not found. If continue option is selected in these cases, requests will be rejected.

Step 4 Make note of the options below the Identity source.

The actions for each option are: Reject, Drop, or Continue. These three options and their respective choices are available with every authentication policy rule, including the default rule. Table 2 describes the three options. Table 3 describes their configurable actions.

Table 2	Authentication	Options
---------	----------------	---------

Option	Description
Authentication Failed	Received explicit response that authentication has failed such as bad credentials, disabled user, and so on. The default course of action is reject.
User not found	No such user was found in any of the identity databases. The default course of action is reject.
Process failed	Unable to access the identity database or databases. The default course of action is drop.

#### **Table 3 Authentication Actions**

Action	Description
Reject	Sends a RADIUS ACCESS-REJECT response to the NAD.
Drop	Drops the ACCESS-REQUEST, without sending a response.

Continue	Proceed to the authorization policy.
----------	--------------------------------------

Step 5 Expand the Dot1X line, and repeat Steps 1 and 2 to change the identity source to be AD1 (Figure 26).

Figure 26 Authentication Policies: 802.1X Rule 💧 Home Operations 🔻 Policy 🔻 💄 Authentication Client Provisioning 🤶 Security Group Access Authorization 🦂 Profiling Policy Elements Posture **Authentication Policy** Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication. Policy Type O Simple 

Rule-Based : If Wired\_MAB Allowed Protocol : Default Networ
 and...
 Allowed Protocol : Default Networ
 and...
 🛛 👻 т МАВ Dot1X : If Wired\_802.1X. ~ Default : use AD1 Identity Source AD1 Options **Identity Source List** If authentication failed Reject Default Rule (If no match) : allow proto ρ ~ If user not found Reject **∲-** 🗐 🗄 If process failed Drop Internal Endpoints Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS MS Internal Users it is not possible to continue processing when authentication fails or LDAP If continue option is selected in these cases, requests will be rejecte AD1 Guest\_Portal\_Sequence Sponsor\_Portal\_Sequence All\_ID\_Stores CAP DenyAccess

Step 6 Click Save.

The authentication rule should look like that shown in Figure 27.

Figure 12 Final Authentication Policy

🏠 Home Operations 🔻 Policy 🔻	Administration 🔻			
Authentication 🧔 Authorization	Refiling 💽 Posture	Client Provisioning	Security Group Access	8 Policy Elements
Authentication Policy				
Define the Authentication Policy by selecting the Policy Type O Simple   Rule-Based	ne protocols that ISE should use to c	ommunicate with the network	k devices, and the identity source	es that it should use for authentication.
MAB	: If Wired_MAB	් allow protocols Allow	wed Protocol : Default Networ	and 🖕
Default	: use Internal Endp	points 🔶		
Dot1X	: If Wired_802.1X	allow protocols Allow	wed Protocol : Default Networ	and 🗸
Default	: use AD1 🕀	•		
Default Rule (If no match)	: allow protocols Allowed I	Protocol : Default Networ	and use identity source : Al	I_ID_Stores 🔶

So, the IF-THEN statement for the ISE authentication policy rule looks like this:

IF Wired_MAB	
THEN Allow the default protocols	
AND Check Credentials with the Internal Endpoints Data Store	
ELSE IF Wired_802.1X or Wireless_802.1X	
THEN Allow the default protocols	
AND Check Credentials with the AD1 Data Store	
ELSE IF No Match	
THEN Allow the default protocols	
AND Check Credentials with the All_ID_Stores Data Store	

**Note:** You can customize authentication rule extensively. In these examples, we have used the default network access as our allowed protocols. This allows the vast majority of authentication types, but using the defaults does not restrict access to a certain type of EAP method.

To configure a customized set of authentication protocols (such as EAP-TLS only), go to Policy → Policy Elements → Results → Authentication → Allowed Protocols.

# Cisco TrustSec System:

- <u>http://www.cisco.com/go/trustsec</u>
- 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: <u>http://www.cisco.com/en/US/products/ps7077/products installation and configuration guides list.html</u>
- 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: <u>http://www.cisco.com/en/US/products/hw/switches/ps4324/products\_installation\_and\_configuration\_guides\_list.ht</u> <u>ml</u>
- 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