ISE Primer

www.INE.com

Course Overview

- Designed to give CCIE Security candidates an intro to ISE and some of it's features.
- Not intended to be a complete ISE course.
  - –Some topics are not discussed.
- Provides Basic overview of core functions.

Instructor Introduction

- Brandon Carroll
  - –CCIE #23837 (Security)
    - 2008
  - –CCNP/CCNP Security/ CCSI/CCSP for many years
  - –Developer / Author / Instructor / Geek

Introduction to the Cisco ISE and TrustSec

www.INE.com

TrustSec Solution Overview

- TrustSec helps secure networks by enforcing identity-based access policies.
- Provides the following:
  - –Who?
  - –What?
  - –Where?
  - –How?

The Elements

- Authentication
  - 802.1x
  - MAB
  - Web
- Authorization
  - VLAN
  - DACL
  - SGT
- Enforcement
  - SGACL
  - Identity Firewall

Guest Access
- Allows Guests on the network

Profiler
- Allow or Deny iPhones and iPads

Posture
- Ensure that endpoints meet certain requirements

MACSec Encryption
- Data Integrity and Confidentiality

Security Group Access
- Authorize users and devices

History Lesson

- We used to have two primary models
  - –NAC Appliances (or even back to Cisco NAC with ACS)
    - Policy Enforcement
    - Guest Services
    - Profiling
    - Multiple Servers
  - –802.1x Infrastructure
    - ACS or more recently ISE

Authentication

- Flexible Methods
  - –802.1x
    - IEEE Standard port-based network access control encapsulating EAP over LAN
  - –Web
  - –MAB

Authorization

- ACLs
- VLANs
- Security Group Access (SGA)
  - User info captured at ingress and each packet is tagged with this info. SGACLs applied at egress and read the SGtags to apply policy.

Guest Access

- Allow Guests to access predetermined resources through wired network access as well as wireless network access.
- Can provide a browser based method of access control.

Device Profiling

- Dynamically identified endpoint devices
- Manage devices based on predefined policies
- Can be used to inventory any IP-based device on the network.

Security Enforcement

- Assess the endpoint
- Provide a means of remediation if necessary
- Provides built-in policies for over 350 security applications
  - Antivirus
  - Management Software

Switch-Port Level Encryption

- Based on 802.1AE
  - MACSec
  - 128-bit AES Encryption
  - Prevents a number of attacks
    - MITM
    - Snooping
  - Endpoint to Access Switch
  - Switch-to-Switch

Solution Components

- Wireless
  - WLC
  - RA-VPN
  - S2S-VPN
  - ISE
- Campus
  - Cat 3K(-X)
  - Cat 4K
  - ISE

- DC
  - Nexus 7K
  - Cat 6500
  - ASR
  - ASA
  - ISE

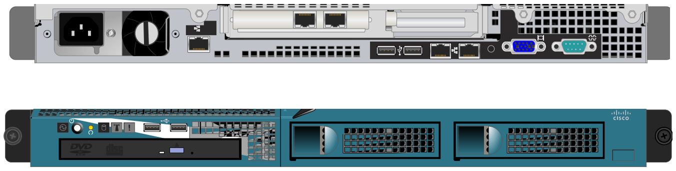
Introduction to ISE

- AAA Server
- Guest life cycle management
- Device Profiling
- Endpoint Posture
- SGA Services
- Monitoring and Troubleshooting
- Hardware or VM

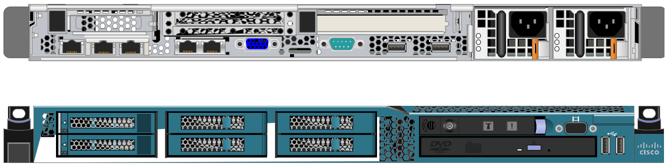
ISE and CCIE v4.0

- Cisco Identity Services Engine Configuration and initialization
- ISE auth result handling
- ISE Profiling Configuration (Probes)
- ISE Guest Services
- ISE Posture Assessment
- ISE Client Provisioning (CPP)
- ISE Configuring AD Integration/Identity Sources
- ISE support for 802.1x
- ISE MAB support
- ISE Web Auth support
- ISE definition and support for VSAs
- Support for MAB in Cisco IOS
- Support for Web Auth in Cisco IOS

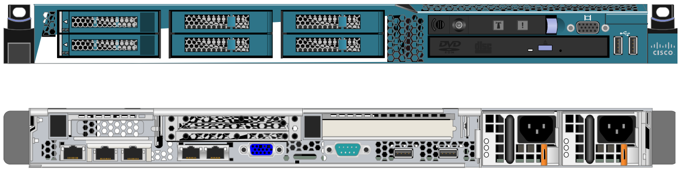
Visual Representations



ISE 3315



ISE 3395



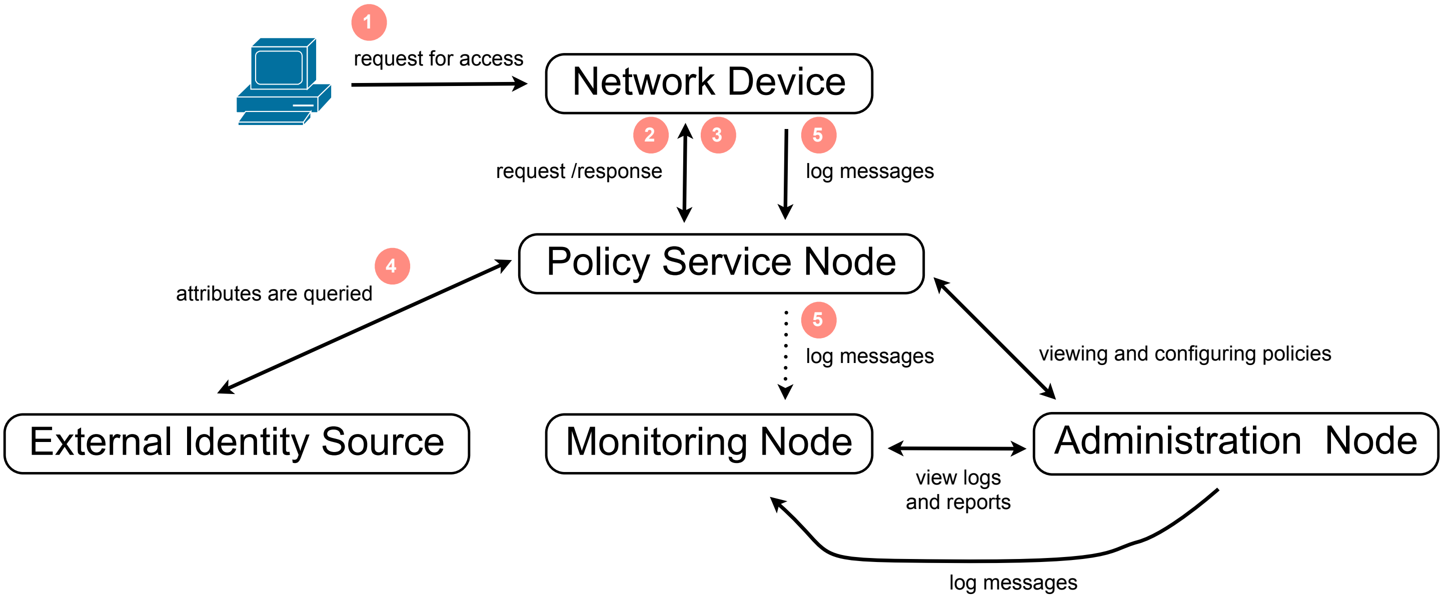
ISE 3355

ISE icons

ISE Software Engines

- Several Software Engines That Interact With One Another
  - External Identity Source
    - Retrieves Policies or Policy Information about a user or a device
  - Administration Node
    - User Interface and Licensing Control
  - Policy Server Node
    - Makes the decisions
  - Network Device
    - Queries the Policy Server Node and enforces what it says
  - Monitoring Node
    - Logging and Reporting Data

Node Interaction



Deploying ISE

Cisco ISE Software Installation

- Pre-installed on HW
- Must be fresh install when using VM
- Process includes
  - –Boot from ISO image
  - –install the OS and ISE application
  - –install process pauses for you to complete the setup dialogue
- CLI Credentials= admin/(defined during setup)

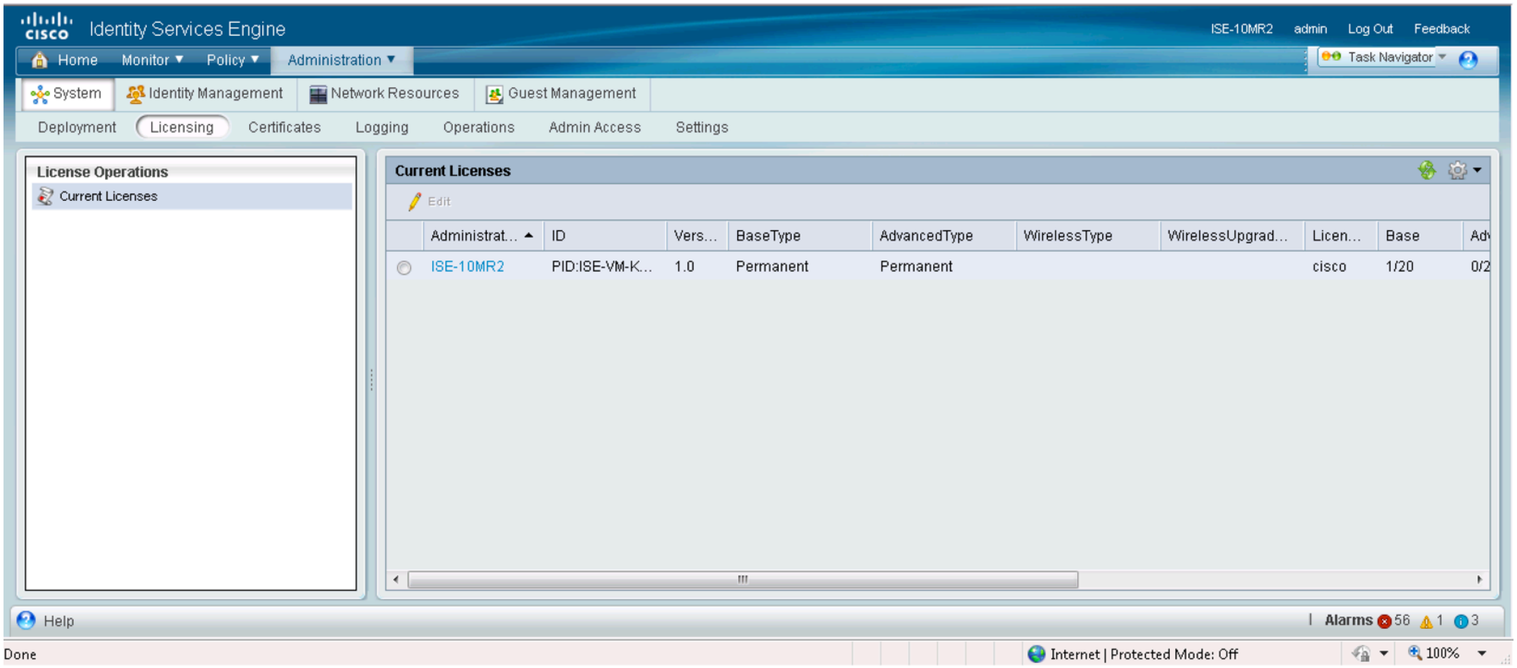
CLI access

- Username “admin”
- Password defined during setup
- Feels like Cisco CLI
  - –show run
  - –show version
  - –show inventory
  - –show interface
  - –show application status ise

GUI Access

- Default Credentials:
  - admin/cisco
- Can be controlled via CLI
- Requires Flash
- Certificates are verified
- Initial Tasks might include
  - CA Configuration, Licensing, Adding Network Devices, Admin User Configuration and NTP/Name-Server

ISE Licensing



	Administrat... ▲	ID	Vers...	BaseType	AdvancedType	WirelessType	WirelessUpgrad...	Licen...	Base	Adv
○	ISE-10MR2	PID:ISE-VM-K...	1.0	Permanent	Permanent			cisco	1/20	0/2

Network Devices

- NADs are AAA Clients
- If not listed in ISE an AAA Client is not able to use the services of ISE
  - devices require a shared secret verified based on IP.
  - if none is defined ISE uses default network device
- NDG's let you group devices based on location and type

CA Certificates

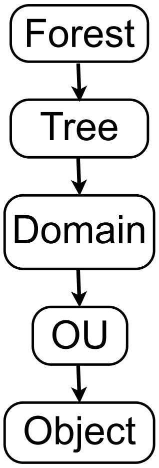
- Local Certificates
  - Identify the ISE to EAP supplicants, external policy servers, and management clients.
- CA Server Certificates
  - Used to verify remote clients to the ISE.

ISE and Active Directory

www.INE.com

ISE and AD Integration

- AD includes the following layers:
  - Object
    - user, client pc, server, printer, other devices
  - Organizational Unit
    - Logical grouping of objects in the domain
    - could be a collection of users
  - Domain
    - Grouping of objects sharing the same domain
  - Tree
    - One of more domains
  - Forest
    - Top Level of AD



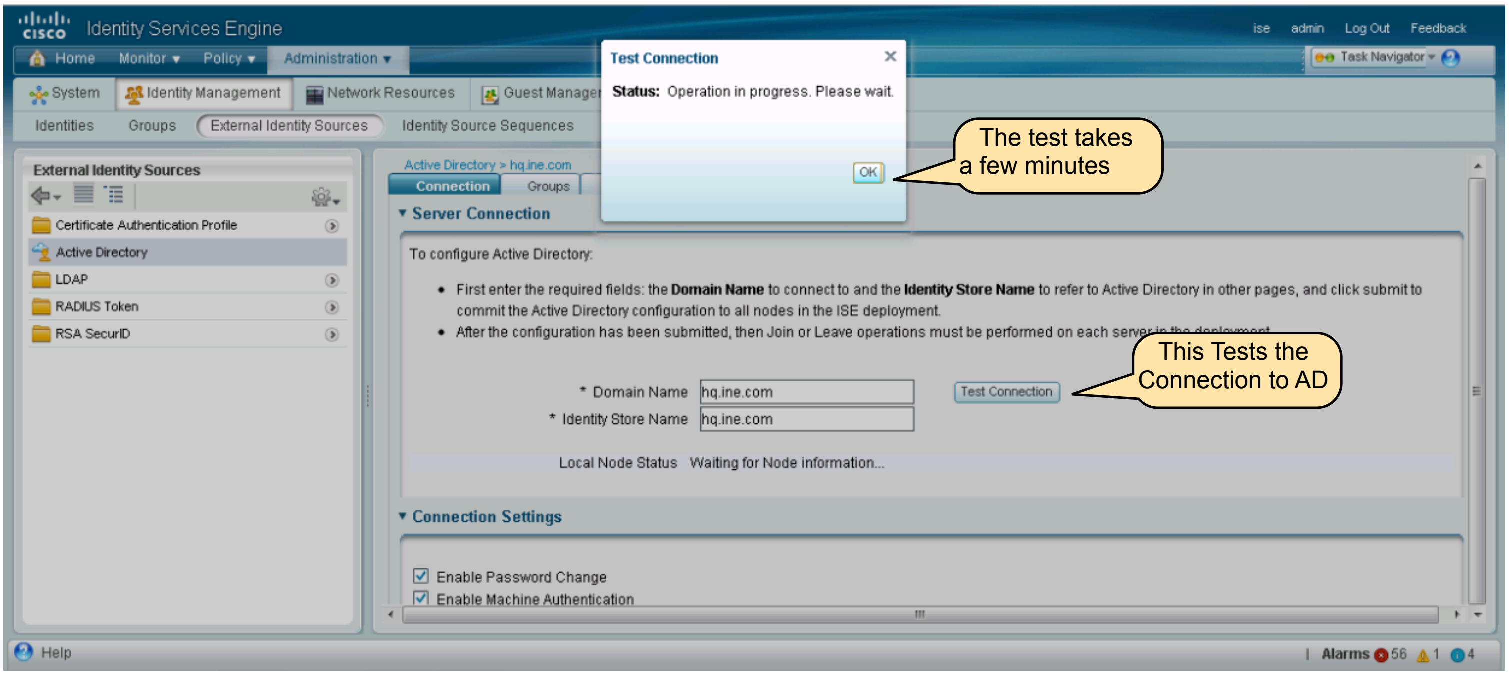
ISE and AD (cont)

- Time Sync must be within 5 minutes
- If there is a firewall in the path specific ports need opened
  - LDAP (UDP/TCP 389)
  - LDAPS (TCP 636)
  - SMB (TCP 445)
  - KDC (TCP 88)
  - Global Catalog (TCP 3268 & 3289)
  - KPASS (TCP 464)
  - NTP (UDP 123)

ISE and AD

- A Username in AD should be predefined for ISE
- The ISE User Role must be “super admin” or “system admin”
- AD can not reside behind a NAT device
- Once you join the AD Domain you can use ISE to configure and retrieve AD Groups.
  - These groups can be used for authorization policy conditions

Verifying ISE Operation with Active Directory


Identity Services Engine
ise admin Log Out Feedback
Home Monitor ▾ Policy ▾ Administration ▾
Task Navigator ▾
System Identity Management Network Resources Guest Manager
Identities Groups External Identity Sources Identity Source Sequences
External Identity Sources
Certificate Authentication Profile
Active Directory
LDAP
RADIUS Token
RSA SecurID
Active Directory > hq.ine.com
Connection Groups
OK
Test Connection
Help
Alarms 56 1 4

Test Connection

Status: Operation in progress. Please wait.

▾ Server Connection

To configure Active Directory:

- First enter the required fields: the **Domain Name** to connect to and the **Identity Store Name** to refer to Active Directory in other pages, and click submit to commit the Active Directory configuration to all nodes in the ISE deployment.
- After the configuration has been submitted, then Join or Leave operations must be performed on each server in the deployment.

* Domain Name hq.ine.com

* Identity Store Name hq.ine.com

Local Node Status Waiting for Node information...

▾ Connection Settings

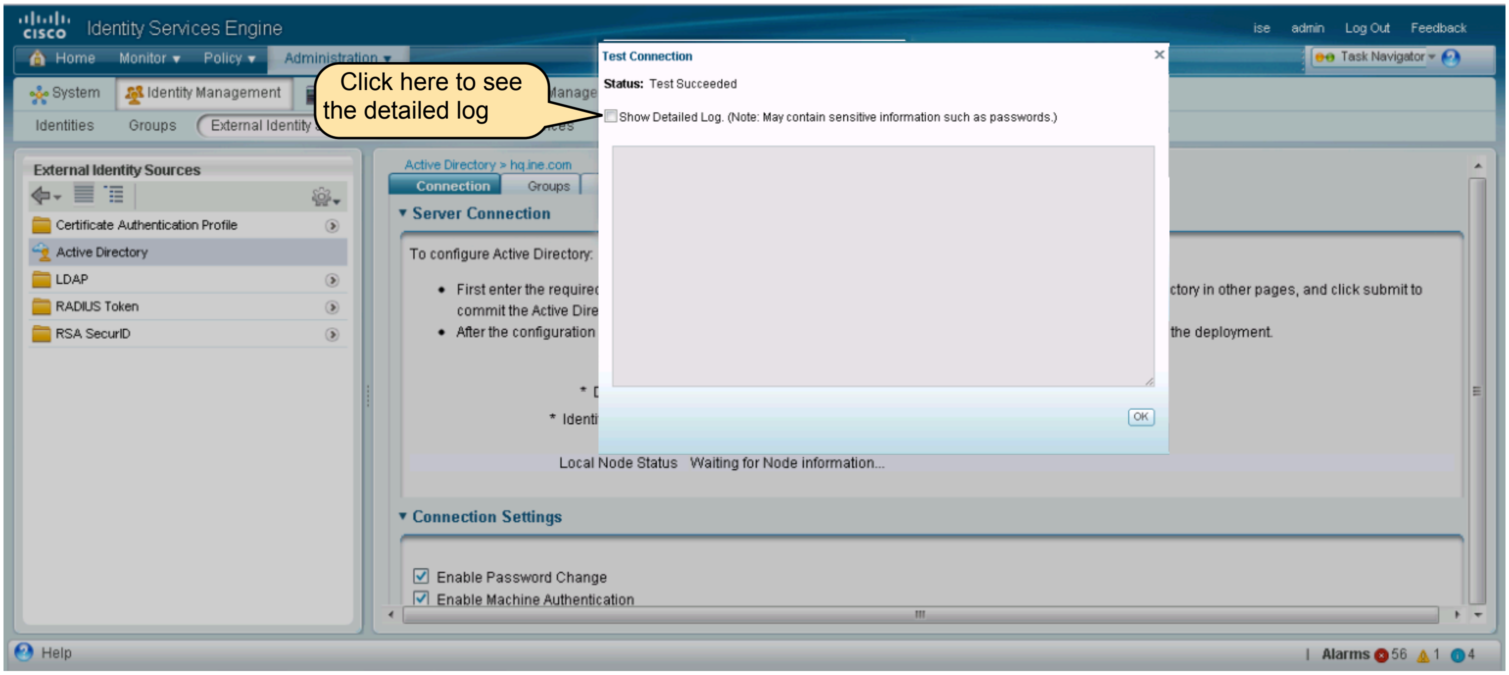
☑ Enable Password Change

☑ Enable Machine Authentication

The test takes a few minutes

This Tests the Connection to AD

Verifying ISE Operation with Active Directory


Identity Services Engine
ise admin Log Out Feedback
Home Monitor ▾ Policy ▾ Administration ▾
Task Navigator ▾
System Identity Management Manage
Identities Groups External Identity
External Identity Sources
Certificate Authentication Profile
Active Directory
LDAP
RADIUS Token
RSA SecurID
Active Directory > hq.ine.com
Connection Groups
Help
Alarms 56 1 4

Click here to see the detailed log

Test Connection

Status: Test Succeeded

☐ Show Detailed Log. (Note: May contain sensitive information such as passwords.)

OK

▾ Server Connection

To configure Active Directory:

- First enter the required … ctory in other pages, and click submit to commit the Active Dire…
- After the configuration … the deployment.

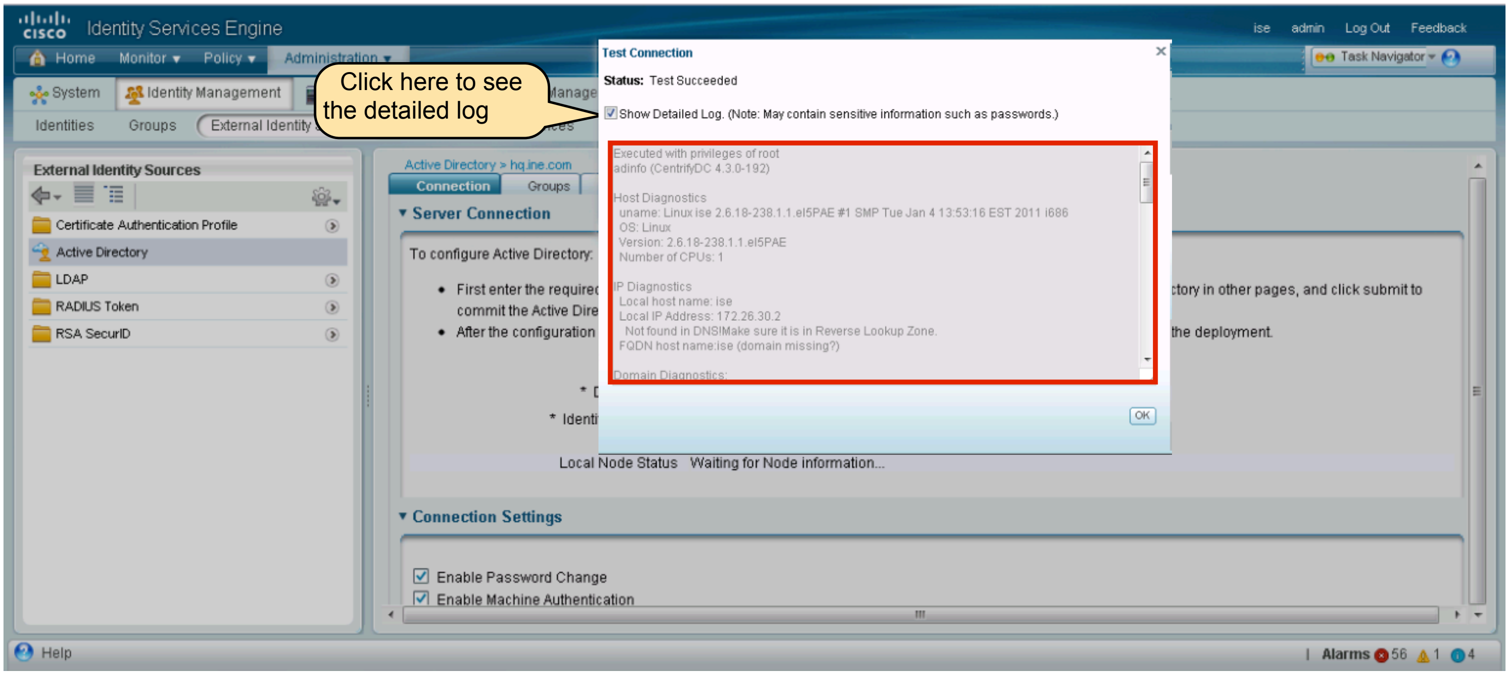
Local Node Status Waiting for Node information...

▾ Connection Settings

☑ Enable Password Change

☑ Enable Machine Authentication

Verifying ISE Operation with Active Directory


Identity Services Engine
ise admin Log Out Feedback
Home Monitor ▾ Policy ▾ Administration ▾
Task Navigator ▾
System Identity Management
Identities Groups External Identity
External Identity Sources
Certificate Authentication Profile
Active Directory
LDAP
RADIUS Token
RSA SecurID
Active Directory > hq.ine.com
Connection Groups
Server Connection
Connection Settings
OK
Help
Alarms 56 1 4

Click here to see the detailed log

Test Connection

Status: Test Succeeded

☑ Show Detailed Log. (Note: May contain sensitive information such as passwords.)

```
Executed with privileges of root
adinfo (CentrifyDC 4.3.0-192)

Host Diagnostics
  uname: Linux ise 2.6.18-238.1.1.el5PAE #1 SMP Tue Jan 4 13:53:16 EST 2011 i686
  OS: Linux
  Version: 2.6.18-238.1.1.el5PAE
  Number of CPUs: 1

IP Diagnostics
  Local host name: ise
  Local IP Address: 172.26.30.2
    Not found in DNS!Make sure it is in Reverse Lookup Zone.
  FQDN host name:ise (domain missing?)

Domain Diagnostics:
```

To configure Active Directory:

- First enter the required … ctory in other pages, and click submit to commit the Active Dire…
- After the configuration … the deployment.

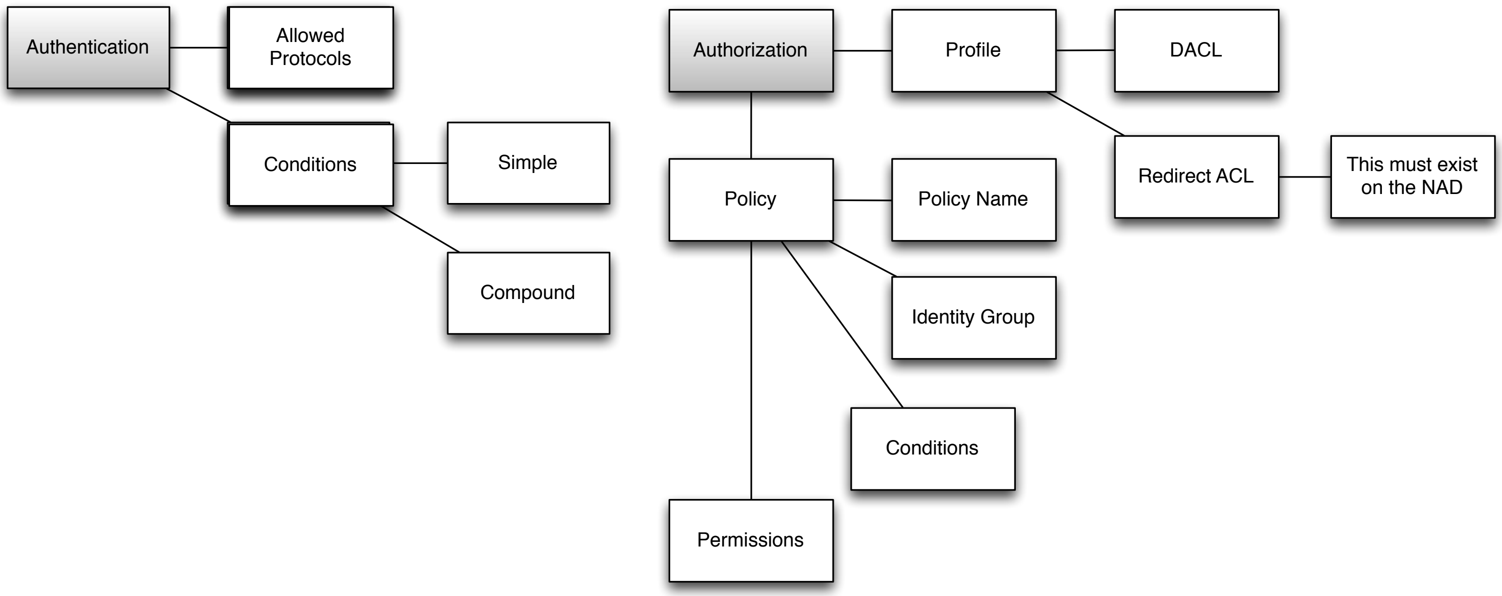
Local Node Status   Waiting for Node information...

☑ Enable Password Change

☑ Enable Machine Authentication

Classification and Policy Enforcement

Using ISE for Policy Enforcement



Authentication

Allowed Protocols

- These are the protocols that ISE should use when communicating with network devices
    - PAP
    - PEAP
    - MS-CHAPv2
    - EAP-MD5
    - EAP-TLS
    - EAP-FAST
    - PEAP-TLS

Conditions

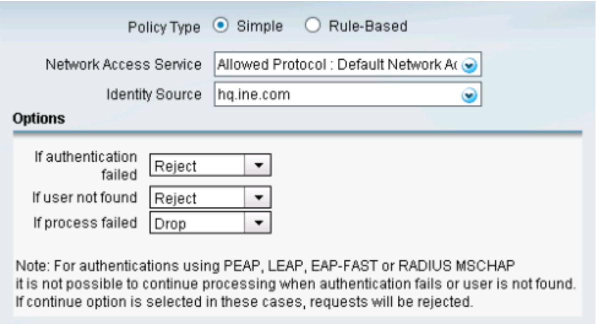
- Attributes are compared to their values.
- Authentication policies can define what the value should or should not be.
- Based on evaluation, the authentication attempt may be performed or not.

Authentication (cont)

- Authentication consists of a network access service and an identity source.
  - –Network Access Service is either an allowed protocol service or a proxy service that will proxy to an external RADIUS Server.
  - –The Identity Source defines where ISE should look when verifying credentials provided by a user or machine.

Policy Enforcement with Simple Policy

- Statically define the allowed protocols and the identity source or identity source sequence
- No conditions are defined
  - –It is assumed all conditions have been met



Policy Type ● Simple ○ Rule-Based

Network Access Service: Allowed Protocol : Default Network Ac

Identity Source: hq.ine.com

Options

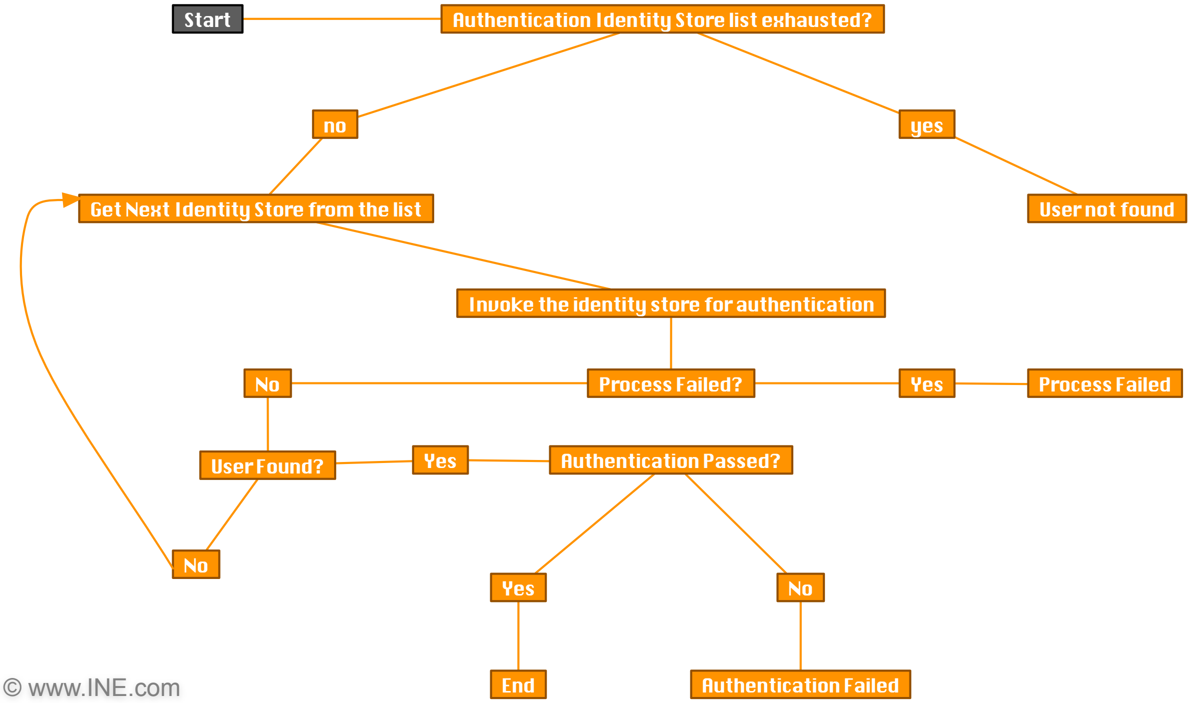
If authentication failed: Reject

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.

Policy Enforcement with Simple Policy



Start

Authentication Identity Store list exhausted?

no

yes

Get Next Identity Store from the list

User not found

Invoke the identity store for authentication

No

Process Failed?

Yes

Process Failed

User Found?

Yes

Authentication Passed?

No

Yes

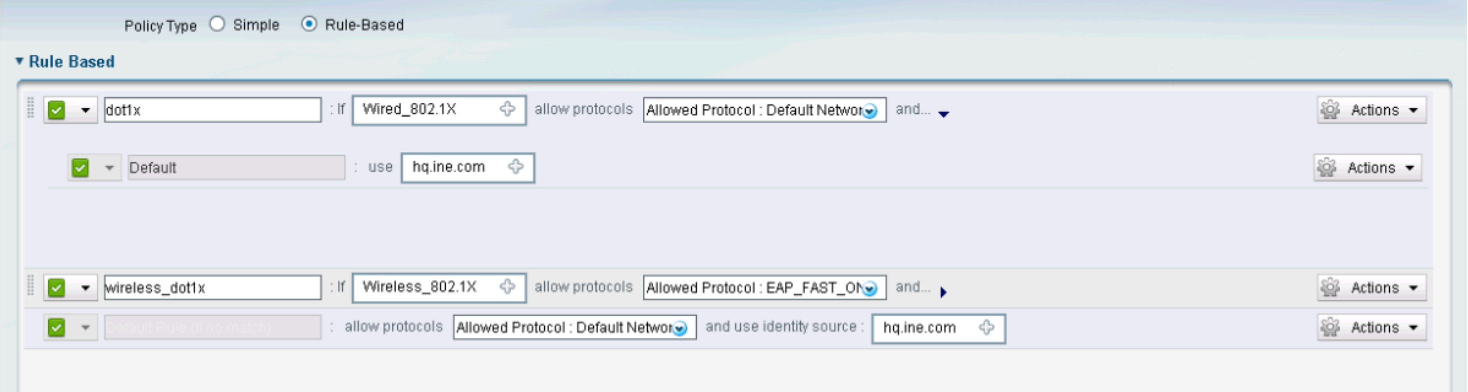
No

End

Authentication Failed

Policy Enforcement with Rule-Based Policy

- Cover a wider variety of variables that can provide more options of what to do with the network traffic.
  - EXAMPLE: If wired 802.1x the use Default Network Access to define allowed protocols and then authenticate with the hq.ine.com AD database.



Policy Type ○ Simple ● Rule-Based

▾ Rule Based

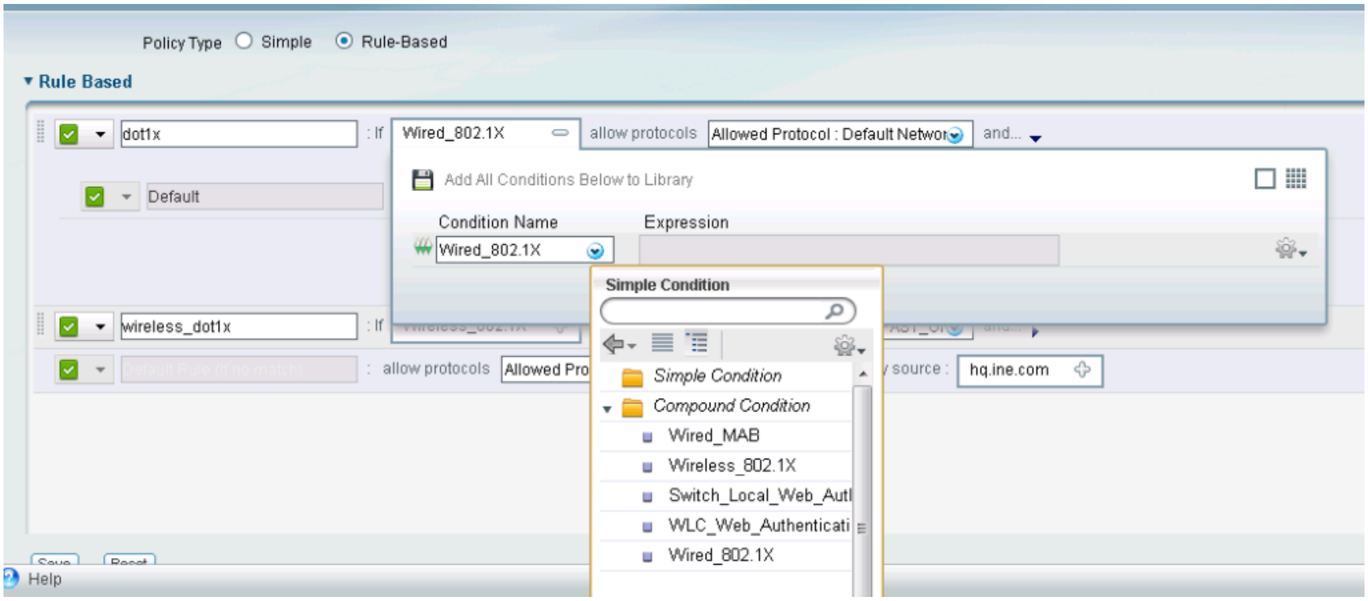
☑ dot1x : If Wired_802.1X allow protocols Allowed Protocol : Default Networ and... Actions

☑ Default : use hq.ine.com Actions

☑ wireless_dot1x : If Wireless_802.1X allow protocols Allowed Protocol : EAP_FAST_ON and... Actions

☑ Default Rule (If no match) : allow protocols Allowed Protocol : Default Networ and use identity source : hq.ine.com Actions

Configuring Cisco ISE for Policy



Policy Type ○ Simple ● Rule-Based

▾ Rule Based

☑ dot1x : If Wired_802.1X allow protocols Allowed Protocol : Default Networ and...

☑ Default

☑ wireless_dot1x : If

☑ : allow protocols Allowed Pro

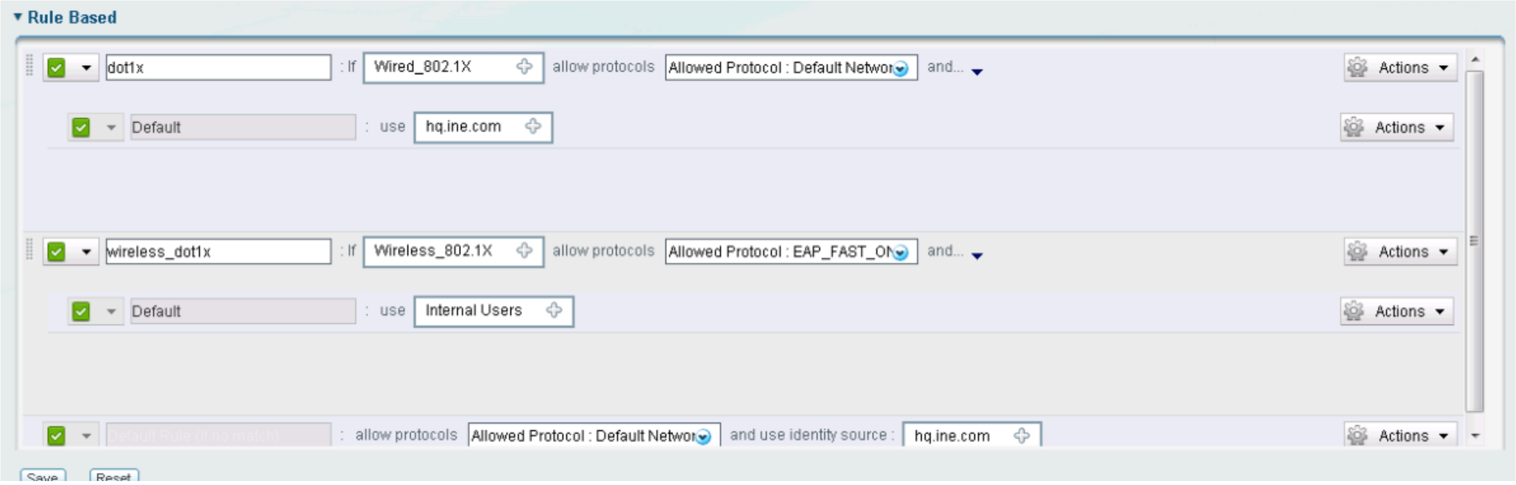
source : hq.ine.com

Add All Conditions Below to Library

Condition Name	Expression
Wired_802.1X	

Copyright © www.INE.com

Verifying Policy Enforcement for Cisco



▾ Rule Based

☑ dot1x : If Wired_802.1X allow protocols Allowed Protocol : Default Networ and...

☑ Default : use hq.ine.com

☑ wireless_dot1x : If Wireless_802.1X allow protocols Allowed Protocol : EAP_FAST_ON and...

☑ Default : use Internal Users

☑ Default Rule (If no match) : allow protocols Allowed Protocol : Default Networ and use identity source : hq.ine.com

Configuring Cisco ISE for Wired 802.1X Authentication

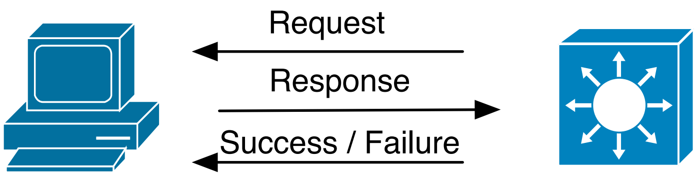
www.INE.com

802.1X Authentication

- 802.1x can be used for authenticating at a switch port or for authenticating wireless users
- Makes use of Extensible Authentication Protocol (EAP).
  - –EAP is not the authentication method, rather it carries arbitrary authentication information.
  - –It’s Media Independent

EAP Packet Types

- There are four packet types
- They are assigned a number that is assigned to the code field in the packet
  - –Request (1)
  - –Response (2)
  - –Success (3)
  - –Failure (4)

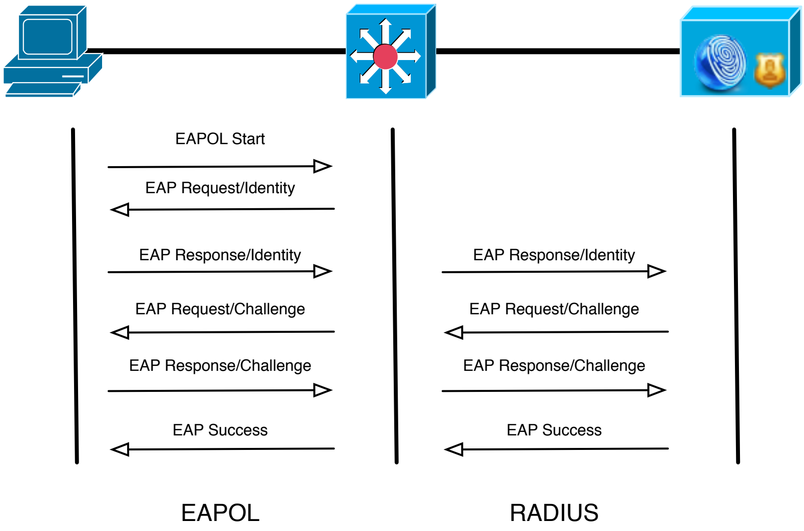


Common EAP methods

- Challenge/Response
  - EAP-MD5
  - EAP-GTC
- Certificate-Based
  - EAP-TLS
- Tunneling
  - PEAP
  - EAP-FAST

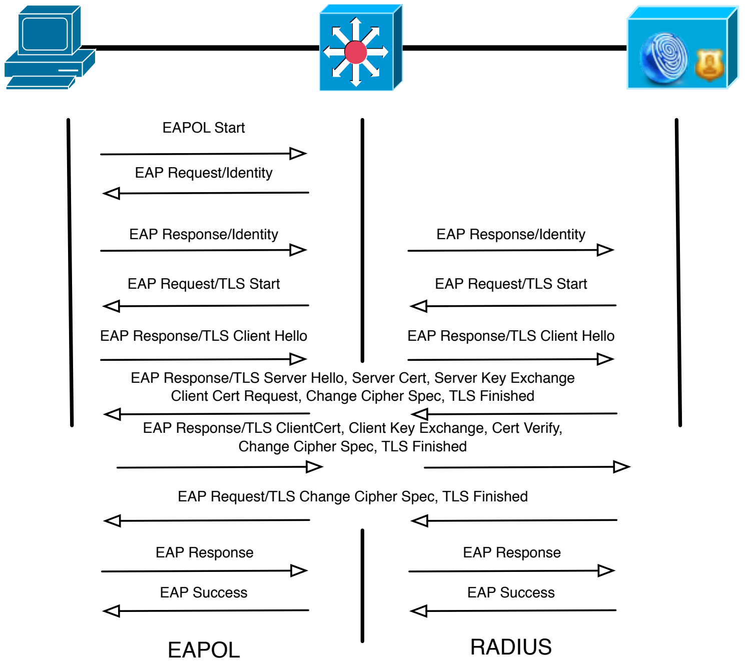
EAP-MD5

- Challenge/Response Method
- ISE sends a challenge
- Client sends a hash of the challenge plus their password



EAP-TLS

- Transport Layer Security
- Mutual Authentication
- Uses Digital Certificates
  - –X.509v3



EAPOL Start

EAP Request/Identity

EAP Response/Identity

EAP Response/Identity

EAP Request/TLS Start

EAP Request/TLS Start

EAP Response/TLS Client Hello

EAP Response/TLS Client Hello

EAP Response/TLS Server Hello, Server Cert, Server Key Exchange
Client Cert Request, Change Cipher Spec, TLS Finished

EAP Response/TLS ClientCert, Client Key Exchange, Cert Verify,
Change Cipher Spec, TLS Finished

EAP Request/TLS Change Cipher Spec, TLS Finished

EAP Response

EAP Response

EAP Success

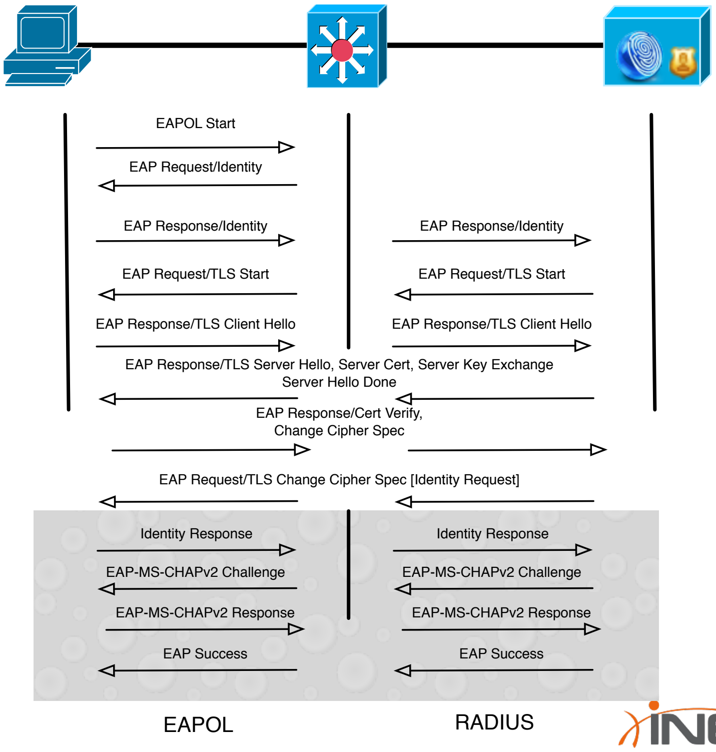
EAP Success

EAPOL

RADIUS

PEAP

- Two Phases
  - supplicant authenticates authentication server with certificate
  - secure tunnel is established (phase 1)
  - Supplicant is authenticated via MS-CHAPv2 in the secure tunnel



EAPOL Start

EAP Request/Identity

EAP Response/Identity

EAP Response/Identity

EAP Request/TLS Start

EAP Request/TLS Start

EAP Response/TLS Client Hello

EAP Response/TLS Client Hello

EAP Response/TLS Server Hello, Server Cert, Server Key Exchange
Server Hello Done

EAP Response/Cert Verify,
Change Cipher Spec

EAP Request/TLS Change Cipher Spec [Identity Request]

Identity Response

Identity Response

EAP-MS-CHAPv2 Challenge

EAP-MS-CHAPv2 Challenge

EAP-MS-CHAPv2 Response

EAP-MS-CHAPv2 Response

EAP Success

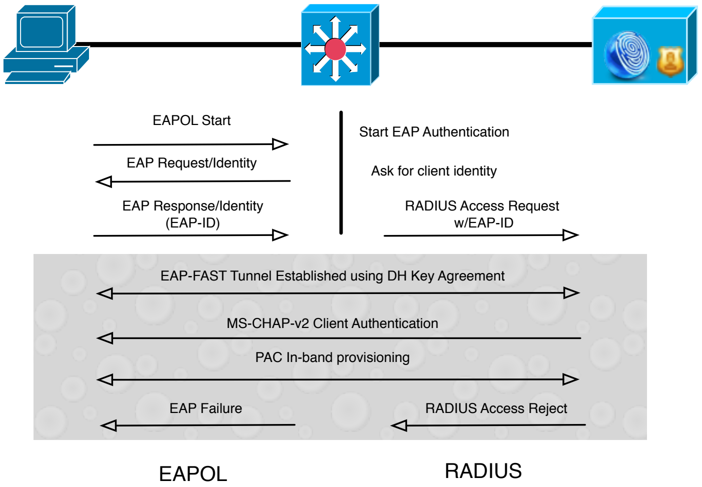
EAP Success

EAPOL

RADIUS

EAP-FAST

- Flexible Authentication via Secure Tunnel
- Phase 0: Protected Access Credentials (PAC) generated.
  - Can be provisioned dynamically or manually
  - Is a unique shared credential that can authenticate the client and the server mutually.
  - Is tied to a user ID and authority ID
  - Removes the need for CA Certificates



EAPOL Start

Start EAP Authentication

EAP Request/Identity

Ask for client identity

EAP Response/Identity (EAP-ID)

RADIUS Access Request w/EAP-ID

EAP-FAST Tunnel Established using DH Key Agreement

MS-CHAP-v2 Client Authentication

PAC In-band provisioning

EAP Failure

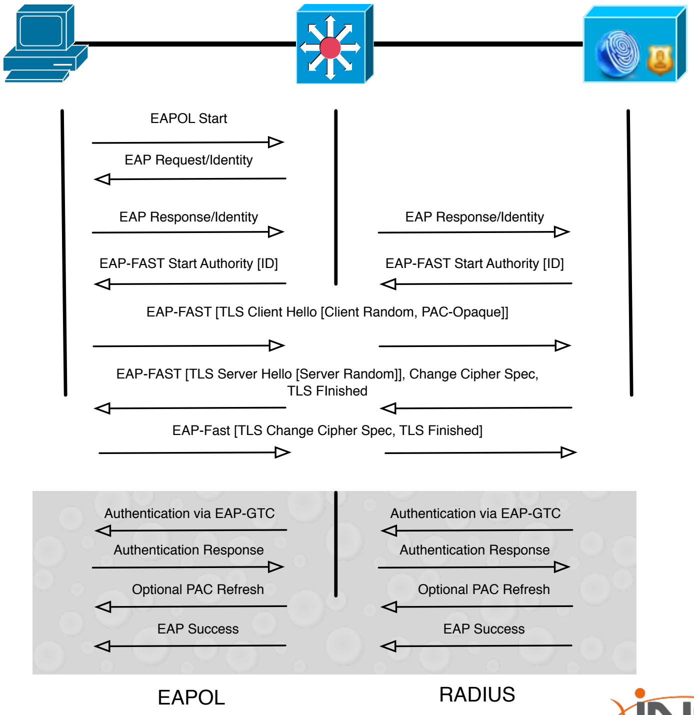
RADIUS Access Reject

EAPOL

RADIUS

EAP-FAST

- Phase 1: Secure Tunnel is Established
- Phase 2: The client is authenticated via the secure tunnel.
  - –Can use EAP-GTC, MS-CHAPv2 and TLS



EAPOL Start

EAP Request/Identity

EAP Response/Identity

EAP Response/Identity

EAP-FAST Start Authority [ID]

EAP-FAST Start Authority [ID]

EAP-FAST [TLS Client Hello [Client Random, PAC-Opaque]]

EAP-FAST [TLS Server Hello [Server Random]], Change Cipher Spec, TLS FInished

EAP-Fast [TLS Change Cipher Spec, TLS Finished]

Authentication via EAP-GTC

Authentication via EAP-GTC

Authentication Response

Authentication Response

Optional PAC Refresh

Optional PAC Refresh

EAP Success

EAP Success

EAPOL

RADIUS

RADIUS

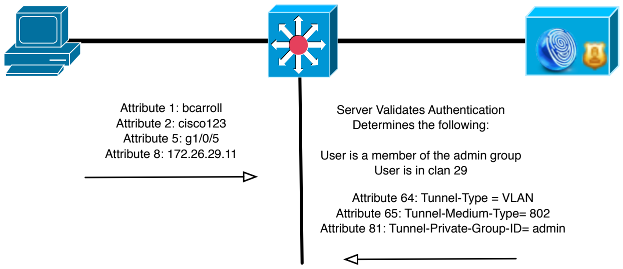
- The Authenticator encapsulates EAP in RADIUS
- Even though EAP attributes are sent, they are limited.
- RADIUS AV Pairs are very important as they can be used by a RADIUS Server to make policy decisions.
- RADIUS Attributes are specified by type, length, and value.

AV-Pairs

- Vendor Specific AV Pairs allow for the protocol to be extended.

RADIUS Attribute	Function
1-User-Name	This is the user that is authenticating
2- User-Password	This is the user password
5- NAS-Port	This is the interface on the NAS (g1/0/5)
8-Framed-IP-Address	This is the user or RADIUS supplied IP address
26- Vendor-Specific	This is ANY attribute defined by a vendor
64- Tunnel-Type	This specifies the encapsulation type
65- Tunnel-Medium-Type	This specifies the physical medium type
81-Tunnel-Private-Group-ID	This specifies the group ID for the session

Example:



Attribute 1: bcarroll
Attribute 2: cisco123
Attribute 5: g1/0/5
Attribute 8: 172.26.29.11

Server Validates Authentication
Determines the following:

User is a member of the admin group
User is in clan 29

Attribute 64: Tunnel-Type = VLAN
Attribute 65: Tunnel-Medium-Type= 802
Attribute 81: Tunnel-Private-Group-ID= admin

802.1x Port Control

- When port control is enabled the port takes on an unauthorized state
- Supplicants can speak EAP to the port
- Once authenticated the port goes Authorized

Lab Time

- Configuring a Windows Client for 802.1X Authentication
  - Wired Auto-Config Service needs enabled
  - Properties now shows authentication tab
- Configuring Cisco ISE for Wired 802.1X Authentication
- Verifying 802.1X Authentication

www.INE.com