SISAS

Implementing Cisco Security Access Solutions

Version 1.0 **Student Guide**

Part Number: 97-3328-01

https://t.me/learningnets



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

DISCLAIMER WARRANTY: THIS CONTENT IS BEING PROVIDED "AS IS" AND AS SUCH MAY INCLUDE TYPOGRAPHICAL, GRAPHICS, OR FORMATTING ERRORS. CISCO MAKES AND YOU RECEIVE NO WARRANTIES IN CONNECTION WITH THE CONTENT PROVIDED HEREUNDER, EXPRESS, IMPLIED, STATUTORY OR IN ANY OTHER PROVISION OF THIS CONTENT OR COMMUNICATION BETWEEN CISCO AND YOU. CISCO SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE. This learning product may contain early release content, and while Cisco believes it to be accurate, it falls subject to the disclaimer above.

© 2014 Cisco Systems, Inc.

https://t.me/learningnets

Welcome Students

Note Students, this letter describes important course evaluation access information.

Welcome to Cisco Systems Learning. Through the Cisco Learning Partner Program, Cisco is committed to bringing you the highest-quality training in the industry. Cisco learning products are designed to advance your professional goals and give you the expertise that you need to build and maintain strategic networks.

Cisco relies on customer feedback to guide business decisions. Therefore, your valuable input will help shape future Cisco course curricula, products, and training offerings. Please complete a brief Cisco online course evaluation of your instructor and the course materials in this student kit. On the final day of class, your instructor will provide you with a URL, directing you to a short post-course evaluation. If there is no Internet access in the classroom, please complete the evaluation within the next 48 hours or as soon as you can access the web.

On behalf of Cisco, thank you for choosing Cisco Learning Partners for your Internet technology training.

Sincerely,
Cisco Systems Learning

https://t.me/learningnets

https://t.me/learningnets

Table of Contents

Course Introduction *I-1*

Overview I-1

Course Goal and Objectives I-3

Course Flow I-4

Your Training Curriculum I-5

Additional References I-8

Threat Mitigation Through Identity Services *1-1*

Identity Services 1-3

Cisco Modular Network Architecture 1-4

Cisco Modular Network Architecture Example Network 1-5

Secure Access Control 1-7

Secure Access Solution Portfolio 1-8

Authentication 1-9

Authorization 1-10

Accounting 1-11

Change of Authorization 1-12

Identity Sources 1-13

RADIUS 1-14

TACACS+ 1-15

Summary 1-16

802.1X and EAP 1-17

IEEE 802.1X Overview 1-19

802.1X Message Flow 1-20

802.1X Authorization 1-21

802.1X VLAN Assignment 1-22

802.1X Downloadable ACLs 1-24

802.1X Host Modes 1-25

802.1X Phased Deployment 1-27

802.1X Monitor Mode 1-28

802.1X Low Impact Mode 1-29

802.1X Closed Mode 1-30

802.1X Deployment Mode Comparison 1-31

802.1X Phased Deployment Guidelines 1-32

Change of Authorization 1-33

MAC Authentication Bypass 1-34

Extensible Authentication Protocol 1-35

Tunnel and Non-Tunnel EAP 1-36

Non-Tunnel EAP Types 1-37

Tunnel EAP Types 1-38

Traditional User and Machine Authentication 1-39

EAP Chaining 1-40

https://t.me/learningnets

EAP Chaining Operation 1-41
EAP Chaining: Corporate Asset and User 1-42
EAP Chaining: Corporate Asset, User Logged Off 1-43
EAP Chaining: Personal Asset with NAM 1-44
EAP Chaining: Personal 3rd Party Asset 1-45
Cisco AnyConnect 3.x Supplicant 1-46
Summary 1-47
Identity System Quick Start 1-49
Logging in to Cisco ISE 1-50
Organization of Cisco ISE GUI 1-51
Local User Database 1-52
Network Access Devices in Cisco ISE 1-53
Cisco ISE Default Authentication Policy 1-55
Switch Configuration Procedure 1-56
Configure Global AAA Parameters 1-57
Configure RADIUS Peering 1-58
Configure Switch for 802.1X Monitor Mode 1-60
Windows Native Supplicant 1-62
Verify Authentication on ISE 1-63
Verify Authentication on Switch 1-65
Summary 1-66
Module Summary 1-67
References 1-67
Module Self-Check 1-69
Cisco ISE Fundamentals 2-1
Cisco ISE Overview 2-3
Cisco ISE Technologies 2-4
Cisco ISE Operational Components 2-5
Cisco ISE as Policy Platform 2-7
Cisco ISE High-Level Flow 2-8
Cisco ISE Personas 2-9
Cisco ISE Deployment Examples 2-10
Summary 2-11
Cisco ISE PKI 2-13
Server Authentication in EAP 2-14
TLS-Protected Communication 2-15
X.509v3 Certificates 2-16
Use of Server Certificate 2-18
First Validation: Verify Server Certificate 2-19
Second Validation: Verify Server Signature 2-20
PKI Enrollment Procedure 2-21
Step 1: Import CA Root Certificate 2-22
Step 2: Generate CSR 2-23
Step 5: Bind Certificate to Pending CSR 2-25

 © 2014 Cisco Systems, Inc.

https://t.me/learningnets

Verify PKI Enrollment 2-27
Summary 2-28
Cisco ISE Authentication 2-29
Cisco ISE Authentication 2-30
Policy Elements in Cisco ISE 2-31
Cisco ISE Authentication Policy Example 2-32
Cisco ISE Rule-Based Authentication 2-33
Authentication Conditions 2-34
Tune Rule-Based Authentication (Situational) 2-35
Define Simple Conditions (Optional) 2-36
Create or Tune Compound Conditions (Optional) 2-37
Define Allowed Protocols (Optional) 2-38
Tune or Create Authentication Rules (Optional) 2-39
Tune Default Authentication Rule (Optional) 2-41
Cisco Network Access Manager 2-42
Networks and Network Groups in Cisco NAM 2-43
Network Settings in Cisco NAM 2-44
Summary 2-45
Cisco ISE External Authentication 2-47
External Authentication 2-48
Active Directory 2-49
Authentication Methods with Active Directory 2-51
AD-Derived Group Membership 2-52
Active Directory Integration Methods 2-53
Active Directory Integration Procedure 2-54
Configure AD Domain and Store 2-55
Test AD Connection 2-56
Join Active Directory 2-57
Select Groups from Directory 2-58
Cisco ISE Identity Source Sequence 2-59
Configure Identity Source Sequence 2-60
Apply Identity Source Sequence 2-62
Verify External Authentication 2-63
Summary 2-64
Module Summary 2-65
References 2-65
Module Self-Check 2-67
Advanced Access Control 3-1
Certificate-Based User Authentication 3-3
EAP-TLS Bidirectional Authentication 3-4
Verification of Client Certificates 3-5
Implementation Procedure for EAP-TLS in Cisco ISE Deployment 3-6
Select CA Certificate for EAP Verification 3-7
Deploy Certificates on Clients 3-8

https://t.me/learningnets

Configure 802.1X Supplicant to Use EAP-TLS 3-9
Configure Supplicant to Use Certificates 3-10
Configure Certificate Authentication Profile 3-11
Apply Certificate Authentication Profile to Identity Source Sequence 3-12
Verify EAP-TLS Operation 3-13
Summary 3-14
Authorization 3-15
Authorization in Cisco ISE 3-16
Authorization Policy Overview 3-17
Downloadable ACLs 3-19
Authorization Profile 3-20
Authorization Policy 3-21
Building Conditions 3-22
Authorization Configuration Procedure 3-23
Configure Rule Matching Logic 3-24
Configure Authorization Profile 3-25
Configure Authorization Policy Rule 3-27
Tune Default Authorization Rule 3-28
Verify User Authorization on ISE 3-29
Verify Machine Authorization on ISE 3-30
Verify Authorization on Switch 3-31
Verify dACL Assignment on Switch 3-32
Summary 3-33
Cisco TrustSec and MACsec 3-35
Cisco TrustSec Overview 3-37
Cisco TrustSec Benefits 3-39
SGT Classification 3-41
Inline SGT Transport 3-42
SGT Exchange Protocol 3-43
Enforcement Using SGACLs 3-44
Enforcement Using SGFW 3-45
SGA Deployment Procedure 3-46
Configure CTS Between ISE and NAD 3-47
Define Security Groups 3-48
Implement Dynamic Classification 3-49
Implement Static Classification 3-50
Implement SGT Transport 3-51
Define SGACLs 3-52
Implement SGACL Enforcement 3-53
Implement SGFW Enforcement on the ASA 3-55
MAC Security 3-56
MACsec Cryptography 3-57
MACsec Hop-by-Hop Operation 3-58
Implement Downlink MACsec on the ISE 3-59
Implement Downlink MACsec on the NAM 3-60

 © 2014 Cisco Systems, Inc.

https://t.me/learningnets

Implement Downlink MACsec on the Switch 3-61
Verify Downlink MACsec 3-62
Summary 3-63
Module Summary 3-65
References 3-65
Module Self-Check 3-67
Web Authentication and Guest Access 4-1
Deploying WebAuth 4-3
Web Authentication 4-5
WebAuth Process 4-6
WebAuth Scenarios 4-7
Central WebAuth Operation 4-8
Central WebAuth Configuration Procedure 4-10
Configure Switch for WebAuth 4-11
Configure MAB to Continue If User Not Found 4-12
Tune the WebAuth Identity Source Sequence 4-13
Configure Pre-WebAuth dACL 4-14
WebAuth Redirect: Authorization Profile 4-15
WebAuth Redirect: Authorization Policy Rule 4-16
Configure Authorization for WebAuth Users 4-17
Verify WebAuth Initiation on the ISE 4-18
Verify WebAuth Redirect on the Switch 4-20
Verify WebAuth Redirect on the Client 4-21
Verify Completed WebAuth on the ISE 4-22
Verify Completed WebAuth on Switch and Client 4-23
Summary 4-24
Deploying Guest Service 4-25
Guest Service Overview 4-27
Guest Service and WebAuth 4-28
Cisco ISE Guest Service Applications 4-29
Admin Portal Configuration Scope 4-30
Sponsor Portal Configuration Scope 4-31
Guest User Portal Functions 4-32
Portal Services Location 4-33
Sponsor Portal Configuration Procedure 4-34
Configure Portal HTTPS Ports 4-35
Manage Sponsor Groups 4-36
Assign Users to Sponsor Groups 4-38
Configure Guest Policies 4-39
Manage Guest Portals: Default or Custom 4-40
Configure Guest Authorization 4-42
Provision Guest Accounts in Sponsor Portal 4-43
Verify Guest Access 4-44
Monitor Guest Access on ISE 4-45

https://t.me/learningnets

Summary 4-46
Module Summary 4-47
References 4-47
Module Self-Check 4-49
Endpoint Access Control Enhancements 5-1
Deploying Posture Service 5-3
Cisco ISE Posture Service Overview 5-5
Posture in Cisco ISE 5-6
Persistent Agents (Windows and Mac) 5-7
Web Agent 5-8
Client Provisioning Process 5-9
Posture Conditions 5-10
CoA in Posture Assessment 5-12
Posture Configuration Procedure 5-13
Download Client Provisioning Resources 5-14
Configure Client Provisioning Policy: Operating System and Conditions 5-15
Posture Policy Building Blocks 5-16
Configure Posture: Condition 5-17
Configure Posture: Remediation 5-18
Configure Posture Policy: Posture Requirement 5-19
Configure Posture: Posture Policy 5-20
Redirect Clients to Client Provisioning Portal 5-21
Configure Authorization Policy for Posture 5-22
Verify Redirection to CPP 5-23
Verify Remediation 5-24
Verify Posture Compliance 5-25
Summary 5-26
Deploying Profiler Service 5-27
Cisco ISE Profiler Service Overview 5-29
Profiler in Cisco ISE 5-31
Cisco ISE Probes 5-32
Commonly Deployed Probes 5-34
Profiling Without Probes 5-37
Cisco ISE Profiler and CoA 5-38
Profiling Policies 5-39
Parent Profiling Policies 5-40
Child Profiling Policies 5-42
Profiling Configuration Procedure and Scenario 5-43
Enable Profiler Service 5-44
Enable CoA in Profiling Feature 5-45
Configure Probes 5-46
Examine Parent Policy 5-47
Examine Parent Conditions 5-48
Configure Profiler Conditions 5-49

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Configure Profiling Policy 5-50
Configure Authorization for Profiled Endpoints 5-51
View Profiled Endpoint Identity Groups 5-52
Verify Profiling in Authentications Page 5-53
View Profiled Endpoints 5-54
Summary 5-55
Implementing BYOD 5-57
The BYOD Challenge 5-58
Device Onboarding 5-60
Single and Dual SSID Design 5-62
Dual SSID Flow 5-63
Authorization Policy in Dual SSID Design 5-64
Connecting to the Network 5-65
Guest Access 5-66
Employee Access Before Endpoint Provisioning 5-67
Native Supplicant Provisioning for Employees 5-68
Provisioning for Employees: Wi-Fi Profile 5-69
Client Provisioning Policy for Employees 5-70
Employee Access After Endpoint Provisioning 5-71
Verify BYOD: Device Registration 5-72
Verify BYOD: Client Provisioning 5-73
Verify BYOD: Connect to the SSID 5-74
Summary 5-75
Module Summary 5-77
References 5-77
Module Self-Check 5-79
Access Control Troubleshooting 6-1
Troubleshooting Network Access Controls 6-3
Troubleshooting Procedure 6-4
Cisco ISE Troubleshooting Tools 6-6
RADIUS Authentication Troubleshooting 6-7
Execute Network Device Command 6-8
Evaluate Configuration Validator 6-9
Posture Troubleshooting 6-10
TCP Dump 6-11
Troubleshooting Authentication Overview 6-12
Troubleshoot 802.1X on Switch 6-13
Troubleshoot RADIUS Peering 6-19
Troubleshoot Peering with User Database 6-22
Troubleshoot Identity Source Sequencing 6-24
Troubleshoot Client-Side Certificate Issues 6-25
Troubleshoot Disallowed Authentication Protocol 6-26
Troubleshoot Machine Authentication 6-27
Web Authentication Troubleshooting Overview 6-28

https://t.me/learningnets

Review ISE Authentication Policy for WebAuth 6-29
Review ISE Authorization Policy for WebAuth 6-30
Review Authorization Profile for WebAuth 6-31
Troubleshoot Mismatch of ACL Name 6-32
Posture Troubleshooting Overview 6-36
Review Posture: Client Provisioning Policy 6-37
Review Posture Policy 6-38
Review Posture Requirements 6-39
Troubleshoot Posture 6-40
Case Study: Troubleshoot Profiling 6-41
Summary 6-42
Module Summary 6-43
References 6-43
Module Self-Check 6-45
Glossary G-1

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Course Introduction

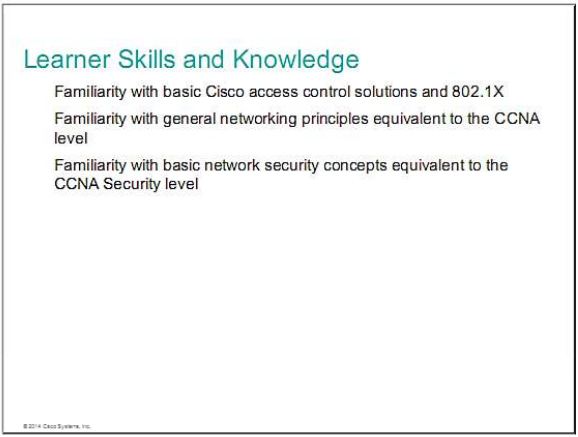
Overview

The Implementing Cisco Security Access Solutions (SISAS) course describes an access control solution that centers on the Cisco Identity Services Engine (ISE). The learners build the solution by implementing basic authentication and then extending the system with the authorization, guest services, Cisco TrustSec, posture, and profiling components. The most fundamental concepts include the authentication methods, such as 802.1X, MAC Authentication Bypass (MAB), and Web authentication (WebAuth). The learners implement various types of the Extensible Authentication Protocol (EAP) using two different 802.1X supplicants: the native Windows OS supplicant and the Cisco AnyConnect supplicant. The Cisco AnyConnect supplicant is used for a range of scenarios, including EAP chaining. Although the Web Authentication and the guest services are often deployed together, the learners first implement the WebAuth feature for employee access and then enable the guest feature to allow guest access. The posture service on the ISE is used to determine the security posture status of the endpoints. The learners use the built-in posture elements pre-configured in the ISE, and also implement a custom remediation to automatically install antivirus software. The ISE offers a wide range of profiling capabilities. The learners test the default functionality with the common probes enabled, and extend the profiling granularity by defining custom policies. The course ends with a troubleshooting lesson and an optional troubleshooting lab exercise.

https://t.me/learningnets

Learner Skills and Knowledge

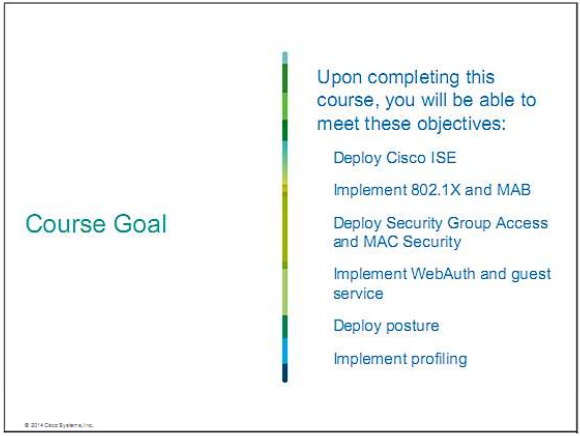
This subtopic lists the skills and knowledge that learners must possess to benefit fully from the course. The subtopic also includes recommended Cisco learning offerings that learners should first complete to benefit fully from this course.



https://t.me/learningnets

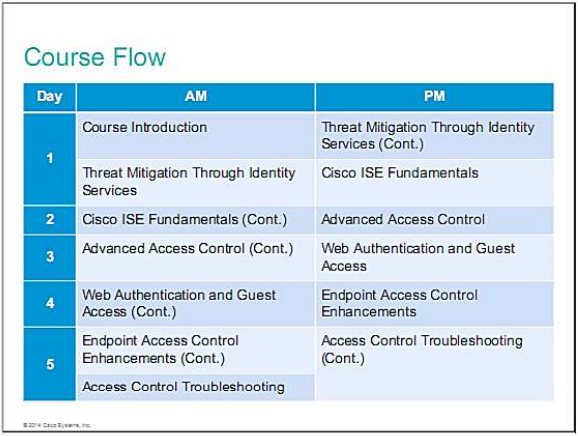
Course Goal and Objectives

This topic describes the course goal and objectives.



Course Flow

This topic presents the suggested flow of the course materials.



The schedule reflects the recommended structure for this course. This structure allows enough time for the instructor to present the course information and for you to work through the lab activities. The exact timing of the subject materials and labs depends on the pace of your specific class.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Your Training Curriculum

This topic presents the training curriculum for this course.



You are encouraged to join the Cisco Certification Community, a discussion forum open to anyone holding a valid Cisco Career Certification (such as Cisco CCIE®, CCNA®, CCDA®, CCNP®, CCDP®, CCIP®, CCNP® Security and CCNP® Voice, or CCSP™). It provides a gathering place for Cisco certified professionals to share questions, suggestions, and information about Cisco Career Certification programs and other certification-related topics. For more information, visit http://www.cisco.com/go/certifications.

Training Curriculum

This subtopic presents the training curriculum for this course.



For more information on certifications, visit http://www.cisco.com/go/certifications.

Note Cisco provides three levels of general certifications for IT professionals with several different tracks to meet individual needs. Cisco also provides focused certifications for designated areas such as cable communications and security. There are many paths to Cisco certification, but only one requirement—passing one or more exams demonstrating knowledge and skill. For details, go to www.cisco.com/go/certifications.

https://t.me/learningnets

Learner Introductions

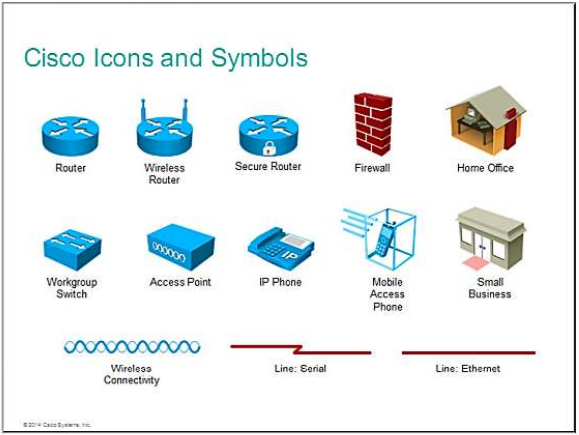
- Your name
- Your company
- Job responsibilities
- Skills and knowledge
- Brief history
- Objective



© 2014 Cisco Systems, Inc.

Additional References

This topic presents the Cisco icons and symbols that are used in this course, as well as information on where to find additional technical references.



Cisco Glossary of Terms

For additional information on Cisco terminology, refer to the Cisco Internetworking Terms and Acronyms glossary of terms at http://docwiki.cisco.com/wiki/Category:Internetworking_Terms_and_Acronyms_(ITA).

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Module 1

Threat Mitigation Through Identity Services

To protect against unauthorized access to controlled or confidential information, enterprise networks require an effective network access control embedded within the network infrastructure.

The Cisco Identity Services Engine is a next-generation identity and access control policy platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations. The unique architecture of Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices. The administrator can use that information to make proactive governance decisions by tying identity to various network elements including access switches, WLCs, VPN gateways, and data center switches. This module introduces the main components of the Cisco ISE architecture and explains the its role in the network access control solution.

Upon completing this module, you will be able to meet these objectives:

- Describe the role of identity services in the secure access solution
- Implement 802.1X and EAP
- Jump start the secure access solution

https://t.me/learningnets

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Lesson 1

Identity Services

Overview

The most secure solution at the access edge is to leverage the intelligence of the network. Cisco offers a host of services designed to enable secure user and host access to enterprise networks. It provides standards-based network access control at the access layer by using the 802.1X protocol to secure the physical ports where end users connect.

This lesson describes the secure access solution and identifies its key components, such as authentication, authorization, accounting, the identity stores, as well as the main authentication proxy protocols: RADIUS and TACACS+.

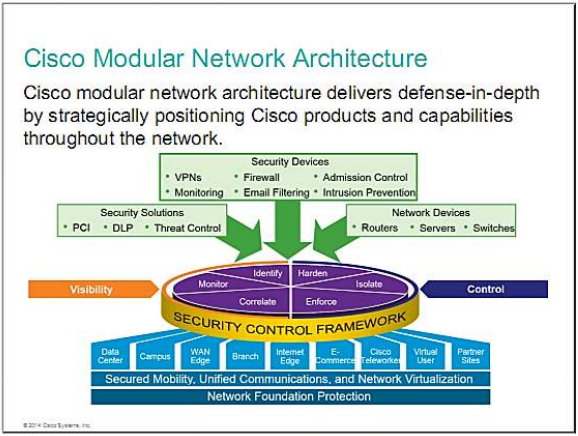
Upon completing this lesson, you will be able to meet these objectives:

- Describe the Cisco modular network architecture
- Describe the Cisco secure access solution
- Describe the secure access portfolio
- Describe the authentication
- Describe the authorization
- Describe AAA accounting
- Describe the CoA
- Describe the identity sources
- Describe RADIUS
- Describe TACACS+

https://t.me/learningnets

Cisco Modular Network Architecture

This topic describes Cisco modular network architecture solution.



Cisco modular network architecture delivers defense-in-depth by strategically positioning Cisco products and capabilities throughout the network and by using the collaborative capabilities between the platforms. A wide range of security technologies are deployed in multiple layers, under a common strategy and administration. Products and capabilities are positioned where they deliver the most value, while facilitating collaboration and operations. The figure illustrates the Cisco modular network architecture.

Cisco modular network architecture is delivered in the form of design blueprints and security solutions:

Design blueprints—Cisco validated designs and security best practice guides. Prescriptive design guidance is provided in CVDs which cover the various PINs present in an enterprise network, such as campus, WAN edge, branches, and data center. Design guidance is also provided for technologies such as unified communications, network virtualization, and network foundation protection, which are present in multiple places in the network. The selection of platforms and capabilities within those designs, is driven by the application of the Cisco Security Control Framework.

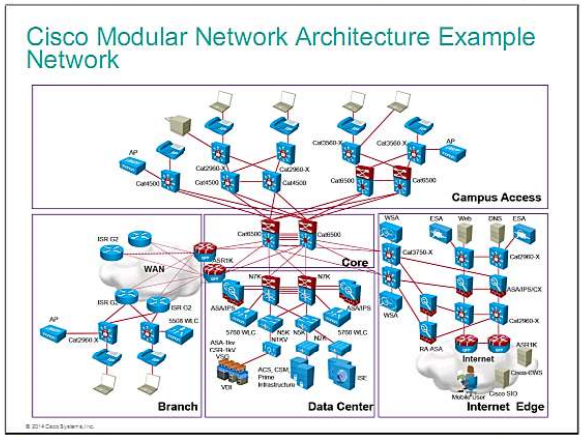
Security solutions—The Cisco SCF and the design blueprints provide the foundation for industry security solutions which address the requirements of specific industries such as retail, financial, healthcare, and manufacturing.

As illustrated in figure above, Cisco security services are embedded as an intrinsic part of the architecture. The Cisco security services support the solution lifecycle and the security products included in the designs.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Cisco Modular Network Architecture Example Network

This topic provides an example of Cisco modular network architecture network design.



The figure illustrates the range of security technologies and products in an example of a network, which is built based on the modular network architecture design principles. In the network, multiple layers of security controls are implemented throughout the network. All network devices and security controls are implemented in the high availability mode, providing confidentiality, integrity, and availability of data, applications, endpoints, and the network itself.

The security architecture shown in the figure is made up of the following security products and technologies:

Endpoint security: organizations today use a complex and diverse set of endpoints, both wired and wireless. These devices need to be secure from data loss, data theft, and privacy invasion, and must meet the local country and
state security requirements. Endpoint security within the example architecture includes the following products:

- Cisco SecureX Context-Aware Security
- Cisco Identity Services Engine
- Cisco Wireless LAN Controller
- Cisco AnyConnect Secure Mobility Client

Network security: One of the most fundamental elements of the Cisco security controls is network security, which is designed to protect the integrity of the network infrastructure itself, where entire network segments may be the target of attacks such as theft of service, service abuse, DoS, and data loss. Network security within the example architecture includes the following products:

- Cisco Adaptive Security Appliance 5500-X Series

https://t.me/learningnets

- Cisco Catalyst 6500 ASA Services Module
- Cisco ASA 1000V Cloud Firewall
- Cisco Virtual Security Gateway
- Cisco ISR G2 Integrated Security Firewall
- Cisco Cloud Services Router 1000V Series
- VPN
- Infrastructure protection on all devices

Content and application security: Organizations can be vulnerable to attacks on data and content. Spam, phishing through e-mail, and web content attacks have all been used to provide an attacker access to a target system. Content security within the example architecture includes the following products:

Cisco Email Security Appliance

Cisco Web Security Appliance

Cisco Intrusion Prevention System

Cisco ASA 5500-X Series NGFW

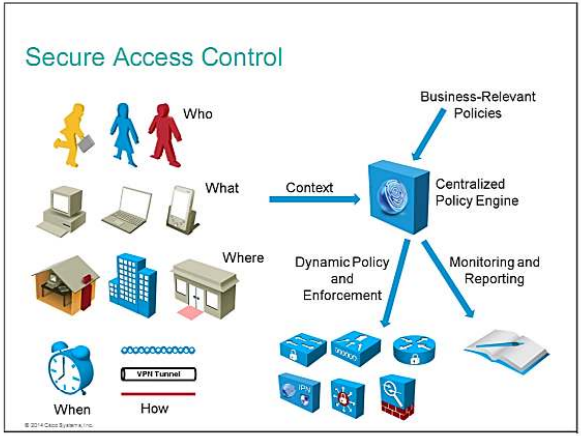
System network and event management: Network management tools help providers automate, simplify, and integrate their network to reduce operational costs. Network management within the example architecture includes the following products:

- Cisco Security Manager
- Cisco Prime Infrastructure
- Cisco Secure Access Control System

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Secure Access Control

This topic describes the Cisco TrustSec solution.



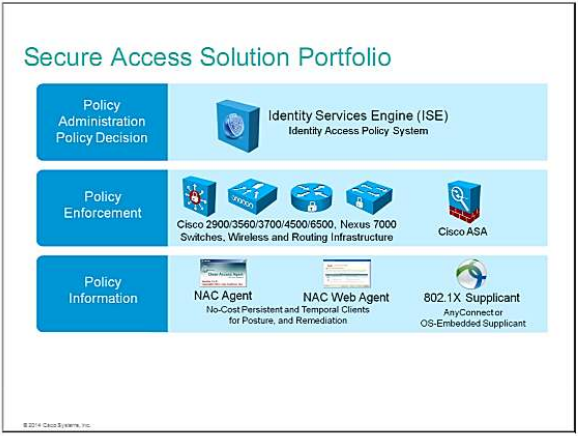
The Cisco secure access solution mitigates security risks by providing comprehensive visibility into where and where who is connecting from what across the entire network infrastructure. It provides exceptional control over who and what accesses the network and where they can go.

Cisco secure access solution builds upon your existing identity-aware access layer infrastructure (switches, routers, wireless controllers, and so on) and is a fully validated solution in which all the components are thoroughly vetted and rigorously tested as an integrated system.

The Cisco secure access system uses standards-based identity and enforcement models, such as IEEE 802.1X and VLAN control. It also has many more advanced identity and enforcement capabilities, such as flexible authentication, dACLs, SGA, device profiling, posture assessments, guest access management, and more.

Secure Access Solution Portfolio

This topic describes the Cisco secure access solution portfolio.



At the heart of the Cisco secure access solution you will find the Cisco Identity Services Engine. Cisco ISE provides a centralized, identity-based policy platform for context-aware access control decisions across the wired, wireless, and VPN infrastructure. Cisco ISE combines AAA, posture, profiler, and guest management features in a single, unified appliance, providing a single point for policy management, monitoring, and troubleshooting.

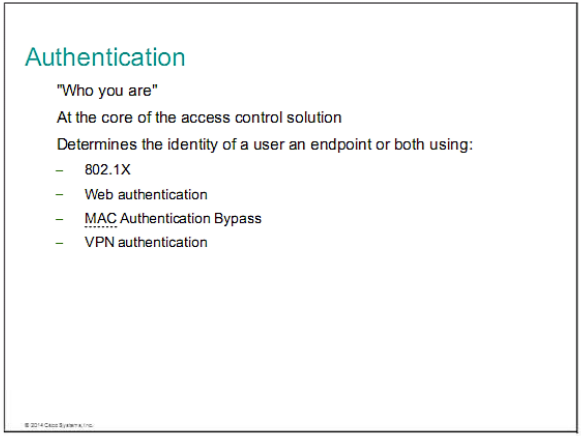
The switched, wireless, and routing infrastructure provides the policy enforcement building block. The network devices ensure that only the expected communications is permitted through the network.

The third tier is responsible for tying the endpoint into the secure access solution. Among other things, it collects the information about the user identities and their endpoints and communicates with other components in the secure access solution. This functionality is typically available as software elements installed on the endpoints, such as the Cisco AnyConnect Mobility client, or the NAC agents.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Authentication

This topic describes the authentication.



The authentication is used to determine the identity of a user or endpoint. For users, it answers the question who the user is. The authentication plays a fundamental role in the access control solution, as many other functions rely on it. The authentication can be performed using a verity of methods.

802.1X authentication requires an agent, which is referred to as a supplicant, to run on the endpoint. Most modern PC operating systems offer a native supplicant. Some vendors, such as Cisco, offer premium supplicants that extend the 802.1X supplicant functionality with additional features.

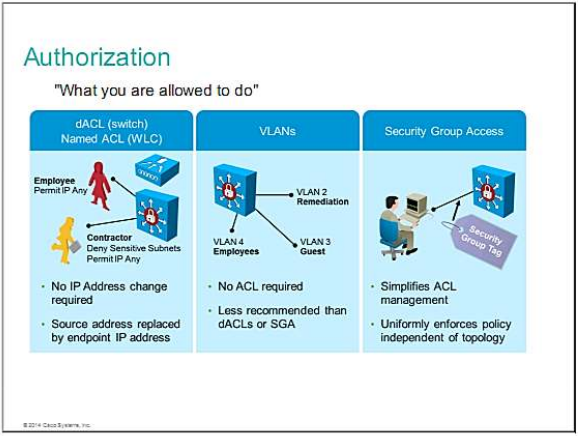
Web authentication provides an authentication option for endpoints that lack an 802.1X supplicant and for endpoints that do have an 802.1X supplicant, but the user fails authentication. An example use case is for guest user access to the network.

MAB is an option to allow certain systems that do not have an 802.1X supplicant, such as a printer or a security camera, to access the network while still maintaining a consistent configuration across switch access ports. MAB utilizes a database of the MAC addresses of systems that are allowed access to the network. It is important to note that MAB is not "MAC authentication." Instead it is an "authentication bypass" that is based on MAC address. MAB specifies a set of MAC addresses that are allowed to skip authentication.

Other common authentication methods include the VPN authentication, in which the users must provide their access credentials before a VPN connection is established.

Authorization

This topic describes the authorization.



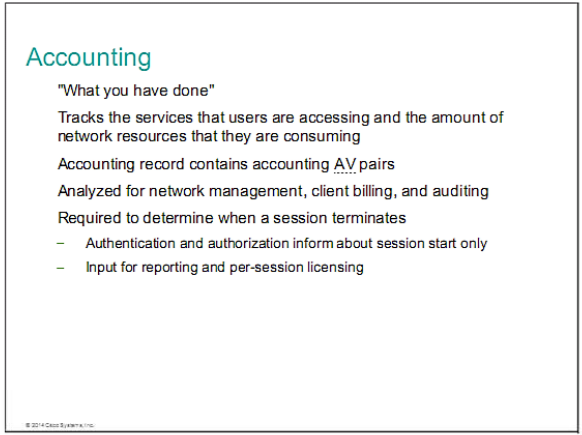
After network users and devices are authenticated and confirmed to comply with an organization's security policy, they are allowed network access. Their subsequent resource and service entitlement is accomplished by the authorization process. The Cisco access control solution supports multiple authorization methods, including ACLs, VLANs, and SGA.

These choices help organizations design their security architecture and services offerings with maximum flexibility and effectiveness. Downloadable, per-session ACLs on the switches, which are named ACLs on wireless LAN controllers, and dynamic VLAN assignments can be implemented at the ingress point where users and devices gain their initial entry to the network. In addition, SGA allows user identity information to be captured and tagged with each data packet. SGACLs can be implemented at an egress point where a network resource (such as a file server) is located. SGA-based access control allows organizations to keep the existing logical design at the access layer, and with flexible policies and services, meet different business requirements without having to redeploy the security controls. This solution tags every packet at the ingress network device and enables the egress network devices to enforce traffic control closest to the destination.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Accounting

This topic describes the accounting.

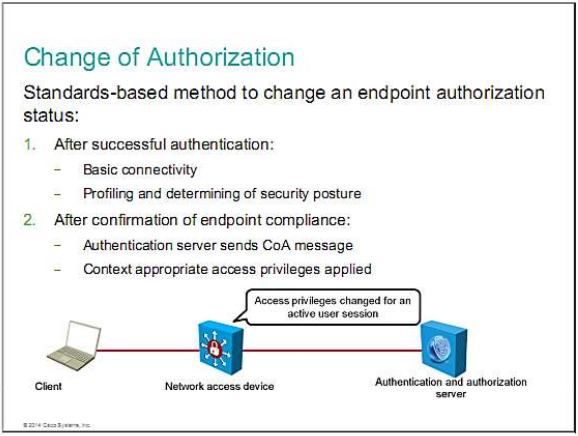


The AAA accounting feature enables you to track the services that users are accessing and the amount of network resources that they are consuming. When AAA accounting is enabled, the network access server reports user activity to the accounting server in the form of accounting records. Each accounting record contains accounting AV pairs and is stored on the security server. This data can then be analyzed for network management, client billing, and auditing.

The Cisco Identity Services Engine uses AAA accounting to determine which access sessions are still active. The authentication and authorization provide information about the session start, but not about session termination. The data about session termination is needed for reporting, per-session licensing, and statistics calculation.

Change of Authorization

This topic describes the CoA.



Traditional RADIUS allows the RADIUS client to make AAA requests to RADIUS servers. If the circumstances changed, there was no mechanism for the RADIUS server to dynamically return to the client with an updated authorization policy. To address this, RADIUS CoA was developed and defined in RFC 5176.

The AAA framework uses CoA messages to dynamically modify active subscriber sessions. For example, RADIUS attributes in CoA messages might instruct the framework to create, modify, or terminate a subscriber service.

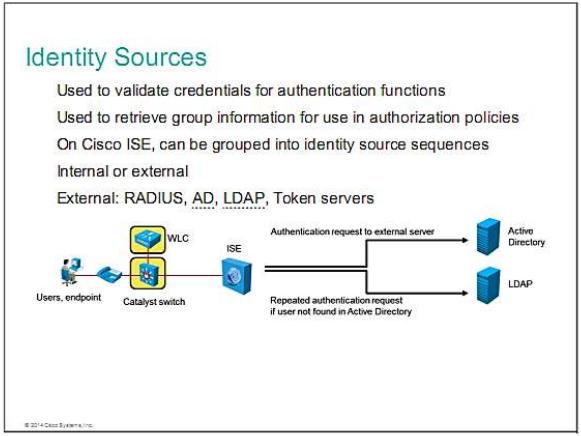
After successful authentication, an endpoint is allowed basic network connectivity. This basic connectivity profile enables the Cisco Identity Services Engine to perform profiling and security posture functions. Once the Cisco ISE establishes the endpoint compliance, it sends a CoA message to the authenticator and supplies extended access privileges, which are typically described in the form of an appropriate dACL.

CoA is also utilized for centralized web authentication. Web authentication is often used as a fallback authentication method. When authentication fails at ISE, ISE can be configured to push an initial policy that only allows web traffic and redirects that web traffic to the web authentication portal. If the user can successfully authenticate via the web authentication portal, then ISE issues a CoA to update the policy on the NAD as appropriate by context.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Identity Sources

This topic describes the identity sources.



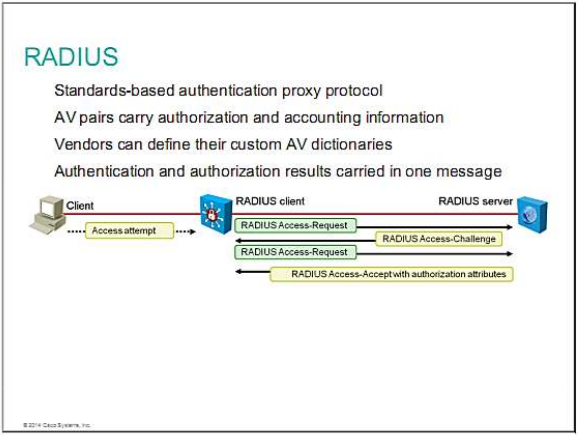
The identity source is the user or endpoint database used to validate credentials for user authentication functions. It can also offer group membership information that is used to determine the applicable authorization policy. Some authenticators, such as the Cisco Identity Services Engine, can group multiple identity sources into an identity source sequence. When specified, Cisco ISE searches these identity sources in the order in which they are defined in this sequence.

Identity sources can be internal or external. Cisco ISE maintains internal databases that can be used as identity sources during the authentication process. The internal user database is commonly used to support guest logins. The internal endpoint database is primarily populated using the Cisco ISE profiler function.

Cisco 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. Cisco ISE supports several commonly implemented identity sources, including Active Directory and LDAP.

RADIUS

This topic describes RADIUS.



RADIUS is a standards-based network protocol that facilitates centralized AAA services. RADIUS uses AV pairs to carry AAA information between the RADIUS client and the RADIUS server. The IETF has defined a standard set of RADIUS attributes. RADIUS is also extendible by vendors who can define VSAs.

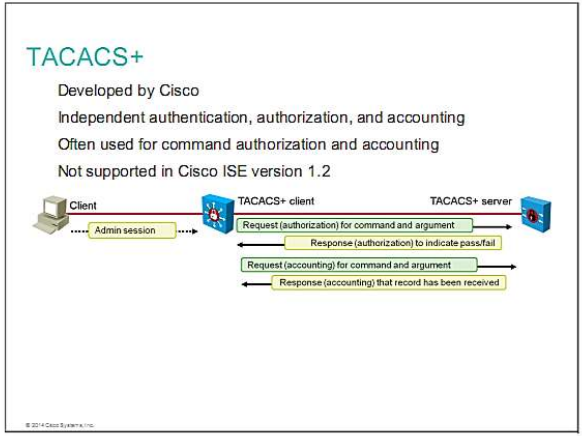
Cisco Identity Services Engine uses dictionaries to organize RADIUS AV pairs. It has built-in system-defined dictionaries for the IETF standard set of AV Pairs as well as several vendor specific dictionaries. New, user-defined dictionaries can be created to support other vendors, if necessary.

RADIUS combines authentication and authorization. An access-accept packet sent by the RADIUS server to the client contains the appropriate authorization details. This makes it difficult to decouple authentication and authorization.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

TACACS+

This topic describes TACACS+.



TACACS+ is an AAA protocol developed by Cisco. It differs from RADIUS mainly through the independent AAA architecture. This allows separate authentication solutions that can still use TACACS+ for authorization and accounting.

A common use of the feature is in the control administrative access to network devices. TACACS+ supports command authorization and accounting on a command by command basis. During a management session, if additional authorization checking is needed, the TACACS+ client checks with a TACACS+ server to determine if the user is granted permission to use a particular command. Also, with command **accounting**, an accounting record can be sent to the TACACS+ server, facilitating a centralized audit trail of administrative activities. This provides greater control over the commands that can be executed on the access server while decoupling from the authentication mechanism.

TACACS+ is not supported in Cisco Identity Services Engine version 1.2. If you want to control the administrative access from the Cisco ISE 1.2 or earlier, there are options using RADIUS. You can authorize exec sessions using privilege levels. In ISE, you can assign a privilege level to a user and this privilege level can be used to define the user's administrative privileges. Also, if the devices have been configured IOS Role Based Access Control, you can assign a CLI view name to a user to define that user's administrative privileges.

https://t.me/learningnets

Summary

This topic summarizes the key points that were discussed in this lesson.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Lesson 2

802.1X and EAP

802.1X is an IEEE standard for media-level access control, offering the capability to permit or deny network connectivity, control VLAN access and apply traffic policy, based on user or machine identity. 802.1X uses the EAP to authenticate users who wish to access the network.

This lesson describes the 802.1X framework and the commonly used EAP variants.

Upon completing this lesson, you will be able to meet these objectives:

- Provide an overview of 802.1X
- Describe the 802.1X message flow
- Describe the 802.1X authorization
- Describe the 802.1X VLAN assignment
- Describe the downloadable ACLs
- Describe the 802.1X host modes
- Describe the 802.1X phased deployment
- Describe the monitor mode
- Describe the low impact mode
- Describe the closed mode
- Compare the 802.1X deployment modes
- Describe the 802.1X phased deployment guidelines
- Describe CoA
- Describe MAB
- Describe EAP
- Describe tunnel and non-tunnel EAP
- Describe non-tunneled EAP types
- Describe tunnel EAP types

https://t.me/learningnets

Describe the traditional user and machine authentication

Describe EAP chaining

Describe the EAP chaining operation

Describe the EAP chaining flow for corporate asset and user

Describe the EAP chaining flow for corporate asset and user logged off

Describe the EAP chaining flow for personal asset with NAM

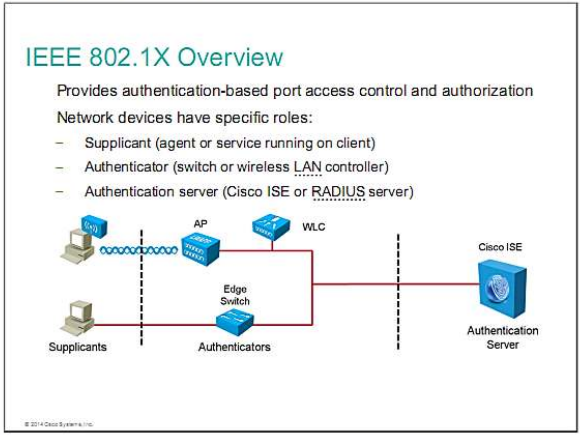
Describe the EAP chaining flow for personal asset with third party supplicant

Describe the AnyConnect supplicant

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

IEEE 802.1X Overview

This topic describes the 802.1X framework.



With 802.1X port-based authentication, network devices have these roles:

Supplicant: This role is an agent or service running on the device that requests access to the network. It responds to requests from the switch. The software code of the supplicant must be 802.1X-compliant.

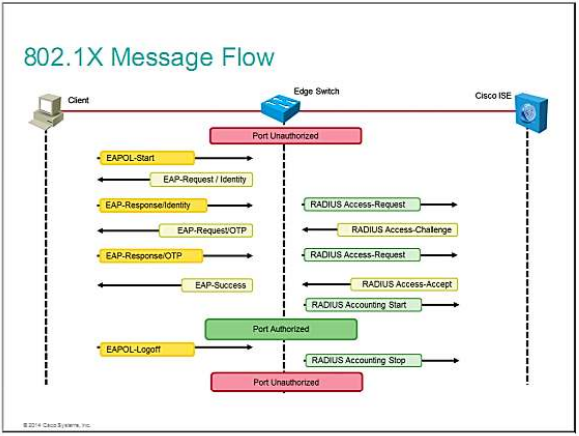
Authenticator: This role controls physical access to the network based on the authentication status of the client. This device acts as an intermediary (proxy) between the client and the authentication server. It requests identity information from the client, verifies that information with the authentication server, and relays the authentication server's response to the client. The authenticator includes the RADIUS client functionality, which is responsible for encapsulating and de-encapsulating the EAP frames and interacting with the authentication server. The most common authenticators are LAN switches and wireless LAN controllers.

Authentication server: This role performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch if the client is authorized to access the network. Because the authenticator acts as the proxy, the authentication service is transparent to the client. Cisco Identity Services Engine acts as the authentication server.

When the authenticator receives EAPOL frames and relays them to the authentication server, the Ethernet header is stripped and the remaining EAP frame is re-encapsulated into RADIUS format. The EAP frames are not modified during encapsulation, and the authentication server must support EAP within the native frame format. The opposite happens in the other direction. When the authenticator receives frames from the authentication server, the RADIUS header of the server is removed, leaving the EAP frame. The EAP frame is then encapsulated using EAPOL and sent to the supplicant.

802.1X Message Flow

This topic describes the 802.1X message flow.



The authentication can be initiated by the supplicant or the authenticator. The authenticator initiates authentication when the link state changes from down to up, or periodically as long as the port remains up and unauthenticated.

The authenticator sends an EAP request or identity frame to the client to request its identity. Upon receipt of the frame, the supplicant responds with an EAP response or identity frame. However, if during bootup, the supplicant does not receive an EAP request or identity frame from the authenticator, the supplicant can initiate authentication by sending an EAPOL start frame, which prompts the authenticator to request the identity of the client.

Note If 802.1X is not enabled or supported on the NAD, any EAPOL frames from the supplicant are dropped. If the supplicant does not receive an EAP request or identity frame after three attempts, the supplicant sends frames as if the port was in authorized state. A port in authorized state effectively means that the supplicant has been successfully authenticated.

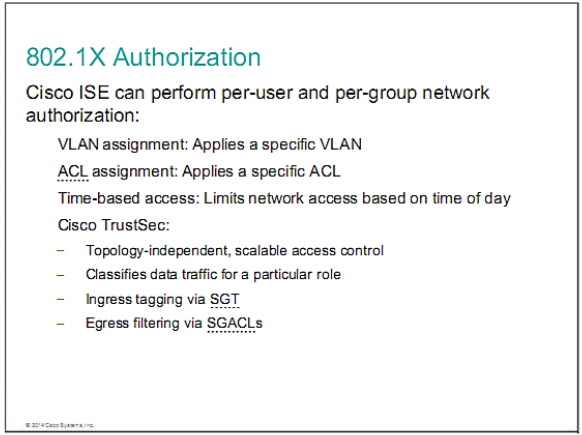
When the supplicant provides its identity, the authenticator begins its role as the intermediary and passes EAP frames between the supplicant and the authentication server until authentication succeeds or fails. If the authentication succeeds, the authenticator port is authorized.

The specific exchange of EAP frames depends on the authentication method that is used. The figure shows a message exchange that was initiated by the supplicant using the OTP authentication method with Cisco Identity Services Engine.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

802.1X Authorization

This topic describes the 802.1X authorization.



The 802.1X framework provides authentication and authorization of clients that seek network access. The authorization features include the following:

VLAN assignment: With VLAN assignment, the authentication server can associate a VLAN with a particular user or group, and instruct the switch to dynamically assign the authenticated user into that VLAN. If your organization uses an access control method that is based on different VLANs (with routed ACLs or a firewall system configured egress to the VLANs), this method can easily provide strong access control and auditing within an enterprise network.

ACL assignment: With ACL assignment, the authentication server can associate an ACL with a particular user or group, and instruct the NAD to dynamically assign the ACL to the session of the user. This mechanism provides a very granular access control method because it extends to the port level.

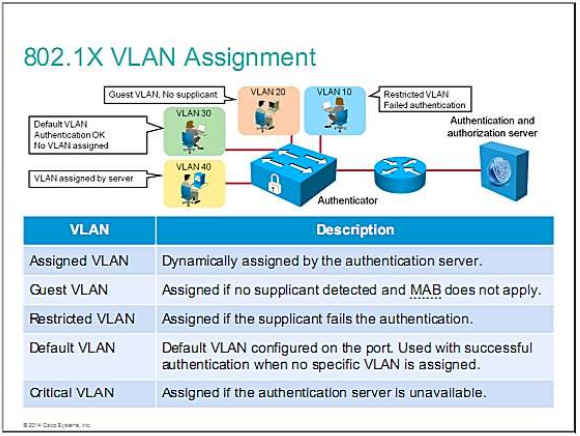
Time-based access: With time-based access, the authentication server can control the times at which a certain user is allowed to connect to the network.

Cisco TrustSec: Security group access provides topology-independent, scalable access control. With security group access, the ingress switches classify data traffic for a particular role and tag the traffic with security group tags. The egress network devices evaluate the security group tags and perform filtering by applying the appropriate security group ACLs to the packets.

https://t.me/learningnets

802.1X VLAN Assignment

This topic describes the 802.1X VLAN assignment.



VLAN	Description
Assigned VLAN	Dynamically assigned by the authentication server.
Guest VLAN	Assigned if no supplicant detected and MAB does not apply.
Restricted VLAN	Assigned if the supplicant fails the authentication.
Default VLAN	Default VLAN configured on the port. Used with successful authentication when no specific VLAN is assigned.
Critical VLAN	Assigned if the authentication server is unavailable.

Assigned VLAN

The assigned VLAN is specified by the Authentication Server in the RADIUS Access-Accept message. Traditionally this is used to assign the appropriate VLAN for users that can successfully authenticate with the Authentication Server. But it can also be used when authentication fails at the Authentication Server. For example, the Authentication Server can be configured to assign a VLAN associated with guest users when both user authentication and MAB fail. This is different than the Guest VLAN described next. The advantage to using an Authentication Server assigned VLAN for guest access is that the guest VLAN assignment and guest access will be centrally logged in the AAA system. This centralized audit trail is not available for any of the other VLAN types described below. The other VLANs described below are managed locally on the switch. For example, if the Authentication Server passes an Access-Reject message back to the switch and the switch uses it's locally configured Guest VLAN or Restricted VLAN, there won't be the centralized audit trail recording access in the AAA system.

Guest VLAN

When 802.1X is enabled on an access port, a user without an 802.1X client is typically denied access to the network. By using the guest VLAN feature of 802.1X, you can offer limited network access to such users. You can configure a guest VLAN for each 802.1X port.

If a guest VLAN is enabled on an 802.1X port, the switch assigns a client to the guest VLAN if the client does not send EAPOL packets or does not reply to the EAP request or identity frame from the authentication server. Multiple non-802.1X-capable clients may be allowed access when the switch port is moved to the guest VLAN.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Restricted VLAN

You can configure a restricted VLAN (sometimes called an authentication-failed VLAN) for each 802.1X port on a switch to provide limited services to clients that cannot access the guest VLAN. These clients are 802.1X-compliant and cannot access another VLAN because they fail the authentication process. A restricted VLAN allows users who do not have valid credentials on an authentication server (typically, visitors to an enterprise) to access a limited set of services. The administrator can control the services that are available to the restricted VLAN.

Note A VLAN can be configured to be both the guest VLAN and the restricted VLAN, if you want to provide the same services to both types of users.

The switch (authenticator) keeps a count of failed authentication attempts for any client. When the count exceeds the maximum permitted number of authentication attempts, the port moves to the restricted VLAN. When the RADIUS server replies with either an EAP failure or an empty response that does not contain an EAP packet, the failed attempt count is incremented. The failed attempt counter resets when the port moves into the restricted VLAN.

Default VLAN

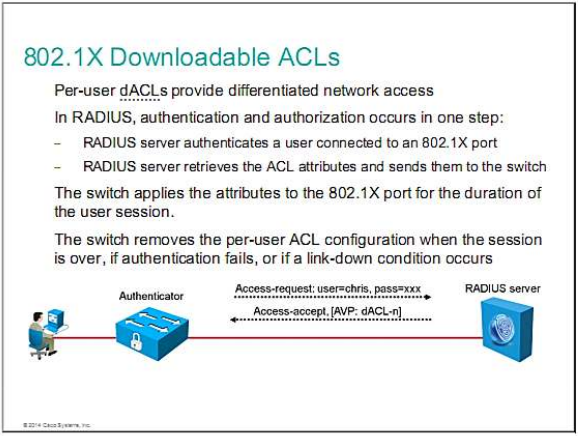
The default VLAN is the VLAN that is configured on the port. When a client successfully authenticates to the server and no dynamic VLAN is assigned by the authentication server, the default VLAN is retained on the port.

Critical VLAN

A critical VLAN can be configured on the switch. The critical VLAN is the VLAN that is applied to the 802.1X-enabled interface if the authentication server is unavailable.

802.1X Downloadable ACLs

This topic describes the 802.1X downloadable ACLs.



You can enable per-user ACLs to provide different levels of network access and service to an 802.1X-authenticated user. When the RADIUS server authenticates a user that is connected to an 802.1X port, it retrieves the ACL attributes based on the user identity and sends them to the switch. The switch applies the attributes to the 802.1X port for the duration of the user session. The switch removes the per-user ACL configuration when the session is over, if authentication fails, or if a link-down condition occurs. The switch does not save RADIUS-specified ACLs in the running configuration. When the port is unauthorized, the switch removes the ACL from the port.

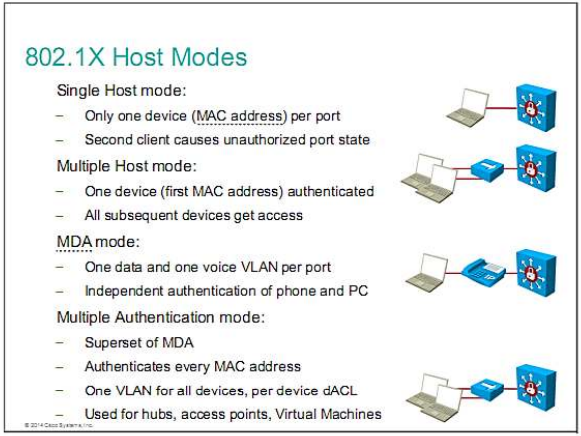
RADIUS supports per-user attributes, including vendor-specific attributes. These VSAs are in octet-string format and are passed to the switch line-by-line as a result of the authorization process. The VSAs that are used for per-user ACLs are inacl#*<n>*. The following is an example depicting the syntax of a dACL:

```
ip:inacl#100=permit ip any 209.165.201.2 255.255.255.255
ip:inacl#200=permit ip any 209.165.201.3 255.255.255.255
ip:inacl#300=deny ip any any
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

802.1X Host Modes

This topic describes the 802.1X host modes.



The host mode of the 802.1X port determines whether more than one client can be authenticated on the port and how authentication will be enforced. You can configure an 802.1X port to use any of the four host modes that are described below. In addition, each mode may be modified to allow pre-authentication open access.

Single Host Mode

In single-host mode, only one client can be connected to the 802.1X-enabled port. The switch detects the client when the port changes to the up state and sends out an EAPOL frame. Access is provided for the client after authentication. Packets from other hosts are dropped. If the client leaves or is replaced with another client, the switch changes the port link state to down, and the port returns to the unauthorized state.

Multiple Host Mode

In Multiple Host mode (often called multi-host mode), you can attach multiple hosts to a single 802.1X-enabled port. In this mode, only one of the attached clients must be authorized for all clients to be granted network access. If the port becomes unauthorized (reauthentication fails or an EAPOL logoff message is received), the authenticator denies network access to all of the attached clients.

Multiple Domain Authentication Mode

MDA mode (often called multi-domain mode) allows an IP phone and a single host behind the IP phone to authenticate independently, using 802.1X, MAB, or (for the host only) web-based authentication. In this application, multidomain refers to two domains (data and voice VLAN), and only one MAC address is allowed per domain. The switch can place the host in the data VLAN and the IP phone in the voice VLAN, but they appear on the same switch port. The data and voice VLAN assignment can be obtained from the VSAs received from the AAA server.

Multiple Authentication Mode

Multiple Authentication mode (often called multi-auth mode) allows one 802.1X or MAB client on the voice VLAN and multiple authenticated 802.1X, MAB, or web authorization clients on the data VLAN. When a hub or access point is connected to an 802.1X port, multi-auth mode provides enhanced security over the multi-host mode by requiring authentication of each connected client. For non-802.1X devices, MAB or web-based authentication can be used as the fallback method for individual host authentications, which allows different hosts to be authenticated through different methods on a single port.

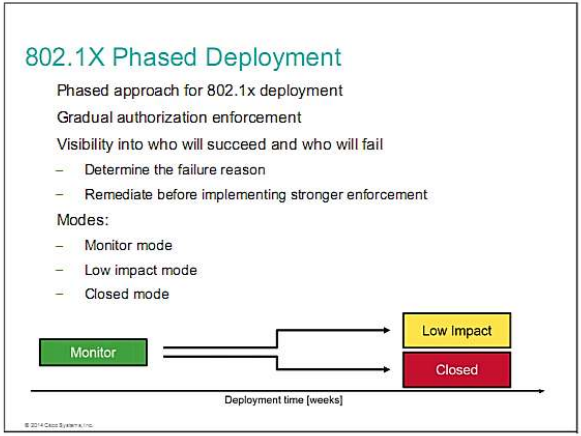
In this mode, the first host that is authorized on the port defines the VLAN assignment, and subsequent hosts will be added to the same VLAN. They may either have no VLAN assignment in the RADIUS database, or their configured group VLAN must match the assigned group VLAN on the port. Otherwise they will be denied access to the port.

Also, if the Authentication Server assigns a dACL, the dACL will be modified to use the authenticated host's IP address as the source address. That is, in multi-auth mode, per-host differentiated dACLs are supported.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

802.1X Phased Deployment

This topic describes the 802.1X phased deployment.

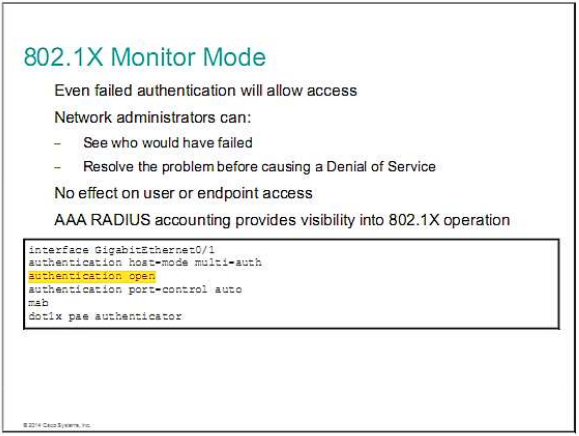


802.1X can be implemented using a phased deployment model that allows for limited impact on network access while gradually introducing authentication and authorization. In the phased approach the network administrators can gain visibility who will succeed and who will fail, determine the failure reason, and remediate the problem before enabling a stronger enforcement mode. The three modes are: monitor, low impact, and closed mode.

A phased deployment will utilize monitor mode first and then will shift to either low impact mode or closed mode. A phased deployment typically also includes the strategy of phases across a topology. For example, implementation may occur sequentially through each remote site and finish with headquarters. Another example would be to implement on wireless networks first and then implement on wired networks.

802.1X Monitor Mode

This topic describes the 802.1X monitor mode.



The monitor mode allows for the deployment of the authentication methods 802.1X, MAB, or web authentication without any effect on user or endpoint access to the network. Monitor mode is like placing a security camera at the door to monitor and record port access behavior. With AAA RADIUS accounting enabled, you can log authentication attempts and gain visibility of whom and what is connecting to your network with an audit trail. You can discover the following information:

Which endpoints, such as PCs, printers, cameras, and so on, are connecting to your network

Where these endpoints connect to the network (switch, port)

Whether they are 802.1X-capable or not

Whether they have valid credentials

In the event of failed MAB attempts, whether the endpoints have known, valid MAC addresses

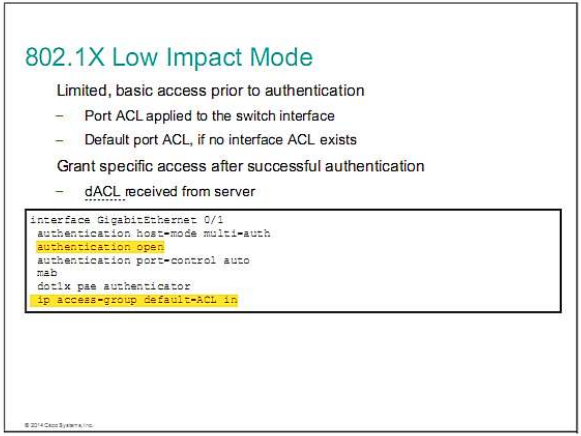
Monitor mode is enabled using 802.1X with the open access and multiauth mode Cisco IOS Software features. Monitor mode is configured with the **authentication open** command.

The default behavior of 802.1X is to block all data traffic except EAPOL. However, the open access feature allows you the option of providing unrestricted access to all traffic, even though authentication (802.1X, MAB, or web authorization) is enabled. Open access is accomplished with no impact to end users or network-attached hosts.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

802.1X Low Impact Mode

This topic describes the 802.1X low impact mode.



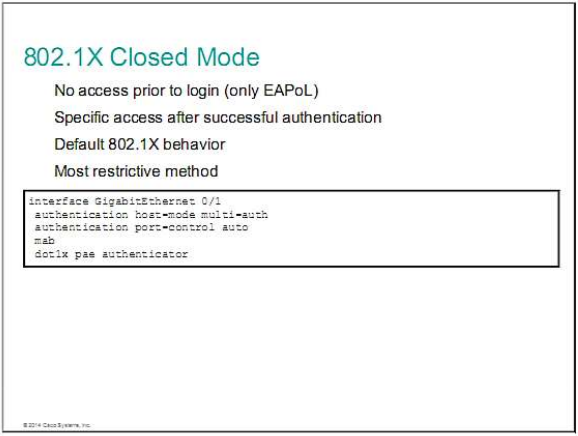
With low-impact mode, you are able to strengthen the security stance by adding an ingress ACL to the 802.1X-enabled switch port that is configured in open mode. This ACL provides the ability to maintain whatever basic connectivity is required for unauthenticated hosts.

This procedure can be used to provide a host that is attached to a default port with the ability to use DHCP, DNS, and perhaps get to the Internet, while blocking access to internal resources.

When a device connected to that switch port authenticates, an appropriate authorization policy can be applied. Options for authorization policies include downloadable ACLs, dynamic VLAN assignment or security group tags.

802.1X Closed Mode

This topic describes the 802.1X closed mode.



The default behavior on a Cisco switch port configured for 802.1X is closed mode. With closed mode, only EAPOL traffic is allowed until the authentication process completes. Authentication is required before any basic network services are available, including DHCP. Consideration of 802.1X timers is very important with closed mode.

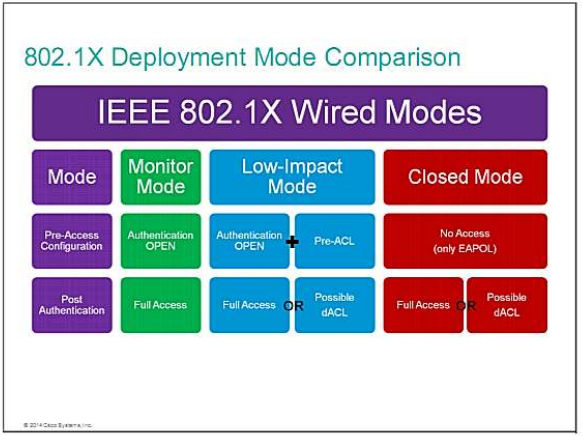
When a device connected to that switch port authenticates, an appropriate authorization policy can be applied. Options for authorization policies include downloadable ACLs, dynamic VLAN assignment or security group tags.

Closed mode was previously called high security mode. This term can be a misnomer. Closed mode is not necessarily more secure than a properly configured low impact mode.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

802.1X Deployment Mode Comparison

This topic contrasts the 802.1X deployment modes.



This figure summarizes the pre-authentication and post-authentication behavior of the three 802.1X deployment phases: monitor, low-impact, and closed modes.

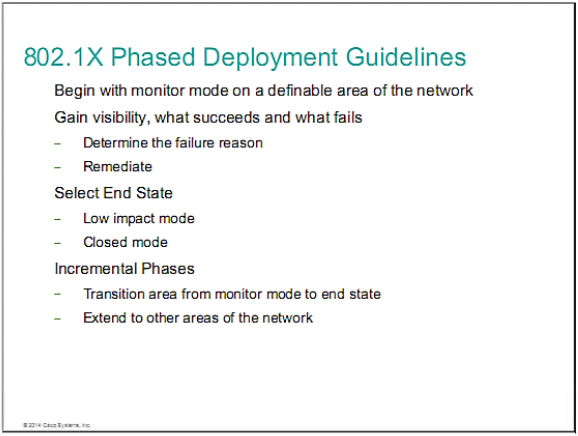
In monitor mode, the open access feature transforms the normal behavior of blocking traffic on an 802.1X-enabled port until authentication and authorization are successfully performed. Full access is provided independently of the authentication results.

In low-impact mode, a pre-authentication ACL is added to the port to permit some basic connectivity. After successful authentication, options to enforce authorization policy include downloadable ACLs, dynamic VLAN assignment and Security Group Tags.

In closed mode, only EAPOL traffic is permitted until the user authenticates. After successful authentication, options to enforce authorization policy include downloadable ACLs, dynamic VLAN assignment and security group tags. The authorization options available in closed mode are identical to the options available in low-impact mode.

802.1X Phased Deployment Guidelines

This topic describes the 802.1X phased deployment guidelines.



802.1X can be implemented using a phased deployment model that allows for limited impact on network access while gradually introducing authentication and authorization. It is generally recommended to begin the phased deployment with monitor mode in a well defined area of the network. Think of this phase as an audit phase. Your network administrators can gain visibility into who will succeed and who will fail, determine the failure reason, and remediate the problem before enabling a stronger enforcement mode.

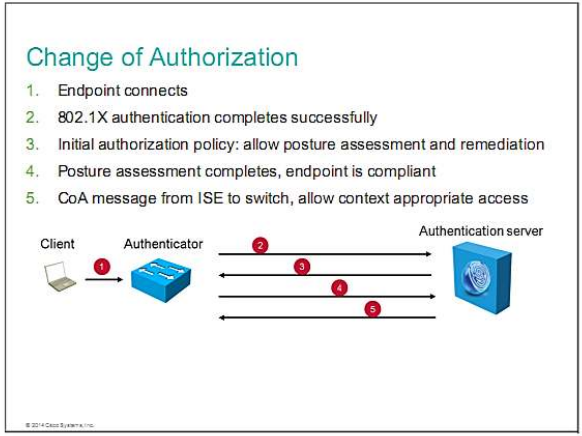
Before moving from monitor mode to a stronger enforcement mode, you must decide whether low impact mode or closed mode is most appropriate. The choice will depend on factors internal to your organization and your organization's security policy. It is possible that different modes may be appropriate in different areas of your network. For example it may be optimal to use low impact mode at the headquarters campus and closed mode at branch offices.

After a successful phase of deployment, it is time to move to the next phase. After a successful audit phase, you can move to the preferred enforcement mode for that area of the network. You can also extend the identity solution to other areas of the network using monitor mode.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Change of Authorization

This topic describes the CoA.



Traditional RADIUS allows the RADIUS client to make AAA requests to RADIUS servers. If the circumstances changed, there was no mechanism for the RADIUS server to dynamically return to the client with an updated authorization policy. To address this, RADIUS CoA was developed and defined in RFC 5176.

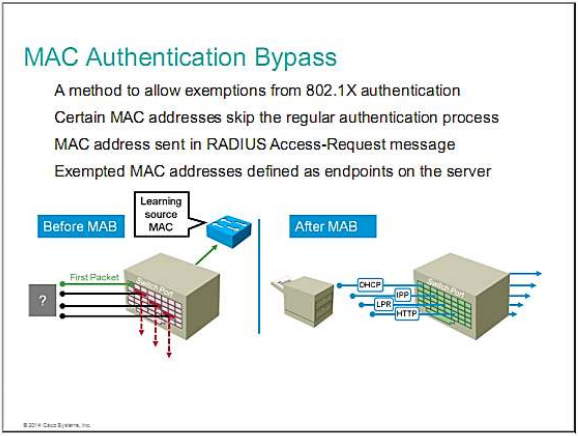
The figure depicts one example of the potential flow using CoA. Note that the example is simplified for instructional purposes and does not necessarily include all real-world considerations or demonstrate real configuration syntax. An explanation of the flow follows:

1. At initial state, a switch port is in an unauthenticated state. The ACL that is in place on the switch port will allow some basic network functionality without authentication, such as DHCP-based IP address assignment, TFTP download of IP phone configurations, Active Directory machine authentication and, of course, 802.1X authentication. An endpoint connects and user authentication that is based on 802.1X completes successfully.
2. Cisco Identity Services Engine is aware of the user identity, but has not yet performed posture assessment. As such, it associates a temporary policy with this session.
3. Cisco ISE sends a RADIUS Access-Accept message to the switch, specifying an authorization policy that allows two things. (1) IP connectivity to Cisco ISE to allow the posture assessment to complete. (2) IP connectivity to a remediation server in case posture assessment fails. This policy is dynamically applied to the switch using a dACL.
4. The posture assessment completes and the endpoint is found to be compliant. Cisco ISE associates a full access policy with the session.
5. Cisco ISE issues a CoA message to the switch, which causes an update to the authorization policy that is assigned to the switch port, granting context appropriate network access.

https://t.me/learningnets

MAC Authentication Bypass

This topic describes the MAB feature.



Not all network devices support an 802.1X supplicant. Printers, security cameras and badge readers are a few examples. Prior to MAB, it was common to simply not configure 802.1X on switch ports supporting such devices. This approach has several drawbacks. It doesn't allow consistent configuration of all access switch ports. It doesn't allow the RADIUS server to maintain access records on those switch ports. It requires reconfiguration of switch ports if devices move. It allows someone with physical access to the wall port to replace the expected device with any device of their choosing. MAB provides a better way of handling devices that do not support an 802.1X supplicant.

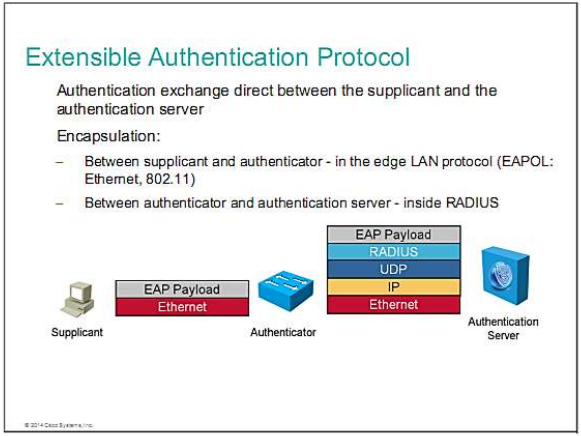
When the MAB feature is enabled on an 802.1X port, the authenticator uses the MAC address as the client identity. The authentication server has a database of client MAC addresses that are allowed to access the network. After detecting a client on an 802.1X port, the authenticator waits for an Ethernet frame from the client. The authenticator sends an Access-Request message using the MAC address of the endpoint as both the username and the password to the RADIUS server. The RADIUS server can then compare the MAC address against entries in its policy database to make authorization decisions.

If an EAPOL packet is detected on the interface during the lifetime of the link, the authenticator determines that the device connected to that interface is an 802.1X-capable supplicant and uses 802.1X authentication (not MAB) to authorize the interface.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Extensible Authentication Protocol

This topic describes the Extensible Authentication Protocol.



802.1X uses the EAP to authenticate users who wish to access the network. EAP messages are exchanged between a supplicant and an authenticator, which are tunneled inside the EAPOL and RADIUS protocols. The authenticator is aware of this interaction, but does not actively participate in it. Instead, it waits for the decision of the authentication server, which is communicated to it natively over the RADIUS protocol. The specific exchange of EAP frames depends on the authentication method (that is, EAP variety) being used.

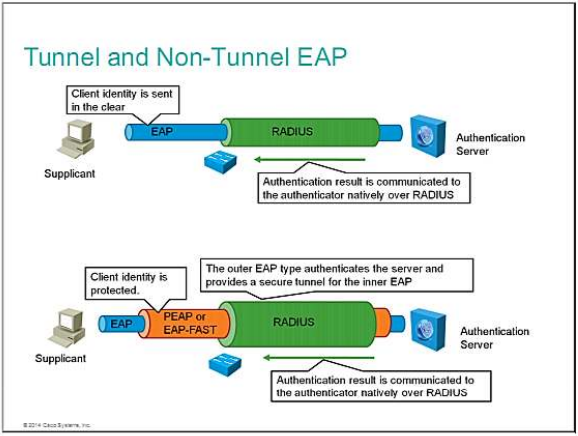
Protocols from the EAP family offload the authentication process from typical authenticators such as systems, applications, and network devices to EAP authentication servers. EAP introduces the philosophy that the supplicant should talk directly to the authentication server, with all intermediate devices acting only as relays. EAP provides two-way authentication between the client and the authentication server. Many authentication methods (some of them hybrid) are possible, and they support many types of credentials.

On the edge of the network, between the authenticating entity (the supplicant) and the authenticator (typically the edge network device), EAP is directly encapsulated in the LAN protocol using EAPOL encapsulation. Between the authenticator and the authentication server, EAP is encapsulated inside RADIUS, with the authenticator acting only as a relay between EAPOL and RADIUS EAP payloads. The result of the authentication process is communicated from the authentication server to the authenticator natively over RADIUS.

The main advantage of EAP is that it is extensible to implement almost arbitrary authentication processes. Furthermore, rather than requiring the authenticator (for example, a LAN switch) to be updated to support each new authentication method, EAP only requires that the authenticating entity (supplicant) and the authentication server speak the authentication protocol. Therefore, using EAP, the interoperability and compatibility of authentication methods becomes simpler.

Tunnel and Non-Tunnel EAP

This topic describes the tunneled and non-tunneled EAP.



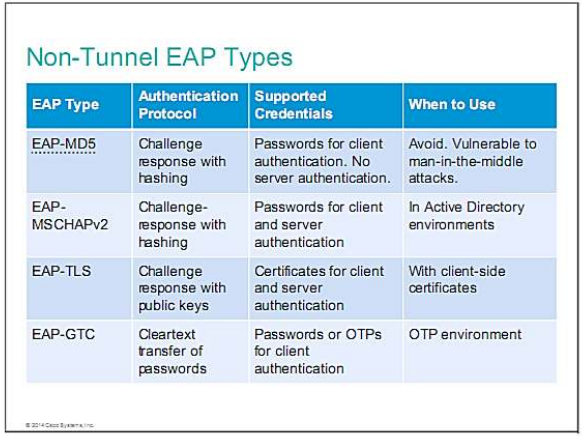
In the simple, non-tunnel EAP architecture a single EAP session exists between the supplicant and the authentication server. In this architecture, the supplicant sends its identity (name) in the clear to the authentication server. This is followed by an exchange that authenticates the authentication server to the user, and the user to the authentication server. If the user is successfully authenticated, the authentication server signals this to the authenticator via the RADIUS protocol. This mode is simple to understand, but has the limitation of transmitting the user identity (but not the credentials) in the clear. This limitation may not be considered a risk for many organizations. Transmitting the challenge-response authentication exchange in the clear can facilitate some passive dictionary attacks, if user passwords are weak. Also, these EAP architectures cannot easily support one-time passwords, because these passwords do not support challenge-response methods that are typically used inside the EAP authentication exchange.

To overcome these limitations, you can use a tunneled EAP architecture, in which an outer EAP encapsulates an inner EAP. The outer EAP provides server authentication, and a cryptographically secure tunnel for the inner EAP method to run in. Typical outer EAPs are PEAP and EAP-FAST. EAP-MSCHAPv2, EAP-TLS and EAP-GTC are commonly used for the inner EAP.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Non-Tunnel EAP Types

This topic describes the non-tunnel EAP types.



EAP has many variations that use different classes of authentication protocols and support different credentials. The most common non-tunneled EAP types are described below.

EAP-MD5: This EAP type is like CHAP and uses a challenge response mechanism with hashing. It only supports passwords as client credentials and does not authenticate the server, making it vulnerable to man-in-the-middle attacks. EAP-MD5 should be avoided, unless it is tunneled inside another EAP that authenticates the server (for example, PEAP).

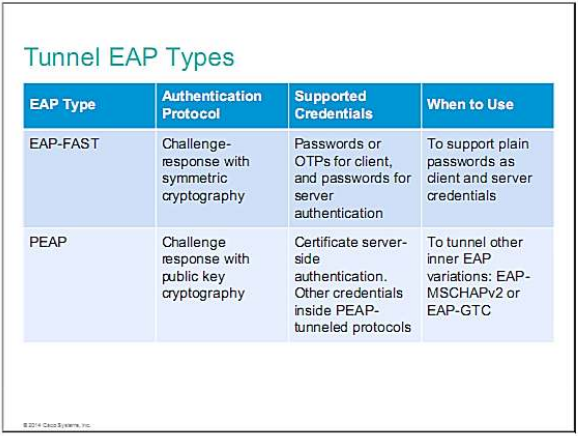
EAP-MSCHAPv2: This EAP type is like EAP-MD5 but provides bidirectional authentication. It supports passwords for both client and server credentials, and can also work with Microsoft password hashes instead of passwords, making it suitable for integration with Windows (domain) password databases. EAP-MSCHAPv2 is therefore recommended in authentication architectures that use plain passwords and can be deployed over untrusted channels.

EAP-TLS: This EAP type is a challenge-response method using public key cryptography. It supports public and private key pairs as client and server credentials. EAP-TLS requires a public key infrastructure (PKI) for public key (certificate) distribution.

EAP-GTC: This is a simple EAP type. It sends the cleartext password or one-time password to the authentication server. EAP-GTC is the only protocol that supports one-time passwords as client credentials, but should always be tunneled inside PEAP or EAP-FAST, which provide a secure communications channel.

Tunnel EAP Types

This topic describes the tunneled EAP types.



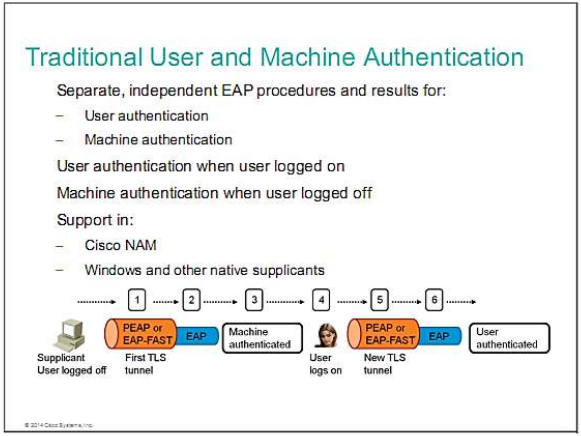
EAP-FAST: This EAP type is a tunneling protocol that can tunnel inner EAP varieties requiring a secure channel. EAP-FAST can use either passwords or a certificate to authenticate a server. It may require secure initial provisioning of server credentials (called the PAC) on clients. You will typically use EAP-FAST or EAP-TLS to tunnel EAP-MSCHAPv2 inside it, to provide identity protection, or to tunnel EAP-GTC inside it. This is particularly true if you need a single authentication protocol that does not require certificates for both your wired and wireless infrastructures.

PEAP: An EAP tunneling protocol that can tunnel inner EAP varieties requiring a secure channel. PEAP authenticates authentication servers using public and private key pairs. It requires administrators to provision the authentication server certificate or root CA certificate on clients. You will typically use PEAP to tunnel EAP-MSCHAPv2 or EAP-TLS inside it, to provide identity protection, or to tunnel EAP-GTC inside it.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Traditional User and Machine Authentication

This topic describes the user and machine authentication.

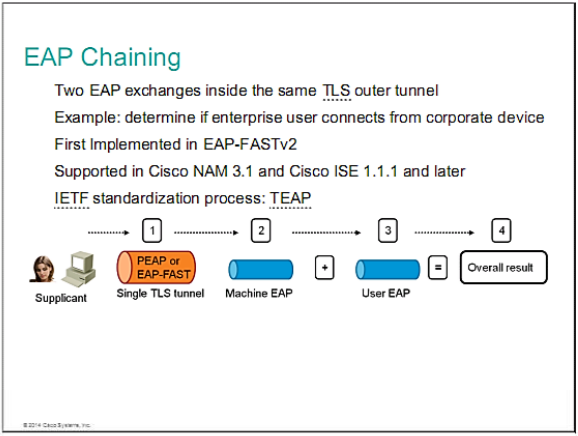


Traditional machine and user authentication works by treating the machine and user as two separate and independent entities. The user authentication is performed when the user logs on. When the user logs off, machine authentication is performed. This traditional philosophy does not have the intelligence of evaluating the user authentication in combination with the machine authentication.

The traditional user and machine authentication is supported by all common supplicants, including the AnyConnect supplicant - NAM, the Windows native supplicant, and other third party vendors.

EAP Chaining

This topic describes the EAP chaining.



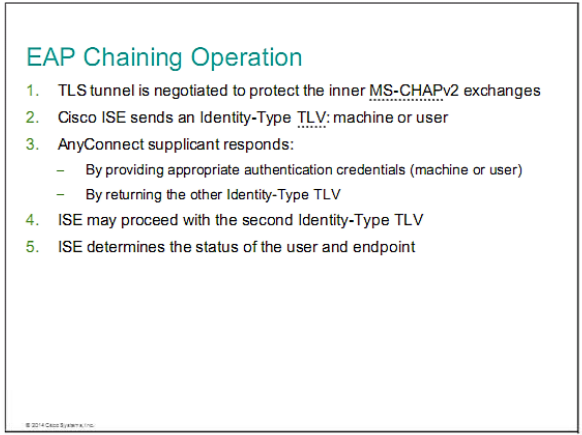
EAP chaining supports machine and user authentication but both authentications are performed inside a single outer TLS tunnel. EAP-FAST protocol is used to establish the outer tunnel and control the order of the inner exchanges. EAP chaining allows you to combine the results of the machine and user authentications into a single overall authentication result. Based on this information you can, for example, assign a the widest privilege set to enterprise users who connect from corporate-managed endpoints.

EAP chaining was first implemented in EAP-FASTv2. EAP-FASTv2 is a Cisco-engineered solution supported by Cisco Network Access Manager 3.1 and Cisco Identity Services Engine 1.1.1 and later. The IETF is working on the standards-based equivalent, TEAP.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

EAP Chaining Operation

This topic describes the EAP chaining operation.



EAP-FAST authentication occurs in two phases. In the first phase EAP-FAST employs a TLS handshake to provide and authenticate key exchanges using TLV objects to establish a protected tunnel. These TLV objects are used to convey authentication related data between the client and server. Once the tunnel is established, the second phase begins with the client and Cisco Identity Services Engine node engaging in further conversations to establish the required authentication and authorization policies. EAP Chaining employs an optional Identity-Type TLV at the start of the second phase of EAP-FAST authentication.

When the secure TLS tunnel has been established, the general EAP chaining flow is based on a request/response exchange:

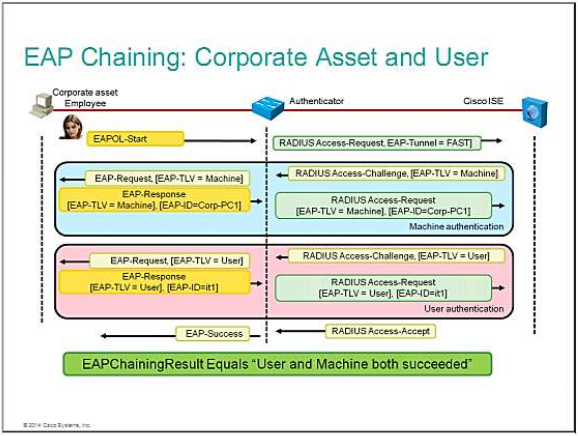
The ISE server sends the optional Identity-Type TLV, machine or user, and request identity to the client.

The client responds back with either the same Identity-Type TLV, or proposes another identity-type.

This exchange will be demonstrated in several deployment scenarios.

EAP Chaining: Corporate Asset and User

This topic describes the EAP chaining flow with corporate asset and user.



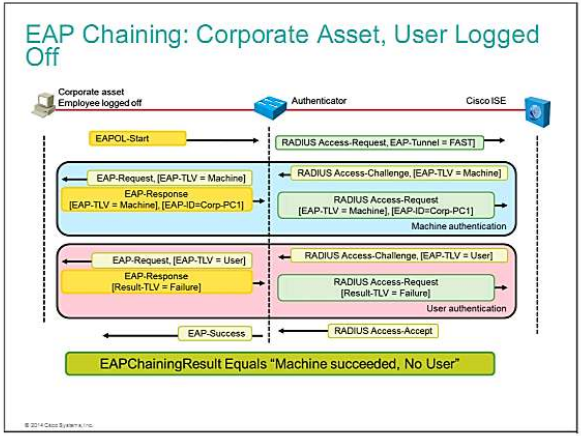
This diagram illustrates the EAP chaining flow when a enterprise user attempts access from a corporate-managed endpoint.

When the TLS tunnel is successfully negotiated, the Cisco Identity Services Engine sends an Identity-Type TLV of type "Machine". Next, the ISE server will recognize whether the client supports EAP Chaining by analyzing the response to the Identity-Type TLV request. If the response contains a matching Identity-Type TLV then the client supports EAP Chaining. In this example, the client matches both Machine and User Identity-Type TLV requests deeming it as a corporate device. The result as presented by the ISE will be described by the expression "EAPChainingResult Equals User and Machine both succeeded".

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

EAP Chaining: Corporate Asset, User Logged Off

This topic describes the EAP chaining flow with corporate asset and user logged off.

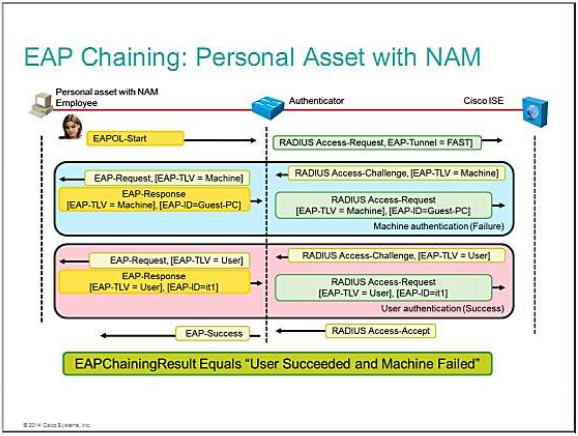


This diagram illustrates the EAP chaining flow when a corporate-managed endpoint is connected to the network and the user is logged off.

In the EAP exchange for user authentication, the supplicant returns the Result-TLV set to "Failure". This result allows the Cisco Identity Services Engine to accept the access request as a successful machine authentication with no user access.

EAP Chaining: Personal Asset with NAM

This topic describes the EAP chaining flow with personal asset running the AnyConnect supplicant.



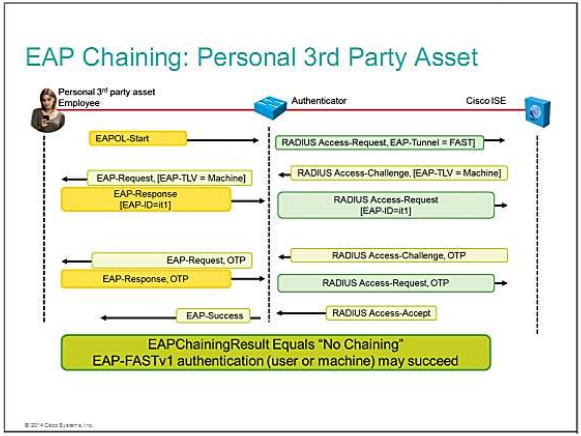
This diagram illustrates the EAP chaining flow when an enterprise user connects from personal asset running the AnyConnect supplicant.

In this example, the client does not match the server's Machine Identity-Type TLV request, since this device is not enrolled in the corporate domain. Authentication continues and matches on the server's User Identity-Type TLV request, thus deeming it as a non-corporate device. The user authentication is successful. The result presented by the Cisco Identity Services Engine will be "EAPChainingResult Equals User Succeeded and Machine Failed".

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

EAP Chaining: Personal 3rd Party Asset

This topic describes the EAP chaining flow with personal asset running a third party supplicant.

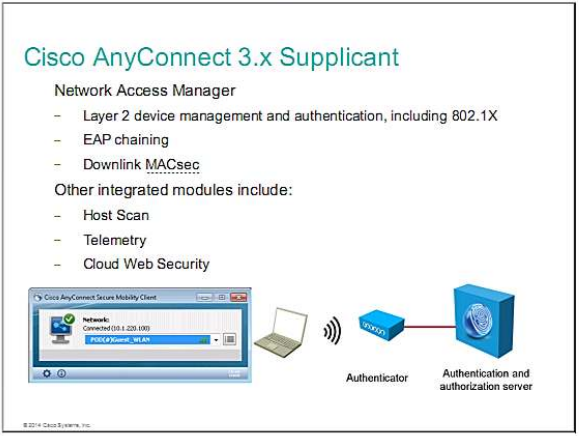


This diagram illustrates the EAP chaining flow when an enterprise user connects from personal asset running a third party supplicant.

If there is no Identity-Type TLV in the response then EAP Chaining is not supported by the client. Normal processing for existing EAP-FASTv1 implementation applies. In this example, the client, being an Android tablet, does not support EAP Chaining and continues with EAP-FAST authentication, deeming this as a non-corporate device. The result presented by the Cisco Identity Services Engine will be "EAPChainingResult Equals No Chaining". The user or machine authentication may succeed using the traditional EAP-FASTv2 method. Depending on the ISE policy, appropriate access privileges will be assigned to the endpoint.

Cisco AnyConnect 3.x Supplicant

This topic describes the Cisco AnyConnect 3.x Supplicant



The Cisco AnyConnect Secure Mobility client is the next-generation VPN client that, starting in version 3.0, integrates several modules of special interest to Cisco Identity Services Engine. The key component is the Network Access Manager. It provides Layer 2 device management and authentication for access to both wired and wireless networks. This functionality includes the 802.1X supplicant and offers support for downlink MACsec. Downlink MACsec offers Layer 2 encryption of traffic between the AnyConnect endpoint and the adjacent switch.

Other integrated modules include:

Host Scan—Provides the AnyConnect Secure Mobility Client the ability to identify the operating system, antivirus, antispyware, and firewall software installed on the host prior to creating a remote access connection to the Cisco Adaptive Security Appliance. Based on this prelogin evaluation, you can control which hosts are allowed to create a remote access connection to the security appliance. The Host Scan application is delivered with the posture module and is the application that gathers this information.

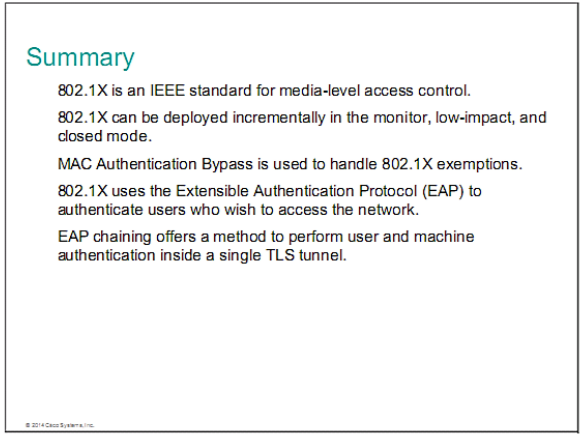
Telemetry—Sends information about the origin of malicious content detected by the antivirus software to the web filtering infrastructure, which uses this data to provide better URL filtering rules.

Cloud Web Security—Routes HTTP and HTTPS traffic to the Cloud Web Security scanning proxy server for content analysis, detection of malware, and administration of acceptable use policies.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Summary

This topic summarizes the key points that were discussed in this lesson.



https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Lesson 3

Identity System Quick Start

There is a great deal of complexity in a full secure access solution. This lesson is intended to provide details on the minimum configuration necessary to quickly get an IEEE 802.1X environment running in monitor mode using the native Windows supplicant, a Cisco switch as the authenticator and Cisco Identity Services Engine as the authentication server. It describes how to configure the Cisco switch for AAA, RADIUS and 802.1X. It describes the configuration of local users and network access devices in Cisco Identity Services Engine. It also explores the default authentication policy in Cisco ISE. IEEE 802.1X monitor mode. It will be up to other lessons to build upon the base that is provided in this lesson.

Upon completing this lesson, you will be able to meet these objectives:

- Describe the logging into the ISE
- Describe the organization of the Cisco ISE GUI
- Describe how to use the internal user database on the Cisco Identity Services Engine
- Describe the NADs
- Describe the default authentication policy on Cisco Identity Services Engine
- Describe the 802.1X authenticator configuration procedure
- Describe the the global AAA settings
- Describe how to configure the RADIUS peering
- Configure the 802.1X global and port settings for monitor mode
- Describe the 802.1X Windows native supplicant
- Describe how to verify authentication on the Cisco Identity Services Engine
- Describe how to verify the authentication status on the switch

https://t.me/learningnets

Logging in to Cisco ISE

This topic describes how to log in to the Cisco Identity Services Engine GUI.



The GUI is the primary configuration and administration method for Cisco ISE. You access the Cisco ISE GUI from a web browser by connecting to the Cisco ISE via HTTPS.

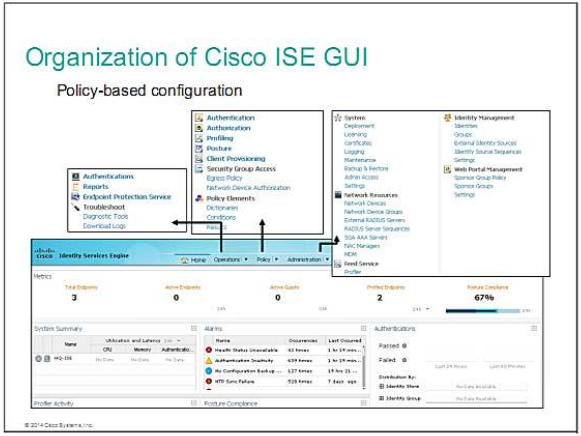
Prior to the first login to the GUI, Cisco ISE must have its base configuration set from the CLI. There is a setup script which walks the administrator through the process. The script prompts for settings such as hostname, domain name, IP address, default gateway, DNS server and NTP server. The setup script also prompts for administrator credentials which will be used for future logins to the CLI and to the GUI.

It must be noted that there are separate administrator accounts for the CLI and for the GUI. The setup script will define two accounts with identical credentials. However, any changes to either account after this assignment are not automatically reflected in the other account. To keep the credentials synchronized requires changing the credentials in both the CLI and the GUI.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Organization of Cisco ISE GUI

This topic describes the organization of the Cisco Identity Services Engine GUI.



The four main tabs are:

Home—Provides a dashboard populated with customizable dashlets that allow you to view important system health and operational status at a glance.

Operations—Provides a list of various monitoring, reporting and troubleshooting tools

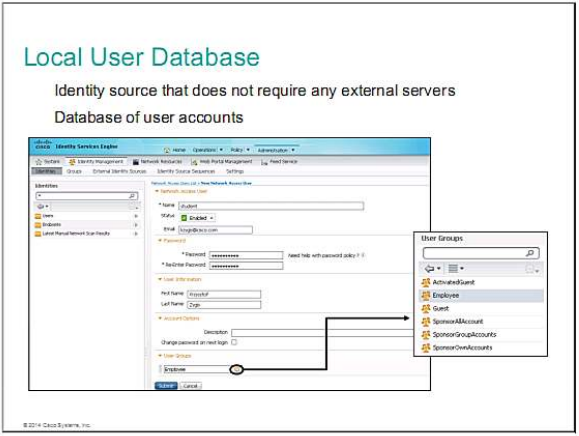
Policy—Provides the configuration point to Cisco ISE's policy oriented features such as authentication, authorization, profiling and posture.

Administration—Provides the configuration point to Cisco ISE's deployment-relevant parameters.

https://t.me/learningnets

Local User Database

This topic describes how to use the internal user database on the Cisco Identity Services Engine.



The internal user database offers a simple way to provision users and endpoints locally on the Cisco ISE. This approach does not require any external servers and is thus applicable to test beds, temporary installations, and very small deployments.

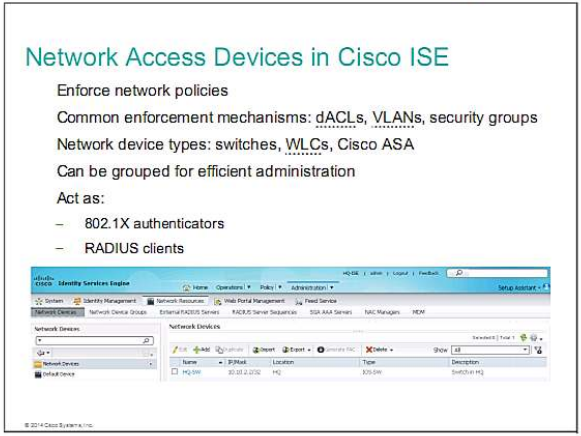
For easier management of user accounts, assign users to user groups. User accounts have a set of attributes. Password is a mandatory attribute of an internal Cisco ISE user.

Note, some protocols, such as EAP- TLS and PEAP-TLS, do not use password-based authentication. The internal database does not support the use of these protocols.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Network Access Devices in Cisco ISE

This topic describes the role of NADs in a Cisco Identity Services Engine deployment.



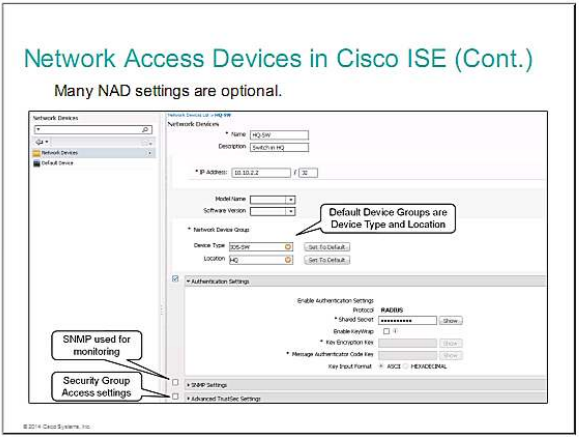
NADs are RADIUS clients and Cisco Identity Services Engine is their RADIUS server. They perform the role of authenticators in an 802.1X environment. They must act as the proxy between the supplicant on the endpoint and Cisco ISE as the authentication server. They are also responsible for enforcing the authorization policy as specified by Cisco ISE.

Cisco ISE decides whether the client traffic should be permitted into the enterprise network and which enforcement mechanisms should be applied. The ISE communicates the decision to the NAD. The NAD is directly responsible for implementing the enforcement options. Common enforcement options include:

- VLAN assignment
- dACLs
- Security group tags

Basic NAD types include the following:

- LAN switches
- WLCs
- Adaptive security appliances



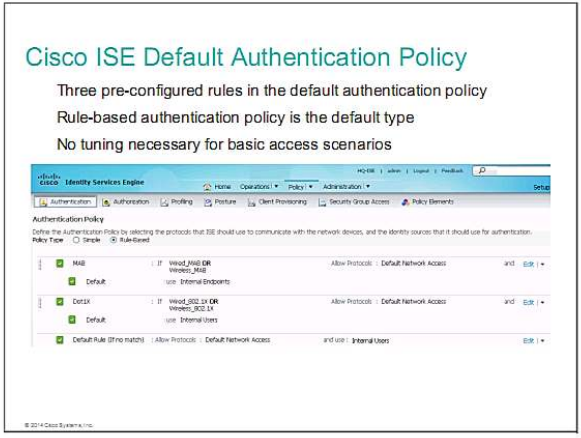
The device name, IP address and network device group settings are required settings for NADs in Cisco ISE. Many settings, such as SNMP, or Security Group Access parameters (in the figure referred to as TrustSec) are optional, and will be used when the enterprise scenario demands it.

Network Device Groups are useful for organizing and selecting devices. By default, Cisco ISE utilizes two device group hierarchies: Device Type and Location. Other hierarchies can be defined. For example, in an enterprise environment using a phased roll out, a parent group named Stage with child groups Monitor Mode, Low Impact Mode and Closed Mode might be defined.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Cisco ISE Default Authentication Policy

This topic describes the default authentication policy on Cisco Identity Services Engine.



Authentication requests are processed immediately after an endpoint attempts to access the network through the NAD. The Cisco ISE evaluates the access path over which the endpoint enters the network and checks the credentials that are stored in the identity source.

The Cisco ISE has an authentication policy that gathers multiple checks into a centralized decision point. The authentication policy contains criteria that define how to validate the user identity and through which NADs the user is allowed to enter. The validation of the user identity is performed against an identity source. The identity source can be the internal database, an external server, or a sequence of multiple sources.

Authentication policies define the protocols that Cisco ISE should use to communicate with the network devices, and the identity sources that it should use for authentication. A policy is a set of conditions and a result.

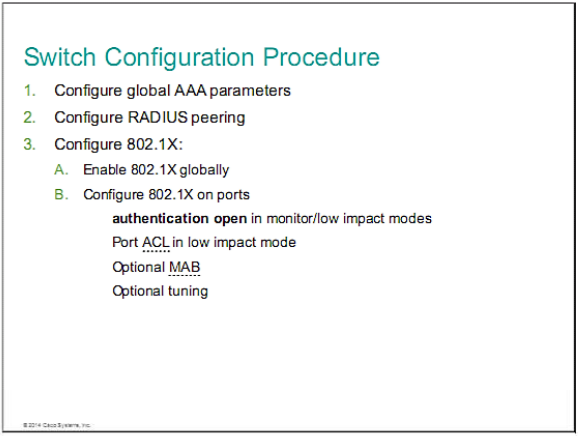
Two types of authentication policies are available in the Cisco ISE: simple and rule-based authentication. Simple authentication does not use any conditions and is not commonly used. Rule-based authentication consists of a set of rules, and each rule can define conditions and resulting actions. Rule-based authentication is the default and more commonly used option.

The ISE comes with three authentication rules preconfigured by default. You do not need to tune the policy for most basic access scenarios.

https://t.me/learningnets

Switch Configuration Procedure

This topic describes the switch configuration procedure.



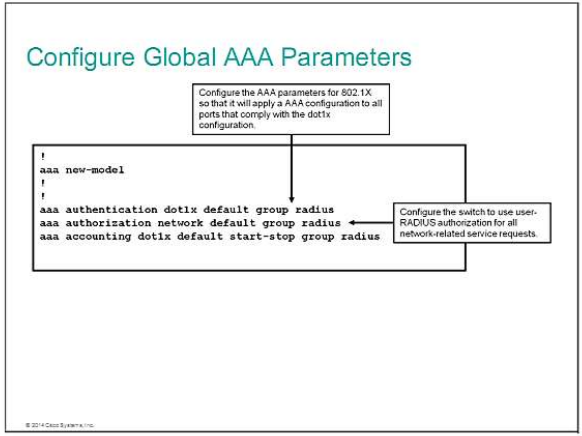
To deploy 802.1X on wired switches, perform these steps:

1. Configure the global AAA parameters.
2. Configure RADIUS association.
3. Configure 802.1X. The 802.1X settings on the switch consist of the command that globally enables 802.1X on the device, and the configuration of individual ports.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Configure Global AAA Parameters

This topic describes how to configure the global AAA settings.



Before you can configure AAA authentication, authorization and accounting, AAA must be globally enabled on the switch. Use the **aaa new-model** command in global configuration mode to do this.

AAA servers can be logically organized into AAA server groups. Group radius is an AAA server group that is defined by default and includes all of the RADIUS servers that are configured on the switch. It is very common to simply reference the group radius in AAA configuration commands.

Use the **aaa authentication dot1x default group radius** command in global configuration mode to define the authentication method used by default on switchports that are configured for 802.1X access.

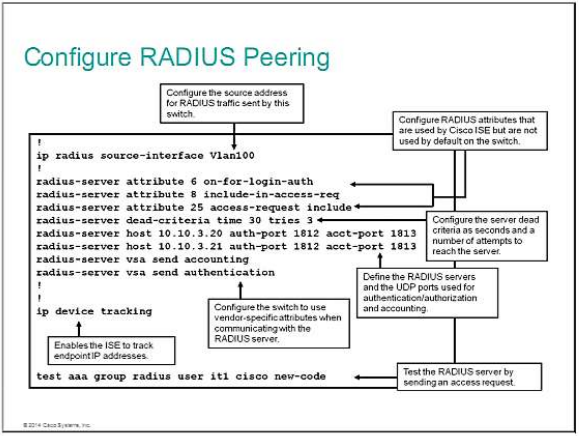
Configure the default AAA authorization method used for network access by issuing the **aaa authorization network default group radius** command in global configuration mode. This command is used to configure the switch to facilitate RADIUS authorization for all network-related service requests, such as 802.1X per-user ACLs or VLAN assignment.

Configure default AAA accounting method used with 802.1X by issuing the **aaa accounting dot1x default start-stop group radius** command in global configuration mode. This command will cause the switch to send RADIUS accounting messages when sessions start and when sessions terminate.

Note that all of the commands shown in this scenario reference the method named default. The method named default indicates the method that will be used if no specific method is configured on an interface or line or service. In more complex scenarios it may be required to configure multiple named methods and reference the named method in appropriate sections of the configuration.

Configure RADIUS Peering

This topic describes how to configure the RADIUS peering.



Configure the RADIUS server using the **radius-server host** *<host>* **auth-port** *<port>* **acct-port** *<port>* command in global configuration mode. By default, the ports that are used for the Cisco Identity Services Engine should be 1812 for authentication and authorization and 1813 for accounting.

Configure the interface from which all RADIUS traffic will be sourced by issuing the **ip radius source-interface** *<interface>* command in global configuration mode. This command will cause all RADIUS traffic to be sourced from the same interface. If the switch consistently uses the same source interface, then the RADIUS can use the traffic's source IP address to easily the switch as the source. The IP address of the source interface is the IP address that should be configured for the NAD in ISE.

Configure the RADIUS server dead criteria by issuing the **radius-server dead-criteria** command in global configuration mode. This command has two primary components:

Time: Set the time in seconds during which the switch does not need to get a valid response from the RADIUS server. The range is from 1 to 120 seconds.

Tries: Set the number of times that the switch does not get a valid response from the RADIUS server before the server is considered unavailable. The range is from 1 to 100.

Not all RADIUS attributes are used in all RADIUS servers in all scenarios. There are some attributes that ISE uses in an 802.1X environment that are not enabled on the switch by default. Configure these RADIUS attributes using the following commands in global configuration mode:

radius-server attribute 6 on-for-login-auth: This command sends the Service Type attribute in the authentication requests. ISE uses the service-type to help distinguish between 802.1X supplicant login requests and MAC Authentication Bypass requests.

radius-server attribute 8 include-in-access-req: This command causes the switch to include the endpoint IP address in the authentication request. The IP address is carried in the Framed-IP-Address RADIUS field.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

radius-server attribute 25 access-request include: This command causes the switch to include the RADIUS Class attribute in the authentication request. This specifies the group of which the user is a member.

radius-server vsa send accounting: This command configures the switch to include vendor-specific attributes in accounting updates.

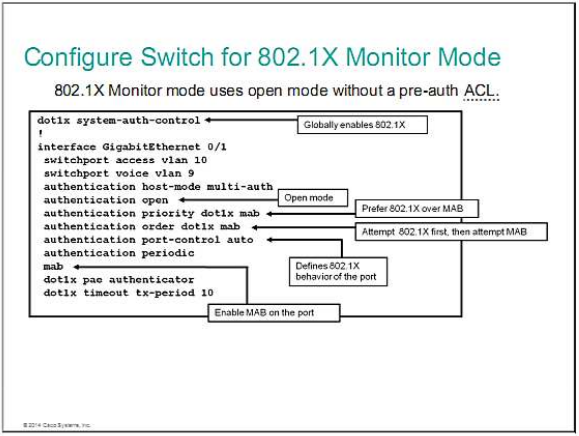
radius-server vsa send authentication: This command configures the switch to include vendor-specific attributes in authentication requests.

The **ip device tracking** command enables the switch to keep a table of source IP addresses utilizing the switchports. The IP addresses will be included in RADIUS authentication requests as long as RADIUS attribute 6 is enabled.

https://t.me/learningnets

Configure Switch for 802.1X Monitor Mode

This topic describes how to configure the switch for 802.1X monitor mode.



Before 802.1X can function on any particular switch port, it must be globally enabled on the switch. This is done in global configuration mode using the **dot1x system-auth-control** configuration command.

Enter interface configuration mode using the **interface** command to configure port-specific settings. Configure the switch port for the correct VLANs by issuing **switchport** commands.

Configure the switch to allow network traffic to the locally assigned VLAN before 802.1X authentication has taken place by issuing the **authentication open** command in interface configuration mode. By default, 802.1X drops all non-EAPOL traffic before a successful 802.1X (or MAB) authentication or web authorization initialization. This mode is referred to as closed mode. The **authentication open** command enables open-access mode, which allows traffic (in both the data and voice VLANs), before successful authentication. If that traffic is not restricted by an ACL locally assigned to the port, it is considered monitor mode. If a locally assigned ACL is in place, limiting the traffic that is allowed before authentication, then it is considered low impact mode.

You may enable MAB on the desired port by issuing the **mab** command in interface configuration mode.

Configure the authentication priority using the **authentication priority** command in interface configuration mode. It is best practice to prefer the stronger authentication method (802.1X), as depicted above.

You may configure the authentication order for the port by issuing the **authentication order** command in interface configuration mode. It is usually the best practice to maintain the order of 802.1X followed by MAB, as depicted above. But in unusual environments which predominantly use MAB, a performance improvement may be seen if the order is reversed.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

The port starts in the unauthorized state. While the port is in this state, the port that is not configured as a voice VLAN port disallows all ingress and egress traffic except for 802.1X, Cisco Discovery Protocol, and STP packets. When a client is successfully authenticated, the port changes to the authorized state and allows all traffic for the client to flow normally. If the port is configured as a voice VLAN port, the port allows VoIP traffic and 802.1X protocol packets before the client is successfully authenticated. If a client that does not support 802.1X connects to an unauthorized 802.1X port, the switch requests the identity of the client. In this situation, if the client does not respond to the request, the port remains in the unauthorized state, and the client is not granted access to the network.

In contrast, when an 802.1X-enabled client connects to a port that is not running the 802.1X standard, the client initiates the authentication process by sending the EAPOL start frame. When no response is received, the client repeats the request for a fixed number of times. Because no response is received, the client begins sending frames as if the port was in the authorized state. You control the port authorization state by using the **dot1x port-control** interface configuration command and these keywords:

force-authorized: This keyword disables 802.1X authentication and causes the port to change to the authorized state without any authentication exchange required. The port sends and receives normal traffic without 802.1X-based authentication of the client. This setting is the default setting.

force-unauthorized: This keyword causes the port to remain in the unauthorized state, and ignore all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the port.

auto: This keyword enables 802.1X authentication and causes the port to begin in the unauthorized state, allowing the processing of EAPOL frames that are sent and received through the port. The authentication process begins when the link state of the port changes from down to up or when an EAPOL start frame is received. The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each client that attempts to access the network is uniquely identified by the switch using the MAC address of the client.

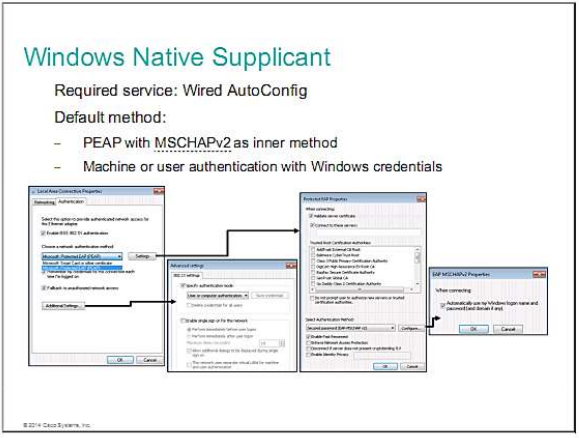
If the client is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated client are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the switch can resend the request. If no response is received from the server after the specified number of attempts, authentication fails and network access is not granted.

When a client logs off, it sends an EAPOL logoff message, causing the switch port to change to the unauthorized state. The port will also change to the unauthorized state if the link state of a port changes from up to down.

https://t.me/learningnets

Windows Native Supplicant

This topic describes the 802.1X Windows native supplicant.



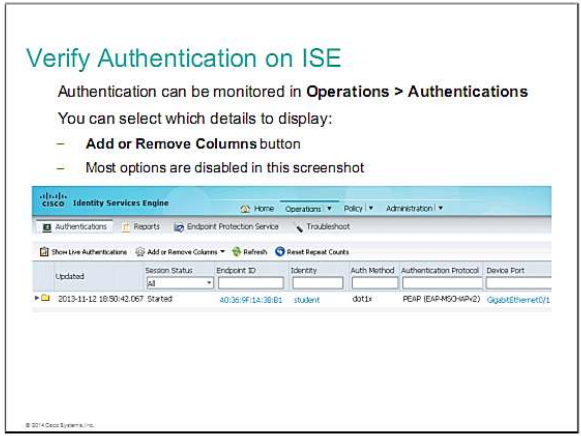
Windows operating systems include a native 802.1X supplicant that is disabled by default. Within an organization, the service is often enabled by Active Directory group policies. You can enable it manually by starting the Wired AutoConfig service. The native supplicant supports PEAP and EAP-GTC.

By default the supplicant uses PEAP with EAP-MSCHAPv2 as the inner authentication method, and is configured for machine or user authentication. If a user is logged in, it will use the user credentials. If no user is logged in and it is a member of AD it will use the machine credentials. Machine credentials are available only after the machine joins the Active Directory. The credentials are provisioned on AD members by the AD controller at the time of joining.

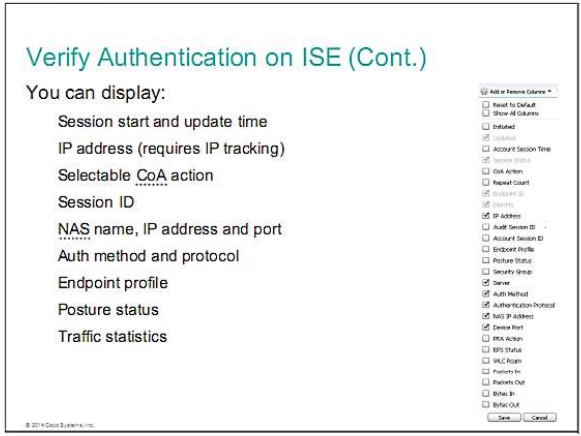
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Verify Authentication on ISE

This topic describes how to verify authentication on the Cisco Identity Services Engine.



The Cisco ISE dashboard provides a summary of all authentications that take place in your network in the **Operations > Authentication** menu. The information displays also the authentication method, session ID and other details. You can select which fields are displayed on this page through the **Add or Remove Columns** button. This screenshot displays only a few of the fields to improve the readability.

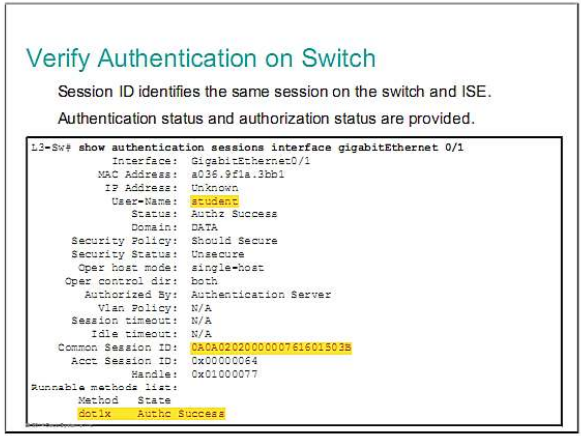


When you click the **Add or Remove Columns** button you will be able to select various details about the access attempt. You need to to save the selection to be effective.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Verify Authentication on Switch

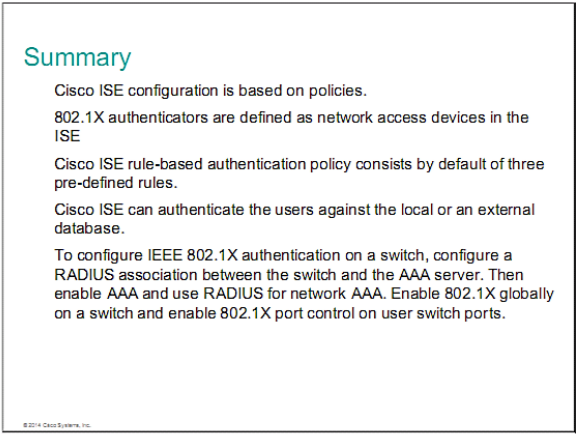
This topic describes how to verify the authentication status on the switch.



In addition to viewing them on the Cisco Identity Services Engine, you may monitor the authentication results on the NADs. The output of the **show authentication session interface** command provides very detailed specifications of authentication and authorization status. It includes the username of the authenticated user, as well as the authentication status, operational status and the authorization policies that have been applied. The common session ID is a unique identifier which is used as a key field to keep the representation of the session synchronized between ISE and the switch. The common session ID can be very useful when troubleshooting 802.1X environments. The session ID can be viewed using additional commands, such as the **show authentication interface** command.

Summary

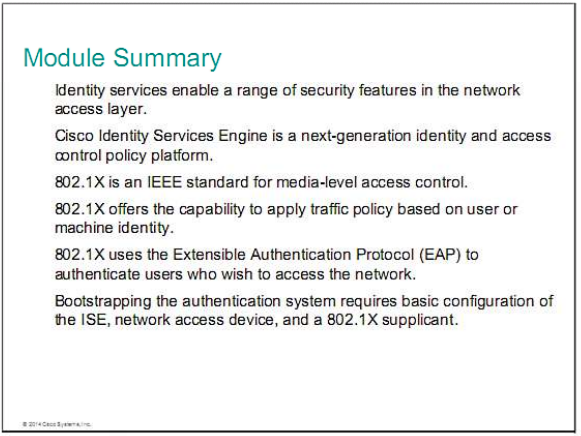
This topic summarizes the key points that were discussed in this lesson.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Module Summary

This topic summarizes the key points that were discussed in this module.



References

For additional information refer to this resource:

Cisco Identity Services Engine User Guide

https://t.me/learningnets

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Module Self-Check

Questions

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

1. Which two are components of the Cisco secure access solution? (Choose two.) (Source: Identity Services)

   A. stateful firewalling
   B. posture service
   C. application layer gateways
   D. TLS encryption
   E. SGA

2. Which two functions leverage CoA? (Choose two.) (Source: Identity Services)

   A. RADIUS
   B. authentication
   C. posture
   D. accounting
   E. profiling

3. What is a benefit of TACACS+ over RADIUS? (Source: Identity Services)

   A. Developed by Cisco
   B. Standards-based protocol
   C. Granular authorization allows command authorization
   D. Granular authorization allows CoA
   E. Granular accounting allows recording of session termination

https://t.me/learningnets

4. Which 802.1X host mode distinguishes between multiple authenticated 802.1X, MAB, or web authorization clients on the data VLAN? (Source: 802.1X and EAP)

   A. Single Host Mode
   B. Multiple Authentication Mode
   C. Multiple Domain Authentication Mode
   D. Multiple Host Mode

5. Which two EAP methods use certificate-based server-side authentication? (Source: 802.1X and EAP)

   A. PEAP
   B. EAP-MD5
   C. EAP-TLS
   D. EAP-MSCHAPv2
   E. EAP-GTC

6. Which EAP method can return the EAP Chaining Result of "User and Machine both succeeded"? (Source: 802.1X and EAP)

   A. EAP-FASTv1
   B. EAP-FASTv2
   C. EAP-TLS
   D. EAP-PEAP
   E. EAP Chaining method

7. Which 802.1X deployment mode(s) do you configure using the **authentication open** command? (Source: Identity System Quick Start)

   A. Open
   B. Low-impact
   C. Monitor
   D. Monitor and low-impact
   E. Low-impact and closed

8. Which two commands do you need to enable the 802.1X supplicant on a switch? (Source: Identity System Quick Start)

   A. aaa authentication dot1x
   B. aaa authentication network
   C. aaa authorization dot1x
   D. aaa authorization network
   E. aaa authorization exec

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

9. Which two statements describe PEAP (EAP-MSCHAPv2)? (Source: Identity System Quick Start)

A. Rarely deployed
B. Default method in the AnyConnect supplicant
C. Use of certificate(s)
D. Engineered by Cisco
E. Inner EAP-MSCHAPv2 exchange protected by TLS

https://t.me/learningnets

Answer Key

1. B, E
2. C, E
3. C
4. B
5. A, C
6. B
7. D
8. A, D
9. C, E

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Module 2

Cisco ISE Fundamentals

The Cisco Identity Services Engine is a next-generation identity and access control policy platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations. The unique architecture of Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices. This module introduces the key components of the Cisco ISE architecture and explains the its function in the network access control solution.

Upon completing this module, you will be able to:

- Describe the key characteristics of Cisco ISE
- Enroll the Cisco ISE in the PKI
- Implement Cisco ISE internal authentication
- Implement Cisco ISE external authentication

https://t.me/learningnets

https://t.me/learningnets

Lesson 1

Cisco ISE Overview

Overview

This lesson provides an overview of the Cisco Identity Services Engine platform. Cisco ISE is a key component of the Cisco secure access architecture. The various concepts that are associated with the Cisco ISE deployment include nodes, personas, and roles. The Cisco ISE solution supports distributed deployments, where the functions are split among separate nodes.

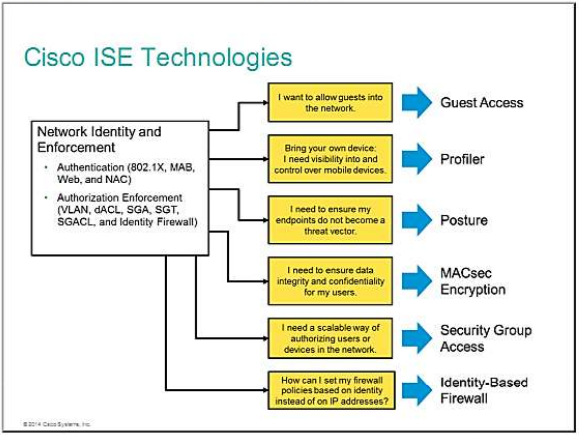
Upon completing this lesson, you will be able to meet the following objectives:

- Identify the Cisco ISE technology areas
- List the access control operational components
- Describe the ISE as a policy platform
- Describe the Cisco ISE high-level flow
- Describe Cisco ISE nodes, personas, and roles
- Describe the Cisco ISE deployment examples

https://t.me/learningnets

Cisco ISE Technologies

This topic describes the Cisco secure access technology areas.



The Cisco secure access solution is deployed in enterprise environments with various security technologies. The Cisco Identity Services Engine offers, among others, these services:

Authentication (IEEE 802.1X, MAB, WebAuth)

Authorization (VLAN, dACL, SXP or SGT, SGACL, identity-based firewall)

The guest access feature enables rich options for provisioning and profiling of guest accounts.

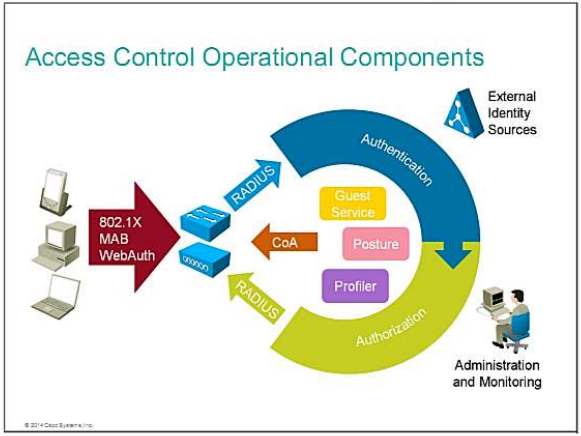
The endpoint profiling service dynamically identifies endpoint devices. It manages these devices intelligently, based on predefined security policies. The profiling service allows you to identify, manage, and inventory all of the IP-enabled devices accessing the network. The posture function verifies endpoint compliance with the governing security policy. Hop-by-hop encryption is accomplished via MACsec.

Cisco Security Group Access establishes clouds of trusted networks to build secure networks. Instead of relying on IP-based configuration, access authorization is based on context, including user identity.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Cisco ISE Operational Components

This topic identifies the Cisco Identity Services Engine operational components.



The key operational components of the access control work together to provide a comprehensive solution. The central decision-making platform, the Cisco Identity Services Engine utilizes standards-based RADIUS for authentication and authorization functions. Authentication processes are carried out from the endpoints through the NADs to Cisco ISE using 802.1X, MAB, or WebAuth. 802.1X is a standards-based network access control that works at Layer 2. MAB is used as an exception to authentication to allow devices that do not have an 802.1X supplicant (such as a security camera or a printer) to access the network based on their MAC address. WebAuth allows users to log in via standard web browsers and is generally deployed for guest logins or to support endpoints that lack an 802.1X supplicant.

User credentials are passed from the NAD to Cisco ISE via a RADIUS Access-Request message. Cisco ISE generally consults an external identity source, such as Microsoft Active Directory or LDAP, for credential verification and for user and group attributes. For guest users who do not have accounts within the external identity sources, Cisco ISE provides guest service features that allow for the management of the life cycle of guest accounts.

After the user identity is verified and its account attributes are processed, an appropriate authorization profile can be applied to its session. Cisco ISE conveys the associated authorization policy to the NAD in a RADIUS Access-Accept reply.

The Cisco ISE posture service allows characteristics of the physical endpoint security posture to be interrogated. For example, operating system service packs and antivirus software status can be examined. The Cisco ISE profiler service can use several probe methodologies to collect many endpoint characteristics. These characteristics are then used to categorize the device into classification groups such as Apple devices or iPhone or iPad.

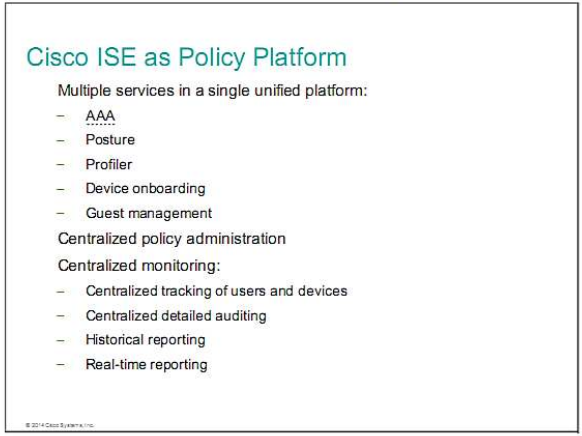
Profile and posture information can be used to determine the authorization policy. Utilization of this information generally relies on the CoA mechanism. CoA is a standards-based method that allows the RADIUS server to send authorization updates to the RADIUS client (the NAD) after the initial authentication and authorization exchange.

Administration and monitoring of all Cisco ISE components, even when the deployment is distributed, is accomplished via a web browser connection to a single centralized interface.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Cisco ISE as Policy Platform

This topic identifies the policy-centric Cisco Identity Services Engine architecture.



A policy-based networking approach helps IT staff to accomplish business goals. For example, they may give authorized users access to sensitive data when they are in certain locations or using specific devices, while restricting access from other locations or from other devices. For a more precise example, a policy might permit a finance manager to access data from anywhere using a company laptop, but restrict access to a specific resource from a personal device outside the office.

A policy is broadly defined as "a definite course or method of action, to guide and determine both present and future decisions."

Allows enterprises to authenticate and authorize users and endpoints through wired, wireless, and VPN networks.

Provides complete guest life-cycle management services.

Enables the ability to discover, classify, and associate identity for all endpoints connecting to the network.

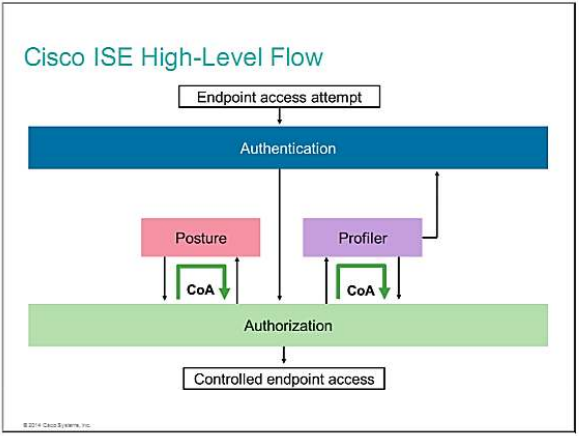
Performs device onboarding, which is used to install required client software on the user endpoints. Examples include supplicants, NAC agents, and other packages.

Enforces security policies by blocking, isolating, and repairing noncompliant machines in a quarantine area without needing administrator attention.

Offers a built-in monitoring, reporting, and troubleshooting console for helpdesk operators and administrators.

Cisco ISE High-Level Flow

This topic presents the high-level flow in Cisco Identity Services Engine processing.



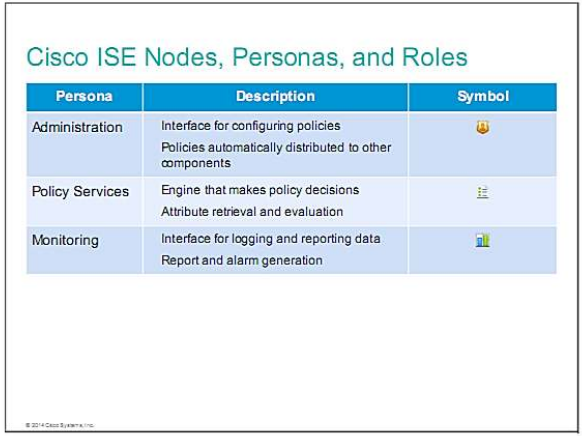
The diagram depicts the general flow of Cisco ISE policy decisions:

1. The endpoint attempts network access via a NAD.
2. Using 802.1X, MAB, or WebAuth, the authentication process ensues.
3. Based on the characteristics of the authentication process, an authorization policy is selected and communicated to the NAD, leading to controlled endpoint access.
4. If posturing services are deployed, the authorization profile that is selected immediately after authentication does not normally provide full network access. Instead, it is normally restricted to allow connectivity only to the Cisco ISE components that are required for posture assessment and potentially to remediation servers. Posture assessment can then begin. If the endpoint is determined to be compliant with the organization security policy, then a more permissive authorization policy can be assigned to the session. To convey the change in policy to the NAD, a CoA message is sent.
5. Similarly, profiler services also make use of CoA. If a profiler is deployed, and a new endpoint connects for the first time, the authorization profile will be one that is associated with unknown devices. After profiling is completed and the endpoint classification is identified, a new authorization policy can be assigned to the session. The new authorization policy is communicated to the NAD using a CoA message.
6. The results of profiler probes are stored in the Cisco ISE internal endpoint database. The endpoint MAC address is the key field in the database entry and uniquely identifies the endpoint. On subsequent access attempts from this endpoint, the endpoint classification from the last profiler update is available as additional context for the initial authorization assignment decision.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Cisco ISE Personas

This topic explains the concepts of Cisco Identity Services Engine nodes, personas, and roles.



A Cisco ISE node is a running installation of the Cisco ISE software. This installation can be on a physical appliance or on a VM within a VMware environment. THe Cisco ISE architecture allows for the separation of services for scalability, performance and high availability. Cisco ISE has three major collections services that are organized into personas. These personas are responsible for different functions within the Cisco ISE architecture. They may be collocated on a single node or distributed across multiple nodes. The three personas are:

Administration persona: This persona is the interface for configuring policies. This persona is the control center in the Cisco ISE deployment, and it also controls the licensing and contains the user interface. The administration persona is also responsible for pushing the configurations out to other nodes in a distributed deployment. Nodes that implement the administration persona are often referred to as admin nodes.

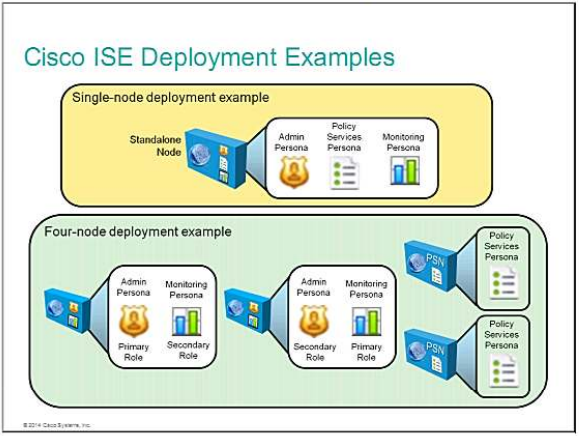
Policy service persona: This persona is the engine that makes policy decisions. This persona is the main runtime engine that processes all the network messaging that pertains to the Cisco ISE deployment. This massaging includes DHCP, Cisco Discovery Protocol, NetFlow, and RADIUS, among others. Nodes that implement the policy service persona are often referred to as policy service nodes.

Monitoring persona: This persona is the interface for logging and report data. This engine collects all logs and correlates them. In addition, it is used to generate reports and any alarms for the Cisco ISE system. Nodes that implement the monitoring persona are often referred to as monitoring nodes.

https://t.me/learningnets

Cisco ISE Deployment Examples

This topic explains the concepts of Cisco Identity Services Engine nodes, personas, and roles.



In the figure, the first example shows a single-node deployment. The initial state of a Cisco ISE node, immediately after installation, is standalone mode. In this mode, all three running personas are collocated on a single Cisco ISE node. A chief limitation of this deployment model is a lack of fault tolerance. There are also scalability limitations because it will support a maximum of 2000 endpoints, regardless of the physical hardware that is used to implement the node.

The second example depicts a distributed deployment. It adds fault tolerance and improves scalability. Note that distributed deployment introduces the concept of a role. There are two administration personas. One has the primary role and the other has the secondary role. The same is true for the monitoring persona. To efficiently spread the workload, the primary roles are implemented on different nodes.

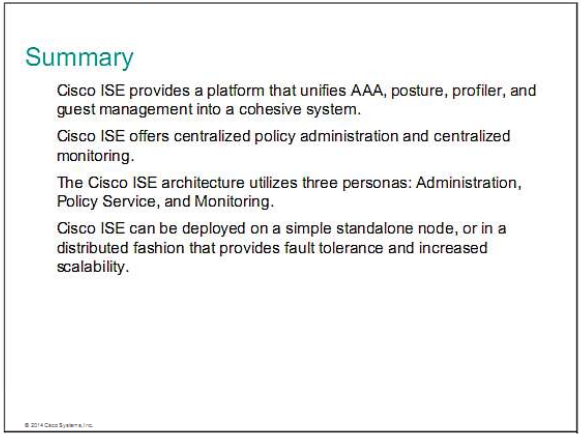
The second example also has improved scalability due to the separation of the policy service persona from the administration and monitoring nodes. When a node only runs the policy service persona, the maximum number of endpoints that is supported by that policy service node is dependent on the hardware platform.

Note that there is no concept of primary or secondary role with the policy service persona. Policy service nodes play the role of RADIUS server to the NADs in the deployment. A particular NAD may be configured to assign a higher priority to one policy service node over another, but the policy service nodes themselves are unaware of the perspective of the NAD.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Summary

This topic summarizes the key points that were discussed in this lesson.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Lesson 2

Cisco ISE PKI

PKI offers a scalable method to secure networks, reduce management overhead, and simplify the deployment of network infrastructures. PKI manages encryption keys and identity information for the components of a network, which participate in secured communications. Any network, from small business networks to the core systems of the world's largest service provider networks, can benefit from the PKI. This lesson describes how to enroll the Cisco Identity Services Engine in the PKI.

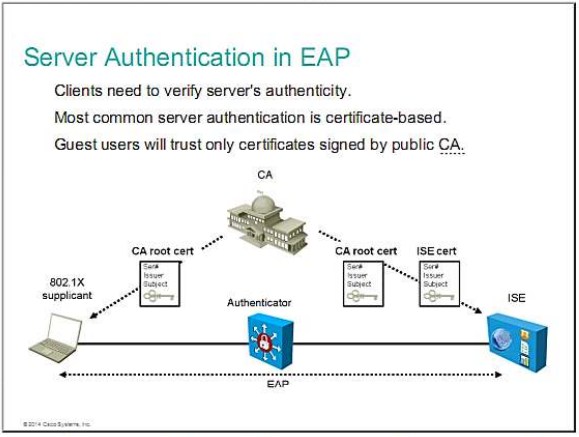
Upon completing this lesson, you will be able to meet these objectives:

- Describe the server authentication in EAP
- Describe the TLS protection in a Cisco ISE environment
- Describe the X.509v3 certificates
- Describe the use of the server certificate
- Describe the validation of the ISE certificate
- Describe the validation of the ISE signature
- Describe the procedure of enrolling the ISE in PKI
- Describe how to import the CA root certificate into the ISE certificate store
- Describe how to generate a certificate signing request (CSR)
- Describe how to bind the returned certificate to the pending CSR
- Describe how to verify the ISE enrollment in the PKI

https://t.me/learningnets

Server Authentication in EAP

This topic describes the server-side authentication in EAP.



EAP differentiates between two authentication halves: server and client authentication. In server authentication the clients verify the server authenticity. In client authentication the server validates the client authenticity. While the client authentication methods differ significantly among various EAP types, the server authentication is based on certificates in most of the common and trusted EAP types.

There are two types of certificates:

Local certificates: These credentials are used to identify the Cisco Identity Services Engine server to other entities such as EAP supplicants, external policy servers, or management clients. Local certificates are also known as identity certificates. Along with the local certificate, a private key is stored in Cisco ISE to prove its authenticity.

Certificate authority certificates: These credentials are used to verify remote certificates that are presented to Cisco ISE. Certificate authority certificates have a dependency relation that forms a CTL hierarchy. This hierarchy connects a certificate with its ultimate root CA and verifies the authenticity of the certificate.

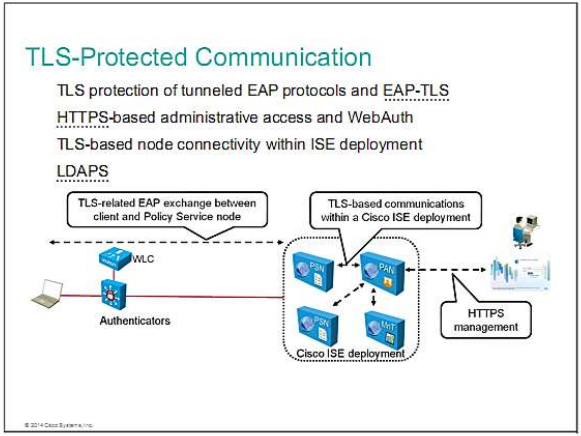
Cisco ISE acts as the EAP server in many secure access solutions. It requires a certificate that can be validated by the clients. When you install a new ISE in the network, it comes with a pre-installed certificate that by default cannot be verified by the client supplicants. To allow a successful certificate validation, a Certificate Authority is used to sign the ISE certificate. The enrollment of the ISE with the CA involves several steps: the CA root certificate must be installed on the ISE, the ISE must issue a CSR to the CA, the CA must grant the requested certificate, and the ISE certificate must be installed on the ISE.

The supplicant will be able to validate the ISE certificate if it has the CA root certificate.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

TLS-Protected Communication

This topic describes TLS-protected communication in the Cisco Identity Services Engine environment.

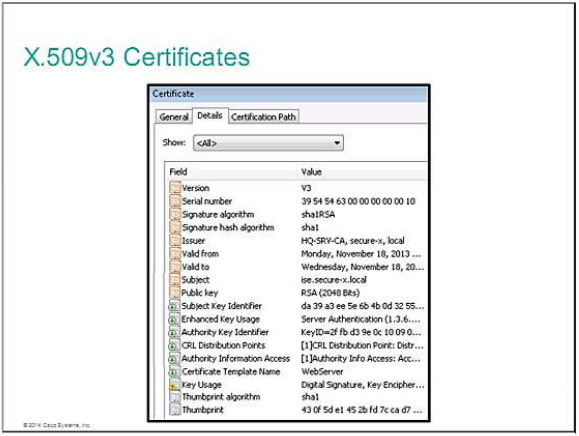


The Cisco ISE relies on a PKI to provide secure communication for the following:

- Client and server authentication for TLS-related EAP protocols.
- HTTPS communication between client browser and the Cisco ISE node for administration sessions.
- TLS-based protection of communications within a Cisco ISE deployment
- LDAPS

X.509v3 Certificates

This topic describes the X.509v3 certificates.



A digital certificate contains specific fields that convey the identity information that is associated with the certificate subject (that is, the entity to which the certificate was issued). The certificate also contains information about the certificate issuer and the issuer signature. The issuer produces the signature by creating a hash of the certificate data and then encrypting the hash with its private key. Other systems receiving a certificate can verify its authenticity using the public key of the issuer, which they generally get from the issuer's own certificate. To verify a certificate, the receiver decrypts the signature using the public key of the issuer. This key should be the hash of the original certificate data. The receiver then hashes the data from the certificate that it received. If the hash matches the decrypted signature, then the certificate data has been verified. Generally, other considerations are taken into account when validating a certificate, including the valid from and valid to dates that are defined within the certificate.

The public key of the certificate subject is a critical piece of identity information. Other entities can send private messages to the subject by encrypting data with the public key of the subject. Because only the subject has the corresponding private key, only the subject can read the message. The fact that only the subject can decrypt the message can be used for authentication.

For example, a simplified description of the setup of a TLS session follows:

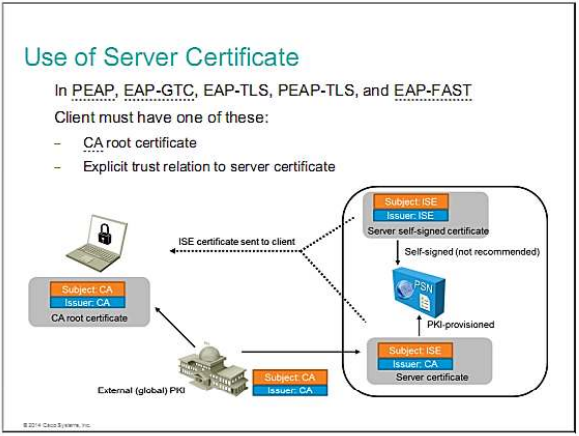
1. The client initiates a connection to the TLS server.
2. The server presents its certificate to the client.
3. The client validates the signature on the certificate.
4. The client generates a session key to use for a shared key encrypted session. The client uses the public key of the server, which is retrieved from the validated certificate, to encrypt the session key.
5. The client sends the encrypted session key to the server and requires future traffic to be encrypted with the session key.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

6. The server uses its private key to decrypt the session key, and uses it to encrypt the rest of the traffic that is associated with that session.

Use of Server Certificate

This topic describes the use of the server certificate.



For most EAP methods, Cisco Identity Services Engine needs to have an identity certificate that the clients will be able to verify. In PEAP and EAP-GTC, clients verify the server certificate, and the server authenticates the clients using other credentials. In EAP-TLS and PEAP-TLS, the sides verify each other using certificates.

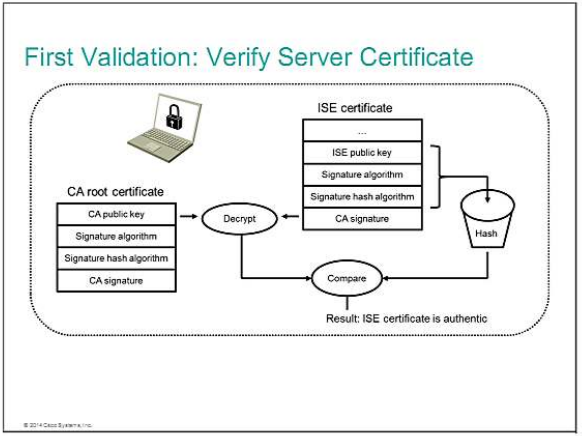
If certificate-based authentication is used, the client needs to verify the server certificate first. This process is used in PEAP, EAP-GTC, EAP-TLS, PEAP-TLS, and EAP-FAST. Cisco ISE acts as the server side and presents its identity certificate to the client.

The Cisco ISE identity certificate is either self-signed or has been issued by a CA. The self-signed certificate is preinstalled on Cisco ISE and can be refreshed. Deploy certificates using the CA to achieve a secure and scalable solution. If the Cisco ISE identity certificate is self-signed, the client needs to be configured to trust it. The client does not have any scalable method to verify self-signed certificates. If the Cisco ISE identity certificate has been issued by a CA, the client needs the CA root certificate to verify any identity certificate that is issued by that CA.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

First Validation: Verify Server Certificate

This topic describes how the client validates the server certificate.

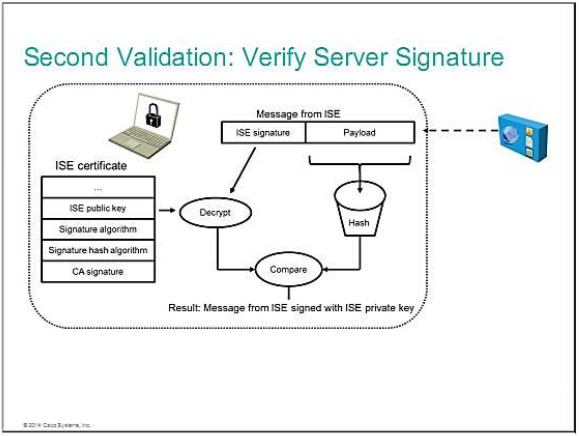


The clients validate the server authenticity in two fundamental steps: first they verify the server certificate and then they verify the server signature.

When the Cisco Identity Services Engine sends the client its identity certificate that has been signed by a CA, the client needs the CA root certificate to verify the ISE certificate. The client extracts the CA public key from the CA root certificate and uses it to decrypt the CA signature in the ISE certificate. The CA signature in the ISE certificate has been computed by hashing the ISE certificate fields and encrypting the result with the CA private key. After the client decrypted the CA signature using the CA public key, the obtained hash, also known as fingerprint or thumbprint, is compared with the hash calculated over the ISE certificate fields. If the fingerprints match, the received ISE certificate is authentic, e.g. it has been signed by the CA with the CA private key.

Second Validation: Verify Server Signature

This topic describes how the client validates the server signature.

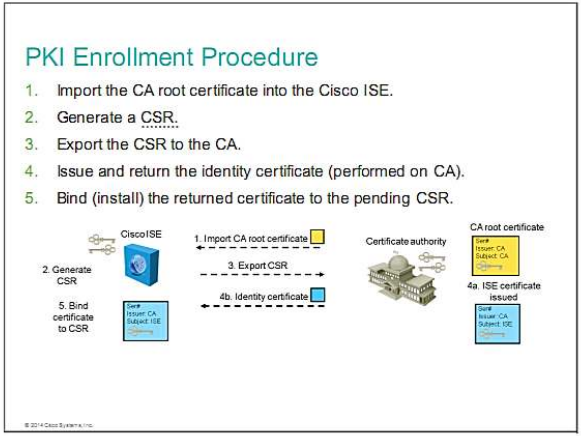


In the second fundamental step the client examines the data arriving from the server. The data, in additional to transporting the Cisco Identity Services Engine certificate, is signed, and the signature is appended to the payload. The signature is hashed by the ISE and the hash is encrypted using the ISE private key. The client extracts the ISE public key from the already verified ISE certificate and uses it to decrypt the ISE signature. The resulting hash is compared with a hash of the received data. If the fingerprints match, the arriving traffic is authentic, e.g. it has been signed by the ISE with the ISE private key.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

PKI Enrollment Procedure

This topic describes the procedure of enrolling the Cisco Identity Services Engine in PKI.

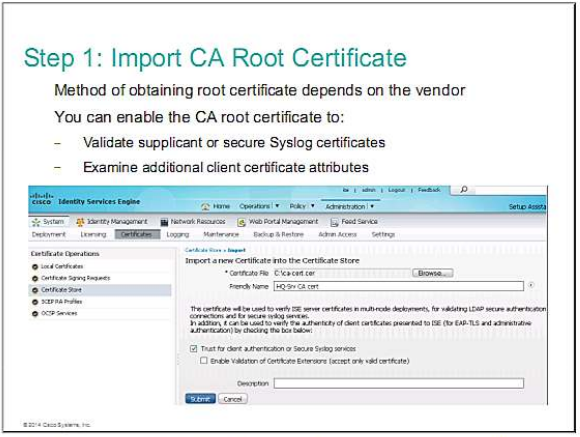


To enroll the Cisco ISE with a PKI, perform these steps:

1. Import the CA certificate into Cisco ISE. You need to obtain the CA certificate from the CA to install it on Cisco ISE.
2. Generate a CSR.
3. Export the CSR and provide it to the CA using an appropriate method.
4. The CA administrator must sign and return Cisco ISE identity certificate. This step may involve some additional verification checks that are imposed by the CA on the enrolling systems.
5. Bind (install) the returned certificate to the pending CSR.

Step 1: Import CA Root Certificate

This topic describes how to import the CA root certificate into the Cisco Identity Services Engine certificate store.



Start the enrollment procedure by obtaining the root CA certificate from the CA. The details vary depending on the CA vendor and type, but usually involve retrieving it via HTTP or FTP. In a PKI, you have to verify the root certificate authenticity over an out-of-band channel. This verification mitigates the risk of accepting a spoofed certificate from an impostor CA.

Import the root certificate into the Cisco ISE certificate store, in the **Administration > System > Certificates > Certificate Store** menu by clicking the **Import** button.

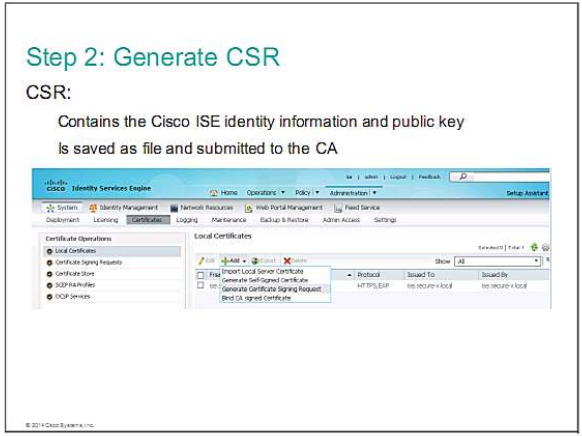
Note that there is a self-signed certificate that is provisioned during the Cisco ISE installation process. This certificate will be used by default, but its usage does not scale well. You could set up a multinode deployment without a CA. In that case, use the self-signed certificates that are installed on each Cisco ISE node during the installation process. You need to copy the self-signed certificate onto other nodes. This process increases the administrative burden each time you need to add a new node or change the current deployment. There are similar complexities that are associated with distributing certificates to endpoints. It is recommended to enroll Cisco ISE with an appropriate PKI.

The CA root certificate is automatically enabled for securing LDAP sessions to an external LDAP server. In many cases, you will use certificates to authenticate clients. For that reason, you need to enable the root certificate for client authentication or secure Syslog services by checking the appropriate check box and optionally allow it to be used for certificate extensions. Certificate extensions allow you to retrieve user certificate information from external user databases and validate additional certificate attributes.

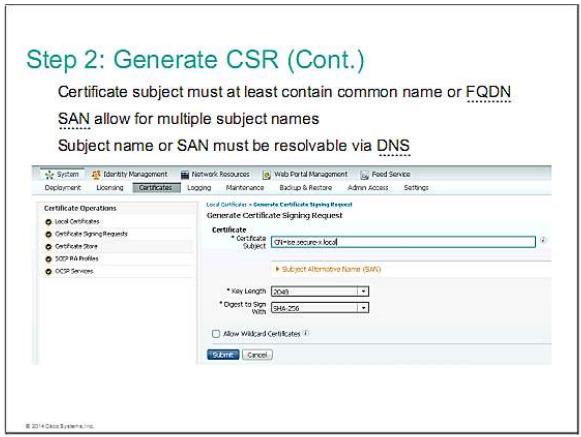
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 2: Generate CSR

This topic describes how to generate a CSR.



To obtain an identity certificate, the Cisco Identity Services Engine needs to generate a CSR. A CSR contains the Cisco ISE identity information and public key and is generated through the **Administration > System > Certificates > Local Certificates > Add > Generate CSR** menu.



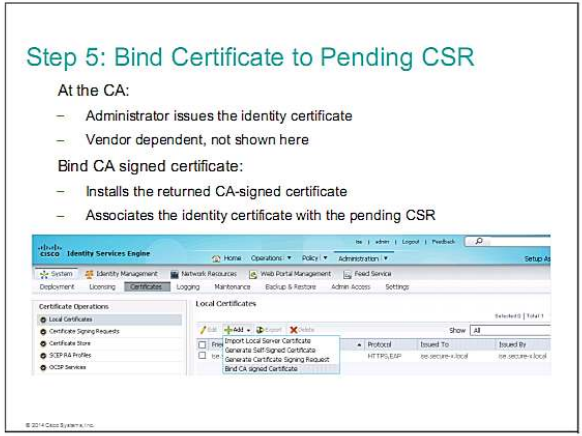
The certificate subject of the generated CSR must at least contain a common name or a FQDN. You can also specify SANs, which allow the mapping of multiple subject names to the same public/private key pair. Cisco ISE supports key lengths of 1024, 2048, or 4096 bits. The key length affects the signature strength. A key length greater than 2048 will currently not allow Cisco IP phones to authenticate using an EAP method, because their maximum key length is 2048.

The hash algorithm options include the methods SHA-1 and SHA-256.

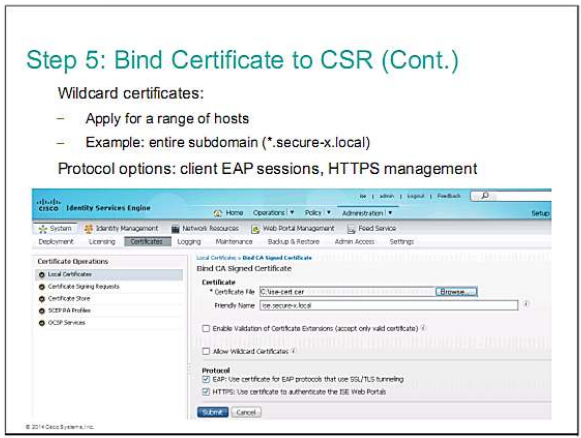
https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Step 5: Bind Certificate to Pending CSR

This topic describes how to bind the returned certificate to the pending CSR.



When you submit the CSR to the CA and obtain an identity certificate from the CA, you need to install the CA-approved and CA-signed identity certificate on the Cisco Identity Services Engine. Install the certificate using the Bind CA Certificate operation, which is available in the **Administration > System > Certificates > Local Certificates > Add > Bind CA Certificate** menu. The binding associates the returned CA-signed certificate with the pending CSR.



To perform the bind operation, you need to navigate to the identity certificate file. You have several options that define the use of the identity certificate:

Enable the use of this identity certificate for certificate extensions that validate certain certificate attributes using an external user database.

Enable the use of wildcard certificates that can apply to a range of hostnames, for example an entire subdomain

Enable the certificate use for EAP authentication of client network access.

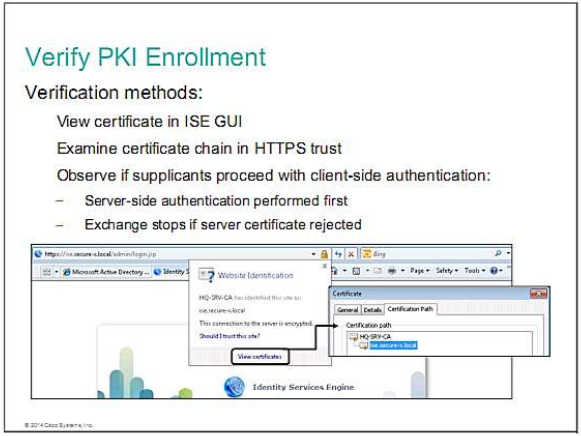
Enable the identity certificate to secure the HTTPS-based administrative access to the Cisco ISE.

Click **Submit** to install the identity certificate on the system. The ISE application service will restart and you will be logged out of the GUI.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Verify PKI Enrollment

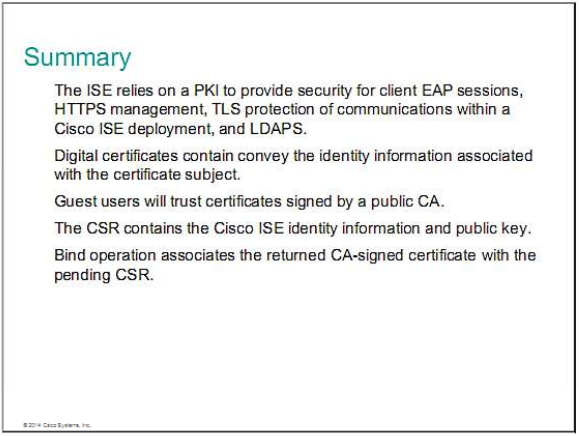
This topic describes how to verify the Cisco Identity Services Engine enrollment in the PKI.



You can verify a successful enrollment of the ISE in PKI using three methods. You can view the ISE identity certificate through the ISE GUI, in the **Administration > System > Certificates > Certificate Store** menu. You can connect via HTTPS to the ISE and verify the trust relationship, as shown in the figure above. You can also observe EAP authentications. Since server authentication is always performed before client authentication, the supplicants must successfully have validated the ISE certificate before you can see any access attempts in the ISE GUI.

Summary

This topic summarizes the key points that were discussed in this lesson.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Lesson 3

Cisco ISE Authentication

Cisco Identity Services Engine can authenticate the users and endpoints against the internal database or against external identity sources. The internal database is often used in a simple deployment without any external servers.

Authentication can be configured on the Cisco ISE as a simple or rule-based authentication policy. This lesson explains the difference between the two types of policies and explains how to configure authentication.

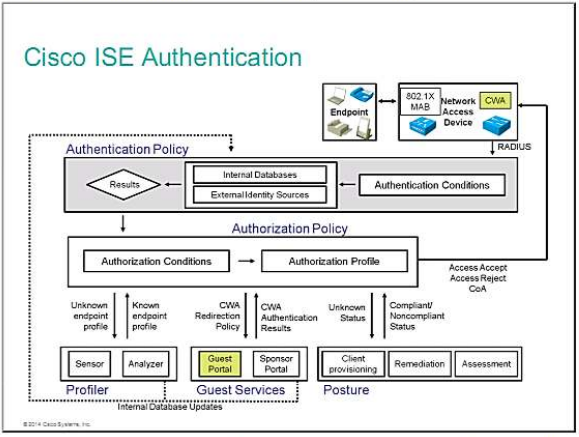
Upon completing this lesson, you will be able to meet these objectives:

- Describe the authentication on Cisco Identity Services Engine
- Describe the policy elements in Cisco ISE
- Describe the authentication policy example in Cisco ISE
- Describe the rule-based authentication on the Cisco ISE
- Describe the authentication conditions
- Describe how to implement rule-based authentication on the Cisco ISE
- Describe how to configure simple authentication conditions
- Describe how to create or tune compound conditions
- Describe how to define the allowed protocols
- Describe how to tune or create authentication rules
- Describe how to tune the default authentication rule
- Describe the Cisco Network Access Manager
- Describe the networks and network groups in the Cisco Network Access Manager
- Describe the network settings in the Cisco Network Access Manager

https://t.me/learningnets

Cisco ISE Authentication

This topic describes the authentication on Cisco Identity Services Engine.



Authentication requests are processed immediately after an endpoint attempts to access the network through a NAD. The Cisco ISE evaluates the access path over which the endpoint enters the network and checks the credentials that are stored in the identity source.

The Cisco ISE has an authentication policy that gathers multiple checks into a centralized decision point. The authentication policy contains criteria that define how to validate the user identity and through which NADs the user is allowed to enter. The validation of the user identity is performed against an identity source. The identity source can be the internal database, an external server, or a sequence of multiple sources.

Authentication policies define the protocols that Cisco ISE should use to communicate with the network devices, and the identity sources that it should use for authentication. A policy is a set of conditions and a result.

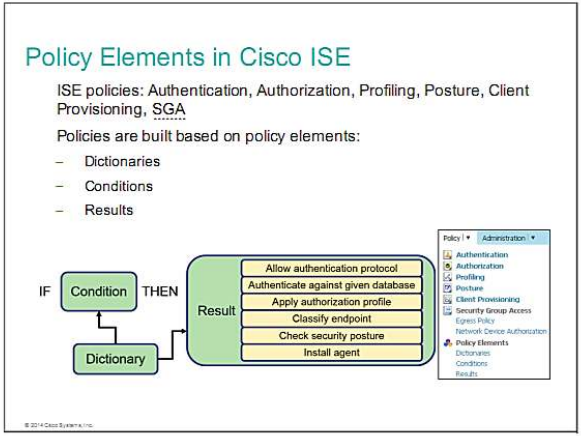
A policy condition consists of an operand (attribute), an operator (equal to, not equal to, greater than, etc.), and a value. Compound conditions are made up of one or more simple conditions that are connected by the AND or OR operator. At run time, the Cisco ISE evaluates the policy condition and then applies the result that you have defined based on whether the policy evaluation returns a true or a false value.

You can configure two types of authentication policies on the Cisco ISE: simple and rule-based authentication. Simple authentication does not use any conditions, and is not commonly deployed. Rule-based authentication consists of a set of rules, and each rule can define conditions and resulting actions. This lesson discusses the more common rule-based authentication.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Policy Elements in Cisco ISE

This topic describes the policy elements in Cisco Identity Services Engine.

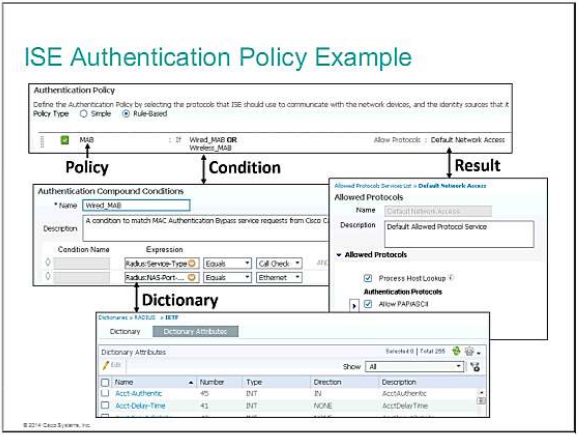


The ISE is a policy-centric platform. Its logic centers on several policies: authentication, authorization, profiling, posture, client provisioning, and Security Group Access. The policies are generally built of conditional statements: if a condition is met then a result will be applied. The conditions and results differ based on the policy type. The results in the authentication policy will define the allowed authentication protocols and the authentication database. The results in the authorization policy will specify the authorization profile to restrict the client privileges. The results in the profiling policy will classify an endpoint to an endpoint identity group. The results in the posture policy will check the security status of an endpoint. The results in the client provisioning policy will specify an agent to be installed on the endpoint. The results in the SGA policy will classify and filter traffic.

Policies use policy elements as building blocks. ISE defines three types of policy elements: dictionaries, conditions and results. Dictionaries specify attributes that are available for use within conditions. Conditions specify a set of requirements that indicate a particular context. Results define the actions that ISE will take when the conditions of a particular policy are met.

Cisco ISE Authentication Policy Example

This topic describes the policy elements in Cisco Identity Services Engine.

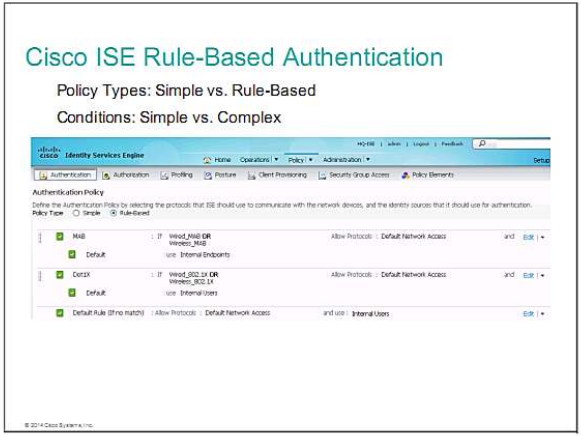


The screen clippings displayed here show an example of how the policy elements (dictionaries, conditions and results) are assembled together to define policies. This policy and these policy elements are among those that are predefined in ISE and are used by default after ISE installation. The authentication policy named MAB is shown. This policy references two conditions: Wired_MAB and Wireless_MAB. The Wired_MAB condition is also shown. It uses two values defined in the RADIUS dictionary. The RADIUS dictionary is also shown, but only the first two attributes in the dictionary are shown. The Wired_MAB condition uses two attributes from the RADIUS dictionary: Service-Type and NAS-Port-Type. The condition requires that the Service-Type to be Call Check and the NAS-Port-Type to be Ethernet. The Wireless_MAB condition (not shown) is similar, requiring the Service-Type to be Call Check and the NAS-Port-Type to be Wireless - IEEE 802.11. There are similar conditions (also not shown) used to match wired and wireless 802.1X. They differ from the MAB conditions by requiring the Service-Type to be Framed. Conditions provide a framework to identify if the context matches a particular situation. The MAB authentication policy references two conditions with a logical or. If either of the conditions match, then the results will be applied. In this case, the result is to set the allowed EAP protocols to be what is defined in the Allowed Protocols list named Default Network Access. This list can be edited by checking and unchecking the authentication protocol options provided by ISE.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Cisco ISE Rule-Based Authentication

This topic describes the rule-based authentication on the Cisco Identity Services Engine.



The default authentication policy is the rule-based authentication policy. It is far more common than the simple authentication policy. The rule-based authentication policy consists of attribute-based conditions that determine the allowed protocols and the identity source or identity source sequence to be used for processing the requests. In a simple authentication policy, you can define the allowed protocols and identity source statically. In a rule-based policy, you can define conditions that allow Cisco ISE to dynamically choose the allowed protocols and identity sources. You can define one or more conditions using any of the attributes from the Cisco ISE dictionary.

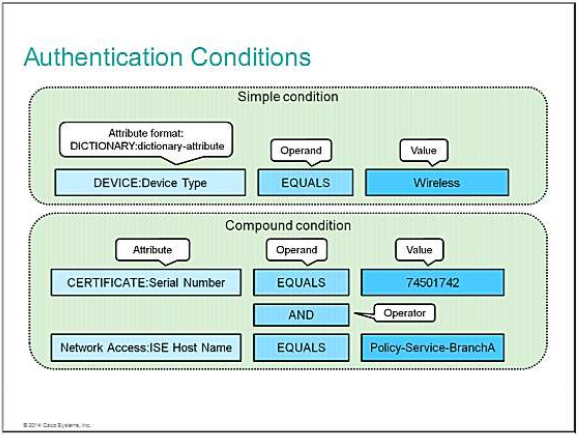
Cisco ISE allows you to create conditions as individual, reusable policy elements that can be referenced from other rule-based policies. You can also create conditions from within the policy creation page. There are two types of conditions:

Simple condition: A simple condition consists of three components: attribute, operand, and value. It can be saved and reused in other rule-based policies. You can use any attribute from the Cisco ISE dictionary and specify any value that fits the attribute.

Compound condition: A compound condition is made up of one or more simple conditions with an AND or OR relationship. These conditions are built in addition to simple conditions and can be saved and reused in other rule-based policies.

Authentication Conditions

This topic describes the authentication conditions.



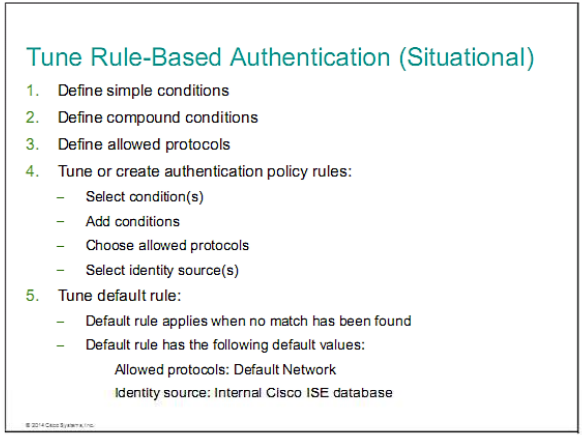
An example of a simple condition is: DEVICE: Device Type Equals Wireless. This syntax includes an attribute, which is written in the format DICTIONARY: dictionary-attribute, the operand, and the value.

The example of the compound condition shown in the figure combines two individual conditions (certificate serial number check and Cisco Identity Services Engine hostname check) using the AND operator. The operands available for use depend on the data type of the attribute (i.e. 'contains' and 'starts with' are available for attributes of type String but not Numeric). The attributes are defined in Cisco ISE dictionaries. The operator that combines the individual conditions can be AND or OR.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Tune Rule-Based Authentication (Situational)

This topic describes how to implement rule-based authentication on the Cisco Identity Services Engine.

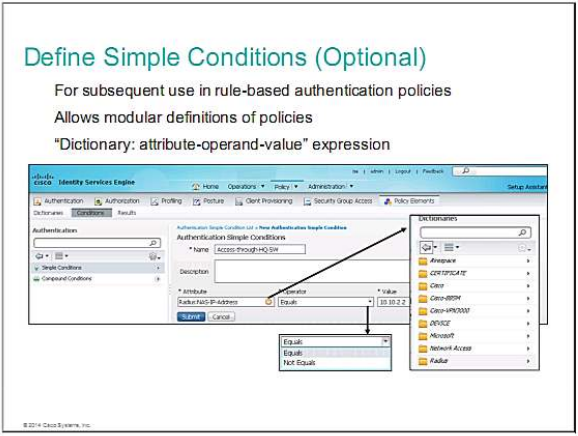


The procedure shown above describes how to define a rule-based authentication policy on Cisco ISE. You will use the procedure only in environments where the default authentication policy must be tuned. All these steps are optional:

1. Define simple conditions
2. Create or tune compound conditions
3. Define allowed protocols
4. Define a rule-based authentication policy. Within this step you will create a new rule, define or add conditions, specify allowed protocols, and choose identity sources
5. Tune the default rule. The default rule defines actions to be taken when no specific match is found. The default settings are to use the Default Network list as the allowed protocols set, and the internal Cisco ISE database as the identity source.

Define Simple Conditions (Optional)

This topic describes how to configure simple authentication conditions.

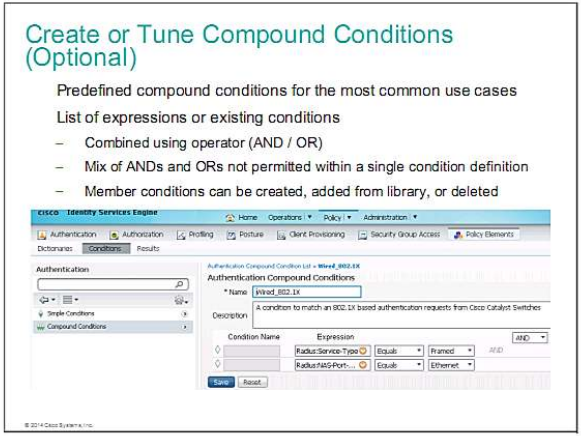


The figure shows how to create a simple condition. It consists of an attribute, an operator, and a value. You can create simple conditions from within the policy pages and also as separate policy elements that can be reused in policies.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Create or Tune Compound Conditions (Optional)

This topic describes how to create or tune compound conditions.



Compound conditions are made up of two or more simple conditions. You can create compound conditions as reusable objects from within the Policy Creation page or from the Conditions page. Cisco Identity Services Engine comes with predefined compound conditions for some of the most common use cases.

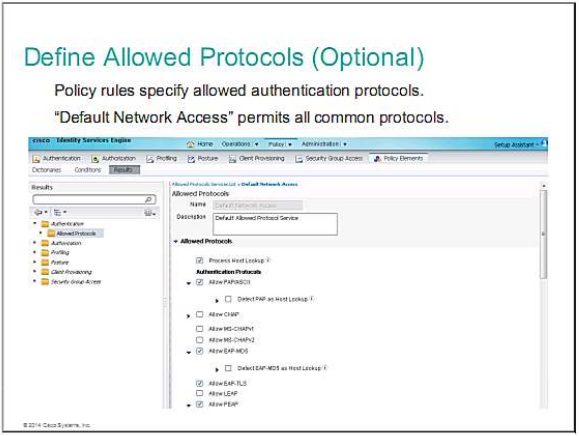
Compound conditions contain multiple expressions that are combined using an AND or OR operator. You can use only a single operator within a compound condition. Mixing of ANDs and ORs is not allowed. For complex rulesets, you may achieve a mix of ANDs and ORs by nesting compound conditions within a hierarchy. A lower-level compound condition may use one of these operators, while a higher-level condition may use the other. Bear in mind that such complexity makes the rulesets difficult to read and understand and should be used with caution.

The example in this figure illustrates a pre-defined compound condition Wired_8021.X consisting of two individual conditions that are combined using the AND operator. This condition is used to match 802.1X access requests from wired switches. The first condition checks if the RADIUS: Service-Type is equal to Framed. The second condition checks if the RADIUS:NAS-Port-Type is Ethernet.

https://t.me/learningnets

Define Allowed Protocols (Optional)

This topic describes how to define the allowed protocols.



In Cisco Identity Services Engine you have the option of using the built-in allowed protocol set or create a custom list of allowed authentication protocols. You can view and customize the default protocol set. It is named Default Network Access and can be edited in the **Policy > Policy Elements > Results > Authentication > Allowed Protocols Services** menu.

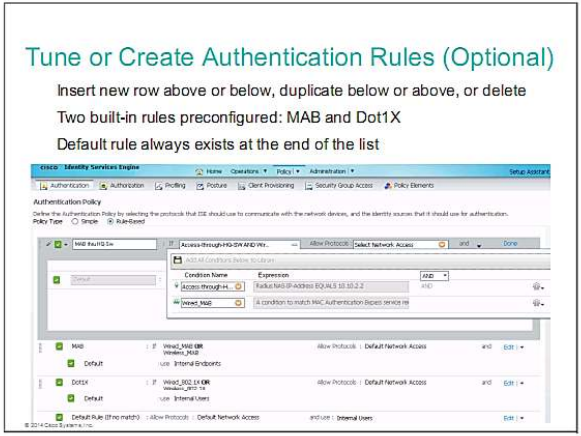
The Default Network Access protocol set is added to the Cisco ISE as a result of the installation procedure. It allows the use of all major EAP methods.

You can modify the Default Network Access protocol set to meet your needs or configure a custom allowed protocol set. The allowed protocol set is referenced by the authentication policy rules.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Tune or Create Authentication Rules (Optional)

This topic describes how to tune or create authentication rules.



You can view the default rule-based authentication policy by selecting the Rule-Based radio button on the Authentication page. The rows that are displayed on this page describe rules that altogether constitute the rule-based policy. The rules are processed in order. The default Cisco Identity Services Engine configuration consists of two built-in rules, MAB and Dot1X, and a default rule that is processed when none of the other rules produces a match.

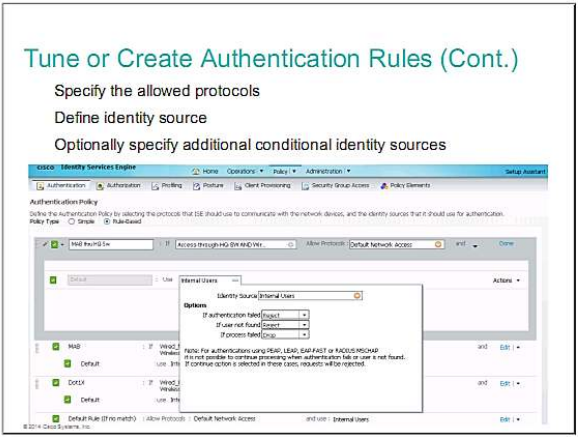
The first two rules check for conditions combined using the OR operator. The MAB rule checks if the compound condition Wired_MAB or the compound condition Wireless_MAB is met. If so, the ISE verifies if the access attempt is made using a permitted authentication protocol, and then attempts to authenticate the client against the internal endpoint database. The DOT1X rule checks if the compound condition Wired_802.1X or the compound condition Wireless_802.1X is met. If so, it verifies if the access attempt is made using a permitted authentication protocol, and attempts to authenticate the client against the internal user database.

You can modify, duplicate, and delete the existing rules, or insert a new rule at any desired position by selecting the appropriate action in the Actions list. The available actions are Insert new row above, Insert new row below, Duplicate above, Duplicate below, and Delete.

When you add a rule to the rule-based policy, you must provide its name, identify one or more conditions, and choose the required allowed protocols service and identity source. The conditions are identified in the Select Attribute section. You can reference any existing simple or compound conditions or create a new one while setting up the authentication rule.

This example illustrates the configuration of conditions in an authentication rule. You click on the plus sign of the Select Attribute menu to unfold it. In this menu you have the option of selecting conditions that already exist in the library, or define new conditions here and add them to the library. Multiple conditions are combined using the OR or AND operator.

https://t.me/learningnets



The next component of an authentication rule is the allowed protocols service. This example uses the Default Network Access object, which you may modify. You unfold the Network Access Services menu by clicking the arrow-down symbol of the Select Network Access field.

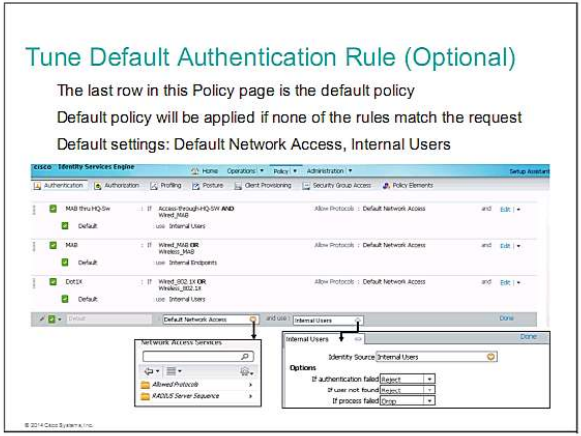
The last element of the authentication rule is the identity source that will be used to authenticate the users when the previously defined conditions and access protocols are matched. The identity source can be the internal database, an external server, or an identity source sequence. An identity source sequence defines the order in which Cisco ISE will look for user credentials in the databases.

An authentication rule can use more than one identity source or identity source sequence. Although not shown in the figure, you can configure an additional set of conditions that need to be matched for a specific identity source to be used for authentication. The conditions that are defined in this section constitute another layer of conditions. The authentication rule itself defines one or more parent-level conditions. The conditions that are used for selecting the identity sources should be thought of as child-level conditions, which are evaluated after the parent-level conditions are met.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Tune Default Authentication Rule (Optional)

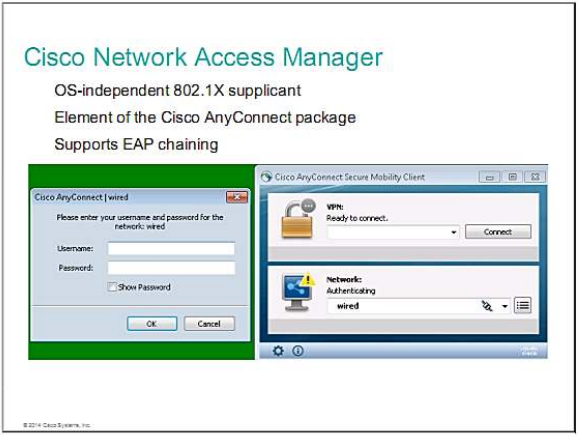
This topic describes how to tune the default authentication rule.



The rule-based authentication policy ends with a default policy that acts as a "catch-all" statement for authentication requests that have not been matched by any previous rules. Like all other rules, it matches the allowed protocols service and selects an identity source or identity source sequence. It does not include any conditions.

Cisco Network Access Manager

This topic describes the Cisco Network Access Manager.



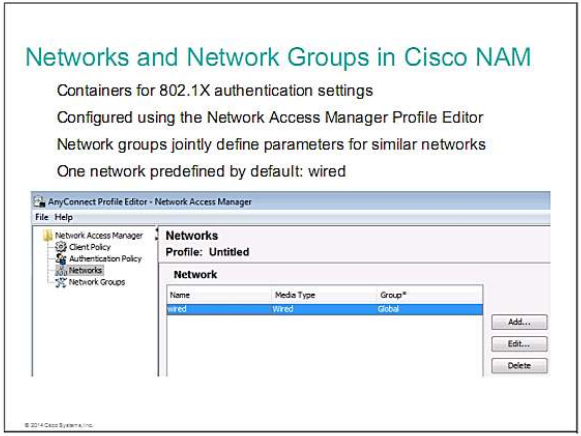
The Cisco NAM is a Cisco-engineered OS-independent client software that provides a secure Layer 2 network in accordance with policies set forth by the enterprise network administrators. The Network Access Manager detects and selects the Layer 2 access network and performs device authentication for access to both wired and wireless networks. The Network Access Manager manages user and device identity and the network access protocols required for secure access. It can prevent end users from making connections that are in violation of administrator-defined policies.

Cisco NAM is a component of the Cisco AnyConnect Security Mobility Client portfolio that can be combined with its other optional elements, such as the Web Security Module. Together with Cisco Identity Services Engine it supports EAP chaining, which allows you to evaluate the type of the client devices that users connect from.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Networks and Network Groups in Cisco NAM

This topic describes the networks and network groups in the Cisco Network Access Manager.

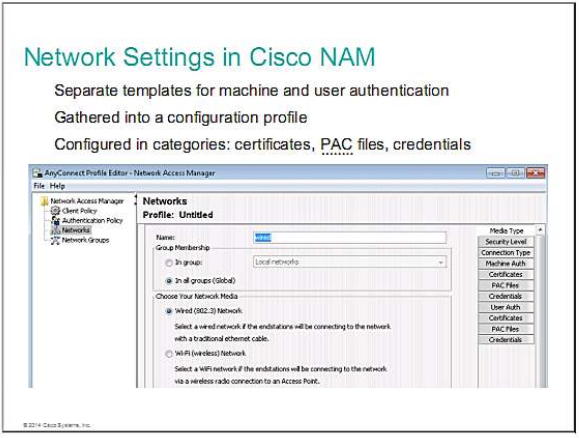


The Cisco NAM Profile Editor allows you to configure pre-defined networks for your enterprise user. You can either configure networks that are available to all groups, or create groups with specific networks. A group is a container for authentication settings applied when the user attempts connection to a given network type. The Networks window runs a wizard that sometimes adds panes to the existing window.

A group, fundamentally, is a collection of configured connections (networks). Every configured connection must belong to a group or a member of all groups.

Network Settings in Cisco NAM

This topic describes the network settings in the Cisco Network Access Manager.

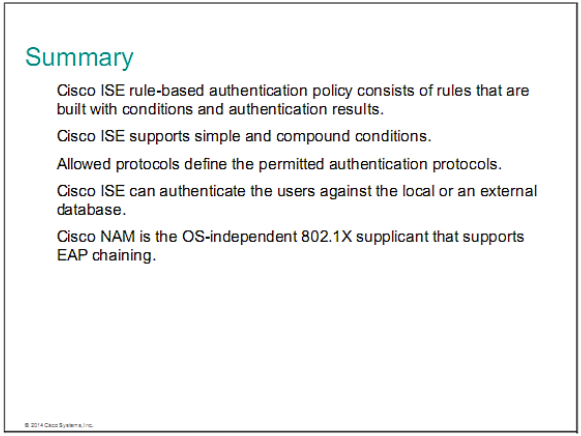


The Cisco NAM Profile Editor enables you to create or edit a wired or a wireless network. The settings for each network vary depending on whether you choose wired or wireless. The settings are grouped in categories. The figure above shows the categories available for the default 'wired' network of media type "Wired (802.3)". They include Security Level, Connection Type, Machine Authentication, along with the related categories Certificates, PAC Files, Credentials, and the User Authentication, along with the related categories Certificates, PAC Files, Credentials. Depending on your scenario you will have to edit only the required settings and leave all other parameters at their default values.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Summary

This topic summarizes the key points that were discussed in this lesson.



https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Lesson 4

Cisco ISE External Authentication

Cisco Identity Services Engine supports a number of external authentication sources, which are also referred to as authentication servers. The authentication servers maintain user databases and store various user attributes. External authentication sources are common in enterprise deployments because they provide a single configuration point for user accounts between various enterprise applications, services, and systems.

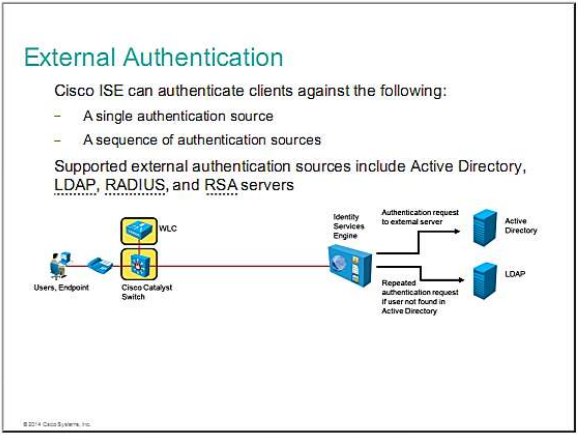
Upon completing this lesson, you will be able to meet these objectives:

- Describe the external authentication
- Describe the Active Directory
- Describe the authentication methods with Active Directory
- Describe the AD-derived group membership
- Describe the methods of integrating Cisco ISE with the Active Directory
- Describe the Active Directory integration procedure
- Describe how to configure the AD domain and store
- Describe how to test the connection to the Active Directory
- Describe how to join the ISE to the Active Directory
- Describe how to select groups from the directory
- Describe the Cisco ISE identity source sequences
- Describe how to configure the identity source sequence
- Describe how to apply the identity source sequence in the authentication policy
- Describe how to verify external authentication

https://t.me/learningnets

External Authentication

This topic describes the external authentication.



Most companies deploy a scalable authentication framework that utilizes external repositories for storing user accounts and user attributes. Such approach allows multiple systems to connect to a single centralized database and request the required information. The external identity source is configured in a redundant fashion to provide a highly available authentication solution.

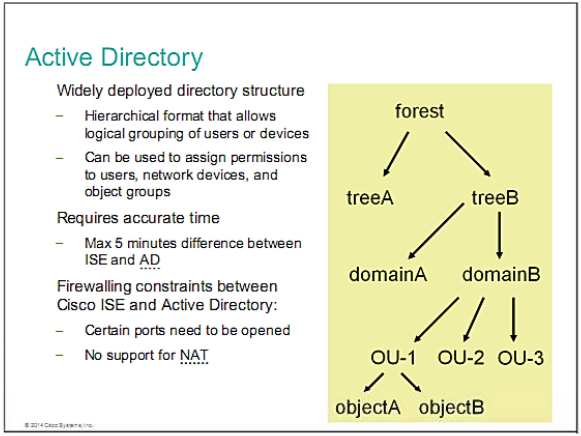
Cisco Identity Services Engine can authenticate clients against a single authentication source or a sequence of authentication sources.

The supported external authentication sources include Active Directory, LDAP, RADIUS, and Secure RSA servers.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Active Directory

This topic describes the Active Directory.



Active Directory is a hierarchical data store that serves as a repository for network user and device information. This network information is stored as individual entities, which are known as objects. Objects may describe devices and entities that are found on the network, such as servers, printers, client PCs, and user accounts.

This directory structure allows network administrators to place objects into groups that share similar network permissions, function, or location on the network. Active Directory is designed to provide permissions for users and network devices that are based on configured corporate policies.

Active Directory utilizes a topology structure that is like DNS, which utilizes a tree for the hierarchical layers. Active Directory includes the following layers:

Object: An object in the Active Directory is any user, client PC, network server, printer, or other device that is integrated within the directory.

Organizational Unit: An organizational unit is a logical grouping of objects within the domain. Organizational units are organized based on the network design. They may be collections of users in the same corporate group, servers in the same cluster, printers on the same floor, or any other grouping of corporate significance.

Domain: A domain is a grouping of objects that shares the same database. This domain may contain a host of objects that are logically grouped as organizational units.

Tree: A tree is a collection of one or more domains that share trust relationships.

Forest: This layer is the top level of the Active Directory. The forest contains one or more trees, and any objects within the same forest share the same global catalog, directory schema, logical structure, and directory configuration.

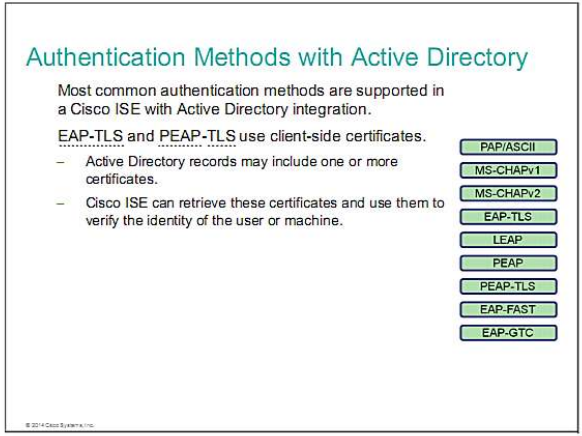
If there is a firewall between Cisco Identity Services Engine and Active Directory, certain ports need to be opened to allow Cisco ISE to communicate with Active Directory. Ensure that the following default ports are open:

Protocol	Port
LDAP	389 (UDP), 389 (TCP)
LDAPS	636 (TCP)
SMB	445 (TCP)
KDC	88 (TCP)
Global Catalog	3268 (TCP), 3269 (TCP)
KPASS	464 (TCP)
NTP	123 (UDP)

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Authentication Methods with Active Directory

This topic describes the authentication methods supported with Active Directory.



Cisco Identity Services Engine supports the following authentication protocols when using Active Directory as the external authentication source:

EAP-FAST andPEAP: Cisco ISE supports user and machine authentication and password changes against Active Directory using EAP-FAST and PEAP with an inner method of MS-CHAPv2 and EAP-GTC.

PAP: Cisco ISE supports authentication against Active Directory using PAP and also allows you to change Active Directory user passwords.

MS-CHAPv1: Cisco ISE supports user and machine authentication against Active Directory using MS-CHAPv1.

MS-CHAPv2: Cisco ISE supports user and machine authentication against Active Directory using MS-CHAPv2.

EAP-GTC: Cisco ISE supports user and machine authentication against Active Directory using EAP-GTC.

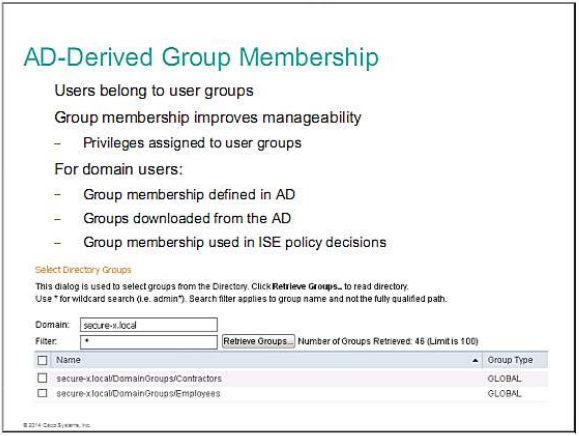
EAP-TLS: Cisco ISE uses the certificate retrieval option to support user and machine authentication against Active Directory using EAP-TLS.

PEAP-TLS: Cisco ISE supports user and machine authentication against Active Directory using PEAP-TLS.

LEAP: Cisco ISE supports user authentication against Active Directory using LEAP.

AD-Derived Group Membership

This topic describes the AD-derived group membership.



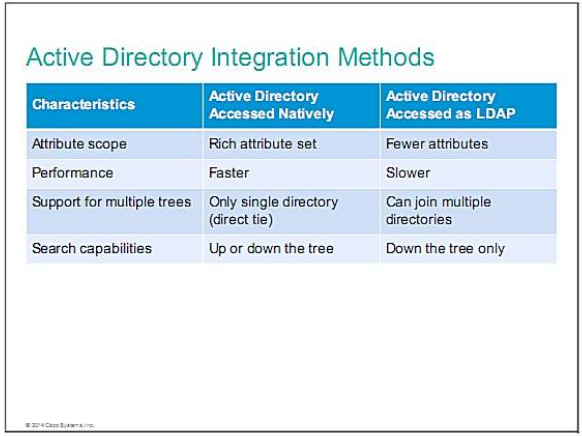
You can improve the manageability of an authentication system by assigning users to groups. Group membership is typically leveraged for assigning the same privileges to a user group. If the users reside in an external repository, the group membership information must be also kept there.

Cisco Identity Services Engine provides an Active Directory as a policy element when AD integration is configured. You can download the appropriate groups from AD into the dictionary. Group membership is then an attribute that can be referenced in conditions that define the requirements for context sensitive polices that are assigned by ISE.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Active Directory Integration Methods

This topic describes the methods of integrating Cisco Identity Services Engine with the Active Directory.



LDAP is a standards-based networking protocol for querying and modifying directory services that run on TCP/IP. LDAP is a lightweight mechanism for accessing an X.500-based directory server. Cisco ISE integrates with an LDAP external database by using the LDAP protocol.

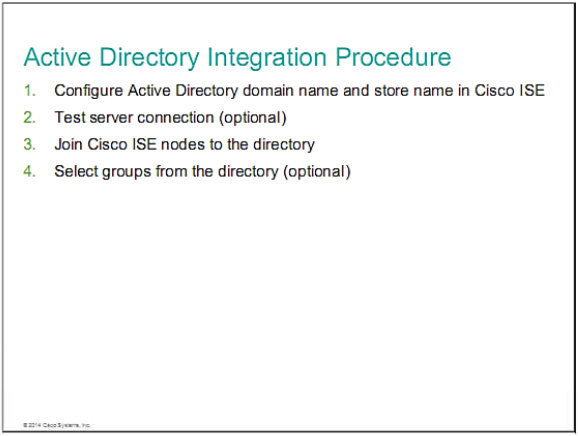
An LDAP directory is organized in a simple tree hierarchy and can be distributed among many servers. Each server can have a replicated version of the total directory, which is synchronized periodically. An entry in the tree contains a set of attributes. Each attribute has a name (an attribute type or attribute description) and one or more values. The attributes are defined in a schema. Cisco ISE has three preconfigured LDAP schemas: Active Directory, Sun Directory Server, and Novell eDirectory.

You can access the Active Directory database either as Active Directory or as LDAP server. Both methods have their pros and cons. If you connect to the AD repository using the Active Directory method, you gain the advantages resulting from the direct tie between the ISE and AD: an extensive attribute range, good performance, search up or down the tree. In this fashion, the ISE can join only a single directory. If you connect to the AD as an LDAP server, you gain the option of joining multiple directories. This method, however, slows down the performance, offers fewer attributes, and supports search down the tree only.

https://t.me/learningnets

Active Directory Integration Procedure

This topic describes how to integrate Cisco Identity Services Engine with an Active Directory database.



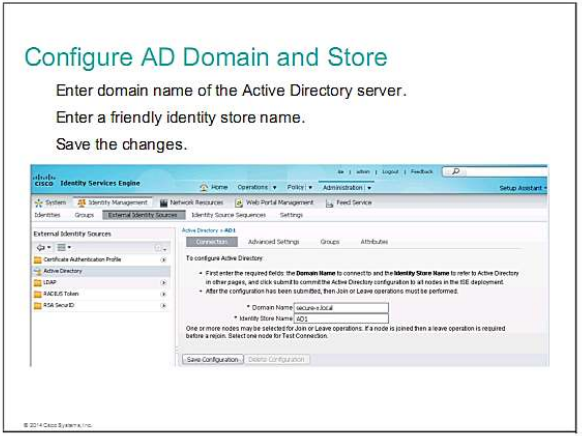
Perform these steps to integrate the Cisco Identity Services Engine with an Active Directory database:

1. Configure Active Directory domain name and store name in Cisco ISE
2. Test server connection (optional)
3. Join Cisco ISE nodes to the directory
4. Select groups from the directory (optional)

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Configure AD Domain and Store

This topic describes how to configure the AD domain and store.

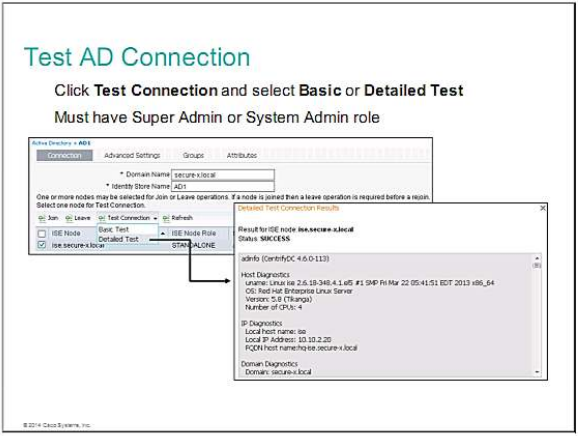


To connect to an Active Directory domain, complete the following steps:

1. Choose **Administration > Identity Management > External Identity Sources**.
2. From the External Identity Sources navigation pane on the left, click **Active Directory**. The Active Directory page appears.
3. Enter the domain name in the Domain Name text box.
4. Enter a friendly name in the Identity Store Name text box for your Active Directory identity source (by default, this value will be AD1).
5. Click **Save Configuration**. Saving the configuration saves the Active Directory domain configuration globally (in the primary as well as the secondary Policy Service nodes).

Test AD Connection

This topic describes how to test the connection to the Active Directory.



After you save the domain name and identity store name, you are presented with the options to join, leave the joined directory, and test the connection to the domain.

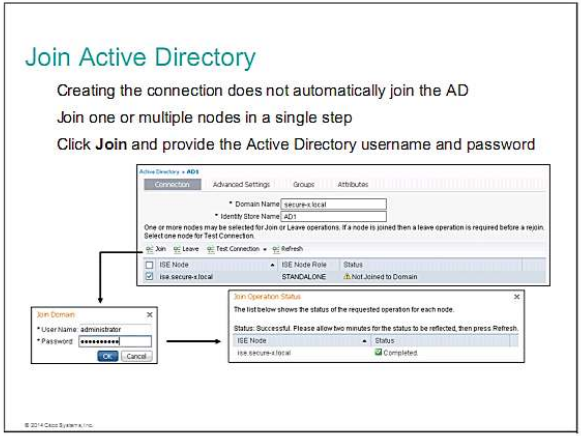
You may test the connection by selecting a specific node from the deployment, clicking the **Test Connection** button, and choosing one of two available methods: **Basic Test** or **Detailed Test**. The difference between the two types lies in the output verbosity.

When you click the **Test Connection** button, a dialog box appears and prompts you to enter the Active Directory username and password.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Join Active Directory

This topic describes how to join the Cisco Identity Services Engine to the Active Directory.

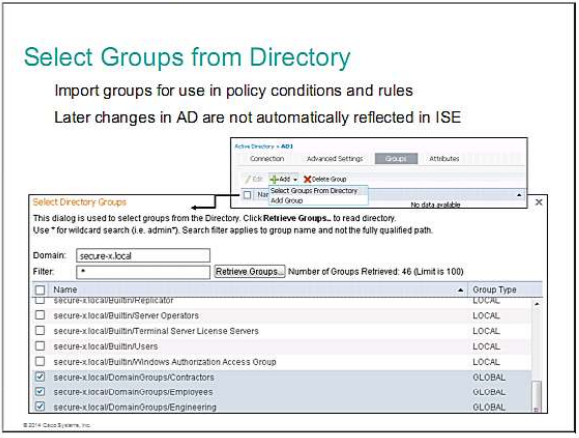


Although you submitted the configuration in a previous step, you have to click **Join** to connect your Cisco Identity Services Engine node to the Active Directory domain. You must manually perform the Join operation for each Policy Service node that should be connected to the Active Directory domain.

In the **Administration > System > Active Directory Operations** menu, choose the node to be joined, click **Join**, and enter the Active Directory administrator username and password in the Join Domain dialog box that appears.

Select Groups from Directory

This topic describes how to select groups from the directory.



When the Cisco Identity Services Engine has joined the Active Directory domain, you can retrieve groups for use with authentication and authorization policies. The retrieved groups are kept on the Cisco ISE and do not change in Cisco ISE when the group information changes in the Active Directory. To update the group information on the Cisco ISE, you need to repeat the retrieve operation.

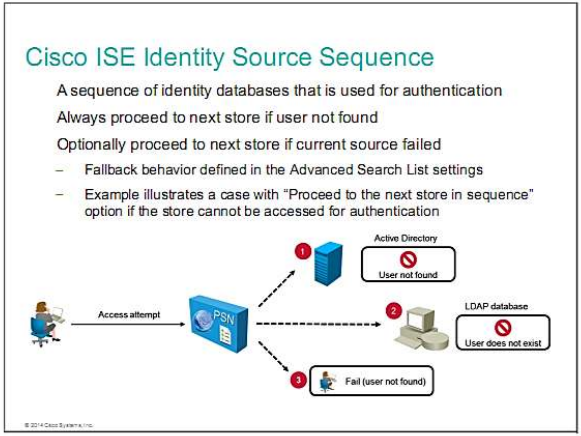
To configure Active Directory groups that will be available for use in authorization policy conditions, navigate to the **Administration > Identity Management > External Identity Sources** menu and select **Active Directory**. Select the **Groups tab** and the **Add > Select Groups From Directory** from the toolbar. Enter the domain name and optionally a filter, and click **Retrieve Groups**. Adding a group in the Cisco ISE does not create the group within the Active Directory database.

The Cisco ISE pulls the group information from the directory and presents the groups in a list. Note, the maximum number of groups that are retrieved with a single query is 100. If your query filter matches more than 100 groups, the group list will be truncated. You can check the groups that should be retrieved and uncheck the ones that you will not use in authentication and authorization definitions. All retrieved groups are checked by default.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Cisco ISE Identity Source Sequence

This topic describes the Cisco Identity Services Engine identity source sequences.



Identity source sequences define the order in which the Cisco ISE will look for user credentials in different databases. If your user information is in more than one database that is connected to your Cisco ISE, you can define the order in which you want the ISE to look for user information in these databases.

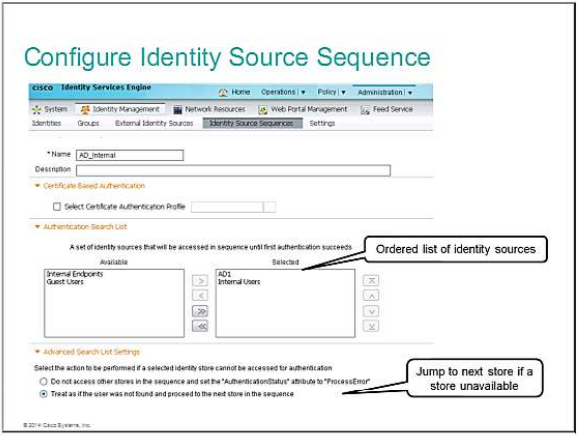
Once a match is found, Cisco ISE does not look any further, but evaluates the credentials and returns the result to the user. This policy is the first match policy.

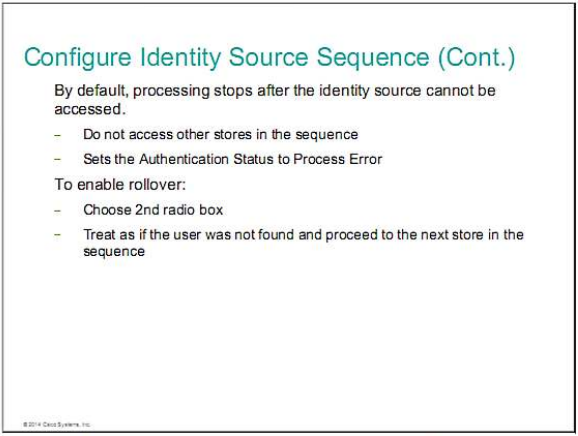
The Cisco ISE behavior is configurable for situations when a certain database cannot be accessed. The two available settings are to continue searching other databases or stop processing.

This example illustrates an identity source sequence of three databases: Active Directory, LDAP, and an internal ISE database. The user is not found in the AD database, and the ISE proceeds to searching the second source. Because the LDAP server is down and the option "Proceed to the next store in the sequence" has been configured, the Cisco ISE falls back to the third identity source. As the user does not exist in the internal ISE database, the authentication fails.

Configure Identity Source Sequence

This topic describes how to configure the identity source sequence.





These two options define the behavior when the database is not accessible:

Do Not Access Other Stores in the Sequence: This option is the default method. It causes the Cisco Identity Services Engine to stop processing the list.

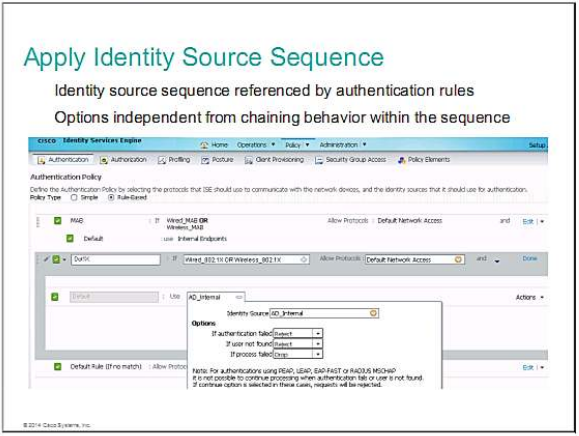
Treat as if the User Was Not Found and Proceed to the Next Store in the Sequence: This method enables failover to the next source if the database is not reachable.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

This example illustrates how to configure an identity source sequence that consists of four sources: Active Directory database, an LDAP repository, the internal user database, and the internal endpoint database.

Apply Identity Source Sequence

This topic describes how to apply the identity source sequence in the authentication policy.

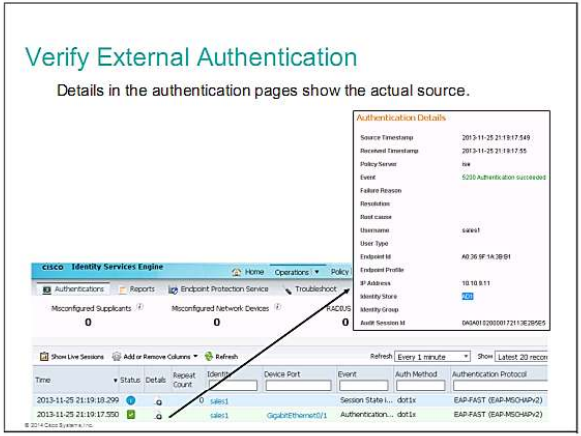


Identities source sequences are applied to the authentication policy rules as results alongside with the allowed protocol specification. The configurable options for the failure scenarios if authentication failed, if user not found, or if process failed describe the failover behavior for the entire sequence, not for its individual identity sources. The failover behavior within the identity source sequence id defined inside the sequence itself and was shown earlier.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Verify External Authentication

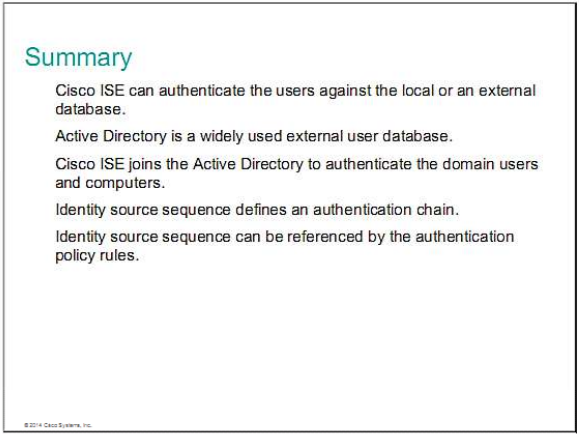
This topic describes how to verify external authentication.



The Cisco Identity Services Engine dashboard provides a summary of all authentications that take place in your network in the **Operations > Authentication** menu. You can click on the **Details** button and see what identity source has been actually used to authenticate the client. In this example, sales1 is a domain user and has been authenticated in the Active Directory.

Summary

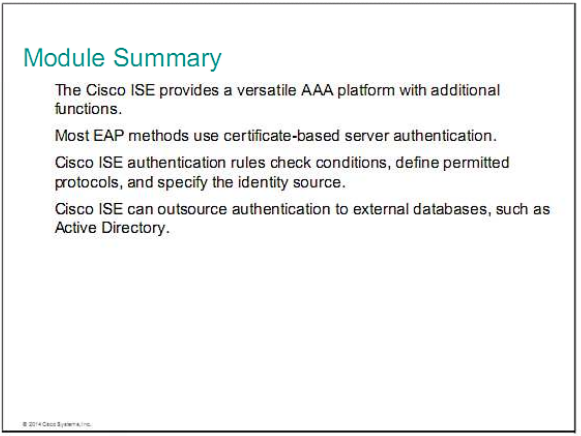
This topic summarizes the key points that were discussed in this lesson.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Module Summary

This topic summarizes the key points that were discussed in this module.



References

For additional information refer to this resource:

Cisco Identity Services Engine User Guide

https://t.me/learningnets

https://t.me/learningnets

Module Self-Check

Questions

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

1. Which Cisco ISE node acts as the RADIUS server to the network access devices? (Source: Cisco ISE Overview)

   A. admin
   B. policy service
   C. monitoring
   D. troubleshooting
   E. monitoring and troubleshooting

2. Which two options are Cisco ISE personas? (Choose two.) (Source: Cisco ISE Overview)

   A. admin
   B. reporting
   C. policy service
   D. profiler
   E. inline posture

3. How would you deploy Cisco ISE personas in a four node deployment? (Choose two.) (Source: Cisco ISE Overview)

   A. One node dedicated to admin persona
   B. Only one node dedicated to policy services persona
   C. Two nodes dedicated to admin and monitoring personas, with reversed primary and secondary roles
   D. Policy services persona running on all four nodes

https://t.me/learningnets

4. Which statement describes the relation between certificate validation and time accuracy? (Source: Cisco ISE PKI)

   A. Time difference between the communicating parties must be shorter than 5 minutes
   B. Time must be synchronized between the communicating parties
   C. The current time on one end must fall within the validity range of the other system's certificate
   D. Time check is optional

5. For which two services can you enable the identity certificate on the ISE? (Choose two.) (Source: Cisco ISE PKI)

   A. EAP exchange
   B. Certificate signing
   C. HTTPS negotiation
   D. Secure RADIUS
   E. IKE

6. Which two protocols use certificate-based server authentication? (Choose two.) (Source: Cisco ISE PKI)

   A. PEAP (EAP-MSCHAPv2)
   B. EAP (EAP-MSCHAPv2)
   C. EAP-FAST (EAP-MSCHAPv2)
   D. EAP-TLS (EAP-MSCHAPv2)
   E. EAP-MSCHAPv2

7. Which two are checked or applied in an ISE authentication rule? (Choose two.) (Source: Cisco ISE Authentication)

   A. allowed protocols
   B. profile
   C. status
   D. complex condition
   E. identity source

8. Which two are policy elements on the Cisco ISE? (Choose two.) (Source: Cisco ISE Authentication)

   A. Attribute
   B. Result
   C. Policy
   D. Rule
   E. Compound condition

9. You have to configure authentication policy for the ISE to accept authentication requests? (True or false) (Source: Cisco ISE Authentication)

   A. True
   B. False

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

10. Which two options can use when integrating ISE with two AD domains? (Choose two.) (Source: Cisco ISE External Authentication)

    A. Access both as Active Directory
    B. Access both as LDAP
    C. Access one as Active Directory, another as RADIUS
    D. Access one as Active Directory, another as LDAP
    E. Access one as LDAP, another as RADIUS

11. Can you deploy EAP chaining with Active Directory? (Source: Cisco ISE External Authentication)

    A. Yes, with EAP-FASTv1
    B. Yes, with EAP-FASTv2
    C. Yes, with EAP-FASTv3
    D. Yes, if Active Directory is accessed as LDAP
    E. No, the required EAP method is not supported with Active Directory

12. An identity source sequence by default checks the next store if the previous store is unavailable. (True or false) (Source: Cisco ISE External Authentication)

    A. True
    B. False

https://t.me/learningnets

Answer Key

1. B
2. A, C
3. C
4. C
5. A, C
6. A, C
7. A, E
8. B, E
9. B
10. B
11. B
12. B

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Module 3

Advanced Access Control

This module describes certificate-based client authentication, Cisco Identity Services Engine authorization, Security Group Access (SGA) and MAC Security (MACsec). These features provide enhanced access control capabilities in the Cisco ISE solution.

The Cisco Security Group Access (SGA) solution uses the device and user identity information that it obtains during authentication to classify the packets as they enter the network. This packet classification is maintained by tagging packets when they enter the SGA network so that they can be properly identified for the purpose of applying security and other policy criteria along the data path. The tag, also called the security group tag (SGT), allows the ISE to enforce access control policies by enabling the endpoint device to act upon the SGT to filter traffic.

MACsec is the IEEE 802.1AE standard for authenticating and encrypting packets between two MACsec-capable devices.

Upon completing this module, you will be able to:

- Describe certificate-based client authentication in EAP-TLS.
- Describe the authorization in Cisco ISE.
- Describe the Cisco Security Group Access (SGA) solution and MACsec.

https://t.me/learningnets

https://t.me/learningnets

Lesson 1

Certificate-Based User Authentication

Advanced Access Control

This lesson describes certificate-based client authentication, which is used in EAP-TLS. EAP-TLS advantages include the openness of the standard, wide vendor support, and high security. The disadvantages of the EAP-TLS method include the need to provision the client certificates and additional PKI requirements.

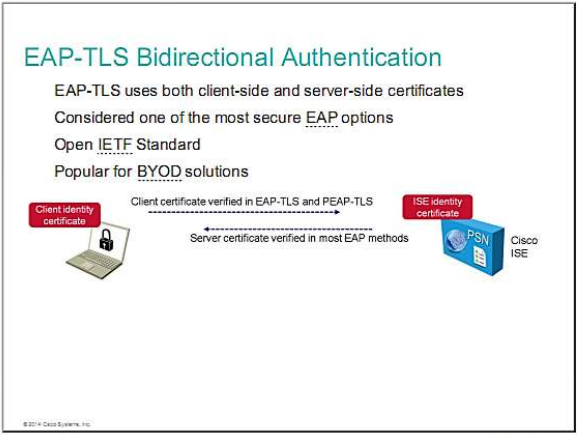
Upon completing this lesson, you will be able to:

- Describe the use of certificates
- Describe the verification of the client certificates
- Describe the implementation procedure for certificate-based client authentication
- Describe how to identify the CA root certificate used for verification of EAP sessions.
- Describe how to deploy certificates on clients
- Describe how to configure the 802.1X supplicant to use EAP-TLS
- Describe how to configure the 802.1X supplicant to use appropriate certificates
- Describe the certificate authentication
- Describe how to apply the certificate authentication profile to an identity source sequence
- Describe how to verify the EAP-TLS operation

https://t.me/learningnets

EAP-TLS Bidirectional Authentication

This topic describes the use of certificates.



EAP-TLS utilizes client-side certificates in addition to server-side certificates. Generally both the client and the server must enroll with the same PKI. Both the client and the server hold a copy of their own identity certificate and a copy of the CA root certificate. When EAP-TLS initiates, both sides will present their identity certificate to the other and both sides will use the CA's public key to verify the signature on the other's identity certificate.

The fact that EAP-TLS uses certificates in a bi-directional fashion, it is considered one of the most secure EAP options. There are no concerns with password capture when using EAP-TLS.

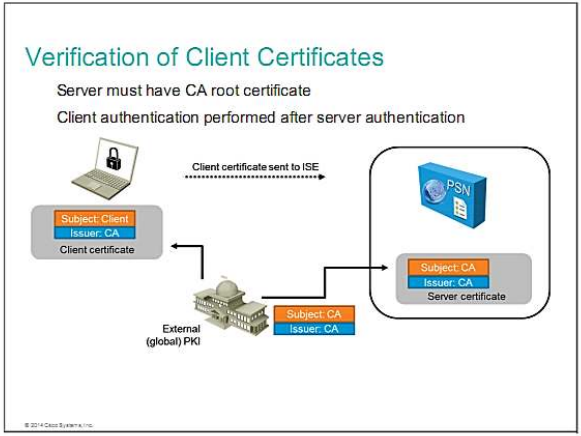
EAP-TLS is an IETF open standard. Virtually all networking vendors support EAP-TLS and it does not require Active Directory on the back end.

EAP-TLS is becoming a popular protocol to support BYOD in the enterprise. One complaint that is often leveraged against EAP-TLS is that there is too much management overhead involved in the provisioning of certificates for every client. This disadvantage may actually be turned into an advantage if strong control over which devices are allowed to access the network is desired. It is relatively easy to set up a policy that doesn't allow connectivity of devices unless they have gone through the certificate provisioning process. Control certificate provision and you control which devices are allowed access.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Verification of Client Certificates

This topic describes the verification of the client certificates.

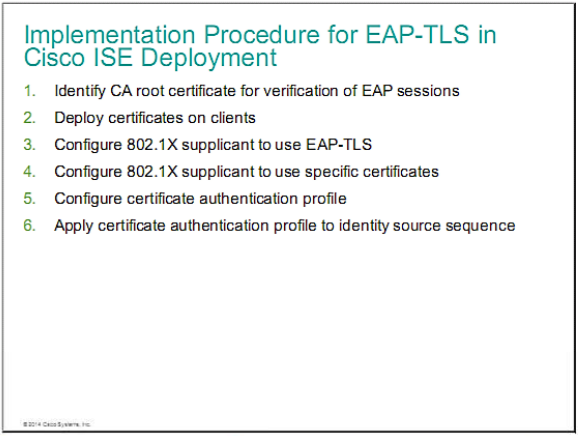


In a Cisco Identity Services Engine deployment, it is the Policy Service Node that acts as the RADIUS server.

With EAP-TLS, the server uses the same process as the client for verifying the peer identity. Both the client and the server have enrolled with the same PKI and hence both have their own identity certificate and the CA root certificate. Potentially they will have the chain of certificates leading to the root CA if the PKI is hierarchical. The server uses the CA's public key, obtained from the CA root certificate to verify the signature on the certificate presented by the client. If the signature proves valid, then the public key included in the the client's certificate must also be valid. The server challenges the client to prove that the client has the private key associated with the public key in the certificate. If the client passes the challenge, its identity is verified.

Implementation Procedure for EAP-TLS in Cisco ISE Deployment

This topic describes the implementation procedure for certificate-based client authentication.



Follow these steps to configure certificate-related tasks on the Cisco Identity Services Engine and on the clients:

1. Identify CA root certificate for verification of EAP sessions.
2. Deploy certificates on clients.
3. Configure 802.1X supplicant to use EAP-TLS.
4. Configure 802.1X supplicant to use specific certificates.
5. Configure certificate authentication profile.
6. Apply certificate authentication profile to identity source sequence.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Select CA Certificate for EAP Verification

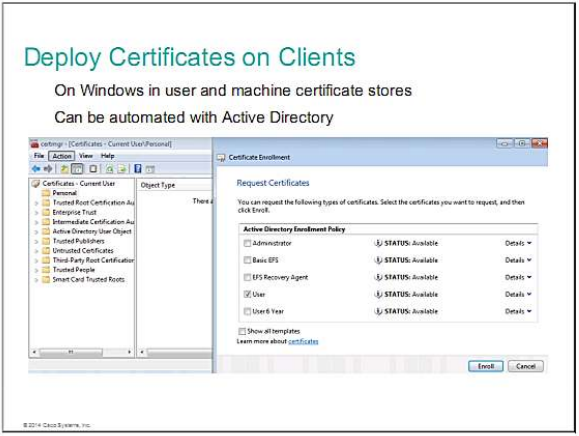
This topic describes how to identify the CA root certificate used for verification of EAP sessions.



Cisco Identity Services Engine must have the "Trust for client authentication or Secure Syslog services" option enabled for the root CA certificate for ISE to support EAP-TLS. When enrolling ISE into a PKI, one of the first steps of the process is to import the CA root certificate into ISE's certificate store. At the time of import, you have the option enable this option. If the option needs to be modified after the root certificate was imported, the certificate settings can still be edited under **Administration > System > Certificates > Certificate Store**.

Deploy Certificates on Clients

This topic describes how to deploy certificates on clients.

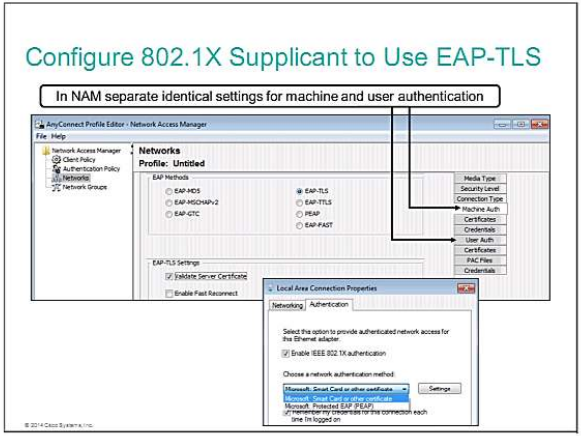


The certificate deployment process for the clients varies based on the operating system and supplicant type. The Windows operating system has two certificate stores: user and machine. The user certificate store is used when a user is logged on. Note, if there are multiple user accounts on a single system, each user will have their own certificate store. The logged on user will be able to access their own certificate store, but not those of other users. The current user can use a certificate from their user store or from a smart card to authenticate to the Cisco Identity Services Engine. The user certificate store can be viewed and managed using the certmgr.msc or the MMC utility. The machine certificate store is consulted for EAP challenges when no user is logged on. It is used to authenticate the computer to the server. The machine certificate store can be viewed and managed with the MMC program by those who have the appropriate domain account privileges. Certificate provisioning can be cumbersome and is often the reason why enterprises are reluctant to deploy EAP-TLS. It can be automated or made semi-automatic in an Active Directory environment.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Configure 802.1X Supplicant to Use EAP-TLS

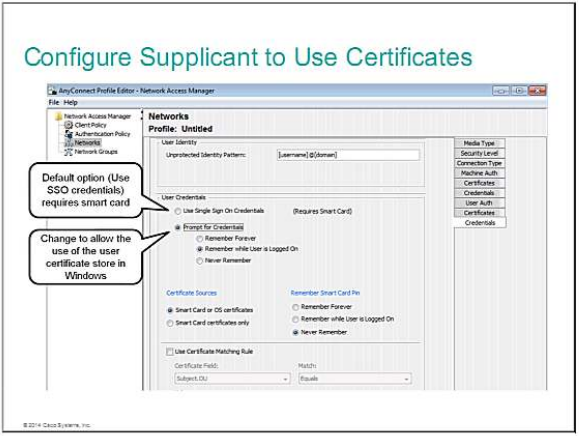
This topic describes how to configure the 802.1X supplicant to use EAP-TLS.



The common 802.1X supplicants do not use EAP-TLS by default. For example, the Network Access Manager of AnyConnect uses EAP-FAST by default. To configure the NAM for EAP-TLS, it must be selected as the EAP method and the option to validate the server credentials must also be selected. This must be configured independently for machine authentication and user authentication. In the Windows native supplicant you need to choose the Smart Card or other certificate option.

Configure Supplicant to Use Certificates

This topic describes how to configure the 802.1X supplicant to use appropriate certificates.

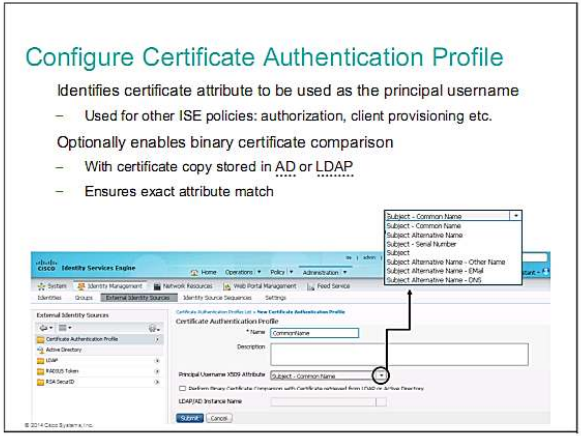


By default, the AnyConnect supplicant requires that a smart card is used to provide the user certificates. To allow the use the user certificate store in the OS, you need to change the setting to **Prompt for Credentials** the profile editor. The sub-option **Remember while User is Logged On** will allow the users logon credentials to be passed to the server without bothering the user with an additional prompt.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Configure Certificate Authentication Profile

This topic describes the certificate authentication profiles.



Certificate authentication profiles are used in authentication policies for certificate-based authentications to verify the authenticity of the user. The certificate authentication profiles allow you to do the following:

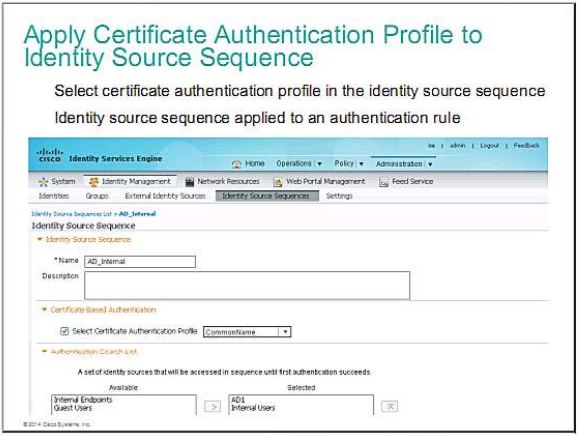
Specify the certificate field that should be used as the principal username. Using this option, Cisco Identity Services Engine verifies if the certificate field has the same value as the username in the identity source. You can set this value to the Common Name, Subject Alternative Name, Subject Serial Number, Subject, Other Name, Email, or DNS.

Specify if a binary comparison of the certificate should be performed. If this option is enabled, Cisco ISE retrieves the user certificate from the identity source and compares it, based on each octet, with the received client certificate. Client certificates can be retrieved from Active Directory or LDAP servers.

https://t.me/learningnets

Apply Certificate Authentication Profile to Identity Source Sequence

This topic describes how to apply the certificate authentication profile to an identity source sequence.

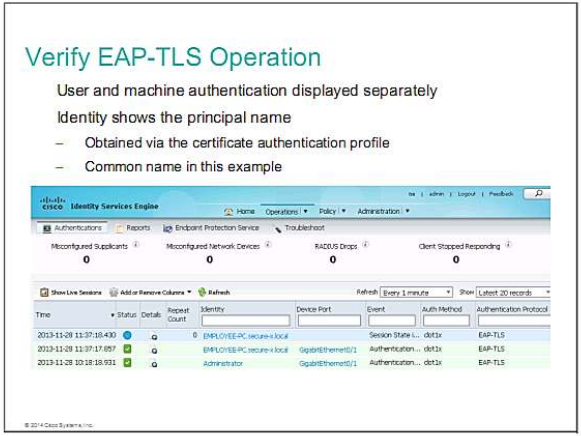


Certificate based authentication is an option that must be enabled in the identity source sequence. When this option is enabled, you must select a previously defined certificate authentication profile. The job of the certificate authentication profile is to specify which field in the client identity certificate identifies the username or machine name and whether or not a binary comparison with a copy of the certificate stored in AD or LDAP is required. Once this option is set in the identity source sequence, the identity source sequence is in turn referenced by an authentication rule.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Verify EAP-TLS Operation

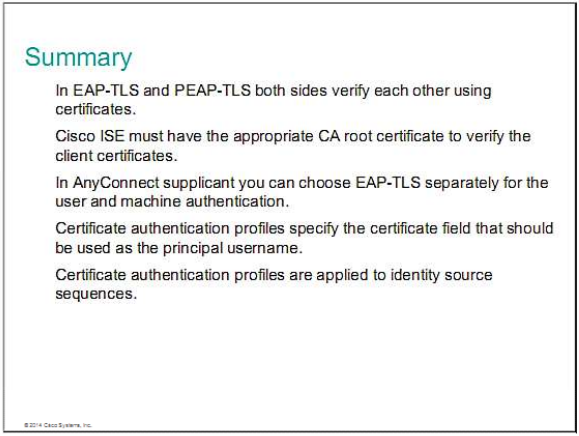
This topic describes how to verify the EAP-TLS operation.



You can view the successful authentications in Cisco Identity Services Engine under **Operations > Authentications > Show Live Authentications**. One of the optional columns to display is Authentication Protocol. The contents of this column can be used to verify the use of EAP-TLS for authentication. The sample output depicted shows two EAP-TLS authentications: one user and one machine. The machine authentication is performed when the user is logged off. The identity displayed in the Identity column is the principal name extracted from the certificate as specified by the certificate authentication profile. In this example the common name has been extracted from the certificate.

Summary

This topic summarizes the key points that were discussed in this lesson.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Lesson 2

Authorization

This lesson describes the authorization in Cisco Identity Services Engine. Authorization is performed after authentication, when the identity of the client is already established. The authorization attributes that are sent via RADIUS to the network access devices are first configured in the ISE as authorization profiles. The authorization policy applies the authorization profiles to the client sessions when appropriate conditions are met.

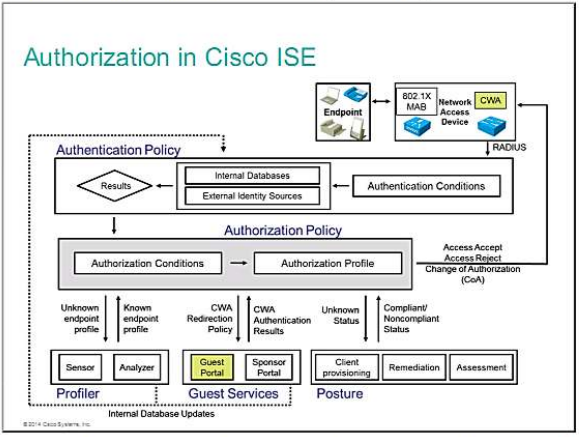
Upon completing this lesson, you will be able to meet these objectives:

- Describe the authorization in the Cisco Identity Services Engine
- Provide an overview of the authorization policy
- Describe the downloadable ACLs
- Describe the authorization profiles
- Describe the authorization policy
- Describe how to build compound conditions
- Describe the authorization configuration procedure
- Describe the rule matching logic
- Describe how to configure an authorization profile
- Describe how to configure an authorization policy rule
- Describe how to tune the default authorization rule
- Describe how to verify the authorization in the ISE GUI
- Describe how to verify machine authorization in the ISE GUI
- Describe how to verify the authorization in the ISE GUI
- Describe how to verify the dACL assignment on the authenticator

https://t.me/learningnets

Authorization in Cisco ISE

This topic describes the authorization in the Cisco Identity Services Engine.

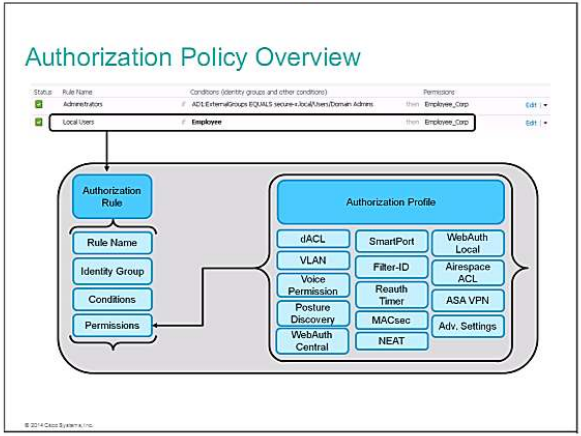


Cisco ISE performs authorization to assign privileges to client sessions. Authorization is performed after authentication when the client identity is established. The process flow on the Cisco ISE, as shown above, splits after authentication is complete. Three separate components—the posture service, the profiler, and the authorization—may be involved in these phases. The posture and profiler services can be used in addition to the authentication and authorization services and, if deployed, they may invoke additional information exchange.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Authorization Policy Overview

This topic provides an overview of the authorization policy.



Similar to authentication, the Cisco Identity Services Engine provides a modular approach to setting up the network authorization policy. The authorization policy is made up of rules. A rule has four components:

Rule Name: A unque alpha-numeric identifier for the rule. It is desirable for the rule name to imply the purpose or the intended context of the rule.

Identity Group: Specification of user or endpoint groups from ISE's internal databases. Any is an option, implying that internal group membership is not significant for this rule. Multiple groups may be specified with a logical OR binding. That is, if multiple groups are specified, membership in any of the groups will result in a match. Examples of groups that may be defined and used include black lists, automatically profiled classes (such as Android, Apple-iDevice, or Cisco-IP-Phone), or classifications defined within the enterprise such as print servers or badge readers.

Conditions: Specification of contextual requirements for the rule. Simple conditions specify an attribute selected from an ISE dictionary along with the value of the attribute required for the condition to match. Compound conditions link together multiple simple conditions with logical AND or OR relationships. Some common examples of attributes that can be specified with conditions include Active Directory group membership, connection type (Ethernet or Wireless - IEEE 802.11), or a wireless SSID (contained in the RADIUS Called-Station-ID field).

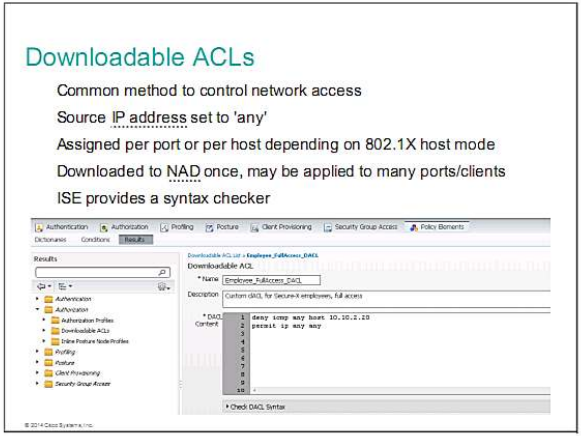
Permissions: Specification of the authorization profile. Authorization profiles are defined separately from the authorization rules. The authorization profile defines an appropriate set of permissions based on a context sensitive match with the identity group and conditions specified by the authentication rule. Common aspects defined in the authorization profile include a downloadable ACL or VLAN assignment. Sometimes authorization profiles are intended to be temporary. For example the profile could set up a posture check. After the posture check, depending on the results, another authorization profile would be enforced to either require posture remediation or to grant appropriate network access.

Cisco ISE is an attribute-based policy system. Identity groups and conditions are used to define what attributes are important for making policy decisions. Authorization profiles, as specified in an authorization rule's permissions, specify the results of the policy decision.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Downloadable ACLs

This topic describes the downloadable ACLs.



The Cisco Identity Services Engine policies are built from policy elements. Dictionaries, conditions and results are the three types of policy elements. A downloadable ACL is an example of result policy element. It is an example of an authorization policy result in particular. dACLs are very common elements used to restrict client access to network resources.

The dACLs are configured and maintained centrally on the Cisco ISE and pushed to the NAD when a client is granted access to the network. The NAD applies the dACL to the client access port in the incoming direction. The NAD will apply the dACL per port or per host depending on the configured 802.1X host mode.

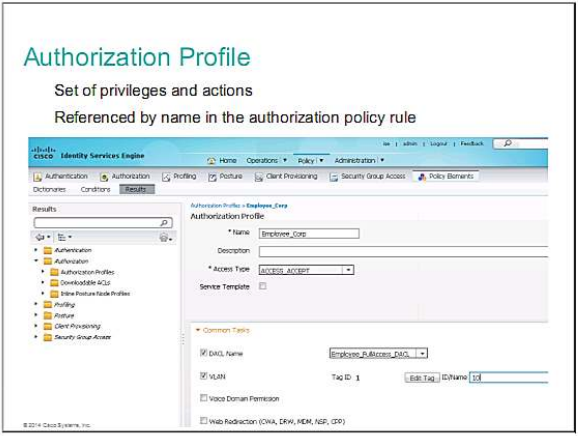
The source IP address configured in the downloadable ACLs is 'any'. The NAD will replace this statement with the actual host IP address. A dACL only needs to be downloaded to the NAD once. If the same dACL is specified in subsequent authorizations, it will not be re-downloaded. The copy that is already resident on the NAD will be applied to any other endpoints that use the same dACL.

The ISE provides a syntax checker to avoid user configuration errors. Cisco ISE is preconfigured with two default dACLs: DENY_ALL_TRAFFIC and PERMIT_ALL_TRAFFIC. These two dACLs, and any administrator defined dACLs, can be referenced by an authorization profile.

https://t.me/learningnets

Authorization Profile

This topic describes the authorization profiles.

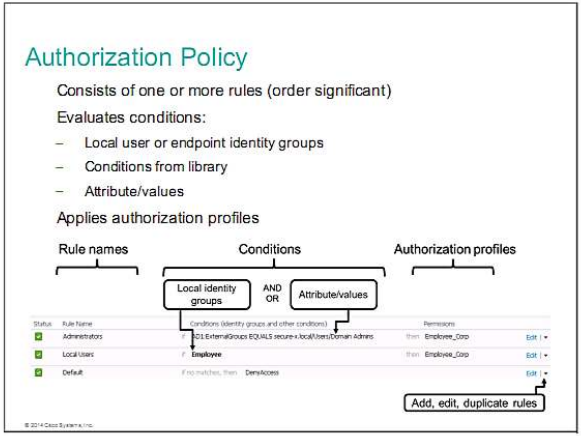


Authorization profiles consist of permissions that are chosen from a set of options. Authorization profiles are applied when an authorization rule that references them is matched. The authentication rules use identity group membership and context specific conditions to define when the authentication rule is applicable. If the requirements are met, then the authorization profile, referenced by name from the authorization rule, is applied. Downloadable ACL assignment, VLAN assignment and Voice Domain access are common examples of permissions specified by an authorization profile. But any setting supported by RADIUS on the device can be defined in the authorization profile.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Authorization Policy

This topic describes the authorization policy.

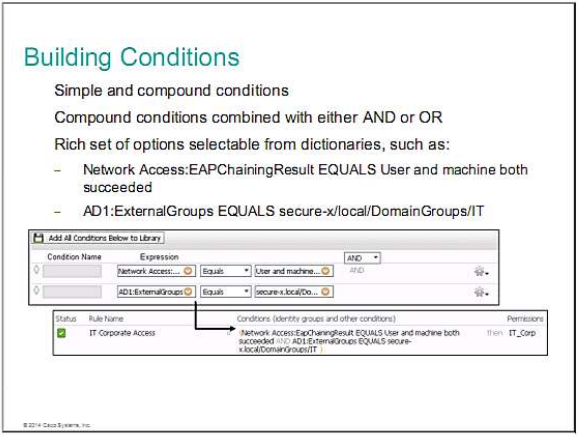


The Cisco Identity Services Engine authorization policy is made up of one or more rules. At deployment, ISE has one authorization rule named Default. It will match all conditions and permits all access. The ISE administrator defines authorization rules to implement the authorization policy. Each authorization rule is defined with a name, a specification of context conditions, and references an authorization policy. The options for specifying conditions are very flexible. Membership in locally defined user and device groups can be combined with attribute/value specifications using attributes defined in the many dictionaries available in ISE. Conditions can be defined within an authorization rule, or they can be defined in the library as an authorization policy element and referenced by one or more authorization rules. When the conditions of an authorization rule are met, the referenced authorization profile is applied. Defining an authorization profile in ISE has no effect unless that profile is referenced by an authorization rule.

The order of authorization rules in an authorization policy is significant. By default, ISE applies only the first matched rule. It can be configured to apply all matched rules. In either case, rule order is significant. If ISE is configured to apply all matched rules, and the rules specify different authorization aspects, for example the first specifies a VLAN and the second specifies a dACL, then both authorization aspects are applied. But, if multiple rules match and they specify the same authorization aspects, then the first match takes precedence. For example if the first matched rule specifies a VLAN and the second matched rule specifies a dACL and a VLAN, then the VLAN specified in the first matched rule and the dACL specified in the second matched rule are applied. The VLAN specified in the second matched rule is ignored. As with ACLs, proper design requires the more specific rules to be higher in the list and less specific rules to be lower in the list. Generally the last rule in the list will match anything and, depending on design requirements, will either permit all traffic or deny all traffic. The administrator has control of where new rules are inserted in the policy table and can move rules up and down in the policy table.

Building Conditions

This topic describes how to build compound conditions.



Conditions can be defined as part of an authorization policy rule or they can be defined as a policy element, added to the library, and then be referenced by one or more authorization policy rules.

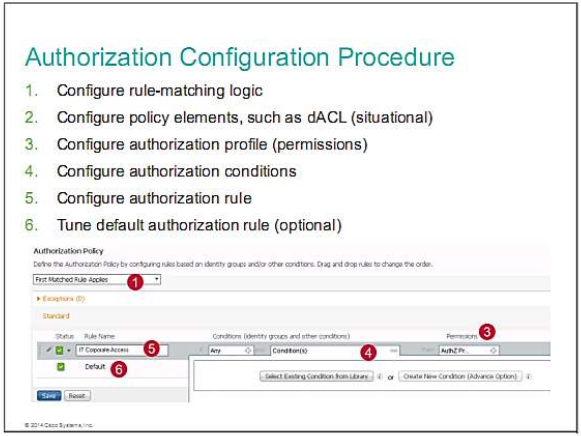
Simple conditions specify an attribute from one of the Cisco Identity Services Engine dictionaries, an operand, and a value. Compound conditions combine multiple conditions with either a logical AND or OR.

There is a robust set of attribute options available across the various Cisco ISE dictionaries. Among the many options, attributes can specify details such as Active Directory group membership, authentication results, network access device characteristics, identity certificate details, profiling results, and posture status.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Authorization Configuration Procedure

This topic describes the authorization configuration procedure.

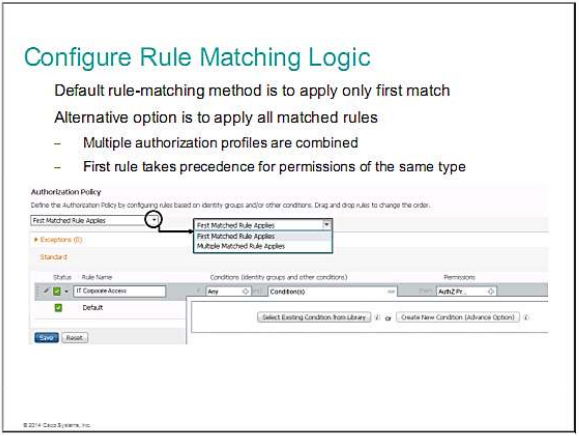


Follow this procedure to implement authorization on the Cisco Identity Services Engine:

1. Configure rule-matching logic (optional)
2. Configure policy element, such as dACL (situational)
3. Configure authorization profile (permissions)
4. Configure authorization conditions
5. Configure authorization rule
6. Tune default authorization rule (optional)

Configure Rule Matching Logic

This topic describes the rule matching logic.



The authorization policy consists of one or more rules that are processed in order.

You can define the processing logic of the authorization policy by choosing one of two options:

First Match Rule Applies: With this option, the Cisco Identity Services Engine applies the authorization profile that is referenced by the first matched rule and finishes the authorization processing for the given client. This option is the default behavior.

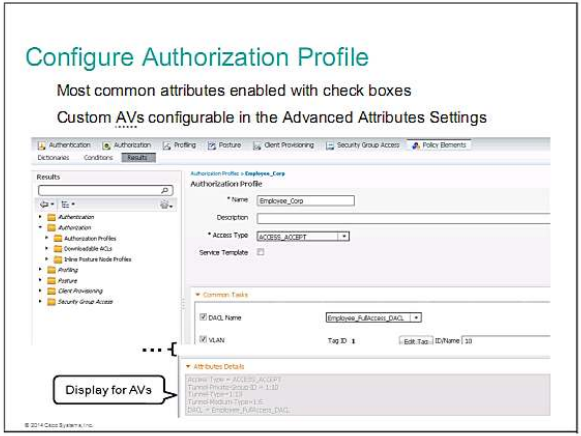
Multiple Matched Rule Applies: In this method, the Cisco ISE continues processing each rule until all rules have been applied. When multiple matching authorization policies are found, Cisco ISE combines the authorization profiles. The authorization profiles of all matched rules are combined and applied to the client. The first rule takes precedence for permissions of the same type.

Typically the processing logic is set before any authorization rules are defined. The rules are designed to operate according to the processing logic. Changing the processing logic after a set of rules are designed and implemented can lead to undesirable results.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Configure Authorization Profile

This topic describes how to configure an authorization profile.



Authorization profiles combine multiple policy elements into a set that can be applied to clients. Cisco Identity Services Engine comes preconfigured with several default authorization profiles, such as Blacklist_Access, Cisco_IP_Phones, DenyAccess, and PermitAccess. You can edit these built-in profiles, but it is not recommended. In practice, you will need more granularity. Therefore you need to create custom authorization profiles. A preconfigured authorization profile may be duplicated to be used as the starting point for the creation of custom authorization profiles.

Although not shown above in its entirety, authorization profiles allow you to configure these elements using appropriate check boxes:

dACL Name: This element is the name of the dACL, which is obtained from the Cisco ISE and applied to the session. The dACL will be applied per user for ports configured in Multi-Auth mode. The dACL is downloaded once per NAD, but can be applied to the session.

WLC ACL: The ACL applied to the endpoint on the WLC. Currently the name of the ACL gets pushed by the ISE.

VLAN: This element is the VLAN that is assigned to the access port as the access VLAN.

Voice Domain: In multidomain authorization mode, if the network switch receives this parameter, the endpoint is placed into the voice domain. This type of authorization is most common for Cisco IP phones.

Posture Discovery: This element is used to enable posture discovery of the endpoint.

Auto Smartport: Cisco Auto Smartport technology enables appropriate QoS parameters to be applied to the port according to a template.

Filter ID: The filter ID is an ACL name that is referenced by the Cisco ISE. The ACL must exist on the NAD and is applied to the client session as a result of the ISE authorization instructions.

Reauthentication: This element enables reauthentication of the endpoint.

https://t.me/learningnets

MACsec Policy: MACsec is the IEEE 802.1AE standard for authenticating and encrypting packets between two adjacent devices. Many Cisco Catalyst switches support 802.1AE encryption with MKA on downlink ports for encryption between the switch and host devices.

NEAT: The NEAT feature allows 802.1X implementation on a switch which is deployed in a non-secured location, such as a conference room, with an upstream connection to a physically secured switch. The downstream switch acts as the supplicant switch and the upstream switch acts as the authenticator switch. The CISP is used to by the downstream switch to identify all authenticated 802.1X hosts to the upstream switch.

Centralized Web Authentication: This element enables web authentication to be performed on Cisco ISE.

Local WebAuth: This value instructs the NAD to perform the authentication locally on the NAD. Cisco ISE sends the NAD a VSA along with a dACL.

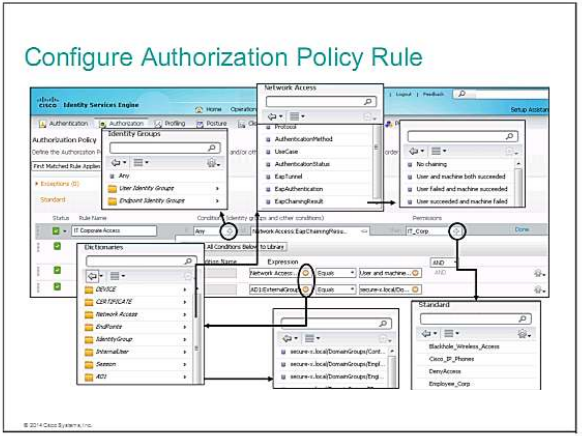
ASA VPN: This parameter enables an ASA VPN group policy to be applied to the endpoint VPN session.

In addition to these common attributes you can define custom AVs using the Advanced Attributes Settings section. All AVs, the common ones and the custom ones are displayed in the Attributes Details section.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Configure Authorization Policy Rule

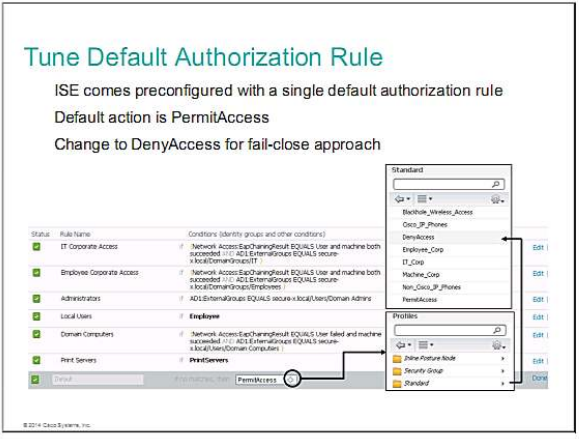
This topic describes how to configure an authorization policy rule.



The authorization policy consists of one or more authorization policy rules. Each rule has a name, specifies one or more conditions, and a permission setting that points to an authorization profile. The rows visible in the **Policy > Authorization** menu represent the individual rules. You can drag and drop the rules to change the sequence. You can create new rules, duplicate and delete the existing rules using the **Edit** button. This figure illustrates the options of clicking various fields in the Cisco Identity Services Engine GUI to open the appropriate attribute dictionaries, and select the appropriate values.

Tune Default Authorization Rule

This topic describes how to tune the default authorization rule.



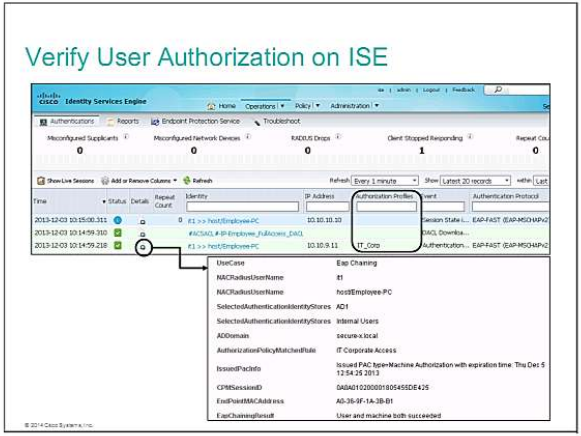
The default rule is the final rule in the authorization policy that is used to define the handling of all client access requests that do not match any explicit authorization rule. Typically, you will tune the default rule, because its preconfigured action is set to PermitAccess, which activates a fail-open logic. This default will lead to less service disruptions during early phases of deployment, but it is not recommended in most enterprise scenarios.

This example shows how to tune the default authorization rule. You click the **plus** symbol near the PermitAccess action, which is the default action within the default authorization rule. You are presented with three permission categories: Inline Posture Node, Security Group, and Standard. You select the **Standard** category and choose your desired authorization profile.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Verify User Authorization on ISE

This topic describes how to verify user authorization in the Cisco Identity Services Engine GUI.



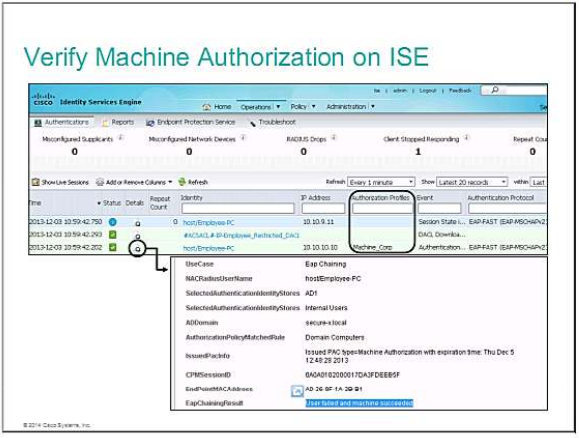
The Cisco ISE dashboard provides a summary of all authentications that take place in your network in the **Operations > Authentication** menu. If you activate the Authorization Profiles column you will see the authorization profile that has been applied to the endpoint.

The top figure depicts the authentication and authorization results of user it1 accessing from a corporate asset. You can recognize the EAP chaining use case by the >> sign between the user and machine identity. Consequently an appropriate authorization profile has been pushed to the session.

You can drill down into an authentication event and examine the RADIUS authentication details. The bottom figure illustrates a fragment of the detailed information. The Use Case is reported as EAP Chaining with the EAP chaining result of 'User and machine both succeeded."

Verify Machine Authorization on ISE

This topic describes how to verify machine authorization in the Cisco Identity Services Engine GUI.

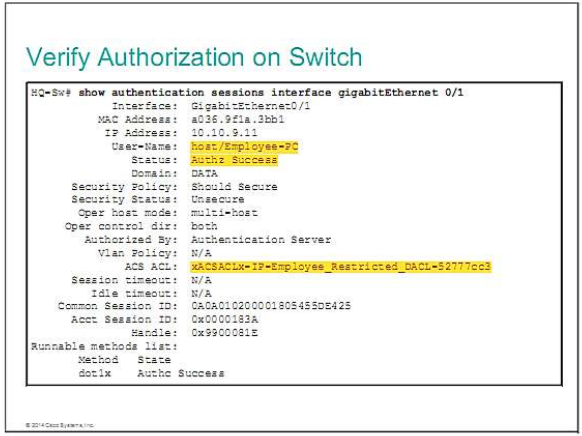


This figure shows an access attempt of the Employee-PC computer, when no user is logged on. The Employee-PC is a corporate-owned asset and for this particular access attempt the authorization profile Machine_Corp is applied. The bottom figure shows the details, where the Use Case is reported as EAP Chaining with the EAP chaining result of "User failed and machine succeeded."

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Verify Authorization on Switch

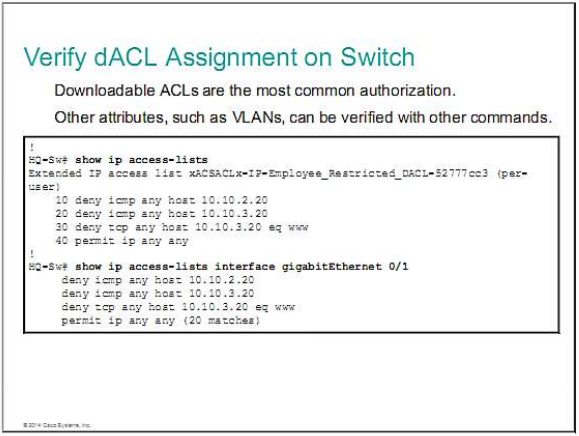
This topic describes how to verify the authorization status on the authenticator.



You may monitor the authentication and authorization results on the NADs in addition to viewing them on the Cisco Identity Services Engine. The output of the **show authentication session interface** command includes the username of the authenticated user and the authorization results. The status of session reports Authorization Success, and a dACL is applied to the endpoint. The NAD is not aware of the authorization profile name that has been used on the Cisco ISE to apply this ACL to the endpoint. It does, however, receive the name of the dACL as defined by ISE. The command output displays also the common session ID that is used for tracking a specific user session.

Verify dACL Assignment on Switch

This topic describes how to verify the dACL assignment on the authenticator.

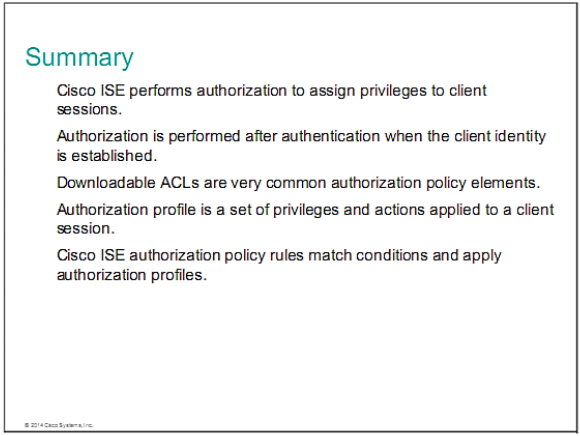


You can verify the dACL download and contents as it will dynamically appear amongst the IP access-lists present on the switch. Note that the **show ip access-lists** command annotates the dACL with "per user." If this dACL is assigned to multiple user sessions, it only needs to be downloaded once from Cisco Identity Services Engine. You can further verify the actual access list that has been applied to the access port. The output of the **show ip access-list interface** command displays the actual authorization results.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Summary

This topic summarizes the key points that were discussed in this lesson.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Lesson 3

Cisco TrustSec and MACsec

Cisco TrustSec simplifies the provisioning and management of secure access to network services and applications. Compared to access control mechanisms that are based on network topology, Cisco TrustSec defines policies using logical policy groupings, so secure access is consistently maintained even as resources are moved in mobile and virtualized networks. De-coupling access entitlements from IP addresses and VLANs simplifies security policy maintenance tasks, lowers operational costs, and allows common access policies to be applied to wired, wireless, and VPN access consistently.

MACsec is the IEEE 802.1AE standard for authenticating and encrypting packets between two MACsec-capable devices. Cisco switches support MACsec on downlink and switch-to-switch ports. Cisco AnyConnect provides MACsec capabilities via software for systems with NICs that do not have MACsec hardware support.

Upon completing this lesson, you will be able to meet these objectives:

- Provide an overview of Cisco TrustSec
- Describe the benefits of the Cisco TrustSec solution
- Describe the classification at the ingress
- Describe the inline SGT transport
- Describe the SGT Exchange Protocol
- Describe the enforcement on SGT-capable devices
- Describe the enforcement on SGT-aware devices
- Describe the SGA deployment procedure
- Describe how to configure CTS between ISE and a network device
- Describe how to define the security groups
- Describe how to implement dynamic classification
- Describe how to implement static classification
- Describe how to implement the SGT Exchange Protocol (SXP)
- Describe how to define SGACLs

https://t.me/learningnets

Describe how to implement SGACL enforcement

Describe how to implement SGFW Enforcement on the ASA

Describe the MAC Security (MACsec)

Describe the MACsec cryptographic features

Describe the MACsec hop-by-hop operation

Describe the downlink MACsec implementation on the ISE

Describe the downlink MACsec implementation on the NAM

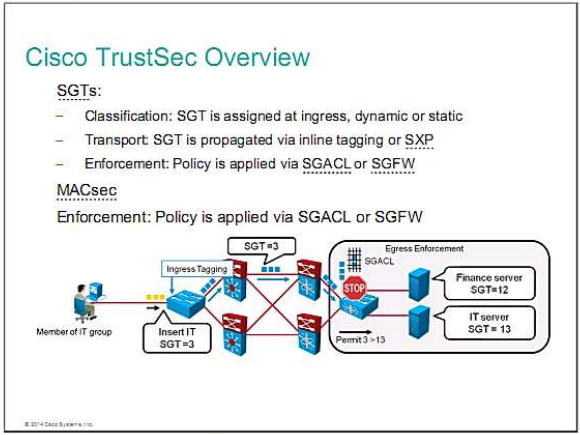
Describe the downlink MACsec implementation on the switch

Describe how to verify downlink MACsec

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Cisco TrustSec Overview

This topic provides an overview of the Cisco TrustSec solution.



Cisco TrustSec incorporates SGTs and MACsec.

Cisco TrustSec classification, transport and policy enforcement functions are embedded in Cisco switching, routing, wireless LAN, and firewall products. By classifying traffic based on the contextual identity of the endpoint versus its IP address, Cisco TrustSec enables more flexible access controls for dynamic networking environments and data centers. The features associated with SGTs on the network devices can be broken into three categories: Classification, Transport and Enforcement.

Classification: Classification is the assignment of SGT to an IP address. This can be accomplished either dynamically or statically. Generally, dynamic classification is done at the access layer and static classification is done in the data center. Dynamic classification utilizes the rich context data available to Cisco Identity Services Engine for making policy decisions. Dynamic classification can be done using 802.1X, MAC Authentication Bypass or Web Authentication. Static classification is generally configured on the switch to which servers are attached. Options for static classification include the mapping of IP address, VLAN or port to an SGT.

Transport: Security group mappings follow the traffic through the network. This can be accomplished either through inline tagging or the SGT eXchange Protocol (SXP). With inline tagging, the SGT is imbedded in the Ethernet frame header. Not all network devices support inline tagging. SXP is used to transport SGT mappings across devices that do not support inline tagging.

Enforcement: Enforcement is implementing a permit or deny policy decision based on the source and destination SGTs. This can be accomplished with SGACLs on switching platforms and SGFW on routing and firewall platforms.

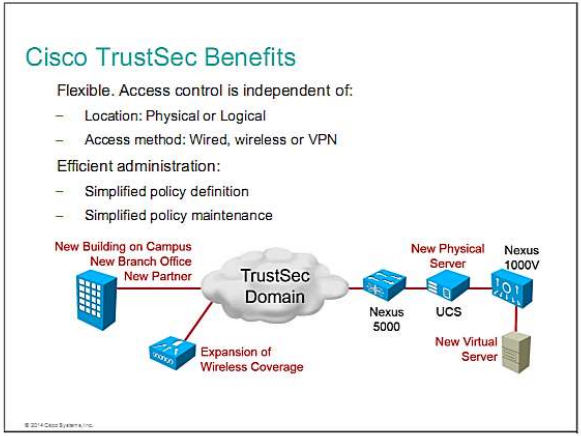
MACsec provides secure communication on wired LANs. When MACsec is used to secure the communication between endpoints on a LAN, each packet on the wire is encrypted using symmetric key cryptography so that communication cannot be monitored or altered on the wire. When MACsec is used in conjunction with Security Group Tags, it provides protection for the tag along with the data contained in the payload of the frame.

Support for Cisco TrustSec features varies by network device platform and software version. It is important to understand the capabilities of the devices available in the network early in the TrustSec solution design phase.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Cisco TrustSec Benefits

This topic describes the benefits of the Cisco TrustSec solution.



At the point of network access, a Cisco TrustSec policy group called a SGT is assigned to an endpoint. This is done considering any of a rich set of attributes including that endpoint's user, device type, posture status, and location attributes. The SGT denotes the endpoint's access entitlements, and all traffic from the endpoint will carry the SGT information. The SGT is used by switches, routers, and firewalls to make forwarding decisions. Because SGT assignments can denote business roles and functions, Cisco TrustSec controls can be defined in terms of business needs and not underlying networking detail. SGTs can span physical locations. SGTs are independent of IP address, subnet or VLAN. SGACL capable switches can implement access controls between systems with the same or different SGT values even if they are on the same VLAN.

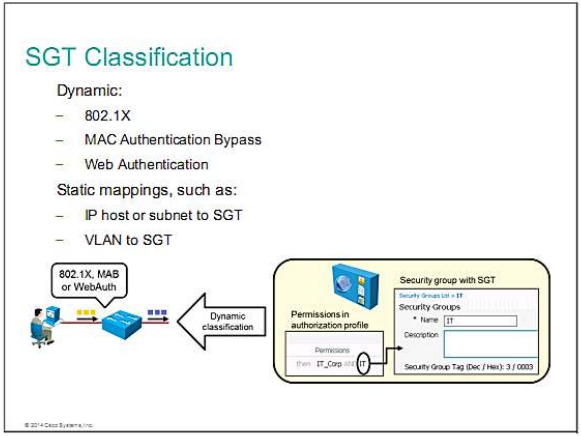
Instead of managing access control on large numbers of prefixed IP addresses, access control is managed across a relatively small number of relevant security group classifications. SGACLs define what services are accessible between two security groups. A simple matrix assigns all SGACLs to source and destination SGT pairs. One matrix provides all policy for the entire TrustSec domain.

When compared to traditional access control policy that is implemented with static ACLs deployed at strategic policy enforcement points, TrustSec offers much simpler maintenance procedures. Traditional ACLs tend to have repetitive entries that cover different source and destination IP addresses. For example, there may be repetitive entries that specify the same services for each subnet serviced by the campus wireless network to each corporate web server IP address. When a new wireless subnet is provisioned or a new web server is brought online, all of the associated ACLs must be updated. In large enterprise environments, these ACLs can be thousands of lines long and very complex. The figure above denotes several other common examples of network growth that would require substantial ACL revisions in a traditional implementation. Similar changes are necessary when aspects of a network are decommissioned such as when a server is retired or a branch office is consolidated. These events are much simpler to administer in a TrustSec solution. With a TrustSec implementation, the newly provisioned resource simply needs to have classification configured at ingress to properly maintain existing SGACL policy. In the event of an implementation that requires the introduction of a new security group, then a new row and column will be added to the matrix. This matrix is updated centrally on Cisco Identity Services Engine and dynamically propagated across the TrustSec domain.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

SGT Classification

This topic describes the classification at ingress.



The frames that enter the Cisco TrustSec domain are marked using a unique 16-bit tag that represents the unique role of the traffic source in the network. The tag can be thought of as a privilege identifier of the source user, device, or entity. The tagging decisions can either be dynamic, that is obtained from the Cisco Identity Services Engine for each client that attempts to access the network, or static.

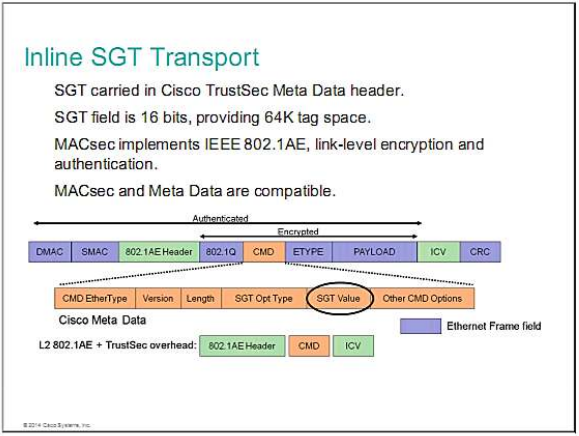
Dynamic tagging can be deployed in combination with 802.1X authentication, MAB authentication Bypass, or Web authentication. In these access methods, the Cisco ISE can push a SGT to the NAD to be inserted into the client traffic. The SGT is applied as a permission in the authorization policy rules. This permission can be assigned in addition to or instead of an authorization profile.

Static tagging can be configured on the NAD or on the ISE and then downloaded to the NAD. Examples of static tagging include a mapping of an IP host or subnet to a SGT, or the mapping of a VLAN to a SGT. Numerous other options exist, with varying support depending on the device platforms and software versions.

Because the SGT contains the security group of the source, the tag can be referred to as the source SGT. The destination device is also assigned to a security group (the destination SG) that can be referred to for simplicity as the DGT, although the actual Cisco TrustSec packet tag does not contain the security group number of the destination device.

Inline SGT Transport

This topic describes the inline SGT transport.



SGTs can be transported inline between two capable devices configured for Cisco TrustSec on their connecting interfaces. Using this method, the sending device will impose the SGT in the outgoing frame's Ethernet header on egress. The receiving device will read and process the SGT from the Ethernet header on ingress.

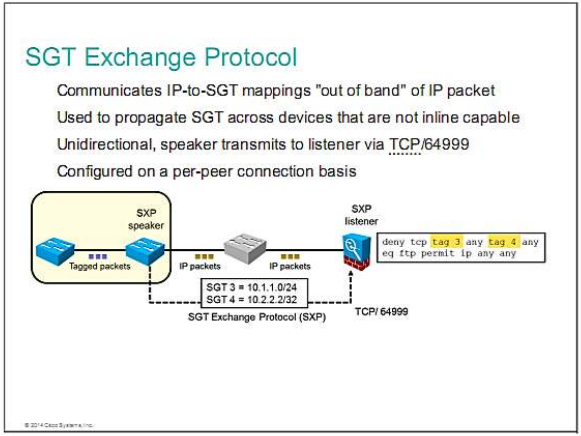
The SGT is imbedded in the Cisco TrustSec Meta Data header. As with other tagging protocols, such as 802.1Q, Meta Data uses a registered ethertype value. Meta Data uses ethertype 0x8909. The SGT is carried in a 16 bit field in the Meta Data header. There is about 20 bytes of overhead due to the use of the Meta Data header.

Frames crossing a link between capable switches may also be protected with MACsec. MACsec is an implementation of 802.1AE, and its header is marked with the ethertype 0x88E5. A MACsec protected frame will put the other tags and the data contained within the fame between the MACsec header and the ICV field. These tags and the frame data are all protected by MACsec encryption and authentication. The increase of the MTU size that results from both 802.1AE and Cisco TrustSec overhead is roughly 40 bytes. The figure illustrates the MACsec overview with the embedded Meta Data header carrying the SGT.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

SGT Exchange Protocol

This topic describes the SGT Exchange Protocol.



Not all Cisco devices are capable of inline SGT transport, nor are network devices from other vendors. SXP, a control plane protocol, allows the propagation of IP to SGT mappings across such boundaries. The main goal is to get the SGT data from the devices that performed classification of connecting endpoints to upstream devices which will perform Cisco TrustSec enforcement based on SGT information.

The SXP connections are point-to-point and use TCP as the underlying transport protocol, using TCP port number 64999 when initiating a connection. When configuring an SXP connection to an SXP peer, you must designate each device as a Speaker or a Listener for that connection. The Speaker mode allows the device to forward all active IP to SGT mappings to upstream devices for policy enforcement. The Listener mode enables a device to receive IP to SGT mappings from downstream devices and use that information in performing policy decisions.

If one end of an SXP connection is configured as Speaker, then the other end must be configured as a Listener, and vice versa. If both devices on each end of an SXP connection are configured with the same role (either both as Speakers or both as Listeners), the SXP connection will fail. Care must be taken when configuring SXP connections to avoid creating loops, unless SXP version 4 or above is deployed. SXP is an evolving protocol. It is important to understand and consider SXP version support on the devices in your network during the Cisco TrustSec solution design. The following summarizes the capabilities of SXP versions 1 through 4:

Version 1: Initial version. Supports IPv4 binding propagation.

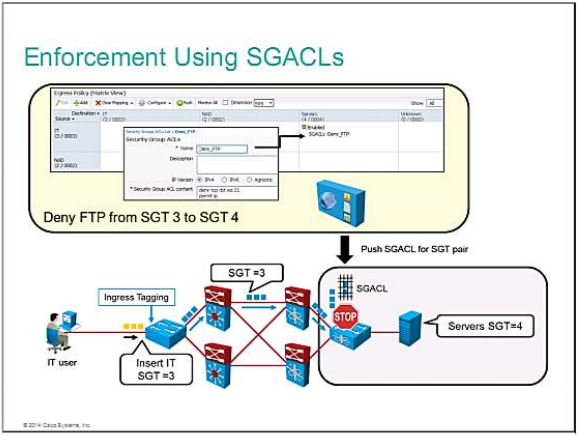
Version 2: Added IPv6 binding propagation and version negotiation.

Version 3: Added support for Subnet to SGT bindings. If speaking to a lower version listener, the speaker will expand the subnet.

Version 4: Adds loop detection and prevention, capability exchange and a built-in keep-alive mechanism.

Enforcement Using SGACLs

This topic describes Cisco TrustSec enforcement with SGACLs.



Using SGACLs, you can control access policies based on source and destination security group tags. Policy enforcement within the Cisco TrustSec domain is represented by a permissions matrix, with source security group numbers on one axis and destination security group numbers on the other axis. Each cell in the body of the matrix can contain an ordered list of SGACLs. Each SGACL specifies the permissions that should be applied to packets originating from the source security group and destined for the destination security group. It is important to note that the source and destinations are specified in the policy matrix and not in the SGACL. Take, for example, the SGACL entry: **deny tcp dst eq 21**. The entry specifies access from the source to the destination's TCP port 21 is denied. Their is no specification of the source or destination group tags in the SGACL. It is the application of the SGACL in the permissions matrix that specifies the source and destination security groups. It is also important to understand that the same SGACL can be applied to multiple source and destination security group pairs within the permissions matrix.

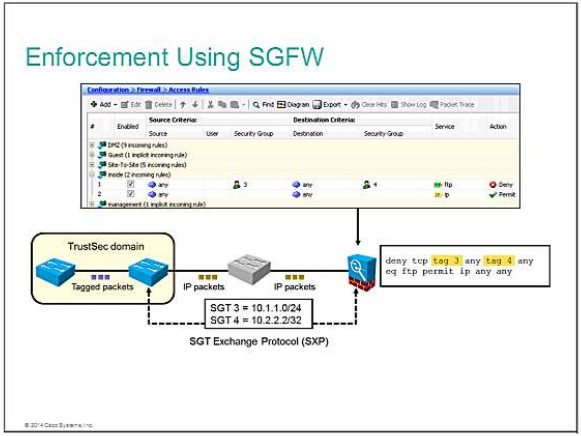
By applying access control between pairs of security groups, Cisco TrustSec achieves role-based, topology-independent access control within the network. Changes in network topology do not normally require a change in the SGACL-based security policy. Some care must be taken to insure the proper classification of new network resources, but the access policy based on business relevant security groups does not change. If the changes do require the creation of a new security group, then the permissions matrix will increase in size by one row and one column. Policy for the new cells is defined centrally in Cisco Identity Services Engine and dynamically deployed to all SGACL enforcement points.

Using role-based permissions greatly reduces the size of ACLs and simplifies their maintenance. With Cisco TrustSec, the number of ACEs configured is determined by the number of permissions specified, resulting in a much smaller number of ACEs than in a traditional IP network. Also, only a single copy of an SGACL needs to reside in the TCAM of a device, regardless of how many times the SGACL is used. The use of SGACLs in Cisco TrustSec typically results in a more efficient use of TCAM resources compared with traditional ACLs.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Enforcement Using SGFW

This topic describes the enforcement with SGFW.

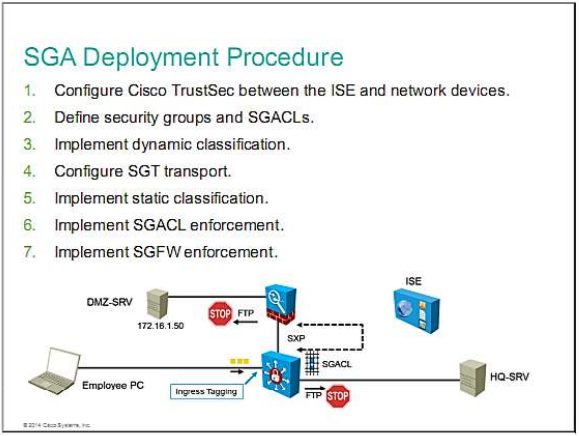


Instead of SGACLs, the Cisco Adaptive Security Appliance and select routing platforms enforce TrustSec policy using SGFW features. Where SGACL policy is centrally managed from Cisco Identity Services Engine, SGFW policy is managed independently on the device configurations. SGFW capabilities were integrated into the ASA rule policy in version 9.0 and into the IOS Zone Based Firewall feature in version 15.2. The figure depicts utilizing security group data in an access control entry on the ASA, both from ASDM and from the CLI. In IOS Zone-Based Firewall, **match security group** statements can be used in class-map definitions. In both cases, security group information can be used in conjunction with other traffic specification mechanisms, such as source and destination IP address, protocol and port numbers. One compelling use case on the ASA is to use security group information to define traffic that should be sent to which virtual IPS sensor resident in the ASA for appropriate deep packet inspection.

ASA's security policy is configured with ACLs. You can create ACLs on the ASA that contain SGTs or security group names. The ASA will enforce policies based on security group names or SGTs, if the ASA has a security group table to map security group names to SGTs, and an SGT-to-IP mapping exists.

SGA Deployment Procedure

This topic describes the SGA deployment procedure.



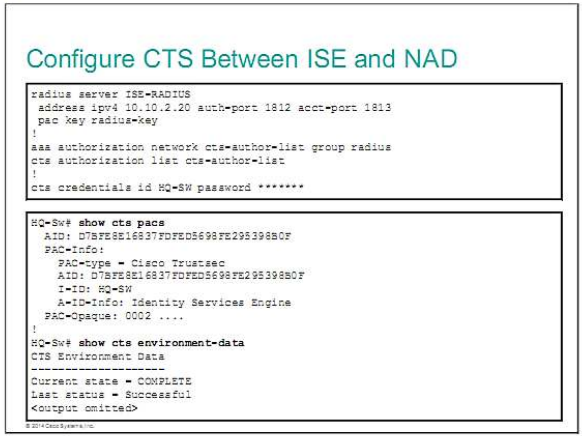
This procedure describes the key steps in deploying the SGA solution:

1. Configure Cisco TrustSec between Cisco Identity Services Engine and network devices
2. Define security groups and SGACLs
3. Implement dynamic classification
4. Implement static classification
5. Configure SGT transport
6. Implement SGACL enforcement
7. Implement SGFW enforcement

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Configure CTS Between ISE and NAD

This topic describes how to configure Cisco TrustSec between the Cisco Identity Services Engine and a network device.



Cisco TrustSec utilizes policies configured centrally on ISE. As such, Cisco TrustSec communication must be enabled between ISE and the network devices.

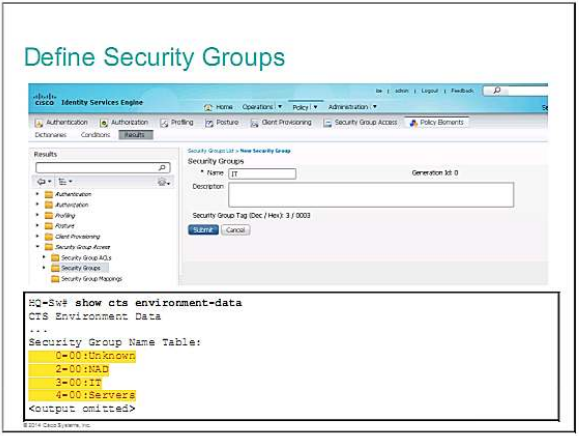
In ISE, this is defined in the NAD configuration under **Administration > Network Resources > Network Devices**. The NAD configuration includes a section named Advanced TrustSec Settings which must be enabled. The password used between ISE and the device is configured here. Optionally, update timers can be modified for this device. Some devices support Cisco TrustSec updates via CoA messages. Most devices do not. Those devices must periodically request updates from ISE. By default, the update intervals are set to 1 day.

The figure shows the configuration of Cisco TrustSec on the switch. This is done by specifying the PAC keyword in the RADIUS server definition, implementing a Cisco TrustSec authorization list and specifying the Cisco TrustSec ID and password.

Once both sides are properly configured, the device will retrieve a PAC file from the ISE. The PAC will be used to secure Cisco TrustSec transactions carried out with RADIUS between the device and ISE. The device will then download the Cisco TrustSec environment data from ISE. The Cisco TrustSec environment data is a collection of information and policies that assists a device to function in the Cisco TrustSec domain.

Define Security Groups

This topic describes how to define the security groups.



A security group is a grouping of network connected devices that share access control policies. New security groups are defined by the administrator in Cisco Identity Services Engine by name with an optional description. The path in ISE is **Policy > Policy Elements > Results, Security Group Access > Security Groups**. ISE will automatically assign a 16 bit number to the security group tag. This number is unique across the Cisco TrustSec domain.

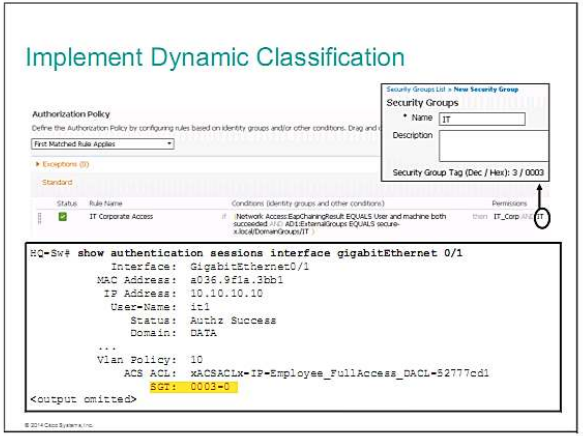
As a result of the Cisco TrustSec environment data download, the network devices obtain the security group table. The security group table maps SGTs to security group names. Security group names are created on the ISE and provide user-friendly names for security groups.

Assignment of security group tags to devices connecting to the network happens either dynamically or statically. Dynamic classification will happen during the authorization process of 802.1X, MAB or Web Authentication. Static classification is defined within the configuration on a network device. Once a security group tag is assigned to a network connected device, the tag information will follow traffic from that device through the Cisco TrustSec domain.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Implement Dynamic Classification

This topic describes how to implement dynamic classification.

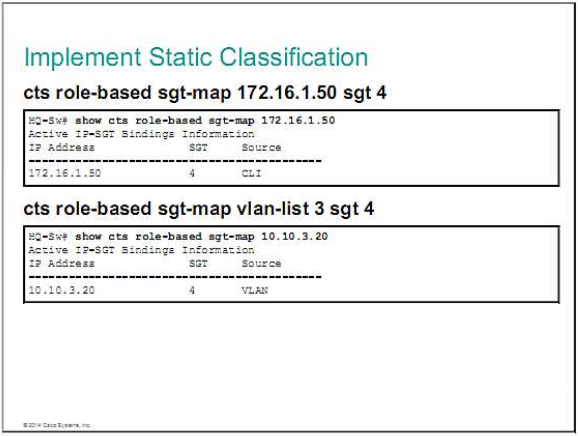


Cisco TrustSec access control is implemented using ingress tagging and egress enforcement. At the ingress point to the Cisco TrustSec domain, traffic from the source is tagged with an SGT containing the security group number of the source entity.

With dynamic classification, security groups are dynamically assigned to the clients as a permission within the Cisco Identity Services Engine authorization policy rule, as shown in the figure. Authorization policy rules can be applied as a result of 802.1X, MAB or Web Authentication. After the dynamic authentication and authorization process is complete, you can verify the SGT assignment in the authentication status on the network device using commands such as **show authentication sessions** or **show cts role-based sgt-map**.

Implement Static Classification

This topic describes how to implement static classification.

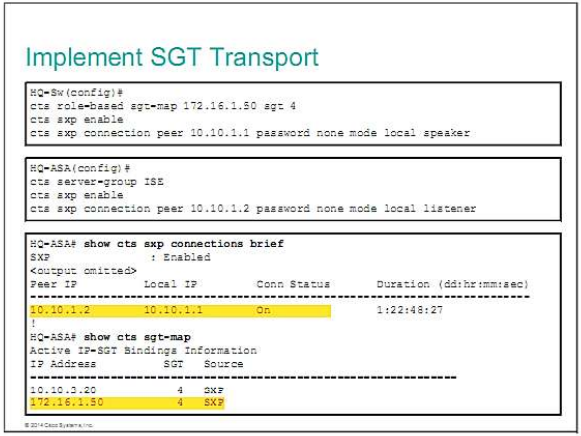


While there are other applications, static classification is generally used to define the SGTs for servers in the data center. Static classification is generally defined on the switch to which the server is directly attached. Options for static assignment depend on the network device platform and software version. Options can include mapping individual IP addresses, subnets, VLANs, layer 2 interfaces or layer 3 interfaces to an SGT. Using the Nexus 1000V in a virtualized environment, SGTs can be defined in port profiles which are assigned to VMs during the provisioning process.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Implement SGT Transport

This topic describes how to implement SGT transport.



SGTs can be propagated between devices via either inline tagging or SGT Exchange Protocol (SXP). In either case, both devices must be capable of the transport mechanism. As of software version 9.1, the Adaptive Security Appliance does not support inline tagging. The slide depicts the configuration of SXP between a Catalyst 3000 family switch and an ASA.

The SXP connection is implemented via TCP from the speaker to the listener. Each device must be configured with the peer IP address and the specification of the speaker/listener roles. In this example, the switch acts as the speaker. It has a statically configured mapping of the IP address 172.16.1.50 to SGT 4. You can verify the SXP connections on both the speaker and the listener with the **show cts scp connections** command. The output on the listener is shown above. You can also verify the received mappings using the **show cts sgt-map** command.

Configuration of inline tagging between two devices is done at interface configuration mode on the interfaces used to connect the two devices. The configuration can be specified locally (cts manual) or centralized (cts dot1x). An example of manual configuration follows:

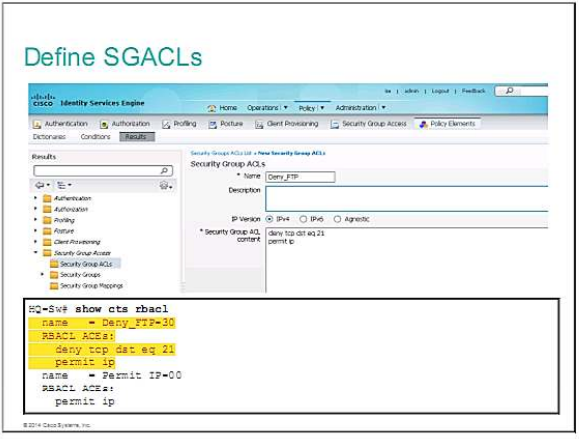
```
cts manual
policy static sgt 2 trusted
```

The **cts manual** command enters Cisco TrustSec configuration mode on the interface. The **policy static sgt 2 trusted** command specifies that any inline tags received on the interface will be honored (trusted) and any frames arriving without a tag will have the SGT 2 imposed on the frame.

https://t.me/learningnets

Define SGACLs

This topic describes how to define SGACLs.



SGACLs are defined in Cisco Identity Services Engine under **Policy > Policy Elements > Results, Security Group Access > Security Group ACLs**. The figure also shows verification that the SGACL has been received by the switch with the **show cts rbacl** command. Note that RBACL, the term used on the IOS CLI, is synominous with SGACL (Security Group ACL).

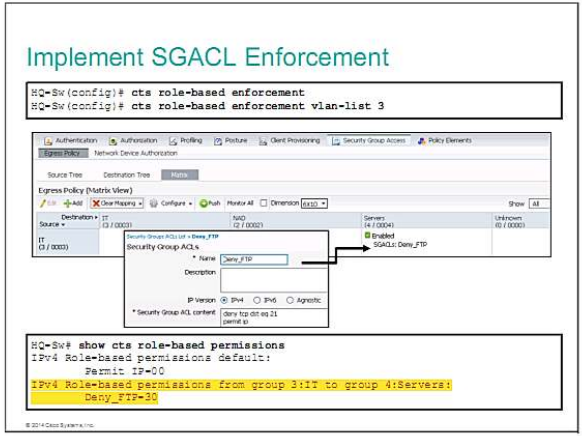
Note that SGACLs do not explicitly specify the source SGT or destination SGT. This specification will happen when the SGACL is applied in the permissions matrix. The following are the options for SGACL entries on the Nexus 7000 running NOS version 4.2:

```
deny all
deny icmp
deny igmp
deny ip
deny tcp [{dest | src} {{eq | gt | lt | neq} port-number | range port-number1 port-
number2}]
deny udp[{dest | src} {{eq | gt | lt | neq} port-number | range port-number1 port-
number2}]
permit all
permit icmp
permit igmp
permit ip
permit tcp [{dest | src} {{eq | gt | lt | neq} port-number | range port-number1 port-
number2}]
permit udp[{dest | src} {{eq | gt | lt | neq} port-number | range port-number1 port-
number2}]
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Implement SGACL Enforcement

This topic describes how to implement SGACL enforcement.



This slide depicts three operations. First, enabling role based enforcement on a network device, both globally and on a specific VLAN. Second, the definition of the egress permissions matrix in Cisco Identity Services Engine. Third, verification that the permissions matrix was successfully transfered from ISE to the network device.

Policy enforcement within the Cisco TrustSec domain is represented by a permissions matrix, with source security group numbers on one axis and destination security group numbers on the other axis. Each row represents a source SGT and each column represents a destination SGT. Each cell in the matrix defines a source SGT/destination SGT pair. Each cell can contain an ordered list of SGACLs which specify the permissions that should be applied to packets originating from the source security group and destined for the destination security group. The matrix can be managed in ISE at **Policy > Security Group Access > Egress Policy > Matrix**. In this scenario, the SGACL named Deny_FTP is assigned to traffic originating from SGT 3 (IT) and destined to SGT 4 (Servers).

In this scenario, enforcement was enabled using the **cts role-based enforcement** and **cts role-based enforcement vlan-list** commands.

You can verify the enforcement using multiple ways. The full output of the **show cts role-based permissions** command is shown here:

```
HQ-Sw# show cts role-based permissions
IPv4 Role-based permissions default:
        Permit IP-00
IPv4 Role-based permissions from group 3:IT to group 4:Servers:
        Deny_FTP-30
```

You can also view the enforcement statistics using the **show cts role-based counters** command:

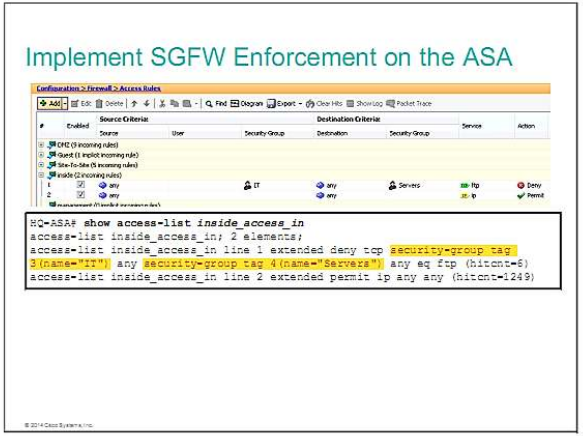
```
HQ-Sw# show cts role-based counters
Role-based IPv4 counters
# '-' in hardware counters field indicates sharing among cells with identical policies
```

```
From    To      SW-Denied       HW-Denied       SW-Permitted    HW-Permitted
*       *       0               0               45566           143279
3       4       0               29              0               21836
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Implement SGFW Enforcement on the ASA

This topic describes how to implement SGFW enforcement on the Cisco Adaptive Security Appliance.



SGFW is implemented on the ASA by utilizing security group tags in the source and/or destination specification in ACL entries. This capability was made available in version 9.0 of the ASA software. The slide depicts a policy that denies FTP from the source group 3 (IT) to the destination group 4 (Servers). This policy is configured in an ACL that is applied inbound to the inside interface. The top figure shows the access rule definition in Cisco Adaptive Security Device Manager. and the bottom figure shows the CLI representation of the access list.

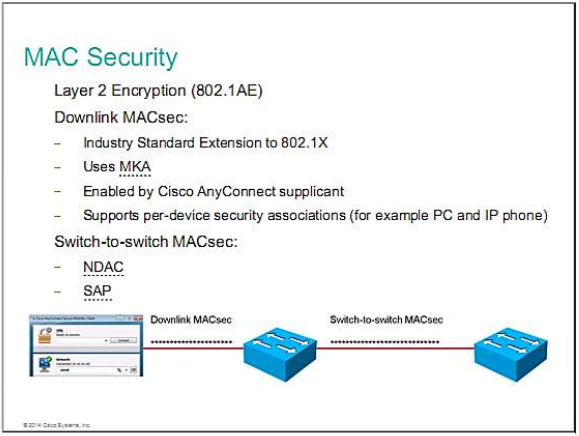
Note that on the ASA, ACLs can also be used by the modular policy framework to classify traffic for various policies. For example, SGT data can be used to classify traffic that will be sent to a particular virtual sensor implemented in a sensor module installed in the ASA.

SGFW is also available for use in IOS zone based firewall since IOS version 15.2. With zone based firewall, security groups can be specified with match clauses in the class-map statements.

https://t.me/learningnets

MAC Security

This topic describes downlink and switch-to-switch MACsec.



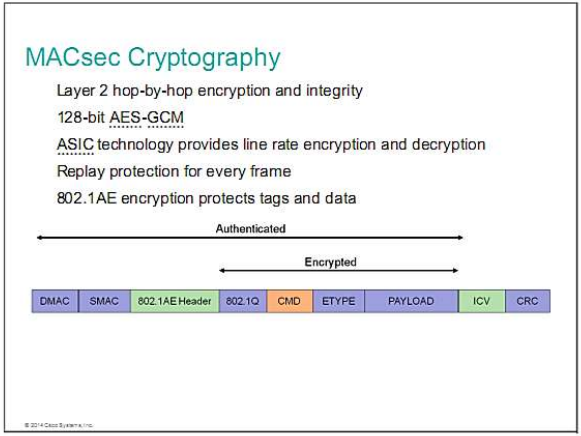
MACsec is the IEEE 802.1AE standard for authenticating and encrypting packets between two MACsec-capable devices. Cisco switches support 802.1AE encryption with MKA on downlink ports for encryption between the switch and host devices. The switches also support MACsec link layer switch-to-switch security by using Cisco TrustSec NDAC and the SAP key exchange. Link layer security can include both packet authentication between switches and MACsec encryption between switches (encryption is optional).

The 802.1AE standard requires supporting protocols for key management, authentication, and authorization. To meet this need, the IEEE proposed an additional standard, 802.1af MAC Key Agreement (802.1X-2010/MKA), an extension of 802.1X that manages short-lived session keys that are used to encode and decode messages. 802.1X-2010/MKA supports per-device security associations in shared media environments, for example, with PCs connected to Cisco IP phones. 802.1AE must be supported on the platform and the respective modules.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

MACsec Cryptography

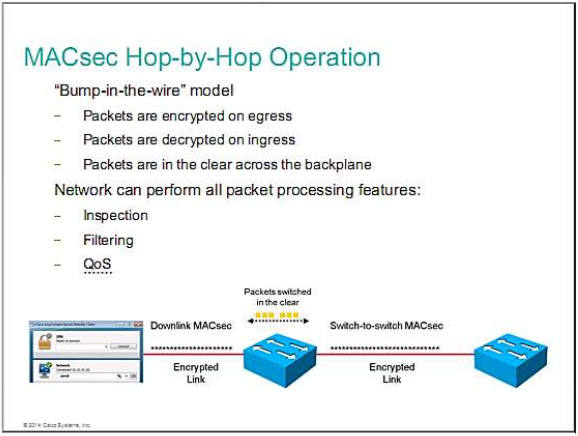
This topic describes the MACsec cryptographic features.



MACsec is a Layer 2 hop-by-hop encryption and integrity solution that is based on the 128-bit AES-GCM cipher. Cisco switches that support MACsec utilize ASIC to provide real-time line rate encryption and decryption. MACsec ensures replay protection for every frame. MACsec standard offers encryption of the frame payload, including the Cisco Meta Data (which contains the SGT) header, and the 802.1Q header.

MACsec Hop-by-Hop Operation

This topic describes the MACsec hop-by-hop operation.



When a frame arrives at a MACsec station, the MACsec Security Entity decrypts the frame if necessary, computes an ICV on the frame, and compares it with the ICV included in the frame. If they match, the station processes the frame as normal. If they do not match, the port processes the frame according to a preset policy, usually discarding it.

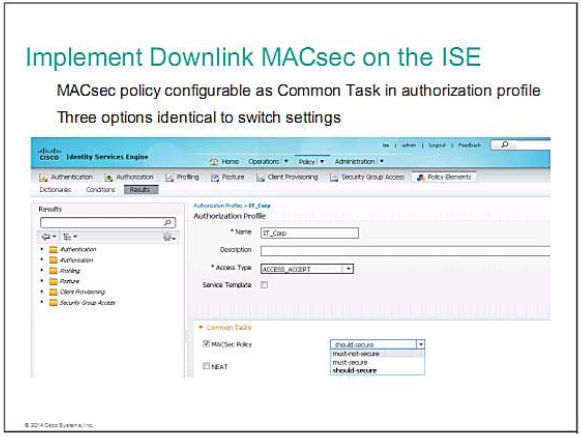
This operational model can be thought of as a "bump in the wire," in which the packets are encrypted on egress interfaces, decrypted on ingress interfaces, and switched in the clear through the device's backplane.

This approach allows the network to perform all current packet processing features, such as packet inspection, stateless and stateful filtering, and QoS processing.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Implement Downlink MACsec on the ISE

This topic describes the downlink MACsec implementation on the Cisco Identity Services Engine.

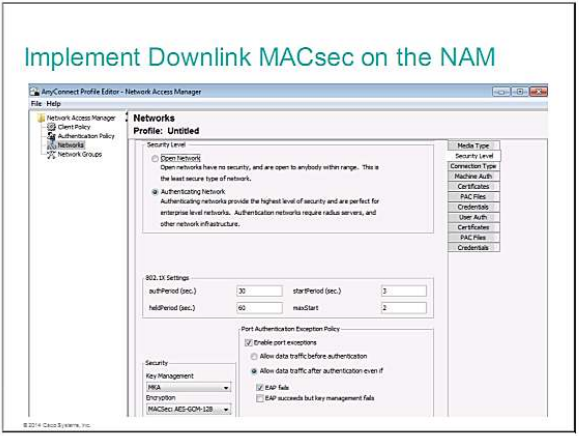


Downlink MACsec policy is configured as an element in the authorization profile in Cisco ISE. To specify MACsec policy for endpoints, you enable MACsec policy and then select the policy option. The options are must-not-secure, must-secure and should-secure. This populates the value for the linksec-policy attribute, a Cisco AV pair sent to the network access device as part of the RADIUS access-accept message.

The MACsec policy defined in ISE will interact with policies configured on and capabilities of both the NAD and the supplicant. For example, if the ISE policy is must-secure and either the supplicant or the switch are not MACsec capable, then access will be rejected. Should-secure will secure if all components are capable and willing, but will allow unsecured access if a component is not MACsec capable or is configured with must-not-secure.

Implement Downlink MACsec on the NAM

This topic describes the downlink MACsec implementation on the NAM.

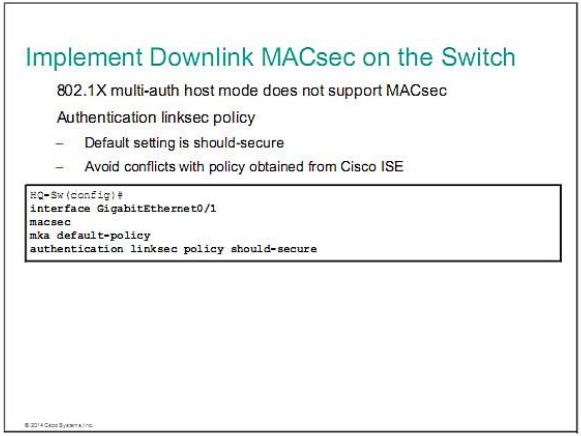


To enable downlink MACsec in the Network Access Manager of Cisco AnyConnect, you must create a profile and configure it to use MKA as the key management method and set the encryption algorithm to MACsec: AES-GCM-128.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Implement Downlink MACsec on the Switch

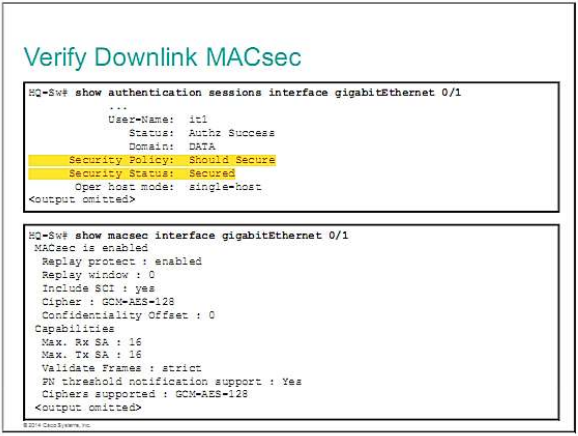
This topic describes the downlink MACsec implementation on the switch.



This figure illustrates the configuration of the MACsec feature on the switch port. Apart from enabling MACsec, you need to enable an MKA policy using the **mka** command. The **authentication linksec policy** command allows you to select one of the three options: must-secure, must-not-secure, and should-secure. The should-secure option is enabled by default.

Verify Downlink MACsec

This topic describes how to verify downlink MACsec.

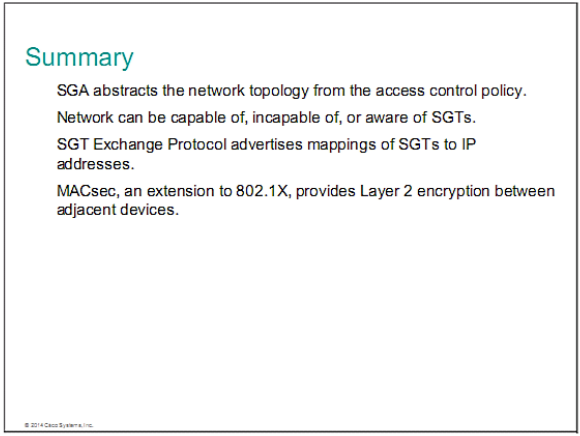


The **show authentication sessions interface** command can be used to verify the MACsec policy that has been negotiated for the switch port as well as the current status of MACsec on the port. You can further examine the crypto details using the **show macsec interface** command.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Summary

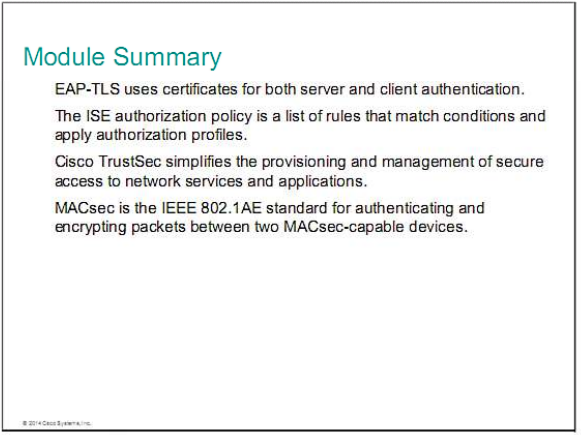
This topic summarizes the key points that were discussed in this lesson.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Module Summary

This topic summarizes the key points that were discussed in this module.



References

For additional information refer to this resource:

Cisco Identity Services Engine User Guide

https://t.me/learningnets

https://t.me/learningnets

Module Self-Check

Questions

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

1. Which EAP method uses client-side certificates? (Source: Certificate-Based User Authentication)

   A. PEAP
   B. EAP-FAST
   C. FAST-TLS
   D. EAP-TLS

2. At minimum, how many certificates does the ISE require to support EAP with client certificates? (Source: Certificate-Based User Authentication)

   A. Depends on the number of clients
   B. Depends on the total number of CA's
   C. 1
   D. 2

3. How do apply a certificate authentication profile in the Cisco ISE? (Source: Certificate-Based User Authentication)

   A. To an identity source
   B. To the authentication policy
   C. To an authentication policy rule
   D. To an identity source sequence

https://t.me/learningnets

4. Which two policy elements are used in authorization? (Source: Authorization)

   A. Authorization assignment
   B. Permission
   C. Allowed Protocols
   D. dACL
   E. Authorization profile

5. How is a dACL transported to the destination? (Source: Authorization)

   A. Via RADIUS to the client
   B. Via RADIUS to the authenticator
   C. Via RADIUS and EAPOL to the client
   D. Via TCP to the switch

6. In which two deployment modes would you set the permission in the default authorization rule to DenyAccess? (Choose two.) (Source: Authorization)

   A. Access
   B. Initial
   C. Closed
   D. Monitor
   E. Low-Impact

7. Which two methods can be used to transport SGTs? (Choose two.) (Source: Cisco TrustSec and MACsec)

   A. TrustSec (CTS) Meta Data (CMD) header in downlink MACsec
   B. TrustSec (CTS) Meta Data (CMD) header in switch-to-switch MACsec
   C. TrustSec (CTS) Meta Data (CMD) header in switch-to-ISE MACsec
   D. SXP
   E. EAP-FAST
   F. RADIUS

8. Cisco ISE can dynamically classify VPN traffic using SGTs. (True or false?) (Source: Cisco TrustSec and MACsec)

   A. True
   B. False

9. Which statement describes the SGFW support on Cisco IOS routers? (Source: Cisco TrustSec and MACsec)

   A. Not available
   B. Available with standard ACLs
   C. Available with extended ACLs
   D. Available with ZBPF
   E. Available with FPM

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Answer Key

1. D
2. D
3. D
4. D, E
5. B
6. C, E
7. B, D
8. A
9. D

https://t.me/learningnets

https://t.me/learningnets

Module 4

Web Authentication and Guest Access

Web Authentication (WebAuth) is a convenient method for authenticating end users who cannot be authenticated using 802.1X. The users are redirected to the guest portal, prompted for authentication, and depending on the outcome, applied an appropriate authorization profile by the Cisco Identity Services Engine (ISE).

The Cisco ISE Guest service allows users, such as guests, visitors, contractors, consultants, and customers to access a network, whether the network is a corporate intranet or the public Internet. Cisco ISE Guest service allows users with the appropriate privileges to easily create sponsor accounts and temporary guest accounts. The Cisco ISE Guest Service performs full authentication of sponsors.

Upon completing this module, you will be able to:

- Describe Cisco ISE WebAuth
- Describe the guest service features of the Cisco ISE

https://t.me/learningnets

https://t.me/learningnets

Lesson 1

Deploying WebAuth

Overview

WebAuth provides network access to users who authenticate using HTTP or HTTPS. WebAuth is typically used for guest network access and may be utilized for other clients without an IEEE 802.1X supplicant. This lesson provides an overview of the process for deploying WebAuth using the Cisco Identity Services Engine platform.

Upon completing this lesson, you will be able to:

- Describe WebAuth
- Describe the WebAuth process
- Describe the WebAuth scenarios
- Describe the Central WebAuth process
- Describe the Central WebAuth configuration procedure
- Describe how to configure a switch for WebAuth
- Describe how to configure the MAB to continue when user is not found
- Describe how to tune the WebAuth identity source sequence
- Describe how to tune the WebAuth identity source sequence
- Describe how to configure an authorization profile for traffic redirection to WebAuth
- Describe how to apply the WebAuth authorization profile
- Describe the authorization policy rule for users who have authenticated via WebAuth
- Describe how to verify how to verify the redirection to WebAuth on the ISE
- Describe how to verify the traffic redirection to WebAuth on the switch
- Describe how to verify WebAuth traffic redirection on the client system
- Describe how to verify how to verify the redirection to WebAuth on the ISE

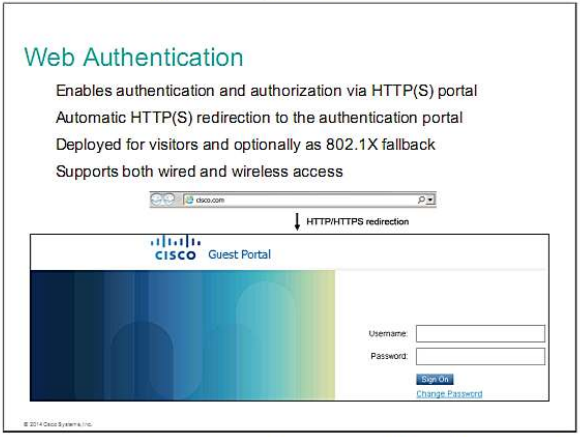
https://t.me/learningnets

Describe how to verify the completed WebAuth authentication on the switch and client

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Web Authentication

This topic describes Cisco Identity Services Engine WebAuth.

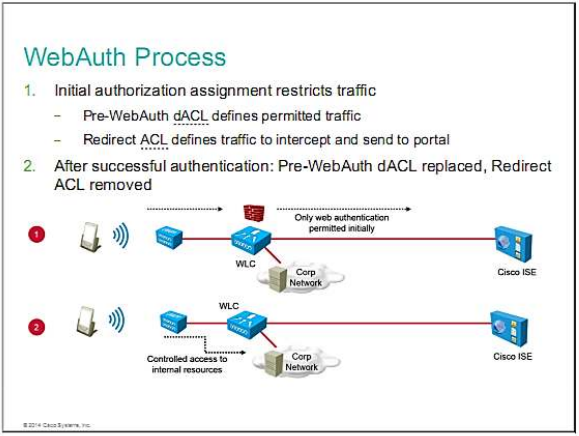


WebAuth enables authentication through a portal accessed via HTTP or HTTPS, followed by the application of the appropriate access authorization profile. Automatic redirection to the authentication web page occurs when an non-authenticated user attempts an HTTP or HTTPS connection.

WebAuth is used primarily for guest access but may be used as a method of last resort for users with an IEEE 802.1X supplicant that is not installed, is misconfigured, or is not functional. If the 802.1X supplicant is not functioning properly, WebAuth may be used to prompt the user for authentication credentials and still provide access to the network. WebAuth may also used for guest users who have an 802.1X supplicant that is installed but who do not have a user account in the appropriate identity database. WebAuth can be implemented in both wired and wireless environments.

WebAuth Process

This topic illustrates the WebAuth process.



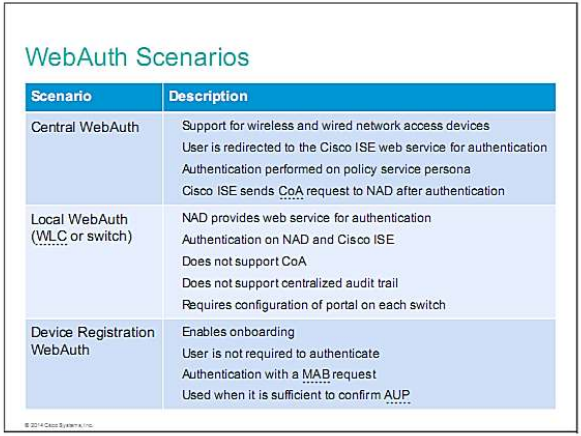
When a guest user first attaches to the local network, either through a wireless or hardwired connection, the connectivity is controlled and provides limited access. Generally a pre-WebAuth dACL is used for this control, but a VLAN assignment may be used instead of or in conjunction with the dACL. The dACL permits only WebAuth traffic and potentially some basic networking services. Working in conjunction with the dACL is a locally configured ACL that defines the traffic that should be intercepted and sent to the web authentication portal. This ACL does not limit traffic that is allowed. Instead, it specifies which of the allowed traffic will be redirected.

To gain greater access to the network, the user attempts an HTTP or HTTPS request from a browser, for example, http://www.cisco.com. Based on the redirection ACL, the NAD intercepts the HTTP request and redirects it to the guest user login portal. After successful authentication, the redirection is removed and the user is assigned an appropriate authorization profile. This new profile specifies a new dACL to control access to the enterprise resources.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

WebAuth Scenarios

This topic identifies WebAuth scenarios.



The Cisco Identity Services Engine supports these web authentication scenarios:

Central WebAuth: This scenario applies to wireless and wired NADs. In this scenario, the user is redirected to the Cisco ISE web service for authentication. The authentication is performed on the Cisco ISE. The Cisco ISE requests a CoA from the NAD after authentication.

Local WebAuth: This scenario differentiates between wireless and wired access:

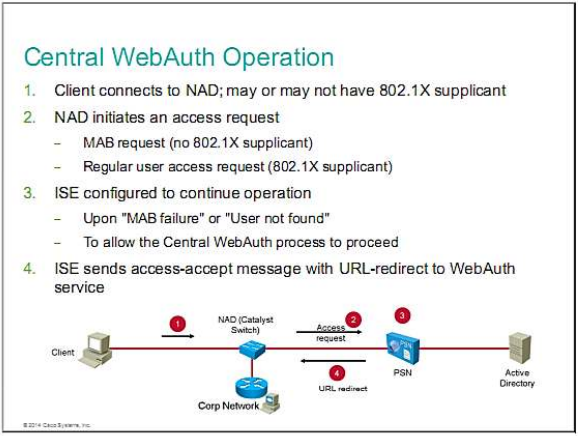
- In the **WLC with Local WebAuth** scenario, the user logs in and is directed to the WLC. The WLC then redirects the user to the guest portal. The guest portal prompts the user for a username and password, and performs an optional AUP. When this process is complete, the user browser is redirected back to the WLC to log in again. The WLC authenticates the user via RADIUS and then redirects the client browser to the original destination.
- In the **Wired NAD with Local WebAuth** scenario, the guest user login portal redirects the guest user login request to the switch. The login request is in the form of an HTTPS URL posted to the switch, and contains the user credentials. The switch receives the user login request and authenticates the user through a RADIUS server that points to the Cisco ISE.

Device Registration WebAuth: In this scenario, the guest user connects to the network with a wireless connection that sends an initial MAB request to the Cisco ISE node. If the user MAC address is not in the endpoint identity store, the Cisco ISE responds with a URL redirection authorization profile. The URL redirection presents the user with an AUP acceptance page when the user attempts to go to any URL.

https://t.me/learningnets

Central WebAuth Operation

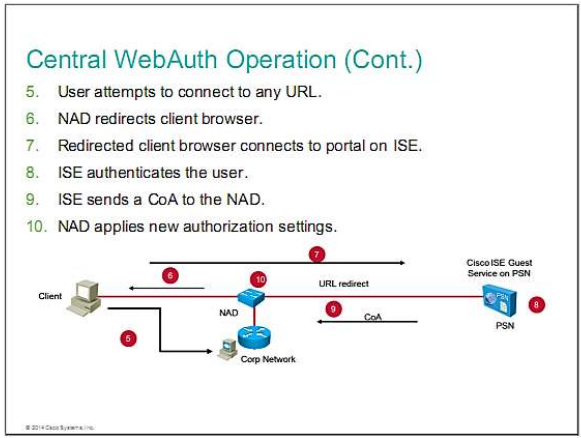
This topic describes the operation of Cisco Identity Services Engine Central WebAuth.



The example that is shown in the figure outlines the steps for Central WebAuth:

1. The client connects to the NAD through a hardwired connection. The client may or may not have an 802.1X supplicant.
2. The NAD initiates a MAB request for an endpoint without a supplicant or a regular access request for an endpoint with a supplicant.
3. ISE processes the request and does not find an endpoint or user. The appropriate authorization rule is configured with a restricted network profile, which contains URL-redirection parameters.
4. ISE sends an access-accept message with URL redirection for Central WebAuth to the NAD. The redirection is to the Central WebAuth service that is running on the policy service node.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets



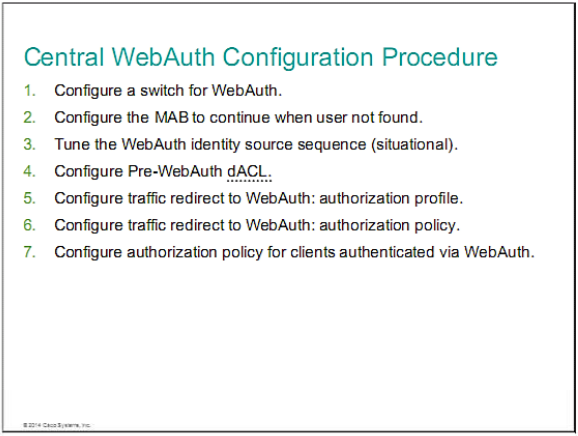
5. The client initiates an HTTP(S) request to any URL using a browser.
6. The NAD sends an HTTP(S) redirect message to the client. The redirection is to the URL that is included in the access-accept message. This URL is for the central web authentication login page. The URL encodes the common session ID which uniquely identifies this endpoint's AAA session for both ISE and the NAD.
7. The redirected client browser connects to the web authentication portal on ISE.
8. ISE displays the authentication portal and requests the username and password. It then authenticates the user against the configured identity store or stores.
9. Upon successful authentication, ISE sends the authorization profile that is associated with the authenticated user in the form of a CoA message to the NAD.
10. The NAD applies the new authorization settings and returns a CoA acknowledgement back to ISE.

After the authentication completes, an authentication successful message is displayed in the user's browser. The message also directs the user to repeat their original URL request. The user is not redirected to their original requested page, they have to manually repeat the request. If permitted by the authorization profile, the connection will succeed for the repeated request.

Note In a distributed deployment, the central web authentication portal is provided on nodes which run the policy service persona. An ISE node which only runs the policy service persona is often called a PSN.

Central WebAuth Configuration Procedure

This topic describes the Central WebAuth configuration procedure.



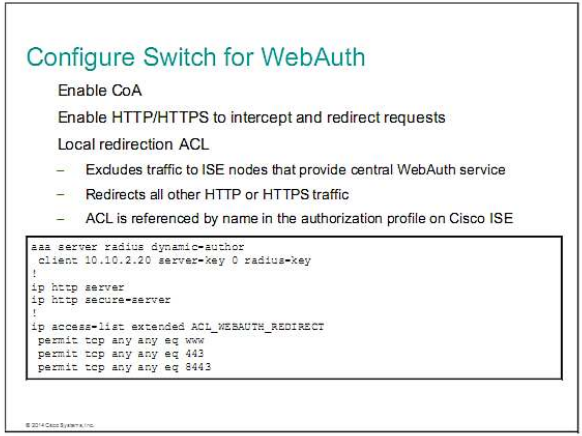
Follow this procedure to implement Central WebAuth on the Cisco Identity Services Engine:

1. Configure a switch for WebAuth
2. Configure the MAB to continue when user not found
3. Tune the WebAuth identity source sequence (situational)
4. Configure Pre-WebAuth dACL
5. Configure traffic redirect to WebAuth: authorization profile
6. Configure traffic redirect to WebAuth: authorization policy
7. Configure an authorization policy rule for clients authenticated via WebAuth

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Configure Switch for WebAuth

This topic describes how to configure a switch for Central WebAuth.



A few features need to be configured on the NADs to support Central WebAuth.

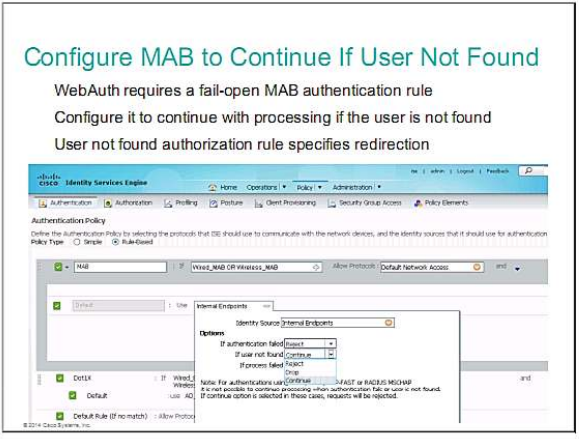
You need to enable the CoA feature. It is enabled in the **aaa server radius dynamic-author** configuration mode using the client command. The client command references the Cisco Identity Services Engine IP address and specifies the shared key. In the standard RADIUS process, authorization specifications are sent to the NAD in an Access-Accept message in response to an Access-Request from the NAD. CoA allows ISE to send new authorization specifications when ISE recognizes the conditions have changed. CoA does not require the NAD to solicit the authorization request.

You must also enable the HTTP and HTTPS services. They are required at the Cisco IOS NAD so that the NAD can intercept web requests and redirect them to the Cisco ISE. While not shown here, it is also recommended that an access-class statement is applied to the HTTP service to limit which IP addresses are allowed to reach the management interface via HTTP or HTTPS.

Lastly, you must configure a local ACL that defines the traffic that is to be redirected. Traffic denied by the ACL is not redirected; traffic that is permitted will be redirected. The ACL shown in the figure, named **ACL_WEBAUTH_REDIRECT**, illustrates this principle. Basic network services such as DNS and DHCP are denied. Web browsing ports are permitted and thus redirected to the primary service node. If your organization implements web proxy services, the proxy ports should also be redirected. This local ACL is referenced by ISE by name in the authorization profile. The local ACL must be a named ACL. Numbered ACLs are not supported.

Configure MAB to Continue If User Not Found

This topic describes how to configure the MAB to continue if the user is not found.



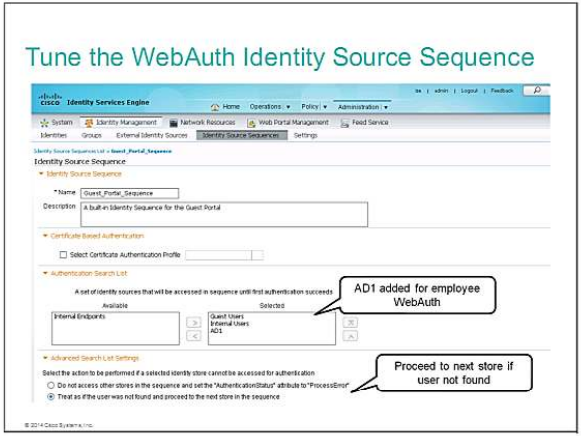
The default Cisco Identity Services Engine configuration consists of two built-in rules, MAB and Dot1X, and a rule named Default Rule that is processed when none of the other rules produces a match. You can modify, duplicate, and delete the existing rules, or insert a new rule at any desired position by selecting the appropriate action in the Actions list. The available actions are: Insert new row above, Insert new row below, Duplicate above, Duplicate below, and Delete.

Central WebAuth makes use of a fail-open MAB authentication rule. The authentication rule must be configured to continue when the user is not found. This configuration allows further actions to be taken by the Cisco ISE and the NAD. MAB will complete with success, but assign the attribute Authentication Status the value of UnknownUser. An authorization policy rule that requires this condition will then be applied and its authorization profile will specify the redirection to the central web authentication portal.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Tune the WebAuth Identity Source Sequence

This topic describes how to tune the WebAuth identity source sequence.

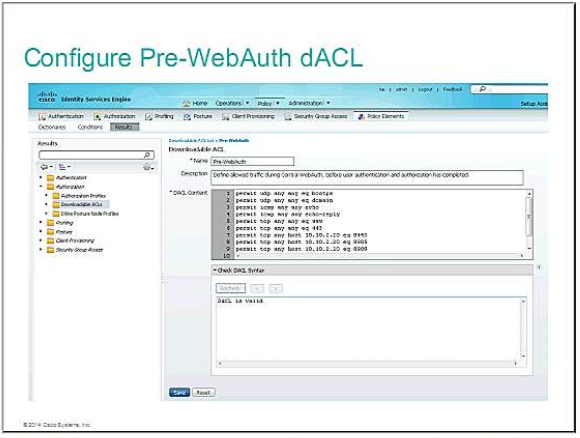


Cisco Identity Services Engine comes preconfigured with an identity source sequence named Guest_Portal_Sequence. It defines the identity stores that the ISE consults when authenticating users via the guest portal. By default, this sequence includes only the Guest Users and the Internal Users.

In scenarios where external identity sources should also be consulted, this identity source sequence should be modified. The example in the figure shows the movement of the Active Directory identity source, AD1, from the Available to the Selected identity sources.

Configure Pre-WebAuth dACL

This topic describes how to create a dACL to control traffic before WebAuth authentication and authorization.



When central web authentication is initiated, Cisco Identity Services Engine will send a dACL and specify the name of a local redirection ACL to the NAD. These two ACLs work together. The dACL will specify what traffic is allowed prior to user authentication and authorization. The redirection ACL will specify what of the allowed traffic will be redirected to the central web authentication portal.

The figure shows the definition of a dACL named Pre-WebAuth. The access control entries in the example are defined as follows:

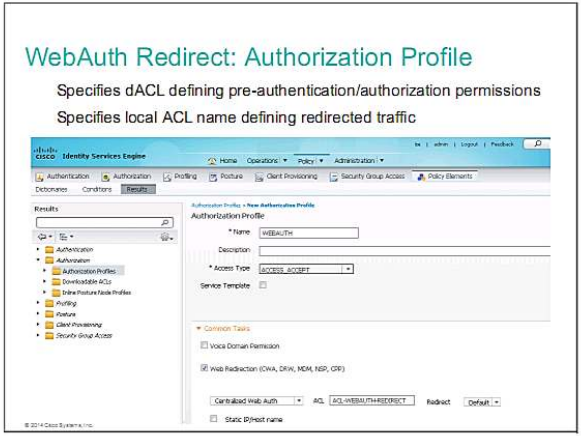
```
permit udp any any eq bootps
permit udp any any eq domain
permit icmp any any echo
permit icmp any any echo-reply
permit tcp any any eq www
permit tcp any any eq 443
permit tcp any host 10.10.2.20 eq 8443
permit tcp any host 10.10.2.20 eq 8905
permit tcp any host 10.10.2.20 eq 8909
permit udp any host 10.10.2.20 eq 8905 8906
permit udp any host 10.10.2.20 eq 8909
```

The requirements of this ACL will vary with the design scenario. In the example ACL, the first two entries permit DHCP and DNS, respectively. The two ICMP entries permit bidirectional ping, which may be helpful for troubleshooting scenarios. HTTP and HTTPS traffic are allowed (and should be redirected by the redirection ACL). Port 8443 is used by the ISE guest portal. Ports 8905 and 8906 are used by the NAC Agent Swiss protocol for ISE posture services. Port 8909 is used for client provisioning activity.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

WebAuth Redirect: Authorization Profile

This topic describes how to configure an authorization profile for traffic redirection to WebAuth.



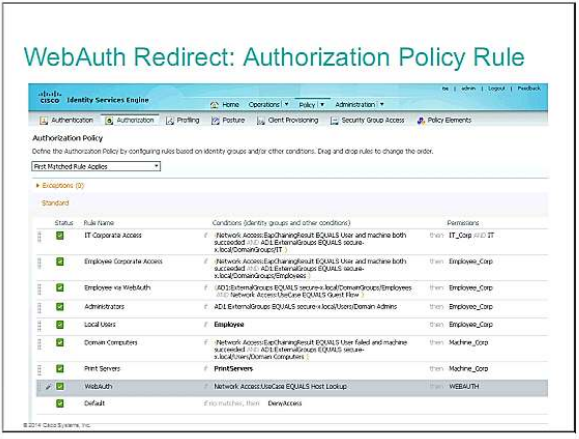
The authorization profile that supports Central WebAuth should define at least two things: It should specify the dACL which will control what traffic is allowed from the endpoint prior to the user successfully completing authentication through the central web authentication portal. It should also specify a named ACL, that must exist on the NAD, which what traffic will redirected to the central web authentication portal.

The named ACL on the NAD must make sure that all HTTP and HTTPS traffic is redirected except the traffic that is destined to the policy service nodes.

The figure depicts the definition of the redirection ACL in the authorization profile. The dACL is also specified in the Common Tasks section of the authorization profile. The distance between the two options made it impossible to show both in a single screen shot.

WebAuth Redirect: Authorization Policy Rule

This topic describes how to to configure an authorization policy rule to redirect traffic to WebAuth.



The authorization profile needs to be assigned to an authorization policy rule to be enacted. The authorization policy rule for central web authentication is typically placed just before the default rule. The authorization rule should have the condition which verifies that the UseCase attribute from the Network Access dictionary is set to the value Host Lookup. This this dictionary value will be set after a failed MAB process.

The figure depicts an authorization policy rule named WebAuth that requires Network Access:UseCase EQUALS Host Lookup and assigns the authorization profile named WEBAUTH (which implements the policy supporting redirection of web traffic to the authentication portal).

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Configure Authorization for WebAuth Users

This topic describes the authorization policy rule for users who have authenticated via WebAuth.



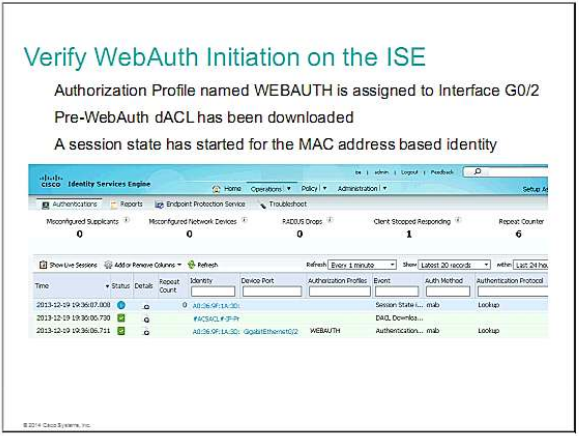
After implementing an authorization policy rule that supports the use of the central web authentication portal, additional rules must be defined to specify authorization profiles for authenticated users. When the user is authorized on the login page, Cisco Identity Services Engine restarts a Layer 2 authentication on the switch port, and a new MAB occurs. The redirection policy will be re-implemented unless other rules are placed ahead of the rule which implements the web redirection.

ISE sets an attribute in the Network Access dictionary to remember a guest-authenticated user. This attribute can be verified with the expression Network Access:UseCase Equals GuestFlow. This condition is met when the user authenticates via WebAuth, and the switch port is set again for a new MAB. The authorization policy rules for central web authentication authenticated users should use this expression in the condition as well as any other expressions necessary to differentiate between the types of users. The authorization policy rule must, of course, specify the appropriate authorization profile for the indicated type of user.

This figure illustrates the specific authorization policy rule for members of the Active Directory group Employees who authenticate via central WebAuth. There are two expressions in the condition: Network Access:UseCase EQUALS GuestFlow and AD1:ExternalGroups EQUALS secure-x.local/DomainGroups/Employees. The authorization profile specified is Employee_Corp.

Verify WebAuth Initiation on the ISE

This topic shows how to verify the redirection to WebAuth on the Cisco Identity Services Engine.



The figure displays an example of what can be expected on the Live Authentications display on ISE when central web authentication has been configured and an endpoint without an 802.1X supplicant connects. This is before the user authenticates via the portal. From bottom to top, an Authorization Profile named WEBAUTH is applied to Interface G0/2. The dACL named Pre-WebAuth has been downloaded. A session state associated with the identity specified by the endpoint's MAC address has been started.

The following documents an example of the steps that are listed in the details report for the event showing the WEBAUTH profile being applied.

```
11001 Received RADIUS Access-Request
11017 RADIUS created a new session
11027 Detected Host Lookup UseCase (Service-Type = Call Check (10))
15049 Evaluating Policy Group
15008 Evaluating Service Selection Policy
15048 Queried PIP
15048 Queried PIP
15004 Matched rule
15041 Evaluating Identity Policy
15006 Matched Default Rule
15013 Selected Identity Source -
24209 Looking up Endpoint in Internal Endpoints IDStore - A0:36:9F:1A:3D:AE
24217 The host is not found in the internal endpoints identity store
22056 Subject not found in the applicable identity store(s)
22058 The advanced option that is configured for an unknown user is used
22060 The 'Continue' advanced option is configured in case of a failed
authentication request
15036 Evaluating Authorization Policy
24432 Looking up user in Active Directory - A0:36:9F:1A:3D:AE
24412 User not found in Active Directory
15048 Queried PIP
15004 Matched rule - WebAuth
15016 Selected Authorization Profile - WEBAUTH
```

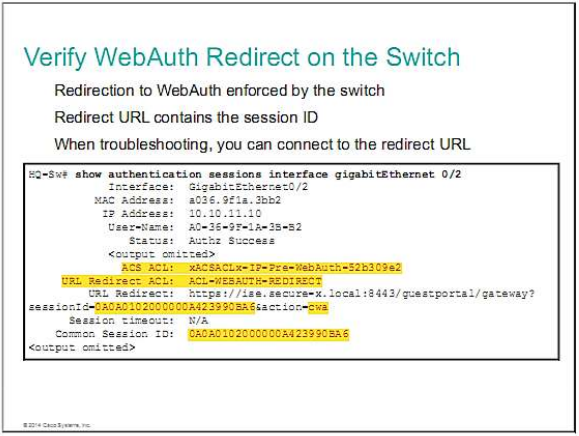

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

```
11022 Added the dACL specified in the Authorization Profile
11002 Returned RADIUS Access-Accept
```

Note that after a failed MAB lookup, the continue option was invoked. Because authentication appeared to complete, but the authentication status is UnknownUser, the authorization policy rule named WebAuth was matched. This led to the selection and application of the authorization profile named WEBAUTH.

Verify WebAuth Redirect on the Switch

This topic shows how to verify the traffic redirection to WebAuth on the switch.



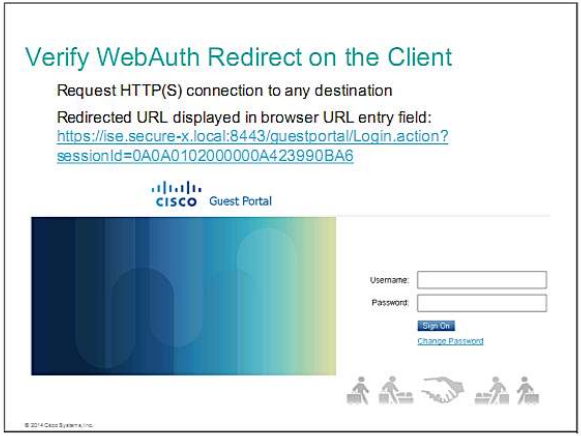
The figure shows an example of the authentication session status on an interface for which central web authentication has been enforced, prior to the user authenticating via the portal. The authorization policy sent by the Cisco Identity Services Engine includes a dACL to restrict traffic prior to user authentication. In this case the dACL is named Pre-WebAuth. The policy also includes the name of a locally configured ACL to specify what of the allowed traffic should be redirected to the portal. In this case the name is ACL-WEBAUTH-REDIRECT. ISE also specifies the URL to where redirections are sent. Note the URL includes the common session ID for this authentication session. With this ID embedded in the URL, ISE will be able to recognize authentication for this session apart from any other central web authentication sessions which may occur in parallel. The common session ID is a unique identifier for this authentication session and is used to keep the NAD and ISE synchronized.

This output may be very helpful when troubleshooting. When a user is not redirected to the guest portal, you can test the HTTPS connectivity by going to the redirect URL, and investigating the results.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Verify WebAuth Redirect on the Client

This topic describes how to verify WebAuth traffic redirection on the client system.



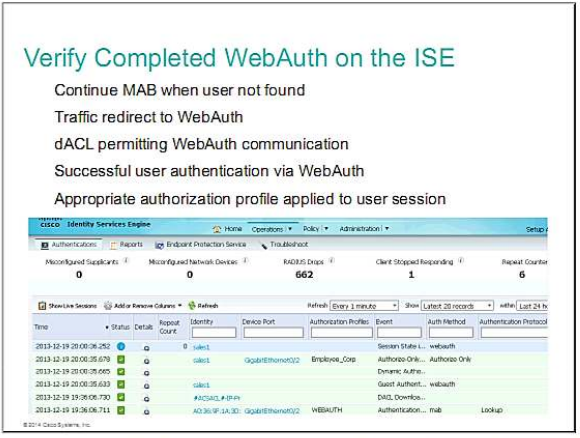
When the traffic redirection to WebAuth has been configured on the Cisco Identity Services Engine and the switch, the user can open a browser and connect via HTTP or HTTPS to any destination. The NAD will redirect the browser to the guest portal and the user is prompted for authentication.

If the user credentials are accepted by the system, the user will be presented with an Acceptable Use Policy statement. The user must accept the policy to continue. After acceptance, ISE will select a new authorization policy based on the user status and send the NAD an authorization policy update via a CoA message. This update will remove the redirection configuration and replace the dACL with one that is appropriate for the user. The browser will display a message that indicates authentication was successful and instructs the user to retry their original connection request.

The portal may be customized in many ways, including changing the logo, color scheme, AUP message and success message. The figure displays the default portal login screen without any customizations.

Verify Completed WebAuth on the ISE

This topic shows how to verify the completed WebAuth authentication on the Cisco Identity Services Engine.



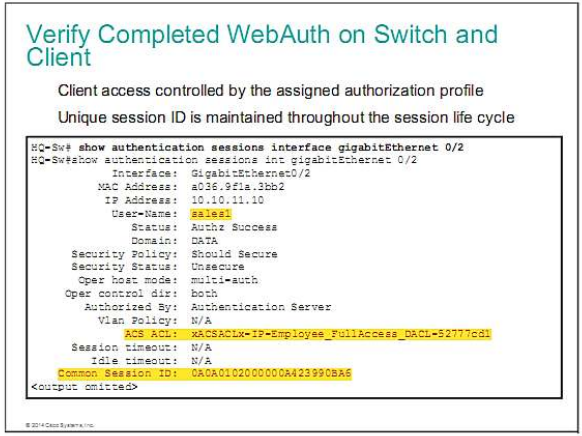
This figure depicts an example of the Live Authentications display after the user has successfully authenticated via central web authentication. From the bottom, the first two events are in response to the setup of the web authentication process. Then the user sales1 successfully authenticates. This leads to the successful application of Dynamic Authorization policy via CoA. The Authorization Profile named Employee_Corp is implemented on interface G0/2 for the Identity sales1. Below provides an example of what is seen in the details report for the event documenting the authorization profile assignment via central web authentication:

```
  11001 Received RADIUS Access-Request
  11017 RADIUS created a new session
  11027 Detected Host Lookup UseCase (Service-Type = Call Check (10))
  15049 Evaluating Policy Group
  15008 Evaluating Service Selection Policy
  15048 Queried PIP
  15048 Queried PIP
  15004 Matched rule
  24423 ISE has not been able to confirm previous successful machine authentication
for user in Active Directory
  15036 Evaluating Authorization Policy
  15048 Queried PIP
  15048 Queried PIP
  15004 Matched rule - Employee via WebAuth
  15016 Selected Authorization Profile - Employee_Corp
  11022 Added the dACL specified in the Authorization Profile
  11002 Returned RADIUS Access-Accept
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Verify Completed WebAuth on Switch and Client

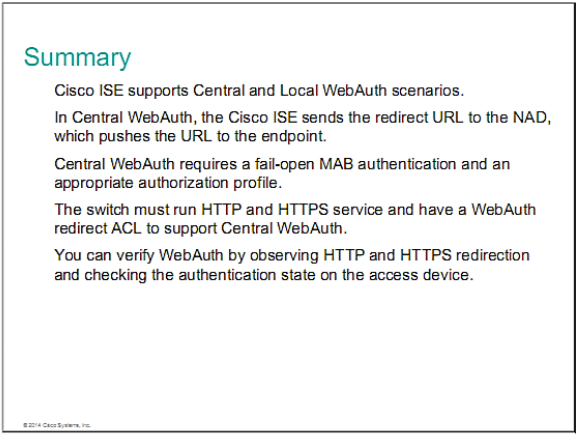
This topic shows how to verify the completed WebAuth authentication on the switch and client.



You can verify the final results on the client and the switch. The client can connect everywhere within the allowed profile. The authentication status on the switch displays the final dACL applied to the user session. The web redirection specifications have been removed. The common session ID remains the same and identifies the session throughout its life cycle.

Summary

This topic summarizes the key points that were discussed in this lesson.



https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Lesson 2

Deploying Guest Service

Overview

Guest services provide the functions that are required to provision temporary user accounts for guest users and to control user access to the network. This lesson provides an overview of the guest services that are offered by the Cisco Identity Services Engine platform and details how to configure the user portals for a network deployment.

Upon completing this lesson you will be able to:

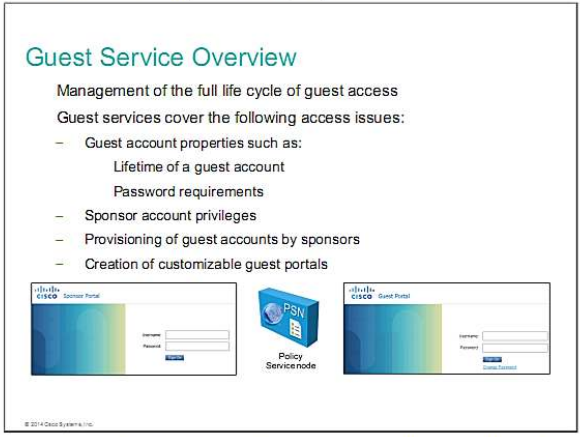
- Describe the purpose of the Cisco ISE guest services
- Describe the interaction between WebAuth and the guest services
- Describe the Cisco ISE guest service applications
- Describe the admin portal configuration scope
- Describe the sponsor portal configuration scope
- Identify the guest user portal functions
- Describe the portals on which the Cisco ISE nodes run
- Describe the guest service configuration procedure
- Configure the portal HTTPS ports
- Describes how to manage sponsor groups
- Assign users to sponsor groups
- Configure the guest policies
- Configure the default or custom guest portal
- Describes the guest authorization
- Describe how to provision guest accounts using the sponsor portal
- Describe how to verify the guest access

https://t.me/learningnets

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Guest Service Overview

This topic describes the Cisco Identity Services Engine guest service.

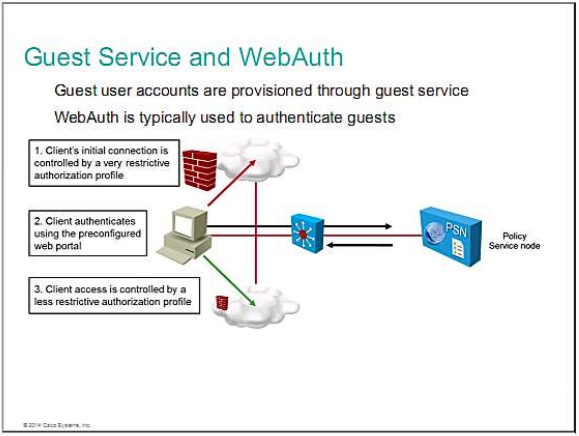


Cisco ISE guest services cover the full life cycle of guest accounts. The users with privileges to create guest accounts are called sponsors. Cisco ISE guest services provide customizable portals for both guests and sponsors.

The Cisco ISE administrator assigns privileges to sponsors, who in turn may define the attributes of the guest users. Any sponsor with appropriate privileges can easily create temporary guest accounts. Cisco ISE allows sponsors to provide account details to the guest by printout, email, or SMS. The entire experience, from user account creation to guest network access, is stored for audit and reporting purposes.

Guest Service and WebAuth

This topic describes how the guest services and WebAuth interoperate.



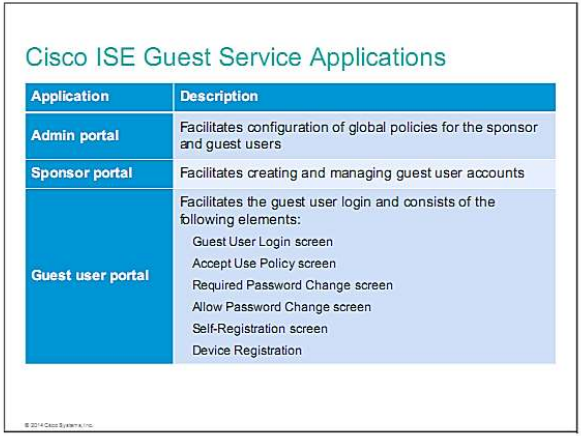
Cisco Identity Services Engine guest services are enabled by the WebAuth functionality. When a guest user first connects to the local network, either through a wireless or wired connection, the Cisco ISE assigns that user a restrictive authorization profile defined to support the WebAuth function.

WebAuth allows guests, visitors, contractors, consultants, or customers to perform an HTTP or HTTPS login to access a network, whether that network is a corporate intranet or the public Internet. Based on the initial restrictive authorization profile, the NAD intercepts the HTTP request and redirects it to the guest user login portal. The user is presented with a login page and must enter a username and password. After successful authentication, the user is associated with the appropriate authorization profile and is provided with controlled network access.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Cisco ISE Guest Service Applications

This topic describes Cisco Identity Services Engine guest service applications.



Cisco ISE guest services include three applications:

Cisco ISE admin portal: This is ISE's main management interface and among many other things this portal facilitates the configuration of global policies for sponsors and guest users.

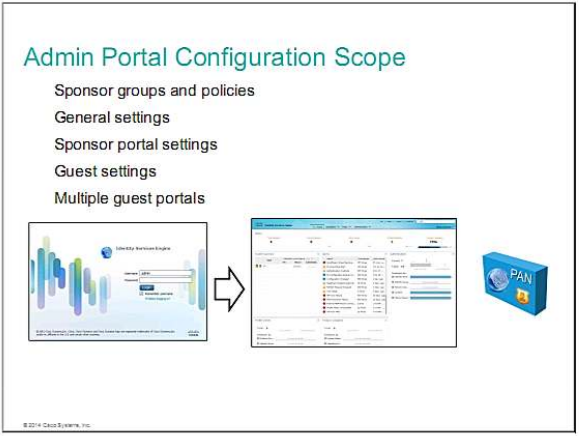
Sponsor portal: This portal is accessed by sponsors and facilitates the creation and management of guest user accounts.

Guest user portal: This portal facilitates the guest user login. It consists of the Guest User Login screen, Acceptable Use Policy screen, Required Password Change screen, Allow Password Change screen, Self-Registration screen, and Device Registration facility.

In a distributed ISE deployment, the admin portal is implemented on the node running the primary admin persona. The Sponsor portal and guest portal are implemented on nodes running the policy services personal and configured to run session services.

Admin Portal Configuration Scope

This topic defines the configuration scope of the admin portal.



From the Cisco Identity Services Engine admin portal, you can configure the following items:

Define sponsor groups and their associated privileges and define authorization rules that specify sponsor group membership.

Definition of general settings including: Specify portal themes including color schemes, logo and banner images, and manner messages. Specify the TCP port used by different portals. Configuration of automatic purging of expired guest accounts.

Sponsor portal settings, such as the language templates, sponsor portal customization, and sponsor identity source sequence.

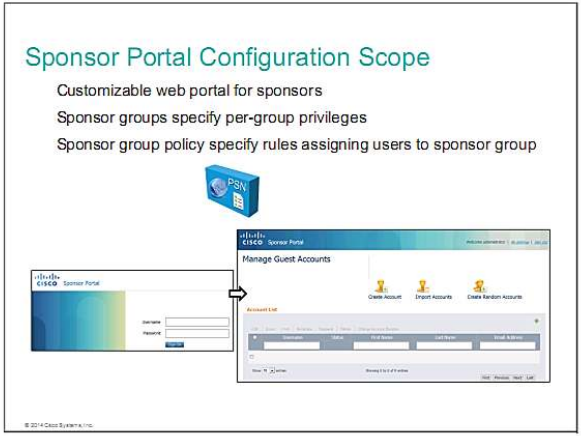
Guest settings, such as username policy, password policy, guest portal policy, guest details policy, multiportal settings, and time profiles.

Multiple guest portals can be configured. For example, the portal for long term contractors can be different than the portal for short term visitors.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Sponsor Portal Configuration Scope

This topic defines the configuration scope of the sponsor portal.



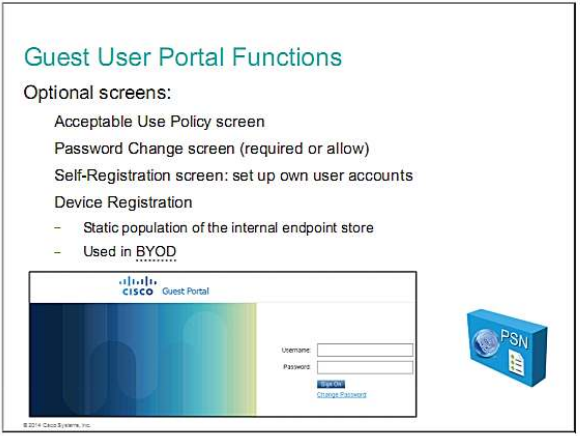
The sponsor portal allows a guest sponsor to create, edit, delete, suspend, reinstate, and view guest user accounts.

Authentication for the sponsor portal uses its own identity source sequence. The default identity source sequence defined in Cisco Identity Services Engine for this purpose is named Sponsor_Portal_Sequence which specifies the internal user database. This sequence can be edited or a new sequence can be defined and assigned to the sponsor portal authentication.

The ISE administrator defines sponsor groups. Each sponsor group has its own unique set of privileges including a set of authorization roles, guest role options and time profile options. The ISE administrator also defines the sponsor group policy which is a set of authorization rules that maps users to sponsor groups.

Guest User Portal Functions

This topic describes the functions of the guest user portal.



The guest user portal consists of the following customizable elements:

Guest User Login screen: This screen enables guest authentication by providing the username and password fields.

Acceptable Use Policy screen: This screen defines the Terms of Use agreement. It can be customized on a per-language basis. Its use is optional. By default it is displayed at first login. Optionally it can be set to display at every login or it can be disabled.

Required Password Change screen: By default, guests are required to change their password upon first login. As such, they will be presented this screen. The requirement can be disabled.

Allow Password Change screen: The guest portal can be configured to provide a change password link at the login screen to allow users to change their passwords anytime after the first login. This screen will be displayed if the user selects that link. This feature is enabled by default.

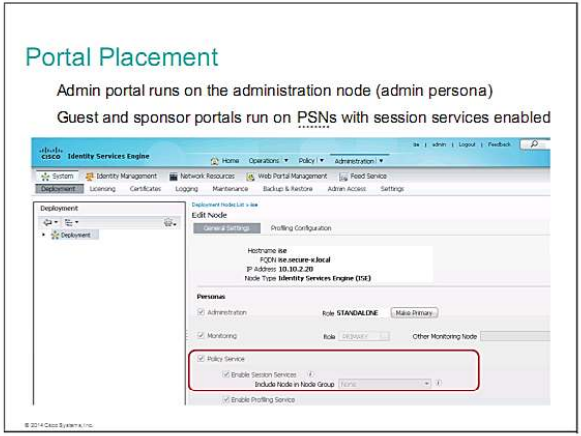
Self-Registration screen: This screen is an optional screen that allows guests to set up their own user accounts.

Device Registration: If enabled, this option allows guest user accounts to self-register a predefined number of endpoints by MAC address. Registration results in static population of the internal endpoint store without a default ID group assignment. User needs valid credentials to register devices.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Portal Services Location

This topic identifies the nodes on which the portals are running.



Cisco Identity Services Engine supports a distributed deployment to allow for multiple Cisco ISE nodes to communicate with one another, providing scalability and fault tolerance. In distributed deployments, ISE functionality is divided amongst the admin, monitoring and policy services personas.

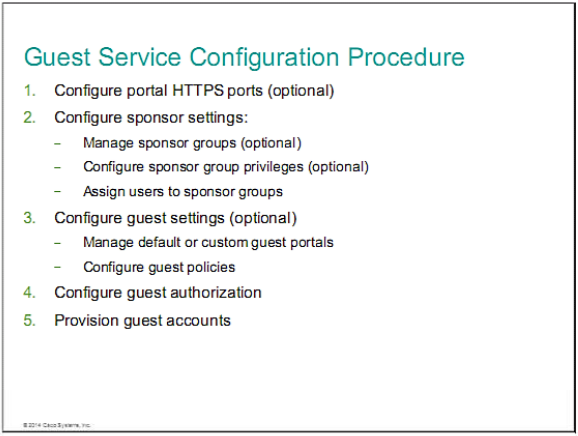
The admin portal runs on the Cisco ISE node running the active admin persona. The guest and sponsor portals run on on all nodes which have the policy service persona configured with the session services functionality enabled.

Guest portals must be located on the same policy service nodes that manage the RADIUS requests that arrive from the NADs. For example, if a node is used to manage RADIUS requests for a NAD that depends on Central WebAuth support, the guest portal must be enabled on that node.

In this figure, the ISE runs in a standalone deployment. In this situation the session services are activated by default and cannot be disabled.

Sponsor Portal Configuration Procedure

This topic describes the configuration procedure of the Cisco Identity Services Engine sponsor portal.



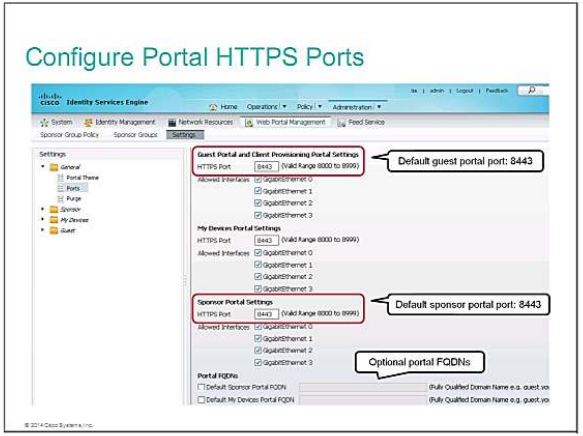
The configuration of the ISE guest services can include many customizable elements. The key steps are listed in this procedure:

1. Configure portal HTTPS ports (optional).
2. Configure sponsor settings:
   - Manage sponsor groups (optional).
   - Configure sponsor group privileges (optional).
   - Assign users to sponsor groups.
3. Configure guest settings (optional).
   - Manage default or custom guest portals.
   - Configure guest policies.
4. Configure guest authorization.
5. Provision guest accounts.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Configure Portal HTTPS Ports

This topic illustrates how to configure portal SSL ports.

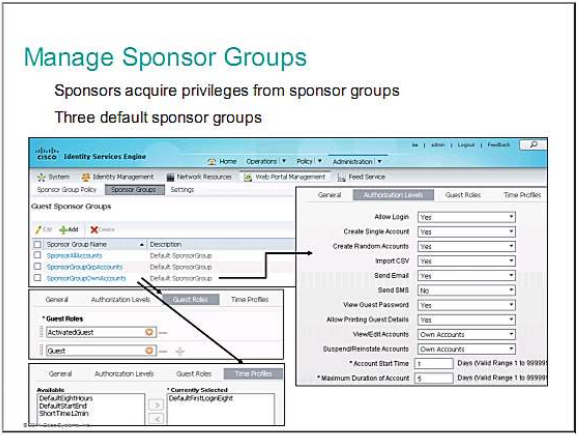


You can customize the sponsor portal and configure general sponsor settings that govern how sponsors access customized web portals to create and manage guest user accounts. To manage the HTTPS ports, choose **Administration > Guest Management > Settings**, click the icon next to **General**, choose **Ports**, and review the default network ports that are used for sponsor and guest portal access. By default, TCP port 8443 is used for secure portal access by both sponsors and guests.

Optionally, you can define an FQDN for the sponsor portal that is easier for the sponsors to remember. If you choose to implement this, you must also insure that DNS resoloution for the FQDN is set up. Also, the certificate installed in ISE should specify this FQDN as a Subject Alternative Name to avoid browser warnings on HTTPS sessions.

Manage Sponsor Groups

This topic describes how to manage sponsor groups.



Users are assigned to sponsor groups, from which they acquire privileges to provision guest users. Cisco Identity Services Engine comes preconfigured with three default sponsor groups:SponsorAllAccounts, SponsorGroupGrpAccounts, and SponsorGroupOwnAccounts. Guest sponsor groups define the permissions and settings for the sponsor user. Sponsor users that belong to a particular sponsor group have a certain set of permissions and settings when they log into the sponsor portal. The ISE administrator manages sponsor groups and sponsor group assignments.

Sponsor group configuration is available under **Administration > Web Portal Management > Sponsor Groups**. The settings for each group are configured under four tabs: General, Authorization Levels, Guest Roles and Time Profiles.

The only setting under the **General** tab is the sponsor group description.

Several permissions are configured under the **Authorization Level** tab. The allowed methods of creating accounts is set here. Create Single Account allows for creation of accounts one at a time. Create Random Accounts and Import CSV allow the creation of a set of accounts. Also, methods of informing guests of their accounts including ID and password information is set here. Options include Send Email, Send SMS, View Guest Password and Allow Printing Guest Details. Other management features such as the ability to View/Edit Accounts and Suspend/Reinstate Accounts is configured here.

The ISE administrator can define different guest roles and allow sponsors in a given sponsor group the privilege to create guest accounts in certain roles. Guest roles allow a sponsor to assign different levels of access to a guest account. These roles are used in the authorization policies to relate guest user accounts to identity groups. You configure the selectable guest roles under the **Guest Roles** tab within the sponsor group configuration menu.

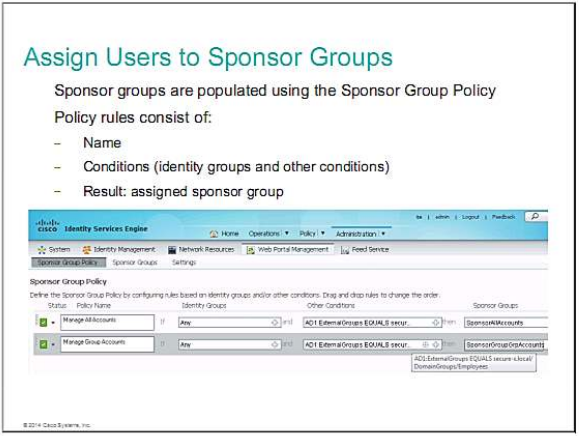
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Time Profiles specify the duration of a guest account in terms of minutes, hours, days or years. When the timer begins (FromCreation, FromFirstLogin or StartEnd) is also set under the time profile. Account expiration notification and any time restrictions (such as logins only permitted on weekdays during business hours) are set under time profiles. The ISE administrator defines the different time profiles and also defines which time profiles are available to the sponsor group under the **Time Profiles** tab.

https://t.me/learningnets

Assign Users to Sponsor Groups

This topic describes how to assign users to sponsor groups.

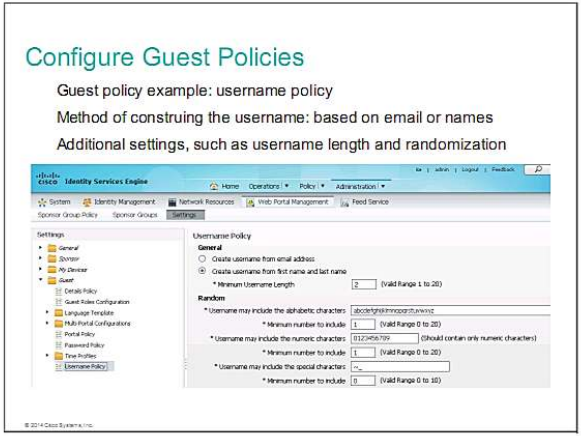


The assignment of the sponsors to sponsor groups is configured in the Sponsor Group Policy. Similar to authorization policy, the sponsor group policy consists of one or more rules. Each rule is identified by a name and includes one or more conditions and a result. The conditions can either identify a user identity group or include other definable conditions. The result specifies the sponsor group assigned to users who meet the conditions in this policy rule. The sponsor users acquire privileges from the sponsor groups.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Configure Guest Policies

This topic explains how to configure the guest username policy.



You can configure various policies that control the generation of guest accounts. One of the available policies is the username policy, which is shown in the figure. The guest **Username Policy** configuration page allows you to specify how usernames will be created for the guest accounts. The **Username Policy** configuration screen has two main sections: **General** and **Random**.

You can create a guest username that is based on the email address or the first and last name of the guest. The configuration is performed in the **Administration > Guest Management > Settings > Guest > Username Policy** menu.

The **Random** configuration section offers the option to choose the characters that are used for generating random user accounts.

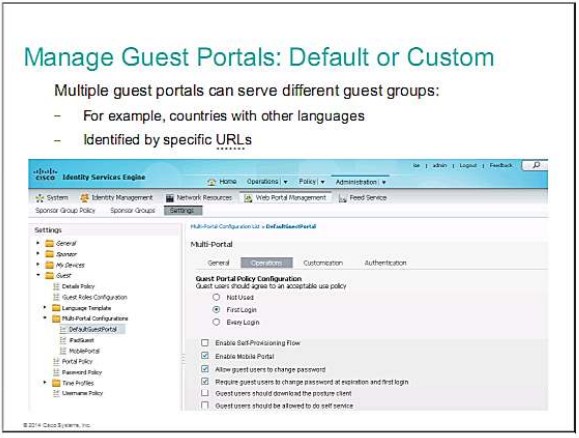
Other configurable policies are the details and the password policy.

The guest details policy determines the data that the sponsor needs to enter to create a guest account. In the **Details** page, the Cisco Identity Services Engine administrator must define the fields that should appear on the Sponsor Guest User Create and Edit pages and in the Guest User Self-Registration page.

The guest password policy determines how the password should be generated for all guest accounts. You can create a password policy that is based upon a mixture of alphabetic, numeric, and special characters.

Manage Guest Portals: Default or Custom

This topic describes how to configure the operation of the default and custom guest portals.



The Cisco Identity Services Engine allows you to host multiple portals on the Cisco ISE policy service nodes. The default portal pages are dynamically generated and provide features such as changing a password and self-registration in the login screen.

The default portal themes have standard Cisco branding by default. There are several simple customizations that can be made under **Administration > Web Portal Management > Settings, General > Portal Theme**. For example you can provide your own login page logo and banner logo as well as background images and color schemes.

You can also choose to completely customize a portal by uploading HTML pages that are specific to your organization. These pages must use plain HTML code and must contain form actions that point to the portal back-end servlets. You must define separate HTML pages for login, AUP, the change-password function, and self-registration. Additionally, when you create custom portals by uploading your own HTML pages, the details policy, language templates, and portal themes do not apply.

The predefined **DefaultGuestPortal**, which is shown in this example, is available under **Guest > Multi-Portal Configurations**.

In the **Operations** tab of the portal configuration, you can define the following guest actions:

Guest users should agree to an AUP. The selectable options are **Not Used**, **First Login**, and **Every Login**.

Allow guest users to change passwords.

Require guest and internal users to change passwords at expiration.

Guest users should download the posture client.

Check the **VLAN DHCP Release** option to refresh the IP address of Windows clients after a VLAN change. This option applies to wired and wireless environments for guests with no posture.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

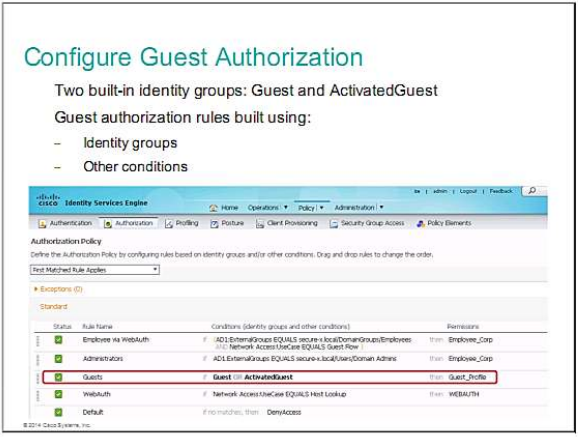
Guest users should be allowed to perform self-service.

Guest users should be allowed to perform device registration.

https://t.me/learningnets

Configure Guest Authorization

This topic describes the guest authorization.



You should configure authorization policy rules for guest users if you don't want them to be authorization using the default rule.

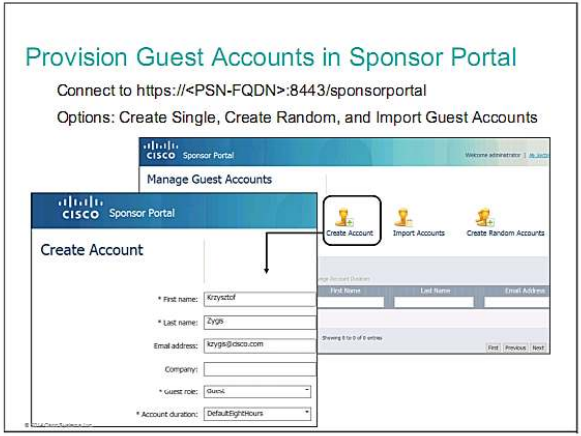
Cisco Identity Services Engine defines two guest roles, Guest and ActivatedGuest. The guest role must authenticate via the web portal. The ActivatedGuest role may authenticate via the web portal or via 802.1X. ISE also provides two user identity groups named Guest and ActivatedGuest. These two groups are assigned to the guest role that matches their name. The guest role assignment of a user identity group is set under **Administration > Web Portal Management > Settings, Guest > Guest Roles Configuration**.

The figure shows the authorization policy rule list, highlighting the rule that assigns users in the either the Guest or the ActivatedGuest user identity group the authorization profile named Guest_Profile.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Provision Guest Accounts in Sponsor Portal

This topic describes how to provision guest accounts using the sponsor portal.



To create guest accounts, connect to the sponsor portal and log in as a sponsor user. The sponsor portal is accessible at the address https://<PSN-FQDN>:8443/sponsorportal. This address assumes that the default port 8443 of the sponsor portal has not been changed for the admin portal.

One method of provisioning guest user accounts is for a sponsor to manually create individual guest user accounts. The attributes that are presented to the sponsor have been defined in the guest details policy. They generally include first name, last name, guest role and account duration.

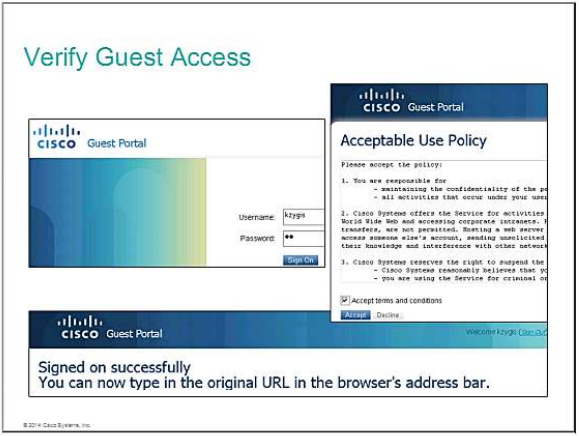
Alternatively, you may create a number of random users with a single request. In order to configure random users in the sponsor portal, choose the **Create Random Guest Accounts** menu from the main **Sponsor Portal** window. You will then specify the number of random users to create, a username prefix (if any), and the guest role to which these users should be added.

The third option is to import guest user accounts from a CSV file. The template file determines the format of the file. The template file can be downloaded and viewed using the **Download Import File Template** button. The file template contains a comma-delimited list of attributes. The file template does not contain any line feed characters.

https://t.me/learningnets

Verify Guest Access

This topic describes how to verify the guest access.



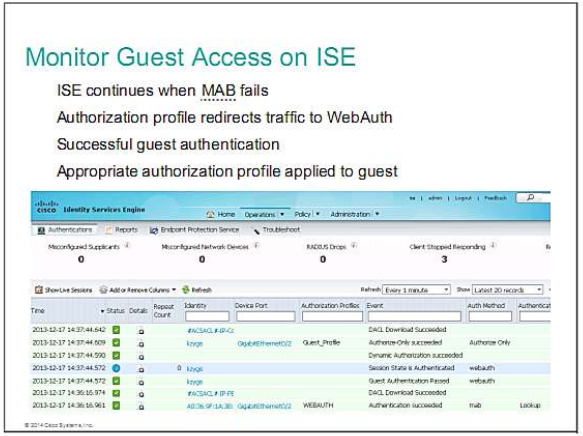
This slide depicts the default authentication operation of the guest portal. The user is first challenged for credentials. If they provide valid credentials they are presented with the **Acceptable Use Policy** page. When user accepts the AUP conditions, they will be required to change the password (now shown here). They are then informed about the successful login and they can reconnect to the original URL, or make any other network connections that are allowed by their authorization profile.

The use of an acceptable use policy and password change requirements are options that can be changed by the Cisco Identity Services Engine administrator.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Monitor Guest Access on ISE

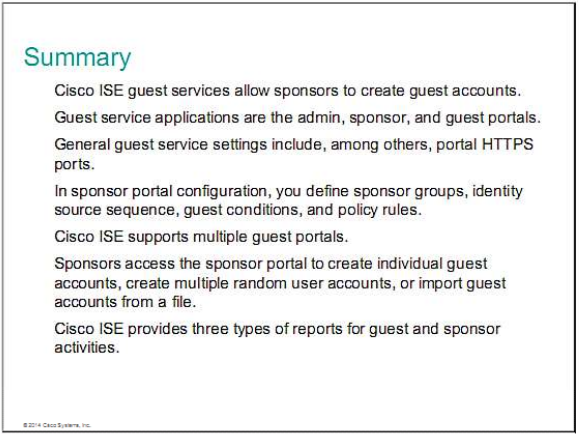
This topic describes how to monitor guest access on the Cisco Identity Services Engine.



You can monitor the guest access in the ISE authentication page. This figure illustrates event records from the process. It starts with a succeeded authentication when the guest user fails the MAB and the ISE continues because the user is not found. The ISE redirects the client traffic to WebAuth using the WEBAUTH authorization profile. When the guest opens a browser and attempts a web connection, the session is redirected to the guest portal. The user successfully authenticates, and the ISE assigns the appropriate authorization profile to the guest session.

Summary

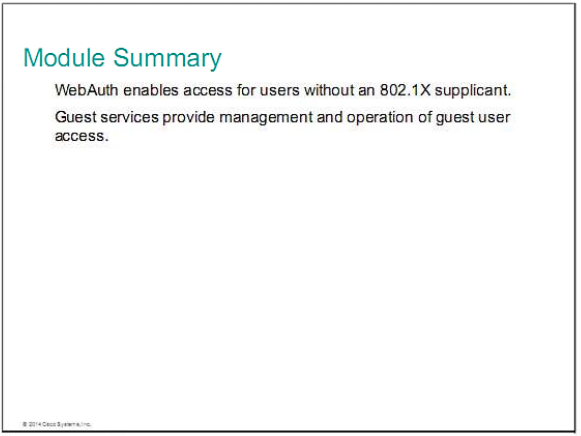
This topic summarizes the key points that were discussed in this lesson.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Module Summary

This topic summarizes the key points that were discussed in this module.



References

For additional information refer to this resource:

Cisco Identity Services Engine User Guide

https://t.me/learningnets

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Module Self-Check

Questions

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

1. In which scenario would you deploy WebAuth? (Source: Deploying WebAuth)

   A. network printers without an 802.1X supplicant
   B. company employees with a new 802.1X supplicant
   C. guest users
   D. sponsors using a new endpoint type

2. Which traffic type must be permitted in the redirection ACL that is configured on the switch? (Source: Deploying WebAuth)

   A. RADIUS communication with the Cisco ISE nodes
   B. synchronization traffic between the Cisco ISE nodes
   C. HTTP or HTTPS traffic to the Cisco ISE policy service nodes
   D. HTTP or HTTPS traffic that is eligible for redirection
   E. all traffic to the Cisco ISE nodes

3. How do you configure the Cisco ISE authentication policy for WebAuth? (Source: Deploying WebAuth)

   A. to continue if the authentication failed
   B. to continue if the user is not found
   C. to continue if the process failed
   D. to continue if the 802.1X supplicant is not available

https://t.me/learningnets

4. What is a valid configuration for the sponsor and guest portals? (Source: Deploying Guest Access Services)

   A. selection of HTTP or HTTPS protocol that should be used
   B. HTTP port
   C. HTTPS port
   D. identity certificate to be used for authentication

5. On which Cisco ISE nodes would you enable sponsor and guest portals? (Source: Deploying Guest Access Services)

   A. the sponsor portal on different nodes than the guest portal, to distribute load
   B. the guest portal preferably on redundant nodes, to distribute load
   C. the sponsor portal on the policy service nodes that process user access requests
   D. the sponsor portal on the admin nodes, because they are used only for provisioning

6. The sponsor group policy can be used to define guest account restrictions. (Source: Deploying Guest Access Services)

   A. true
   B. false

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Answer Key

1. C
2. D
3. B
4. C
5. C
6. A

https://t.me/learningnets

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Module 5

Endpoint Access Control Enhancements

The Cisco Identity Services Engine offers a range of advanced endpoint access control features. You can use them to enforce compliance and enhance infrastructure security. This module discusses the posture, profiler and Bring Your Own Device (BYOD) solutions.

Upon completing this module, you will be able to:

- Describe the posture assessment and the use of NAC agents
- Describe the Cisco ISE profiler and the endpoint identity groups
- Describe the BYOD solution elements and device onboarding

https://t.me/learningnets

https://t.me/learningnets

Lesson 1

Deploying Posture Service

Overview

The Cisco Identity Services Engine posture service provides you with the ability to check the health of endpoints and, depending on the results, assign appropriate connectivity permissions. Cisco ISE determines the security posture by obtaining from the NAC agent of the endpoint the status of various software components, such as service packs, software patches, and antivirus and antispyware applications.

Upon completing this lesson, you will be able to:

- Describe the Cisco ISE posture service
- Identify the posture service in the overall Cisco ISE processing flow
- Describe the persistent NAC agents
- Describe the Cisco NAC Web Agent
- Describe the client provisioning process
- Describe the posture conditions
- Describe the role of Change of Authorization in the posture assessment
- Describe the posture configuration procedure
- Describe how to download the client provisioning resources to the ISE
- Describe the configuration of the client provisioning policy
- Describe the posture policy building blocks
- Describe the configuration of posture conditions
- Describe the configuration of posture remediation
- Describe the configuration of posture requirements
- Describe the configuration of posture policy rules
- Describe the configuration of posture-related authorization conditions

https://t.me/learningnets

Describe the configuration of posture-related authorization policy

Describe how to verify client redirection to CPP

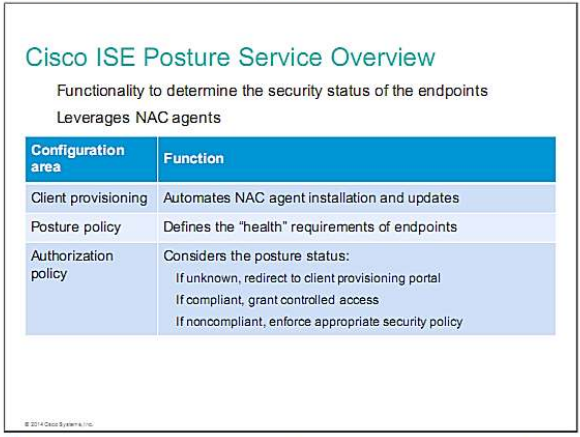
Describe how to verify the remediation

Describe posture verification using the Cisco ISE authentications page

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Cisco ISE Posture Service Overview

This topic describes the functional areas of the posture service.



The Cisco Identity Services Engine posture service allows you to check the security posture of the endpoints that are connecting to your Cisco ISE-enabled network. The Cisco ISE validates that the endpoint state is compliant with your corporate security policies before a client is given access to protected areas of your network.

The security posture of the endpoints is communicated to the Cisco ISE policy service node by NAC agents. The NAC agents are installed on the clients and interact with the posture service to enforce security policies on the endpoints. They assist you in evaluating clients against posture policies and ensuring that clients meet requirements that are required for compliance with the security policies of your organization.

The posture service has three main functional areas:

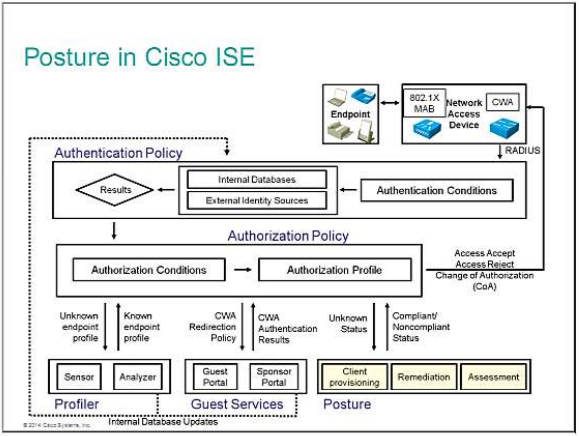
Client provisioning: Client provisioning automates NAC agent deployment by pushing the software to endpoints that do not have the required version of the expected NAC agent. The client provisioning is facilitated by the client provisioning portal.

Posture policy: Posture policy defines the terms compliant and noncompliant in a specific company policy. For example, compliance may mean a certain version of antivirus and antispyware software that is installed on the endpoint.

Authorization policy: The authorization policy is implemented in a way that reflects the noncompliant and compliant states of the endpoints. The authorization policy will enforce stricter security policy on noncompliant endpoints and grant more privileges to compliant endpoints. If the endpoint status is unknown, the authorization policy will redirect the traffic to the client provisioning portal.

Posture in Cisco ISE

This topic identifies the posture service in the Cisco Identity Services Engine processing.



The posture service is an optional function of the Cisco ISE that may or may not be deployed in a Cisco ISE environment. The posture service interacts with the Cisco ISE authorization function via the CoA.

Immediately after authentication, the posture status of the endpoint is unknown. When the posture service is invoked and the endpoint status is assessed, the status will change to noncompliant or compliant:

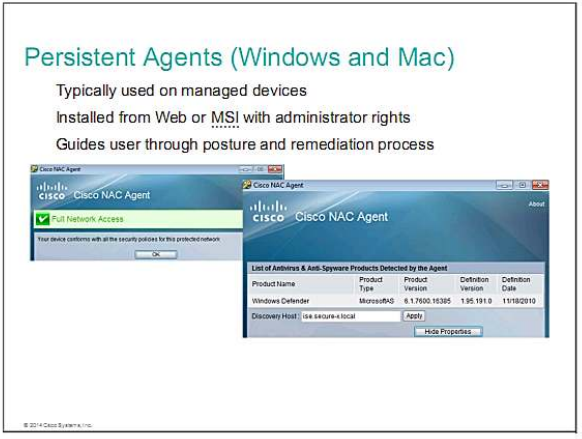
When the noncompliant status is returned by the posture service, a CoA is issued, and the Cisco ISE applies the appropriate authorization policy to the endpoint. This authorization policy typically enables the endpoint to access necessary remediation resources. After successful remediation, the endpoint is assessed again and its status is changed to compliant.

When the compliant status is returned by the posture service, a CoA is issued, and the Cisco ISE applies the appropriate authorization policy to the endpoint. This authorization policy enables the endpoint to access internal enterprise resources without a risk of infection. Periodic reassessment of the security posture ensures that the health of the system is maintained while the endpoint is granted controlled access to the enterprise resources.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Persistent Agents (Windows and Mac)

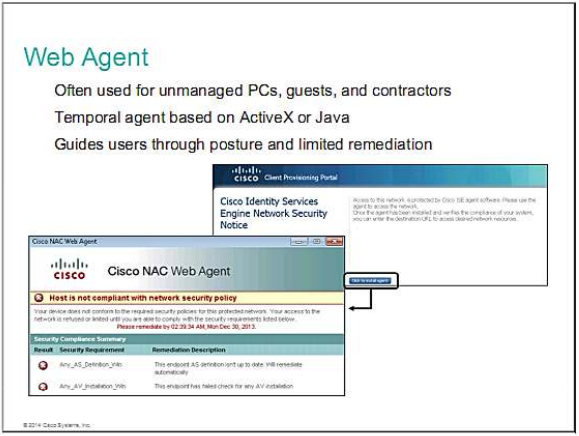
This topic describes the persistent NAC agents for Windows and Mac endpoints.



The persistent NAC agents, available for Windows and Mac computers, are typically used on managed devices. They support localization, using the more common languages. The agents can be installed from the Web browser or using the MSI package. Administrator rights are required to install or update the agent software. The agents are capable of handling user logons and SSO in an 802.1X environment. The NAC agents guide users through the posture service, support the posture remediation, and inform the policy service node about an IP address change that occurs while a session is active. The Cisco Identity Services Engine supports automatic NAC agent updates.

Web Agent

This topic describes the Cisco Network Admission Control Web Agent.

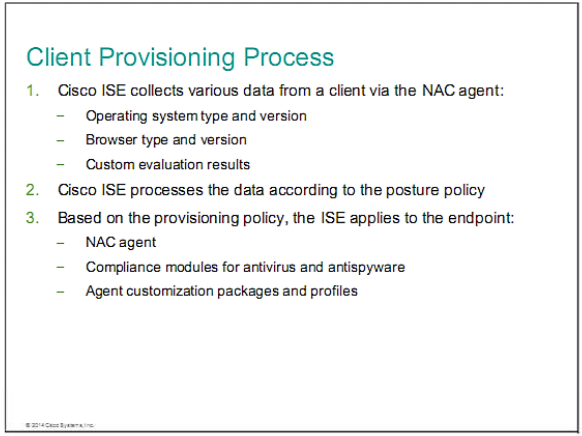


The Cisco NAC Web Agent is typically used for unmanaged PCs and guest access. The agent is temporal, and requires ActiveX or Java to be installed on the endpoints. It supports the Cisco Identity Services Engine posture service, but offers less remediation options than the persistent agents. The web agent is also capable of refreshing endpoint DHCP addresses in the case where policy application enforces a VLAN change.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Client Provisioning Process

This topic describes the client provisioning process.



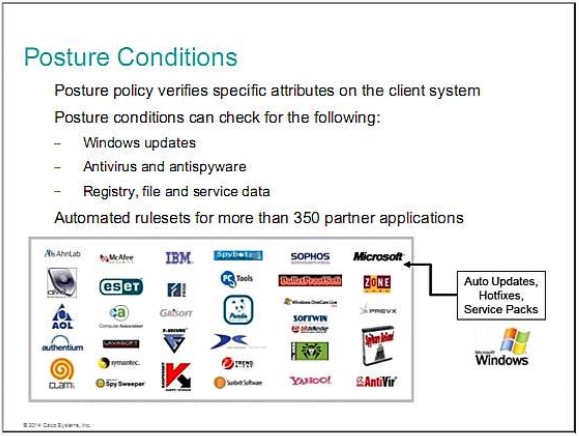
Client provisioning is responsible for pushing appropriate NAC agent software or configuring a native NAC supplicant on the endpoints. The Cisco Identity Services Engine looks at various elements when classifying the endpoint, such as the client machine operating system and version, the client machine browser type and version, the group to which the user belongs, and the condition evaluation results (based on applied dictionary attributes).

After the Cisco ISE classifies an endpoint, it uses client provisioning resource policies to ensure that the endpoint is set up with an appropriate agent version, up-to-date compliance modules for antivirus and antispyware vendor support, and correct agent customization packages and profiles. The up-to-date compliance modules for antivirus and antispyware software are needed to verify if the endpoints run the required antivirus and antispyware applications and have up-to-date signature databases. Instead of using the NAC agent, client provisioning could configure an appropriate native supplicant on the client device.

The customization of the client package parameters is achieved with the use of profiles that define the software packages that are to be provisioned, their version, and if applicable, their database version.

Posture Conditions

This topic describes the posture conditions.



Posture conditions are used to check specific attributes on the client system. A posture condition can be one or any combination of the following conditions:

File condition: This simple condition checks the existence of a file, the date of a file, and the versions of a file on the client. This condition is available for Windows computers.

Registry condition: This simple condition checks for the existence of a registry key or the value of the registry key on the client. This condition is available for Windows computers.

Application condition: This simple condition checks whether an application (process) is running on the client. This condition is available for Windows computers.

Service condition: This simple condition checks whether a service is running on the client. This condition is available for Windows computers.

Dictionary simple condition: This simple condition checks an attribute that is associated to an operator and the operator to a value.

Examples of common posture conditions include the following:

Windows update verification: This posture condition verifies the proper service pack and patch levels.

Virus application verification: This posture condition verifies that the client has the correct antivirus software installed. This function may also be used in a less restrictive capacity to verify that the client simply has any antivirus installed.

Virus definition verification: This posture condition verifies that virus definitions are newer than a specific date.

Windows screen saver password verification: This posture condition verifies that the client has a Windows screen saver password configured.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

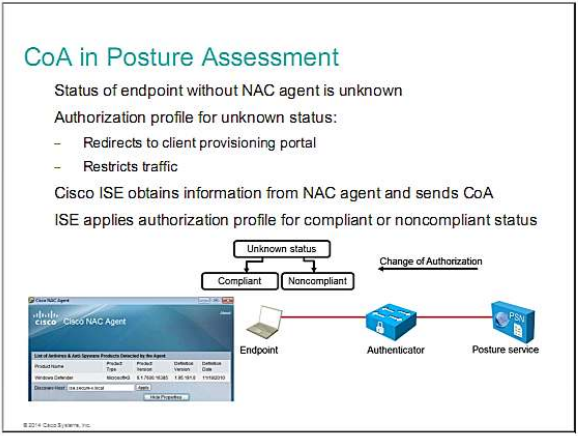
Registry entry verification: This posture condition verifies the client registry key.

The Cisco Identity Services Engine provides automated rulesets to simplify management for more than 350 partner applications, including Microsoft Windows, online services, and antivirus software vendors.

When deploying posture services, maintenance of current posture elements should be considered. ISE supports updates from www.cisco.com. The updates can be manually initiated or scheduled to run on a recurring timer. These features are available in the ISE administration GUI under **Administration > System > Settings, Posture > Updates**.

CoA in Posture Assessment

This topic describes the role of Change of Authorization in the posture assessment.



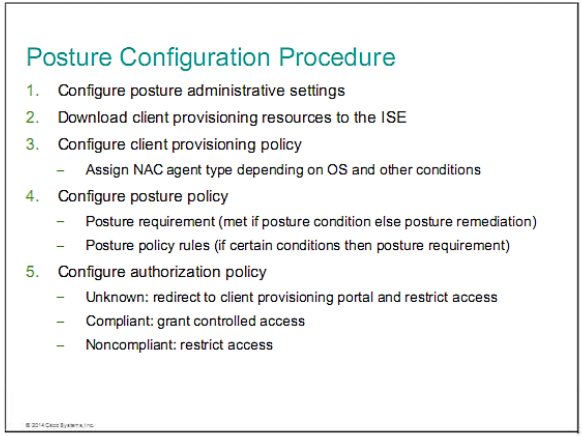
The Cisco Identity Services Engine uses the CoA feature to facilitate the posture service. When a new endpoint is connected to the network, if it does not have a NAC agent then its posture status is unknown. The ISE authorization policy has a rule that matches the unknown status, redirects the client to the client provisioning portal and restricts the client traffic. When the user opens a browser, the session will be redirected to the client provisioning portal and the user will install an appropriate NAC agent.

The NAC agent collects the security posture information and sends to the ISE. The ISE declares the endpoint as either compliant or noncompliant. The ISE sends the CoA to signal the endpoint that a new authorization profile will be applied and assigns an appropriate authorization profile to the client session,

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Posture Configuration Procedure

This topic describes the posture configuration procedure.



Posture administrative settings pertain to the client provisioning service, agent profiles, posture settings, reassessments, and updates. They are omitted from this lesson in favor of the key elements. The settings are defined under **Administration > System > Settings, Posture** in the Cisco Identity Services Engine administration GUI. In a production environment, the posture update policy should be considered. Posture updates include a set of predefined checks, rules, and support charts for antivirus and antispyware for both Windows and Macintosh operating systems, and operating systems information that are supported by Cisco. You can also update Cisco ISE offline from a file on your local system, which contains the latest archives of updates. Timer based automatic posture updates can be configured in the posture administrative settings.

To support client provisioning, you should first download the appropriate agents to ISE.

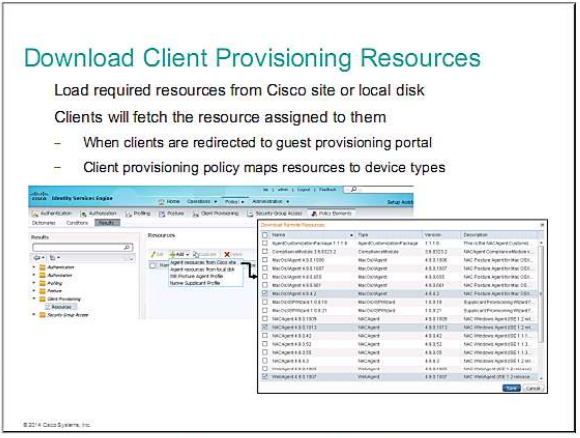
The client provisioning function is responsible for the automatic update of installed NAC agent software and the automatic configuration of a native supplicant, along with the required packages, on the endpoints.

A posture policy defines the technical terms that describe the compliance requirements. For example, a compliant endpoint can be a client machine with up-to-date antivirus software. A posture policy consists of one or more rules, and each rule is identified by a name and configured to match one or more conditions.

Although not strictly a part of the posture service, the Cisco ISE authorization policy plays a pivotal role in the overall posture operation. The authorization policy needs to be adjusted to reflect the compliant, noncompliant, and unknown endpoint states.

Download Client Provisioning Resources

This topic describes how to download the client provisioning resources to the Cisco Identity Services Engine.



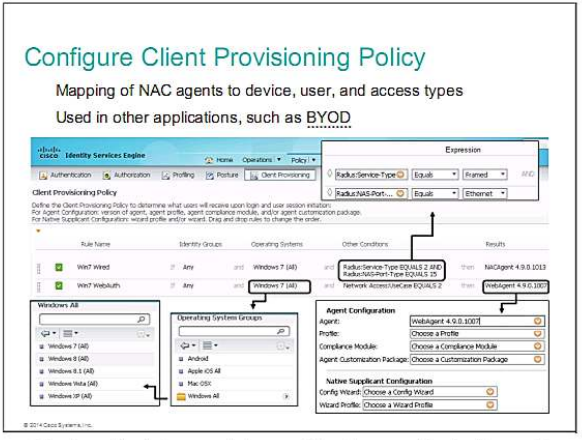
Client provisioning is responsible for the automatic update of installed NAC agent software and the automatic configuration of a native supplicant on the endpoints.

You need to download the required client provisioning resources to the ISE. When downloaded, the ISE will be able to redirect the endpoints to the client provisioning portal from which they will be able to fetch the NAC agent suited for them. The type of the NAC agent appropriate for each device type is defined by the client provisioning policy.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Configure Client Provisioning Policy: Operating System and Conditions

This topic describes the configuration of the operating system checks and conditions for a client provisioning policy.



The client provisioning policy is the central element of the client provisioning feature. The policy is built using an intuitive approach that you know from the authentication and authorization policies. Client provisioning consists of one or more rules that you can edit, delete, duplicate, and reorder. Each rule has a set of conditions (identity groups, operating system type, and other conditions) and, if they are met, the specified results are applied. The results define the required NAC agent or native supplicant software.

When specifying the operating system condition, choose from the predefined operating system types, such as Android, Mac OS X, Apple iOS, or Microsoft Windows. You can collectively select the **Windows All** option or specify Windows 8, Windows 8.1, Windows 7, Vista, or XP individually.

Each client provisioning rule contains the **Results** column. The results contain the **NAC Agent Configuration** and the **Native Supplicant Configuration** sections. The results are used to define the software that will be provisioned on the endpoint if all conditions in the policy rule are met.

Depending on the endpoint operating systems that are used in your environment, you may want to provision a native supplicant software. In that case, you have the option of specifying the required configuration wizard and wizard profile.

The NAC agent settings allow you to specify the following:

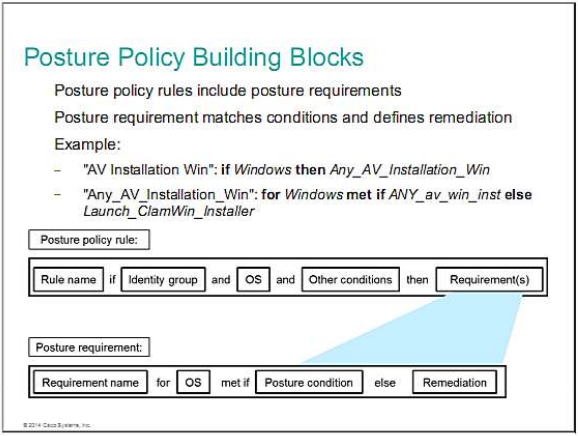
The NAC agent type and release.

The agent profile that you used to define various timers.

The compliance module.

Posture Policy Building Blocks

This topic identifies the building blocks of a posture policy.



A posture policy defines the technical terms that describe the compliance requirements. For example, a up-to-date antivirus software may be a requirement for compliance. A posture policy consists of one or more rules, and each rule is identified by a name and configured to match one or more conditions.

The posture condition can be specified as a single or compound condition in several categories: file, registry, service, application, regular compound condition, antivirus, and antispyware.

The differentiator of the posture policy from other policy types is the requirements definition. The requirements are written as an expression: "Requirement for 'OS' met if 'posture condition' else 'remediation.'"

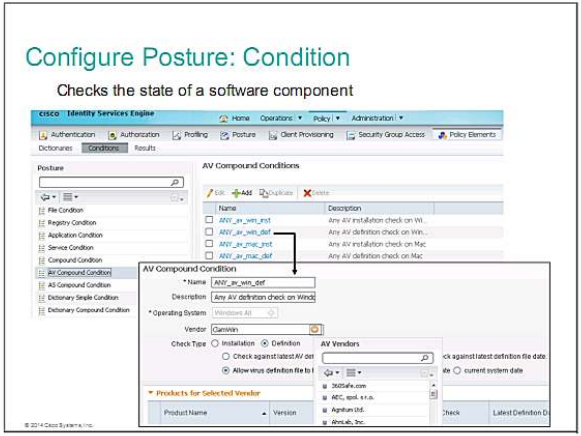
The remediation defines the action that must be performed, if the posture condition is not met, for the endpoint to achieve the compliant status. The remediation actions can be of different types: antispyware remediation, antivirus remediation, file remediation, launch program remediation, link remediation, Windows Server Update Services remediation, or Windows Update remediation.

The above example of a posture policy rule and a corresponding posture requirement can be used to install ClamWin antivirus software if no AV software is found on the endpoint. The posture policy rule named "AV Installation Win" could read: if Windows then Any_AV_Installation_Win. The posture requirement named "Any_AV_Installation_Win" could read: for Windows met if ANY_av_win_inst else Launch_ClamWin_Installer. The Any_AV_Installation_Win requirement is one of the default requirements pre-installed on the Cisco Identity Services Engine. The ANY_av_win_inst condition is one of the default conditions preinstalled on the ISE that checks for any installed AV software. The configuration of the Launch_ClamWin_Installer remediation will be demonstrated in the configuration procedure.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Configure Posture: Condition

This topic explains how to configure a posture condition.

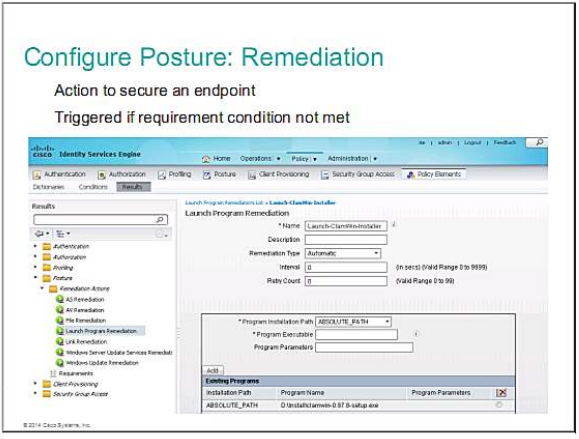


Posture conditions are used to check the state of a software component on the client endpoint. They can have different types, including file, registry, application, and service. The AV, AS conditions check for the existence of and the update status of AV and AS software.

This figure illustrates an AV compound condition. The **Vendor** drop-down box allows you to match any vendor or a specific manufacturer. The **Check Type** radio buttons allow you to specify whether the Cisco Identity Services Engine should only check the existence of the antivirus software on the endpoints (**Installation**), or the up-to-date state (**Definition**). The remaining fields are used to define the version requirements.

Configure Posture: Remediation

This topic describes how to configure the remediation.



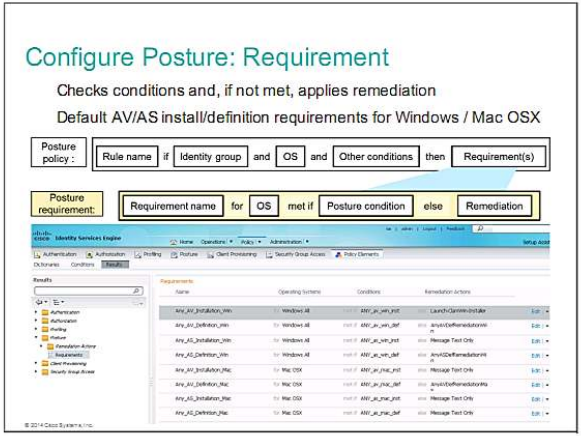
The remediation is an action performed to secure an endpoint. It is launched if the requirement condition is not met. The remediation can be manual or automatic. There are various remediation types: AS, AV, File, Launch Program, Link, Windows Server Update Services, and Windows Update.

This scenario shows a launch program remediation. It will install ClamWin antivirus if no AV software is identified on the endpoint. The remediation specifies the absolute path of the executable. The executable will be launched automatically by the NAC agent.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Configure Posture Policy: Posture Requirement

This topic describes how to configure posture requirements.



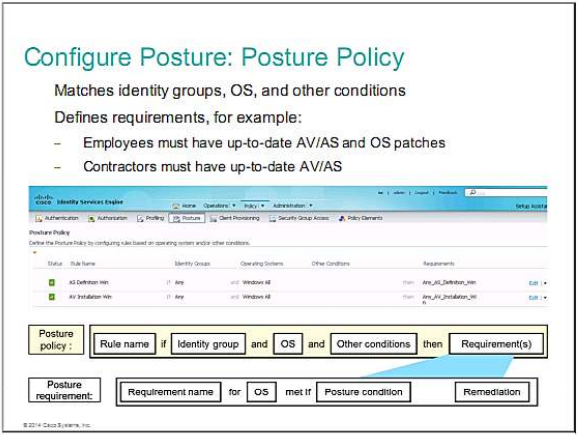
The posture requirements define the "healthy" state of an endpoint. Eight requirements are preinstalled on the Cisco Identity Services Engine and they are all disabled by default. The built-in conditions check for the presence of any antivirus and antispyware software on Windows or Mac endpoints, respectively. They provide a good starting point for defining a policy that requires antivirus and antispyware software to be installed on the client computers without having to specify the details of the software vendor and signature database. You can manipulate the existing requirements or create your own requirements.

The posture requirements are written as a expressions: "Requirement met if 'posture condition' else 'remediation.'" Although not needed in this scenario, multiple conditions may be combined using one of the three options: **All Selected Conditions Succeed**, **Any Selected Condition Succeeds**, **No Selected Condition Succeeds**.

This figure illustrates the AV/AS requirements that are by default installed in the ISE. The first requirement (Any_AV_Installation_Win) has been updated to automatically install AV if the endpoint does not have any AV software. The remediation action has been set to 'Launch-ClamWin-Installer'. All other requierments are left at their default values.

Configure Posture: Posture Policy

This topic describes how to configure a posture policy rule.



The posture policy defines the requirements that endpoints must meet to achieve the compliant status. The policy consists of rules that check one or multiple conditions: identity groups, OS, and other conditions and specify a given requirement.

In this scenario, the policy consists of two rules defined for Windows endpoints: "AS Definition Win" and "AV Installation Win". Both rules reference requirements that exist on the Cisco Identity Services Engine by default: Any_AS_Definition_Win and Any_AV_Installation_Win.

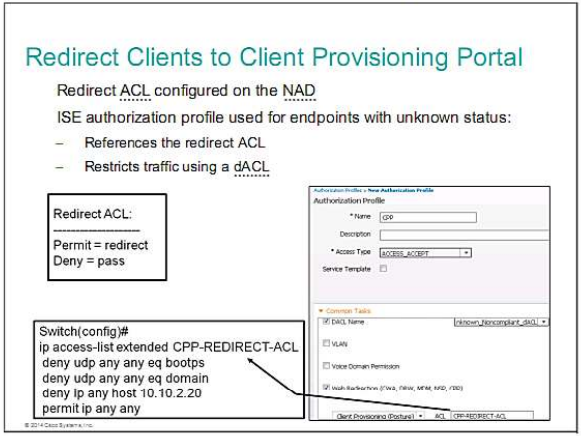
The 'Any_AS_Definition_Win' requirement enforces that any discovered AS software will be updated. It is its default configuration.

The 'Any_AV_Installation_Win' requirement enforces that ClamWin will be installed if no AV software is discovered.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Redirect Clients to Client Provisioning Portal

This topic describes how to redirect traffic to the client provisioning portal.



The endpoints must be redirected to the client provisioning portal to install the agent suitable for them. This redirection is configured jointly on the network access device and the Cisco Identity Services Engine.

The switch must have a redirect ACL configured locally. It is referenced by name in the authorization profile. The ACL permits the traffic that should be redirected and denies the traffic that will not be redirected. This ACL will typically deny basic services, such as DHCP and DNS, and the communication between the NAC agent and the ISE. You can make the ACL more specific any deny only the TCP/UDP ports used by the NAC agents in your environment. Refer to www.cisco.com for specific port numbers.

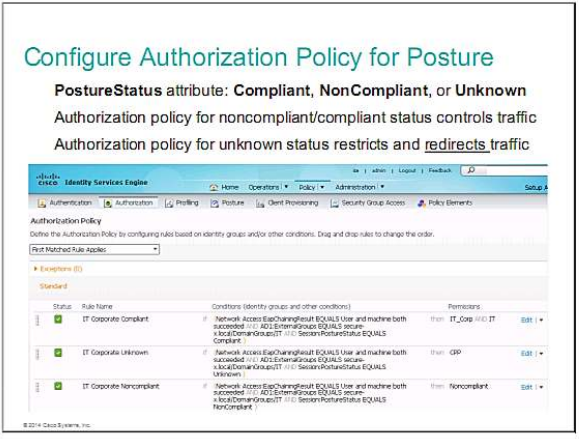
The redirect ACL configured on the switch is referenced by an authorization profile on the ISE. The authorization profile, in this example named CPP, has two functions. It restricts the client traffic using the Unknown_Noncompliant_dACL, and enforces client redirection to the CPP. The ACL name defined on the ISE must match the local ACL defined on the switch.

The authorization profile is referenced by an authorization policy rule. In this scenario, the CPP authorization profile will be referenced by an authorization policy rule with a condition specifying the posture status is unknown.

https://t.me/learningnets

Configure Authorization Policy for Posture

This topic describes how to configure posture-related authorization policy.



The conditions that are defined within the authorization rule should consider the posture status. The status can be ascertained by evaluating the **PostureStatus** attribute, which is available in the **Session** system dictionary. The attribute can assume one of three values: **Compliant**, **NonCompliant**, or **Unknown**.

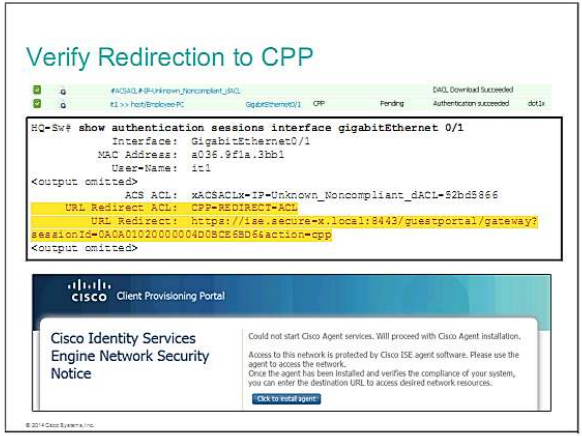
You can configure both simple and compound conditions to evaluate the **Session:PostureStatus** attribute. you could, for example, define a compound condition that combines two expressions using the **OR** operator: **Session:PostureStatus Equal NonCompliant OR Session:PostureStatus Equal Unknown**.

This figure illustrates three authorization policy rules for the IT users accessing the network for corporate resources. The first, named IT Corporate Compliant, matches the posture status Compliant, and applies appropriate permissions. The second, named IT Corporate Unknown, matches the unknown posture status, and assigns the CPP authorization profile, which restricts access and redirects the clients to the client provisioning portal. The third, named IT Corporate Noncompliant, matches the posture status Noncompliant, and restricts the client traffic.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Verify Redirection to CPP

This topic describes how to verify client redirection to CPP.



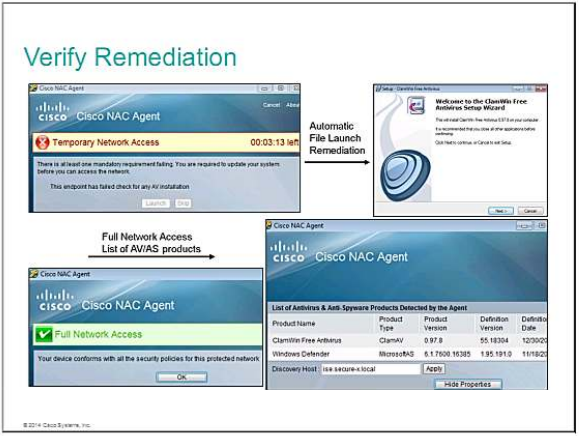
You may verify the traffic redirection to the client provisioning portal in several different ways, including: on the Cisco Identity Services Engine, on the switch, and on the client. The top most figure shows the information displayed in the ISE GUI. The posture status of the endpoint is reported as pending and the CPP authorization profile is applied to the client session. The term pending is used here to describe unknown posture status. The CPP authorization profile restricts and redirects traffic.

You can examine the restriction and redirection parameters on the switch by running the **show authentication session interface** command. The output displays the endpoint authentication and authorization status, along with various authorization parameters that have been applied to the port. The dACL has a name that incorporates the dACL name as it is defined on the ISE. This dACL is used to restrict network access to only the necessary network traffic. The redirect URL includes the client session ID. The client is being directed to the client provisioning resource that is suitable for this client. The redirect URL also specifies the action that should be taken at the ISE portal, in this case action=cpp.

The last figure illustrates the browser redirected to the client provisioning portal. The client can download and install the NAC agent.

Verify Remediation

This topic describes how to verify the remediation.

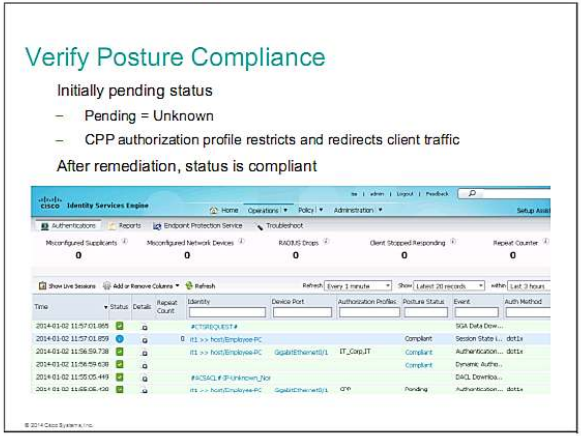


After NAC agent installation, the NAC agent reports posture status to the Cisco Identity Services Engine. The ISE evaluates the information and may instruct the NAC agent to perform remediation. In this example, the File Launch Remediation is used to start the ClamWin installation. The user must complete the installation wizard. When the installation process has been completed and the definition files updated, the NAC agent reports compliance status and lists the discovered AV and AS components.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Verify Posture Compliance

This topic illustrates how to verify the posture service in the Cisco Identity Services Engine GUI.

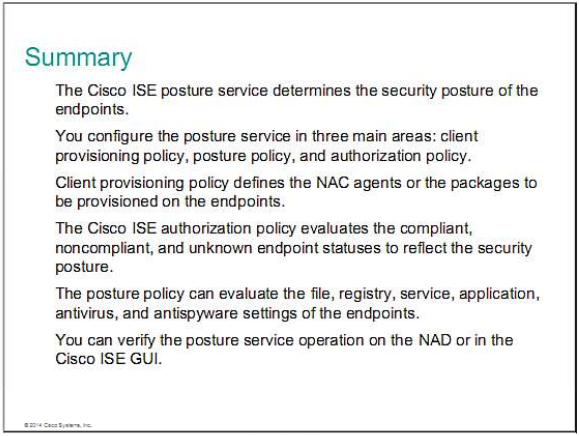


You can monitor the posture status of the endpoints in the live authentications page found under **Operations > Authentications** in the ISE administrative GUI. The "pending" status indicates that the status has not yet been established. When the posture is unknown, the CPP authorization profile is applied to the client to restricts and redirect user traffic. When the remediation is complete, the posture status can be determined. In this example the posture status is compliant.

https://t.me/learningnets

Summary

This topic summarizes the key points that were discussed in this lesson.



https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Lesson 2

Deploying Profiler Service

Overview

To ensure and maintain appropriate access to your enterprise network, the profiler service collects an attribute or a set of attributes of all the endpoints on your network and classifies them according to their profiles.

This lesson provides an overview of the profiler service that is offered as part of the Cisco Identity Services Engine platform and describes how to implement profiling in a Cisco ISE network.

Upon completing this lesson, you will be able to:

- Describe the purpose of the profiler service
- Describe the position of the profiler in overall Cisco ISE processing
- Describe the Cisco ISE probes
- Describe the most common probes
- Describe the profiling operation without the use of probes
- Explain the relevance of CoA for the profiler operation
- Describe the use of profiling policies
- Describe the parent profiling policies
- Describe the child profiling policies
- Describe the profiler configuration procedure
- Enable the profiler service
- Enable CoA for the profiling service
- Configure the probes
- Examine the parent policy
- Examine the parent conditions

https://t.me/learningnets

Configure the profiler conditions

Configure the profiler policy

Adjust the authorization policy for the profiler service

View the profiled endpoint identity groups

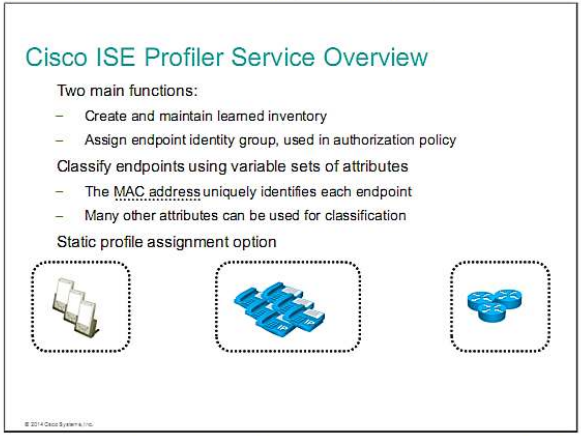
Verify profiling in the ISE authentications page

View profiled endpoints

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Cisco ISE Profiler Service Overview

This topic provides an overview of the Cisco Identity Services Engine profiler service.



The primary goal of the profiler is to classify the endpoint using the most appropriate endpoint profile. The profile specifies the endpoint identity group. The endpoint identity group is an attribute that you can use when defining conditions in the authentication and authorization policies.

Profiling is useful in situations where certain corporate assets must be differentiated from noncorporate assets. It may be used to help regulate network access and further assign network authorization that is based on the policy group of the device.

An endpoint is a network-capable device that connects to your enterprise network. The MAC address is always the unique identifier of an endpoint, but you can further identify an endpoint using a varying set of attributes and the values that are associated to them (called attribute-value pairs). You can attach a varying set of attributes to endpoints based on their capability, the capability and configuration of the NADs, and the methods (probes) that you use to collect these attributes.

You can associate each endpoint on your network to an existing endpoint identity group in the system, or to a new group that you can create and associate to a parent group. By grouping endpoints, and applying endpoint profiling policies to the group, you can determine the mapping of endpoints to the endpoint profiles by checking the corresponding endpoint profiling policies.

Enterprises deploy the profiler service for two main reasons:

To create a learned inventory: The profiler service provides a contextual inventory of all the endpoints that are using your network resources. It discovers the devices that are connected to your network and finds where these devices exist on your network. This can be used to populate the MAB database during the monitor mode phase of a phased deployment.

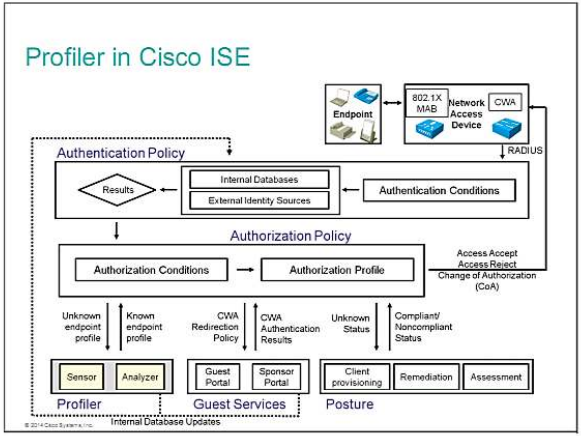
To determine the applicable endpoint identity group: The result of the profiler service is the binding of a device to a device profile. The identity group that is specified by the device profile can be used as a condition in the authorization policy, and can thus affect the network permissions that the endpoint receives.

The administrator can statically assign an endpoint to an endpoint identity group. If this is done, attributes associated with the endpoint continue to be updated, but the attribute values are not evaluated. The static assignment remains until manually removed by an administrator.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Profiler in Cisco ISE

This topic describes the position of the profiler service in overall Cisco Identity Services Engine processing.

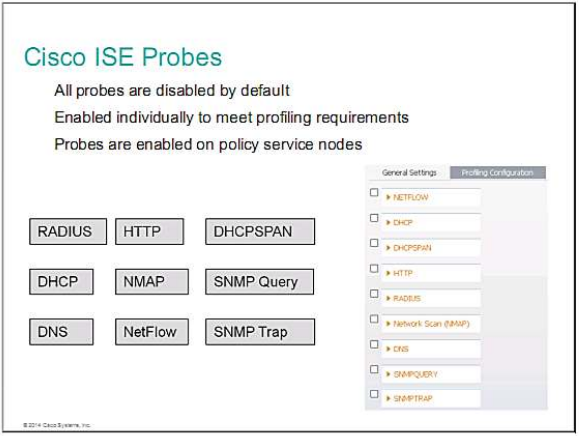


The profiler service represents an additional block in the Cisco ISE information flow. You can think of it as a function that provides the endpoint identity group attribute to the authorization policy. The authorization will have different privileges for devices with undetermined and determined endpoint identity groups.

https://t.me/learningnets

Cisco ISE Probes

This topic describes the Cisco Identity Services Engine probes.



A probe is a method that is used to collect an attribute or a set of attributes from an endpoint on your network. The probe allows you to create or update endpoints with their matched profile in the database.

The Cisco ISE GUI contains the configuration options that allow you to enable or disable the probes on each node. The probes are activated on policy service nodes. Cisco ISE supports various probes, and choosing the appropriate ones for a specific environment is not very straightforward.

The ISE allows you enable these probes:

The RADIUS probe can be used to evaluate the RADIUS attributes received from the NAD. Of primary relevance is the building of the MAC to IP address bindings. In RADIUS access-requests, the Calling-Station-ID field specifies the endpoint's MAC address and the Framed-IP-Address field specifies the endpoint's IP address. The RADIUS probe also enables access to the IOS Device Sensor data on devices that support the feature.

The SNMP Trap probe is used to receive information about MAC notification, linkup, linkdown, and other events carried in SNMP informs. The SNMP Trap probe receives information from the specific NADs when ports come up or go down and endpoints disconnect or connect to your network. The SNMPTrap probe should always be paired with the SNMPQuery probe. It's primary purpose is to trigger appropriately timed SNMP queries .

The SNMP Query probe performs system queries at regular intervals, pulling system and CDP data from the NAD. It also performs interface queries when triggered by the SNMPTrap probe. The interface query pulls interface data including VLAN, session and CDP data.

The DHCP probe allows the Cisco ISE profiling service to collect DHCP request attributes from the DHCP client. DHCP requests carry a user-agent field that helps specify the OS of the device. Information such as the requested DHCP options and the DHCP hostname can be useful in classifying a device.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

The DNS probe allows the profiler to lookup an endpoint, and get the FQDN of that endpoint. This reverse DNS lookup is performed by PSN against its locally configured name server to retrieve the endpoint FQDN The lookup is triggered upon learning the IP address of endpoint.

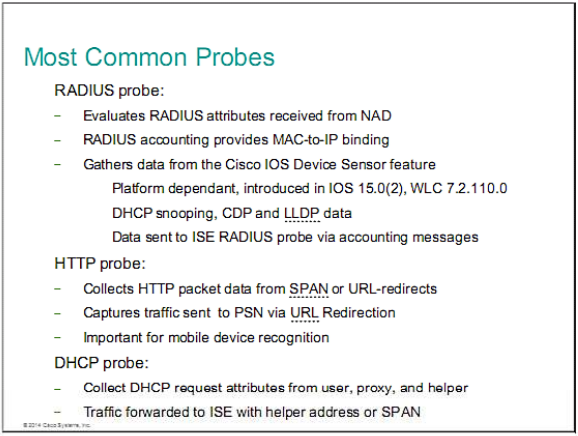
The HTTP Probe enables the profiler to capture the User-Agent field presented by a web browser to the web server. The user-agent field typically identifies the browser, software vendor, operating system and version information to the web server. The HTTP probe requires the IP to MAC address binding to be provided by a different probe.

The NetFlow probe allows you to collect and analyze NetFlow data. NetFlow provides records of connections between endpoints including IP addresses, protocols and ports. An example use case for this data within ISE is to recognize which network applications and services are active on a device. The NetFlow probe consumes a relatively large amount of resources on the ISE node. It should only be enabled in special use cases. The NetFlow probe requires anther probe to provide the IP to MAC address mapping.

NMAP is integrated with the Cisco ISE profiler to augment its profiling capability for better endpoint classification, particularly mobile devices. You can either perform a manual subnet scan on a specific subnet by using the Network Scan probe, or you can associate a network scan action to a profiler policy to perform a dynamic scan on an endpoint. The NMAP probe requires the IP to MAC address binding to be provided by a different probe.

Commonly Deployed Probes

This topic describes the most common probes.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

RADIUS Probe

With the RADIUS request and response messages received from the RADIUS servers, the profiler can collect RADIUS attributes, which can be used for profiling endpoints. You can create a profiling condition of RADIUS type, where you can use the Framed-IP-Address attribute to obtain the endpoint IP address. Similarly, the Calling-Station-ID attribute can, depending on the NAD configuration, contain the endpoint MAC address. The MAC address can be used to obtain OUI for NIC vendor classification.

You must enable RADIUS authentication and accounting on the network access device. You can also include options to send various attributes via RADIUS. The three options recommended for the RADIUS probe are:

- The **radius-server attribute 6 on-for-login-auth** command is used to sends the Service-Type attribute in the authentication packets.
- The **radius-server attribute 8 include-in-access-req** command is used to send the IP address of a user to the PSN in the access request. This gives the PSN a hint of the user IP address in advance of user authentication. Based on this information the PSN builds a map of user names and addresses. Using the mapping information, the PSN begins preparing user login information to have available upon successful user authentication.
- The **radius-server attribute 25** command is used to include the class attribute in access-request. The class attribute is not sent by default.

The Device Sensor feature, available on Cisco IOS devices, is used to gather raw endpoint data from network devices using protocols such as Cisco Discovery Protocol, LLDP, and DHCP. The Cisco Identity Services Engine analyzer acts as the external client of the device sensor, and will use RADIUS accounting to receive the data about the endpoint. The device sensor sends to the Cisco ISE client notifications and accounting messages containing profiling data along with the session events, and other session-related data, such as MAC address and ingress port. By default, for each supported peer protocol, client notifications and accounting events are only generated where an incoming packet includes a TLV that has not previously been received in the context of a given session. You can enable client notifications and accounting events for all TLV changes, where either a new TLV has been received or a previously received TLV has been received with a different value using CLI commands.

Device Sensor is enabled by default. The following TLVs are included by default:

- Cisco Discovery Protocol filter--secondport-status-type and powernet-event-type (type 28 and 29)
- LLDP filter--organizationally-specific (type 127)
- DHCP filter--message-type (type 53)

HTTP Probe

The HTTP Probe enables the profiler to capture the information provided by the web browser in the HTTP User-Agent field, as well as other HTTP attributes from the request messages. Cisco ISE provides many default profiles, which are built into the system to identify endpoints based on the User-Agent attribute. The HTTP data is important for, among other things, mobile device recognition. Identifying different mobile and portable IP enabled devices is made more reliable by having the Cisco ISE node capture data during a guest login or client provisioning download. This allows the profiler to collect the User-Agent attribute, as well as other HTTP attributes, from the request messages and then identify devices such as Apple devices. The Cisco ISE probe listens to communication from the web browsers on both port 80, as well as port 8080.

https://t.me/learningnets

DHCP Probe

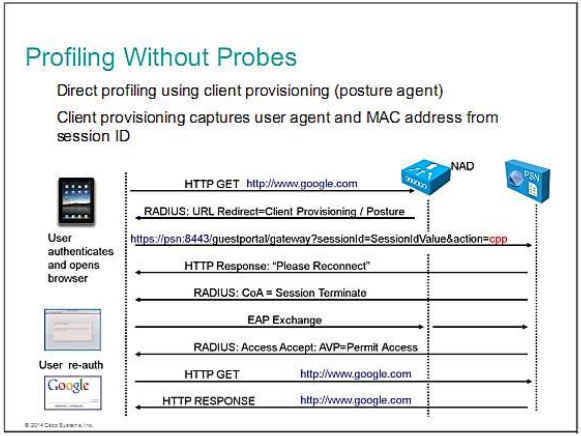
The DHCP probe allows the Cisco ISE profiling service to collect DHCP request attributes from DHCP user, proxy, and helper. The probe evaluates DHCP requests of INIT-REBOOT, and SELECTING message types. Other DHCP message types, such as RENEWING, and REBINDING, are also processed but they are not used for profiling endpoints. Any attribute parsed out of DHCP packets is mapped to endpoint attributes.

When you configure a gateway device to interoperate with the DHCP probe, you will use the **ip helper-address** command to send the DHCP requests to the Policy Service node, in addition to the real DHCP server, proxy, or helper address.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Profiling Without Probes

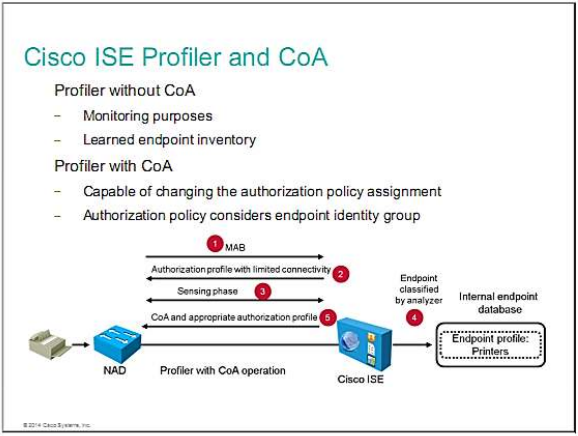
This topic describes the profiling service without the use of probes.



The profiler service attempts to profile the endpoints even when probes are not enabled. This figure illustrates a successful profiling process, in which the policy service obtains the endpoint attributes from the NAC agent that is provisioned on the endpoint by the client provisioning feature.

Cisco ISE Profiler and CoA

This topic describes how CoA affects the profiler operation.



CoA is not absolutely necessary for the Cisco Identity Services Engine profiler service operation. If you have some NADs in your network that do not support CoA, you may still deploy the profiler service for endpoint monitoring. In this case, the profiler service can be used to establish a learned inventory.

When CoA is supported on the NADs, you can use the profiler service to push tailored authorization policies to the endpoints. When the endpoint authenticates, it receives a restrictive authorization policy that enables the sensing traffic to be exchanged. Once the endpoint profile has been determined, the Cisco ISE sends a CoA to the NAD and instructs the NAD to apply an adjusted policy.

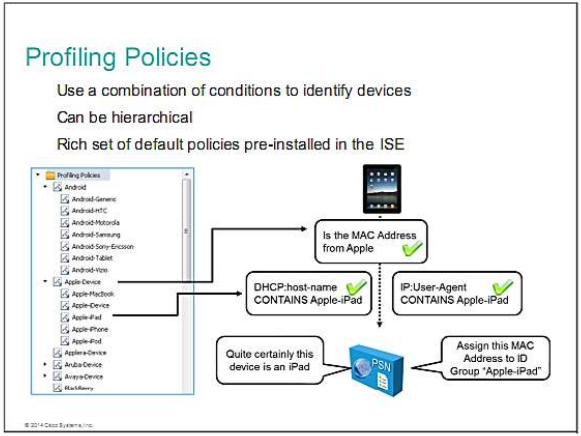
The profiler service implements the CoA when one of the following cases leads to a condition where a different policy profile becomes appropriate:

- Static assignment of an endpoint
- Exception action is configured
- Endpoint is profiled for the first time or endpoint is deleted
- Endpoint identity group has changed

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Profiling Policies

This topic describes the profiling policies.

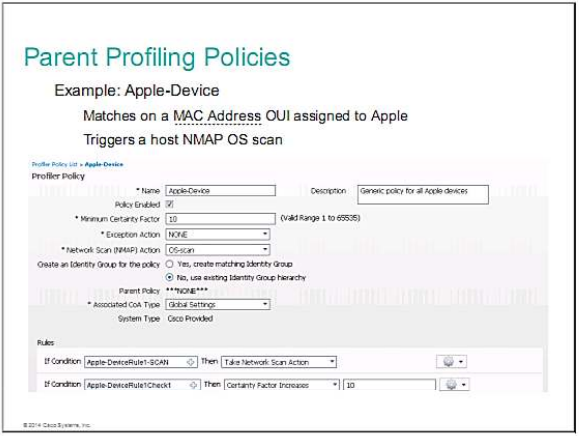


The profiler service evaluates endpoint attributes and assigns the endpoint to endpoint identity groups. The logic of this evaluation and assignment is defined in the profiling policies. The profiling policies use a combination of conditions to identify devices. Cisco Identity Services Engine comes with a large number of preconfigured profiling policies. You can extend the default by configuring your custom policies.

This figure illustrates the hierarchical profiling policy for Apple devices and Apple iPads. When profiling policies are in a hierarchy, the child policies are not evaluated unless the parent policy is matched. In this case, the **Apple-Device** policy is the parent policy. It matches off a simple condition, the endpoint's MAC address contains an Apple OIU. This match allows the more refined child policies to be evaluated. Data from the endpoint hostname and its browser's User-Agent field indicate that the endpoint is an iPad.

Parent Profiling Policies

This topic describes the parent profiling policies.



This figure illustrates the parent policy **Apple-Device**. The policy specifies two rules. The condition of the first rule is that the MAC address OUI matches Apple. The OUI is the first 24 bits of the MAC address. It is sometimes called a vendor code, but the more appropriate term is an MA-L. NIC manufactures must register with the IEEE to obtain MA-Ls to use in the MAC addresses on their NICs. Cisco Identity Services Engine maintains an OUI table to determine the NIC vendor. The first rule states that if the OUI matches Apple, then a network scan action should be taken. Note that the Network Scan (NMAP) Action field specifies an OS-scan. The results of this NMAP OS scan will be available to the child policies. The condition of the second rule is also that the MAC address OUI matches Apple. This can be confirmed by expanding the condition or by examining the condition definition under **Policy > Policy Elements > Conditions, Profiling**. The second rule states that if the OUI matches Apple, then increase the certainty factor of the profile by 10. Note that the Minimum Certainty Factor is set to 10. Matching this rule is enough to match the policy.

The profiling policy contains these settings:

Minimum Certainty Factor: Each policy has a minimum certainty factor (an integer value) associated to it. Rules in the policy, if their conditions are met, can increment the certainty factor for an endpoint towards the profile policy match.

Exception Action: This option allows you to trigger an exception action (a single configurable action) that is taken when an endpoint matches the profiling policy. The exception action is triggered when the endpoint profiling policy is matched, and at least one rule specifying an exception action matches. The exception actions are conveyed to the NAD via CoA. Options for exception actions include port bounce and reauth.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Network Scan Action: An endpoint scan action scans a single endpoint as compared to resource intensive network scans, which you could perform manually when configuring the NMAP probes. It improves the overall classification of endpoints, and redefines an endpoint profile for an endpoint. You can associate a single network scan action to an endpoint profiling policy. Cisco ISE predefines three scanning types for a network scan actions. Once an endpoint is appropriately profiled, the configured network scan action cannot be used against that endpoint. For example, scanning an Apple-Device allows you to classify the scanned endpoint to an Apple device. Once an OS-scan determines the operating system that an endpoint is running, it is matched to an appropriate profile for an Apple device. The following are the scanning types that are predefined in any network scan action for an endpoint scan:

- **OS-scan**. This type scans an operating system and OS version that an endpoint is running. It is a resource intensive scan.
- **SNMPPortsAndOS-scan**. This type scans an operating system and OS version that an endpoint is running, as well as triggers an SNMP Query when SNMP ports (161 and 162) are open. It can be used for endpoints that are identified and matched initially with an Unknown profile for better classification.
- **CommonPortsAndOS-scan**. This type scans an operating system and OS version that an endpoint is running, as well as common ports (TCP and UDP), but not SNMP ports.

Create Matching Identity Group: This option allows you to create a matching identity group as a child of the profiled identity group, when an endpoint profile matches an existing profile. For example, the **Apple-Device** endpoint identity group is created on the **Endpoints Identity Groups** page when endpoints that are discovered on your network match the **Apple-Device** profile.

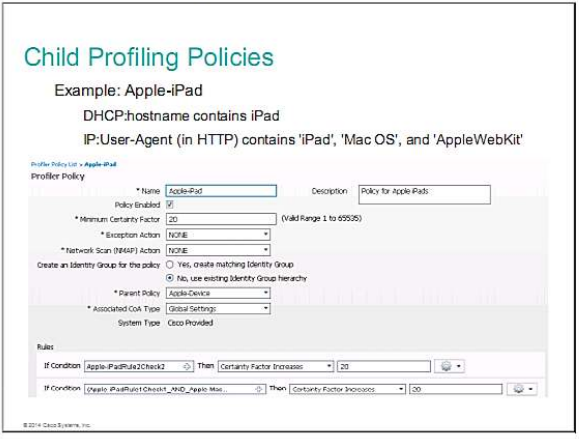
Use Hierarchy: When checked, this option allows you to make use of endpoint profiling policy hierarchy to assign endpoints to one of the matching parent endpoint identity groups, and to the endpoint identity groups that are associated to the parent identity group. For example, endpoints that match an existing profile are grouped under the appropriate parent endpoint identity group. Endpoints that do not match any existing profiles are grouped under Unknown, and endpoints that match an existing profile are grouped under Profiled endpoint identity groups. If endpoints match the **Cisco-IP-Phone** profile, then they are grouped under **Cisco-IP-Phone**, and endpoints that match the **Workstation** profile are grouped under **Workstation** endpoint identity groups. The **Cisco-IP-Phone** and **Workstation** identity groups are associated with the profiled endpoint identity group in the system.

Parent Policy: This option allows you to choose an endpoint profiling policy from which this policy can inherit conditions.

https://t.me/learningnets

Child Profiling Policies

This topic describes the child profiling policies.



This figure illustrates the child policy **Apple-iPad**. Note the Parent Policy field specifies Apple-Device. This child policy will not be evaluated unless the parent policy first matches. This policy specifies two rules, each capable of increasing the certainty factor by 20. Note that the minimum certainty factor is 20, so matching the conditions of either rule is sufficient for the profile assignment.

The first rule examines the DHCP:host-name attribute. The condition matches if the attribute contains iPad. The second rule examines the user-agent string. The condition matches if the user-agent string contains each of the following sub-strings: iPad, Mac OS, AppleWebKit.

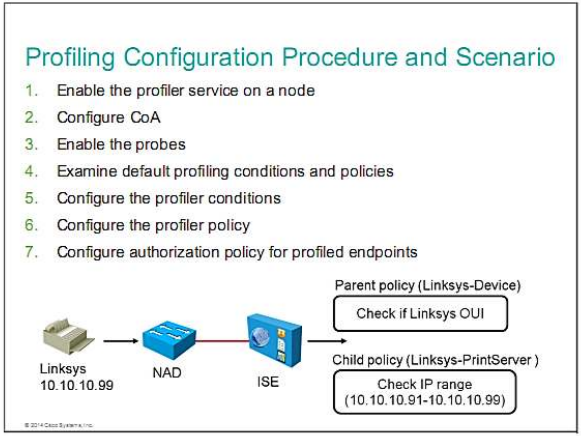
To examine the details of conditions specified in the rules, you can find the condition, by name, under **Policy > Policy Elements > Conditions, Profiler**. You can also perform a read only expansion of the condition details by hovering the mouse pointer over the condition field and clicking the **details** icon that appears, as shown in the figure below.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Profiling Configuration Procedure and Scenario

This topic describes the profiling configuration procedure and shows an example scenario.

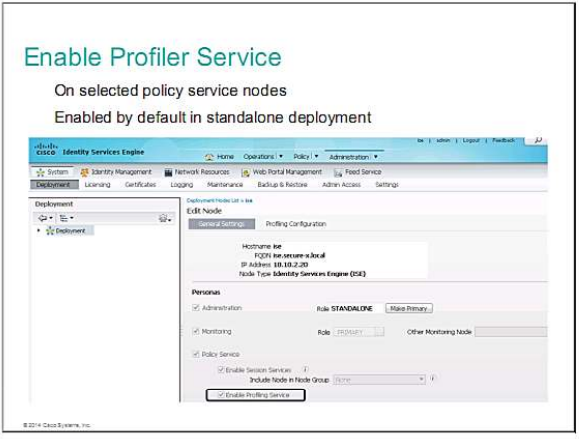


Follow these steps to configure the profiler service on the Cisco Identity Services Engine:

1. Enable the profiler service on a Cisco ISE node
2. Configure CoA
3. Configure the probes
4. Examine default profiling conditions and policies
5. Optionally configure custom profiler conditions
6. Optionally configure custom profiler policies
7. Configure authorization policy for profiled endpoints

Enable Profiler Service

This topic describes how to enable the profiler service.



You can deploy Cisco Identity Services Engine either in a standalone environment (on a single node), or in a distributed environment (on multiple nodes). The profiling service is associated with the Policy Service persona. Determining which policy service nodes should run policy services in a distributed deployment is an advanced design topic. To manage the Cisco ISE deployment, choose **Administration > System > Deployment**, choose the appropriate node from the **Deployment Nodes** page, and click **Edit**.

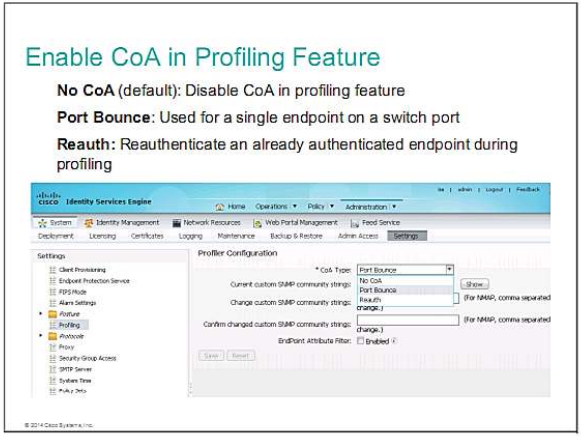
The configuration page contains the **General** settings tab to configure the deployment and the **Profiling Configuration** tab to configure the probes on each node. If the policy service persona is disabled, or if it is enabled but the **Enable Profiling Service** option is not selected, then the Cisco ISE administrator user interface does not display the **Profiling Configuration** tab. If the policy service persona is disabled on any Cisco ISE node, Cisco ISE displays only the **General** settings tab and does not display the **Profiling Configuration** tab, which prevents you from configuring the probes on the node.

In a standalone ISE deployment, the profiler service is by default enabled on the standalone node. As shown in the figure, it cannot be disabled.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Enable CoA in Profiling Feature

This topic describes how to enable CoA for the profiling service.



The Cisco Identity Services Engine allows a global configuration to issue a CoA for endpoints that are already authenticated to the network. This global configuration of CoA gives the profiler service more control over endpoints.

You can use the global configuration option to disable CoA by using the default No CoA option. Alternatively, you can enable CoA by using the Port Bounce and Reauthentication options. If you have configured Port Bounce CoA in Cisco ISE, the profiler service may still issue other CoAs on a port.

The CoA selections are as follows:

No CoA: Use this default option to disable the use of CoA in the profiling service.

Port Bounce: Use this option if there is only one session on a switch port. If the port has multiple endpoints that are attached, use the Reauth option.

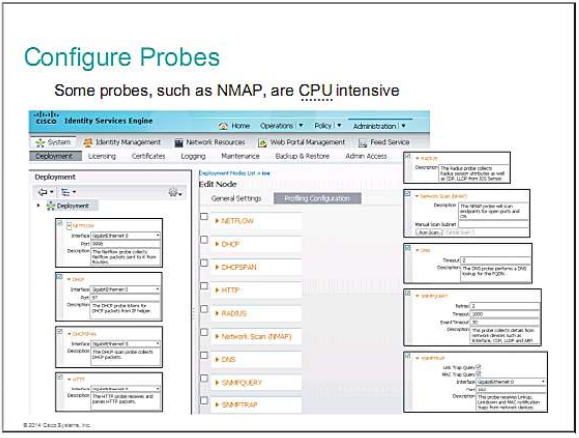
Reauth: Use this option to enforce reauthentication of each authenticated endpoint when profiled.

If you have multiple active sessions on a single port, the profiler service issues a CoA with the Reauth option even though you have configured CoA with the Port Bounce option. This function potentially avoids disconnecting other sessions, which might occur with the Port Bounce option.

https://t.me/learningnets

Configure Probes

This topic describes how to configure probes.



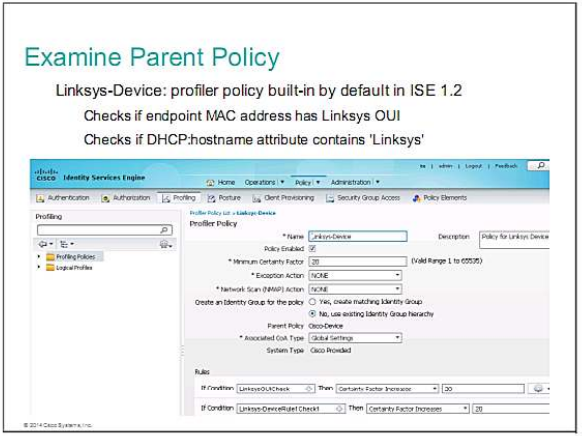
A probe is a mechanism that is used to collect attributes associated with endpoints on your network. The probe results allow you to create or update endpoints with their matched profile in the database.

The **Profiling Configuration** tab on the **Edit Node** page contains the configuration options that allow you to enable or disable the probes on each policy service node. This allows a node-specific configuration of probes in a distributed deployment. The **Deployment** menu window displays the registered nodes in your deployment. You can select a node from the **Deployment** menu window.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Examine Parent Policy

This topic describes the configuration of profiler conditions.



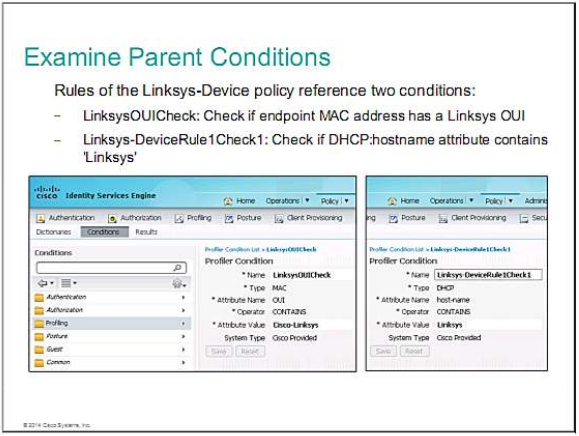
Cisco Identity Services Engine 1.2 has a preconfigured default profiling policy, named Linksys-Device. This profiler policy will be used as a parent policy in this configuration scenario. The policy has two rules. Each rule is capable of increasing the certainty factor by 20. The policy has a minimum certainty factor of 20, so matching the conditions of either rule is sufficient to meet this profiler policy. Each rule has a single condition. The conditions are described as follows:

If endpoint MAC address has Linksys OUI (for example via the RADIUS probe).

If the DHCP:hostname attribute contains the string 'Linksys'

Examine Parent Conditions

This topic describes how to examine the parent conditions.

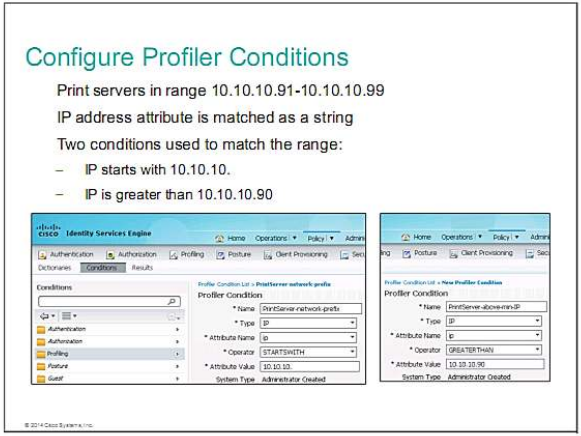


This figure illustrates the definition of the two profiling conditions that are referenced by the Linksys-Device profiling policy. Profiling conditions are used in the same way that authentication and authorization conditions are used in authentication and authorization policies. You can use the built-in conditions or define custom conditions. Simple conditions define a single match statement. Compound conditions specify a set of condition statements.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Configure Profiler Conditions

This topic describes the configuration of profiler conditions.



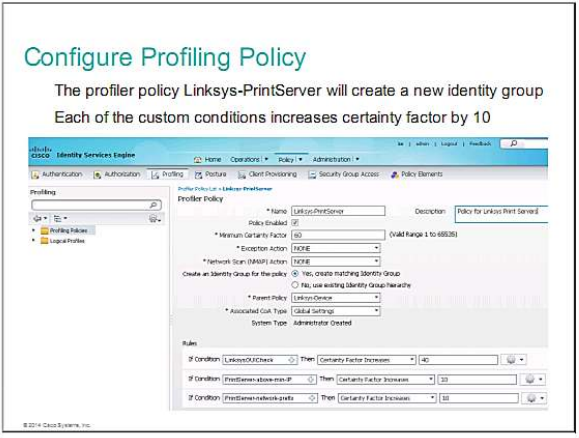
In this scenario, the print servers are manufactured by Linksys and have been given static IP addresses in the range 10.10.10.91-10.10.10.99. A profiling policy will be defined that is a child of the LinksysDevice profiler policy and will further differentiate based on IP address. The figure shows the configuration of two profiler conditions. Profiling conditions match the IP addresses as strings, not as numbers. Therefore the two conditions required to match this address range are:

The endpoint IP address must start with "10.10.10."

The endpoint IP address must be greater than "10.10.10.90"

Configure Profiling Policy

This topic describes how to configure the profiler policy.

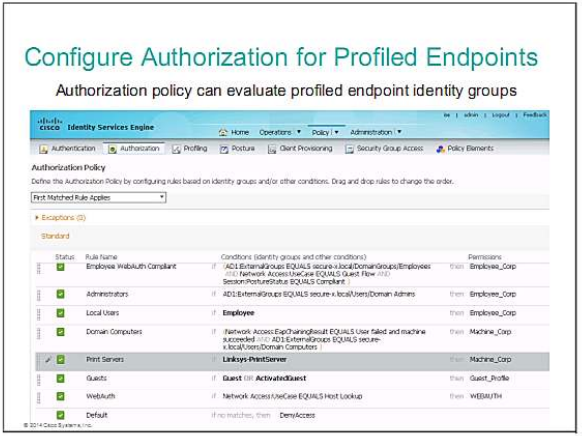


In this scenario you add a new profiling policy, named Linksys-PrintServer. It is defined as a child policy to the Linksys-Device profiler policy. It contains three conditions. One condition checks the Linksys OUI and raises teh certainty factor by 40. The two remaining conditions are used to match the IP range and each raises the certainty factor by 20. All three conditions must be met to profile the endpoint, because the minimum required certainty factor is 60.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Configure Authorization for Profiled Endpoints

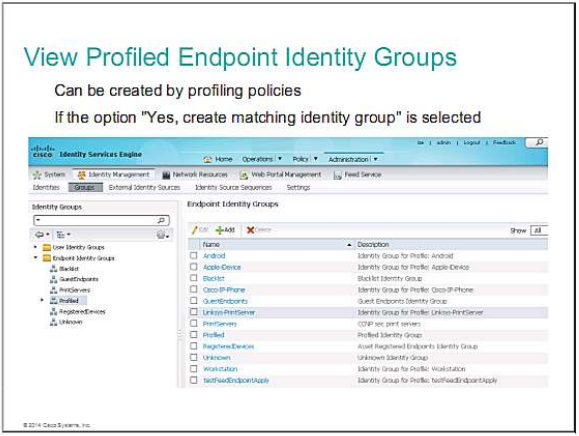
This topic describes how to adjust the authorization policy to the profiler service.



A common application of the profiler service is to provide differentiated access based on the endpoint profile. To accomplish this, you must configure the authorization policy to reflect the device profile assignment. This figure illustrates the authorization rule named **Print Servers**. To define the conditions within this authorization rule, edit the identity group details field of the authorization rule, navigate through **Identity Groups > Endpoint Identity Groups > Profiled**, and then choose the endpoint profile that has been created by the profiling policy.

View Profiled Endpoint Identity Groups

This topic describes how to view the profiled endpoint identity groups.

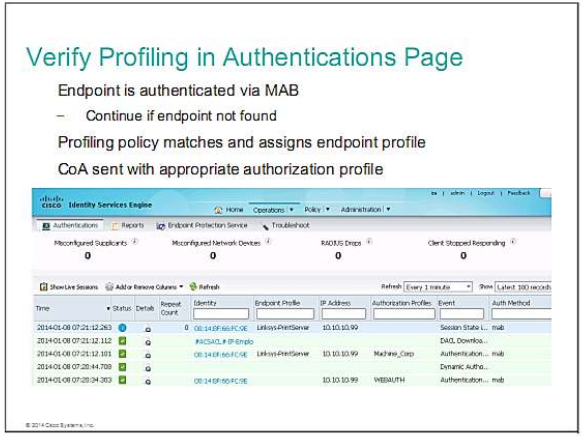


If you select the option "**Yes, create matching identity group**" in the profiling policy configuration, a profiled endpoint identity group will be automatically created in the Cisco Identity Services Engine. This group is added even before any endpoints are profiled using the given policy. You can view the profiled endpoint identity group in the **Administration > Identity Management > Groups > Endpoint Identity Groups > Profiled**. The figure shows that the group Linksys-PrintServer has been created. Selecting a particular endpoint identity group link will display a table of all endpoints that are currently assigned to that group.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Verify Profiling in Authentications Page

This topic describes how to verify profiling in the Cisco Identity Services Engine authentications page.

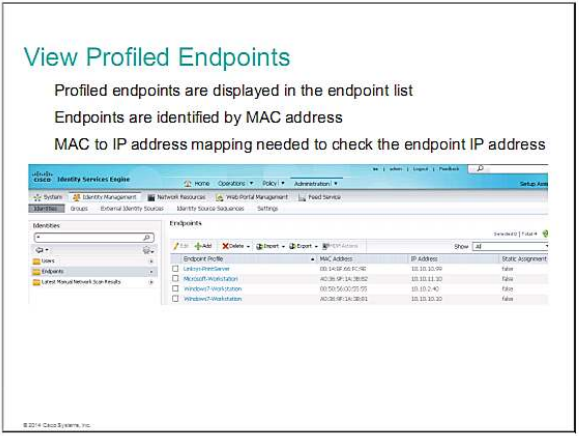


The Live Authentications page, at **Operations > Authentications**, displays the results of the authentication, profiling, and authorization processes. The figure depicts an endpoint that first had no endpoint profile assignment and was assigned the authorization profile named WEBAUTH. After dynamic profiling, it is assigned the Linksys-PrintServer endpoint profile and the Machine_Corp authorization profile.

https://t.me/learningnets

View Profiled Endpoints

This topic describes how to view profiled endpoints.



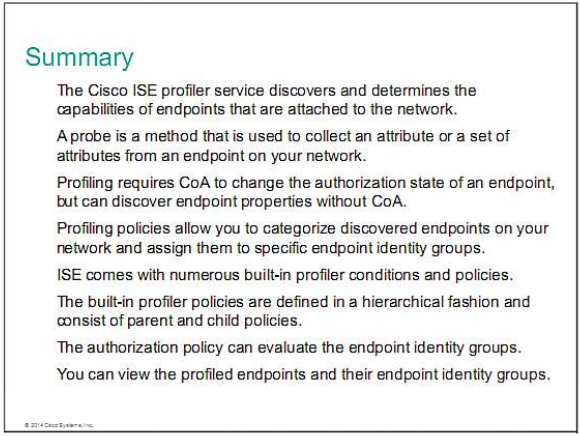
To view the profiled endpoints, choose **Administration > Identity Management > Identities > Endpoints**. This page provides information about endpoints that have been discovered by profiling or that have been statically assigned an endpoint identity group. The endpoints are identified by their MAC addresses. In this scenario, the MAC to IP address mapping was needed to check the endpoint IP address and properly profile the endpoint. Both attributes have been obtained using the RADIUS probe.

In a production deployment, the number of endpoints displayed in this table can be cumbersome. This table, like most tables in Cisco Identity Services Engine, does offer the option to use the quick filter or advanced filter to limit which entries are displayed in the table. Also, you have the option to navigate to **Administration > Identity Management > Groups** and display tables for individual endpoint identity groups.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Summary

This topic summarizes the key points that were discussed in this lesson.



https://t.me/learningnets

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Lesson 3

Implementing BYOD

Overview

The Cisco Identity Services Engine, combined with the Cisco Wireless LAN Controller, Cisco APs, and wired switches, provides comprehensive BYOD capabilities and solutions in one system. This lesson provides students with the knowledge and skills needed to deploy a BYOD solution to onboard company-owned or personally owned wireless devices.

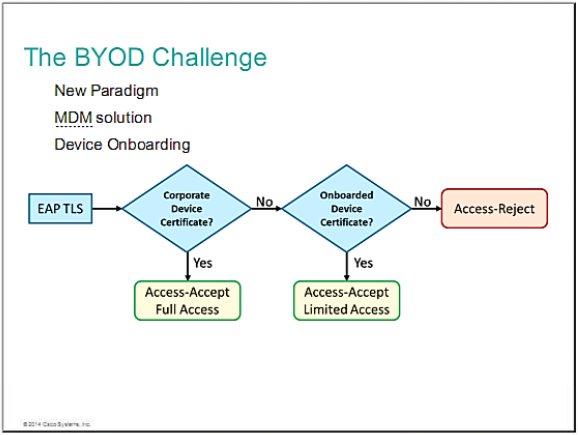
Upon completing this lesson, you will be able to:

- Describe the BYOD challenge
- Describe device onboarding
- Describe the single and dual SSID designs
- Describe the dual SSID flow
- Describe the authorization policy in the dual SSID flow
- Describe how the endpoint connects to the network
- Describe guest access in BYOD
- Describe employee access before endpoint provisioning
- Describe native supplicant provisioning for employees
- Describe the Wi-Fi profile
- Describe the client provisioning policy for employees
- Describe employee access after endpoint provisioning
- Describe the verification of BYOD device registration
- Describe the verification of BYOD client provisioning
- Describe how to connect to the SSID in BYOD

https://t.me/learningnets

The BYOD Challenge

This topic describes the challenges of the BYOD phenomenon.



Apple released the first iPhone in 2007 and the first iPad in 2010. At that time, the common opinion amongst IT professionals was that these types of devices would never be allowed to directly access corporate networks. In fact, some companies originally implemented the Cisco Identity Services Engine to defend against this threat. With ISE profiling, they could recognize iDevices and reject access for them. But the opinions have quickly shifted, and the acceptance of BYOD is becoming common. One reason is that employees are demanding the use of the devices which make them the most productive. Restrictions and control are still desired, though. Much about the security stance that is guaranteed with a corporate owned and managed asset cannot be taken for granted with a BYOD device. Traditional systems which provided authorization based solely on the user ID no longer suffice. Authorization must consider both user authentication and device authentication.

MDM solutions represent a technology that rose in the same time frame as BYOD. MDM solutions seek to ensure security standards are implemented on mobile devices. Options for security standards can include encryption, PIN protected screen locks and remote wipe capabilities. While MDM and BYOD are related, they can exist together or independently. MDM platforms can work with mobile devices that are provided by the company or they can work with BYOD devices. ISE provides integration with several of the industry leading MDM solutions.

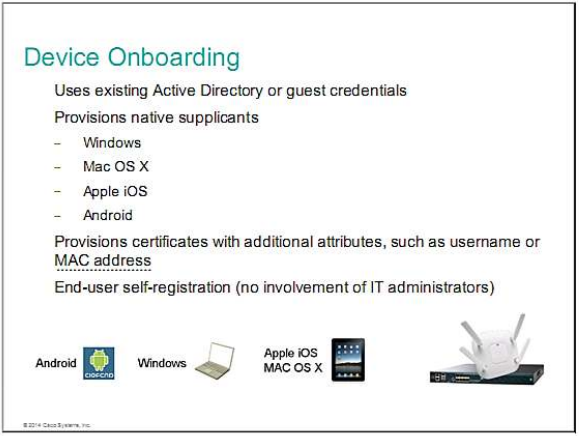
MDM solutions, often licensed on a per-device basis, can be expensive. Many companies would simply like to distinguish between devices that are owned by employees versus devices that are brought in with a visitor. This is where device onboarding fits in. The idea of device onboarding is that employees can register their own devices. The onboarding process requires the employee to authenticate and includes the provisioning of a device certificate for the onboarded device. ISE provides a solution for employee self-service onboarding and registration.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

ISE authorization policy can integrate with either MDM solutions and with simpler BYOD onboarding. The figure shows a flowchart of a simple policy that considers the device. EAP-TLS requires a client side certificate on the device. If the certificate identifies a corporate owned and managed device, then a more privileged access is granted. If the certificate identifies an onboarded device, then a less privileged access is granted. If neither of these are the case, access is rejected. Certificates could also be used to identify devices that are under the management of an MDM solution.

Device Onboarding

This topic describes the device onboarding used in the BYOD solution.



Cisco provides a comprehensive BYOD solution architecture that combines elements across the network for a unified approach to secure device access, visibility, and policy control. To solve the many challenges that exist, a BYOD implementation is not a single product, but should be integrated into an intelligent network.

Wired switches are supported in the BYOD solution, but wireless access is more common.

Onboarding for new devices involves certificate enrollment and profile provisioning, and should be easy for end users with minimal intervention by IT, especially for employee-owned devices. Device choice does not mean that you have to give up security. IT needs to establish the minimum security baseline that any device must meet to access the corporate network. Proper device authentication is critical to ensure that the onboarding of new devices and the access of other devices is secure and protects the entire network infrastructure, but authentication should also be as simple as possible for both the IT personnel and the user.

The Cisco Identity Services Engine offers a suite of security features:

- Supplicant provisioning on all major platforms using profiling
- In-band and out-of-band asset registration portal
- Self-service user-based registration
- Flexible dot1x profiles
- Blacklisting and reinstating of devices

As networks started implementing wireless in their organizations, a unique wireless network name, which is also known as an SSID, was needed, along with a username and password. Digital certificates and two-factor authentication provide a more secure method to access the network. The end-user typically must download client software to request a certificate or provide a secure token for access.

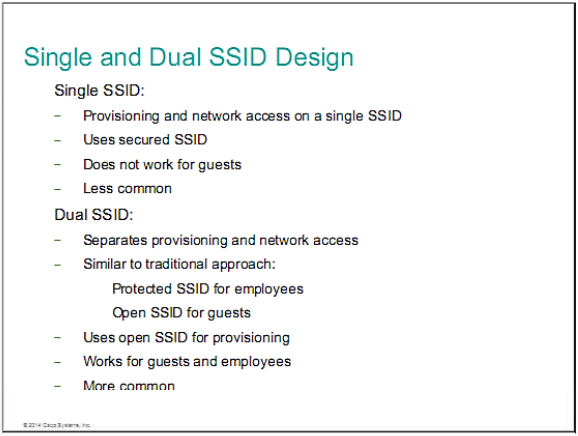
© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Deploying digital certificates on non-PC-based devices requires a different process because many of these devices do not natively support all the features and functionality that are needed to create or download and install digital client certificates.

https://t.me/learningnets

Single and Dual SSID Design

This topic describes the two BYOD designs.



When designing WLAN networks, these three aspects should be taken into consideration:

The role of the WLAN

The authentication mechanism for the WLAN

The number of WLANs present in a network

This design guideline logically separates the WLAN into two distinct logical functions—provisioning and network access. These two functions can be provided by two different WLANs, which is known as dual SSID, or WLANs combined into one, which is known as single SSID. The following examples cover both single and dual SSID deployment models.

When deciding whether to implement a single or dual SSID configuration, consider the following:

Some organizations prefer to have a dedicated SSID for onboarding of devices. This keeps the traffic segregated and enhances security on the network.

Other organizations see dual SSID as an extra management burden because they will have to manage two SSIDs.

The single SSID solution does not work for guests and is therefore not common.

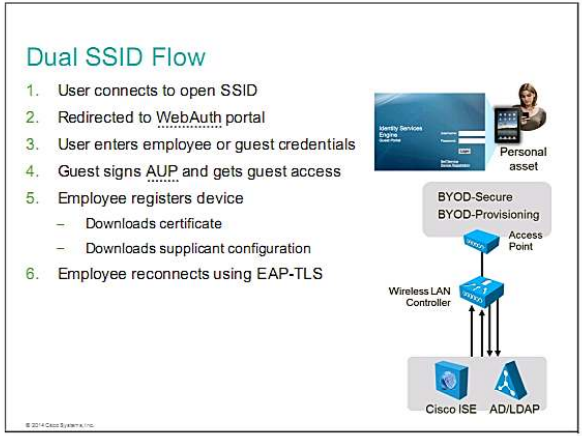
The dual SSID approach works both for guests and employees, and is the preferred method.

The unique requirements and preferences of an organization will dictate which model to deploy. The Cisco Identity Services Engine and Cisco Wireless LAN Controller configurations may easily be changed to support either option.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Dual SSID Flow

This topic describes the BYOD flow in the dual SSID design.



In this design, there are two SSIDs. One provides enrollment and provisioning, and the other provides secure network access. After connecting to the BYOD_Provisioning SSID and completing the enrollment and provisioning steps, the user connects to the BYOD_Secure SSID, which provides the network access.

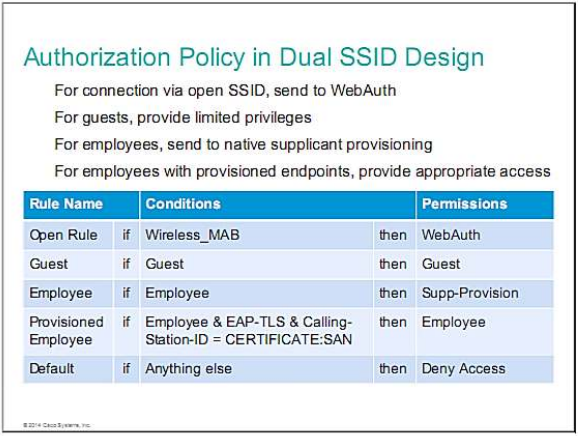
When implementing dual SSID, the provisioning SSID can be either open or password-protected. When the provisioning SSID is open, any user can connect to the SSID; however, if it is password-protected, then only users that have Active Directory group membership are allowed to connect to the SSID. After the user is provisioned, it is assumed that the user will switch to the second SSID for regular network access. To prevent the user from staying connected to the provisioning SSID, an access list must be created that provides access to only the Cisco Identity Services Engine, DHCP, and DNS.

In this example, there are two SSIDs, one that is open for guests and their devices, and one used for employee authentication:

1. A user associates to the guest provisioning SSID.
2. The user opens a browser and is redirected to the Cisco ISE Central WebAuth portal.
3. The user enters an employee username and password in the guest portal.
4. The Cisco ISE authenticates the user, and based on the fact that the user is an employee and not a guest, the user is directed to the Employee Device Registration guest page.
5. The MAC address of the user is prepopulated in the Employee Device Registration guest page for **DeviceID** and the user enters a description and accepts an AUP (if required).
6. The user chooses **Accept** and begins downloading and installing the supplicant.
7. The user device supplicant is provisioned and any certificates are provisioned.
8. The user can then manually associate to the hidden SSID and authenticate via EAP-TLS.

Authorization Policy in Dual SSID Design

This topic describes the authorization policy rules in the dual SSID design.



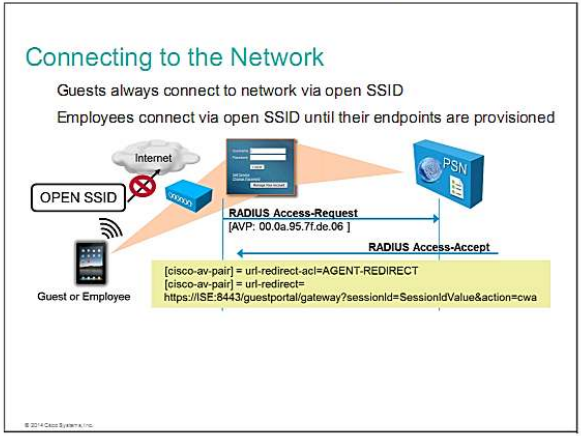
The figure summarizes the key rules in the Cisco Identity Services Engine authorization policy. Users who connect via the open SSID are sent to WebAuth. The Wireless_MAB rule is configured to "Continue" if the user is not found. Once a user is authenticated as a guest, the system provides limited privileges. When employees connect to the network via the open SSID, they are sent to the native supplicant provisioning. The employees who connect using provisioned endpoints are granted appropriate network access.

The Cisco ISE enables self-provisioning, which allows employees to register their personal wireless devices. The Cisco ISE provisions the device with its native supplicant during device registration. The BYOD system leads the employee through a series of provisioning steps the first time the personal device is brought to work and registered. The user can use existing Active Directory or guest credentials. The BYOD authentication type will then determine the type of secure policy that the user will receive. Certificates can be provisioned while registering the device.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Connecting to the Network

This topic describes the process of connecting to the network using the single SSID.

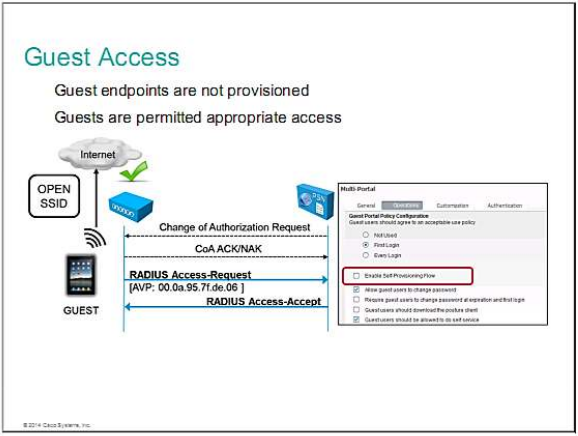


The open SSID allows guests and employees to connect to the network. Guests always connect to the network via open SSID. The employees connect via open SSID in the initial phase, when their endpoints have not yet been provisioned.

https://t.me/learningnets

Guest Access

This topic describes the guest access process.

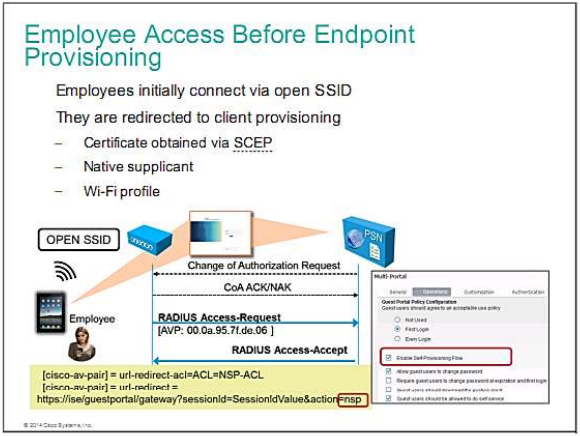


Guests are redirected to the guest portal. Their endpoints are not provisioned because the **Enable Self-Provisioning Flow** option in the **Multi-Portal** page is not set. After successful authentication, guests continue using the open SSID to access the allowed resources. Commonly, the guest policy allows access only to Internet resources.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Employee Access Before Endpoint Provisioning

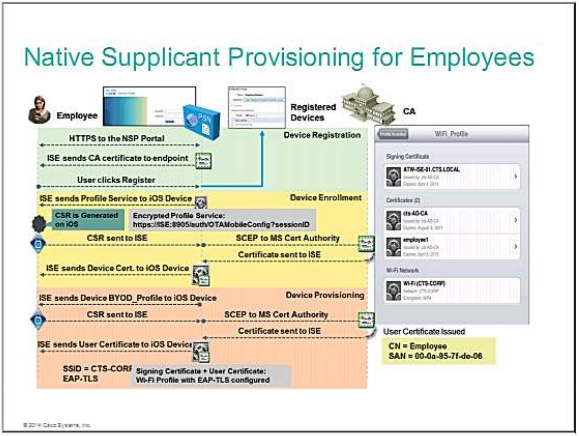
This topic describes the access of the employees before their endpoints are provisioned.



Employees initially connect via open SSID and are then redirected to client provisioning. The employee endpoints obtain certificates, which are provisioned via SCEP, obtain a native supplicant, and obtain a Wi-Fi profile.

Native Supplicant Provisioning for Employees

This topic describes the native supplicant provisioning process for iOS endpoints.

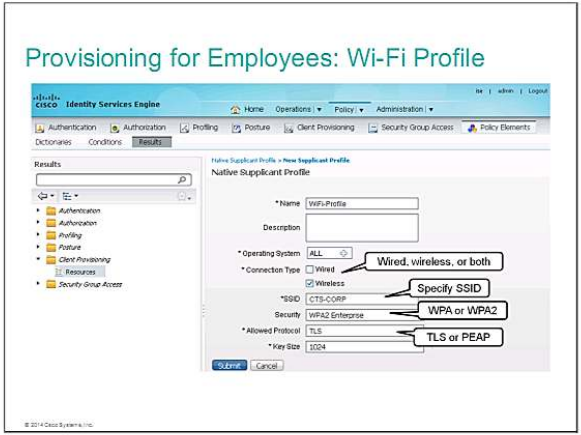


Supplicants can be automatically provisioned with a certificate. When an employee accesses the network with a personal device, the user will open a web page and receive a redirect. The Cisco Identity Services Engine will return a CA certificate for trust purposes. The user will be offered the opportunity to register the device. The Cisco ISE will then add the user to the registered devices list as an identity group and begin device enrollment. For example, it might ask the user to create a CSR based on user information like the UDI, the MAC address, and some other attributes. That information is sent to the Cisco ISE, where, because it is a SCEP proxy, it will forward the request to the CA server. The certificate will then be issued. The Cisco ISE can now push the profile that the user is going to use for the final connection. It will then create a new CSR, which is pushed back. A key point to note here is that the common name value is now the employee name that the user used when logging in, and the SAN value is the MAC address of that endpoint.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Provisioning for Employees: Wi-Fi Profile

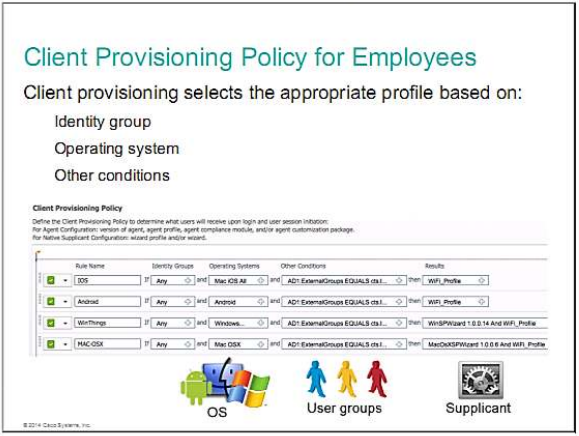
This topic describes the configuration of the supplicant profile that is provisioned on the employee endpoints.



The Wi-Fi profile, configured by navigating to **Policy > Policy Elements > Results > Client Provisioning > Resources**, defines the wired or wireless connectivity settings for employees. These settings are used by the native supplicant after the provisioning phase. They define the connection type (wireless or wired), SSID, security (WPA or WPA2), allowed protocol (TLS or PEAP), and the key size.

Client Provisioning Policy for Employees

This topic describes how to configure the client provisioning policy for employees.

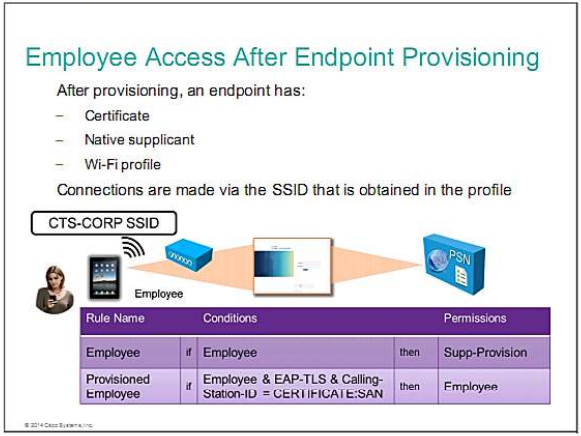


The client provisioning policy defines the profiles that are provisioned on endpoints, depending on the user identity group, the endpoint operating system, and other conditions.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Employee Access After Endpoint Provisioning

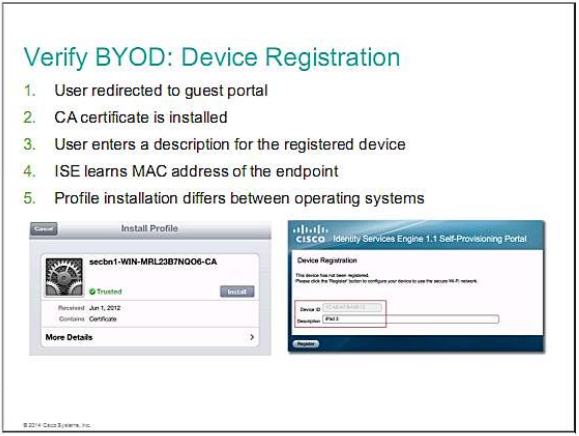
This topic describes employee access after endpoints have been provisioned.



After the successful provisioning of employee endpoints, the employees connect using the specified SSID and security parameters.

Verify BYOD: Device Registration

This topic describes the user experience when going through the BYOD device registration phase.



In this scenario, the employee connects with a mobile device to the provisioning SSID and is redirected to the guest portal for registration after opening a browser. The employee logs in using Active Directory credentials.

After the CA certificate is installed, the user enters a description for the device being registered. The Cisco Identity Services Engine learns the MAC address of the endpoint and the profile installation begins.

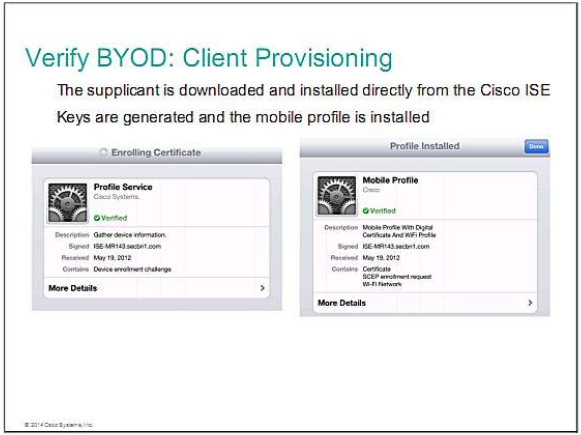
If profiling is being used, additional attributes will be sent to the Cisco ISE that will determine the type of Apple device and add it to the nominated endpoint group. This group will then determine the authorization profile that the user will receive.

This scenario shows the procedure on an Apple iOS device—an iPhone, iPad, or iPod. It differs slightly from the user experience on Android devices.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Verify BYOD: Client Provisioning

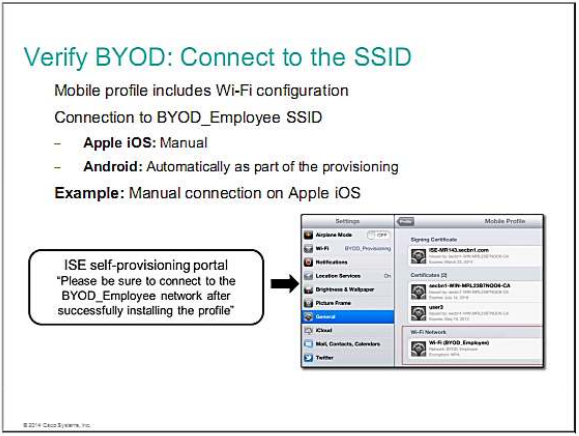
This topic describes the user experience when going through the client provisioning phase on an Apple iOS device.



The supplicant profile is downloaded and installed on the endpoint. Keys are then generated and the certificate is enrolled. The Wi-Fi profile that is required to connect to the BYOD_Employee SSID is installed.

Verify BYOD: Connect to the SSID

This topic describes the user experience when connecting to the SSID on Apple iOS.



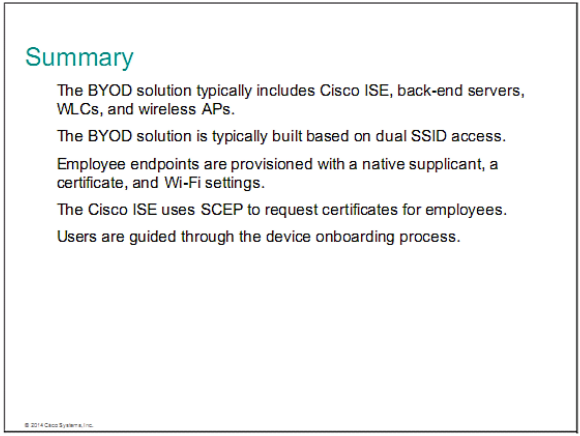
The Wi-Fi profile that is required to connect to the BYOD_Employee SSID is installed. On Apple iOS devices, the employee is required to manually connect to the BYOD_Employee SSID. On Android endpoints, the connection to the BYOD_Employee SSID is performed automatically as part of the provisioning process.

The example in the figure illustrates the manual connection on Apple iOS.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Summary

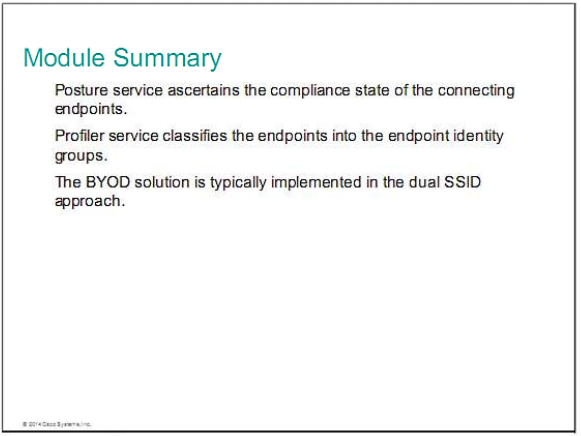
This topic summarizes the key points that were discussed in this lesson.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Module Summary

This topic summarizes the key points that were discussed in this module.



References

For additional information refer to this resource:

Cisco Identity Services Engine User Guide

https://t.me/learningnets

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Module Self-Check

Questions

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

1. On which nodes does the posture service run? (Source: Deploying Posture Service)

   A. on all nodes in the Cisco ISE deployment
   B. by default, on all nodes in the Cisco ISE deployment
   C. on all nodes in the Cisco ISE deployment with the session services enabled
   D. on all nodes in the Cisco ISE deployment with the profiler service enabled
   E. on all policy service nodes in the Cisco ISE deployment
   F. by default, on all policy service nodes in the Cisco ISE deployment
   G. on all policy service nodes in the Cisco ISE deployment with the session services enabled
   H. on all policy service nodes in the Cisco ISE deployment with the profiler service enabled

2. What are the two building blocks of the Cisco ISE posture policy? (Choose two.) (Source: Deploying Posture Service)

   A. requirements
   B. authorization policy rule
   C. client provisioning
   D. remediation
   E. dictionary attributes

3. Posture updates can be scheduled automatically. (Source: Deploying Posture Service)

   A. true
   B. false

https://t.me/learningnets

4. What is the basic unique representation of an endpoint by the profiler service? (Source: Deploying Profiler Service)

   A. endpoint profile
   B. endpoint ID
   C. MAC address
   D. IP address

5. On which two nodes does the analyzer run? (Choose two.) (Source: Deploying Profiler Service)

   A. admin nodes with the profiler service enabled
   B. admin nodes with the analyzer service enabled
   C. admin nodes also acting as the sensors
   D. policy service nodes with the profiler service enabled
   E. policy service nodes with the analyzer service enabled
   F. policy service nodes also acting as the sensors

6. CoA support is required to run the profiler service. (Source: Deploying Profiler Service)

   A. true
   B. false

7. Which software is provisioned as a result of device onboarding? (Source: Implementing BYOD)

   A. Web Agent
   B. native supplicant for Windows
   C. NAC Agent for Macintosh
   D. NAC Agent for Windows

8. Open SSID is used for provisioning in both single and dual SSID scenarios. (Source: Implementing BYOD)

   A. true
   B. false

9. Which approach is most common when deploying BYOD? (Source: Implementing BYOD)

   A. mixed
   B. single SSID
   C. dual SSID
   D. fixed SSID

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Answer Key

1. G
2. A, D
3. A
4. C
5. C, F
6. B
7. B
8. A
9. C

https://t.me/learningnets

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Module 6

Access Control Troubleshooting

The Cisco Identity Services Engine offers a a number of troubleshooting tools. The general tools include RADIUS Authentication Troubleshooting, Execute Network Device Command, Evaluate Configuration Validator, Posture Troubleshooting, and TCP Dump. You will learn about the most efficient strategies when troubleshooting Cisco network access control.

Upon completing this module, you will be able to:

Troubleshoot Cisco network access controls.

https://t.me/learningnets

https://t.me/learningnets

Lesson 1

Troubleshooting Network Access Controls

Overview

Network access control mechanisms restrict access to the network based on identity or security posture. The network access devices force user or machine authentication prior to granting access to the network. In addition, guest access can be granted to a quarantine area for remediation of any problems that may have caused authentication failure. This quarantine is enforced through an inline network device, or through changes to an existing access device. Network access control encompasses various components that interoperate. To effectively troubleshoot the solution, you need to understand the operation of AAA, 802.1X, MAB, and know the troubleshooting tools available on the Cisco Identity Services Engine and the network access devices.

Upon completing this lesson, you will be able to identify and troubleshoot problems when implementing and operating Cisco access control solutions. You will be able to meet these objectives:

- Describe how to troubleshoot the profiler service
- Describe the troubleshooting tools available on Cisco ISE
- Describe the RADIUS Authentication Troubleshooting tool
- Describe the Execute Network Device Command tool
- Describe the Evaluate Configuration Validator tool
- Describe the Posture Troubleshooting tool
- Describe the TCP Dump tool
- Describe troubleshooting of 802.1x authentication
- Describe how to troubleshoot the 802.1X operation on an access switch
- Describe how to troubleshoot RADIUS peering
- Describe how to troubleshoot peering with the back-end user database

https://t.me/learningnets

Describe how to troubleshoot identity source sequencing

Describe how to troubleshoot client-side certificate issues

Describe how to troubleshoot disallowed authentication protocol issues

Describe how to troubleshoot machine authentication

Describe how to troubleshoot Central WebAuth

Describe the ISE authentication policy settings that are required for Central WebAuth

Describe the Cisco ISE authorization policy settings that are required for WebAuth

Describe the ISE authorization profile that is used for traffic redirection

Describe how to troubleshoot a mismatch of the ACL name

Describe how to troubleshoot the posture service

Describe the use of the client provisioning policy in the posture service

Describe the Cisco ISE posture policy

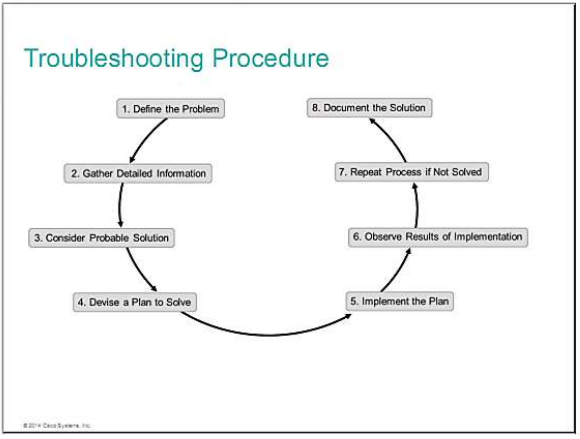
Describe the Cisco ISE posture requirements

Describe how to troubleshoot a posture service problem

Describe how to troubleshoot the profiler service

Troubleshooting Procedure

This topic describes general troubleshooting procedure.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

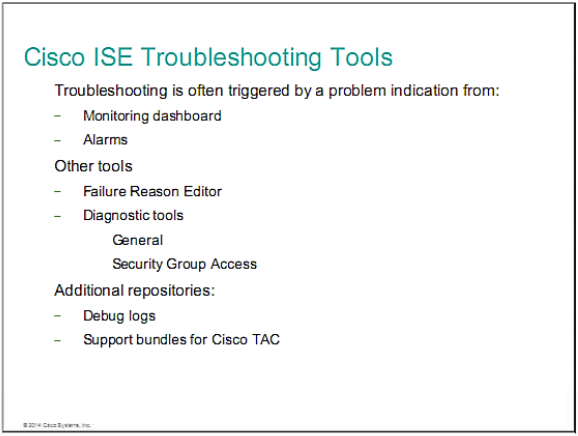
Effective troubleshooting requires a structured approach. This flow has proven very successful when troubleshooting problems:

1. **Define the problem:** Look for symptoms and then determine the problems that could result in the symptoms you found. An example of such a symptom is a host that is not responding to the requests from the clients. One possible cause of this can be a misconfiguration of the host.
2. **Gather detailed information:** Collect as much information as you can about the reported issue. Ask the affected users for information, and look for information in different sources such as the NMS, debug and **show** commands, and so on.
3. **Consider a probable solution:** With all the information you collected, try to determine the elements that might not be causing the problem. An example could be the hardware. If you can eliminate the hardware as a cause, you can concentrate on the software.
4. **Devise a plan to solve the problem:** Determine the most likely cause of the problem and devise the plan.
5. **Implement the plan:** Start implementing the action plan step by step and see if any of the symptoms start disappearing. Carefully keep track of any changes so you can revert any counter effective or ineffective changes.
6. **Observe the results of implementation:** Whenever a change is made, look at the results or impact of the change. You can always use the diagnostic tools for additional help or information.
7. **Repeat the process if the problem is not solved:** If the problem has not been resolved, follow the process again until there is no problem in the network.
8. **Document the solution:** This step is one of the most important steps. Any change in the device configuration should be documented and communicated to the technical staff. It is always easier to troubleshoot a well-documented network.

https://t.me/learningnets

Cisco ISE Troubleshooting Tools

This topic describes the troubleshooting tools that are available on Cisco Identity Services Engine.



Cisco ISE offers several tools that assist you in the troubleshooting process and provide you with a problem description upon which you can act. You can receive a problem indication from the Monitoring dashboard and from the Alarms pages.

Useful troubleshooting tools include the Failure Reason Editor and the General and Security Group Access diagnostic tools. The debug logs may be useful when troubleshooting system faults that are not easily solved using first-level methods. If you escalate a problem and report it to Cisco Technical Assistance Center, you will need to package the system information into support bundles.

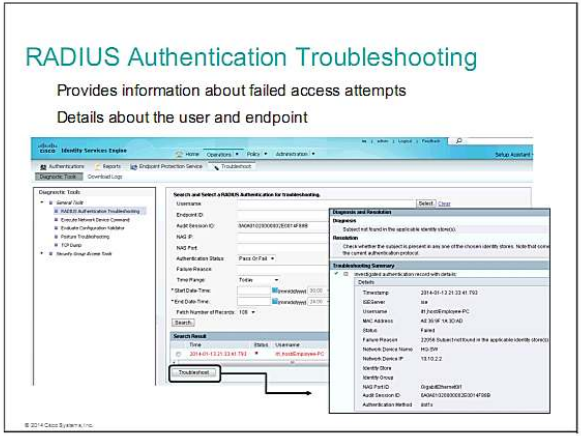
The Execute Network Device Command diagnostic tool allows you to run the **show** command on any network device from the centralized Cisco ISE dashboard. The results are exactly what you would see on a console, and can be used to identify problems in the configuration of the device.

The TCP Dump utility monitors the contents of packets on a network interface that match a given Boolean expression. You can use the TCP Dump utility to troubleshoot problems on your network. Cisco ISE troubleshooting diagnostic tools provide an intuitive user interface for this utility.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

RADIUS Authentication Troubleshooting

This topic describes the RADIUS Authentication Troubleshooting tool.

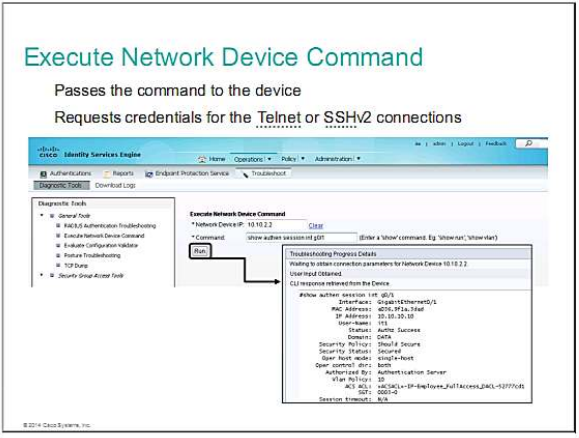


The RADIUS Authentication Troubleshooting tool examines different aspects of a session and provides some details which may not have been available in the detailed authentication report. It also provides some advice on resolution for issues found in the diagnosed session. The tool provides the ability to search and select an individual authentication session based on criteria such as username, MAC address, NAD IP, and date/time ranges. It even allows you to search on an individual common session ID.

In the simple example shown in the figure, the problem was that the subject was not found in the applicable identity stores. This could indicate an issue with the identity source sequence configuration. It could also mean, as suggested, that the identity source may not be compatible with the EAP protocol used by 802.1X.

Execute Network Device Command

This topic describes the Execute Network Device Command tool.

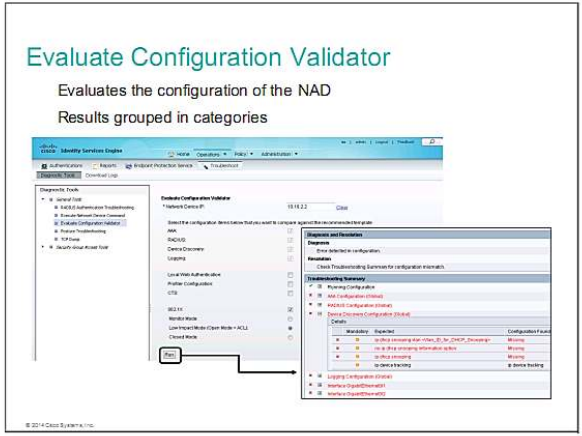


The Execute Network Device Command tool does what its name suggests. It is designed to allow you to run a show command against a network device from within Cisco Identity Services Engine. To initialize the tool, you must specify a device by IP address or DNS hostname and you must specify the command to execute. The tool does not parse the command. It simply passes the command to the device. This means there is no syntax validation, but it does allow acceptable command line abbreviations. Once the tool is initialized, it will also request credentials for the device and allow you to select to connect via Telnet or SSHv2. After command execution, the results are displayed. The example depicted in the figure shows the execution of an abbreviated form of the **show authentication session interface GigabitEthernet 0/1** command.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Evaluate Configuration Validator

This topic describes the RADIUS Authentication Troubleshooting tool.



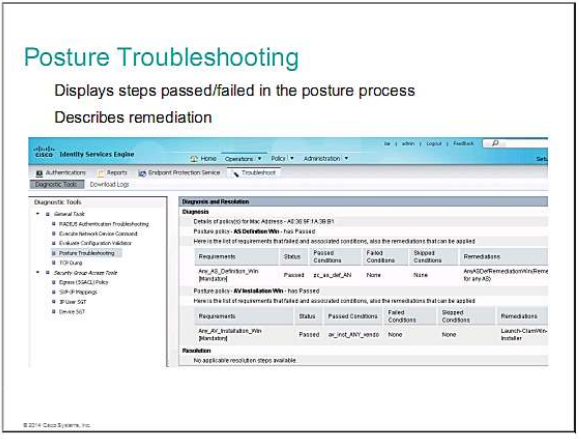
The Evaluate Configuration Validator tool is very useful, but its output should be considered recommendations, not requirements. To initiate the tool, you specify the NAD by IP address or hostname and you specify the sections of the configuration that it should validate. The tool examines the configuration and compares it to a template and reports on any differences it finds between the two. The administrator should consider the report and determine if the configuration should be modified to coincide with the template or not. It is quite possible that there are more than one way to configure equivalent behavior. It is also possible that you are intentionally not implementing all features between the NAD and Cisco Identity Services Engine.

The tool allows you to specify the NAD and to select the aspects of the configuration that it will evaluate. When the tool is executed, it will ask you choose between Telnet and SSHv2 and to provide administrative login credentials. When the tool finishes, it provides a hierarchical report, allowing you to expand and collapse details on a per section basis.

In the example depicted, the tool is showing that DHCP snooping features have not been configured globally on the NAD. This can impact profiling. Note that the IP device tracking feature is enabled. This can provide a MAC to IP address mapping which is made available with the standard RADIUS profiling probe. But, DHCP snooping can support more accurate IP tracking results. Also, if the NAD supports the IOS device sensor feature, then other DHCP data can be provided for profiling, such as the contents of the DHCP client-identifier field.

Posture Troubleshooting

This topic describes the Posture Troubleshooting tool.

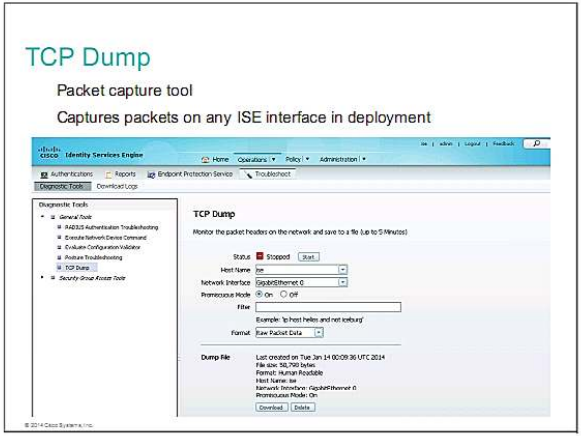


The Posture Troubleshooting tool helps you find the cause of a posture check failure. You can easily identify which endpoints were successful in posture and which were not. If an endpoint failed in posture, the tool lists the steps failed in the posture process. It describes which mandatory and optional checks passed and failed. You can determine this information by filtering requests based on parameters, such as username, MAC address, posture status, and so on.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

TCP Dump

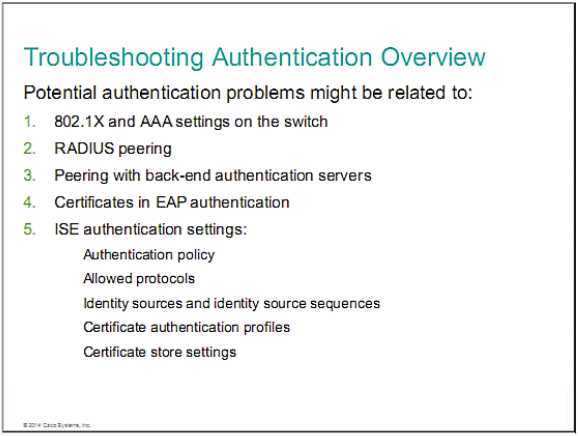
This topic describes the TCP Dump tool.



Packet captures are an extremely valuable troubleshooting tool. They allow you to dive deeper than you can with the GUI, CLI debugs and various logging technologies. Generally, to accomplish a packet capture, you must configure SPAN on a switch and set up a packet capture tool on the SPAN destination port. To make this much easier from Cisco Identity Services Engine's perspective, TCP dump has been built directly into ISE. You can use TCP dump to capture the packets that are sent by and received on any particular interface on any ISE node in the deployment. You can choose for the dump to be formatted as raw packet data, which can be downloaded as a Pcap file which can be downloaded and read by a packet analyzer on your workstation. You can also choose for the dump to be formatted as human readable, in which case it is formatted as a text file that can be loaded into a text processor on your workstation.

Troubleshooting Authentication Overview

This topic describes the troubleshooting of IEEE 802.1X authentication.

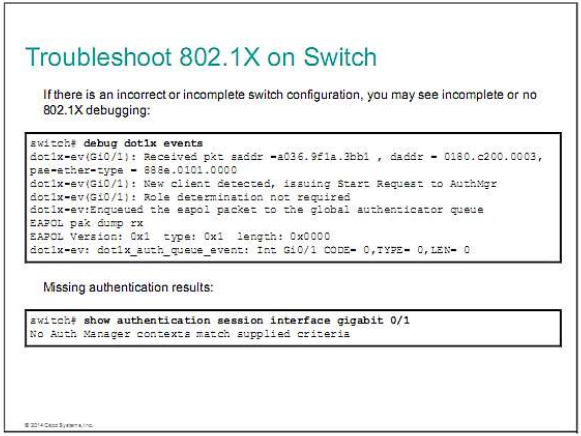


802.1X authentication failures can occur as a result of various reasons. The list in the figure summarizes the most common problems, which are discussed in the several next topics.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

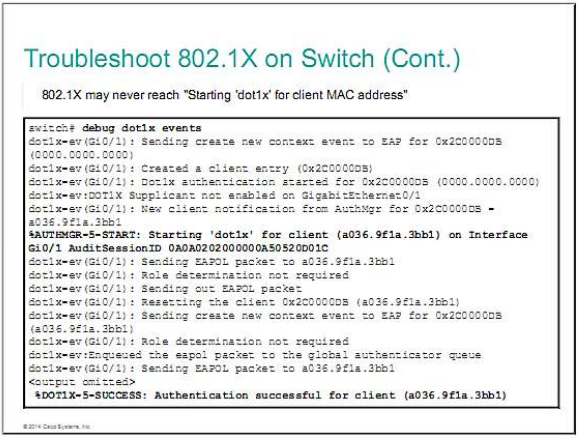
Troubleshoot 802.1X on Switch

This topic describes the troubleshooting of IEEE 802.1X operation on an access switch.



The 802.1X authentication can fail due to an incorrect 802.1X configuration on the access switch. You can monitor the 802.1X operation using the **debug dot1x** command This command provides several options for differentiated output granularity. Depending on the 802.1X misconfiguration, you may not see any debugging output at all or you may see that the 802.1x never completes.

In this example, the 802.1X procedure never reaches the expected phase "Starting 'dot1x' for client MAC address," and therefore the port is never authenticated.



When the switch configuration is complete, the 802.1X procedure goes through the "Starting 'dot1x' for client MAC address" phase and the port is authenticated. Complete debugging output and port authentication status verification are shown in the following output:

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

```
switch# debug dot1x events
Sep  5 09:24:38.611: dot1x-ev(Gi0/1): Interface state changed to UP
Sep  5 09:24:38.653: dot1x-ev(Gi0/1): Sending create new context event to EAP for
0x2C0000DB (0000.0000.0000)
Sep  5 09:24:38.653: dot1x-ev(Gi0/1): Created a client entry (0x2C0000DB)
Sep  5 09:24:38.653: dot1x-ev(Gi0/1): Dot1x authentication started for 0x2C0000DB
(0000.0000.0000)
Sep  5 09:24:38.653: dot1x-ev:DOT1X Supplicant not enabled on GigabitEthernet0/1
Sep  5 09:24:38.661: dot1x-ev(Gi0/1): New client notification from AuthMgr for
0x2C0000DB - a036.9f1a.3bb1
Sep  5 09:24:38.661: %AUTHMGR-5-START: Starting 'dot1x' for client (a036.9f1a.3bb1)
on Interface Gi0/1 AuditSessionID 0A0A0202000000A50520D01C
Sep  5 09:24:38.661: dot1x-ev(Gi0/1): Sending EAPOL packet to a036.9f1a.3bb1
Sep  5 09:24:38.661: dot1x-ev(Gi0/1): Role determination not required
Sep  5 09:24:38.661: dot1x-ev(Gi0/1): Sending out EAPOL packet
Sep  5 09:24:38.661: dot1x-ev(Gi0/1): Resetting the client 0x2C0000DB (a036.9f1a.3bb1)
Sep  5 09:24:38.661: dot1x-ev(Gi0/1): Sending create new context event to EAP for
0x2C0000DB (a036.9f1a.3bb1)
Sep  5 09:24:38.661: dot1x-ev(Gi0/1): Role determination not required
Sep  5 09:24:38.661: dot1x-ev:Enqueued the eapol packet to the global authenticator
queue
Sep  5 09:24:38.661: dot1x-ev(Gi0/1): Sending EAPOL packet to a036.9f1a.3bb1
Sep  5 09:24:38.661: dot1x-ev(Gi0/1): Role determination not required
Sep  5 09:24:38.661: dot1x-ev(Gi0/1): Sending out EAPOL packet
Sep  5 09:24:38.661: EAPOL pak dump rx
Sep  5 09:24:38.661: EAPOL Version: 0x1  type: 0x1  length: 0x0000
Sep  5 09:24:38.661: dot1x-ev:dot1x_auth_queue_event: Int Gi0/1 CODE= 0,TYPE= 0,LEN= 0
Sep  5 09:24:38.661: dot1x-ev(Gi0/1): Received pkt saddr =a036.9f1a.3bb1 , daddr =
0180.c200.0003, pae-ether-type = 888e.0101.0000
Sep  5 09:24:38.661: dot1x-ev(Gi0/1): Resetting the client 0x2C0000DB (a036.9f1a.3bb1)
Sep  5 09:24:38.661: dot1x-ev(Gi0/1): Sending create new context event to EAP for
0x2C0000DB (a036.9f1a.3bb1)
Sep  5 09:24:38.661: dot1x-ev(Gi0/1): Sending EAPOL packet to a036.9f1a.3bb1
Sep  5 09:24:38.670: dot1x-ev(Gi0/1): Role determination not required
Sep  5 09:24:38.670: dot1x-ev(Gi0/1): Sending out EAPOL packet
Sep  5 09:24:38.670: dot1x-ev(Gi0/1): Role determination not required
Sep  5 09:24:38.670: dot1x-ev:Enqueued the eapol packet to the global authenticator
queue
Sep  5 09:24:38.670: EAPOL pak dump rx
Sep  5 09:24:38.670: EAPOL Version: 0x1  type: 0x0  length: 0x000C
Sep  5 09:24:38.670: dot1x-ev:dot1x_auth_queue_event: Int Gi0/1 CODE= 2,TYPE= 1,LEN=
12
Sep  5 09:24:38.670: dot1x-ev(Gi0/1): Received pkt saddr =a036.9f1a.3bb1 , daddr =
0180.c200.0003, pae-ether-type = 888e.0100.000c
Sep  5 09:24:38.670: dot1x-ev(Gi0/1): dot1x_sendRespToServer: Response sent to the
server from 0x2C0000DB (a036.9f1a.3bb1)
Sep  5 09:24:38.670: dot1x-ev(Gi0/1): Role determination not required
Sep  5 09:24:38.670: dot1x-ev:Enqueued the eapol packet to the global authenticator
queue
Sep  5 09:24:38.670: EAPOL pak dump rx
Sep  5 09:24:38.670: EAPOL Version: 0x1  type: 0x0  length: 0x000C
Sep  5 09:24:38.670: dot1x-ev:dot1x_auth_queue_event: Int Gi0/1 CODE= 2,TYPE= 1,LEN=
12
Sep  5 09:24:38.670: dot1x-ev(Gi0/1): Received pkt saddr =a036.9f1a.3bb1 , daddr =
0180.c200.0003, pae-ether-type = 888e.0100.000c
Sep  5 09:24:38.670: dot1x-ev(Gi0/1): Role determination not required
Sep  5 09:24:38.670: dot1x-ev:Enqueued the eapol packet to the global authenticator
queue
Sep  5 09:24:38.670: EAPOL pak dump rx
Sep  5 09:24:38.670: EAPOL Version: 0x1  type: 0x0  length: 0x000C
Sep  5 09:24:38.670: dot1x-ev:dot1x_auth_queue_event: Int Gi0/1 CODE= 2,TYPE= 1,LEN=
12
```

```
Sep  5 09:24:38.678: dot1x-ev(Gi0/1): Received pkt saddr =a036.9f1a.3bb1 , daddr =
0180.c200.0003, pae-ether-type = 888e.0100.000c
Sep  5 09:24:38.678: dot1x-ev(Gi0/1): Sending EAPOL packet to a036.9f1a.3bb1
Sep  5 09:24:38.678: dot1x-ev(Gi0/1): Role determination not required
Sep  5 09:24:38.678: dot1x-ev(Gi0/1): Sending out EAPOL packet
Sep  5 09:24:38.686: dot1x-ev(Gi0/1): Role determination not required
Sep  5 09:24:38.686: dot1x-ev:Enqueued the eapol packet to the global authenticator
queue
Sep  5 09:24:38.686: EAPOL pak dump rx
Sep  5 09:24:38.686: EAPOL Version: 0x1  type: 0x0  length: 0x0006
Sep  5 09:24:38.686: dot1x-ev:dot1x_auth_queue_event: Int Gi0/1 CODE= 2,TYPE= 3,LEN= 6
Sep  5 09:24:38.686: dot1x-ev(Gi0/1): Received pkt saddr =a036.9f1a.3bb1 , daddr =
0180.c200.0003, pae-ether-type = 888e.0100.0006
Sep  5 09:24:38.695: dot1x-ev(Gi0/1): dot1x_sendRespToServer: Response sent to the
server from 0x2C0000DB (a036.9f1a.3bb1)
Sep  5 09:24:38.703: dot1x-ev(Gi0/1): Sending EAPOL packet to a036.9f1a.3bb1
Sep  5 09:24:38.703: dot1x-ev(Gi0/1): Role determination not required
Sep  5 09:24:38.703: dot1x-ev(Gi0/1): Sending out EAPOL packet
Sep  5 09:24:38.703: dot1x-ev(Gi0/1): Role determination not required
Sep  5 09:24:38.703: dot1x-ev:Enqueued the eapol packet to the global authenticator
queue
Sep  5 09:24:38.703: EAPOL pak dump rx
Sep  5 09:24:38.703: EAPOL Version: 0x1  type: 0x0  length: 0x0089
Sep  5 09:24:38.703: dot1x-ev:dot1x_auth_queue_event: Int Gi0/1 CODE= 2,TYPE= 25,LEN=
137
Sep  5 09:24:38.703: dot1x-ev(Gi0/1): Received pkt saddr =a036.9f1a.3bb1 , daddr =
0180.c200.0003, pae-ether-type = 888e.0100.0089
Sep  5 09:24:38.703: dot1x-ev(Gi0/1): dot1x_sendRespToServer: Response sent to the
server from 0x2C0000DB (a036.9f1a.3bb1)
Sep  5 09:24:38.712: dot1x-ev(Gi0/1): Sending EAPOL packet to a036.9f1a.3bb1
Sep  5 09:24:38.712: dot1x-ev(Gi0/1): Role determination not required
Sep  5 09:24:38.712: dot1x-ev(Gi0/1): Sending out EAPOL packet
Sep  5 09:24:38.712: dot1x-ev(Gi0/1): Role determination not required
Sep  5 09:24:38.712: dot1x-ev:Enqueued the eapol packet to the global authenticator
queue
Sep  5 09:24:38.712: EAPOL pak dump rx
Sep  5 09:24:38.712: EAPOL Version: 0x1  type: 0x0  length: 0x0006
Sep  5 09:24:38.712: dot1x-ev:dot1x_auth_queue_event: Int Gi0/1 CODE= 2,TYPE= 25,LEN=
6
Sep  5 09:24:38.712: dot1x-ev(Gi0/1): Received pkt saddr =a036.9f1a.3bb1 , daddr =
0180.c200.0003, pae-ether-type = 888e.0100.0006
Sep  5 09:24:38.712: dot1x-ev(Gi0/1): dot1x_sendRespToServer: Response sent to the
server from 0x2C0000DB (a036.9f1a.3bb1)
Sep  5 09:24:38.728: dot1x-ev(Gi0/1): Sending EAPOL packet to a036.9f1a.3bb1
Sep  5 09:24:38.728: dot1x-ev(Gi0/1): Role determination not required
Sep  5 09:24:38.728: dot1x-ev(Gi0/1): Sending out EAPOL packet
Sep  5 09:24:38.728: dot1x-ev(Gi0/1): Role determination not required
Sep  5 09:24:38.728: dot1x-ev:Enqueued the eapol packet to the global authenticator
queue
Sep  5 09:24:38.728: EAPOL pak dump rx
Sep  5 09:24:38.737: EAPOL Version: 0x1  type: 0x0  length: 0x0006
Sep  5 09:24:38.737: dot1x-ev:dot1x_auth_queue_event: Int Gi0/1 CODE= 2,TYPE= 25,LEN=
6
Sep  5 09:24:38.737: dot1x-ev(Gi0/1): Received pkt saddr =a036.9f1a.3bb1 , daddr =
0180.c200.0003, pae-ether-type = 888e.0100.0006
Sep  5 09:24:38.737: dot1x-ev(Gi0/1): dot1x_sendRespToServer: Response sent to the
server from 0x2C0000DB (a036.9f1a.3bb1)
Sep  5 09:24:38.737: dot1x-ev(Gi0/1): Sending EAPOL packet to a036.9f1a.3bb1
Sep  5 09:24:38.737: dot1x-ev(Gi0/1): Role determination not required
Sep  5 09:24:38.737: dot1x-ev(Gi0/1): Sending out EAPOL packet
Sep  5 09:24:38.745: dot1x-ev(Gi0/1): Role determination not required
Sep  5 09:24:38.745: dot1x-ev:Enqueued the eapol packet to the global authenticator
queue
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

```
Sep  5 09:24:38.745: EAPOL pak dump rx
Sep  5 09:24:38.745: EAPOL Version: 0x1  type: 0x0  length: 0x0150
Sep  5 09:24:38.745: dot1x-ev:dot1x_auth_queue_event: Int Gi0/1 CODE= 2,TYPE= 25,LEN=
336
Sep  5 09:24:38.745: dot1x-ev(Gi0/1): Received pkt saddr =a036.9f1a.3bb1 , daddr =
0180.c200.0003, pae-ether-type = 888e.0100.0150
Sep  5 09:24:38.745: dot1x-ev(Gi0/1): dot1x_sendRespToServer: Response sent to the
server from 0x2C0000DB (a036.9f1a.3bb1)
Sep  5 09:24:38.787: dot1x-ev(Gi0/1): Sending EAPOL packet to a036.9f1a.3bb1
Sep  5 09:24:38.787: dot1x-ev(Gi0/1): Role determination not required
Sep  5 09:24:38.787: dot1x-ev(Gi0/1): Sending out EAPOL packet
Sep  5 09:24:38.787: dot1x-ev(Gi0/1): Role determination not required
Sep  5 09:24:38.787: dot1x-ev:Enqueued the eapol packet to the global authenticator
queue
Sep  5 09:24:38.787: EAPOL pak dump rx
Sep  5 09:24:38.787: EAPOL Version: 0x1  type: 0x0  length: 0x0006
Sep  5 09:24:38.787: dot1x-ev:dot1x_auth_queue_event: Int Gi0/1 CODE= 2,TYPE= 25,LEN=
6
Sep  5 09:24:38.795: dot1x-ev(Gi0/1): Received pkt saddr =a036.9f1a.3bb1 , daddr =
0180.c200.0003, pae-ether-type = 888e.0100.0006
Sep  5 09:24:38.795: dot1x-ev(Gi0/1): dot1x_sendRespToServer: Response sent to the
server from 0x2C0000DB (a036.9f1a.3bb1)
Sep  5 09:24:38.795: dot1x-ev(Gi0/1): Sending EAPOL packet to a036.9f1a.3bb1
Sep  5 09:24:38.795: dot1x-ev(Gi0/1): Role determination not required
Sep  5 09:24:38.795: dot1x-ev(Gi0/1): Sending out EAPOL packet
Sep  5 09:24:38.804: dot1x-ev(Gi0/1): Role determination not required
Sep  5 09:24:38.804: dot1x-ev:Enqueued the eapol packet to the global authenticator
queue
Sep  5 09:24:38.804: EAPOL pak dump rx
Sep  5 09:24:38.804: EAPOL Version: 0x1  type: 0x0  length: 0x002B
Sep  5 09:24:38.804: dot1x-ev:dot1x_auth_queue_event: Int Gi0/1 CODE= 2,TYPE= 25,LEN=
43
Sep  5 09:24:38.804: dot1x-ev(Gi0/1): Received pkt saddr =a036.9f1a.3bb1 , daddr =
0180.c200.0003, pae-ether-type = 888e.0100.002b
Sep  5 09:24:38.812: dot1x-ev(Gi0/1): dot1x_sendRespToServer: Response sent to the
server from 0x2C0000DB (a036.9f1a.3bb1)
Sep  5 09:24:38.812: dot1x-ev(Gi0/1): Sending EAPOL packet to a036.9f1a.3bb1
Sep  5 09:24:38.812: dot1x-ev(Gi0/1): Role determination not required
Sep  5 09:24:38.812: dot1x-ev(Gi0/1): Sending out EAPOL packet
Sep  5 09:24:38.821: dot1x-ev(Gi0/1): Role determination not required
Sep  5 09:24:38.821: dot1x-ev:Enqueued the eapol packet to the global authenticator
queue
Sep  5 09:24:38.821: EAPOL pak dump rx
Sep  5 09:24:38.821: EAPOL Version: 0x1  type: 0x0  length: 0x006B
Sep  5 09:24:38.821: dot1x-ev:dot1x_auth_queue_event: Int Gi0/1 CODE= 2,TYPE= 25,LEN=
107
Sep  5 09:24:38.821: dot1x-ev(Gi0/1): Received pkt saddr =a036.9f1a.3bb1 , daddr =
0180.c200.0003, pae-ether-type = 888e.0100.006b
Sep  5 09:24:38.821: dot1x-ev(Gi0/1): dot1x_sendRespToServer: Response sent to the
server from 0x2C0000DB (a036.9f1a.3bb1)
Sep  5 09:24:38.837: dot1x-ev(Gi0/1): Sending EAPOL packet to a036.9f1a.3bb1
Sep  5 09:24:38.837: dot1x-ev(Gi0/1): Role determination not required
Sep  5 09:24:38.837: dot1x-ev(Gi0/1): Sending out EAPOL packet
Sep  5 09:24:38.846: dot1x-ev(Gi0/1): Role determination not required
Sep  5 09:24:38.846: dot1x-ev:Enqueued the eapol packet to the global authenticator
queue
Sep  5 09:24:38.846: EAPOL pak dump rx
Sep  5 09:24:38.846: EAPOL Version: 0x1  type: 0x0  length: 0x002B
Sep  5 09:24:38.846: dot1x-ev:dot1x_auth_queue_event: Int Gi0/1 CODE= 2,TYPE= 25,LEN=
43
Sep  5 09:24:38.854: dot1x-ev(Gi0/1): Received pkt saddr =a036.9f1a.3bb1 , daddr =
0180.c200.0003, pae-ether-type = 888e.0100.002b
```

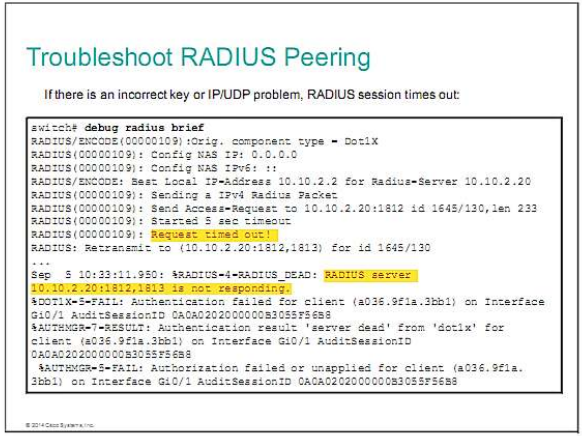

https://t.me/learningnets

```
Sep  5 09:24:38.854: dot1x-ev(Gi0/1): dot1x_sendRespToServer: Response sent to the
server from 0x2C0000DB (a036.9f1a.3bb1)
Sep  5 09:24:38.854: dot1x-ev(Gi0/1): Sending EAPOL packet to a036.9f1a.3bb1
Sep  5 09:24:38.854: dot1x-ev(Gi0/1): Role determination not required
Sep  5 09:24:38.854: dot1x-ev(Gi0/1): Sending out EAPOL packet
Sep  5 09:24:38.863: dot1x-ev(Gi0/1): Role determination not required
Sep  5 09:24:38.863: dot1x-ev:Enqueued the eapol packet to the global authenticator
queue
Sep  5 09:24:38.863: EAPOL pak dump rx
Sep  5 09:24:38.863: EAPOL Version: 0x1  type: 0x0  length: 0x002B
Sep  5 09:24:38.863: dot1x-ev: dot1x_auth_queue_event: Int Gi0/1 CODE= 2,TYPE=
25,LEN= 43
Sep  5 09:24:38.863: dot1x-ev(Gi0/1): Received pkt saddr =a036.9f1a.3bb1 , daddr =
0180.c200.0003, pae-ether-type = 888e.0100.002b
Sep  5 09:24:38.863: dot1x-ev(Gi0/1): dot1x_sendRespToServer: Response sent to the
server from 0x2C0000DB (a036.9f1a.3bb1)
Sep  5 09:24:38.896: %DOT1X-5-SUCCESS: Authentication successful for client
(a036.9f1a.3bb1) on Interface Gi0/1 AuditSessionID 0A0A0202000000A50520D01C
switch# show authentication sessions interface gigabit 0/1
            Interface:  GigabitEthernet0/1
          MAC Address:  a036.9f1a.3bb1
           IP Address:  10.10.9.16
            User-Name:  student
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-Employee_ACL-51959ffa
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A0A0202000000B0054F0E5E
      Acct Session ID:  0x000000ED
               Handle:  0x340000B1
Runnable methods list:
       Method   State
       dot1x    Authc Success
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Troubleshoot RADIUS Peering

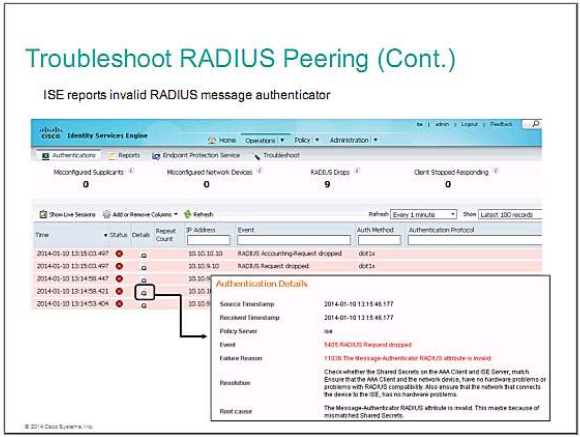
This topic describes how to troubleshoot RADIUS peering.



You can troubleshoot RADIUS peering problems on the switch or on the Cisco Identity Services Engine. The output of the **debug radius brief** command, shown in the figure, indicates that the RADIUS server is not responding to the switch. There are several possible reasons for this. The switch configuration must properly define the RADIUS server and the RADIUS server must be configured to recognize the switch. If either side specifies the wrong IP address or wrong RADIUS key, they will not peer properly. There can also be problems with network connectivity between the two devices, including the possibility of a firewall blocking the required UDP ports. The output of the **debug radius authentication** command, shown in the following output, includes the attributes that are sent to the RADIUS host:

```
switch# debug radius authentication
Sep  5 10:41:42.779: RADIUS/ENCODE(0000010B):Orig. component type = Dot1X
Sep  5 10:41:42.779: RADIUS(0000010B): Config NAS IP: 0.0.0.0
Sep  5 10:41:42.779: RADIUS(0000010B): Config NAS IPv6: ::
Sep  5 10:41:42.787: RADIUS/ENCODE(0000010B): acct_session_id: 242
Sep  5 10:41:42.787: RADIUS(0000010B): sending
Sep  5 10:41:42.787: RADIUS/ENCODE: Best Local IP-Address 10.10.2.2 for Radius-Server
10.10.2.20
Sep  5 10:41:42.787: RADIUS(0000010B): Sending a IPv4 Radius Packet
Sep  5 10:41:42.787: RADIUS(0000010B): Send Access-Request to 10.10.2.20:1812 id
1645/132,len 233
Sep  5 10:41:42.787: RADIUS:  authenticator 63 01 20 5F 59 73 E6 A9 - 37 BE B0 6E F9
D7 9E 85
Sep  5 10:41:42.787: RADIUS:  User-Name           [1]   9   "student"
Sep  5 10:41:42.787: RADIUS:  Service-
Type        [6]   6   Framed                  [2]
Sep  5 10:41:42.787: RADIUS:  Vendor, Cisco       [26]  27
Sep  5 10:41:42.787: RADIUS:   Cisco AVpair       [1]   21  "service-type=Framed"
Sep  5 10:41:42.787: RADIUS:  Framed-IP-Address   [8]   6   10.10.9.16
Sep  5 10:41:42.787: RADIUS:  Framed-MTU          [12]  6   1500
Sep  5 10:41:42.787: RADIUS:  Called-Station-Id   [30]  19  "AC-F2-C5-5B-FC-01"
Sep  5 10:41:42.787: RADIUS:  Calling-Station-Id  [31]  19  "A0-36-9F-1A-3B-B1"
Sep  5 10:41:42.787: RADIUS:  EAP-Message         [79]  14
Sep  5 10:41:42.787: RADIUS:   02 01 00 0C 01 73 74 75 64 65 6E
74          [ student]
Sep  5 10:41:42.787: RADIUS:  Message-Authenticato[80]  18
Sep  5 10:41:42.787: RADIUS:   7E D3 F0 5E 17 02 9E 6G 3G 6F 03 A7 D9 6G 51
C0          [ ~^f6ofQ]
Sep  5 10:41:42.787: RADIUS:  EAP-Key-Name        [102] 2   *
Sep  5 10:41:42.787: RADIUS:  Vendor, Cisco       [26]  49
Sep  5 10:41:42.787: RADIUS:   Cisco AVpair       [1]   43  "audit-session-
id=0A0A0202000000B505675F78"
Sep  5 10:41:42.787: RADIUS:  NAS-Port-Type
[61]  6   Ethernet                [15]
Sep  5 10:41:42.787: RADIUS:  NAS-Port            [5]   6   50001
Sep  5 10:41:42.787: RADIUS:  NAS-Port-Id         [87]  20  "GigabitEthernet0/1"
Sep  5 10:41:42.787: RADIUS:  NAS-IP-Address      [4]   6   10.10.2.2
Sep  5 10:41:42.787: RADIUS(0000010B): Started 5 sec timeout
Sep  5 10:41:47.820: RADIUS(0000010B): Request timed out!
Sep  5 10:41:47.820: %RADIUS-4-RADIUS_DEAD: RADIUS server 10.10.2.20:1812,1813 is not
responding.
Sep  5 10:42:20.946: %DOT1X-5-FAIL: Authentication failed for client (a036.9f1a.3bb1)
on Interface Gi0/1 AuditSessionID 0A0A0202000000B505675F78
Sep  5 10:42:20.946: %AUTHMGR-7-RESULT: Authentication result 'server dead' from
'dot1x' for client (a036.9f1a.3bb1) on Interface Gi0/1 AuditSessionID
0A0A0202000000B505675F78
Sep  5 10:42:20.946: %AUTHMGR-5-FAIL: Authorization failed or unapplied for client
(a036.9f1a.3bb1) on Interface Gi0/1 AuditSessionID 0A0A0202000000B505675F78
```


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

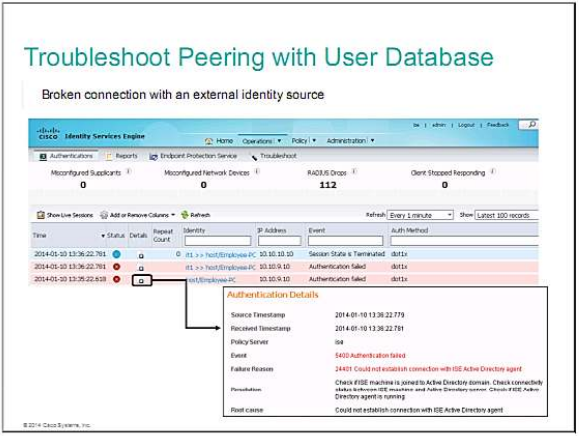


On the RADIUS server side, you may or may not see any authentication attempts. In this example, Cisco ISE acts as the RADIUS server. ISE has the NAD defined in its configuration, but the shared key is incorrect. The Cisco ISE is receiving authentication attempts from a valid NAD and you can see the authentication failures in the live authentications displayed in the **Operations > Authentications** page. If the NAD was not defined on the ISE, or IP connectivity failed, you would not see any failures on this page.

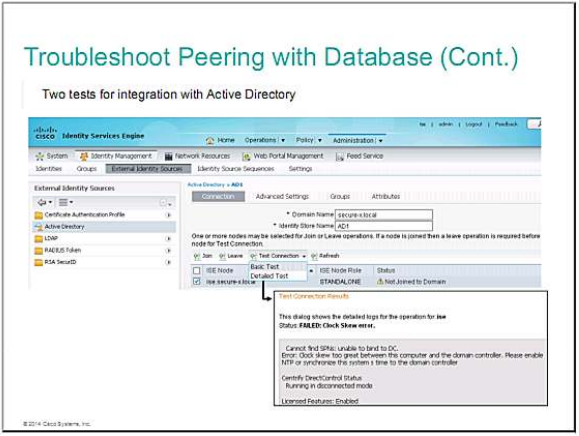
For each authentication event, you can click the **Details** icon to generate a details report. From this you can examine additional detailed information. When the event is a failure, it provide a failure reason as well as resolution guidance.

Troubleshoot Peering with User Database

This topic describes how to troubleshoot peering with the back-end user database.



Authentication failures can result from peering problems between the Cisco Identity Services Engine and the back-end user database. When you see failed authentication attempts in the Cisco ISE authentication page, you can click the Details icon and investigate the reason. In this case, you see that the Active Directory operation has failed because of an unspecified error in the Cisco ISE. You should check the status of the Active Directory integration.

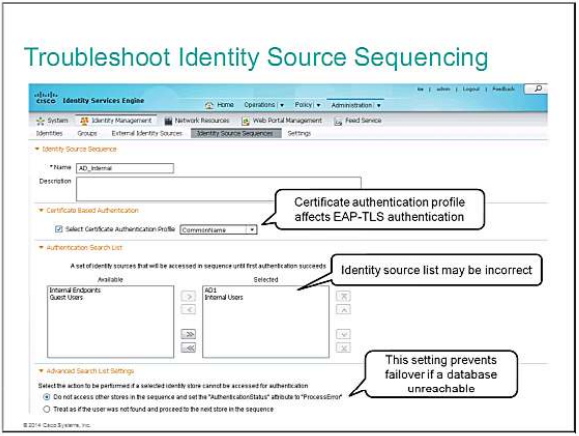


https://t.me/learningnets
© 2014 Cisco Systems, Inc.

You can check the status of the Active Directory integration by choosing **Administration > Identity Management > External Identity Sources > Active Directory**. In this case it is immediately apparent that the status is incorrect. Instead of "Connected," Cisco Identity Services Engine reports "Joined to Domain but Disconnected." From here you can test the connection to Active Directory. ISE offers two test methods: Basic and Detailed. Running the detailed test will provide the most information. In this case, the connection failure is caused by a time skew between ISE and Active Directory. In an Active Directory integration, the time skew must not be larger than a few minutes. You should make sure that NTP is used and is operational to avoid time synchronization issues.

Troubleshoot Identity Source Sequencing

This topic describes how to troubleshoot identity source sequencing.

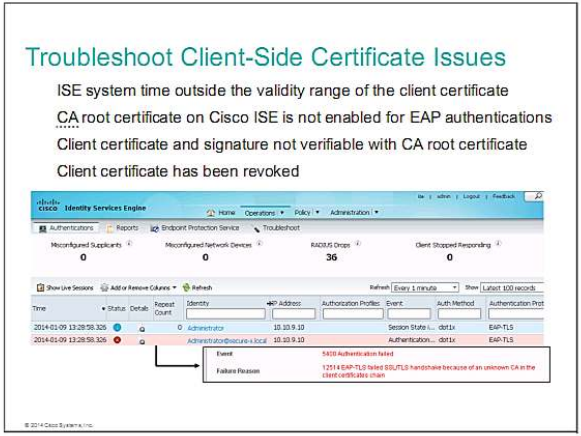


Cisco Identity Services Engine uses identity source sequences to allow multiple authentication sources to be queried in sequential order. It is possible for there to be configuration errors associated with a single source, such as an incorrect certificate authentication profile. There can also be issues with the sequence such as improper identity source order, or an undesired failover setting defining what to do in case a given source in the sequence is unavailable.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Troubleshoot Client-Side Certificate Issues

This topic describes how to troubleshoot client-side certificate issues.



Authentication failures can be caused by problems related to client-side certificate authentication. A client certificate is used in EAP-TLS authentication and other types of authentication. Potential issues include the following:

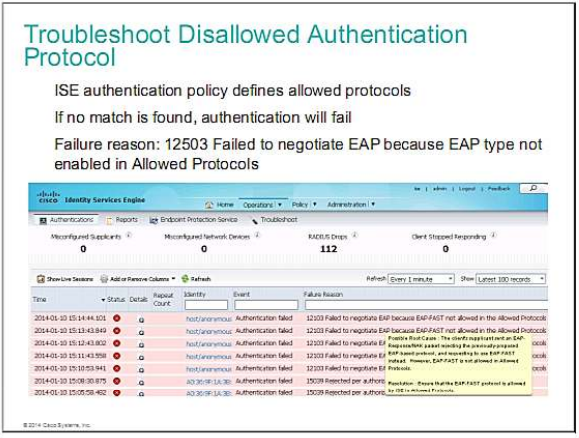
- The current system time on the Cisco Identity Services Engine may be outside the validity range of the client certificate.
- The CA root certificate in the Cisco ISE certificate store may not be enabled for EAP authentications.
- The client certificate and signature may not be verifiable using the CA root certificates.
- The client certificate may have been revoked.

In this example, you see a failed authentication attempt. The EAP-TLS handshake failed because of an unknown CA in the client certificates chain. You can view more detailed information if you click the **Details** icon.

https://t.me/learningnets

Troubleshoot Disallowed Authentication Protocol

This topic describes how to troubleshoot disallowed authentication protocol issues.

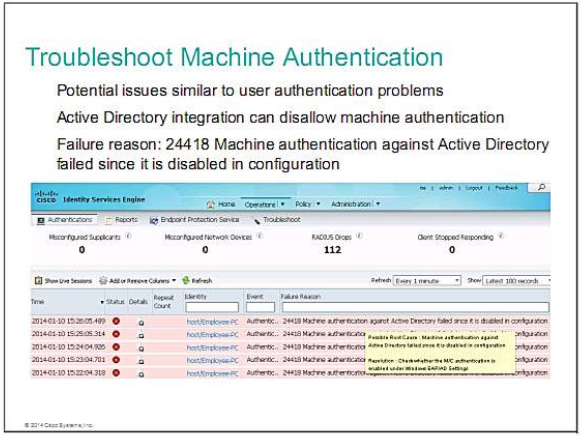


IEEE 802.1x authentication will fail if the client authentication protocol is not allowed by the Cisco Identity Services Engine. The ISE defines the allowed authentication protocols in each authentication rule. The authentication will fail in case of a mismatch. Authentication policy rules are defined under **Policy > Authentication**.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Troubleshoot Machine Authentication

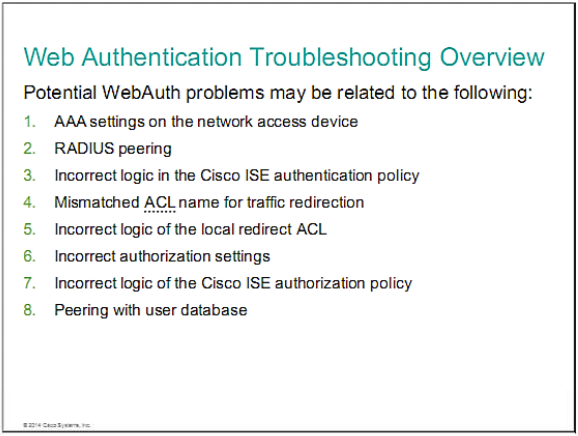
This topic describes the troubleshooting of machine authentication.



Machine authentication problems are similar to user authentication issues and can have various causes. A special case for failing machine authentication can be related to an integration setting with external identity databases. You can disallow external machine authentication. In the example that is shown in the figure, the Cisco Identity Services Engine has been configured to block machine authentication attempts against the Active Directory.

Web Authentication Troubleshooting Overview

This topic describes the troubleshooting of central WebAuth.

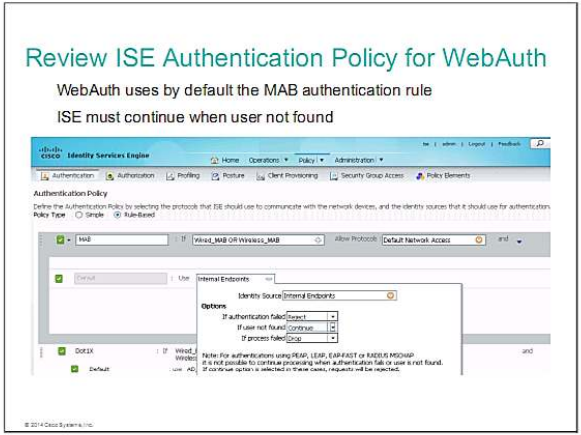


Central WebAuth depends on the MAB functionality. It will fail with incorrect AAA settings on the NAD or broken RADIUS peering. It relies on the authentication policy to continue if the MAB rule fails. A potential problem of the Central WebAuth is that the redirect ACL is configured on the NAD, and it is referenced by the authorization profile on the Cisco Identity Services Engine. A potential name mismatch, an error in the redirect ACL, or a misconfiguration of the authorization profile will cause the WebAuth redirection to fail. Other problems can be related to the logic of the Cisco ISE authorization policy, where the authorization rules for unauthenticated and authenticated users and guests must be defined in the correct order. Central WebAuth can be used for employee access and therefore depends on the peering with the back-end user database.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Review ISE Authentication Policy for WebAuth

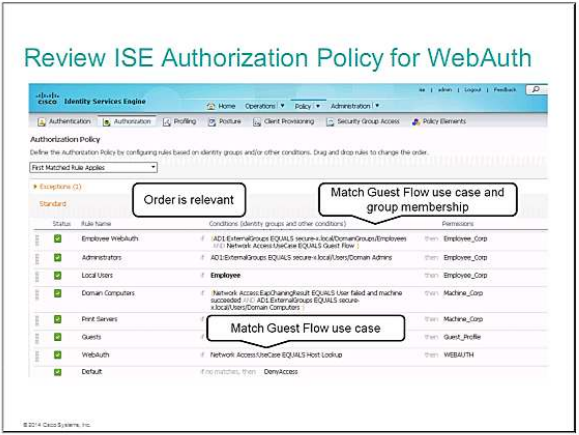
This topic describes the Cisco Identity Services Engine authentication policy settings that are required for WebAuth.



Central WebAuth requires that the MAB authentication rule on Cisco ISE is configured for fail-open operation if the endpoint MAC address is not found in the endpoint database. This approach effectively allows the authorization policy to take over the decision-making process for this endpoint. The Cisco ISE authorization must have several rules.

Review ISE Authorization Policy for WebAuth

This topic describes the Cisco Identity Services Engine authentication policy settings that are required for WebAuth.



This figure illustrates a basic authorization policy that is required for Central WebAuth and guest access. It does not show the authorization rules at the top of the authorization policy. The rules at the top are used to define permissions for the various users and endpoints that access via 802.1X and are profiled. The two rules required for the WebAuth operation are Employee WebAuth, shown at the top, and WebAuth, the second last.

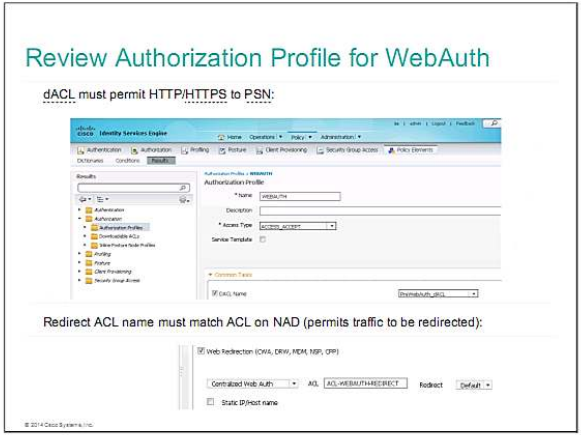
The Employee WebAuth rule defines the authorization profile used for the employees who authenticate using WebAuth. The condition for the rule is the appropriate group membership and Network Access: Use Case Equals Host Lookup. The Network Access Use Case Host Lookup is the method used for MAB.

The second to last rule, WebAuth, matches the network access use case (Host Lookup) and pushes the authorization profile (WEBAUTH) to redirect traffic for WebAuth. This rule is only effective if the MAB authentication rule is configured to continue if the user is not found.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Review Authorization Profile for WebAuth

This topic describes the Cisco Identity Services Engine authorization profile that is used for traffic redirection.

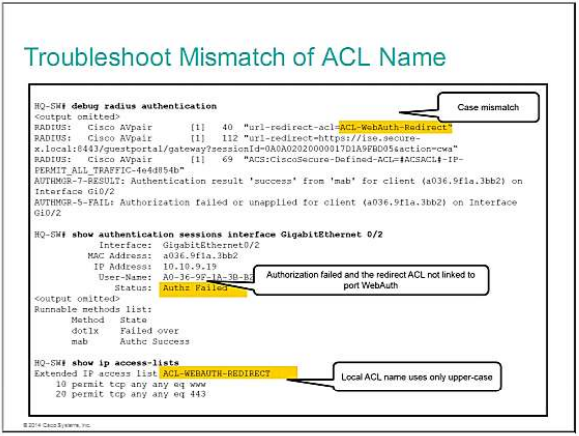


Central WebAuth requires an authorization profile on Cisco ISE that is used to redirect HTTP and HTTPS traffic to WebAuth. An example of this profile is shown in the figure. The profile references an ACL that must be configured on the NAD. The ACL defines the traffic that will be redirected to the central WebAuth portal. If the NAD is a Cisco switch, the local ACL must permit HTTP and HTTPS traffic, which will be redirected to WebAuth.

Potential pitfalls include a mismatch in the ACL name, and incorrect permit and deny definitions in the local ACL.

Troubleshoot Mismatch of ACL Name

This topic describes how to troubleshoot a mismatch of the ACL name.



A potential pitfall with central WebAuth is a mismatch between the name of the redirect ACL on the network access device and in the authorization profile on Cisco Identity Services Engine. You can troubleshoot such a problem by debugging the RADIUS authentication on the network access device and verifying the authentication results on the port. The following output displays the full output of the **debug radius authentication** command in a scenario where the names have inconsistent lower- and uppercase letters.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

```
HQ-SW# debug radius authentication
Sep  9 13:35:40.969: %DOT1X-5-FAIL: Authentication failed for client (a036.9f1a.3bb2)
on Interface Gi0/2 AuditSessionID 0A0A02020000017D1A9FBD05
Sep  9 13:35:40.969: %AUTHMGR-7-RESULT: Authentication result 'no-response' from
'dot1x' for client (a036.9f1a.3bb2) on Interface Gi0/2 AuditSessionID
0A0A02020000017D1A9FBD05
Sep  9 13:35:40.969: %AUTHMGR-7-FAILOVER: Failing over from 'dot1x' for client
(a036.9f1a.3bb2) on Interface Gi0/2 AuditSessionID 0A0A02020000017D1A9FBD05
Sep  9 13:35:40.969: %AUTHMGR-5-START: Starting 'mab' for client (a036.9f1a.3bb2) on
Interface Gi0/2 AuditSessionID 0A0A02020000017D1A9FBD05
Sep  9 13:35:40.969: RADIUS/ENCODE(000001D8):Orig. component type = Dot1X
Sep  9 13:35:40.969: RADIUS(000001D8): Config NAS IP: 0.0.0.0
Sep  9 13:35:40.969: RADIUS(000001D8): Config NAS IPv6: ::
Sep  9 13:35:40.969: RADIUS/ENCODE(000001D8): acct_session_id: 447
Sep  9 13:35:40.969: RADIUS(000001D8): sending
Sep  9 13:35:40.969: RADIUS/ENCODE: Best Local IP-Address 10.10.2.2 for Radius-Server
10.10.2.20
Sep  9 13:35:40.969: RADIUS(000001D8): Sending a IPv4 Radius Packet
Sep  9 13:35:40.969: RADIUS(000001D8): Send Access-Request to 10.10.2.20:1812 id
1645/94,len 246
Sep  9 13:35:40.969: RADIUS:  authenticator 56 B6 96 54 70 8B 70 16 - 58 19 FA 52 2B
5C 80 3F
Sep  9 13:35:40.977: RADIUS:  User-Name           [1]   14  "a0369f1a3bb2"
Sep  9 13:35:40.977: RADIUS:  User-Password       [2]   18  *
Sep  9 13:35:40.977: RADIUS:  Service-Type        [6]   6   Call Check
[10]
Sep  9 13:35:40.977: RADIUS:  Vendor, Cisco       [26]  31
Sep  9 13:35:40.977: RADIUS:   Cisco AVpair       [1]   25  "service-type=Call Check"
Sep  9 13:35:40.977: RADIUS:  Framed-IP-Address   [8]   6   10.10.9.19
Sep  9 13:35:40.977: RADIUS:  Framed-MTU          [12]  6   1500
Sep  9 13:35:40.977: RADIUS:  Called-Station-Id   [30]  19  "AC-F2-C5-5B-FC-02"
Sep  9 13:35:40.977: RADIUS:  Calling-Station-Id  [31]  19  "A0-36-9F-1A-3B-B2"
Sep  9 13:35:40.977: RADIUS:  Message-Authenticator[80]  18
Sep  9 13:35:40.977: RADIUS:   64 27 D1 A3 D0 CC 1B 62 3B A3 DE 70 D6 2F 45
04           [ d'b;p/E]
Sep  9 13:35:40.977: RADIUS:  EAP-Key-Name        [102] 2   *
Sep  9 13:35:40.977: RADIUS:  Vendor, Cisco       [26]  49
Sep  9 13:35:40.977: RADIUS:   Cisco AVpair       [1]   43  "audit-session-
id=0A0A02020000017D1A9FBD05"
Sep  9 13:35:40.977: RADIUS:  NAS-Port-Type
[61]  6   Ethernet                [15]
Sep  9 13:35:40.977: RADIUS:  NAS-Port            [5]   6   50002
Sep  9 13:35:40.977: RADIUS:  NAS-Port-Id         [87]  20  "GigabitEthernet0/2"
Sep  9 13:35:40.977: RADIUS:  NAS-IP-Address      [4]   6   10.10.2.2
Sep  9 13:35:40.977: RADIUS(000001D8): Started 5 sec timeout
Sep  9 13:35:41.019: RADIUS: Received from id 1645/94 10.10.2.20:1812, Access-Accept,
len 391
Sep  9 13:35:41.019: RADIUS:  authenticator A5 4A 0C 60 D8 0F 08 63 - 24 3B 02 F9 06
D0 2F 1A
Sep  9 13:35:41.019: RADIUS:  User-Name           [1]   19  "A0-36-9F-1A-3B-B2"
Sep  9 13:35:41.019: RADIUS:  State               [24]  40
Sep  9 13:35:41.019: RADIUS:   52 65 61 75 74 68 53 65 73 73 69 6F 6E 3A 30
41  [ReauthSession:0A]
Sep  9 13:35:41.019: RADIUS:   30 41 30 32 30 32 30 30 30 30 30 31 37 44 31
41  [0A02020000017D1A]
Sep  9 13:35:41.019: RADIUS:   39 46 42 44 30 35            [ 9FBD05]
Sep  9 13:35:41.019: RADIUS:  Class               [25]  49
Sep  9 13:35:41.028: RADIUS:   43 41 43 53 3A 30 41 30 41 30 32 30 32 30 30 30  [CACS:
0A0A0202000]
Sep  9 13:35:41.028: RADIUS:   30 30 31 37 44 31 41 39 46 42 44 30 35 3A 69
73  [0017D1A9FBD05:is]
```


https://t.me/learningnets

```
Sep  9 13:35:41.028: RADIUS:   65 2F 31 36 37 37 38 32 32 37 38 2F 36 31 30   [ e/
167782278/610]
Sep  9 13:35:41.028: RADIUS:  Termination-Action  [29]  6   1
Sep  9 13:35:41.028: RADIUS:  Message-Authenticato[80]  18
Sep  9 13:35:41.028: RADIUS:   13 FB 55 86 75 A8 3C 13 B3 E7 73 23 02 5A EC
6C           [ Uu<s#Zl]
Sep  9 13:35:41.028: RADIUS:  Vendor, Cisco       [26]  46
Sep  9 13:35:41.028: RADIUS:   Cisco AVpair       [1]   40  "url-redirect-acl=ACL-
WebAuth-Redirect"
Sep  9 13:35:41.028: RADIUS:  Vendor, Cisco       [26]  118
Sep  9 13:35:41.028: RADIUS:   Cisco AVpair       [1]   112 "url-redirect=https://
ise.secure-x.local:8443/guestportal/gateway?
sessionId=0A0A02020000017D1A9FBD05&action=cwa"
Sep  9 13:35:41.028: RADIUS:  Vendor, Cisco       [26]  75
Sep  9 13:35:41.028: RADIUS:   Cisco AVpair       [1]   69  "ACS:CiscoSecure-Defined-
ACL=#ACSACL#-IP-PERMIT_ALL_TRAFFIC-4e4d854b"
Sep  9 13:35:41.028: RADIUS(000001D8): Received from id 1645/94
Sep  9 13:35:41.028: %MAB-5-SUCCESS: Authentication successful for client (a036.9f1a.
3bb2) on Interface Gi0/2 AuditSessionID 0A0A02020000017D1A9FBD05
Sep  9 13:35:41.028: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab'
for client (a036.9f1a.3bb2) on Interface Gi0/2 AuditSessionID 0A0A02020000017D1A9FBD05
Sep  9 13:35:41.053: %AUTHMGR-5-FAIL: Authorization failed or unapplied for client
(a036.9f1a.3bb2) on Interface Gi0/2 AuditSessionID 0A0A02020000017D1A9FBD05
Sep  9 13:35:41.992: %AUTHMGR-5-SUCCESS: Authorization succeeded for client
(a036.9f1a.3bb2) on Interface Gi0/2 AuditSessionID 0A0A02020000017D1A9FBD05
Sep  9 13:35:57.427: %DOT1X-5-FAIL: Authentication failed for client (a036.9f1a.3bb1)
on Interface Gi0/1 AuditSessionID 0A0A02020000012A0C8A999D
Sep  9 13:35:57.427: %AUTHMGR-7-RESULT: Authentication result 'no-response' from
'dot1x' for client (a036.9f1a.3bb1) on Interface Gi0/1 AuditSessionID
0A0A02020000012A0C8A999D
Sep  9 13:35:57.427: %AUTHMGR-7-FAILOVER: Failing over from 'dot1x' for client
(a036.9f1a.3bb1) on Interface Gi0/1 AuditSessionID 0A0A02020000012A0C8A999D
Sep  9 13:35:57.427: %AUTHMGR-7-NOMOREMETHODS: Exhausted all authentication methods
for client (a036.9f1a.3bb1) on Interface Gi0/1 AuditSessionID 0A0A02020000012A0C8A999D
Sep  9 13:35:57.427: %AUTHMGR-5-FAIL: Authorization failed or unapplied for client
(a036.9f1a.3bb1) on Interface Gi0/1 AuditSessionID 0A0A02020000012A0C8A999D
```

The authentication results on the access interface are as follows:

```
HQ-SW# show authentication sessions interface gigabitEthernet 0/2
            Interface:  GigabitEthernet0/2
          MAC Address:  a036.9f1a.3bb2
           IP Address:  10.10.9.19
            User-Name:  A0-36-9F-1A-3B-B2
               Status:  Authz Failed
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
         Vlan Policy:  N/A
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A0A02020000017D1A9FBD05
      Acct Session ID:  0x000001BF
               Handle:  0xCD00017E
Runnable methods list:
       Method   State
       dot1x    Failed over
       mab      Authc Success
```


© 2014 Cisco Systems, Inc.
https://t.me/learningnets

If you check the ACL names on the switch, you will find a mismatch:

```
HQ-SW# show ip access-lists
Extended IP access list ACL-WEBAUTH-REDIRECT
    10 permit tcp any any eq www
    20 permit tcp any any eq 443
```

When you correct the ACL name, you will find that the authorization profile is applied as expected:

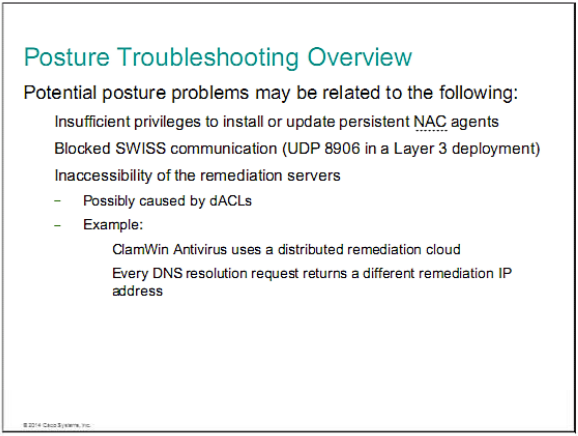
```
HQ-SW# show authentication session interface gigabit 0/2
            Interface:  GigabitEthernet0/2
          MAC Address:  a036.9f1a.3bb2
           IP Address:  10.10.9.19
            User-Name:  A0-36-9F-1A-3B-B2
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-4e4d854b
     URL Redirect ACL:  ACL-WEBAUTH-REDIRECT
        URL Redirect:  https://ise.secure-x.local:8443/guestportal/gateway?
sessionId=0A0A02020000017E1AC53B8E&action=cwa
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A0A02020000017E1AC53B8E
      Acct Session ID:  0x000001C0
              Handle:  0x6800017F
Runnable methods list:
       Method   State
       dot1x    Failed over
       mab      Authc Success
```

The user is then redirected to WebAuth, and when authenticated successfully and all other settings are correct, the port will be authorized with the user or guest profile.

https://t.me/learningnets

Posture Troubleshooting Overview

This topic describes how to troubleshoot the posture service.



The posture service relies on persistent or nonpersistent NAC agents. Persistent NAC agents, which are available for Windows and Mac computers, are typically used on managed devices. Persistent agents can be installed from the Web browser or using the MSI package. You must have administrator rights to install or update a persistent agent.

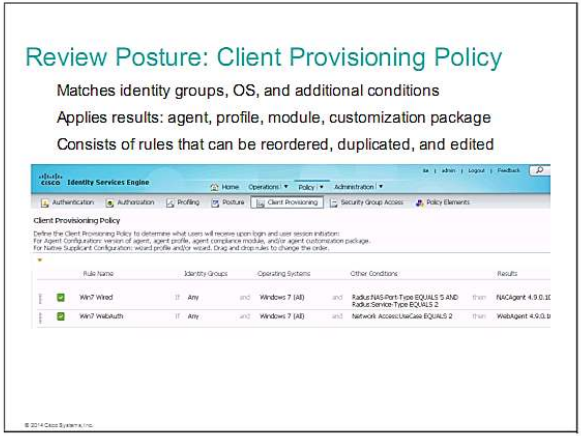
The SWISS protocol is a stateless request-response protocol that allows NAC agents that are running on managed clients, to retrieve configuration and operational information from the Cisco Identity Services Engine. The NAC agent connects to the Cisco ISE server by sending out SWISS unicast packets on UDP port 8905 in a Layer 2 deployment and on UDP port 8906 in a Layer 3 deployment. If the SWISS communication is filtered, the posture service will not function properly.

Another potential pitfall is when clients cannot access the remediation servers. This may be caused by an overly strict dACL defined for client provisioning on ISE. Some antisypware and antivirus programs, such as the ClamWin antivirus, use a a distributed remediation cloud. The cloud consists of numerous hosts that serve the software and definition updates. Every time the ClamWin agent resolves the hostname of the remediation server, it gets a different IP address. This situation is very difficult to handle with static dACLs for non-compliant endpoints.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Review Posture: Client Provisioning Policy

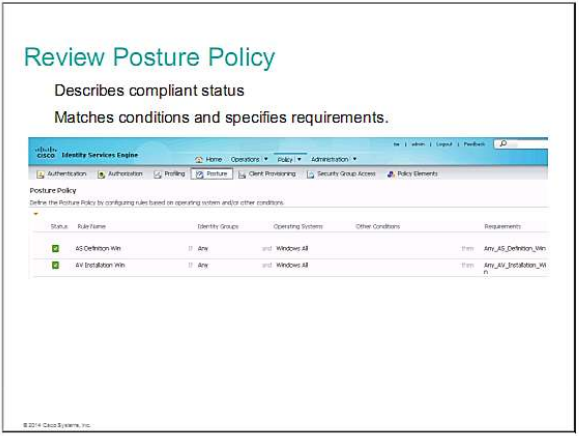
This topic describes the use of the client provisioning policy in the posture service.



The Client Provisioning Policy is an essential component of the posture service. It defines the agent software that is used to obtain the posture information for the given endpoint type. In this example, a persistent NAC agent should be provisioned on Windows endpoints that authenticate using IEEE 802.1x, and a web agent should be provisioned on Windows endpoints that use WebAuth.

Review Posture Policy

This topic describes the Cisco Identity Services Engine posture policy.



A posture policy defines the technical requirements that define compliant status. For example, the posture policy may define a compliant endpoint as a client machine with up-to-date antivirus software. A posture policy consists of one or more rules, and each rule is identified by a name and configured to match one or more conditions.

The posture policy is differentiated from other policy types by the requirements definition. The requirements are written as an expression: "Requirement for OS met if posture condition, else remediation'"

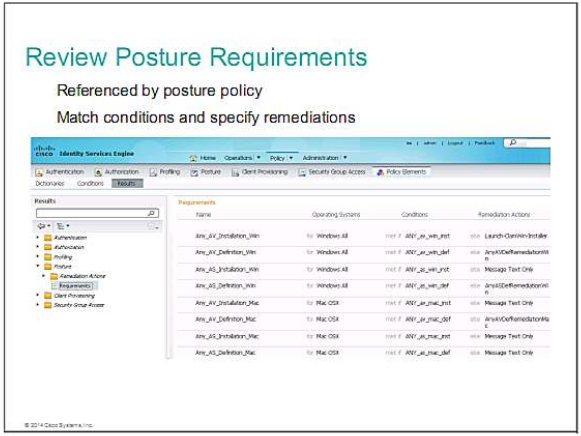
The posture condition can be specified as a single or compound condition. Several types of posture attributes may be evaluated: file, registry, service, application, regular compound condition, antivirus, and antispyware.

The posture policy rules match conditions and specify the posture requirements.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Review Posture Requirements

This topic describes the Cisco Identity Services Engine posture requirements.



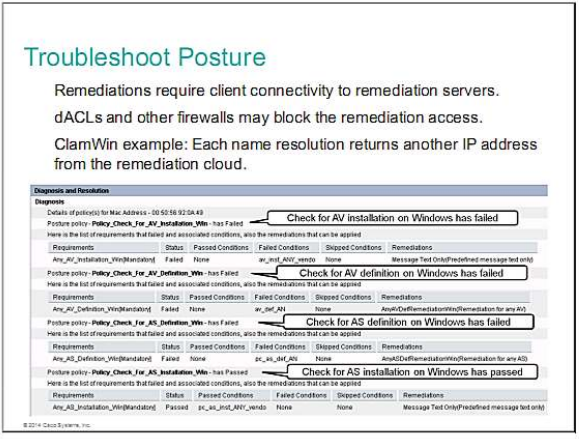
The posture policy rules match conditions and specify the posture requirements. The posture requirements specify the attributes of a "healthy" state for an endpoint. Eight built-in conditions check for the presence of any antivirus and antispyware software on Windows or OS-X endpoints, respectively. They provide a good starting point for defining a policy that requires antivirus and antispyware software to be installed on the client computers without having to specify the details of the software vendor and signature database. The requirements match the conditions and define the remediations to be taken when the conditions are not met.

The remediation defines the action that must be performed if the posture condition is not met. The goal is to allow the endpoint to achieve compliant status. The remediation actions can be of different types: antispyware remediation, antivirus remediation, file remediation, launch program remediation, link remediation, Windows Server Update Services remediation, Windows Update remediation.

To effectively troubleshoot the posture service, you should understand how the posture policy, requirements, and remediation actions interoperate.

Troubleshoot Posture

This topic describes how to troubleshoot posture.



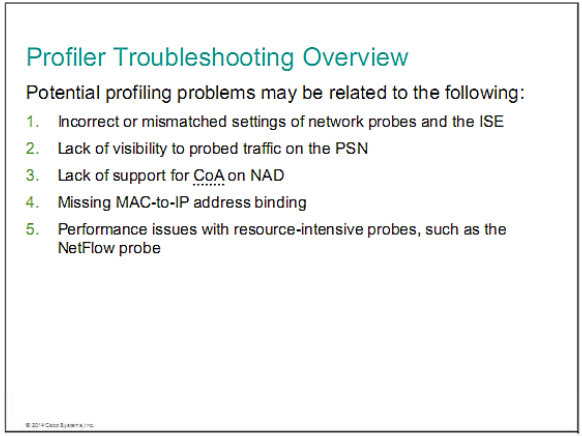
When you experience problems with the posture service, you should validate the overall posture design. In this scenario, the antivirus installation remediation has been modified to install ClamWin antivirus. Despite correct settings, when the NAC agent is installed on the endpoint, it reports noncompliant status.

In this situation, the reason for the failure is not related to a problem with the posture configuration, but with the reachabillity to the remediation resources. The endpoints require connectivity to the remediation servers. If dACLs and other firewalls block access to remediation, the remediation is bound to fail. The ClamWin antivirus, for example uses a distributed cloud of remediation resources. Every time a client resolves the name of the remediation server, it gets a different IP address. This situation is difficult to handle with an dACL or any other network ACL.

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Case Study: Troubleshoot Profiling

This topic describes how to troubleshoot the profiler service.



The profiler service collects an attribute or a set of attributes of all the endpoints on your network and classifies them according to their profiles. The Cisco Identity Services Engine uses profiler probes to collect an attribute or a set of attributes from an endpoint on your network. The probe allows you to create or update endpoints with their matched profile in the database. Some probes interoperate with agents in the network devices, and if they are misconfigured, the profiler cannot obtain the endpoint attributes. Similarly, probes which interrogate particular network traffic won't function if they are not exposed to that traffic. For example, the DHCP probe requires the use of ip helper features on routing devices to forward DHCP requests to the PSN running the DHCP probe.

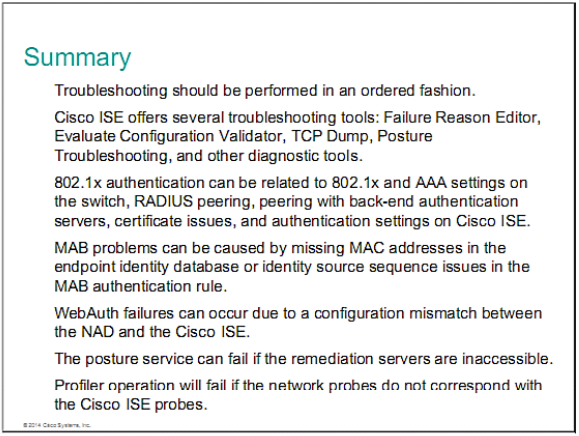
CoA is not absolutely necessary for profiler service operation. If you have some NADs in your network that do not support CoA, you may still deploy the profiler service for endpoint monitoring. In this case, the profiler service can be used to establish a learned inventory. When CoA is supported on the NADs, you can use the profiler service to push tailored authorization policies to the endpoints. When the endpoint authenticates, it receives a restrictive authorization policy that enables the profiling process to complete. Once the endpoint profile is ascertained, an authorization policy that considers the endpoint profile man be assigned. ISE then sends a CoA to the NAD, instructing the NAD to apply an adjusted policy. Clearly, if you expect the authorization policy to reflect the endpoint profile, a lack of CoA support will cause an inadequate authorization policy to be enforced on the endpoints.

Endpoint profiling in Cisco ISE identifies each endpoint on your network, and groups the identified endpoints according to their profiles. The MAC address is used for the unique identifier of each endpoint. Some probes work only at the IP layer. Data collected from those probes can only be incorporated into the endpoint's collected attributes if the MAC to IP address binding already exists.

Finally, you may experience performance issues when deploying resource-intensive probes. The probes consume different amounts of resources depending on their type. For example, the NetFlow probe is more resource-intensive than a DNS probe.

Summary

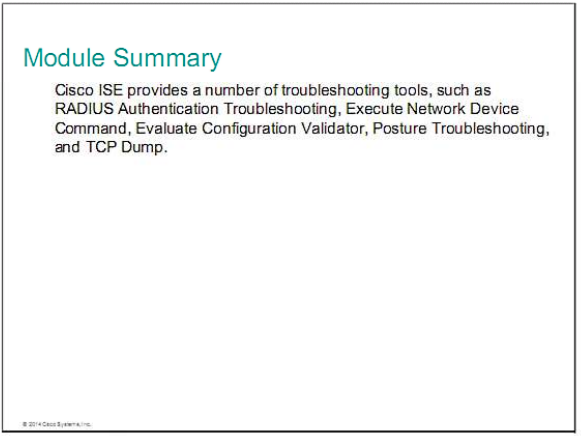
This topic summarizes the key points that were discussed in this lesson.



© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Module Summary

This topic summarizes the key points that were discussed in this module.



References

For additional information refer to this resource:

Cisco Identity Services Engine User Guide

https://t.me/learningnets

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Module Self-Check

Questions

Use the questions here to review what you learned in this module. The correct answers and solutions are found in the Module Self-Check Answer Key.

1. Which tool can you help identify the reason why an endpoint IP address does not show in the ISE authentication page? (Source: Troubleshooting Network Access Controls)

   A. RADIUS Authentication Troubleshooting
   B. Posture Troubleshooting
   C. Evaluate Configuration Validator
   D. TCP Dump
   E. Execute Network Device Command

2. Which two ISE configuration elements should you check when troubleshooting client certificate authentication problems? (Choose two.) (Source: Troubleshooting Network Access Controls)

   A. Settings of the CA root certificate
   B. Settings of the client certificate
   C. Identity source sequence
   D. Certificate identity store

3. Which two statements correctly describe the use of ACLs in Central WebAuth? (Choose two.) (Source: Troubleshooting Network Access Controls)

   A. Two dACLs are pushed to the NAD
   B. Two ACL names are pushed to the NAD
   C. One dACL and one ACL name are pushed to the NAD
   D. The ISE pushes the redirect ACL name instead of the redirect ACL to accommodate varying redirect logic on different NAD types
   E. The dACL used in the Central WebAuth authorization profile permits traffic to be redirected

https://t.me/learningnets

Answer Key

1. C

2. A, C

3. C, D

© 2014 Cisco Systems, Inc.
https://t.me/learningnets

Glossary

Term	Definition
AAA	authentication, authorization, and accounting. Pronounced "triple a."
ACE	access control entry.
ACL	access control list. A list kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).
AD	Active Directory
AD	advertised distance.
AES	Advanced Encryption Standard.
AP	access point. A node on a wireless network that allows other wireless devices to connect to a wired network.
AS	Anti-Spyware
ASA	adaptive security appliance
ASDM	Cisco Adaptive Security Device Manager. Delivers security management and monitoring through an intuitive, easy-to-use, web-based management interface.
ASIC	application-specific integrated circuit.
AUP	acceptable use policy. Many transit networks have policies that restrict the use to which the network can be put. The enforcement of AUPs varies with the network.
AV	attribute-value
AV	attribute values
AV	anti-virus
BYOD	bring your own device
CA	certification authority. Entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate.
CDP	CRL distribution point.
CHAP	Challenge Handshake Authentication Protocol. Security feature supported on lines using PPP encapsulation that prevents unauthorized access. CHAP does not itself prevent unauthorized access, but merely identifies the remote end. The router or access server then determines whether that user is allowed access.
CISP	Client Information Signaling Protocol
CLI	command-line interface. An interface that allows the user to interact with the operating system by entering commands and optional arguments. The UNIX operating system and DOS provide CLIs.

https://t.me/learningnets

Term	Definition
CoA	Change of Authorization.
CPP	Client Provisioning Portal
CPU	central processing unit. The hardware within a computer system or smartphone that carries out the instructions of a computer program by performing the basic arithmetical, logical, and input-output operations of the system.
CSR	certificate signing request.
CSV	comma separated values. Commonly used no-frills text file format used for import from and import to spreadsheets and SQL databases.
CTL	Certificate Trust List
dACL	downloadable access control list.
DGT	destination group tag
DHCP	Dynamic Host Configuration Protocol. Provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.
DNS	Domain Name System. System used on the Internet for translating names of network nodes into addresses.
DoS	denial of service. An intentional or unintentional attack on a device that makes the resource unavailable to perform its normal function.
EAP	Extensible Authentication Protocol. Framework that supports multiple, optional authentication mechanisms for PPP, including cleartext passwords, challenge-response, and arbitrary dialog sequences.
EAP-FAST	Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling.
EAP-GTC	Protected Extensible Authentication Protocol-Generic Token Card.
EAP-MD5	Extensible Authentication Protocol-Message Digest 5.
EAP-MSCHAPv2	Microsoft CHAP version 2 EAP
EAPOL	Extensible Authentication Protocol over LAN
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
Ethernet	Baseband LAN specification invented by Xerox Corporation and developed jointly by Xerox, Intel, and Digital Equipment Corporation. Ethernet networks use CSMA/CD and run over a variety of cable types at 10 Mb/s. Ethernet is similar to the IEEE 802.3 series of standards.
FQDN	fully qualified domain name. FQDN is the full name of a system, rather than just its host name. For example, aldebaran is a host name, and aldebaran.interop.com is an FQDN.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Term	Definition
FTP	File Transfer Protocol. Application protocol, part of the TCP/IP protocol stack, used for transferring files between network nodes. FTP is defined in RFC 959.
GCM	Galois Counter Mode.
GUI	graphical user interface. A user environment that uses pictorial as well as textual representations of the input and the output of applications and the hierarchical or other data structure in which information is stored. Such conventions as buttons, icons, and windows are typical, and many actions are performed using a pointing device (such as a mouse). Microsoft Windows and the Apple Macintosh are prominent examples of platforms using a GUI.
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol. Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing. Documented in RFC 792.
ICV	integrity check value.
IEEE	Institute of Electrical and Electronics Engineers. Professional organization whose activities include the development of communications and network standards. IEEE LAN standards are the predominant LAN standards today.
IETF	Internet Engineering Task Force. Task force consisting of over 80 working groups responsible for developing Internet standards. The IETF operates under the auspices of ISOC.
IP address	32-bit address assigned to hosts using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as 4 octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, and the host number is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and subnetwork information from the IP address. CIDR provides a new way of representing IP addresses and subnet masks. Also called an Internet address.
IPS	intrusion prevention system.
IPv4	IP version 4. Internet Protocol version 4 is the fourth version in the development of the IP and the first version of the protocol to be widely deployed. Along with IPv6, IPv4 is at the core of standards-based internetworking methods of the Internet. IPv4 is still used to route most traffic across the Internet. IPv4 is a connectionless protocol for use on packet-switched link layer networks (for example, Ethernet). It operates on a best-effort delivery model in that it does not guarantee delivery and does not assure proper sequencing or avoidance of duplicate delivery.

https://t.me/learningnets

Term	Definition
IPv6	IP version 6. Replacement for the current version of IP (version 4). IPv6 includes support for flow ID in the packet header, which can be used to identify flows. Formerly called IPng (next generation).
KDC	key distribution center
LAN	local-area network. High-speed, low-error data network covering a relatively small geographic area (up to a few thousand meters). LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area. LAN standards specify cabling and signaling at the physical and data link layers of the OSI model. Ethernet, FDDI, and Token Ring are widely used LAN technologies.
LDAP	Lightweight Directory Access Protocol. Protocol that provides access for management and browser applications that provide read/write interactive access to the X.500 Directory.
LDAPS	Lightweight Directory Access Protocol over Secure Sockets Layer/ Transport Layer Security
LEAP	Lightweight Extensible Authentication Protocol.
LLDP	Link Layer Discovery Protocol
MAB	MAC authentication bypass.
MAC	Media Access Control. Lower of the two sublayers of the data link layer defined by the IEEE. The MAC sublayer handles access to shared media, such as whether token passing or contention will be used.
MAC address	Standardized data link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network and to create and update routing tables and data structures. MAC addresses are 6 bytes long and are controlled by the IEEE. Also known as a hardware address, MAC layer address, and physical address.
MACsec	Media Access Control Security. MACsec encryption provides MAC-layer encryption over wired networks using OOB methods for encryption keying.
MA-L	MAC Address Block - Large
MDA	multidomain authentication.
MDM	Mobile Device Management
MKA	MACsec Key Agreement.
MMC	Microsoft Management Console
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol.
MSCHAPv2	Microsoft CHAP version 2
MSI	Macintosh Installer.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Term	Definition
MTU	maximum transmission unit. Maximum packet size, in bytes, that a particular interface can handle.
NAC	Network Admission Control.
NAD	network access device.
NAM	Network Access Manager
NAM	Network Analysis Module
NAS	network access server. Cisco platform (or collection of platforms, such as an AccessPath system) that interfaces between the packet world (for example, the Internet) and the circuit world (for example, the PSTN).
NAS	network-attached storage
NAT	Network Address Translation. Mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space. Also known as Network Address Translator.
NDAC	Network Device Admission Control
NEAT	Network Edge Access Topology
NetFlow	A feature of some routers that allows them to categorize incoming packets into flows. Because packets in a flow often can be treated in the same way, this classification can be used to bypass some of the work of the router and accelerate its switching operation.
NGFW	Next-Generation Firewall
NIC	network interface card. Board that provides network communication capabilities to and from a computer system. Also called an adapter.
NMS	network management system. System responsible for managing at least part of a network. An NMS is generally a reasonably powerful and well-equipped computer, such as an engineering workstation. NMSs communicate with agents to help keep track of network statistics and resources.
NTP	Network Time Protocol. Protocol built on top of TCP that ensures accurate local timekeeping with reference to radio and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.
OTP	one-time password
OUI	Organizational Unique Identifier. Three octets that are assigned by the IEEE in a block of 48-bit LAN addresses.
PAC	Protected Access Credentials.

https://t.me/learningnets

Term	Definition
PAP	Password Authentication Protocol. Authentication protocol that allows PPP peers to authenticate one another. The remote router attempting to connect to the local router is required to send an authentication request. Unlike CHAP, PAP passes the password and the host name or username in the clear (unencrypted). PAP does not itself prevent unauthorized access but merely identifies the remote end. The router or access server then determines whether that user is allowed access. PAP is supported only on PPP lines.
PEAP	Protected Extensible Authentication Protocol
PIN	places in the network
PKI	public-key infrastructure. System of CAs (and, optionally, RAs and other supporting servers and agents) that perform some set of certificate management, archive management, key management, and token management functions for a community of users in an application of asymmetric cryptography.
PSN	Policy Service Node
PSN	packet-switched network
QoS	quality of service. Measure of performance for a transmission system that reflects its transmission quality and service availability.
RADIUS	Remote Authentication Dial-In User Service. Database for authenticating modem and ISDN connections and for tracking connection time.
RBACL	Role Based ACL
RFC	Request for Comments. Document series that is used as the primary means for communicating information about the Internet. Some RFCs are designated by the IAB as Internet standards. Most RFCs document protocol specifications, such as Telnet and FTP, but some RFCs are humorous or historical. RFCs are available online from numerous sources.
RSA	Acronym stands for Rivest, Shamir, and Adleman, the inventors of the technique. Public-key cryptographic system that can be used for encryption and authentication.
SAN	Subject Alternative Name.
SAP	Security Association Protocol
SCEP	Simple Certificate Enrollment Protocol.
SGA	Security Group Access.
SGACL	security group access control list.
SGFW	Security Group Firewall
SGT	security group tag.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Term	Definition
SHA-1	Secure Hash Algorithm 1. Algorithm that takes a message of less than 264 bits in length and produces a 160-bit message digest. The large message digest provides security against brute-force collision and inversion attacks. SHA-1 [NIS94c] is a revision to SHA that was published in 1994.
SHA-256	Secure Hash Algorithm. SHA-256 is part of the SHA-2 set of cryptographic hash functions.
SMB	Server Message Block Protocol
SMS	short message service
SNMP	Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.
SPAN	Switched Port Analyzer. SPAN is a feature that is available on switches based on Cisco IOS and NX-OS Software that allows traffic received on a port or VLAN to be copied to another port for analysis. It is also referred to as "port mirroring."
SSH	Secure Shell Protocol. Protocol that provides a secure remote connection to a router through a TCP application.
SSID	Service Set Identifier.
SSID	Service Set Identifier.
SSL	Secure Socket Layer. Encryption technology for the Web used to provide secure transactions, such as the transmission of credit card numbers for e-commerce.
SSO	single sign-on.
STP	Spanning Tree Protocol. Bridge protocol that uses the spanning-tree algorithm, enabling a learning bridge to dynamically work around loops in a network topology by creating a spanning tree. Bridges exchange BPDU messages with other bridges to detect loops, and then remove the loops by shutting down selected bridge interfaces. Refers to both the IEEE 802.1 Spanning Tree Protocol standard and the earlier Digital Equipment Corporation Spanning Tree Protocol upon which it is based. The IEEE version supports bridge domains and allows the bridge to construct a loop-free topology across an extended LAN. The IEEE version generally is preferred over the Digital version.
SXP	Security Exchange Protocol.
syslog	system logging.
TACACS+	Terminal Access Controller Access Control System Plus. Proprietary Cisco enhancement to TACACS. Provides additional support for authentication, authorization, and accounting.
TCAM	ternary content addressable memory

https://t.me/learningnets

Term	Definition
TCP	Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.
TCP/IP	Transmission Control Protocol/Internet Protocol. Common name for the suite of protocols developed by the U.S. DoD in the 1970s to support the construction of worldwide internetworks. TCP and IP are the two best-known protocols in the suite.
TEAP	Tunneled EAP
Telnet	Standard terminal emulation protocol in the TCP/IP protocol stack. Telnet is used for remote terminal connection, enabling users to log into remote systems and use resources as if they were connected to a local system. Telnet is defined in RFC 854.
TFTP	Trivial File Transfer Protocol. A simplified version of FTP that is generally used for automated transfer of configuration or boot files from one computer to another over a network, usually without the use of client authentication.
TLS	Transport Layer Security. A future IETF protocol to replace SSL.
TLV	type, length, value.
UDI	unique device identifier.
UDP	User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.
URL	uniform resource locator. Type of formatted identifier that describes the access method and the location of an information resource object on the Internet. [RFC 1738]
VLAN	virtual LAN. Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.
VM	virtual machine.
VoIP	Voice over IP. The capability to carry normal telephony-style voice over an IP-based internet with POTS-like functionality, reliability, and voice quality. VoIP enables a router to carry voice traffic (for example, telephone calls and faxes) over an IP network. In VoIP, the DSP segments the voice signal into frames, which then are coupled in groups of two and stored in voice packets. These voice packets are transported using IP in compliance with ITU-T specification H.323.

https://t.me/learningnets
© 2014 Cisco Systems, Inc.

Term	Definition
VPN	virtual private network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses tunneling to encrypt all information at the IP level.
VSA	vendor-specific attribute. An attribute that has been implemented by a particular vendor. It uses the attribute Vendor-Specific to encapsulate the resulting AV pair: essentially, Vendor-Specific = protocol:attribute = value.
WAN	wide-area network. Data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers. Frame Relay, SMDS, and X.25 are examples of WANs.
WebAuth	web authentication.
WLAN	wireless LAN. A LAN is a high-speed, low-error data network covering a relatively small geographic area (up to a few thousand meters). LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area. LAN standards specify cabling and signaling at the physical and data link layers of the OSI model. Ethernet, FDDI, and Token Ring are widely used LAN technologies.
WLC	wireless LAN controller. A centralized network device that is used to control lightweight wireless APs.
WPA	WiFi Protected Access
WPA2	WiFi Protected Access 2

https://t.me/learningnets