



Cisco Expo 2012

Posture Assessment with ISE

György Ács

Consulting Systems Engineer, C|EH – Cisco

T-SECA4

Prosíme, ptejte se nás

- Twitter www.twitter.com/CiscoCZ
- Talk2cisco www.talk2cisco.cz/dotazy
- SMS 721 994 600



ISE as a Posture Assessment



ISE with NAC functionality

Analysis of Antivirus, Antispyware, personal FW processes ... quarantine and remediation services + passive reassessment

About Posture Assessment

Authentication

Authenticate User

Authenticate PC
corporate asset ?

Authenticate Guests
(WEB)

Profile Devices, MAB

Posture

Compliance Check
OS, Hotfix, Antivirus,
Personal Firewall

Quarantine

Remediation
Fix problem,
make PC compliant

Authorization

Create different
Zones to segment
network

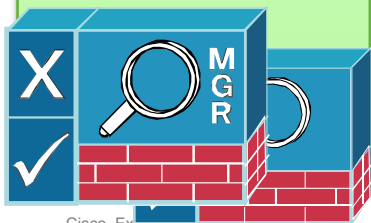
Assign VLAN to port

Assign ACL to port

NAC appliance vs. ISE

802.1X authentication + posture + profiling + guest

NAC Appliance	Description	ISE – NEW
Checks	File, Service, Registry, AV/AS checks	Posture Conditions
Rules	Multiple simple conditions are built together	Compound Posture Conditions
Requirements	Requirements are used with <u>Operating Systems</u> . They contain compound conditions. Each Requirement has a selected <u>Remediation action</u> .	Posture Requirements
Role Requirements	Posture policies can be evaluated based on <u>Identity Groups, OS, and dictionary attributes</u> . Policies contain the Requirements	Posture Policy



Posture Assessment in Wired and Wireless environments



802.1X End User Authentication with Posture

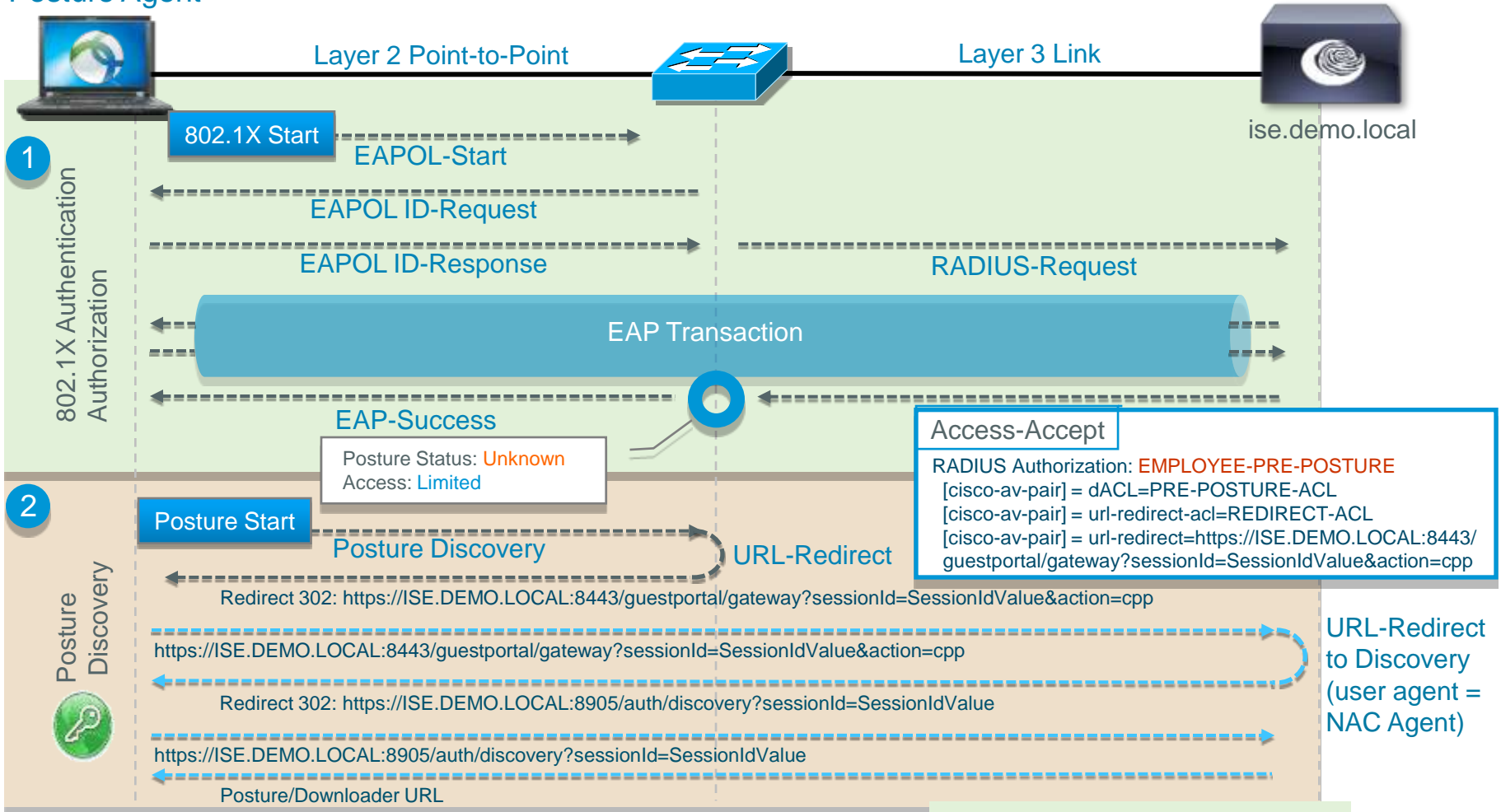
Suppliant /
Posture Agent

Authenticator

Authentication Server

Layer 2 Point-to-Point

Layer 3 Link



Flow continues to next slide

802.1X End User Authentication with Posture

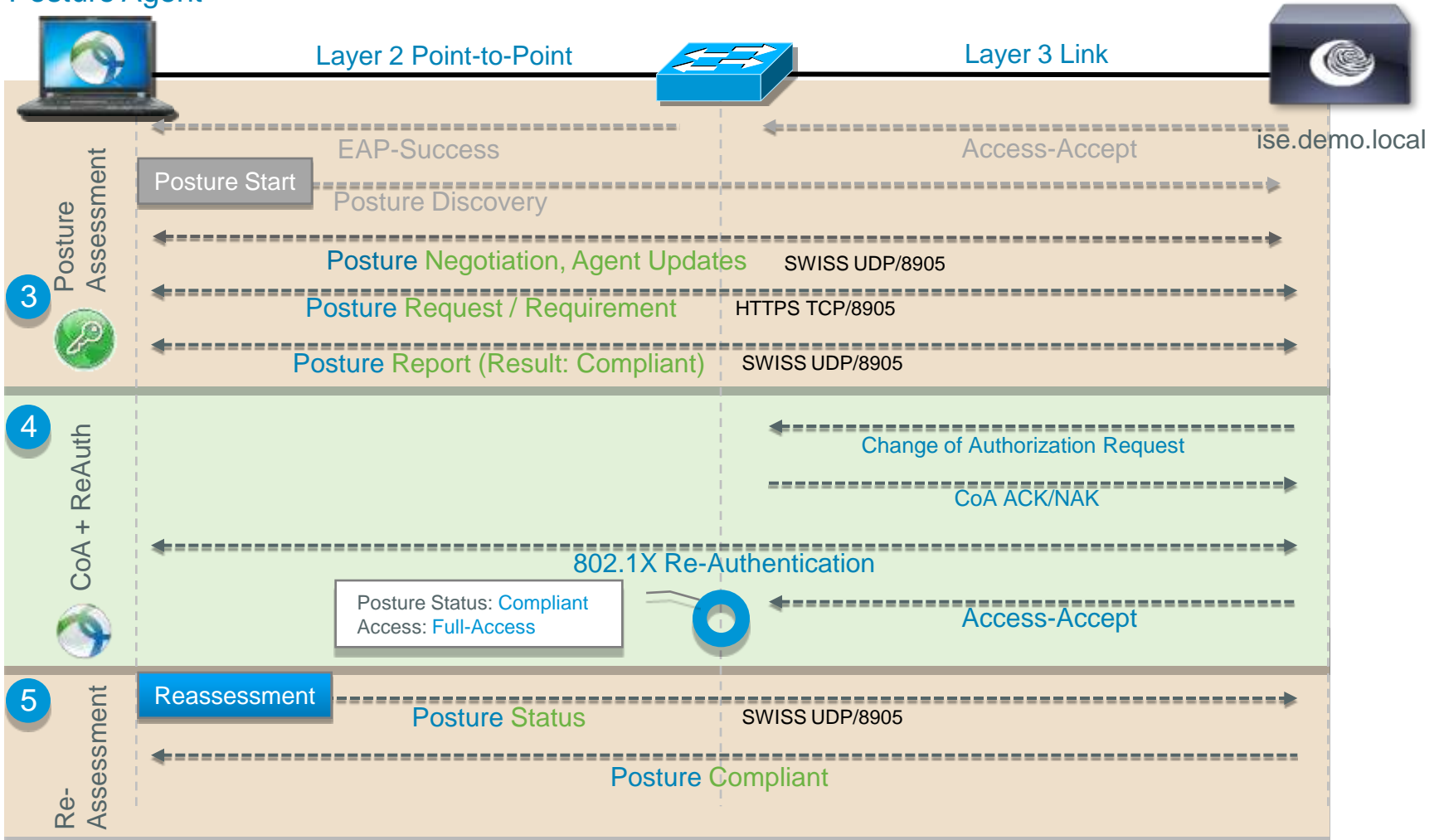
Supplicant /
Posture Agent

Authenticator

Authentication Server

Layer 2 Point-to-Point

Layer 3 Link



Clients and provisioning



Global Client Provisioning and Posture Options

- General Settings
- Reassessments
- Updates
- Acceptable Use Policy

Posture General Settings ⓘ

Remediation Timer Minutes ⓘ

Network Transition Delay Seconds ⓘ

Default Posture Status ⓘ

Automatically Close Login Success Screen After Seconds ⓘ

Home Operations Policy Administration

System Identity Management Network Resources Guest Management

Deployment Licensing Certificates Logging Maintenance Admin Access Settings

Settings

- Client Provisioning
- Endpoint Protection Service
- FIPS Mode
- Monitoring
- Posture
 - General Settings
 - Reassessments
 - Updates
 - Acceptable Use Policy

Client Provisioning

* Enable Provisioning: ⓘ

* Enable Automatic Download: ⓘ

* Update Feed URL: ⓘ

Policy Based Acceptable Use Policy

Acceptable use policy Configurations List > **Guest**

Acceptable User Policy

* Configuration Name **Guest**

Configuration Description

Show AUP to Agent users (for Agent and Web Agent on Windows only)

Use URL for AUP message

Use file for AUP message (Please upload a zip file. The zip file must be less than 10 MB.)

* AUP URL

Group Selection Rules

1. Posture AUP is not applicable for guest portal login (use guest portal login AUP)
2. Each configuration must have a unique group or a unique configuration name
3. No two configurations may have any group in common.
4. If a config already exists with a group of 'Any', then no other configurations can be created with a group of 'Any'.
5. If a config with a group of 'Any' must be created, delete all other configurations with a group of 'Any'.

* Select User Identity Groups

▼ Acceptable use policy configurations

configurations list

Existing Acceptable Use Policy Configurations	User Identity Groups
<input type="radio"/> Guest	Guest

Per User Identity Group

What else is needed?

- Agents
MAC OSX, Windows and WebAgent
- Compliance Module
- Agent Customization package
- Agent profile -> user interface

Resource files from local disk
or Cisco site

The screenshot shows the Cisco ISE GUI with the 'Resources' tab selected. The 'Resources' table contains the following data:

Name	Type	Version
Agent resources from Cisco site		
MacOsXAgent	MacOsXAgent	4.9.0.647
ISE Posture Agent Profile	NACAgentConfig	Not Applicable
AgentProfile-Guest	NACAgentConfig	Not Applicable
NACAgent 4.9.0.32	NACAgent	4.9.0.32
ComplianceModule 3.4.26.1	ComplianceModule	3.4.26.1
WebAgent 4.9.0.19	WebAgent	4.9.0.19

Agent Profile

Resources > New Profile

ISE Posture Agent Profile

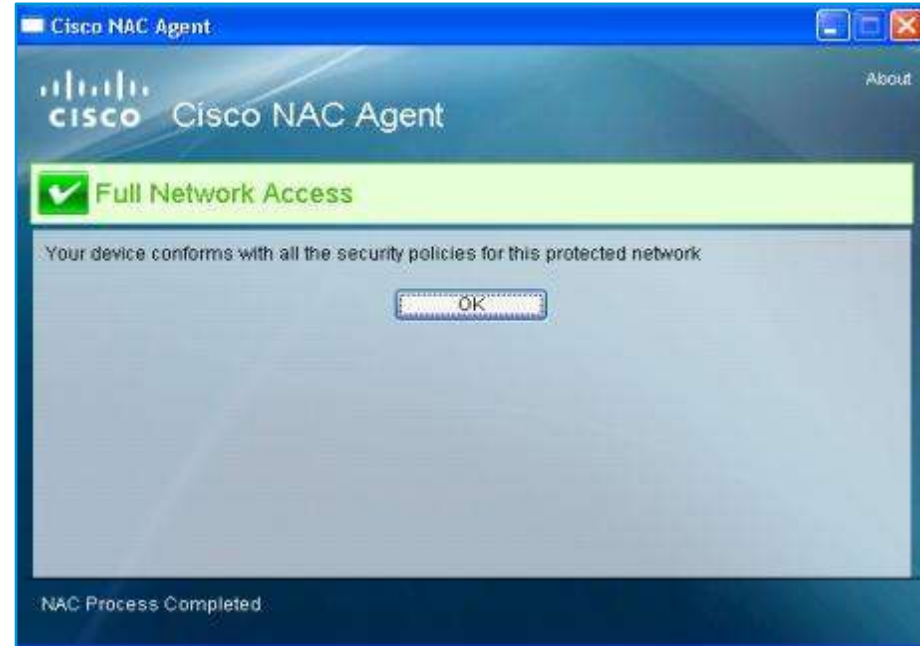
Profile Name:

Separated Profiles for Windows and OSX

Parameter Description	Parameter Value	Mode	Notes
VLAN detect interval in secs (<i>VlanDetectInterval</i>): (0-900):	<input type="text" value="0"/>	merge ▼	For OSX, i
Enable VLAN detect without UI? (<i>EnableVlanDetectWithoutUI</i>):	no ▼	merge ▼	OSX: N/A
Disable Agent exit? (<i>DisableExit</i>):	no ▼	merge ▼	OSX: N/A
Allow CRL checks? (<i>AllowCRLChecks</i>):	yes ▼	overwrite ▼	OSX: N/A
Accessibility mode? (<i>AccessibilityMode</i>):	no ▼	merge ▼	OSX: N/A
Check signature? (<i>SignatureCheck</i>):	no ▼	overwrite ▼	OSX: N/A
Bypass summary screen? (<i>BypassSummaryScreen</i>):	yes ▼	merge ▼	OSX: N/A
MAC exception list (<i>ExceptionMACList</i>):	<input type="text"/>	merge ▼	OSX: N/A
Discovery host (<i>DiscoveryHost</i>):	<input type="text"/>	overwrite ▼	
Discovery host editable? (<i>DiscoveryHostEditable</i>):	yes ▼	overwrite ▼	OSX: N/A
Server name rules (<i>ServerNameRules</i>):	<input type="text"/>	overwrite ▼	OSX: N/A
Generated MAC (<i>GeneratedMAC</i>):	<input type="text"/>	merge ▼	OSX: N/A
Language info (<i>Locale</i>):	default ▼	merge ▼	OSX: N/A
Posture report filter (<i>PostureReportFilter</i>):	displayFailed ▼	merge ▼	OSX: N/A

NAC Agent (Persistent)

- Windows or MAC
- Localized (ISE 1.1 : 10 languages)
- Installed from Web or MSI
- Handles user logon
- Single-Sign-On: 802.1X
- Checks Posture
 - Remediates Posture
 - Guides user through process
 - Automatic remediation
 - Refreshes IP address
- Automatic update of the agent via ISE



Typical Use Case: Managed Devices

Agent Customization Package



A table showing agent configurations. A green arrow points from the "branding package" box to the "WebAgent" row.

Type	Version
MacOsXAgent	4.9.0.647
ComplianceModule	3.4.26.1
NACAgentConfig	Not Applicable
NACAgent	4.9.0.32
WebAgent	4.9.0.19

branding package

NAC Web Agent

- Windows
- Temporary (ActiveX)
- User logon
- Checks Posture
- Limited Remediation
- Refreshes IP address

Cisco Identity Services Engine Network Security Notice

Cisco NAC Web Agent

Host is not compliant with network security policy

Your device does not conform to the required security policies for this protected network. Your access to the network is refused or limited until you are able to comply with the security requirements listed below.
Please remediate by 08:24:29 PM, Sat Feb 05, 2011.

Result	Security Requirement	Remediation Suggestion
✗	Guest_AV Current	All Guests must have Antivirus software installed with current signatures. Please update your AV software signatures now.
✓	Screen Saver On and Secure	
✓	Guest_AV Installed	

Cisco NAC Web Agent Version 4.9.0.6 - Report Generated 08:22:49 PM, Sat Feb 05, 2011

Remaining 00:01:36

Re-Scan Save Report Cancel

Typical Use Case: Unmanaged PCs,
Guests, Contractors

Provisioning based on Policy

Policy states : Enabled, Disabled, Monitor

provision policy based on
endpoint operating system
user identity group
dictionary based conditions

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results	Actions
employee	If Any and Window...	Window...	budlabsec.com:ExternalGroups E...	NACAgent 4.9.0.32	Actions
employee_hu	If Any and Window...	Window...	budlabsec.com:ExternalGroups E...	NACAgent 4.9.0.32	Actions
guest_copy	If Gu...	Any	Condition(s)	WebAgent 4.9.0.19	Actions

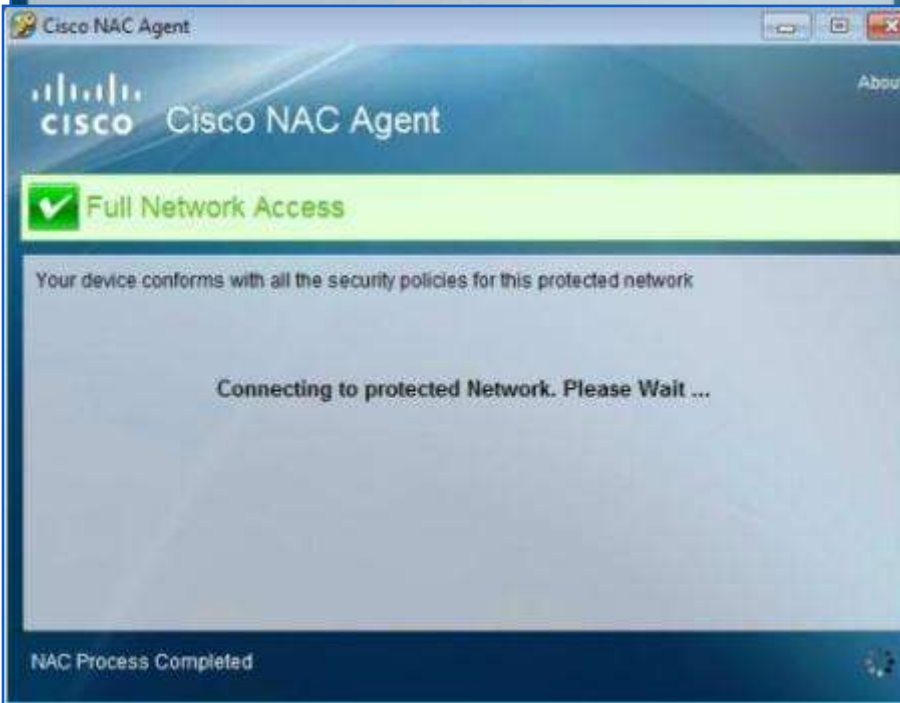
First-match policy will be selected when there are multiple matches

Agent specification is mandatory, other resources are optional

Any and Condition(s) then WebAgent 4.9.0.19

- Agent: WebAgent 4.9.0.19 Is Upgrade Mandatory
- Profile: Choose a Profile
- Compliance Module: Choose a Compliance Module
- Agent Customization Package: Choose a Customization Package

ISE – Provisioning Posture Agents



Posture elements and features



Posture Assessment Elements

File

Registry

Applications

Service

Compound Cond.

AntiVirus

AntiSpyware

Custom Conditions

The screenshot shows the Cisco Posture Assessment interface. On the left is a sidebar with categories: File, Registry, Applications, Service, Compound Cond., AntiVirus, AntiSpyware, and Custom Conditions. Yellow arrows point from these categories to the corresponding items in the main window's sidebar. The main window has a 'Posture' header and a search bar. Below it is a list of condition types: File Condition, Registry Condition, Application Condition, Service Condition, Compound Condition, AV Condition, AS Condition, Dictionary, and Dictionary. A green callout bubble points to the 'Registry Conditions' table, containing the text: 'Cisco Predefined Checks for File, Registry, Application, Service, Compound, and AV, AS compound Conditions + User defined'. The 'Registry Conditions' table has columns for Name, Description, Registry Type, and Condition Type.

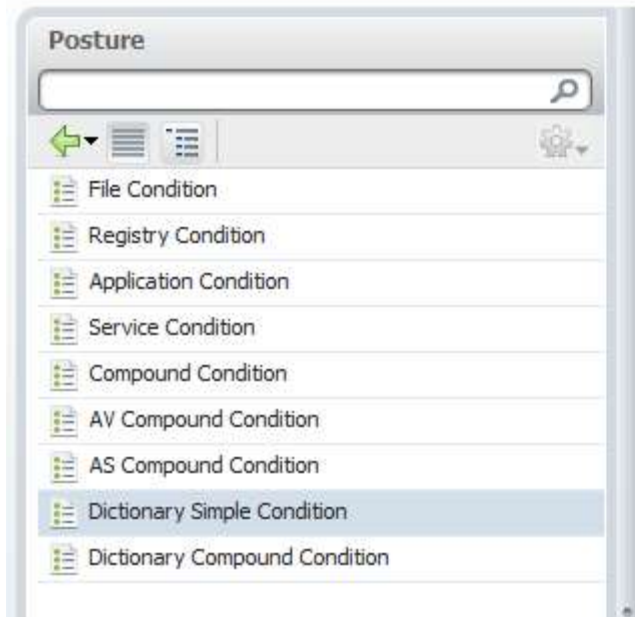
Name	Description	Registry Type	Condition Type
<input type="checkbox"/> pc_CSA_Version_5_0_0_0_gt	Cisco Predefined Check: CSA later	RegistryValue	Cisco-Defined
<input type="checkbox"/> pc_CSA_Version_6_0_0_0_lt	Cisco Predefined Check: CSA earlie	RegistryValue	Cisco-Defined
<input type="checkbox"/> pc_HotFix896358_XP	Cisco Predefined Check: Critical Up	RegistryKey	Cisco-Defined
<input type="checkbox"/> pc_HotFix896423_XP	Cisco Predefined Check: Critical Up	RegistryKey	Cisco-Defined
<input type="checkbox"/> pc_HotFix901214_XP	Cisco Predefined Check	RegistryKey	Cisco-Defined
<input type="checkbox"/> pc_HotFix902400_XP	Cisco Predefined Check: Critical Up	RegistryKey	Cisco-Defined
<input type="checkbox"/> pc_Hotfix323255	Cisco Predefined Check	RegistryKey	Cisco-Defined
<input type="checkbox"/> pc_Hotfix329390	Cisco Predefined Check	RegistryKey	Cisco-Defined
<input type="checkbox"/> pc_Hotfix823182	Cisco Predefined Check	RegistryKey	Cisco-Defined
<input type="checkbox"/> pc_Hotfix823559	Cisco Predefined Check	RegistryKey	Cisco-Defined
<input type="checkbox"/> pc_Hotfix824146	Cisco Predefined Check	RegistryKey	Cisco-Defined
<input type="checkbox"/> pc_Hotfix825119	Cisco Predefined Check	RegistryKey	Cisco-Defined
<input type="checkbox"/> pc_Hotfix828741	Cisco Predefined Check	RegistryKey	Cisco-Defined
<input type="checkbox"/> pc_Hotfix835732	Cisco Predefined Check	RegistryKey	Cisco-Defined
<input type="checkbox"/> pc_Hotfix840987_XP	Cisco Predefined Check: Security L	RegistryKey	Cisco-Defined
<input type="checkbox"/> pc_Hotfix841873_XP	Cisco Predefined Check: Security L	RegistryKey	Cisco-Defined

Dictionary Simple Conditions



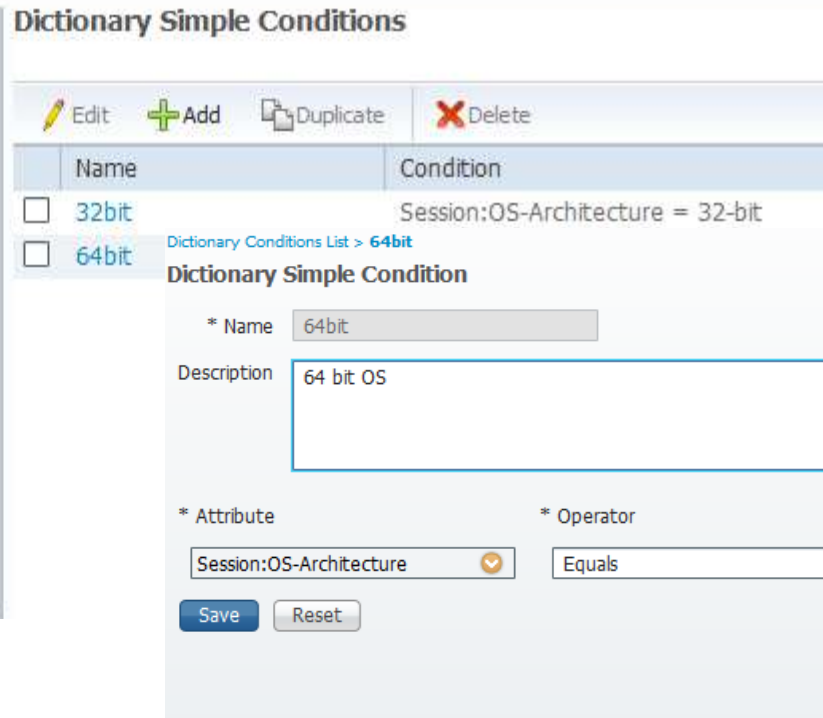
The navigation bar for Cisco Identity Services Engine includes the following elements:

- Logo: CISCO Identity Services Engine
- Menu: Home | Monitor | Policy | Administration
- Icons: Authentication, Authorization, Profiling, Posture, Client Provisioning, Security Group
- Sub-menu: Dictionaries | **Conditions** | Results



The Posture sidebar contains a search bar and a list of condition types:

- File Condition
- Registry Condition
- Application Condition
- Service Condition
- Compound Condition
- AV Compound Condition
- AS Compound Condition
- Dictionary Simple Condition**
- Dictionary Compound Condition



Dictionary Simple Conditions

Actions: Edit, Add, Duplicate, Delete

Name	Condition
<input type="checkbox"/> 32bit	Session:OS-Architecture = 32-bit
<input type="checkbox"/> 64bit	Dictionary Conditions List > 64bit

Dictionary Simple Condition

* Name: 64bit

Description: 64 bit OS

* Attribute: Session:OS-Architecture | * Operator: Equals | * Value: 64-bit

Buttons: Save, Reset

- Originally : empty
- Frequently used (dictionary) conditions make the policy easy

Dictionary Compound Condition

Dictionary Compound Conditions List > 64bitOS_Employee

Dictionary Compound Condition

* Name 64bitOS_Employee

Description

Condition Name	Expression		AND
64bit	64 bit OS	AND	
employee	employee		

Save Reset

- A dictionary compound condition is a logical combination of more than one dictionary simple condition (a dictionary attribute that is associated with a value).
- It is a set of dictionary simple conditions (dictionary attributes that are associated with values) that are logically combined with an AND, or an OR operator.

Compound Condition

The screenshot shows a web-based interface for configuring network policies. At the top, there are tabs for Authentication, Authorization, Profiling, Posture, Client Provisioning, Security Group Access, and Policy Editor. Below these, there are sub-tabs for Dictionaries, Conditions, and Results. The main area is titled 'Posture' and contains a search bar and a list of condition types: File Condition, Registry Condition, Application Condition, Service Condition, Compound Condition (selected), AV Compound Condition, AS Compound Condition, Dictionary Simple Condition, and Dictionary Compound Condition. The 'Compound Condition' configuration window is open, showing the following details:

- Compound Conditions List > **pr_McAfee_Update**
- Compound Condition**
- * Name: **pr_McAfee_Update**
- Description: **Cisco Predefined Rule**
- * Operating System: **Windows All**
- Conditions: `pc_McAfee_Professional_Def_Update | pc_McAfee_ASaP_Def_Update | pc_McAfee_Enterprise_Def_Update | pc_McAfee_Enterprise_8_Def_Update`
- Buttons: Cancel

- A compound condition includes one or more simple conditions, or compound conditions of the type file, registry, application, service, or dictionary conditions.
- You can combine one or more conditions using an AND (ampersand [&]), an OR (horizontal bar [|]), or a NOT (exclamation point [!]) operator to create a compound condition.

Preconfigured Conditions, 300+

File, Registry, Application, Service, Compound, and AV, AS compound Conditions

File Conditions

View Edit Add Duplicate Delete

Name	Description
<input type="checkbox"/> pc_KB925902_1_MS07-017_Vista	Cisco Predefined Check: Critical Up
<input type="checkbox"/> pc_KB925902_2_MS07-017_Vista	Cisco Predefined Check: Critical Up
<input type="checkbox"/> pc_KB929123_1_MS07-034_Vista	Cisco Predefined Check: Critical Up
<input type="checkbox"/> pc_KB929123_2_MS07-034_Vista	Cisco Predefined Check: Critical Up
<input type="checkbox"/> pc_KB930178_1_MS07-021_Vista	Cisco Predefined Check: Critical Up
<input type="checkbox"/> pc_KB930178_2_MS07-021_Vista	Cisco Predefined Check: Critical Up
<input type="checkbox"/> pc_KB943055_MS08-008_Vista	Cisco Predefined Check: Critical Up
<input type="checkbox"/> pc_KB946026_1_MS08-007_Vista	Cisco Predefined Check: Critical Up
<input type="checkbox"/> pc_KB946026_2_MS08-007_Vista	Cisco Predefined Check: Critical Up
<input type="checkbox"/> pc_KB951376_1_MS08-030_Vista	Cisco Predefined Check: Critical Up
<input type="checkbox"/> pc_KB953838_1_MS08-045_Vista	Cisco Predefined Check: Critical Up
<input type="checkbox"/> pc_KB953838_2_MS08-045_Vista	Cisco Predefined Check: Critical Up
<input type="checkbox"/> pc_KB956802_MS08-071_Vista	Cisco Predefined Check: Critical Up
<input type="checkbox"/> pc_KB958690_MS09-006_Vista	Cisco Predefined Check: Critical Up
<input type="checkbox"/> pc_KB959349_MS08-075_Vista	Cisco Predefined Check: Critical Up
<input type="checkbox"/> pc_KB960803_MS09-013_Vista	Cisco Predefined Check: Critical Up
<input type="checkbox"/> pc_MSXML3_MS08-069_Vista	Cisco Predefined Check: Critical Up
<input type="checkbox"/> pc_MSXML3r_MS08-069_Vista	Cisco Predefined Check: Critical Up
<input type="checkbox"/> pc_MSXML4_MS07-042	Cisco Predefined Check: Check ms
<input type="checkbox"/> pc_MSXML5_MS07-042	Cisco Predefined Check: Check ms
<input type="checkbox"/> pc_MSXML6_MS07-042	Cisco Predefined Check: Check ms
<input type="checkbox"/> pc_MSXML6_MS07-042_Vista	Cisco Predefined Check: Check for
<input type="checkbox"/> pc_MSXML6r_MS07-042_Vista	Cisco Predefined Check: Check for
<input type="checkbox"/> pc_MS_MRT-Hotfix890830	Cisco Predefined Check: KB890830

Registry Conditions List > pc_IE9_0

Registry Condition

* Name **pc_IE9_0**

Description **Cisco Predefined Check: Chec**

Registry Type

Registry Root Key * Sub Key

* Value Name

Value DataType

Value Operator

Value Data **9.0**

* Operating System

Does PC have IE installed ?

Cancel

SYSTEM_32\gdi32.dll	Cisco-Defined
SYSTEM_32\Win32k.sys	Cisco-Defined
SYSTEM_ROOT\Explorer.exe	Cisco-Defined
SYSTEM_32\winhttp.dll	Cisco-Defined
SYSTEM_32\msxml3.dll	Cisco-Defined
SYSTEM_32\msxml3r.dll	Cisco-Defined
SYSTEM_32\msxml4.dll	Cisco-Defined
SYSTEM_32\msxml5.dll	Cisco-Defined
SYSTEM_32\msxml6.dll	Cisco-Defined
SYSTEM_32\msxml6.dll	Cisco-Defined
SYSTEM_32\msxml6r.dll	Cisco-Defined
SYSTEM_ROOT\Debug\mrt.log	Cisco-Defined

Posture Policy hierarchy

Posture Conditions



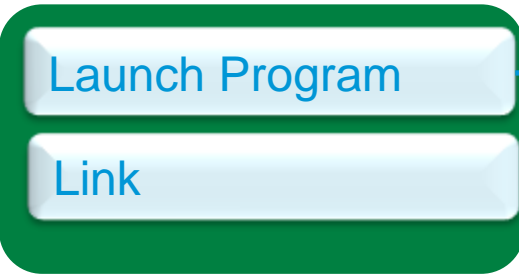
Requirements



Policies



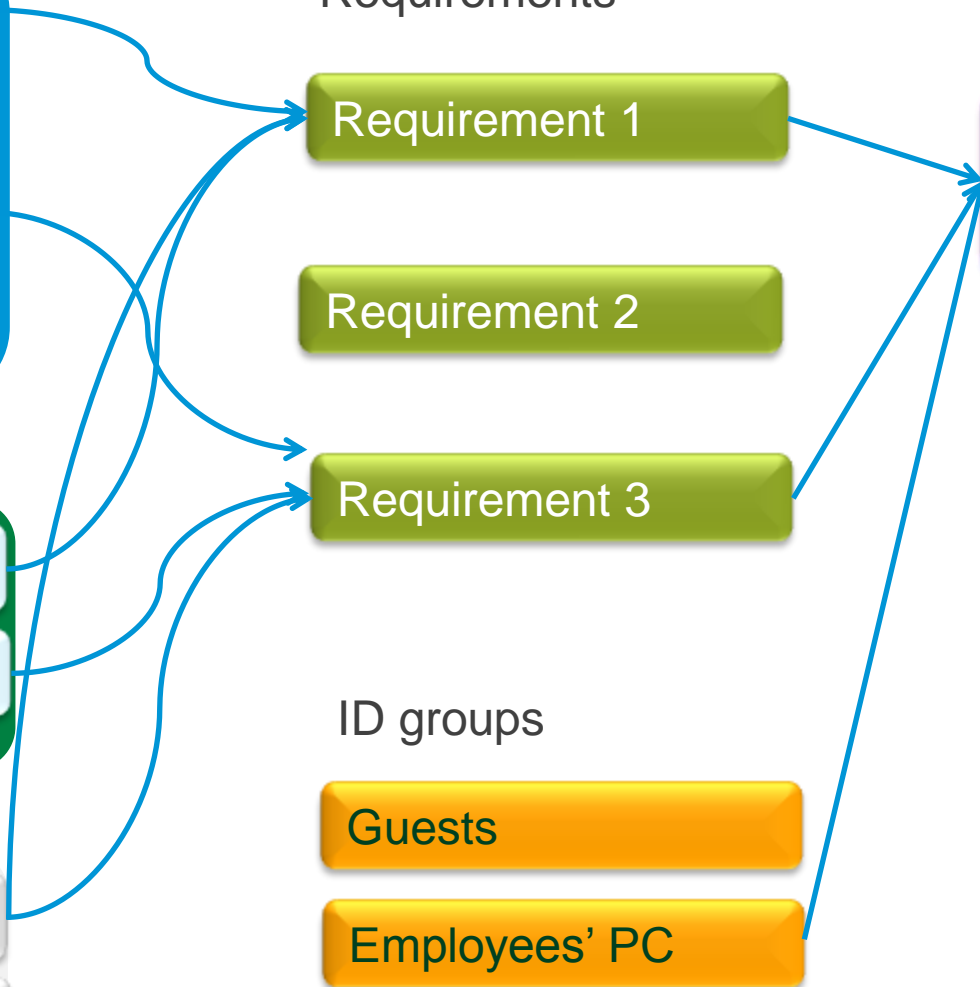
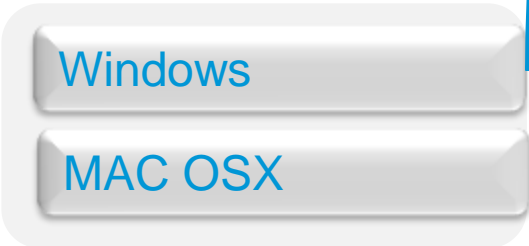
Remediation actions



ID groups



OS



Requirements

Predefined AV/AS requirements

Easy requirement fine-tuning

Name	Operating Systems	Conditions	Remediation Actions
Any_AV_Installation_1	for Windo...	met if ANY_av_...	else Message T...
Any_AV_Definition_W	for Windo...	me	
Any_AS_Installation_1	for Windo...	me	
Any_AS_Definition_W	for Windo...	me	
Any_AV_Installation_1	for Mac OSX	me	
Any_AV_Definition_M	for Mac OSX	me	
Any_AS_Installation_1	for Mac OSX	met if ANY_as_m...	else Message
Any_AS_Definition_M	for Mac OSX	met if ANY_as_m...	else Message
TEST	for Windo...	met if NotePad	else Message

Context Menu Options:

- Duplicate
- Insert new Requirement
- Delete

Default AV, AS, Installation and Definition Condition

Anti-virus Compound Conditions List > **ANY_av_win_inst**

AV Compound Condition

* Name: ANY_av_win_inst
Description: Any AV installation check on Win
* Operating System: Windows All
Vendor: ANY
Check Type: Installation Definition

Products for Selected Vendor

Product Name	Version	Remediation Support	Definition Check	Latest Definition Date	Latest Definition Version	install
<input checked="" type="checkbox"/> ANY	ANY	N/A	YES	N/A	N/A	N/A

AV (Any) is needed

Anti-virus Compound Conditions List > **ANY_av_win_def**

AV Compound Condition

* Name: ANY_av_win_def
Description: Any AV definition check on Wind
* Operating System: Windows All
Vendor: ANY
Check Type: Installation Definition
 Check against latest AV definition file version available. Otherwise check against latest definition file date.
 Allow virus definition file to be 5 days older than latest file date current system date

Products for Selected Vendor

Product Name	Version	Remediation Support	Definition Check	Latest Definition Date	Latest Definition Version	install
<input checked="" type="checkbox"/> ANY	ANY	N/A	YES	N/A	N/A	N/A

Max 5 days old AV definition file

Create a Requirement

for met if else

- Name

- Operating Systems (OR)

Example:

- Conditions (AND)

Operator

Condition types

Simple conditions

Compound conditions

- Remediation

Action

Message

Windo... met if else

Windows 7 (All) or Windows Vista (All)

met if else

All selected conditions succeed

All selected conditions succeed

Any selected conditions succeeds

No selected conditions succeeds

pc_IE7_0

for met if else

Action

Message Shown to Agent User

Start your Firewall

Remediation

Results

Windows Server Update Services Remediations List > **New Windows Server Update Services Remediation**

Windows Server Update Services Remediation

* Name

Description

Remediation Type

Interval

Retry Count

Validate Windows updates using Cisco Rules Severity Level

Windows Updates Severity Level

Update to latest OS Service Pack

Windows Updates Installation Source Microsoft Server Managed Server

Installation Wizard Interface Setting Show UI No UI

Remediation types:

Automatic—The NAC Agents automatically updates Windows clients with the latest WSUS updates

Manual—The user manually updates the Windows client with the latest WSUS updates from a Microsoft-managed WSUS server, or from the locally administered WSUS server for compliance.

Launch Program Remediation

- Allows administrators to launch a qualified (**signed**) remediation program through the Agent. Multiple programs are permitted, and they are launched in the same sequence as specified by the administrator.


Note:

A valid digital signature signed by certificate is required if user in client machine does not have admin privileges.

* Program Installation Path

* Program Executable

Program Parameters

Existing Programs			
Installation Path	Program Name	Program Parameters	
NONE	c:\firewall.exe		

Windows Update Remediation

- Allows administrators to check and modify Windows Update settings, and launch Windows Updater on client machines where users have Administrator privileges.
- The Windows Update remediation provides an Update button on the (persistent) Agent for remediation. When the end user clicks the Update button, the Agent launches the Automatic Updates Agent and forces it to get the update software from an external WSUS server.

WSUS remediation should be optional, it is a long process

Windows Update Remediations List > New Windows Update Remediation

Windows Update Remediation

* Name	<input type="text" value="Windows Update"/>
Description	<input type="text" value="Windows Update"/>
Remediation Type	<input type="text" value="Automatic"/>
Interval	<input type="text" value="0"/> (in secs) (Valid Range 0 to 9999)
Retry Count	<input type="text" value="0"/> (Valid Range 0 to 99)
Windows Update Setting	<input type="text" value="Do not change setting"/>
Override User's Windows Update setting with administrator's	<input type="text" value="Do not change setting"/> <input type="text" value="Notify to download and install"/> <input type="text" value="Automatically download and notify to install"/> <input type="text" value="Automatically download and install"/>



ISE Posture Assessment/Remediation

	NAC Agent for Windows	Web Agent for Windows	NAC Agent for Mac OS X
Posture Assessment Options	OS/Service Packs/Hotfixes Process Check Registry Check File Check Application Check AV Installation AV Version/AV Definition Date AS Installation AS Version/AS Definition Date Windows Update Running Windows Update Configuration WSUS Compliance Settings	OS/Service Packs/Hotfixes Process Check Registry Check File Check Application Check AV Installation AV Version/AV Definition Date AS Installation AS Version/AS Definition Date Windows Update Running Windows Update Configuration WSUS Compliance Settings	AV Installation AV Version/Def Date AS Installation AS Version/Def Date
Remediation Options	Message Text (Local Check) URL Link (Link Distribution) File Distribution Launch Program AV Definition Update AS Definition Update Windows Update WSUS	Message Text URL Link File Distribution	Message Text URL Link AV Live Update (AS Live Update)

Posture Policy

- Posture Policies tie the Requirements to Identity Groups and other Conditions together to make a Policy
- Once a User is Authenticated, Posture Policy is checked for the Identity Group/User
- If Posture passes, users will be assigned a new Authorization Policy

The screenshot displays the Cisco Identity Services Engine (ISE) interface for configuring Posture Policies. The top navigation bar includes the Cisco logo, 'Identity Services Engine', and user information (ise11, admin, Log Out, Feedback). The main navigation menu shows 'Home', 'Monitor', 'Policy', and 'Administration'. Below this, there are tabs for 'Authentication', 'Authorization', 'Profiling', 'Posture', 'Client Provisioning', 'Security Group Access', and 'Policy Elements'. The 'Posture Policy' section is active, showing a table of policies.

Status	Rule Name	Identity Groups	Operating Systems	Other Conditions	Requirements	Actions
<input checked="" type="checkbox"/>	MyApplPolicy	If Any and	Windows All	(Optional) Dictionary Attr...	then TEST	Actions
<input type="checkbox"/>	Policy_Check_Fo	If Any and	Mac OSX	(Optional) Dictionary Attr...	then Any_AS_Definition_Win	Actions
<input checked="" type="checkbox"/>	Policy_Check_Fo	If Any and	Windows All	(Optional) Dictionary Attr...	then Any_AS_Definition_Win	Actions
<input type="checkbox"/>	Policy_Check_Fo	If Any and	Mac OSX	(Optional) Dictionary Attr...	then Any_AV_D...	Actions
<input checked="" type="checkbox"/>	Policy_Check_Fo	If Any and	Windows All	(Optional) Dictionary Attr...	then Any_AV_D...	Actions
<input type="checkbox"/>	Policy_Check_Fo	If Any and	Mac OSX	(Optional) Dictionary Attr...	then Any_AV_D...	Actions
<input checked="" type="checkbox"/>	Policy_Check_Fo	If Any and	Windows All	(Optional) Dictionary Attr...	then Any_AV_D...	Actions

The 'Requirements Details' popup for 'Any_AS_Definition_Win' shows:

Name	Enforcement
Any_AS_Definition_Win	Mandatory

Posture Policy Status

Status	Rule Name	Identity Groups	Operating Systems	Other Conditions	Requirements
<input checked="" type="checkbox"/>	MyAppPolicy	If Any and	Windows All	(Optional) Dictionary Attr...	then TEST
<input type="checkbox"/>	Policy_Check_Fo	If Any and	Mac OSX	(Optional) Dictionary Attr...	then Any_AS_D...
<input checked="" type="checkbox"/>	Policy_Check_Fo	If Any and	Windows All	(Optional) Dictionary Attr...	then Any_AS_D...
<input type="checkbox"/>	Policy_Check_Fo	If Any and	Mac OSX		
<input checked="" type="checkbox"/>	Policy_Check_Fo	If Any and	Windows A		
<input type="checkbox"/>	Policy_Check_Fo	If Any and	Mac OSX		

Any_AS_Definition_Win

Mandatory

Optional

Audit

Mandatory—This option enforces the client to meet the posture requirement, otherwise no / restricted access

Optional—The client can bypass the requirement, but can have network access.

	(Optional) Dictionary Attr...	then	Any_AS_D...
<input checked="" type="checkbox"/>	Any_AS_Definition_Win		
<input checked="" type="checkbox"/> Mandatory			
<input type="checkbox"/> Optional			
<input type="checkbox"/> Audit			

Audit—This option checks the client for the posture requirement without notifying the user. It does not affect user network access.

Authorization Policy

Best Practice: Authz Policy rules should distinguish two compliance states

Session:PostureStatus: Posture = Compliant

Session:PostureStatus: Posture != Compliant
(inc. Unknown and NonCompliant)

Status	Rule Name	Identity Groups	Other Conditions	Actions
▼	Profiled Cisco IP Phones	Cisco-IP-Phone	-	IP Phones
▼	Domain_Computer	Any	demo.local:ExternalGroups EQUALS demo.local/Users/Domain Computers	login
▼	Employee	Any	demo.local:ExternalGroups EQUALS demo.local/Users/employees AND Session:PostureStatus EQUALS Compliant	Employee
▼	Employee_PreCompliant	Any	demo.local:ExternalGroups EQUALS demo.local/Users/employees AND Session:PostureStatus NOT EQUALS Compliant	Posture_Remediation
▼	Contractor	Contractor	Session:PostureStatus EQUALS Compliant	Guest
▼	Guest	Guest	Session:PostureStatus EQUALS Compliant	Guest
▼	Default	Any	-	Remediation

Best Practice: Add remediation ACLs for Posture Status != Compliant

Policy Based Re-Assessment

Reassessment Configurations List > **New Reassessment Configuration**

Reassessment Configuration

* Configuration Name

Configuration Description

Use Reassessment Enforcement?

Enforcement Type

Interval minutes. ⓘ

Grace Time minutes. ⓘ

Group Selection Rules

1. Each configuration must have a unique group or a unique combination of groups.
2. No two configurations may have any group in common.
3. If a config already exists with a group of 'Any', then no other configs can be created unless -
 - i. the existing config with a group of 'Any' is updated to reflect a group (or groups) other than 'Any', or
 - ii. the existing config with a group of 'Any' is deleted
4. If a config with a group of 'Any' must be created, delete all other configs first.

* Select User Identity Groups

continue, logoff or remediate

- Configurable per Role = User ID group

Let's configure it!



Let's check the running firewall service

The screenshot displays the Cisco Identity Services Engine (ISE) interface for configuring Posture Policies. The navigation bar includes Home, Operations, Policy, and Administration. The main menu shows Authentication, Authorization, Profiling, Posture, Client Provisioning, Security Group Access, and Policy Elements. The Posture Policy configuration page shows a table of policies with the following columns: Status, Rule Name, Identity Groups, Operating Systems, Other Conditions, and Requirements.

Status	Rule Name	Identity Groups	Operating Systems	Other Conditions	Requirements
⊘	Policy_Check_Fo	Any	Mac OSX	(Optional) Dictionary Attr...	Any_AS_D...
✓	Policy_Check_Fo	Any	Windows All	(Optional) Dictionary Attr...	Any_AS_D...
⊘	Policy_Check_Fo	Any	Mac OSX	(Optional) Dictionary Attr...	Any_AS_I...
✓	Policy_Check_Fo	Any	Windows All	(Optional) Dictionary Attr...	Any_AS_I...
⊘	Policy_Check_Fo	Any	Mac OSX	(Optional) Dictionary Attr...	Any_AV_D...
✓	Policy_Check_Fo	Any	Windows All	(Optional) Dictionary Attr...	Any_AV_D...
⊘	Policy_Check_Fo	Any	Mac OSX	(Optional) Dictionary Attr...	Any_AV_I...
✓	Policy_Check_Fo	Any	Windows All	(Optional) Dictionary Attr...	Any_AV_I...
✓	firewall	Any	Windows All	(Optional) Dictionary Attr...	firewall-ser...

Notification: Server Response All operations completed successfully

Posture Status Monitoring

Authentications | Endpoint Protection Service | Alarms | Reports | Troubleshoot

Live Authentications

Refresh Every 3 seconds | Show Latest 20 records | within Last 24 hours

Time	Status	Details	Username	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status
Dec 21,11 01:35:43.142 AM	✓		gacs@cisco.com	00:0C:29:A9:C7:6C					Guest	
Dec 21,11 01:35:42.832 AM	✓		00:30:05:9E:58:10	00:30:05:9E:58:10	10.1.1.51	sw	FastEthernet1/0/16	web-auth		Pending
Dec 21,11 01:35:25.434 AM	✓		00:0C:29:A9:C7:6C	00:0C:29:A9:C7:6C	10.1.1.53	sw	FastEthernet1/0/16	web-auth		Pending
Dec 21,11 01:29:03.236 AM	✓		gacs@cisco.com	00:0C:29:A9:C7:6C					Guest	
Dec 21,11 01:28:41.192 AM	✓		00:0C:29:A9:C7:6C	00:0C:29:A9:C7:6C	10.1.1.53	sw	FastEthernet1/0/16	web-auth		Pending
Dec 21,11 01:28:31.622 AM	✓		00:30:05:9E:58:10	00:30:05:9E:58:10	10.1.1.51	sw	FastEthernet1/0/16	web-auth		Pending
Dec 21,11 01:20:18.184 AM	✓		gacs@cisco.com	00:0C:29:A9:C7:6C					Guest	
Dec 21,11 01:19:17.488 AM	✓		gacs@cisco.com	00:0C:29:A9:C7:6C					Guest	
Dec 21,11 01:18:08.938 AM	✓		00:30:05:9E:58:10	00:30:05:9E:58:10	10.1.1.51	sw	FastEthernet1/0/16	web-auth		Pending
Dec 21,11 01:17:51.800 AM	✓		00:0C:29:A9:C7:6C	00:0C:29:A9:C7:6C	10.1.1.53	sw	FastEthernet1/0/16	web-auth		Pending

Posture Log

Identity Services Engine

Username: user2
Mac Address: 00:0C:29:D0:E2:82
IP address: 10.100.10.11
Session ID: 0A64C8010005B9CC3E9EC55C
Client Operating System: Windows 7 Enterprise 64-bit AMD
Client NAC Agent: Cisco NAC Agent for Windows 4.9.0.15
PKA Enforcement: Yes
CoA: N/A
PRA Grace Time: 5
PRA Interval: 60
PRA Action: remediate
User Agreement Status: NotEnabled
System Name: PCLAB-7-064
System Domain: bnlab-fr.cisco.com
System User: user2
User Domain: BNLAB-FR

Product Name	Product Id	Product Version	Definition Version	Definition Date
McAfee VirusScan Enterprise	McAfeeAV	8.7.0.570	6316	04/14/2011

Product Name	Product Id	Product Version	Definition Version	Definition Date
Windows Defender	MicrosoftAS	6.1.7600.16385	1.93.917.0	11/01/2010
McAfee AntiSpyware Enterprise Module	McAfeeAS	8.7.0.129	6316	04/14/2011

Posture Report
Posture Status: Compliant
Logged At: Apr 15, 2011 5:46:35 142 PM

User2, Windows 7 64 bits, Av McAfee, Antispyware, MS and McAfee, result: compliant

Posture Reports

- Posture Report (Monitor -> Reports -> Catalog -> Posture)

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Monitor', 'Policy', and 'Administration'. Below this, there are tabs for 'Authentications', 'Endpoint Protection Service', 'Alarms', 'Reports', and 'Troubleshoot'. The 'Reports' tab is active, and the 'Catalog' sub-tab is selected. On the left, a 'Reports' sidebar lists various report categories, with 'Posture' selected. The main content area is titled 'Posture' and contains a table of reports. A red box highlights the table, which has columns for 'Report Name' and 'Type'. The table lists two reports: 'Posture Detail Assessment' and 'Posture Trend', both of type 'System Report'. Below the table are buttons for 'Run', 'Add To Favorite', and 'Delete'. A help message at the bottom explains that for 'System Report' type reports, users should hover over the 'Report Name' and click on it to run the report for today, and then click on 'Run' to select additional options.


Reports

- AAA Protocol
- Allowed Protocol
- Server Instance
- Endpoint
- Failure Reason
- Network Device
- User
- Security Group Access
- Session Directory
- Posture

Posture

Filter:

Report Name	Type
<input type="radio"/> Posture Detail Assessment	System Report
<input type="radio"/> Posture Trend	System Report

 For reports of type 'System Report', hover mouse over the 'Report Name'. Click on 'Report Name' to run report for today. Select a Report and click on 'Run' button to select additional options.

DEMO



Best Practices, considerations

- **Design Posture:** Describe posture policy requirements for endpoint compliance. This may include many areas such as asset checking, application and services checking, and antivirus and antispyware checks, as well as customized checks for specific use cases. Describe remediation plans and include remediation servers that need to be integrated into the design.

Rule Name	OS (Windows /MacOS)	Conditions	Posture Agent	Checks	Remediation	Enforcement (Audit/Opt/Mandatory)	When Assessed (Login/PRA/Both)
Employee_AV	Windows XP/7	AD group= Employee	NAC Agent for Windows	AV Rule: Microsoft Security Essentials 2.x	Live update (Automatic)	Mandatory	Both
Employee_Asset	Windows XP/7	AD group= Employee	NAC Agent for Windows	Custom registry check	Link redirect to policy page (Manual)	Mandatory	Login
Contractor_AV	Windows ALL	ID Group= Contractor	Web Agent	AV_Rule: Any AV w/current signatures	Local Message regarding AV Policy	Mandatory	Login

Summary

- Integrated Posture Assessment

- Part of TrustSec

- Standard 802.1X and Posture

- Policy based provisioning

- Wired, wireless and VPN*

- Corporate users (802.1X) and Guest (WebAuth)

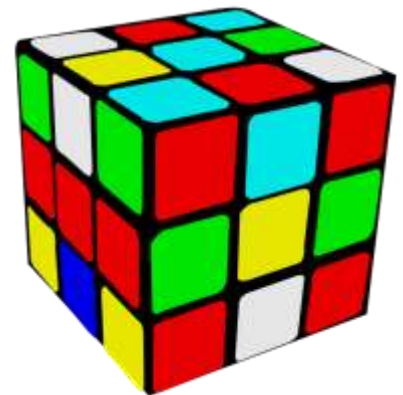
- Leveraged NAC Appliance architecture

- Flexible configuration

- Preconfigured policy set

- User configurable policies

$$\int_b^a f(x)dx$$



Otázky a odpovědi

- Twitter www.twitter.com/CiscoCZ
- Talk2Cisco www.talk2cisco.cz/dotazy
- SMS 721 994 600

- Zveme Vás na **Ptali jste se...** v sále **LEO**
 - 1.den 17:45 – 18:30
 - 2.den 16:30 – 17:00

**Prosíme, ohodnot'te
tuto přednášku.**

