



Cisco ISE Integration with OPSWAT Gears for checking Disk Encryption

Imran Bashir
Cisco Technical Marketing



Table of Contents

Table of Contents	2
Introduction.....	3
What Is the Cisco TrustSec System?.....	4
About the TrustSec How-To Guides	4
Overview.....	5
Solution.....	6



Introduction

Cisco ISE can perform posture assessments to endpoints connected to the network and enforces the appropriate compliance policies for endpoints through a persistent client-based agent or a temporal agent.

With Cisco ISE administrators have the ability to create powerful policies that include, but are not limited to, checks for the latest OS patch, antivirus and antispymware packages with current definition file variables (version, date, etc.), antimalware packages, registry settings (key, value, etc.), patch management, disk encryption, mobile PIN-lock or rooted or jailbroken status, application presence, and USB-attached media.

Cisco ISE also supports automatic remediation of PC clients as well as periodic reassessments alongside leading enterprise patch-management systems to make sure the endpoint is not in violation of company policies.

What Is the Cisco TrustSec System?

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

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

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

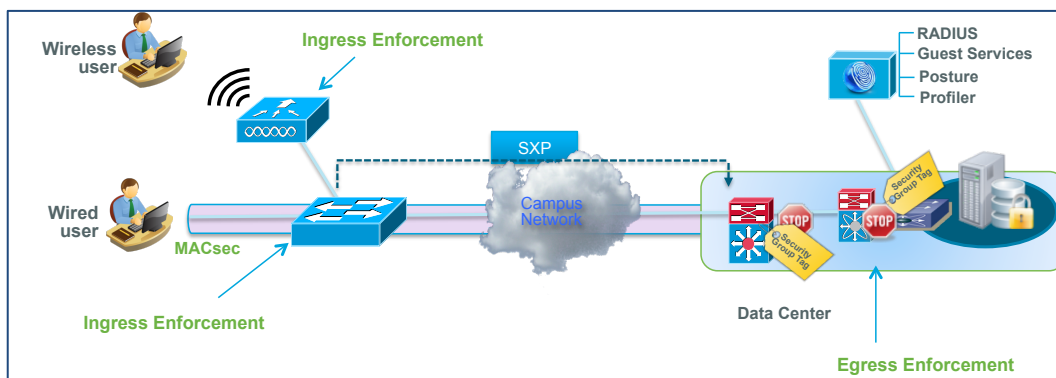


Figure 1.

About the TrustSec How-To Guides

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



Overview

This document covers how can administrators can write a policy to check for multiple disk encryption vendors across their users, with Cisco ISE administrator can create multiple disk encryption conditions by comining the posture conditions into a single posture requirement with the "Any selected conditions succeeds option".

In summary, the document covers the following

- Demonstrate Disk Encryption checks using Cisco ISE for Windows and OSX platforms
- Use Agents for Encryption checks for Employees and dissolvable agents for contractors or guest



Solution

Windows: OPSWAT can edit the registry settings for windows when the disk encryption is ON/ OFF, later NAC agent can check on that registry setting and use it as posture

OSx: OPSWAT can create a file for Osx when the disk encryption is ON/ OFF, but **OSx NAC agent can only check for AV/ AS and cannot check for files**

Leverage OPSWAT agent and dissolvable agent to check for disk encryption on/ off

1. As mentioned earlier Customer is requiring ISE to check for disk encryption on Osx which is not possible today with NAC agent
2. Customer is using OPSWAT Gears which can check for disk encryption
3. ISE today can add GEARS as the AV posture check but cannot check on Definition update

[Anti-virus Compound Conditions List](#) > [New Anti-virus Compound Condition](#)

AV Compound Condition

* Name

Description

* Operating System

Vendor

Check Type Installation Definition

▼ **Products for Selected Vendor**

	Product Name	Version	Remediation Support	Definition Check
<input type="checkbox"/>	ANY	ANY	N/A	NO
<input checked="" type="checkbox"/>	GEARS Client	4.x	NO	NO

4. OPSWAT provided an enhancement (July 15th, 2014) for V2 library where NAC agent can now match on definition update
5. Logic is that if Disk is NOT encrypted return a date which is older than 999 days (e.g. 1969)
6. If disk encryption is enabled, return today's date.
7. ISE policies will match on definition dates and make the posture decision.

Window's OS: OPSWAT agent can update registry settings when the encryption is on/ off.

OPSWAT Persistent Agent changes the following registry setting

Compliance Check: HKEY_LOCAL_MACHINE\Software\Wow6432Node\OPSWAT\Gears Client\Status

Key Check: HKEY_LOCAL_MACHINE\Software\Wow6432Node\OPSWAT\Gears Client\Config

OPSWAT dissolvable/ on-demand Agent changes the following registry setting

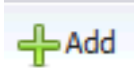
Compliance Check: HKEY_CURRENT_USER\Software\OPSWAT\Gears OnDemand\Config

Key Check: HKEY_CURRENT_USER\Software\OPSWAT\Gears OnDemand\Config



Step 1: Create the following 4 Posture registry conditions and a posture compound condition to check for Windows registry checks

Policy -> Conditions -> Posture -> Registry Conditions



Click

GEARSCOMP_INSTALL = Registry check for OPSWAT persistent agent which will check for compliance, if disk is encrypted OPSWAT persistent agent will set this registry as 1 otherwise as 0

Registry Conditions List > GEARSCOMP_INSTALL

Registry Condition

* Name	GEARSCOMP_INSTALL		
Description	Gears posture check		
Registry Type	RegistryValue		
Registry Root Key	HKLM	* Sub Key	Software\Wow6432Node\OPSW (enter sub-key without leading backslash)
* Value Name	Policy		
Value DataType	String		
Value Operator	equals		
Value Data	1		
* Operating System	Windows All		
<input type="button" value="Save"/> <input type="button" value="Reset"/>			

NOTE: Sub Key = Software\Wow6432Node\OPSWAT\Gears Client\Status

GEARSKEY_INSTALL = Registry check for OPSWAT Key which will ensure that its the same/ corporate account key, if key is NOT included in the posture check then anyone can sign-up for OPSWAT account and have their own policy checks.

Registry Conditions List > GEARSKEY_INSTALL

Registry Condition

* Name	GEARSKEY_INSTALL		
Description	Gears posture check for Key		
Registry Type	RegistryValue		
Registry Root Key	HKLM	* Sub Key	Software\Wow6432Node\OPSW (enter sub-key without leading backslash)
* Value Name	RegistrationKey		
Value DataType	String		
Value Operator	equals		
Value Data	71017c3b32c661bdb631925a37		
* Operating System	Windows All		
<input type="button" value="Save"/> <input type="button" value="Reset"/>			

NOTE: Sub Key = Software\Wow6432Node\OPSWAT\Gears Client\Config

GEARSCOMP = Registry check for OPSWAT dissolvable/ on-demand agent which will check for compliance, if disk is encrypted OPSWAT persistent agent will set this registry as 1 otherwise as 0



Registry Conditions List > GEARSCOMP

Registry Condition

* Name	<input type="text" value="GEARSCOMP"/>
Description	<input type="text" value="Gears posture check"/>
Registry Type	<input type="text" value="RegistryValue"/>
Registry Root Key	<input type="text" value="HKCU"/>
* Sub Key	<input type="text" value="Software\OPSWAT\Gears OnDer"/> (enter sub-key without leading backslash)
* Value Name	<input type="text" value="Policy"/>
Value DataType	<input type="text" value="String"/>
Value Operator	<input type="text" value="equals"/>
Value Data	<input type="text" value="1"/>
* Operating System	<input type="text" value="Windows All"/>

NOTE: Sub Key =Software\OPSWAT\Gears OnDemand\Config

GEARSKY = Registry check for OPSWAT Key which will ensure that its the same/ corporate account key, if key is NOT included in the posture check then anyone can sign-up for OPSWAT account and have their own policy checks.

Registry Conditions List > GEARSKY

Registry Condition

* Name	<input type="text" value="GEARSKY"/>
Description	<input type="text" value="Gears posture check for Key"/>
Registry Type	<input type="text" value="RegistryValue"/>
Registry Root Key	<input type="text" value="HKCU"/>
* Sub Key	<input type="text" value="Software\OPSWAT\Gears OnDer"/> (enter sub-key without leading backslash)
* Value Name	<input type="text" value="RegistrationKey"/>
Value DataType	<input type="text" value="String"/>
Value Operator	<input type="text" value="equals"/>
Value Data	<input type="text" value="71017c3b32c661bdb631925a37"/>
* Operating System	<input type="text" value="Windows All"/>

NOTE: Sub Key = Software\OPSWAT\Gears OnDemand\Config

Gears-OSx: AV compound condition for Osx to leverage OPSWAT agent definition date option, i.e. If date returned is today's date then Osx disk encryption is ON, else if date return is older than 999 days then Osx disk encryption is OFF



Anti-virus Compound Conditions List > Gears-OSx

AV Compound Condition

* Name

Description

* Operating System

Vendor

Check Type Installation Definition

Check against latest AV definition file version if available. Otherwise check against latest definition file date.

Allow virus definition file to be days older than latest file date current system date

Products for Selected Vendor

	Product Name	Version	Remediation Support	Definition Check	Latest Definition Date
<input type="checkbox"/>	ANY	ANY	N/A	NO	
<input checked="" type="checkbox"/>	GEARS Client	10.x	NO	YES	07/20/2014
<input type="checkbox"/>	GEARS Client	4.x	NO	NO	
<input type="checkbox"/>	GEARS Client	7.x	NO	NO	

Gears_Chk: Finally create a compound condition to combine these checks for windows

Policy -> Conditions -> Posture -> Compound Conditions



Click

Compound Conditions List > Gears_Chk

Compound Condition

* Name

Description

* Operating System

Select a condition to insert below

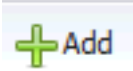
(GEARSCOMP & GEARSKEY) | (GEARSCOMP_INSTALL & GEARSKEY_INSTALL)

NOTE: Expression = (GEARSCOMP & GEARSKEY) | (GEARSCOMP_INSTALL & GEARSKEY_INSTALL)



Step 2: Create a Posture requirement to use the above created conditions

Policy -> Results -> Posture -> Requirements



Click

GEARS Win: Posture requirement to check for Windows registry compliance and Key check for both OPSWAT persistent or OPSWAT on-demand agents

GEARS Win for Windows All met if Gears_Chk else Message Text Only

Action Message Text Only

Message Shown to Agent User Client Disk Encryption is Disabled
Please enable Disk Encryption to proceed.

GEARS-OSx: Requirement check for Osx leveraging the AV compound condition created earlier for OPSWAT definition check

GEARS-OSx for Mac OSX met if Gears-OSx else Message Text Only

Action Message Text Only

Message Shown to Agent User Disk Encryption not enabled
Please enable disk encryption or contact admin

OPTIONAL: If there is an issue with compound condition, please create individual conditions without using the compound condition e.g.

GEARS:

GEARS for Windows All met if GEARSKEY & GEARS COMP else Message Text Only

Action Message Text Only

Message Shown to Agent User Client Disk Encryption is Disabled
Please enable Disk Encryption to proceed.

Step 3: Create posture policies for Osx and Windows

Policy -> Posture

OS X If Any and Mac OSX then GEAR-OSx



Windows 7 GEARS If Any and Windows 7 (All) then GEARS Win

Step 4: Finally create the Authorization Policies

Policy Result Authorization Profile

Policy -> Results -> Authorization -> Authorization Profiles

Posture Remediation

Authorization Profiles > Posture Remediation

Authorization Profile

* Name Posture Remediation

Description

* Access Type ACCESS_ACCEPT

Service Template

DACL Name POSTURE_REMEDIATION_ACL

VLAN Tag ID 1 Edit Tag ID/Name 10

Web Redirection (CWA, DRW, MDM, NSP, CPP)

Client Provisioning (Posture)

ACL ACL-AGENT-REDIRECT-2

Attributes Details

```
Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = :10
Tunnel-Type=1:13
Tunnel-Medium-Type=1:6
DACL = POSTURE_REMEDIATION_ACL
cisco-av-pair = url-redirect-ac=ACL-AGENT-REDIRECT-2
cisco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cpp
Session-Timeout = 1800
Termination-Action = RADIUS-Request
Idle-Timeout = 1200
```

Employee Access:



Authorization Profiles > Employee_Access

Authorization Profile

* Name

Description

* Access Type

Service Template

Common Tasks

DACL Name

VLAN Tag ID **1** ID/Name

Airespace ACL Name

Attributes Details

```
Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:10
Tunnel-Type=1:13
Tunnel-Medium-Type=1:6
DACL = EMPLOYEE_ACL
Airespace-ACL-Name = EMPLOYEE_ACL
Session-Timeout = 36000
Termination-Action = RADIUS-Request
Idle-Timeout = 1800
```

Now Create Authorization Policy

Policy -> Authorization

Pre-Compliant Authorization policy

<input checked="" type="checkbox"/>	Pre-Compliant	if (Radius:Service-Type EQUALS Framed AND Session:PostureStatus NOT_EQUALS Compliant)	then Posture_Remediation
-------------------------------------	---------------	--	--------------------------

Compliant Authorization policy

<input checked="" type="checkbox"/>	EMPLOYEES Compliant	if EMPLOYEES AND PostureCompliant	then Employee_Access
-------------------------------------	---------------------	-----------------------------------	----------------------

Authorization Simple Condition Details

Name	PostureCompliant
Description	Session:PostureStatus Equals Compliant
Condition	Session:PostureStatus EQUALS Compliant

PostureCompliant details =