

## PEAP-TLS: Microsoft Supplicant configuration (Windows 7) and Aruba ClearPass

This document describes how to configure ClearPass and Windows 7 for PEAP-TLS (Microsoft PEAP with Client Certificate authentication). ClearPass Policy manager version 6.2.4 was used to test and create the procedure below, however earlier versions of ClearPass should work similar.

PEAP-TLS uses EAP PEAP as the outer-tunnel (authentication session protection), and EAP-TLS as the inner tunnel (authentication). The use of PEAP as the outer-tunnel allows the use of Microsoft NAP for posture assessment. First, EAP-PEAP will be configured, later in this document that will be extended with basic Microsoft NAP posture.

Certificates were enrolled from a Windows 2008R2 domain controller running the Microsoft Enterprise PKI (Certificate Services).

Document version is 1.0-20140114. Please send updates for this document to hrobers at arubanetworks.com.

### ClearPass Configuration

In the Service Authentication tab, select both TLS and PEAP authentication methods, select your AD as authentication source, and configure 'Strip usernames' because the certificate contains the username as [user@domain.tld](#), and AD recognizes only the user part.

Configuration » Services » Edit - WLAN-WPA2

#### Services - WLAN-WPA2

Summary	Service	Authentication	Authorization	Roles	Enforcement
<b>Authentication Methods:</b>					
		EAP TLS - OCSP [EAP PEAP]	<div>Move Up</div> <div>Move Down</div> <div>Remove</div> <div>View Details</div> <div>Modify</div>		
		--Select to Add--			
<b>Authentication Sources:</b>					
		[Local User Repository] [Local SQL DB] dc-02.nl [Active Directory]	<div>Move Up</div> <div>Move Down</div> <div>Remove</div> <div>View Details</div> <div>Modify</div>		
		--Select to Add--			
<b>Strip Username Rules:</b>					
		<input checked="" type="checkbox"/> Enable to specify a comma-separated list of rules to strip username prefixes or suffixes user:@ If username precedes domain name, use user:<separator> (e.g., user:@) Otherwise, use <separator>:user (e.g., \:user)			

The EAP-TLS – OSCP is a Authentication method with OSCP configured:

**Edit Authentication Method**

**General**

Name: EAP TLS - OSCP

Description: Default settings for EAP-TLS

Type: EAP-TLS

**Method Details**

Session Resumption: ☒ Enable

Session Timeout: 6 hours

Authorization Required: ☒ Enable

Certificate Comparison: Do not compare

Verify Certificate using OSCP: Optional

Override OSCP URL from Client: ☐ Enable

OCSP URL:

Copy Save Cancel

OCSP is optional and during testing you may want not to do OCSP and Authorization.

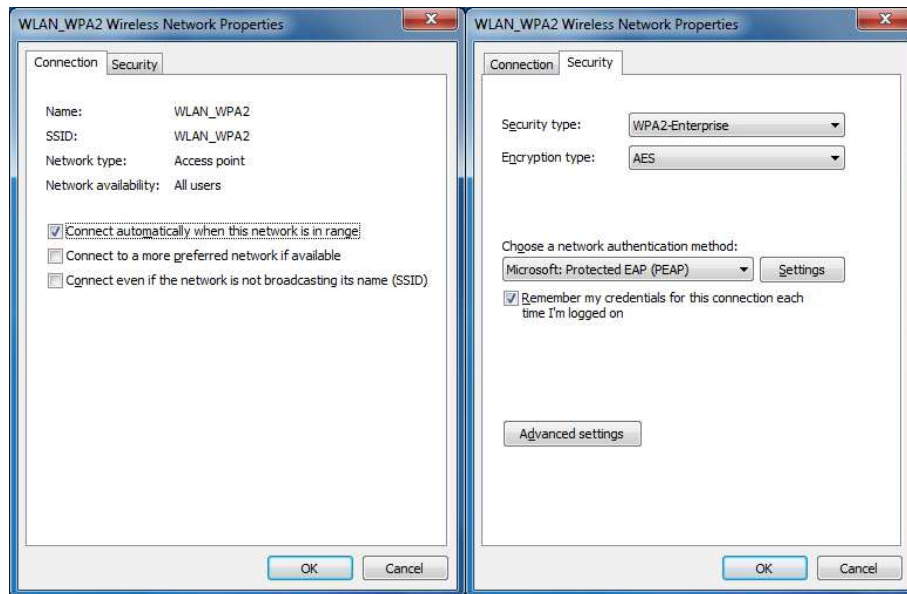
Also optional, in the role-mapping you may use information from the certificate (like Subject-DN in the screenshot below); or from AD (like Authorization:dc-02.nl:Groups in the screenshot below):

#### Role Mappings - Lab-role-mapping

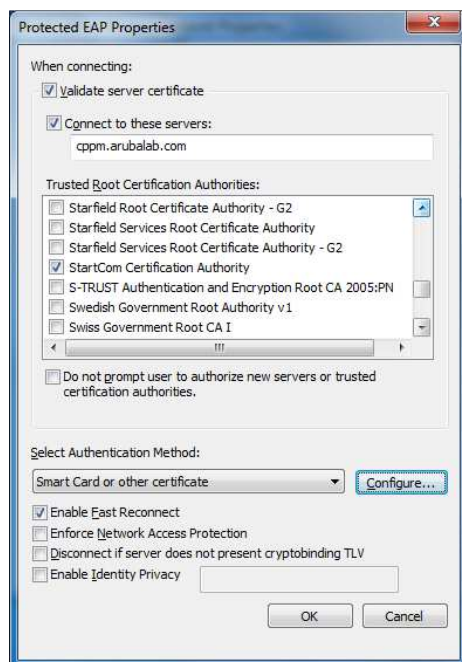
Summary	Policy	Mapping Rules
<b>Policy:</b>		
Policy Name:	Lab-role-mapping	
Description:		
Default Role:	[Guest]	
<b>Mapping Rules:</b>		
Rules Evaluation Algorithm:	Evaluate all	
Conditions	Role Name	
1. (Authorization:dc-02.nl:Groups EQUALS LABEmployee)	[Employee]	
2. (Authentication:OuterMethod EQUALS EAP-PEAP)	PEAP-User	
3. (Authorization:dc-02.nl:Groups EQUALS Domain Admins)	Domain Admins	
4. (Certificate:Subject-DN CONTAINS NL)	[Other]	
5. (Connection:Client-Mac-Address BELONGS_TO_GROUP prefix-08-00-07)	[MAC Caching]	
6. (Authorization:[Endpoints Repository]:OS Family EQUALS Apple)	[Onboard iOS]	
7. (Certificate:Subject-DN EQUALS %{Endpoint:Certificate})	CertificateMatch	

## Microsoft Supplicant configuration (Windows 7)

Configure WPA2-Enterprise, and PEAP on the security tab of the network configuration:

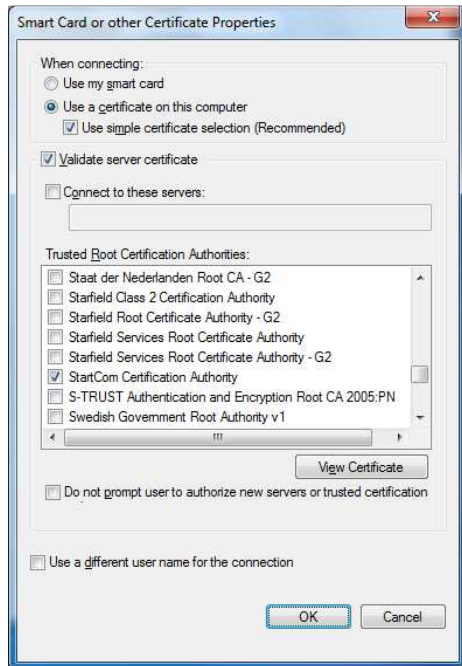


Go to the PEAP Settings. In the PEAP Settings configure server certificate validation (you may leave this turned off during testing), and select the **Authentication method: Smartcard or Certificate**:

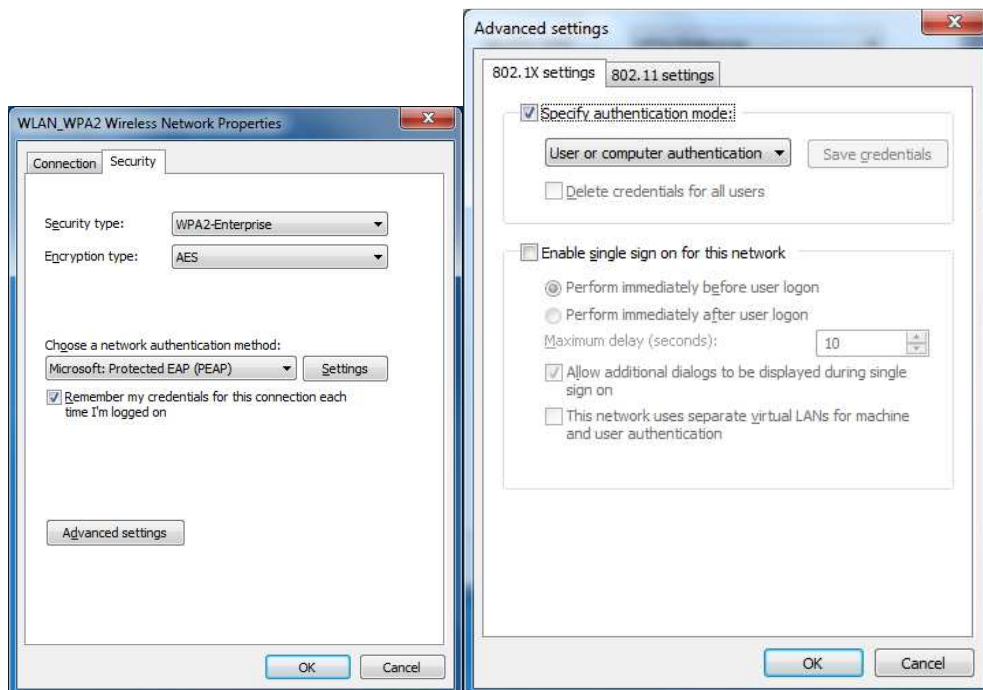


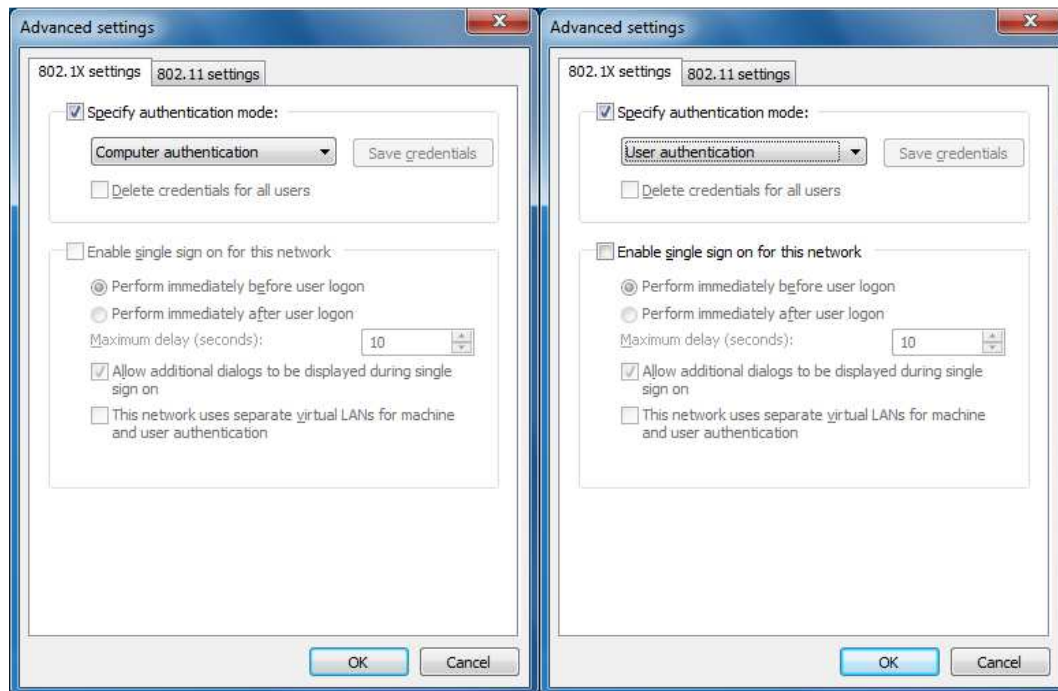
Note that Enforce Network Access Protection is an option here; it is not with EAP-TLS!

In Configure configure the server certificate validation again, now for the inner TLS tunnel. The previous configuration was for the Outer PEAP tunnel. For client certificates enrolled from the AD Microsoft Enterprise CA to your computer, select 'Use a certificate on this computer'.



Return to the Security tab top-level, and press Advanced settings. Here you can select if a user certificate should be used (User authentication), the computer certificate (Computer authentication) or your system should switch from a Computer certificate when no user is logged in to a User certificate if a user is logged in:

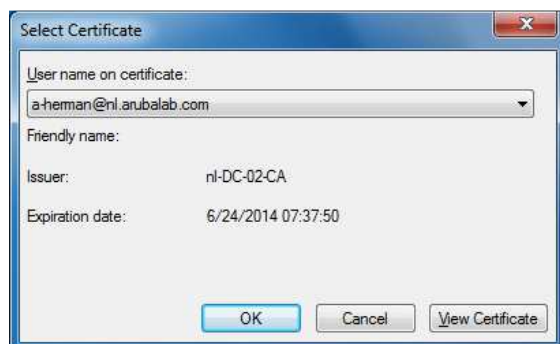




Note that when switching from Computer to User authentication, a short interruption of the network connectivity will occur. If you also switch VLANs (different VLAN for computer authentication than for user authentication), use the 'Enable single sign on for this network' option. Safe value in most cases is to use only computer authentication, as that is always available; but that will not allow you to create user-based policies.

## First time connect

On the first time connect: you are requested for more information, select your certificate. Only if you have more than one client certificate.



## Validating the authentication in the ClearPass Access-Tracker

The Access Tracker shows successful authentications if everything is configured correctly:

192.168.32.22	RADIUS	a-herman@nl.arubalab	WLAN-WPA2	ACCEPT	2014/01/14 10:16:25
192.168.32.22	RADIUS	host/LAB-WIN7-01.nl.	WLAN-WPA2	ACCEPT	2014/01/14 10:15:49

**Request Details**

**Summary** Input Output

Session Identifier:	R00000dc2-08-52d50045
Date and Time:	Jan 14, 2014 10:15:49 CET
End-Host Identifier:	0016CE2CB280
Username:	host/LAB-WIN7-01.nl.arubalab.com
Access Device IP/Port:	192.168.31.1:0
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	WLAN-WPA2
Authentication Method:	EAP-PEAP,EAP-TLS
Authentication Source:	AD:dc-02.nl.arubalab.com
Authorization Source:	[Endpoints Repository], dc-02.nl
Roles:	PEAP-User, [Machine Authenticated], [Other]
Enforcement Profiles:	[Update Endpoint Known], Set Domain, Role-machine
Service Monitor Mode:	Disabled

Change Status Export Show Logs Close

**Request Details**

**Summary** Input Output

Radius:IETF:Service-Type	1
Radius:IETF:User-Name	host/LAB-WIN7-01.nl.arubalab.com
Radius:Microsoft:MS-MPPE-Recv-Key	0x7a5e5d0f24ad19d4021619bc1afd942307eac2409376c7b4aed1b39f042f6e9
Radius:Microsoft:MS-MPPE-Send-Key	0x2aa2536722160c90b050978117d06cfd0d77f0b33fcaac75140feb9d61fa99

Authorization Attributes

Authorization:dc-02.nl:UserDN	CN=LAB-WIN7-01,CN=Computers,DC=nl,DC=arubalab,DC=com
-------------------------------	--

## Request Details

## Summary

## Input

## Output

Certificate:Issuer-CN	nl-DC-02-CA
Certificate:Issuer-DC	com, arubalab, nl
Certificate:Issuer-DN	CN=nl-DC-02-CA,DC=nl,DC=arubalab,DC=com
Certificate:Not-Valid-After	2014-06-30 19:26:51
Certificate:Serial-Number	49:9b:82:0c:00:00:00:00:13
Certificate:Subject-AltName-DNS	LAB-WIN7-01.nl.arubalab.com
Certificate:Subject-CN	LAB-WIN7-01.nl.arubalab.com
Certificate:Subject-DN	CN=LAB-WIN7-01.nl.arubalab.com
Certificate:Version	3

Certificate:Issuer-CN	nl-DC-02-CA
Certificate:Issuer-DC	com, arubalab, nl
Certificate:Issuer-DN	CN=nl-DC-02-CA,DC=nl,DC=arubalab,DC=com
Certificate:Not-Valid-After	2014-06-30 19:26:51
Certificate:Serial-Number	49:9b:82:0c:00:00:00:00:13
Certificate:Subject-AltName-DNS	LAB-WIN7-01.nl.arubalab.com
Certificate:Subject-CN	LAB-WIN7-01.nl.arubalab.com
Certificate:Subject-DN	CN=LAB-WIN7-01.nl.arubalab.com
Certificate:Version	3

## Request Details

## Summary

## Input

## Output

Session Identifier:	R00000dc3-08-52d50069
Date and Time:	Jan 14, 2014 10:16:25 CET
End-Host Identifier:	0016CE2CB280
Username:	a-herman@nl.arubalab.com
Access Device IP/Port:	192.168.31.1:0
System Posture Status:	UNKNOWN (100)

## Policies Used -

Service:	WLAN-WPA2
Authentication Method:	EAP-PEAP,EAP-TLS
Authentication Source:	AD:dc-02.nl.arubalab.com
Authorization Source:	[Endpoints Repository], dc-02.nl
Roles:	Domain Admins, PEAP-User, [Machine Authenticated], [Other], [User Authenticated]
Enforcement Profiles:	Admin-X, Session-timeout 15 minutes
Service Monitor Mode:	Disabled

Change Status

Export

Show Logs

Close









## Adding Microsoft NAP to the Service

One of the reasons to use PEAP-TLS is for Microsoft NAP. NAP requires PEAP as the outer-tunnel. This section shows how to create and validate a basic NAP policy. Note that Posture processing is part of ClearPass Onguard, and Onguard licensing applies. Each ClearPass appliance comes with a 25 device Enterprise license which makes OnGuard available for 25 devices without additional licensing.

## ClearPass Service configuration

In the ClearPass service, enable Posture under the Service tab. The Posture tab should now appear:

### Services - WLAN-WPA2

Summary	Service	Authentication	Authorization	Roles	Posture	Enforcement
Name:	WLAN-WPA2					
Description:	Aruba 802.1X Wireless Access Service					
Type:	Aruba 802.1X Wireless					
Status:	Enabled					
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement					
More Options:	<input checked="" type="checkbox"/> Authorization <input checked="" type="checkbox"/> Posture Compliance <input type="checkbox"/> Audit End-hosts <input type="checkbox"/> Profile Endpoints					
<b>Service Rule</b>						
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions:						
Type	Name	Operator	Value			
1. Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)	 		
2. Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)	 		
3. Radius:Aruba	Aruba-Essid-Name	EXISTS		 		
4. Click to add...						

On the posture tab create a NAP service. Leave Posture Servers empty, as ClearPass has a Posture server built-in:

### Services - WLAN-WPA2

Summary	Service	Authentication	Authorization	Roles	Posture	Enforcement
<b>Posture Policies:</b>						
Posture Policies: Only NAP agent type posture policies are applicable for this service						
		NAP-Windows		<a href="#">Remove</a> <a href="#">View Details</a> <a href="#">Modify</a>		
		--Select to Add--		<a href="#">Add new Posture Policy</a>		
Default Posture Token: UNKNOWN (100)						
Remediate End-Hosts: <input type="checkbox"/> Enable auto-remediation of non-compliant end-hosts						
Remediation URL: <input type="text"/>						
<b>Posture Servers:</b>						
				<a href="#">Remove</a> <a href="#">View Details</a> <a href="#">Modify</a>		
		--Select to Add--		<a href="#">Add new Posture Server</a>		



## Posture Policies - NAP-Windows

Summary	Policy	Posture Plugins	Rules
<b>Policy:</b>			
Policy Name:	NAP-Windows		
Description:			
Posture Agent:	Supplicant		
Host Operating System:	WINDOWS		
Restrict by Roles:	null		
<b>Posture Plugins:</b>			
The list of selected plugins:			
Plugin Name	Plugin Configuration	Status	
1. Windows System Health Validator	<a href="#">View</a>	Configured	
2. Windows Security Health Validator	<a href="#">View</a>	Configured	
<b>Rules:</b>			
Rules Evaluation Algorithm: First applicable			
Conditions	Posture Token		
1. Passes all SHV checks - Windows System Health Validator Windows Security Health Validator	HEALTHY		
2. Fails one or more SHV checks - Windows System Health Validator Windows Security Health Validator	INFECTED		

**Windows Security Health Validator**

Antivirus Application up to date: Enabled

**Windows 7:**  
Virus Protection Check: Enabled  
Antivirus Application up to date: Enabled

**Automatic Updates**  
**Windows 7:**  
Automatic Updates Check: Enabled

**Security Updates**  
**Windows 8:**  
Client must have all available security updates installed: Important and above  
Client must have checked for new security updates within last: 120 hours

**Windows 7:**  
Client must have all available security updates installed: Important and above  
Client must have checked for new security updates within last: 22 hours

Close

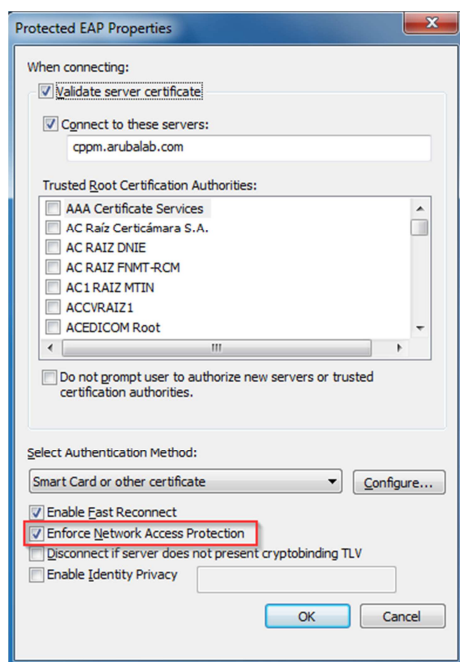
## Windows 7 client configuration

Enabling NAP on Windows 7 takes several steps:

1. NAP Agent is disabled by default. Turn it on in Network Services, then Network Access Protection Agent, switch it on and make it start Automatic.
2. Wired Zero Config (802.1x) is disabled by default, turn on (+ automatic start): Wired AutoConfig service; if you want to do NAP on wired (not WLAN)
3. WLAN Zero Config (802.1x) is enabled by default; leave it that way if you want NAP over WLAN.
4. Enable the NAP Client components
  - Run napclcfg.msc
  - Go to "Enforcement Clients"
  - Enable "EAP Quarantine Enforcement Client"

NAP only works on PEAP secured connections.

Enable NAP in the Supplicant on the client under PEAP Settings:



## Validation in the access-tracker

The access-tracker should now show the posture status of the device:

**Request Details**

Summary Input Output Accounting

Session Identifier:	R00000dcb-08-52d510a5
Date and Time:	Jan 14, 2014 11:25:42 CET
End-Host Identifier:	0016CE2CB280
Username:	a-herman@nl.arubalab.com
Access Device IP/Port:	192.168.31.1:0
System Posture Status:	HEALTHY (0)

**Policies Used -**

Service:	WLAN-WPA2
Authentication Method:	EAP-PEAP,EAP-TLS
Authentication Source:	AD:dc-02.nl.arubalab.com
Authorization Source:	[Endpoints Repository], dc-02.nl
Roles:	Domain Admins, PEAP-User, [Machine Authenticated], [Other], [User Authenticated]
Enforcement Profiles:	Admin-X, Session-timeout 15 minutes
Service Monitor Mode:	Disabled

Change Status Export Show Logs Close

**Request Details**

Summary Input Output Accounting

**Authorization Attributes**

**Posture Request**

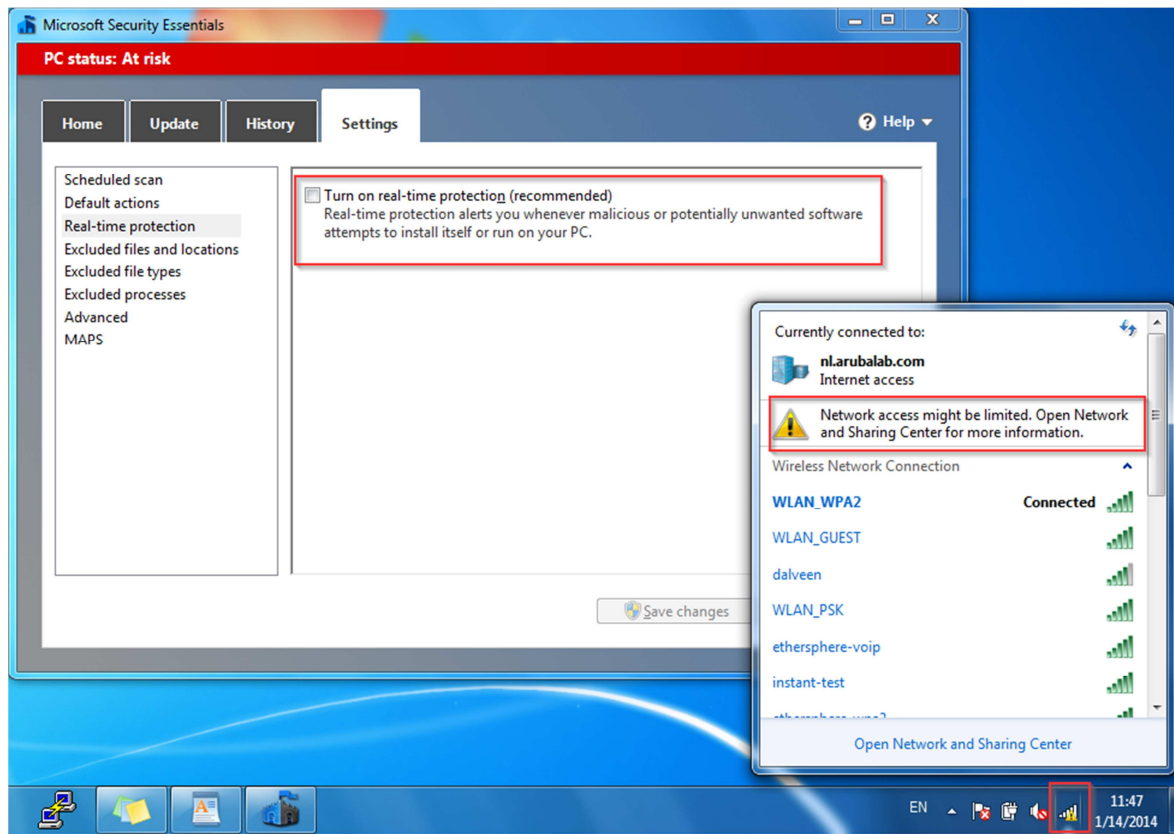
OS:ServicePack	1
OS:Version	Windows 7
SecurityCenter:AntiSpyware:Enabled	Yes
SecurityCenter:AntiSpyware:UpToDate	Yes
SecurityCenter:AntiVirus:Enabled	Yes
SecurityCenter:AntiVirus:UpToDate	Yes
SecurityCenter:AutomaticUpdate:Enabled	Yes
SecurityCenter:Firewall:Enabled	Yes
SecurityCenter:Updates:LastSync	20
SecurityCenter:Updates:Missing	None
SecurityCenter:WindowsServerUpdateServices:Enabled	No
SecurityCenter:WindowsUpdate:Enabled	Yes


**Computed Attributes**

Change Status Export Show Logs Close

## Disable anti-virus on the client

Now disable the antivirus to become non-compliant:



Note the yellow exclamation sign in your network icon in the taskbar:  as indication that something is wrong.

## Infected in Access Tracker

In the CPPM access-tracker, a new request came in:

**Request Details**

SummaryInputOutput

Session Identifier:	R00000dcc-08-52d51577
Date and Time:	Jan 14, 2014 11:46:15 CET
End-Host Identifier:	0016CE2CB280
Username:	a-herman@nl.arubalab.com
Access Device IP/Port:	192.168.31.1:0
System Posture Status:	INFECTED (30)

Policies Used -

Service:	WLAN-WPA2
Authentication Method:	EAP-PEAP
Authentication Source:	AD:dc-02.nl.arubalab.com
Authorization Source:	[Endpoints Repository], dc-02.nl
Roles:	Domain Admins, PEAP-User, [Machine Authenticated], [Other], [User Authenticated]
Enforcement Profiles:	Admin-X, Session-timeout 15 minutes
Service Monitor Mode:	Disabled

Change StatusExportShow LogsClose

**Request Details**

SummaryInputOutput

Authorization Attributes

Posture Request

OS:ServicePack	1
OS:Version	Windows 7
SecurityCenter:AntiSpyware:Enabled	No
SecurityCenter:AntiSpyware:UpToDate	Yes
SecurityCenter:AntiVirus:Enabled	No
SecurityCenter:AntiVirus:UpToDate	Yes
SecurityCenter:AutomaticUpdate:Enabled	Yes
SecurityCenter:Firewall:Enabled	Yes
SecurityCenter:Updates:LastSync	20
SecurityCenter:Updates:Missing	None
SecurityCenter:WindowsServerUpdateServices:Enabled	No
SecurityCenter:WindowsUpdate:Enabled	Yes

Change StatusExportShow LogsClose

## Using posture status in you policy

You can now use the Tips:Posture in your enforcement policy:

Rules Editor

Conditions

Match ALL of the following conditions:

Type	Name	Operator	Value
1. Tips	Posture	EQUALS	HEALTHY (0)
2. Click to add...			

Enforcement Profiles

Profile Names:

Move Up

Move Down

Remove

--Select to Add--

HEALTHY (0)

CHECKUP (10)

TRANSITION (15)

QUARANTINE (20)

INFECTED (30)

UNKNOWN (100)

Save

Cancel