



Cisco TrustSec How-To Guide: Central Web Authentication

For Comments, please email: howtoguides@external.cisco.com

Current Document Version: 3.0

August 27, 2012

Table of Contents

Table of Contents 1

Introduction 3

What Is the TrustSec System?3

About the TrustSec How-To Guides3

What does it mean to be "TrustSec Certified"? 4

Web Authentication 5

Why Web Authentication?5

Web Authentication Flow5

Central Web Authentication 7

CWA Configuration Explained..... 8

Access Control Lists Defined on a Cisco Switch for CWA.....8

Access control lists defined on a Cisco WLC for CWA8

Cisco ISE Authorization Profile for CWA 10

Appendix A: References..... 11

TrustSec System: 11

Device Configuration Guides: 11

Introduction

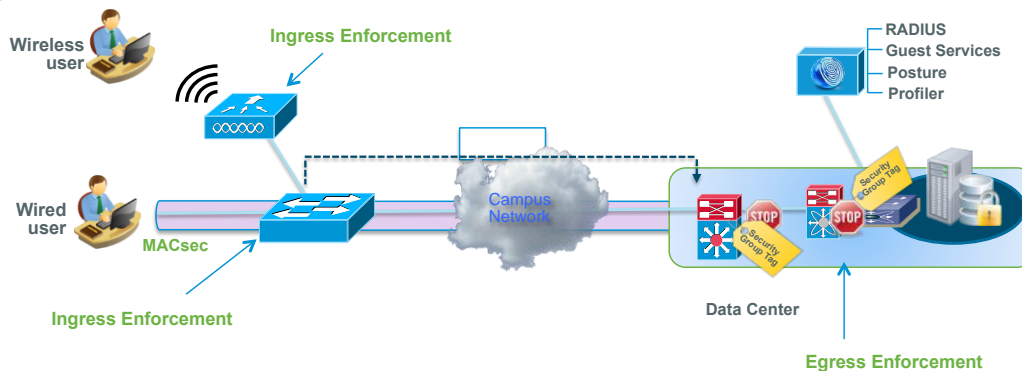
What Is the Cisco TrustSec System?

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 who 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: TrustSec Architecture Overview

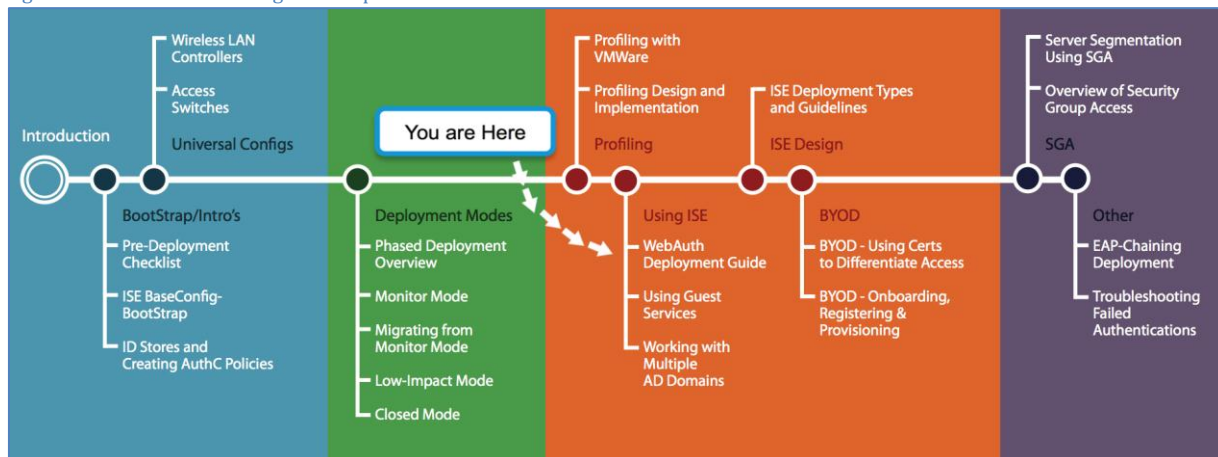


About the TrustSec How-To Guides

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 the entire system, or simply pick the single use-case that meets your specific need.

Each guide in this series comes with a subway-style “You Are Here” map to help you identify the stage the document addresses and pinpoint where you are in the TrustSec deployment process (Figure 2).

Figure 2: How-To Guide Navigation Map



What does it mean to be ‘TrustSec Certified’?

Each TrustSec version number (for example, TrustSec Version 2.0, Version 2.1, and so on) is a certified design or architecture. All the technology making up the architecture has undergone thorough architectural design development and lab testing. For a How-To Guide to be marked “TrustSec certified,” all the elements discussed in the document must meet the following criteria:

- Products incorporated in the design must be generally available.
- Deployment, operation, and management of components within the system must exhibit repeatable processes.
- All configurations and products used in the design must have been fully tested as an integrated solution.

Many features may exist that could benefit your deployment, but if they were not part of the tested solution, they will not be marked as “TrustSec “certified”. The TrustSec team strives to provide regular updates to these documents that will include new features as they become available, and are integrated into the TrustSec test plans, pilot deployments, and system revisions. (i.e., TrustSec 2.2 certification).

Additionally, many features and scenarios have been tested, but are not considered a best practice, and therefore are not included in these documents. As an example, certain IEEE 802.1X timers and local web authentication features are not included.

Note: Within this document, we describe the recommended method of deployment, and a few different options depending on the level of security needed in your environment. These methods are examples and step-by-step instructions for TrustSec deployment as prescribed by Cisco best practices to help ensure a successful project deployment.

Web Authentication

Why Web Authentication?

The TrustSec solution relies on three mechanisms to authenticate users and devices:

- IEEE 802.1X is the primary authentication protocol used for users and endpoints with embedded supplicants.
- MAC Authentication Bypass (MAB) is used to authenticate endpoints that do not have the ability to perform IEEE 802.1X. It requires maintaining a database of the MAC addresses of all trusted endpoints.
- Web Authentication is the third mechanism. It presents the users with a web-portal through which users can submit their credentials and authenticate to the network.

Web authentication is primarily used in the following cases:

- To authenticate temporary users

It is essential for organizations to provide network access to temporary users such as guests and contractors. Temporary users are most likely to use devices that are beyond the control of an organization's IT services. As a result, temporary users are not going to have endpoints configured for IEEE 802.1X. Web Authentication is a convenient mechanism to have such users authenticate and sign an acceptable user policy. Authenticating temporary access users also has the added benefit of making it possible to monitor their activities, allowing organizations to meet compliance requirements.

- As a fall back authentication mechanism for regular network users

Often, regular network users with devices configured for IEEE 802.1X devices are likely to fail authentication. This can happen for various reasons like expiration of passwords/ certificates and misconfigured supplicants. Web Authentication provides a means for such users to authenticate themselves and remediate issues that are preventing them from authenticating via IEEE 802.1X.

- Device registration

Users often have personal devices, like tablets and smartphones, that they use to access the Internet and other corporate applications. It is increasingly important for IT to be able to link every such device to a user to help ensure that it has appropriate access to network resources. Web Authentication can be used as a means to allow users to register their personal devices. Once registered, the device can be either given full or limited access to network resources based on the organization's security policy and the user's role in the organization.

Web Authentication Flow

The typical web authentication flow consists of the following events:

1. The user attempts to connect to the wired network. The user can either be a guest/contractor or an employee who fails IEEE 802.1X authentication. The reasons for IEEE 802.1X authentication failure can range from misconfigured supplicants to expired credentials.
2. Once IEEE 802.1X times out, the switch attempts MAB. MAB results in a failure, too.
3. At this point, Web Authentication is invoked. This can happen in one of two ways:
 - Local Web Authentication (LWA)

LWA is a process where the network access device, switch, or wireless LAN controller (WLC) handles the Web Authentication locally. It requires every network access device to be configured with the web-portal pages. Configuring and managing the web-portals on every network access device in a production network is a difficult task. LWA supports only access control list (ACL)-based enforcement and does not support RADIUS change of authorization (CoA). RADIUS CoA is required for posture assessment and enforcement based on profiling.

- Central Web Authentication (CWA)

CWA is a process where a policy server, like Cisco Identity Services Engine (ISE), is used to centrally authenticate users via Web Authentication. Having a central policy server for Web Authentication makes it easier to implement operationally. CWA supports both ACL and VLAN-based enforcement. Additionally, RADIUS CoA is also supported. This allows for posture assessment and enforcement based on profiling.

Note: CWA for wireless networks was introduced in Cisco Wireless LAN Controller Software Release 7.2

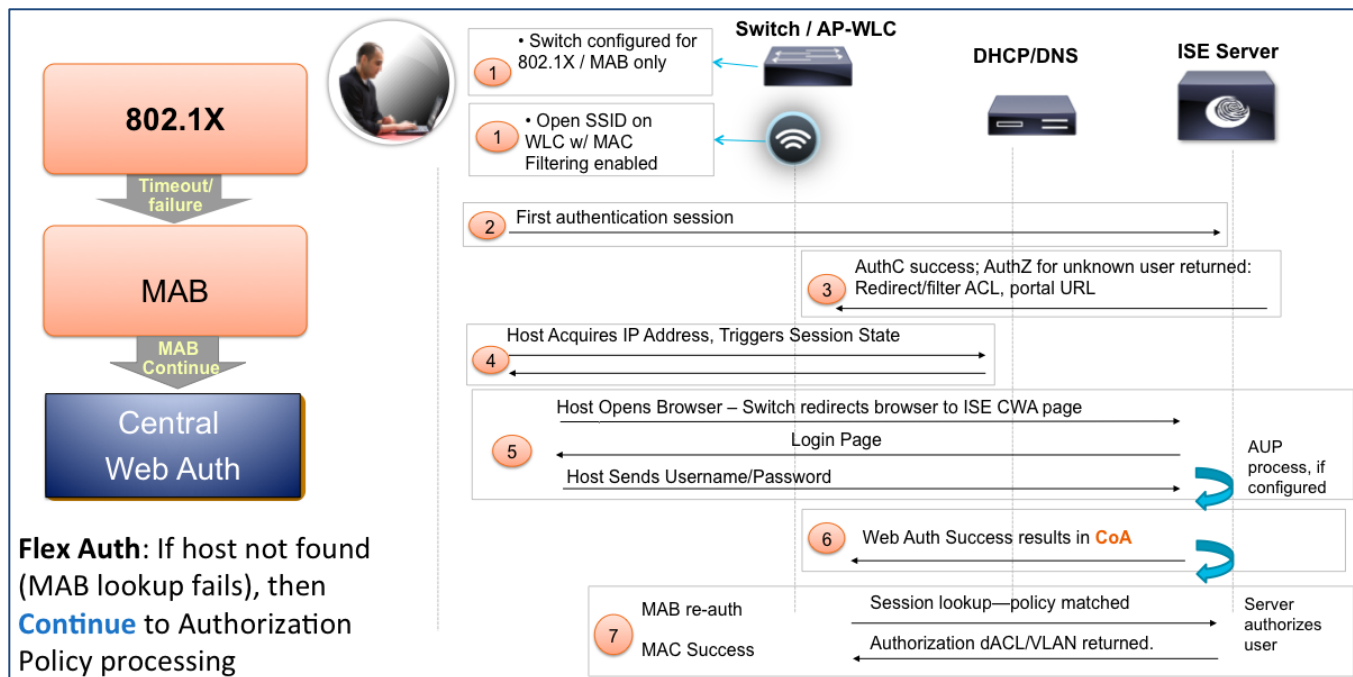
The Web Authentication flow is slightly different for a wireless user. Here the user connects to an open SSID, which is configured to accept only Web Authentication. So effectively, once the user associates to the open SSID, they are at step 3 of the web authentication process.

Cisco recommends using CWA because it is operationally more efficient and supports additional features like posture assessment and enforcement based on profiling. To limit the scope of this document, we will discuss only CWA. Please refer to the [TrustSec 2.0 Design and Implementation Guide](#) for information on Local Web Authentication.

Central Web Authentication

Figure 3 explains the CWA flow in detail.

Figure 3 Central Web Authentication Processing Flow



Step 1 The Cisco switch is configured for IEEE 802.1X and MAB. The Cisco WLC is configured with an open SSID with MAC filtering enabled.

Note: Refer to the following How-To guides for detailed steps on configuring the switch and Cisco WLC for CWA

[HowTo-10-Universal_Switch_Configuration](#)

[HowTo-11-Universal_WLC_Configuration](#)

Step 2 The user connects to the wired port or associates with the open wireless SSID. If the user connects to the wired port, first IEEE 802.1X either timeouts or fail. The Cisco switch then falls back to MAB. Cisco ISE does not find the endpoint in the Internal Endpoints identity store. At this point, instead of sending a RADIUS access-reject message to the switch, Cisco ISE sends a RADIUS access-accept.

Step 3 Along with the RADIUS access-accept, Cisco ISE also pushes down a filter ACL, **PERMIT_ALL_TRAFFIC**, a redirect ACL, **ACL-WEBAUTH-REDIRECT**, and the web-portal URL. The RADIUS access-accept instructs the switch to open up the port for regular network traffic, which is now restricted based on the port and redirect ACLs.

Step 4 The endpoint is now able to get an IP address and resolve DNS queries. It also triggers a new session on ISE. This session has a unique session ID.

Step 5 Once the user launches a web browser, the switch or Cisco WLC redirects the browser to the ISE CWA web-portal URL. At this point, the user enters their credentials and accepts any configured Acceptable Use Policies (AUPs).

Step 6 Cisco ISE sends a RADIUS CoA message to the network access device.

Step 7 The network access device re-authenticates the endpoint and places it in the same session created earlier. Cisco ISE now sends the appropriate access policy to the network access device.

CWA Configuration Explained

This section explains how the various redirect/ filter ACLs and redirect policies configured on Cisco ISE, Cisco switches, and Cisco Wireless LAN Controller operate to enable CWA.

Note: For detailed configuration steps refer to

Switch: Global Switch Configuration

WLC: Base configuration for the Wireless LAN Controller

Access Control Lists Defined on a Cisco Switch for CWA

Switchport ACL

This is either the **ACL-ALLOW** or **ACL-DEFAULT**, depending on whether your deployment is using Monitor Mode or Low-Impact Mode. This ACL controls what traffic is allowed through the port prior to redirection. This ACL is specific to Cisco IOS® Software devices only. Its primary use is to restrict traffic when the **Authentication Open** command is used.

Redirect ACL on Cisco Switches

The redirect ACL is the **ACL-WEBAUTH-REDIRECT**, defined on the switch as follows:

```
C3750X(config)#ip access-list ext ACL-WEBAUTH-REDIRECT
C3750X(config-ext-nacl)#remark explicitly deny DNS from being redirected to address a bug
C3750X(config-ext-nacl)#deny udp any any eq 53
C3750X(config-ext-nacl)#remark redirect all applicable traffic to the ISE Server
C3750X(config-ext-nacl)#permit tcp any any eq 80
C3750X(config-ext-nacl)#permit tcp any any eq 443
C3750X(config-ext-nacl)#remark all other traffic will be implicitly denied from the redirection
```

Cisco ISE instructs the switch to invoke this redirect ACL via a vendor specific attribute. The Vendor Specific Attribute (VSA) is defined as a part of the authorization profile in ISE. This ACL helps the switch identify traffic that should be redirected to ISE to allow Central Web Authentication (CWA).

For Web Authentication to work, you want the host machine to have access to basic network services like DHCP and DNS. Therefore, you do not want to redirect DHCP and DNS traffic. The **deny udp any any eq 53** statement in the ACL instructs the switch to deny redirection for User Datagram Protocol (UDP) traffic on port 53. As a result, the host machine will have access to DNS services.

Note: The Cisco switch redirects DNS traffic due to an existing bug. A workaround is to specifically instruct the switch not to redirect DNS traffic.

While we allow the host machine access to basic network services, we want to redirect all web traffic from the host. The **permit tcp any any eq 80** and **permit tcp any any eq 443** statements in the ACL instruct the switch to redirect HTTP and HTTPS traffic. The URL to which the traffic should be redirected is defined in another VSA and is discussed later.

Access control lists defined on a Cisco WLC for CWA

1. Redirect ACL on the Cisco WLC

The redirect ACL on the Cisco WLC is also named **ACL-WEBAUTH-REDIRECT** to maintain consistency with the switch configuration. This ACL is defined as shown below.

Figure 4 - ACL on Wireless LAN Controller for Web Authentication

Security

AAA

General

RADIUS

Authentication

Accounting

Fallback

TACACS+

LDAP

Local Net Users

MAC Filtering

Disabled Clients

User Login Policies

AP Policies

Password Policies

Local EAP

Priority Order

Certificate

Access Control Lists

Access Control Lists

Access Control Lists > Edit

General

Access List Name

ACL-WEBAUTH-REDIRECT

Deny Counters

879

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any	41
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	74
3	Permit	10.1.100.3 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0
4	Permit	0.0.0.0 / 0.0.0.0	10.1.100.3 / 255.255.255.255	Any	Any	Any	Any	Any	0

If you compare the switch redirect ACL and the WLC redirect ACL, you will see the differences. We use the statement **deny udp any any eq 53** to stop DNS traffic from being redirected on the switch and on the WLC we use a permit action for DNS traffic. This is because the redirect ACL on the WLC is just a regular wireless ACL. Hence, the ACL rules have permit statements for allowed traffic flows like DNS and traffic to ISE (10.1.100.3). Any other traffic is caught by the implicit deny statement and is re-directed to the redirect URL set in the ISE. This ACL is invoked when ISE sends the VSA through the authorization profile.

In summary,

- The redirect ACL, ACL-WEBAUTH-REDIRECT, has to be configured in advance on both the Cisco switch and the Cisco WLC
- The redirect ACL is invoked using the VSA defined in the ISE authorization profile.
- The URL to which traffic should get redirected is also specified in the ISE authorization profile as a VSA.
- While defining the redirect ACL on the switch, a deny statement exempts traffic from re-direction and a permit statement redirects the specified traffic.
- The redirect ACL on the WLC is just a regular wireless ACL. A permit statement exempts traffic from redirection and a deny statement redirects the specified traffic. The ACL has an implicit deny statement at the end.
- Additionally, the ISE authorization policy can also send a DACL to replace the existing pre-authentication switchport ACL.

Cisco ISE Authorization Profile for CWA

This section will explain how the various ACLs and redirect URLs are defined within the Cisco ISE authorization policy. Based on the configuration in the Low-Impact how to guide, your ISE authorization profile for WEBAUTH should look like the figure below.

Figure 5 - WebAuth Authorization Profile defined in ISE

Authorization Profiles > WebAuth

Authorization Profile

* Name:

Description:

* Access Type:

Common Tasks

☒ DACL Name:

☐ VLAN

☐ Voice Domain Permission

☒ Web Authentication: ACL: Redirect:

☐ Auto Smart Port

☐ Filter-ID

Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT
DACL = PERMIT_ALL_TRAFFIC
cisco-av-pair = url-redirect-acl=ACL-WEBAUTH-REDIRECT
cisco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cwa

The authorization profile has the following:

- RADIUS access_accept.

This instructs the switchport of a successful authentication. As a result the switch opens up the port and allows traffic through.

- PERMIT_ALL_TRAFFIC DACL

This is a downloadable switchport ACL. This ACL will replace the pre-authentication ACL you have configured on the switchport.

- Web Authentication parameters

There are three different parameters listed here. First we set the web authentication method to Centralized. We then mention what ACL needs to be applied. On the switch we would invoke the redirect ACL and on the WLC we would invoke the wireless ACL. The redirect field specifies the redirect URL. In this case, we are just going to use the default ISE guest portal.

This is the same set of parameters you would need to change to use web authentication for posture assessment, supplicant provisioning and device registration.

- Attribute details

This section is populated automatically. It shows you the various vendor specific attributes being used. Notice how the ACL-WEBAUTH-REDIRECT is listed as a url-redirect-acl. The url-redirect value specifies url to which traffic will be redirected.

Appendix A: References

TrustSec System:

- <http://www.cisco.com/go/trustsec>
- http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

Device Configuration Guides:

Cisco Identity Services Engine User Guides:

http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

For more information about Cisco IOS Software, Cisco IOS XE Software, and Cisco NX-OS Software releases, please refer to following URLs:

- For Cisco Catalyst 2900 series switches:
http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 3000 series switches:
http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 3000-X series switches:
http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 4500 series switches:
http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 6500 series switches:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html
- For Cisco ASR 1000 series routers:
http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html

For Cisco Wireless LAN Controllers: <http://www.cisco.com/en/US/docs/wireless/controller/7.2/configuration/guide/cg.html>