



Cisco TrustSec How-To Guide: Migrating from Monitor Mode

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 Cisco TrustSec System?.....	3
About the TrustSec How-To Guides.....	3
<i>What does it mean to be "TrustSec Certified"?</i>	4
Migrating from Monitor Mode	5
Moving from Monitor Mode to Low-Impact Mode.....	5
<i>Using a Phased Approach</i>	5
<i>Moving One Switch at a Time</i>	5
<i>Committing to Low-Impact Mode</i>	7
<i>Change the Default Port ACL</i>	8
<i>Wired Access-802.1X and MAB Authentication</i>	8
<i>Examining Additional User Information</i>	9
<i>Configuration for Role-Specific Access</i>	10
<i>Closed Mode (Formerly High-Security Mode)</i>	14
Appendix A: References.....	15
TrustSec System:	15
Device Configuration Guides:	15

Introduction

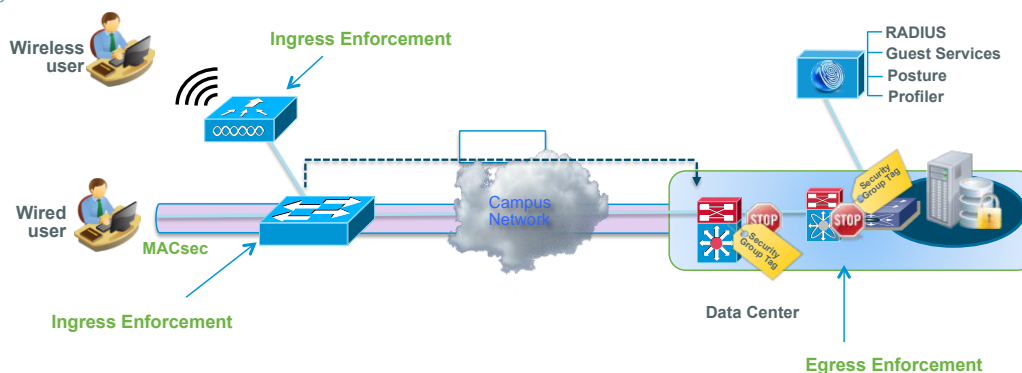
What Is the Cisco TrustSec System?

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

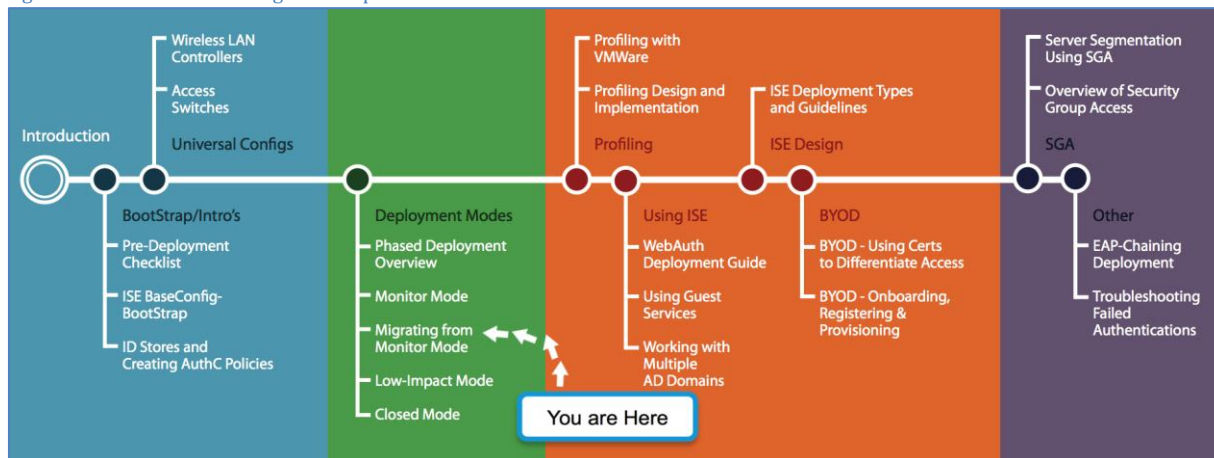


About the TrustSec How-To Guides

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.

Migrating from Monitor Mode

The TrustSec How-To Guide on universal switch configuration explained a universally applicable method of configuring a switch for a TrustSec Version 2.1 deployment. It ended with the switch in Monitor Mode to start the first phase of a TrustSec deployment.

In Monitor Mode, authentication occurs but network access is not restricted based on the authentication result. A combination of Cisco Identity Services Engine (ISE) policies and switchport commands is used to give all devices full access to the network. In Monitor Mode, network administrators can determine which users or devices would have failed authentication and why.

This guide explains how to successfully transition from Monitor Mode to an enforcement phase of deployment (Low-Impact Mode or Closed Mode), where access to the network is restricted to only those devices or users that are properly authenticated.

Moving from Monitor Mode to Low-Impact Mode

The deployment modes beyond Monitor Mode gradually build access controls into the design through port-based ACLs, dACLs, and/or VLANs. Port-based ACLs are locally defined on the switchport and are used for filtering traffic before it is successfully authenticated. dACLs and VLAN assignments are centrally defined on Cisco ISE within authorization profiles and are downloaded to the switches after successful authentication.

Using a Phased Approach

It is important to note that authorization policies are applied to *each* authenticated session. In other words, all switches move from Monitor Mode to Low-Impact Mode at the same time, and, for all authenticated users, the access controls are provided by the authorization filtering their network access.

During your deployment rollout, you may not wish to have everyone migrate at the same time. This section explains two methods of phasing the migration: moving one switch at a time, and committing to Low-Impact Mode.

Moving One Switch at a Time

One way to phase the migration is to designate switches that are in Low-Impact Mode instead of Monitor Mode. This is done by creating a network device group called “Stage” and, within the Stage group, creating groups called “Low Impact” or “Closed.”

Procedure 1 Create a Network Device Group to Indicate Which Switches Are in Low-Impact Mode

Step 1 Navigate to Administration → Network Resources → Network Device Groups → Groups.

Step 2 Click Add to add a group. Set the name and device type to **Stage**.

Figure 3: Stage NDG

CISCO Identity Services Engine

Home Operations Policy Administration

System Identity Management Network Resources Web Portal Management

Network Devices Network Device Groups External RADIUS Servers RADIUS Server Sequences SGA AAA Servers NAC Managers

Network Device Groups

Network Device Groups List > New Network Device Type

Network Device Groups

* Name Stage

Description

* Type Stage

Submit Cancel

Step 3 Click Submit.

Step 4 Navigate to the newly created Stage group.

Step 5 Add a group. Set the name to **LowImpact**.

Figure 4: Low-Impact NDG

CISCO Identity Services Engine

Home Operations Policy Administration

System Identity Management Network Resources Web Portal Management

Network Devices Network Device Groups External RADIUS Servers RADIUS Server Sequences SGA AAA Servers NAC Managers

Network Device Groups

Network Device Groups > Stage List > New Network Device Group

Network Device Groups

* Name LowImpact

Description

* Type Stage

Submit Cancel

Step 6 Click Submit.

Step 7 Navigate to Administration → Network Resources → Network Devices.

Step 8 Edit the access layer switch that you wish to move to Low-Impact Mode.

Step 9 Set Stage to LowImpact.

Figure 5: Adding Network Device to NDG

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes Home, Operations, Policy, and Administration. The left sidebar shows the Network Devices list. The main form is titled 'Network Devices' and contains the following fields:

- * Name: 3K-X
- Description: (empty)
- * IP Address: 10.1.48.2 / 32
- Model Name: (empty)
- Software Version: (empty)
- * Network Device Group
 - Location: All Locations
 - Device Type: Access_Layer
 - Stage: LowImpact

A red arrow points to the 'Set To Default' button next to the Stage field.

Step 10 Click Save.

Committing to Low-Impact Mode

Low-Impact Mode has two stages. Stage 1 provides filtered access prior to authentication and provides full network access after successful user or device authentication. Stage 2 provides role-specific access control, rather than fully open network access. For more on the different deployment modes, please reference the TrustSec How-To Guide that discusses deployment options.

Stage 1

Here, our goal is to change the default port ACL to one that restricts access. The level of restriction is entirely up to the deployment plan. We will examine a few default port ACLs that have been used in the field, then discuss what complications may exist in your deployment, and how to adjust the default port ACL appropriately.

Following are two suggested default port ACLs.

ACL-DEFAULT (the recommended, secure default port ACL):

```
ip access-list extended ACL-DEFAULT
remark DHCP
permit udp any eq bootpc any eq bootps
remark DNS
permit udp any any eq domain
remark Ping
permit icmp any any
remark PXE / TFTP
permit udp any any eq tftp
remark Drop all the rest
deny ip any any log
```

The second suggested default port ACL opens several Microsoft ports to allow devices to communicate with Active Directory before login in order to improve login times. Opening Microsoft-specific ports may also be accomplished with the machine authentication.

ACL-DFLT-LESS-RESTRICT:

```
ip access-list extended ACL-DFLT-LESS-RESTRICT
 remark DHCP, DNS, ICMP
 permit udp any eq bootpc any eq bootps !DHCP
 permit udp any any eq domain !DNS
 permit icmp any any !ICMP Ping
 remark Allow Microsoft Ports (used for better login performance)
 permit tcp any host 10.1.100.10 eq 88 !Kerberos
 permit udp any host 10.1.100.10 eq 88 !Kerberos
 permit udp any host 10.1.100.10 eq 123 !NTP
 permit tcp any host 10.1.100.10 eq 135 !RPC
 permit udp any host 10.1.100.10 eq 137 !NetBIOS-Nameservice
 permit tcp any host 10.1.100.10 eq 139 !NetBIOS-SSN
 permit tcp any host 10.1.100.10 eq 389 !LDAP
 permit udp any host 10.1.100.10 eq 389 !LDAP
 permit tcp any host 10.1.100.10 eq 445 !MS-DC/SMB
 permit tcp any host 10.1.100.10 eq 636 !LDAP w/ SSL
 permit udp any host 10.1.100.10 eq 636 !LDAP w/ SSL
 permit tcp any host 10.1.100.10 eq 1025 !non-standard RPC
 permit tcp any host 10.1.100.10 eq 1026 !non-standard RPC
 remark PXE / TFTP
 permit udp any any eq tftp
 remark Drop all the rest
 deny ip any any log
```

Slow Logins

If a login remains slow, it is possible that another application is the cause. Today's enterprise environments tend to have numerous corporate applications installed on them. Some are very "chatty" and will continuously try to communicate with their management servers. Following are some suggested methods to identify the application that is causing the slow login:

- Option 1: Use a network packet sniffer application to identify all traffic attempts prior to login.
- Option 2: Implement a similar access list on a Cisco ASA Adaptive Security Appliance to log all attempts and all drops. Leave the default port ACL as ACL-ALLOW (permit ip any any).

Change the Default Port ACL

Procedure 1 Replace ACL-ALLOW with ACL-DEFAULT on the Switch

Step 1 Apply the initial ACL (ACL-ALLOW).

```
C3750X(config-if-range)#ip access-group ACL-DEFAULT in
```

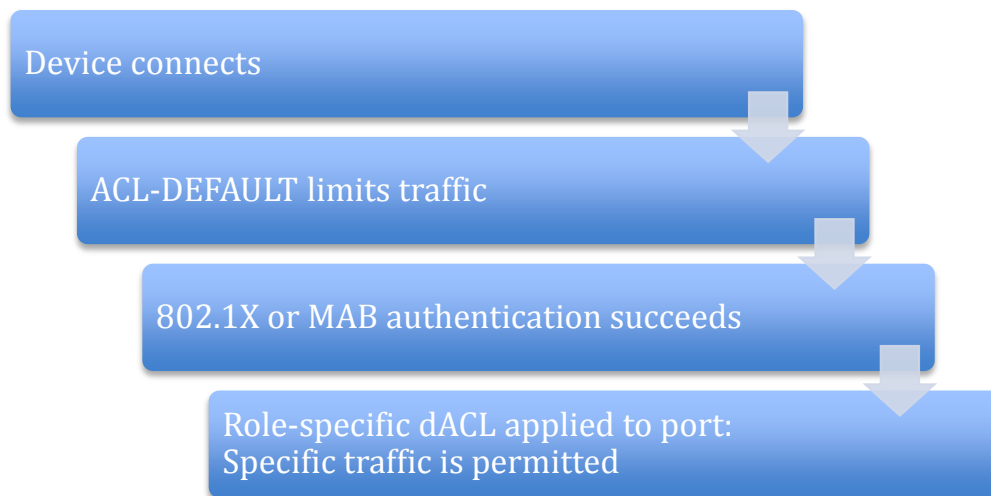
Stage 2

Wired Access-802.1X and MAB Authentication

At this stage, all wired devices should be authenticating either by 802.1X or MAB, and thereby given full access to the network. It is now time to secure the network even more by differentiating the access that is granted per user. Full access after an authentication may be enough security for some deployments, but is not secure enough for most companies.

This differentiation of access is done by applying a specific dACL to each user or device session. This is a critical component of this phase of a TrustSec deployment. The dACL overrides the default port ACL for the specific device that authenticated (handled per session). Without the dACL, a device would still be subjected to the default port ACL. The big difference between this phase and the previous one is the specific authorization result that will be issued per user or device based on the role of that user (Figure 22).

Figure 6: Low-Impact Mode Process at End-State



Examining Additional User Information

Until this point, if a user was a member of the Domain Users group, that user received full network access. To improve security, we will look at additional groups and provide differentiated access to each group. Please reference the table of Active Directory users and group membership.

Procedure 1 Add Additional Groups to the Active Directory Connector

Step 1 Navigate to Administration → External Identity Sources → Active Directory.

Step 2 Click the Groups tab.

Step 3 Click Add → Select Groups from Active Directory.

Step 4 Click Retrieve Groups.

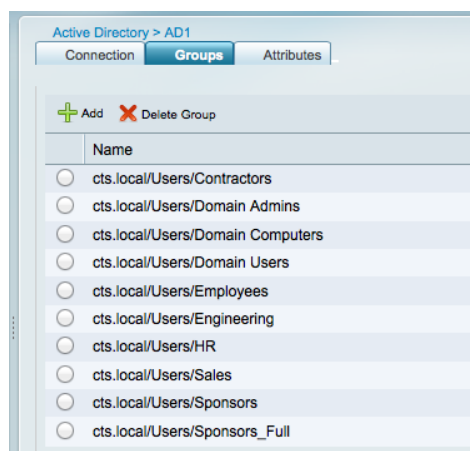
Note: When AD has more than 100 groups, use the filter options to find the specific group you are looking for.

Step 5 Select the additional groups.

In our example, we will be selecting the Engineering, Sales, and HR groups.

Step 6 Click OK. A screenshot of our final group selection follows:

Figure 7: Selecting Groups from AD



Step 7 Scroll to the bottom and click Save Configuration.

Note: If you don't save the configuration, the additional groups will not be retrieved from Active Directory during authorization.

Procedure 1 Create Additional Downloadable ACLs for Each Main Role

Repeat this procedure for each role that requires a different authorization. For the purposes of documentation, we will explain the creation of the HR dACL and then show the final screen with all the dACLs defined.

Cisco Best Practice: Keep all dACLs small. dACL support on a switch is related to the amount of available Ternary Content Addressable Memory (TCAM) space. Each ASIC in a switch has its own TCAM, and the number of ASICs per port will vary between switch models. The amount of TCAM assigned to each ASIC also varies between switch models (i.e., there is more TCAM on a Cisco Catalyst 3750 Switch than on a Cisco Catalyst 2960 Switch). The limit of dACL support for Cisco switches is 64 ACEs (64 lines).

Step 1 Navigate to Policy → Policy Elements → Results → Authorization → Downloadable ACLs.

Step 2 Click Add.

```
Name = HR-ACL
Description = dACL for HR users (Enforcement Mode)
DACL Content =
    Deny ip any <ip_address_range_of_engineering_servers>
    permit ip any any
```

Warning: There is no syntax checking in Cisco ISE. If the dACL syntax is incorrect, it will not apply to the session.

Step 3 Click Submit.

Step 4 Repeat the entire procedure for each distinct role type.

Following is a screen shot of the final dACL list used in our example:

Figure 8: List of dACLs



Name	Description
AD-Machine-ACL	dACL used to permit Windows to communicate to AD for Mac...
Contractor-ACL	dACL for use with Contractor Role (Enforcement Mode)
DENY_ALL_TRAFFIC	Deny all traffic
Employee-ACL	dACL for employees who have not already been Authorized (...)
Engineering-ACL	dACL for Engineering Role (Enforcement Mode)
GUEST	dACL for GUEST users (Authentication Mode)
HR-ACL	dACL for HR users (Enforcement Mode)
PERMIT_ALL_TRAFFIC	Allow all Traffic
Sales-ACL	dACL for Sales Role (Enforcement Mode)

Procedure 2 Create Additional Authorization Profiles for Each Main Role

Repeat this procedure for each role that requires a different authorization. As we did with Procedure 1, for the purposes of documentation, we will explain the creation of the HR Authorization Profile and then show the final screen with all the authorization profiles defined.

Step 1 Navigate to Policy → Policy Elements → Results → Authorization → Authorization Profiles.

Step 2 Click Add.

Step 3 Complete the authorization profile with the following information:

```
Name = HR-Profile
Description = Authorization Profile for HR role (Enforcement Mode)
Access-Type = ACCESS_ACCEPT
-- Common Tasks
☒ DACL Name = HR-ACL
☒ Wireless LAN Controller (WLC) = HR-ACL
```

Note: The Wireless LAN Controller (WLC) field is used to apply a wireless ACL (wACL) that is locally defined on the WLC. WLCs do not currently support dACLs.

Step 4 Click Submit.

Step 5 Repeat the entire procedure for each distinct role type.

Procedure 3 Create Another Authorization Profile for Employees.

We have singled out this specific authorization profile to replace the current “Domain Users” authorization rule. This authorization profile and its associated rule will be used as a catch-all for employees who may not have been authorized by a more specific role.

Step 1 Navigate to Policy → Policy Elements → Results → Authorization → Authorization Profiles.

Step 2 Click Add.

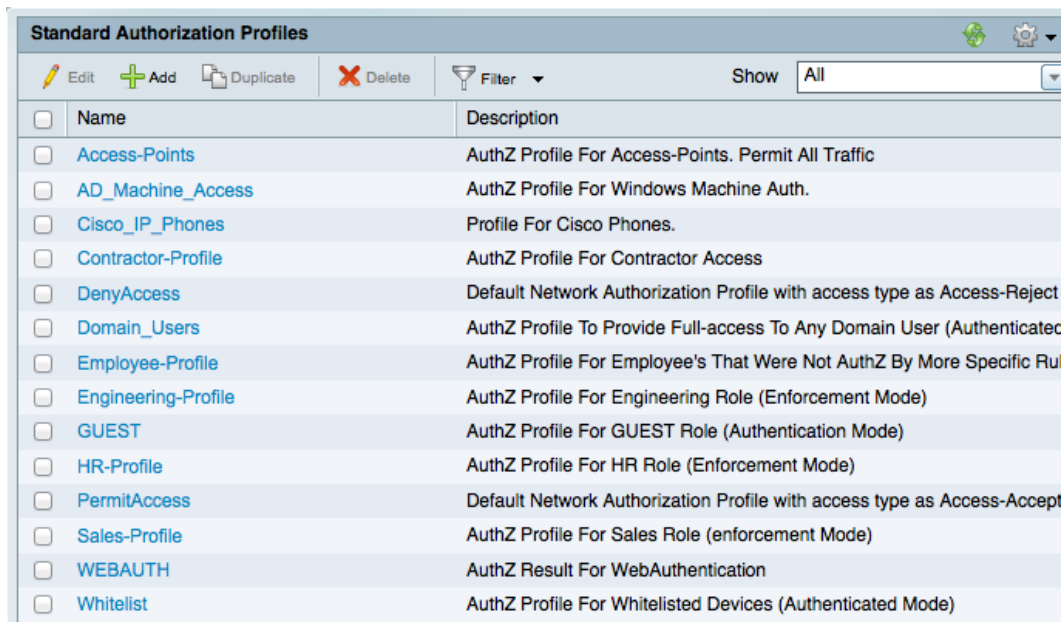
Step 3 Complete the authorization profile with the following information:

Name = **Employee-Profile**
Description = **Authorization Profile for Employees (Enforcement Mode)**
Access-Type = **ACCESS_ACCEPT**
-- Common Tasks
☒ DACL Name = **Employee-ACL**
☒ Wireless LAN Controller (WLC) = **Employee-ACL**

Step 4 Click Submit.

Following is a screenshot of the final authorization profile list used in our example:

Figure 9: Standard Authorization Profiles



Standard Authorization Profiles	
<input type="checkbox"/> Name	Description
<input type="checkbox"/> Access-Points	AuthZ Profile For Access-Points. Permit All Traffic
<input type="checkbox"/> AD_Machine_Access	AuthZ Profile For Windows Machine Auth.
<input type="checkbox"/> Cisco_IP_Phones	Profile For Cisco Phones.
<input type="checkbox"/> Contractor-Profile	AuthZ Profile For Contractor Access
<input type="checkbox"/> DenyAccess	Default Network Authorization Profile with access type as Access-Reject
<input type="checkbox"/> Domain_Users	AuthZ Profile To Provide Full-access To Any Domain User (Authenticated
<input type="checkbox"/> Employee-Profile	AuthZ Profile For Employee's That Were Not AuthZ By More Specific Ru
<input type="checkbox"/> Engineering-Profile	AuthZ Profile For Engineering Role (Enforcement Mode)
<input type="checkbox"/> GUEST	AuthZ Profile For GUEST Role (Authentication Mode)
<input type="checkbox"/> HR-Profile	AuthZ Profile For HR Role (Enforcement Mode)
<input type="checkbox"/> PermitAccess	Default Network Authorization Profile with access type as Access-Accept
<input type="checkbox"/> Sales-Profile	AuthZ Profile For Sales Role (enforcement Mode)
<input type="checkbox"/> WEBAUTH	AuthZ Result For WebAuthentication
<input type="checkbox"/> Whitelist	AuthZ Profile For Whitelisted Devices (Authenticated Mode)

Procedure 4 Adjust the Domain Computer Authorization

In Low-Impact Mode, we created a Domain Computers authorization profile and permitted all traffic by using the PERMIT_ALL_TRAFFIC dACL. In Enforcement Mode, traffic should be locked down so that only the required ports for those Windows Domain members can communicate with Active Directory.

Step 1 Navigate to Policy → Policy Elements → Results → Authorization → Downloadable ACLs.

Step 2 Click Add.

Step 3 Complete the new dACL as follows:

Name = **AD-Machine-ACL**

Description = **dACL used to permit Windows to communicate to AD for Machine Auth (Enforcement Mode)**

DACL Content =

```
permit udp any eq bootpc any eq bootps !DHCP
permit udp any any eq domain !DNS
permit icmp any any !ICMP Ping
permit tcp any host 10.1.100.10 eq 88 !Kerberos
permit udp any host 10.1.100.10 eq 88 !Kerberos
permit udp any host 10.1.100.10 eq 123 !NTP
permit tcp any host 10.1.100.10 eq 135 !RPC
permit udp any host 10.1.100.10 eq 137 !NetBIOS-Nameservice
permit tcp any host 10.1.100.10 eq 139 !NetBIOS-SSN
permit tcp any host 10.1.100.10 eq 389 !LDAP
permit udp any host 10.1.100.10 eq 389 !LDAP
permit tcp any host 10.1.100.10 eq 445 !MS-DC/SMB
permit tcp any host 10.1.100.10 eq 636 !LDAP w/ SSL
permit udp any host 10.1.100.10 eq 636 !LDAP w/ SSL
permit tcp any host 10.1.100.10 eq 1025 !non-standard RPC
permit tcp any host 10.1.100.10 eq 1026 !non-standard RPC
```

Step 4 Create this same ACL on the Wireless LAN Controller.

Step 5 Navigate to Policy → Policy Elements → Results → Authorization → Authorization Profiles.

Step 6 Click AD_Machine_Access.

Step 7 Modify the Authorization Profile as follows:

```
Name = AD_Machine_Access
Description = Authorization Profile for Windows Machine Auth.
Access-Type = ACCESS_ACCEPT
-- Common Tasks
☒ DACL Name = AD-Machine-ACL
☒ Wireless LAN Controller (WLC) = AD-Machine-ACL
```

Procedure 5 Create Additional Authorization Policy Rules for Each Main Role

Repeat this procedure for each role that requires a different authorization. For the purposes of documentation, we will explain the creation of the HR authorization policy rule, and then show the final screen with all the authorization policy rules defined.


Step 1 Navigate to Policy → Authorization.

Step 2 Insert a new Policy rule below the Whitelist rule.

Step 3 Name the rule **HR-Rule**.

Step 4 Leave Identity Group as Any.

Step 5 In Other Conditions, choose AD1:External Groups → Equals → HR.

Step 6 Click the gear icon. 

Step 7 Add an attribute.

Step 8 Set the expression to Device:Stage → Equals → LowImpact.

Step 9 For the permissions, choose Standard → HR-Profile.


Step 10 Click Save.

Step 11 Repeat the entire procedure for each distinct role type.

Procedure 6 Disable the Domain Users Rule

Step 1 Navigate to Policy → Authorization.

Step 2 Click the green arrow under Status, for the Domain Users Rule.

Step 3 Change to  Disabled.

Step 4 Click Save.

Step 5 The Final Rule table should be similar to the table below:

Table 1: Final Rule Table

Status	Rule Name		Identity Groups		Other Conditions		Permissions
<input checked="" type="checkbox"/>	Blacklisted	if	Blacklisted	and	Condition(s)	then	DenyAccess
<input checked="" type="checkbox"/>	Profiled Cisco IP Phones	if	Cisco-IP-Phone	and	Condition(s)	then	Cisco_IP_Phones
<input checked="" type="checkbox"/>	Profiled Cisco APs	if	Cisco-Access-Point	and	Condition(s)	then	Access-Points
<input checked="" type="checkbox"/>	Whitelist	if	Whitelist	and	Condition(s)	then	Whitelist
<input checked="" type="checkbox"/>	HR Rule	if	Any	and	AD1:ExternalGroups EQUALS HR AND Device:Stage Equals Stage#LowImpact	then	HR-Profile
<input checked="" type="checkbox"/>	Engineering Rule	if	Any	and	AD1:ExternalGroups EQUALS Engineering AND Device:Stage Equals Stage#LowImpact	then	Engineering-Profile
<input checked="" type="checkbox"/>	Sales Rule	if	Any	and	AD1:ExternalGroups EQUALS Sales AND Device:Stage Equals Stage#LowImpact	then	Sales-Profile
<input checked="" type="checkbox"/>	Employee Rule	if	Any	and	AD1:ExternalGroups EQUALS Employees AND Device:Stage Equals Stage#LowImpact	then	Employee-Profile
<input checked="" type="checkbox"/>	Contractor Rule	if	Any	and	AD1:ExternalGroups EQUALS Contractors AND Device:Stage Equals Stage#LowImpact	then	Contractor-Profile
<input checked="" type="checkbox"/>	Machine Auth	if	Any	and	AD1:ExternalGroups EQUALS Domain Computers AND Device:Stage Equals Stage#LowImpact	then	AD_Machine_Access
<input type="checkbox"/>	Domain User	if	Any	and	AD1:ExternalGroups EQUALS Domain Users AND Device:Stage Equals Stage#LowImpact	then	Domain_Users
<input checked="" type="checkbox"/>	GUEST	if	GUEST	and	Condition(s)	then	GUEST
<input checked="" type="checkbox"/>	Default	if no matches, then			WEBAUTH		

Procedure 7 Consider Moving to Multi-Domain Authentication (MDA) Mode

As discussed in the initial `HowTo-10-Universal_Switch_Config` guide, we configured the use of Multiple Authentication (Multi-Auth). Multi-Auth Mode allows a virtually unlimited number of MAC addresses per switchport, and requires an authenticated session for every MAC address. Multi-Auth Mode is used to help prevent an accidental denial of service to users with unauthorized hubs in their cubical or with other situational anomalies.

Multi-Domain Authentication Mode is recommended because it is the most secure and provides the most value from a security perspective. MDA Mode will allow a single MAC address in the data domain and a single MAC address in the voice domain per port.

Note: Future functions, such as MACsec (Layer 2 encryption between the endpoint and the switchport) require MDA or Single-Auth Mode, and will not function in Multi-Auth Mode.

Closed Mode (Formerly High-Security Mode)

Closed Mode represents the default 802.1X behavior. In Closed Mode, a switchport will not permit any traffic other than Extensible Authentication Protocol over LAN (EAPoL) prior to an authorization result from the AAA server. This is often the desired end-state for a deployment because it provides strong security. Like Low-Impact Mode, Closed Mode is capable of using all the enforcement mechanisms available in a TrustSec deployment (dVLAN, dACL, SGA, etc.), but could possibly have some impact on the operational models of an IT deployment.

Procedure 1 Remove Open Authentication

Step 1 Remove open authentication.

```
C3750X(config-if-range)# no authentication open
```

Step 2 Remove the port ACL.

```
C3750X(config-if-range)# no ip access-group ACL-DEFAULT in
```

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>