
# Cisco TrustSec How-To Guide: Low-Impact Mode

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

Current Document Version: 3.0

August 27, 2012

# Table of Contents

# Introduction

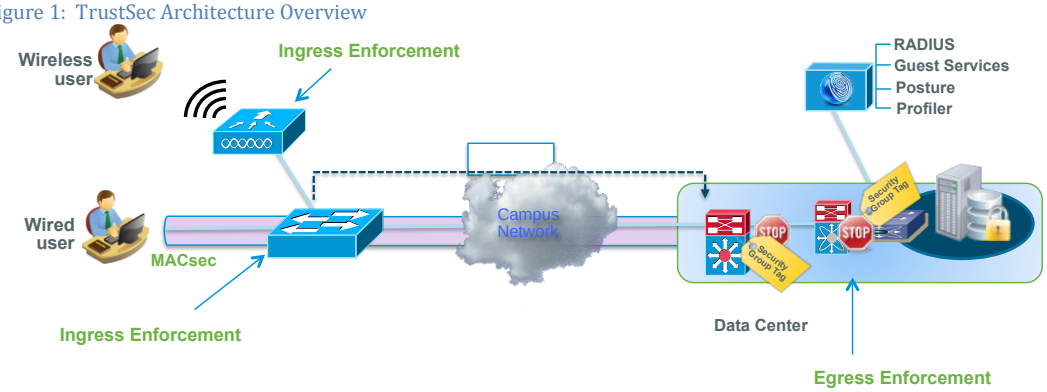
## What Is the Cisco TrustSec System?

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

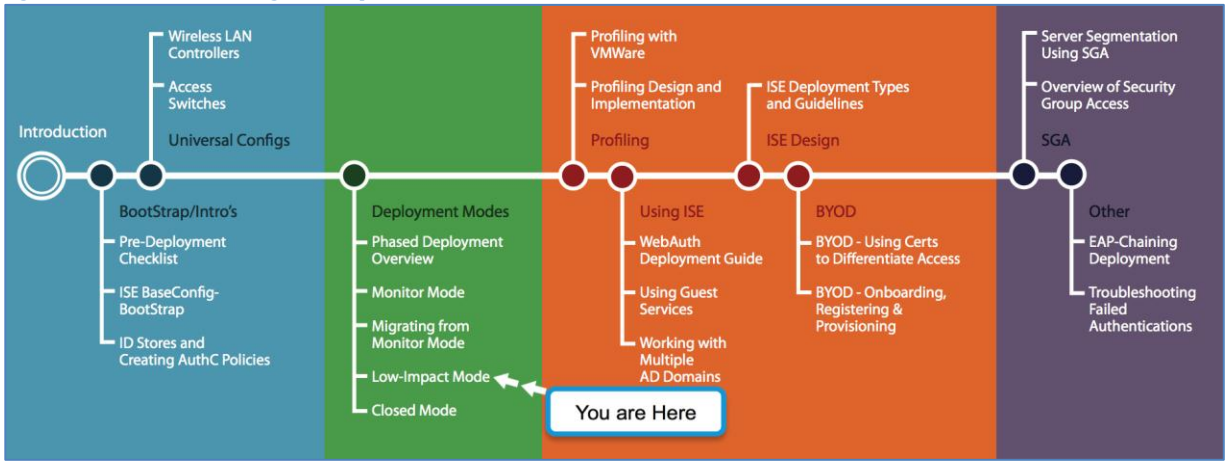



## About the TrustSec How-To Guides

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 is 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.

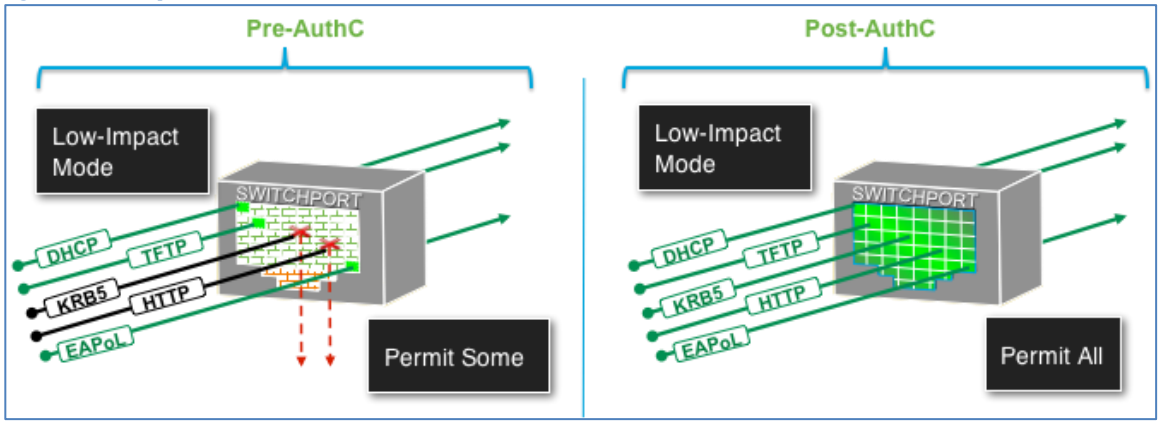
# Low-Impact Mode

## Overview of Low-Impact Mode

Compared to Monitor Mode, Low-Impact Mode incrementally increases the security level of the network by configuring an ingress port ACL on the open access TrustSec-enabled port. This provides basic connectivity for guests, contractors, and unauthenticated hosts while selectively limiting access, introducing a higher level of security. Access can be differentiated based on successful authentication and authorization by combining downloadable access control lists (dACLs) with the TrustSec-enabled port, which uses 802.1X, MAC Authentication Bypass (MAB), and/or web authentication.

In Low-Impact Mode, we add security to the framework that we built in Monitor Mode by applying an ACL to the switchport, allowing very limited network access prior to authentication. After users or devices have successfully authenticated, they are granted full network access (Figure 3).

Figure 3 Low-Impact Mode Port Behavior

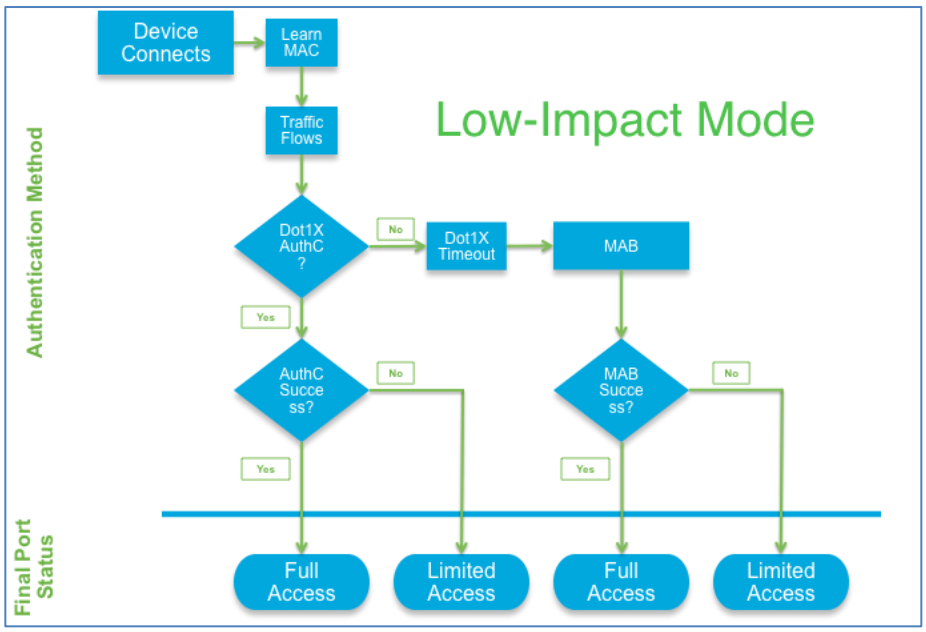



An example of how this feature may be used is giving any device attaching to the network the ability to use DHCP and DNS and perhaps get to the Internet while blocking its access to internal resources. When a device connected to that same switchport passes authentication, a dACL is applied that will permit all traffic.

This mode continues to use open authentication on the switchports while providing strong levels of security for non-authenticated devices. However, because a limited set of traffic will always flow regardless of the authentication state of a device, this mode becomes ideal and pragmatic for today's enterprises by allowing "regular" IT operational activities to occur, such as re-imaging workstations with Pre Execution Environment (PXE) solutions.

We will follow a similar flow for wireless access. A user or device authenticating to a wireless network with valid credentials will be authorized for full network access. Access should be tightened with additional security and specific access based on the role of the user or device.

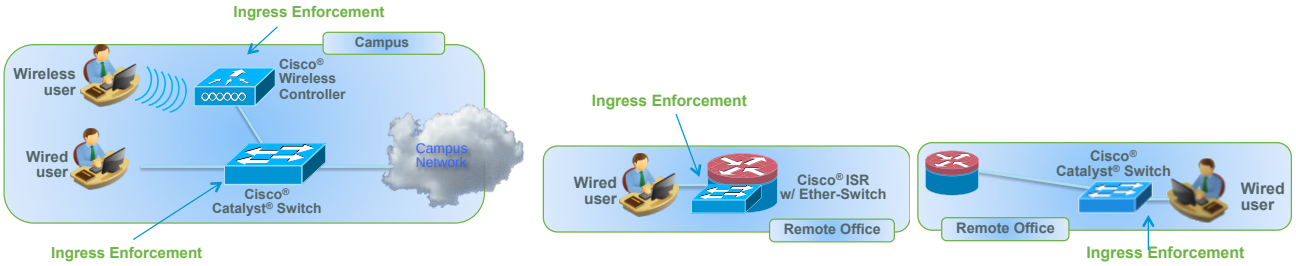
Figure 4 Low-Impact Mode Flowchart




## Understand the Flow Before Deployment

Like the TrustSec How-To Guide for Monitor Mode, this guide covers wired access in campus and remote offices. The solution test includes the use of the Cisco EtherSwitch® Services Module in the Integrated Services Router (ISR) for remote-office locations. With authentication added, we can also introduce wireless access to the network; this guide also provides step-by-step instructions on wireless deployment.

Figure 5 Typical Authenticated Access Scenarios




### Wired Access

At this stage, all wired devices should be authenticating by either 802.1X or MAB. It is now time to add security to limit traffic from devices that have not been authenticated and introduce the topics of web authentication and guest access.

Low-Impact Mode is a deployment strategy that adds security to the framework built Monitor Mode. It does so by applying an ACL to the switchport that allows very limited network access prior to authentication. We will refer to that ACL as the "default ACL" or "port ACL." We configured this in the HowTo-10-Universal_Switch_Configuration guide and it was named ACL-DEFAULT. The purpose of this ACL is to allow critical traffic to flow prior to an authentication. It may be necessary to open additional traffic depending on your environment.

After users or devices successfully authenticate, they are granted full network access with a downloadable ACL (dACL) that permits all traffic. This is a critical component of this phase of 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 subject to the ACL-DEFAULT that is assigned to the port (Figure 6).

Figure 6 Process for Authentication Mode


# Deployment of Low-Impact Mode

## Create an Authorization Rule for Other Network Devices – Cisco Wireless Access Points

Cisco IP phones and wireless access points are two of the more common endpoints that may need access to the network. Both have configurable supplicants and may require special access. IP phones will require access to the voice domain. Wireless access points will typically need specific types of network access; at a minimum, they require Domain Name System (DNS), Trivial File Transfer Protocol (TFTP), Dynamic Host Control Protocol (DHCP), Lightweight Access Point Protocol (LWAP), and Control and Provisioning of Wireless Access Points (CAPWAP) protocols. For this reason, we will create a separate authorization rule for access points that permits all traffic.

### Procedure 1 Create an Identity Group Based on Profiling Policies

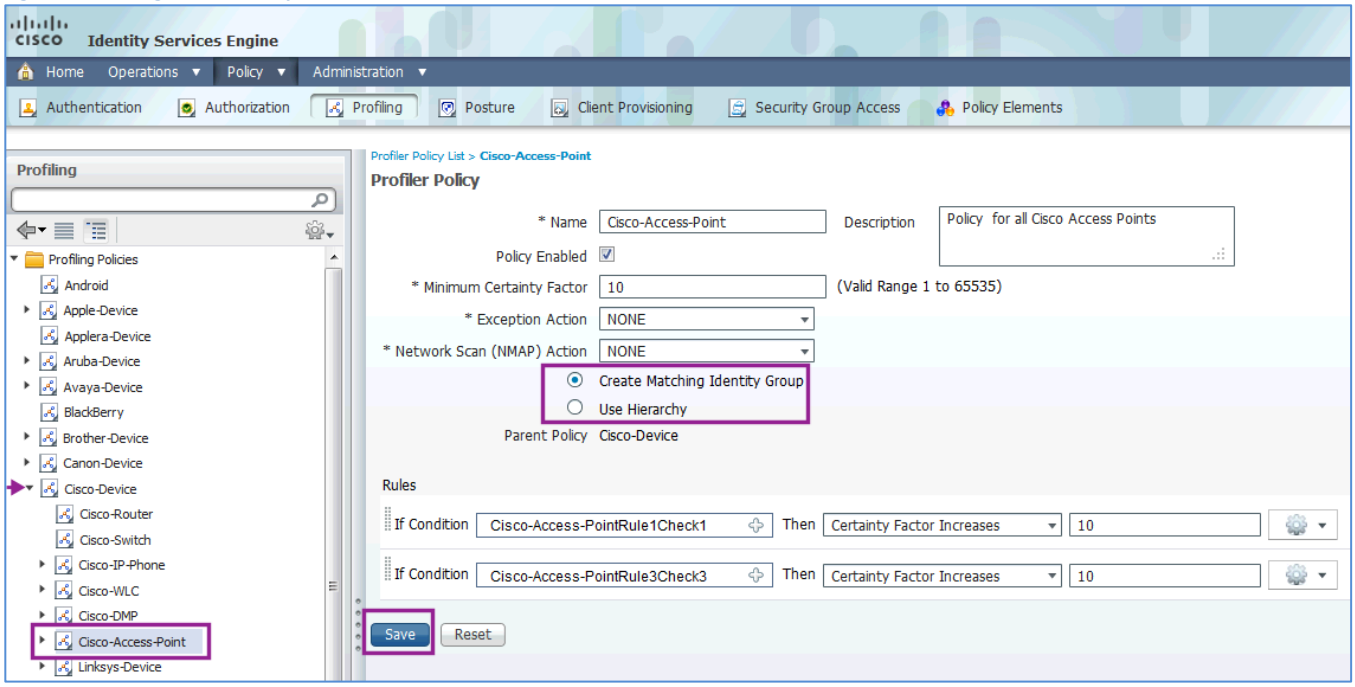
**Step 1** Navigate to Policy → Profiling.

**Step 2** Expand the Profiling Policies container. Expand Cisco-Device.

**Step 3** Highlight Cisco-Access-Point.

**Step 4** Select Create Matching Identity Group.

Figure 7 Creating Profiler Policy



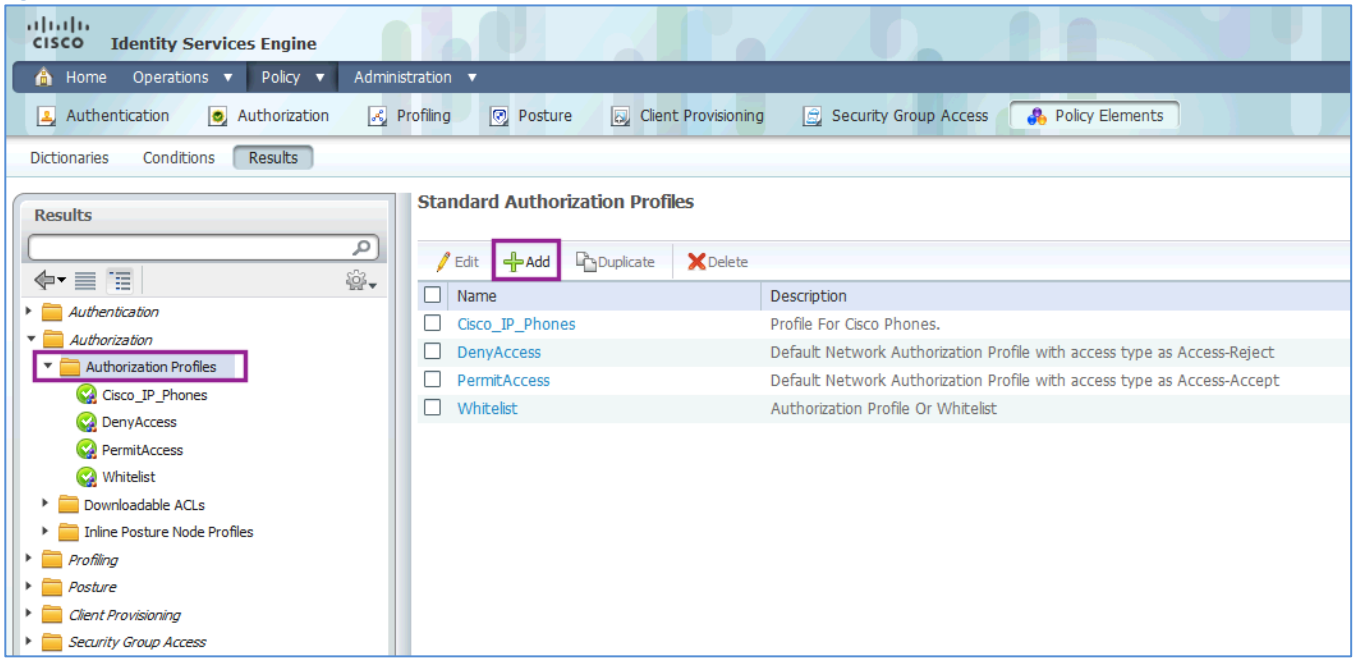

**Step 5** Click Save.

## Procedure 2 Create a New Authorization Profile

**Note:** The authorization profile will be exactly the same as the prebuilt Permit-Access profile. The purpose of creating a new authorization profile is to have a unique authorization profile that can be changed during the deployment of Low-Impact Mode.

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

Figure 8 Add an Authorization Profile




**Step 1** Click Add.

**Step 2** Configure the new authorization profile.

Name = **Access-Points**

Description = **Authorization Profile for Access-Points**

```
Access-Type = ACCESS_ACCEPT
-- Common Tasks
☑  DACL Name = PERMIT_ALL_TRAFFIC
```

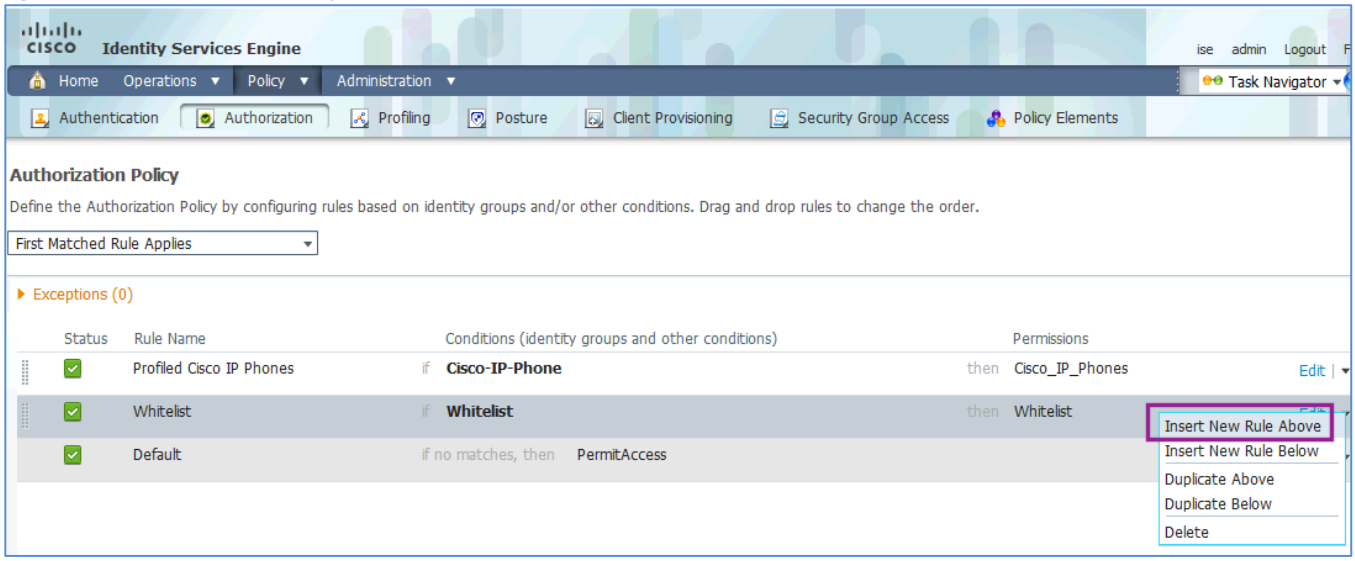
**Step 3** Click Submit.

## Procedure 3 Add a Rule to the Authorization Policy for Access Points

**Step 1** Navigate to Policy → Authorization.

**Step 2** Click the Actions pull-down menu at the end of the Whitelist authorization policy. Select Insert New Rule Above.

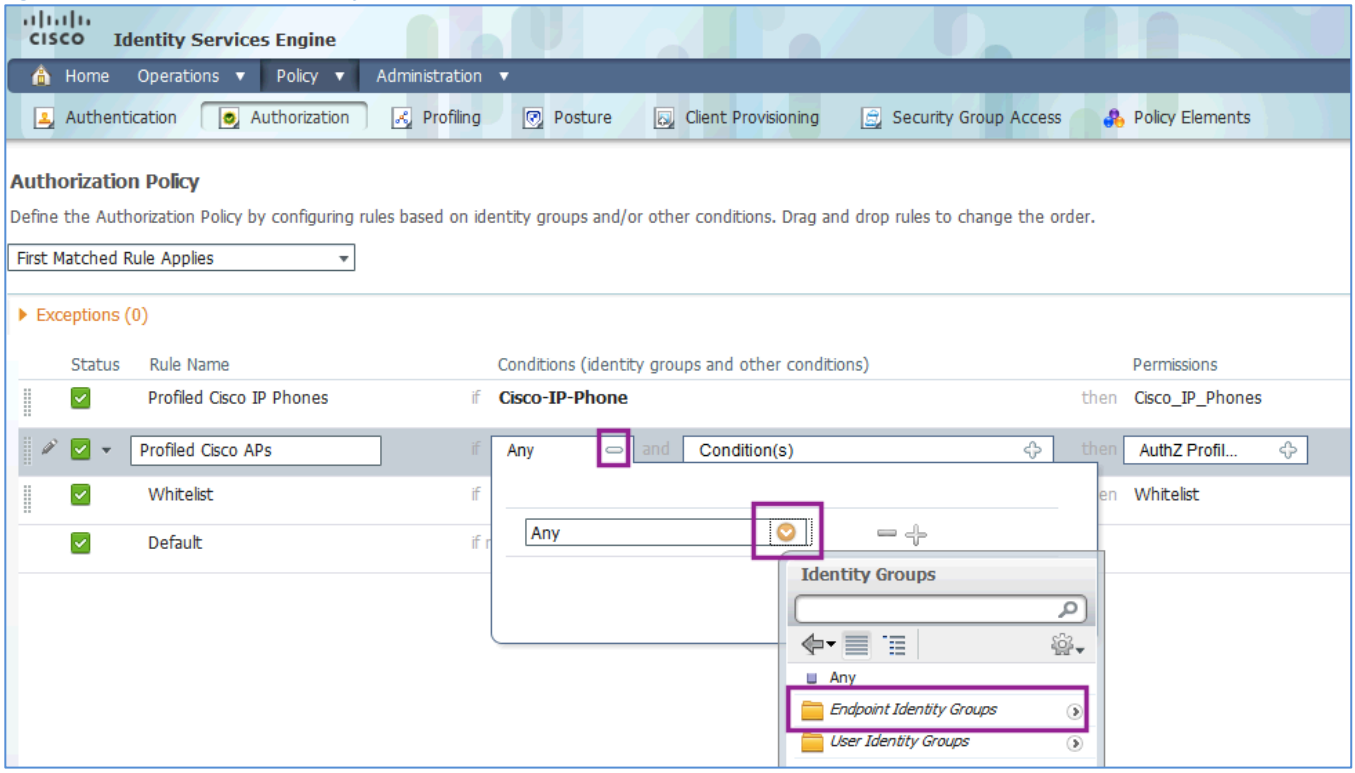
Figure 9 Add an Authorization Policy




**Step 3** Name the new rule: Profiled Cisco APs.

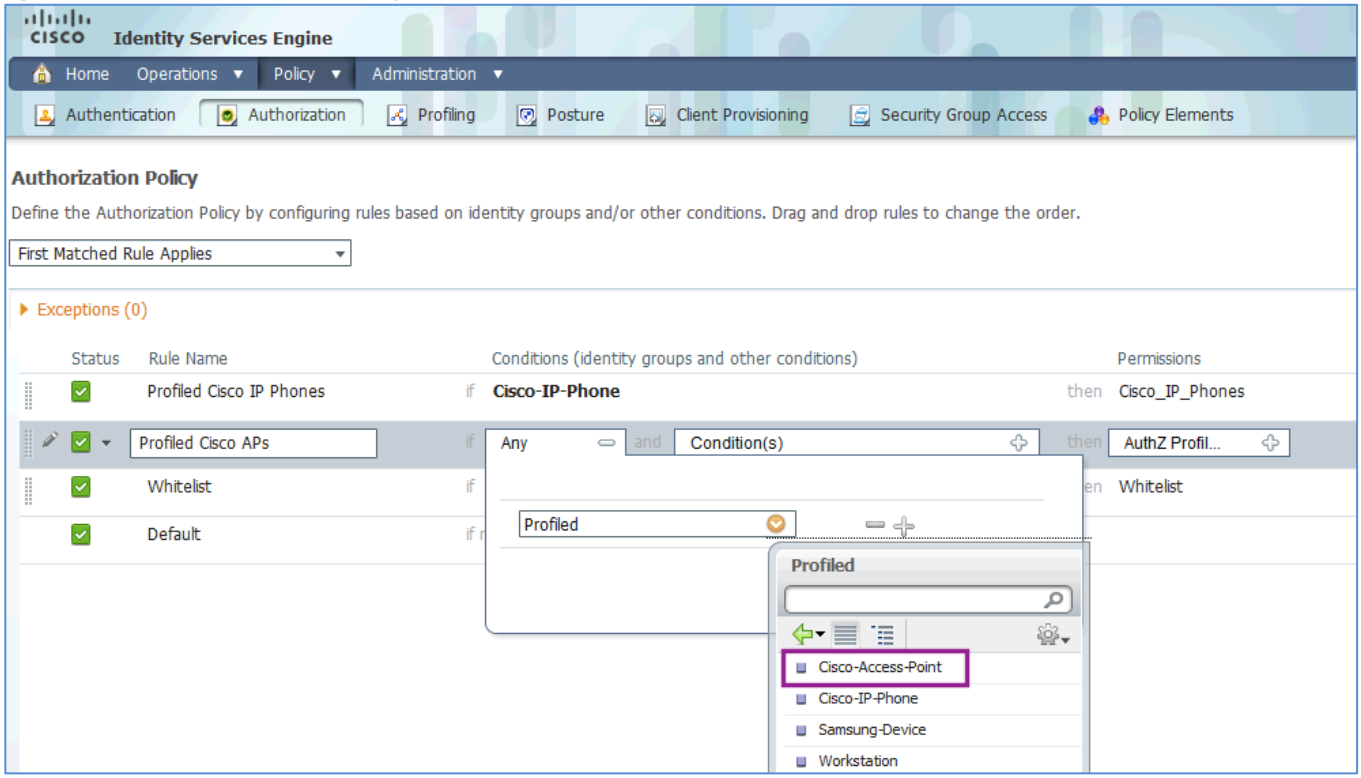
**Step 4** Click the "+" sign under the Identity Groups column.

Figure 10 Add Profiled Cisco APs Policy



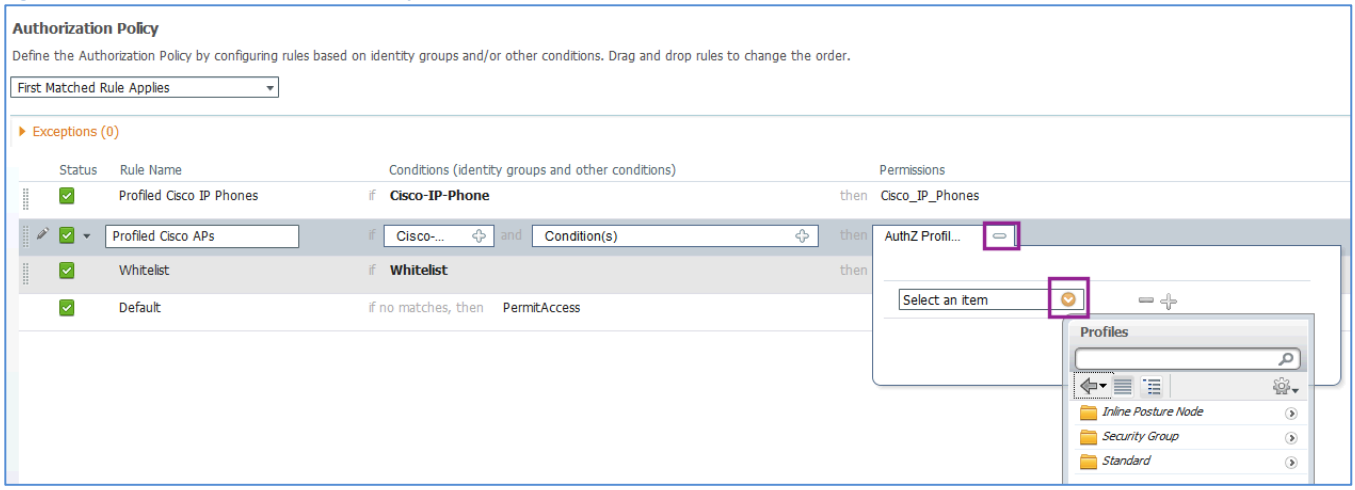

**Step 5** Select Endpoint Identity Groups → Profiled → Cisco-Access-Point (created in Procedure 1).

Figure 11 Select the Condition for the Policy



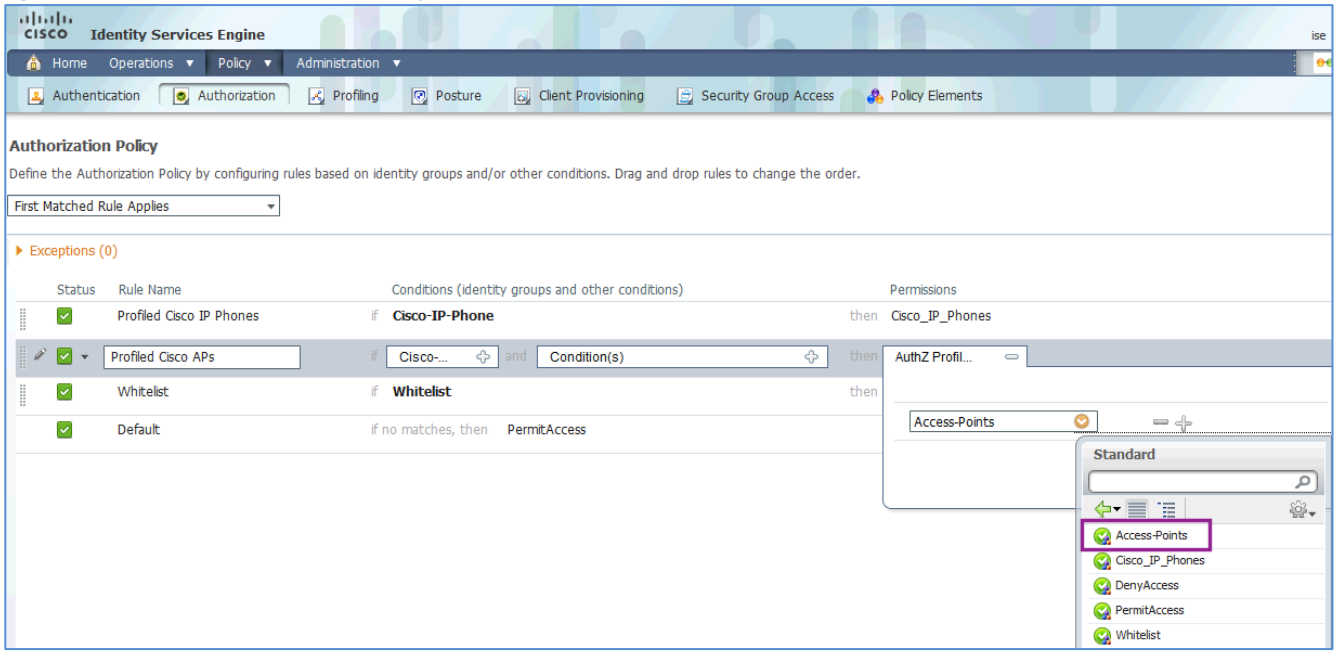

**Step 6** Click the "+" sign in the Permissions column.

Figure 12 Select the Permission for the Policy




Step 7 Select Standard → Access-Points (created in Procedure 1).

Figure 13 Select the Access Point for the Policy




Step 8 Click Save.

## Create an Authorization Rule for Windows Machine Authentication

Windows machine authentication is used to allow Windows-based computers to communicate to the Active Directory domain for group policy and other updates while the user is not logged in. This better suits enterprise environments, where machines may be running without an interactive user being logged in.

**Note:** It is not currently possible to enforce a dual authentication of both machine and user. There is an enhancement underway in the standards body and within Cisco for EAP-Chaining within EAP-FASTv2. EAP-Chaining will allow a single authentication to include both machine and user credentials. For more EAP-Chaining information, please refer to the TrustSec EAP Chaining Deployment How-To Guide.

There are multiple ways to accomplish machine authentication; for example, using a certificate such as Extensible Authentication Protocol Transport Layer Security (EAP-TLS). However, when using a non-certificate-based EAP method such as Protected Extensible Authentication Protocol (PEAP) with Microsoft Challenge Handshake Authentication Protocol Version 2 (PEAP-MSCHAPv2), Windows supplicants also have the ability to send the computer name as the credential. Cisco ISE can be configured to verify that the computer exists in Active Directory, and, if so, provide connectivity.

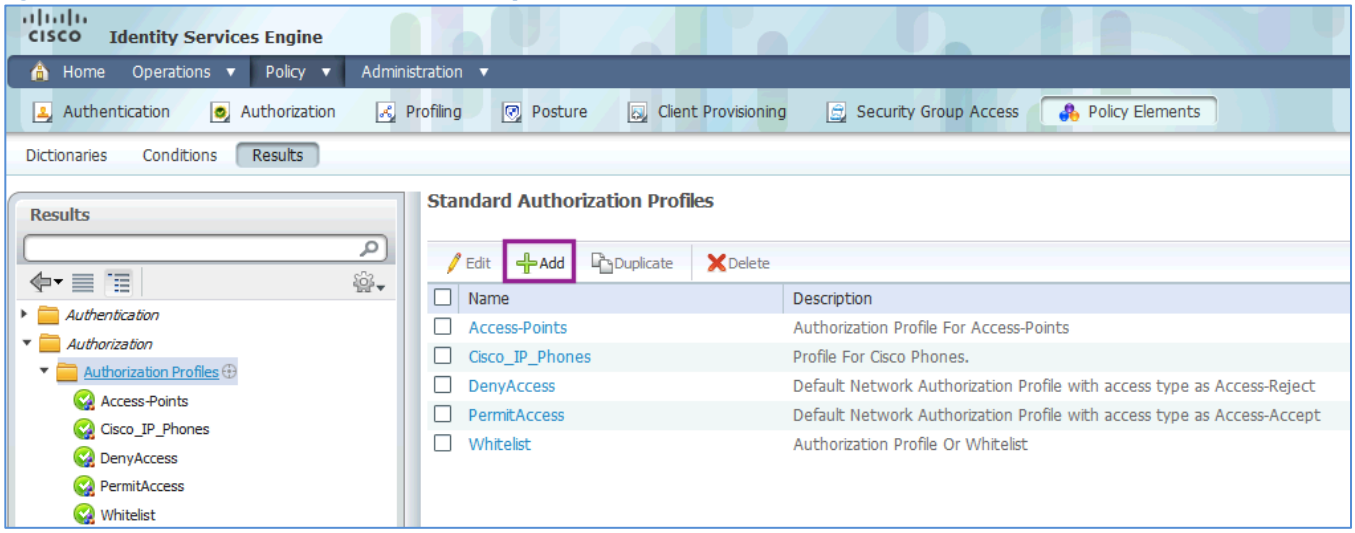
Because this phase is part of the Monitor Mode phase of deployment, we will configure the authorization rule to permit full access to the computer.

**Note:** When the user logs in to a machine-authenticated Windows endpoint, the supplicant will start a new authentication by sending an EAP over LAN (EAPoL)-Start message to the switchport. After the new authentication completes, a new authorization result may be sent to the switchport to update the authorization profile, if desired.

## Procedure 1 Create an Authorization Profile for Domain Computers

**Step 1** Navigate to Policy → Policy Elements → Results.

Figure 14 Add an Authorization Profile for Domain Computers




**Step 2** Click Add.

**Step 3** Configure the new authorization profile.

```
Name = AD_Machine_Access
Description = Authorization Profile for Windows Machine Auth
Access-Type = ACCESS_ACCEPT
-- Common Tasks
☑ DACL Name = PERMIT_ALL_TRAFFIC
☑ Airespace ACL Name = PERMIT_ALL_TRAFFIC
```

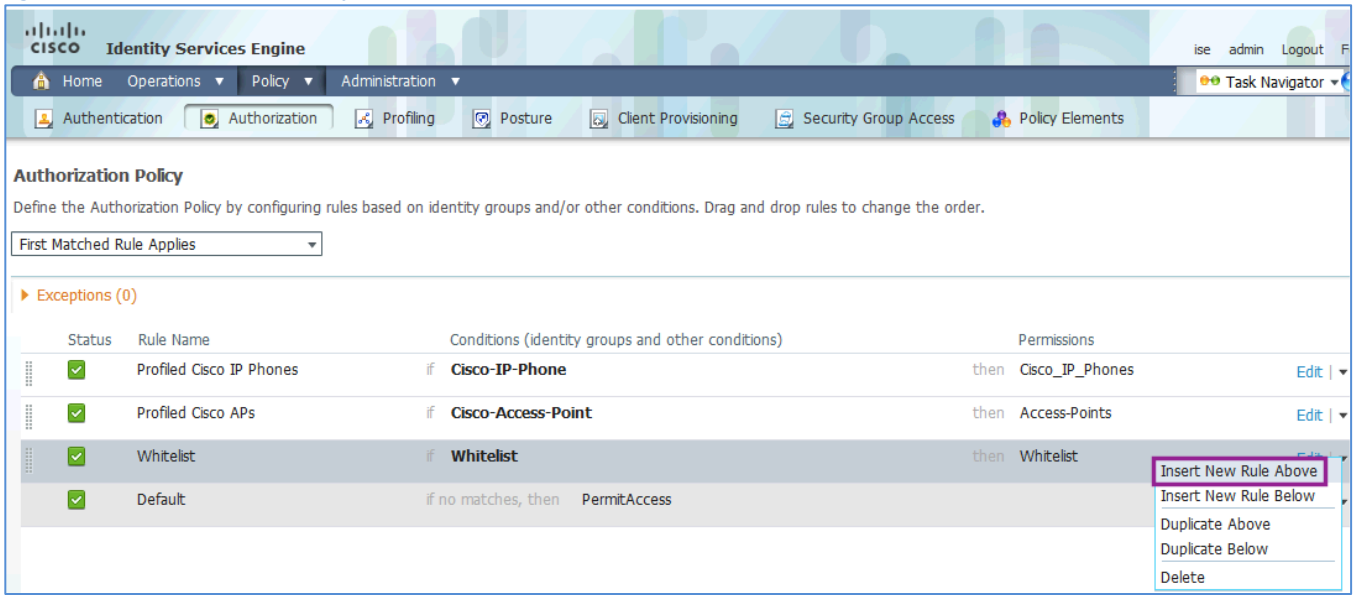
**Step 4** Scroll to the bottom, and click Submit.

## Procedure 2 Create the Domain Computer Authorization Rule

**Step 1** Navigate to Policy → Authorization.

**Step 2** Click the Action button next to the Whitelist Rule, and select 'Insert New Rule Below'.

Figure 15 Add an Authorization Policy for Whitelist



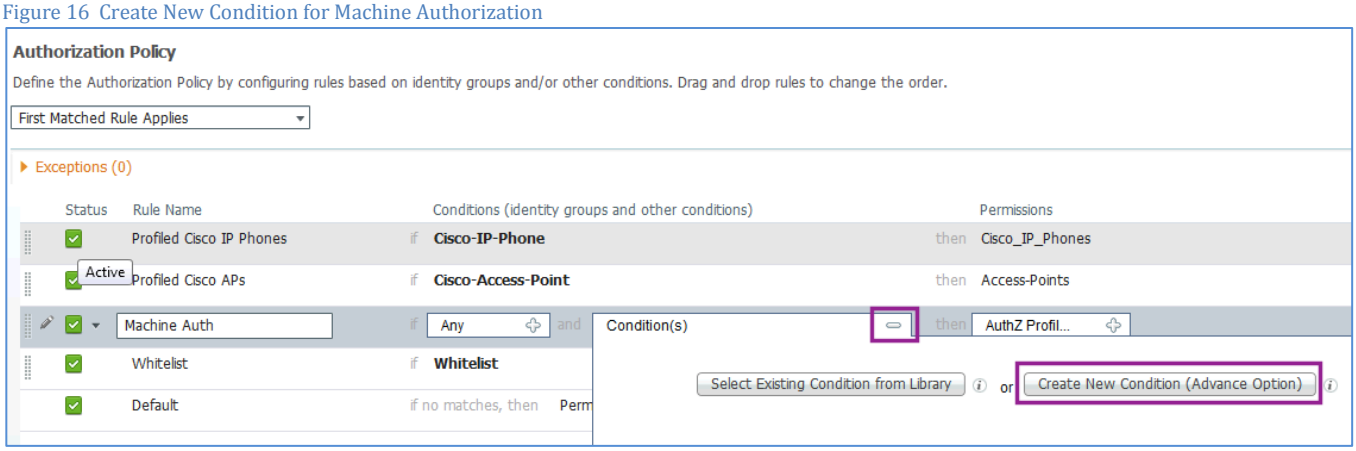

Step 3 Name the rule **Machine Auth.**

Step 4 Do not change the Identity Group; leave it as Any.

Step 5 Click the "+" sign to choose conditions.

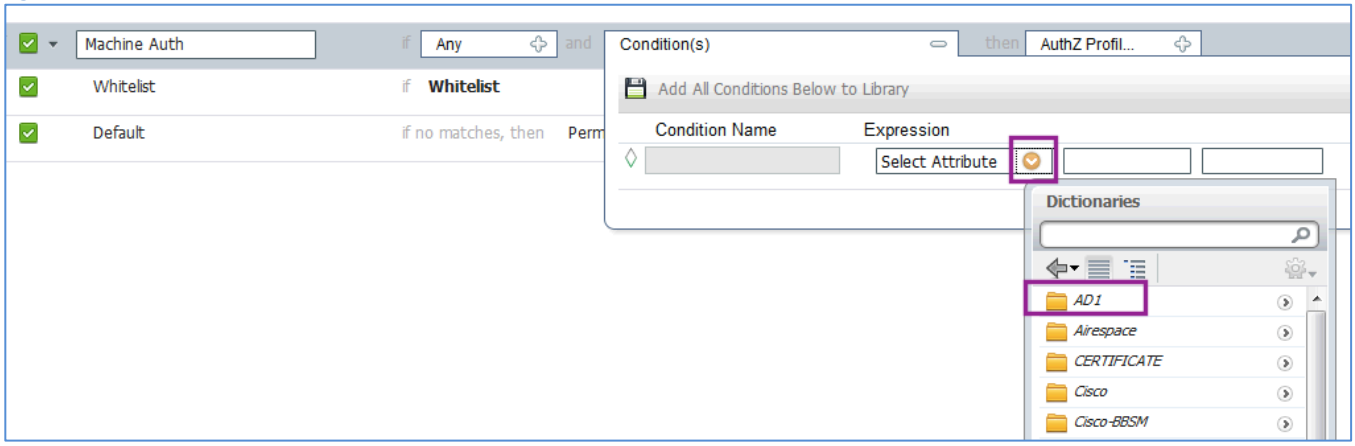
Step 6 Click Create New Condition.

Figure 16 Create New Condition for Machine Authorization



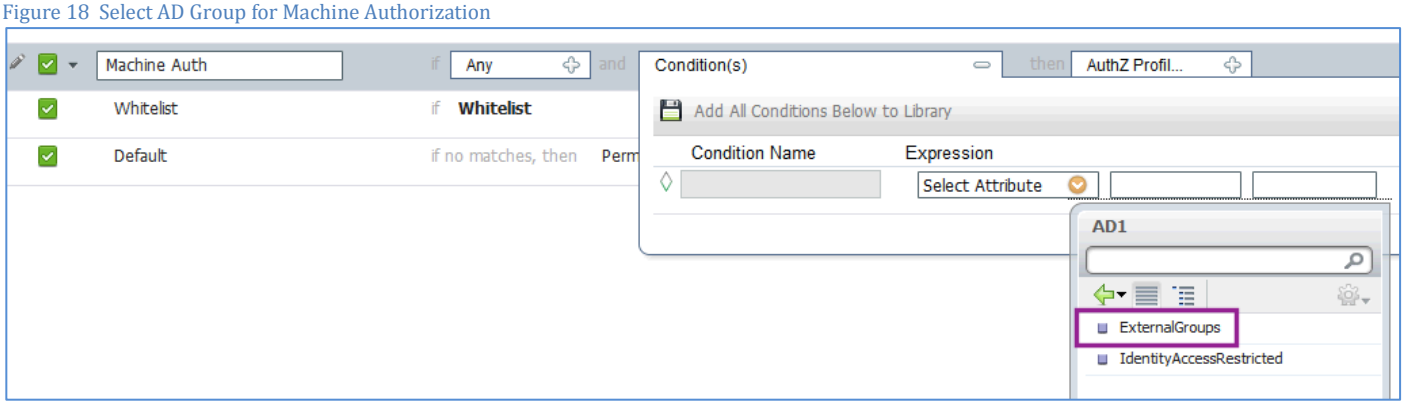

Step 7 Use the Expression pull-down menu to choose the attribute AD1.

Figure 17 Choose the Attribute for Machine Authorization



**Step 8** Select AD1 → ExternalGroups.

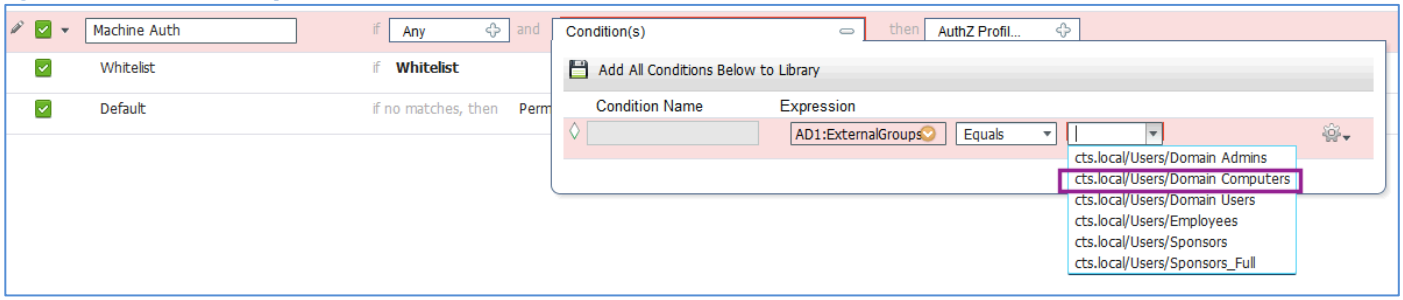
Figure 18 Select AD Group for Machine Authorization




**Step 9** Select Equals.

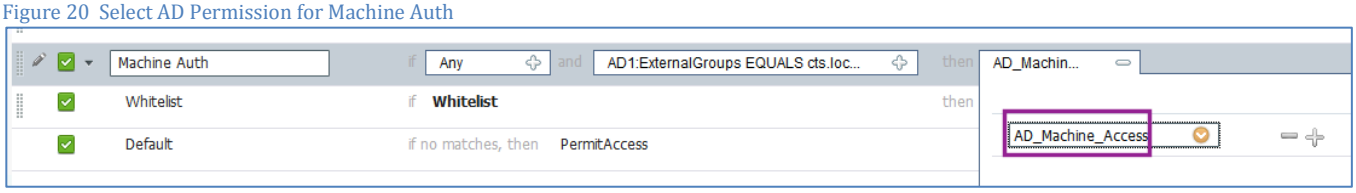
**Step 10** Select cts.local/Users/Domain Computers.

Figure 19 Select Domain Computers for Machine Authorization




**Step 11** In the Permissions column, choose Standard → AD_Machine_Access from the pull-down menu.

Figure 20 Select AD Permission for Machine Auth




**Step 12** Click Save.

## Create an Authorization Rule for Authenticated Users

One big difference between Monitor Mode and Low-Impact Mode is that in Low-Impact Mode, a user or device must successfully authenticate to the network in order to gain access. Therefore, we need to have a specific authorization rule for each user or device type. To accomplish this, we will create a new authorization rule that permits full access to any member of the Domain Users Active Directory group.

**Note:** When there is a need to create a specific access policy, it is highly recommended to create an authorization rule for each security group in AD and to discontinue the use of the Domain Users rule.

### Procedure 1 Create the Domain Users Authorization Profile

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

**Step 2** Click Add.

**Step 3** Configure the new authorization profile as described. Click Save.

```
Name = Domain_Users
Description = Authorization Profile to provide full-access to Users (Low-Impact Mode)
Access-Type = ACCESS_ACCEPT
-- Common Tasks
☑ DACL Name = PERMIT_ALL_TRAFFIC
```

## Procedure 2 Create the Domain Users Authorization Rule

**Step 1** Navigate to Policy → Authorization.

**Step 2** Insert a new rule below Machine Auth.

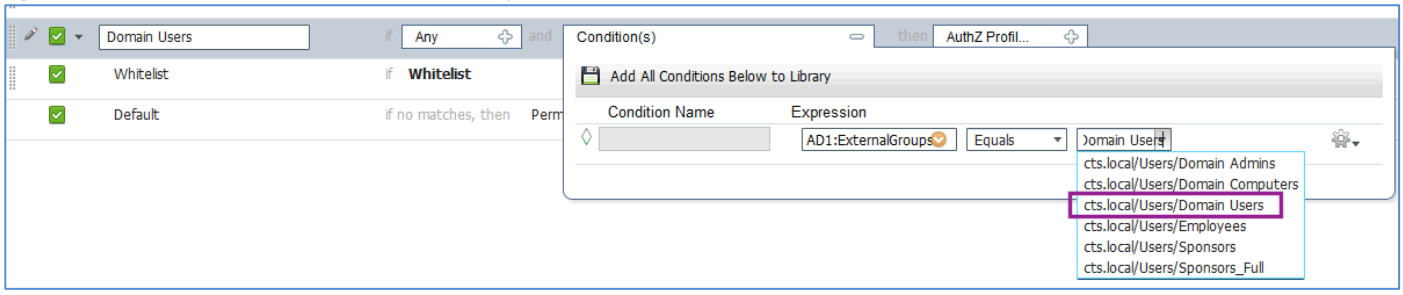
**Step 3** Name the new rule **Domain Users.**

**Step 4** Leave Identity Groups as Any.

**Step 5** Create a new condition. Choose AD1 → External Groups.

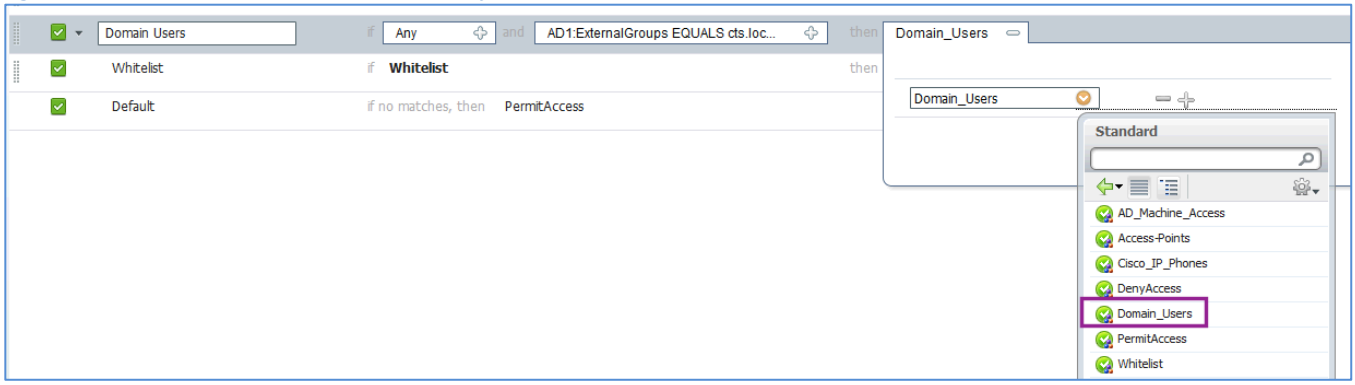
**Step 6** Set the condition to equals. Select cts.local/Users/Domain Users.

Figure 21 Choose Domain Users for Authorization Policy




**Step 7** Set the permission to Domain_Users.

Figure 22 Set the Permission for Domain Users Policy




**Step 8** Click Save.

## Wireless Access

Wireless networks have transitioned from being an optional mode of connectivity to being the primary medium used by most people. The advances in wireless technology and the proliferation of Wi-Fi-capable devices such as laptops, mobile phones, and tablets have made wireless security one of the biggest challenges for IT administrators. IT administrators have to identify users connecting to the wireless network and need to be able to differentiate between users using corporate assets and users using personal assets on the corporate networks.

The use cases we will cover are:

1. Employees that are using corporate devices (laptops/tablets: EAP-TLS) and are posture-compliant = full access (VLAN + no ACL)

2. Employees using their personal devices (PEAP) = Internet-only access (same VLAN + named ACL restricting access)

3. Guests = Internet-only access (enforced using ACLs)

TrustSec uses technologies such as IEEE 802.1X authentication and profiling to allow IT administrators to provide differentiated access on wireless networks in a scalable and easily manageable manner. TrustSec uses Cisco ISE as a central policy-management server to help provide secure wireless networks and enables organization to allow their users to bring their own devices (a standard now known as “BYOD”).

This document outlines the steps to configure Cisco ISE and the Cisco Wireless LAN Controller (WLC) to enable differentiated access on wireless networks to allow BYOD. We will also highlight how TrustSec allows you to provide guests with wireless access.

The use cases we will cover are:

1. Employees that are using corporate devices (laptops/tablets: EAP-TLS) and are posture-compliant = full access (VLAN + no ACL)

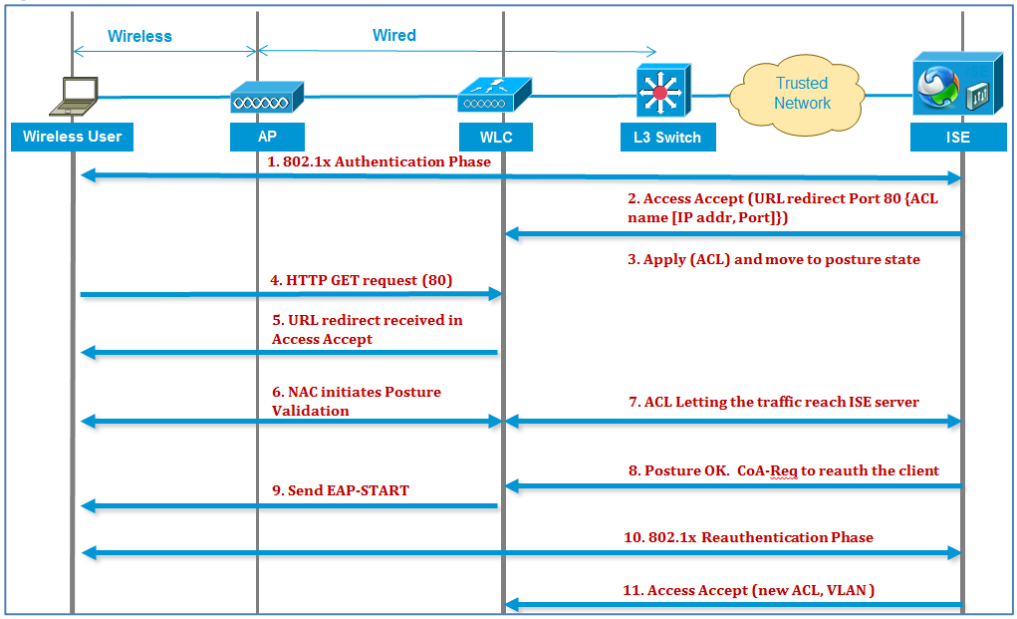
2. Employees using their personal devices (PEAP) = Internet-only access (same VLAN + named ACL restricting access)

3. Guests = Internet-only access (enforced using ACLs)

## Elaboration on Wireless Access

Cisco ISE’s ability to enforce wired and wireless access policy makes it easy for IT administrators to provide users with a similar network access experience across both access mediums. Cisco ISE allows us to perform user authentication, device profiling, and posture assessment on a wireless network configured for IEEE 802.1X authentication. The authentication and authorization flow for wireless users is explained in Figure 23.

Figure 23 Wireless 802.1X Authentication Flow




1. Client successfully authenticates using dot1x authentication.

2. RADIUS Access Accept carries redirected URL for port 80 and pre-auth ACLs that includes allowing IP addresses and ports **or** quarantine VLAN.

3. Client will be redirected to the URL provided in Access Accept and put into Posture_Req until posture validation is complete.

4. NAC agent on client initiates posture validation (traffic to port 80): Agent sends HTTP discovery request to port 80, which the controller redirects to a URL provided in Access Accept. Cisco ISE knows that the client is trying to reach it and responds directly to the client. This way the client learns about Cisco ISE server IP and, from now on, the client talks directly with Cisco ISE server.

5. WLC allows this traffic because we have configured our ACL to allow it. In the case of VLAN override, we simply bridge the traffic so that it reaches the Cisco ISE server.

6. When the Cisco ISE client completes assessment, a RADIUS CoA-Req with re-auth service is sent to WLC, which initiates re-authentication of the client (by sending EAP-START). When re-authentication succeeds, Cisco ISE sends Access Accept with a new ACL (if any) and no URL redirect **or** access VLAN.

7. WLC supports CoA-Req and Disconnect-Req as per RFC 3576. WLC needs to support CoA-Req for re-auth service, as per RFC 5176.

8. Instead of downloadable ACLs, we need to use preconfigured ACLs on the WLC. The Cisco ISE server sends the ACL name, which is already configured in the WLC.

9. This design should work for both VLAN and ACL cases. In the case of VLAN override, we redirect the port 80 and allow (bridge) the rest of the traffic on the quarantined VLAN. For the ACL, we will apply the pre-auth ACL we got in Access Accept.

## Wireless in Branch Offices

In a typical wireless deployment, all traffic from an access point is tunneled back to a WLC from where it is introduced on the network. This tunneling is known as the Split-MAC architecture for wireless networks. Because all the traffic is switched centrally at the WLC, Cisco ISE pushes the policy down to the WLC.

Although the Split-MAC architecture works well for campus WLAN deployments, it is not recommended for remote-site deployments. Access points installed at remote sites would typically communicate with the WLAN located in a data center. Using the Split-MAC architecture requires all user traffic to travel first over the WAN to the WLC before it is switched. This creates an additional load on WAN links. Cisco recommends using the Hybrid Remote Edge Access Point (H-REAP) or Local MAC architecture. The H-REAP model forwards only the control traffic to the WLC over the WAN link, and all user data is switched locally at the remote site (Table 1).

Table 1 TrustSec Features on Wireless Controllers

| TrustSec Features | Cisco 5508 Wireless Controller and Cisco Wireless Services Module 2 (WiSM-2) | | Cisco Flex 7500 Series Wireless Controller[1] | |
|---|---|---|---|---|
| | Central Switching | Local Switching | Central Switching | Local Switching |
| Basic AAA Functions | Yes | Yes | N/A | Yes |
| Profiling | Yes | No | N/A | No |
| Posturing | Yes | No | N/A | No |
| VLAN Override | Yes | No | N/A | No |
| ACL Override | Yes | No | N/A | No |
| Guest Provisioning | No | No | No | No |

## Web Authentication

Configuration of Web Authentication is a critical step when moving transparently from Monitor Mode into Low-Impact Mode. Until this point, the default rule (the "rule of last resort") in the authorization policy was set to PermitAccess, meaning that if a device does not meet any of the more specific criteria mentioned previously, we will allow it full access to the network.

By implementing Web Authentication, we will provide a different authorization rule of last resort. If you are not authorized by one of the more specific rules, then the user/device will be forced into an authorization state where traffic is extremely limited and the switch/WLC will redirect all web traffic to the Web Authentication captive portal. This redirection provides a webpage for users (guests and employees alike) to authenticate to the network and receive an authorization result.

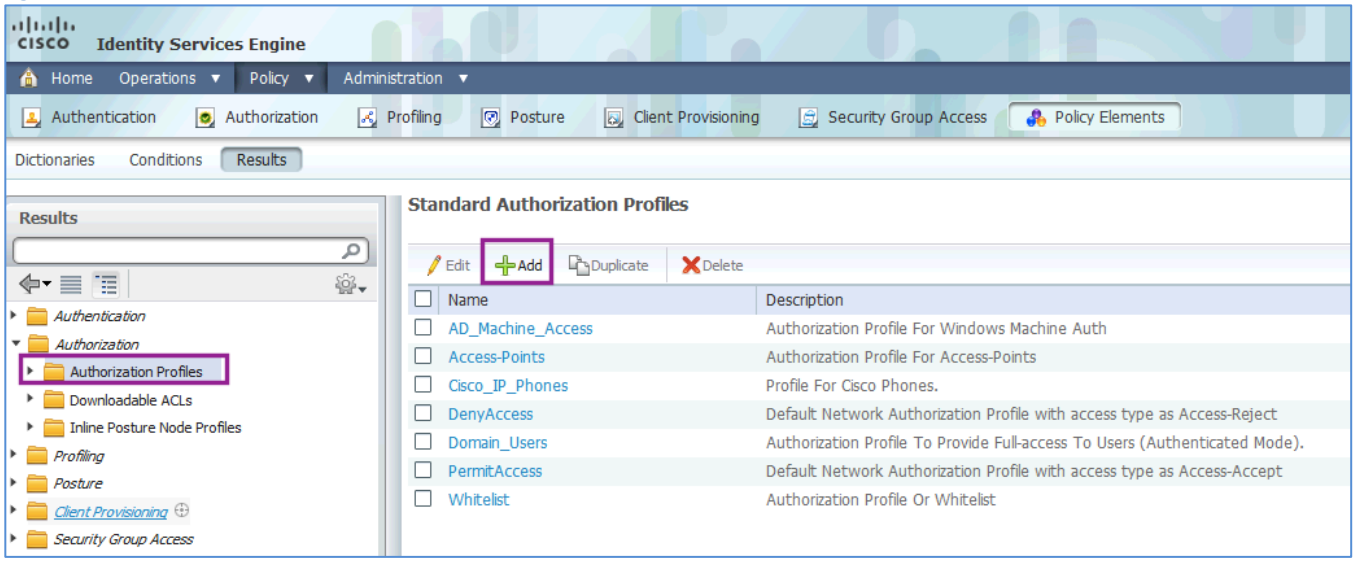
There are two different Web Authentication types. There is Local WebAuth, where the webpages and the authentication transaction occur locally to a switch or WLC. Then there is a more advanced centralized Web Authentication method where the switch or WLC redirects web traffic to a centralized captive portal on ISE, and the authentication transaction occurs at the ISE instead of locally on the WLC.

[1] WLC 7.2.110.0 added support for TrustSec with HREAP, but it has not yet been through testing for TrustSec version and therefore is not included in this document.

## Procedure 1 Create a WEBAUTH Authorization Profile

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

Figure 24 Create a WebAuth Authorization Profile




**Step 2** Name the authorization profile **WEBAUTH.**

**Step 3** Leave the access type as ACCESS_ACCEPT.

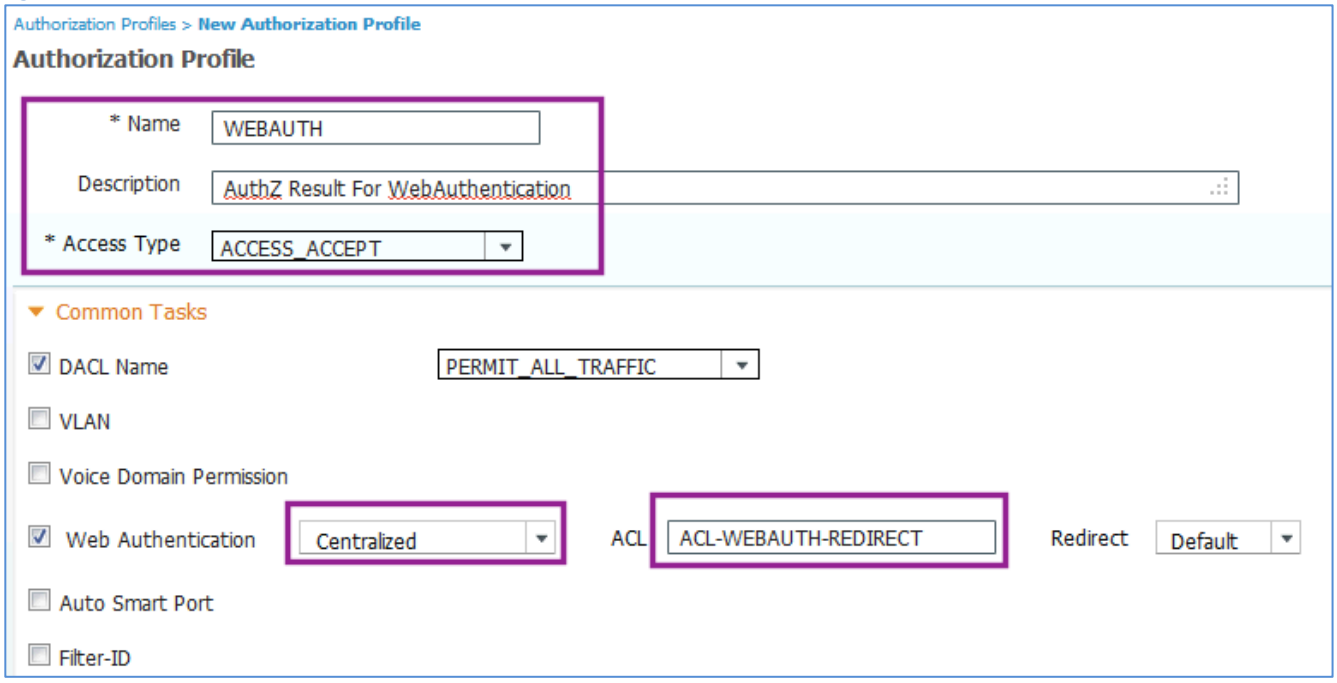
**Step 4** Set the dACL to PERMIT_ALL_TRAFFIC.

**Step 5** Enable Centralized Web Authentication, and enter **ACL-WEBAUTH-REDIRECT** as the ACL.

**Step 6** The ACL-WEBAUTH-REDIRECT ACL is built on the switch. This ACL identifies the "interesting" traffic. Traffic matching that ACL will be redirected to the Centralized Web Authentication Portal. This ACL is distinctly different from a dACL that limits traffic through the port.

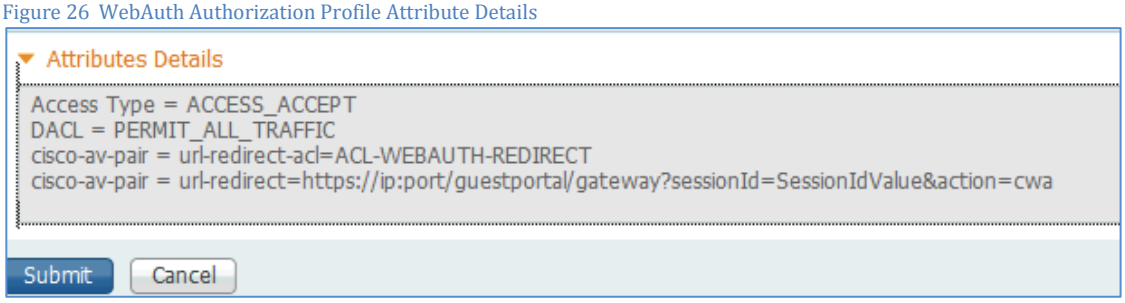
**Step 7** Leave the redirect as Default.

Figure 25 WebAuth Authorization Profile Details




Step 8 Scroll to the bottom of the page and validate that the Attributes Details look like the one in Figure 26.

Figure 26 WebAuth Authorization Profile Attribute Details




Step 9 Click Submit.

## Guest Access

We have just configured Web Authentication that may be used for employees and for guests. Even though the lifecycle is known as guest lifecycle management, it can refer to any user needing network access. Cisco ISE provides mechanisms to create multiple guest types and control which sponsor groups are able to create each guest type.

For the purposes of this document, we will have only a single guest type. A single authorization rule will need to be created for that guest type.

## Cisco ISE Configuration – Configure the Guest Authorization

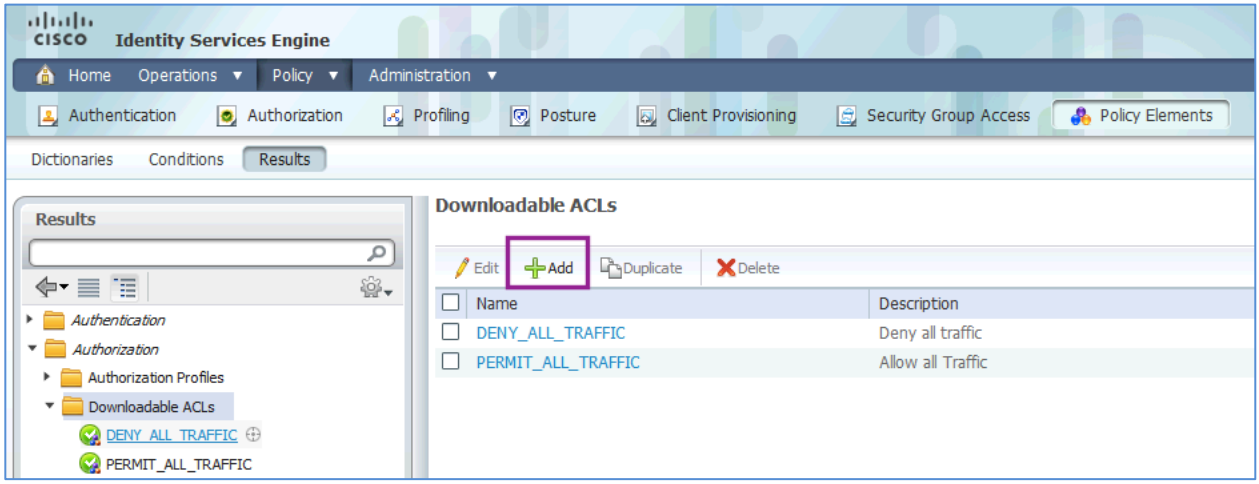
Authorization for guest users is a complex topic. For the purposes of this design guide, we will authorize the guest users into the guest VLAN, and provide a downloadable ACL that permits all traffic ingress at the switch.

This type of authorization is commonly used and assumes the network infrastructure is what is isolating the guest user from the remainder of the corporate network. This type of isolation is often accomplished using network virtualization (VRF instances) or even simply access lists at the Layer 3 edge.

### Procedure 1 Create a GUEST Downloadable ACL.

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

Figure 27 Create a dACL




**Step 2** Click Add.

**Step 3** Configure the new dACL.

```
Name = GUEST
Description = dACL for GUEST users (Authentication Mode)
DACL Content = 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 4** Click Submit.

### Procedure 2 Create a Guest Authorization Profile

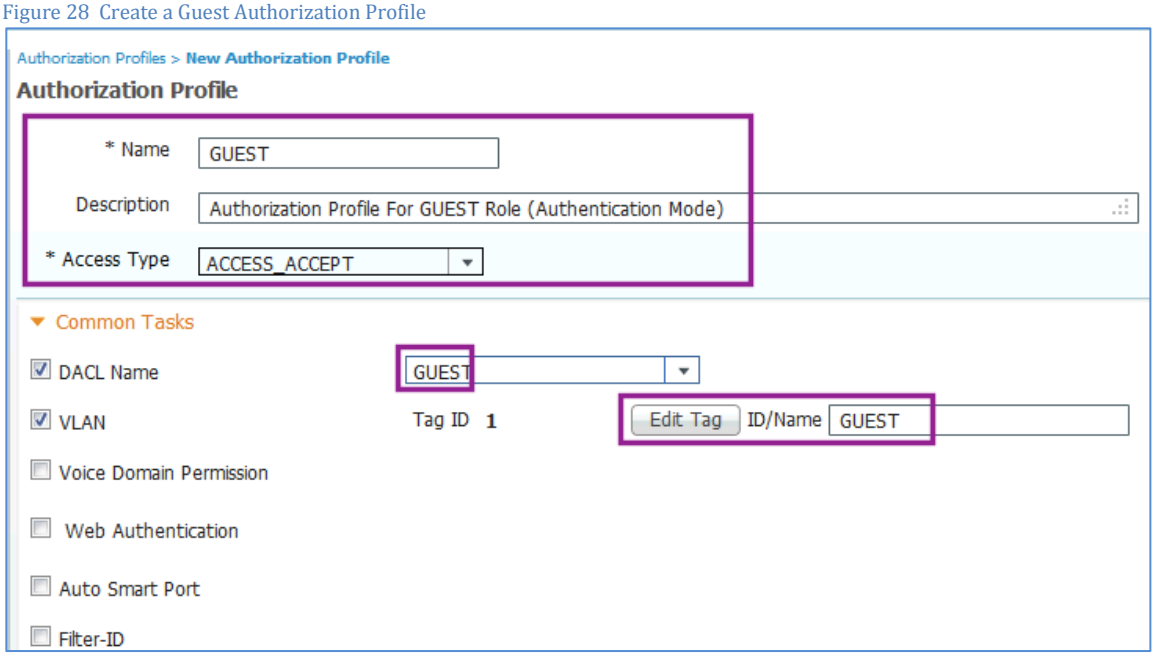
**Step 1** Navigate to Policy → Policy Elements → Results → Authorization → Authorization Profiles.

**Step 2** Click Add.

**Step 3** Configure the new authorization profile.

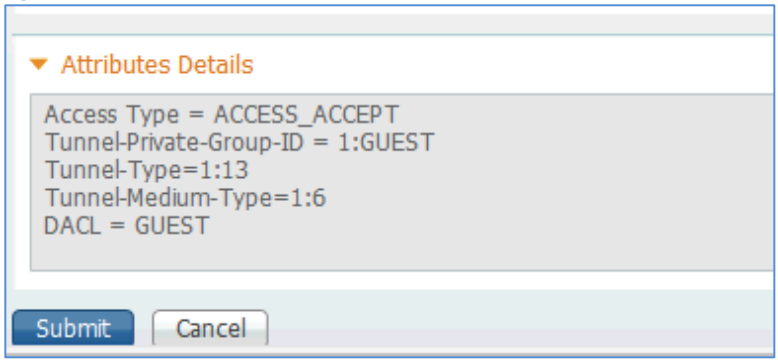
```
Name = GUEST
Description = Authorization Profile for GUEST role (Authentication Mode)
Access-Type = ACCESS_ACCEPT
-- Common Tasks
☑ DACL Name = GUEST
☑ VLAN = GUEST
```

Figure 28 Create a Guest Authorization Profile




**Step 4** Scroll to the bottom of the page. Make sure the Attributes Details look like those in Figure 29, and click Submit.

Figure 29 Guest Authorization Profile Attributes Details




**Note:** The switchport host mode is extremely important when using VLAN assignment. VLAN assignment is not recommended when using Multi-Auth or Multi-Host Modes. Only one VLAN may be assigned to the data domain and one VLAN to the voice domain. Multi-Auth and Multi-Host Modes allow for more than one device in the data domain; therefore, the first VLAN assigned to the port will take effect for all switchports.

## Procedure 3 Create a Guest Authorization Policy Rule

**Step 1** Navigate to Policy → Authorization.

**Step 2** Insert a new rule above the Default rule (bottom of the Policy table).

**Step 3** Name the new rule **GUEST.**

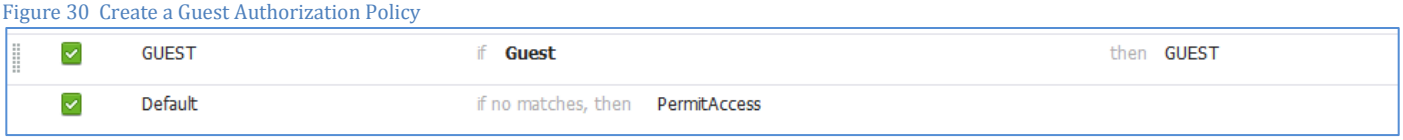
**Step 4** Under Identity Groups, click the "+" sign on the picker.

**Step 5** Choose User Identity Groups → GUEST.

**Step 6** Leave Other Conditions alone.

**Step 7** For Permissions, click the "+" sign and select **Standard → GUEST.**

Figure 30 Create a Guest Authorization Policy




**Step 8** Click Save.

## Cisco ISE Configuration – Guest Account Creation

### Procedure 4 Configure Guest User in the Sponsor Portal

**Step 1** From your web browser, navigate to the sponsor portal at:

`https://<portal_host_or_IP_address>:8443/sponsorportal`

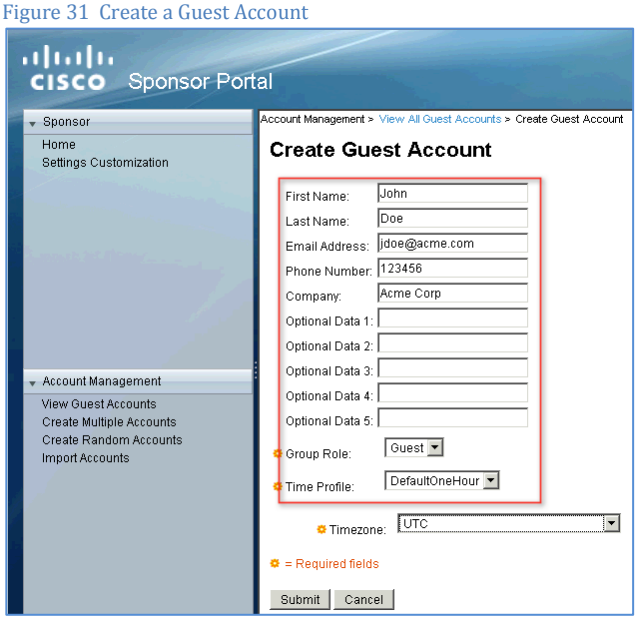
**Step 2** Log in to the portal using the sponsor user's credentials.

**Step 3** Navigate to Create Guest Account.

**Step 4** Configure, at a minimum, the required fields shown in Figure 31.

**Step 5** Click Submit.

Figure 31 Create a Guest Account




## Change Default Authorization to WebAuth and Test

### Procedure 1 Change the Default Authorization Rule to WebAuth

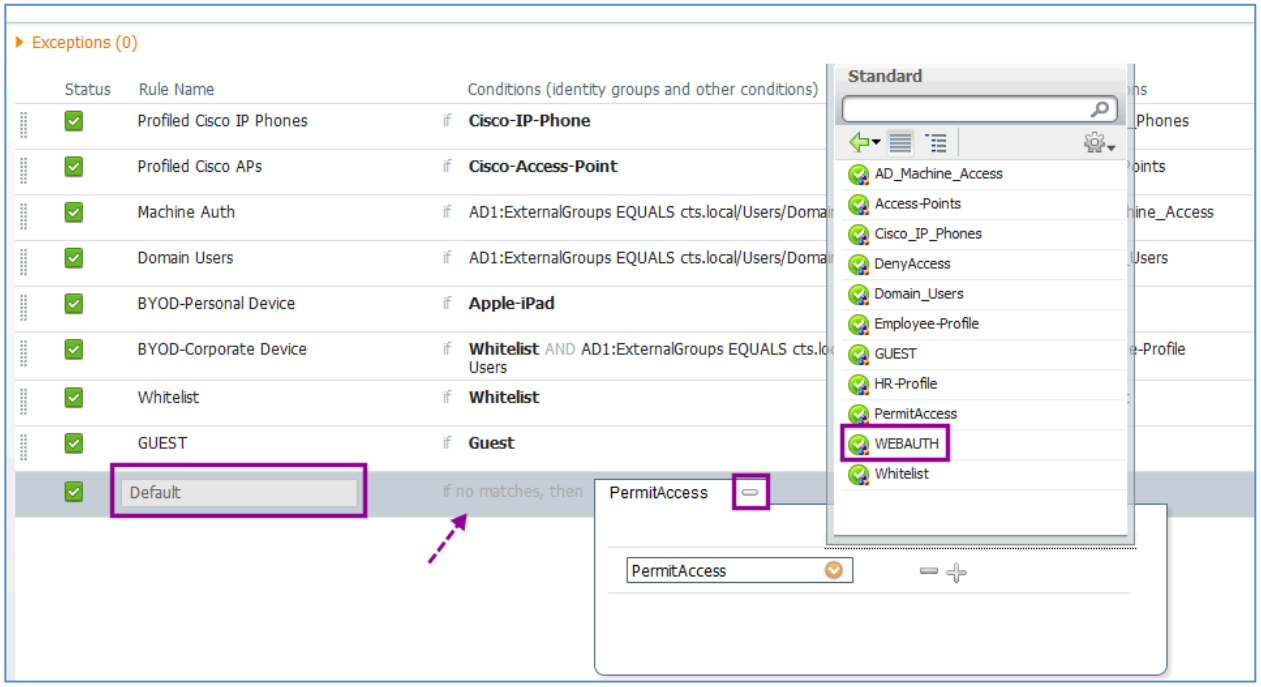
**Warning:** Before completing this step, ensure you are ready for Low-Impact Mode. After this procedure, any device that does not have a specific authorization rule will be put into the WEBAUTH authorization state.

**Step 1** Navigate to Policy → Authorization.

**Step 2** Scroll to the bottom, and click the "+" sign in the picker, next to "if no matches, then".

**Step 3** Select Standard → WEBAUTH. Click Save.

Figure 32 Change the Default Authorization Rule to WebAuth




## Procedure 2 Test Web Authentication

**Step 1** Now that the "authorization of last resort" has been set to WebAuth, it is time to verify that WebAuth is working correctly.

**Step 2** Connect to the network with a Windows or Mac device that does not have a configured supplicant.

**Step 3** On the switch, verify the authorization result.

```
C3750X#show authentication session interface <interface_name>
```

```
C3750X#show authentication session int gig1/0/2
            Interface:  GigabitEthernet1/0/2
          MAC Address:  0050.5687.0004
           IP Address:  10.1.10.50
            User-Name:  00-50-56-87-00-04
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Group:  N/A
              ACS ACL:  xACSACLx-IP-PERMIT ALL_TRAFFIC-4dc4ad0d
     URL Redirect ACL:  ACL-WEBAUTH-REDIRECT
         URL Redirect:
https://ise.cts.local:8443/guestportal/gateway?sessionId=0A0130020000000F2703ACFF&action=cwa
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A0130020000000F2703ACFF
      Acct Session ID:  0x00000012
               Handle:  0x7E00000F

Runnable methods list:

       Method   State
       dot1x    Failed over
       mab      Authc Success
```

**Step 4** View the Cisco ISE Live Authentication Log for the session.

Figure 33 Log for Web Authentication

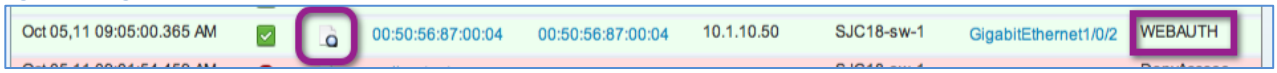
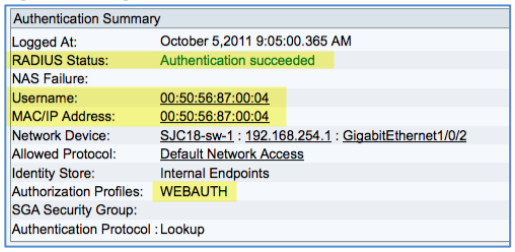
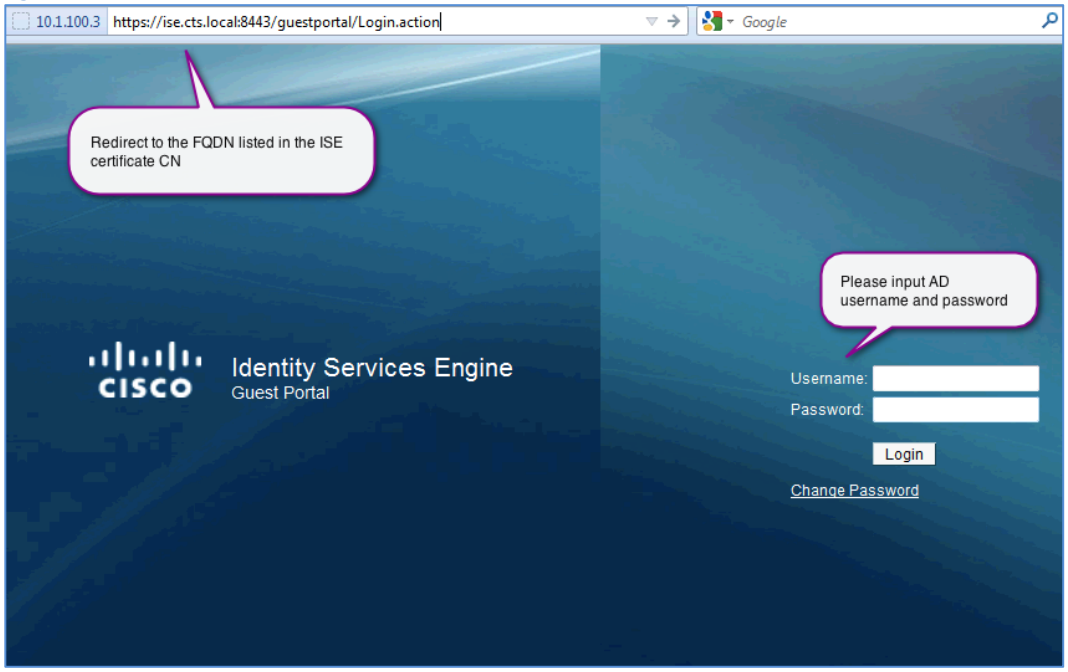



Figure 34 Log Detail for Web Authentication




**Step 5** On the client, open a web browser. Traffic will be automatically redirected to Cisco ISE.

Figure 35 Web Redirect




**Common Issue:** If Cisco ISE is not in the DNS, this redirection will fail. Ensure that all Cisco ISE nodes are listed correctly in the DNS. We entered "employee1," which is a valid AD user account.

**Step 6** The Acceptable Use policy will display, and Employee1 accepts it.

**Step 7** A new authorization occurs. View the results on the switch and the Live Authentications Log:

```
C3750X#show authentication session interface <interface_name>
```

```
C3750X#show authen sess int g1/0/2
           Interface:  GigabitEthernet1/0/2
         MAC Address:  0050.5687.0004
          IP Address:  10.1.10.50
            User-Name:  employee1
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-auth
    Oper control dir:  both
```

```
        Authorized By:  Authentication Server
           Vlan Group:  N/A
              ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-4dc4ad0d
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A0130020000001127DC1A50
      Acct Session ID:  0x00000014
               Handle:  0x53000011

Runnable methods list:
       Method   State
       dot1x    Failed over
       mab      Authc Success
```

**Note:** Notice the changes in the output. The URL redirection is no longer there, and the username is known.

Figure 36 Log for Employee1 Authentication

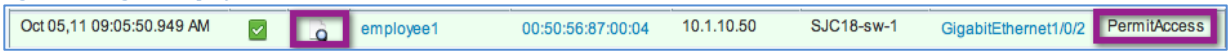
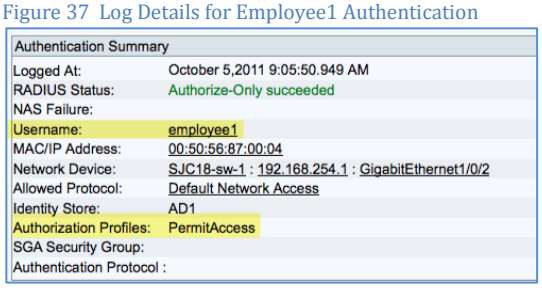



Figure 37 Log Details for Employee1 Authentication




## Configure Cisco ISE for Wireless Guest Access

Organizations typically have an open SSID to provide guest access. When a guest user is connected to the SSID, they will be redirected to the Cisco ISE guest portal. Here, they can use the guest credentials (created by a sponsor) and gain access to the network.

**Note:** Using "anchor" controllers located in a DMZ to completely isolate guest traffic from corporate traffic is a recommended best practice. Because it was not part of the TrustSec Systems Test, however, it cannot be part of this documentation. Even so, please be warned that because Cisco ISE would typically be located within a data center, it is difficult to allow a client whose traffic is going through an anchor controller located in a DMZ to send traffic back to the data center. This concern will be addressed in a future release of Cisco ISE.

### Procedure 1 Define the Guest ACL on the WLC

Refer to HowTo-11-Universal_WLC_Configuration for more information on creating a wACL.

**Step 1** Add rules for the guest wACL (Table 2).

Table 2 Guest wACL

| Guest wACL | | | |
|---|---|---|---|
| Sequence | 1 | 2 | 3 |
| Source | Any | Any | Any |
| Destination | IP address<br>10.1.20.1<br>255.255.255.255 | IP address<br>10.1.0.0<br>255.255.0.0 | Any |
| Protocol | Any | Any | Any |
| DSCP | Any | Any | Any |

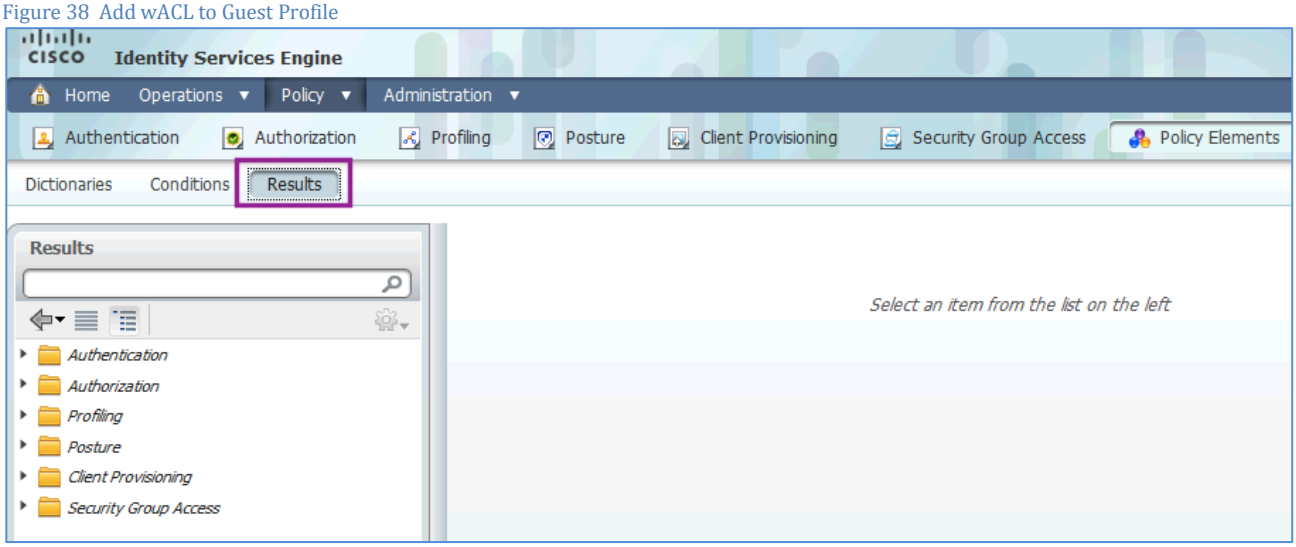
| | | | |
|---|---|---|---|
| Direction | Any | Any | Any |
| Action | Permit | Deny | Permit |

**Note:** DNS is permitted by default for pre-authenticated endpoints.

## Procedure 2 Add the wACL to the Guest Authorization Profile on Cisco ISE

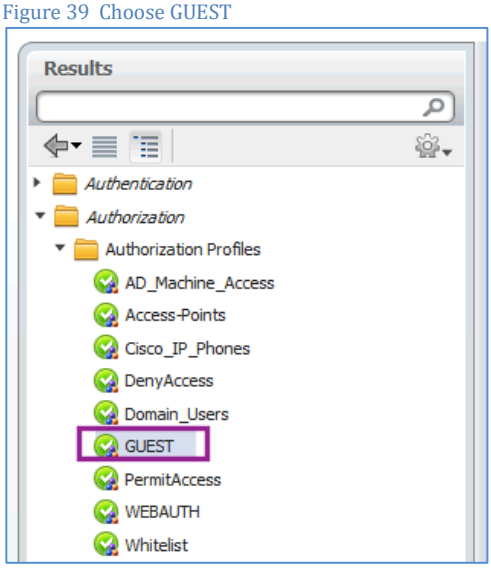
**Step 1** On Cisco ISE, navigate to Policy → Policy Elements → Results.

Figure 38 Add wACL to Guest Profile




**Step 2** Select Authorization → Authorization Profiles → GUEST.

Figure 39 Choose GUEST




**Step 3** Add the wACL value under the Common Tasks section.

- ☑ DACL Name = **PERMIT_ALL_TRAFFIC**
- ☑ Airespace ACL Name = **GUEST-ACL**

# Committing to Low-Impact Mode

At this stage, the Cisco ISE policies have all been created to allow all authenticated devices to have full access to the network; Web Authentication has been configured, and sponsored guest access and guest account creation is operational. However, the default port ACL on the switches still allows all traffic.

To fully commit to Low-Impace Mode, we must 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 ACLs that have been used in the field, and discuss what complications may exist in your deployment and how to adjust the default ACL appropriately.

Following are two suggested default ACLs. We configured the first one in the HowTo-10-Universal_Switch_Configuration How-To Guide.

ACL-DEFAULT (the recommended, secure default 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 we accomplished in the "Create an Authorization Profile for Domain Computers" procedure.

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
```

**Note:** If 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:

Option1: Use a network packet sniffer application to identify all traffic attempts prior to login.

Option2: 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

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

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

## Examining Additional User Information

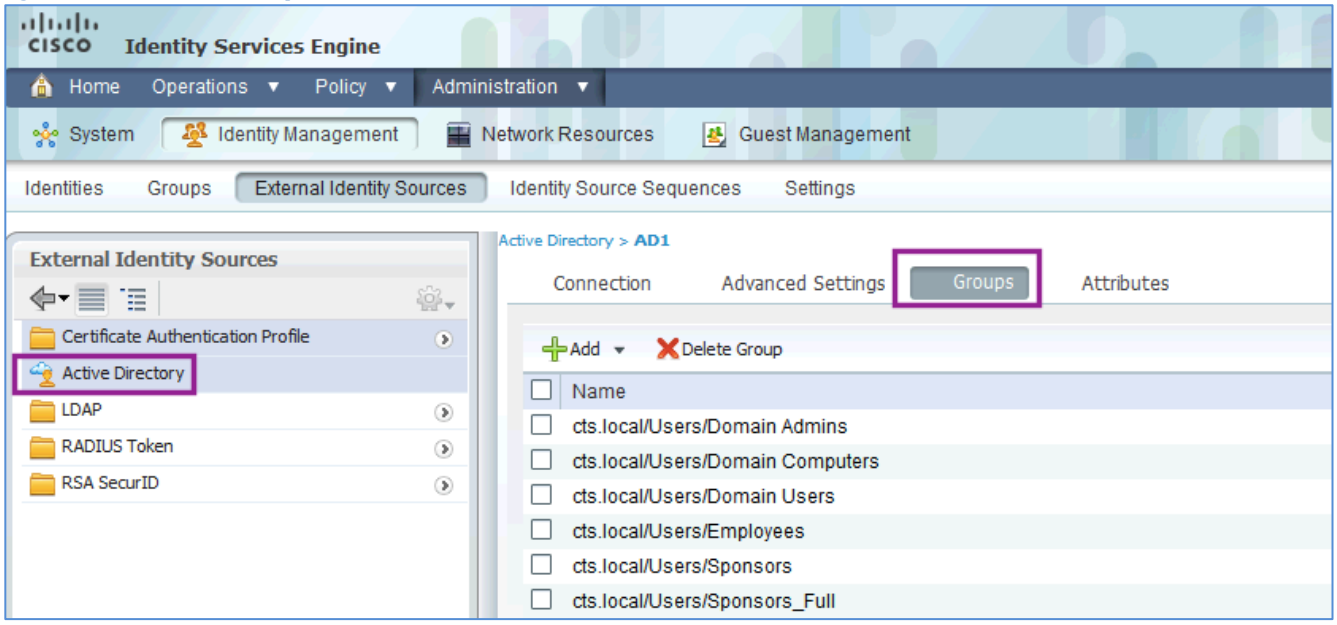
Until this point, if a user was a member of the Domain Users group, that user received full network access. To improve security, we will look at additional groups, and provide differentiated access to each group. Please reference the table of Active Directory users and group membership.

### Procedure 1 Add Additional Groups to the Active Directory Connector

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

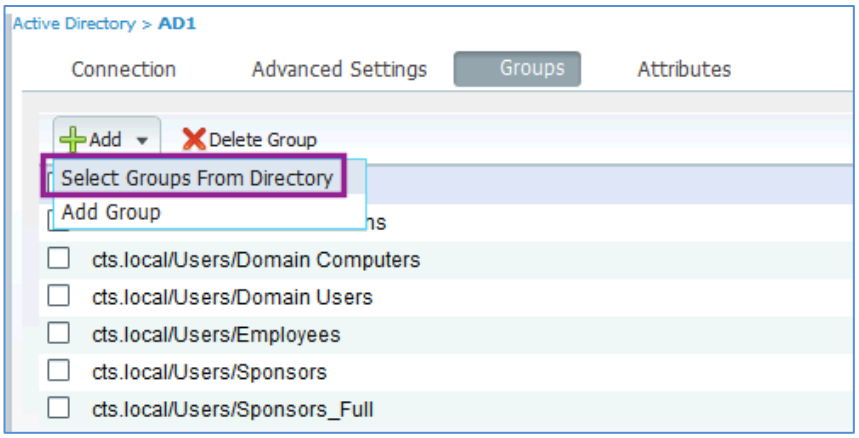
**Step 2** Click the Groups tab.

Figure 40 Add Additional Groups




**Step 3** Click Add → Select Groups From Directory.

Figure 41 Select Groups from Active Directory




**Step 4** Click Retrieve Groups.

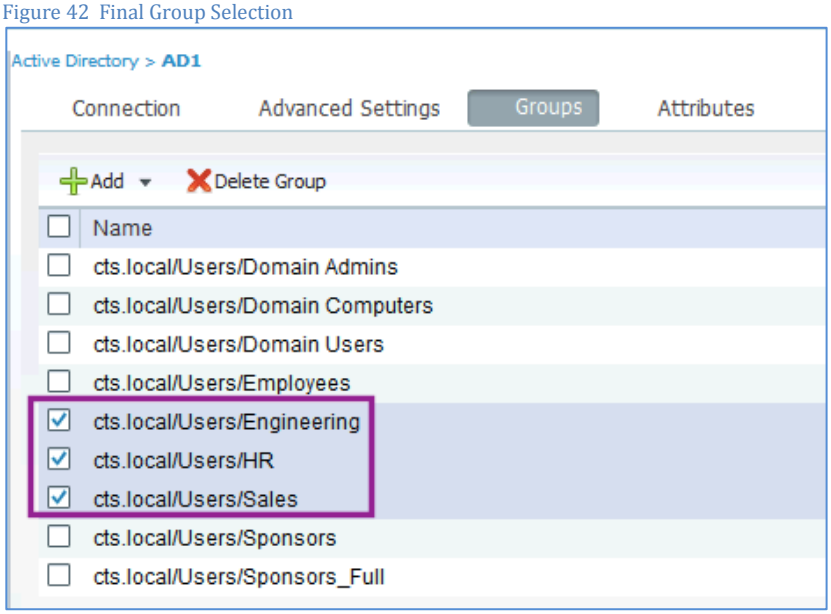
**Note:** When Active Directory has more than 100 groups, use the filter options to find the specific group you are looking for.

**Step 5** Select the additional groups.

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

**Step 6** Click OK. Figure 42 shows a screenshot of our final group selection.

Figure 42 Final Group Selection




**Step 7** Scroll to the bottom of the page and click Save Configuration.

**Note:** Without saving the configuration, the additional groups will not be retrieved from Active Directory during authorization.

## Procedure 1 Create Additional dACLs 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.

**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
DACL Content =
   Deny ip any <ip_address_range_of_HR_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.

## Procedure 2 Create wACLs for Each Main Role

Repeat this procedure for each role that requires a different authorization. The wACL for an HR user is shown for reference.

**Best Practice:** For consistency, all wACLs should use the same name as the dACLs defined for wired access.

Table 3 Rules for HR wACL

| HR-ACL | | | | | | |
|---|---|---|---|---|---|---|
| Sequence | Source | Destination | Protocol | DSCP | Direction | Action |
| 1 | Any | IP address<br>10.1.100.87<br>255.255.255.255 | Any | Any | Any | Deny |
| 2 | Any | Any | Any | Any | Any | Permit |

## Procedure 3 Create Additional Authorization Profiles 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 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.
Access-Type = ACCESS_ACCEPT
-- Common Tasks
☑ DACL Name = HR-ACL
☑ Airespace ACL Name = HR-ACL
```

**Note:** The WLC field is used to apply a wACL that is locally defined on the WLC.

**Step 4** Click Submit.

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

## Procedure 4 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
Access-Type = ACCESS_ACCEPT
-- Common Tasks
☑  DACL Name = Employee-ACL
☑  Airespace ACL Name = Employee-ACL
```

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

**Step 5** Click Submit.

## Procedure 5 Adjust the Domain Computers Authorization

In Low-Impact Mode, we created a Domain Computers authorization profile, which permitted all traffic by using the PERMIT_ALL_TRAFFIC dACL.

**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
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 WLC.

**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**
☑ Airespace ACL Name= **AD-Machine-ACL**

## Procedure 6 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** For the permissions, choose Standard → HR-Profile.

**Step 7** Click Save.

**Step 8** Repeat the entire procedure for each distinct role type.

## Procedure 7 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 Table 4.

Table 4 Final Rule Table

| Status | Rule Name | | Identity Groups | | Other Conditions | | Permissions |
|---|---|---|---|---|---|---|---|
| ☑ | Blacklisted | if | Blacklisted | And | Condition(s) | then | DenyAccess |
| ☑ | Profiled Cisco IP Phones | if | Cisco-IP-Phone | And | Condition(s) | then | Cisco_IP_Phones |
| ☑ | Profiled Cisco APs | if | Cisco-Access-Point | And | Condition(s) | then | Access-Points |
| ☑ | Whitelist | if | Whitelist | And | Condition(s) | then | Whitelist |

| Status | Rule Name | | Identity Groups | | Other Conditions | | Permissions |
|---|---|---|---|---|---|---|---|
| ☑ | HR Rule | if | Any | And | AD1:ExternalGroups EQUALS HR | then | HR-Profile |
| ☑ | Engineering Rule | if | Any | And | AD1:ExternalGroups EQUALS Engineering | then | Engineering-Profile |
| ☑ | Sales Rule | if | Any | And | AD1:ExternalGroups EQUALS Sales | then | Sales-Profile |
| ☑ | Employee Rule | if | Any | And | AD1:ExternalGroups EQUALS Employees | then | Employee-Profile |
| ☑ | Contractor Rule | if | Any | And | AD1:ExternalGroups EQUALS Contractors | then | Contractor-Profile |
| ☑ | Machine Auth | if | Any | And | AD1:ExternalGroups EQUALS Domain Computers | then | AD_Machine_Access |
| ☑ | Domain User | if | Any | And | AD1:ExternalGroups EQUALS Domain Users | then | Domain_Users |
| ☑ | GUEST | if | GUEST | And | Condition(s) | then | GUEST |
| ☑ | Default | if no matches, then | | | WEBAUTH | | |

## Procedure 8 Consider Moving to Multi-Domain Authentication (MDA) Mode

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 cubicle or with other situational anomalies.

For design scenarios that require specific types of access, Multi-Domain Authentication (MDA) 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.

# 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