



SECURITY

# Cisco ISE for BYOD and Secure Unified Access

Second Edition

ciscopress.com

Aaron T. Woland, CCIE® No. 20113  
Jamey Heary, CCIE® No. 7680

## About This E-Book

EPUB is an open, industry-standard format for e-books. However, support for EPUB and its many features varies across reading devices and applications. Use your device or app settings to customize the presentation to your liking. Settings that you can customize often include font, font size, single or double column, landscape or portrait mode, and figures that you can click or tap to enlarge. For additional information about the settings and features on your reading device or app, visit the device manufacturer's Web site.

Many titles include programming code or configuration examples. To optimize the presentation of these elements, view the e-book in single-column, landscape mode and adjust the font size to the smallest setting. In addition to presenting code and configurations in the reflowable text format, we have included images of the code that mimic the presentation found in the print book; therefore, where the reflowable format may compromise the presentation of the code listing, you will see a "Click here to view code image" link. Click the link to view the print-fidelity code image. To return to the previous page viewed, click the Back button on your device or app.

# **Cisco ISE for BYOD and Secure Unified Access**

**Second Edition**

Aaron T. Woland, CCIE No. 20113

Jamey Heary, CCIE No. 7680

**Cisco Press**

800 East 96th Street

Indianapolis, Indiana 46240 USA

# **Cisco ISE for BYOD and Secure Unified Access Second Edition**

Aaron T. Woland

Jamey Heary

Copyright© 2017 Cisco Systems, Inc.

Published by: Cisco Press 800 East 96th Street Indianapolis, IN 46240 USA

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotations in a review.

Printed in the United States of America

First Printing June 2017

Library of Congress Control Number: 2017938614

ISBN-13: 978-1-58714-473-8

ISBN-10: 1-58714-473-5

## **Warning and Disclaimer**

This book is designed to provide information about Cisco Identity Services Engine, Cisco TrustSec, and Secure Network Access. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

## **Trademark Acknowledgments**

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as

affecting the validity of any trademark or service mark.

## **Special Sales**

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at [corpsales@pearsoned.com](mailto:corpsales@pearsoned.com) or (800) 382-3419.

For government sales inquiries, please contact [governmentsales@pearsoned.com](mailto:governmentsales@pearsoned.com).

For questions about sales outside the U.S., please contact [intlcs@pearson.com](mailto:intlcs@pearson.com).

## **Feedback Information**

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at [feedback@ciscopress.com](mailto:feedback@ciscopress.com). Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

**Editor-in-Chief:** Mark Taub

**Alliances Manager, Cisco Press:** Ron Fligge

**Executive Editor:** Mary Beth Ray

**Managing Editor:** Sandra Schroeder

**Development Editor:** Christopher Cleveland

**Senior Project Editor:** Tonya Simpson

**Copy Editor:** Bill McManus

**Technical Editor:** Pete Karelis

**Editorial Assistant:** Vanessa Evans

**Cover Designer:** Chuti Prasertsith

**Composition:** codeMantra

**Indexer:** Erika Millen

**Proofreader:** Sasirekha Durairajan



**Americas Headquarters**

Cisco Systems. Inc.

San Jose, CA

**Asia Pacific Headquarters**

Cisco Systems (USA) Pte. Ltd.

Singapore

**Europe Headquarters**

Cisco Systems International BV Amsterdam,

The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

# About the Authors

**Aaron Woland**, CCIE No. 20113, is a Principal Engineer in Cisco's Security Group and works with Cisco's largest customers all over the world. His primary job responsibilities include Secure Access and Identity deployments with ISE, solution enhancements, standards development, Advanced Threat Security and solution futures. Aaron joined Cisco in 2005 and is currently a member of numerous security advisory boards and standards body working groups. Prior to joining Cisco, Aaron spent 12 years as a consultant and technical trainer. His areas of expertise include network and host security architecture and implementation, regulatory compliance, and route-switch and wireless.

Aaron is the author of many Cisco white papers and design guides and is co-author of CCNP Security SISAS 300-208 Official Cert Guide; Cisco Next-Generation Security Solutions: All-in-one Cisco ASA Firepower Services, NGIPS, and AMP; and CCNA Security 210-260 Complete Video Course.

Aaron is one of only five inaugural members of the Hall of Fame Elite for Distinguished Speakers at Cisco Live, and is a security columnist for Network World, where he blogs on all things related to secure network access. His other certifications include GHIC, GSEC, Certified Ethical Hacker, MCSE, VCP, CCSP, CCNP, CCDP, and many other industry certifications. You can follow Aaron on Twitter: @aaronwoland.

**Jamey Heary, CCIE No. 7680**, is a Distinguished Systems Engineer at Cisco Systems, where he leads the Global Security Architecture Team, GSAT. Jamey and his GSAT team work as trusted security advisors and architects to Cisco's largest customers worldwide. Jamey sits on the PCI Security Standards Council's Board of Advisors, where he provides strategic and technical guidance for future PCI standards. Jamey is the author of Cisco NAC Appliance: Enforcing Host Security with Clean Access. He also has a patent on a new DDoS mitigation and firewall IP reputation technique. Jamey blogged for many years on Network World on security topics and is a Cisco Live Distinguished Speaker. Jamey sits on numerous security advisory boards for Cisco Systems and was a founding member of several Cisco security customer user groups across the United States. His other certifications include CISSP, and he is a Certified HIPAA Security Professional. He has been working in the IT field for 24 years and in IT security for 20 years. You can contact Jamey at [jheary@appledreams.com](mailto:jheary@appledreams.com).

## About the Technical Reviewer

**Epaminondas “Pete” Karelis**, CCIE Emeritus #8068, is the director of enterprise architecture for Venable LLP, an AmLaw 100 law firm, and has been in IT for more than 20 years. He views himself as a technologist, and has a strong focus on the integration of systems, storage, security, virtualization, and networking. In addition to the Cisco certifications (CCNA, CCDA, CCNP, CCIE R&S) he has held Microsoft (MCSE, MCT) and Checkpoint (CCSE) certifications. Coupled with his strong scripting, programming, and API integration skills, as well as his storage and virtualization experience, he is uniquely enabled to create tightly integrated solutions that incorporate the network with the application and server infrastructure. The ISE Anycast solution mentioned in this book is one of his examples of integrating network awareness with application and service delivery to allow for high availability without the use of load balancers. In his spare time, Pete enjoys spending time with his wife and two beautiful children, as well as reading tech blogs and keeping up to date on future technologies and open-source developments.

## Dedications

**From Aaron:** First and foremost, this book is dedicated to my amazing best friend, fellow adventurer, and wife, Suzanne. This book would surely not exist without your continued support, encouragement, and patience, as well as the sheer number of nights you took care of our newborn twins so I could write. Thank you for putting up with all the long nights and weekends I had to be writing. You are beyond amazing.

To Mom and Pop: You have always believed in me and supported me in absolutely everything I've ever pursued; showed pride in my accomplishments, no matter how small; encouraged me to never stop learning; engrained in me the value of hard work; and inspired me to strive for a career in a field that I love. I hope I can continue to fill your lives with pride and happiness, and if I succeed it will still only be a fraction of what you deserve.

To my four incredible daughters, Eden, Nyah, Netanya, and Cassandra: You girls are my inspiration, my pride and joy, and continue to make me want to be a better man. Eden, when I look at you and your accomplishments over your 18 years of life, I swell with pride. You are so intelligent, kind, and hard working. You will make a brilliant engineer one day, or if you change your mind, I know you will be brilliant in whatever career you find yourself pursuing (perhaps a dolphin trainer). Nyah, you are my morning star, my princess. You have the biggest heart, the kindest soul, and a brilliant mind. You excel at everything you put your mind to, and I look forward to watching you grow and use that power to change the world. Maybe you will follow in my footsteps. I can't wait to see it for myself. Natty and Cassie: You are only 12 weeks old as I write this, yet you have already filled my life with so much joy that I cannot describe it! It is bewildering and addicting to watch you every day and see your growth, wondering what you will be like as you grow up in this limitless world.

To my brother, Dr. Bradley Woland: Thank you for being so ambitious, so driven. It forced my competitive nature to always want more. As I stated when I rambled on in the 12-minute wedding speech, you do not only succeed at everything you try, you crush it! If you were a bum, I would never have pushed myself to the levels that I have. To his beautiful wife, Claire: I am so happy that you are a member of my family now; your kindness, intelligence, and wit certainly keep my brother in check and keep us all smiling.

To my sister, Anna: If I hadn't always had to compete with you for our parents' attention and to keep my things during our "garage sales," I would probably have grown up very naive and vulnerable. You drove me to think outside the box and find new ways to accomplish the things I wanted to do. Seeing you succeed in life and in school truly had a profound effect on my life. Thank you for marrying Eddie, my brilliant brother-in-law. Eddie convinced me that I could actually have a career in this technology stuff, and

without his influence, I would probably be in law enforcement or under the hood of car. To my grandparents, Jack, Lola, Herb, and Ida: You have taught me what it means to be alive and the true definition of courage, survival, perseverance, hard work, and never giving up.

Monty Shafer: the world lost a great man this year, and I lost a brother. You started out as my student, but you've taught me so much in this world. I know that you're up there, watching over Kiersten, Haley, and Devin and all of us whom you loved.

Finally, to Sash Altus, who is undoubtedly rockin' out in heaven with Monty and Dan while my grandparents are complaining about the noise.

**From Jamey:** This book is dedicated to my beautiful, supportive, and amazing wife, Becca, and our two incredible sons, Liam and Conor, without whose support and sacrifice this book would not have been possible. Becca, you continue to amaze me with your ability to motivate me in life and support my endeavors even when they make life harder for you. Thanks for putting up with the late nights and weekends I had to spend behind the keyboard instead of playing games, Legos, football, or some other fun family activity. You are all the greatest, and I couldn't have done this without you!

Thanks to my parents for their sacrifices and providing me with every opportunity to succeed in life as I was growing up. Dad, you got me my first job in technology that kicked off this whole rewarding career. Know that I cherish greatly the continuous love and support you've both provided throughout my life.

# Acknowledgments

## From Aaron:

There are so many people to acknowledge. This feels like a speech at the Academy Awards, and I'm afraid I will leave out too many people.

Thomas Howard and Allan Bolding, for their continued support, encouragement, and guidance. Most importantly, for believing in me even though I can be difficult at times. I could not have done any of it without you.

Craig Hyps, Principal Technical Marketing Engineer at Cisco: You are a machine. You possess such deep technical knowledge on absolutely everything (not just pop culture). Your constant references to pop culture keep me laughing, and your influence can be found on content all throughout the book and this industry. “Can you dig it?”

Christopher Heffner, Security Architect at Cisco and my “brother from another mother,” for convincing me to step up and take a swing at being an author, and for twisting my arm to put “pen to paper” again.

Jonny Rabinowitz and Christopher Murray: You guys continue to set an incredibly high bar, and somehow move that bar higher all the time. You have a fight in you to never lose, never give up, and always do the right thing, and that fight is completely infectious. Your constant enthusiasm, energy, brilliance, and expertise have impressed me and inspired me.

I am honored to work with so many brilliant and talented people every day. Among them: Jesse Dubois, Vivek Santuka, Doug Gash, Chad Mitchell, Jamie Sanbower, Moses Hernandez, Andrew Benhase, Avinash Kumar, Victor Ashe, Jeff Fanelli, Louis Roggo, Kyle King, Tim Snow, Andrew Ossipov, Mike Storm, Jason Frazier, Amit Tropper, and Shai Michelson. You guys truly amaze me, seriously.

To ISE’s world-class TME team: Hosuk Won, Tim Abbott, Hsing-Tsu Lai, Imran Bashir, Hari Holla, Ziad Sarieddine, John Eppich, Fay-Ann Lee, Jason Kunst, Krishnan Thiruvengadam, and Paul Carco. World-class is not a strong enough adjective to describe this team. You are beyond inspirational, and I am proud to be a member of this team.

Darrin Miller, Nancy Cam-Winget, and Jamey Heary, Distinguished Engineers who set the bar so incredibly high. You are truly inspirational; people to look up to and aspire to be like, and I appreciate all the guidance you have given me.

Max Pritkin, I think you have forgotten more about certificates and PKI than most experts will ever know (if you ever forgot anything, that is). You have taught me so much, and I look forward to learning more from your vast knowledge and unique way of making complex technology seem easy.

To the world’s greatest Engineering Team, and of course I mean the people who spend

their days writing and testing the code that makes up Cisco ISE. You guys continue to show the world what it means to be “world-class.”

To our technical editor, Epaminondas (Pete) Karelis: Thank you for agreeing to take this project on, and for making us look so good! You are a wealth of knowledge, and you did an amazing job catching all of my blunders in this book. I value your leadership almost as much as your friendship.

John Herbert, from movingpackets.net, I learned so much from you in such a short time span. Your brilliance is only superseded by your wit! I hope to be listening to recordings of you harassing the “Your computer has been hacked and we need to protect it” scammers for many years to come.

My colleagues: Naasief Edross, Russell Rice, Dalton Hamilton, Tom Foucha, Matt Robertson, Randy Rivera, Brian Ford, Paul Russell, Brendan O’Connell, Jeremy Hyman, Kevin Sullivan, Mason Harris, David Anderson, Luc Billot, Dave White Jr., Nevin Absher, Ned Zaldivar, Mark Kassem, Greg Tillett, Chuck Parker, Shelly Cadora, Ralph Schmieder, Corey Elinburg, Scott Kenewell, Larry Boggis, Chad Sullivan, Dave Klein, Nelson Figueroa, Kevin Redmon, Konrad Reszka, Steven Grimes, Jay Cedrone, Peter Marchand, Eric Howard, Marty Roesch, and so many more! The contributions you make to this industry inspire me every day.

Last, but not least: to all those at Cisco Press, especially Mary Beth Ray and Chris Cleveland. I thank you and your team of editors for making Jamey and me look so good. Apparently, it takes an army of folks to do so. I’m sorry for all the times you had to correct our grammar.

### **From Jamey:**

The cool thing about going second in the acknowledgements section is I can just say, I echo Aaron’s sentiments! So many people have made it possible for this book to exist, and for that matter, for the most excellent ISE solution to exist to write about in the first place. “Great job!” to the policy and access business unit; your tireless efforts are bearing fruit. Thank you.

Thank you to Aaron Woland, for pushing the idea of our writing this second edition of the book and making it real. Your technical kung fu is impressive, as is your ability to put pen to paper so others can understand and follow along. It was yet another fun ride!

Thank you to our most awesome tech editor, Pete Karelis. Your attention to detail helped make this book great! Special thanks to Chris Cleveland and Mary Beth Ray and the whole Cisco Press team. As Aaron stated, your contributions and tireless efforts are supremely appreciated. Thanks for this opportunity.

I know I must have forgotten some people; so many have helped me along this journey. Thank you!



# **Contents at a Glance**

## Introduction

## **Part I Identity-Enabled Network: Unite!**

Chapter 1 Regain Control of Your IT Security

Chapter 2 Fundamentals of AAA

Chapter 3 Introducing Cisco Identity Services Engine

## **Part II The Blueprint, Designing an ISE-Enabled Network**

Chapter 4 The Building Blocks in an Identity Services Engine Design

Chapter 5 Making Sense of the ISE Deployment Design Options

Chapter 6 Quick Setup of an ISE Proof of Concept

## **Part III The Foundation, Building a Context-Aware Security Policy**

Chapter 7 Building a Cisco ISE Network Access Security Policy

Chapter 8 Building a Device Security Policy

Chapter 9 Building an ISE Accounting and Auditing Policy

## **Part IV Let's Configure!**

Chapter 10 Profiling Basics and Visibility

Chapter 11 Bootstrapping Network Access Devices

Chapter 12 Network Authorization Policy Elements

Chapter 13 Authentication and Authorization Policies

Chapter 14 Guest Lifecycle Management

Chapter 15 Client Posture Assessment

Chapter 16 Supplicant Configuration

Chapter 17 BYOD: Self-Service Onboarding and Registration

Chapter 18 Setting Up and Maintaining a Distributed ISE Deployment

Chapter 19 Remote Access VPN and Cisco ISE

Chapter 20 Deployment Phases

## **Part V Advanced Secure Access Features**

[Chapter 21 Advanced Profiling Configuration](#)

[Chapter 22 Cisco TrustSec AKA Security Group Access](#)

[Chapter 23 Passive Identities, ISE-PIC, and EasyConnect](#)

[Chapter 24 ISE Ecosystems: The Platform eXchange Grid \(pxGrid\)](#)

## **Part VI Monitoring, Maintenance, and Troubleshooting for Network Access AAA**

[Chapter 25 Understanding Monitoring, Reporting, and Alerting](#)

[Chapter 26 Troubleshooting](#)

[Chapter 27 Upgrading ISE](#)

## **Part VII Device Administration**

[Chapter 28 Device Administration Fundamentals](#)

[Chapter 29 Configuring Device Admin AAA with Cisco IOS](#)

[Chapter 30 Configuring Device Admin AAA with Cisco WLC](#)

[Chapter 31 Configuring Device Admin AAA with Cisco Nexus Switches](#)

## **Part VIII Appendixes**

[Appendix A Sample User Community Deployment Messaging Material](#)

[Appendix B Sample ISE Deployment Questionnaire](#)

[Appendix C Sample Switch Configurations](#)

[Appendix D The ISE CA and How Cert-Based Auth Works](#)

[Index](#)

# **Contents**

## **Introduction**

### **Part I Identity-Enabled Network: Unite!**

#### **Chapter 1 Regain Control of Your IT Security**

Security: Still a Weakest-Link Problem

Cisco Identity Services Engine

Sources for Providing Identity and Context Awareness

Unleash the Power of Centralized Policy

Summary

#### **Chapter 2 Fundamentals of AAA**

Triple-A

Compare and Select AAA Options 10

Device Administration

Network Access

TACACS+

TACACS+ Authentication Messages

TACACS+ Authorization and Accounting Messages

RADIUS

AV Pairs

Change of Authorization

Comparing RADIUS and TACACS+

Summary

#### **Chapter 3 Introducing Cisco Identity Services Engine**

Architecture Approach to Centralized and Dynamic Network Security Policy Enforcement

Cisco Identity Services Engine Features and Benefits

ISE Platform Support and Compatibility

Cisco Identity Services Engine Policy Construct

ISE Authorization Rules

Summary

## Part II The Blueprint, Designing an ISE-Enabled Network

### Chapter 4 The Building Blocks in an Identity Services Engine Design

[ISE Solution Components Explained](#)

[Infrastructure Components](#)

[Policy Components](#)

[Endpoint Components](#)

[ISE Personas](#)

[ISE Licensing, Requirements, and Performance](#)

[ISE Licensing](#)

[ISE Requirements](#)

[ISE Performance](#)

[ISE Policy-Based Structure Explained](#)

[Summary](#)

### Chapter 5 Making Sense of the ISE Deployment Design Options

[Centralized Versus Distributed Deployment](#)

[Centralized Deployment](#)

[Distributed Deployment](#)

[Summary](#)

### Chapter 6 Quick Setup of an ISE Proof of Concept

[Deploy ISE for Wireless in 15 Minutes](#)

[Wireless Setup Wizard Configuration](#)

[Guest Self-Registration Wizard](#)

[Secure Access Wizard](#)

[Bring Your Own Device \(BYOD\) Wizard](#)

[Deploy ISE to Gain Visibility in 15 Minutes](#)

[Visibility Setup Wizard](#)

[Configuring Cisco Switches to Send ISE Profiling Data](#)

[Summary](#)

## Part III The Foundation, Building a Context-Aware Security Policy

### Chapter 7 Building a Cisco ISE Network Access Security Policy

[Components of a Cisco ISE Network Access Security Policy](#)

Network Access Security Policy Checklist

Involving the Right People in the Creation of the Network Access Security Policy

Determining the High-Level Goals for Network Access Security

Common High-Level Network Access Security Goals

Network Access Security Policy Decision Matrix

Defining the Security Domains

Understanding and Defining ISE Authorization Rules

Commonly Configured Rules and Their Purpose

Establishing Acceptable Use Policies

Host Security Posture Assessment Rules to Consider

Sample NASP Format for Documenting ISE Posture Requirements

Common Checks, Rules, and Requirements

Method for Adding Posture Policy Rules

Research and Information

Establishing Criteria to Determine the Validity of a Security Posture Check, Rule, or Requirement in Your Organization

Method for Determining What Posture Policy Rules a Particular Security Requirement Should Be Applied To

Method for Deploying and Enforcing Security Requirements

Defining Dynamic Network Access Privileges

Enforcement Methods Available with ISE

Commonly Used Network Access Policies

Summary

## **Chapter 8 Building a Device Security Policy**

ISE Device Profiling

ISE Profiling Policies

ISE Profiler Data Sources

Using Device Profiles in Authorization Rules

Threat-Centric NAC

Using TC-NAC as Part of Your Incident Response Process

Summary

## Chapter 9 Building an ISE Accounting and Auditing Policy

Why You Need Accounting and Auditing for ISE

Using PCI DSS as Your ISE Auditing Framework

ISE Policy for PCI 10.1: Ensuring Unique Usernames and Passwords

ISE Policy for PCI 10.2 and 10.3: Audit Log Collection

ISE Policy for PCI 10.5.3, 10.5.4, and 10.7: Ensure the Integrity and Confidentiality of Audit Log Data

ISE Policy for PCI 10.6: Review Audit Data Regularly

Cisco ISE User Accounting

Summary

## Part IV Let's Configure!

### Chapter 10 Profiling Basics and Visibility

Understanding Profiling Concepts

ISE Profiler Work Center

ISE Profiling Probes

Probe Configuration

DHCP and DHCPSPAN Probes

RADIUS Probe

Network Scan (NMAP) Probe

DNS Probe

SNMPQUERY and SNMPTRAP Probes

Active Directory Probe

HTTP Probe

HTTP Profiling Without Probes

NetFlow Probe

Infrastructure Configuration

DHCP Helper

SPAN Configuration

VLAN ACL Captures

Device Sensor

VMware Configurations to Allow Promiscuous Mode

Profiling Policies

[Profiler Feed Service](#)

[Configuring the Profiler Feed Service](#)

[Verifying the Profiler Feed Service](#)

[Offline Manual Update](#)

[Endpoint Profile Policies](#)

[Context Visibility](#)

[Logical Profiles](#)

[ISE Profiler and CoA](#)

[Global CoA](#)

[Per-Profile CoA](#)

[Global Profiler Settings](#)

[Configure SNMP Settings for Probes](#)

[Endpoint Attribute Filtering](#)

[NMAP Scan Subnet Exclusions](#)

[Profiles in Authorization Policies](#)

[Endpoint Identity Groups](#)

[EndPointPolicy](#)

[Importing Profiles](#)

[Verifying Profiling](#)

[The Dashboard](#)

[Endpoints Dashboard](#)

[Context Visibility](#)

[Device Sensor Show Commands](#)

[Triggered NetFlow: A Woland-Santuka Pro Tip](#)

[Summary](#)

## **Chapter 11 Bootstrapping Network Access Devices**

[Cisco Catalyst Switches](#)

[Global Configuration Settings for Classic IOS and IOS 15.x Switches](#)

[Configure Certificates on a Switch](#)

[Enable the Switch HTTP/HTTPS Server](#)

[Global AAA Commands](#)

[Global RADIUS Commands](#)

[Create Local Access Control Lists for Classic IOS and IOS 15.x](#)  
[Global 802.1X Commands](#)  
[Global Logging Commands \(Optional\)](#)  
[Global Profiling Commands](#)  
[Interface Configuration Settings for Classic IOS and IOS 15.x Switches](#)  
[Configure Interfaces as Switch Ports](#)  
[Configure Flexible Authentication and High Availability](#)  
[Configure Authentication Settings](#)  
[Configure Authentication Timers](#)  
[Apply the Initial ACL to the Port and Enable Authentication](#)  
[Configuration Settings for C3PL Switches](#)  
[Why Use C3PL?](#)  
[Global Configuration for C3PL](#)  
[Global RADIUS Commands for C3PL](#)  
[Configure Local ACLs and Local Service Templates](#)  
[Global 802.1X Commands](#)  
[C3PL Fundamentals](#)  
[Configure the C3PL Policies](#)  
[Cisco Wireless LAN Controllers](#)  
[AireOS Features and Version History](#)  
[Configure the AAA Servers](#)  
[Add the RADIUS Authentication Servers](#)  
[Add the RADIUS Accounting Servers](#)  
[Configure RADIUS Fallback \(High Availability\)](#)  
[Configure the Airespace ACLs](#)  
[Create the Web Authentication Redirection ACL](#)  
[Add Google URLs for ACL Bypass](#)  
[Create the Dynamic Interfaces for the Client VLANs](#)  
[Create the Employee Dynamic Interface](#)  
[Create the Guest Dynamic Interface](#)  
[Create the Wireless LANs](#)  
[Create the Guest WLAN](#)  
[Create the Corporate SSID](#)

[Summary](#)

## [Chapter 12 Network Authorization Policy Elements](#)

[ISE Authorization Policy Elements](#)

[Authorization Results](#)

[Configuring Authorization Downloadable ACLs](#)

[Configuring Authorization Profiles](#)

[Summary](#)

## [Chapter 13 Authentication and Authorization Policies](#)

[Relationship Between Authentication and Authorization](#)

[Enable Policy Sets](#)

[Authentication Policy Goals](#)

[Accept Only Allowed Protocols](#)

[Route to the Correct Identity Store](#)

[Validate the Identity](#)

[Pass the Request to the Authorization Policy](#)

[Understanding Authentication Policies](#)

[Conditions](#)

[Allowed Protocols](#)

[Authentication Protocol Primer](#)

[Identity Store](#)

[Options](#)

[Common Authentication Policy Examples](#)

[Using the Wireless SSID](#)

[Remote-Access VPN](#)

[Alternative ID Stores Based on EAP Type](#)

[Authorization Policies](#)

[Goals of Authorization Policies](#)

[Understanding Authorization Policies](#)

[Role-Specific Authorization Rules](#)

[Authorization Policy Example](#)

[Employee and Corporate Machine Full-Access Rule](#)

[Internet Only for Mobile Devices](#)

[Employee Limited Access Rule](#)  
[Saving Attributes for Reuse](#)  
[Summary](#)

## **Chapter 14 Guest Lifecycle Management**

[Overview of ISE Guest Services](#)  
[Hotspot Guest Portal Configuration](#)  
[Sponsored Guest Portal Configuration](#)  
[Create an Active Directory Identity Store](#)  
[Create ISE Guest Types](#)  
[Create Guest Sponsor Groups](#)  
[Authentication and Authorization Guest Policies](#)  
[Guest Pre-Authentication Authorization Policy](#)  
[Guest Post-Authentication Authorization Policy](#)  
[Guest Sponsor Portal Configuration](#)  
[Guest Portal Interface and IP Configuration](#)  
[Sponsor and Guest Portal Customization](#)  
[Sponsor Portal Behavior and Flow Settings](#)  
[Sponsor Portal Page Customization](#)  
[Guest Portal Behavior and Flow Settings](#)  
[Guest Portal Page Customization](#)  
[Creating Multiple Guest Portals](#)  
[Guest Sponsor Portal Usage](#)  
[Sponsor Portal Layout](#)  
[Creating Guest Accounts](#)  
[Managing Guest Accounts](#)  
[Configuration of Network Devices for Guest CWA](#)  
[Wired Switches](#)  
[Wireless LAN Controllers](#)  
[Summary](#)

## **Chapter 15 Client Posture Assessment**

[ISE Posture Assessment Flow](#)  
[Configure Global Posture and Client Provisioning Settings](#)

[Posture Client Provisioning Global Setup](#)

[Posture Global Setup](#)

[Posture General Settings](#)

[Posture Reassessments](#)

[Posture Updates](#)

[Acceptable Use Policy Enforcement](#)

[Configure the AnyConnect and NAC Client Provisioning Rules](#)

[AnyConnect Agent with ISE Compliance Module](#)

[AnyConnect Posture Profile Creation](#)

[AnyConnect Configuration File Creation](#)

[AnyConnect Client Provisioning Policy](#)

[Configure the Client Provisioning Portal](#)

[Configure Posture Elements](#)

[Configure Posture Conditions](#)

[Configure Posture Remediations](#)

[Configure Posture Requirements](#)

[Configure Posture Policy](#)

[Configure Host Application Visibility and Context Collection \(Optional\)](#)

[Enable Posture Client Provisioning and Assessment in Your ISE Authorization Policies](#)

[Posture Client Provisioning](#)

[Authorization Based On Posture Compliance](#)

[Posture Reports and Troubleshooting](#)

[Enable Posture Assessment in the Network](#)

[Summary](#)

## **Chapter 16 Suplicant Configuration**

[Comparison of Popular Suplicants](#)

[Configuring Common Suplicants](#)

[Mac OS X 10.8.2 Native Suplicant Configuration](#)

[Windows GPO Configuration for Wired Suplicant](#)

[Windows 7, 8/8.1, and 10 Native Suplicant Configuration](#)

[Cisco AnyConnect Secure Mobility Client NAM](#)

[Summary](#)

## [Chapter 17 BYOD: Self-Service Onboarding and Registration](#)

[BYOD Challenges](#)

[Onboarding Process](#)

[BYOD Onboarding](#)

[Dual SSID](#)

[Single SSID](#)

[Configuring NADs for Onboarding](#)

[ISE Configuration for Onboarding](#)

[End-User Experience](#)

[Configuring ISE for Onboarding](#)

[BYOD Onboarding Process Detailed](#)

[MDM Onboarding](#)

[Integration Points](#)

[Configuring MDM Integration](#)

[Configuring MDM Onboarding Policies](#)

[The Opposite of BYOD: Identify Corporate Systems](#)

[EAP Chaining](#)

[Summary](#)

## [Chapter 18 Setting Up and Maintaining a Distributed ISE Deployment](#)

[Configuring ISE Nodes in a Distributed Environment](#)

[Make the Policy Administration Node a Primary Device](#)

[Register an ISE Node to the Deployment](#)

[Ensure the Persona of All Nodes Is Accurate](#)

[Understanding the HA Options Available](#)

[Primary and Secondary Nodes](#)

[Monitoring & Troubleshooting Nodes](#)

[Policy Administration Nodes](#)

[Policy Service Nodes and Node Groups](#)

[Create a Node Group](#)

[Add the Policy Service Nodes to the Node Group](#)

[Using Load Balancers](#)

[General Guidelines](#)  
[Failure Scenarios](#)  
[Anycast HA for ISE PSNs](#)  
[Cisco IOS Load Balancing](#)  
[Maintaining ISE Deployments](#)  
[Patching ISE](#)  
[Backup and Restore](#)  
[Summary](#)

## **[Chapter 19 Remote Access VPN and Cisco ISE](#)**

[Introduction to VPNs](#)  
[Client-Based Remote Access VPN](#)  
[Configuring a Client-Based RA-VPN on the Cisco ASA](#)  
[Download the Latest AnyConnect Headend Packages](#)  
[Prepare the Headend](#)  
[Add an AnyConnect Connection Profile](#)  
[Add the ISE PSNs to the AAA Server Group](#)  
[Add a Client Address Pool](#)  
[Perform Network Reachability Tasks](#)  
[Configure ISE for the ASA VPN](#)  
[Testing the Configuration](#)  
[Perform a Basic AAA Test](#)  
[Log In to the ASA Web Portal](#)  
[Connect to the VPN via AnyConnect](#)  
[Remote Access VPN and Posture](#)  
[RA-VPN with Posture Flows](#)  
[Adding the Access Control Lists to ISE and the ASA](#)  
[Adding Posture Policies to the VPN Policy Set](#)  
[Watching It Work](#)  
[Extending the ASA Remote Access VPN Capabilities](#)  
[Double Authentication](#)  
[Certificate-Based Authentication](#)  
[Provisioning Certificates](#)

[Authenticating the VPN with Certificates](#)

[Connecting to the VPN via CertProfile](#)

[Summary](#)

## [Chapter 20 Deployment Phases](#)

[Why Use a Phased Approach?](#)

[A Phased Approach](#)

[Authentication Open Versus Standard 802.1X](#)

[Monitor Mode](#)

[Prepare ISE for a Staged Deployment](#)

[Create the Network Device Groups](#)

[Create the Policy Sets](#)

[Low-Impact Mode](#)

[Closed Mode](#)

[Transitioning from Monitor Mode to Your End State](#)

[Wireless Networks](#)

[Summary](#)

## [Part V Advanced Secure Access Features](#)

### [Chapter 21 Advanced Profiling Configuration](#)

[Profiler Work Center](#)

[Creating Custom Profiles for Unknown Endpoints](#)

[Identifying Unique Values for an Unknown Device](#)

[Collecting Information for Custom Profiles](#)

[Creating Custom Profiler Conditions](#)

[Creating Custom Profiler Policies](#)

[Advanced NetFlow Probe Configuration](#)

[Commonly Used NetFlow Attributes](#)

[Example Profiler Policy Using NetFlow](#)

[Designing for Efficient Collection of NetFlow Data](#)

[Configuration of NetFlow on Cisco Devices](#)

[Profiler CoA and Exceptions](#)

[Types of CoA](#)

[Creating Exceptions Actions](#)

[Configuring CoA and Exceptions in Profiler Policies](#)

[Profiler Monitoring and Reporting](#)

[Summary](#)

## [Chapter 22 Cisco TrustSec AKA Security Group Access](#)

[Ingress Access Control Challenges](#)

[VLAN Assignment](#)

[Ingress Access Control Lists](#)

[What Is TrustSec?](#)

[So, What Is a Security Group Tag?](#)

[Defining the SGTs](#)

[Classification](#)

[Dynamically Assigning an SGT via 802.1X](#)

[Manually Assigning an SGT at the Port](#)

[Manually Binding IP Addresses to SGTs](#)

[Access Layer Devices That Do Not Support SGTs](#)

[Transport: SGT eXchange Protocol \(SXP\)](#)

[SXP Design](#)

[Configuring SXP on IOS Devices](#)

[Configuring SXP on Wireless LAN Controllers](#)

[Configuring SXP on Cisco ASA](#)

[Configuring SXP on ISE](#)

[Transport: pxGrid](#)

[Transport: Native Tagging](#)

[Configuring Native SGT Propagation \(Tagging\)](#)

[Configuring SGT Propagation on Cisco IOS Switches](#)

[Configuring SGT Propagation on a Catalyst 6500](#)

[Configuring SGT Propagation on a Nexus Series Switch](#)

[Enforcement](#)

[Traffic Enforcement with SGACLs](#)

[Creating TrustSec Matrices in ISE](#)

[Traffic Enforcement with Security Group Firewalls](#)

[Security Group Firewall on the ASA](#)

## Security Group Firewall on the ISR and ASR Summary

### **Chapter 23 Passive Identities, ISE-PIC, and EasyConnect**

Passive Authentication

Identity Sharing

Tenet 1: Learn

Active Directory

Syslog Sources

REST API Sources

Learning More Is Critical

Tenet 2: Share

pxGrid

CDA-RADIUS

Tenet 3: Use

Integration Details

Integration Summary

Tenet 4: Update

Logoff Detection with the Endpoint Probe

WMI Update Events

Session Timeouts

ISE Passive Identity Connector

EasyConnect

Summary

### **Chapter 24 ISE Ecosystems: The Platform eXchange Grid (pxGrid)**

The Many Integration Types of the Ecosystem

MDM Integration

Rapid Threat Containment

Platform Exchange Grid

pxGrid in Action

Configuring ISE for pxGrid

Configuring pxGrid Participants

Configuring Firepower Management Center for pxGrid

[Configuring the Web Security Appliance for pxGrid](#)

[Configuring Stealthwatch for pxGrid](#)

[Summary](#)

## [Part VI Monitoring, Maintenance, and Troubleshooting for Network Access AAA](#)

### [Chapter 25 Understanding Monitoring, Reporting, and Alerting](#)

[ISE Monitoring](#)

[Cisco ISE Home Page](#)

[Context Visibility Views](#)

[RADIUS Live Logs and Live Sessions](#)

[Global Search](#)

[Monitoring Node in a Distributed Deployment](#)

[Device Configuration for Monitoring](#)

[ISE Reporting](#)

[Data Repository Setup](#)

[ISE Alarms](#)

[Summary](#)

### [Chapter 26 Troubleshooting](#)

[Diagnostic Tools](#)

[RADIUS Authentication Troubleshooting](#)

[Evaluate Configuration Validator](#)

[TCP Dump](#)

[Endpoint Debug](#)

[Session Trace](#)

[Troubleshooting Methodology](#)

[Troubleshooting Authentication and Authorization](#)

[Log Deduplication](#)

[Active Troubleshooting](#)

[Option 1: No Live Logs Entry Exists](#)

[Option 2: An Entry Exists in the Live Logs](#)

[General High-Level Troubleshooting Flowchart](#)

[Troubleshooting WebAuth and URL Redirection](#)

[Debug Situations: ISE Logs](#)

## The Support Bundle

### Summary

## Chapter 27 Upgrading ISE

The Upgrade Process

Repositories

Configuring a Repository

Repository Types and Configuration

Performing the Upgrade

Command-Line Upgrade

Summary

## Part VII Device Administration

### Chapter 28 Device Administration Fundamentals

Device Administration in ISE

Large Deployments

Medium Deployments

Small Deployments

Enabling TACACS+ in ISE

Network Devices

Device Administration Global Settings

Connection Settings

Password Change Control

Session Key Assignment

Device Administration Work Center

Overview

Identities

Network Resources

Policy Elements

Device Admin Policy Sets

Reports

Summary

### Chapter 29 Configuring Device Admin AAA with Cisco IOS

## Preparing ISE for Incoming AAA Requests

Preparing the Policy Results

Create the Authorization Results for Network Administrators

Create the Authorization Results for Network Operators

Create the Authorization Results for Security Administrators

Create the Authorization Results for the Helpdesk

Preparing the Policy Set

Configuring the Network Access Device

Time to Test

Summary

## **Chapter 30 Configuring Device Admin AAA with Cisco WLC**

Overview of WLC Device Admin AAA

Configuring ISE and the WLC for Device Admin AAA

Preparing ISE for WLC Device Admin AAA

Prepare the Network Device

Prepare the Policy Results

Configure the Policy Set

Adding ISE to the WLC TACACS+ Servers

Testing and Troubleshooting

Summary

## **Chapter 31 Configuring Device Admin AAA with Cisco Nexus Switches**

Overview of NX-OS Device Admin AAA

Configuring ISE and the Nexus for Device Admin AAA

Preparing ISE for Nexus Device Admin AAA

Prepare the Network Device

Prepare the Policy Results

Configure the Policy Set

Preparing the Nexus Switch for TACACS+ with ISE

Enable TACACS+ and Add ISE to NX-OS

Summary

## **Part VIII Appendixes**

## Appendix A Sample User Community Deployment Messaging Material

- [Sample Identity Services Engine Requirement Change Notification Email](#)
- [Sample Identity Services Engine Notice for a Bulletin Board or Poster](#)
- [Sample Identity Services Engine Letter to Students](#)

## Appendix B Sample ISE Deployment Questionnaire

### Appendix C Sample Switch Configurations

- [Catalyst 3000 Series, 12.2\(55\)SE](#)
- [Catalyst 3000 Series, 15.0\(2\)SE](#)
- [Catalyst 4500 Series, IOS-XE 3.3.0 / 15.1\(1\)SG](#)
- [Catalyst 6500 Series, 12.2\(33\)SXJ](#)

## Appendix D The ISE CA and How Cert-Based Auth Works

### Certificate-Based Authentication

- [Has the Digital Certificate Been Signed by a Trusted CA?](#)
- [Has the Certificate Expired?](#)
- [Has the Certificate Been Revoked?](#)
- [Has the Client Provided Proof of Possession?](#)
- [So, What Does Any of This Have to Do with Active Directory?](#)

### ISE's Internal Certificate Authority

- [Why Put a CA into ISE?](#)
- [ISE CA PKI Hierarchy](#)
- [The Endpoint CA](#)
- [Reissuing CA Certificates](#)
- [Configuring ISE to be a Subordinate CA to an Existing PKI](#)
- [Backing Up the Certificates](#)
- [Issuing Certificates from the ISE CA](#)

## Index

# Reader Services

Register your copy at [www.ciscopress.com/title/9781587144738](http://www.ciscopress.com/title/9781587144738) for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to [www.ciscopress.com/register](http://www.ciscopress.com/register) and log in or create an account\*. Enter the product ISBN 9781587144738 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

\*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

## Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- Italic indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

# Introduction

Today's networks have evolved into a system without well-defined borders/perimeters that contain data access from both trusted and untrusted devices. Cisco broadly calls this trend borderless networking. The Cisco Secure Access architecture and Cisco Identity Services Engine (ISE) were developed to provide organizations with a solution to secure and regain control of borderless networks in a Bring Your Own Device (BYOD) world.

A few basic truths become apparent when trying to secure a borderless network. First, you can no longer trust internal data traffic. There are just too many ingress points into the network and too many untrusted devices/users inside the network to be able to trust it implicitly. Second, given the lack of internal trust, it becomes necessary to authenticate and authorize all users into the network regardless of their connection type: wired, wireless, or VPN. Third, because of the proliferation of untrusted and unmanaged devices connecting to your internal network, device control and posture assessment become critical. Each device must be checked for security compliance before it is allowed access to your network resources. These checks vary according to your security policy, but usually involve checking the device type, location, management status, and operating-system patch level, and ensuring that antimalware software is running and up to date.

This book addresses the complete lifecycle of protecting a modern borderless network using Cisco Secure Access and ISE solutions. Secure access and ISE design, implementation, and troubleshooting are covered in depth. This book explains the many details of the solution and how it can be used to secure borderless networks. At its heart, this solution allows organizations to identify and apply network security policies based on user identity, device type, device behavior, and other attributes, such as security posture. Technologies such as 802.1X, profiling, guest access, network admission control, RADIUS, device administration, TACACS+, and TrustSec are covered in depth.

The goal is to boil down and simplify the architectural details and present them in one reference without trying to replace the existing design, installation, and configuration guides already available from Cisco.

## Who Should Read This Book?

This book is targeted primarily to a technical audience involved in architecting, deploying, and delivering secure networks and enabling mobile services. It can help them make informed choices, and enable them to have an engaging discussion with their organization, on how they can achieve their security and availability goals, while reaping the benefits of a secure access solution.

This book is helpful to those looking to deploy Cisco ISE to secure your wired, wireless, and VPN access. It is also useful for those moving to a BYOD IT model.

## How This Book Is Organized

This book is organized into 31 chapters distributed across 7 different parts, each based on a main theme. As a bonus, four appendixes are included as Part VIII to provide added value to readers. Although this book can be read cover to cover, readers can move between chapters and parts, covering only the content that interests them. The seven parts of the book are described first:

**Part I, “[Identity-Enabled Network: Unite!](#)”**: Examines the evolution of identity-enabled networks. It provides an overview of security issues facing today’s networks and what has been the history of trying to combat this problem. This part covers a foundation-building review of AAA, 802.1X, the NAC framework, NAC appliance, the evolution into Secure Access, and the creation of Cisco ISE. It discusses the issues faced with the consumerization of information technology, the mass influx of personal devices, ensuring only the correct users, correct devices, with the correct software are allowed to access the corporate network unfettered.

**Part II, “[The Blueprint, Designing an ISE-Enabled Network](#)”**: Covers the high-level design phase of a secure network access project. Solution diagrams are included. This part covers the different ISE functions available, how to distribute these functions, and the solution taxonomy. It discusses the enforcement devices that are part of this solution and ones that are not. Change of Authorization (CoA) is introduced. All these concepts are clarified and reinforced throughout the other parts.

**Part III, “[The Foundation, Building a Context-Aware Security Policy](#)”**: Describes how to create a context-aware security policy for the network and devices. This is often the hardest part of a secure network access project. This part covers the departments that need to be involved, the policies to be considered, and best practices. Coverage includes some lessons learned and landmines to watch out for. Screenshots and flow diagrams are included in this part to aid in the readers’ understanding of the process, how communication occurs and in what order, and how to configure the miscellaneous device supplicants.

**Part IV, “[Let’s Configure!](#)”**: Details the step-by-step configuration of ISE, the network access devices (NAD), and supplicants. The goal of this part is to have the entire infrastructure and policy management configured and ready to begin the actual deployment. Technology and complex topics are explained along with the configuration steps, aiding in the understanding of the configuration steps by tying them together with the technological explanation.

**Part V, “[Advanced Secure Access Features](#)”**: Dives into some of the more advanced

solution features that truly differentiate the ISE secure access system. This part covers advanced configurations of the ISE profiling engine, Cisco TrustSec, high availability, backups, passive identity capabilities, EasyConnect, and context sharing with the Platform eXchange Grid (pxGrid).

## **Part VI, “Monitoring, Maintenance, and Troubleshooting for Network Access**

**AAA**”: Examines the maintenance of ISE, backups, and upgrades. It covers how to troubleshoot not only ISE, but the entire secure access system, and how to use the tools provided in the ISE product. Common monitoring and maintenance tasks, as well as troubleshooting tools, are explained from a help-desk support technician’s point of view.

**Part VII, “Device Administration”**: All new material for this second edition, this part covers the principles of device administration AAA and TACACS+, how to design it with ISE, and the step-by-step configuration of key Cisco network devices: Catalyst switches, Wireless LAN Controllers, and Nexus data center switches.

Here is an overview of each of the 31 chapters:

- **Chapter 1, “Regain Control of Your IT Security”**: This chapter introduces the concepts that brought us to the current evolutionary stage of network access security. It discusses the explosion of mobility, virtualization, social networking, and ubiquitous network access coupled with the consumerization of information technology.
- **Chapter 2, “Fundamentals of AAA”**: This chapter reviews the critical security concept of authentication, authorization, and accounting (AAA); compares and contrasts the two main AAA types of network access and device administration; and dives into the foundations of RADIUS and TACACS+.
- **Chapter 3, “Introducing Cisco Identity Services Engine”**: Cisco ISE makes up the backbone of Cisco’s next-generation, context-aware, identity-based security policy solution. This chapter introduces this revolutionary product and provides an overview of its functions and capabilities.
- **Chapter 4, “The Building Blocks in an Identity Services Engine Design”**: This chapter covers the components of the secure access solution, including ISE personas, licensing model, and the policy structure.
- **Chapter 5, “Making Sense of the ISE Deployment Design Options”**: This chapter examines all the available personas in ISE and design options with the combination of those personas.
- **Chapter 6, “Quick Setup of an ISE Proof of Concept”**: This chapter provides a high-level overview of the ISE personas, walks you through the initial configuration (called bootstrapping) of ISE itself, and introduces role-based access control

(RBAC).

- **[Chapter 7, “Building a Cisco ISE Network Access Security Policy”](#)**: This chapter guides you through the process of creating a comprehensive network access security policy (NASP) that you can use in an environment that is safeguarded by Cisco ISE.
- **[Chapter 8, “Building a Device Security Policy”](#)**: This chapter explores ISE device profiling and Threat-Centric NAC features in some detail. The goal is to disclose the different ways in which ISE can identify device types and other contextual information about devices for use in an ISE policy.
- **[Chapter 9, “Building an ISE Accounting and Auditing Policy”](#)**: This chapter covers why you need accounting and auditing for ISE; using PCI DSS as your ISE auditing framework; and Cisco ISE user accounting. Understanding and keeping track of what is happening inside the network and inside of ISE is critical to achieving a successful ISE deployment.
- **[Chapter 10, “Profiling Basics and Visibility”](#)**: This chapter introduces the concepts of profiling and configuration choices needed to create a foundation to build upon. It examines the different profiling mechanisms and the pros and cons related to each, discussing best practices and configuration details.
- **[Chapter 11, “Bootstrapping Network Access Devices”](#)**: This key chapter examines the configuration of the NADs themselves and focuses on best practices to ensure a successful ongoing deployment.
- **[Chapter 12, “Network Authorization Policy Elements”](#)**: This chapter examines the logical roles within an organization and how to create authorization results to assign the correct level of access based on that role.
- **[Chapter 13, “Authentication and Authorization Policies”](#)**: This chapter explains the distinct and important difference between authentication and authorization policies, presents the pieces that make up the policies, and provides examples of how to create a policy in ISE that enforces the logical policies created in [Chapter 12](#).
- **[Chapter 14, “Guest Lifecycle Management”](#)**: Guest access has become an expected resource at companies in today’s world. This chapter explains the full secure guest lifecycle management, from Web Authentication (WebAuth) to sponsored guest access and self-registration options.
- **[Chapter 15, “Client Posture Assessment”](#)**: This chapter examines endpoint posture assessment and remediation actions, the configuration of the extensive checks and requirements, and how to tie them into an authorization policy.
- **[Chapter 16, “Suplicant Configuration”](#)**: This chapter looks at configuration

examples of the most popular supplicants.

- **[Chapter 17, “BYOD: Self-Service Onboarding and Registration”](#)**: This critical chapter goes through a detailed examination of BYOD concepts, policies, and flows. Both the user and administrative experiences are detailed, as well as the integration between ISE and third-party MDM vendors and ISE’s internal certificate authority (CA).
- **[Chapter 18, “Setting Up and Maintaining a Distributed ISE Deployment”](#)**: Cisco ISE can be deployed in a scalable distributed model or as a standalone device. This chapter examines how ISE can be deployed in this distributed model, and the caveats associated. It also details high availability (HA) with technologies such as load balancing.
- **[Chapter 19, “Remote Access VPN and Cisco ISE”](#)**: This chapter details the integration of ISE with remote access VPNs using the Cisco ASA.
- **[Chapter 20, “Deployment Phases”](#)**: This chapter explains the best practices related to phasing in a secure network access deployment. The chapter goes through the phases of Monitor Mode, Low-Impact Mode, and Closed Mode deployments.
- **[Chapter 21, “Advanced Profiling Configuration”](#)**: This chapter builds on what was learned and configured in [Chapter 10](#), examining how to profile unknown endpoints and looking deeper into the profiling policies themselves.
- **[Chapter 22, “Cisco TrustSec AKA Security Group Access”](#)**: This chapter introduces the next-generation policy model known as Cisco TrustSec and Security Group Tags.
- **[Chapter 23, “Passive Identities, ISE-PIC, and EasyConnect”](#)**: Brand new for this second edition, this chapter compares and contrasts active versus passive identities, and the EasyConnect method of network access control.
- **[Chapter 24, “ISE Ecosystems: The Platform eXchange Grid \(pxGrid\)”](#)**: Also brand new for this edition, this chapter discusses the use of ISE as the center of a security ecosystem, the importance of context sharing, and the best practices for deploying the Platform eXchange Grid (pxGrid).
- **[Chapter 25, “Understanding Monitoring, Reporting, and Alerting”](#)**: This chapter explains the extensive and redesigned monitoring, reporting, and alerting mechanisms built into the ISE solution.
- **[Chapter 26, “Troubleshooting”](#)**: This chapter aids the reader when having to troubleshoot the ISE identity-enabled network and its many moving parts.
- **[Chapter 27, “Upgrading ISE”](#)**: This chapter focuses on the upgrading of ISE nodes using both the graphical tool and the command line, with a heavy focus on the secondary PAN first (SPF) method of upgrade.

- [\*\*Chapter 28, “Device Administration Fundamentals”\*\*](#): This chapter details the integration of device administration AAA and TACACS+ into the ISE solution and the design options for deploying it in parallel or in conjunction with network access AAA.
- [\*\*Chapter 29, “Configuring Device Admin AAA with Cisco IOS”\*\*](#): Building on [Chapter 29](#), this chapter details the configuration of ISE and Cisco IOS–based Catalyst switches for the purposes of device administration AAA with TACACS+.
- [\*\*Chapter 30, “Configuring Device Admin AAA with Cisco WLC”\*\*](#): This chapter details the configuration of ISE and Cisco Wireless LAN Controllers for the purposes of device administration AAA with TACACS+.
- [\*\*Chapter 31, “Configuring Device Admin AAA with Cisco Nexus Switches”\*\*](#): This chapter details the configuration of ISE and Cisco Wireless LAN Controllers for the purposes of device administration AAA with TACACS+.

# **Part I Identity-Enabled Network: Unite!**

[Chapter 1 Regain Control of Your IT Security](#)

[Chapter 2 Fundamentals of AAA](#)

[Chapter 3 Introducing Cisco Identity Services Engine](#)

# Chapter 1 Regain Control of Your IT Security

This chapter covers the following topics:

- The weakest-link security problem
- Introduction to Cisco ISE
- Introduction to identity and context

The explosion of mobility, virtualization, social networking, and ubiquitous network access coupled with the consumerization of information technology brings new security challenges to organizations, including:

- Insufficient security controls for non-corporate-owned devices, especially consumer-class devices such as the iPhone and iPad. This is known as the Bring Your Own Device (BYOD) phenomenon.
- An increased potential for the loss of sensitive data, which can cause an array of problems for your business, customers, and partners.
- Dissolution of network security boundaries (borderless networks), resulting in an increased number of entry points to your network and, therefore, an increased risk to your business.
- Increased complexity in maintaining compliance with security and privacy regulations, laws, and other enforced standards such as Payment Card Industry Data Security Standard (PCI-DSS).

IT network and security policies, budgets, and resources are not keeping pace with the rapid innovations happening in our business models, workplace, and technology. With today's security challenges and threats growing more sophisticated and broad, traditional network security approaches are no longer sufficient without augmentation. Organizations require security systems that can provide more actionable intelligence, that are pervasively deployed, and that are more tightly integrated with other installed networking and security tools than they have been in the past.

The threat landscape has also evolved dramatically in the last couple years. Attackers are now using social-engineering techniques to gain trusted credentials on your network and services. Social engineering, essentially hacking people, is the fastest-growing attack vector today. Many of the recent breaches can be traced back to attackers obtaining trusted credentials that allowed them to pivot throughout the breached networks just like any other user would. This raises serious concerns, such as how do you protect against an attacker that has admin credentials on your Microsoft Active Directory (AD) domain? One way is to ensure that each user connecting into the network is dynamically limited to access to only those services that they require. We call this dynamic network segmentation, or micro-segmentation.

The purpose of this chapter is to define the major focus areas that need to be considered to take back, and continue to maintain, control of your IT security. This must be accomplished in the face of recent technology trends while still enabling businesses to function efficiently. The secret lies in centralized, pervasive security policy control.

## Security: Still a Weakest-Link Problem

The bad guys are always looking for the path of least resistance to their targets. Why waste effort attacking a hardened target system directly when you can get there by quickly compromising something weaker and using its privileges to exploit your target? This is the basic principle of the weakest-link problem. The information you are trying to protect is only as secure as the weakest entry point (link) to that information. This has always been true in IT security. The big change is in the increase of the sum total of links, or entry points, that must be dealt with. Additionally, the use of social engineering is on the rise due to its high success rate.

Never before have networks and their data been more accessible by external untrusted individuals. Also, the number of devices in today's typical network has grown dramatically over time with the addition of network-capable nodes such as IP phones, IP videoconferencing systems, and mobile devices such as cell phones and tablets. Most recently, the phenomenon of the Internet of Things (IoT) is causing an explosion in the number of network devices. These devices range from IP cameras, home automation devices, appliances, cars, smart watches, and so many more. Just think about all the devices you have that are connected to your home network. Now extrapolate that number to your company. It's an amazing number of devices, each with its own operating system, vulnerabilities, and security concerns.

Today's networks allow access from literally anywhere on the globe via a combination of wireless, wired, and virtual private networks (VPNs), guest portals, cloud services, consumer devices, mobile devices, business-to-business (B2B) connections...and the list goes on.

Back in the day, prior to the expansion of cost-effective mobile computing and networkable handheld devices, networks were composed of stationary corporate-owned desktop PCs, each of which often had only one employee assigned to it for dedicated usage. Now each employee has numerous network-attached devices, most or all of which are highly mobile. For example, on his home network one of this book's authors has an iPhone, an iPad, an Apple Watch, a Windows 7 PC, a MacBook Air, a Verizon MiFi device, a Wi-Fi corporate IP Phone, a Cisco telepresence system, and a desk IP Phone. And those are just the devices he uses for work! It doesn't include his home devices or cloud services, which easily triples the number. Some of these are personal devices, while others are corporate-owned assets. But all have a risk profile to his company.

No organizations today are closed entities with well-defined network security perimeters. This leads us to the concepts of ubiquitous access and borderless networks. Gone are the days of a nicely defined network security perimeter made up of a firewall that guards against unauthorized access from the outside. Security architecture is changing from a point defense perimeter approach to a defense-in-depth network security architecture that is policy-driven and threat-focused.

Here are some fundamental shifts created by today's environment:

- You can no longer simply trust the packets on your internal networks.
- The network must require identity- and context-aware access control at all attachment points—wired, wireless, and VPN (internal and external).
- Security policies must become identity- and context-aware, as well as centrally managed.
- Security and network systems must work together seamlessly to create an architecture that works effectively.
- Integrated and automated threat defense is now a requirement. Static defenses are too easily bypassed and manual policy change and remediation is too slow to defend against the threats.

Today, networks are most secure at their traditional network perimeter, namely the Internet-facing access points. However, the security of the internal networks, especially wired networks, behind those impressive perimeter fortress walls is sorely lacking. By and large, once a user gains access to the internal networks, they are given free and unrestricted network access. In addition, the pervasiveness of mobility has thrown the concept of internal vs. external out the window. Mobile devices roam between both internal and external networks while sometimes connecting to both simultaneously. Never before has the average employee been so connected in so many ways in so many places. Effectively dealing with the security risks that spring forth from this new networking reality by using the Cisco Identity Services Engine (ISE) and Cisco Secure Access are the focus of this book.

## Cisco Identity Services Engine

Cisco describes its Identity Services Engine solution in this way:

A different approach is required to both manage and secure the evolving mobile enterprise. With superior user and device visibility, Cisco ISE simplifies the mobility experience for enterprises. It also shares vital contextual data with integrated technology partner solutions. With the integration, consolidation, and automation that Cisco ISE provides, you can identify, contain, and remediate threats faster. The Cisco Identity Services Engine is a next-generation identity and access

control policy platform that enables enterprises to facilitate new business services, enhance infrastructure security, enforce compliance, and streamline service operations. Its unique architecture allows enterprises to gather real-time contextual information from networks, users, and devices to make proactive governance decisions by enforcing policy across the network infrastructure—wired, wireless, and VPN.

At a high level, the Cisco ISE and Secure Access solution provide the following services:

- Gain awareness of everything hitting your network.
- Control network access securely, consistently, and efficiently.
- Relieve the stress of a complex access management environment.

Some of the key capabilities that ISE will provide are:

- User identity awareness and control.
- Network, user, and device context awareness. Examples of context include operating system patch level, AD group member, antivirus client installed and up to date, device type such as printer, physical location of device, risk profile of device, and more.
- A centralized security policy across wired, wireless, and VPN access for simpler corporate governance.
- Centralized guest access management that is both feature-rich and easy to use.
- System-wide visibility into who, where, and what is on a network.
- Authentication, authorization, and accounting (AAA), device profiling, device posture, mobile device onboarding, and guest services in a single solution to simplify deployments and cut operational costs via ISE.
- Automated device profiling/identification using ISE-based traffic probes, Cisco IOS device sensors included in Cisco switches, and active endpoint scanning.
- Simplified BYOD onboarding through self-service device registration and provisioning. Significantly reduces the burden on IT without sacrificing security.
- TACACS+ device AAA.
- Cisco TrustSec policy management and enforcement using security group tagging.
- Built-in certificate authority (CA) specifically designed to make it simple to use.
- Ability to share the information and context inside of ISE with other devices, such as next-generation firewalls (NGFW) and using Cisco Platform Exchange Grid (pxGrid).

To summarize, the Cisco ISE solution allows you to connect any user on any device to

any segment of your network more easily, reliably, and securely. The rich policy-based nature of the ISE solution provides you with identity- and context-based access differentiation.

## Sources for Providing Identity and Context Awareness

Having identity awareness in the network simply means that you are able to determine and authenticate the individuality of the user or group of users trying to gain access to your network. To establish individuality, combine both a username (or equivalent) and any other available user attributes. For example, Jamey Heary successfully authenticated onto the network using his AD account JHeary. JHeary is a member of both the Users and Contractors groups. There is now an identity for the user JHeary that can be utilized to determine which network policy ISE should assign to the network.

ISE can obtain identity information and validate its authenticity using several methods and sources, including AD. This identity information can be user-based, endpoint-based, or both. Here are the most common methods ISE uses to obtain identity information:

- **802.1X:** 802.1X is an IEEE standard for Layer 2 access control to wired and wireless networks. As an example, WPA2 Enterprise uses 802.1X plus Extensible Authentication Protocol (EAP) for authentication. 802.1X can use either user identity or machine identity, or it can use both. 802.1X offers the capability to permit or deny Layer 2 network connectivity, assign a VLAN, and apply various other traffic- and network-related policies.
- **Redirect to web portal:** A user's web browser is automatically redirected to a user authentication web page (in other words, a web authentication) where they can input their identity via a customized web form.
- **Guest access:** Users are identified as guest users in various ways. Common methods are no authentication, temporary credentials, temporary event key, and social network credentials like Facebook. Guest access can also be defined based on connection information. For example, anyone who connects to the public-net wireless service set identifier (SSID) is considered a guest user.
- **VPN authentication:** Users enter their credentials into their VPN client before a VPN tunnel or a Secure Sockets Layer (SSL) VPN is allowed to pass traffic.
- **Easy Connect:** ISE policy allows users to log on to Active Directory from their domain-joined PC. ISE then applies an updated network policy based on their AD credentials and groups.
- **MAC address authentication bypass:** ISE uses the endpoint's hardware MAC address from its network interface card to gain access to the network. This is called MAC Authentication Bypass (MAB). Because of the ease of MAC forgery, it is

recommended to use additional methods such as device-profiling information to ensure authenticity.

Now that identity awareness has been established, you need to gather real-time contextual information from networks, users, and devices. Cisco ISE has several ways of collecting and using contextual information. Here are some of the more common context sources:

- User authorization attributes from identity sources such as Lightweight Directory Access Protocol (LDAP), AD, RADIUS, or the internal ISE user database.
- Device attributes from LDAP using a machine account lookup.
- An integrated device profiling engine that actively and/or passively scans a device or monitors its network behavior to determine what kind of device it is. For example, if a device has a MAC address owned by Apple and its browser user-agent string includes the words “Apple iPad,” then the profiling engine will classify it as an Apple iPad.
- Location information such as physical location, network access type (wired, wireless, VPN), GPS location, and switch port location.
- Device posture, which gathers posture information from the host. Posture information reported to ISE can include OS type and version, OS patches, service pack level, security software, application inventory, running processes, registry keys, digital certificates, and many others.
- Context information gathered from other network and security solutions such as Cisco Advanced Malware Protection (AMP), Cisco Stealthwatch, Cisco NGFW, a Qualys vulnerability scanner, and many others. Context examples include vulnerability data found on host, malware running on host, host connecting to malicious content, and other threat-centric contexts.

## Unleash the Power of Centralized Policy

The final step is putting identity and context information to work via ISE’s policy framework. Cisco ISE provides a centralized view from which you can administrate the policy of up to 500,000 endpoints enterprise-wide regardless of their network access type—wired, wireless, or VPN. Cisco ISE also supports network devices from multiple vendors. The policies you create will monitor and enforce users’ compliance with any written security policy and other corporate governance regulations your organization has in place. Additionally, ISE can automate the quarantine and remediation of users/hosts based on live threat data. For example, if Cisco AMP finds malware on a host, it can tell ISE to quarantine that host on the network. ISE is capable of performing simple or complex, yet elegant, policy rules that are both identity- and context-aware. Once a policy rule is matched, its permissions are applied to the network and/or device.

It is in this way that ISE's centralized policy structure is able to greatly simplify and restore your visibility, control, and governance of the network.

The kinds of permissions that ISE can grant once a policy match is obtained are extensive. Here are a few of the popular ones:

- Deny any network access
- Permit all network access
- Restrict network access by downloading an access control list (ACL) to the access device (switch, wireless controller, VPN headend)
- Change the assigned VLAN on a switch port or wireless connection
- Redirect client for web authentication
- Auto-provision the device's 802.1X supplicant or client
- Assign a Security Group Tag (SGT) to all data frames
- Execute an Auto Smartports macro on a Cisco switch

[Figure 1-1](#) depicts some of the permissions that are available using Cisco ISE. In the following chapters of this book, we will explore permissions and the other topics of this chapter in more detail.

Authorization Profiles > [New Authorization Profile](#)

**Authorization Profile**

* Name	example
Description	permissions
* Access Type	ACCESS_ACCEPT

Network Device Profile Cisco

Service Template

Track Movement

Passive Identity Tracking

**Common Tasks**

<input checked="" type="checkbox"/> DACL Name	PERMIT_ALL_TRAFFIC
<input type="checkbox"/> ACL (Filter-ID)	
<input checked="" type="checkbox"/> VLAN	Tag ID 1  ID/Name corp
<input type="checkbox"/> Voice Domain Permission	

## **Figure 1-1 Cisco ISE Permission Authorization Profile Example**

### **Summary**

This chapter examined the increasing security risks, threats, and corporate governance challenges being faced in our borderless networks that are filled with highly mobile corporate-owned and personally owned devices. This chapter focused on network security as a weakest-link problem in an environment where the number of links is exponentially expanding due to mobility, virtualization, IoT, and the consumerization of IT. Cisco Identity Services Engine and Cisco Secure Access were introduced as solutions to help alleviate these risks and challenges. The secret to efficiently tackling these tasks is pervasive and centralized policy control of all devices and network access methods. In this book, we will explore the topics of this chapter in much more detail.

# Chapter 2 Fundamentals of AAA

This chapter covers the following topics:

- Authentication, authorization, and accounting (AAA)
- Terminal Access Controller Access-Control System Plus (TACACS+)
- Remote Authentication Dial-In User Service (RADIUS)

In the world of security, we can only be as secure as our controls permit us to be. There are laws in the United States defining what a passenger of an airplane is permitted to bring onboard. If the TSA agents weren't operating the metal detectors and X-ray machines (and all the other things that slow us down when trying to reach our airplanes), then how would the FAA ever really enforce those policies?

With technology, we are faced with the same challenges. We need to have controls in place to ensure that only the correct entities are using our technological "gadgets." The same security concepts from the airport can be applied to many use cases, including human interaction with a computer, a computer's interaction with a network, and even an application's interaction with data.

This security principle is known as authentication, authorization, and accounting (AAA), often referred to as Triple-A.

Before allowing someone or something to perform an action, you must ensure you know who that entity actually is (authentication) and if the entity is permitted, what level of access should be granted (authorization). Additionally, you need to ensure that accurate records are maintained showing that the action has occurred, so you keep a security log of the events (accounting).

The concepts of AAA can be applied to many different aspects of a technology lifecycle. However, this book will focus on the two main aspects of AAA related to network security:

- **Device administration AAA:** Controlling access to who can log in to a network device console, Telnet session, Secure Shell (SSH) session, or other method is one form of AAA that you should be aware of. This is AAA for device administration, and although it can often seem similar to network access AAA, it has a completely different purpose and requires different policy constructs.
- **Network access AAA:** Securing network access can provide the identity of the endpoint, device, or user before permitting the entity to communicate with the network. This is AAA for network access and is the type of AAA that is most focused on in this book.

## Triple-A

Authentication, simply put, is the validation of an identity, also known as a credential. It is a very important step in the process of performing any sort of secure access control, regardless of what you are controlling. Forget about information technology for a second, and consider paying for groceries with a credit card. As a credit card owner, you have the choice to sign the back of the card or to write “check ID” on the back. The more secure method is to force the validation of the credential (the ID) of the person using that card and ensure that credential matches the name on the front of the credit card.

Having a cashier check the identity of the card user to ensure the person in front of them matches the person shown on the ID itself is authentication. Ensuring that the identity matches the name printed on the credit card is authorization. Think about this scenario: Jamey Heary goes into a retail store and hands the cashier a credit card to pay for the \$10,000 of electronics he is purchasing. He passes his driver’s license to the cashier, who verifies that the picture matches Jamey. It is certainly his identity; however, the name printed on the credit card is Aaron Woland. Should the credit card transaction go through? Of course not (and he better not try).

Jamey’s attempt to use Aaron’s credit card is now in the log files of the point of sale system, the video monitoring system of the store, and other systems. This is the accounting portion of AAA. It’s a critical piece that is required for reporting, audits, and more.

It will become paramount for you as a security professional to understand the difference and purpose of all three A’s in the Triple-A security principal.

## Compare and Select AAA Options

As previously described in this chapter, there are two uses of AAA that you will focus on in this book—device administration and network access.

## Device Administration

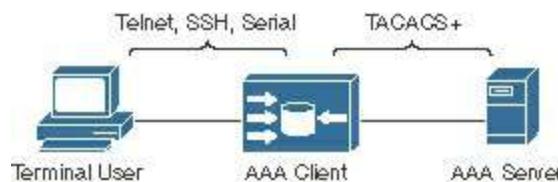
AAA for device administration is a method of AAA for controlling access to a network device console, Telnet session, SSH session, or other method of accessing the device operating system itself where configuration of the device occurs. For example, imagine your company has an Active Directory group named Cisco Administrators, which should have full access (privilege level 15) to the Cisco switches in the company’s network. Members of Cisco Administrators should therefore be able to make changes to virtual local-area networks (VLANs), see the entire running configuration of the device, and more.

There could be another group named Cisco Operators who should only be allowed to view the output of **show** commands, and not be allowed to configure anything in the

device. Device administration AAA provides this capability.

However, device administration AAA can get much more granular. Cisco Identity Services Engine (ISE) has a capability to provide command sets, which are listings of commands that are permitted or denied to be executed by an authenticated user. In other words, a user can authenticate to the Cisco IOS shell, and ISE can permit or deny the user's execution of individual commands, if you choose.

[Figure 2-1](#) illustrates device administration.



**Figure 2-1** Device Administration AAA

Administering devices can be very interactive in nature, with the need to authenticate once but authorize many times during a single administrative session in the command line of a device. As such, it lends itself well to using the Terminal Access Controller Access-Control System (TACACS) client/server protocol, more so than Remote Authentication Dial-In User Service (RADIUS). As the name describes, TACACS was designed for device administration AAA to authenticate and authorize users into mainframe and Unix terminals and other terminals or consoles.

Both the TACACS and RADIUS protocols will be discussed in more depth within this chapter; however, because TACACS separates out the authorization portion of AAA, allowing for a single authentication and multiple authorizations within the same session, it lends itself to device administration more than RADIUS. RADIUS does not provide the capability to control which commands can be executed.

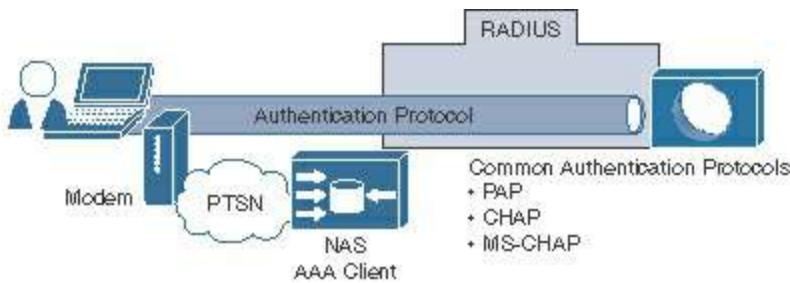
## Network Access

Secure network access is essentially all about learning the identity of the user or endpoint before permitting that entity to communicate within the network. This type of AAA is the main focus in this book. Network access AAA really took a strong hold back in the day of modems and dial-up networking with plain old telephone service (POTS). Companies provided network access to workers from outside the physical boundaries of the company's buildings with the use of modems. People gained Internet access by using dial-up to an Internet service provider (ISP) over their modems, as well. Basically, all that was needed was a modem and a phone line.

Of course, allowing anyone to dial in to the company network just by dialing the modem's phone number was not a secure practice. The user needed to be authenticated and authorized before being allowed to connect. That is where RADIUS came into play originally, as is evident in the name of the protocol (Remote Authentication Dial-In User

Service). RADIUS was used between the network access device (NAD) and the authentication server. The authentication was normally Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), or Microsoft CHAP (MS-CHAP).

[Figure 2-2](#) illustrates dial-up remote access.



**Figure 2-2** Dial-Up Remote Access

As technology continued to evolve and direct dial-in to a company was replaced by remote-access virtual private networks (VPN), Wi-Fi became prevalent, and the IEEE standardized on a method to use Extensible Authentication Protocol (EAP) over local-area networks (IEEE 802.1X), RADIUS was used as the protocol of choice to carry the authentication traffic. In fact, IEEE 802.1X cannot use TACACS. It must use RADIUS.

**Note** There is another protocol similar to RADIUS, known as DIAMETER, that may also be used with 802.1X. However, it is mostly found in the service provider space and is out of scope for this book.

In today's world, RADIUS is the protocol used almost exclusively with network access AAA and is the main control plane in use between Cisco ISE and the network devices themselves.

## TACACS+

As previously introduced, TACACS is a protocol set created and intended for controlling access to mainframe and Unix terminals. Cisco created a new protocol called TACACS+, which was released as an open standard in the early 1990s.

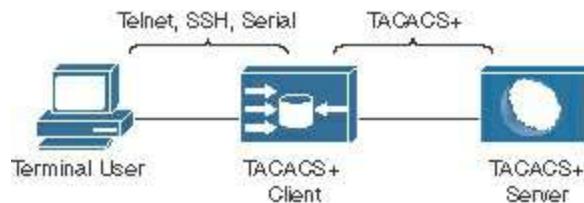
TACACS+ may be derived from TACACS, but it is a completely separate and non-backward-compatible protocol designed for AAA. Although TACACS+ is mainly used for device administration AAA, it can also be used for some types of network access AAA.

TACACS+ became a supported protocol with Cisco ISE in version 2.0. Prior to ISE 2.0, the Cisco Secure Access Control Server (ACS) was Cisco's primary AAA server product for enterprises that needed to use TACACS+ for device administration AAA.

However, starting with ISE 2.0, ISE has replaced ACS as Cisco's enterprise flagship AAA server for both RADIUS and TACACS+.

**Note** Other Cisco products support TACACS+, such as the Cisco Access Registrar solution. However, those solutions are geared toward service providers and are not germane to this book.

TACACS+ uses Transmission Control Protocol (TCP) port 49 to communicate between the TACACS+ client and the TACACS+ server. An example is a Cisco switch authenticating and authorizing administrative access to the switch's IOS CLI. The switch is the TACACS+ client, and Cisco ISE is the server, as illustrated in [Figure 2-3](#).



**Figure 2-3** TACACS+ Client–Server Communication

One of the key differentiators of TACACS+ is its capability to separate authentication, authorization, and accounting as separate and independent functions. This is why TACACS+ is so commonly used for device administration, even though RADIUS is still certainly capable of providing device administration AAA.

Device administration can be very interactive in nature, with the need to authenticate once but authorize many times during a single administrative session in the command line of a device. A router or switch may need to authorize a user's activity on a per-command basis. TACACS+ is designed to accommodate that type of authorization need. As the name describes, TACACS+ was designed for device administration AAA to authenticate and authorize users into mainframe and Unix terminals and other terminals or consoles.

TACACS+ communication between the client and server uses different message types depending on the function. In other words, different messages may be used for authentication than are used for authorization and accounting. Another very interesting point to know is that TACACS+ communication will encrypt the entire body of the packet to assure privacy of any credentials being transported and that any messages transported over the session will not be modified in transit.

## TACACS+ Authentication Messages

When using TACACS+ for authentication, only three types of packets are exchanged between the client (the network device) and the server:

- **START:** This packet is used to begin the authentication request between the AAA client and the AAA server.
- **REPLY:** Messages sent from the AAA server to the AAA client.
- **CONTINUE:** Messages from the AAA client used to respond to the AAA server requests for username and password.

The following paragraphs describe the authentication flow process and the messages used.

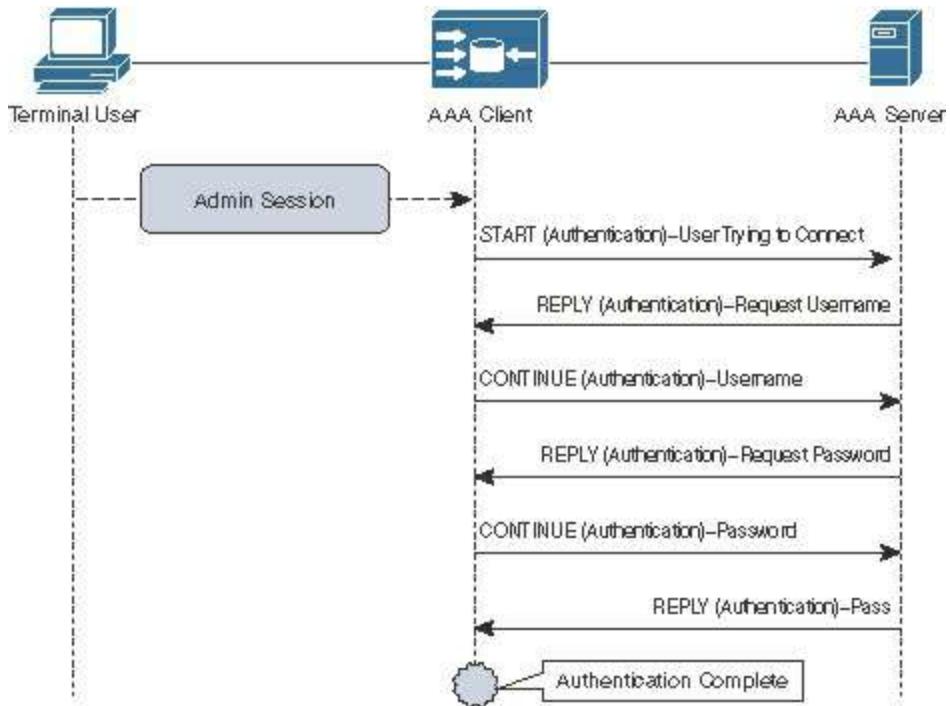
When an authentication request is sent from the client to the server, it begins with a START message from the network device to the server. The START message tells the server that an authentication request is coming. All messages from the server to the network device (client) will be a REPLY during authentication. The server sends a REPLY message asking for the client to retrieve the username. The username is sent to the server within a CONTINUE message.

After the server receives the username, it sends a REPLY message back to the client requesting the password, which is sent back to the server in a CONTINUE message. The server then sends a final REPLY message with the pass or fail status of the authentication request.

The possible values returned from the AAA server to the AAA client within the final REPLY message are:

- **ACCEPT:** The user authentication succeeded and the authorization process may begin, if the AAA client is configured for authorization.
- **REJECT:** The user authentication has failed. The login will be denied or the end user will be prompted to try again, depending on the configuration of the AAA client.
- **ERROR:** An error occurred at some point during the authentication. AAA clients will typically attempt to authenticate the user again or attempt a different method of authenticating the user.
- **CONTINUE:** The user is prompted for additional information. This is not to be confused with the CONTINUE message sent from the AAA client to the AAA server. This value is sent from the AAA server within a REPLY message, indicating that more information is required. CONTINUE is also used for generating additional prompts to gather more information during the logon process. This is used for items such as changing a password or requesting a second authentication (such as username, password, and secure token).

[Figure 2-4](#) illustrates the authentication messages between the client and server.



**Figure 2-4 TACACS+ Authentication Communication Flows**

## TACACS+ Authorization and Accounting Messages

When using TACACS+ for authorization, only two messages are used between the AAA client and the AAA server:

- **REQUEST:** This message is sent from the AAA client to the AAA server to request an authorization. The authorization may be related to access to a CLI shell or possibly to authorize a specific command. The protocol doesn't distinguish between a request for shell access or a request for a CLI command authorization. The function requested is known as a service. For example, the service would be shell for CLI access to a device running Cisco IOS. Each service may be communicated with attribute-value (AV) pairs. You can find more about specific TACACS+ AV pairs at <http://bit.ly/1mF27aT>.
- **RESPONSE:** This message is sent from the AAA server back to the AAA client with the result of the authorization request, including specific details such as the privilege level assigned to the end user. RESPONSE messages may contain one of five replies:
  - **FAIL:** Indicates the user should be denied access to the requested service.
  - **PASS\_ADD:** Indicates a successful authorization and that the information contained within the RESPONSE message should be used in addition to the requested information. If no additional arguments are returned by the AAA server within the RESPONSE message, then the request is simply authorized as is.
  - **PASS\_REPLACE:** Indicates a successful authorization but the server has chosen to

ignore the REQUEST and is replacing it with the information sent back in the RESPONSE.

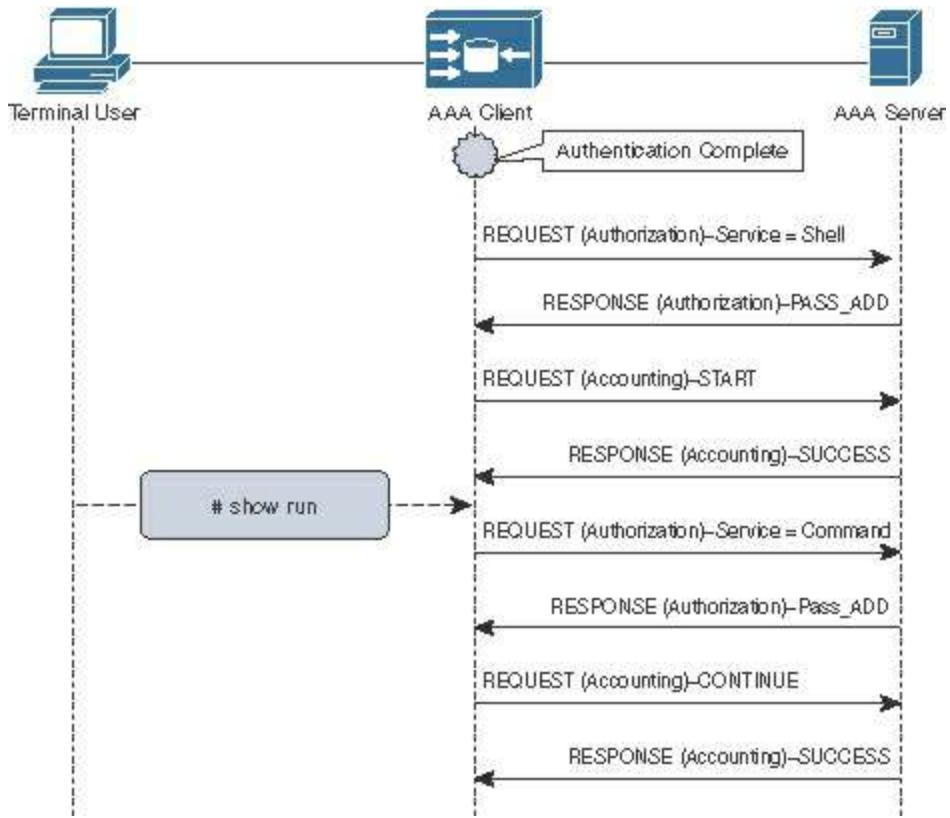
- **FOLLOW:** Indicates that the AAA server wants the AAA client to send the authorization request to a different server. The new server information will be listed in the RESPONSE packet. The AAA client can either use that new server or treat the response as a FAIL.
- **ERROR:** Indicates a problem occurring on the AAA server and that further troubleshooting needs to occur.

A key function of AAA that cannot be overlooked is accounting. It is crucial to security to have a record of what has transpired. In addition to the authorization request being sent to the AAA server, there should be accounting records of the activities of the user.

Much like authorization messages, only two message types are used in accounting:

- **REQUEST:** This message is sent from the AAA client to the AAA server to indicate a notification of activity. One of three values may be included with the REQUEST:
  - **START:** A start record indicates that a service has begun.
  - **STOP:** The stop record indicates that the service has ended.
  - **CONTINUE:** The continue record, also sometimes referred to as a Watchdog or UPDATE record, is sent when a service has already started and is in progress but there is updated information to provide in relation to the service.
- **RESPONSE:** This message is sent from the AAA server back to the AAA client with the result of the accounting REQUEST and may contain one of three replies:
  - **SUCCESS:** Indicates that the server received the record from the client.
  - **ERROR:** Indicates an error on the server and that the record was not stored.
  - **FOLLOW:** Indicates that the server wants the client to send the record to a different AAA server and includes that server's information in the RESPONSE.

[Figure 2-5](#) illustrates an end user being authorized to access the IOS exec CLI. The figure is a direct continuation of the authentication sequence shown in [Figure 2-4](#). In this illustration, the end user gets authorized to enter the IOS exec and is authorized to run the **show run** command.



**Figure 2-5** TACACS+ Authorization and Accounting Communication Flows

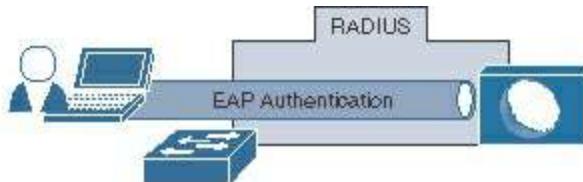
We cover TACACS+ in much more detail in Part VII, “Device Administration.”

## RADIUS

RADIUS is an IETF standard for AAA. As with TACACS+, it follows a client/server model in which the client initiates the requests to the server. RADIUS is the protocol of choice for network access AAA, and it's time to get very familiar with RADIUS. If you connect to a secure wireless network regularly, RADIUS is most likely being used between the wireless device and the AAA server. Why? Because RADIUS is the transport protocol for EAP, along with many other authentication protocols.

Originally, RADIUS was used to extend the authentications from the Layer 2 Point-to-Point Protocol (PPP) used between the end user and the network access server (NAS) and carry that authentication traffic from the NAS to the AAA server performing the authentication. This enabled a Layer 2 authentication protocol to be extended across Layer 3 boundaries to a centralized authentication server.

As described previously in this chapter, RADIUS has evolved far beyond just the dial-up networking use cases it was originally created for. Today it is still used in the same way, carrying the authentication traffic from the network device to the authentication server. With IEEE 802.1X, RADIUS is used to extend the Layer 2 EAP from the end user to the authentication server, as illustrated in [Figure 2-6](#).



**Figure 2-6** RADIUS Carries the Layer 2 EAP Communication

There are many differences between RADIUS and TACACS+. One such difference is that authentication and authorization are not separated in a RADIUS transaction. When the authentication request is sent to an AAA server, the AAA client expects to have the authorization result sent back in reply.

There are only a few message types with RADIUS authentication and authorization:

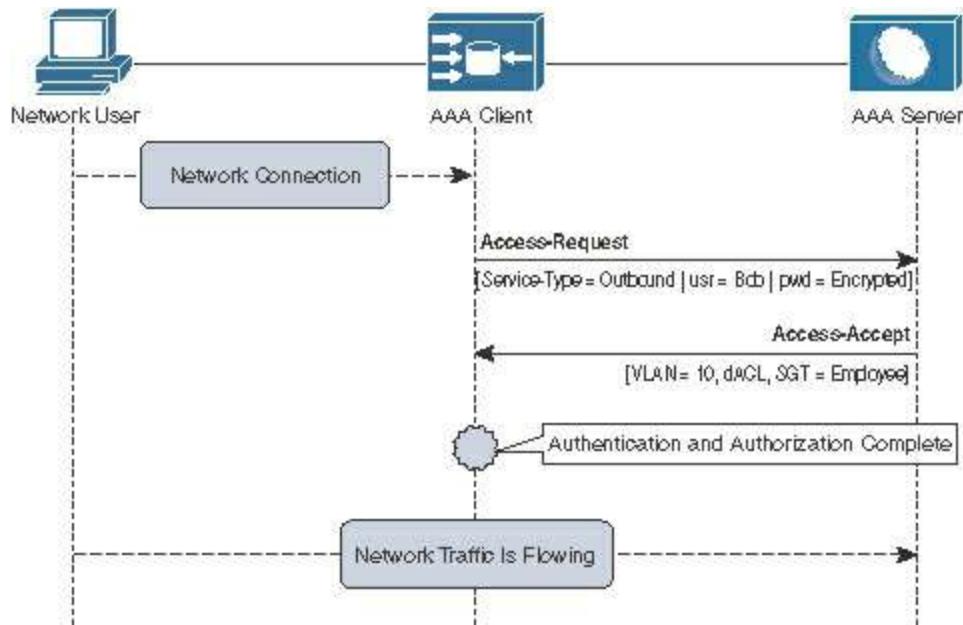
- **Access-Request:** This message is sent from the AAA client to the AAA server to request an authentication and authorization. The request could be for network access or for device shell access—RADIUS does not discriminate. The function requested is known as a service type. For example, the service type may be framed for an IEEE 802.1X authentication. [Table 2-1](#) outlines some common RADIUS service types. You can find a more complete listing of RADIUS service types at <http://bit.ly/1CGDE8Y>.

Value	Service Type Name	Commonly Used For
1	Login	Login request; often used with web authentications with non-Cisco network equipment
2	Framed	IEEE 802.1X
5	Outbound	Local web authentication
10	Call-Check	MAC Authentication Bypass (MAB)

**Table 2-1** Common RADIUS Service Types

- **Access-Accept:** Sent from the AAA server to the AAA client signaling a passed authentication. The authorization result will be included as AV pairs, which may include items such as the assigned VLAN, a downloadable access control list (dACL), a Security Group Tag (SGT), and much more.
- **Access-Reject:** Sent from the AAA server to the AAA client signaling the authentication failure. The failed authentication also signifies that no authorization has been granted.
- **Access-Challenge:** This optional message may be sent from the AAA server to the AAA client when additional information is needed, such as a second password for two-factor authentications.

[Figure 2-7](#) illustrates a sample RADIUS flow.



**Figure 2-7** RADIUS Authentication and Authorization Communication Flows

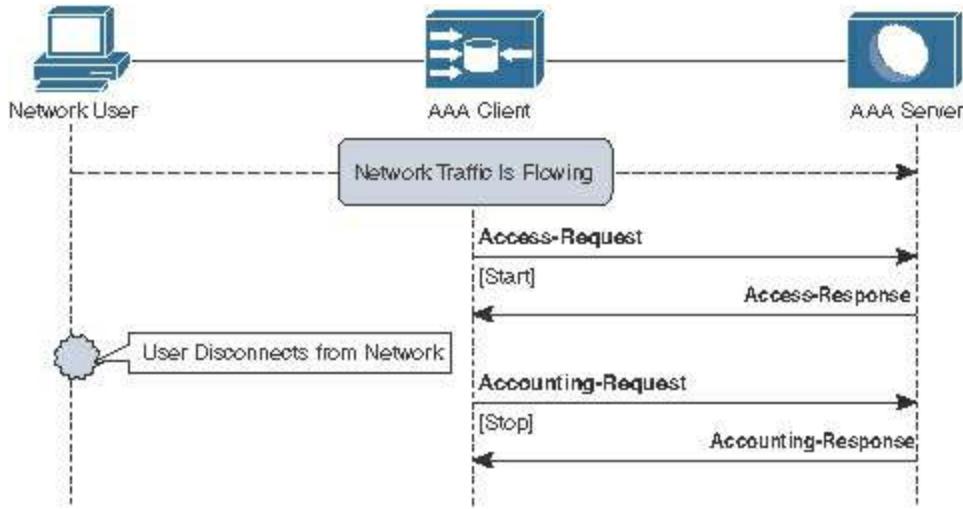
When looking at [Figure 2-7](#), keep in mind that authentication and authorization are combined with RADIUS. The Access-Accept message includes the AV pairs defining what the user is authorized to do.

A key function of AAA that cannot be overlooked is accounting. It is crucial to security to have a record of what has transpired. In addition to the authorization request being sent to the AAA server, there should be accounting records of the activities of the user.

Only two message types are used in accounting:

- **Accounting-Request:** This message is sent by the AAA client to the AAA server. It may include time, packets, Dynamic Host Configuration Protocol (DHCP) information, Cisco Discovery Protocol (CDP) information, and so on. The message may be a START message indicating that service has begun or a STOP message indicating the service has ended.
- **Accounting-Response:** This message acts like an acknowledgement of receipt, so the AAA client knows the accounting message was received by the AAA server.

[Figure 2-8](#) illustrates a sample RADIUS accounting flow. The figure is a direct continuation of [Figure 2-7](#) where the authentication and authorization occurred.



**Figure 2-8 RADIUS Authentication and Authorization Communication Flows**

Unlike TACACS+, RADIUS uses UDP as the transmission protocol. The standard ports used by RADIUS are UDP 1812 for authentication and UDP 1813 for accounting. However, Cisco supported RADIUS before the standard was ratified and the ports used were UDP 1645 (authentication) and UDP 1646 (accounting). Most Cisco devices will support using either set of ports to ensure backward compatibility.

## AV Pairs

As you noticed, attribute-value pairs (AV pairs) are referenced all through the TACACS+ and RADIUS sections. When communicating with an AAA protocol, there are many attributes that can be referenced to clearly dictate answers or results. The RADIUS server may be assigning an attribute to the authentication session like a VLAN, for example. The VLAN placeholder is the attribute, and the actual assigned VLAN number is the value for that placeholder. The placeholder and its assigned value are paired together and are referred to as attribute-value pairs (AV pairs).

## Change of Authorization

Because RADIUS was always defined to be a client/server architecture, with the client always initiating the conversation, it became challenging for the AAA server to take action. As RADIUS was defined, the AAA server could only assign an authorization as a result of an authentication request.

As technology advanced, many new demands appeared, including the capability for the network to kick out misbehaving clients, to quarantine them, or basically to just change their access.

How can that happen when the network access is using a RADIUS control plane and the AAA client must always initiate the RADIUS conversations? That is where RFC 3576 and its successor RFC 5176 come in. These RFCs define a new enhancement to

RADIUS known as Dynamic Authorization Extensions to RADIUS or, as it is more commonly called, Change of Authorization (CoA).

CoA is what allows a RADIUS server to initiate a conversation to the network device and disconnect a user's session, bounce the port (perform a shut/no-shut), or even tell the device to reauthenticate the user. As you learn more about Cisco ISE and the advanced functionality it brings to network access AAA, you will also see how critically important CoA is.

## Comparing RADIUS and TACACS+

[Table 2-2](#) summarizes the two main AAA protocols: RADIUS and TACACS+.

Value	Service Type Name	Commonly Used For
1	Login	Login request; often used with web authentications with non-Cisco network equipment
2	Framed	IEEE 802.1X
5	Outbound	Local web authentication
10	Call-Check	MAC Authentication Bypass (MAB)

**Table 2-2** Comparison of RADIUS and TACACS+

## Summary

This chapter examined the security principle of authentication, authorization, and accounting (AAA) and its importance in the security world. It introduced the different types of AAA relevant to networks, network access AAA and device administration AAA. This chapter compared and contrasted the two most common AAA protocols, RADIUS and TACACS+, revealing that TACACS+ is best suited for device administration while RADIUS is best suited for network access.

# Chapter 3 Introducing Cisco Identity Services Engine

This chapter covers the following topics:

- Architecture approach to centralized and dynamic network security policy enforcement
- ISE features and benefits
- ISE policy construct

Cisco Secure Access is the term Cisco uses to describe its network access control system. It is an all-encompassing term that generally relates to the Cisco Secure architecture with all its components, hosts, and devices, working together to secure an organization's hosts and network access. At a high level, Cisco Secure Access is the architecture that allows you to set policy for who can gain access to your network and what they can do while they are there. This might include a host connecting to a switch port, a wireless network, or a VPN. Cisco Secure Access enables you to granularly control initial, and ongoing, access to the network and all its services using policies. It controls where users and devices can go on a network and what they can do. This architecture covers all the network access methods including wired, wireless, and VPN.

Cisco Identity Services Engine (ISE) is the central policy engine for the Cisco Secure Access architecture. It is the heart and soul, the backbone, of Secure Access. Without ISE, Cisco Secure Access cannot exist. As a policy engine solution, ISE lets you gain awareness of everything hitting your network, provides access control consistently and efficiently, and relieves the stress of complex network access management.

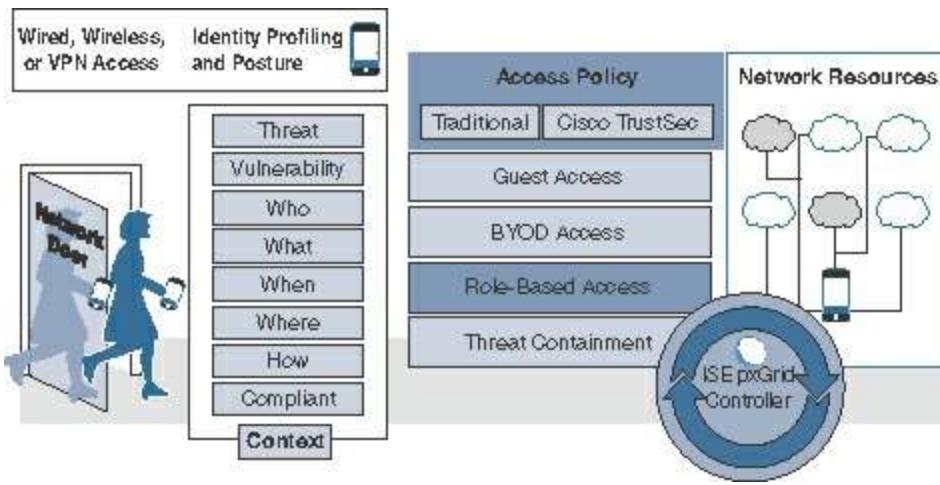
## Architecture Approach to Centralized and Dynamic Network Security Policy Enforcement

A bit of history is required to understand how the Network Access Control (NAC) and authentication, authorization, and accounting (AAA) server markets have evolved to date. This will set the stage for a discussion of the architecture approach that Cisco ISE now implements. Prior to 2004, Cisco developed a NAC solution called Cisco NAC Framework. It was heavily based on 802.1X and integration with network services. Unfortunately, it was ahead of its time and never widely deployed. It can be argued that it was the right approach to security, but back then, the clients, devices, switches, operating systems, and just about everything else in the network weren't capable or ready for an 802.1X-based integrated solution.

In response to the slow adoption of the NAC Framework, Cisco acquired Perfigo, and in 2004 released the Cisco NAC Appliance solution that was based on the Perfigo technology. Cisco NAC Appliance provided an overlay NAC solution that did not require, nor use, 802.1X or an architecture approach. It was a pure overlay technology

using Simple Network Management Protocol (SNMP) and inline NAC appliances to get the job done. Over the years, this solution gained traction and quickly became the most deployed and highest rated NAC solution on the market. As the maturation and proliferation of support for 802.1X grew over the years, it became clear to Cisco that it was time to reintroduce a next-generation NAC solution that was based on 802.1X and embraced an architecture approach instead of an overlay design.

In 2011, Cisco released Cisco ISE to provide its customers with an 802.1X-based NAC solution. ISE was a new, built from the ground up, security policy control system. Since 2011, Cisco has continued to aggressively evolve and innovate on the ISE solution and the Cisco Secure Access architecture. [Figure 3-1](#) depicts the concept of how Cisco ISE operates.



**Figure 3-1** Cisco ISE Centralized Policy Control Operation

So many capabilities that used to require separate systems, vendors, and training can now be collapsed into a single solution, ISE. New capabilities that we only dreamed of in 2011 have been added. Let's examine the business and IT benefits of deploying and operationalizing the capabilities of ISE:

- **Centralize network access control** based on business role and security policy to provide a consistent network access policy for end users whether they connect through wired, wireless, or VPN. All this can be done from a centralized ISE console that then distributes enforcement across the entire network and security infrastructure.
- **Simplify security audit and compliance** using ISE's single management console for simpler policy creation, visibility, and reporting across all company networks. IT can easily validate compliance for audits, regulatory requirements, and mandated federal guidelines.
- **Secure business- and context-based access** per your company policies. ISE can match users, endpoints, and each endpoint's security posture plus other attributes

such as time, location, and access method, thus creating an all-encompassing contextual identity. With this identity, IT administrators can apply precise network security policy controls.

- **Gain greater network visibility** and more accurate host/node identification with ISE profiling and profile feed service capabilities. This functionality provides detailed real-time and historical visibility of all the devices on the network.
- **Simplify the guest experience** using the robust capabilities that ISE provides for allowing guests to quickly and easily connect to your network. Guests can use a coffee-shop hotspot, self-service registration, or sponsored access to get to specific resources. ISE includes fully customizable, branded guest portals, created in minutes with dynamic visual workflows that let you easily manage the guest policy and experience.
- **Accelerate bring-your-own-device (BYOD) and enterprise mobility** with simple out-of-the-box setup, self-service device onboarding and management, internal device certificate management, and integration with enterprise mobility management (EMM) partners. This allows an organization to quickly and easily move to the more secure EAP-TLS wireless for the enterprise and/or allow BYOD devices to connect without sacrificing corporate security. Users can manage devices according to the business policies defined by IT administrators. The IT staff can get the automated device provisioning, profiling, and posturing it needs to comply with security policies. At the same time, employees can get their own devices onto the network without requiring IT assistance.
- **Dynamically construct a software-defined segmentation policy** that segments users, devices, and nodes on your network based on security policy. ISE uses Cisco TrustSec technology to define context-based access control policies using Security Group Tags (SGT). This policy is then pushed to TrustSec-capable network devices for enforcement. When used in a security group ACL (SGACL), SGTs allow you to dynamically segment the network without the complexity and overhead of traditional segmentation methods such as VLANs and ACLs. Additionally, security devices can alert ISE to live host threat activity such that ISE can change a user/host SGT value dynamically. The new SGT value typically quarantines the host from doing additional damage on the network, kind of like turning on your deflector shields.
- **Share user, device, and other contextual data** within the Cisco Secure Access architecture as well as with Cisco partner solutions. ISE uses Cisco Platform Exchange Grid (pxGrid) technology to share rich contextual data between products. This technology improves threat visibility and accelerates the capabilities to detect, investigate, mitigate, and remediate security threats. pxGrid improves a system's overall contextual awareness and thus decreases time to containment of network

threats.

- **Automatically contain threats** through Cisco pxGrid technology or ISE APIs. ISE automates the defense of your network based on live threat data from multiple security systems. ISE can quarantine systems, change their SGT, disconnect nodes from the network, apply new access lists, and perform many other remediation actions.
- **Network device administration access control and auditing** using TACACS+. Cisco ISE supports full TACACS+ to provide you with AAA services to all your network and security devices. Cisco even has a Cisco ACS-to-ISE migration tool to speed the transfer of your ACS policies to ISE.

## Cisco Identity Services Engine Features and Benefits

ISE has a lot of features and benefits. To help you get quickly up to speed on the major features, [Table 3-1](#) lists them and describes the benefits each offers.

ISE Feature	Benefits
Centralized management	<p>Helps administrators centrally configure and manage profiler, posture, guest, authentication, and authorization services in a single web-based GUI console.</p> <p>Simplifies administration by providing integrated management services from a single pane of glass.</p>
Business-policy enforcement	<p>Provides a rule-based, attribute-driven policy model for flexible and business-relevant access control policies. Also provides the ability to create fine-grained policies by pulling attributes from predefined dictionaries.</p> <p>Includes attributes such as user and endpoint identity, posture validation, authentication protocols, profiling identity, and other external attribute sources. These can be created dynamically and saved for later use.</p> <p>Integrates with multiple external identity repositories such as Microsoft Active Directory, Lightweight Directory Access Protocol (LDAP), RADIUS, RSA one-time password (OTP), certificate authorities for both authentication and authorization, and support for Open Database Connectivity (ODBC).</p>

Access control	Provides a range of access control options, including downloadable access control lists (dACLs), VLAN assignments, URL redirections, named ACLs, and SGTs using the advanced capabilities of network devices enabled with Cisco TrustSec technology.
Secure supplicant-less network access with Easy Connect	Provides the ability to swiftly roll out highly secure network access without configuring endpoints for authentication and authorization. Derives authentication and authorization from login information across application layers, allowing user access without requiring an 802.1X supplicant to exist on the endpoint.
Source-Group Tag Exchange Protocol (SXP) support	Acts as an SXP speaker or listener as defined in SXP draft and as the network's source of truth for SGT information. Bridges over the segments that are not compliant with Cisco TrustSec policies to make sure that differentiated role-based access is provided across the entire network.
Guest lifecycle management	Provides a streamlined experience for implementing and customizing guest network access. Creates corporate-branded guest experiences, with advertisements and promotions, in minutes. Support is built in for hotspot, sponsored, self-service, and numerous other access workflows. Provides the administration with real-time visual flows that bring the effects of the guest flow design to life. Tracks access across your network for security and compliance demands and full guest auditing. Time limits, account expirations, and Short Message Service (SMS) verification offer additional security controls.
Streamlined device onboarding	Offers automatic supplicant provisioning and certificate enrollment for standard PC and mobile computing platforms. This reduces IT help desk cases along with providing more secure access and a better experience to users. Enables end users to add and manage their devices with self-service portals and supports Security Assertion Markup Language (SAML) 2.0 for web portals. Integrates with mobile device management (MDM)/EMM vendors to enroll mobile devices and help ensure that they are compliant with access policy.

Built-in AAA services	<p>Uses standard RADIUS protocol for authentication, authorization, and accounting (AAA).</p> <p>Supports a wide range of authentication protocols, including, but not limited to, Password Authentication Protocol (PAP), Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), Extensible Authentication Protocol MD5 (EAP-MD5), Protected EAP (PEAP), EAP Flexible Authentication via Secure Tunneling (EAP-FAST), EAP Transport Layer Security (EAP-TLS), and EAP Tunneled Transport Layer Security (EAP-TTLS). Note: Cisco ISE is the only RADIUS server to support EAP chaining of machine and user credentials.</p>
Device administration access control and auditing	<p>Supports TACACS+ protocol to authenticate, authorize, and audit users when they access devices that support the TACACS+ protocol, such as network devices and servers.</p> <p>Grants users access to commands on every device based on their credentials, the group they belong to, where they connect from, and what action they are trying to take on the device.</p> <p>Provides access to device configuration on a need-to-know and need-to-act basis while keeping audit trails for every change in the network.</p>
Internal certificate authority	<p>Offers an easy-to-deploy internal certificate authority (CA) to simplify certificate management for devices. There is no need to add the significant complexity of an external CA application.</p> <p>Provides a single console to manage endpoints and their certificates. Certificate status is checked through the standards-based Online Certificate Status Protocol (OCSP). Certificate revocation is automatic.</p> <p>Supports standalone deployments and subordinate ones (that is, ones in which the CA is integrated with your existing enterprise public key infrastructure, or PKI).</p> <p>Facilitates the manual creation of bulk or single certificates and key pairs to connect these devices to the network with a high degree of security.</p>
Device profiling	<p>Ships with predefined device templates for many types of endpoints, such as IP phones, printers, IP cameras, smartphones, and tablets.</p> <p>Creates custom device templates to automatically detect, classify, and associate custom-defined identities when endpoints connect to the network.</p> <p>Helps to create endpoint-specific authorization policies based on device type.</p> <p>Collects endpoint attribute data with active scanning and passive network monitoring and telemetry.</p>

Device-profile feed service	<p>Delivers automatic updates of Cisco's validated device profiles for various IP-enabled devices from multiple vendors. It detects all the newest devices and simplifies the task of keeping up with them.</p> <p>Offers a mechanism where partners and customers can share their customized profile information to be vetted by Cisco and redistributed.</p>
Endpoint posture service	<p>Performs endpoint posture assessment on PCs and mobile devices connecting to the network.</p> <p>Works through a persistent client-based agent, a temporal agent, or a query to an external MDM/EMM vendor's system to validate that an endpoint conforms to appropriate compliance policies.</p> <p>Provides the ability to create powerful policies that include, but are not limited to, checks for the latest OS patches, antivirus and anti-spyware packages with current definition file variables (version, date, etc.), antimalware packages, registry settings (key, value, etc.), patch management, disk encryption, mobile PIN-lock or rooted or jailbroken status, application presence, USB attached media, and so on.</p> <p>Supports the automatic remediation of PC clients as well as periodic reassessments alongside leading enterprise patch-management systems to make sure the endpoint is not in violation of company policies.</p> <p>Requires the AnyConnect 4.x agent for posture assessment on these OS platforms: Microsoft Windows 7, 8, or 10 (32-bit or 64-bit) and Mac OS X 10.7, 10.8, 10.9, or 10.11.</p>
Extensive multi-forest Active Directory support	<p>Provides comprehensive authentication and authorization against multi-forest Microsoft Active Directory domains.</p> <p>Groups multiple disjointed domains into logical groups.</p> <p>Configurations of complex Active Directory topologies are simplified to support ever-changing business environments.</p> <p>Includes flexible identity rewriting rules to smooth the solution's transition and integration.</p> <p>Supports Microsoft Active Directory 2003, 2008, 2008R2, 2012, 2012R2, and 2016.</p>
Cisco Rapid Threat Containment	<p>Takes network mitigation and investigation actions in response to security events.</p> <p>Integrates Cisco ISE and Cisco security technology partner solutions in a broad variety of technology areas.</p> <p>Uses Cisco pxGrid as a highly scalable IT clearinghouse for multiple security tools to communicate with each other in real time, automatically.</p>

Monitoring and troubleshooting	Offers a built-in web console for monitoring, reporting, and troubleshooting to assist help desk and network operators in quickly identifying and resolving issues.  Provides robust historical and real-time reporting for all services. Logs all activities and offers real-time dashboard metrics of all users and endpoints connecting to the network.
Government Certifications	Meets the requirements of Federal Information Processing Standard (FIPS) 140-2, Common Criteria, ISO 27001, and Unified Capabilities Approved Product List. Also IPv6, ready.  Note: Certifications may not be available on all releases, or they may be in varying states of approval. Current certifications and releases can be found at <a href="http://www.cisco.com/web/strategy/government/sec_cert.html">http://www.cisco.com/web/strategy/government/sec_cert.html</a> .

**Table 3-1 Cisco ISE Features and Benefits**

## ISE Platform Support and Compatibility

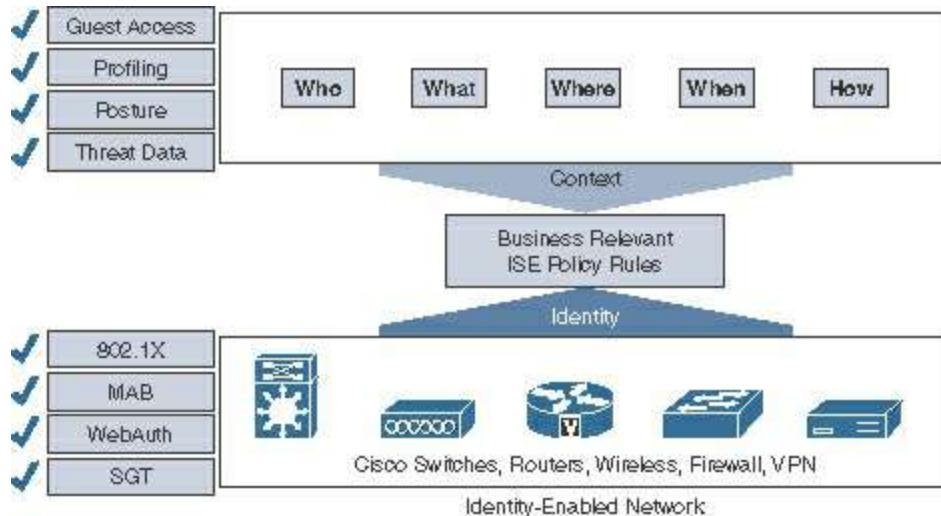
ISE is available as a physical or virtual appliance. Both physical and virtual form factors can be used to create ISE clusters to serve larger organizations and provide the scale, redundancy, and failover required of a critical enterprise system.

ISE virtual appliances are supported on VMware ESXi 5.x and 6.x or Kernel-based Virtual Machine (KVM) on Red Hat 7.x. A production deployment should be run on hardware that equals or exceeds the configurations of the current physical ISE platforms. For lab or testing environments that provide no product services, the solution can be run on virtual targets that have at least 4 GB of memory and at least 200 GB of hard drive space available.

For physical platform support of ISE, please refer to the Cisco Secure Network Server Data Sheet on Cisco.com.

## Cisco Identity Services Engine Policy Construct

The Cisco ISE product line was first introduced to provide network access control using RADIUS and 802.1X. Cisco created it to provide businesses with an integrated architecture approach to their network access and policy requirements. The ISE solution now provides many more capabilities, including consolidated and comprehensive network and threat visibility using identity and contextual awareness. This includes the who, what, where, when, and how of network access. [Figure 3-2](#) illustrates the high-level components of an ISE policy. [Figure 3-2](#) is not meant to be all encompassing, but rather an example.



**Figure 3-2 Cisco ISE Policy Construct**

Let's break down the information found in [Figure 3-2](#) into its constituent parts. The two main parts are Context and Identity. Identity provides knowledge of the user or device; this gives us the who. Context extends the amount of information we have about an identity to provide additional information such as what, where, when, and how. The consolidation of identity and context allows the creation of business-relevant policies. Here is a good example of what this would look like: Jamey Heary (who) logged in to the network in building 4 (where) using Cisco AnyConnect (what) today at 9 p.m. (when) using his iPhone (how). ISE, working with a Cisco Mobility Services Engine, can even determine a wireless node's actual location within 3 meters and change its ISE policy based on location.

Now that you know what information you want to include in your ISE policies, you need to figure out how to gather that data. A major strength of Cisco ISE is its ability to support all access methods—wired, wireless, and VPN—into a single policy table. To do this, ISE relies on network systems for both the collection of identity and context and the enforcement of policy. The left side of [Figure 3-2](#) provides some examples of how identity and context information can be collected by the ISE architecture. This is not a comprehensive list. Let's take a look at each of these in some detail, starting with identity.

Identity can be gathered in multiple ways using the ISE solution. The following methods are available, in order of preference:

- **802.1X:** IEEE 802.1X is the standard for port-based network access control. The protocol uses Extensible Authentication Protocol (EAP), a flexible authentication framework defined in RFC 3748. The protocol defines three components in the authentication process:
- **Supplicant:** The agent on the device/PC that is used to access the network. The supplicant is either built in or added onto the operating system. It requests

authentication by the authenticator.

- **Authenticator:** The device that controls the status of a link; typically a wired switch or Wireless LAN Controller (WLC). EAP data is first encapsulated in EAP over LAN (EAPoL) frames between the supplicant and authenticator, then re-encapsulated between the authenticator and ISE using RADIUS.
- **Authentication server:** A backend server that authenticates the credentials provided by supplicants. For example, the WLC passes credentials from the supplicant via RADIUS to ISE for authentication.
- **VPN/RADIUS authentication:** By using ISE to authenticate your VPN clients, ISE then knows the identity of your VPN users. For example, Cisco ASA sends credentials from the VPN client via RADIUS to ISE for authentication.
- **Cisco ASA identity firewall:** Cisco ASA supports identity firewalling (IDFW). ASA can use ISE as an authentication server for this purpose. In this way, ISE learns the identity of all users passing through the IDFW-enabled Cisco ASA.
- **Web authentication:** Provides authentication via web page, usually via a URL redirect of the user's browser. The built-in Guest Server functionality of ISE provides this web portal service. For example, a user attaches to a wireless network without authentication—that is, open mode. The user's browser is then redirected to the login page hosted by ISE. ISE collects the credentials and performs the authentication.
- **MAC Authentication Bypass (MAB):** MAB relies on a MAC address for authentication. A MAC address is a globally unique identifier that is assigned to all network-attached devices, and therefore it is often referred to as a hardware or physical address. Because it is a globally unique identifier, it can be used in authentication. However, the ability to assign your own MAC address to your device means that, by itself, a MAC address is not a strong form of authentication. Later on, you will read about how ISE Profiler functionality with MAB provides you with a much more secure alternative to just MAB.

Let's look at a MAB example. A printer that does not support 802.1X attaches to the wired network. 802.1X authentication times out and MAB takes over. The switch sends the printer's MAC address to ISE. ISE then verifies the MAC address is allowed using its MAC address database or some external database containing a list of approved MAC addresses.

**Caution** MAB by itself is not an authentication mechanism. MAB, as its name implies, bypasses authentication.

- **TrustSec Security Group Tags:** ISE can use Security Group Tags for

authentication and authorization as well. An SGT is a value that is inserted into the client's data frames by a network device, such as a switch. This tag can be read by another network device receiving the data frame. It is then used to apply a security policy. For example, data frames with a `guest_user` tag are allowed to communicate only with nodes that have a `guest_internet` tag. ISE can statically map an IP address to an SGT. ISE collects and can distribute all of the IP-to-SGT mapping tables to the network nodes to enforce policy against.

- **Unauthenticated/authenticated guest access:** ISE includes a Guest Server functionality that provides a guest user splash page and, optionally, a user agreement page and/or a page that asks for information from the user such as their email address, name, company, and so forth. Guests are allowed access without providing identity information, which is usually termed unauthenticated guest access. This is what you would find at your local café that provides free Internet access. Guests are not authenticated by ISE, but, instead, any actions or information they provide are cataloged. In contrast, authenticated guest access allows Internet access to guests using temporary credentials that expire after a set time period. Guests are provided with these credentials through SMS, a printed handout, or other means. In almost all cases, the network access that a guest receives is severely restricted in comparison to what an authenticated employee receives, and usually allows only Internet access.

The most secure methods, which we recommend that you implement in your network, are 802.1X, VPN authentication, and ASA Identity Firewall logins. All of these techniques provide a robust and seamless user experience. If these are not available for use in specific scenarios within your own network, then employ MAB with ISE Profiler, use web authentication through a browser-based web portal page, or offer an unauthenticated or authenticated guest access option.

## ISE Authorization Rules

After authentication is complete, ISE performs its policy enforcement, also known as authorization. ISE can utilize dozens of policy attributes to each policy rule in a consolidated policy rule table for authorization. Here is a sampling of some of the more popular policy attributes available for use in ISE:

- Posture assessment results
- Active Directory group membership
- Active Directory user-based attributes (company name, department, address, job title, and so on)
- Location
- Access method (MAB, 802.1X, wired, wireless, and so on)

- Time and date
- Profiler match for device type
- If device has been registered with ISE or enrolled with an MDM
- Digital certificate information (commonly used to determine corporate vs. noncorporate assets)
- Hundreds of RADIUS attributes and values

The ISE policy rule table can be evaluated on a first-match basis (most common) or multiple-match basis. If there are no matches, then a default catch-all rule is enforced. [Figure 3-3](#) shows an example ISE authorization policy.

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
	Medical Devices Class D	If Medical-Devices-Type-D	then Medical_Class_D
	Cisco_IP_Phone	If Cisco-IP-Phone	then Cisco_IP_Phones AND SJC19_Cisco_IPPhones
	SJCM_Guest_Wired_Compliant	If (Wired_MAB AND Session:PostureStatus EQUALS Compliant )	then CWA-Access AND SJC19_Wired_Guest_devices
	SJCM_Guest_Unsupported_Access	If (Wired_MAB AND EndPoints:LogicalProfile EQUALS Unsupported )	then CWA-Access AND SJC19_Wired_Unsupported
	SJCM_Guest_Wired_unkn_own	If Wired_MAB	then CWA-Redirect_Wired

**Figure 3-3** Cisco ISE Authorization Policy Example

## Summary

Cisco ISE has revolutionized the way we protect our networks. The Cisco Secure Access architecture with ISE allows IT to seamlessly deploy a network access control and visibility solution across the entire network architecture using a robust centralized policy framework. ISE uses several innovative capabilities to ensure that the solution is as simple as possible to deploy and operationalize, and the solution is dynamic and can change your protection profile in real time based on live threats. A new approach is needed to regain control of and actively defend modern network access. ISE, with all of its many capabilities, provides that new approach.

## **Part II The Blueprint, Designing an ISE-Enabled Network**

[Chapter 4 The Building Blocks in an Identity Services Engine Design](#)

[Chapter 5 Making Sense of the ISE Deployment Design Options](#)

[Chapter 6 Quick Setup of an ISE Proof of Concept](#)

# Chapter 4 The Building Blocks in an Identity Services Engine Design

This chapter covers the following topics:

- ISE solution components
- ISE personas
- ISE licensing, requirements, and performance guidance
- ISE policy-based structure

Knowing how to properly design security solutions is what separates the professional from the amateur. Without a proper design, the eventual implementation will most likely be a disaster. One of the keys to success when designing a security solution is to first understand all of the pieces, or building blocks, you have to work with. After you understand the building blocks, you need to become skilled at manipulating them in ways that best fit your environment. This chapter focuses on the building blocks that are available with the ISE solution and architecture. The purpose and function of each building block are covered in this chapter. [Chapter 5, “Making Sense of the ISE Deployment Design Options,”](#) discusses your options for manipulating these building blocks.

## ISE Solution Components Explained

At a high level, the following are the three solution component groups that make up the ISE architecture:

- Infrastructure components
- Policy components
- Endpoint components

Each group has a distinct role to play in the ISE solution. Let's examine the roles and functions of these groups in more detail.

## Infrastructure Components

Infrastructure components are those devices that ISE will work with to create the secure access architecture. These are devices such as wireless controllers, switches, VPN concentrators, next-generation firewalls, authentication services such as Active Directory, and many others. The exact components you require will vary based on your ISE use cases and business objectives. Infrastructure components supported by Cisco ISE are numerous, with more added regularly. These network infrastructure devices include both Cisco-branded devices and non-Cisco devices. Full ISE functionality can

be achieved with non-Cisco branded devices starting in ISE 2.0; however, the Cisco-branded devices, predictably, provide more functionality with better integration into the ISE solution. Pay particular attention to the recommended code versions of the components to ensure the best experience.

**Note** For the latest support list of infrastructure components, refer to the most recent release of Cisco Identity Services Engine Network Component Compatibility at  
[http://www.cisco.com/en/US/products/ps11640/products\\_device\\_support\\_tables\\_list](http://www.cisco.com/en/US/products/ps11640/products_device_support_tables_list)

ISE will interact with infrastructure devices, such as switches, to perform various features. Unfortunately, not all infrastructure devices support the functionality necessary for a given ISE feature to work. Therefore, it is necessary to understand the most common functionality to look for support for on your devices. The following list contains the functionality that you want to ensure a device supports when you evaluate it:

- **MAC Authentication Bypass (MAB):** Using the MAC address of an endpoint that cannot authenticate itself to the network.
- **802.1X:** The IEEE standard for communicating identity credentials using Extensible Authentication Protocol (EAP) over LAN.
- **Web Authentication:** Authenticating users attempting network access via a web page. Web Authentication has two deployment modes:
  - **Central Web Authentication (CWA):** The most popular option, controlled by ISE.
  - **Local Web Authentication (LWA):** Performed by the switch or Wireless LAN Controller (WLC) and cannot perform CoA (described next), modify the port virtual LAN (VLAN), or support session ID.
- **Change of Authorization (CoA):** RADIUS attribute that ISE issues to an access device to force the session to be reauthenticated. CoA forms the backbone of the 802.1X ISE solution.
- **VLAN:** The Layer 2 broadcast domain that might be assigned to incoming devices.
- **Downloadable ACL (dACL):** An access control list that is sent from ISE to the access device to restrict the session.
- **Security Group Tag (SGT):** SGTs are the main component in the Cisco TrustSec architecture. ISE serves as the main policy engine for a TrustSec architecture and, as such, can assign and manipulate SGTs. ISE uses the various policy rules and context it has gathered to determine the appropriate SGT for a particular host and

user. This tag is then sent to a network device, which can then insert the SGT into the host's frames/packets or make enforcement decisions based on SGT-to-IP mappings.

- **Cisco IOS Device Sensor:** Enables profiling functionality built into the Cisco IOS Catalyst Switch or Cisco WLC hardware. This allows profiling to occur locally at the access device instead of centrally at an ISE node.

Now that you know the functionalities to look for in a network device, [Table 4-1](#) maps them to ISE features. This gives you a better idea of what device functionality is required to enable a given ISE feature.

Feature	Functionality
AAA	802.1X, MAB, VLAN assignment, dACL
Profiling	RADIUS CoA and profiling probes
BYOD	RADIUS CoA, URL redirection + SessionID
Guest	RADIUS CoA, URL redirection + SessionID, Local Web Auth
Posture	RADIUS CoA, URL redirection + SessionID
MDM	RADIUS CoA, URL redirection + SessionID
TrustSec	SGT classification

**Table 4-1** Feature to Functionality Mapping

[Table 4-2](#) shows a partial mapping of ISE supported devices to ISE features. It also provides recommended minimum OS levels for the device to be used with ISE.

Device	Recommended OS <sup>1</sup> Minimum OS <sup>3</sup>	AAA	Profiling	BYOD	Guest	Posture	MDM	TrustSec <sup>2</sup>
Cisco Access Switches								
IE 2000	IOS 15.2(2) E4	✓	✓	✓	✓	✓	✓	✓
IE 3000	IOS 15.0(2) EB	✓	✓	✓	✓	✓	✓	✓
CGS 2520	IOS 15.2(3)E3	✓	✓	✓	✓	✓	✓	✓
	IOS 15.2(3)E3	✓	✓	✓	✓	✓	✓	✓

Catalyst 2960 LAN Base	IOS 12.2.55-SE10	✓	✓	✓	✓	✓	✓	X
	IOS v12.2.(55)SE5	✓	✓	✓	✓	✓	✓	X
Catalyst 2960-C	IOS 15.2(2)E4	✓	✓	✓	✓	✓	✓	✓
Catalyst 3560-C	IOS 12.2.(55) EX3	✓	✓	✓	✓	✓	✓	✓
Catalyst 2960-Plus	IOS 15.2(2)E4	✓	✓	✓	✓	✓	✓	✓
Catalyst 2960-SF	IOS 15.0(2)SE7	✓	✓	✓	✓	✓	✓	X
Catalyst 2960-S	IOS 15.2(2)E4	✓	✓	✓	✓	✓	✓	✓
	IOS 12.2.(55)SE5	✓	✓	✓	✓	✓	✓	X
Catalyst 2960-XR	IOS 15.2(2)E4	✓	✓	✓	✓	✓	✓	✓
Catalyst 2960-X	IOS 15.0.2A-EX5	✓	✓	✓	✓	✓	✓	X
Catalyst 2960-CX	IOS 15.2(3)E1	✓	✓	✓	✓	✓	✓	✓
Catalyst 3560-CX	IOS 15.2(3)E	✓	✓	✓	✓	✓	✓	✓
Catalyst 3560G	IOS 12.2.(55)SE10	✓	✓	✓	✓	✓	✓	✓
Catalyst 3750G	IOS 12.2.(55)SE5	✓	✓	✓	✓	✓	✓	✓
Catalyst 3560V2	IOS 12.2.(55)SE10	✓	✓	✓	✓	✓	✓	✓
Catalyst 3750V2	IOS 12.2.(55)SE5	✓	✓	✓	✓	✓	✓	✓
Catalyst 3560-E	IOS 12.2.(55)SE10	✓	✓	✓	✓	✓	✓	✓
Catalyst 3750-E	IOS 12.2.(55)SE5	✓	✓	✓	✓	✓	✓	✓
Catalyst 3560-X	IOS 15.2(2)E4	✓	✓	✓	✓	✓	✓	✓
Catalyst 3750-X	IOS 12.2.(55)SE5	✓	✓	✓	✓	✓	✓	✓
Catalyst 3850	IOS-XE 3.6.4	✓	✓	✓	✓	✓	✓	✓
Catalyst 3650	IOS-XE 3.3.5.E	✓	✓	✓	✓	✓	✓	✓
Catalyst 4500-X	IOS-XE 3.6.4	✓	✓	✓	✓	✓	✓	✓
	IOS-XE 3.4.4 SG	✓	✓	✓	✓	✓	✓	✓
Catalyst 4500	IOS-XE 3.6.4	✓	✓	✓	✓	✓	✓	✓
Supervisor 7-E, 7L-E	IOS-XE 3.4.4 SG	✓	✓	✓	✓	✓	✓	✓
Catalyst 4500	IOS 15.2(2)E4	✓	✓	✓	✓	✓	✓	✓
Supervisor 6-E, 6L-E	IOS 15.2(2)E	✓	✓	✓	✓	✓	✓	✓

Catalyst 4500 Supervisor 8-E	IOS-XE 3.6.4	✓	✓	✓	✓	✓	✓	✓
	IOS-XE 3.3.2 XO	✓	✓	✓	✓	✓	✓	✓
Catalyst 6500-E (Supervisor 32)	IOS 12.2(33)SXJ10	✓	✓	✓	✓	✓	✓	✓
	IOS 12.2(33)SXI6	✓	✓	✓	✓	✓	✓	✓
Catalyst 6500-E (Supervisor 720)	IOS 15.1(2)SY7	✓	✓	✓	✓	✓	✓	✓
	IOS v12.2(33)SXI6	✓	✓	✓	✓	✓	✓	✓
Catalyst 6500-E (VS-S2T-10G)	IOS 152-1.SY1a	✓	✓	✓	✓	✓	✓	✓
	IOS 15.0(1)SY1	✓	✓	✓	✓	✓	✓	✓
Catalyst 6807-XL	IOS 152-1.SY1a	✓	✓	✓	✓	✓	✓	✓
Catalyst 6880-X (VS-S2T-10G)	IOS 15.0(1)SY1	✓	✓	✓	✓	✓	✓	✓
Cat 6848ia	IOS 152-1.SY1a	✓	✓	✓	✓	✓	✓	✓
	IOS 15.1(2) SY+	✓	✓	✓	✓	✓	✓	✓
Meraki MS Platforms	Latest Version	✓	✓	X	!	X	X	X
	Latest Version	✓	✓	X	!	X	X	X

#### Third-Party Access Switches

Avaya ERS 2526T	4.4	✓	!	X	X	X	X	X
	4.4	✓	!	X	X	X	X	X
Brocade ICX 6610	8.0.20	✓	✓	X	X	X	X	X
	8.0.20	✓	✓	X	X	X	X	X
HP H3C	5.20.99	✓	!	X	X	X	X	X
HP ProCurve	5.20.99	✓	!	X	X	X	X	X
HP ProCurve 2900	WB.15.18.0007	✓	✓	✓	✓	✓	✓	X
	WB.15.18.0007	✓	✓	✓	✓	✓	✓	X
Juniper EX3200	12.3R6.6	✓	!	X	X	X	X	X
	12.3R6.6	✓	!	X	X	X	X	X

#### Cisco Wireless LAN Controllers<sup>4</sup>

WLC 2100	AirOS 7.0.252.0	!	✓	X	!	X	X	X
	AirOS 7.0.116.0	!	✓	X	!	X	X	X

WLC 4400	AirOS 7.0.252.0	!	✓	X	!	X	X	X
	AirOS 7.0.116.0	!	✓	X	!	X	X	X
WLC 2500	AirOS 8.0.135.0	✓	✓	✓	✓	✓	✓	✓
	AirOS 7.2.103.0	!	✓	✓	✓	✓	✓	X
WLC 5508	AirOS 8.0.135.0	✓	✓	✓	✓	✓	✓	✓
	AirOS 7.0.116.0	!	✓	X	!	X	X	✓
WLC 5520	AirOS 8.1.131.0	✓	✓	✓	✓	✓	✓	✓
	AirOS 8.1.122.0	✓	✓	✓	✓	✓	✓	✓
WLC 7500	AirOS 8.0.135.0	✓	✓	✓	✓	✓	✓	X
	AirOS 7.2.103.0	!	✓	X	X	X	X	X
WLC 8510	AirOS 8.0.135.0	✓	✓	✓	✓	✓	✓	X
	AirOS 7.4.121.0	✓	✓	X	X	X	✓	X
WLC 8540	AirOS 8.1.131.0	✓	✓	✓	✓	✓	✓	X
	AirOS 8.1.122.0	✓	✓	✓	✓	✓	✓	X
vWLC	AirOS 8.0.135.0	✓	✓	✓	✓	✓	✓	X
	AirOS 7.4.121.0	✓	✓	✓	✓	✓	✓	X
WiSM1 6500	AirOS 7.0.252.0	!	✓	X	!	X	X	X
	AirOS 7.0.116.0	!	✓	X	!	X	X	X
WiSM2 6500	AirOS 8.0.135.0	✓	✓	✓	✓	✓	✓	✓
	AirOS 7.2.103.0	!	✓	✓	✓	✓	✓	✓
WLC 5760	IOS-XE 3.6.4	✓	✓	✓	✓	✓	✓	✓
	IOS-XE 3.3	✓	✓	✓	✓	✓	✓	✓
WLC for ISR (ISR2 ISM, SRE700, and SRE900)	AirOS 7.0.116.0	!	✓	X	!	X	X	X
	AirOS 7.0.116.0	!	✓	X	!	X	X	X
Meraki MR Platforms	Public Beta	✓	✓	✓	✓	✓	✓	X
	Latest Version	✓	!	X	!	X	X	X

#### Third-Party Wireless LAN Controllers

Aruba 3200XM	6.4	✓	✓	✓	✓	✓	✓	X
Aruba 650	6.4	✓	✓	✓	✓	✓	✓	X

Motorola RFS 4000	5.5	✓	✓	✓	✓	✓	✓	X
	5.5	✓	✓	✓	✓	✓	✓	X
HP 830	35073P5	✓	✓	✓	✓	✓	✓	X
	35073P5	✓	✓	✓	✓	✓	✓	X
Ruckus ZD1200	9.9.0.0	✓	✓	X	X	X	X	X
	9.9.0.0	✓	✓	X	X	X	X	X

**Table 4-2** ISE Supported Infrastructure Components—Partial List

✓—Fully supported

X—Not supported

!—Limited support, some functionalities are not supported

1. Recommended OS is the version tested for compatibility and stability.
2. For a complete ISE Compatibility list, see <http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-device-support-tables-list.html>.
3. Minimum OS is the version in which the features were introduced.
4. Cisco WLCs and Wireless Service Modules (WiSMs) do not support dACLs but support named ACLs. Autonomous AP deployments do not support endpoint posturing. Profiling services are supported for 802.1X-authenticated WLANs starting from WLC release 7.0.116.0 and for MAB-authenticated WLANs starting from WLC 7.2.110.0. FlexConnect, previously known as Hybrid Remote Edge Access Point (HREAP) mode, is supported with central authentication configuration deployment starting from WLC 7.2.110.0. For additional details regarding FlexConnect support, refer to the release notes for the applicable wireless controller platform.

**Table 4-3** lists the most capable and recommended infrastructure components for each category (at the time of writing).

Access Switches	Campus Core Switches	Wireless Controllers	Routers	Firewall
Catalyst 2960-plus	Catalyst 6500/6800 Supervisor VS-S2T-10G	WLC 5520	ISR 4000 Models	ASA 9.5+
Catalyst 3850/3650	Catalyst 4500 Supervisor 8-E	WLC 5760	ASR 1000 Models	Firepower NGFW 6.2+
Catalyst 4500x		WiSM 2 for Catalyst 6500	ISR Models 15.3.2T+	

**Table 4-3** Recommended Infrastructure Components

## Policy Components

The Cisco ISE solution provides wired, wireless, and VPN context-aware access control management in the following areas:

- Cisco ISE determines whether users are accessing the network on an authorized, policy-compliant device.
- Cisco ISE establishes user identity, location, and access history, which can be used for compliance and reporting.
- Cisco ISE assigns policy and services based on the host and user context. Examples are assigned user role, AD group, location, device type, etc.
- Cisco ISE grants authenticated users access to specific segments of the network, or specific applications and services, or both, based on authorization results.

Cisco ISE comprises the one and only policy component in the ISE solution. Having a single centralized policy engine signifies the power inherent in the ISE solution. Cisco ISE provides a flexible attribute-based access control solution that combines on a single platform authentication, authorization, and accounting (AAA); TACACS+; RADIUS; posture; profiling; certificate authority (CA) server; and guest management services. Administrators can centrally create and manage access control policies for users and endpoints in a consistent fashion, and gain end-to-end visibility into everything that is connected to the network. Cisco ISE automatically discovers and classifies endpoints, provides the right level of access based on identity and context, and provides the ability to enforce endpoint compliance by checking a device's posture. Cisco ISE also provides advanced enforcement capabilities, including TrustSec through the use of SGTs, Security Group Firewalls such as the Cisco ASA, and Security Group ACLs (SGACL). Finally, ISE provides a dynamic quarantine service that any outside device can use to tell ISE to quarantine a host on the network. ISE will instantiate the policy change, which is then enforced by a network access device such as a Wireless LAN Controller. The most popular use case is FirePOWER next-generation firewall/IPS (NGFW/NGIPS) telling ISE to quarantine a host it has an indication of compromise for.

## Endpoint Components

The network endpoints play an integral role in the total ISE solution. It is the endpoint that authenticates to ISE using 802.1X, MAB, EasyConnect, or web authentication. It is also from the endpoint that ISE gathers posture information to ensure a host is in compliance with security policies. Here are the recommended endpoint components (these are recommended, not required):

- **802.1X supplicant/agent:** A supplicant is basically just software that understands how to communicate via Extensible Authentication Protocol over LAN (EAPoL). There are many supplicants available for use. A supplicant is built into Windows and Mac OS X that is good enough for most ISE deployments. An open source Linux supplicant is also available. Supplicants are also available via Cisco AnyConnect and other third-party supplicant software agents. Cisco IP Phones, video equipment, printers, and many other devices now come with built-in supplicants. Additionally, nearly any device that is able to use Wi-Fi will have a native supplicant.
- **Cisco AnyConnect Compliance Module:** For Windows, Mac OS X, and Linux. Provides host posture information to ISE. This includes information such as whether antivirus is installed, running, and up to date, whether the operating system is fully patched, whether certain registry keys are present, and many more.

In many cases, you will have wired devices on your network that are not capable of performing 802.1X. This is typically the case with wired printers, IP Phones, badge readers, HVAC, and other industrial or biomedical endpoints. It is for this reason that ISE has a profiler service that can automate the process of properly identifying and authorizing devices that can't do it by themselves.

## ISE Personas

The ISE architecture has many personas to help it scale to large networks and large numbers of users and devices. Cisco ISE has a highly available and scalable architecture that supports standalone and distributed deployments. ISE standalone mode means that all the personas are on a single ISE appliance or a pair of ISE appliances. ISE distributed mode means that the personas are spread out and dedicated to just particular ISE appliances. ISE has three main personas. The persona or personas of an ISE node determine the services it provides. An ISE node can assume any or all of the following personas:

- **Administration:** Allows you to perform all administrative operations in a standalone or distributed Cisco ISE deployment. The Administration node provides a single pane of glass for management. It handles all system-related and policy-based configuration. In a distributed ISE deployment, you can have a single or a high-availability (HA) pair of nodes running the Administration persona. An HA pair is highly recommended. An ISE node dedicated to the administration persona is known as a Policy Administration Node (PAN).
- **Policy Service:** Provides network access, posture, guest access, client provisioning, web portals, and profiling services. This persona evaluates the policies and makes all the decisions. You can have more than one node assume this

persona. When a node is dedicated to the Policy Service persona, it is referred to as a Policy Service Node (PSN). Typically, a distributed deployment would have more than one PSN, and they might be geographically separated from each other.

- **Monitoring:** Enables Cisco ISE to function as the log collector and store log messages from all the Administration and Policy Service Nodes in your network. This persona provides advanced monitoring and troubleshooting tools that you can use to manage your network and resources effectively. A node with this persona aggregates and correlates the data that it collects to provide you with meaningful information in the form of reports. Cisco ISE allows you to have a maximum of two nodes with this persona, both of which can take on primary or secondary roles for high availability. Both the primary and secondary Monitoring nodes collect log messages. If the primary Monitoring node goes down, the secondary Monitoring node automatically becomes the primary Monitoring node. When an ISE node is dedicated to the Monitoring persona, it is referred to as a Monitoring & Troubleshooting Node (MnT).
- **pxGrid:** Cisco pxGrid is used to share the context-sensitive information from Cisco ISE session directory to other policy network systems such as Cisco NGFW or Stealthwatch. The pxGrid framework can also be used to exchange policy and configuration settings between nodes.

**Note** Due to the high performance requirements of the Monitoring persona, in midsize to large deployments, it is recommended that you dedicate a node to specifically run this persona.

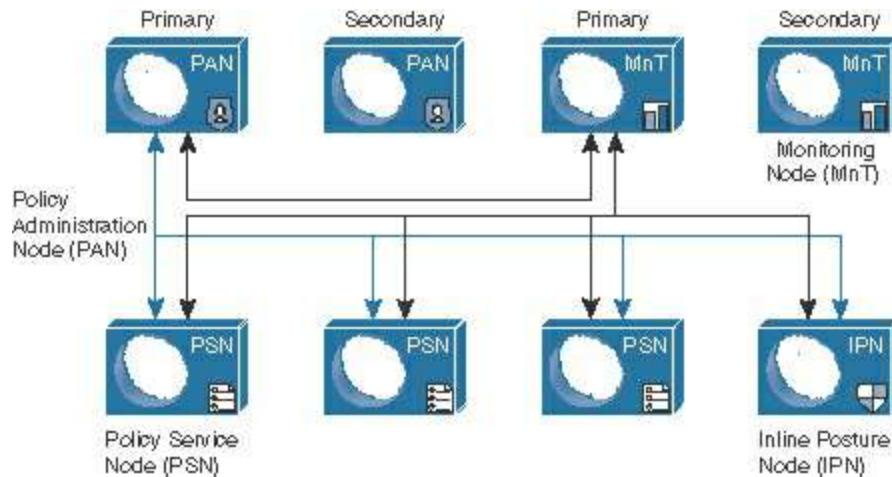
ISE also has two node types that determine the node's functions:

- ISE node
- Inline Posture Node (IPN)

**Note** The Inline Posture Node type has been deprecated in ISE 2.0+. It is described here for completeness but is no longer a recommended or viable deployment option. Use a Cisco ASA instead of an IPN.

Only the ISE node type can be configured with one or more of the previously discussed personas. The IPN must be a dedicated node and cannot assume any of the personas. As an IPN, it is logically or physically inline in the network. Typically, this means it is behind a VPN headend device or behind a non-Cisco WLC that cannot support CoA or another required feature. While inline, this node type can block traffic and apply other network policies as per the ISE policy rule table.

[Figure 4-1](#) provides an idea of how these personas and node types look logically. Only the primary connections are shown, for simplicity.



**Figure 4-1** ISE Persona and Node Types

## ISE Licensing, Requirements, and Performance

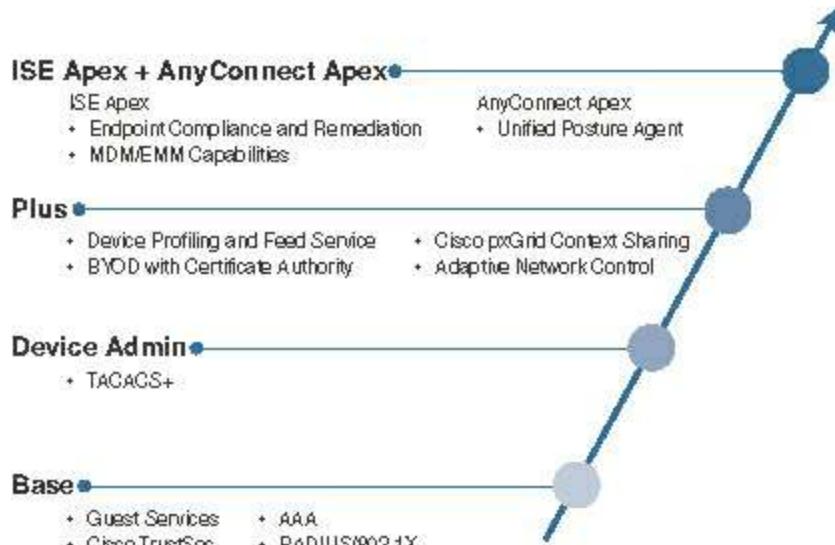
This section discusses the centralized ISE licensing model, hardware and virtual machine requirements, and the published performance of an ISE node.

### ISE Licensing

Identity Services Engine licensing is fairly straightforward. To maximize flexibility for customers, licensing in Cisco ISE is supplied in different packages as Base, Plus, Apex, Device Administration, and AnyConnect Apex. Start with the Base license, then deploy other licenses on top as needed.

Cisco ISE allows the total number of Plus and Apex licenses to be equal to or less than the total number of Base licenses. Apex and Plus licenses can be installed independently without any restriction on the number of Apex versus Plus licenses. Cisco ISE licenses are based on the number of concurrent endpoints with active network connections, whereas AnyConnect Apex licenses are on a per-user basis. The AnyConnect Apex license count can exceed the Cisco ISE Base license count.

[Figure 4-2](#) depicts the ISE license types and functionalities.



**Figure 4-2 ISE Licensing**

The licenses shown in [Figure 4-2](#) would additionally include a user count and term. For example, L-ISE-PLUS3Y-100= means a 100-user advanced license that is valid for 3 years. To assist you in understanding what licenses you may need for your deployment, refer to [Figure 4-3](#).

Benefit	Use case	Base Perpetual				Device Admin* Perpetual	Plus Term (1,3,5 year)				ISE Apex + AnyConnect Apex Term (1,3,5 year)			
		RADIUS / 802.1x	AAA	TrustSec security group tagging	Guest services		Rapid threat containment	ANC/EPS	Device profiling and feed service	BYOD with CA	pxGrid context sharing	MDM / EMM	Threat-Centric NAC	Posture (endpoint compliance and remediation)
Control all access from one place	Guest Provide unique guest permissions to visitors.	●	●		●									
	Secure access Control user access and ensure device authentication.	●	●	●										
	Device Admin Differentiate access for device administrators.					●								
BYOD Seamlessly onboard devices with the right access.	BYOD Seamlessly onboard devices with the right access.	●	●	●					●	●				
	Visibility See when, where, and why users are on your network.	●	●	●						●				
	Integration Share information with other products.	●	●	●					●		●			
Compliance Ensure that endpoints meet network standards.	Compliance Ensure that endpoints meet network standards.	●	●	●								●		●
	Segmentation Limit exposure with pre-defined access segmentation.	●	●	●					●	●				
	Containment Reduce risk with rapid threat containment.	●	●	●				●	●	●				
Stop threats from getting in and spreading	Prevention Prevent breaches at the endpoint level.	●	●	●										●

**Figure 4-3 ISE Licensing Use Case Mapping: Features Included by License Type**

## ISE Requirements

Cisco ISE comes in two form factors: physical appliance and virtual appliance. The physical appliance comes with the server hardware. The virtual appliance comes as a VMware virtual appliance package that you can load onto a VMware ESX server. ISE virtual is also available as a KVM appliance package. At the time of writing, the physical appliance comes in two form factors: small and large.

Given that the physical appliances will be upgraded once or twice a year by Cisco, be sure to check [Cisco.com](http://Cisco.com) for the latest specifications.

For the virtual appliance, the specifications for the virtual machine (VM) host should be sized at or above the specifications for the physical appliance you are trying to match. For example, if you want to have performance similar to that of a Medium physical appliance, then you would build a VM with the specifications of a Medium appliance. Hard drives with 10-K or higher RPM are highly recommended for ISE VM. VMware VMotion and cloning are only supported in ISE version 1.2 or later. It is possible to decrease the HD requirements in certain situations. Here are the ISE persona minimum disk space requirements for production VM deployments:

- Standalone ISE: 600 GB
- Administration: 200 GB
- Monitoring: 600 GB
- Administration and Monitoring: 600 GB
- Administration, Monitoring, and Policy Service: 600 GB
- Policy Service: 100 GB (200 GB strongly recommended)

**Note** Do not use Intel Hyper-Threading Technology for the ISE VM. Ensure that the correct number of cores are allocated per VM; it is the cores that matter in the configuration.

**Note** ISE version 1.2 (and later) moved to a 64-bit OS, thus enabling it to address more than 4 GB of RAM memory.

## ISE Performance

ISE performance is dependent on several factors and, unfortunately, is not a straightforward or precise calculation. It is dependent on the node type, persona(s), policy complexity, bandwidth requirements, and several other variables. [Figure 4-4](#) and [Figure 4-5](#) dissect the different performance specs for ISE. Use typical design guidance when using performance metrics: never exceed 80 percent of stated capacity, and design for 50 percent or less out of the gate. This allows you to build growth into the architecture and ensures that you have a healthy buffer in case your environment doesn't mirror the performance metrics tested and documented by Cisco.

Deployment Model	Platform	Max Active Sessions per Deployment	Max # Dedicated PSNs
Standalone (all personas on same node)  (2 nodes redundant)	3415	5,000	0
	3495	10,000	0
	3515	7,500	0
	3595	20,000	0
Admin + MnT on same node; Dedicated PSN  (Minimum 4 nodes redundant)	3415 as Admin+MNT	5,000	5
	3495 as Admin+MNT	10,000	5
	3515 as Admin+MNT	7,500	5
	3595 as Admin+MNT	20,000	5
Dedicated Admin and MnT nodes  (Minimum 6 nodes redundant)	3495 as Admin and MNT	250,000	40
	3595 as Admin and MNT	500,000	50
Max Active Sessions != Max Endpoints; ISE 2.1 supports 1.5M Endpoints in DB			

Figure 4-4 ISE 2.1 Max Active Session Counts by Deployment Model and Platform

Scaling per PSN	Platform	Max Concurrent Sessions per PSN
Dedicated Policy nodes  (Max Sessions Gated by Deployment Maximums)	SNS-3415	5,000
	SNS-3495	20,000
	SNS-3515	7,500
	SNS-3595	40,000

Figure 4-5 ISE 2.1 Max Concurrent Session Counts by Platform

ISE 2.1 adds increased scalability. Here are the new specs:

- Max concurrent active sessions per deployment = **500k** (up from 250k)  
Requires PAN and MnT nodes to be 3595 or VM equivalent
- Max internal endpoints = **1.5M** (up from 1M)
- Max internal users = **300k** (up from 25k)
- Max network access devices = **100k** (up from 30k)
- Max PSNs per deployment = **50** (up from 40)

## ISE Policy-Based Structure Explained

The Identity Services Engine solution relies on a policy-driven rule set to make its decisions. ISE has several different policy types that are all consolidated into a policy set. A policy set is a grouping of several different policy rules from both authentication and authorization policies. You can then have multiple policy sets that are processed in order, top down. Finally, you can have global exception rules across the entire ISE deployment. The following policy rule types can be called within an ISE policy set:

- Authentication policy
- Authorization policy
- Profiling policy
- Device posture policy

- Client provisioning policy
- Security group access policy
- Guest policy

Each policy type will be explained in the configuration section of this book. To enable the policy set view, choose **Administration > System > Settings > Policy** and select **Policy Set**. Given the power of policy sets, it is a best practice to enable this feature.

For now, just realize that, as part of preparing for your ISE deployment, you have these policy types at your disposal. [Figure 4-6](#) shows a simple example of a policy set.

The screenshot shows the Cisco ISE Policy Sets interface. On the left, there's a sidebar titled "Policy Sets" with a search bar and icons for creating, deleting, and saving policy sets. Below the search bar is a tree view of policy sets: "Summary of Policies" (selected), "Global Exceptions", "Wireless-Guest" (selected), "Guest Users", "ATS" (selected), and "Default". At the bottom of the sidebar are "Save Order" and "Reset Order" buttons. The main right pane is titled "Access Policy Sets" and contains a table with three rows:

Status	Name	Description	Conditions
<input checked="" type="checkbox"/>	Wireless-Guest	Guest Users	WLC_Web_Authentication
<input checked="" type="checkbox"/>	ATS	Advanced Threat Security Team	DEVICE:Device Type STARTS WITH Device Type#All Device Types
<input checked="" type="checkbox"/>	Default	Default Policy Set	

**Figure 4-6** ISE Policy Set Example

In the left pane of [Figure 4-6](#), you can see the policy sets. These policy sets are processed from the top down, beginning with the Global Exceptions policy set. Within each set you will see authentication policies and authorization policies that make up the set. These policy rules are also processed from the top down, thus making the ordering of rules very important. Always put the most used rules at the top.

## Summary

This chapter provided a baseline to understand all of the building blocks you have to work with inside of ISE. With this knowledge, you can begin to understand your ISE options for the following:

- ISE solution components
- ISE personas
- ISE licensing, requirements, and performance
- ISE policy structure

Next, [Chapter 5](#) explores all of the details of the various deployment options for ISE.

# Chapter 5 Making Sense of the ISE Deployment Design Options

This chapter covers the following topics:

- Centralized versus distributed deployment

Cisco Identity Services Engine supports two different design and deployment options. This chapter explains the options with the goal of helping you to select the best one for your environment. The deployment options are broken down into two main topics to consider: centralized and distributed. This chapter examines these and other ISE design options.

[Chapter 4](#), “[The Building Blocks in an Identity Services Engine Design](#),” already discussed the operation of ISE standalone mode versus distributed mode. For standalone mode, the design of the deployment is very simple: you locate the standalone node at the best network location for its job. This is typically in a data center but at a minimum needs to be somewhere that has reliable environmental conditions and reliable connectivity to the network access devices (NAD), external identity servers, and other critical services. A failed ISE standalone node is something to be avoided at all costs. As discussed in [Chapter 4](#), all ISE node types, such as Administration, Monitoring, and Policy Service, can be made highly available. It is highly recommended to always deploy your standalone node and distributed nodes using high availability. When ISE is deployed in standalone mode, with all node types running on one ISE appliance, you can deploy a secondary standalone ISE node to act as a backup to the original primary server and all of its running services/nodes. The node types are broken out from standalone mode to distributed mode when scaling beyond 20,000 simultaneous endpoints on a Cisco SNS 3595 appliance (less when on smaller appliance models).

When deploying Cisco ISE in a distributed deployment with high availability, it is important to know how to configure each node persona’s high availability. Both the Admin and Monitoring nodes work in a primary/standby configuration whereby one active node does all of the work until it fails, at which time the other, backup node, takes over. The Policy Service Node (PSN) is different in that it is made resilient either by load balancing between several PSNs or by configuring your NADs with a list of available PSNs to choose from. In the latter case, if the NAD detects a failure of a PSN, it will choose the next one in its list.

## Centralized Versus Distributed Deployment

A centralized deployment is one in which all of your ISE nodes are physically located in one location, usually adjacent to each other at Layer 2. All local and any remote sites connect to the centrally deployed ISE nodes.

A distributed deployment is one in which your ISE PSNs are physically and strategically dispersed in multiple locations. Your Administration and Monitoring nodes remain at your most robust central network location, and only your PSNs are distributed.

In either deployment mode, your configuration, monitoring, and all ISE admin functions have a consolidated, single-pane-of-glass look and feel for the administrators. Also, both deployment methods support the ISE maximum number of concurrent endpoints in a single ISE deployment, which in version 2.2 is 500,000 endpoints.

**Note** The final deployment configuration doesn't need to be determined at the outset of your ISE deployment. In almost all cases, you should do your initial ISE deployment, also known as a proof of concept, in centralized mode.

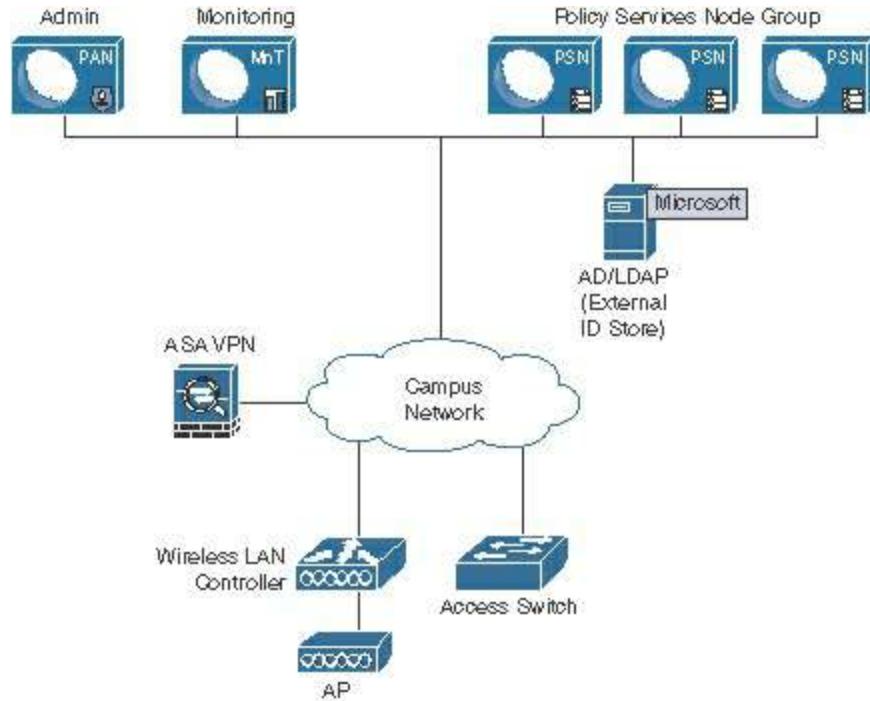
Whenever you have two or more PSNs that are Layer 2 adjacent, you should use the Node Group function in ISE, which enables you to not only load-balance between multiple PSNs within the same group but also detect a failure of a PSN within the group. It is recommended that you do not exceed a maximum of four PSNs per node group. All PSNs in a group exchange multicast update packets to detect a failure of a server within the group. If a PSN fails, then the group sends a Change of Authorization (CoA) to the NAD for any sessions in the pending state. A session is in the pending state if it has been authorized but posture assessment is not yet complete. The CoA forces the client to reauthenticate to a new available ISE PSN.

Node groups and high availability are both covered in greater detail in [Chapter 18, “Setting Up a Distributed ISE Deployment.”](#)

## Centralized Deployment

Centralized deployment is the most popular method with which to start an ISE deployment. In a centralized deployment, all ISE nodes are located in the same physical location, with LAN-like bandwidth and latency expected between all ISE nodes.

Centralized deployment should be used for small, medium-sized, or large deployments that have a single campus location and/or small remote sites. Centralized deployment mode also works best if you have remote sites that already connect to a common central site for the vast majority of their services. [Figure 5-1](#) shows an example diagram of a centralized ISE deployment.



**Figure 5-1 ISE Centralized Deployment**

Deploying ISE in a campus or other area where all clients and ISE nodes are connected via LAN transport is the ideal situation for a centralized ISE deployment. However, this doesn't exclude you from using this method when you have remote sites that are not using a LAN-like transport, especially if those sites have a small number of clients at each. The following are things to consider for centralized deployment with remote sites and clients:

- Number of clients at the remote sites
- Bandwidth available between the client NADs and the ISE PSN
- Reliability of WAN links/circuits between client NADs and ISE nodes
- Resiliency requirements if the WAN goes down between the client NADs and ISE
- Whether quality of service (QoS) is deployed on the networks between the client NADs and ISE

Calculating exact ISE bandwidth requirements is not a simple or straightforward exercise. There are just too many variables in the mix for that to be the case. However, there are some general guidelines available for estimating your bandwidth needs. The minimum bandwidth required between a client and its PSN with posture assessment enabled is 128 bps per endpoint. You can, and should, use QoS to ensure the ISE traffic is prioritized appropriately over the WAN. [Table 5-1](#) provides some general guidance on bandwidth requirements.

<b>Process</b>	<b>Flow</b>	<b>Bandwidth Guidance</b>
Min. BW client to PSN with posture	Client to PSN	128 bps per endpoint
AAA RADIUS functions	NAD to PSN	Very low
Posture no remediation	Client to PSN	Low
Web Authentication/Guest Services	Client to PSN	Low (be sure to keep any custom web page graphics to small sizes)
Posture remediation	Client to remediation sources	Depends on size and location of remediation files
Profiling with DHCP, SNMP, DNS, HTTP	NAD to PSN	Low
Profiling with NetFlow, SPAN <sup>1</sup>	NAD to PSN	Medium to very high depending on the capture filters and amount of NetFlow traffic
Syslog monitoring traffic	NAD to monitoring node	Low to medium when set to informational and no logging of ACLs
NAC client install or upgrade	Client to PSN	Medium (client software is approx. 30 Mb in size); use QoS to rate-limit

1. SPAN = Switched Port Analyzer.

**Table 5-1** Centralized ISE Deployment Bandwidth Guidance

For centralized deployment to work over a WAN, you must have highly reliable WAN links. To ensure your critical ISE communication is successful end to end every time, use QoS. At a minimum, you should use QoS to prioritize all RADIUS and TACACS+ communications between NADs and ISE PSNs such that other traffic will not saturate the links to the point that ISE traffic is delayed or dropped, causing authentication and posturing issues for those active clients.

Centralized mode depends on the availability of communications between clients, NADs, and ISE nodes at all times. If this communication is broken temporarily, Cisco ISE does have some resiliency features that can ensure a working solution during the failure. Having robust WAN redundancy in your network greatly reduces the risk of this problem. During an outage, your currently connected clients typically are not impacted, but new clients coming on are impacted. It is up to the local NAD (switch or WLC) to determine how to treat new devices connecting during an ISE outage. Catalyst switches

support several failure scenario solutions: fail open, fail closed, or fail to a specific VLAN or local authentication service. This is covered in more detail in [Chapter 11](#), “[Bootstrapping Network Access Devices](#).”

## Distributed Deployment

Even though the centralized deployment method is generally recommended, there are some use cases where a distributed deployment works better. Here are some examples:

- You have remote sites with unreliable or low-bandwidth WAN circuits.
- You have a local authentication service at your remote sites, such as a local Active Directory server.
- You have sizable or critical remote sites. You need to improve remote site resiliency against a WAN outage.
- You have regional or geographically disperse data centers that aggregate WAN connections.
- You want to increase ISE resiliency by distributing ISE nodes across two data centers.
- You need the ISE PSN profiler to be local to the clients it is serving. This is typically for cases in which you are forced to use SPAN or NetFlow probes to profile clients. Deploying a PSN remotely eliminates the potentially large WAN bandwidth requirements.

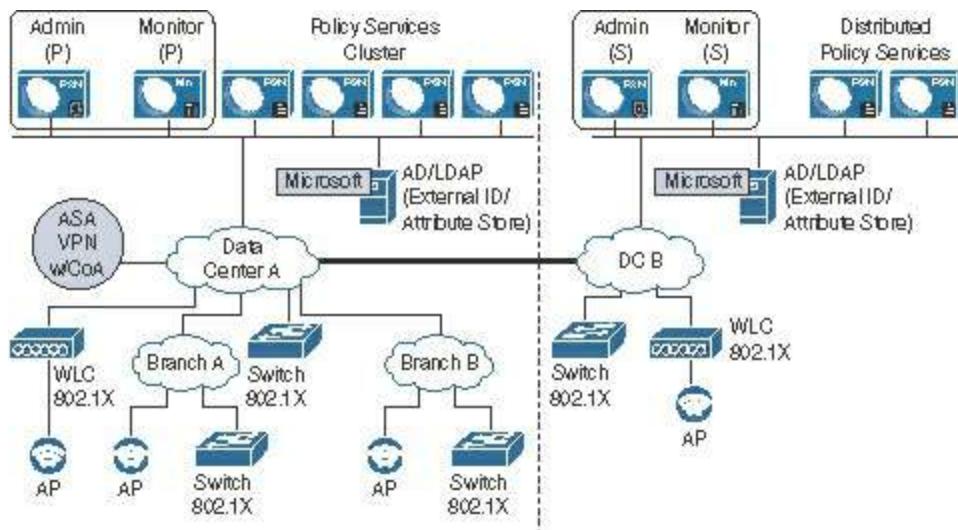
**Note** You must use ISE version 1.2 or greater for a distributed deployment. ISE version 2.1 or later is recommended.

Typically, in a distributed ISE deployment, the Admin and Monitoring nodes are both centralized, while the PSNs are geographically dispersed. Also popular is to split your Admin and PSNs between two data centers/sites. This allows you to survive a data center outage at a single site.

**Note** The nodes in an Admin HA pair or Monitoring HA pair do not need to be Layer 2 adjacent; they can be multiple Layer 3 hops away from each other. However, resilient, low-latency, high-bandwidth links must be available between the primary and secondary nodes.

**Note** For ISE 2.1 and later, the maximum latency between the Admin node and any other ISE node, including secondary Admin, MnT, and PSN, is 300 ms. Maximum latency is 200 ms for ISE 2.0 or earlier. Low latency is most critical between PSNs and the primary Policy Administration Node (PAN).

In this model, you are placing your PSNs closer to both your NADs and your clients. This results in better performance and a more scalable ISE deployment, especially when working with high-latency, bandwidth-constrained, or unreliable WAN connections. [Figure 5-2](#) depicts an example ISE distributed deployment model.



**Figure 5-2** ISE Distributed Deployment

In a distributed deployment such as the one shown in [Figure 5-2](#), the databases between all of the ISE nodes are automatically synchronized. The primary Admin node is the source of all database replication traffic. Its job is to replicate the database to all other ISE nodes, including monitoring, policy services, and a secondary Admin node. Upon registering a secondary node (that is, as any node that is not the Admin primary) with the primary Admin node, a database sync connection is automatically set up between the two nodes. A full copy of the database is kept up to date in near real time on all nodes by the primary Admin node. This includes configuration changes. You can view the status of replication from the Deployment pages of the ISE Administrative user interface.

In a distributed deployment, having adequate bandwidth is most critical between

- PSNs and Primary PAN (database replication)
- PSNs and MnT (audit logging)

Database synchronization also happens in a centralized deployment, but because these nodes have LAN connectivity, you don't need to worry about bandwidth. Over a WAN,

however, you do need to consider the ramifications of database replications, especially as they pertain to latency and bandwidth requirements. To this end, Cisco has developed a bandwidth and latency calculator to help you determine the correct specifications required. Bandwidth required for RADIUS traffic is not included. The calculator is focused on inter-ISE node bandwidth requirements. The calculator can be accessed at <https://communities.cisco.com/docs/DOC-64317>. In lieu of the calculator, [Table 5-2](#) provides some general guidance.

Description	Requirement
Minimum bandwidth between Monitoring and Policy Service nodes	1 Mbps
Minimum bandwidth between Monitoring and Admin nodes	256 Kbps
Minimum bandwidth between Client and Policy Service node with posture	128 bps per endpoint
Minimum bandwidth between Monitoring and Monitoring nodes (redundant)	256 Kbps
Minimum bandwidth between Admin and Policy Service nodes (redundant admin)	256 Kbps

**Table 5-2** Minimum Bandwidth Requirements

[Table 5-2](#) lists the absolute minimum, so be sure to scale up as required. Additionally, all database sync and replication traffic should be given QoS priority just below RADIUS, voice, and video but above normal traffic types.

A partial database replication is triggered whenever a PSN sends a database update to the primary Admin node. The primary Admin node then initiates an update replication to all other ISE nodes. When deploying ISE distributed PSNs, note that AAA/RADIUS and posture-assessment features cause very minimal database replication traffic. ISE profiling and Guest Services, however, can cause lots of database replication traffic due to their frequent database writes and updates. As a result, lower latency and higher bandwidth WAN links are necessary when using these services within your ISE deployment.

**Note** NetFlow and SPAN-based collection methods are not supported for distributed deployments due to the potentially high volume of data replication required by these methods.

In the event of a loss of connectivity to the Admin node, distributed PSNs will continue to provide full authentication and authorization services to their local NADs and endpoints. This assumes that the cut-off PSN still has access to its AAA resources. Note

that the following disruptions occur on the PSN until the Admin node is brought back online:

- Cannot authenticate new sponsored or self-service Guest user accounts.
- Cannot profile new endpoints.
- Logging is interrupted if connectivity between the PSN and Monitoring node is also lost.
- Automatic client provisioning services will not function.

## Summary

This chapter examined the centralized deployment mode and the distributed deployment mode. It suggested that in most cases, the centralized mode should be used. However, it also presented use cases in which the distributed mode is preferable. See [Chapter 18](#) for details on the configuration when distributing the ISE personas.

# Chapter 6 Quick Setup of an ISE Proof of Concept

This chapter covers the following topics:

- Deploy ISE for wireless in 15 minutes
- Deploy ISE to gain visibility in 15 minutes

Many of us tech geeks learn best by doing and experiencing things hands-on. The barrier to this is usually time and effort to set everything up. Well, that barrier has been drastically lowered for you with ISE 2.2+. Starting with version 2.2, ISE includes some very powerful configuration wizards that enable you to set up an ISE proof of value in your development environment in just a couple hours. The idea is to be able to set up ISE quickly and easily, run through its functionality, and prove out ISE's value for your organization in a real environment. This chapter steps you through how to get ISE up and running from scratch for a few common use cases very quickly. The Cisco ISE team has been working to make the deployment of ISE quicker and easier release to release so look for even more enhancements in future versions.

## Deploy ISE for Wireless in 15 Minutes

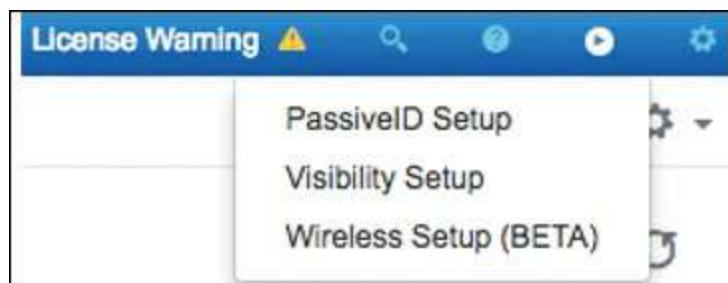
ISE 2.2 added a new setup wizard called Wireless Setup. The wizard can configure both the Identity Services Engine and a Cisco Wireless LAN Controller (WLC) plus connect ISE to Active Directory. This section walks you through using the Wireless Setup Wizard to quickly deploy ISE with the following services configured:

- **Guest wireless access:** This functionality provides the full guest wireless portal experience, including creating customized portal pages. Guest self-registration is the configuration demonstrated in this section, but you can also select a hotspot or sponsored guest configuration instead using the wizard. Self-registration enables your guests to fill out a simple information form and create their own accounts. You control how long those accounts remain active; the default is 24 hours. The wizard sets up both ISE and the Cisco WLC.
- **Secure wireless access with WPA2, 802.1X, and PEAP authentication:** This functionality provides wireless access to your corporate users. The most popular wireless settings for a typical business protected Wi-Fi network will be utilized, including WPA2, 802.1X, PEAP, and Active Directory authentication of users. The wizard sets up ISE and the Cisco WLC and connects ISE to Active Directory for user authentication.
- **Bring Your Own Device (BYOD) wireless access:** This functionality provides your employees with the option to securely provision and use their own wireless devices on either your corporate network or a specific BYOD network you specify. The employees will be able to enroll and remove their own devices from a

customized device portal.

## Wireless Setup Wizard Configuration

Once you have the ISE appliance bootstrapped and on the network, log in to the ISE GUI at <https://<ISE IP>/admin>. If this is your first time logging in, you will be presented with the option to run the Wireless Setup Wizard; select it. If this is not your first time logging in, you can find the wizard in the upper-right corner of the GUI under the **Play** icon, as shown in [Figure 6-1](#).



**Figure 6-1** Wireless Setup Wizard Startup

After you launch the wizard, you are presented with the three major configuration options. See [Figure 6-2](#) for details. You can choose to run one, two, or all three of these in any order.

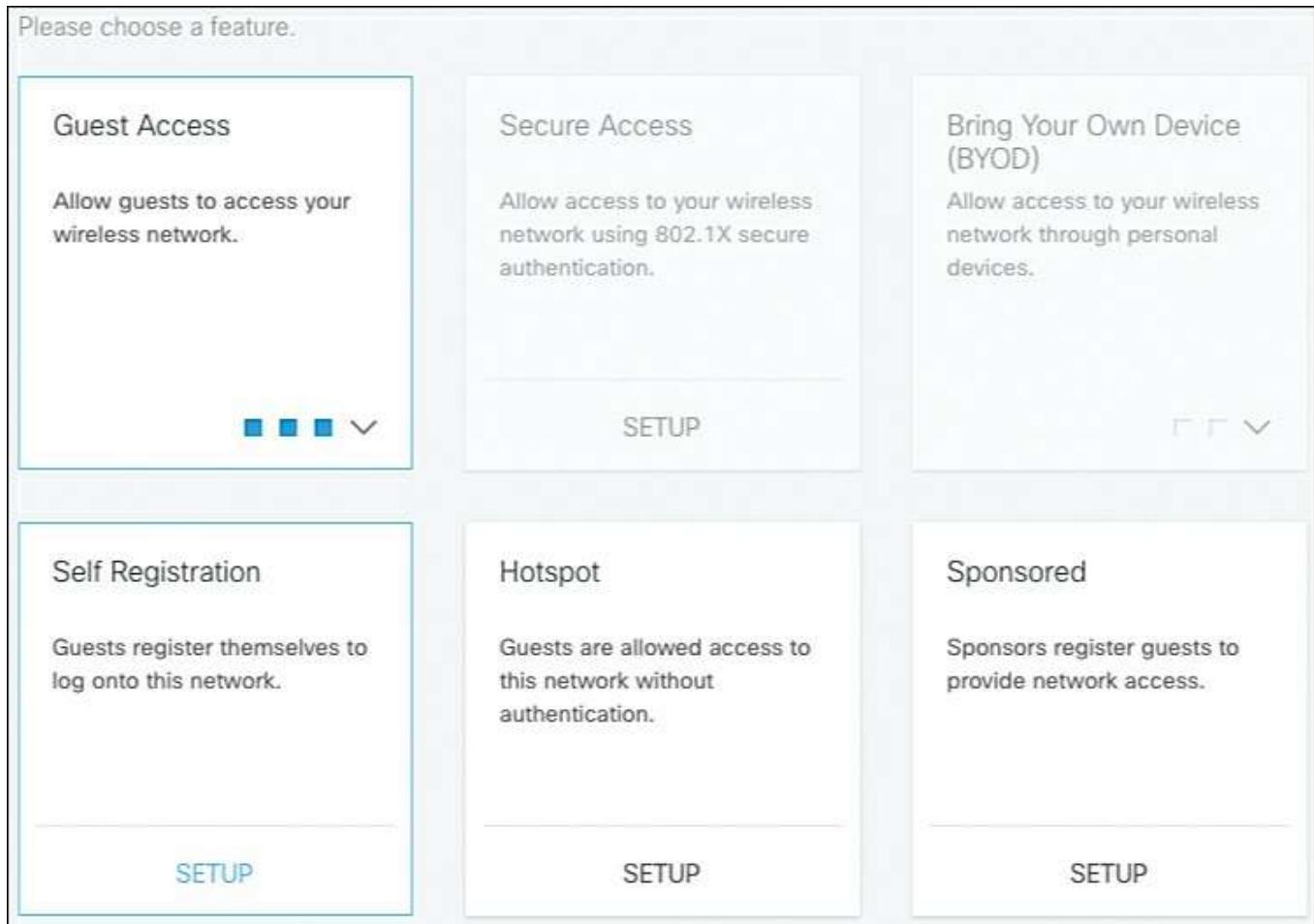
A screenshot of the "Wireless Setup Wizard Home Page". The page has a light gray background with a white header section. The header contains the text "What can we help you set up today?" and a note: "Please choose a feature. ISE Wireless Setup is beta software - do not use in production networks." Below the header, there are three main options: "Guest Access", "Secure Access", and "Bring Your Own Device (BYOD)". Each option has a brief description and a small icon. At the bottom center of the page is a large button labeled "SETUP".

**Figure 6-2** Wireless Setup Wizard Home Page

**Note** At the time of writing, this wizard is in beta. By the time you read this, it likely won't still be in beta. Regardless, heed the warnings and disclaimers in your version of the ISE wizard.

As illustrated in [Figure 6-3](#), the Guest Access tile has three different suboptions to choose from: Self Registration, Hotspot, and Sponsored. For purposes of this example, choose **Self Registration**.

**Note** All examples in this chapter assume that your WLC is not already configured with wireless settings. If your WLC does have SSIDs, VLANs, and so forth already configured, that is okay too. The wizard will display your existing values for selection or allow you to create new ones.



**Figure 6-3** Wireless Setup Wizard Guest Types

## Guest Self-Registration Wizard

These steps show you how to configure the guest self-registration service. This enables guests to register themselves, via a web portal, to log in to a network.

**Step 1.** Enter the information for your wireless controller, as shown in [Figure 6-4](#). Best practice for shared secrets is to use at least a 16-character password. Click **Register**.

SETUP | SELF REGISTRATION

Wireless LAN Controller

1 Register a Wireless LAN Controller.

2 WLC IP ADDRESS  
10.1.100.212

3 USERNAME  
admin

4 PASSWORD  
.....

5 SHARED SECRET  
.....|

**Register**

The screenshot shows a user interface for 'Self Registration'. At the top, it says 'SETUP | SELF REGISTRATION'. Below that, it says 'Wireless LAN Controller'. A large blue box highlights 'Step 1'. Inside the box, it says 'Register a Wireless LAN Controller.' followed by a numbered list from 1 to 5. Step 1 is 'WLC IP ADDRESS' with the value '10.1.100.212'. Step 2 is 'USERNAME' with the value 'admin'. Step 3 is 'PASSWORD' with several dots. Step 4 is 'SHARED SECRET' with several dots and a cursor. At the bottom right is a green 'Register' button.

**Figure 6-4** Self-Registration Step 1

**Step 2.** Configure the wireless SSID and the network interface or VLAN that you want your guest users to be dropped onto. Next configure the account duration and the URL redirect behavior for after guest login completes (see [Figure 6-5](#)). Click **Add**.

SETUP | SELF REGISTRATION

Wireless Network

1 Add a Wireless network.

2 WIRELESS NETWORK NAME (SSID)  
corp\_guest

3 DEFAULT WLC INTERFACE (VLAN)  
management

4 ACCOUNT ACCESS DURATION  
1 day

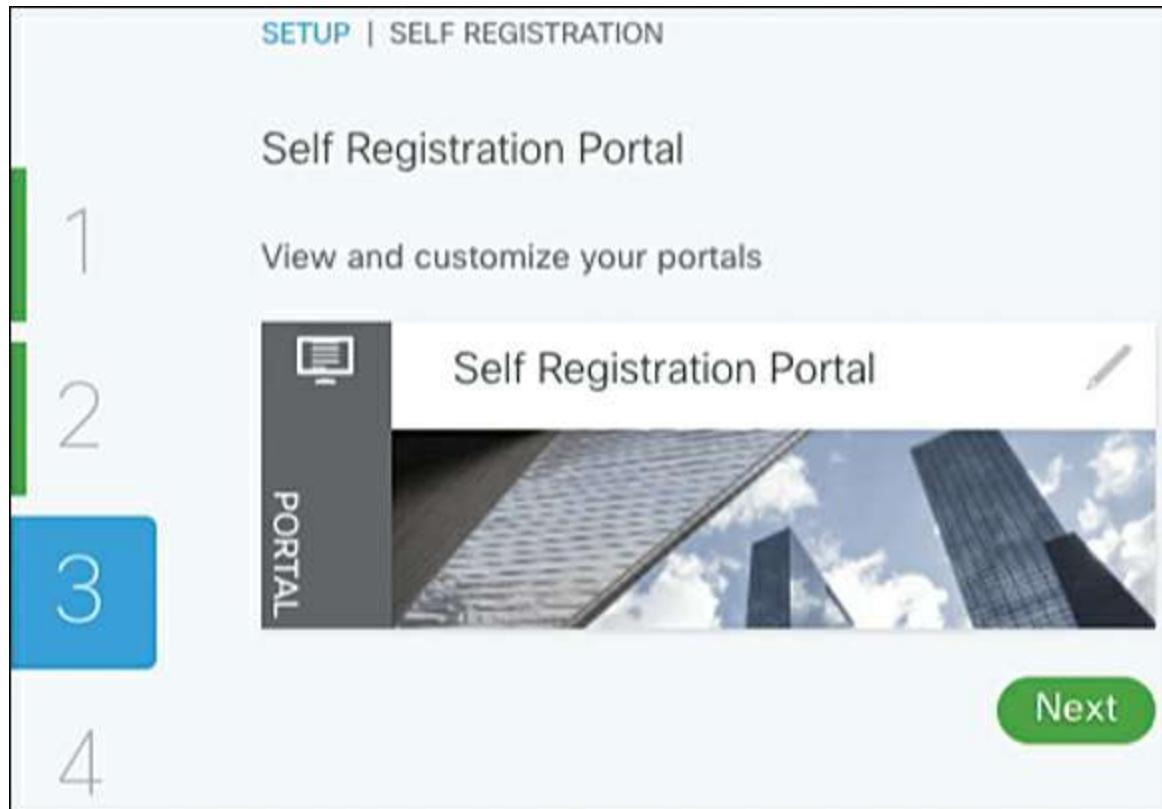
POST LOGIN REDIRECT  
Redirect to original URL

Add

This screenshot shows the 'Wireless Network' configuration page. It includes four numbered steps: Step 1 (Add a Wireless network), Step 2 (WIRELESS NETWORK NAME (SSID) set to 'corp\_guest'), Step 3 (DEFAULT WLC INTERFACE (VLAN) set to 'management'), and Step 4 (ACCOUNT ACCESS DURATION set to '1 day'). Step 2 is highlighted with a blue background. A green 'Add' button is located at the bottom right. The top navigation bar says 'SETUP | SELF REGISTRATION'.

**Figure 6-5** Self-Registration Step 2

**Step 3.** Customize the guest portal pages. From the screen displayed in [Figure 6-6](#), click the pencil icon to edit your portal pages.



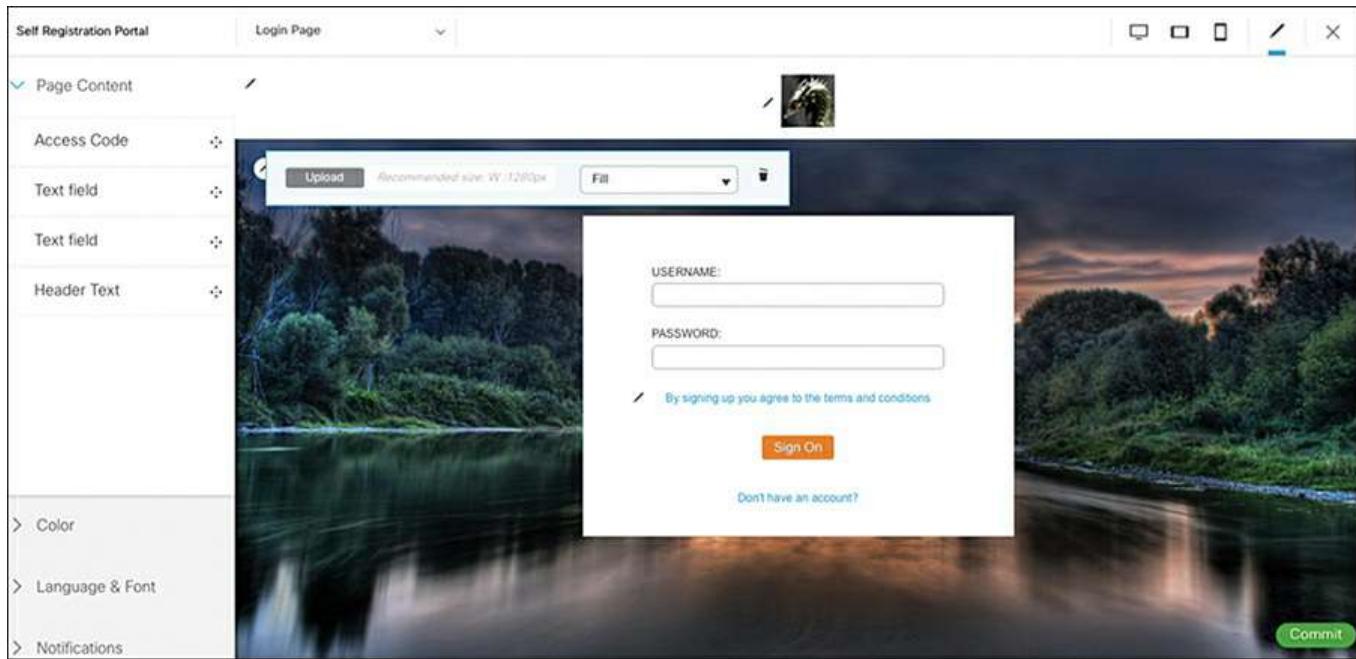
**Figure 6-6** Self-Registration Step 3

This takes you to the portal editor, in which you customize three pages, as shown in [Figure 6-7](#). You need to go through each page to ensure it looks the way you want it. Each page has similar steps, so only the Login Page steps are shown.

A screenshot of the portal editor showing the "Page Content" section for the "Login Page". On the left, there is a tree view with "Self Registration Portal" expanded and "Page Content" selected. On the right, a dropdown menu is open under "Login Page", listing "Login Page" (which is selected and highlighted), "Registration Page", and "Registration Success".

**Figure 6-7** Self-Registration Portal Pages

**Step 4.** From the drop-down list, choose **Login Page**. [Figure 6-8](#) shows a partially customized page. Everywhere you see the pencil icon indicates an area you can customize. You can upload your own background and icon images, you can and should change the terms and conditions, and you can add additional text fields. To add a new text field, drag the text field from the left column onto the login page.



**Figure 6-8** Self-Registration Portal Customization

The icons in the upper-right corner are preview buttons for different types of devices. Click one to see what your page would look like on that device type.

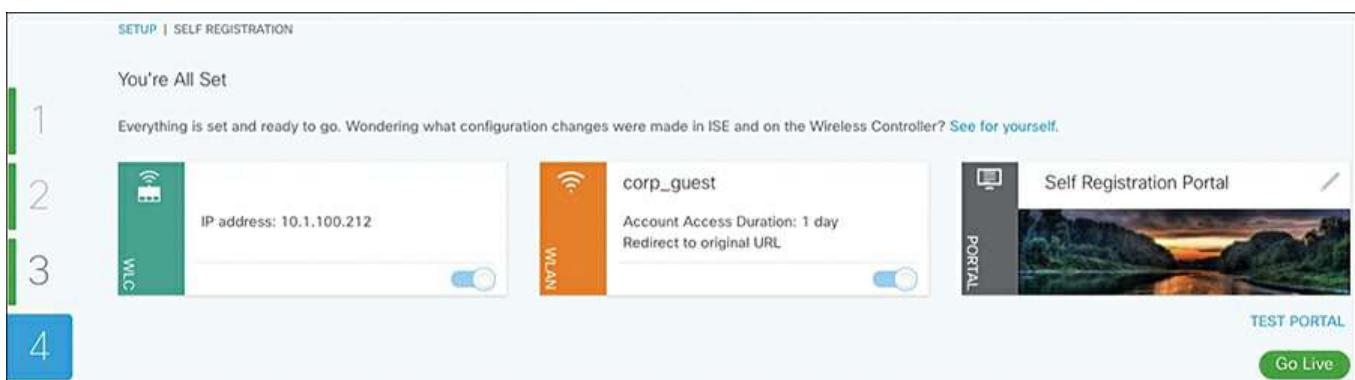
**Step 5.** Customize your notifications by clicking the **Notifications** menu in the lower-left area of the page. This enables you to tell the system how you want to send credentials to guests for the new accounts they create. It also allows you to customize the text in the message to the guest. [Figure 6-9](#) depicts the various options available.



**Figure 6-9** Self-Registration Portal Notifications

**Step 6.** Click the **Commit** button when you are satisfied with your customizations.

**Step 7.** Click the **Test Portal** button to launch the real portal from ISE so that you can check your work. If you need to make changes, just click the pencil icon again and continue editing your portal. Click **Next** to proceed to step 4 of the wizard, as shown in [Figure 6-10](#).



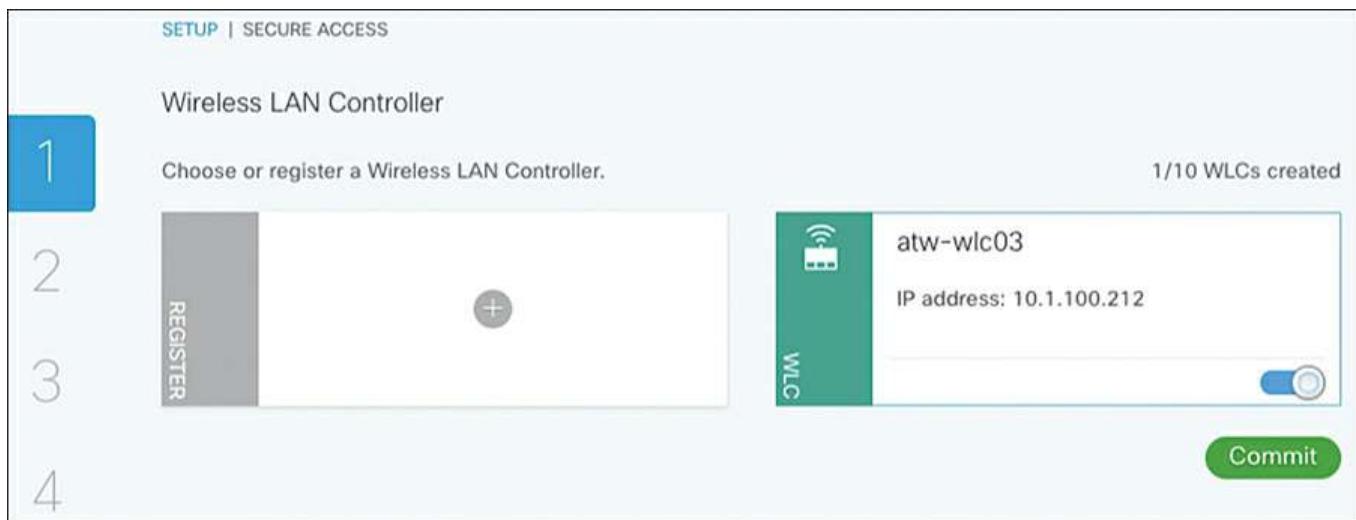
**Figure 6-10** Self-Registration Portal Go Live

**Step 8.** Check your work and click the **Go Live** button to finish the setup. Your guests can now log in via wireless to your network.

## Secure Access Wizard

This wizard guides you through the steps to configure Active Directory user authentication on your wireless network using ISE. Go to the Wireless Setup Wizard and select **Setup** under Secure Access (refer to [Figure 6-2](#)).

**Step 1.** From the screen shown in [Figure 6-11](#), select the WLC that you want to set up and click **Commit**.



**Figure 6-11** Secure Access Step 1

**Step 2.** From the screen shown in [Figure 6-12](#), choose the wireless network from the list of networks already configured on your WLC or click + to create a new one. The default WLC interface is the wired interface or VLAN that authorized users will drop onto from wireless. Click **Add**.

SETUP | SECURE ACCESS

Wireless Network

1 Choose or add a wireless network. The wireless network you select will remain disabled until the end of your setup where you can 'Go Live.'

2 ADD

3

4 Register a wireless network.  
WIRELESS NETWORK NAME (SSID)  
corp\_user

DEFAULT WLC INTERFACE (VLAN)  
management

Add

This screenshot shows the 'Wireless Network' configuration step. It includes a numbered list from 1 to 4. Step 1 is a general instruction. Step 2 shows a grey 'ADD' button. Step 3 is a placeholder. Step 4 shows a form for adding a wireless network, with the SSID 'corp\_user' entered and the default VLAN set to 'management'. An 'Add' button is at the bottom.

**Figure 6-12** Secure Access Step 2

**Step 3.** From the screen shown in [Figure 6-13](#), set up your AD by entering your domain name and a user/pwd for an AD services account for ISE to use. Click **Join**.

SETUP | SECURE ACCESS

Active Directory

1 Join an AD Group

2

3 ACTIVE DIRECTORY DOMAIN  
ise.local

domain.com

4 USERNAME  
administrator

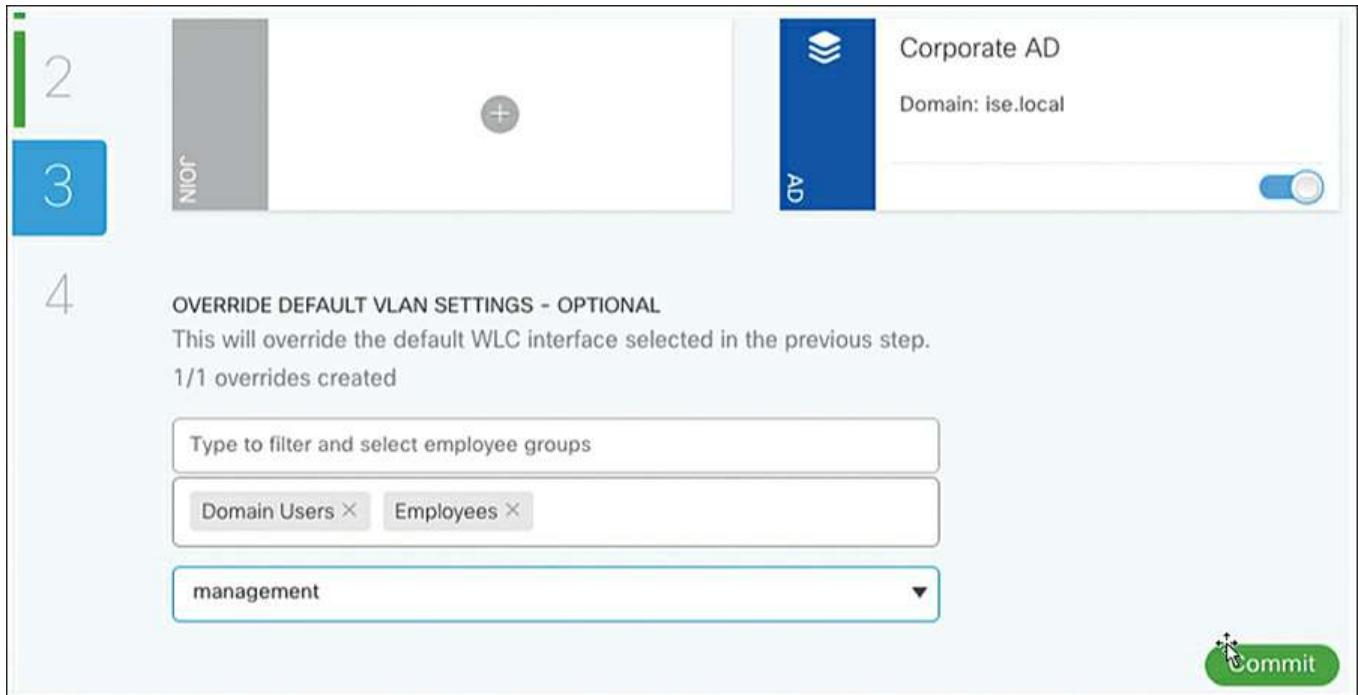
PASSWORD  
.....

Join

This screenshot shows the 'Active Directory' configuration step. It includes a numbered list from 1 to 4. Step 1 is a general instruction. Step 2 is a placeholder. Step 3 shows the 'ACTIVE DIRECTORY DOMAIN' field with 'ise.local' entered. Step 4 shows the 'USERNAME' field with 'administrator' entered and the 'PASSWORD' field containing several dots. A 'Join' button is at the bottom.

**Figure 6-13** Secure Access Step 3

Once joined, you may want to set up AD user groups that should drop onto a different wired interface or VLAN (see [Figure 6-14](#)).



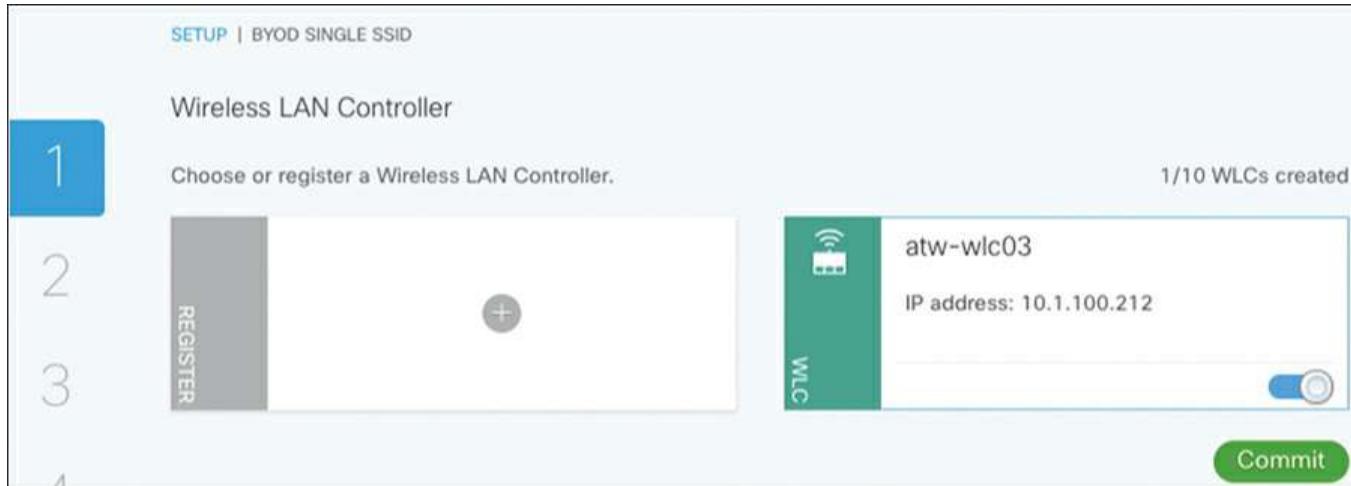
**Figure 6-14** Secure Access Override Default VLAN Settings

**Step 4.** Click **Commit**, and then on step 4 click the **Go Live** button. Your AD users can now log in to your wireless network securely.

### Bring Your Own Device (BYOD) Wizard

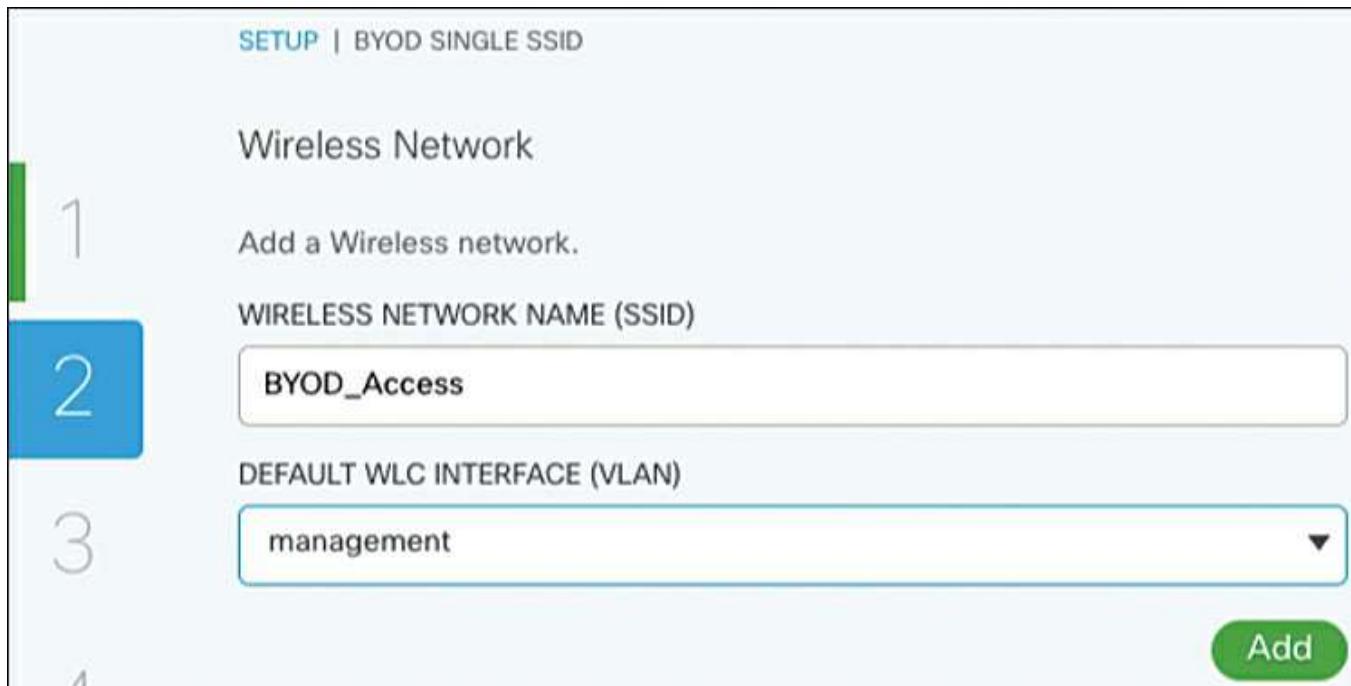
The BYOD wizard will configure ISE to allow access to your wireless networks using registered and compliant personal or corporate devices. From the Wireless Setup Wizard, click **Bring Your Own Device**, select either **Single** or **Dual SSID**, and then click **Setup**. This example shows setup of Single SSID.

**Step 1.** From the screen shown in [Figure 6-15](#), select your WLC or add a new one. Click **Commit**.



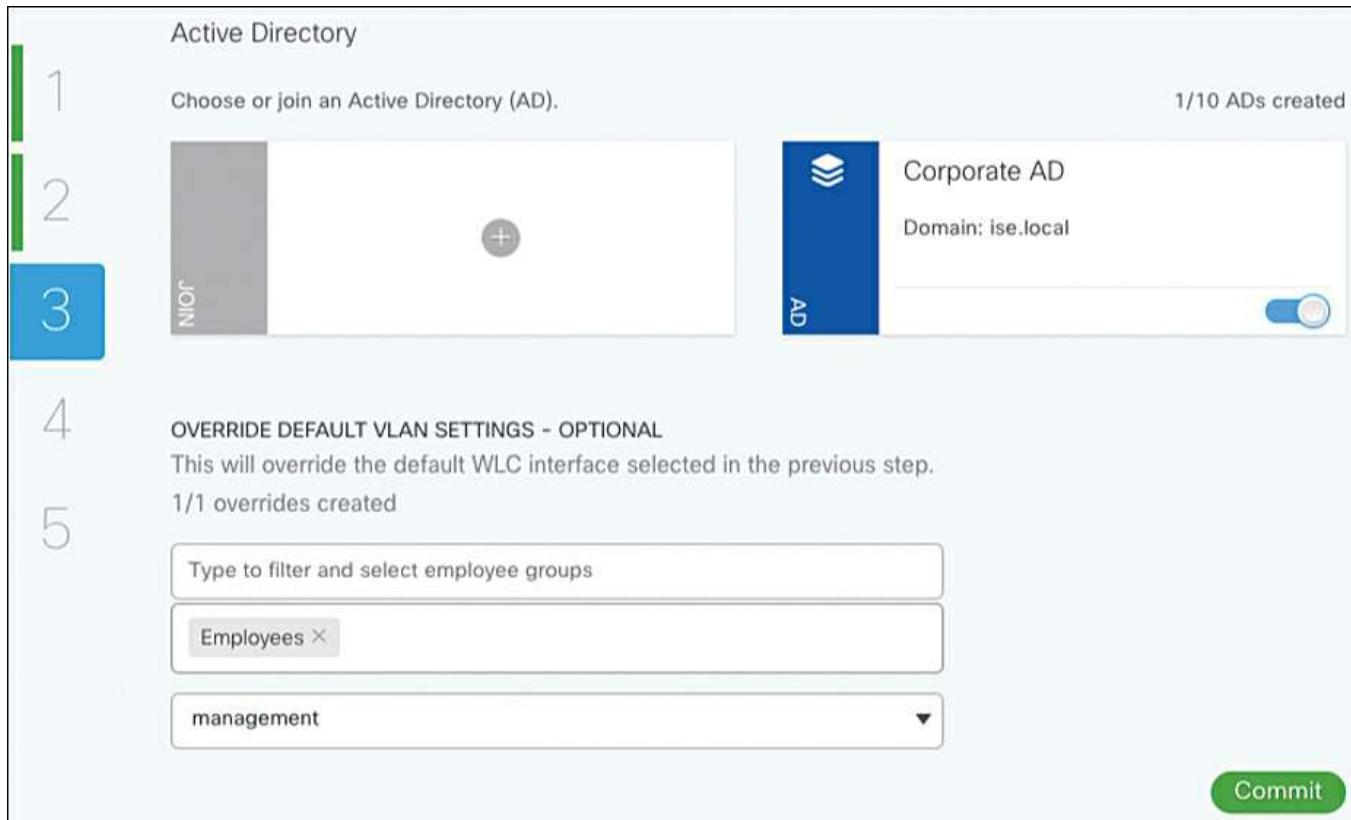
**Figure 6-15** BYOD Step 1

**Step 2.** From the screen shown in [Figure 6-16](#), add your wireless SSID and network you want to use for BYOD devices. Click **Add**.



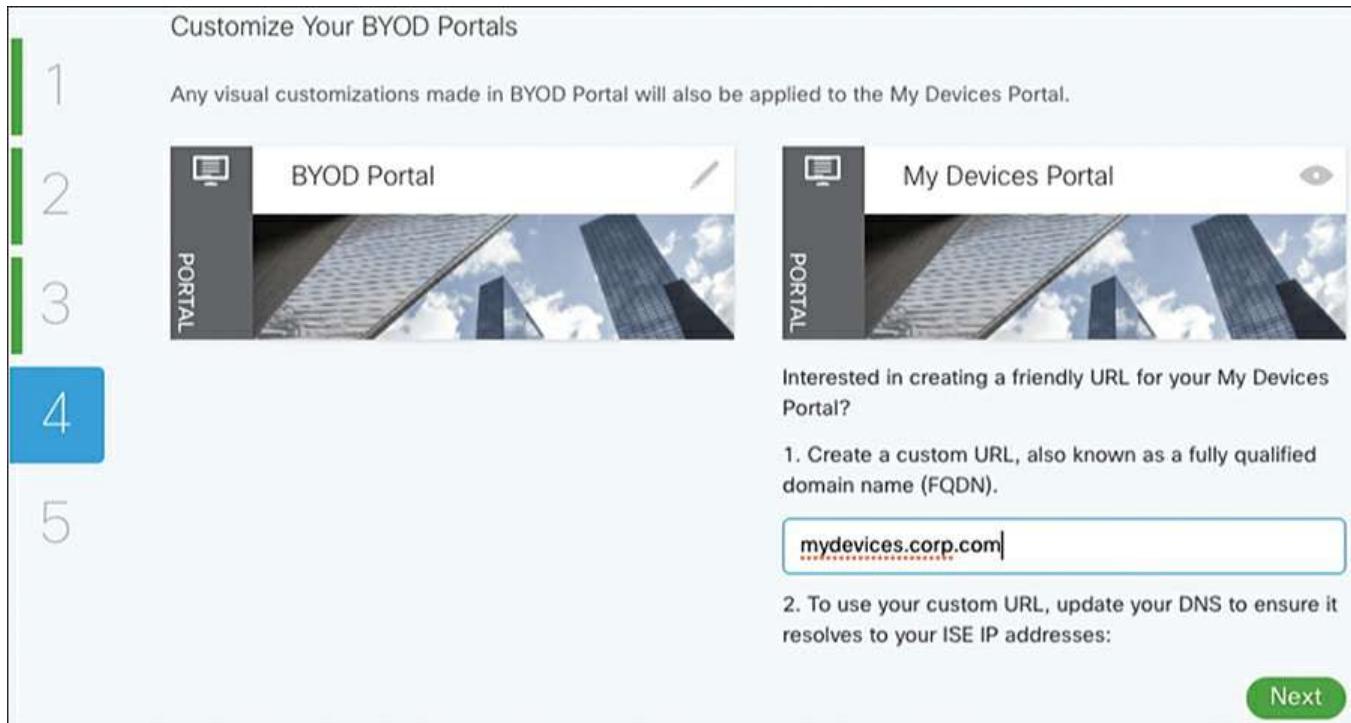
**Figure 6-16** BYOD Step 2

**Step 3.** Select your AD controller and, optionally, configure Override Default VLAN Settings. This enables you to change the default WLC interface that a particular user group drops onto after authorization. (see [Figure 6-17](#)).



**Figure 6-17** BYOD Step 3

**Step 4.** You should customize both the BYOD portal and the My Devices portal. The customization works just like the Guest portal customization we reviewed previously. Enter a custom URL for your portal so employees can remember it easily (see [Figure 6-18](#)). Add this domain into your DNS server and point it to ISE. Be sure to preview your portals before you go to step 5 of the wizard. Once done, click **Next**. Check your work and then click the **Go Live** button. Your employees can now register, enroll, and remove their BYOD devices securely on your wireless network.



**Figure 6-18** BYOD Step 4

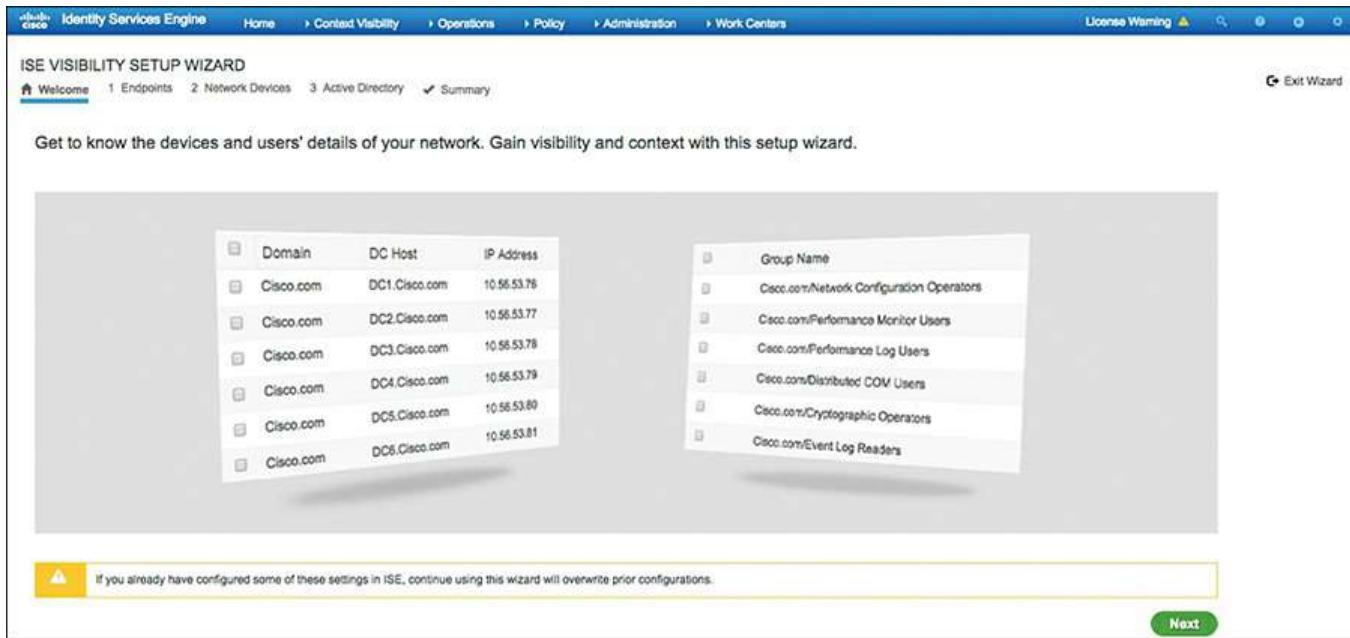
You have now completed all of the functions in the Wireless Setup Wizard. To get back to the ISE dashboard, click the **Back to ISE** link in the upper-right corner of the screen.

## Deploy ISE to Gain Visibility in 15 Minutes

Gaining visibility into what is on your network is a key first step to deploying ISE. Starting in ISE 2.1, the ISE Visibility Setup Wizard is available to help you quickly set up ISE Profiler, NMAP, and other features that show you what types of devices are connecting to your network. It even polls Active Directory for host OS information. The Visibility Setup Wizard configures ISE to be ready for network switches, WLCs, and firewalls to send profiling data to it. After the wizard is completed, you will start to see contextual data from hosts; however, you should then take the next step and manually configure key network devices to send profiling data to ISE. This will greatly enhance your ISE contextual and visibility data.

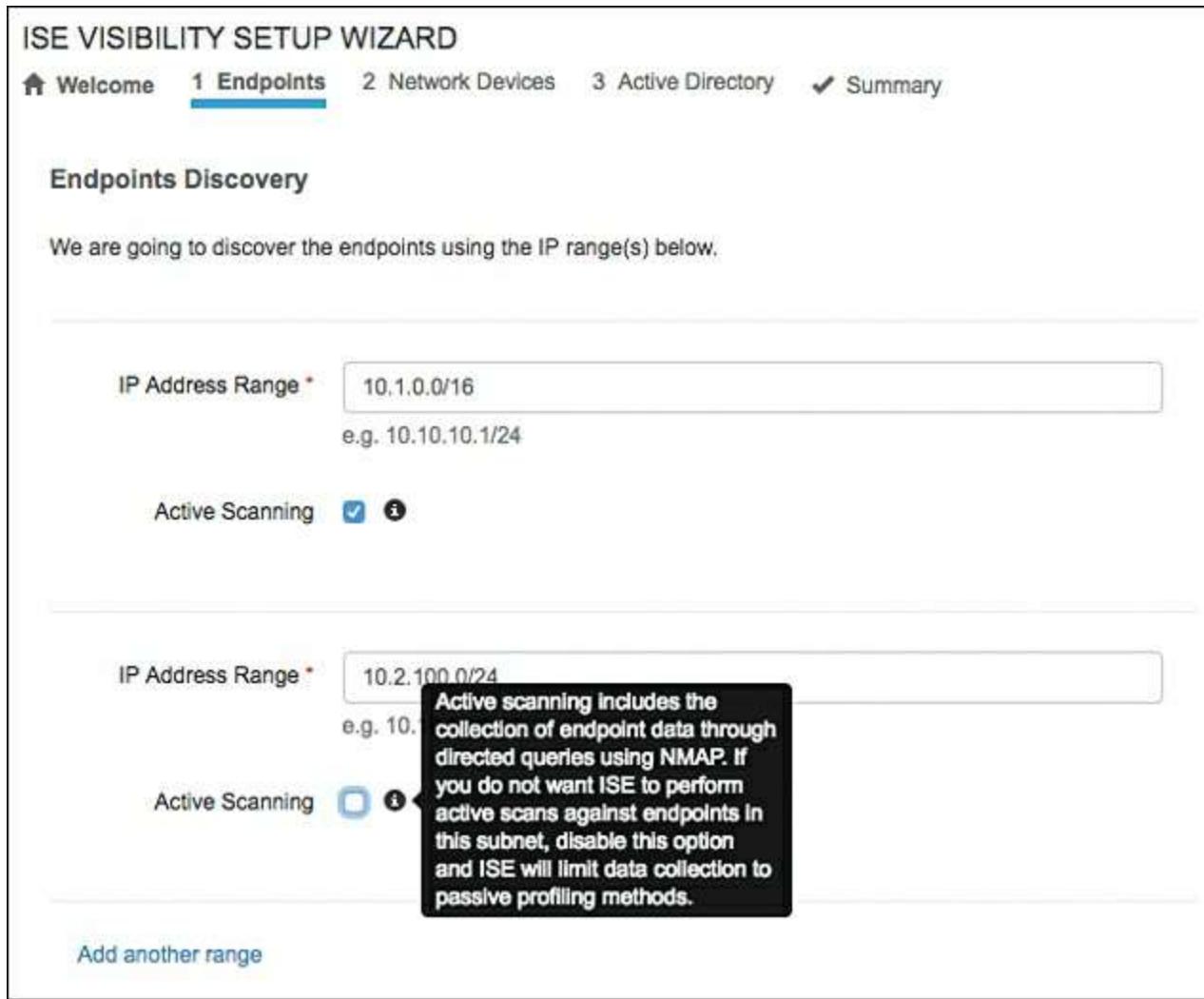
## Visibility Setup Wizard

Log in to the ISE GUI. Open the Visibility Setup Wizard by clicking the **Play** icon in the upper-right corner of the ISE GUI and choosing the **Visibility Setup** link. This launches the wizard's Welcome page, shown in [Figure 6-19](#). Click **Next** and complete the following steps. After each step, click **Next** to move on to the next step.



**Figure 6-19** Visibility Setup Wizard Welcome Page

**Step 1.** The first wizard step is to configure the IP address ranges you want ISE to scan for hosts, as shown in [Figure 6-20](#). If you prefer not to run an active NMAP scan, then uncheck the Active Scanning check box. Not running an active scan decreases the amount of context ISE is able to gather.



**Figure 6-20** Visibility Setup Wizard Step 1

**Step 2.** The second wizard step is to add your network devices into ISE so that it can discover them and the hosts connected to them. This also allows ISE, via SNMP, to receive host connectivity and port information. [Figure 6-21](#) depicts the devices that are added, while [Figure 6-22](#) shows an example of adding a device. To add a device, click **Add**.

Network Device Discovery					
Total Added (2)		Failed (0)			
<a href="#">Scan</a> <a href="#">Add</a> <a href="#">Remove</a> <a href="#">Add Location</a> <a href="#">Filter</a>					
Name	IP Address	Device Type	Location	Description	Action
Cisco_switch	192.168.254.1	switch	Denver	3750X	<a href="#">Edit</a>
NAD_10.1.100.212	10.1.100.212	All Device Types	All Locations	Network Device created by Wireless Setup Wizard...	<a href="#">Edit</a>

**Figure 6-21** Visibility Setup Wizard Step 2

Edit Network Device X

Name *	Cisco_switch
IP Address *	192.168.254.1
Location	Denver
Device Type	switch
Description	3750X

SNMP Settings

SNMP Version *	2c
RO Community *	***** <span style="float: right;">Show</span>

Cancel Save

**Figure 6-22** Visibility Setup Wizard Step 2: Adding a Device

The Location and Device Type fields are free-form fields you should use to logically organize your devices. Location could be a city or it could be a closet on the third floor; whatever works best for your organization. Click **Save**.

**Step 3.** Step three of the wizard is where you connect to Active Directory. ISE will pull host OS information and other attributes from AD. If you have already configured AD in ISE, you can click the **Skip** link. If not, see [Figure 6-23](#) for configuration details.

Home Welcome 1 Endpoints 2 Network Devices **3 Active Directory** ✓ Summary

### Connect to Active Directory (AD)

Connect Active Directory server to get user identity information. You can add one or more Active Directories.

Display Name \* ise.local

Domain FQDN \* ise.local

ISE Node \* atw-ise231.securitydemo.net

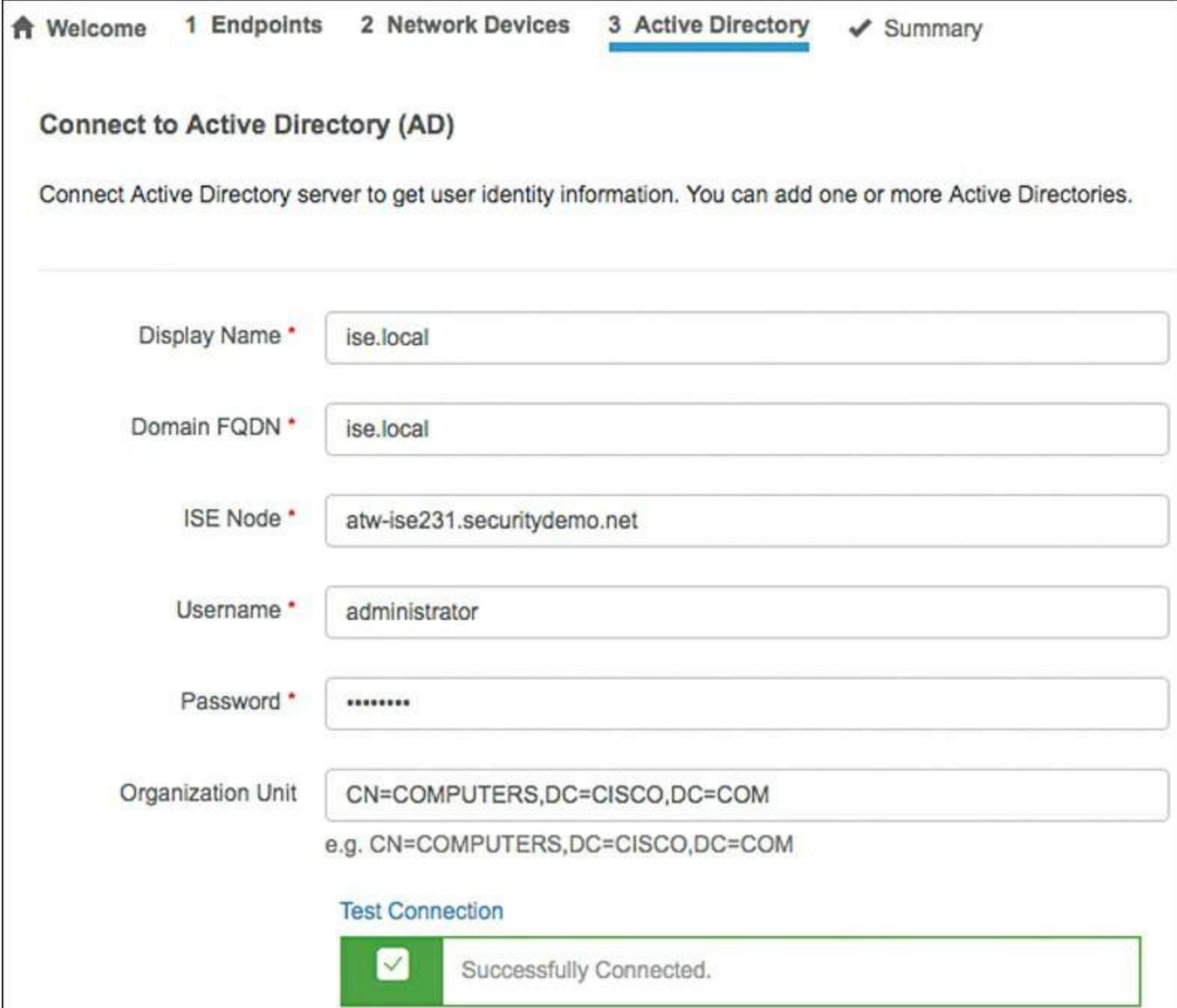
Username \* administrator

Password \* .....

Organization Unit CN=COMPUTERS,DC=CISCO,DC=COM  
e.g. CN=COMPUTERS,DC=CISCO,DC=COM

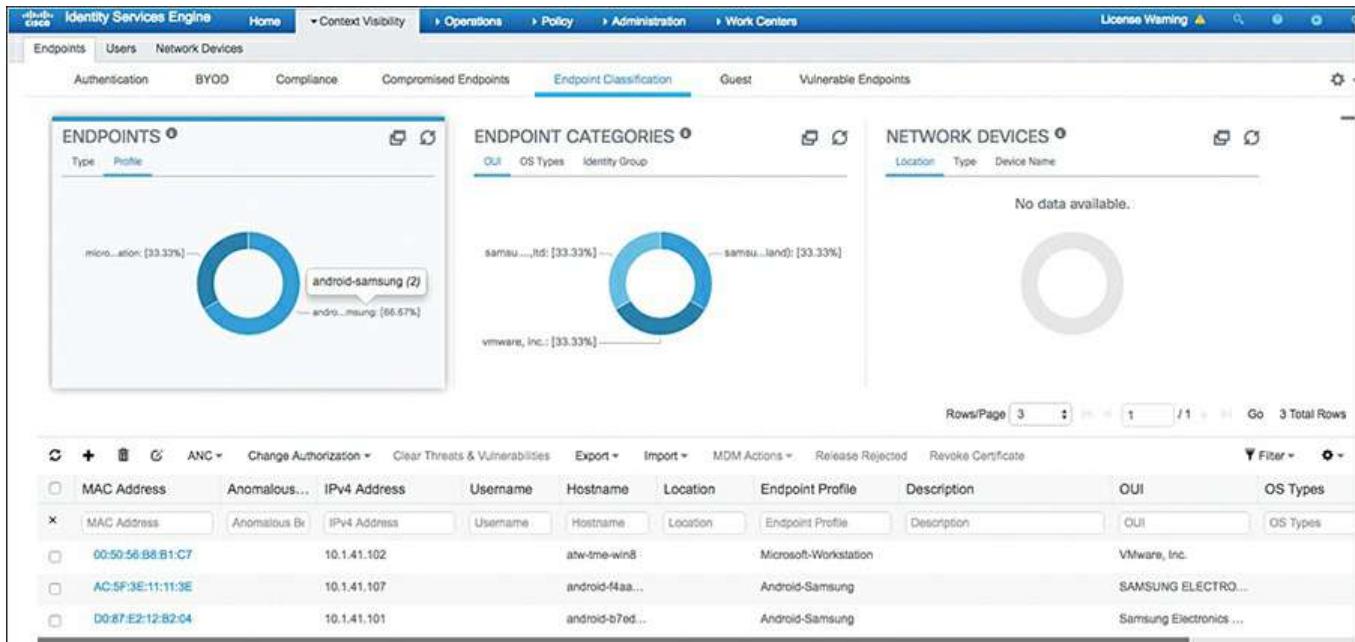
[Test Connection](#)

Successfully Connected.



**Figure 6-23** Visibility Setup Wizard Step 3

**Step 4.** The final step, four, is just a summary screen of all your previous steps. From here, you can click the **Edit** button and go back to a previous step. To complete, click **Test Connection** on AD one last time. If successful, you can click **Exit Wizard**. You're done! ISE is now profiling your network, collecting context and visibility data. Let it run for at least an hour and then check the page at **Context Visibility > Endpoints > Endpoint Classification**, as shown in [Figure 6-24](#).



**Figure 6-24** Endpoint Classification Page

Notice at the bottom of the page the list of all the devices and their contextual information. By checking a row, you can then issue actions on that host, such as those listed in [Figure 6-25](#).

<input type="checkbox"/>	MAC Address	Anomalous Br.	IPv4 Address	Username	Hostname	Location	Endpoint Profile	Description	OUI	OS Types			
<input type="checkbox"/>	MAC Address	Anomalous Br.	IPv4 Address	Username	Hostname	Location	Endpoint Profile	Description	OUI	OS Types			
<input type="checkbox"/>	00:50:56:B8:B1:C7		10.1.41.102		atw-tme-win8		Microsoft-Workstation			VMware, Inc.			
<input type="checkbox"/>	AC:5F:3E:11:11:3E		10.1.41.107		android-f4aa...		Android-Samsung			SAMSUNG ELECTRO...			
<input type="checkbox"/>	D0:87:E2:12:B2:04		10.1.41.101		android-b7ed...		Android-Samsung			Samsung Electronics ...			

**Figure 6-25** Endpoint Classification Page Actions

The most common profiling data probes for ISE are the RADIUS, SNMPQUERY, DHCP, Network Scan (NMAP), and Active Directory probes. The probes are sent from the Policy Service Nodes in an ISE deployment. The Visibility Setup Wizard discussed previously has already configured all of these profiler probes.

To verify the probes' configuration or make changes, go to **Administration > System > Deployment**. Click your ISE PSN node. On the General Settings tab, ensure that the profiling service, under the policy service, is checked.

Next, click the **Profiling Configuration** tab. Verify that all of the probes checked in [Figure 6-26](#) are enabled.

Deployment Nodes List > atw-ise231

Edit Node

General Settings Profiling Configuration

- ▶ NETFLOW
- ▶ DHCP
- ▶ DHCPSPAN
- ▶ HTTP
- ▶ RADIUS
- ▶ Network Scan (NMAP)
- ▶ DNS
- ▶ SNMPQUERY
- ▶ SNMPTRAP
- ▶ Active Directory

Figure 6-26 Profiling Probes Configuration

## Configuring Cisco Switches to Send ISE Profiling Data

The most common profiling probes used with Cisco switches are SNMPQUERY, RADIUS, and DHCP.

### SNMPQUERY Probe

The SNMPQUERY probe is used by ISE to send SNMP Get requests to access devices, such as switches, to collect relevant endpoint data stored in their SNMP MIBs. There are two types of SNMP queries that the ISE PSN performs: System Query (Polled) and Interface Query (Triggered). This probe also collects Cisco Discovery Protocol (CDP) information.

**Step 1.** Configure all of your switches with a read-only community string such as **snmp-server community ciscoro RO 10, access-list 10 permit 1.1.1.1**. For better security, always configure an ACL when you configure community strings.

**Step 2.** CDP is usually enabled by default on switches. To verify, ensure that the global command **cdp run** and the switch port command **cdp enable** are configured.

## RADIUS Probe

For RADIUS, you just need to add the device to ISE for standard RADIUS communications and configure RADIUS AAA on the switches.

Configure all of your switches with RADIUS AAA using the following IOS commands:

[Click here to view code image](#)

```
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
ip radius source-interface <Interface>
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server host <ISE_PSN_Address> auth-port 1812 acct-port 1813 key xxx
radius-server vsa send accounting
radius-server vsa send authentication
```

## DHCP Probe

This probe collects attributes from within the DHCP client request. It uses the DHCP helper or relay commands on switches or routers.

From the CLI of your Cisco switches or routers that are currently acting as DHCP relays, add a second relay or helper statement to send a copy of the DHCP request to your ISE PSN.

Under each routed interface relaying DHCP for hosts, add the following IOS command:

```
ip helper-address ISE_PSN_address
```

Or NX-OS command

```
ip dhcp relay ISE_PSN_address
```

The address specified should be to the PSN interface with the DHCP probe enabled. For redundancy, you can add more IP Helper statements to relay DHCP to other PSNs. However, doing so adds additional load on your PSNs, so use this sparingly.

## Summary

This chapter has shown you how to get ISE up and running and providing value very

quickly. At this point you have secure wireless for guests, employees, and employee BYOD devices. You also have ISE authenticating with Active Directory and collecting context and visibility profiling data from your network. The multiple profiler probes you configured will show you who, what, and where devices and users are on your network. That is a nice start to your ISE deployment—well done!

# **Part III The Foundation, Building a Context-Aware Security Policy**

[Chapter 7 Building a Cisco ISE Network Access Security Policy](#)

[Chapter 8 Building a Device Security Policy](#)

[Chapter 9 Building an ISE Accounting and Auditing Policy](#)

# Chapter 7 Building a Cisco ISE Network Access Security Policy

This chapter covers the following topics:

- Components of a Cisco ISE network access security policy
- Determining the high-level goals for network access security
- Defining the security domains
- Understanding and defining ISE authorization rules
- Establishing acceptable use policies
- Host security posture assessment rules to consider
- Defining dynamic network access privileges

In order for any network-centric security solution to be successful, a solid network access security policy (NASP) must first be in place. Once a policy is in place, ISE will enforce the policy network-wide. A NASP defines, in as much detail as is practical, the type of network access that will be given to users and device types.

Because network and device security threats are constantly changing, a NASP must also be a living, changeable document. This book does not attempt to assemble an all-encompassing NASP, but instead focuses on showing you how to build policies that are relevant to the Cisco ISE solution. Thus, this chapter guides you through the process of creating a comprehensive NASP that you can use in an environment that is safeguarded by Cisco ISE. Building a NASP is not always straightforward, and can be frustrating at times, but stick with it; your hard work will be rewarded in the end. The key to a successful ISE deployment is not to try to accomplish everything in the first phase. Start with the easy and quick approach, like what was shown in [Chapter 6](#).

## Components of a Cisco ISE Network Access Security Policy

One of the hardest things about writing a comprehensive network access security policy is figuring out what should be included. This chapter guides you through the parts and pieces that, at a minimum, should be included in any NASP written for the Cisco ISE solution. For your ISE solution to be most effective, you must first determine exactly what an acceptable network access security posture is under different circumstances and contexts. After you do so, you can then translate your NASP into the proper checks, rules, and security requirements that ISE will use to determine the correct policy to apply to the network and/or device. For example, if the device is not a corporate asset and is connected to the corporate wireless network, then a strict NASP should be enforced. However, if a registered corporate asset of the same device type connects to corporate wireless, a less strict NASP should be enforced. You also need to determine

what the NASP should be for different types of devices and their security posture. For example, if a contractor logs in to your network using a Windows 10 laptop, the security policy would differ from the same user logging in with a Mac OS X laptop.

An ISE NASP is made up of several different policy types. When combined inside ISE, these policy types provide you with the ultimate in flexibility for achieving a truly context-aware network access decision. The following are main policy types for which ISE will obtain contextual information it can then use to build such policies:

- **Authentication Policy:** Verifies the user's and/or device's identity or provides unauthenticated guest access. For example: Authenticate all wireless users against the corporate Active Directory (AD).
- **Authorization Policy:** Describes both the contextual attributes used for authorization of the user and/or device and the enforcement method triggered once a policy rule is matched. For example: Users who are members of the AD group Employees and are using an approved company-owned device are allowed to use the wireless SSID corp. All of your dynamic segmentation policies, including TrustSec policies, will be configured here.
- **Host Posture Assessment Policy:** Deals with the security level of the host itself. Different operating systems and device types offer different levels of posture assessment capability. ISE can also integrate with a third-party Mobile Device Management (MDM) system to gather posture information from mobile devices such as iPhones and iPads. An example policy: All Windows 10 PCs must have all corporate patches and be running an approved up-to-date antimalware software package such as Cisco AMP.
- **Device Profiling Policy:** Allows you to set policy based on the type of device trying to access your network. Profiling is an agentless method of passively watching the device's behavior and/or responses to determine what type it is. For example: If a user connects with an iPhone, do not allow them access to any data center or HR resources.

The preceding list is not comprehensive but showcases the most popular policy types typically included in a comprehensive network access security policy. A BYOD policy would be made up of the different listed policies combined into a specific BYOD policy and, as such, is not included as its own policy type in this chapter. However, you may choose to, and likely will, have a separate BYOD policy within your NASP that ISE will enforce.

## Network Access Security Policy Checklist

The following is a checklist of the most common steps considered necessary to create an ISE network access security policy. Each checklist item will be explained in detail in

the subsequent sections of this chapter. Use this checklist, along with the detailed explanations, to get a head start in the creation of your own unique NASP.

- Obtain senior management sponsors that will support you through the creation of the NASP and the deployment of the ISE solution.
- Determine which people and departments need to be involved in the creation of the NASP. Make sure they are included right from the start of the project.
- Determine what your high-level goals for network access security are.
- Break up your organization into security domains. The requirements of the NASP can then be customized for each security domain as necessary.
- Define authorization rules that are relevant for your organization.
- Establish an acceptable use policy (AUP) for your network.
- Define the ISE network access security checks, rules, and requirements for each authorization rule.
- Define the network access privileges that should be granted to each authorization rule.
- Establish a Network Access Security Policy life-cycle process that ensures the regular updating and changing of the NASP's checks, rules, and requirements.

## **Involving the Right People in the Creation of the Network Access Security Policy**

At the very beginning of the planning for an ISE deployment or purchase, it is extremely important to obtain project sponsorship from senior-level management. Given that ISE will force a change on the user community's behavior and network access, this is a mandatory step. Without senior-level sponsorship, a few activist users who are not happy with or willing to accept the new policy changes could derail your ISE deployment. Having the endorsement of senior management grants you the power to push back on those users in a constructive way.

Too often the security group spends the time to develop sound security policies and practices only to be told that they are overly restrictive and need to be changed. This can be avoided by making sure that you keep your sponsors involved and up to date on the progress and content of your NASP. It is also critical that you have your final version approved by your sponsorship committee prior to releasing it to the user community. Try to anticipate the type of reaction, resistance, and questions the user community will have. Be ready with solid rebuttals, facts, and collateral to combat their arguments, answer their questions, and make them feel more comfortable that the new NASP is the correct one and best for the business.

One of the first steps in the creation of any NASP is the formation of the network access

security policy committee. This committee should be made up of the principal persons whose group or users will be most affected by or have some ownership in the new policy. It is a best practice to keep the committee small in the beginning phases of the policy creation. Once this core team has a clear policy direction, some substance, and some content, then the NASP committee should be expanded to include more key persons.

When the NASP reaches a completed draft format, the NASP committee should again be expanded. This time the expansion is to include those principal persons who do not have any direct ownership or responsibility for the creation of the NASP but do have a sizeable user community that will be directly affected by the policy's proposed changes. This last group serves to scrutinize the policies in your NASP draft to make sure the policies do not inhibit business practices or workflow, are practical, and have achieved the proper balance of risk mitigation versus ease of network access for the organization.

Once a final NASP version has been created, the entire committee must agree to present a united front when the new policy begins to be enforced inside the organization. A nonunited, or splintered, NASP committee almost always will result in the splintering or haphazard adoption of the NASP within the organization.

The following is a list of the most common principal persons that should be a part of the creation of a NASP. Additionally, the CSO and CIO must be sponsors or core committee members. You should modify this list for your environment.

- Sponsors should include the following:
  - At least one executive-level sponsor other than the CSO/CIO.
  - At least one company board member. If this is too inconvenient for your organization to arrange, then settle for a presentation to the board of your ISE project, its goals, and its business relevance.
  - An attorney from the legal department, to review your AUP and legal disclaimers, at a minimum.
- Core NASP committee members should include key persons from the following groups:
  - Security group
  - Networking group
  - Server group
  - Desktop support group
  - Operations group
  - Security incident response team
- Extended NASP committee members should include key persons from the following

groups:

- Human resources group
- Legal group
- Audit/compliance group
- Final NASP committee members should include key persons from the following groups:
  - Managers of large end-user groups within the organization (such as division heads, department heads, and so on).
  - The end-user community, for feedback and impact analysis. Be sure to select at least one “newbie” end user.

This list should be used as a guideline and is not meant to be all-inclusive. The goal of committee member selection is to ensure that the committee has adequate representation from all key stakeholders, budget holders, management, legal counsel, and technical staff. Some of the groups listed might not be included if your ISE deployment will be limited in scope or functionality. Each group will have a slightly different role to fulfill on the committee. Make sure that you communicate up front what their roles will be. Try to keep your core group to less than ten people so that it can operate efficiently.

## Determining the High-Level Goals for Network Access Security

Determining what your high-level goals are for network access security is a critical step toward the completion of a comprehensive network access security policy. These high-level goals will serve as your benchmarks and guides throughout the NASP creation process. The final NASP document should represent a detailed plan that achieves these high-level goals. It is important to periodically refer to these high-level goals to ensure your NASP remains focused and on target to meet your stated security goals.

Among the references for creating a security policy, one that has stood the test of time is RFC 2196, “Site Security Handbook.” The following is an excerpt:

Your goals will be largely determined by the following key tradeoffs:

**1. services offered versus security provided –**

Each service offered to users carries its own security risks. For some services the risk outweighs the benefit of the service and the administrator may choose to eliminate the service rather than try to secure it.

**2. ease of use versus security –**

The easiest system to use would allow access to any user and require no passwords; that is, there would be no security. Requiring passwords makes the system a little less convenient, but more secure. Requiring device-generated one-

time passwords makes the system even more difficult to use, but much more secure.

### 3. cost of security versus risk of loss –

There are many different costs to security: monetary (i.e., the cost of purchasing security hardware and software like firewalls and one-time password generators), performance (i.e., encryption and decryption take time), and ease of use (as mentioned above). There are also many levels of risk: loss of privacy (i.e., the reading of information by unauthorized individuals), loss of data (i.e., the corruption or erasure of information), and the loss of service (e.g., the filling of data storage space, usage of computational resources, and denial of network access). Each type of cost must be weighed against each type of loss.

**Note** For more detailed information about the creation of network access security goals and security policies in general, reference IETF RFC 2196 at <http://www.ietf.org/rfc/rfc2196.txt>.

Your final high-level network access security goals will be the result of establishing a fine balance among the preceding trade-offs. The result of each trade-off will be different for each organization or division within an organization.

## Common High-Level Network Access Security Goals

Here are some examples of network access security goals that are frequently instituted in organizations that deploy an ISE solution. These examples are meant to be a sampling and not a comprehensive list.

- Enforce a consistent context-based dynamic segmentation security policy across the infrastructure.
- Obtain system-wide visibility showing who, what, how, and where a user or device is on the wired, wireless, or VPN network.
- Protect the network from unauthorized access, both internal and external, at all network access points.
- Authenticate all users attempting to gain access to the network.
- Authorize all users, based on risk, attempting to gain access to the network.
- Assign a TrustSec Security Group Tag (SGT) to all wired, wireless, and VPN users after network authorization.
- Provide differentiated network access based on user and device attributes, risk profile, and role.
- All non-guest mobile devices must be enrolled in the corporate mobile device management (MDM) system.

- All users must periodically acknowledge an acceptable use policy before being granted network access.
- All PCs and Macs must be running an approved antimalware and personal firewall program that is continuously up to date.
- All non-guest devices must be running an approved operating system version that is up to date.
- Any device that is found to be running banned software applications will be denied network access.
- All guest devices must be segmented from non-guest devices and other guest devices and provided only regulated Internet access.
- Compromised users or endpoints must be alerted and quarantined on the network to limit the scope of the breach.

It is common for an organization to modify its network access security goals based on a specific network location or access type. For example, an organization might have a policy that states that all devices connecting through wireless in the Denver data center must be corporate-owned in order to gain network access.

Many organizations choose to deploy an ISE solution gradually by enforcing their network access security policies incrementally. The following is a list of common best practice policy enforcement phases:

**Note** Deploying ISE to protect wireless networks is by far the easiest solution to build and maintain. Among the various reasons for this, the primary reason is that the protocols used for wireless client AAA are robust and easy to deploy. Thus, the list that follows includes wireless deployments first. Wireless is the low-hanging fruit for an ISE deployment. The different wired deployment modes in the list that follows will be covered in detail in subsequent chapters.

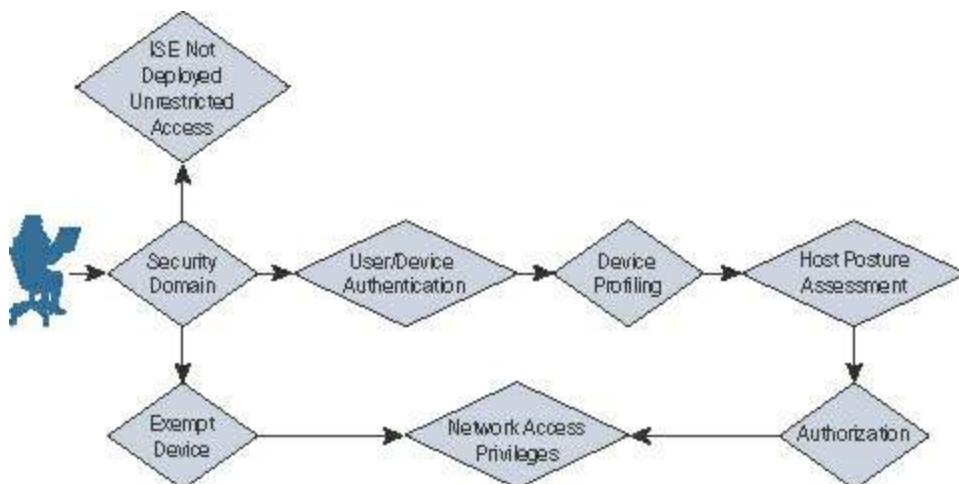
- Deploy wireless guest access security policies.
- Deploy wireless authentication and lightweight authorization access control policies.
- Deploy policies for wired and wireless network visibility profiling of users and devices.
- If applicable, deploy mobile device provisioning and enrollment into an MDM system.
- Deploy wired 802.1X and MAC Authentication Bypass (MAB) for AAA in Monitor Mode.
- Deploy wired 802.1X for AAA in Low-Impact Mode.

- Deploy wired 802.1X for AAA in Closed Mode.

Then, as the adoption of the ISE solution grows, the network access security policy enforcement can be spread ubiquitously throughout the organization.

## Network Access Security Policy Decision Matrix

[Figure 7-1](#) summarizes the process for determining the exact network access security policy that will be enforced for a given user, for a given device, or in a given network location.



**Figure 7-1** Network Access Security Policy Decision Matrix

The following list explains the device security policy decision steps shown in [Figure 7-1](#). Following this list are several sections that describe these decision steps in greater detail.

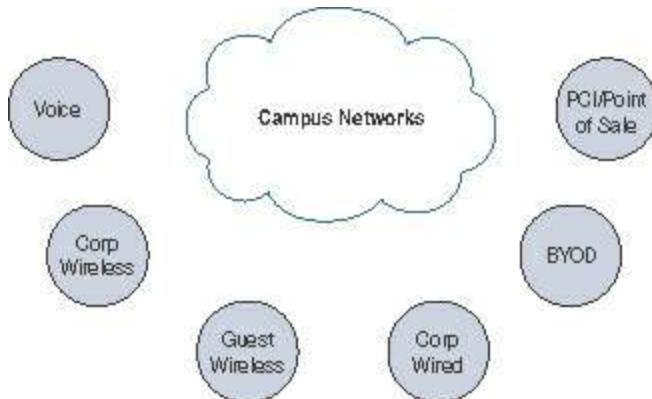
1. The device connects to a location on the network.
2. The device is determined to be a member of a certain security domain. The NASP must define what the security domains are for the organization. The NASP must define one of three choices for each unique security domain:
  - The security domain does not have ISE deployed, thus allowing unrestricted network access. The NASP for this security domain states that no network access security policies are to be enforced in this domain.
  - The security domain has ISE deployed but exempts specific devices from ISE access control when they are seen on the network.
  - The security domain has ISE deployed and forces all devices to comply fully with the ISE NASP.
3. If the device is a member of the exempt list, then it flows directly to the network access privileges. The remaining steps are bypassed. The NASP must define exactly what the network access privileges will be for each type of exempt device.

It is possible to have different network access security policies for different types of exempt devices. For example, you can have an exempt network access security policy that allows IP phones to access the network unrestricted.

4. If the device is part of a security domain that requires full compliance with the ISE policy, then the user/device is forced to authenticate. The NASP should determine exactly how the user and/or device is authenticated and verified.
5. After successfully authenticating, the device is then profiled to figure out what kind of device it is.
6. The posture of the device is checked to determine whether the host is in compliance. The NASP should define what the security requirements are.
7. If the host is in compliance with the security requirements, it is authorized. The authorization rules are parsed and the first rule matched is executed upon.
8. The network access policies assigned to the matched authorization rule are enforced. The NASP should define the type of network access that should be granted to clients. The access requirements are produced from a combination of authentication, authorization, profiler, and posture rules combined.

## Defining the Security Domains

A security domain is used to group things together that have a common risk profile, under a common network access security policy. These things could be a combination of user groups, locations, network types, device types, and/or business function. Security domains allow you to break your security policy into manageable sections. For example, you might have a Guest Wireless security domain or a Corporate Wireless security domain. [Figure 7-2](#) shows an example of security domains.



**Figure 7-2** Sample Security Domains

Most organizations need to define the security domains that are depicted in [Figure 7-2](#). Each one of these groups usually requires its own unique network access security policy and thus should be its own security domain. (A few other common security domains that

are not depicted are Data Center and Internet of Things [IoT] security domains.) Separating these areas into unique security domains allows you to create unique network access security policies for each. The more compartmentalized your NASP is, the more granular and targeted it can be while at the same time keeping things manageable and realistic. This results in a more locked-down network access security policy for your organization that can be operationalized. Using security domains is optional, of course, but makes a great way to segment your NASP. Above all, try to keep your NASP short and concise; the keep it short and simple (KISS) principle applies here.

Here are some commonly used security domains:

- **Remote Access:** This domain includes any device that is accessing the network remotely via VPN and/or dial-up modem.
- **OOB Management:** This domain includes any device that resides on the out-of-band network management network. This is typically a highly secured domain.
- **Internet Access:** This domain includes any device that accesses the Internet. An example policy for this domain could be: Before a device is allowed to access the Internet, its operating system and antivirus software must be up to date.
- **Guest:** This domain includes any device that is a guest on the network. This domain typically is segmented into access types as well (for example, guest wireless, guest VPN, and guest LAN domains). This allows for the creation of very granular network access security policies for guests.
- **Wired:** This domain includes any device that connects to the network via a wired switch port. It is very common to separate security domains by VLAN or location at the LAN level. This allows the NASP to have policies for specific VLANs and locations instead of having one generic policy for all wired devices.
- **Wireless:** This domain includes any device that uses wireless to access the network. It is common for the wireless domain to be separated out by VLAN or location (for example, a guest wireless security domain or a Denver campus wireless security domain).

This list is by no means comprehensive, but it should serve to give you a good start in the creation of your own security domains.

## **Understanding and Defining ISE Authorization Rules**

The effective use of authorization rules is a key component to any successful ISE deployment. ISE is very much rule-based. An authorization rule defines the network access security policies that will be required for its members. ISE evaluates authorization rules top down and first match, just like a router ACL. Because of this, the

rule order is important in ISE. Additionally, your most-often-hit rules should be at the top for efficiency of the system. The concept of authorization rules is the backbone of ISE.

The login information is used to gather attributes from an external identity server such as LDAP, AD, or RADIUS.

**Tip** It is a best practice to map attributes from an external authentication server (such as AD, LDAP, or RADIUS) to an authorization rule in ISE. A common attribute used is MemberOf in Windows AD. This allows authorization rules to be based on existing AD groups within your organization. For example, an LDAP user Conor is a MemberOf AD group employee.

ISE authorization rules have policies that determine which ISE functions will be performed on clients. All clients that match the authorization rule will be subjected to its security permissions. The common permissions that can be controlled by authorization rules are as follows:

- Access Type (Accept/Reject)
- Apply a TrustSec Security Group Tag to the client traffic
- Downloadable ACLs
- VLAN Assignment
- Airespace ACL Name—Assigns ACL in Cisco WLC to client traffic
- Voice Domain Permission
- Initiate Web Authentication
- Execute Switch Auto Smartports macro
- Apply an Interface Template
- Periodically assess host vulnerabilities
- Filter-ID—Sends ACL via RADIUS filter attribute
- Reauthentication—Decide if you want to maintain connectivity during reauthentication
- MACsec Policy—Sets 802.1ae link-by-link encryption to must-secure, should-secure, or must-not-secure
- Network Edge Authentication Topology (NEAT)—Allows you to authenticate network devices (such as switches) to other network devices via 802.1X
- ASA VPN attributes
- Client posture assessment

- Network Scanner—NMAP
- Acceptable Use Policy

As you can see, authorization rules have a number of common permission controls available. ISE also has numerous advanced permissions via advanced attribute settings when defining your permissions.

## Commonly Configured Rules and Their Purpose

This section focuses mostly on the rules that are commonly found in the network access security policies of organizations that use the ISE solution. The goal is to present you with a solid starting point from which to determine the authorization rule needs of your organization's network access security policy.

Let's explore some of the most commonly used rules. Remember, a rule defines the rights and privileges a client will have once they pass authentication, authorization, and posture assessment. All organizations must have their own customized rules. The number and purpose of these rules will vary according to your environment. Each of the rules you build should have a separate policy definition section in your NASP document. Here are some of the most commonly configured rules:

- Guest/visitor Rule
- Employee Rule
- Corporate Authorization Rule
- Contractor/Temp Rule
- Student Rule
- Faculty Rule
- Rules based on network location, such as Denver Authorization Rule
- Admin Rule
- Staff Rule
- Wireless Authorization Rule
- VPN Authorization Rule
- Printers and other non-802.1X devices rule(s)

The non-802.1X-capable device rules, coupled with the ISE profiler, can be used to segment and limit access to/from the noninteractive network devices, such as some printers, faxes, IP Phones, and so on. This enables you to create very strict network access policies for these devices. These policies should allow them to communicate only by using protocols that match the services they provide.

## **Establishing Acceptable Use Policies**

A network acceptable use policy (AUP) is a clear and concise document that defines what users can and cannot do on a network. However, the primary focus of the AUP is to communicate to users what they cannot do. It also lays out the penalties for noncompliance and provides support contact information. Ideally, all users must accept the organization's AUP the first time they attempt to access the network and must periodically re-acknowledge the AUP thereafter. The problem has always been enforcing this requirement. Without some kind of network access control system, ubiquitous enforcement is not possible. The ISE solution supports the enforcement and auditing of network acceptable use policies.

Before creating your AUP for ISE users and guests, determine who needs to be involved and what the approval process for a final policy will look like. Create an AUP committee that includes, at a minimum, persons from the legal and IT departments. Draft a flow chart of the expected approval process the AUP will have to go through. Next, determine which documents the committee needs to produce to successfully complete the AUP. For example, to have an AUP approved in the education space, it is customary to require the following documents:

- **Justification and purpose for creating an AUP:** This typically needs to be presented to the school board and must be approved in the beginning to allow for the creation of the AUP committee.
- **A high-level AUP specifically created for or by the school board to establish the framework from which the final detailed AUP will be crafted:** It establishes the major security goals and network use guidelines. This must be approved by the school board.
- **A parent letter and permission form informing them of the AUP and the use of ISE to enforce this AUP:** This must be approved by the school board.
- **The final Acceptable Use Policy document:** Typically, this is created by the committee and presented to the school board for approval. This is the document that will be used by the ISE solution.

In general, an acceptable use policy will include these parts or sections:

- **AUP Overview or Purpose:** Serves as an introduction to the AUP.
- **AUP Scope or Coverage:** Defines who must comply with this acceptable use policy.
- **Acceptable Network Use Guidelines:** Conveys the appropriate use of the network.
- **Unacceptable or Prohibited Network Uses:** This section may have several

subsections, such as a subsection for email, copyrighted material, viruses and worms, unauthorized access, illegal activity, and so forth.

- **Violation or Enforcement Policy:** Communicates the penalties and/or legal action that could be taken against AUP violators.
- **Privacy Disclaimer:** Indicates that the organization assumes no responsibility or liability for a user's privacy while using the network.
- **Definitions:** Fully defines all acronyms and terms used in the document.
- **Legal Disclaimer:** Purpose is to release the organization from any and all legal liabilities resulting from the AUP itself or network use. Let the lawyers define this one.
- **Right to Modification:** A disclaimer communicating your ability to modify this policy at any time without notice.
- **Contact Information:** Provides users with a point of contact for additional information, questions, or complaints.

Your AUP may include more or fewer sections than those listed. The preceding list of sections should give you a general idea of what to include in your AUP.

**Tip** To find additional information about AUPs, such as "How To" guides and examples, search Google using the keywords **network acceptable use policy**. For AUP samples, check out the SANS policy site at <https://www.sans.org/security-resources/policies/>.

The ISE solution has two methods for enforcing an AUP:

- **Via a guest portal login:** Used only by users that log in via web authentication.
- **Via the Cisco AnyConnect w/ISE Posture Module Agent:** Used only by users that have the Agent installed.

Both methods can, and typically do, use and enforce the same AUP. Both methods enforce the policy by denying users network access until they acknowledge or accept the network AUP. Once they accept the policy, they are granted network access.

The enforcement of an AUP is an optional feature. Enforcement can be selectively enabled as well. Enforcement can be turned on or off based on the client's identity group. Additionally, it can be enabled and disabled based on the use of web login or the NAC agent. For example, you might want to enable AUP enforcement just for guest clients. ISE can also support enforcement of periodic AUP acceptance.

## Host Security Posture Assessment Rules to Consider

This section covers the process of how to include host posture criteria into an organization's network access security policy document. One of the powerful features of ISE when using the Cisco AnyConnect Posture Agent is its ability to perform very granular device security posture assessments and remediation on Windows and Mac devices. Therefore, your NASP should contain the checks, rules, and requirements that ISE will use. This includes the discovery, enforcement, and remediation policies that ISE will employ on Windows and Mac devices. Because the agent is loaded on the device, it has the ability to read into the device's registry, applications, services, and file system. The Cisco AnyConnect Posture Agent can be installed directly onto the client or brought down as a temporary agent via a browser. The main difference between the two methods is that the temporary web agent doesn't have the rights to perform remediation actions for the user.

The full agent offers robust remediation capabilities for a device that fails a security requirement, such as antivirus software that is not up to date. The remediation capabilities include file distribution, link distribution, delivery of instructions, and, most notably, an auto-update mechanism for antivirus, antispyware, Windows OS patches, and client firewall rules. The NASP should include the details on how devices will be remediated under different circumstances.

All posture assessment and remediation configuration is done using the ISE GUI. It is here that you define the posture policy by configuring rules based on operating system and/or other conditions that will satisfy the policies contained in your corporate NASP document. Before you create your NASP for ISE, it is important to understand the ISE process for posture assessment. This process uses a combination of policy checks, rules, and requirements. The ISE posture service checks the health (posture) of the clients for compliance with your corporate network security policies before the host gains privileged network access. The ISE Client Provisioning service deploys the AnyConnect Posture Agent to any hosts that don't have it installed and set up.

Rules like the one shown in [Figure 7-3](#) are configured at the ISE Admin node.

Condition	Description	File Path	Status
pc_W81_KB3078601_MS15-080	Cisco Predefined Check: Microsoft Windows 8.1	SYSTEM_32\Win32k.sys	Cisco-Defined
pc_XP_KB2802968_MS13-020	Cisco Predefined Check: Microsoft Windows XP SP3	SYSTEM_32\oleaut32.dll	Cisco-Defined
pc_W8_KB2727528_MS12-072	Cisco Predefined Check: Microsoft Windows 8	SYSTEM_32\synceng.dll	Cisco-Defined
pc_KB929123_2_MS07-034_Vista	Cisco Predefined Check: Microsoft Windows Vista SP2	SYSTEM_PROGRAMS\Windows\system32\kernel32.dll	Cisco-Defined
pc_KB918439_MS06-022_XP_S...	Cisco Predefined Check: Microsoft Windows XP SP2	SYSTEM_32\gdiplus.dll	Cisco-Defined
pc_W8_KB3078601_MS15-080	Cisco Predefined Check: Microsoft Windows 8.1	SYSTEM_32\Win32k.sys	Cisco-Defined
pc_W10_KB3097617_MS15-109	Cisco Predefined Check: Microsoft Windows 10	SYSTEM_32\shell32.dll	Cisco-Defined
pc_W81_KB2893294_MS13-098	Cisco Predefined Check: Microsoft Windows 8.1	SYSTEM_32\imagehlp.dll	Cisco-Defined
pc_W7_64_KB3197868_MS16-1...	Cisco Predefined Check: Microsoft Windows 7 SP1	SYSTEM_ROOT\sysnative\msctf.dll	Cisco-Defined
pc_W8_KB3124001_MS16-005	Cisco Predefined Check: Microsoft Windows 8	SYSTEM_32\Gdi32.dll	Cisco-Defined
pc_W7_64_KB3197868_MS16-1...	Cisco Predefined Check: Microsoft Windows 7 SP1	SYSTEM_ROOT\sysnative\msvcp140.dll	Cisco-Defined
pc_W7_MSXML_6_MS12-043	Cisco Predefined Check: Microsoft XML Core Services	SYSTEM_32\msxml6.dll	Cisco-Defined
pc_RDPC_64_EARLIER_6	Cisco Predefined Check: RDPC	SYSTEM_ROOT\sysnative\mssts.dll	Cisco-Defined
pc_RDPC_64_EARLIER_7	Cisco Predefined Check: RDPC	SYSTEM_ROOT\sysnative\mssts.dll	Cisco-Defined
pc_W7_64_KB2992611_MS14-066	Cisco Predefined Check: Microsoft Windows 7 SP1	SYSTEM_ROOT\sysnative\ischar.dll	Cisco-Defined
pc_Vista_KB2476490_MS11-038	Cisco Predefined Check: Microsoft Windows Vista SP2	SYSTEM_32\oleaut32.dll	Cisco-Defined
pc_KB918439_MS06-022_XP_S...	Cisco Predefined Check: Microsoft Windows XP SP2	SYSTEM_32\gpl400.dll	Cisco-Defined
pc_Vista64_KB3078071_MS15...	Cisco Predefined Check: Microsoft Windows Vista SP2	SYSTEM_ROOT\sysnative\urim.dll	Cisco-Defined
pc_W7_KB3078071_MS15-079...	Cisco Predefined Check: Microsoft Windows 7 SP1	SYSTEM_32\urimon.dll	Cisco-Defined
pc_W7_KB3078071_MS15-079...	Cisco Predefined Check: Microsoft Windows 7 SP1	SYSTEM_32\urimon.dll	Cisco-Defined

**Figure 7-3** File Condition Check Examples

ISE file condition checks, such as the ones shown in [Figure 7-3](#), are the Cisco predefined checks that are downloaded from Cisco every two hours. Checks can be groups of several checks combined together using Boolean operators. They can also be operating-system-specific.

ISE then allows you to create posture rules that combine multiple checks into a compound condition. [Figure 7-4](#) shows a sampling of the Cisco predefined rules in ISE.

Rule Name	Type	Description	Status
pr_Mcafee_Application	Cisco Predefined Rule	Cisco-Defined	
pr_Mcafee_Update	Cisco Predefined Rule	Cisco-Defined	
pr_TrendMicro_Installation	Cisco Predefined Rule	Cisco-Defined	
pr_TrendMicro_Update	Cisco Predefined Rule	Cisco-Defined	
pr_TrendMicro_App	Cisco Predefined Rule	Cisco-Defined	
pr_JTrend_VB_Corp_Installation	Cisco Predefined Rule: Check fo...	Cisco-Defined	
pr_JTrend_VB_Corp_Application	Cisco Predefined Rule: Check fo...	Cisco-Defined	
pr_JTrend_VB_Corp_Update	Cisco Predefined Rule: Check fo...	Cisco-Defined	
pr_JTrend_VB2007_Installation	Cisco Predefined Rule: Check fo...	Cisco-Defined	
pr_JTrend_VB2007_Application	Cisco Predefined Rule: Check fo...	Cisco-Defined	
pr_JTrend_VB2007_Update	Cisco Predefined Rule: Check fo...	Cisco-Defined	
pr_Fail_On_MDAC_26_KB9115...	Cisco Predefined Rule	Cisco-Defined	
pr_MS_Malware_Removal_Tool	Cisco Predefined Rule	Cisco-Defined	
pr_CSA_Agent_Version_5_0	Cisco Predefined Rule: CSA 5.0 ...	Cisco-Defined	
pr_CSA_Agent_Service_Running	Cisco Predefined Rule: CSA ser...	Cisco-Defined	
pr_XP_MCE_Hotfixes	Cisco Predefined Rule: Windows...	Cisco-Defined	
pr_XP64_Hotfixes	Cisco Predefined Rule: XP 64 bit...	Cisco-Defined	
pr_Vista32_Hotfixes	Cisco Predefined Rule: Vista 32 ...	Cisco-Defined	
pr_Win7_64_Hotfixes	Cisco Predefined Rule: Windows...	Cisco-Defined	

**Figure 7-4 Compound Condition Rules Example**

ISE requirements, like the ones shown in [Figure 7-5](#), define what remediation action is offered to any noncompliant users. In this example, the Windows System Center Configuration Manager (SCCM) service is being turned on to ensure that all SCCM-enforced updates are installed on the PC.

Requirement	For	Using	Status	Met If	Then	Edit
Any_AM_Definition_Mac	Mac OSX	using 4.x or later	using Disabled	met if ANY_am_mac_def	then	Edit
AnyAVDefRemediationMac						Edit
Any_AV_Installation_Win	Windows All	using 3.x or earlier	using Disabled	met if ANY_av_win_inst	then	Edit
Any_AS_Installation_Win	Windows All	using 3.x or earlier	using Disabled	met if ANY_as_win_inst	then	Edit
Any_AV_DefRemediationWin						Edit
Any_AS_DefRemediationWin						Edit
Any_AV_Installation_Mac	Mac OSX	using 3.x or earlier	using Disabled	met if ANY_av_mac_inst	then	Edit
Any_AV_DefRemediationMac						Edit
Any_AS_Installation_Mac	Mac OSX	using 3.x or earlier	using Disabled	met if ANY_as_mac_inst	then	Edit

**Figure 7-5 Requirement Examples**

If all matching requirement rules are passed, then the client is marked as posture-compliant. Otherwise, the client is marked posture-noncompliant. This overall status

can then be used in authorization rules to properly adapt network access privileges. [Figure 7-6](#) shows an example of restricting a noncompliant host using a downloadable ACL (dACL) that only allows hosts to get to remediation resources.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The 'Authorization Policy' tab is selected. Below the navigation, there are tabs for Overview, Network devices, Client Provisioning, Policy Elements, Posture Policy, Authentication Policy, Authorization Policy (which is selected), Troubleshoot, Reports, and Settings. The main content area displays a table of authorization rules:

Status	Rule Name	Conditions (Identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Wireless Black List Default	If Blacklist AND Wireless_Access	then Blackhole_Wireless_Access
<input checked="" type="checkbox"/>	Profiled Cisco IP Phones	If Cisco-IP-Phone	then Cisco_IP_Phones
<input checked="" type="checkbox"/>	Profiled Non Cisco IP Phones	If Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones
<input type="checkbox"/>	Compliant_Devices_Access	If (Network_Access_Authentication_Passed AND Compliant_Devices)	then PermitAccess
<input type="checkbox"/>	Employee_EAP-TLS	If (Wireless_802.1X AND BYOD_Is_Registered AND EAP-TLS AND MAC_in_SAN)	then PermitAccess AND BYOD
<input type="checkbox"/>	Employee_Onboarding	If (Wireless_802.1X AND EAP-MSCHAPv2)	then NSP_Onboard AND BYOD
<input type="checkbox"/>	Wi-Fi_Guest_Access	If (Guest_Flow AND Wireless_MAB)	then PermitAccess AND Guests
<input type="checkbox"/>	Wi-Fi_Redirect_to_Guest_Login	If Wireless_MAB	then Cisco_WebAuth
<input checked="" type="checkbox"/>	Posture_noncompliant_win	If Employee AND (Network_Access_Authentication_Passed AND Session:PostureStatus EQUALS NonCompliant AND EndPoints:PostureApplicable EQUALS Yes)	then Limited_access_noncompliant
<input checked="" type="checkbox"/>	Default	If no matches, then DenyAccess	

**Figure 7-6** Posture-Aware Authorization Rule Example

Here is a summary of the rules and requirements structure in ISE:

- Rules are made up of one or more checks that can be combined into an expression using the Boolean operators and “&”, or “|”, not “!”, and evaluation priority parentheses “()”. If the result is true, then the client passes the rule.
- Requirements are made up of one or more rules. A requirement can specify that a device must pass any selected rule, all selected rules, or no selected rules in order for the device to pass the requirement.
- Requirements also define the mechanism to use and the instructions that will allow the client to remediate any failed rules. For example: Distribute a file or link with the instructions “Click the link and download, install, and run the XYZVirus cleaning tool.”
- Requirements are mapped to authorization rules and/or operating system types.

[Table 7-1](#) shows the posture assessment options available in ISE when using the various Cisco AnyConnect Posture Agent software versions. You can see that the Windows AnyConnect Posture Agent has the most functionality of the three types.

<b>ISE Posture Agent for Windows</b>	<b>Web Agent for Windows</b>	<b>ISE Posture Agent for Mac OS X</b>
Operating System/Service Packs/Hotfixes	Operating System/Service Packs/Hotfixes	—
Service Check	Service Check	Service Check (AC 4.1 and ISE 1.4)
Registry Check	Registry Check	—
File Check	File Check	File Check (AC 4.1 and ISE 1.4)
Application Check	Application Check	Application Check (AC 4.1 and ISE 1.4)
Antivirus Installation	Antivirus Installation	Antivirus Installation
Antivirus Version/Antivirus Definition Date	Antivirus Version/Antivirus Definition Date	Antivirus Version/Antivirus Definition Date
Antispyware Installation	Antispyware Installation	Antispyware Installation
Antispyware Version/ Antispyware Definition Date	Antispyware Version/ Antispyware Definition Date	Antispyware Version/ Antispyware Definition Date
Patch Management Check (AC 4.1 and ISE 1.4)	—	Patch Management Check (AC 4.1 and ISE 1.4)
Windows Update Running	Windows Update Running	—
Windows Update Configuration	Windows Update Configuration	—
WSUS Compliance Settings	WSUS Compliance Settings	—

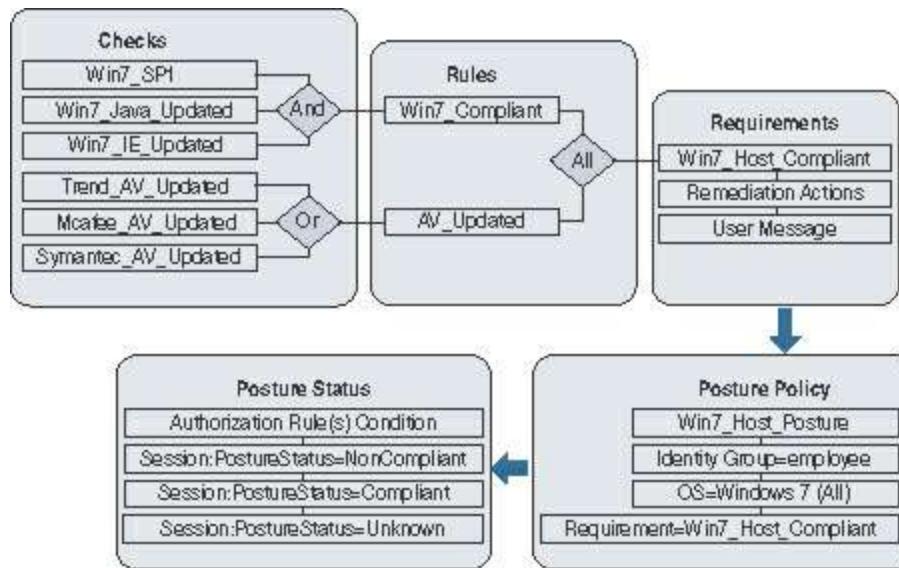
**Table 7-1** Posture Assessment Options

[Table 7-2](#) displays all of the different remediation actions that the various AnyConnect Posture Agents can perform. Again, the Windows AnyConnect Posture Agent has the most functionality. These actions can be done for the user transparently or user interaction can be implemented.

ISE Posture Agent for Windows	Web Agent for Windows	ISE Posture Agent for Mac OS X
Message Text (Local Check)	Message Text (Local Check)	Message Text (Local Check)
URL Link (Link Distribution)	URL Link (Link Distribution)	URL Link (Link Distribution)
File Distribution	File Distribution	—
Launch Program	—	—
Antivirus Definition Update	—	Antivirus Live Update
Antispyware Definition Update	—	Antispyware Live Update
Patch Management Remediation (AC 4.1 and ISE 1.4)	—	—
Windows Update	—	—
WSUS	—	—

**Table 7-2 Posture Remediation Options**

Now that we have explored all of the posture variables and features, let's take a look at a final summary flow of posture assessment in ISE. [Figure 7-7](#) illustrates the order of operations ISE takes from checks to the final posture policy evaluation.



**Figure 7-7 ISE Posture Assessment Process**

## Sample NASP Format for Documenting ISE Posture Requirements

As discussed, ISE uses several mechanisms to define what it should look for, or posture assess, on a given device. It also has several mechanisms for the proper remediation of any failed security requirements. Ultimately, the network access security privileges a client receives are based on the posture status result (for example, compliant) of a matched policy rule, which in turn is used as an authorization rule condition that the client matches. With this in mind, your NASP should have sections for each posture policy rule, and under each you should have the checks, rules, and requirements that pertain to clients of that posture policy rule. Here is a nice example of a NASP formatted in this way:

# Employee Posture Policy

Table of Contents for Employee Posture Policy:

- I. Identity Group Criteria pg xxx
- II. Acceptable Use Policy pg xxx
- III. Windows 7 Security Requirements pg xxx
  - 1. Approved AV Installed & Up to Date pg xxx
    - a. Security checks pg xxx
    - b. Security rules pg xxx

**I. Identity Group Criteria**— Any user that is a member of the employees group in Active Directory.

**II. Acceptable Use Policy**— Reference which AUP, if any, is to be enforced by ISE. For example, you might reference an AUP called Trusted\_User\_AUP. It is common that only a reference to an AUP name is put here and the actual AUP document lives in its own section within the NASP document. This allows for easy reuse of AUP policies across multiple roles.

## III. Windows 7 Security Requirements

- 1. Approved AV Installed & Up to Date

Trend\_AV\_Requirement—Link distribution that points to the Trend client download page on the corporate antivirus server.

Trend\_AV\_Requirement to Rule Mapping—Map requirement

Trend\_AV\_Installed to rule Map requirementTrend\_AV\_Installed. Requirement met if any rules succeed.

a. Security Rules –

Trend\_AV\_Installed rule—Rule expression only includes the Trend\_AV\_Installed check.

b. Security Checks –

Trend\_AV\_Installed check—Corporate Trend Micro antivirus client must be installed on all Windows devices.

The ISE solution has lots of predefined checks and rules that you can use to build your posture rules. All of the built-in checks have a pc\_ preceding their name, such as pc\_AutoUpdateCheck. All of the built-in rules have a pr\_ preceding their name, such as pr\_AutoUpdateCheck. These checks and rules are constantly updated by Cisco and are automatically downloaded by ISE. Also, ISE has auto-update support for Microsoft Windows, numerous antivirus vendors, and antispyware vendors out of the box. This

means that ISE keeps up to date with the latest versions, .dat files, and hotfixes available for each of the supported vendors automatically. Keep this in mind when creating your ISE network access security policy.

## Common Checks, Rules, and Requirements

The following are some of the most common checks, rules, and requirements implemented by administrators of the ISE solution. All of the examples shown have corresponding Cisco predefined checks and rules and are auto-updated by ISE.

- An antivirus program must be installed, running, and up to date. Most organizations specify specific AV programs for certain posture policy rules. For example, the employee posture rule may state that clients must use corporate Trend Micro AV, whereas the guest posture rule may state that clients are allowed to use any of the numerous ISE-supported AV vendors.
- An antispyware program must be installed, running, and up to date. Most organizations specify specific AS programs for certain authorization rules. For example, the employee posture rule may state that clients must use the corporate Webroot AS client, whereas the guest policy rule may state that clients are allowed to use any of the ISE-supported AS vendors.
- All Windows 7 clients must be running Service Pack 1. The built-in registry check is called pc\_W7\_SP1.
- All Windows clients must have the Windows auto-update service running. By default, ISE looks to make sure the wuauserv service is running. The built-in check is called pc\_AutoUpdateCheck. The built-in rule is called pr\_AutoUpdateCheck\_Rule.
- All 64-bit Windows 7 and 8 hosts must have installed the latest critical Microsoft security hotfixes as defined by the ISE rule pr\_Win7\_64\_Hotfixes and pr\_Win8\_64\_Hotfixes, respectively. These rules, and their corresponding checks, are continuously updated by Cisco. They include the most critical security hotfixes for Windows 7 and Windows 8 operating systems. They do not, however, include every security update that Microsoft has ever released for each operating system. If you require additional hotfixes, you can duplicate the relevant pr\_Win\_64\_Hotfixes predefined rule to include them.
- All requirements dealing with the updating of antivirus and antispyware programs will use the built-in AV Definition Update type. These rules are preconfigured to map to the matrix of AV and AS vendors and products supported by ISE. These rules do not require you to configure any checks and are continuously updated by Cisco. If the user fails these requirements, the user can be presented with an Update button. When clicked, this Update button auto-launches the update program for the

AV or AS program that failed the policy.

## Method for Adding Posture Policy Rules

Many organizations do not have a process in place to determine if, when, and how a security update should be added to their network access security policy document. Organizations that lack this type of process, or method, are in greater danger of making bad decisions about the security updates they choose to install. For this reason, it is important for organizations to establish and follow a formal method for adding and updating their posture policy rules. This section deals with this topic as it pertains to the initial creation and subsequent revisions of the NASP document. Knowing which host security patches to enforce using ISE is a big job. The goal is to provide the information necessary for you to set up your own method, or process, for determining which posture rules you want to include in your initial NASP for ISE. A secondary goal is to provide the information necessary for you to set up your own method, or process, for determining when to add, change, and delete the checks, rules, and requirements that make up your host posture policy rules in ISE.

## Research and Information

The ISE solution comes with many preconfigured checks and rules, such as the ones described previously. Simply implementing these built-in policies will go a long way toward increasing the security posture of most organizations' devices and networks. However, these are by no means the only security checks and rules that are available. In many cases, your organization may choose to implement checks, rules, and requirements that are beyond the scope of the predefined ones. When this occurs, it is vital that you are able to find the information and research needed to make the most informed decision possible. Regardless of whether or not the security fixes you put in place use the built-in policies, custom policies, or a combination of both, it is vital that you understand the purpose of the fixes, their impact, and their severity level. It is also necessary to remain informed about the emergence of new vulnerabilities, exploits, and viruses. Obtaining this information is not always trivial. Following are some of the commonly used security websites, blogs, and resources available online. Most are free but some also offer a paid service.

- **SecurityFocus** (<http://www.securityfocus.com>): Famous for its Bugtraq list. This is one of the best places for obtaining the latest vulnerability information.
- **SecLists.Org Mailing Lists** (<http://seclists.org>): This site is a mashup of the best security sites. It is your one-stop shop for staying in the know on the latest security news.
- **Microsoft TechNet Security Center** (<https://technet.microsoft.com/en->

[us/security/](#)): This web portal serves as a good jumping-off point for investigating any Microsoft security vulnerabilities, updates, and exploits.

- **Microsoft Security Bulletin** (<https://technet.microsoft.com/en-us/security/bulletins>): This website has a nice search engine for Microsoft security bulletins. The site also has a link to sign up to receive security bulletins via email or RSS. The search engine allows you to search for vulnerabilities based on severity level and operating system type and version.
- **National Cyber Awareness System** (<https://www.us-cert.gov/ncas/>): The U.S. Computer Emergency Readiness Team (US-CERT) created this website to ensure that you have access to timely information about security topics and threats. You can sign up to receive alerts from US-CERT.
- Government sites such as the **National Vulnerability Database** (<https://nvd.nist.gov>) and **U.S. Computer readiness team** (<https://www.us-cert.gov>) are filled with timely security alert information and are vendor-agnostic.
- **Metasploit** (<https://www.metasploit.com>): This site does not offer any security information but does provide a very easy-to-use security tool that will help you test the security of your devices.
- **Cisco Security** (<https://tools.cisco.com/security/center/home.x>): This website serves as a security portal to find information regarding security bulletins from all the major application and operating system vendors. It also provides a wealth of cybersecurity reports and response bulletins.

These websites and others like them can be found throughout the Internet. They can be powerful tools for gathering the security information needed to make an informed decision on which security patches ISE should enforce.

## **Establishing Criteria to Determine the Validity of a Security Posture Check, Rule, or Requirement in Your Organization**

Your organization's network access security policy should have a section that documents the criteria to be used to decide if a proposed security check, rule, or requirement needs to be added to ISE. The establishment of set criteria will serve to improve the accuracy of the decision process. The criteria used should be tailored for your specific environment and should refrain from using generalities whenever possible. The more fine-grained the criteria used, the more informed the decision process will be.

For every proposed and existing security fix in the NASP, and subsequently in ISE, you should be familiar with, or know where to obtain, the following information regarding a security vulnerability:

- What products, applications, and versions are affected?
- What is the severity level or Common Vulnerability Scoring System (CVSS) score? See <https://www.first.org/cvss> for more information on CVSS.
- What is the potential impact or risk to the organization if the vulnerability is exploited? This point should be explored in detail, noting a best- and worst-case scenario.
- Can the vulnerability be exploited remotely?
- Are exploits publicly available?
- Is the use of the affected software widespread in your organization?
- Are the ports, protocols, and devices in question being blocked using a firewall, IPS, personal firewall, or ISE already? If so, to what extent does this mitigate the exploit risk?
- Is a patch available for the vulnerability?
- If a patch is available, is it possible to test the patch to make sure it works as advertised?
- If no testing can be done, is the risk of deploying a faulty patch less than the risk of the vulnerability?
- If no patch is available, is it possible to use any of the security features in ISE to help mitigate this feature? If no, is it possible to use any other security products to do so?

Before taking action, it is important to understand what the expected overhead on the IT staff might be if the new patch or fix is implemented. This should be explored in detail, noting a best- and worst-case scenario. Here are some of the topics for consideration:

- How stable is the new patch?
- Is additional helpdesk load necessary?
- Is additional IT staff load necessary?
- What is required of the end-user community?
- Was additional network load created due to deployment of new patches?
- If deploying patches over the WAN, what is the potential impact?
- Who will perform any testing needed? What resources are required to perform the testing?
- What is needed to set up the deployment method for distributing the patch or update?
- What is the expected impact on and reactions from the user community if the fix for the vulnerability is rolled out?

## **Method for Determining What Posture Policy Rules a Particular Security Requirement Should Be Applied To**

Once you have decided that a security fix or patch should be deployed in your environment, the next step is to decide which posture rules should receive the fix or if you should create a new rule. Additionally, it is important to determine whether the fix should be mandatory or optional. This might vary based on posture rule. It is a best practice to deploy new security requirements as optional first and then, after a set amount of time, make them mandatory. This results in the least impact possible on the user community. However, if a vulnerability poses significant risk to the organization, then the new security requirement should be rolled out as mandatory initially.

Here are some things to consider when deciding which posture rules should receive a new security requirement:

- Do all identity groups run the affected software?
- Do any of the identity groups pose a greater risk than others if the patch causes adverse affects on clients? In other words, do certain posture rules contain clients that, if debilitated due to a bad patch, would significantly affect the organization? If so, would starting with less-risky rules first to further assess the robustness of the patch make sense?
- Do any posture rules have an elevated exposure to the vulnerability in question? If so, does this elevated exposure warrant mandatory enforcement of the new security requirement?
- Does the security requirement apply to the guest posture rule, if one exists?

## **Method for Deploying and Enforcing Security Requirements**

Once you have decided that a security requirement should be added to the NASP and ISE, you need to come up with a deployment strategy. As previously discussed in [Table 7-2](#), a requirement remediation has the following options: file distribution, link distribution, launch executable, message only, AV definition update, AS definition update, and Windows update.

The easiest options to deploy are the update types because they use the built-in deployment and updating mechanisms already configured on the local device. For example, the requirement type of Windows update uses the Windows Update service already present on and configured for the client that needs the updates.

Regardless of the requirement type chosen, the following deployment questions should be considered:

- Should the deployment method be the same for all posture rules?

- Which deployment method would be the most efficient at reaching the posture rules in question?
- Should the enforcement of the new security requirement be optional, audit, or mandatory in the beginning? Does this vary by posture rule or identity group?
- If optional, should the requirement be made mandatory at some point in time? If so, define the time period between optional and mandatory. Does this vary by posture rule?
- If audit only, what is the goal of the audit? What will be done with the data collected?
- Will it ensure clients in quarantine have privileges to access the proposed remediation resources? For example, if you use a link to [www.fixme.com](http://www.fixme.com) as your deployment method, you need to ensure that access to this URL is not restricted.

## Defining Dynamic Network Access Privileges

The ISE solution has several methods available to dynamically grant and restrict the network access privileges of clients. Most of these methods are defined per authorization rule. A network access security policy for ISE should include details on which network access privileges should be given to which authorization rules and devices. The authorization rules should take into consideration the posture status of a device (unknown, compliant, noncompliant) to determine the access privileges given. Here is an example that uses access control rules in ISE: A client in the contractor authorization rule should be granted access to the Internet only on TCP ports 80 and 443, and should be denied access all other network access. The following common and easily understandable syntax can be used for documenting ISE access control policies in the NASP. Typically, these rules are found under their corresponding authorization rule section in the NASP.

[Click here to view code image](#)

```
<line #> Permit|Deny <protocol> from <device(s) | network(s)> to <device(s) | network(s)> equaling | not equaling port(s) <list of port numbers or names>
Description: <explanation of rule>
```

The previous example would be written in the NASP under the contractor authorization rule/traffic control subsection as follows:

[Click here to view code image](#)

```
10 Deny IP from any to any internal network
Description: Block IP traffic from anyone to any internal subnet or device.
20 Permit tcp from guest authorization rule to any equaling ports 53,80 & 443
Description: Allow web traffic from clients in the guest authorization rule to the internet
```

30 Deny IP from guest authorization rule to any  
Description: Block everything else

Formatting the rules in this way not only makes them unambiguous but allows them to be easily translated into the traffic control rules configured in the ISE Manager.

## Enforcement Methods Available with ISE

ISE supports numerous types of permissions that can be applied to an authorization rule result. Not all enforcement methods supported by ISE are supported in all modes of operation. This issue applies mostly to limitations of the hardware the client is connected to. For example, to support security group tagging, the wired switch or wireless controller has to support it. [Table 7-3](#) lists the different network access control permission methods available and provides a brief description for each.

Enforcement or Control Method	Description
Access control rules	The equivalent of network ACLs. They permit and deny traffic like a stateless firewall would.
VLAN segmentation	Dynamically changing the Layer 2 VLAN based on the authorization rule matched by the connected client.
Smartport Macro	Ability to run the macro that can affect just about anything on that switch port, including QoS settings.
Reauthentication	The timer serves as an absolute time limit for a client in a given authorization rule. Once the timer is expired, the client is reauthenticated.
Security Group Tag	Cisco TrustSec tag applied by the network to every frame sent from the client. Requires switch or WLC support.
MACsec encryption	Wire-speed Layer 2 encryption via 802.1ae. Requires switch or WLC support.
Web authentication	Forces a URL redirect to a web authentication page.
Cisco RADIUS AV pair values	Almost any Cisco or other vendor AV pair can be manipulated with ISE as part of authorization permissions.

**Table 7-3** ISE Authorization Rule Permissions

## Commonly Used Network Access Policies

In short, a network access policy defines what a user and device can and cannot do on

the network. Although the exact rules that make up any network access policy will be customized for a particular environment, there are some commonalities shared between organizations. This section focuses on those common elements. Your NASP typically covers all of the enforcement methods ISE supports (see [Table 7-3](#)). Access control lists are almost always tied to an authorization rule in ISE. Some authorization rules (such as guest) usually have very restrictive network access policies, while others typically are wide open (such as employee). Also, it is always a best practice to lock down the network access rule on any noncompliant posture authorization rule.

Here are some popular or mandatory authorization rules shown with a common example of their associated NASP. This is formatted for an ISE NASP. You can choose to use this NASP format or develop your own. It is important to ensure that your NASP is well documented. Note that these pick up where the earlier sample NASP left off, at section IV. (See the section “Sample NASP Format for Documenting ISE Posture Requirements.”)

## **Employee Authorization Rule**

Table of Contents for Employee Security Policy:

- I. Members pg xxx
- II. Acceptable Use Policy pg xxx
- III. Windows 7 Security Requirements pg xxx
  - 1. Approved AV Installed & Up to Date pg xxx
    - a. Security checks pg xxx
    - b. Security rules pg xxx
- IV. Network Access Permissions pg xxx
  - 1. VLAN Segmentation pg xxx
    - a. Noncompliant Posture VLAN pg xxx
    - b. Access VLAN Name/ID pg xxx
  - 2. Access Control List pg xxx
  - 3. Auto Smartports Macro pg xxx
  - 4. SGT number pg xxx
- IV. Network Access Permissions
  - 1. VLAN Segmentation – Yes
    - a. Noncompliant Posture VLAN = quarantine-vlan/100
    - b. Access VLAN Name/ID = employees/10

## 2. Access Control List – Yes

### a. Compliant ACL = permit All IP

### b. Noncompliant ACL =

5 Permit TCP from any to "AUP web server" equaling 80

Description: Allow anyone to access the acceptable use policy link

10 Permit TCP from any to "Link based remediation resources" equaling 80 & 443

Description: Allow web traffic to the appropriate remediation resources

20 Permit TCP from any to "file based remediation" equaling 80 & 443

Description: Allow web traffic to the cam for remediation file distribution

30 Permit UDP from any to "dmz DNS Server" equaling DNS

Description: Allow DNS only to the dmz dns server

40 Deny IP from any to any

Description: Block everything else

## 3. Auto Smartports Macro – no

## 4. SGT number – 10

The subsequent partial example does not show the full NASP format. Only the sections relevant to the network access permissions are shown.

### Guest Authorization Rule

## 1. VLAN Segmentation – Yes

### a. Noncompliant Posture VLAN = None, no posture required

### b. Access VLAN Name/ID = guest/20

## 2. Access Control List –

10 Permit UDP from any to "dmz DNS Server" equaling DNS

Description: Allow DNS but only to the dmz dns server

20 Deny IP from any to any internal network

Description: Block IP traffic from guests to any internal subnet or device.

30 permit IP from host to any external IP subnet

Description: Allow everything not internal

## 3. Auto Smartports Macro – no

## 4. SGT number – 20

## Summary

This chapter examined the intricacies of creating a network access security policy for a Cisco ISE deployment. It included the following recommendations:

- Create and follow a NASP checklist.
- Make sure to obtain executive buy-in for the creation and subsequent enforcement of a NASP.
- Create a NASP committee. Be sure to involve the right people.
- Determine your organization's high-level network access security goals. Use these as guides when creating the detailed network access security policy.
- Break up your organization into security domains.
- Determine and create the authorization rules necessary for your organization.
- Create one or more acceptable use policies.
- Determine if host posture checks will be used. If so, decide what checks, rules, and requirements will be enforced for each posture rule.
- Establish and follow a method for adds, moves, and changes to authorization rules and posture rule checks, rules, and requirements.
- Determine a method for deploying the AnyConnect Posture Agent and/or remediation resources.
- Determine which network access permissions should be assigned to each authorization rule.
- Either use the NASP document formatting shown throughout this chapter or pick your own formatting. It is important to document your NASP in a concise and easily understood manner.

# Chapter 8 Building a Device Security Policy

This chapter covers the following topics:

- ISE device profiling
- Threat-Centric NAC

Cisco Identity Services Engine takes into account the security of the individual devices when determining which network access control policy to invoke. [Chapter 7, “Building a Cisco ISE Network Access Security Policy,”](#) discussed the creation of a network access security policy (NASP), part of which took into account the device’s security posture. Device posture assessment is one of several tools that Cisco ISE can use to determine the actual security of a network-connected device. ISE can also use the following features to determine the device security policy to implement:

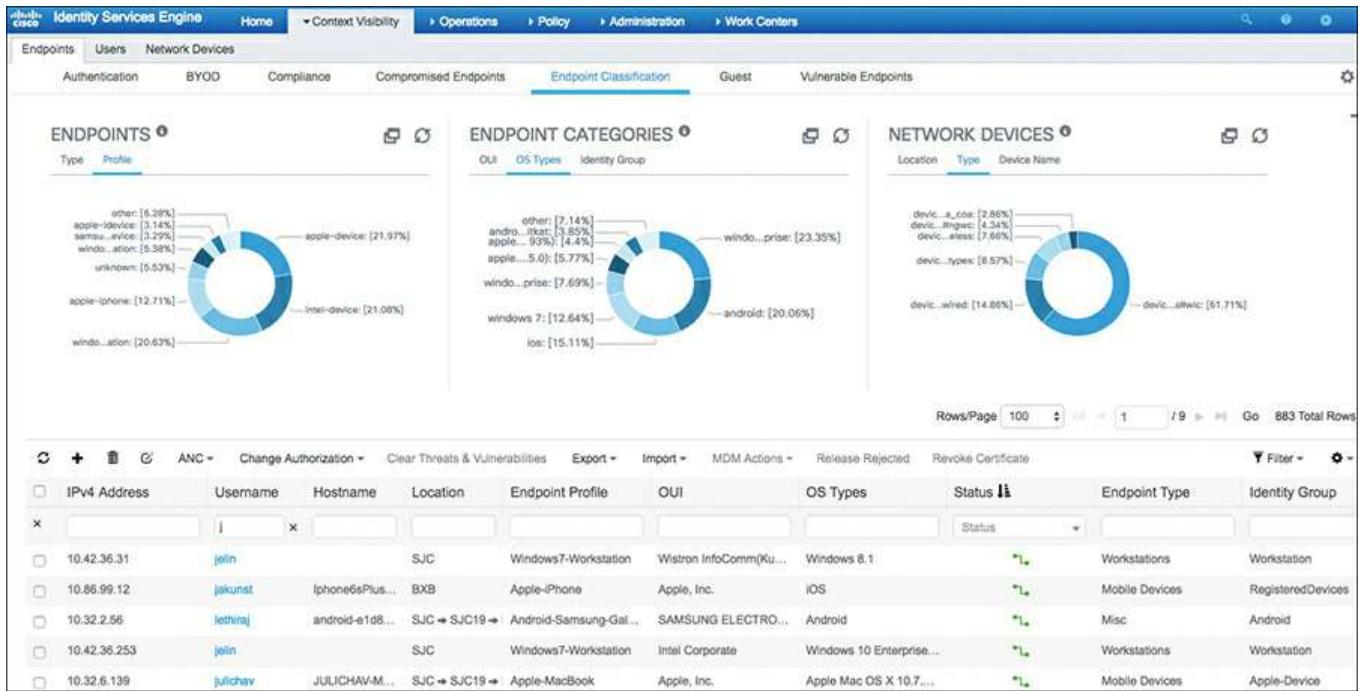
- Device profiling
- Threat-Centric NAC

This chapter explores these features in some detail. The goal is to disclose the different ways in which ISE can identify device types and other contextual information about devices for use in an ISE policy.

## ISE Device Profiling

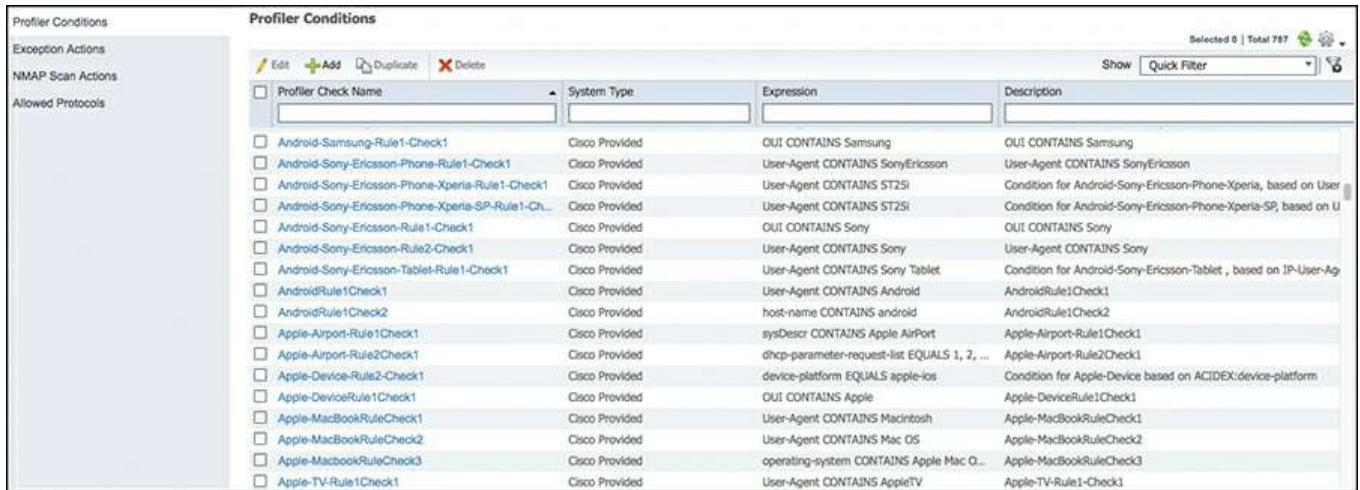
ISE includes a built-in device profiling function. ISE device profiling is one of the most useful and easy-to-deploy ISE features. All ISE deployments should include profiling in their setup. ISE profiling collects both passive and active device data, including device behavior, to determine what kind of device it is seeing. Profiling is capable of showing you all the devices that are connected to your network, their type, their behavior, and the logged-in user.

Cisco ISE includes hundreds of built-in profiling rules and device profiler conditions. These are updated dynamically using the profiler feed service. ISE profiling gathers information from multiple data sources to make a device type determination. This information is matched against the ISE profiler conditions until a best match is made. That condition is then used to match a profiler policy rule. Once a profiler policy rule is matched, the result can then be used as an ISE authorization rule condition. It is in this way that ISE can provide different network privileges based on a device profile. [Figure 8-1](#) shows a sampling of the visibility you have with ISE profiler.



**Figure 8-1 ISE Profiler Endpoint Context Visibility**

Each condition shown in [Figure 8-2](#) depicts a sampling of the ISE profiler conditions that come preinstalled with ISE. ISE will also receive updated and new profiles through its profiler feed service. The feed service connects to [Cisco.com](#) to see if any new profile data is available for download. If so, it will download and update its profiling database accordingly.



**Figure 8-2 ISE Profiler Conditions**

The policy shown in [Figure 8-3](#) shows just one of four checks that are used to determine if a device is an Apple iPad.

Profiler Condition List > Apple-iPadRule1Check1

### Profiler Condition

* Name	<b>Apple-iPadRule1Check1</b>	Description	Apple-iPadRule1Check1
* Type	IP		
* Attribute Name	User-Agent		
* Operator	CONTAINS		
* Attribute Value	iPad		
System Type	Cisco Provided		
<input type="button" value="Save"/> <input type="button" value="Reset"/>			

**Figure 8-3** ISE Apple iPad Profiler Conditions

The example condition shown in [Figure 8-3](#) matches the user-agent string from a web browser.

## ISE Profiling Policies

The Cisco ISE conditions just discussed are used to create your ISE device profile policies. Sticking with the Apple iPad profile example, [Figure 8-4](#) shows the profiler policy that uses the iPad condition shown in [Figure 8-3](#).

Profiling

Profiler Policy List > Apple-iPad

### Profiler Policy

* Name	<b>Apple-iPad</b>	Description	Policy for Apple iPads
Policy Enabled	<input checked="" type="checkbox"/>		
* Minimum Certainty Factor	20	(Valid Range 1 to 65535)	
* Exception Action	NONE		
* Network Scan (NMAP) Action	NONE		
Create an Identity Group for the policy	<input checked="" type="radio"/> Yes, create matching Identity Group <input type="radio"/> No, use existing Identity Group hierarchy		
* Parent Policy	Apple-Device		
* Associated CoA Type	Global Settings		
System Type	Cisco Provided		
<b>Rules</b>			
If Condition	Apple-iPadRule2Check2	Then	Certainty Factor Increases 20
If Condition	Apple-iPadRule1Check1	Then	Certainty Factor Increases 20
<input type="button" value="Save"/> <input type="button" value="Reset"/>			

**Figure 8-4** ISE Apple iPad Profiler Policy

The policy shown in [Figure 8-4](#) uses two rules. Both rules, if matched, will raise the certainty factor by 20 points. This profiler policy defines that the minimum certainty

factor for this policy to be matched is 20. It is also important to note that in order for this policy to even be processed by ISE, the defined parent policy must have been matched first by the device being profiled. The parent policy in this Apple iPad policy is shown to be Apple-Device.

When you are creating your device security policy for Cisco ISE, be sure to include the logic that is used by ISE profiler in that policy. A profile is made up of two mandatory components, conditions (as shown in [Figure 8-3](#)) and policy rules (as shown in [Figure 8-4](#)), and one optional component, Logical Profiles. The policy should include the following for any custom-created profiles needed:

- **Device Profile Condition(s) Definition:** Match criteria needed (that is, user-agent string, MAC OUI, DHCP hostname, etc.).
- **Device Profile Policy:**
  - Rules definition of policy and amount to raise the certainty factor. Rules use the conditions above.
  - Define the minimum certainty factor for the policy.
  - Define any parent policies.
  - If you want to use this in an authorization policy, then check Yes, Create Matching Identity Group.
- **Device Logical Profile (optional):** A grouping of multiple profile policies into a single logical profile rule.

## ISE Profiler Data Sources

To create a profiler condition to match against, you first need to understand what match criteria is offered by Cisco ISE. [Figure 8-5](#) shows the various types of conditions that can be used to match a device's behavior against.



**Figure 8-5** ISE Profiler Condition Types

Each of these 15+ condition types has several subtypes to choose from as well. This allows you to create very specific conditions on which to match against. For example, the IP type can match against a specific browser user-agent string.

**Note** In an ISE distributed deployment, the Profiler Service runs as a part of the Policy Service node but the profiler configuration is done from the Admin node.

## Using Device Profiles in Authorization Rules

Once you have your profiler policies in place and matching correctly on devices, you now need to configure ISE authorization rules to use your profiles. [Figure 8-6](#) depicts an example of a rule that matches on Apple iPad devices that are accessing the network using wireless. The resulting permissions are to restrict iPads to only Internet access.

Standard			
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Wireless Black List Default	If <b>Blacklist AND Wireless_Access</b>	then <b>Blackhole_Wireless_Access</b>
<input checked="" type="checkbox"/>	Profiled Cisco IP Phones	If <b>Cisco-IP-Phone</b>	then <b>Cisco_IP_Phones</b>
<input checked="" type="checkbox"/>	Restrict Apple iPads	If <b>Apple-iPad AND Wireless_Access</b>	then <b>Internet_Only</b>

**Figure 8-6** ISE Apple iPad Authorization Policy

## Threat-Centric NAC

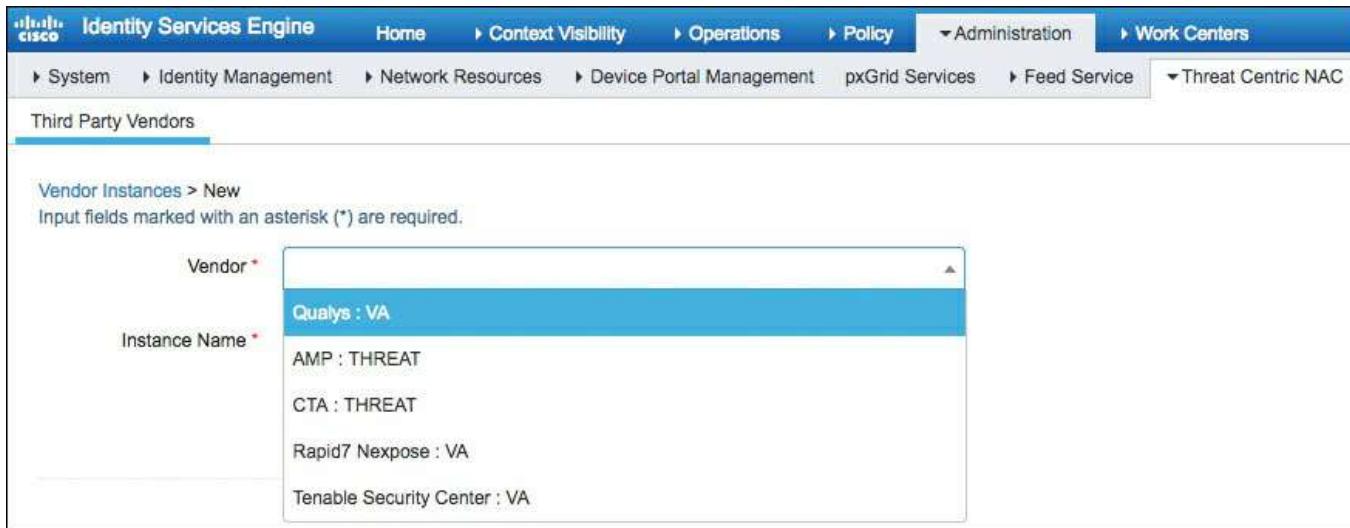
Threat-Centric Network Access Control (TC-NAC) was added to ISE in 2.1 and expanded in subsequent releases. TC-NAC enables ISE to collect threat and vulnerability data from many third-party threat and vulnerability scanners and software. This gives ISE a threat and risk view into the hosts it is controlling access rights for. TC-NAC enables you to have visibility into any vulnerable hosts on your network and to take dynamic network quarantine actions when required. ISE can create authorization policies based on vulnerability attributes, such as Common Vulnerability Scoring System (CVSS) scores, received from your third-party threat and vulnerability assessment software. Threat severity levels and vulnerability assessment results can be used to dynamically control the access level of an endpoint or a user.

You can configure the external vulnerability and threat software to send high-fidelity Indications of Compromise (IoC), Threat Detected events, and CVSS scores to Cisco ISE. This data can then be used in ISE TC-NAC authorization policies to dynamically or manually change an endpoint's network access privileges accordingly.

You should write ISE TC-NAC policies and rules into your NASP device security policy just like you did for ISE profiler in [Chapter 7](#). You should determine which vendors should be added to ISE, at which CVSS score thresholds action should be taken, and which action ISE should take based on a threat or VA issue. These and other policy considerations are discussed in this section.

As of version 2.2, Cisco ISE supports the following adapters, as shown in [Figure 8-7](#):

- Cisco Advanced Malware Protection (AMP) for Endpoints
- Cisco Cognitive Threat Analytics (CTA)
- Qualys
- Rapid7 Nexpose
- Tenable Security Center



**Figure 8-7 ISE TC-NAC Software Support**

[Figure 8-7](#) also shows that some of the supported vendors send threat data to ISE (designated as THREAT) while others send Vulnerability Assessment (VA) data to ISE. When a vulnerability event is received for an endpoint, Cisco ISE can automatically trigger a Change of Authorization (CoA) for that endpoint. However, a CoA is not triggered automatically when a threat event is received and must be done manually.

To take action on a host with a threat event, go the **Context Visibility > Endpoints > Compromised Endpoints** page and select the endpoint(s). Next, click **ANC** (Adaptive Network Control) and select **Assign a Policy**. Select the policy, such as Quarantine, to assign to the endpoint(s). Now Cisco ISE triggers a CoA for that endpoint(s) and applies the corresponding ANC policy. If an ANC policy is not available, Cisco ISE triggers a CoA for that endpoint and applies the original authorization policy. You can use the Clear Threat and Vulnerabilities option on the Compromised Endpoints page to clear the threat and vulnerabilities ISE associated with an endpoint.

The following ISE dictionary attributes can be used in creating ISE authorization conditions:

- CTA-Course\_Of\_Action (values can be Internal Blocking, Eradication, or Monitoring)
- Qualys-CVSS\_Base\_Score
- Qualys-CVSS\_Temporal\_Score
- Rapid7 Nexpose-CVSS\_Base\_Score
- Tenable Security Center-CVSS\_Base\_Score
- Tenable Security Center-CVSS\_Temporal\_Score

The valid CVSS range is from 0 to 10 for both Base Score and Temporal Score attributes. Zero is benign while a score of nine to ten is usually considered critical. For

more information on CVSS scoring, see <https://www.first.org/cvss>.

You can create an authorization policy by using the vulnerability CVSS score or the CTA result to dynamically quarantine or change the access permissions of a host. [Figure 8-8](#) shows a couple sample authorization rules. As you can see, all of the authorization attributes, such as User ID, in ISE can be added to a threat exception rule.

The screenshot shows the 'Authorization Policy' configuration page in ISE. The top navigation bar includes tabs for Authentication, Authorization (which is selected), Profiling, Posture, Client Provisioning, and Policy Elements. A sub-header 'First Matched Rule Applies' is visible. The main content area is titled 'Exceptions (2)'. It lists two entries:

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
	Threat_VA_Detected	If Employee AND Threat:Qualys-CVSS_Base_Score GREATER 7 OR Threat:Rapid7_Nexpose-CVSS_Base_Score GREATER 7 OR Threat:Tenable Security Center-CVSS_Base_Score GREATER 7	then Quarantined_Systems AND Quarantine
	Threat_CTA_Detected	If Threat:CTA-Course_Of_Action EQUALS Internal Blocking OR Threat:CTA-Course_Of_Action EQUALS Eradication	then Quarantined_Systems AND Quarantine

Below this, under 'Standard' rules, there are three more entries:

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
	Wireless Black List Default	If Blacklist AND Wireless_Access	then Blackhole_Wireless_Access
	Profiled Cisco IP Phones	If Cisco-IP-Phone	then Cisco_IP_Phones
	Restrict Apple iPads	If Apple-iPad AND Wireless_Access	then Internet_Only

**Figure 8-8** ISE TC-NAC Authorization Exception Rule

**Note** The Threat-Centric NAC service requires an ISE Apex license.

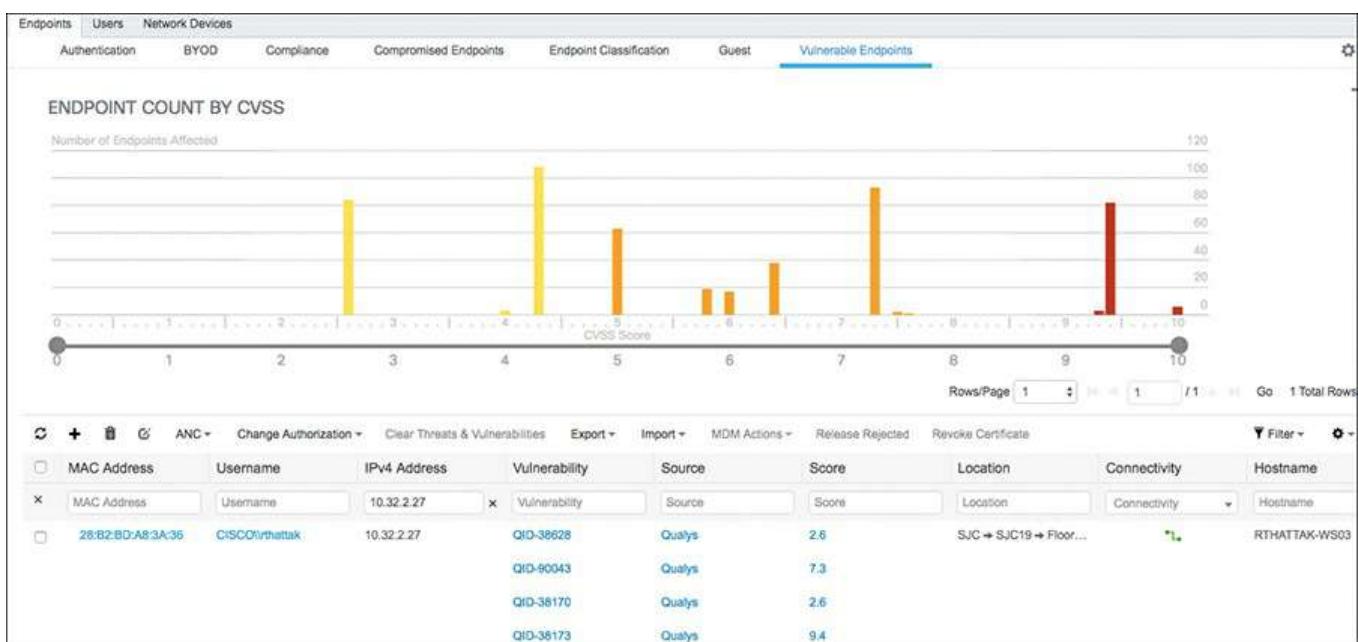
## Using TC-NAC as Part of Your Incident Response Process

You should consider adding some TC-NAC procedures to your security Incident Response (IR) policy. This section reviews the various ISE TC-NAC screens that are good to consult during a live IR investigation. Let's start with the TC-NAC Live Log screen, which displays the incident type, adapter name, matching authorization rule, and authorization profiles (old and new) for an endpoint. You can also view the detailed information for an event. To access the TC-NAC Live Log screen go to **Operations > Threat-Centric NAC Live Logs**.

Even more powerful is the **Context visibility > Endpoints** page. Here you can view and sort based on all sorts of contextual information, such as Authentication, Compromised Endpoints and Vulnerable Endpoints. [Figure 8-9](#) shows the full list of submenu choices for Endpoints in Context Visibility. You can use the filters in each of these submenus to quickly find the endpoint(s) under investigation.

**Figure 8-9** ISE TC-NAC Incident Response Pages

You can view the vulnerability information for endpoints on the Vulnerable Endpoints page. [Figures 8-10](#) and [8-11](#) show how you can quickly filter based on whatever incident information you have available to find much more context about the hosts in the incident under investigation. [Figure 8-10](#) shows using just an IP address to filter on. Immediately, you have all sorts of other useful information.



**Figure 8-10** ISE TC-NAC Vulnerable Endpoints

Endpoints    Users    Network Devices

Filters: \*10.32.2.27

Endpoints > QID-38173

28:B2:BD:A8:3A:36   

MAC Address: 28:B2:BD:A8:3A:36  
 Username: CISCO\rthattak  
 Endpoint Profile: Windows7-Workstation  
 Current IP Address: 10.32.2.27  
 Location: SJC ➔ SJC19 ➔ Floors2and4

Applications    Attributes    Authentication    Threats    Vulnerabilities

**QID-38628**

Title: SSL/TLS Server supports TLSv1.0  
 CVSS score: 2.6  
 CVEIDS:  
 Reported by: Qualys  
 Reported at: Tue Jan 03 10:52:19 PST 2017

**QID-90043**

Title: SMB Signing Disabled or SMB Signing Not Required  
 CVSS score: 7.3  
 CVEIDS:  
 Reported by: Qualys  
 Reported at: Tue Jan 03 10:52:19 PST 2017

**Figure 8-11 ISE TC-NAC Vulnerable Endpoint Detail**

From that one IP address, ISE is able to tell you who is logged into the host, the location and switch port the host is connected to, hostname, OS, vulnerabilities, active threats, applications running, and much more. Having this type of information at your fingertips can greatly speed up your incident response investigation.

For TC-NAC specific reports go to **Operations > Reports > Threat Centric NAC**. The following reports are available for the Threat-Centric NAC service:

- **Adapter Status:** The Status report displays the status of the threat and vulnerability external software connection.

- **COA Events:** When a vulnerability event is received for an endpoint, Cisco ISE triggers a CoA for that endpoint. The CoA Events report displays the status of these CoA events. It also displays the old and new authorization rules and the profile details for these endpoints.
- **Threat Events:** The Threat Events report provides a list of all the threat events that Cisco ISE receives from the various adapters that you have configured. Vulnerability Assessment events are not included in this report.
- **Vulnerability Assessment:** The Vulnerability Assessment report provides information about the assessments that are happening for your endpoints. You can view this report to check if the assessment is happening based on the configured policy.

## Summary

This chapter covered the features and functionality that Cisco ISE has for enforcing a device security policy and providing you with great device visibility and posture awareness. The three main features Cisco ISE has for this job are host posture assessment (covered in [Chapter 7](#)), Threat-Centric NAC, and device profiling. A device security policy for your organization should be written very similarly to the logic structure that Cisco ISE uses for device posture assessment, Threat-Centric NAC, and profiling. This will ease the translation from written policy to ISE policy.

# Chapter 9 Building an ISE Accounting and Auditing Policy

This chapter covers the following topics:

- Why you need accounting and auditing for ISE
- Using PCI DSS as your ISE auditing framework
- Cisco ISE user accounting

Keeping track of what is happening inside the network and inside of ISE is critical to understanding how the ISE solution is behaving. It is also critical for compliance and internal audit reasons. For example, auditing the changes that each ISE administrator makes to the configuration is extremely important. ISE Accounting is the mechanism that absorbs the RADIUS accounting packets from network devices such as switches, Wireless LAN Controllers, and ASA VPN headends. ISE Auditing is the logging and reporting of everything that happens internal to ISE. This includes administrator configuration changes, ISE system health, processing of ISE rules, and full logging of authentication and authorization activities.

**Note** In a distributed ISE deployment, the Policy Administration Node (PAN) handles all system-related configuration and configurations auditing. The Policy Service Node (PSN) handles all of the network access device (NAD) RADIUS accounting packets. All of the relevant information is also sent from the other nodes to the Monitoring & Troubleshooting Node (MnT) for purposes of creating accounting and auditing reports.

## Why You Need Accounting and Auditing for ISE

Logging mechanisms, such as RADIUS accounting and ISE configuration auditing, provide the ability to track user and administrator activities. This is critical in preventing, detecting, or minimizing the impact of a security compromise. This information can also speed along an incident response investigation. The presence of these logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise or just a configuration mistake is very difficult, if not impossible, without accounting and auditing records.

Creating a comprehensive ISE audit trail is necessary for passing many of your compliance audits. The Payment Card Industry Data Security Standard (PCI DSS), a standard for the protection of credit card data, provides a robust framework for auditing requirements. It is highly likely that if you follow the auditing recommendations in the

PCI DSS standard, you will pass most other types of logging audits. It is for that reason that we are reusing much of the PCI DSS framework for the ISE accounting and auditing policy recommendations in this chapter.

## Using PCI DSS as Your ISE Auditing Framework

PCI DSS Requirement 10, “Track and monitor all access to network resources and cardholder data,” and its subrequirements lay out a nice framework you can use to build your own auditing policy for Cisco ISE. [Table 9-1](https://www.pcisecuritystandards.org/document_library) depicts the relevant section from the PCI DSS 3.2 standard (available at

[https://www.pcisecuritystandards.org/document\\_library](https://www.pcisecuritystandards.org/document_library)). The left column describes the requirement and the right column describes how you could audit that requirement to ensure it is being met. The Cisco ISE solution is capable of meeting all of PCI Requirement 10.

PCI DSS Requirements	Testing Procedures
10.1 Implement audit trails to link all access to system components to each individual user.	10.1 Verify, through observation and interviewing the system administrator, that: <ul style="list-style-type: none"><li>■ Audit trails are enabled and active for system components.</li><li>■ Access to system components is linked to individual users.</li></ul>
10.2 Implement automated audit trails for all system components to reconstruct the following events:	10.2 Through interviews of responsible personnel, observation of audit logs, and examination of audit log settings, perform the following:
10.2.1 All individual user accesses to cardholder data	10.2.1 Verify all individual access to cardholder data is logged.
10.2.2 All actions taken by any individual with root or administrative privileges	10.2.2 Verify all actions taken by any individual with root or administrative privileges are logged.

10.2.3 Access to all audit trails	10.2.3 Verify access to all audit trails is logged.
10.2.4 Invalid logical access attempts	10.2.4 Verify invalid logical access attempts are logged.
10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges	10.2.5.a Verify use of identification and authentication mechanisms is logged. 10.2.5.b Verify all elevation of privileges is logged. 10.2.5.c Verify all changes, additions, or deletions to any account with root or administrative privileges are logged.
10.2.6 Initialization, stopping, or pausing of the audit logs	Verify the following are logged: ■ Initialization of audit logs. ■ Stopping or pausing of audit logs.
10.2.7 Creation and deletion of system-level objects	10.2.7 Verify creation and deletion of system level objects are logged.
10.3 Record at least the following audit trail entries for all system components for each event:	10.3 Through interviews and observation of audit logs, for each auditable event (from 10.2), perform the following:
10.3.1 User identification	10.3.1 Verify user identification is included in log entries.
10.3.2 Type of event	10.3.2 Verify type of event is included in log entries.
10.3.3 Date and time	10.3.3 Verify date and time stamp is included in log entries.
10.3.4 Success or failure indication	10.3.4 Verify success or failure indication is included in log entries.
10.3.5 Origination of event	10.3.5 Verify origination of event is included in log entries.
10.3.6 Identity or name of affected data, system component, or resource	10.3.6 Verify identity or name of affected data, system component, or resources is included in log entries.

**10.4** Using time synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.

Note: One example of time synchronization technology is Network Time Protocol (NTP).

---

**10.4.1** Critical systems have the correct and consistent time.

**10.4** Examine configuration standards and processes to verify that time synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2.

**10.4.1.a** Examine the process for acquiring, distributing and storing the correct time within the organization to verify that:

- Only the designated central time server(s) receives time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC.
- Where there is more than one designated time server, the time servers peer with one another to keep accurate time.
- Systems receive time information only from designated central time server(s).

**10.4.1.b** Observe the time-related system-parameter settings for a sample of system components to verify:

- Only the designated central time server(s) receives time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC.

- Where there is more than one designated time server, the designated central time server(s) peer with one another to keep accurate time.
- Systems receive time only from designated central time server(s).

---

**10.4.2** Time data is protected.

**10.4.2.a** Examine system configurations and time synchronization settings to verify that access to time data is restricted to only personnel with a business need to access time data.

**10.4.2.b** Examine system configurations, time synchronization settings and logs, and processes to verify that any changes to time settings on critical systems are logged, monitored, and reviewed.

---

**10.4.3** Time settings are received from industry-accepted time sources.

**10.4.3** Examine systems configurations to verify that the time server(s) accept time updates from specific, industry-accepted external sources (to prevent a malicious individual from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the time updates (to prevent unauthorized use of internal time servers).

---

**10.5** Secure audit trails so they cannot be altered.

**10.5** Interview system administrators and examine system configurations and permissions to verify that audit trails are secured so that they cannot be altered as follows:

---

10.5.1 Limit viewing of audit trails to those with a job-related need.	10.5.1 Only individuals who have a job-related need can view audit trail files.
10.5.2 Protect audit trail files from unauthorized modifications.	10.5.2 Current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	10.5.3 Current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter.
10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.	10.5.4 Logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are written onto a secure, centralized, internal log server or media.
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	10.5.5 Examine system settings, monitored files, and results from monitoring activities to verify the use of file-integrity monitoring or change-detection software on logs.
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.  Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement.	10.6 Perform the following:  <p>10.6.1 Review the following at least daily:</p> <ul style="list-style-type: none"><li>■ All security events</li><li>■ Logs of all system components that store, process, or transmit CHD and/or SAD</li><li>■ Logs of all critical system components</li></ul> <p>10.6.1.a Examine security policies and procedures to verify that procedures are defined for reviewing the following at least daily, either manually or via log tools:</p> <ul style="list-style-type: none"><li>■ All security events</li><li>■ Logs of all system components that store, process, or transmit CHD and/or SAD</li></ul>

- Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).
  - Logs of all critical system components
  - Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)
- 

**10.6.1.b** Observe processes and interview personnel to verify that the following are reviewed at least daily:

- All security events
- Logs of all system components that store, process, or transmit CHD and/or SAD
- Logs of all critical system components
- Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).

---

**10.6.2** Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.

**10.6.2.a** Examine security policies and procedures to verify that procedures are defined for reviewing logs of all other system components periodically—either manually or via log tools—based on the organization's policies and risk management strategy.

---

	10.6.2.b Examine the organization's risk-assessment documentation and interview personnel to verify that reviews are performed in accordance with organization's policies and risk management strategy.
10.6.3 Follow up exceptions and anomalies identified during the review process.	10.6.3.a Examine security policies and procedures to verify that procedures are defined for following up on exceptions and anomalies identified during the review process.  10.6.3.b Observe processes and interview personnel to verify that follow-up to exceptions and anomalies is performed.
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	10.7.a Examine security policies and procedures to verify that they define the following: <ul style="list-style-type: none"><li>■ Audit log retention policies</li><li>■ Procedures for retaining audit logs for at least one year, with a minimum of three months immediately available online</li></ul> 10.7.b Interview personnel and examine audit logs to verify that audit logs are retained for at least one year.
10.8 Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of:	10.7.c Interview personnel and observe processes to verify that at least the last three months' logs are immediately available for analysis.  10.8.a Examine documented policies and procedures to verify that processes are defined for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of:

- Firewalls
  - IDS/IPS
  - FIM
  - Anti-virus
  - Physical access controls
  - Logical access controls
  - Audit logging mechanisms
  - Segmentation controls (if used)
- Firewalls
  - IDS/IPS
  - FIM
  - Anti-virus
  - Physical access controls
  - Logical access controls
  - Audit logging mechanisms
  - Segmentation controls (if used)

Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.

---

**10.8.b** Examine detection and alerting processes and interview personnel to verify that processes are implemented for all critical security controls, and that failure of a critical security control results in the generation of an alert.

---

**10.8.1** Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include:

- Restoring security functions
- Identifying and documenting the duration (date and time start to end) of the security failure
- Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause
- Identifying and addressing any security issues that arose during the failure

**10.8.1.a** Examine documented policies and procedures and interview personnel to verify processes are defined and implemented to respond to a security control failure, and include:

- Restoring security functions
- Identifying and documenting the duration (date and time start to end) of the security failure
- Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause
- Identifying and addressing any security issues that arose during the failure

- Performing a risk assessment to determine whether further actions are required as a result of the security failure
  - Implementing controls to prevent cause of failure from reoccurring
  - Resuming monitoring of security controls
- Performing a risk assessment to determine whether further actions are required as a result of the security failure
  - Implementing controls to prevent cause of failure from reoccurring
  - Resuming monitoring of security controls

Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.

	<p><b>10.8.1.b</b> Examine records to verify that security control failures are documented to include:</p> <ul style="list-style-type: none"><li>■ Identification of cause(s) of the failure, including root cause</li><li>■ Duration (date and time start and end) of the security failure</li><li>■ Details of the remediation required to address the root cause</li></ul>
<p><b>10.9</b> Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.</p>	<p><b>10.9</b> Examine documentation and interview personnel to verify that security policies and operational procedures for monitoring all access to network resources and cardholder data are:</p> <ul style="list-style-type: none"><li>■ Documented</li><li>■ In use</li><li>■ Known to all affected parties</li></ul>

**Table 9-1 PCI DSS 3.2 Requirement 10**

The following sections depict some examples of how to configure ISE to meet a sampling of the requirements in Requirement 10.

## **ISE Policy for PCI 10.1: Ensuring Unique Usernames and Passwords**

To ensure that each administrator of Cisco ISE has a unique username and password for auditing purposes, you must utilize RBAC for administrator users. [Figure 9-1](#) shows an

example of creating a local ISE super administrator account.

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes links for Home, Context Visibility, Operations, Policy, Administration, System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Services, Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Backup & Restore, Admin Access, and Admin User. The left sidebar has sections for Authentication, Authorization, Administrators (Admin Users, Admin Groups), and Settings. The main content area is titled "Administrators List > New Administrator". It contains fields for Admin User (Name: jheary, Status: Enabled, Email: jheary@nowhere.com, External checkbox, Inactive account never disabled checkbox), Password (Password and Re-Enter Password fields, both containing '\*\*\*\*\*', and a Generate Password button), User Information (First Name: jamey, Last Name: heary), Account Options (disabled), and Admin Groups (Super Admin selected). A plus sign icon is available to add more groups.

**Figure 9-1** Creating a Local ISE Administrator

Each administrator should have their own account with the proper level of privileges required for them to do their job. Always exercise the concept of least privilege when assigning administrators a privilege level. You want them to have only the bare minimum privileges they require. You can use the built-in administrator authorization permissions or create your own inside of ISE. The authorization permissions are broken down into two types: Menu Access and Data Access. Menu Access permissions determine which menus the administrator can see. Data Access permissions allow you to grant full or no access to the following data in the Cisco ISE interface: Admin Groups, User Identity Groups, Endpoint Identity Groups, Locations, and Device Types.

[Figure 9-2](#) depicts the Menu Access permissions screen (located at **Administration > System > Admin Access**) showing the help desk menu permissions. You can see that access to some menus is allowed and is blocked to others.

The screenshot shows the 'Edit Menu Access Permission' page. On the left, a sidebar lists 'Authentication', 'Authorization', and 'Permissions'. Under 'Permissions', 'Menu Access' is selected, showing 'Data Access' and 'Policy' under 'ISE Navigation Structure'. In the main area, a table titled 'Menu Access Privileges' contains a single row for 'Helpdesk Admin Menu Access'. The 'Name' field is 'Helpdesk Admin Menu Access', and the 'Description' field is 'Access permission for Operations tab.' To the right, a panel titled 'Permissions for Menu Access' shows two radio buttons: 'Show' (selected) and 'Hide'.

Figure 9-2 Menu Access Permissions

## ISE Policy for PCI 10.2 and 10.3: Audit Log Collection

PCI Requirement 10.2 and its multiple subrequirements explain the types of audit logs that should be enabled on a system like ISE to ensure proper audit trails are created. Cisco ISE includes robust auditing controls and configuration options you can use to comply with PCI DSS 10.2 requirements. The requirements of PCI DSS 10.3 are met by the internals of the way ISE logs events and occur without your having to do any additional configuration.

The audit logs that ISE can create are broken into logging categories, as shown in [Figure 9-3](#) (navigate to **Administration > System > Logging > Logging Categories**). As a best practice, all of these categories should be enabled for local logging level (as shown in the Local Log Level column).

Logging Categories						
		Edit				
		Category		Targets	Severity	Local Log
	AAA Audit	AAA Audit		LogCollector,SecureSyslogCollector	INFO	enable
		Failed Attempts		LogCollector,ProfilerRadiusProbe	INFO	enable
		Passed Authentifications		LogCollector,ProfilerRadiusProbe	INFO	disable
	AAA Diagnostics	AAA Diagnostics		LogCollector	WARN	enable
		Administrator Authentication and Authorization			WARN	enable
		Authentication Flow Diagnostics			WARN	enable
		Identity Stores Diagnostics			WARN	enable
		Policy Diagnostics			WARN	enable
		RADIUS Diagnostics		LogCollector	WARN	enable
		Guest		LogCollector	INFO	enable
		MyDevices		LogCollector	INFO	enable
		AD Connector		LogCollector	INFO	enable
		TACACS Diagnostics		LogCollector	WARN	enable
	Accounting	Accounting		LogCollector,securesyslog_server1	INFO	enable

**Figure 9-3** ISE Audit/Logging Categories

The Targets column indicates to which logging servers the messages will be sent for logging and storage. Targets are typically UDP syslog servers or secure syslog servers, as explained next.

## ISE Policy for PCI 10.5.3, 10.5.4, and 10.7: Ensure the Integrity and Confidentiality of Audit Log Data

To ensure the integrity and confidentiality of audit log data, copying the logs to a non-ISE logging server is recommended. This ensures that in the event of an ISE compromise, administrator error, or system failure, the audit trail logs are not lost. You can also apply file integrity checking tools on the external log server data store for additional protection. [Figure 9-4](#) illustrates the configuration options for configuring remote logging targets.

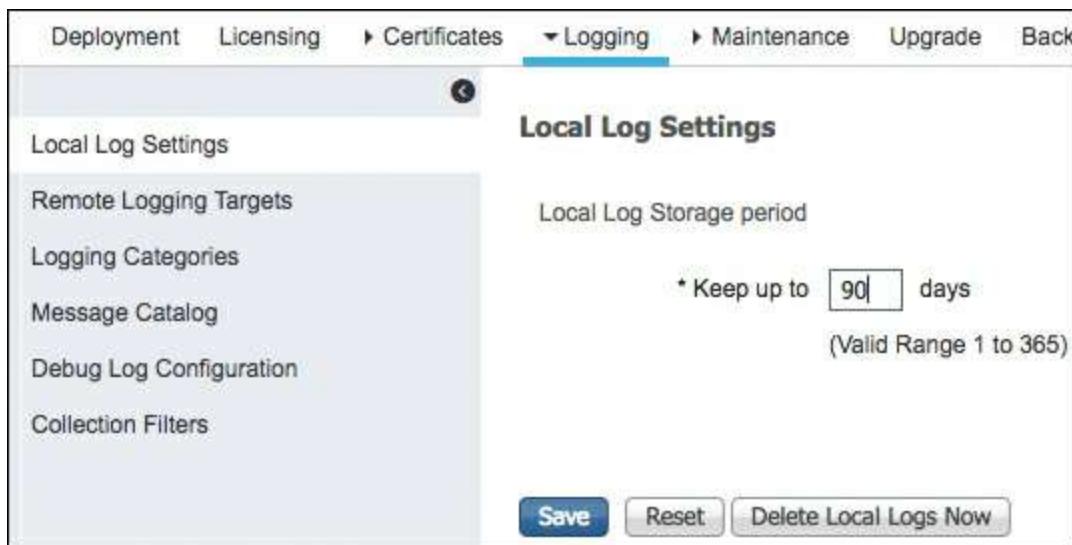
Remote Logging Targets						
	Name	IP Address	Port	Type	Description	Status
	LogCollector	127.0.0.1	20514	UDP SysLog	Syslog Target for Log Collector	Enabled
	ProfilerRadiusProbe	127.0.0.1	30514	Profiler SysLog	Syslog Target for Profiler RADIUS Probe	Enabled
	SecureSyslogCollector	127.0.0.1	6514	Secure SysLog	Secure Syslog Collector	Enabled
	TCPLogCollector	127.0.0.1	1468	TCP SysLog	TCP SysLog collector	Disabled
	securesyslog_server1	4.4.4.4	6514	Secure SysLog		Enabled

**Figure 9-4** Configuring ISE Remote Logging Targets

The type of log server targets supported include UDP syslog, TCP syslog, and secure syslog.

PCI Requirement 10.7 requires you to keep audit logs for a period of one year, with at least 90 days' worth of logs kept readily available. The ISE default is only 1 day. To comply with 10.7, it is recommended that you configure ISE to keep 90 days of local

audit logs, as shown in [Figure 9-5](#), and use your external logging target servers for the long-term, one-year storage. This allows Cisco ISE to operate without the burden of a large audit log data store. If 90 days' worth of audit data is too large to be stored locally on ISE, then use the external logging servers and reduce the number of days' worth of logs the ISE local log stores. ISE will auto-prune the oldest logs first if it runs out of space.



**Figure 9-5** ISE Local Log Data Retention Policy

## ISE Policy for PCI 10.6: Review Audit Data Regularly

Now that you have Cisco ISE set up to produce the proper audit trails, you need to review that data regularly. PCI requires that you review the logs of AAA servers such as Cisco ISE on a daily basis, which is a great practice to follow but a fairly tall order for today's overworked administrators. Luckily, Cisco ISE has built-in reports and scheduled reports that can be created and, if desired, emailed to you daily. The Internal Administrator Summary report, shown in [Figure 9-6](#) and located at **Operations > Reports > Audit**, is a good place to go to review all of the different administrator activity reports for ISE administrators.

**Figure 9-6** ISE Internal Administrator Summary Report

Clicking any of the document magnifying-glass icons in the different columns will open and run a report for that column. Clicking any of the hyperlinks in the report will spawn another audit report with more detail of the event. [Figure 9-7](#) depicts an example of an ISE administrator configuration detail change report.

**Configuration Audit Detail**

From 2017-01-08 00:00:00.0 to 2017-01-15 14:39:05.701  
Generated At: 2017-01-15 14:39:05.05

**Details**

Logged At	2017-01-15 12:56:00.682
Server Time	2017-01-15 12:56:00.682 -8:00
Administrator	admin
Object Type	UPSLogTarget
Object Name	securesyslog_server1
Event	Added configuration
IP Address	10.1.100.231
Interface	GUI
ISE Server	All
Source ISE Server	atw-ise231

**Modified Properties**

Modified Properties

Object created: Port = 6514\Facility Code = LOCAL6\Length = 1024\Description = \Include Alarms = FALSE\status = ENABLED\Buffer Message = TRUE

**Figure 9-7** ISE Administrator Change Configuration Audit Report

Any ISE report that you run can be saved as a scheduled report or added to My Reports (shown at the top of the navigation pane in [Figure 9-6](#)). Before you create a scheduled

report, you first have to set up a data repository in which to store the reports. Go to **Administration > System > Maintenance > Repository** to create one. For scheduled reports, you can input the relevant data, as shown in [Figure 9-8](#), such as an email address to send the report to, frequency, and so forth.

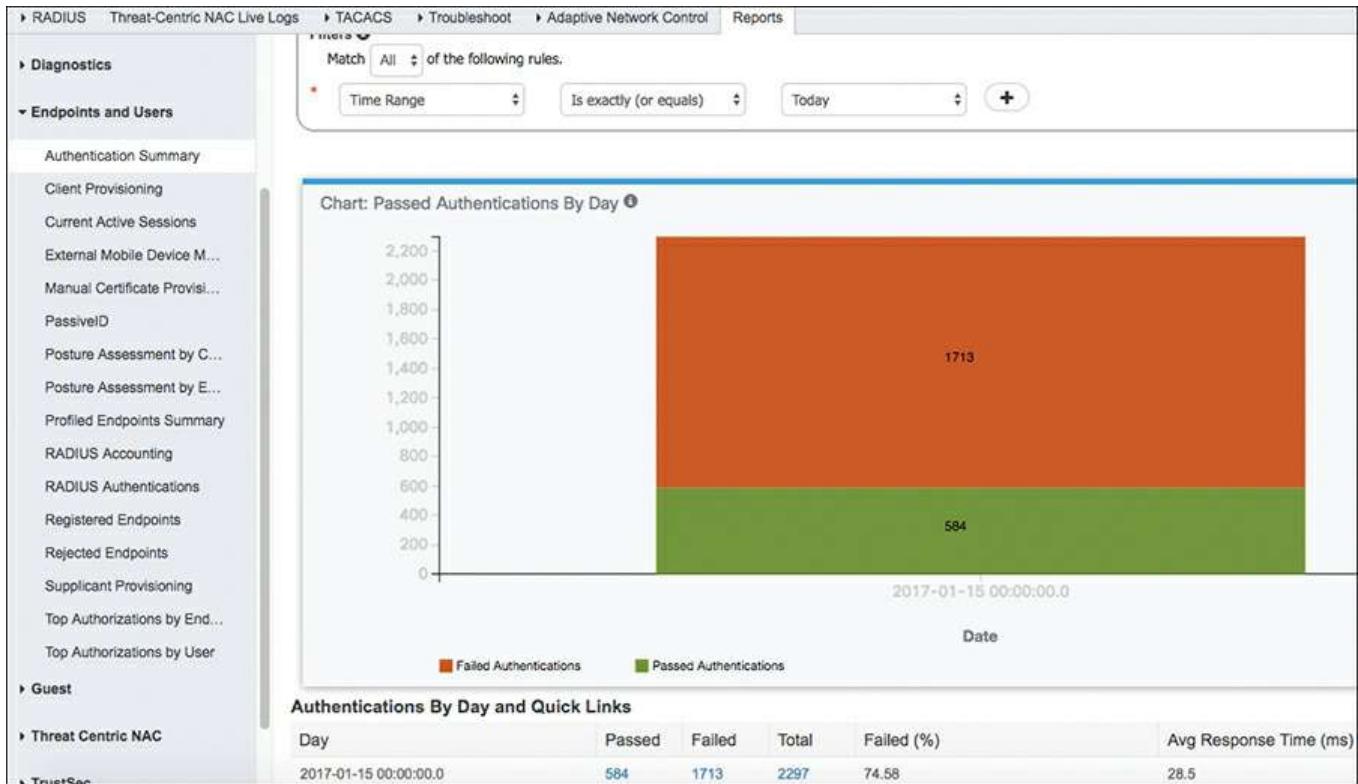
Save as Schedule Window

*Name	Daily_Configuration_Change_Report
Description	Change Audit
*Repository	Reports
Email	jheary@nowhere.com
Frequency	Daily
At Time	11:30 PM
On Day	<input checked="" type="checkbox"/> Monday <input checked="" type="checkbox"/> Tuesday <input checked="" type="checkbox"/> Wednesday <input checked="" type="checkbox"/> Thursday <input checked="" type="checkbox"/> Friday <input type="checkbox"/> Saturday <input type="checkbox"/> Sunday
Start Date	2017-01-15
End Date	2018-01-15

**Figure 9-8** Scheduled Admin Change Configuration Report

## Cisco ISE User Accounting

In addition to auditing the administrators of ISE, it is also important to be able to audit the users authenticated via ISE. For this function, Cisco ISE offers the same user reporting structure that was just reviewed for administrators. It is found in the **Operations > Reports > Endpoints and Users** section of the ISE GUI. The **Authentications Summary** report shown in [Figure 9-9](#) is a good example of a user audit report.



**Figure 9-9** User Authentication Summary Report

As you can see in [Figure 9-9](#), many user and device detailed reports are available in the Endpoints and Users section under Reports. [Figure 9-10](#) depicts one of them, the Top Authorizations by User report.



**Figure 9-10** Top User Authorizations Report

## Summary

Proper auditing and accounting is instrumental in operating the ISE solution. It assists with troubleshooting tasks, compliance reporting, and finding configuration errors and security compromises. By using PCI Requirement 10 as your guide, you will likely be able to pass audits against other security standards, including your own internal audit. Having said that, it is not a panacea, so be sure to check the regulations you will be audited against to ensure you configure Cisco ISE appropriately.



## **Part IV Let's Configure!**

[Chapter 10 Profiling Basics and Visibility](#)

[Chapter 11 Bootstrapping Network Access Devices](#)

[Chapter 12 Network Authorization Policy Elements](#)

[Chapter 13 Authentication and Authorization Policies](#)

[Chapter 14 Guest Lifecycle Management](#)

[Chapter 15 Client Posture Assessment](#)

[Chapter 16 Suplicant Configuration](#)

[Chapter 17 BYOD: Self-Service Onboarding and Registration](#)

[Chapter 18 Setting Up and Maintaining a Distributed ISE Deployment](#)

[Chapter 19 Remote Access VPN and Cisco ISE](#)

[Chapter 20 Deployment Phases](#)

# Chapter 10 Profiling Basics and Visibility

This chapter covers the following topics:

- Understanding profiling concepts
- Infrastructure configuration
- Profiling policies
- ISE Profiler and CoA
- Profiles in authorization policies
- Verifying profiling
- Triggered NetFlow: A Woland-Santuka pro tip

In this chapter we will examine profiling concepts and why profiling is so important to the context-aware policies necessary in today's business environment. We will dive into the manner in which profiling has evolved from a Band-Aid for deploying 802.1X deployments to the inventory and visibility tool that it is today. You will learn about the multitude of ways that Cisco Identity Services Engine (ISE) can glean the profiling data (probes) and you will learn how to configure the infrastructure to efficiently use the ISE profiling probes, including when ISE is within a VMware virtual environment.

## Understanding Profiling Concepts

The term profiling has been used a lot in today's society and can often have negative connotations. Police and security professionals may use a series of attributes about a human being, such as hair and eye color, the way they are dressed, and the way they behave to help profile them quickly as being a threat or a non-threat. However, this is ultimately guesswork that (hopefully) becomes more accurate with experience and practice.

Profiling as it relates to network access is very similar. However, the term should be thought of in a positive light as it relates to the Cisco TrustSec system and the Cisco ISE solution.

The Cisco ISE Profiler is the component of the Cisco ISE platform that is responsible for endpoint detection and classification. It does so by using a probe or series of probes that collect attributes about an endpoint. The Profiler then compares the collected attributes to predefined device profiles (such as a set of signatures) to locate a match.

Why would profiling be an important technology for a company rolling out an identity solution? In the early days of identity-based networks and 802.1X, countless man-hours were spent identifying all the devices that did not have supplicants—in other words, the devices that could not authenticate to the network using 802.1X, such as printers and fax machines. You had to identify all the switch ports that were connected to the printer and

configure those ports to either

- Not use 802.1X
- Use MAC Authentication Bypass (MAB)

MAB is an extension to 802.1X that allows the switch to send the device's MAC address to the authentication server. If that MAC address is in the approved list of devices, then the authentication server sends back an accept result, thereby allowing specific MAC addresses to skip authentication.

Imagine just how many-man hours were spent collecting and maintaining this list of MAC addresses. An onboarding process was required so that when a new printer was added to the network, its MAC address was added to the approved list, and so forth. Obviously, some enhancements to this onboarding process were required. There had to be some way to build this list more dynamically and save all those man-hours of prep and maintenance.

This is where profiling technology enters the picture. It allows you to collect attributes about devices from a multitude of sources such as DHCP, NetFlow, HTTP user-agent strings, NMAP scans, and more. Those collected attributes are then compared to a set of signatures, similar to the way an intrusion prevention system (IPS) works. These signatures are more commonly referred to as profiles.

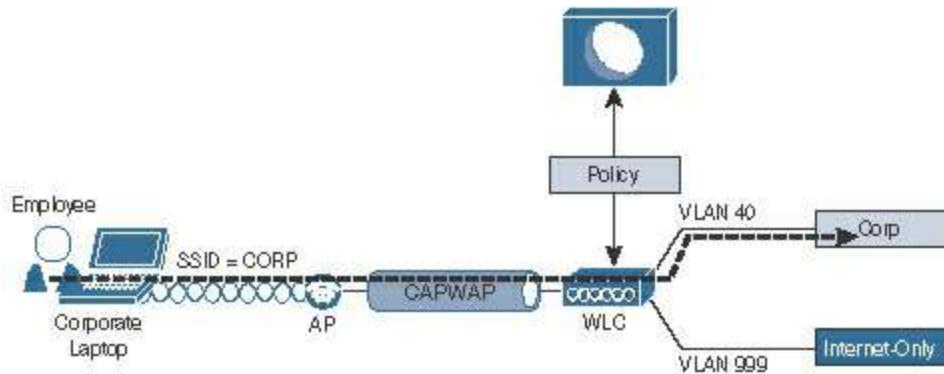
Following is an example of how profiling technology works:

1. The Profiler collects a MAC address that belongs to Epson, Inc.
2. The Profiler does an NMAP scan on the IP address and sees that common printer ports are open.
3. Based on those two attributes, the system assigns that device to the profile "Epson Printer."

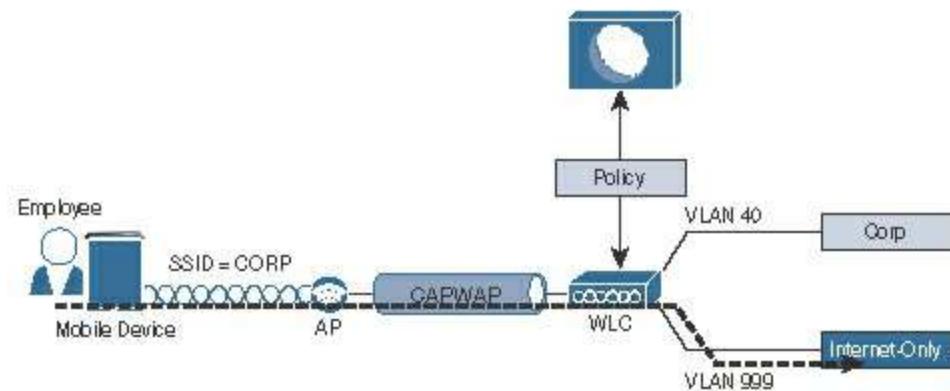
Profiling technology has evolved to the point that now your authentication server has the capability to use that profiling data for much more than just building the list of MAC addresses permitted to use MAB.

Cisco ISE uses the resulting collection and classification data from the Profiler as conditions in the authorization policy. Now you can build an authorization policy that looks at much more than your identity credentials. You can combine a user's identity with the classification result and invoke specific authorization results.

[Figures 10-1](#) and [10-2](#) provide an example of a differentiated authorization policy based on profiling.



**Figure 10-1** Employee Using Corporate Laptop to Gain Full Access



**Figure 10-2** Same Employee Credentials on a Mobile Device Gets Limited Access

Users connecting to the same wireless SSID and using the same credentials can be associated to different wired VLAN interfaces based on the device profile, such as the following:

- Employees using corporate laptops with their Active Directory user ID are assigned to the corporate VLAN and given full access to the network.
- Employees using mobile devices with their same Active Directory user ID are assigned to a GUEST VLAN and provided Internet access only.

Although it may be quite intuitive to visualize the types of network access policies you will be able to create based on the device's profile, the design of where and how the Profiler collects the data about the endpoints requires thought and planning.

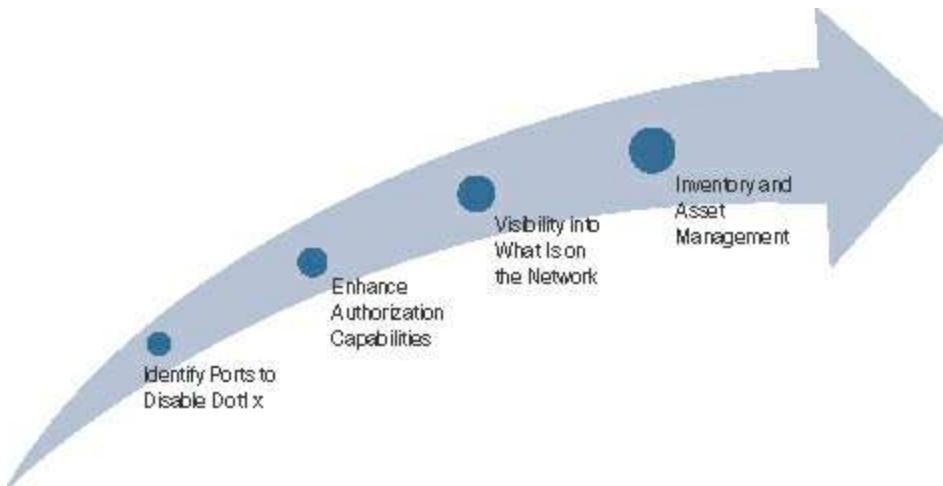
One of the first questions a security team may ask when discovering profiling with any network access control solutions is, “Can we use this as an anti-spoofing solution?” Remember that MAC Authentication Bypass is a very limited replacement for a strong authentication. It would be fairly easy for a malicious user to unplug a printer from the wall, configure her laptop to use the same MAC address as the printer (spoofing), and gain access to the network.

You should always keep in mind that profiling is a technology that compares collected attributes about an endpoint to a set of signatures called profiling policies to make the

best guess of what a device is. Can this type of technology be used to prevent spoofing? Sure. However, it is very difficult to accomplish anti-spoofing with this type of technology. It would require a lot of tuning, trial and error, and constant adjustment, which makes it too operationally expensive and untenable.

A best-practice approach is to use a least-privilege strategy instead. If the previously mentioned malicious user is successful in spoofing the MAC address of the printer and gains network access, what level of network access should that device have? In other words, the authorization policy for printers should not provide full network access, but provide a limited subset of access instead. For example, a printer should only be permitted to communicate using network ports critical to printer operations (such as TCP port 9100 or 9600).

Profiling technology and the value it provides continue to evolve beyond MAB lists, beyond attributes in an authorization policy, and toward inventory of network-attached assets. [Figure 10-3](#) illustrates this evolution of profiling, which will be evident in many aspects of ISE version 2.1 and beyond.



**Figure 10-3** Profiling Technology Evolution

## ISE Profiler Work Center

Beginning with ISE 2.0, the administrative experience within the ISE GUI has been shifting to the use of Work Centers. As the name implies, an ISE Work Center is designed to provide a single location where all tasks associated with the specific process can be accomplished. In this case, the Profiler Work Center is designed to provide you, the ISE admin, with a single section of the GUI to accomplish all the tasks related to profiling.

The Profiler Work Center is intuitively located under **Work Centers > Profiler**, as shown in [Figure 10-4](#). As with all Work Centers in the ISE GUI, you can pretty much get everything configured if you just follow the steps from left to right.

**Profiler Overview**

Prepare 1	Define 2	Go Live & Monitor 3
<b>Network Preparation</b> Configure the <a href="#">network devices</a> that you will be using for profiling.	<b>Logical Endpoint Groups</b> Review and customize <a href="#">logical profiles</a> that enable you to organize endpoints into groups that make sense for your organization.	<b>Auditing</b> Examine the <a href="#">endpoint classification</a> to see how endpoints are profiled and customize the displayed information to meet your needs.
<b>Profiling Configuration</b> Check the <a href="#">Enable Profiling Service</a> option and specify the profiling configuration for each node in your <a href="#">deployment</a> that will be profiling endpoints.	<b>Profiling Policies</b> Create custom <a href="#">profiling policies</a> for devices unique to your organization.	<b>Troubleshooting</b> <a href="#">Troubleshoot</a> issues using diagnostic tools.
<b>Feed Service</b> Configure the <a href="#">feed service</a> to automatically or manually update your profiling policies.	<b>Endpoint Access</b> Add profile and logical profile conditions to your <a href="#">authorization policy</a> .	
<b>Settings</b> Check the defaults for profiler configuration <a href="#">settings</a> such as change of authorization to make sure they are acceptable.		
Configure your network devices to send probe data to ISE.		

**Figure 10-4** Profiler Overview Screen

## ISE Profiling Probes

As described, the Cisco ISE solution is capable of providing access policies where the decisions may be made based on who, what, where, when, how, and other factors. Profiling is focused on the “what” elements of the policy. For the policy engine to know what the device is, you must first collect that data.

The Cisco ISE solution uses a number of collection mechanisms known as probes. Each probe is software designed to collect data to be used in a profiling decision. An example of this would be the HTTP probe, which captures HTTP traffic and enables the Profiler to examine attributes from the traffic, such as HTTP user-agent strings. Without the probe enabled on the policy server, the data would never be collected. The good news is that, starting in ISE version 1.3, profiling and a default set of probes are enabled by default.

## Probe Configuration

You enable the probes on each Policy Service Node (PSN) where appropriate. In the Administration GUI of the Policy Administration Node (PAN), navigate to **Work Centers > Profiler > Node Config**. The same screen may also be found under **Administration > System > Deployment**. From here, select the PSN that you are

configuring the probes for. You will repeat these steps for each PSN in your deployment.

**Step 1.** Select one of the Policy Services Nodes, as shown in [Figure 10-5](#). In this case, the node is still standalone, which means that it is a single node running all personas (Administration, Monitoring, and Policy Service).

Hostname	Node Type	Personas	Role(s)	Services	Node Status
atw-ise237	ISE	Administration, Monitoring, Policy Service	STANDALONE	SESSION...	SESSION... (green checkmark)

**Figure 10-5** ISE Deployment Screen

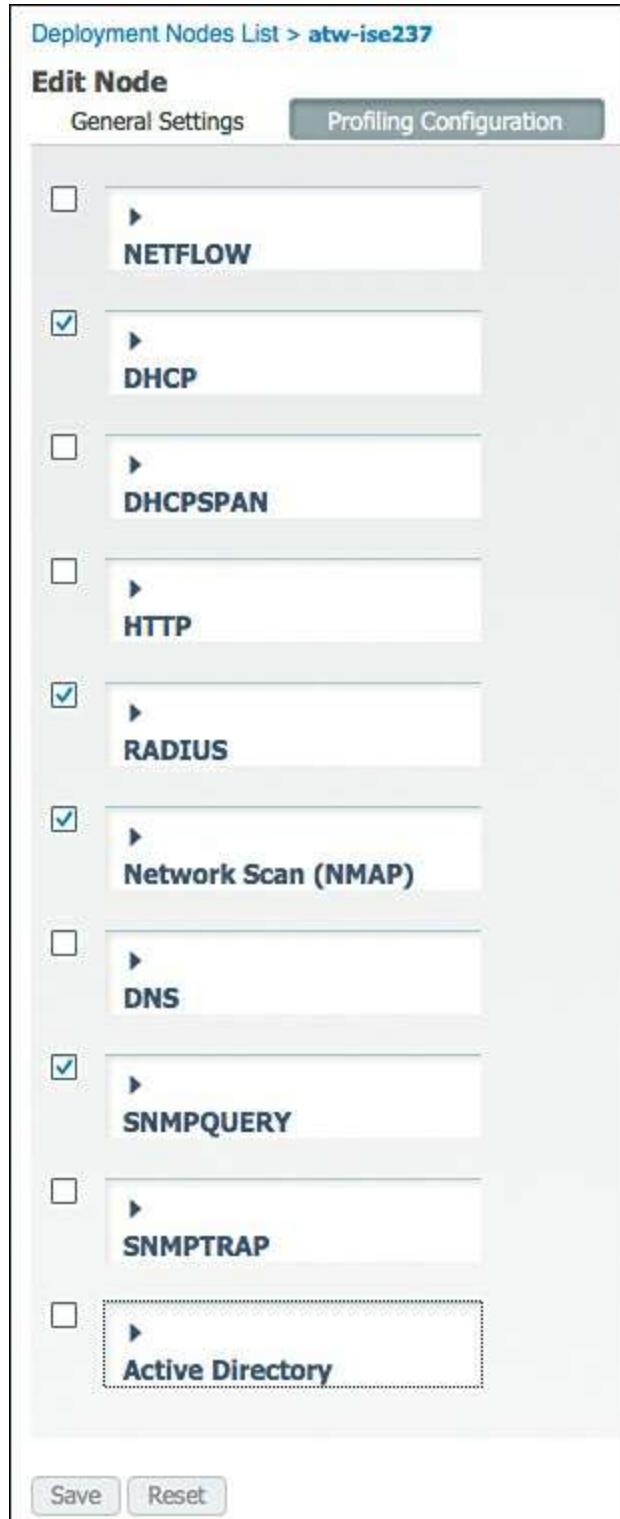
**Step 2.** On the General Settings tab, note that the **Enable Profiling Service** check box is selected, as shown in [Figure 10-6](#). This service is enabled by default on all PSNs, and is not configurable when in standalone mode.

Persona	Role
Administration	STANDALONE
Monitoring	PRIMARY
Policy Service	

Enable Profiling Service

**Figure 10-6** General Settings

**Step 3.** Select the **Profiling Configuration** tab, as shown in [Figure 10-7](#).



**Figure 10-7** Profiling Configuration

The following ten probes are available on each Policy Services Node, as shown in [Figure 10-7](#):

- NETFLOW
- DHCP

- DHCPSPAN
- HTTP
- RADIUS
- Network Scan (NMAP)
- DNS
- SNMPQUERY
- SNMPTRAP
- Active Directory

Next we examine each probe in detail (but not in the preceding order).

## DHCP and DHCPSPAN Probes

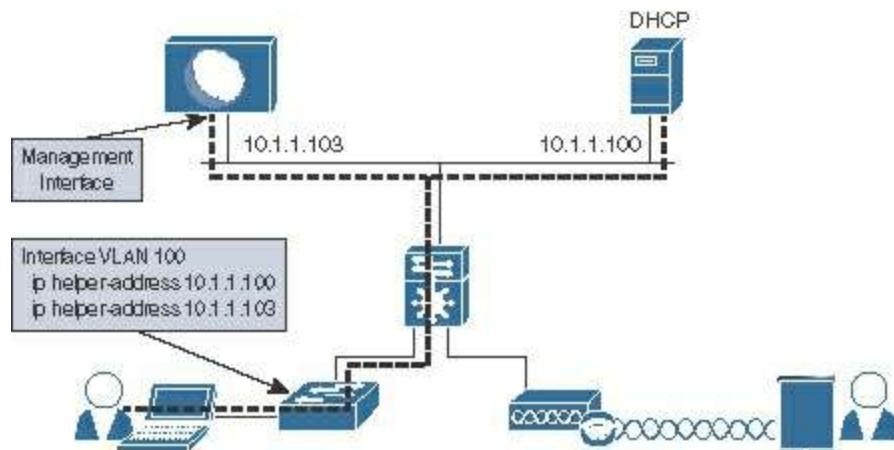
DHCP can be one of the most useful data sources for an endpoint device. A primary use of DHCP in profiling is to capture the device MAC address; however, there are many other uses for the data. Much like HTTP, DHCP requests will also carry a User-Agent field that helps to identify the operating system of the device. Some organizations have been known to use a custom DHCP user-agent string, which helps to identify the device as a corporate asset.

Not only the populated fields from the DHCP Client, but other attributes, such as requested DHCP Options and DHCP Host-Name, can be very useful in classifying the device.

There are two DHCP probes, each working in a slightly different way: DHCP and DHCPSPAN.

### DHCP Probe

The DHCP probe requires the DHCP requests to be sent directly to the ISE PSN(s). This is often done by using the **ip helper-address** interface configuration command and is illustrated in [Figure 10-8](#).

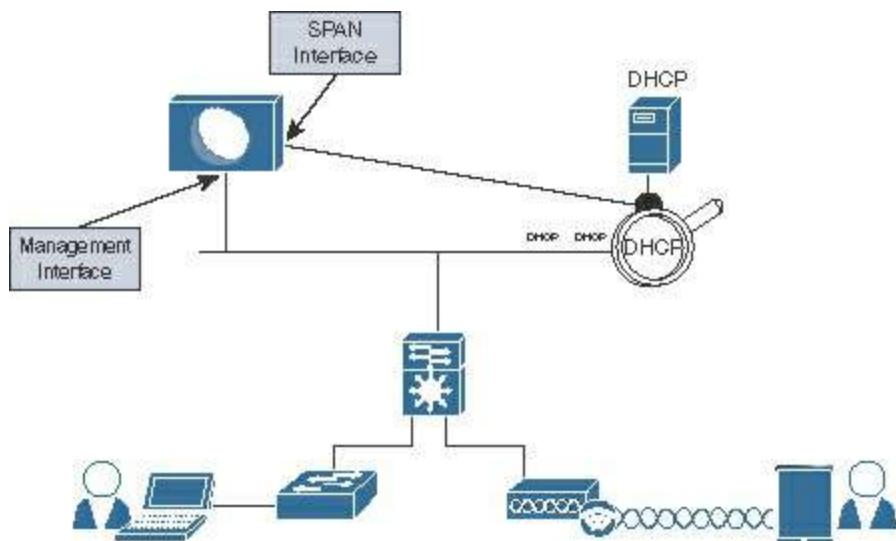


**Figure 10-8 DHCP with ip helper-address Logical Design**

The **ip helper-address** command on a Layer 3 interface will convert a DHCP broadcast (which is a Layer 2 broadcast) to a unicast or directed broadcast (which sends the broadcast to all hosts on a specific subnet). Simply add the IP address of your PSN(s) to the list of helper addresses, and it will be copied on all DHCP requests.

### DHCPSpan Probe

Another way for ISE to glean the DHCP requests and even the DHCP responses is the use of a Switched Port Analyzer (SPAN) session in true promiscuous mode. A SPAN session copies all traffic to/from a source interface on a switch to the destination interface, which would be one of ISE's interfaces assigned to the DHCPSpan probe. [Figure 10-9](#) illustrates the logical design of using SPAN.



**Figure 10-9 DHCP SPAN Logical Design**

When using the SPAN method, you will need to consider where the best location is to create the SPAN session and gather the data. One recommended location is the DHCP server, where the DHCP probe will see both ends of the conversation (request and response). However, there are caveats to this method, such as, “What if the organization uses distributed DHCP servers?” This is why the non-SPAN method tends to be the most commonly deployed.

### Considerations with the Cisco WLC

Regardless of the SPAN or “helper-address” methods of using the DHCP probe(s), when using a Cisco Wireless LAN Controller (WLC), the WLC has a default configuration of acting as a RADIUS proxy, which is its own form of a “helper-address” where the WLC acts as a middleman for all DHCP transactions. Unfortunately, this behavior has a negative effect on the DHCP probe and must be disabled on the WLC.

Upon doing so, the DHCP requests from wireless endpoints appear as broadcast messages on the VLAN, and an IP helper-address statement should be configured on the Layer-3 interface of that VLAN (the switch or router).

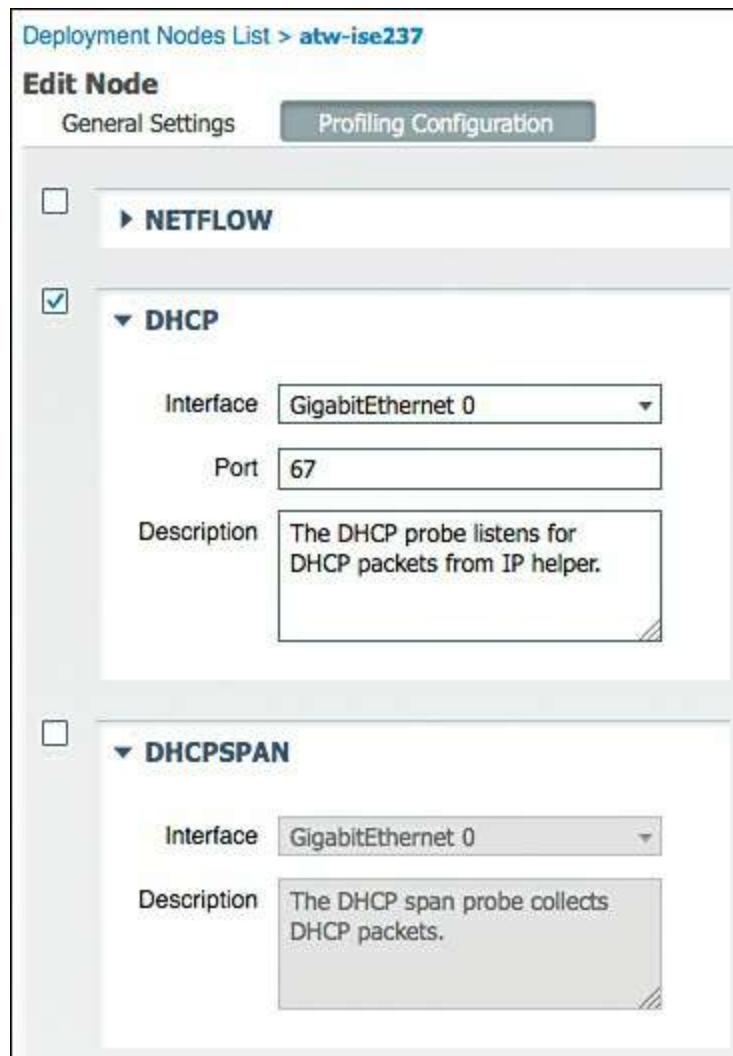
## Probe Configuration

Minimal configuration is required on the ISE side to enable the DHCP probe(s). From the Profiling Configuration tab displayed in [Figure 10-7](#):

**Step 1.** Notice that DHCP is enabled by default. This default setting has existed since ISE 1.3.

**Step 2.** GigabitEthernet 0 is the default interface. You can choose a different interface or all interfaces. You can't choose multiple interfaces individually. The choice is a single interface or all interfaces.

[Figure 10-10](#) shows the DHCP probes. You should never need to enable both probes for the same interface. That would cause double processing of DHCP packets and be wasteful of system resources.



## Figure 10-10 DHCP Probes

**Note** If you are using only device-sensor capable infrastructure, neither DHCP probe needs to be enabled.

### RADIUS Probe

RADIUS is the primary communication mechanism from a network access device (NAD) to the authentication server (ISE). RADIUS packets contain useful data to help classify a device that exists within RADIUS communication.

Originally, the focus was on the MAC address and IP address of the device. By having this data conveyed in the RADIUS packet, ISE can build the all-important MAC-to-IP address bindings. Because the endpoint database uses MAC addresses as the unique identifier for all endpoints, these bindings are absolutely critical. Without them, the Layer 3 probes, such as HTTP and NMAP scanning, would never work correctly.

The Calling-Station-ID field in the RADIUS packet provides the endpoint's MAC address, and the Framed-IP-Address field provides its IP address in the RADIUS accounting packet.

Additionally, the RADIUS probe can trigger the SNMPQUERY probe to poll the NAD (see the SNMP probe information later in the chapter).

Most importantly, with the proliferation of device-sensor capable switches and wireless controllers, the RADIUS probe becomes even more critical. Device-sensor is a feature in the switch or controller that collects endpoint attributes locally and then sends those attributes to ISE within RADIUS accounting packets.

By allowing the network device to proactively send the profiling data to ISE, the architecture has placed the collection agents as close to the endpoint as possible, at the point of access to the network. Additionally, it has eliminated the need to send the **ip helper-address** information to ISE and the need to reactively query the switches for CDP/LLDP information (see the later discussion of the SNMPQUERY probe).

### Considerations with RADIUS Probe

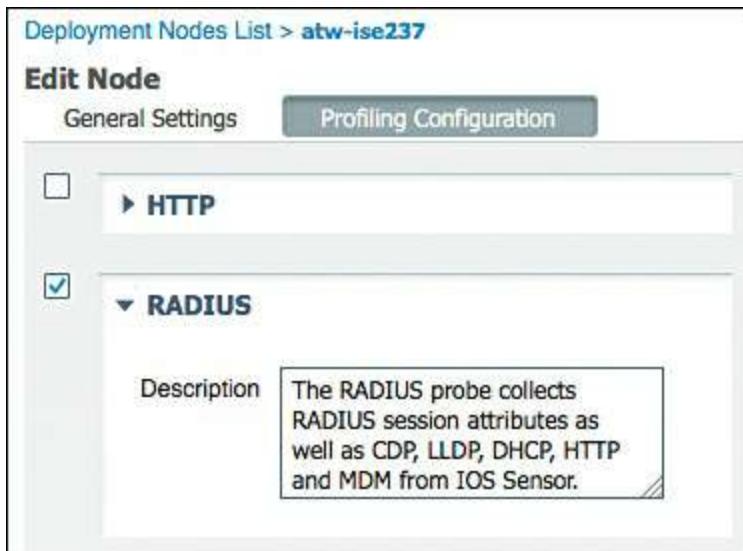
All NADs in the Secure Unified Access deployment should be configured to send RADIUS accounting packets. It is also important to note that the Cisco switch must learn the endpoint's IP address via DHCP snooping or IP Device Tracking to fill in the Framed-IP-Address field.

It is possible for a network device to send too much information, or to send accounting packets too often.

## Probe Configuration

The RADIUS probe has been enabled by default since ISE version 1.3. There is minimal configuration available on the ISE side to enable or configure the RADIUS probe. From the Profiling Configuration tab displayed in [Figure 10-11](#), click the check box next to the RADIUS probe to enable it.

Although there is not really any configuration possible with this probe, it is one of the most useful probes, especially when combined with Device Sensor.



**Figure 10-11 RADIUS Probe**

## Network Scan (NMAP) Probe

A welcome improvement to ISE version 1.1 was the addition of the Endpoint Scanning (NMAP) probe, which is now called the Network Scan (NMAP) probe in version 2.1. NMAP is a tool that uses port scans, SNMP, and other mechanisms to identify a device's Operating System, or other attributes of the device. The NMAP probe may be manually run against a single IP-Address or subnet. More importantly, the profiler engine can be configured to react to a profiling event with a reactive NMAP probe.

For example, when an endpoint is discovered to be an Apple-Device, ISE automatically launches an NMAP OS-Scan against that endpoint to determine if it is running macOS or iOS. From the results of that scan, ISE further classifies the device as a Mac or a mobile device.

ISE version 2.1 enhances that NMAP probe even further by leveraging the Server Message Block (SMB) protocol for probing Windows devices, leveraging McAfee ePolicy Orchestrator (ePO) ports to recognize corporate assets, and allowing custom ports to be configured to help identify custom devices.

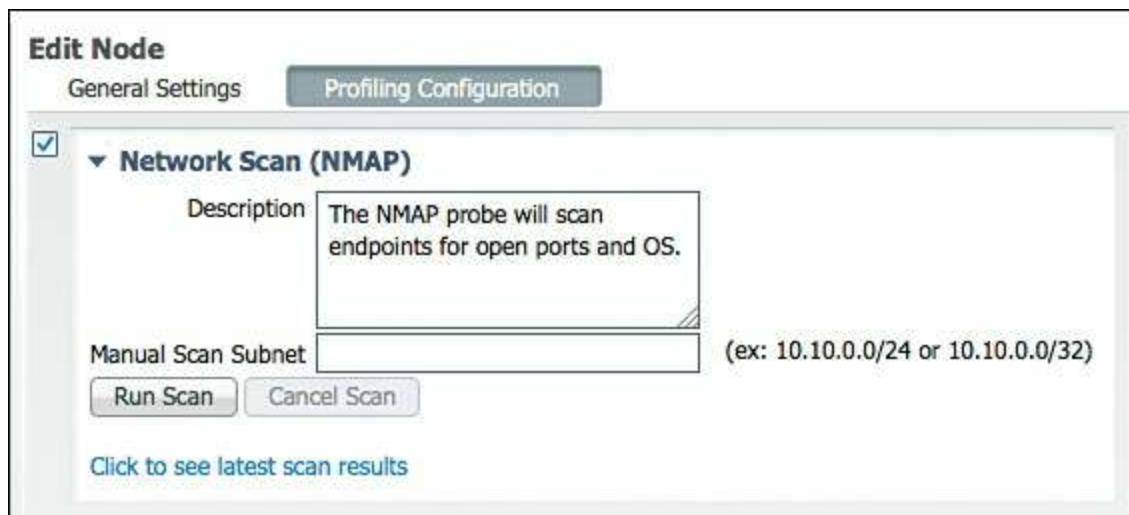
## Considerations with the NMAP Probe

The NMAP probe is executed against an IP address or range of IP addresses. However, it is absolutely crucial to keep in mind that the endpoint database uses a MAC address as the unique identifier of any endpoint. As such, the Policy Services Node relies on the MAC address-to-IP-address binding to update an endpoint's attributes with the results of the NMAP scan. Therefore, it is critical that the PSN receive valid information from the other probes.

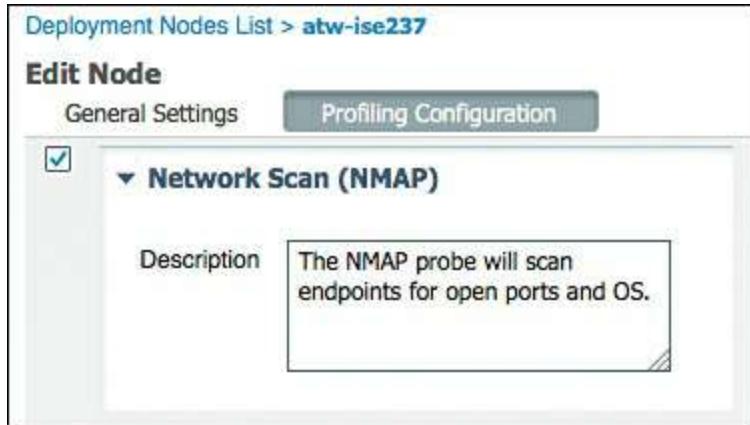
The NMAP probe can be manually run against a single IP address or subnet, or (more commonly) an NMAP scan can be triggered as an action of a profile.

## Probe Configuration

As with the other probes discussed thus far, only minimal configuration is needed for the NMAP probe. From the Profiling Configuration tab, displayed in [Figure 10-12](#) (ISE 1.2) and [10-13](#) (ISE 2.1), click the check box next to the Network Scan (NMAP) probe to enable it. [Figure 10-12](#) shows the NMAP probe configuration that exists in ISE 1.2 through ISE version 2.0, offering the option to run a manual scan against a single node or an entire network. [Figure 10-13](#) shows the same NMAP probe configuration in ISE 2.1. The manual scan option has been relocated and enhanced.



**Figure 10-12** Network Scan (NMAP) Probe in ISE 1.4



**Figure 10-13** Network Scan (NMAP) Probe in ISE 2.1

Beginning in ISE 2.1, the NMAP manual scan option is located at **Work Centers > Profiler > Manual Scans**, as shown in [Figure 10-14](#). This is a brilliant enhancement because it provides a lot more control and visibility from a single place. The following steps cover the options:

**Figure 10-14** Manual NMAP Scan

**Step 1.** Select which node in the deployment to run the scan from. This is important, because certain nodes may be closer to the target network, or certain nodes may not be able to reach some networks.

**Step 2.** Provide a subnet or host address (/32) to scan from that host.

**Step 3.** Choose either **Specify Scan Options**, as shown in [Figure 10-15](#), or **Select an Existing NMAP Scan Action**, as shown in [Figure 10-16](#).

**Run Manual NMAP Scan**

Node *	atw-ise237
Manual Scan Subnet *	10.1.41.0 / 24
Scan Options	<input checked="" type="radio"/> Specify scan options <input type="radio"/> Select an existing NMAP scan action
Configure NMAP scan subnet exclusions at: <a href="#">Work Centers &gt; Profiler &gt; Settings &gt; NMAP Scan Subnet Exclusions</a>	
<a href="#">Run Scan</a> <a href="#">Cancel Scan</a> <a href="#">Save As Scan Action...</a> <small>Click to see scan results</small>	
<small>Configure NMAP scan actions at: <a href="#">Work Centers &gt; Profiler &gt; Policy Elements &gt; NMAP Scan Actions</a></small>	

**Figure 10-15** Specify Scan Options

If you choose **Specify Scan Options**, you can click **Save As Scan Action** to store the new action and add it to the library of available scan actions. Those available scan actions are listed in the Existing NMAP Scan Actions drop-down menu (see [Figure 10-16](#)) when you choose **Select an Existing NMAP Scan Action**.

**Run Manual NMAP Scan**

Node *	atw-ise237
Manual Scan Subnet *	10.1.41.0 / 24
Scan Options	<input type="radio"/> Specify scan options <input checked="" type="radio"/> Select an existing NMAP scan action
Configure NMAP scan subnet exclusions at: <a href="#">Work Centers &gt; Profiler &gt; Settings &gt; NMAP Scan Subnet Exclusions</a>	
<a href="#">Run Scan</a> <a href="#">Cancel Scan</a> <small>Click to see scan results</small>	
<b>Existing NMAP Scan Actions</b> <div style="border: 1px solid #ccc; padding: 5px;">         Select Scan actions          OS-scan          SNMPPortsAndOS-scan          MCAFEEPOOrchestratorClientscan       </div>	

**Figure 10-16** Select an Existing NMAP Scan Action

**Step 4.** For purposes of demonstration, choose **Specify Scan Options**. The following are the scan options that are available on the right side of the screen:

- **OS:** This option leverages the NMAP capability to attempt OS detection by examining TCP/IP fingerprints; in other words, it tries to detect what the OS is

by the window size and other default settings in the TCP/IP stack.

- **SNMP Port:** The scan checks whether SNMP is listening on the discovered host. If it is, the SNMP probe can be used to perform an SNMP walk of the device.
- **Common Ports:** NMAP scans a predefined set of TCP and UDP ports.
- **Custom Ports:** Often, an organization has devices that are unique to the environment, especially when Internet of Things (IoT) devices are in use. This option is used to define specific ports that would help identify those devices.
- **Include Service Version Information:** The NMAP scan captures any detailed information that the vendor displays in banners associated with different services. This setting requires Common Ports or Custom Ports to be enabled as a prerequisite.
- **Run SMB Discovery Script:** SMB is used mainly by Microsoft operating systems. This option can be used to try to determine the OS, computer name, domain name, NetBIOS computer name, NetBIOS domain name, workgroup, time zone, and more.
- **Skip NMAP Host Discovery:** NMAP host discovery is used to probe to ensure an endpoint exists before performing deeper scans. The host discovery mechanism provides better performance by not wasting cycles trying to scan endpoints that do not exist. Enabling this bypass option ensures that the deeper scans are always attempted on each IP address in the scan range. This setting only applies to manual scans. When an NMAP scan action is triggered, the host discovery is always skipped and the endpoint is deep scanned.

#### Step 5. Click **Run Scan** to run the manual scan.

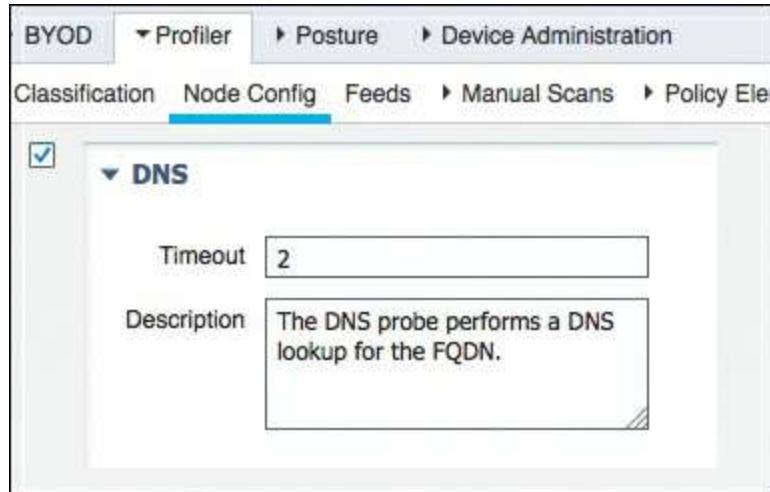
The NMAP probe will be explored in more detail in [Chapter 20, “Deployment Phases.”](#)

### DNS Probe

The DNS probe is used to collect the fully qualified domain name (FQDN) of an endpoint using a reverse lookup for the static or dynamic DNS registration of that endpoint. It is quite useful when looking for a specific DNS name format of corporate assets (Active Directory members).

A reverse DNS lookup will be completed only when an endpoint is detected by one of the DHCP, RADIUS, HTTP, or SNMP probes.

To enable the DNS probe, click the check box next to the DNS probe to enable it, as shown in [Figure 10-17](#). This probe uses the name-server configuration from the Identity Services Engine node itself.



**Figure 10-17** DNS Probe

## SNMPQUERY and SNMPTRAP Probes

SNMP is used to query NADs that do not yet support the Cisco Device Sensor. After enabling the SNMPQUERY probe, ISE polls all of the SNMP-enabled NADs at the configured polling interval.

**Note** It is recommended to remove SNMP settings from NADs that support Device Sensor, to avoid double work and wasted processing.

There are two SNMP probes: SNMPTRAP and SNMPQUERY.

### SNMPTRAP Probe

The SNMPTRAP probe receives information from the configured NAD(s) that support MAC notification, linkup, linkdown, and informs. The purpose of this probe is two-fold: it is used to trigger the SNMPQUERY probe and it is used as a toggle switch to allow the SNMPQUERY probe to reactively query a NAD instead of waiting for the periodic polling interval. Therefore, for the SNMPTRAP probe to be functional, you must also enable the SNMPQUERY probe.

The SNMPTRAP probe receives information from the specific NAD(s) when the MAC address table changes or when link state changes on a switch port. To make this feature functional, you must configure the NAD to send SNMP traps or informs.

### SNMPQUERY Probe

The SNMPQUERY probe does the bulk of the work. There are actually three different kinds of SNMPQUERY probes:

- **System probe:** Polls all NADs that are configured for SNMP at the configured

interval.

- **Interface probe:** Occurs in response to an SNMPTRAP or RADIUS accounting start packet (only if the SNMPTRAP probe is enabled).
- **Network Scan (NMAP) probe:** Triggers the SNMP walk of an endpoint.

When querying a NAD, ISE looks for interface data (which interface, which VLAN), session data (if the interface is Ethernet), Cisco Discovery Protocol (CDP), and Link Layer Discovery Protocol (LLDP) data. The CDP and LLDP data can be very useful in identifying a device type by its registered capabilities and similar attributes.

**Note** For distributed deployments, NAD polling is distributed among all Policy Services Nodes enabled for SNMPQUERY probes.

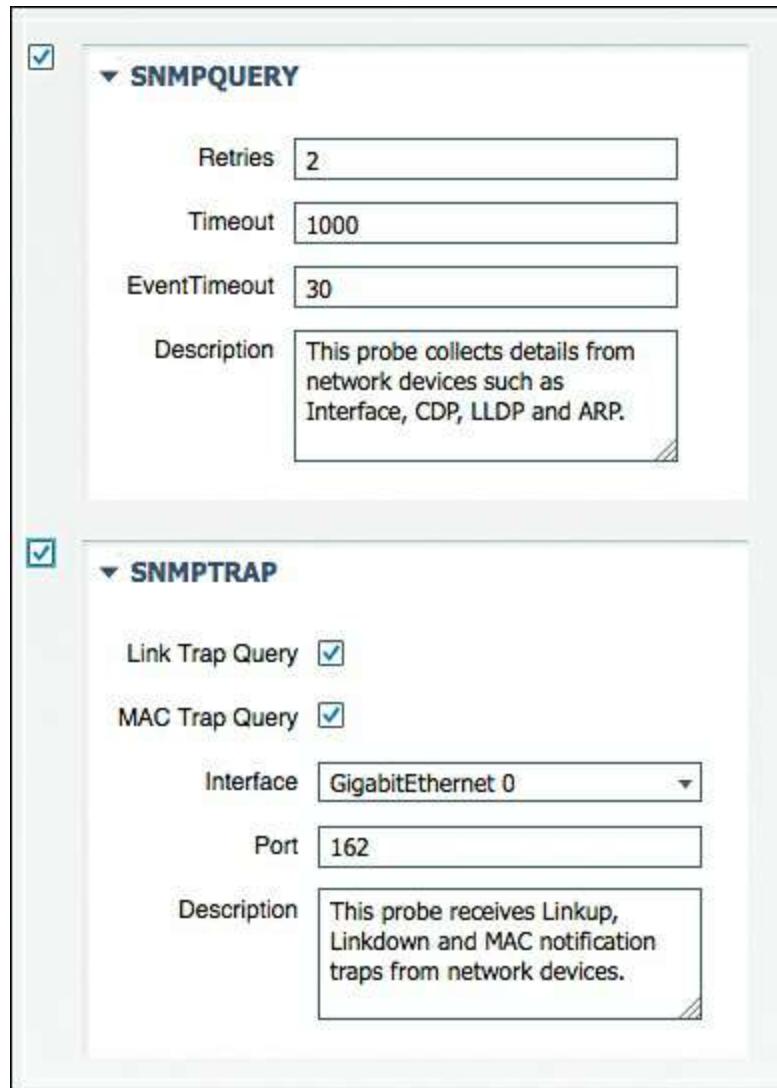
## Probe Configuration

Although there is a bit of configuration to these probes, such as the trap types to examine and the SNMP port, it is recommended that you leave these at their default settings unless directed otherwise by Cisco TAC.

**Step 1.** Click the check box next to the SNMPQUERY and SNMPTRAP probes to enable them.

**Step 2.** For the SNMPTRAP probe, select either the GigabitEthernet 0 interface or all interfaces. You can't choose multiple interfaces individually. The choice is a single interface or all interfaces.

[Figure 10-18](#) shows the enabled SNMP probes and their default settings.



**Figure 10-18** SNMP Probes

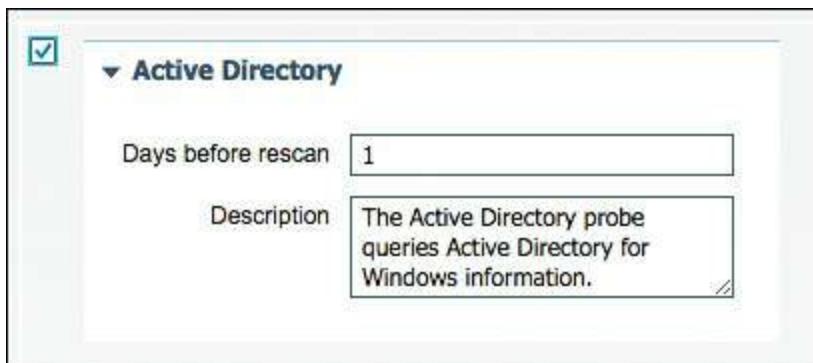
## Active Directory Probe

Added to ISE 2.1, the Active Directory (AD) probe is designed to help answer the question, “Is this endpoint a corporate asset?” This probe leverages what is known as the Active Directory Run Time (ADRT) connector, which is the powerful Active Directory connector introduced back in ISE 1.3. After a computer hostname is learned from either the DHCP probe or DNS probe, the AD probe will search in AD for attributes and allow the following attributes to be used in profiler policy creation:

- **AD-Host-Exists:** If the endpoint exists in AD, then it helps identify that it could be a corporate system.
- **AD-Join-Point:** Defines the AD domain where the host was located.
- **AD-Operating-System:** The OS type version of the endpoint.
- **AD-OS-Version:** The version of that endpoint’s OS.

■ **AD-Service-Pack:** The service pack version of the endpoint.

As this list of attributes demonstrates, this probe provides customers some decent flexibility to identify systems and glean inventory of those systems. [Figure 10-19](#) shows the Active Directory probe configuration. The configuration is limited to enabling (or disabling) the probe and configuring the number of days before rescanning for attributes.



**Figure 10-19** Active Directory Probe Configuration

## HTTP Probe

When applications use HTTP, such as a web browser or even software like Microsoft Outlook and Windows Update, it typically identifies itself, its application type, operating system, software vendor, and software revision by submitting an identification string to its operating peer. This information is transmitted in an HTTP Request-Header field called the User-Agent field.

Cisco ISE uses the information in HTTP packets, especially the User-Agent field, to help match signatures of what profile a device belongs in. The User-Agent field can tell ISE the difference between the various Windows versions, Android, Linux, Mac OS, and iOS device types, sometimes delivering OS and version details not available from other profile attributes. [Example 10-1](#) shows the user-agent string for Mac OS.

### Example 10-1 User Agent for Mac OS X 10.11 (El Capitan)

[Click here to view code image](#)

```
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11) AppleWebKit/601.1.27  
(KHTML, like Gecko)  
Version/8.1 Safari/601.1.27
```

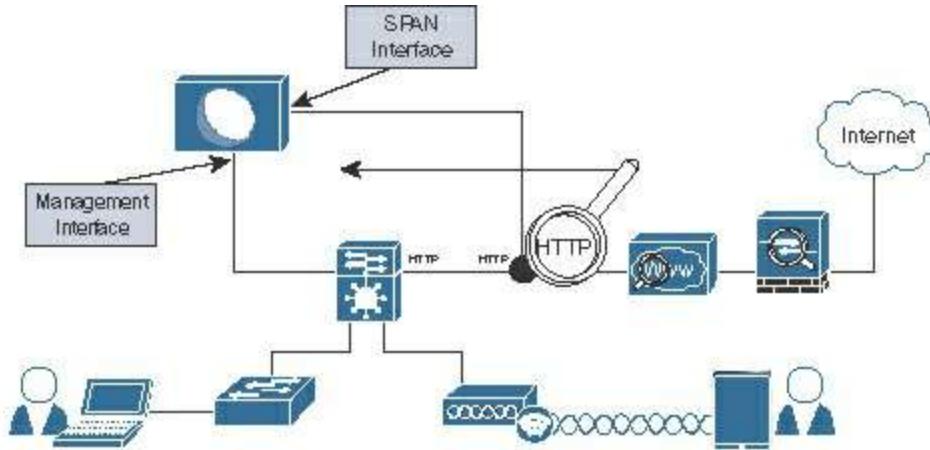
[Example 10-2](#) shows the User Agent for Windows 8.1.

### Example 10-2 User Agent for Windows 8.1

[Click here to view code image](#)

Mozilla/5.0Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; Touch; rv:11.0) like Gecko

As you can see, HTTP packet inspection is a key element to profiling effectively. [Figure 10-20](#) illustrates the logical design of ISE examining the HTTP packets.



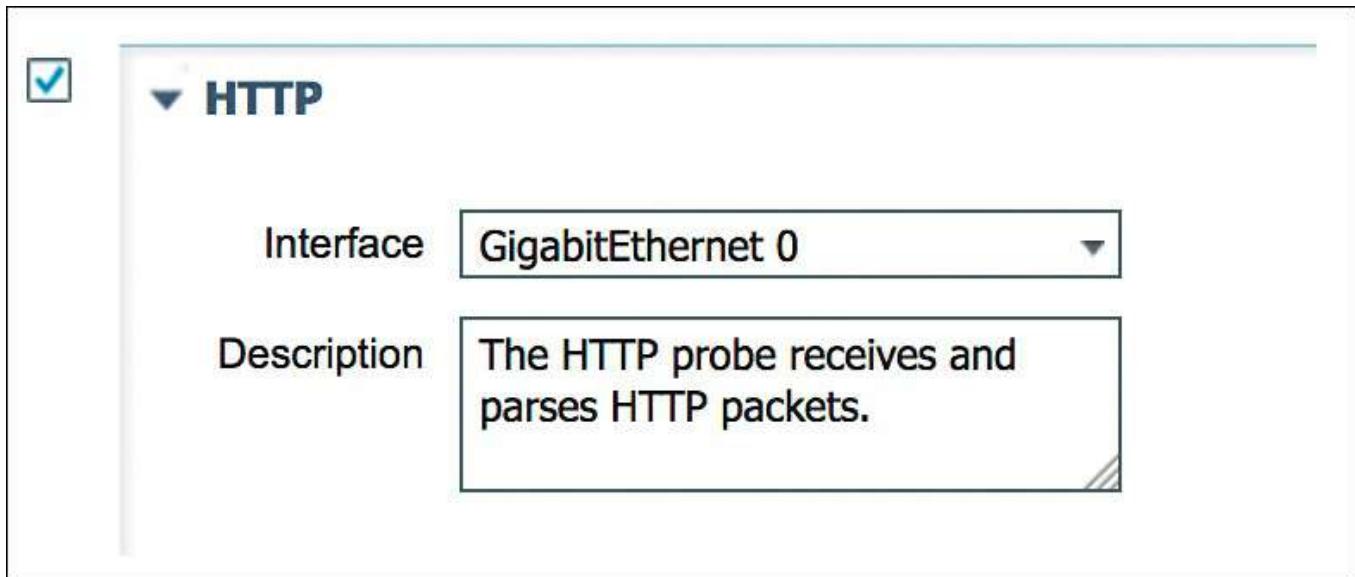
**Figure 10-20** HTTP SPAN Logical Design

There are two primary mechanisms for the HTTP probe to collect the HTTP traffic:

- **Use a SPAN session in true promiscuous mode:** When using the SPAN method, consider the best location to create the SPAN session and gather the data. One recommended location is the Internet edge, where a network organization typically deploys a Cisco IronPort Web Security Appliance.
- **Use a SPAN session in conjunction with a filter to limit the traffic visible to ISE:** Another option to use with the SPAN design is the use of VLAN ACL (VACL) captures on a Catalyst 6500 or ACL-based SPAN sessions on a Nexus 7000. These options allow you to build an ACL that defines exactly what traffic you want to capture and send along to ISE, instead of a pure promiscuous SPAN, where the ISE interface will see all traffic. This is a better way to manage the resource utilization on your ISE server when available.

As you can see, there are multiple ways to use the HTTP probe, and you should consider what works best for your environment and then deploy with that approach. In many environments, it is best to not use SPAN at all, but instead leverage ISE's own portals to capture the user-agent strings.

To configure the HTTP probe, click the check box next to the HTTP probe to enable it, as shown in [Figure 10-21](#). Select either the GigabitEthernet 0 interface or all interfaces.



**Figure 10-21** HTTP Probe

## HTTP Profiling Without Probes

ISE deployments do not require the use of SPAN sessions or VACL captures to receive the HTTP user-agent strings. The Web Portal system within ISE itself has been outfitted to collect the user-agent details from the web browser that is communicating with an ISE portal. This occurs regardless of whether profiling is enabled. The user-agent string is used to determine which OS is connecting and therefore which agent or client to send to the endpoint (in the cases of client provisioning and native supplicant provisioning).

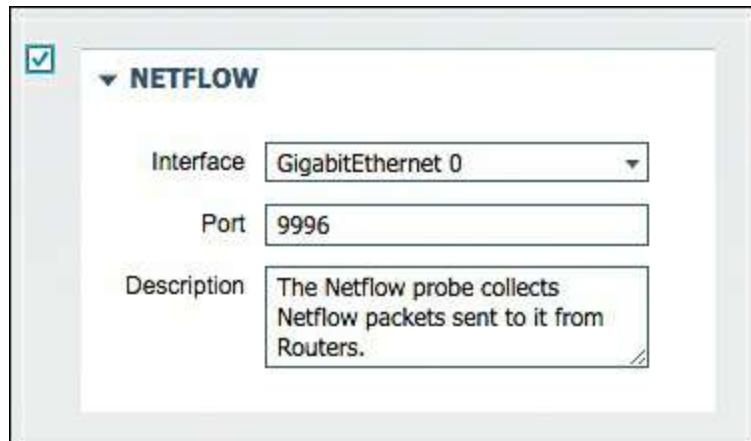
When any portal collects that user-agent string, it is automatically passed over to the profiling engine within ISE, without requiring the HTTP probe to be enabled. It is a simple and efficient way to get the extremely valuable user-agent string without having to rely on the computationally expensive SPAN methods.

## NetFlow Probe

NetFlow is an incredibly useful and undervalued security tool. Essentially, it is similar to a phone bill. A phone bill does not include transcripts of all the conversations you have had; instead, it is a summary record of all calls sent and received, including the duration of the call. Cisco routers and switches support NetFlow, sending a “record” of each packet that has been routed, including the ports and other very usable information.

Just enabling NetFlow in your infrastructure and forwarding all its data to ISE can quickly oversubscribe your Policy Services Node. If you are planning to use the NetFlow probe, it is highly recommended that you have a robust solution, such as Cisco Stealthwatch (from Cisco’s acquisition of Lancope), to filter out any unnecessary data and send only what you truly need to ISE. For that reason, this book does not focus on the NetFlow. It is recommended that you perform extensive planning prior to its use.

Configuring the NetFlow probe is limited to enabling the check box next to the NetFlow probe and selecting either the GigabitEthernet 0 interface or all interfaces. [Figure 10-22](#) shows the enabled NetFlow probe.



**Figure 10-22** NetFlow Probe

## Infrastructure Configuration

As an overall best practice, it is recommended to examine the cost-benefit analysis of using processor-intensive probes or probe designs. For example, it is often recommended to use DHCP Helper instead of configuring a SPAN session and examining a multitude of traffic that may or may not be relevant.

Let's use HTTP traffic as an example. HTTP traffic is extremely useful for identifying the OS on a client endpoint; however, HTTP SPAN can consume a large amount of system resources on the Policy Services Node. Additionally, it may not be critical to have full visibility into the user-agent strings of all devices, such as corporate-managed Windows devices.

Some deployments use VACL captures, which can limit what traffic is sent via the capture interface. Other deployments use the authorization policy in ISE to send unknown devices to an ISE portal, allowing the portal to update the profiling data (see the “HTTP Profiling Without Probes” section).

Craig Hyps is a Principal Technical Marketing Engineer with the ISE team and has presented a brilliant session at Cisco Live events many times related to designing ISE for scale and high availability. The session number may change depending on the year and location, but you can find the sessions, including video-on-demand recordings, by visiting <http://www.ciscolive.com>, navigating to **Learn Online > On-demand Library**, and then searching the Sessions category for “ISE for Scale and High Availability” or searching the Speakers category for the name “Hyps.” That session is fantastic and highly recommended for additional learning on this topic.

## DHCP Helper

As shown earlier in [Figure 10-8](#), the **ip helper-address** commands are configured on the default gateway for each of the access-layer VLANs. To configure the destination address to copy DHCP requests to, enter interface configuration mode of the Layer 3 address for the VLAN and enter the **ip helper-address [ip-address]** command. One method is to add the DHCP server and all applicable ISE Policy Service Nodes to the list of helper-address destinations.

[Figure 10-23](#) shows example output from a Layer 3 interface that is configured to send DHCP requests to the DHCP server in addition to two different ISE PSNs.

```
C6K-DIST#sho run int VLAN41
Building configuration...
```

```
Current configuration : 152 bytes
```

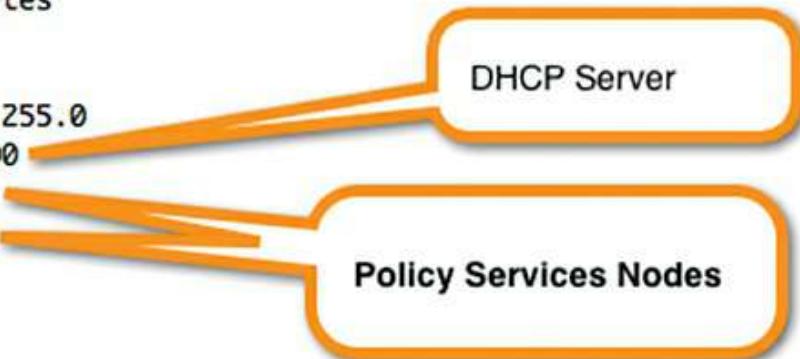
```
!
```

```
interface Vlan41
```

```
  ip address 10.1.41.1 255.255.255.0
  ip helper-address 10.1.100.100
  ip helper-address 10.1.100.3
  ip helper-address 10.1.100.4
```

```
end
```

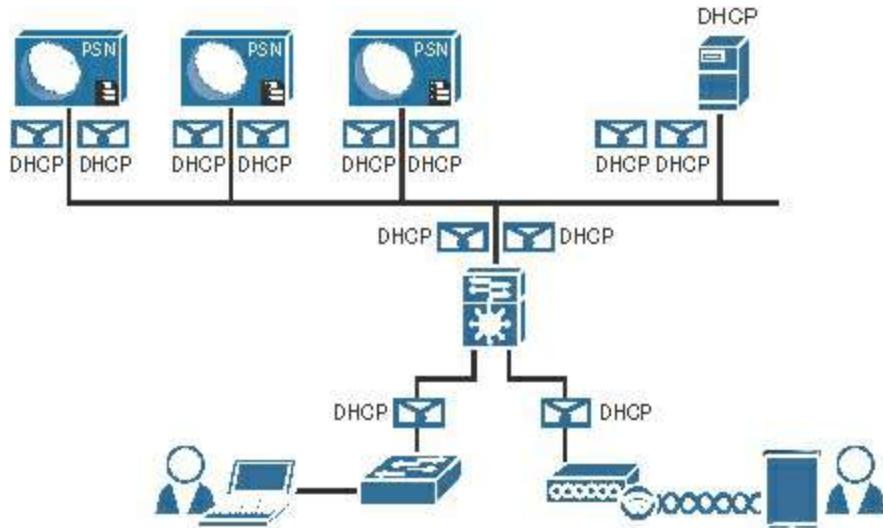
```
C6K-DIST#
```



**Figure 10-23 ip helper-address Settings**

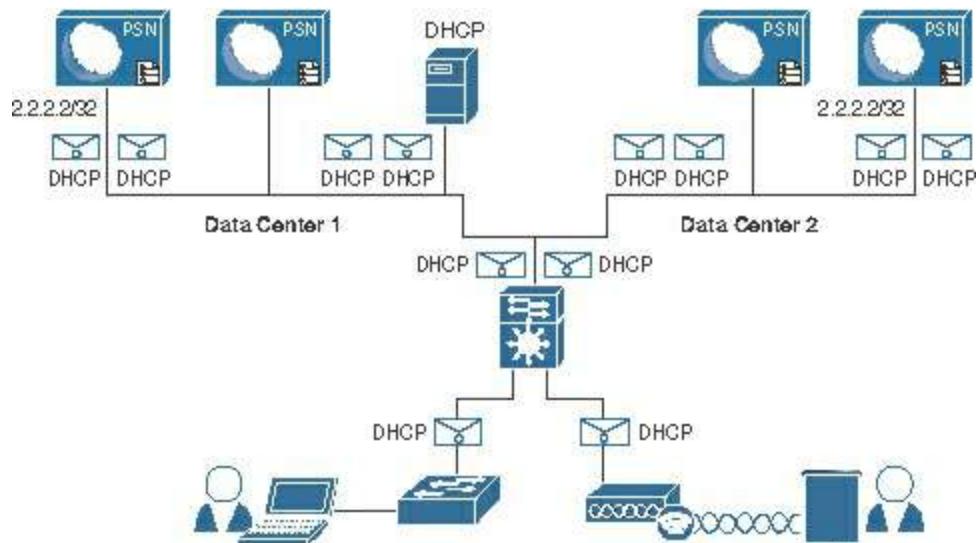
Copying all the DHCP requests to all the PSNs can have undesirable results, especially in large deployments. It will cause all PSNs that receive the DHCP packet to believe they should be owners of the endpoint data and therefore cause excess data replication. To alleviate that, it is often much more desirable to keep the DHCP traffic going to a specific PSN that is designated for profiling. Redundancy can be provided by leveraging techniques such as Anycast between two PSNs, possibly between PSNs located in different data centers.

[Figure 10-24](#) illustrates the DHCP traffic reaching the DHCP server but also all three PSNs in the network. In such a scenario, all three PSNs would claim ownership of the endpoint record and data replication between them would ensue. Whichever PSN ends up owning the RADIUS session would be the ultimate owner of the endpoint record and the data would replicate once more to it.



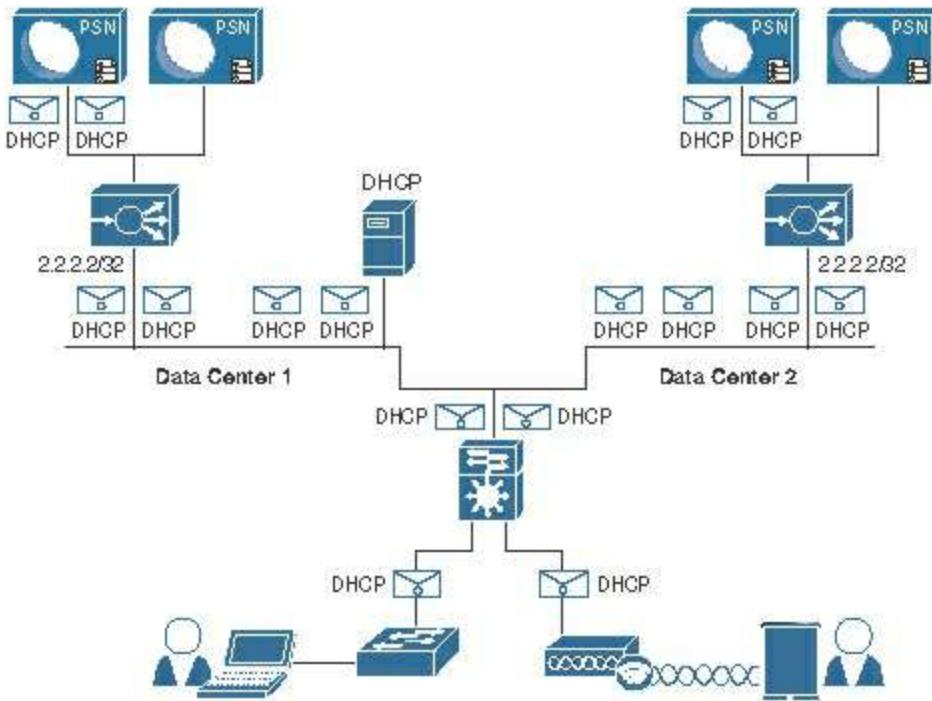
**Figure 10-24** ip helper Sending DHCP to All Nodes

[Figure 10-25](#) illustrates using two data centers with Anycast, where the same IP address exists in both data centers and routing is used to determine which one receives the DHCP packets. This provides redundancy for profiling while limiting how many replications must occur. See [Chapter 18, “Setting Up a Distributed ISE Deployment,”](#) for more information on Anycast.



**Figure 10-25** ip helper Sending DHCP to Anycast Address in Two Data Centers

[Figure 10-26](#) illustrates using two data centers with load balancers in each data center. The load balancers are configured with a single virtual IP (VIP) each, and in this case the same IP address exists on both VIPs (Anycast), with routing used to determine which one receives the DHCP packets. This provides redundancy for profiling, provides redundancy for RADIUS, and permits linear scaling by adding more PSNs behind each VIP, all while limiting how many replications must occur. (Chapter 18 also provides more information on load balancers.)



**Figure 10-26 ip helper** Sending DHCP to VIPs Using Anycast in Two Data Centers

These figures are examples of design choices for profiling that provide redundancy. These are just examples—you can imagine how many different variations and configuration alternatives exist. For more details on scaling and high availability, check out the recorded VoDs of the legendary Craig Hyps's Cisco Live presentations at <http://www.ciscolive.com> (using the search methods previously described).

As the technical editor of this book, E. Pete Karelis, so kindly pointed out, this is a good place to mention that the **ip helper** command will send more than just DHCP traffic to the destination. Enabling IP helper will also forward other broadcasts as unicasts in addition to BOOTPC/BOOTPS(DHCP):

```
Time (37), DNS (53), TACACS (49), NetBIOS Name (137), NetBIOS Datagram (138), TFTP (69)
```

They can be filtered out with the **no ip forward protocol udp** port-number command. Generally, it's good hygiene to not forward unnecessary traffic across your network.

## SPAN Configuration

A monitor session is configured in global-configuration mode, and can be local (SPAN) or remote (RSPAN). [Example 10-3](#) shows a SPAN configuration where an Internet-facing VLAN is the source of the session and an interface on the Policy Services Node is the destination. For more on SPAN configuration, see:

<http://www.cisco.com/c/en/us/support/docs-switches-catalyst-6500-series-switches/10570-41.html>.

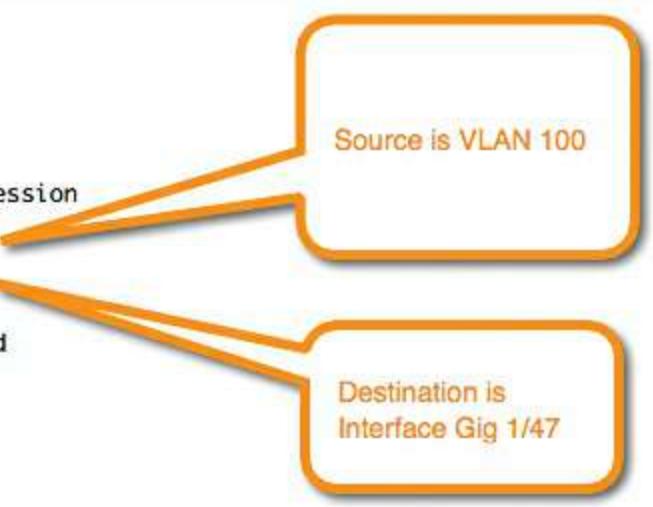
### Example 10-3 monitor session Command Input

[Click here to view code image](#)

```
DC-4948 (config) # monitor session [1-4] source [interface | vlan] [rx | tx ]  
DC-4948 (config) # monitor session [1-4] destination interface  
[interface_name]
```

[Figure 10-27](#) shows the output of the **show monitor session** command, where you can see the source and destination of the session.

```
DC-4948#  
DC-4948#  
DC-4948#  
DC-4948#show monitor session 1  
Session 1  
-----  
Type : Local Session  
Source VLANs :  
    Both : 100  
Destination Ports : Gi1/47  
    Encapsulation : Native  
    Ingress : Disabled  
    Learning : Disabled  
Filter Pkt Type :  
    RX Only : Good  
DC-4948#
```



**Figure 10-27** Example Monitor Session (SPAN) Configuration

### VLAN ACL Captures

VACL capture configuration is a multistep process, as demonstrated in the following example:

**Step 1.** Build an access list to classify the traffic you want to capture:

```
C6K-DIST(config) # ip access-list extended HTTP_TRAFFIC  
C6K-DIST(config-ext-nacl) # permit tcp any any eq www
```

**Step 2.** Build an access list for all the rest of the traffic:

```
C6K-DIST(config) # ip access-list extended ALL_TRAFFIC  
C6K-DIST(config-ext-nacl) # permit ip any any
```

**Step 3.** Create a VLAN access-map sequence to “capture” HTTP traffic:

```
C6K-DIST(config) # vlan access-map HTTP_MAP 10  
C6K-DIST(config-access-map) # match ip address HTTP_TRAFFIC
```

```
C6K-DIST(config-access-map)# action forward capture
```

**Step 4.** Add a new sequence to the access map to forward all other traffic:

```
C6K-DIST(config)# vlan access-map HTTP_MAP 20
C6K-DIST(config-access-map)# match ip address ALL_TRAFFIC
C6K-DIST(config-access-map)# action forward
```

**Step 5.** Apply the VLAN access map to the VLAN list:

```
C6K-DIST(config)# vlan filter HTTP_MAP vlan-list 41,42
```

**Step 6.** Configure the “destination” port for the PSN’s SPAN interface:

```
C6K-DIST(config-if)# switchport capture allowed vlan 41
C6K-DIST(config-if)# switchport capture allowed vlan add 42
C6K-DIST(config-if)# switchport capture
```

## Device Sensor

As described in the “RADIUS Probe” section, Device Sensor is a feature in the switch or wireless controller that collects endpoint attributes locally and then sends those attributes to ISE within RADIUS accounting packets. By allowing the network device to proactively send the profiling data to ISE, it can create a very elegant and distributed profiling architecture by placing the collection agents as close to the endpoint as possible. It also eliminates a lot of the redundancy considerations discussed in the “DHCP and DHCPSPAN Probes” section as well as the need to reactively query the switches for CDP/LLDP information. This greatly increases the scalability and performance of profiling by proactively sending the information to the correct ISE PSN automatically and removing any requirement for ISE to reactively reach out for the data.

Device Sensor made its way into Cisco switches in IOS 15.0(1) and IOS-XE 3.3.0. The Cisco WLC added Device Sensor capabilities in AireOS version 7.3.

Device Sensor requires a multipart configuration. The first portion is to configure the Device Sensor filter lists. These lists inform Device Sensor of which items to consider important for each of the different protocols.

Device Sensor supports three protocols: DHCP, CDP, and LLDP. Therefore, you must create one list for each protocol, as follows:

**Step 1.** Create a list for DHCP.

You need to configure three options for ISE: **host-name** , **class-identifier** , and **client-identifier** :

```
C3750X(config)# device-sensor filter-list dhcp list dhcp_list_name
C3750X(config-sensor-dhcplist)# option name host-name
C3750X(config-sensor-dhcplist)# option name class-identifier
```

```
C3750X(config-sensor-dhcplist)# option name client-identifier
```

## Step 2. Create a list for CDP.

You need to configure two CDP options for ISE: **device-name** and **platform-type** :

```
C3750X(config)# device-sensor filter-list cdp list cdp_list_name  
C3750X(config-sensor-cdplist)# tlv name device-name  
C3750X(config-sensor-cdplist)# tlv name platform-type
```

## Step 3. Create a list for LLDP.

You need to configure three LLDP options for ISE: **port-id** , **system-name** , and **system-description** :

```
C3750X(config)# device-sensor filter-list lldp list lldp_list_name  
C3750X(config-sensor-lldplist)# tlv name port-id  
C3750X(config-sensor-lldplist)# tlv name system-name  
C3750X(config-sensor-lldplist)# tlv name system-description
```

## Step 4. Include the lists created in Steps 1–3 in the Device Sensor.

In the preceding steps, you defined what options that Device Sensor should store. At this point, configure Device Sensor to use those lists:

```
C3750X(config)# device-sensor filter-spec dhcp include list  
    dhcp_list_name  
C3750X(config)# device-sensor filter-spec lldp include list  
    cdp_list_name  
C3750X(config)# device-sensor filter-spec cdp include list  
    lldp_list_name
```

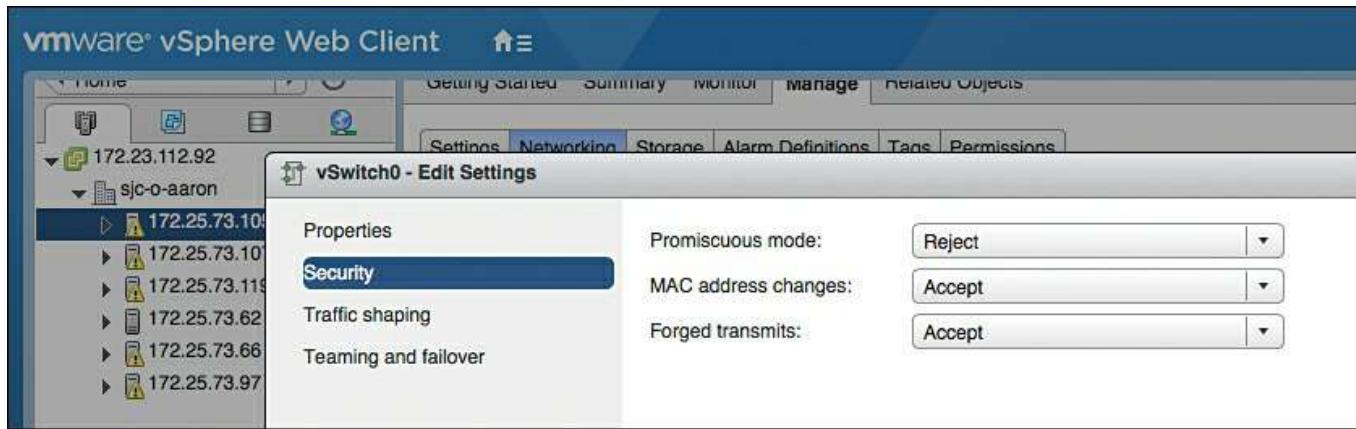
## Step 5. Enable Device Sensor.

Device Sensor is now configured. Enable the device-sensor service to run on the switch, and configure when it will send its updates:

```
C3750X(config)# device-sensor accounting  
C3750X(config)# device-sensor notify all-changes
```

## VMware Configurations to Allow Promiscuous Mode

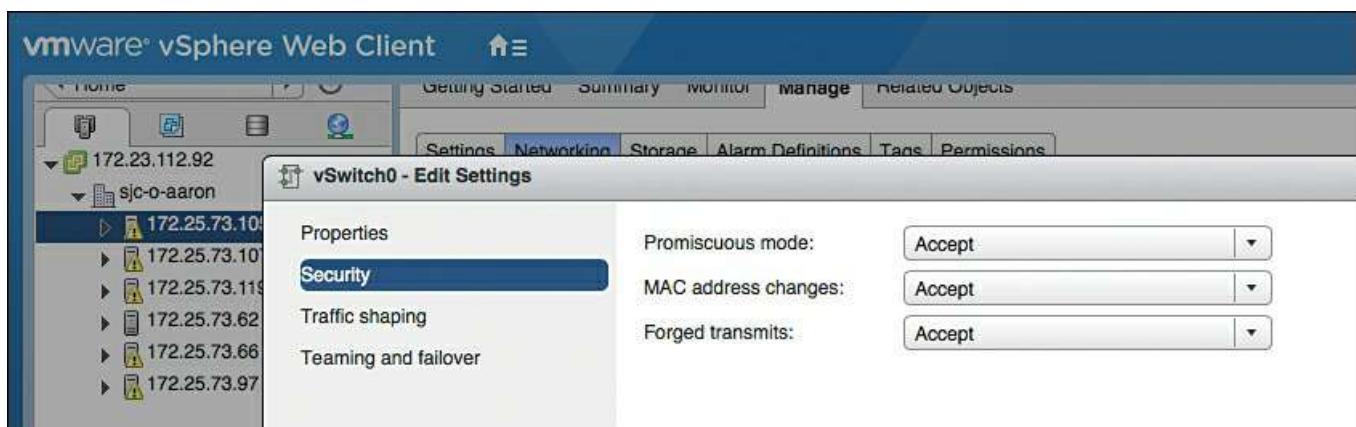
As shown in [Figure 10-28](#), a VMware vSwitch rejects promiscuous mode by default. To use SPAN type probes with ISE, you configure the vSwitch to allow promiscuous connections.



**Figure 10-28** Default vSwitch Configuration

To modify the configuration and enable promiscuous traffic, follow these steps:

- Step 1.** Highlight the vSwitch and click **Edit Settings**.
- Step 2.** In the Edit Settings dialog box, click **Security** in the navigation menu.
- Step 3.** Change the Promiscuous Mode drop-down to **Accept**, as shown in [Figure 10-29](#).



**Figure 10-29** Promiscuous vSwitch Setting

## Profiling Policies

Collecting the data for profiling is only part of the solution. The other aspects are to have endpoint signatures and a policy engine to compare the collected attributes to those signatures, which will lead to the assignment of the endpoint profile.

The profiling engine is a policy engine that works a lot like an intrusion detection system (IDS) that compares traffic to a set of signatures to identify suspicious activity. The profiling engine has hundreds of built-in signatures, called profiles, that are designed to match when certain attributes exist. Additionally, much like an IDS system, an update service enables the engine to download new signatures.

## Profiler Feed Service

Although ISE comes with a very large and comprehensive list of signatures to classify endpoints (profiles), there are so many more devices that are produced almost daily (think of the next smartphone or version of the phone's OS); and there is a constant stream of new profiles created by Cisco that should be shared to the ISE deployments of the world. That's why Cisco created a profiler feed service. When a new device is released to market, Cisco creates a profile for it. New profiles are created from Cisco partners and device manufacturers. Cisco also has a team that focuses on profile creation. The ISE profiler feed service is used to distribute these new profiles after the Quality Assurance (QA) team has approved them.

### Configuring the Profiler Feed Service

Configuring the feed service is straightforward. Once enabled, it reaches out to [Cisco.com](https://Cisco.com) at the set time interval and downloads any published profiles. Among its many features, it offers an option to send an email alert to the administrator when an update occurs, an Undo Latest button for reversing the latest update, a Test Feed Service Connection button to ensure the feed service is reachable and working, a link to view a report on the latest updates, and an option to send your information anonymously to Cisco to help with understanding how many customers are utilizing the feed service.

[Figure 10-30](#) shows a configured Profiler Feed Service Configuration screen, which is located under both **Administration > Feed Service > Profiler** and **Work Centers > Profiler > Feeds**.

**Identity Services Engine**

Home ▶ Context Visibility ▶ Operations ▶ Policy ▶ Administration

▶ Network Access ▶ Guest Access ▶ TrustSec ▶ BYOD ▶ Profiler ▶ Posture ▶ Device Administration

Overview Ext Id Sources Network Devices Endpoint Classification Node Config Feeds ▶ Manual Scans ▶ Policy Eler

### Profiler Feed Service Configuration

**Online Subscription Update**   **Offline Manual Update**

Update occur automatically at a regularly scheduled interval and can also be done manually.

Enable Online Subscription Update

Automatically check for updates every day at  hh  mm UTC [i](#)

**Update Now**

**Test Feed Service Connection**   Test result: Success

Notify administrator when download occurs  
Administrator email address

Provide Cisco anonymous information to help improve profiling accuracy [i](#)

Include Administrator Information (optional)

First name   
Last name   
Email address   
Phone

**Save**   **Reset**

**Latest Update**

Latest applied feed occurred on: 2016-06-01 01:16:00 UTC

**Undo Latest**

[Go to Update Report Page](#)

The screenshot shows the configuration interface for the Profiler Feed Service. It includes sections for enabling online subscription updates, setting the update schedule (every day at 01:16 UTC), testing the feed service connection (success), notifying administrators via email (set to loxx@cisco.com), and providing optional Cisco anonymous information for improved profiling accuracy. The anonymous information section includes fields for First name (Aaron), Last name (Woland), Email address (loxx@cisco.com), and Phone (000-002-0113). At the bottom, it shows the latest update occurred on June 1, 2016, at 01:16:00 UTC, with options to undo the latest update or go to the update report page.

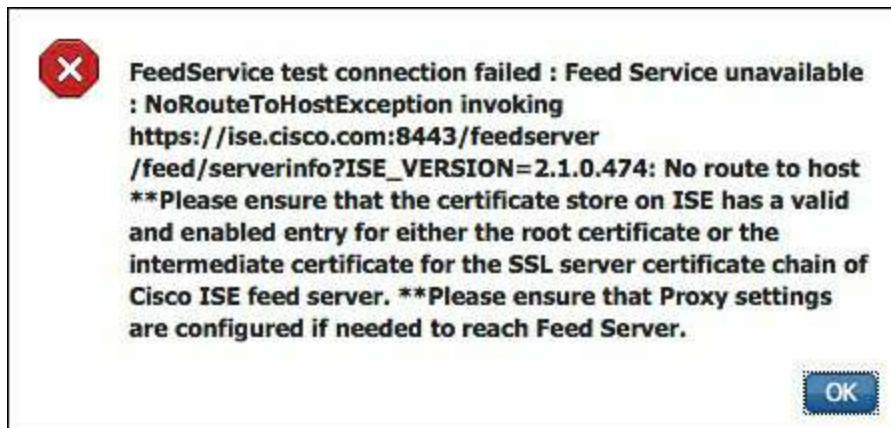
**Figure 10-30** Configured Profiler Feed Service

If you don't want to wait for a configured interval for the feed service to run, you can

click the **Update Now** button. Be cautious with manually updating the profiles during a production workday. When the profiles are updated, it causes all endpoints in the endpoint database to be compared against the new list of profiles. In other words, a complete re-profiling of endpoints occurs and that can be very processor-intensive.

## Verifying the Profiler Feed Service

The Test Feed Service Connection button in [Figure 10-30](#) was added in ISE version 1.4. The test verifies not only reachability of the feed server, but also that the connection is successful. [Figure 10-31](#) shows an example of a failure message when a proxy server is required but none is configured.



**Figure 10-31** Feed Service Connection Failure

Another method to verify that the feed service is working is to click the **Go to Update Report Page** link on the Profiler Feed Service Configuration screen, as shown in [Figure 10-32](#).



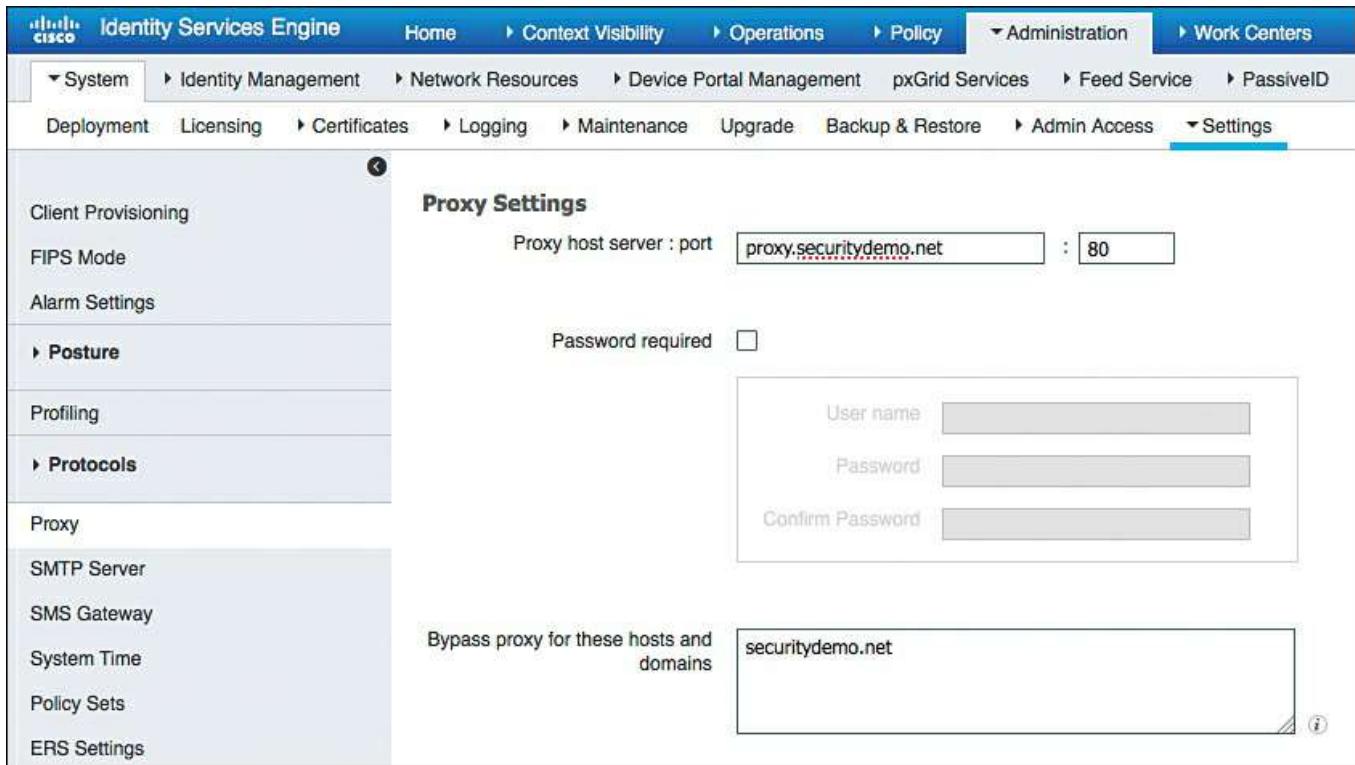
**Figure 10-32** Go to Update Report Page Link

Clicking that link opens another window with the Change Configuration Audit report prefiltered for the feed service-related entries, as shown in [Figure 10-33](#).

Change Configuration Audit						
Logged At	Administrator	Server	Interface	Object Type	Object Name	Event
2015-01-06 01:06:42.725	FeedService	atw-cp-ise02	GUI	FeedEndpointPoli	RICOH-Aficio-MP	Changed configuration
2015-01-06 01:06:42.231	FeedService	atw-cp-ise02	GUI	EndpointPolicy	RICOH-Aficio-MP	Added configuration
2015-01-06 01:06:41.885	FeedService	atw-cp-ise02	GUI	Rule	RICOH-Aficio-MP	Added configuration
2015-01-06 01:06:41.804	FeedService	atw-cp-ise02	GUI	Check	RICOH-Aficio-MP	Added configuration
2015-01-06 01:06:41.738	FeedService	atw-cp-ise02	GUI	FeedEndpointPoli	RICOH-Aficio-MP	Changed configuration
2015-01-06 01:06:41.243	FeedService	atw-cp-ise02	GUI	EndpointPolicy	RICOH-Aficio-MP	Added configuration
2015-01-06 01:06:40.893	FeedService	atw-cp-ise02	GUI	Rule	RICOH-Aficio-MP	Added configuration
2015-01-06 01:06:40.813	FeedService	atw-cp-ise02	GUI	Check	RICOH-Aficio-MP	Added configuration
2015-01-06 01:06:40.745	FeedService	atw-cp-ise02	GUI	FeedEndpointPoli	RICOH-Aficio-MP	Changed configuration
2015-01-06 01:06:40.253	FeedService	atw-cp-ise02	GUI	EndpointPolicy	RICOH-Aficio-MP	Added configuration
2015-01-06 01:06:39.898	FeedService	atw-cp-ise02	GUI	Rule	RICOH-Aficio-MP	Added configuration
2015-01-06 01:06:39.816	FeedService	atw-cp-ise02	GUI	Check	RICOH-Aficio-MP	Added configuration
2015-01-06 01:06:39.737	FeedService	atw-cp-ise02	GUI	FeedEndpointPoli	RICOH-Aficio-MP	Changed configuration
2015-01-06 01:06:39.247	FeedService	atw-cp-ise02	GUI	EndpointPolicy	RICOH-Aficio-MP	Added configuration
2015-01-06 01:06:38.878	FeedService	atw-cp-ise02	GUI	Rule	RICOH-Aficio-MP	Added configuration

**Figure 10-33** Change Configuration Audit for Feed Service

Because ISE must be able to reach [Cisco.com](http://Cisco.com) for the profiler feed service to function, you may need to configure ISE to use a proxy server to reach the Internet. This optional configuration is located at **Administration > System > Settings > Proxy**, as shown in [Figure 10-34](#).



**Figure 10-34** Proxy Setting

## Offline Manual Update

Not all organizations are permitted to allow ISE to communicate outbound to the feed service. Many are deployed in air-gapped networks. For those environments, an offline manual update was added in ISE version 2.1.

To use the offline feed update, follow these steps:

**Step 1.** Navigate to the offline feed service page via either **Administration > Feed Service > Profiler > Offline Manual Update**, as shown in [Figure 10-35](#), or **Work Centers > Profiler > Feeds > Offline Manual Update**.

**Profiler Feed Service Configuration**

Online Subscription Update    Offline Manual Update

Updates are downloaded manually and then must be applied to take effect.

Download Updated Profile Policies *(i)*

Choose the Profile Policies file to use for the manual update.

Browse...    No file selected.

Apply Update

**Latest Update**

Latest applied feed occurred on:

Undo Latest

**Figure 10-35** Offline Manual Update Tab

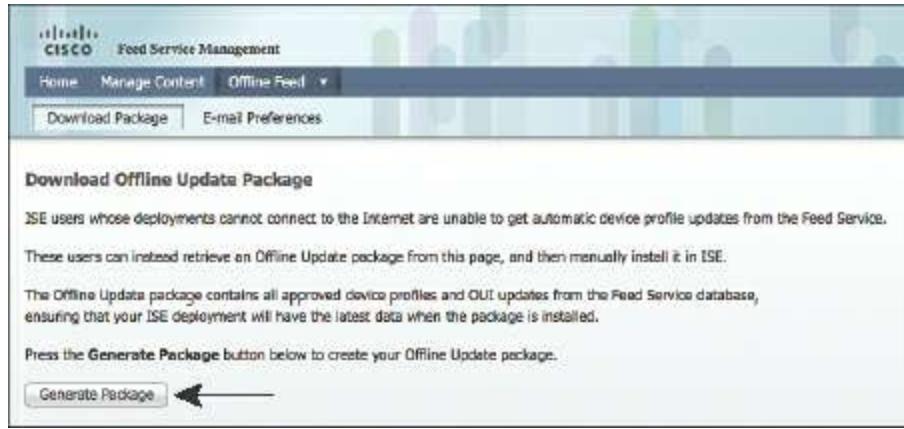
**Step 2.** Click **Download Updated Profile Policies**. This opens the feed service at <http://ise.cisco.com/partner>. Log in with your [Cisco.com](#) user ID and password.

**Step 3.** Choose **Offline Feed > Download Package** , as shown in [Figure 10-36](#).



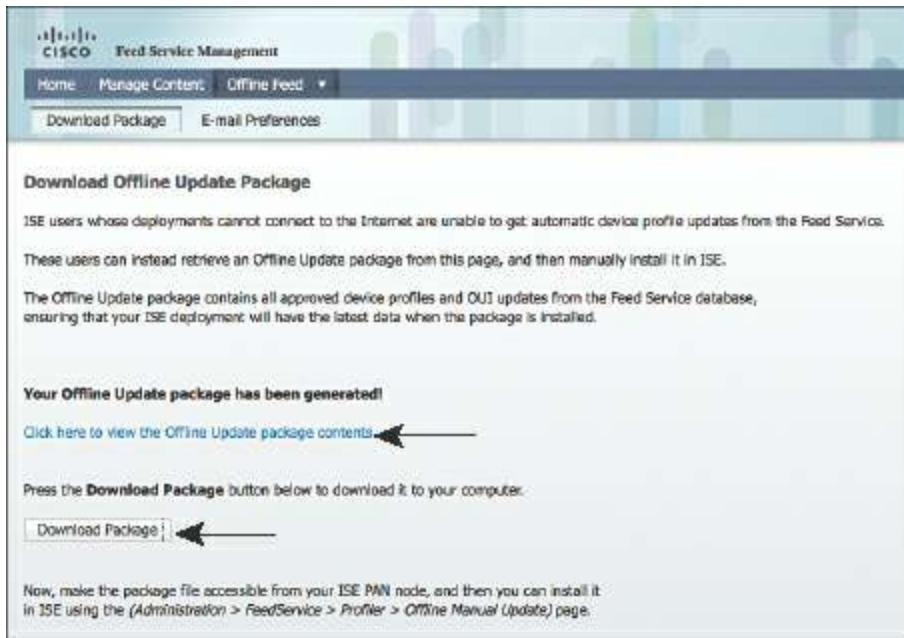
**Figure 10-36** Download Package Option

**Step 4.** Click **Generate Package** , as shown in [Figure 10-37](#).



**Figure 10-37** Generate Package Button

**Step 5.** Click **Download Package** , as shown in [Figure 10-38](#), and save the resulting tar.gz.gpg file.



**Figure 10-38** Download Package Button and Link to View Package Contents

**Step 6.** To see the contents of the Offline Update package, click the **Click Here to View the Offline Update Package Contents** link shown in [Figure 10-38](#), which launches another window that displays the contents, as shown in [Figure 10-39](#).

# Cisco ISE Feed Service - Offline Update Package

**Package Creation Date:** Tue May 31 20:49:00 PDT 2016

This report lists the approved device profiles contained in this Offline Update Package.

Device profiles in each feed are listed newest first.

**Feed:** [Profiler:1](#) (204 approved device profiles)

**Feed:** [Profiler:2](#) (63 approved device profiles, **2 new in last 30 days**)

**Feed:** [Profiler:3](#) (7 approved device profiles)

**Feed:** [OUI](#) (OUI data was last updated from IEEE on Tue May 31 19:19 PDT 2016)

## Feed: Profiler:1

### 1. Device Profile: Router (v1)

**Description:** Profiler Policy for Router

**Approved:** Mon Apr 25 02:18 PDT 2016

**Feed:** Profiler:1

### 2. Device Profile: HP-Printer (v2)

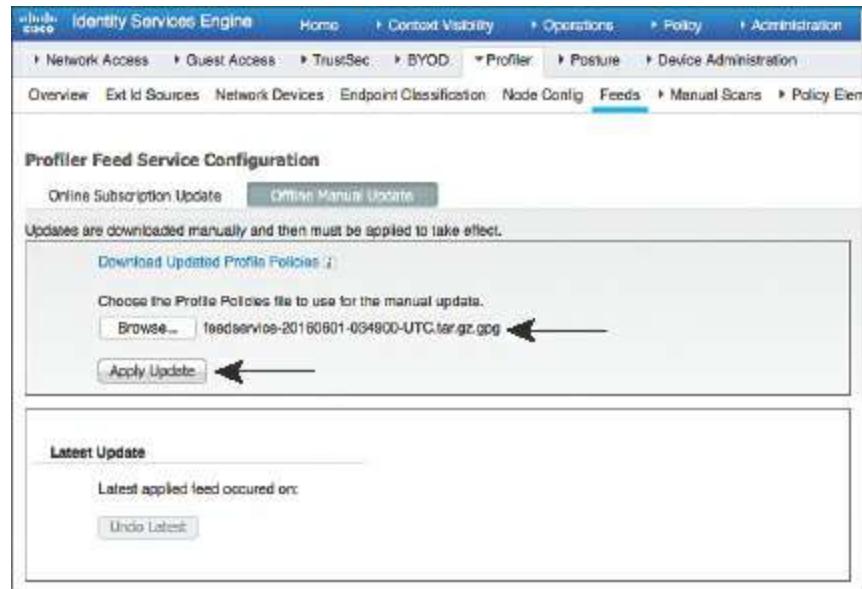
**Description:** Profiler Policy for HP-Printer

**Approved:** Fri Apr 15 00:18 PDT 2016

**Feed:** Profiler:1

**Figure 10-39** Cisco ISE Feed Service Offline Update Package Contents

**Step 7.** Back on the Offline Manual Update tab (shown in [Figure 10-35](#)), click **Browse** to locate the tar.gz.gpg file that you downloaded in Step 6. Select the file and click **Apply Update** , as shown in [Figure 10-40](#).



**Figure 10-40** Apply Update Button

## Endpoint Profile Policies

As previously described, the profiler probes collect attributes of endpoints. The endpoint profiler policies are similar to signatures, because they define the endpoint profiles themselves. For example, to match an Apple-Device profile, the endpoint must have a MAC address beginning with an Apple OUI.

Each endpoint profile policy defines a set of attributes that must be matched for a device to be classified as that endpoint type. ISE has a large number of predefined profile policies, and you can use the feed service to update those policies and provide new ones.

You can view the endpoint profile policies by navigating to **Policy > Profiling** or, as seen in [Figure 10-41, Work Centers > Profiler > Profiling Policies](#).

Profiling Policy Name	Policy Enabled	System Type	Description
2Wire-Device	Enabled	Cisco Provided	Policy for 2Wire-Device
3Com-Device	Enabled	Cisco Provided	Policy for 3Com-Device
Aastra-Device	Enabled	Cisco Provided	Policy for Aastra-Device
Aerohive-Device	Enabled	Cisco Provided	Policy for Aerohive-Device
American-Power-Convers	Enabled	Cisco Provided	Policy for American-Power-Conversion-Device
Android	Enabled	Cisco Provided	Policy for all Android Smartphones
Apple-Device	Enabled	Cisco Provided	Policy for Apple-Device
Applera-Device	Enabled	Cisco Provided	Policy for Applera-Device
Arris-Device	Enabled	Cisco Provided	Policy for Arris-Device
Aruba-Device	Enabled	Cisco Provided	Policy for Aruba-Device
Asus-Device	Enabled	Cisco Provided	Policy for Asus-Device
Atrie-Device	Enabled	Cisco Provided	Policy for Atrie-Device
Automated-Logic-Device	Enabled	Cisco Provided	Policy for Automated-Logic-Device
Avaya-Device	Enabled	Cisco Provided	Policy for Avaya-Device
Axis-Device	Enabled	Cisco Provided	Policy for Axis-Device
Belkin-Device	Enabled	Cisco Provided	Policy for Belkin-Device
BlackBerry	Enabled	Cisco Provided	Policy for BlackBerry
Brother-Device	Enabled	Cisco Provided	Policy for Brother-Device
Canon-Device	Enabled	Cisco Provided	Policy for Canon-Device
CareFusion-Alaris-Pump	Enabled	Cisco Provided	Policy for CareFusion-Alaris-Pump
Cisco-Device	Enabled	Cisco Provided	Policy for Cisco-Device
Compex-Device	Enabled	Cisco Provided	Policy for Compex-Device
Crestron-Device	Enabled	Cisco Provided	Policy for Crestron-Device
Cyber-Power-System-Dev	Enabled	Cisco Provided	Policy for Cyber-Power-System-Device
DLink-Device	Enabled	Cisco Provided	Policy for DLink-Device
Dell-Device	Enabled	Cisco Provided	Policy for Dell-Device
Draeger-Device	Enabled	Cisco Provided	Policy for Draeger-Device
EMC-Device	Enabled	Cisco Provided	Policy for EMC-Device
Enterasys-Device	Enabled	Cisco Provided	Policy for Enterasys-Device
Android	Enabled	Cisco Provided	Policy for all Android Smartphones
Android-Amazon	Enabled	Cisco Provided	Policy for Android Amazon Kindle
Android-Amazon-Kindle	Enabled	Cisco Provided	Policy for Android Amazon Kindle
Android-Amazon-Phone	Enabled	Cisco Provided	Policy for Android Amazon Phone
Android-Amazon-TV	Enabled	Cisco Provided	Policy for Android Amazon TV
Android-Asus	Enabled	Cisco Provided	Policy for Android-Asus
Android-Google	Enabled	Cisco Provided	Policy for Android-Google
Android-Google-Glass	Enabled	Cisco Provided	Policy for Android-Google Glass
Android-HTC	Enabled	Cisco Provided	Policy for Android-HTC
Android-HTC-Phone	Enabled	Cisco Provided	Policy for Android-HTC-Phone
Android-HTC-Phone-One-S	Enabled	Cisco Provided	Policy for Android-HTC-Phone One S
Android-HTC-Phone-Sensation-	Enabled	Cisco Provided	Policy for Android-HTC-Phone Sensation
Android-HTC-Phone-Wildfire-S	Enabled	Cisco Provided	Policy for Android-HTC-Phone Wildfire S
Android-LG	Enabled	Cisco Provided	Policy for Android-LG
Android-Lenovo	Enabled	Cisco Provided	Policy for Android-Lenovo
Android-Lenovo-Phone	Enabled	Cisco Provided	Policy for Android-Lenovo Phone
Android-Lenovo-Phone-A660	Enabled	Cisco Provided	Policy for Android-Lenovo Phone A660
Android-Lenovo-Phone-P780	Enabled	Cisco Provided	Policy for Android-Lenovo Phone P780
Android-Micromax	Enabled	Cisco Provided	Policy for Android-Micromax

**Figure 10-41 Profiling Policies Screen**

Each profile is listed as Cisco Provided or Administrator Modified. This classification ensures that the feed service will not override a profile that has been changed by the administrator.

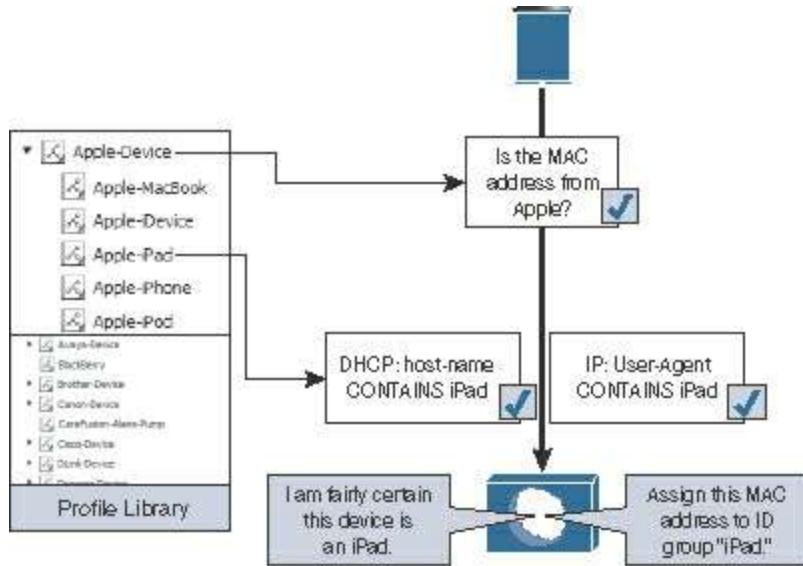
Profiles are hierarchical and inclusive in nature, and you may pick any level to use within your authorization policies, enabling you to be very specific or broad in your rules. [Figure 10-42](#) shows a parent policy named **Android** with a child policy named **Android HTC**, which in turn has another child policy named **Android HTC-Phone** (**Android > Android-HTC > Android-HTC-Phone** ).



**Figure 10-42** Android Profile Hierarchy Example

When building an authorization policy, you can choose to use the profile at any point in that chain. If you were to select Android, it would apply to all devices classified as Android as well as anything classified as a child profile of Android. For example, it would include Android-Sony-Ericsson-Tablet.

To serve as further examples of the hierarchy, there is a predefined authorization rule named Profiled Cisco IP Phones. This rule permits full access to the network and assigns permission to join the Voice VLAN—for all devices that are profiled as a Cisco-IP-Phone parent profile and any of the child profiles. [Figure 10-43](#) displays how a profile hierarchy is built within ISE.



**Figure 10-43** Profiling Hierarchy Illustrated

[Figure 10-44](#) shows this rule.

Status	Rule Name	Conditions (identify groups and other conditions)	Permissions
✓	Wireless Black List Default	Blacklist AND Wireless_Access	Then: Blackhole_Wireless_Access
✓	Profiled Cisco IP Phones	Cisco-IP-Phone	Then: Cisco_IP_Phones
✓	Profiled Non Cisco IP Phones	Non_Cisco_Profied_Phones	Then: Non_Cisco_IP_Phones

**Figure 10-44** Default Profiled Cisco IP Phones Rule

Continuing to examine policy hierarchy and how it works, you will dig into a specific example in the next section, drilling into the endpoint details.

## Context Visibility

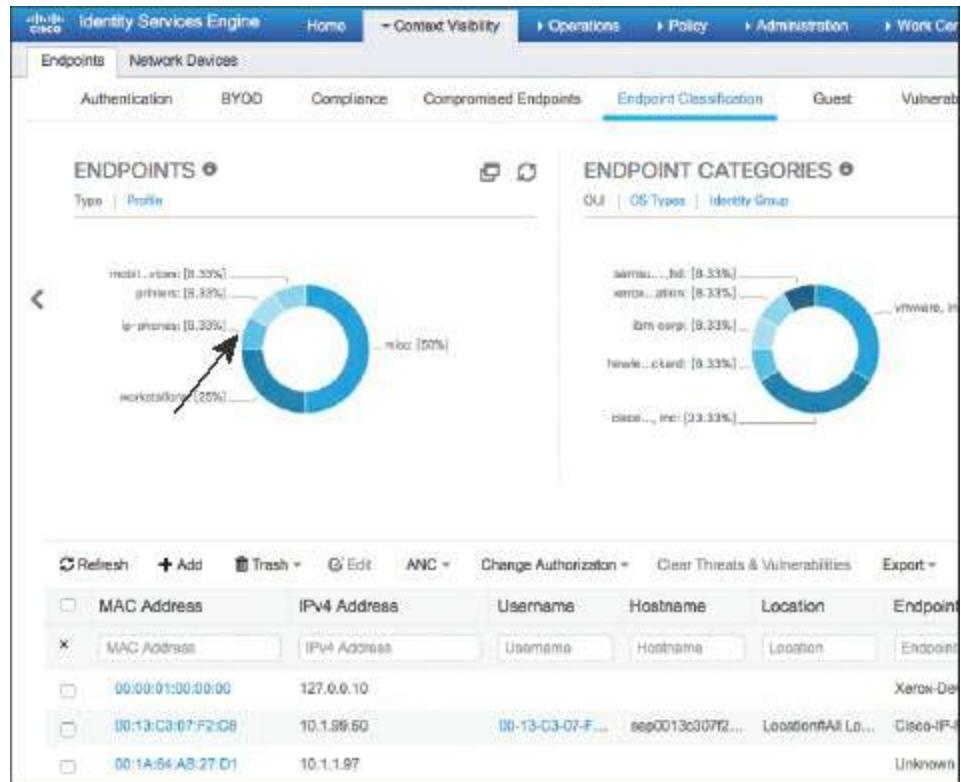
In ISE 2.0 and earlier, the endpoints were hidden away under **Administration > Identity Management > Identities > Endpoints**. Beginning with ISE 2.1, the endpoints have been brought front and center with a major presence on the main dashboard, a full Profiler Work Center, and a new GUI area known as Context Visibility.

In the example network in the figures, there is a Cisco 7970 IP Phone, and that phone has been granted access from the Profiled Cisco IP Phones default authorization rule that you examined in [Figure 10-44](#), which permits all endpoints matching a Cisco-IP-Phone profiler identity group.

Start by examining the endpoint attributes and comparing them to the profiling policies:

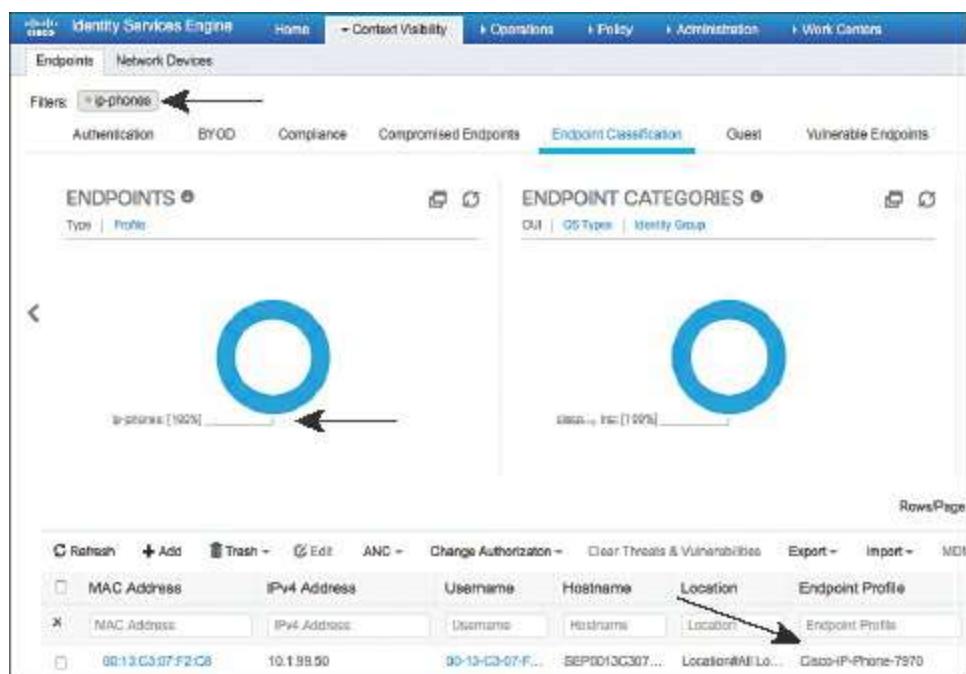
**Step 1.** Navigate to **Context Visibility > Endpoints**.

**Step 2.** Click **Endpoint Classification**, as shown in [Figure 10-45](#).



**Figure 10-45** Endpoint Classification

**Step 3.** In the Endpoints dashlet in the upper left, click **ip-phones**. This begins to filter the list, as pointed out in [Figure 10-46](#).



**Figure 10-46** Endpoint Classification, Filtered for ip-phones

**Step 4.** Click the MAC Address, **00:13:C3:07:F2:C8**, to display the endpoint details, shown in [Figure 10-47](#).

Endpoints > 00:13:C3:07:F2:C8

00:13:C3:07:F2:C8   

MAC Address: 00:13:C3:07:F2:C8  
Username: 00-13-C3-07-F2-C8  
Endpoint Profile: Cisco-IP-Phone-7970  
Current IP Address: 10.1.99.50  
Location:

Attributes    Authentication    Threats    Vulnerabilities

**General Attributes**

Description	
Static Assignment	false
Endpoint Policy	Cisco-IP-Phone-7970
Static Group Assignment	false
Identity Group Assignment	Cisco-IP-Phone

**Custom Attributes**

 Filter 

Attribute Name	Attribute Value
x Attribute Name	Attribute Value

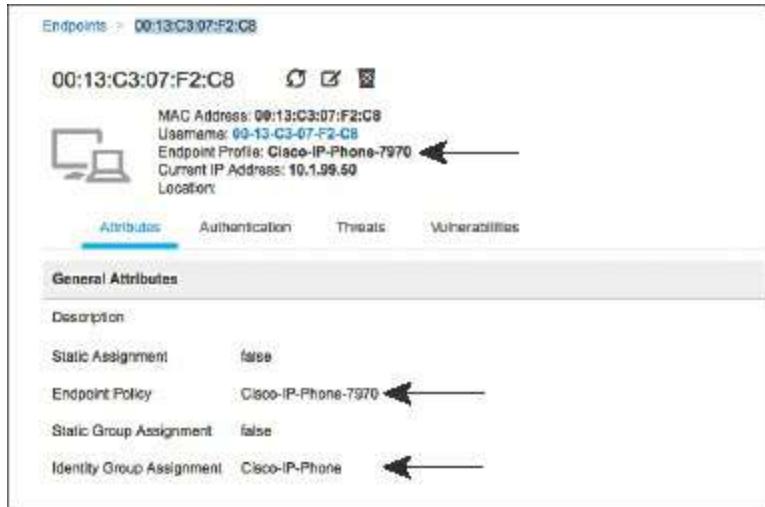
No data found. Add custom attributes here.

**Other Attributes**

22-tcp	ssh
443-tcp	https
80-tcp	http
AAA-Server	atw-ise247
AllowedProtocolMatchedRule	Dot1X

**Figure 10-47** Endpoint Details: 00:13:C3:07:F2:C8

**Step 5.** Notice that the Endpoint Policy (the profile of the device) is Cisco-IPPhone-7970 and the Identity Group Assignment is Cisco-IP-Phone, as you can see in [Figure 10-48](#).



**Figure 10-48** Endpoint Policy and Identity Group Assignment

**Step 6.** Scroll down the endpoint details to see much more information. The database stores copious details about an endpoint to aid you in identification, classification, asset management, and visibility. Additionally, under the Other Attributes section, shown in [Figure 10-49](#), you see that AuthorizationPolicyMatchedRule is Profiled Cisco IP Phones, which means the correct authorization rule is being matched.

Other Attributes	
22-tcp	ssh
443-tcp	https
80-tcp	http
AAA-Server	btw-l86247
AllowedProtocolMatchedRule	Dot1X
AuthenticationIdentityStore	Internal Endpoints
AuthenticationMethod	Lookup
AuthorizationPolicyMatchedRule	Profiled Cisco IP Phones
BYODRegistration	Unknown
Called-Station-ID	1C-DF-0F-31-B0-01
Calling-Station-ID	00-13-C3-07-F2-C8
DestinationIPAddress	10.1.100.247

**Figure 10-49** Endpoint Details: AuthorizationPolicyMatchedRule

**Step 7.** Scroll further down in the endpoint details to see that the EndPointSource is the RADIUS probe, as shown in [Figure 10-50](#). That means the RADIUS probe provided the most information needed to classify this device (which must have arrived from Device Sensor on the NAD).

DeviceRegistrationStatus	NotRegistered
ElapsedDays	1
EndPointMACAddress	00-13-C3-07-F2-C8
EndPointIPPolicy	Cisco-IP-Phone-7970
EndPointProfilerServer	80w-ibc247.securitydemo.net
EndPointSource	RADIUS Probe
FailureReason	12514 EAP-TLS failed SSL/TLS handshake because of an unknown CA in the client certificates chain
IdentityGroup	Cisco-IP-Phone
InactiveDays	0
IsThirdPartyDeviceFlow	false
LastNmapScanTime	2016-Jun-01 20:48:31 UTC
Location	Location#All Locations#North America#SJC
MACAddress	00:13:C3:07:F2:C8
MatchedPolicy	Cisco-IP-Phone-7970
MessageCode	3001

**Figure 10-50** Endpoint Details: EndPointSource

**Step 8.** Continue scrolling down the list of attributes and notice the CDP cached data from the switch that was sent to ISE via the RADIUS probe, as shown in [Figure 10-51](#).

Total Certainty Factor	205
UseCase	Host Lookup
User-Name	00-13-C3-07-F2-C8
UserType	Host
allowEasyWiredSession	false
cdpCacheCapabilities	H,P,M
cdpCacheDeviceId	SEP0013C307F2C8
cdpCachePlatform	Cisco IP Phone 7970
cdpCacheVersion	SCQP70.9-1-1SR1S
dhcp-class-identifier	Cisco Systems, Inc. IP Phone CP-7970G
dhcp-client-identifier	01:00:13:c3:07:f2:c8
dhcp-parameter-request-list	1, 66, 6, 3, 15, 160, 35
dhcp-requested-address	10.1.99.50
host-name	SEP0013C307F2C8
ip	10.1.99.50
operating-system	Cisco IP Phone 7941, 7961, 7965G, or 7975
operating-system-result	Cisco IP Phone 7941, 7961, 7965G, or 7975

**Figure 10-51** Endpoint Details: CDP Data

You can see these attributes of the endpoint, but how is that used within the profiling policy? To answer that question, examine the profiling policy hierarchy for the endpoint.

**Step 9.** Navigate to either **Work Centers > Profiler > Profiling Policies > Cisco-Device** or **Policy > Profiling > Cisco-Device**. Cisco-Device is the top level of the profiling hierarchy for this endpoint. Clicking that will open the Cisco-

Device profile, as displayed in [Figure 10-52](#).

The screenshot shows the 'Profiler Policy List > Cisco-Device' configuration page. The policy is named 'Cisco-Device' with a description 'Generic policy for all Cisco devices'. It is enabled and has a minimum certainty factor of 10. The exception action is set to 'NONE'. The network scan (NMAP) action is 'OS-scan'. There is an option to 'Create an Identity Group for the policy' with two choices: 'Yes, create matching identity group' (radio button) and 'No, use existing Identity Group hierarchy' (radio button selected). The parent policy is listed as 'NONE'. The associated CoA type is 'Global Settings' and the system type is 'Cisco Provided'. The 'Rules' section contains eight entries, each defining an if-condition followed by a then-action (Certainty Factor Increases by 10). The conditions include 'Cisco-DeviceRule3Check1', 'VeriLinkOUICheck', 'Rule for Cisco DHCP Class Identifier', 'Cisco-DeviceRule4Check1', 'Rule for Cisco Device - BNMP', 'Rule for Cisco CDP Cache Platform', 'Cisco-DeviceRule1Check1', and 'LinksysOUICheck'. At the bottom are 'Save' and 'Reset' buttons.

**Figure 10-52** Cisco-Device Profiling Policy

Using [Figure 10-52](#) as a reference point, note the following details:

The Minimum Certainty Factor of this profile is 10. Certainty factor is an aggregate value between 1 and 65535. Each of the conditions at the bottom of the policy that are matched will add up to equal the endpoint's certainty value. The higher the value, the more certain the ISE Profiler is that an endpoint matches the specific profile.

- The OUI is Cisco Systems, Inc, as shown in [Figure 10-53](#), and that matches the condition for Cisco-Device, as shown in [Figure 10-54](#). This is one possible mapping that meets the minimum certainty value and should match the endpoint to this parent policy.

Network Device Profile	Cisco
NetworkDeviceGroups	Device Type>All Device Type<Switches<Access-Layer<Cisco, Location>All Locations<North America<SJC, Stage<Stage
NetworkDeviceName	3750-X
NetworkDeviceProfileId	a99d7d4a-156e-492b-a573-70aeb365be8d
NetworkDeviceProfileName	Cisco
NmapScanCount	1
OUI	Cisco Systems, Inc. ←
OpenSSLErrorMessage	SSL alert: code=0x230=560 'source=local'; type=fatal'; message="Unknown CA - error unable to get issuer certificate locally"
OpenSSLErrorStack	140440179803200:error:140890B2:SSL routines:SSL3_GET_CLIENT_CERTIFICATE:no certificate returned:s3_srvr.c:3370:
OriginalUserName	0013c30712e8

**Figure 10-53 OUI of the Endpoint**

Rules

If Condition	Cisco-DeviceRule3Check1	Then	Certainty Factor Increases	10
If Condition	VertlinkOUICheck	Then	Certainty Factor Increases	10
If Condition	Rule for Cisco DHCP Class Identifier	Then	Certainty Factor Increases	10
If Condition	Cisco-DeviceRule4Check1	Then	Certainty Factor Increases	5
If Condition	Rule for Cisco Device - SNMP	Then	Certainty Factor Increases	10
If Condition	Rule for Cisco CDP Cache Plat	Then	Certainty Factor Increases	10
If Condition	Cisco-DeviceRule1Check1	Then	Certainty Factor Increases	10
If Condition	LinksysOUICheck	Then	Certainty Factor Increases	10

Conditions Details

- Name: Cisco-DeviceRule1Check1
- Description: Cisco-DeviceRule1Check1
- Expression: MAC:OUI CONTAINS CISCO ←

Save Reset

**Figure 10-54 OUI Condition in Cisco-Device Policy**

- There is a Network Scan (NMAP) Action set to OS-Scan. For this action to occur, there must be a condition in the profile that has a result to trigger the network scan. [Figure 10-55](#) displays this mapping of the condition to the action.

Profiler Policy List > Cisco-Device

**Profiler Policy**

* Name:	Cisco-Device	Description:	Generic policy for all Cisco devices
Policy Enabled: <input checked="" type="checkbox"/>			
* Minimum Certainty Factor:	10	(Valid Range 1 to 65535)	
* Exception Action:	NONE		
* Network Scan (NMAP) Action:	OS-scan		
Create an Identity Group for the policy:			
<input type="radio"/> Yes, create matching Identity Group <input checked="" type="radio"/> No, use existing Identity Group hierarchy			
Parent Policy: ***NONE***			
* Associated CoA Type:	Global Settings		
System Type: Cisco Provided			
<b>Rules</b>			
If Condition:	LinksysOUICheck	Then:	Certainty Factor Increases by 10
If Condition:	Cisco-Meraki-Device-Rule1Check1	Then:	Certainty Factor Increases by 10
If Condition:	PolycomOUICheck	Then:	Certainty Factor Increases by 5
If Condition:	Cisco-DeviceRule1-SCAN	Then:	Take Network Scan Action
If Condition:	TivellaOUICheck	Then:	Certainty Factor Increases by 10
If Condition:	Rule for Cisco Device - LLDP	Then:	Certainty Factor Increases by 10
If Condition:	Cisco-Device-Rule5-Check1	Then:	Certainty Factor Increases by 10
If Condition:	Rule for Cisco TelePresence	Then:	Certainty Factor Increases by 10

**Figure 10-55** Network Scan Action and Condition with Scan Result

- This profiling policy has a tremendous number of conditions, most of which add a certainty value of 5 or 10. The certainty value only needs to be a minimum of 10 to match the profile, so matching any one of these conditions will most likely equal a match.

**Step 10.** Continuing down the tree of the profiling policy, navigate to **Work Centers > Profiler > Profiling Policies > Cisco Device > Cisco-IP-Phone**, as shown in [Figure 10-56](#), to examine the conditions that are used for this policy.

Profiler Policy List > Cisco-IP-Phone

### Profiler Policy

* Name	Cisco-IP-Phone	Description	Policy for all Cisco IP Phones
Policy Enabled	<input checked="" type="checkbox"/>		
* Minimum Certainty Factor	20	(Valid Range 1 to 65535)	
* Exception Action	NONE		
* Network Scan (NMAP) Action	NONE		
Create an Identity Group for the policy	<input checked="" type="radio"/> Yes, create matching Identity Group <input type="radio"/> No, use existing Identity Group hierarchy		
Parent Policy	Cisco-Device		
* Associated CoA Type	Global Settings		
System Type	Cisco Provided		
<b>Rules</b>			
If Condition	CiscoIPPhoneDHCPClassIdentifierCheck	+	Then Certainty Factor Increases 20
If Condition	CiscoIPPhoneCDPDeviceIdCheck	+	Then Certainty Factor Increases 5
If Condition	CiscoIPPhoneDHCPClassIdentifierCheck2	+	Then Certainty Factor Increases 20
If Condition	Cisco-IP-Phone-Rule2Check1	+	Then Certainty Factor Increases 20
If Condition	CiscoIPPhoneCdpCachePlatformCheck	+	Then Certainty Factor Increases 20
If Condition	CiscoIPPhoneCapabilitiesCheck	+	Then Certainty Factor Increases 20
If Condition	Cisco-IP-PhoneRule3Check1	+	Then Certainty Factor Increases 20
If Condition	Cisco-IP-Phone-Rule8-Check1	+	Then Certainty Factor Increases 20
<input type="button" value="Save"/> <input type="button" value="Reset"/>			

**Figure 10-56 Cisco-IP-Phone Profiling Policy**

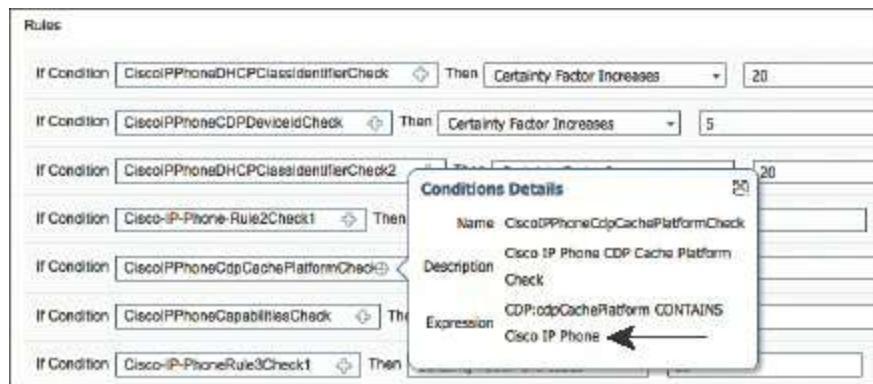
Using this profile as a reference point, note the following details:

To be compared to this profiling policy, the device must first match its parent policy. In this case, the device has to match the Cisco-Device policy before these conditions will ever be examined.

- The Minimum Certainty Factor of this profile is 20, as shown in [Figure 10-56](#). Certainty factor is an aggregate value between 1 and 65535. Each of the conditions at the bottom of the policy may add more certainty to this profile, if

they are matched.

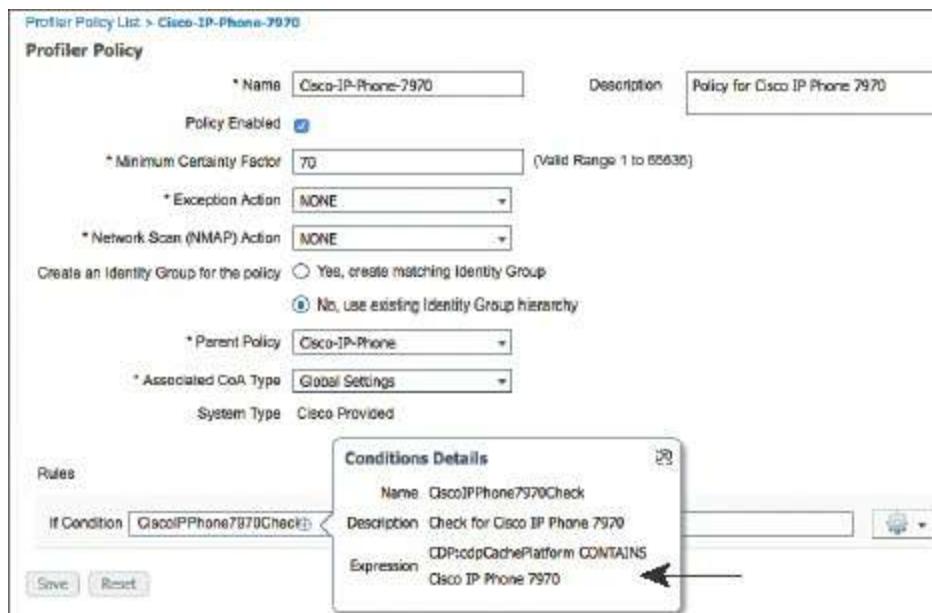
- The CDP Cache, shown in [Figure 10-51](#), shows that the cdpCachePlatform attribute was sent as Cisco IP Phone 7970.
- [Figure 10-57](#) shows the Cisco-IP-Phone profile policy uses a condition looking for the cdpCachePlatform value to contain Cisco IP Phone and increase the certainty by 20.



**Figure 10-57** cdpCachePlatform Condition

This step examined Cisco-IP-Phone, but what does it take to get one step further—to reach the final Cisco-IP-Phone-7970 profile?

**Step 11.** Navigate to **Work Centers > Profiler > Profiling Policies > Cisco Device > Cisco-IP-Phone > Cisco-IP-Phone-7970** to examine conditions used in this policy, as shown [Figure 10-58](#).



**Figure 10-58** Cisco-IP-Phone-7970 Profile

Using [Figure 10-58](#) as a reference, note the following details:

To be compared to this profiling policy, the device must first match its parent policy. In this case, the device has to match the Cisco-Device and Cisco-IP-Phone policy before these conditions will ever be looked at.

- The profile itself has only one condition: the cdpCachePlatform attribute is Cisco IP Phone 7970, which [Figure 10-51](#) has confirmed.

Rarely would you build an authorization policy that is specific to the point of the model number of the Cisco IP Phone; instead, you would just use the Cisco-IP-Phone parent policy in your authorization policies.

## Logical Profiles

After ISE 1.0 was first released, many customers quickly requested the capability to group profiles that are not hierarchical—for example, to create a profile group named IP-Phones that contains all the individual profiles of IP phones, Cisco and non-Cisco alike. Cisco answered that request in ISE 1.2 by introducing the concept of logical profiles, which are groupings of profiles. ISE version 2.1 adds more logical profiles, such as Cameras, Gaming Devices, Home Network Devices, Medical Devices, and more.

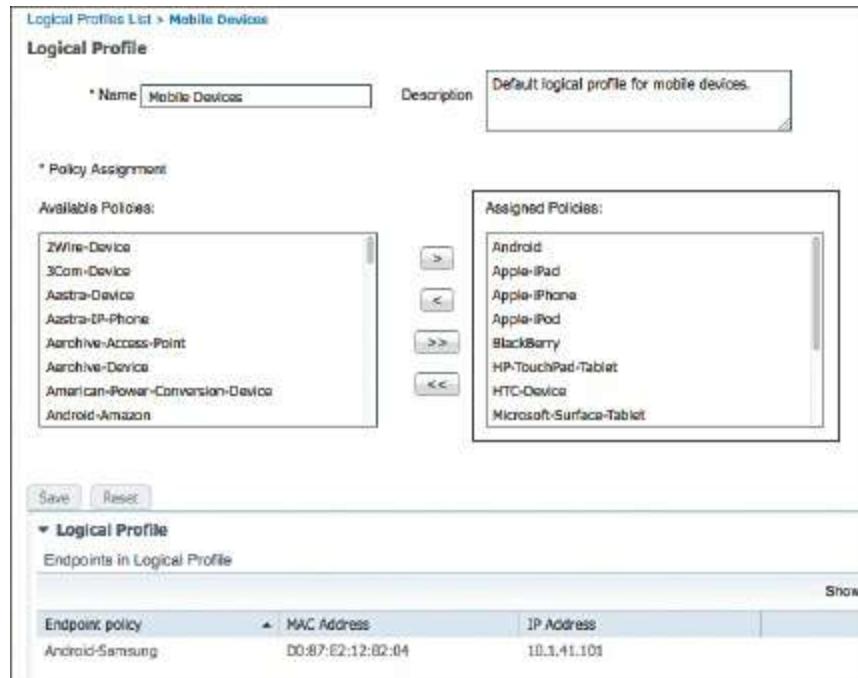
To examine the logical profiles in ISE, navigate to **Work Centers > Profiler > Profiling Policies > Logical Profiles**, as shown in [Figure 10-59](#).

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes links for Home, Context Visibility, Operations, Policy, Administration, and Work Centers. Under Work Centers, the Profiler section is selected. The main content area displays the 'Logical Profiles' page. On the left, there is a sidebar titled 'Profiling' with a search bar and a tree view showing categories: Profiling Policies and Logical Profiles. Under Logical Profiles, several sub-categories are listed: Cameras, Gaming Devices, Home Network Devices, IP-Phones, Infrastructure Network De, Medical Devices, Mobile Devices, and Printers. The main panel is titled 'Logical Profiles' and contains a table with the following data:

Logical Profiles	System Type	Description
Cameras	Cisco Provided	Default logical profile for cameras.
Gaming Devices	Cisco Provided	Default logical profile for gaming devices.
Home Network Devices	Cisco Provided	Default logical profile for home network devices.
IP-Phones	Cisco Provided	Default logical profile for IP Phones.
Infrastructure Network De	Cisco Provided	Default logical profile for infrastructure network devices.
Medical Devices	Cisco Provided	Default logical profile for medical devices.
Mobile Devices	Cisco Provided	Default logical profile for mobile devices.
Printers	Cisco Provided	Default logical profile for printers.

**Figure 10-59** Logical Profiles

[Figure 10-60](#) shows the contents of the Mobile Devices logical profile. Notice that the logical profile contains Android, Apple-iPad, and other mobile endpoint profiles.



**Figure 10-60** Mobile Devices Logical Profile

Logical profiles are not limited to only those defined by Cisco. You can also create your own.

## ISE Profiler and CoA

When using an endpoint profile as an attribute within your authorization policy, you will be providing differentiated results for specific profiles. However, there is often a “chicken and the egg” phenomenon happening simultaneously. You cannot provide the right access to a device without knowing what that device is, yet you cannot find out what the device is without providing some level of access so the endpoint will be active on the network and ISE can identify the endpoint profile.

Enter the concept of change of authorization (CoA). Without CoA, the only time a policy server such as ISE is permitted to send a command to the NAD is during a response to an authentication request. This created numerous issues because there would not be a way to disconnect a bad actor from the network or change the level of access an endpoint is permitted to have based on a newer data element that has been learned by the profiling engine. The current authorization to the network would have to sustain until the next time the endpoint has to authenticate.

Because the authorization policy can be configured to send different results for an endpoint before it is profiled, and then send another level of authorization after the endpoint profile becomes more solidified, and the final result after the endpoint profile is definitely known, you cannot wait for the next authentication request each time. Instead, the profiling engine can use CoA to change the level for each state the endpoint goes through. Stated a bit more succinctly, because ISE learns more about endpoints at

random time intervals, ISE can send a CoA to the network access device to have a different level of access applied to the session.

There are two main areas for configuring CoA with profiling. A global setting enables CoA for profiling in the ISE deployment, and a CoA can be configured on a per-profile basis.

## Global CoA

To enable CoA for profiling in the ISE cube, and to configure the CoA type used by profiling globally, navigate to either **Administration > System > Settings > Profiler** or **Work Centers > Profiler > Settings** (as shown in [Figure 10-61](#)).

The screenshot shows the 'Profiler Configuration' page in the Cisco ISE interface. The 'CoA Type' dropdown menu is open, showing the following options:

- No CoA (selected)
- No CoA
- Port Bounce
- Reauth

**Figure 10-61** Profiler Global Settings

As shown in [Figure 10-61](#), the default setting is No CoA. Click the drop-down list, as shown in [Figure 10-62](#), to see the other choices: Port Bounce and Reauth.

The screenshot shows the 'Profiler Configuration' page with the 'CoA Type' dropdown expanded. The list includes:

- No CoA (selected)
- No CoA
- Port Bounce
- Reauth

**Figure 10-62** Profiler CoA Types

The Port Bounce CoA performs a **shutdown** on the switch port and then perform a **no shutdown** to reenable it. This causes the link state to change, simulating the unplugging and plugging in of network cable. The benefit to this type of CoA is that many devices will try to renew their DHCP assigned IP addresses when the link state changes.

Additionally, there is a built-in failsafe to never send a Port Bounce when more than one MAC address is seen on the switch port. That failsafe is in place to ensure there is no negative impact on IP telephony. When more than one MAC address exists on the switch port, a Reauth will be sent instead.

The Reauth CoA instructs the NAD to initiate a new authentication to the endpoint, sending another EAPoL Start message to trigger the supplicant to send the credentials again, or (in the case of MAB) the NAD will resend a RADIUS authentication with the endpoint MAC address as the identity credential. Either way, there is a new authentication, but that authentication maintains the same authentication session ID. By maintaining the session ID, ISE is able to tie together the multiple states of the endpoint.

Regardless of the CoA type used, ISE has now forced a new authentication attempt so that a different authorization result can be sent to the NAD, providing the correct level of network access with the latest profiling information being used. However, setting a global CoA type to Port Bounce is not recommended. The safer bet is to use the Reauth option.

After the profiler CoA is enabled globally, a CoA is automatically sent for any endpoint that transitions from unknown to any known profile.

## Per-Profile CoA

ISE 1.2 added a setting to profiles that enables an administrator to control her own destiny with CoA. This came about with the need to send a Port Bounce CoA for certain devices only, while using the global Reauth CoA for the remaining endpoints. This is known as the per-profile CoA. When a CoA type is configured for a profile, it is used when an endpoint is classified as that profile type. [Figure 10-63](#) shows this setting.

The screenshot shows the 'Profiler Policy List' interface with a single policy entry for 'Xerox-Device'. The policy details are as follows:

- Name:** Xerox-Device
- Description:** Generic Policy for all Xerox Devices
- Policy Enabled:**
- Minimum Certainty Factor:** 10 (Valid Range 1 to 65535)
- Exception Action:** NONE
- Network Scan (NMAP) Action:** SNMPPortsAndOS-scan
- Create an Identity Group for the policy:**  Yes, create matching Identity Group  
  No, use existing Identity Group hierarchy
- Parent Policy:** \*\*\*NONE\*\*\*
- Associated CoA Type:** Port Bounce
- System Type:** Cisco Provided

At the bottom, there is a 'Rules' section with a configuration for an 'If Condition': If Condition Xerox-Device-SNMP Then Certainty Factor Increases LD.

**Figure 10-63** Per-Profile CoA

As shown in [Figure 10-63](#), a device that is profiled as a Xerox-Device now triggers a

Port Bounce CoA, causing the link to go down and back up again, which in turn triggers the endpoint to request a new IP address from the DHCP server. This is very useful when a device is using MAB and needs to be assigned to a different VLAN.

## Global Profiler Settings

Additional settings related to profiling are set at the global (system-wide) level, not just the global CoA type. These include the SNMP community strings for NMAP SNMP walks and the enable setting for endpoint attribute filtering.

### Configure SNMP Settings for Probes

The SNMPQUERY probe uses the SNMP community strings that are defined as part of the NAD entry under **Administration > Network Resources > Network Devices**. Theoretically, each NAD could have a different community string.

As described in the “Network Scan (NMAP)” section, NMAP uses SNMP to examine endpoints. For this to function, the ISE Profiler must know what SNMP community strings to use. The community strings to use are configured within **Work Centers > Profiler > Settings** by listing each community string one-by-one with a comma separating each value. After they are saved, the two text boxes are erased, and you must click the **Show** button to see the configured strings, as shown in [Figure 10-64](#).



**Figure 10-64** Global SNMP Settings for NMAP Probe

### Endpoint Attribute Filtering

Profiler can and does collect a lot of data about endpoints. It stores all that data and replicates it to the other ISE nodes in the deployment. To help keep the replication traffic down, ISE has the EndPoint Attribute Filter, which you enable at **Work Centers > Profiler > Settings**, as shown in [Figure 10-65](#).

The screenshot shows the 'Profiler Configuration' page. At the top, there's a dropdown for 'CoA Type' set to 'Reauth'. Below it, fields for 'Current custom SNMP community strings' and 'Change custom SNMP community strings' are shown, along with a 'Show' button and a note about NMAP comma-separated fields. A 'Confirm changed custom SNMP community strings' field is also present. In the center, there's a section titled 'Notes for EndPoint Attribute Filter' with a note about enabling the filter to keep significant attributes and discard others. A checkbox labeled 'Enabled' is checked. At the bottom are 'Save' and 'Reset' buttons.

**Figure 10-65** Enabling EndPoint Attribute Filter

When the filtering is enabled, Profiler will build a whitelist of attributes that are used in the existing profiler policies. In other words, Profiler examines every policy that is enabled and creates a list of attributes that are needed for all those policies. Only those attributes will now be collected and stored in the endpoint database.

Use of the EndPoint Attribute Filter is highly recommended but only after a deployment has been up and running properly for an extended period of time. If you use it right away, you run the risk of not profiling all of your initial devices, because it is theoretically possible to ignore attributes that will be needed to uniquely identify the endpoint type.

## NMAP Scan Subnet Exclusions

Another global setting for the Profiler service is NMAP Scan Subnet Exclusions, shown in [Figure 10-66](#). Many organizations have special devices that do not like to be scanned, or that can be negatively impacted if you scan them, and therefore the organization prohibits it, such as medical devices or manufacturing equipment. This setting enables administrators to exclude those networks from being scanned by the NMAP engine.

The screenshot shows the 'Profiler Settings' section under 'NMAP Scan Subnet Exclusions'. It lists two IP address ranges with their subnet masks: '10.1.254.0 / 24' and '172.16.99.0 / 25'. There are 'Delete' and 'Add' buttons for managing exclusions. At the bottom are 'Reset' and 'Save' buttons.

**Figure 10-66** NMAP Scan Subnet Exclusions

## Profiles in Authorization Policies

As you saw with the profiled Cisco-IP-Phone authorization rule earlier in this chapter, the profile can be used as a condition of an authorization policy rule in the form of an Identity Group. Originally, ISE required an Identity Group in order to use any of the profiling policies in the rule; however, it has evolved into the ability to use the profile directly (called the EndPointPolicy).

## Endpoint Identity Groups

Local identities within the ISE database may be in the form of user identities or endpoint identities. Identity Groups may contain multiple identities, although an identity (user or endpoint) can be a member of only one Identity Group at a time.

To create an Identity Group based on the profile, select the **Yes, Create Matching Identity Group** option on the profile, as displayed in [Figure 10-67](#).

The screenshot shows the 'Profiler Policy List > Android' screen. A new policy is being created with the following details:

- Name:** Android
- Description:** Policy for [empty field]
- Policy Enabled:**
- Minimum Certainty Factor:** 30 (Valid Range 1 to 8835)
- Exception Action:** NONE
- Network Scan (NMAP) Action:** NONE
- Create an Identity Group for this policy:**
  - Yes, create matching Identity Group
  - No, use existing Identity Group hierarchy
- Parent Policy:** \*\*\*NONE\*\*\*
- Associated CoA Type:** Global Settings
- System Type:** Cisco Provided

**Figure 10-67** Create Matching Identity Group

If that option is selected, the matching Identity Group can be found under **Administration > Identity Management > Groups > Endpoint Identity Groups** (as shown in [Figure 10-68](#)).

Name	Description
<input type="checkbox"/> Android	Identity Group for Profile: Android
<input type="checkbox"/> Apple-iDevice	Identity Group for Profile: Apple-iDevice
<input type="checkbox"/> Axis-Device	Identity Group for Profile: Axis-Device
<input type="checkbox"/> BlackBerry	Identity Group for Profile: BlackBerry
<input type="checkbox"/> Blacklist	Blacklist Identity Group
<input type="checkbox"/> Cisco-IP-Phone	Identity Group for Profile: Cisco-IP-Phone
<input type="checkbox"/> Cisco-Meraki-Device	Identity Group for Profile: Cisco-Meraki-Device
<input type="checkbox"/> Epson-Device	Identity Group for Profile: Epson-Device
<input type="checkbox"/> GuestEndpoints	Guest Endpoints Identity Group
<input type="checkbox"/> Juniper-Device	Identity Group for Profile: Juniper-Device
<input type="checkbox"/> Profiled	Profiled Identity Group
<input type="checkbox"/> RegisteredDevices	Asset Registered Endpoints Identity Group
<input type="checkbox"/> Sony-Device	Identity Group for Profile: Sony-Device
<input type="checkbox"/> Synology-Device	Identity Group for Profile: Synology-Device
<input type="checkbox"/> Trendnet-Device	Identity Group for Profile: Trendnet-Device
<input type="checkbox"/> Unknown	Unknown Identity Group
<input type="checkbox"/> Vizio-Device	Identity Group for Profile: Vizio-Device
<input type="checkbox"/> Workstation	Identity Group for Profile: Workstation

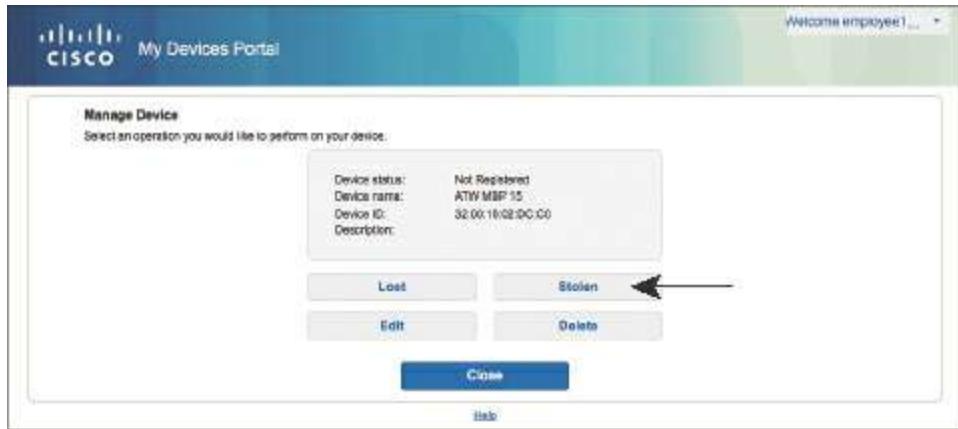
**Figure 10-68** Endpoint Identity Groups

In ISE 1.0, using endpoint Identity Groups was the only way to include profiles in authorization policies. The use of these Identity Groups for profiling has been deprecated in favor of using the actual endpoint profile or logical profiles directly in the authorization policy. It is a lot more flexible and less operationally expensive.

Therefore, starting with ISE 1.2, endpoint Identity Groups are used for a different purpose. They are used for more of a MAC address management (MAM) model, where you can create a static list of MAC addresses to be authorized specifically. For example, you could create a list of all Apple iPads that are owned by the company so they can be differentiated from personally owned iPads.

The Blacklist Identity Group is a perfect example of Identity Group usage in this manner. If a user's personal device is stolen, he can log in to the My Devices Portal and identify the device as Stolen, as shown in [Figure 10-69](#). This immediately adds the endpoint to the Blacklist group, as shown in [Figure 10-70](#). The device is now denied

network access by default, as shown in [Figure 10-71](#).



**Figure 10-69** Identifying an Endpoint as Stolen

A screenshot of the Cisco Identity Services Engine interface. The top navigation bar includes "Identity Services Engine", "Home", "Context Visibility", "Operations", "Policy", and "Administration". Under "Administration", "Identity Management" is selected, with "Groups" currently active. The left sidebar shows "Identity Groups" with categories: "Endpoint Identity Groups" (containing "Blacklist", "GuestEndpoints", "Profiled", "RegisteredDevices", and "Unknown"), and "User Identity Groups". The main panel shows "Endpoint Identity Group List &gt; Blacklist". It displays a group named "Blacklist" with a description "Blacklist Identity Group". There are "Save" and "Reset" buttons. Below is a table titled "Identity Group Endpoints" with columns "MAC Address", "Static Group Assignment", and "EndPoint Profile". One entry is listed: "32:00:16:02:DC:C0" with "true" under "Static Group Assignment" and "Unknown" under "EndPoint Profile".

**Figure 10-70** Blacklisted Devices

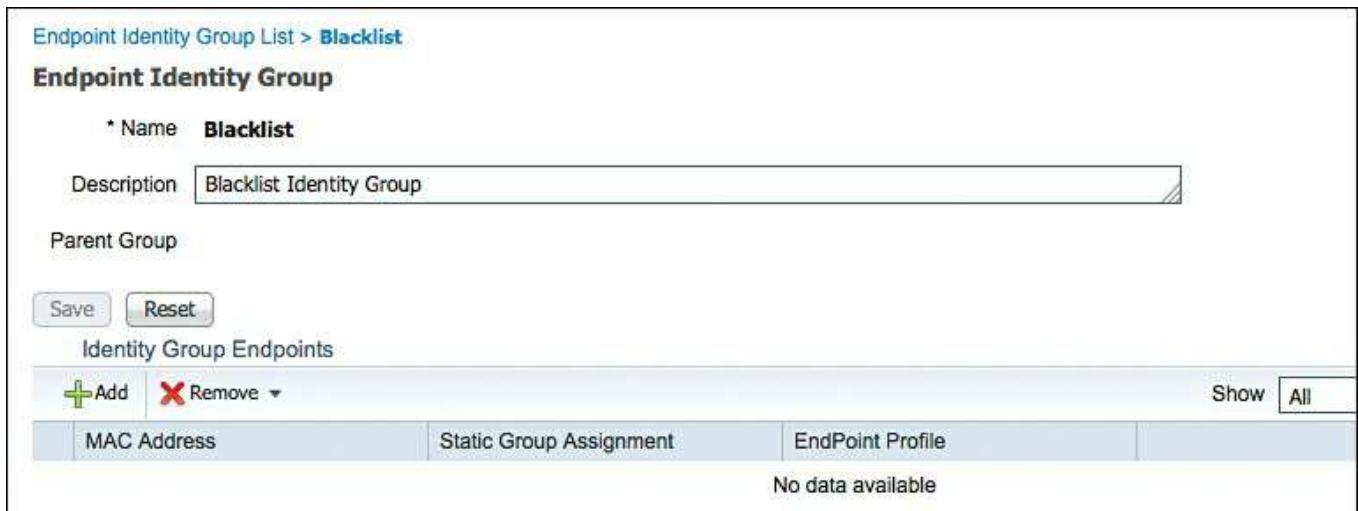
A screenshot of the Cisco Identity Services Engine interface, specifically the "Authorization Policy" section. The top navigation bar includes "Identity Services Engine", "Home", "Context Visibility", "Operations", "Policy", "Administration", and "Work Centers". The "Policy" tab is selected. The main content area is titled "Authorization Policy" and describes it as "Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order. For Policy Export go to Administration &gt; System &gt; Backup &amp; Restore &gt; Policy Export Page". It shows a dropdown "First Matched Rule Applies" set to "First". Below is a table titled "Exceptions (0)" with columns "Status", "Rule Name", "Conditions (Identity groups and other conditions)", and "Permissions". Three rules are listed: "Wireless Block List Default" (conditions: "Blacklist AND Wireless\_Access", permission: "Blockhole\_Wireless\_Access"), "Profiled Cisco IP Phones" (conditions: "Cisco\_IP\_Phone", permission: "Cisco\_IP\_Phones"), and "Profiled Non Cisco IP Phones" (conditions: "Non\_Cisco\_Profied\_Phones", permission: "Non\_Cisco\_IP\_Phones").

**Figure 10-71** Default Blacklist Authorization Rule

From the My Devices Portal, selecting Reinstate (see [Figure 10-72](#)) moves the device from the Blacklist group to the RegisteredDevices group. [Figure 10-73](#) shows the empty Blacklist group.



**Figure 10-72** Reinstating the Endpoint



Endpoint Identity Group List > Blacklist

**Endpoint Identity Group**

\* Name **Blacklist**

Description **Blacklist Identity Group**

Parent Group

Save Reset

Identity Group Endpoints

MAC Address	Static Group Assignment	EndPoint Profile
No data available		

**Figure 10-73** Empty Blacklist Endpoint Identity Group

## EndPointPolicy

Beginning with ISE 1.2, Identity Groups are no longer the way to apply policy based on the endpoint's profile. Policy is now built with the actual profile through the use of the Endpoints:EndPointPolicy attribute.

To see the use of the profile in a policy, you will duplicate the existing onboarding authorization rule and then modify that new rule to use the Android profile, which does not have a corresponding Identity Group.

From the ISE GUI, do the following:

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

**Step 2.** Duplicate the default Employee\_Onboarding rule.

**Step 3.** Name the rule **Employee\_Onboarding\_Android**.

**Step 4.** Add a new condition to the existing Wireless\_802.1X and MSCHAP conditions of **Endpoints > EndPointPolicy**.

**Step 5.** Choose **Android** from the list of endpoint policies.

[Figure 10-74](#) shows the resulting authorization rule.

Status	Rule Name	Conditions (Identify groups and other conditions)	Permissions
Active	Wireless Black List Default	Blocklist AND Wireless_Access	Blockhole_Wireless_Access
Active	Profiled Cisco IP Phones	Cisco-IP-Phone	Cisco_IP_Phones
Active	Profiled Non Cisco IP Phones	Non_Cisco_Profiled_Phones	Non_Cisco_IP_Phones
Active	Compliant_Device_Acces	Network_Access_Authentication_Passed AND Compliant_Devices	PermitAccess
Active	Employee_EAP-TLS	Wireless_802.1X AND BYOD_H_Registered AND EAP-TLS AND MAC_in_SAN	PermitAccess AND BYOD
Active	Employee_Onboarding_Android	Wireless_802.1X AND EAP-MSCHAPv2 AND EndPointEndPointPolicy EQUALS Android	NSP_Onboard AND BYOD
Active	Employee_Onboarding	Wireless_802.1X AND EAP-MSCHAPv2	NSP_Onboard AND BYOD
Active	Unknown Endpoint	Unknown AND Network_Access_Authentication_Passed	United Access AND CollectData
Active	Basic_Authenticated_Access	Network_Access_Authentication_Passed	PermitAccess
Active	Default	None	DenyAccess

**Figure 10-74** Authorization Rule Using EndPointPolicy Condition

Throughout all of this, always keep in mind the simplicity of using logical profiles to streamline your authorization policies, and limit the number of individual EndPointPolicies that you need to add to your authorization rules.

## Importing Profiles

As you have read, you can create profiles as the ISE administrator or have them downloaded via the profiler feed service. They can also be exported and imported with ISE. This is extremely useful for value-add from Cisco partners; or even the ability to import specific profiles for your individual business vertical.

For example, Craig Hyps, introduced earlier (Principal TME for ISE), has devised an entire medical industry package that contains over 250 medical device profiles. In this case, if you are an ISE administrator focused on the healthcare vertical, you could download this medical NAC package and import all 250+ profiles. Customers who are not in the medical industry would not need to waste any profiling CPU cycles looking for endpoints that are not relevant for their environment.

This approach to profile distribution is similar to that used to distribute signature packs with IDSs. Signature packs are a way to ensure the IDS keeps the important signature types in memory and does not install the unimportant ones. [Figure 10-75](#) shows the medical NAC profile package being selected for import in the GUI at **Work Centers > Profiler > Profiling Policies > Import**. The import could be a single profile or a combined package of many profiles. The profile or series of profiles will be in a single XML file.

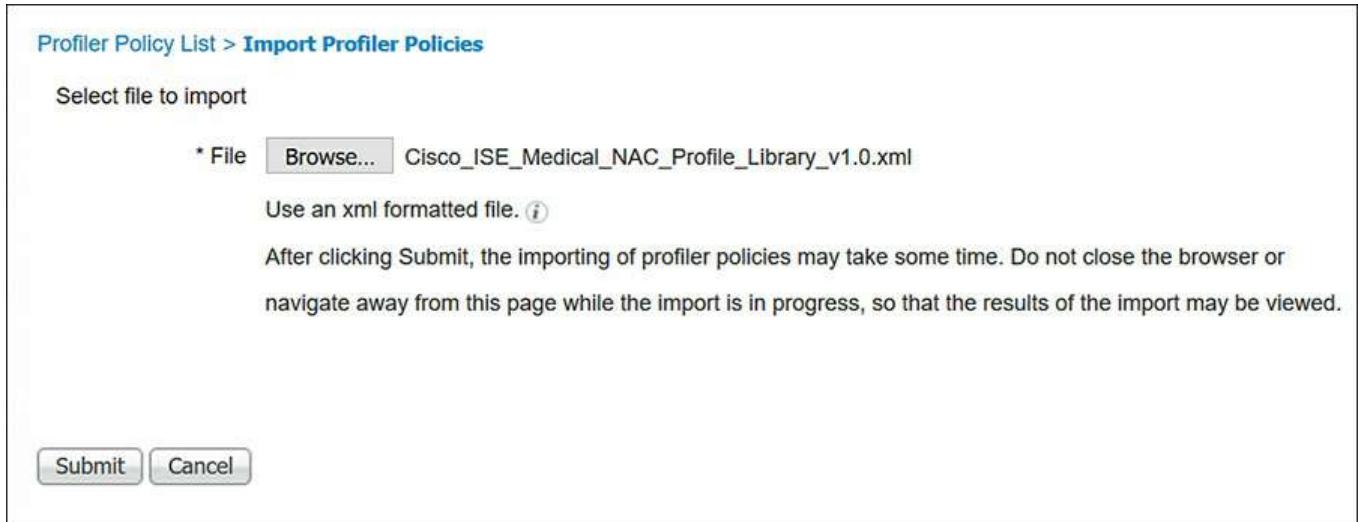
Profiler Policy List > Import Profiler Policies

Select file to import

\* File  Cisco\_ISE\_Medical\_NAC\_Profile\_Library\_v1.0.xml

Use an xml formatted file. [\(i\)](#)

After clicking Submit, the importing of profiler policies may take some time. Do not close the browser or navigate away from this page while the import is in progress, so that the results of the import may be viewed.



**Figure 10-75** Importing a Profile or Profile Package

After clicking Submit, the import begins and a status bar appears, as shown in [Figure 10-76](#). After the import is complete, all the imported profiles are now part of the profile policies and all endpoints in the database undergo a re-profiling process.

Profiler Policy List > Import Profiler Policies

Select file to import

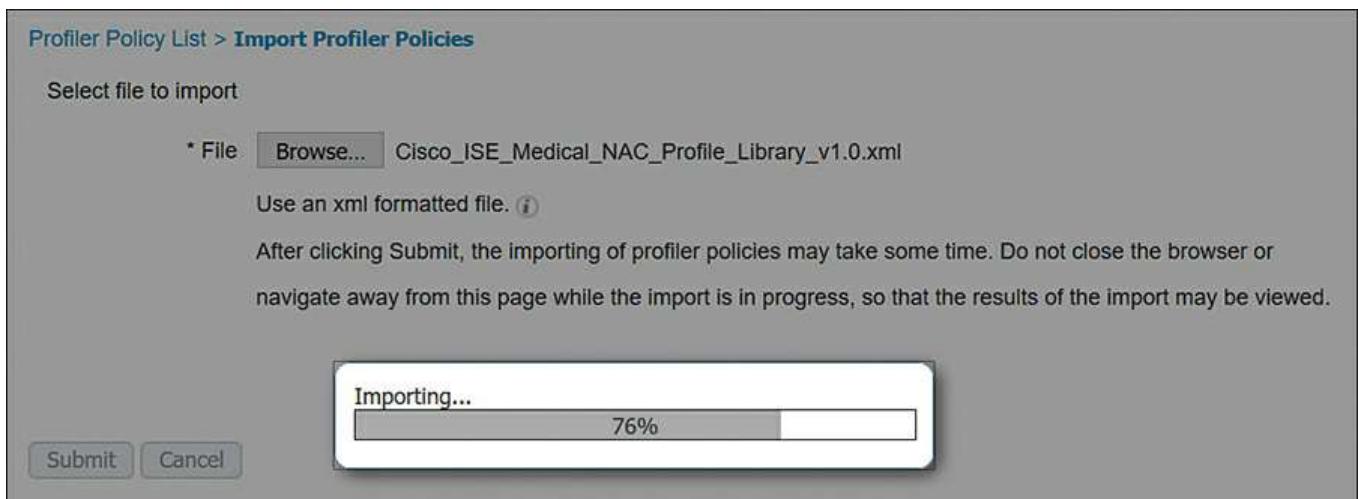
\* File  Cisco\_ISE\_Medical\_NAC\_Profile\_Library\_v1.0.xml

Use an xml formatted file. [\(i\)](#)

After clicking Submit, the importing of profiler policies may take some time. Do not close the browser or navigate away from this page while the import is in progress, so that the results of the import may be viewed.

Importing...

76%



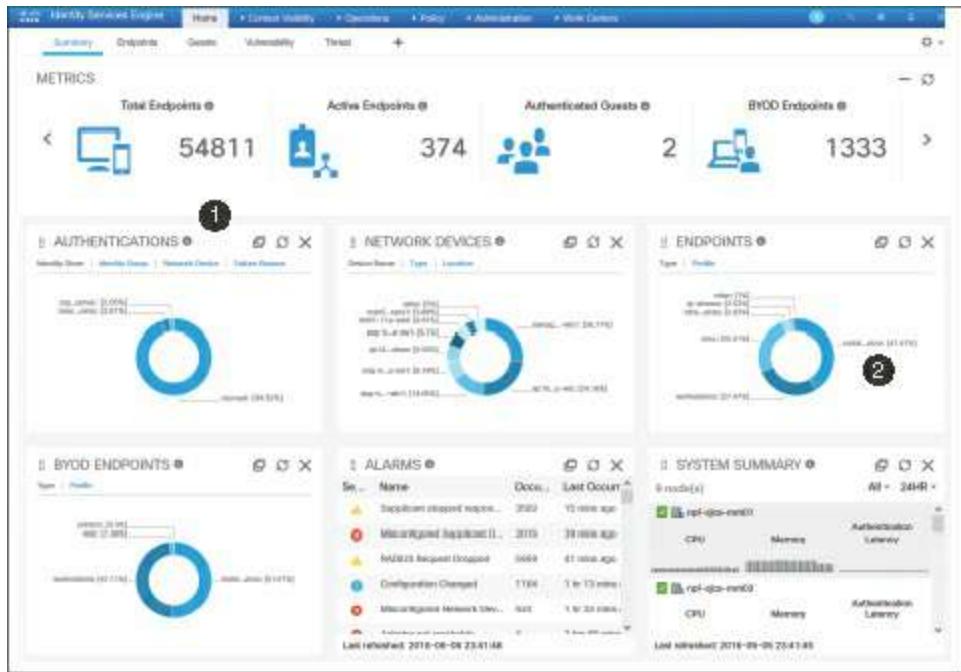
**Figure 10-76** Importing Status

## Verifying Profiling

There are a few key places to check to verify profiling operation: within the ISE GUI and by examining the network device itself.

## The Dashboard

The dashboard is always the first screen you see when you log in to the ISE GUI. The dashboard has two places to look to see if profiling is working, as shown in [Figure 10-77](#):

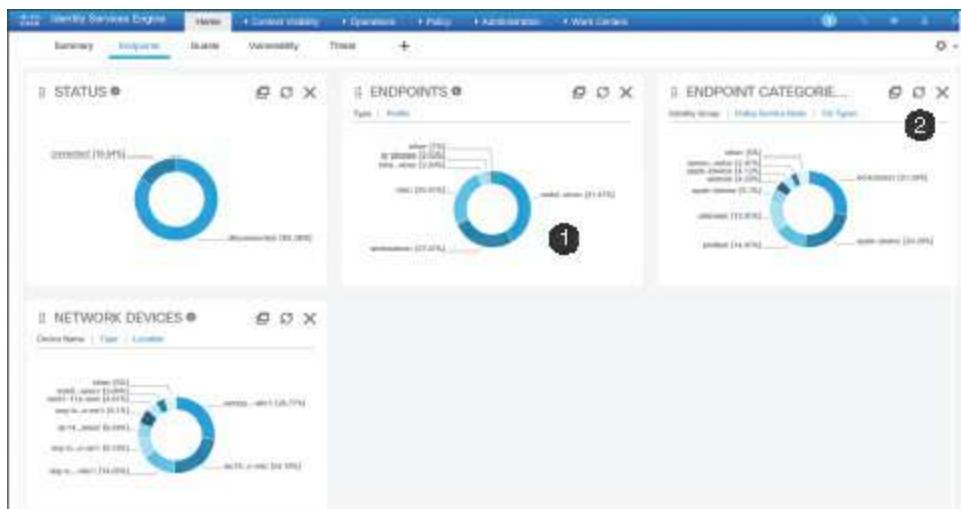


**Figure 10-77** Cisco ISE Dashboard

- 1. Total Endpoints counter:** Shows the number of endpoints that are currently in the endpoint database. Clicking it launches an endpoints-focused dashboard.
- 2. Endpoints widget:** Shows the breakdown of the known endpoints and their profiles.

## Endpoints Dashboard

From the ISE Home screen, several dashboards are available, such as Summary, Endpoints, and Guests. Selecting the Endpoints Dashboard displays a screen similar to what you see in [Figure 10-78](#). This dashboard is focused solely on displaying information about endpoints.



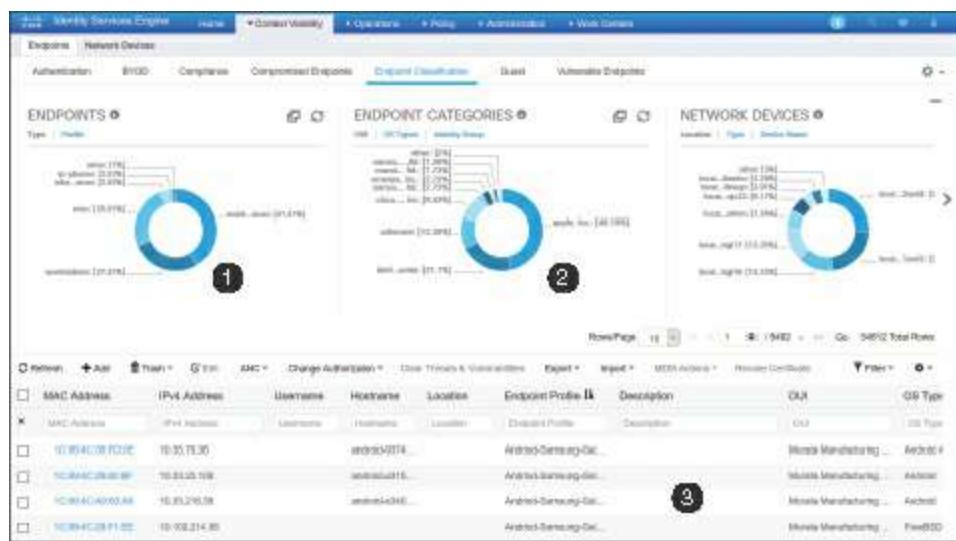
**Figure 10-78** Endpoints Dashboard

Examining [Figure 10-78](#), the following two areas of the dashboard are called out:

- 1. Endpoints widget:** Shows the breakdown of the known endpoints and their profiles.
- 2. Endpoint Categories widget:** Shows the categorization of the endpoints, sorted by Identity Group, or even by operating system. Clicking one of the categories launches another window into the Context Visibility tooling, prefILTERED on the category that you clicked.

## Context Visibility

Context Visibility is a fancy label for “asset inventory on steroids.” Beginning with ISE 2.1, it is the go-to method of examining the endpoints on the network and drilling into the data available in the system about those endpoints. Navigating to **Context Visibility > Endpoints > Endpoints Classification** is a great way to examine the profiling activity in your environment and what endpoints have been identified and classified. [Figure 10-79](#) shows the Endpoints Classification dashboard within Context Visibility.



**Figure 10-79** Context Visibility > Endpoints > Endpoint Classification

Examining [Figure 10-79](#), the following three areas of the dashboard are called out:

- 1. Endpoints widget:** Shows the breakdown of the known endpoints and their profiles.
- 2. Endpoint Categories widget:** Shows the categorization of the endpoints, sorted by Identity Group, or even by operating system. Clicking on one of the categories will filter the Endpoints list at the bottom.
- 3. Endpoints List:** A filterable and exportable list of endpoints and their context data that is available within the database.

## Device Sensor Show Commands

In addition to the ISE GUI, Cisco network devices can aid in verifying that profiling is happening correctly. With Cisco switches that run device-sensor, there is a **show** command specifically for the device-sensor capability in the switch: **show device-sensor cache [ all | mac ]**. [Example 10-4](#) shows the output of the **show** command. Although the values may not make a lot of sense to a human being, they show that the device-sensor is collecting and caching profiling data.

### Example 10-4 show device-sensor cache all Command Output

[Click here to view code image](#)

```
3750-X# show device-sensor cache all
Device: 0050.5687.0004 on port GigabitEthernet1/0/2
-----
Proto Type:Name          Len Value
dhcp   43:vendor-encapsulated-optio 5 2B 03 DC 01 00
dhcp   55:parameter-request-list    14 37 0C 01 0F 03 06 2C 2E 2F
1F 21 F9 2B FC
dhcp   60:class-identifier       10 3C 08 4D 53 46 54 20 35 2E
30
dhcp   12:host-name            12 0C 0A 58 59 5A 2D 42 69 6F
4D 65 64
dhcp   61:client-identifier     9 3D 07 01 00 50 56 87 00 04
dhcp   77:user-class-id        13 4D 0B 73 79 6D 75 6E 75 73
2D 62 69 6F
```

## Triggered NetFlow: A Woland-Santuka Pro Tip

Vivek Santuka, CCIE No. 17621, is a Consulting Systems Engineer at Cisco Systems who focuses on ISE for Cisco's largest customers around the world. Aaron Woland and Vivek devised the methodology discussed in this section, which they like to call "Triggered NetFlow."

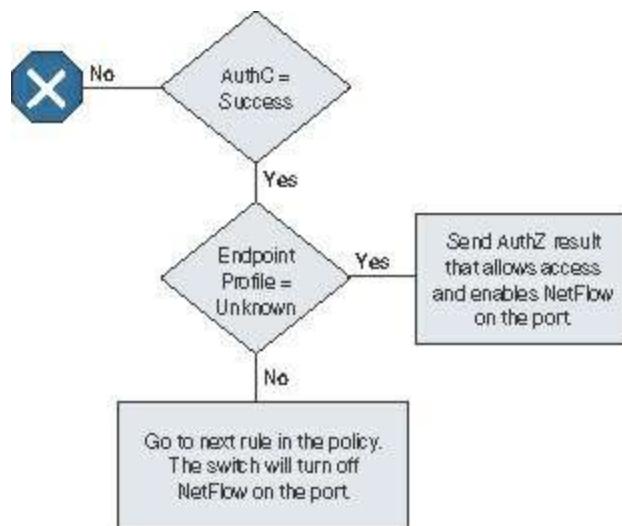
As you read in the "NetFlow Probe" section, the challenge with using NetFlow is that it requires de-duplication capabilities, scalable flow collection, and so forth. However, it is incredibly useful for identifying general-use compute platforms that are used in environment-specific ways, such as medical devices based on the Windows operating system. It's also very useful in identifying IoT devices that are otherwise unknown.

The best way to help identify these devices that are unique to an organization's environment is to examine the traffic patterns. For example, it's possible that a hospital's IV pump may only be uniquely identified by seeing the destination systems

that it communicates to within the hospital data center.

In those cases, NetFlow is the perfect identification tool because it will match on the traffic flow instead of endpoint attributes. However, that does not mean it's operationally feasible to enable NetFlow in the entire organization and risk overwhelming ISE with all those flows.

Triggered NetFlow is a deployment methodology designed to flip NetFlow on only when and where it is needed, and turn it back off immediately afterward. It is not a new technology, but a combination of existing technologies within ISE and the Cisco switching infrastructure. The overall concept follows the flow illustrated in [Figure 10-80](#). With any successful authentication where the endpoint profile is unknown, the authorization result will include a Security Group Tag (let's just call the SGT "CollectData"). When that SGT is received by the switch, an Embedded Event Manager (EEM) script is executed that enables NetFlow on that switch port.



**Figure 10-80** Logical Flow for Triggered NetFlow

The use of this solution requires that you have an understanding of how ISE authentications and authorizations work, how to use the EEM, and how to configure NetFlow within Cisco IOS. Knowledge of how TrustSec (aka Security Group Tags) functions is not required, but it can't hurt.

There are many different ways to accomplish this same task. The method outlined and tested by Aaron and Vivek is just one such example. If you have experience using the switch features and want to deviate from this specific prescribed solution, go right ahead! Please do, and perhaps post on the ISE forums (<http://cs.co/ise-community/>) so others may benefit from your tweaks. With that in mind, [Example 10-5](#) shows the EEM script that Aaron and Vivek used, while [Example 10-6](#) shows the example NetFlow configuration.

### Example 10-5 Sample EEM Script for Triggered NetFlow

[Click here to view code image](#)

```
event manager applet CaptureData
event syslog pattern "Authorization succeeded for client"
action 1.0 regexp "Interface (.*) AuditSessionID" "$_syslog_msg" match
intname
action 1.1 cli command "enable"
action 1.2 cli command "show auth sess int $intname | i SGT"
action 1.3 set sgttag "0000-0"
action 1.4 regexp "000C-0" "$sgttag"
action 1.5 regexp "SGT:  (.*)" "$_cli_result" match sgttag
action 1.6 regexp "000C-0" "$sgttag"
action 1.7 if $_regexp_result eq "1"
action 1.8  cli command "conf t"
action 1.9  cli command "int $intname"
action 2.0  cli command "ip flow ingress"
action 2.1 else
action 2.2  cli command "conf t"
action 2.3  cli command "int $intname"
action 2.4  cli command "no ip flow ingress"
action 2.5 end
```

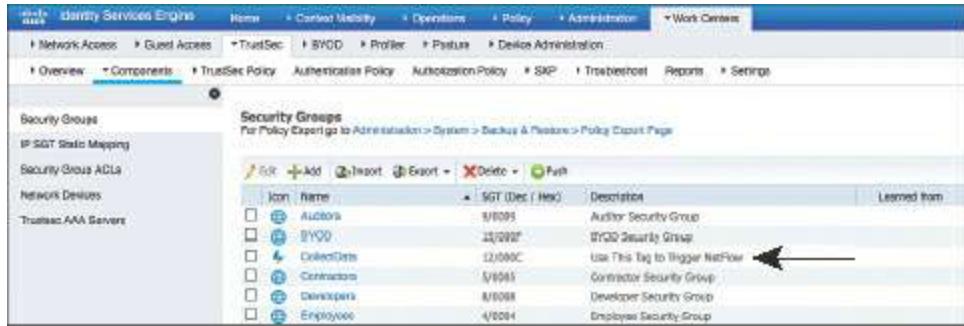
## Example 10-6 Sample NetFlow Configuration

[Click here to view code image](#)

```
flow record ise-flows
description export only flows needed by ise
match datalink mac source-address
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match transport tcp flags
!
flow exporter ISE
description Export to ISE PSN1
destination 10.1.100.234
source TenGigabitEthernet1/1/1
transport udp 9996
!
flow exporter ISE-flows
!
flow monitor ISE-Flows
description Used for ISE Profiler
record ise-flows
exporter ISE

cache timeout active 60
!
flow monitor CaptureData
record ise-flows
!
flow monitor test
```

[Figure 10-81](#) shows the SGT that was created to trigger the NetFlow application on the port.



**Figure 10-81** CollectData Security Group Tag

[Figure 10-82](#) shows the authorization rule for the unknown endpoints, which permits a limited network access and includes the CollectData SGT.

Unknown Endpoint	If    Unknown AND Network_Access_Authentication_Passed	then    Limited Access AND CollectData
------------------	--	--

**Figure 10-82** Unknown Endpoint Authorization Rule

We hope you found this pro tip useful, even if it was just to help you consider how to leverage existing technologies to enable a better ISE deployment for your specific needs for your organization.

## Summary

This chapter introduced the importance of device profiling for any network environment where identity is being enforced. It also introduced the new Context Visibility tooling within ISE 2.1, the probe deployment options, logical profiles, importing profiles, and feed service usage.

There are many probes that Cisco ISE can use, and the value of each probe is specific to your environment and needs. There is a direct correlation between the difficulty in deploying a probe and its inherent value to your Secure Access deployment, so ensure that you are using what is best for your organization.

# Chapter 11 Bootstrapping Network Access Devices

This chapter covers the following topics:

- Cisco Catalyst Switches
- Cisco Wireless LAN Controllers

I don't know about you, but when I go to put on my boots, I have to grab the bootstraps to pull the boots onto my feet. I can't wear them, or even begin to lace them up, without first pulling them on. So, "bootstrapping" is a critical step for me to be successful in wearing my chosen boots. This is where the metaphor "bootstrapping" came from. In the context of this chapter, it refers to configuring a device to work with Cisco ISE secure network access. Before end users attempt to connect their devices to the network and have them be authenticated, the network access device (NAD) must be configured to authenticate those devices.

Two NAD types are the focus of this chapter, Cisco Catalyst Switches and Cisco Wireless LAN Controllers (WLC). For both NAD types, the focus is on establishing a predictable, repeatable configuration that follows Cisco best practices for most situations.

## Cisco Catalyst Switches

Cisco started as a networking company, taking the lead in the world for multiprotocol routers and very shortly thereafter leading the world in network switching. Cisco now has the vast majority of the market share for switching infrastructure. Because of that long-standing market leadership position, some people might not expect Cisco to continue to innovate its switching technology. Of course, that's not Cisco's style. Even though Cisco has more ports configured for 802.1X in the world than any other vendor, it continues working to make the authentication experience even better and more feature-rich. With that continuous innovation of switching products comes a bit of confusion as to which versions support which new features. This section is intended to clear up any confusion you might have.

The following list classifies the switch capabilities into a few unofficial groupings intended to simplify the evolution of Cisco switches and facilitate their discussion in this chapter:

- **Classic IOS:** This grouping includes IOS 12.2(55)SE versions. Compared to non-Cisco switches, these switches are considered to be rock-solid workhorses, very stable and feature rich—but still missing some of the newer advances in network authentication, profiling, and TrustSec. These are still the most common switches encountered in the field during Secure Access deployments—they are tried and true and die-hard. Because they don't have the advanced profiling capabilities, such as

Device Sensor, they are configured for SNMP polling from ISE instead.

- **IOS 15.x:** This grouping includes the IOS 15.x flavors and their IOS-XE counterparts. These platforms add some incredible features and functions, such as the IOS Device Sensor described in detail in [Chapter 10, “Profiling Basics and Visibility.”](#) With the Device Sensor capabilities, the switch collects profiling attributes locally and sends them to ISE in a RADIUS accounting packet. With this capability, the switch should not be configured for SNMP polling; instead, it must be configured to collect the profiling attributes. Overall, the configuration style on these switches is the same as that for the classic IOS switches, but some differences exist due to the more advanced capabilities.
- **C3PL:** The newer 15.2.x and IOS-XE 3.6.x switches follow the Cisco Common Classification Policy Language (C3PL) style of configuration. This provides some intriguing and advanced authentication features, as well as a very different configuration style that has powerful options, but it can be confusing when learning how to use it. However, many administrators who start to use this configuration style end up loving it and rarely want to go back to the classic methods of configuration. At the time of writing, this is the least common type of deployment in the field, but it is gaining in popularity.

## Global Configuration Settings for Classic IOS and IOS 15.x Switches

This section covers the global configuration of all the non-C3PL switches participating in the Secure Access System. In other words, this section focuses on the configuration of both the classic IOS and IOS 15.x switches. C3PL switches are covered later in the chapter, in the section “Common Classification Policy Language (C3PL) Switches.”

### Configure Certificates on a Switch

Within the Cisco Secure Access system, the switch performs the URL redirection for web authentication and the redirection of the discovery traffic from the posture to the Policy Service Node.

Performing URL redirection at the Layer 2 access (edge) device is a vast improvement over previous NAC solutions that require an appliance to capture web traffic and perform redirection to a web authentication page. This simplifies the deployment for both web authentication and the posture agent discovery process. The switch needs to be configured to redirect nonencrypted HTTP traffic and encrypted HTTP traffic (HTTPS).

From global configuration mode on the switch, perform the following steps:

**Step 1.** Set the DNS domain name on the switch.

Cisco IOS does not allow for certificates, or even self-generated keys, to be created and installed without first defining a DNS domain name on the device.

Type **ip domain-name** domain-name at the global configuration prompt.

## **Step 2.** Generate keys to be used for HTTPS.

Type **crypto key generate rsa general-keys modulus 2048** at the global configuration prompt.

## **Enable the Switch HTTP/HTTPS Server**

The embedded HTTP/S server in Cisco IOS Software is used to grab HTTP traffic from the user and redirect that user's browser to the Centralized Web Authentication (CWA) portal, a device registration portal, or even to the Mobile Device Management (MDM) onboarding portal. This same function is used for redirecting the Posture Agent's traffic to the Policy Service Node.

To enable the HTTP server, follow these steps:

### **Step 1.** Enable the HTTP server in global configuration mode.

Type **ip http server** at the global configuration prompt.

### **Step 2.** Enable the HTTP Secure (HTTPS) server.

Type **ip http secure-server** at the global configuration prompt.

Many organizations want to ensure that this redirection process using the switch's internal HTTP server is decoupled from the management of the switch itself. If you are not using HTTP for management, then decoupling the HTTP server is highly encouraged. You can accomplish this by following the next two steps.

### **Step 3.** Type **ip http active-session-modules none** in global configuration mode.

### **Step 4.** Type **ip http secure-active-session-modules none** in global configuration mode.

## **Global AAA Commands**

The following steps walk you through the commands to enable and configure authentication, authorization, and accounting (AAA) from global configuration mode. Each step includes a description of why you type the command and what it does.

### **Step 1.** Enable AAA on the access switch(es).

By default, the AAA subsystem of the Cisco switch is disabled. Prior to enabling the AAA subsystem, none of the required commands are available in the configuration. Enable AAA as follows:

```
C3560X(config) # aaa new-model
```

**Note** An interesting tidbit of history is that the command **aaa new-model** got its name because the AAA subsystem was replaced back in the 9.x days of Cisco IOS. The original AAA subsystem was deprecated and eventually removed from IOS, and now the “new model” is the only available subsystem. Thanks to Pete Karelis for that fun bit of trivia.

## Step 2. Create an authentication method for 802.1X.

An authentication method is required to instruct the switch to use a particular group of RADIUS servers for 802.1X authentication requests. Create the authentication method as follows:

```
C3560X(config) # aaa authentication dot1x default group radius
```

## Step 3. Create an authorization method for 802.1X.

The method created in Step 2 enables the user/device identity (username/password or certificate) to be validated by the RADIUS Server. However, simply having valid credentials is not enough. An authorization is also required. The authorization is what defines that the user or device is actually allowed to access the network, and what level of access is actually permitted. Create the authorization method as follows:

```
C3560X(config) # aaa authorization network default group radius
```

## Step 4. Create an accounting method for 802.1X.

RADIUS accounting packets are extremely useful, and in many cases are required. These types of packets ensure that the RADIUS server (Cisco ISE) knows the exact state of the switch port and endpoint. Without the accounting packets, Cisco ISE would have knowledge only of the authentication and authorization communication. Accounting packets provide information on when to terminate a live session, as well as local decisions made by the switch (such as AuthFail VLAN assignment, etc.).

If the switch supports Device Sensor, the sensor data will be sent to ISE using the RADIUS accounting configuration. Create the accounting method as follows:

```
C3560X(config) # aaa accounting dot1x default start-stop group radius
```

## Step 5. Configure periodic RADIUS accounting updates.

Periodic RADIUS accounting packets allow Cisco ISE to track which sessions are still active on the network. The following command configures periodic updates to be sent whenever there is new information, as well as a periodic update once per 24 hours (1440 minutes) to show ISE that the session is still

alive:

```
C3560X(config) # aaa accounting update newinfo periodic 1440
```

## Global RADIUS Commands

In the case of global RADIUS commands, a small difference exists between the classic IOS switches and the IOS 15.x switches. The reason for this difference is that IOS 15.x is gaining support for IPv6 infrastructure and classic IOS is limited to IPv4.

### Classic IOS

You can configure a proactive method to check the availability of the RADIUS server. With this practice, the switch sends periodic test authentication messages to the RADIUS server (Cisco ISE). It is looking for a RADIUS response from the server. A success message is not necessary—a failed authentication will suffice, because it shows that the server is alive.

The following steps walk you through adding the RADIUS server to your configuration and enabling the proactive RADIUS server health checks:

**Step 1.** Within global configuration mode, add a username and password for the RADIUS keepalive, which is proactively checking the online status of the RADIUS server.

The username you create here will be added to the local user database in Cisco ISE at a later step. This account will be used in a later step where you define the RADIUS server.

```
C3560X(config) # username radius-test password password
```

**Step 2.** Add the Cisco ISE servers to the RADIUS group.

In this step you add each Cisco ISE Policy Service Node (PSN) to the switch configuration, using the test account you created previously. The server is proactively checked for responses one time per hour, in addition to any authentications or authorizations occurring through normal processes. Repeat this configuration for each PSN:

[Click here to view code image](#)

```
C3560X(config) # radius-server host ise_ip_address auth-port 1812  
acct-port 1813 test username radius-test key shared_secret
```

**Step 3.** Set the dead criteria.

The switch has been configured to proactively check the Cisco ISE server for RADIUS responses. Now configure the counters on the switch to determine if the server is alive or dead. The following configuration settings are set to wait 5

seconds for a response from the RADIUS server and to attempt the test three times before marking the server dead. If a Cisco ISE server doesn't have a valid response within 15 seconds, it is marked as dead. Also set the value of how long the server will be marked dead, which is set to 15 minutes in the following example.

[Click here to view code image](#)

```
C3560X(config) # radius-server dead-criteria time 5 tries 3  
C3560X(config) # radius-server deadtime 15
```

#### Step 4. Enable Change of Authorization (CoA).

Previously, you defined the IP address of a RADIUS server that the switch will send RADIUS messages to. However, you define the servers that are allowed to perform Change of Authorization (RFC 3576) operations in a different listing, also within global configuration mode:

[Click here to view code image](#)

```
C3560X(config) # aaa server radius dynamic-author  
C3560X(config-locsvr-da-radius) # client ise_ip_address server-  
key shared_secret
```

Repeat the command for each of the PSNs and the Monitoring (MNT) nodes of the ISE cube (deployment).

#### Step 5. Configure the switch to use the Cisco vendor-specific attributes (VSA).

Here you configure the switch to send any defined VSAs to Cisco ISE PSNs during authentication requests and accounting updates:

[Click here to view code image](#)

```
C3560X(config) # radius-server vsa send authentication  
C3560X(config) # radius-server vsa send accounting
```

#### Step 6. Enable the VSAs:

These VSAs are used to ensure the service-type, framed-ip-address, and class attributes are sent in the RADIUS communications to ISE.

[Click here to view code image](#)

```
C3560X(config) # radius-server attribute 6 on-for-login-auth  
C3560X(config) # radius-server attribute 8 include-in-access-req  
C3560X(config) # radius-server attribute 25 access-request include
```

#### Step 7. Ensure that the switch always sends traffic from the correct interface.

Switches may often have multiple IP addresses associated to them. Therefore, it is a best practice to always force any management communications to occur

through a specific interface. This interface IP address must match the IP address defined in the Cisco ISE Network Device object.

[Click here to view code image](#)

```
C3560X(config) # ip radius source-interface interface_name  
C3560X(config) # snmp-server trap-source interface_name  
C3560X(config) # snmp-server source-interface informs interface_name
```

## IOS 15.x Switches

As with the classic IOS switches, you can configure a proactive method to check the availability of the RADIUS server. With this practice, the switch sends periodic test authentication messages to the RADIUS server (Cisco ISE). It is looking for a RADIUS response from the server. A success message is not necessary—a failed authentication will suffice, because it shows that the server is alive.

The following steps walk you through adding the RADIUS server to your configuration and enabling the proactive RADIUS server health checks:

**Step 1.** Within global configuration mode, add a username and password for the RADIUS keepalive.

The username you create here will be added to the local user database in Cisco ISE at a later step. This account will be used in a later step where you define the RADIUS server.

[Click here to view code image](#)

```
Cat4503(config) # username radius-test password password
```

**Step 2.** Add the Cisco ISE PSNs as RADIUS servers.

This is where the configuration differs quite a bit from the classic IOS configuration. You create an object for the RADIUS server and then apply configuration to that object:

[Click here to view code image](#)

```
Cat4503(config) # radius server server-name  
Cat4503(config-radius-server) # address ipv4 address auth-port 1812  
                               acct-port 1813  
Cat4503(config-radius-server) # key Shared-Secret  
Cat4503(config-radius-server) # automate-tester username radius-test  
                               probe-on
```

**Step 3.** Set the dead criteria.

The switch has been configured to proactively check the Cisco ISE server for RADIUS responses. Now configure the counters on the switch to determine if the server is alive or dead. The following configuration settings are set to wait 5

seconds for a response from the RADIUS server and to attempt the test three times before marking the server dead. If a Cisco ISE server doesn't have a valid response within 15 seconds, it is marked as dead. We also set the value of how long the server will be marked dead, which is set to 15 minutes in the following example.

[Click here to view code image](#)

```
Cat4503(config)# radius-server dead-criteria time 5 tries 3  
Cat4503(config)# radius-server deadtime 15
```

#### Step 4. Enable Change of Authorization (CoA).

Previously you defined the IP address of a RADIUS server that the switch will send RADIUS messages to. However, you define the servers that are allowed to perform Change of Authorization (RFC 3576) operations in a different listing, also within global configuration mode:

[Click here to view code image](#)

```
Cat4503(config)# aaa server radius dynamic-author  
Cat4503(config-locsvr-da-radius)# client ise_ip_address server-  
key shared_secret
```

Repeat the command for each of the PSNs and the MNT nodes of the ISE cube (deployment).

#### Step 5. Configure the switch to use the Cisco vendor-specific attributes.

Here you configure the switch to send any defined VSAs to Cisco ISE PSNs during authentication requests and accounting updates:

[Click here to view code image](#)

```
Cat4503(config)# radius-server vsa send authentication  
Cat4503(config)# radius-server vsa send accounting
```

#### Step 6. Enable the VSAs:

These VSAs are used to ensure the service-type, framed-ip-address, and class attributes are sent in the RADIUS communications to ISE.

[Click here to view code image](#)

```
Cat4503(config)# radius-server attribute 6 on-for-login-auth  
Cat4503(config)# radius-server attribute 8 include-in-access-req  
Cat4503(config)# radius-server attribute 25 access-request include
```

#### Step 7. Ensure that the switch always sends traffic from the correct interface.

Switches may often have multiple IP addresses associated to them. Therefore, it is a best practice to always force any management communications to occur

through a specific interface. This interface IP address must match the IP address defined in the Cisco ISE Network Device object.

[Click here to view code image](#)

```
Cat4503(config)# ip radius source-interface interface_name  
Cat4503(config)# snmp-server trap-source interface_name  
Cat4503(config)# snmp-server source-interface informs interface_name
```

## Create Local Access Control Lists for Classic IOS and IOS 15.x

Certain functions on the switch require the use of locally configured access control lists (ACL), such as URL redirection. Some of these ACLs that are created are used immediately, and some may not be used until a much later phase of your deployment. The goal of this section is to prepare the switches for all possible deployment models at one time, and limit the operational expense of repeated switch configuration.

You create these local ACLs in the following steps:

**Step 1.** Add the following ACL to be used on switch ports in Monitor Mode:

[Click here to view code image](#)

```
C3560X(config)# ip access-list extended ACL-ALLOW  
C3560X(config-ext-nacl)# permit ip any any
```

**Step 2.** Add the following ACL to be used on switch ports in Low-Impact Mode:

[Click here to view code image](#)

```
C3560X(config)# ip access-list ext ACL-DEFAULT  
C3560X(config-ext-nacl)# remark DHCP  
C3560X(config-ext-nacl)# permit udp any eq bootpc any eq bootps  
C3560X(config-ext-nacl)# remark DNS  
C3560X(config-ext-nacl)# permit udp any any eq domain  
C3560X(config-ext-nacl)# remark Ping  
C3560X(config-ext-nacl)# permit icmp any any  
C3560X(config-ext-nacl)# remark PXE / TFTP  
C3560X(config-ext-nacl)# permit udp any any eq tftp  
C3560X(config-ext-nacl)# remark Drop all the rest  
C3560X(config-ext-nacl)# deny ip any any log
```

**Step 3.** Add the following ACL to be used for URL redirection with web authentication:

[Click here to view code image](#)

```
C3560X(config)# ip access-list extended ACL-WEBAUTH-REDIRECT  
C3560X(config-ext-nacl)# remark explicitly deny DNS from being  
      redirected to address a bug
```

```
C3560X(config-ext-nacl)# deny udp any any eq 53
C3560X(config-ext-nacl)# remark redirect all applicable traffic to the
ISE Server
C3560X(config-ext-nacl)# permit tcp any any eq 80
C3560X(config-ext-nacl)# permit tcp any any eq 443
C3560X(config-ext-nacl)# remark all other traffic will be implicitly
denied from the redirection
```

**Step 4.** Add the following ACL to be used for URL redirection with the Posture Agent:

[Click here to view code image](#)

```
C3560X(config)# ip access-list extended ACL-AGENT-REDIRECT
C3560X(config-ext-nacl)# remark explicitly deny DNS and DHCP from being
redirected
C3560X(config-ext-nacl)# deny udp any any eq 53 bootps
C3560X(config-ext-nacl)# remark redirect HTTP traffic only
C3560X(config-ext-nacl)# permit tcp any any eq 80
C3560X(config-ext-nacl)# remark all other traffic will be implicitly
denied from the redirection
```

## Global 802.1X Commands

The following steps walk you through the commands to enable and configure 802.1X from global configuration mode. Each step includes a description of why you type the command and what it does.

**Step 1.** Enable 802.1X globally on the switch.

Enabling 802.1X globally on the switch does not actually enable authentication on any of the switch ports. Authentication is configured, but it is not enabled until the later sections where you configure Monitor Mode.

```
C3560X(config)# dot1x system-auth-control
```

**Step 2.** Enable downloadable ACLs (dACL) to function.

dACLs are a very common enforcement mechanism in a Cisco TrustSec deployment. For dACLs to function properly on a switch, IP device tracking must be enabled globally:

```
C3560X(config)# ip device tracking
```

## Global Logging Commands (Optional)

The following steps walk you through the commands to enable and configure logging from global configuration mode. Each step includes a description of why you type the command and what it does.

## **Step 1.** Enable syslog on the switch.

Syslog may be generated on Cisco IOS Software in many events. Some of the syslog messages can be sent to the ISE MNT node to be used for troubleshooting purposes. Enabling this across all NADs all the time is not recommended; instead, enable it only when beginning your project and when troubleshooting.

To ensure Cisco ISE is able to compile appropriate syslog messages from the switch, use the following commands.

[Click here to view code image](#)

```
C3560X(config) # logging monitor informational
C3560X(config) # logging origin-id ip
C3560X(config) # logging source-interface interface_id
C3560X(config) # logging host ISE_MNT_PERSONA_IP_Address_x transport udp port 20514
```

## **Step 2.** Set up standard logging functions on the switch to support possible troubleshooting/recording for Cisco ISE functions.

Enterprise Policy Manager (EPM) is a part of the Cisco IOS Software module that is responsible for features such as web authentication and dACLs. Enabling EPM logging generates a syslog related to dACL authorization, and part of the log can be correlated inside Cisco ISE when such logs are sent to Cisco ISE.

```
C3560X(config) # epm logging
```

Only the following NAD syslog messages are actually collected and used by Cisco ISE:

- AP-6-AUTH\_PROXY\_AUDIT\_START
- AP-6-AUTH\_PROXY\_AUDIT\_STOP
- AP-1-AUTH\_PROXY\_DOS\_ATTACK
- AP-1-AUTH\_PROXY\_RETRIES\_EXCEEDED
- AP-1-AUTH\_PROXY\_FALLBACK\_REQ
- AP-1-AUTH\_PROXY\_AAA\_DOWN
- AUTHMGR-5-MACMOVE
- AUTHMGR-5-MACREPLACE
- MKA-5-SESSION\_START
- MKA-5-SESSION\_STOP
- MKA-5-SESSION\_REAUTH
- MKA-5-SESSION\_UNSECURED
- MKA-5-SESSION\_SECURED

- MKA-5-KEEPALIVE\_TIMEOUT
- DOT1X-5-SUCCESS / FAIL
- MAB-5-SUCCESS / FAIL
- AUTHMGR-5-START / SUCCESS / FAIL
- AUTHMGR-SP-5-VLANASSIGN / VLANASSIGNERR
- EPM-6-POLICY\_REQ
- EPM-6-POLICY\_APP\_SUCCESS / FAILURE
- EPM-6-IPEVENT
- DOT1X\_SWITCH-5-ERR\_VLAN\_NOT\_FOUND
- RADIUS-4-RADIUS\_DEAD

## Global Profiling Commands

This section separates the configuration of devices that support Device Sensor and the configuration of devices that must rely on SNMP for profiling.

### Cisco IOS 15.x Switches with Device Sensor Capabilities

Cisco IOS Device Sensor requires a multipart configuration. The first part is to configure the device-sensor filter lists, which inform Device Sensor of which items to care about for the different protocols.

Device Sensor supports three protocols: Dynamic Host Configuration Protocol (DHCP), Cisco Discovery Protocol (CDP), and Link Layer Discovery Protocol (LLDP). Create one list for each protocol by following these steps:

#### Step 1. Create a list for DHCP.

You need to configure three options for ISE—**host-name**, **class-identifier**, and **client-identifier**:

[Click here to view code image](#)

```
C3560X(config) # device-sensor filter-list dhcp list dhcp_list_name
C3560X(config-sensor-dhcplist)# option name host-name
C3560X(config-sensor-dhcplist)# option name class-identifier
C3560X(config-sensor-dhcplist)# option name client-identifier
```

#### Step 2. Create a list for CDP.

You need to configure two CDP options for ISE—**device-name** and **platform-type**:

[Click here to view code image](#)

```
C3560X(config) # device-sensor filter-list cdp list cdp_list_name  
C3560X(config-sensor-cdplist)# tlv name device-name  
C3560X(config-sensor-cdplist)# tlv name platform-type
```

### Step 3. Create a list for LLDP.

You need to configure three LLDP options for ISE—**port-id**, **system-name**, and **system-description**:

[Click here to view code image](#)

```
C3560X(config) # device-sensor filter-list lldp list lldp_list_name  
C3560X(config-sensor-lldplist)# tlv name port-id  
C3560X(config-sensor-lldplist)# tlv name system-name  
C3560X(config-sensor-lldplist)# tlv name system-description
```

### Step 4. Include the lists created in Steps 1–3 in the Device Sensor.

In the first three steps, you defined which options Device Sensor should store.

Now configure Device Sensor to use those lists:

[Click here to view code image](#)

```
C3560X(config) # device-sensor filter-spec dhcp include  
list dhcp_list_name  
C3560X(config) # device-sensor filter-spec cdp include list  
cdp_list_name  
C3560X(config) # device-sensor filter-spec lldp include list  
lldp_list_name
```

### Step 5. Enable Device Sensor.

Device Sensor is now configured but needs to be enabled. Enable Device Sensor to run on the switch and configure when it will send its updates:

[Click here to view code image](#)

```
C3560X(config) # device-sensor accounting  
C3560X(config) # device-sensor notify all-changes
```

## Classic IOS Switches Without Device Sensor Capability

The ISE Policy Service Node uses SNMP to query the switch for certain attributes to help identify the devices that are connected to the switch. As such, you need to configure SNMP communities for Cisco ISE to query, as well as SNMP traps to be sent to Cisco ISE.

### Step 1. Configure a read-only SNMP community.

ISE only requires read-only SNMP access. Ensure that this community string matches the one configured in the Network Device object in Cisco ISE:

```
C3560X(config) # snmp-server community community_string RO
```

## Step 2. Configure the switch to send traps.

Now enable an SNMP trap to be sent with changes to the MAC address table. A trap that includes the device MAC address and interface identifier is sent to Cisco ISE whenever a new address is inserted, removed, or moved in the address table.

```
C3560X(config) # snmp-server enable traps mac-notification change move threshold
```

## Step 3. Add Cisco ISE as an SNMP trap receiver (optional).

If you will be using the SNMPTRAP probe, add a server as a trap receiver for the configured MAC notification. This is not needed in most cases, and you don't want to send traps and use the RADIUS probe together because both trigger the SNMPQUERY probe.

```
C3560X(config) # snmp-server host ise_ip_address version 2c
community_string mac-notification
```

Sample configurations are provided in Appendix C, “Sample Switch Configurations.”

# Interface Configuration Settings for Classic IOS and IOS 15.x Switches

You have just completed the global configuration settings of the access layer switches, including RADIUS, SNMP, profiling, and AAA methods.

This section focuses on building a single port configuration that can be used across your entire Secure Unified Access deployment, regardless of the switch type, the deployment stage, or which deployment model you choose.

## Configure Interfaces as Switch Ports

One of the first things to do before configuring any of the authentication settings on the switch port is to ensure that the switch port is configured as a Layer 2 port, not a Layer 3 port. This command is a simple, one-word command that you run, and from that point the other commands you run will all take effect.

### Step 1. Enter interface configuration mode for the switch port range:

```
C3560X(config) # interface range first_interface - last_interface
```

### Step 2. Ensure that the ports are Layer 2 switch ports:

```
C3560X(config-if-range) # switchport
```

### Step 3. Configure the port for Layer 2 edge, using the **host** macro.

The **host** macro automatically runs three commands for you. It configures the port to be an access port (nontrunk), disables channel groups, and configures spanning tree to be in portfast mode.

[Click here to view code image](#)

```
C3560X(config-if-range)# switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
```

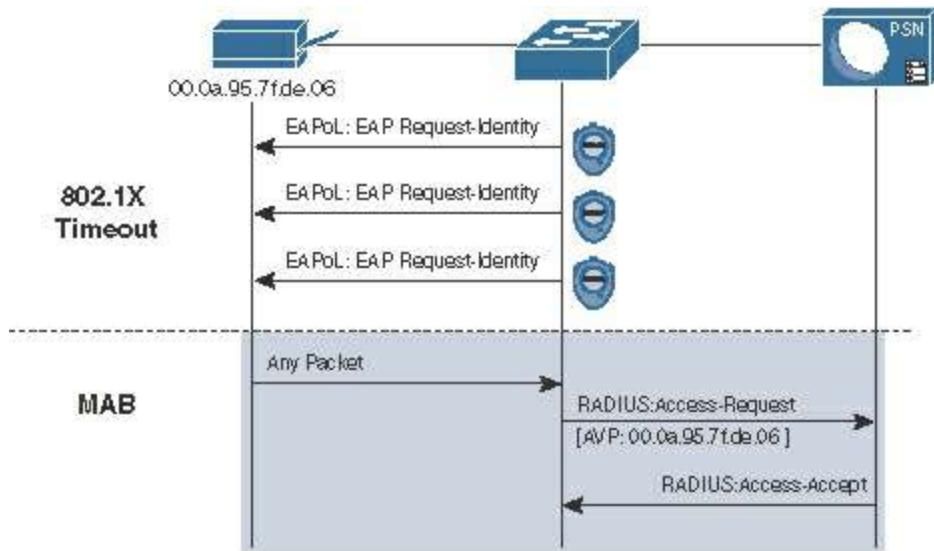
## Configure Flexible Authentication and High Availability

The default behavior of 802.1X is to deny access to the network when an authentication fails. In many of the early customer deployments of 802.1X, this behavior was discovered to be undesirable because it does not allow for guest access and does not allow employees to remediate their computer systems and gain full network access.

The next phase in handling 802.1X authentication failures was to provide an “Auth-Fail VLAN” to allow a device/user that failed authentication to be granted access to a VLAN that provided limited resources. This was a step in the right direction, but it was still missing some practicality, especially in environments that must use MAC Authentication Bypass (MAB) for all the printers and other nonauthenticating devices. With the default behavior of 802.1X, an administrator has to configure ports for printers and other devices that do not have supplicants differently from the ports where they plan to do authentication.

In response to these issues, Cisco created Flexible Authentication (Flex-Auth). Flex-Auth enables a network administrator to set an authentication order and priority on the switch port, thereby allowing the port to attempt, in order, 802.1X, MAB, and then WebAuth. All of these functions are provided while maintaining the same configuration on all access ports, thereby providing a much simpler operational model for customers than is provided by traditional 802.1X deployments.

As mentioned previously, there are multiple methods of authentication on a switch port: 802.1X (dot1x), MAB, and WebAuth. With 802.1X authentication, the switch sends an identity request (EAP-Identity-Request) periodically after the link state has changed to up (see the “Configure Authentication Timers” section for recommended timer changes). Additionally, the endpoint supplicant should send a periodic EAP over LAN Start (EAPoL-Start) message into the switch port to speed up authentication. If a device is not able to authenticate, it merely waits until the dot1x timeout occurs, and then MAB occurs. Assuming the device MAC address is in the correct database, it is then authorized to access the network. [Figure 11-1](#) illustrates this concept.



**Figure 11-1 Flexible Authentication**

The following steps walk you through the configuration of Flex-Auth and the configurable actions for authentication high availability:

### Step 1. Configure the authentication method priority on the switch ports.

The best practice is to always prefer the stronger authentication method, dot1x, which is also the default of all Cisco switches:

```
C3560X(config-if-range)# authentication priority dot1x mab
```

### Step 2. Configure the authentication method order on the switch ports.

There are certain deployment methods where MAB should occur before 802.1X authentication. For those corner cases, Cisco switches allow a network administrator to set a user-definable authentication order. However, the best practice is to maintain the order of dot1x and then MAB:

```
C3560X(config-if-range)# authentication order dot1x mab
```

### Step 3. Configure the port to use Flex-Auth:

```
C3560X(config-if-range)# authentication event fail action next-method
```

### Step 4. Configure the port to use a local VLAN for voice and data when the RADIUS server is “dead” (when it stops responding).

In the “Global RADIUS Commands” section, you configured the RADIUS server entry to use a test account that proactively alerts the switch when Cisco ISE has stopped responding to RADIUS requests. Now you will configure the switch port to locally authorize the port when that server is found to be dead, and reinitialize authentication when the server becomes alive again:

[Click here to view code image](#)

```
C3560X(config-if-range)# authentication event server dead action
```

```
authorize vlan vlan-id
C3560X(config-if-range)# authentication event server dead action
    authorize voice
C3560X(config-if-range)# authentication event server alive action
    reinitialize
```

**Step 5.** Configure the port to use a local VLAN when the RADIUS server is “dead” and to allow existing and new hosts.

This feature was introduced to resolve problems with multiple authenticating hosts on a single port when a portion of them have already been authenticated while the RADIUS server was operational, and others (new hosts) are trying to authenticate when the RADIUS server is down.

Prior to the introduction of this new feature, all authenticated hosts (when the RADIUS server is up) get full access to network and the others (the new hosts) do not get access to the network. With this new feature/CLI configuration, when new hosts try to access the network and the RADIUS server is down, that port is reinitialized immediately and all hosts (in this port) get the same VLAN.

```
C3560X(config-if-range)# authentication event server dead action
    reinitialize vlan vlan-id
```

**Step 6.** Set the host mode of the port.

The default behavior of an 802.1X-enabled port is to authorize only a single MAC address per port. There are other options, most notably Multi-Domain Authentication (MDA) and Multiple Authentication (Multi-Auth) modes. During the initial phases of any Cisco TrustSec deployment, it is best practice to use Multi-Auth mode to ensure that there is no denial of service while deploying 802.1X.

**Note** Port Security is not compatible with 802.1X, because 802.1X handles this function natively.

Multi-Auth mode allows virtually unlimited MAC addresses per switch port, and requires an authenticated session for every MAC address. When the deployment moves into the late stages of the authenticated phase, or into the enforcement phase, it is then recommended that you use MDA mode, which allows a single MAC address in the Data domain and a single MAC address in the Voice domain per port. Set the host mode of the port as follows:

```
C3560X(config-if-range)# authentication host-mode multi-auth
```

**Step 7.** Configure the violation action.

When an authentication violation occurs, such as more MAC addresses than are

allowed on the port, the default action is to put the port into an err-disabled state. Although this behavior may seem to be a nice, secure behavior, it can create an accidental denial of service, especially during the initial phases of deployment. Therefore, set the action to be **restrict**, as follows. This mode of operation allows the first authenticated device to continue with its authorization, and denies any additional devices.

```
C3560X(config-if-range)# authentication violation restrict
```

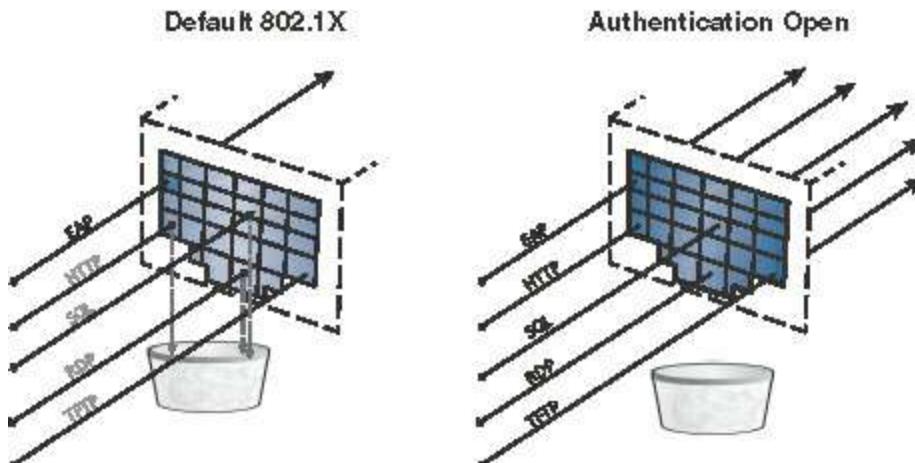
## Configure Authentication Settings

802.1X is designed to be binary by default. Successful authentication means the user is authorized to access the network. Unsuccessful authentication means the user has no access to the network. This paradigm does not lend itself very well to a modern organization. Most organizations need to do workstation imaging with Preboot Execution Environments (PXE), or may have some thin clients that have to boot with DHCP and don't have any way to run a supplicant.

Additionally, when early adopters of 802.1X deployed authentication companywide, there were repercussions. Many issues arose. For example, supplicants were misconfigured; there were unknown devices that could not authenticate because of a lack of supplicant, and other reasons.

Cisco created Open Authentication to aid with deployments. Open Authentication allows all traffic to flow through the switch port, even without the port being authorized. This feature permits authentication to be configured across the entire organization, but does not deny access to any device.

[Figure 11-2](#) depicts the difference between a port with the default behavior of 802.1X versus a port with Open Authentication configured. This is a key feature that enables the phased approach to deploying authentication.



**Figure 11-2** Default 802.1X Authentication Versus Open Authentication

Perform the following steps to configure authentication:

**Step 1.** Set the port for Open Authentication:

```
C3560X(config-if-range)# authentication open
```

**Step 2.** Enable MAC Authentication Bypass on the port:

```
C3560X(config-if-range)# mab
```

**Step 3.** Enable the port to perform IEEE 802.1X authentication:

```
C3560X(config-if-range)# dot1x pae authenticator
```

## Configure Authentication Timers

Many timers can be modified as needed in a deployment. Unless you are experiencing a specific problem where adjusting the timer may correct unwanted behavior, it is recommended that you leave all timers at their default values except for the 802.1X Transmit (tx-period) timer. The tx-period timer defaults to a value of 30 seconds. Leaving this value at 30 seconds provides a default wait of 90 seconds ( $3 \times$  tx-period) before a switch port begins the next method of authentication, and activates the MAB process for nonauthenticating devices.

Based on numerous deployments, we recommend that you set the tx-period value to 10 seconds to provide the most optimal time for MAB devices. Setting the value to less than 10 seconds may result in unwanted behavior; setting the value greater than 10 seconds may result in DHCP timeouts. To configure the tx-period timer to 10 seconds, enter the following command:

```
C3560X(config-if-range)# dot1x timeout tx-period 10
```

## Apply the Initial ACL to the Port and Enable Authentication

The following steps prepare the port for Monitor Mode, in which a default ACL is applied on the port without denying any traffic:

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

```
C3560X(config-if-range)# ip access-group ACL-ALLOW in
```

**Step 2. (Optional)** Enable authentication.

If you wish to enable authentication now, you may do so as follows. However, we recommend that you wait until after you configure your policies for Monitor Mode. See [Chapter 20, “Deploying in Phases,”](#) for more details on Monitor Mode.

```
C3560X(config-if-range)# authentication port-control auto
```

**Note** The preceding command is required to enable authentication (802.1X, MAB, WebAuth). Without this command, everything appears to be working, but no authentication is sent to the RADIUS server.

## Configuration Settings for C3PL Switches

This section reviews configuration for the newer 15.2.x and IOS-XE 3.6.x switches that follow the Cisco Common Classification Policy Language (C3PL) style of configuration. An interesting side note is that these types of switches still accept the old style of commands. In fact, that is the default, and you must enable the C3PL style of commands with the global configuration command **authentication display new-style**.

That command is a little misleading, because it changes much more than just the display. It completely changes the way that you, the administrator, interact with the switch and changes the available features. To change back to the classic model of configuring authentication and the classic features, use the **authentication display legacy** command.

It's very important to note that after you start configuring the C3PL policies themselves, you cannot revert to the legacy mode. You can switch back only if you haven't configured C3PL yet; otherwise, you have to erase the switch configuration and reload or restore an older backup configuration.

### Why Use C3PL?

This new syntax offers many benefits, most of which are located under the hood and not noticeable to the end user. For example, C3PL allows the configuration to exist in memory once and be invoked multiple times. This is a processor- and memory-efficiency enhancement. Among the administrator-facing differences, the most notable benefits are:

- 802.1X and MAB can run simultaneously without having to sequence the two distinctive authentication processes, whereby 802.1X authentication has to be failed for MAB to start.
- The use of service templates to control preconfigured ACL on the interface in the event of RADIUS not being available.

With the classic platforms, the sequencing of 802.1X and MAB can result in certain MAB endpoints not being able to get IP addresses in a timely manner. By processing 802.1X and MAB simultaneously, the endpoints can receive a DHCP-assigned IP address in a timely manner. Additionally, with classic platforms, a static ACL is often applied to interfaces in order to restrict network access for devices that have not

authenticated yet. In those cases, the ACL remains applied to devices attempting to connect while the RADIUS server is unavailable, resulting in denial of service until the RADIUS server is reachable. This may seem desirable in theory, but it actually makes life more difficult for the policy server administrator, and is not recommended.

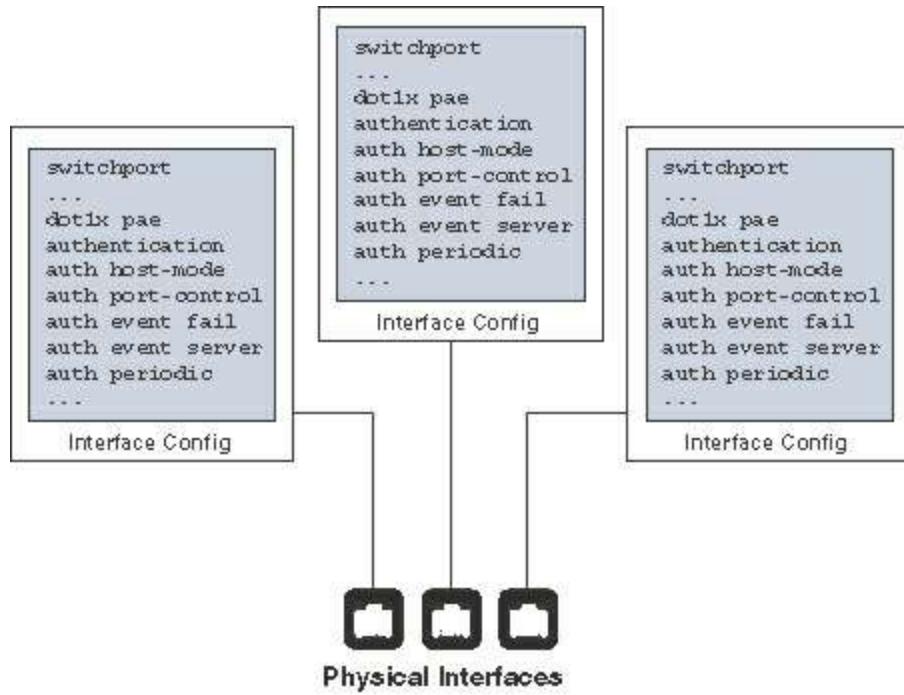
Now that you've just been let down, let's build you back up. The new C3PL style does provide some very useful enhancements such as service templates. With the introduction of service templates, another ACL that would permit network access can be applied to the interface when a certain condition matches, such as when the RADIUS server is not reachable. This is known as the Critical ACL functionality.

C3PL also has a feature known as differentiated authentication, which enables you to authenticate different methods with different servers. For example, you can send MAB to ServerA and 802.1X authentications to ServerB. Although this is a neat concept, it does not apply to Secure Access deployments with ISE because it does not maintain state with a single policy server, which defeats the point of having a solution like ISE.

There is also a pretty cool feature in C3PL known as Critical MAB. This allows the switch to use a locally defined list of MAC addresses in the event that the centralized RADIUS server is unavailable.

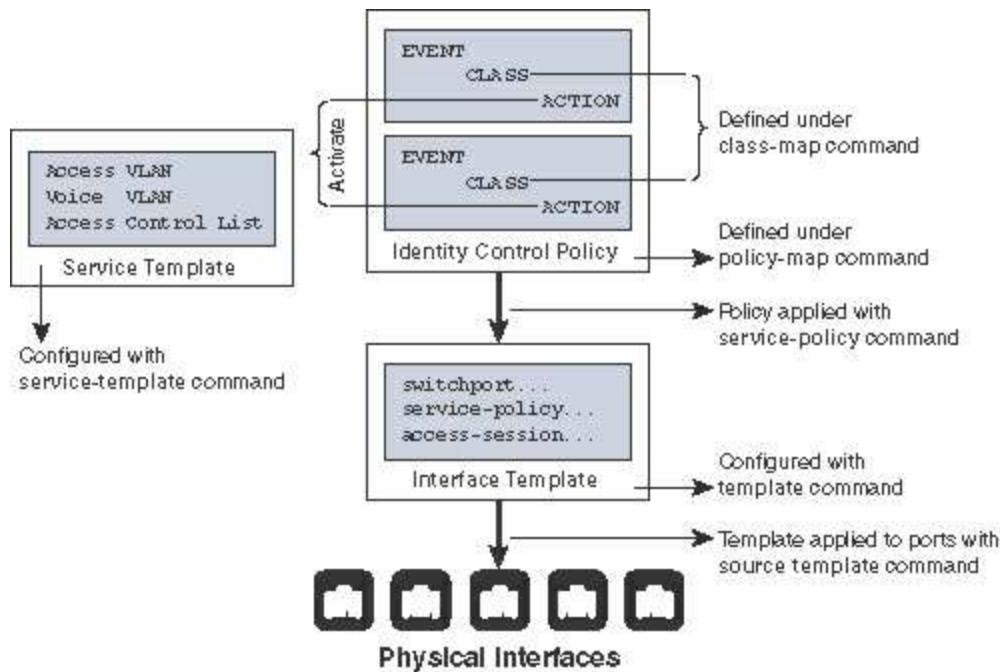
Basically, the use of C3PL is recommended in a Secure Access deployment with ISE only in cases where you require the use of Critical ACL, Critical MAB, or interface templates. Otherwise, just continue to use the classic method of authentication configuration and keep your configurations across all platforms similar.

[Figure 11-3](#) illustrates the traditional method, where each interface has its own configuration associated to it.



**Figure 11-3** Classic Configuration

In contrast, [Figure 11-4](#) illustrates the C3PL method, which offers much more flexibility to configure what is applied to the interface and when.



**Figure 11-4** C3PL Configuration

## Global Configuration for C3PL

As with the Classic IOS and IOS 15.x switches, you need to configure certificates for

URL redirection.

From global configuration mode on the switch, perform the following steps:

**Step 1.** Set the DNS domain name on the switch.

Cisco IOS does not allow for certificates, or even self-generated keys, to be created and installed without first defining a DNS domain name on the device.

Type **ip domain-name** domain-name at the global configuration prompt.

**Step 2.** Generate self-signed keys to be used for HTTPS.

Type **crypto key generate rsa general-keys mod 2048** at the global configuration prompt.

**Step 3.** Enable the HTTP server in global configuration mode.

Type **ip http server** at the global configuration prompt.

**Step 4.** Enable the HTTP Secure server in global configuration mode.

Type **ip http secure-server** at the global configuration prompt.

Many organizations want to ensure that this redirection process using the switch's internal HTTP server is decoupled from the management of the switch itself. If you are not using HTTP for management, then decoupling the HTTP server is highly encouraged. You can accomplish this by following the next two steps.

**Step 5.** Type **ip http active-session-modules none** in global configuration mode.

**Step 6.** Type **ip http secure-active-session-modules none** in global configuration mode.

Now you will enable the C3PL configuration style. Remember that under the covers the same authentication engine is at work and IOS is doing the translation; however, you cannot use the C3PL-specific configurations without switching to the new style of configuration.

**Step 7.** Within privileged EXEC mode, enable the new style of configuration:

```
C3850# authentication display new-style
```

**Step 8.** Enable the AAA subsystem:

```
C3850 (config) # aaa new-model
```

**Step 9.** Ensure that any of the services that AAA network security services provide will use the same session ID:

```
C3850 (config) # aaa session-id common
```

**Step 10.** Create an authentication method for 802.1X.

An authentication method is required to instruct the switch to use a particular group of RADIUS servers for 802.1X authentication requests. Create the

authentication method as follows:

```
C3850(config)# aaa authentication dot1x default group radius
```

### Step 11. Create an authorization method for 802.1X.

The authorization is what defines that the user or device is actually allowed to access the network, and what level of access is actually permitted. Create the authorization method as follows:

```
C3850(config)# aaa authorization network default group radius
```

### Step 12. Create an accounting method for 802.1X.

RADIUS accounting packets are extremely useful, and in many cases are required. These types of packets ensure that the RADIUS server (Cisco ISE) knows the exact state of the switch port and endpoint. Without the accounting packets, Cisco ISE would have knowledge only of the authentication and authorization communication. Accounting packets provide information on when to terminate a live session, as well as local decisions made by the switch (such as AuthFail VLAN assignment, etc.). Create the accounting method as follows:

```
C3850(config)# aaa accounting dot1x default start-stop group radius
```

### Step 13. Configure periodic RADIUS accounting updates.

Periodic RADIUS accounting packets allow Cisco ISE to track which sessions are still active on the network. The following command configures periodic updates to be sent whenever there is new information, as well as a periodic update once per 24 hours (1440 minutes) to show ISE that the session is still alive:

```
C3850(config)# aaa accounting update newinfo periodic 1440
```

## Global RADIUS Commands for C3PL

As with the classic IOS and IOS 15.x switches, you can configure a proactive method to check the availability of the RADIUS server. With this practice, the switch sends periodic test authentication messages to the RADIUS server (Cisco ISE). It is looking for a RADIUS response from the server. A success message is not necessary—a failed authentication will suffice, because it shows that the server is alive.

The following steps walk you through adding the RADIUS server to your configuration and enabling the proactive RADIUS server health checks:

### Step 1. Within global configuration mode, add a username and password for the RADIUS keepalive.

The username you create here will be added to the local user database in Cisco ISE at a later step. This account will be used in a later step where you define the

RADIUS server.

```
C3850(config) # username radius-test password password
```

## Step 2. Add the Cisco ISE PSNs as RADIUS servers.

This is where the configuration differs quite a bit from the classic IOS configuration. You create an object for the RADIUS server and then apply configuration to that object:

[Click here to view code image](#)

```
C3850(config) # radius server server-name  
C3850(config-radius-server) # address ipv4 address auth-port 1812  
    acct-port 1813  
C3850(config-radius-server) # key Shared-Secret  
C3850(config-radius-server) # automate-tester username radius-test  
    probe-on
```

## Step 3. Set the dead criteria.

The switch has been configured to proactively check the Cisco ISE server for RADIUS responses. Now configure the counters on the switch to determine if the server is alive or dead. The following configuration settings are to wait 5 seconds for a response from the RADIUS server and to attempt the test three times before marking the server dead. If a Cisco ISE server doesn't have a valid response within 15 seconds, it is marked as dead. The following configuration also sets the value of how long the server will be marked dead to 15 minutes. High availability is covered in more detail in [Chapter 18, “Setting Up a Distributed ISE Deployment.”](#)

[Click here to view code image](#)

```
C3850(config) # radius-server dead-criteria time 5 tries 3  
C3850(config) # radius-server deadtime 15
```

## Step 4. Enable Change of Authorization (CoA).

Previously, you defined the IP address of a RADIUS server that the switch will send RADIUS messages to. However, you define the servers that are allowed to perform Change of Authorization (RFC 3576) operations in a different listing, also within global configuration mode:

[Click here to view code image](#)

```
C3850(config) # aaa server radius dynamic-author  
C3850(config-locsvr-da-radius) # client ise_ip_address server-key  
    shared_secret
```

Repeat the client command for each PSN and MNT node.

## Step 5. Configure the switch to use the Cisco vendor-specific attributes (VSA).

Here you configure the switch to send any defined VSAs to Cisco ISE PSNs during authentication requests and accounting updates:

[Click here to view code image](#)

```
C3850(config)# radius-server vsa send authentication  
C3850(config)# radius-server vsa send accounting
```

## Step 6. Enable the VSAs.

Enabling the VSAs requires two additional entries compared to enabling them on non-C3PL switches. In the newer IOS-XE based devices, attribute 31 (calling-station-id) is no longer on by default:

[Click here to view code image](#)

```
C3850(config)# radius-server attribute 6 on-for-login-auth  
C3850(config)# radius-server attribute 8 include-in-access-req  
C3850(config)# radius-server attribute 25 access-request include  
C3850(config)# radius-server attribute 31 mac format ietf upper-case  
C3850(config)# radius-server attribute 31 send nas-port-detail mac-only
```

## Step 7. Ensure that the switch always sends traffic from the correct interface.

Switches may often have multiple IP addresses associated to them. Therefore, it is a best practice to always force any management communications to occur through a specific interface. This interface IP address must match the IP address defined in the Cisco ISE Network Device object.

[Click here to view code image](#)

```
Cat4503(config)# ip radius source-interface interface_name  
Cat4503(config)# snmp-server trap-source interface_name  
Cat4503(config)# snmp-server source-interface informs interface_name
```

## Configure Local ACLs and Local Service Templates

As with the other switch type classifications, certain functions on C3PL switches require the use of locally configured ACLs, such as URL redirection. Some of these ACLs that are created are used immediately, and some may not be used until a much later phase of your deployment. The goal of this section is to prepare the switches for all possible deployment models at one time, and limit the operational expense of repeated switch configuration.

### Step 1. Add the following ACL to be used on switch ports in Monitor Mode:

[Click here to view code image](#)

```
C3850(config)# ip access-list extended ACL-ALLOW
```

```
C3850(config-ext-nacl)# permit ip any any
```

**Step 2.** Add the following ACL to be used on switch ports in Low-Impact Mode:

[Click here to view code image](#)

```
C3850(config)# ip access-list extended ACL-DEFAULT
C3850(config-ext-nacl)# remark DHCP
C3850(config-ext-nacl)# permit udp any eq bootpc any eq bootps
C3850(config-ext-nacl)# remark DNS
C3850(config-ext-nacl)# permit udp any any eq domain
C3850(config-ext-nacl)# remark Ping
C3850(config-ext-nacl)# permit icmp any any
C3850(config-ext-nacl)# remark PXE / TFTP
C3850(config-ext-nacl)# permit udp any any eq tftp
C3850(config-ext-nacl)# remark Drop all the rest
C3850(config-ext-nacl)# deny ip any any log
```

**Step 3.** Add the following ACL to be used for URL redirection with web authentication:

[Click here to view code image](#)

```
C3850(config)# ip access-list extended ACL-WEBAUTH-REDIRECT
C3850(config-ext-nacl)# remark explicitly deny DNS from being
    redirected to address a bug
C3850(config-ext-nacl)# deny udp any any eq 53
C3850(config-ext-nacl)# remark redirect all applicable traffic to the
    ISE Server
C3850(config-ext-nacl)# permit tcp any any eq 80
C3850(config-ext-nacl)# permit tcp any any eq 443
C3850(config-ext-nacl)# remark all other traffic will be implicitly
    denied from the redirection
```

**Step 4.** Add the following ACL to be used for URL redirection with the Posture Agent:

[Click here to view code image](#)

```
C3850(config)# ip access-list extended ACL-AGENT-REDIRECT
C3850(config-ext-nacl)# remark explicitly deny DNS and DHCP from being
    redirected
C3850(config-ext-nacl)# deny udp any any eq 53 bootps
C3850(config-ext-nacl)# remark redirect HTTP traffic only
C3850(config-ext-nacl)# permit tcp any any eq 80
C3850(config-ext-nacl)# remark all other traffic will be implicitly
    denied from the redirection
```

Service templates are new to C3PL switches. A service template is similar to an ISE authorization profile but can be locally present on the switch. A service template is a

collection of VLAN, Named ACL, Timer, and URL Redirect string that can be applied based on the C3PL event. Just like dACLs, service templates can be centrally located on ISE and be downloaded during authorization. However, here you are going to create a service template local to the switch to apply when none of the configured RADIUS servers (ISE PSNs) are reachable to process 802.1X or MAB requests (known as the critical-auth state).

Add the following service template named CRITICAL to be used when no RADIUS servers are available, also known as the critical-auth state:

[Click here to view code image](#)

```
C3850(config) # service-template CRITICAL
C3850(config-service-template) # description Apply for Critical Auth
C3850(config-service-template) # access-group ACL-ALLOW
```

## Global 802.1X Commands

The following steps walk you through the commands to enable and configure 802.1X from global configuration mode. Each step includes a description of why you type the command and what it does.

### Step 1. Enable 802.1X globally on the switch.

Enabling 802.1X globally on the switch does not actually enable authentication on any of the switch ports. Authentication will be configured, but it is not enabled at this point.

```
C3560X(config) # dot1x system-auth-control
```

### Step 2. Enable downloadable ACLs to function.

dACLs are a very common enforcement mechanism in a Cisco TrustSec deployment. For dACLs to function properly on a switch, IP device tracking must be enabled globally:

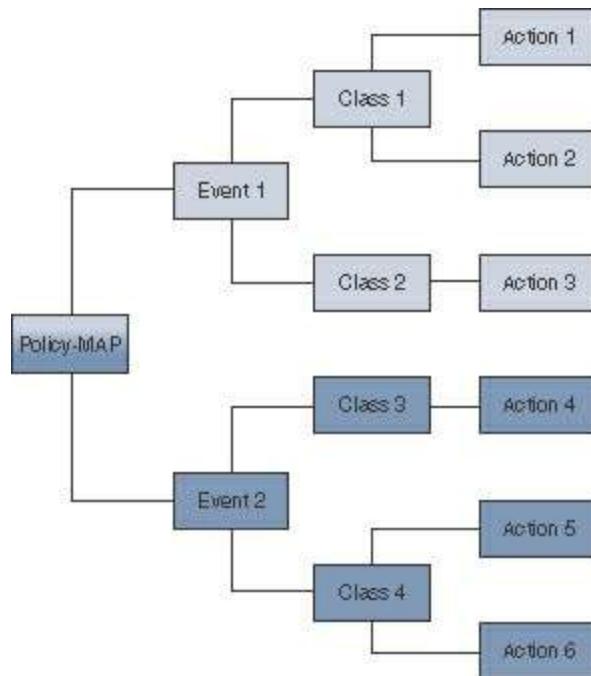
```
C3560X(config) # ip device tracking
```

**Note** In some uncommon cases, Windows 7 and some other devices do not respond to ARPs. Windows displays “Duplicate IP Address Detected: 0.0.0.0.” In such instances, you might need to use the command **ip device tracking use SVI**.

## C3PL Fundamentals

The Cisco Common Classification Policy Language is used across a variety of Cisco

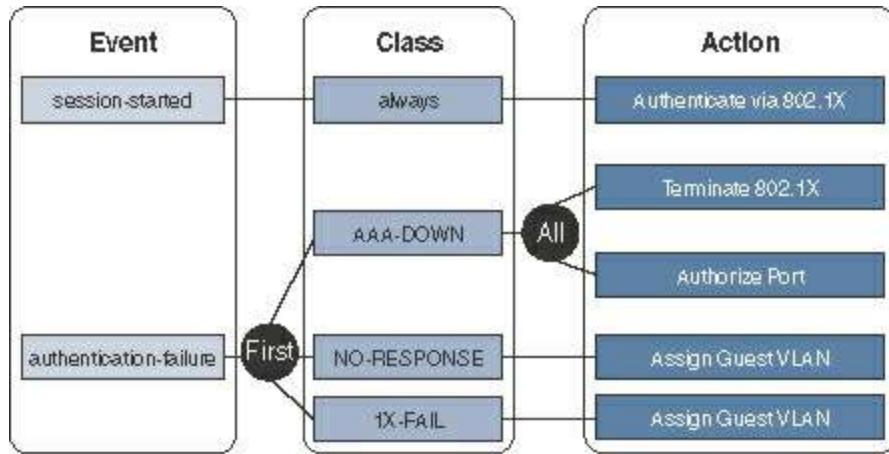
solutions, including Catalyst switches, Cisco routers, Cisco ASA firewalls, and more. With these C3PL devices, the configuration is made up of building blocks. Policies contain one or more events, events contain one or more classes, and classes contain one or more conditions to be matched. [Figure 11-5](#) illustrates this concept.



**Figure 11-5** C3PL Hierarchy

## Configure the C3PL Policies

The class is the base-level object and the first item that you configure for the C3PL policy. After you create the class, you create a policy with an event. That event calls the class that you created previously. [Figure 11-6](#) illustrates the relationship of an event to classes and the relationships of the classes to actions. This illustration was created by a truly gifted Technical Marketing Engineer at Cisco named Hariprasad (“Hari”) Holla. Hari has presented on this topic many times at Cisco Live, and you can even watch VoD recordings of those sessions for free at <http://www.ciscolive.com>; navigate to **Learn Online > On-demand Library > Speakers** and enter **Hariprasad Holla** as the search string.



**Figure 11-6** Event, Class, and Action Relationships (Courtesy Hariprasad Holla)

## Configure Control Classes

A control class defines the conditions under which the actions of a control policy are executed. You define whether all, any, or none of the conditions must evaluate to true to execute the actions of the control policy. Control classes are evaluated based on the event specified in the control policy.

**Note** If this is first time C3PL-type commands are being used on this switch, it will present a warning that it cannot revert to legacy mode unless the switch configuration is cleared.

**Step 1.** Configure a control class for when none of the RADIUS servers are available (the critical-auth state):

[Click here to view code image](#)

```
C3850(config)# class-map type control subscriber match-any AAA-DOWN
C3850(config-filter-control-classmap)# match result-type aaa-timeout
```

**Step 2.** Configure a control class for when 802.1X authentication fails for the session:

[Click here to view code image](#)

```
C3850(config)# class-map type control subscriber match-all DOT1X-FAILED
C3850(config-filter-control-classmap)# match method dot1x
C3850(config-filter-control-classmap)# match result-type method dot1x
    authoritative
```

## Configure Control Policies

Control policies are used to dictate which actions should be taken in response to the specified events. The policy contains one or more rules that associate a control class with one or more actions. The actions that you can configure in a rule are specific to the

event itself. In other words, you wouldn't have a MAB action apply to a dot1x event. Control policies typically control the authentication of the end user or endpoint and the applying services to the authentication session, or even to a physical interface. [Figure 11-6](#) shows this hierarchy and the relationship between the components of the policy. In the following steps, you create a control policy leveraging the control classes you created in the previous section and then apply the policy to a range of interfaces on the switch:

**Step 1.** Configure a control policy that will be applied to all 802.1X/MAB-enabled interfaces.

```
C3850(config)# policy-map type control subscriber DOT1X-DEFAULT
```

**Step 2.** Configure actions for when the session starts.

The following configuration enables 802.1X and MAB to run simultaneously, assigning a higher priority for 802.1X over MAB. This practice is not recommended for production environments; it is presented here just to illustrate that MAB and 802.1X can be run at the same time.

[Click here to view code image](#)

```
C3850(config-event-control-policymap)# event session-started match-all
C3850(config-class-control-policymap)# 10 class always do-all
C3850(config-action-control-policymap)# 10 authenticate using dot1x
    priority 10
C3850(config-action-control-policymap)# 20 authenticate using mab
    priority 20
```

**Step 3.** Configure actions for policy violations:

[Click here to view code image](#)

```
C3850(config-action-control-policymap)# event violation match-all
C3850(config-class-control-policymap)# 10 class always do-all
C3850(config-action-control-policymap)# 10 restrict
```

**Step 4.** Configure the switch to attempt to authenticate the endpoint using 802.1X when a supplicant is detected on the endpoint:

[Click here to view code image](#)

```
C3850(config-action-control-policymap)# event agent-found match-all
C3850(config-class-control-policymap)# 10 class always do-all
C3850(config-action-control-policymap)# 10 authenticate using dot1x
```

**Step 5.** Configure the action for 802.1X authentication failures, or when there is a lack of ISE PSNs (RADIUS servers) available:

[Click here to view code image](#)

```
C3850 (config-action-control-policymap) # event authentication-failure
match-all
C3850 (config-class-control-policymap) # 10 class AAA-DOWN do-all
C3850 (config-action-control-policymap) # 10 authorize
C3850 (config-action-control-policymap) # 20 activate service-template
CRITICAL
C3850 (config-action-control-policymap) # 30 terminate dot1x
C3850 (config-action-control-policymap) # 40 terminate mab
C3850 (config-action-control-policymap) # 20 class DOT1X-FAILED do-all
C3850 (config-action-control-policymap) # 10 authenticate using mab
```

**Note** Because we will be using Centralized WebAuth (CWA), which sends ACCESS-ACCEPT even for unknown MAC addresses, there will be no failure for MAB, thus a failure event for MAB is not defined in the preceding configuration.

## Apply the Control Policy to the Interfaces

Now that the policy is created, it needs to be applied to the access-layer interfaces with the **service-policy** command. Not all aspects of the 802.1X configuration are completed in C3PL, so some configuration items will occur at the interfaces separately.

**Step 1.** Apply the control policy to the interface range:

[Click here to view code image](#)

```
C3850 (config) # interface range GigabitEthernet 1/0/1 - 24
C3850 (config-if-range) # description Dot1X Enabled Ports
C3850 (config-if-range) # switchport host
C3850 (config-if-range) # service-policy type control subscriber
DOT1X-DEFAULT
```

**Step 2.** Apply the remaining interface configuration:

[Click here to view code image](#)

```
C3850 (config-if-range) # authentication periodic
C3850 (config-if-range) # authentication timer reauthenticate server
C3850 (config-if-range) # mab
C3850 (config-if-range) # ip access-group DEFAULT-ACL in
C3850 (config-if-range) # access-session host-mode multi-auth
C3850 (config-if-range) # no access-session closed
C3850 (config-if-range) # dot1x timeout tx-period 10
C3850 (config-if-range) # access-session port-control auto
C3850 (config-if-range) # no shutdown
```

## Cisco Wireless LAN Controllers

This section reviews the configuration for the Cisco Wireless LAN Controller. The focus is on version 8.3, which includes many nice enhancements to the WLC, such as the integrated Device Sensor technology, URL-based ACLs, and support for FlexConnect access points. WLC Version 8.3 also adds the very desirable feature of being able to secure your guest network with pre-shared keys instead of leaving it open and unencrypted.

If you ever have any questions or concerns about which version of the WLC is best, the most stable, and the most recommended, check out this website:

<https://supportforums.cisco.com/document/12481821/tac-recommended-aireos>. That is where a team made up of Wireless TAC and ISE TAC give their joint recommendations based on their experiences.

## AireOS Features and Version History

Much like any other product decision, your choice of WLC version needs to be based on examining which features you want or need for your environment and weighing the benefit of those features against the older versions that might not have them, but are more of a known and proven entity. To help you with your version decision, [Table 11-1](#) identifies some ISE-related features that have been added to the WLC since version 7.0.

Cisco WLC Version	Secure Access Features Added
AireOS 7.0	URL redirection, CoA, and ISE-NAC features are limited to 802.1X-enabled networks only.  Open SSIDs must use Local WebAuth (LWA) without posture or onboarding capabilities.
AireOS 7.2	URL redirection, CoA, and ISE-NAC features are enabled on open and dot1x-enabled WLANs.  Device Sensor functionality added.
AireOS 7.3	FlexConnect support for the ISE-NAC features added.  CLI support for DNS snooping and URL-based ACLs.  TrustSec support with SGT Exchange Protocol (SXP).
AireOS 7.4	mDNS snooping.  Application Visibility and Control (AVC).  NetFlow support.
AireOS 7.6	GUI configuration of DNS snooping and URL-based ACLs introduced.
AireOS 8.0	HTTPS redirection support added.  Application Visibility and Control (AVC).
AireOS 8.1	
AireOS 8.2	
AireOS 8.3	True URL filtering provided.  RADIUS-NAC renamed to ISE-NAC, RFC 3576 renamed to “Support for CoA.”

**Table 11-1** AireOS Features and Version History

Now that you've examined the different versions, it is time to begin the configuration of the Wireless LAN Controller.

As with the previous section covering configuration of Cisco Catalyst Switches, this section assumes that you have established basic connectivity with the NAD and are now ready to bootstrap the WLC for use with ISE.

## Configure the AAA Servers

The first step in bootstrapping the WLC is to add the ISE Policy Service Nodes to the WLC as RADIUS authentication and accounting servers.

## Add the RADIUS Authentication Servers

In the following steps, you add the ISE PSNs as RADIUS authentication servers in the WLC.

From the WLC GUI, perform the following steps:

**Step 1.** Navigate to **Security > RADIUS > Authentication**.

**Step 2.** Ensure that MAC Delimiter is set to **Hyphen**.

This ensures that the format of the MAC address is aa-bb-cc-dd-ee-ff, which is the way ISE expects it to be. [Figure 11-7](#) shows the MAC Delimiter setting.



**Figure 11-7** Security > RADIUS > Authentication > MAC Delimiter

**Step 3.** Click **New** to add the ISE Policy Service Node.

**Step 4.** In the Server IP Address field, enter the IP address of the PSN (or the virtual IP address, if using a load balancer).

**Step 5.** In the Shared Secret field, enter the shared secret. This must match what is configured in ISE for the Network Device object.

**Step 6.** In the Port Number field, enter **1812** for authentication.

**Step 7.** From the Server Status drop-down list, choose **Enabled**.

**Step 8.** From the Support for CoA drop-down list, choose **Enabled** (in older WLC version, this field is labeled Support for RFC 3576).

**Step 9.** In the Server Timeout field, change the default setting to 5 seconds, which should work nicely.

**Step 10.** For Network User, check the **Enable** check box. This simply indicates that the RADIUS server may be used for network authentications.

**Step 11.** Click **Apply** in the upper-right corner.

**Step 12.** Click **Save Configuration** at the top of the screen.

[Figure 11-8](#) shows a completed server configuration.

The screenshot shows the Cisco Wireless LAN Controller (WLC) GUI under the Security tab. On the left, a navigation tree includes AAA, RADIUS (selected), TACACS+, Local EAP, Advanced EAP, Priority Order, Certificate, Access Control Lists, Wireless Protection Policies, and Web Auth. The main panel is titled "RADIUS Authentication Servers > New". It contains fields for Server Index (Priority: 9), Server IP Address (10.1.100.245), Shared Secret Format (ASCII), Shared Secret, Confirm Shared Secret, Key Wrap (unchecked), Port Number (1812), Server Status (Enabled), Support for CoA (Enabled), Server Timeout (2 seconds), Network User (Enable checked), Management (Enable unchecked), Management Retransmit Timeout (5 seconds), Tunnel Proxy (unchecked), and IPSec (unchecked).

**Figure 11-8** RADIUS Authentication Server Configuration

Repeat these steps for each Policy Service Node that you need to add.

## Add the RADIUS Accounting Servers

Now that you have defined the ISE PSNs for authentication, you need to define them again for accounting.

From the WLC GUI, perform the following steps:

**Step 1.** Navigate to **Security > RADIUS > Accounting**.

**Step 2.** From the MAC Delimiter drop-down list, choose **Hyphen**, as shown in [Figure 11-9](#).

The screenshot shows the Cisco WLC GUI under the Security tab. The navigation tree on the left shows AAA (selected) and RADIUS (under AAA). The main panel is titled "RADIUS Accounting Servers". It displays two dropdown menus: "Acct Called Station ID Type" set to "System MAC Address" and "MAC Delimiter" set to "Hyphen".

**Figure 11-9 Security > RADIUS > Accounting > MAC Delimiter**

**Step 3.** Click **New** to add the ISE Policy Service Node.

**Step 4.** In the Server IP Address field, add the IP address of the PSN.

**Step 5.** In the Shared Secret field, enter the shared secret to match what is configured on ISE.

**Step 6.** In the Port Number field, enter **1813**.

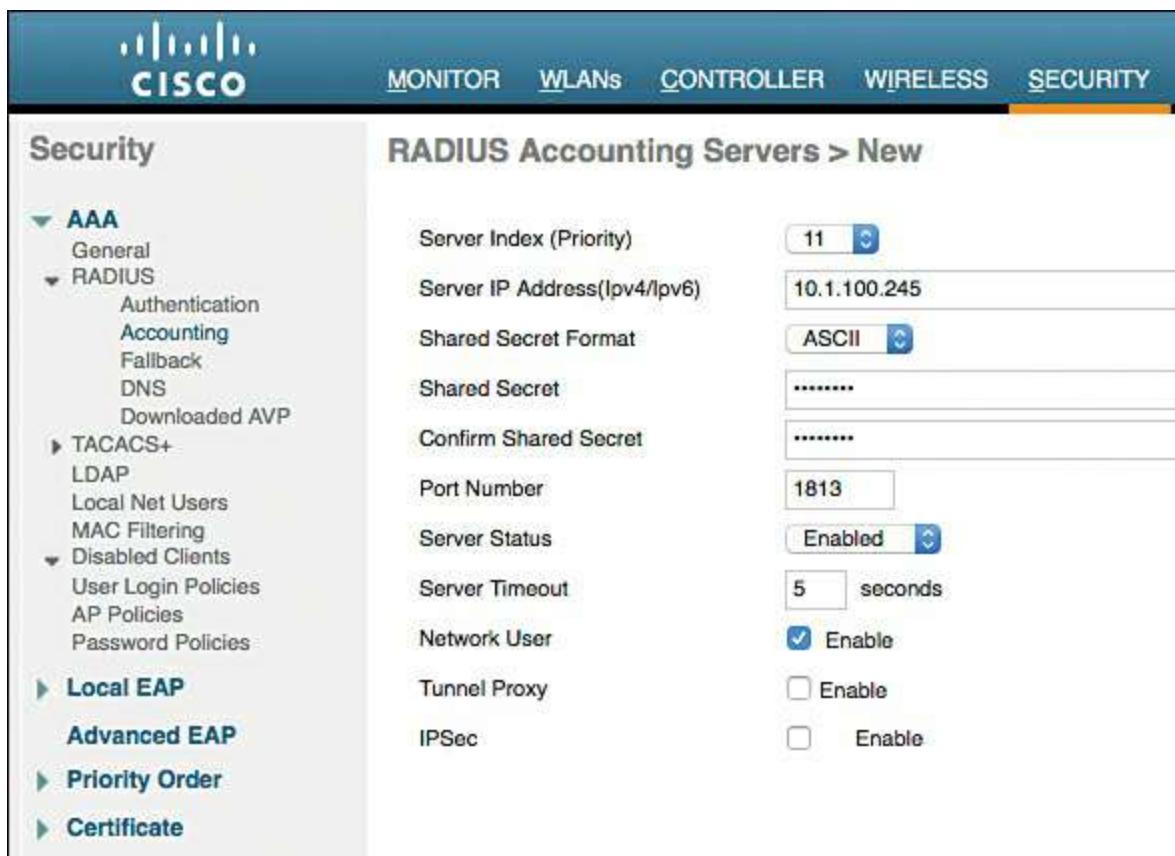
**Step 7.** From the Server Status drop-down list, choose **Enabled**.

**Step 8.** For the **Network User**, check the **Enable** check box.

**Step 9.** Click **Apply** in the upper-right corner.

**Step 10.** Click **Save Configuration** at the top of the screen.

[Figure 11-10](#) shows a completed server entry.



The screenshot shows the Cisco Wireless LAN Controller (WLC) interface under the **SECURITY** tab. On the left, a navigation tree is visible with sections like AAA, RADIUS, TACACS+, Local EAP, Advanced EAP, Priority Order, and Certificate. The main panel is titled "RADIUS Accounting Servers > New". It contains the following configuration fields:

Server Index (Priority)	11
Server IP Address(Ipv4/Ipv6)	10.1.100.245
Shared Secret Format	ASCII
Shared Secret	.....
Confirm Shared Secret	.....
Port Number	1813
Server Status	Enabled
Server Timeout	5 seconds
Network User	<input checked="" type="checkbox"/> Enable
Tunnel Proxy	<input type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

**Figure 11-10 RADIUS Accounting Server Configuration**

Repeat these steps for each Policy Service Node that you need to add.

### Configure RADIUS Fallback (High Availability)

The primary RADIUS server (the server with the lowest server index) is assumed to be

the most preferable server for the Cisco WLC. If the primary server becomes unresponsive, the controller switches to the next active server (the server with the next lowest server index). The controller continues to use this backup server, unless you configure the controller either to fall back to the primary RADIUS server when it recovers and becomes responsive or to switch to a more preferable server from the available backup servers.

From the WLC GUI, perform the following steps:

**Step 1.** Navigate to **Security > AAA > RADIUS > Fallback**.

**Step 2.** From the Fallback Mode drop-down list, choose **Active**.

Selecting Active causes the Cisco WLC to revert to a server with a lower priority from the available backup servers by using RADIUS probe messages to proactively determine whether a server that has been marked inactive is back online.

**Step 3.** In the Username field, enter the name to be sent in the inactive server probes.

We have been using radius-test as the username so far in the book. Technically, you do not need to enter a password for this test user account, because the system simply looks for a response from the RADIUS server; pass or fail does not matter.

**Step 4.** In the Interval in Sec field, enter a value. The interval states the inactive time in passive mode and probe interval in active mode. The valid range is 180 to 3600 seconds, and the default value is 300 seconds.

[Figure 11-11](#) shows the fallback settings for RADIUS.



**Figure 11-11** Fallback Parameters

## Configure the Airespace ACLs

Earlier in the chapter, you pre-staged the Cisco Catalyst Switches with local ACLs. Similarly, pre-stage the WLC with a Web Authentication ACL named

**ACL\_WEBAUTH\_REDIRECT**. This ACL name is used specifically because it matches the preconfigured setting in ISE, which may make your job a little easier if this is a brand-new (aka greenfield) deployment. Beginning with ISE 2.0, there are some smart-default configurations that ship with ISE to make unboxing ISE and setting it up

very fast and easy. The smart-default configurations for Guest and BYOD include the use of the redirect ACL with this specific name.

Naturally, you can use whatever name you wish, and simply change the configuration built in to ISE. However, for the purposes of this book, we will keep the same ACL name.

## Create the Web Authentication Redirection ACL

As with the Cisco Catalyst Switches, you need a local ACL on the WLC to redirect web traffic to the Centralized Web Authentication portal. However, with the Catalyst Switch, a **permit** statement means that the traffic should be redirected, and a **deny** statement describes traffic that should not be redirected. With the switch, you need two ACLs: one to define what gets redirected, and a second one to filter traffic (permit or deny traffic flow).

The WLC has a single ACL, and it pulls double-duty. It permits and denies traffic flow, but at the same time it redirects the traffic that is denied to the Centralized Web Authentication portal.

From the WLC GUI, perform the following steps:

**Step 1.** Navigate to **Security > Access Control Lists > Access Control Lists**, as shown in [Figure 11-12](#).

**Enable Counters**

Name	Type
<a href="#">HR-ACL</a>	IPv4
<a href="#">NSP-ACL</a>	IPv4
<a href="#">ACL-AGENT-REDIRECT</a>	IPv4
<a href="#">GUEST_PSP_ONLY</a>	IPv4
<a href="#">ACL-GUEST-ACCESS</a>	IPv4
<a href="#">BLACKHOLE</a>	IPv4
<a href="#">Internet-Only</a>	IPv4
<a href="#">Restricted</a>	IPv4
<a href="#">ACL-MDM-REDIRECT</a>	IPv4
<a href="#">Employee_Limited</a>	IPv4

**Foot Notes**

1. Counter configuration is global for acl, urlacl and layer2acl.

**Figure 11-12** Security > Access Control Lists > Access Control Lists

**Step 2.** Click **New** to add a new ACL.

**Step 3.** In the Access Control List Name field, fill in the name  
**ACL\_WEBAUTH\_REDIRECT**.

**Step 4.** Click **Apply**.

**Step 5.** When you return to the main Access Control Lists screen, click the new entry:  
**ACL\_WEBAUTH\_REDIRECT**.

**Step 6.** Click **Add New Rule** in the upper-right corner.

A rule in the WLC is the equivalent of an access control entry (ACE) in the switch. It is a line in the ACL.

**Step 7.** Create a set of rules for this ACL that does the following:

- Permits all traffic outbound (toward the client).
- Permits DNS.
- Permits TCP port 8443 to the ISE servers. For simplicity, you may want to permit all traffic to the ISE nodes. It also allows you to reuse the same ACL for

most use cases.

- Denies all other traffic—which will redirect all denied web traffic.

[Figure 11-13](#) shows an example of a completed ACL.

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0	0.0.0.0	Any	Any	Any	Any	Outbound	
2	Permit	0.0.0.0	0.0.0.0	UDP	Any	DNS	Any	Any	
3	Permit	0.0.0.0	10.1.100.240 - 255.255.255.240	Any	Any	Any	Any	Inbound	
4	Permit	0.0.0.0	10.1.100.254 - 255.255.255.240	Any	Any	Any	Any	Inbound	
5	Permit	0.0.0.0	10.1.103.0 - 255.255.255.0	Any	Any	Any	Any	Inbound	
6	Deny	0.0.0.0	0.0.0.0	Any	Any	Any	Any	Inbound	

**Figure 11-13** ACL\_WEBAUTH\_REDIRECT Example

## Add Google URLs for ACL Bypass

When Android endpoints go through the BYOD onboarding process, they must have access to the Google Play Store to download the Network Setup Assistant app. However, allowing that access through your network is not as simple as just entering an IP address in the ACL—hundreds of addresses may resolve to the DNS names needed for the Google Play Store. Beginning with WLC version 7.6, Airespace ACLs include the capability to use DNS-based ACLs in the form of URL lists.

To add Google URLs for ACL bypass, follow these steps:

**Step 1.** Navigate to **Security > Access Control Lists > Access Control Lists**.

**Step 2.** Hover your mouse pointer over the blue-and-white drop-down arrow icon to the right of the ACL\_WEBAUTH\_REDIRECT ACL that you created in the previous section.

**Step 3.** Click **Add-Remove URL**, as shown in [Figure 11-14](#).



**Figure 11-14** Hovering Over Add-Remove URL Option

You are now brought to the URL List. The URLs that you enter here are configured with an implicit wildcard in the first portion. In other words, entering

google.com matches \*.google.com. Any matches to these URL entries will be permitted through the ACL.

#### Step 4. Enter the URLs that are to be permitted through the ACL.

In the United States, entering google.com and clients.google.com typically does the trick. In other countries, other URLs may need to be entered for the smooth operation of Android endpoints. One solution that has worked is to add .\*.\* for the domain extensions. In other words, enter google.\*.\* instead of google.com and enter android.clients.google.\*.\* instead of android.clients.google.com.

[Figure 11-15](#) shows an example URL list.

The screenshot shows a configuration interface titled "ACL > ACL\_WEBAUTH\_REDIRECT > URL List". It includes a search bar labeled "URL String Name" and an "Add" button. Below this, there is a table with two columns: "URL Name" and "Value". The table contains two rows: one for "clients.android.google.com" and another for "google.com".

URL Name	Value
clients.android.google.com	
google.com	

**Figure 11-15** URL List

## Create the Dynamic Interfaces for the Client VLANs

When you want to assign a user or device to a VLAN on a Catalyst Switch, just assign the VLAN to the port, and the entire switch port will now be assigned to that particular VLAN.

The WLC has only a few physical connections to the wired network, and it must bridge all wireless users from their RF network (Wi-Fi) to the physical wired network. The WLC must also have the ability to assign a different VLAN per authenticated session (if necessary). If you are thinking that the WLC just needs to be connected with a trunk, you are correct.

The WLC is configured to use 802.1Q to tag traffic for a specific VLAN as that traffic exits the controller. However, the controller calls this a dynamic interface because the WLC can either assign a physical interface to traffic or assign an 802.1Q tag to traffic.

In this section, you will create two dynamic interfaces: one for employee traffic and one for guest traffic.

### Create the Employee Dynamic Interface

This interface will be used for all successful authentications to the Corporate WLAN, providing full access to the entire network.

From the WLC GUI, perform the following steps:

**Step 1.** Choose **Controller > Interfaces**.

**Step 2.** Click **New**.

**Step 3.** Name your interface. Use the name **employee** for purposes of this example.

**Step 4.** In the VLAN Identifier field, enter the VLAN ID to be used in the 802.1Q tag (**41** in this example).

**Step 5.** Click **Apply**.

**Step 6.** Click the new interface named **employee**.

You most likely will not need to change any settings until you reach the Physical Information section.

**Step 7.** In the Interface Address section, provide an IP address, netmask, and gateway for the VLAN in the respective fields.

**Step 8.** In the DHCP Information section, in the Primary DHCP Server field, enter the DHCP server address.

**Step 9.** Click **Apply**.

[Figure 11-16](#) shows an example employee dynamic interface configuration.

## Interfaces > Edit

### General Information

Interface Name employee  
MAC Address d0:d0:fd:91:e2:65

### Configuration

Guest Lan   
Quarantine   
Quarantine Vlan Id 0  
NAS-ID none

### Physical Information

Port Number 2  
Backup Port 0  
Active Port 2  
Enable Dynamic AP Management

### Interface Address

VLAN Identifier 41  
IP Address 10.1.41.2  
Netmask 255.255.255.0  
Gateway 10.1.41.1  
IPv6 Address ::  
Prefix Length 128  
IPv6 Gateway ::  
Link Local IPv6 Address fe80::d2d0:fdff:fe91:e260/64

### DHCP Information

Primary DHCP Server 10.10.100.100  
Secondary DHCP Server   
DHCP Proxy Mode Global   
Enable DHCP Option 82

**Figure 11-16** Example Employee Dynamic Interface Configuration

## Create the Guest Dynamic Interface

The guest dynamic interface is used for all devices connecting to the Guest WLAN, as well as for unsuccessful or unauthorized authentications to the Corporate WLAN. This interface has Internet access only.

From the WLC GUI, perform the following steps:

**Step 1.** Choose **Controller > Interfaces**.

**Step 2.** Click **New**.

**Step 3.** Name your interface. Use the name **Guest** for purposes of this example.

**Step 4.** In the VLAN Identifier field, enter the VLAN ID to be used in the 802.1Q tag (**42** in the example).

**Step 5.** Click **Apply**.

**Step 6.** Click the new interface named **Guest**.

You most likely will not need to change any settings until you reach the Physical Information section. In the Configuration section, do not enable the Guest LAN check box. This is not for guest WLANs; it is for providing guest access to directly connected wired LANs.

**Step 7.** In the Interface Address section, provide an IP address, netmask, and gateway for the VLAN in the respective fields.

**Step 8.** In the DHCP Information section, in the Primary DHCP Server field, enter the DHCP server address.

**Step 9.** Click **Apply**.

[Figure 11-17](#) shows an example guest dynamic interface configuration.

## Interfaces > Edit

### General Information

Interface Name guest  
MAC Address d0:d0:fd:91:e2:65

### Configuration

Guest Lan   
Quarantine   
Quarantine Vlan Id 0  
NAS-ID none

### Physical Information

Port Number 2  
Backup Port 0  
Active Port 2  
Enable Dynamic AP Management

### Interface Address

VLAN Identifier 42  
IP Address 10.1.42.2  
Netmask 255.255.255.0  
Gateway 10.1.42.1  
IPv6 Address ::  
Prefix Length 128  
IPv6 Gateway ::  
Link Local IPv6 Address fe80::d2d0:fdff:fe91:e260/64

### DHCP Information

Primary DHCP Server 10.1.100.100  
Secondary DHCP Server  
DHCP Proxy Mode Global   
Enable DHCP Option 82

**Figure 11-17 Example Dynamic Guest Interface Configuration**

## Create the Wireless LANs

Now that the RADIUS servers, ACLs, and dynamic interfaces are all created and configured, we will move on to creating two WLANs: one for guests (Guest) and one for corporate users (Corporate). The Guest WLAN will be an “open” WLAN, while the Corporate WLAN will be configured to use 802.1X to authenticate devices. With the WLC version 8.3 and newer, the Guest network can also be configured to use WPA/WPA2 with a pre-shared key.

## Create the Guest WLAN

The Guest WLAN will be created as an open SSID, but it will send the endpoint MAC addresses to ISE over RADIUS for MAB, just like the wired networks.

From the WLC GUI, perform the following steps:

**Step 1.** Click the **WLANs** menu.

**Step 2.** Click **Create New**.

**Step 3.** Click **Go**.

**Step 4.** From the Type drop-down list, choose **WLAN**.

**Step 5.** In the Profile Name field, enter the WLAN profile name; use **ISE-Guest** for purposes of this example, as shown in [Figure 11-18](#).



**Figure 11-18** Example Guest WLAN Creation

**Step 6.** In the SSID field, enter an SSID name; use **ISE-Guest** in this example.

**Step 7.** Click **Apply**.

The Edit ‘ISE-Guest’ screen opens with the General tab displayed, as shown in [Figure 11-19](#), which is where you can enable and disable the WLAN and configure other general options.

WLANS > Edit 'ISE-Guest'

General	Security	QoS	Policy-Mapping	Advanced
Profile Name Type SSID Status	ISE-Guest WLAN ISE-Guest <input checked="" type="checkbox"/> Enabled			
Security Policies	MAC Filtering (Modifications done under security tab will appear after applying the changes.)			
Radio Policy	All			
Interface/Interface Group(G)	guest			
Multicast Vlan Feature	<input type="checkbox"/> Enabled			
Broadcast SSID	<input checked="" type="checkbox"/> Enabled			
NAS-ID	none			

**Figure 11-19** General Tab for ISE-Guest

- Step 8.** If you are ready to work with this SSID, check the **Enabled** check box to the right of Status.
- Step 9.** From the Interface/Interface Group(G) drop-down list, choose the **Guest** interface that you created previously.
- Step 10.** Check the **Enabled** check box to the right of Broadcast SSID if you want to broadcast the SSID, which is the general practice for open guest networks.
- Step 11.** Click the **Security** tab, shown in [Figure 11-20](#) with the Layer 2 subtab displayed (the default).

WLANS > Edit 'ISE-Guest'

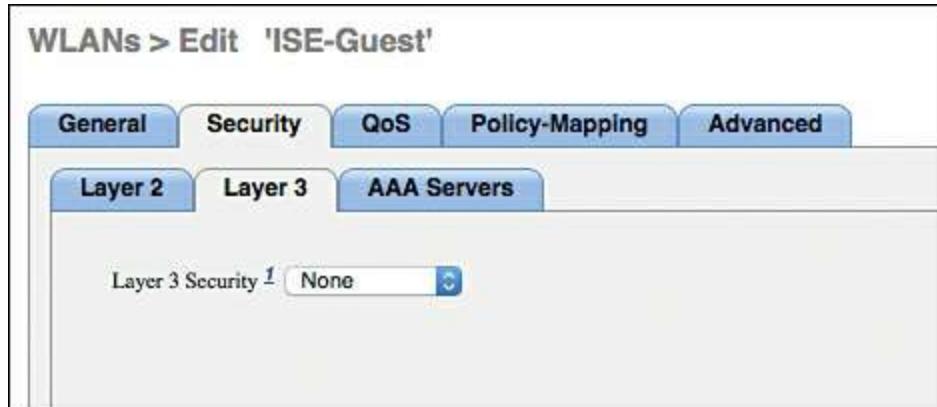
General	Security	QoS	Policy-Mapping	Advanced
Layer 2	Layer 3	AAA Servers		
Layer 2 Security	None			
MAC Filtering	<input checked="" type="checkbox"/>			
Fast Transition				
Fast Transition	Adaptive			
Over the DS	<input checked="" type="checkbox"/>			
Reassociation Timeout	20	Seconds		

**Figure 11-20** Layer 2 Security Subtab for ISE-Guest

**Step 12.** From the Layer 2 Security drop-down list, change from the default (WPA+WPA2) to **None**.

**Step 13.** Check the **MAC Filtering** check box (which is wireless MAB).

**Step 14.** Click the **Layer 3** subtab, shown in [Figure 11-21](#), which is used to configure Local Web Authentication (LWA).



**Figure 11-21** Layer 3 Security Subtab for ISE-Guest

**Step 15.** From the Layer 3 Security drop-down list, choose **None**.

**Step 16.** Click the **AAA Servers** subtab, shown in [Figure 11-22](#).



**Figure 11-22** AAA Servers Subtab for ISE-Guest

The Cisco WLC enables administrators to specify different authentication and accounting servers. However, this configuration is incompatible with an ISE RADIUS server. ISE provides session services that are tied together from the session ID in the authentication packet and the session ID in the accounting packet.

**Step 17.** Check the **Enabled** check box under both Authentication Servers and Accounting Servers and select your respective ISE Policy Service Node(s) in the columns.

**Step 18.** In the RADIUS Server Accounting section, check the **Enabled** check box to the right of Interim Update.

**Step 19.** Set the Interim Interval to 0 seconds.

**Note** For WLC versions 7.6 and earlier, the recommendation is to disable interim updates (leave the corresponding Enabled check box unchecked). For version 8.0 and later, interim updates should be enabled with an interval of 0 seconds, as specified in Step 19. With this setting, an accounting update is sent only when the client IP address changes. Device Sensor updates are not impacted.

**Step 20.** Click **Apply**.

**Step 21.** Click the **Advanced** tab, the top portion of which is shown in [Figure 11-23](#).

The screenshot shows the 'WLANs > Edit 'ISE-Guest'' configuration page. The 'Advanced' tab is selected. The configuration includes:

- Allow AAA Override:** Enabled (checkbox checked).
- Coverage Hole Detection:** Enabled (checkbox checked).
- Enable Session Timeout:** Enabled (checkbox checked), with a value of 28800 seconds.
- Aironet IE:** Enabled (checkbox checked).
- Diagnostic Channel:** Enabled (checkbox checked).
- Override Interface ACL:** IPv4: None, IPv6: None.
- Layer2 Acl:** None.
- URL ACL:** None.
- P2P Blocking Action:** Disabled.
- Client Exclusion:** Enabled (checkbox checked), with a Timeout Value of 30 seconds.
- Maximum Allowed Clients:** 0.
- Static IP Tunneling:** Enabled (checkbox checked).
- Wi-Fi Direct Clients Policy:** Allow.
- Maximum Allowed Clients Per AP Radio:** 200.
- Clear HotSpot Configuration:** Enabled (checkbox checked).
- Client user idle:** (dropdown menu).

**DHCP:**

- DHCP Server: Override (checkbox unchecked).
- DHCP Addr. Assignment: Required (checkbox checked).

**OEAP:**

- Split Tunnel: Enabled (checkbox unchecked).

**Management Frame Protection (MFP):**

- MFP Client Protection: Optional (dropdown menu).

**DTIM Period (in beacon intervals):**

- 802.11a/n (1 - 255): 1.
- 802.11b/g/n (1 - 255): 1.

**NAC:**

- NAC State: ISE NAC (dropdown menu).

**Load Balancing and Band Select:**

- Client Load Balancing: (checkbox unchecked).

**Figure 11-23** Advanced Tab (Top) for ISE-Guest

**Step 22.** Check the **Enabled** check box for Allow AAA Override.

This enables ISE to assign a VLAN and ACL that are different from those configured on the WLAN and interface by default.

**Step 23.** Check the **Enabled** check box for Enable Session Timeout, and set the Session Timeout to **28800** seconds.

The default value of 1800 has been known to be too short in many environments.

**Step 24.** In the NAC section, from the NAC State drop-down list, choose **ISE NAC**.

In versions earlier than 8.3, this setting is named Radius NAC instead of ISE NAC. Regardless of the name, this setting is critical for URL Redirection,

Centralized Web Authentication (CWA), Posture Assessment, Native Supplicant Provisioning, MDM redirections, and more.

**Step 25.** Check the **Enabled** check box for Client Exclusion and change the Timeout Value to **30** seconds.

**Step 26.** In the DHCP section on the right side of the screen, check the **Required** check box for DHCP Addr. Assignment.

This setting is required for the DHCP Device Sensor built in to the WLC.

**Step 27.** Scroll down to the middle of the Advanced tab and, under Radius Client Profiling, check both the **DHCP Profiling** and **HTTP Profiling** options, as shown in [Figure 11-24](#).

The screenshot shows the 'Advanced' tab of the 'ISE-Guest' WLAN configuration. The 'Radius Client Profiling' section is expanded, showing 'DHCP Profiling' and 'HTTP Profiling' both checked. Other sections like 'Voice', 'Local Client Profiling', 'PMIP', and 'Universal AP Admin Support' are also visible but not fully expanded.

**Figure 11-24** Advanced Tab (Middle) for ISE-Guest

Note in [Figure 11-24](#) that the Cisco WLC has two different client profiling options: Radius Client Profiling, which sends the attributes to ISE within RADIUS accounting packets, and Local Client Profiling, where the WLC keeps the information and uses it locally. Although the interface appears to offer the option to enable both types of profiling, they are mutually exclusive and cannot be enabled at the same time.

**Step 28.** Click **Apply** in the upper-right corner.

**Step 29.** Click **Save Configuration** at the top of the screen.

## Create the Corporate SSID

The Corporate WLAN is created as a closed SSID and requires 802.1X authentication for an endpoint to associate to the WLAN. Unlike wired networks, wireless networks have the added benefit of truly rejecting all access without a successful authentication. Users are attuned to the requirement of configuring software in order to connect to a wireless network. The same is not true when it comes to wired networks.

From the WLC GUI, perform the following steps:

**Step 1.** Click the **WLANS** menu.

**Step 2.** Click **Create New**.

**Step 3.** Click **Go**.

**Step 4.** From the Type drop-down list, choose **WLAN**.

**Step 5.** In the Profile Name field, enter the WLAN profile name; use **ISE** for purposes of this example, as shown in [Figure 11-25](#).



**Figure 11-25** Example Corporate WLAN Creation

**Step 6.** In the SSID field, enter an SSID name; use **ISE** in this example.

In this example, the SSID name ISE is used because it is the SSID name that is preconfigured in the smart-default for ISE 2.0 and later prebuilt native supplicant profile. Using this SSID name will help speed up your installation and demo-ability, just like using the ACL\_WEBAUTH\_REDIRECT name for the Airespace ACL.

**Step 7.** Click **Apply**.

The Edit 'ISE' screen opens with the General tab displayed, as shown in [Figure 11-26](#).

WLANS > Edit 'ISE'

General	Security	QoS	Policy-Mapping	Advanced
Profile Name	ISE			
Type	WLAN			
SSID	ISE			
Status	<input checked="" type="checkbox"/> Enabled			
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)			
Radio Policy	All			
Interface/Interface Group(G)	employee			
Multicast Vlan Feature	<input type="checkbox"/> Enabled			
Broadcast SSID	<input checked="" type="checkbox"/> Enabled			
NAS-ID	none			

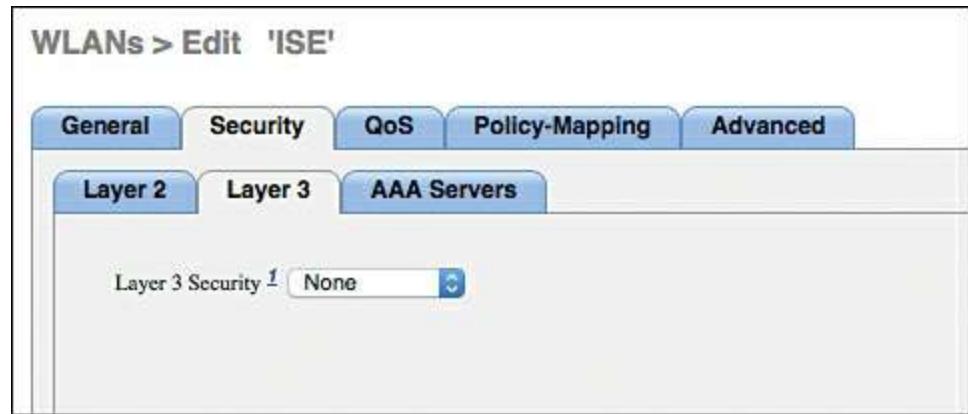
**Figure 11-26** General Tab for ISE Corporate WLAN

- Step 8.** If you are ready to work with this SSID, check the **Enabled** check box to the right of Status.
- Step 9.** From the Interface/Interface Group(G) drop-down list, choose the **Employee** interface that you created previously.
- Step 10.** Click the **Security** tab, shown in [Figure 11-27](#) with the Layer 2 subtab displayed (the default).



**Figure 11-27** Layer 2 Security Subtab for ISE Corporate WLAN

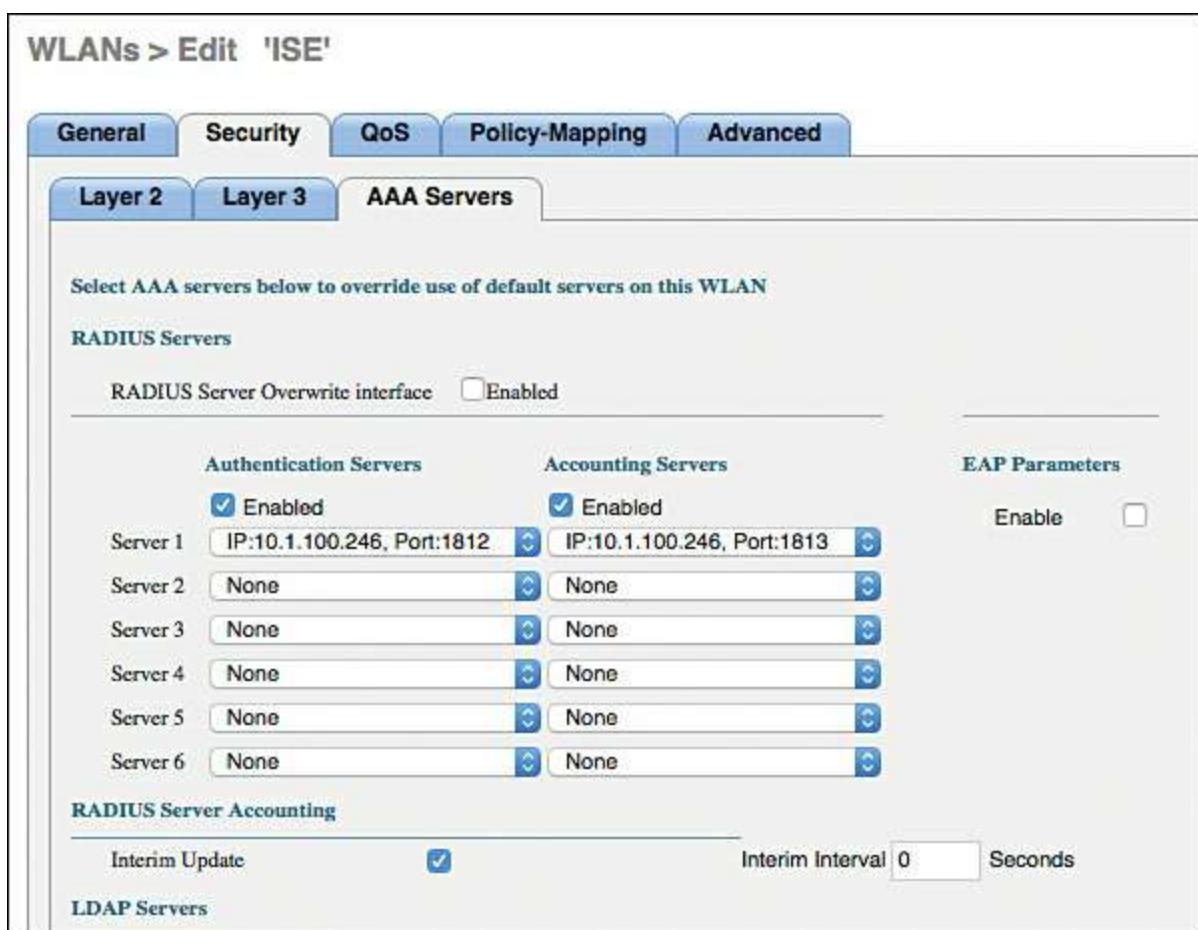
- Step 11.** In the Layer 2 Security field, the default setting of **WPA+WPA2** is correct for this sample configuration.
- Step 12.** Do not check the MAC Filtering check box.
- Step 13.** In the Authentication Key Management section, check the **Enabled** check box for 802.1X.
- Step 14.** Click the **Layer 3** subtab, shown in [Figure 11-28](#).



**Figure 11-28** Layer 3 Security Subtab for ISE Corporate WLAN

**Step 15.** From the Layer 3 Security drop-down list, choose **None**.

**Step 16.** Click the **AAA Servers** subtab, shown in [Figure 11-29](#).



**Figure 11-29** AAA Servers Subtab for ISE Corporate WLAN

The Cisco WLC enables administrators to specify different authentication and accounting servers. However, this configuration is incompatible with an ISE RADIUS server. ISE provides session services that are tied together from the session ID in the authentication packet and the session ID in the accounting packet.

**Step 17.** Check the **Enabled** check box under both Authentication Servers and Accounting Servers and select your respective ISE Policy Service Node(s) in the columns.

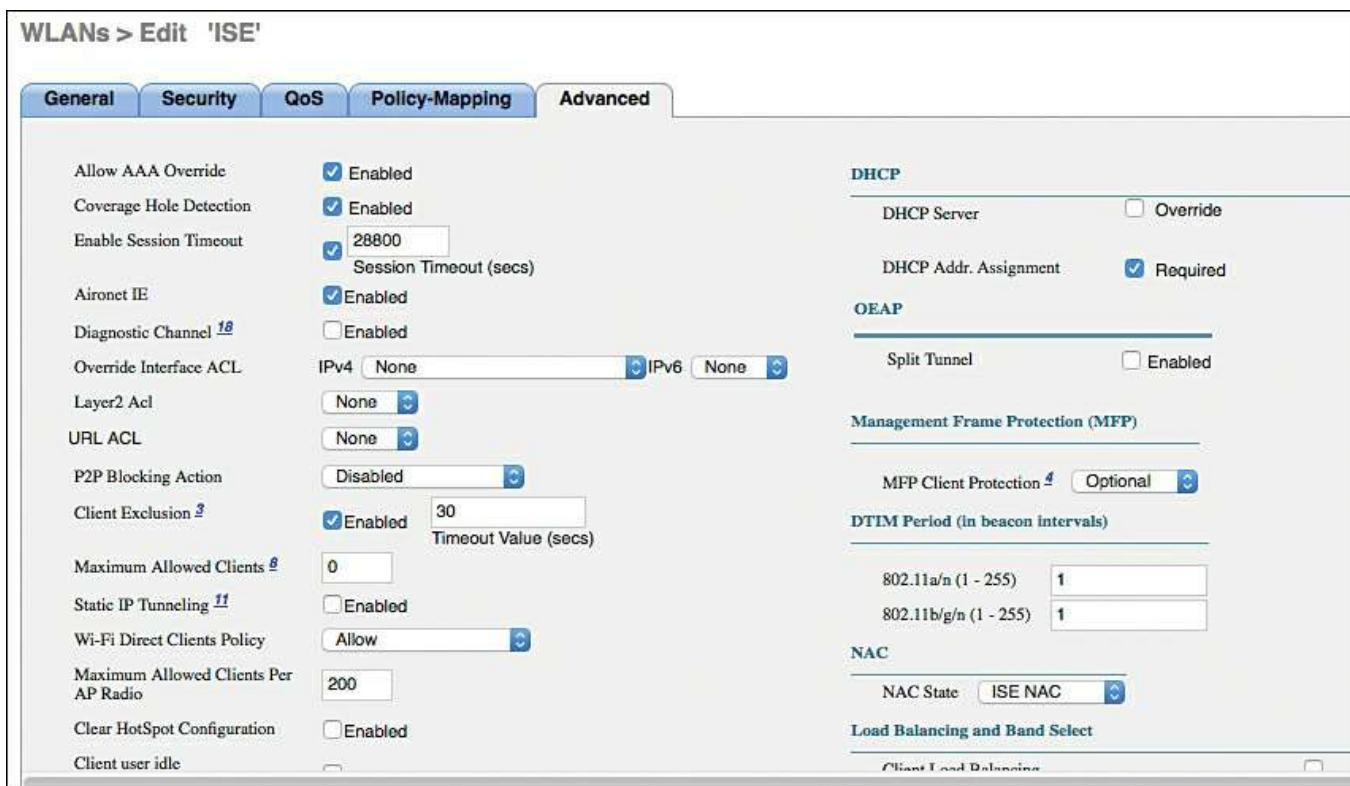
**Step 18.** In the RADIUS Server Accounting section, check the **Enabled** check box to the right of Interim Update.

**Step 19.** Set the Interim Interval to **0** seconds.

**Note** For WLC versions 7.6 and earlier, the recommendation is to disable interim updates (leave the corresponding Enabled check box unchecked). For version 8.0 and later, interim updates should be enabled with an interval of 0 seconds, as specified in Step 19. With this setting, an accounting update is sent only when the client IP address changes. Device Sensor updates are not impacted.

**Step 20.** Click **Apply**.

**Step 21.** Click the **Advanced** tab, the top portion of which is shown in [Figure 11-30](#).



**Figure 11-30** Advanced Tab (Top) for ISE Corporate WLAN

**Step 22.** Check the **Enable** check box for Allow AAA Override.

This enables ISE to assign a VLAN and ACL that are different from those that are configured on the WLAN and interface by default.

**Step 23.** Check the **Enabled** check box for Enable Session Timeout and set the Session Timeout to **28800** seconds.

The default value of 1800 has been known to be too short in many environments.

**Step 24.** In the NAC section, from the NAC State drop-down list, choose **ISE NAC**.

In versions earlier than 8.3, this setting is named Radius NAC instead of ISE NAC. Regardless of the name, this setting is critical for URL Redirection, Centralized Web Authentication (CWA), Posture Assessment, Native Supplicant Provisioning, MDM redirections, and more.

**Step 25.** Check the **Enabled** check box for Client Exclusion and change the Timeout Value to **30** seconds.

**Step 26.** In the DHCP section on the right side of the screen, check the **Required** check box for **DHCP Addr. Assignment**.

This setting is required for the DHCP Device Sensor built into the WLC.

**Step 27.** Scroll down to the middle of the Advanced tab and, under Radius Client Profiling, check both the **DHCP Profiling** and **HTTP Profiling** options, as shown in [Figure 11-31](#).

Note in [Figure 11-31](#) that the Cisco WLC has two different client profiling options: Radius Client Profiling, which sends the attributes to ISE within RADIUS accounting packets, and Local Client Profiling, where the WLC keeps the information and uses it locally. Although the interface appears to offer the option to enable both types of profiling, they are mutually exclusive and cannot be enabled at the same time.

**Off Channel Scanning Defer**

Scan Defer Priority	0	1	2	3	4	5	6	7
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Scan Defer Time(msecs)

**FlexConnect**

FlexConnect Local Switching <sup>2</sup>	<input type="checkbox"/> Enabled
FlexConnect Local Auth <sup>12</sup>	<input type="checkbox"/> Enabled
Learn Client IP Address <sup>5</sup>	<input checked="" type="checkbox"/> Enabled
Vlan based Central Switching <sup>13</sup>	<input type="checkbox"/> Enabled
Central DHCP Processing	<input type="checkbox"/> Enabled
Override DNS	<input type="checkbox"/> Enabled
NAT-PAT	<input type="checkbox"/> Enabled
Central Assoc	<input type="checkbox"/> Enabled

**Lync**

Lync Server	<input type="button" value="Disabled"/>
-------------	---

**11k**

Assisted Roaming Prediction	<input type="checkbox"/>
-----------------------------	--------------------------

**Voice**

Media Session Snooping	<input type="checkbox"/> Enabled
Re-anchor Roamed Voice Clients	<input type="checkbox"/> Enabled
KTS based CAC Policy	<input type="checkbox"/> Enabled

**Radius Client Profiling**

DHCP Profiling	<input checked="" type="checkbox"/>
HTTP Profiling	<input checked="" type="checkbox"/>

**Local Client Profiling**

DHCP Profiling	<input type="checkbox"/>
HTTP Profiling	<input type="checkbox"/>

**PMIP**

PMIP Mobility Type	<input type="checkbox"/>
PMIP NAI Type	<input type="button" value="Hexadecimal"/>
PMIP Profile	<input type="button" value="None"/>
PMIP Realm	<input type="text"/>

**Universal AP Admin Support**

Universal AP Admin	<input type="checkbox"/>
--------------------	--------------------------

**Figure 11-31 Advanced Tab (Middle) for ISE Corporate WLAN**

**Step 28.** Click **Apply** in the upper-right corner.

**Step 29.** Click **Save Configuration** at the top of the screen.

## Summary

This chapter reviewed the best practice configurations for Cisco Catalyst Switches and Cisco Wireless LAN Controllers. It walked you through the configuration of these network access devices for use in all scenarios and all deployment phases of the Secure Unified Access system.

An identity system like this one is so much more than just the Policy Server. The NADs themselves along with their advanced capabilities are absolutely critical to having a successful system. That is why the NAD configurations provided in this chapter are absolutely mission critical to the success of your project.

# Chapter 12 Network Authorization Policy Elements

This chapter covers the following topics:

- ISE network authorization policy elements
- Authorization results

This chapter focuses on exploring network authorization policy elements, with an emphasis on the authorization results policy elements. Cisco ISE network authorization policies are used to define and control a user's or device's access on the network. These policies apply for all access methods: wired, wireless, and VPN.

## ISE Authorization Policy Elements

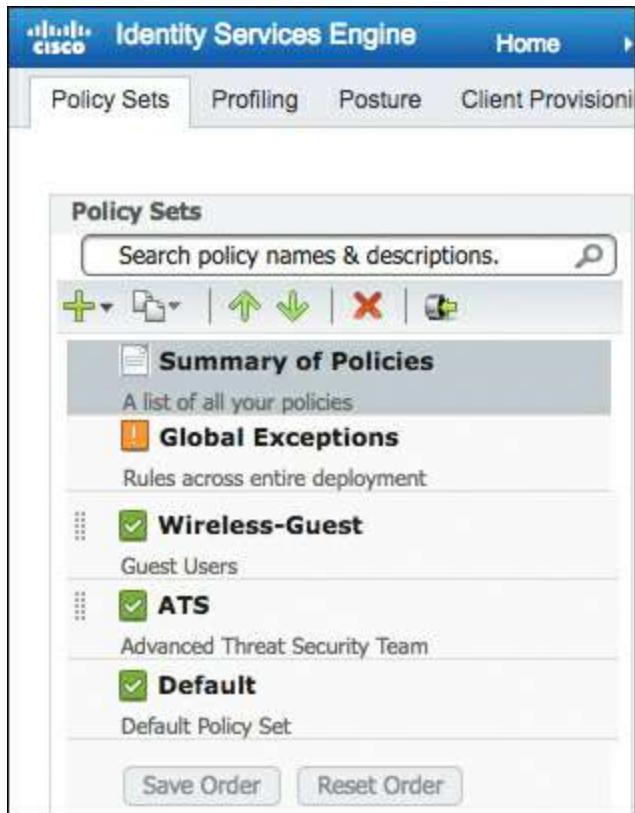
An ISE authorization policy is made up of user-defined policy rules. A policy typically has more than one rule, but this is not required. ISE provides two policy execution options:

- First matched rules apply
- Multiple matched rule applies

The default, first matched rules apply, is by far the most commonly used option in deployments. It works like a firewall ACL in that once a rule is matched, execution stops and no further rule processing occurs. With multiple matched rule applies, ISE evaluates all rules and combines the permissions for all matched rules.

If ISE had only a single policy table for everything, it would get unwieldy fairly quickly. Therefore, ISE has policy sets. Using policy sets enables you, as the administrator, to break up your authentication and authorization policies in multiple separate policies for a specific use case. Together, this is called a policy set. Policy sets can be combined to create a full policy or can be used individually for a specific use case. Policy sets are disabled by default, but it is highly recommended that you enable them in

**Administration > System > Settings > Policy Sets.** [Figure 12-1](#) depicts policy sets.



**Figure 12-1 ISE Policy Sets**

Within an ISE authorization policy, there are three policy types. Each policy has a section at the top for Exceptions, a section for Standard Policies, and a rule at the bottom of the Standard Policies section for Default. The following is a brief explanation of each policy type. [Figure 12-2](#) shows an example of these rule types.

- **Exception Policies:** These policy rules are used to override standard and default policy rules. Exception policy rules are evaluated first and, if matched, take precedence over standard and default rules in the policy. This rule type is usually used when you need to make a temporary change to ISE policy quickly. They are also great for making permanent exceptions for specialized groups, device types, locations, and so on.

Global Exceptions	
Rules across entire deployment	
<input checked="" type="checkbox"/>	Wireless-Guest
Guest Users	
<input checked="" type="checkbox"/>	ATS
Advanced Threat Security Team	
<input checked="" type="checkbox"/>	Default
Default Policy Set	
<a href="#">Save Order</a> <a href="#">Reset Order</a>	

Authorization Policy			
<a href="#">Exceptions (0)</a>			
Standard			
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<a href="#">Edit</a>	<input checked="" type="checkbox"/> Guest Access	If Wireless_Access	then Guests
	<input checked="" type="checkbox"/> Default	If no matches, then	DenyAccess
<a href="#">Save Order</a> <a href="#">Reset Order</a>			

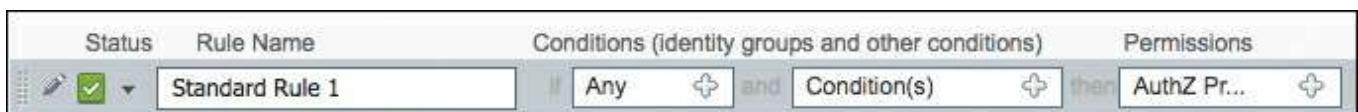
**Figure 12-2 ISE Policy Rule Types**

- **Standard Policies:** These policy rules are the regular/typical rules that you would

spend most of your time writing. They are the core of ISE functionality.

- **Default Rule:** The catch-all rule at the bottom of every authorization policy is the default rule type. If none of the exception or standard policy rules match, then the action specified in the default rule is matched and executed. This rule is typically defined as a simple deny access or permit access but can have any permissions you need instead.

ISE authorization policy rules are made by combining policy elements. Each policy rule within a policy has at least four elements: rule status, rule name, identity groups and conditions, and permissions. This makes up the basic structure of a policy rule. [Figure 12-3](#) shows a generic rule template and the elements within.



**Figure 12-3** ISE Policy Rule Elements

ISE policy rule elements are defined by ISE conditions. Cisco ISE allows you to create conditions as individual and reusable policy elements that can be referred from other rule-based policies. There are two types of conditions:

- **Simple condition:** A simple condition consists of an operand (attribute), an operator (equal to, not equal to, greater than, and so on), and a value. You can save simple conditions and reuse them in other rule-based policies. Simple condition takes the form A operand B, where A can be any attribute from the Cisco ISE dictionary and B is the value(s) that the attribute A can take. For example, Device Type Equals Switch.
- **Compound condition:** A compound condition consists of one or more simple conditions that are connected by the AND or OR operator. Compound conditions are built on top of simple conditions. You can save and reuse compound conditions in other rule-based policies. For example, ((A = B) AND (C = D)), such as ((Device Type = Switch) AND (AD Group = Employees)).

The elements and attributes that you use to create your conditions and policies are stored in the ISE Policy Elements database (**Policy > Policy Elements**). Cisco ISE policy elements are objects that are used in an authorization policy. Cisco ISE policy elements are broken up into three high-level groups:

- **Dictionaries:** The dictionaries contain objects that are used throughout ISE to define conditions, policies, profiles, and more. A dictionary object's purpose is to “teach” ISE how to categorize external data that it either receives (syslog, SNMP trap, RADIUS, and so on) or asks for (polling, AD query, RADIUS, and so on). ISE predefines hundreds of system dictionary objects for you. System-defined

dictionaries are read-only. You cannot create, edit, or delete any system-defined attribute in a system dictionary. For example, ISE includes a predefined CERTIFICATE dictionary, which contains many predefined CERTIFICATE attributes, as shown on the left in [Figure 12-4](#) with the Issuer-Common Name attribute selected. The values and mapping to ISE internal names are shown on the right in [Figure 12-4](#). ISE also allows you to create your own custom dictionary and custom dictionary attributes.

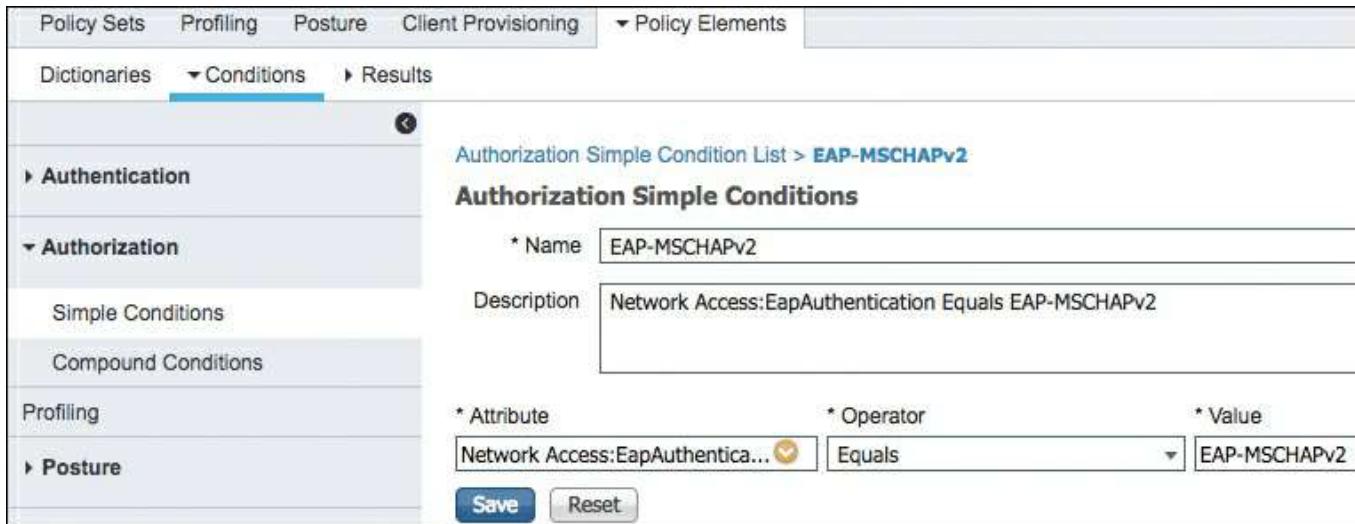
The screenshot shows the ISE web interface under the 'Policy Elements' tab. In the navigation bar, 'Dictionaries' is selected. The main content area displays the 'View Dictionary Attribute' page for the 'CERTIFICATE' dictionary, specifically for the 'Issuer - Common Name' attribute. The left sidebar lists various dictionaries: ACTIVEDIRECTORY\_PROBE, AD-SecurityDemo, APIC, CDP, and CERTIFICATE. Under 'CERTIFICATE', several attributes are listed: Binary Encoded, Days to Expiry, Extended Key Usage - Name, Extended Key Usage - OID, Is Expired, Issuer, and Issuer - Common Name. The 'Issuer - Common Name' attribute is currently selected, highlighted in blue. The right panel shows the attribute details:

* Attribute Name	Issuer - Common Name
Description	Issuer - Common Name
* Internal Name	Issuer - Common Name
* Data Type	STRING
* Dictionary	CERTIFICATE

An unchecked checkbox below the fields says 'Allow attribute multiple times in Authorization Profile'. The 'Allowed Values' section is empty. A table at the bottom lists the allowed values for the 'Issuer - Common Name' attribute, with columns for Name, Value, and is Default.

**Figure 12-4** ISE Dictionary Policy Element

- **Conditions:** Conditions are policy elements that define a simple or compound expression to match against. Authorization Condition policy elements are Dictionary objects used to define a simple or compound expression to match against. Conditions are used in authorization policies as explained previously. [Figure 12-5](#) shows an example of a condition that matches when the value in dictionary element Network Access:EapAuthentication equals EAP-MSCHAPv2. Other common conditions include things such as Active Directory group membership, time of day, and much more. ISE includes some default conditions to speed deployment.



**Figure 12-5** ISE Condition Policy Element

- **Results:** Results are policy elements that define a group of network access control privileges. Authorization policy element Results are used to define and group authorization permissions. These are then referenced in an ISE authorization Policy Rule permissions column. Authorization results are broken into two groups: Authorization Profiles and Downloadable ACLs. Results elements are explained in detail in this chapter.

## Authorization Results

Authorization results define the permissions that are allowed when an authorization policy rule is matched. They are, in general, the RADIUS attributes that will be sent to the network access devices (NAD) to control some aspect of access control for the session. As discussed, authorization results are broken into two groups: authorization profiles and downloadable ACLs. Authorization profiles act like permission templates and, as such, define all of the different access control permissions you want to apply to a matched policy rule. For example, suppose you want to change a matched user's VLAN to contractors and permit them network access. To do this, you would create an authorization profile that includes Access Type set to Access\_Accept and VLAN name set to Contractors. Authorization profiles can include lots of different permissions and permission types. One popular permission is a downloadable access control list (dACL). This section explores dACLs and the other permission controls available in ISE. The basic idea is that you define authorization profiles that contain various permissions and then assign those permissions to an authorization policy rule in a policy set. See [Figure 12-6](#) for an example authorization policy rule showing permissions set to an authorization profile.

<input checked="" type="checkbox"/>	Basic_Authenticated_Acces	If	Network_Access_Authentication_Passed	then	PermitAccess
<input checked="" type="checkbox"/>	Default		If no matches, then		DenyAccess

**Figure 12-6 ISE Authorization Policy Rule with Permissions**

## Configuring Authorization Downloadable ACLs

An ACL is like a firewall policy. It contains a list of access control entries (ACE). dACLs, previously mentioned, are ACLs that can be dynamically downloaded on-demand from ISE to Cisco switches. Once you create a dACL on ISE, the dACL is then added to an authorization profile. Each ACE defines a traffic control rule to permit or deny packets. The syntax for writing ACEs in ISE is just like the syntax you would use to write them on the switch that you are sending them to.

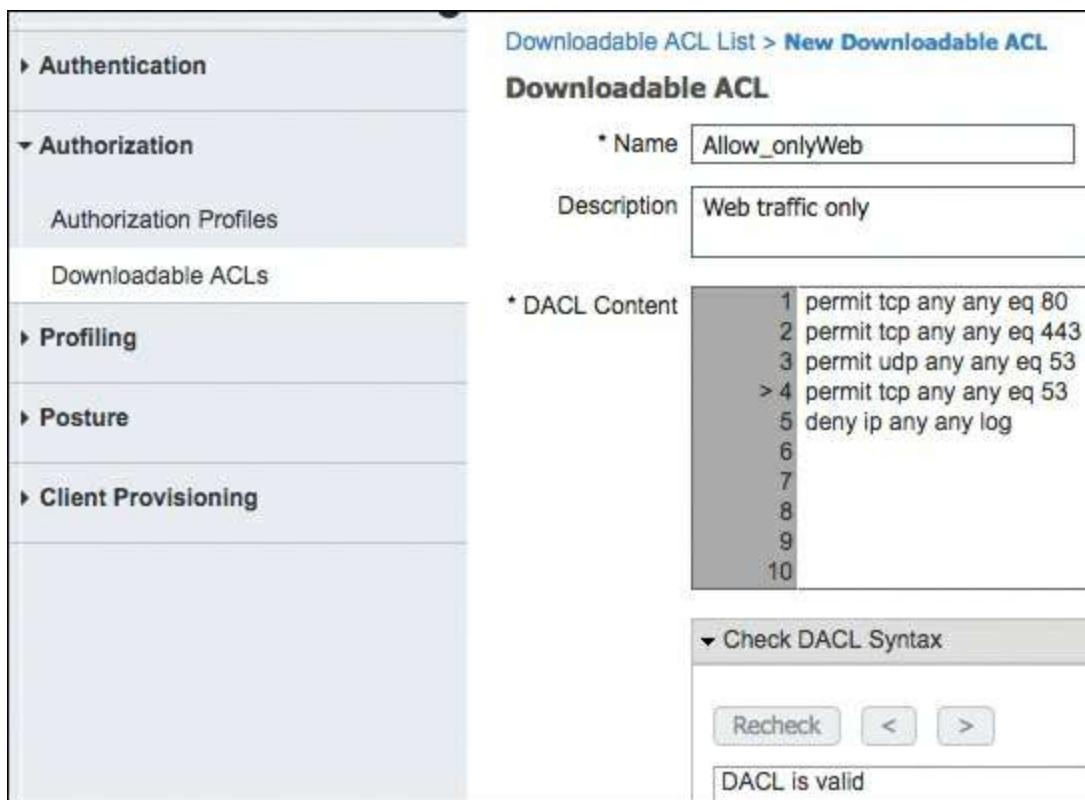
ACEs use the following attributes:

- **Source and destination protocols:** Authentication Header Protocol (**ahp**), Enhanced Interior Gateway Routing Protocol (**eigrp**), Encapsulation Security Payload (**esp**), generic routing encapsulation (**gre**), Internet Control Message Protocol (**icmp**), Internet Group Management Protocol (**igmp**), any Interior Protocol (**ip**), IP in IP tunneling (**ipinip**), KA9Q NOS-compatible IP over IP tunneling (**nos**), Open Shortest Path First routing (**ospf**), Payload Compression Protocol (**pcp**), Protocol-Independent Multicast (**pim**), Transmission Control Protocol (**tcp**), or User Datagram Protocol (**udp**).
- **Source and destination IP address:** The source IP address must always be **any**. The NAD will replace **any** with the source IP address of the connected device. dACLs are only supported on switches; the Cisco Wireless LAN Controller (WLC) uses a different mechanism called Airespace ACLs.
- **Protocol source and destination ports:** Available ports are from 0 to 65535 for TCP and UDP.
- **Remark:** ACL comments.
- **Cisco syntax for a TCP ACL:** `access-list access-list-number {deny | permit} tcp source source-wildcard [operator port] destination destination-wildcard [operator port] [established] [precedence precedence] [tos tos] [fragments] [log] [log-input] [time-range time-range-name] [dscp dscp] [flag]`.
- All ACL have an implicit **deny** at the end of them.
- If you use the **time-range** feature, you must manually configure the time range on the switch. ISE can then call the time-range in the ACL. Be sure to check that the naming matches exactly.

**Note** The **log** keyword should be used sparingly because logging is done in software on the switch. Also, the first packet that triggers the ACL causes a logging message right away, and subsequent packets are collected over 5-minute intervals before they appear as logged. The logging message includes the access list number, whether the packet was permitted or denied, the source IP address of the packet, and the number of packets from that source permitted or denied in the prior 5-minute interval. The **smartlog** keyword at the end of an ACE uses NetFlow records export and therefore may be more efficient on the switch. The ISE syntax checker as of version 2.2 doesn't think it is valid, but it is.

To configure a dACL, go to **Policy > Policy Elements > Results > Authorization > Downloadable ACLs** and click **Add**. You can also duplicate an existing ACL and edit the duplicate.

[Figure 12-7](#) shows an example of an ISE dACL configuration. As you can see, ACL error checking is built into ISE to ensure your syntax is correct.



**Figure 12-7** ISE dACL Example

Cisco ISE includes a basic dACL syntax checker to help to ensure your ACE statements are correct. If you enter malformed syntax and click the Recheck button, the syntax checker will show you the error along with some assistance. The help is very similar to what you would receive at the command-line interface (CLI) of the switch itself.

The dACL syntax checker is able to check for basic ACL fields but does not support all the ACL commands that a particular Cisco switch might support. Therefore, the syntax checker may report an error even if your syntax is correct. The dACL is a free-text field and ISE will send whatever it contains to the device regardless of the syntax checker results. At that point, it is up to you to ensure that your syntax is correct without the help of the syntax checker. If correct, the dACL will work just fine, regardless of the error shown in the syntax checker.

## Configuring Authorization Profiles

An authorization profile acts as a container in which a number of specific permissions allow access to a set of network services. The authorization profile defines a set of permissions to be granted for a network access request. The authorization profile attributes are delivered via RADIUS. The RADIUS code is configured in the profile along with one or more attribute-value pairs (AVP). [Figure 12-8](#) shows one example. The most common permission settings are Access\_Accept/Access Reject, dACL name, Airespace ACL Name, VLAN, and Reauthentication timers.

Standard Authorization Profile Details	
Name	Quarantine user
Description	
Attributes Details	
Access	ACCESS_ACCEPT
Type	
DACL	Limited_Traffic
Name	
Posture	ACL=posture_redirect ( <a href="https://ip:port/portal/gateway?sessionId=SessionIdValue&amp;portal=4cb1f740-e371-11e6-92ce-005056873bd0&amp;action=cpp">https://ip:port/portal/gateway?sessionId=SessionIdValue&amp;portal=4cb1f740-e371-11e6-92ce-005056873bd0&amp;action=cpp</a> )
Discovery	

**Figure 12-8** Authorization Profile Permissions

To configure an authorization profile, go to **Policy > Policy Elements > Results > Authorization > Authorization Profiles** and click **Add**. You can also duplicate an existing profile and then edit it. [Figure 12-9](#) shows an example profile.

Authorization Profiles > Quarantine user

**Authorization Profile**

* Name	Employee_Permissions
Description	Full Access
* Access Type	ACCESS_ACCEPT
Network Device Profile	Cisco
Service Template	<input checked="" type="checkbox"/>
Track Movement	<input type="checkbox"/>
Passive Identity Tracking	<input type="checkbox"/>

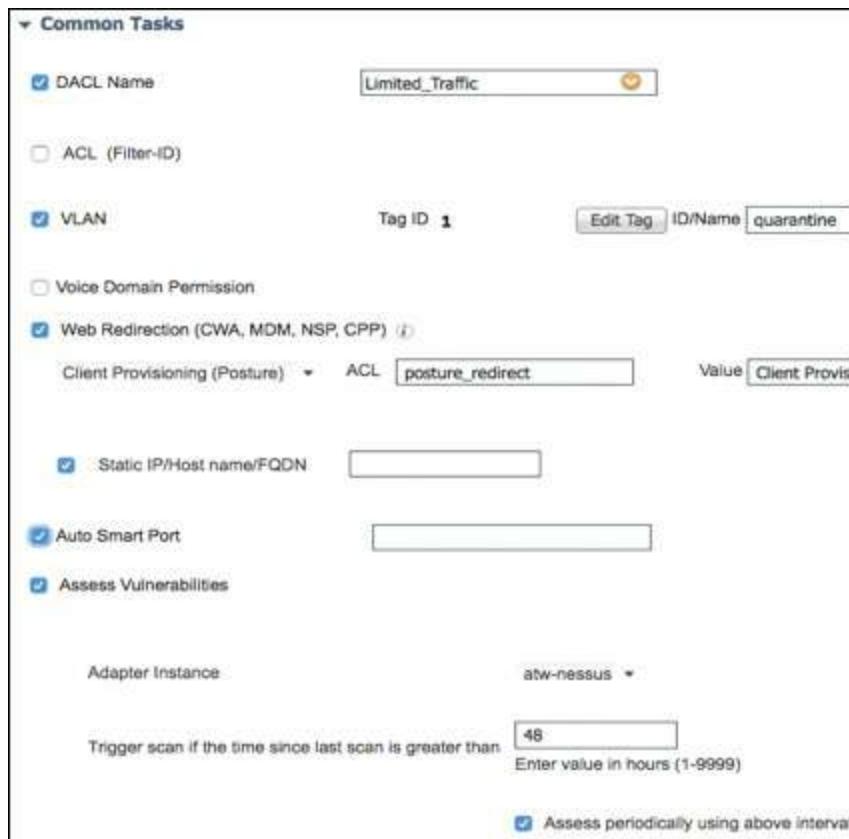
**Figure 12-9 Authorization Profile Example**

[Figure 12-9](#) displays the following authorization profile fields:

- **Name:** Enter a descriptive name; spaces are allowed here, as are ! # \$ % & ‘ ( ) \* + , - . / ; = ? @ \_ { . }
- **Description:** Enter an explanatory description.
- **Access Type:** The only two options are Access\_Accept and Access\_Reject. If you use Access\_Reject, the user is unconditionally denied access to all requested network resources.
- **Service Template:** Checking this check box tells ISE to use the profile name as the SA-NET profile name. SA-NET profiles are configured on newer Cisco switches. Ensure the naming matches exactly between ISE and the switch. Cisco ISE sends the name of the service template to the device, and the device downloads the content (RADIUS attributes) of the template if it does not already have a cached or statically defined version of it. In addition, Cisco ISE sends Change of Authorization (CoA) notifications to the device if a RADIUS attribute was added, removed, or changed in the service template.
- **Track Movement:** ISE can integrate with the Cisco Mobility Services Engine (MSE) to enable device tracking based on physical location. This physical location can then be used in ISE authorization rules to change permissions based on a device’s physical location. A device’s location is reported by MSE once, upon ISE session establishment. However, if you would like to track a device’s movement every 5 minutes, then check this check box. Note that Track Movement could impact the performance of ISE if not used judiciously, so use it sparingly in your policy.
- **Passive Identity Tracking:** If you are using ISE EasyConnect, then you must enable this feature. This enables the EasyConnect process to run and for ISE to issue

CoAs. [Chapter 6](#), “[Quick Setup of an ISE Proof of Concept](#),” covers EasyConnect in more detail.

The final section in the authorization profile is called Common Tasks. This is a collection of the commonly used permissions. They are presented in plain-English format to make it easy for the administrator to configure. In the background, they are translated into RADIUS attributes and AV pairs. [Figure 12-10](#) depicts the Common Tasks list in a profile.



**Figure 12-10** Authorization Profile Common Tasks Partial List

## Summary

ISE authorization is made up of several different elements that work together to create an authorization policy set. These policy sets are then matched against to create a permissions list for an ISE user or device session.

Authorization profiles hold the permissions list returned to a network access device when a RADIUS request is accepted. Cisco ISE provides a mechanism that enables you to configure common tasks to support commonly used permissions and attributes.

Policy elements are components used to define the authorization policy. The policy elements are as follows:

- Dictionaries

- Condition(s)

- Results

These policy elements are referenced when you create policy rules, and your choice of conditions and attributes can create specific types of authorization profiles. A firm understanding of the ISE authorization policy structure and elements is key to a successful ISE deployment.

# Chapter 13 Authentication and Authorization Policies

This chapter covers the following topics:

- Relationship between authentication and authorization
- Authentication policies
- Authorization policies
- Saving attributes for reuse

The previous chapter focused on the levels of authorization you should provide for users and devices based on your logical security policy. You will build policies in ISE that employ network authorization results, such as downloadable access control lists (dACL) and authorization profiles to accommodate the enforcement of that “paper policy.”

These authorization profiles are the end result: the final decision of a login session or a particular stage of a login session.

This chapter examines how to build the authentication and authorization policies that will eventually assign those results that were created in [Chapter 11, “Bootstrapping Network Access Devices.”](#) These policies can be equated to the rules in a firewall and are constructed in a similar fashion.

## Relationship Between Authentication and Authorization

Many IT professionals, especially those with backgrounds in wireless technologies, tend to confuse the terms authentication and authorization and what they actually do. Wireless is used as an example here because it has experienced such tremendous growth over the past few years, and with that growth, security capabilities have increased tremendously. Wireless was the most prevalent use case of 802.1X authentication, and in the vast majority of wireless environments, a user was given full network access as long as her username and password were correct (meaning that authentication was successful).

An authentication is, simply put, “validating credentials.” If you go into a bank and request a withdrawal from an account, the bank teller asks for ID. You pass your driver’s license to the bank teller, and the teller inspects the driver’s license, going through a checklist of sorts:

- Does the picture on the license look like the person in front of the teller’s window?
- Is the license from a recognized authority (i.e., one of the U.S. states or territories)?

Let’s say, for conversation’s sake, that you handed the teller a valid ID (authentication was successful); does that mean you are entitled to the money you asked for?

The next step of the bank teller is to check the account and ensure that the person requesting the withdrawal is entitled to complete that transaction. Perhaps you are allowed to withdraw up to \$1,000, but no more. This is the process of authorization. Just having a successful authentication does not prove entitlement.

This is why most of the time working within a product like ISE is spent setting up and tuning the authorization policy. Authorization is where the bulk of the final decisions are made.

## Enable Policy Sets

An authentication policy leads to an authorization policy. This makes sense, because you cannot authorize someone if you don't know who they are first, right? The ISE user interface is built this way, with the authentication and authorization policies being separate.

However, having just a single authentication policy and a single authorization policy that have to work for all the many different use cases gets to be very cumbersome, hard to navigate, and difficult to troubleshoot.

That is where policy sets come into play. A policy set is a separate pair of authentication and authorization rules. Back in the ACS 5.x days, we called it "service selection rules." Policy sets were introduced in ISE version 1.2. Many of us who have a lot of experience deploying 802.1X in networks have said that policy sets were the only way to deploy successfully.

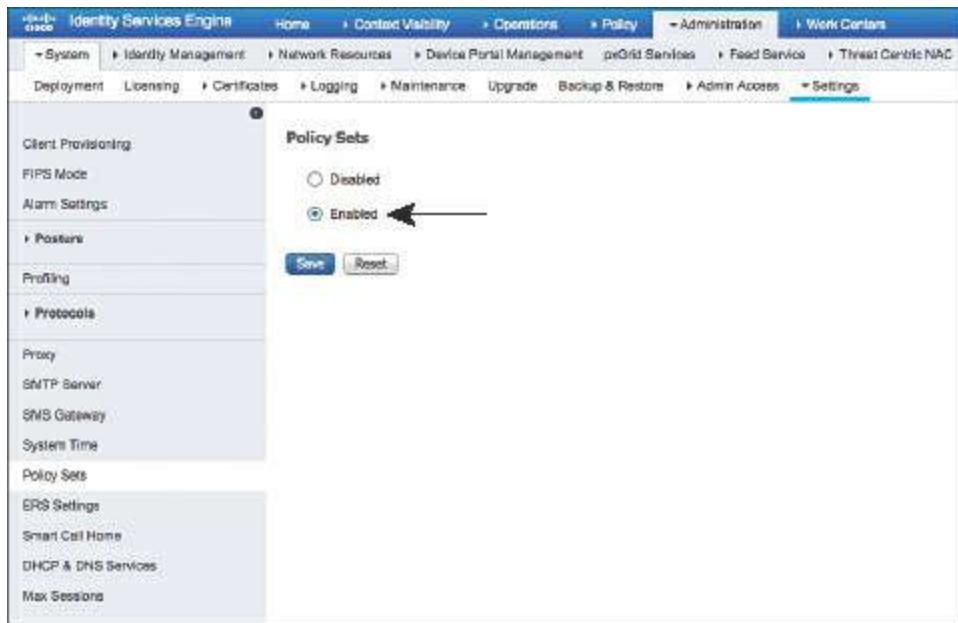
For instance, let's assume there is a wireless LAN (WLAN) named WOLAND-GUEST for all guest users to use, and a completely different WLAN named WOLAND-CORP for employees to use. Those two distinct networks will have completely different policies assigned to them. Different authentication types would be expected on the guest network, as well as different authorizations assigned to the users who join those networks.

By leveraging policy sets, we can organize our policies so that the guest policies are completely separate from the employee policies in the ISE GUI. This helps us keep logical separation in our own management of the solution, but also enables easier troubleshooting as well.

By changing the ISE GUI to start using policy sets, we are following Cisco TAC and TME best practices, and we are simultaneously helping this book along by adding in the illustration of the relationship between authentications and authorizations.

From the ISE GUI, navigate to **Administration > System > Settings > Policy Sets**, click **Enabled**, as shown in [Figure 13-1](#), and then click **Save**. When you click **Save**, you will be logged out of the GUI so that the GUI framework may be reinitialized with the correct policy set model. This is not a reboot of the appliance, just a log-off and re-

login instead.



**Figure 13-1** Enabling Policy Sets

Log back into ISE and you will see Policy Sets under the Policy menu, as well as any of the Work Centers where the authentication and authorization polices are applicable.

Navigate to **Work Centers > Network Access > Policy Sets**, or **Policy > Policy Sets** as shown in [Figure 13-2](#). As you see in [Figure 13-2](#), there is a summary of all the policy sets that exist in the main window on the right side, while you can add, move, and create new policy sets on the left side.



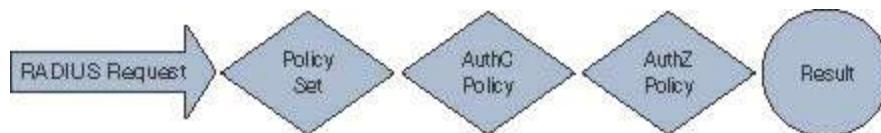
**Figure 13-2** Policy Sets Overview

Click the **Default** policy set on the left side to see the authentication and authorization policies expand on the right side, as shown in [Figure 13-3](#).

The screenshot shows the Cisco Identity Services Engine (ISE) interface. On the left, there's a sidebar with 'Policy Sets' and a search bar. Below it are sections for 'Summary of Policies', 'Global Exceptions', and 'Default'. The 'Default' section is selected. At the bottom of the sidebar are 'Save Order' and 'Reset Order' buttons. The main content area is titled 'Default' and 'Default Policy Set'. It contains two main sections: 'Authentication Policy' and 'Authorization Policy'. Under 'Authentication Policy', there are rules for MAB and Dot1X. Under 'Authorization Policy', there are many rules for exceptions like 'Wireless Black List Default', 'Profiled Cisco IP Phones', and 'Compliant\_Devices\_Access'. Each rule has conditions and permissions. At the bottom of the main panel are 'Save' and 'Reset' buttons.

**Figure 13-3** Default Policy Set

Notice the flow in [Figure 13-3](#). An incoming RADIUS request matches a top-level rule, where the policy set is determined. The next step is to process the authentication followed by the authorization. [Figure 13-4](#) illustrates that flow.



**Figure 13-4** Overview of Policy Sets Flow

The incoming network access request will be processed by the designated authentication policy, which leads to the authorization policy. It is the authorization result that dictates if access is granted and, if so, what is allowed and what is not.

## Authentication Policy Goals

Authentication policies have the following goals, but the ultimate end goal of an authentication policy is to determine if the identity credential is valid or not:

1. Drop incoming requests that aren't allowed and prevent them from taking up any more processing power.

2. Route authentication requests to the correct identity store (sometimes called a policy information point [PIP]).
3. Validate the identity.
4. Pass successful authentications through to the authorization policy.

## Accept Only Allowed Protocols

By default, ISE allows nearly all supported authentication protocols. However, it would behoove the organization to lock this down to only the ones that are expected and supported. This serves a few purposes: keep the load on the PSNs down and use the authentication protocol to help choose the right identity store.

## Route to the Correct Identity Store

Once the authentication request is accepted, ISE makes a routing decision. The identity store that should be checked is based on the incoming authentication request. Obviously, if a certificate is being presented, ISE should not try and validate that certificate against the internal user database.

If your company has multiple lines of business, it may also have more than one Active Directory domain or more than one LDAP store. Using attributes in the authentication request, you can pick the correct domain or LDAP store.

## Validate the Identity

After the correct identity store has been identified, ISE confirms the credentials are valid. If it's a username and password, ISE checks whether they match what is in the directory store. If it's a certificate, ISE checks whether it trusts the certificate signer and whether the certificate has been revoked.

## Pass the Request to the Authorization Policy

If the authentication failed, the policy can reject the request without wasting the CPU cycles required to compare the request to the authorization policy. Also, if the request did not match any of the configured rules, should a reject message be sent? However, when the request passes authentication, it is now time for the hand-off to the authorization policy.

## Understanding Authentication Policies

Now that you understand the four main responsibilities of the authentication policy, it will be easier to understand why you are doing the things that are introduced in this section.

Something we like to call “smart defaults” were added to the product beginning with

Cisco ISE 1.4 and enhanced further in each release. These settings are designed to make it very quick and easy to start using ISE immediately after the install completes. In fact, with ISE 2.0, the authors of this book can have the entire system set up all the way through BYOD onboarding in less than 20 minutes thanks to these smart default settings.

To help you understand authentication policies and smart defaults in more depth, this section examines some of the default policies and takes a deeper look at the out-of-the-box settings.

From the ISE GUI, navigate to **Work Centers > Network Access > Policy Sets > Default**, or **Policy > Policy Sets**, as displayed previously in [Figure 13-3](#).

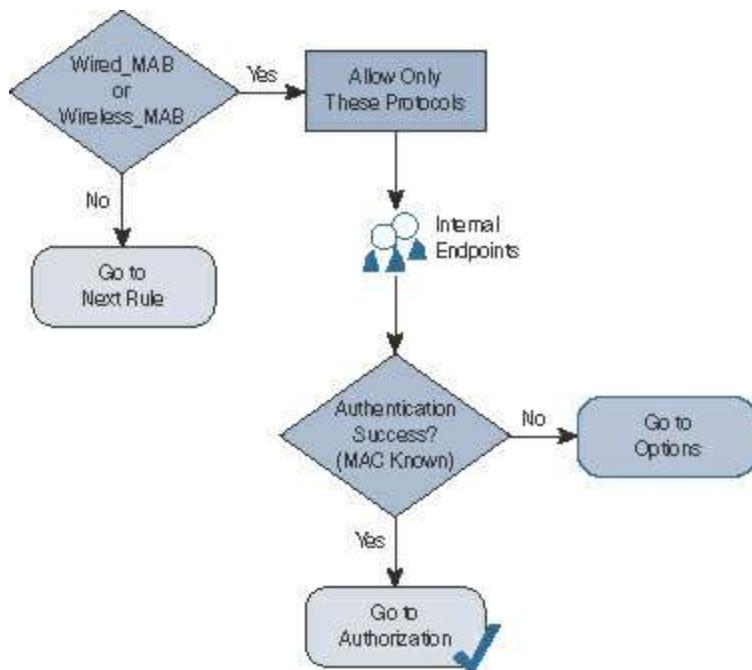
Basic authentication policy rules are logically organized in this manner:

**IF conditions THEN ALLOW PROTOCOLS IN AllowedProtocolList  
AND CHECK THE IDENTITY STORE IN LIST IdentityStore**

Rules are processed in a top-down, first-match order, just like a firewall policy or an access list. So, if the conditions do not match, the authentication is compared to the next rule in the policy.

As shown in the upper-right quadrant of [Figure 13-3](#), ISE is preconfigured with a default rule for MAC Authentication Bypass (MAB). Use this rule to dig into authentication rules and how they work. If you have a live ISE system, it may help to follow along with the text.

[Figure 13-5](#) demonstrates the MAB rule in flowchart format.



**Figure 13-5 MAB Rule Flow Chart**

## Conditions

As [Figures 13-4](#) and [13-5](#) indicate, the conditions of this MAB rule state, “If the authentication request is Wired\_MAB or Wireless\_MAB, it matches this rule.” You can expand these conditions by hovering your mouse pointer over the conditions in ISE and clicking the target icon that appears or by looking directly at the authentication conditions shown in the following steps:

**Step 1.** Navigate to **Work Centers > Network Access > Policy Elements > Conditions > Authentication Compound Conditions.**

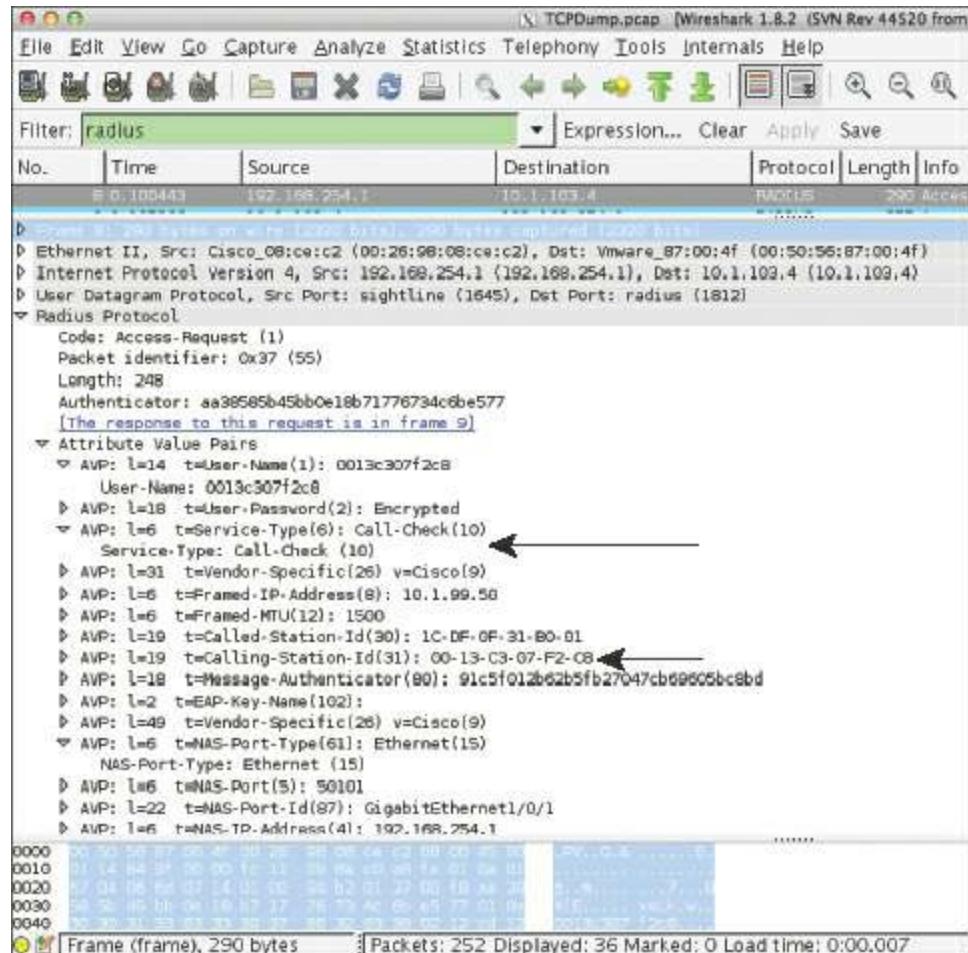
**Step 2.** Select **Wired\_MAB**.

As you can see in [Figure 13-6](#), the Wired\_MAB condition is mapped to different dictionary attributes per network device vendor.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine', 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', 'Work Centers', 'Network Access', 'Guest Access', 'TrustSec', 'BYOD', 'Profilier', 'Posture', 'Device Administration', 'PassiveID', 'Overview', 'Identities', 'Id Groups', 'Ext Id Sources', 'Network Resources', 'Policy Elements' (which is selected), 'Policy Sets', 'Troubleshoot', 'Reports', 'Settings', and 'Dictionaries'. The main content area is titled 'Authentication Compound Conditions - All Profiles'. A sidebar on the left lists 'Conditions' (Authentication Simple Conditions, Authentication Compound Cond..., Authorization Simple Conditions, Authorization Compound Cond..., Time and Date Conditions) and 'Results'. The main pane displays the 'Wired\_MAB' condition details: Name: Wired\_MAB, Description: 'A condition to match MAC Authentication Bypass service based authentication requests from switches, according to the corresponding MAB attributes defined in the device profile.', and a note: 'During policy rule evaluation the authentication condition will be determined dynamically, from the network device's profile configuration.' Below this, a section titled 'Select a network device profile to view current attribute details:' shows buttons for 'Cisco', 'AlcatelWired', 'HPWired', 'BrocadeWired', and 'HPWired\_SNMP\_CoA'. Under the Cisco button, it says 'Radius:NAS-Port-Type = Ethernet' and 'Radius:Service-Type = Call Check'. A note below states: 'These Network Device Profiles have not been configured for this flow. Therefore, this condition is not applicable to devices associated with these profiles. Click to view: ArubaWireless, MotorolaWireless, RuckusWireless, HPWireless'. A 'close' button is at the bottom.

**Figure 13-6** Wired\_MAB Condition for Cisco Network Device Profile

For Cisco, the condition is looking for the RADIUS NAS-Port-Type to be Ethernet and Service-Type to be Call Check. This combination of attributes from the RADIUS authentication packet notifies ISE that it is a MAB request from a switch. [Figure 13-7](#) highlights these key attributes in a packet capture of the MAB authentication request.



**Figure 13-7** Packet Capture of Wired MAB

It's important to note that different vendors will use different attributes. The same compound condition will get mapped to different attributes so it may be leveraged by different network vendors without requiring separate policies.

[Figure 13-8](#) shows the settings after clicking BrocadeWired. Brocade switches send MAB requests using a Service-Type of Framed, which is the same Service-Type that many vendors use for 802.1X authentications.

**Note** The RADIUS Service-Type attribute is supposed to define the type of RADIUS request, and a unique one would be used for each authentication request type. However, MAB is not a standard and therefore there is no set attribute to use.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes links for Home, Context Visibility, Options, Policy, Administration, and Work Centers. Under Work Centers, Network Access, Guest Access, TrustSec, BYOD, Profile, Posture, Device Administration, and Identity Providers are listed. Below these, Overview, Identities, Id Groups, Ext Id Sources, Network Resources, Device Groups, Policy Elements (which is selected and highlighted in blue), Policy Sets, Troubleshoot, and Reports are shown. On the left, a sidebar titled 'Conditions' lists 'Authentication Simple Conditions', 'Authentication Compound Cond...', 'Authorization Simple Conditions', 'Authorization Compound Cond...', and 'Time and Date Conditions'. Below this is a 'Results' section which is currently empty. The main content area is titled 'Authentication Compound Conditions - All Profiles'. It displays a condition named 'Wired\_MAB' with the following details:  
Name: Wired\_MAB  
Description: A condition to match MAC Authentication Bypass service based authentication requests from switches defined in the device profile.  
During policy rule evaluation the authentication condition will be determined dynamically, from the network device's profile configuration.  
Select a network device profile to view current attribute details:  
Buttons: Cisco, BrocadeWired, HPWireless, BrocadeWireless, HPWireless\_MAB\_Gui.  
Listed attributes:  
Radius:NAS-Port-Type = Ethernet  
Radius:Service-Type = Framed  
Radius:User-Name = Radius:Calling-Station-ID  
View BrocadeWired Network Device Profile  
A note below states: 'These Network Device Profiles have not been configured for this flow. Therefore, this condition is not applicable to devices associated with these profiles. Click to view: ...'  
Listed vendor names: ArubaWireless, MotorolaWireless, RuckusWireless, HPWireless.  
A 'Done' button is at the bottom.

**Figure 13-8** Wired\_MAB Condition for BrocadeWired Network Device Profile

To see the different vendor mappings, click the network device vendor name; however, the main focus of this book is on the Cisco network devices.

**Step 3.** Navigate to **Work Centers > Network Access > Policy Elements > Conditions > Authentication Compound Conditions.**

**Step 4.** Select **Wireless\_MAB**.

As shown in [Figure 13-9](#), Wireless\_MAB is similar to Wired\_MAB; however, it uses a NAS-Port-Type of Wireless - IEEE 802.11. This combination of attributes from the RADIUS authentication packet tells ISE that it is a MAB request from a wireless device.

## Authentication Compound Conditions - All Profiles

Name Wireless\_MAB  
Description A condition to match MAC Authentication Bypass service based authentication requests from wireless LAN MAB attributes defined in the device profile.

During policy rule evaluation the authentication condition will be determined dynamically, from the network device's profile configuration.

Select a network device profile to view current attribute details:

[Cisco](#)

[ArubaWireless](#)

[MotorolaWireless](#)

[RuckusWireless](#)

[HPWireless](#)

Radius:NAS-Port-Type = Wireless - IEEE 802.11

Radius:Service-Type = Call Check

[View Cisco Network Device Profile](#)

 These Network Device Profiles have not been configured for this flow.

Therefore, this condition is not applicable to devices associated with these profiles. Click to view: :

[AlcatelWired](#)

[HPWired](#)

[BrocadeWired](#)

[HPWired\\_SNMP\\_CoA](#)

[close](#)

**Figure 13-9** Wireless\_MAB Condition for Cisco Network Device Profile

## Allowed Protocols

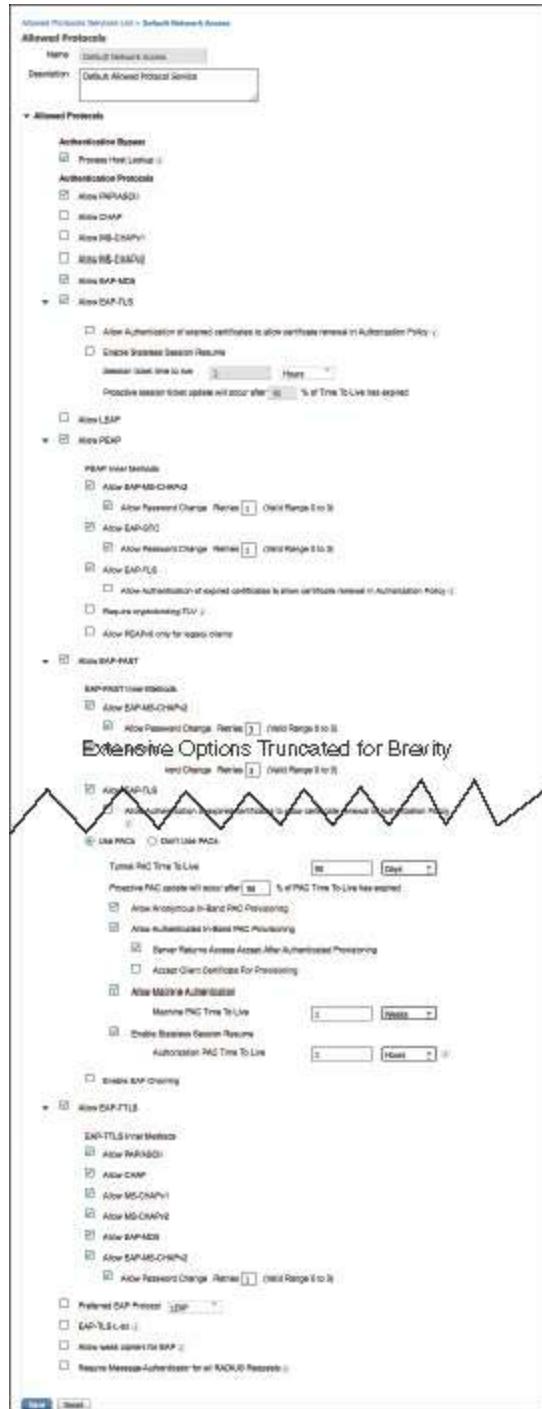
After the conditions are matched, the rule now dictates what authentication protocols are permitted. Looking at the predefined MAB rule, this rule uses the Default Network Access list of allowed protocols (which is almost every supported authentication protocol).

Let's examine the default allowed protocols. From the ISE GUI, perform the following steps:

**Step 1.** Navigate to **Work Centers > Network Access > Policy Elements > Results > Allowed Protocols.**

**Step 2.** Select **Default Network Access.**

As you can see in [Figure 13-10](#), the list of supported protocols and their options is extensive. This default list is inclusive with the intention of making deployments work easily for customers, but security best practice is to lock this down to only the protocols needed for that rule.



**Figure 13-10 Default Network Access**

## Authentication Protocol Primer

This section examines the most common authentication protocols seen in most environments, so you can create a more specific list of allowed protocols for your deployment. Let's follow the Allowed Protocols list shown in [Figure 13-10](#), from the top down:

- **PAP:** Password Authentication Protocol. The username is sent in the clear, and the password is optionally encrypted. PAP is normally used with MAB, and some

devices use PAP for web authentications. We recommend you enable this for the MAB rule only and disable PAP for any authentication rules for real authentications. Checking the check box for Detect PAP as Host Lookup allows PAP authentications to access the internal endpoints database. If this check box is not checked, MAB does not work.

- **CHAP:** Challenge Handshake Authentication Protocol. The username and password are encrypted using a challenge sent from the server. CHAP is not often used with network access; however, some vendors send MAB using CHAP instead of PAP.

Checking the check box for Detect CHAP as Host Lookup allows CHAP authentications to access the internal endpoints database. If this check box is not checked, MAB does not work.

- **EAP:** Extensible Authentication Protocol has a host of flavors, which are discussed in the sections that follow.

## Extensible Authentication Protocol (EAP) Types

EAP is an authentication framework providing for the transport and usage of identity credentials. EAP encapsulates the usernames, passwords, and certificates that a client is sending for purposes of authentication. There are many different EAP types, each of which has its own benefit and downside. As an interesting side note, 802.1X defines EAP over LAN (EAPoL).

- **EAP-MD5:** Uses a Message Digest algorithm to hide the credentials in a hash. The hash is sent to the server, where it is compared to a local hash to see if the credentials are accurate. However, EAP-MD5 does not have a mechanism for mutual authentication. That means the server validates the client, but the client does not authenticate the server (i.e., does not check to see if it should trust the server). EAP-MD5 is common on some IP phones, and some switches may send MAB requests within EAP-MD5. Checking the check box for Detect EAP-MD5 as Host Lookup allows EAP-MD5 authentications to access the internal endpoints database. Without this check box checked, MAB does not work.

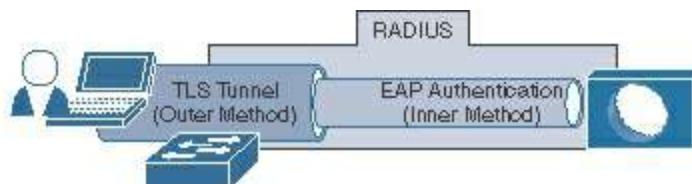
- **EAP-TLS:** Uses Transport Layer Security to provide the secure identity transaction. This is similar to Secure Sockets Layer (SSL) and the way encryption is formed between your web browser and a secure website. EAP-TLS has the benefit of being an open IETF standard, and it is considered universally supported. EAP-TLS uses X.509 certificates and provides the ability to support mutual authentication, where the client must trust the server's certificate, and vice versa. It is considered among the most secure EAP types, because password capture is not an option; the endpoint must still have the private key. EAP-TLS has solidified

itself as the EAP type of choice when supporting BYOD in the enterprise.

## Tunneled EAP Types

The EAP types previously described transmit their credentials immediately. These next three EAP types form encrypted tunnels first and then transmit the credentials within the tunnel (see [Figure 13-11](#)):

- **PEAP:** Protected EAP. Originally proposed by Microsoft, this EAP tunnel type has quickly become the most popular and widely deployed EAP method in the world. PEAP forms a potentially encrypted TLS tunnel between the client and server, using the X.509 certificate on the server in much the same way the SSL tunnel is established between a web browser and a secure website. After the tunnel is formed, PEAP uses one of the EAP types listed next as an inner method, authenticating the client using EAP within the outer tunnel:
  - **EAP-MS-CHAPv2:** When using this inner method, the client's credentials are sent to the server encrypted within an MS-CHAPv2 session. This is the most common inner method, as it allows for simple transmission of username and password, or even computer name and computer passwords, to the RADIUS server, which in turn authenticates them to Active Directory.
  - **EAP-GTC:** EAP-Generic Token Card. This inner method created by Cisco as an alternative to MS-CHAPv2 allows generic authentications to virtually any identity store, including one-time password (OTP) token servers, LDAP, NetIQ eDirectory (formerly Novell), and more.
  - **EAP-TLS:** Although rarely used and not widely known, PEAP is capable of using EAP-TLS as an inner method.



**Figure 13-11** Tunneled EAP Types (PEAP and FAST)

- **EAP-FAST:** EAP Flexible Authentication via Secure Tunnel. This is similar to PEAP. FAST was created by Cisco as an alternative to PEAP that allows for faster reauthentications and supports faster wireless roaming. Just like PEAP, FAST forms a TLS outer tunnel and then transmits the client credentials within that TLS tunnel. Where FAST differs from PEAP is the ability to use Protected Access Credentials (PAC). A PAC can be thought of like a secure cookie, stored locally on the host as "proof" of a successful authentication.
- **EAP-MS-CHAPv2:** When using this inner method, the client's credentials are

sent to the server encrypted within an MS-CHAPv2 session. This is the most common inner method, as it allows for simple transmission of username and password, or even computer name and computer passwords, to the RADIUS server, which in turn authenticates them to Active Directory.

- **EAP-GTC:** EAP-Generic Token Card. This inner method was created by Cisco as an alternative to MS-CHAPv2 that allows generic authentications to virtually any identity store, including OTP token servers, LDAP, NetIQ eDirectory, and more.
- **EAP-TLS:** EAP-FAST is capable of using EAP-TLS as an inner method. This became popular with EAP chaining.
- **EAP Chaining with EAP-FASTv2:** As an enhancement to EAP-FAST, a differentiation was made to have a user PAC and a machine PAC. After a successful machine authentication, ISE issues a machine PAC to the client. Then, when processing a user authentication, ISE requests the machine PAC to prove that the machine was successfully authenticated, too. This is the first time in 802.1X history that multiple credentials have been able to be authenticated within a single EAP transaction, and it is known as EAP chaining. The IETF is creating a new open standard based on EAP-FASTv2 and, at the time of writing, is to be referred to as EAP-TEAP (tunneled EAP), which should eventually be supported by all major vendors.
- **EAP-TTLS:** EAP Tunneled Transport Layer Security. This is also similar to PEAP and EAP-FAST, as it too establishes an outer TLS tunnel to then pass the identity credentials securely within that tunnel. While EAP-FAST is most often credited as a Cisco EAP type, and PEAP is often credited to Microsoft, EAP-TTLS is always credited to Funk Software, which was acquired by Juniper. EAP-TTLS is most often found in Juniper UAC deployments and sometimes in European education networks that use a solution called eduroam (education roaming). As with all tunneled EAP types, numerous inner methods can be used within the tunnel, such as:
  - PAP/ASCII
  - CHAP
  - MS-CHAPv1
  - MS-CHAPv2
  - EAP-MD5
  - EAP-MS-CHAPv2

## Certificate Renewal for EAP-TLS

Whether using EAP-TLS by itself or as an inner method, one fact holds true: user

certificates can and do expire. In that case, a user or computer needs to request a new certificate. When the computer is managed by an endpoint manager, such as Active Directory, it typically takes care of the renewal of certificates. However, when the certificate is issued via a BYOD onboarding mechanism, there is nothing within the authentication protocol (PEAP or EAP-TLS) that handles renewing the certificate. Instead, the user must be run through the BYOD onboarding process another time and issued another certificate.

Part of certificate validation during an authentication is to ensure the certificate is valid. If a certificate has expired, it is no longer considered valid. That poses a chicken-and-egg problem for an ISE administrator. The endpoint may have to allow the certificate to expire before allowing it to be renewed, yet an expired certificate will fail authentication and therefore shouldn't be permitted for use with network access.

To address this problem, there is a setting under all EAP-TLS methods in the Allowed Protocols list to allow authentication of expired certificates to allow certificate renewal in the authorization policy, as shown in [Figure 13-12](#). Checking this check box instructs ISE to still permit access with an expired certificate to enable the end user to go through the onboarding process again.



**Figure 13-12** Allowing Authentication of Expired Certificates

## Identity Store

After processing the allowed protocols, the authentication request is then authenticated against the chosen identity store, or in this case of MAB, it is compared to the internal endpoints database (list of MAC addresses stored locally on ISE).

If the MAC address is known, it is considered to be a successful MAB (notice it was not termed successful authentication). MAB is exactly that, bypassing authentication, and it is not considered a secure authentication.

The selected identity source may also be an identity source sequence, which attempts a series of identity stores in order.

## Options

Every authentication rule has a set of options stored with the identity store selection. These options tell ISE what to do if an authentication fails, if the user/device is

unknown, or if the process fails. The options are Reject, Continue, and Drop:

- **Reject:** Send Access-Reject back to the NAD.
- **Continue:** Continue to the authorization policy regardless of authentication pass/fail. (Used with web authentication.)
- **Drop:** Do not respond to the NAD; NAD will treat as if RADIUS server is dead.

## Common Authentication Policy Examples

This section considers a few quick examples of authentication policies, based on common use cases or simply because they are interesting.

### Using the Wireless SSID

One of the most common authentication policy requests that the authors get is to treat authentications differently based on the SSID of the wireless network. Creating the policy is not difficult; what becomes challenging is the identification of the attribute to use, because Source-SSID is not a field in a RADIUS packet. In fact, RADIUS was designed before Wi-Fi and therefore one of the existing RADIUS attributes is overloaded with additional use cases, such as identifying the SSID. The RADIUS attribute commonly used is Called-Station-ID. That is the field used to identify the wireless SSID name.

Beginning with ISE version 2.1, a new authentication dictionary was added to ISE, called normalized RADIUS. Cisco created this dictionary to make the creation of policies like this one easier, across the gamut of network devices, because different network device vendors may use different attributes to identify the SSID. Now, by using the Normalized RADIUS > SSID dictionary object, you can create one rule that looks for a specific SSID, and have that rule match for Cisco, Aruba, Ruckus...you name it. The translation is done in the background to match whatever is defined in the network device profile for the vendor.

For this example, let's build a rule for an SSID named CiscoPress. This rule will be configured to

- Only match authentications coming from that SSID
- Allow only EAP-FAST authentications
- Utilize EAP chaining
- Authenticate against Active Directory

From the ISE GUI, perform the following steps:

**Step 1.** Navigate to **Work Centers > Network Access > Policy Sets**.

**Step 2.** Select the **Default** policy set.

**Step 3.** In the Authentication Policy section, insert a new rule above the preconfigured Dot1X rule.

**Step 4.** Provide a name for the rule. For purposes of this example, name it **CiscoPress SSID**.

**Step 5.** For the condition, choose **Normalized RADIUS > SSID**.

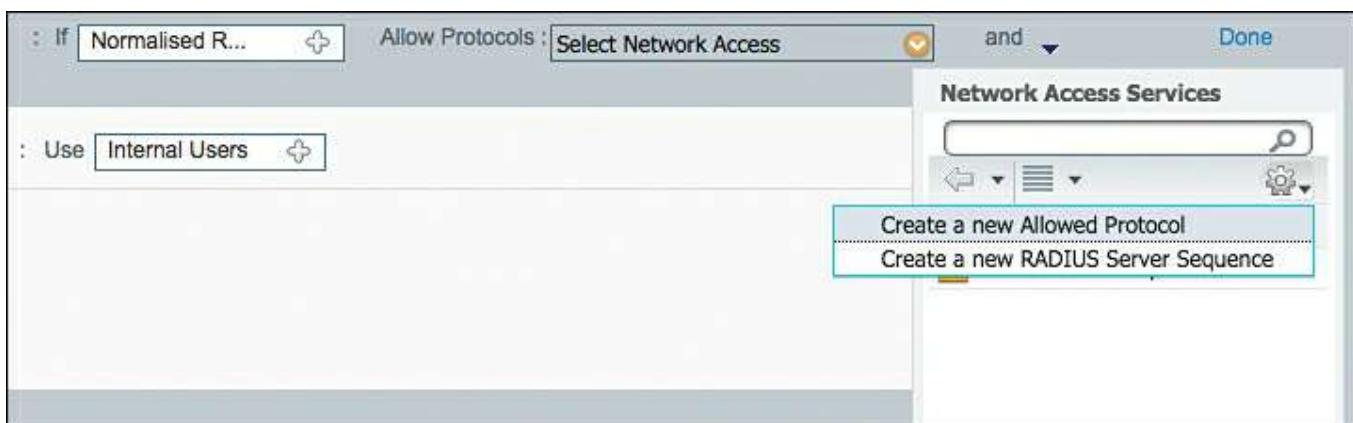
**Step 6.** Select **Contains** from the middle drop-down under Description.

**Step 7.** Type the SSID name in the text box. [Figure 13-13](#) shows the condition.



**Figure 13-13** SSID Contains CiscoPress

**Step 8.** Create a new allowed protocol object that only allows EAP-FAST, as shown in [Figure 13-14](#). Select the drop-down for Allowed Protocols.



**Figure 13-14** Creating a New Allowed Protocol

**Step 9.** Click the cog icon and choose **Create a New Allowed Protocol**.

**Step 10.** In the Name text box, enter a name of the new allowed protocol (**EAP-FAST Only** for purposes of this example).

**Step 11.** (Optional) Provide a description.

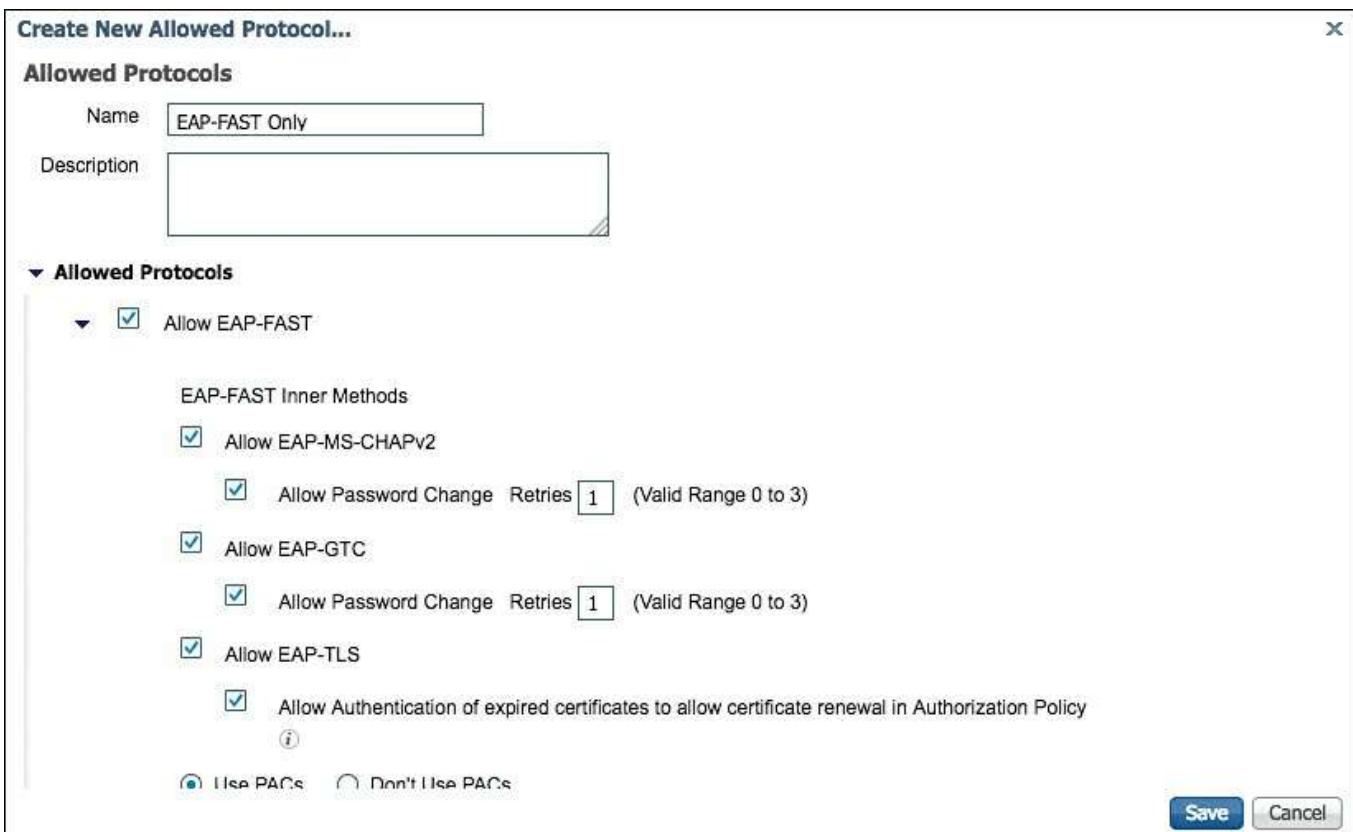
**Step 12.** Working top-down, ensure that all the check boxes are unchecked until you reach Allow EAP-FAST.

**Step 13.** Check the **Allow EAP-FAST** check box (if it isn't already checked).

**Step 14.** For ease of use, enable EAP-MS-CHAPv2, EAP-GTC, and EAP-TLS for inner methods by checking the corresponding check boxes under EAP-FAST Inner Methods.

**Step 15.** Click the **Use PACs** radio button for faster session re-establishment, and to allow EAP chaining.

[Figure 13-15](#) shows the EAP-FAST settings for the new Allowed Protocols definition.



**Figure 13-15** Adding a New Protocol to Allowed Protocols

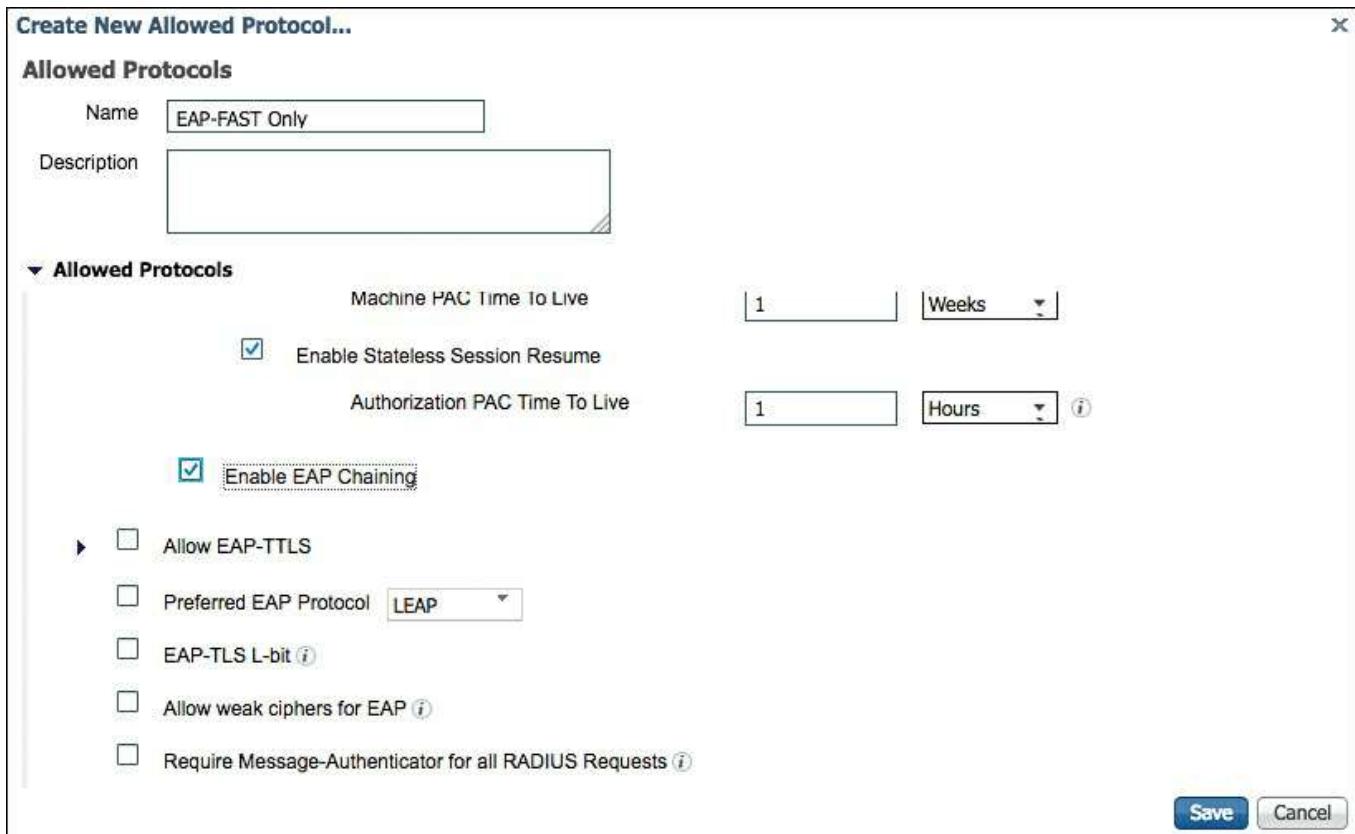
**Step 16.** For ease of deployment, check the **Allow Anonymous In-Band PAC Provisioning** and **Allow Authenticated In-Band PAC Provisioning** check boxes.

**Step 17.** Check the boxes for **Server Returns Access-Accept After Authenticated Provisioning** and **Accept Client Certificate For Provisioning**.

**Step 18.** Check the **Allow Machine Authentication** check box.

**Step 19.** Check the **Enable Stateless Session Resume** check box.

**Step 20.** Check the Enable EAP Chaining check box, as shown in [Figure 13-16](#).

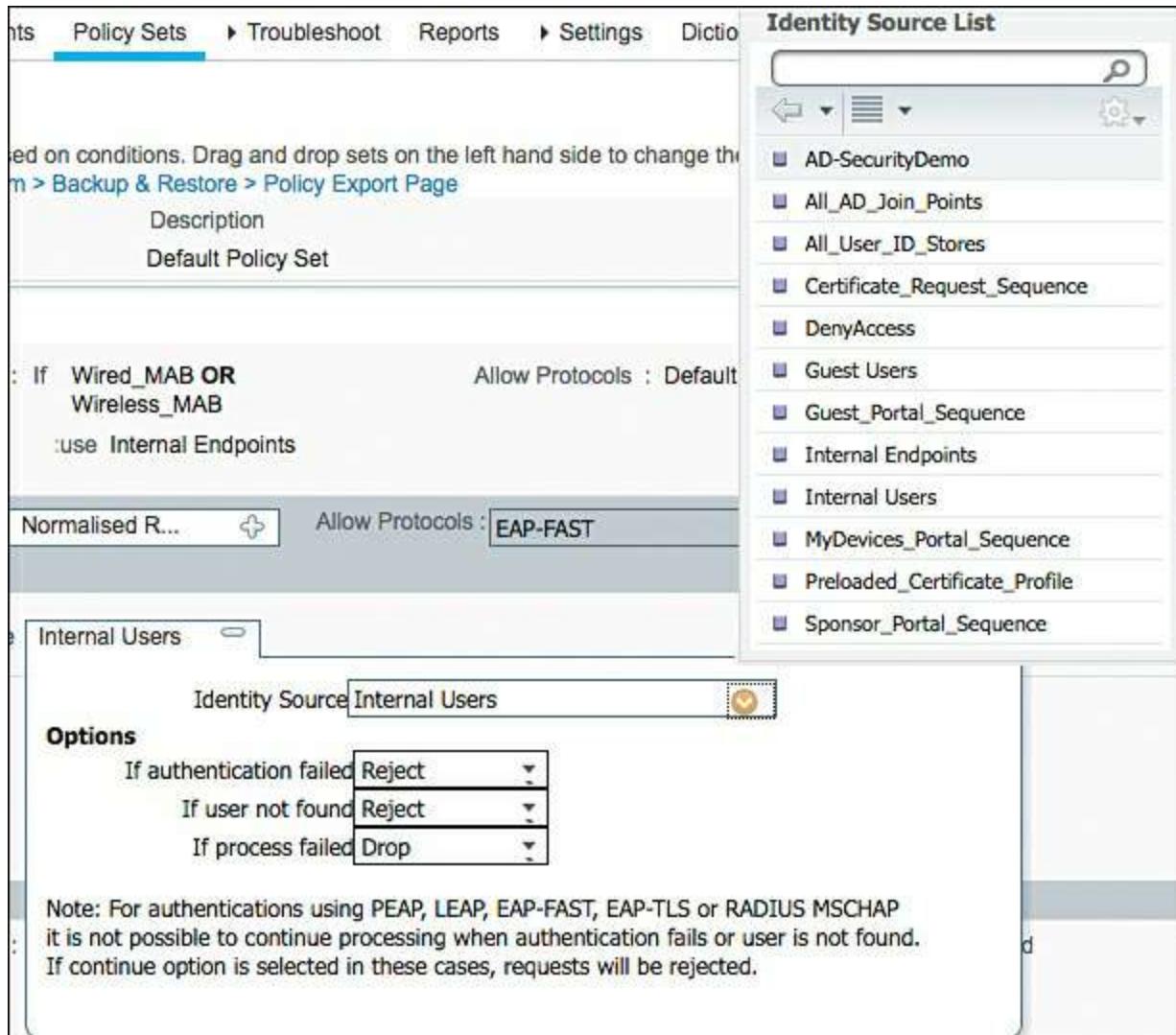


**Figure 13-16** Adding a New Protocol to Allowed Protocols, Continued

**Step 21.** Because you are only allowing one protocol, there is no need to set a preferred EAP protocol, so leave the Preferred EAP Protocol check box unchecked.

**Step 22.** Click **Save**.

**Step 23.** Click the drop-down arrow for the Identity Source field (currently set to Internal Users), as shown in [Figure 13-17](#).



**Figure 13-17** Selecting the AD Identity Source

**Step 24.** In the list of choices, choose your Active Directory source. In this example, choose **AD-SecurityDemo**. Another option is to use the built-in **All\_AD\_Join\_Points** source, which will systematically try each and every joined AD domain.

**Step 25.** Under Options, leave the default settings for what action to take if authentication fails, the user is not found, or the process fails.

**Step 26.** Click **Done**.

**Step 27.** Click **Save**.

Figure 13-18 shows the completed authentication rule.



**Figure 13-18** Completed CiscoPress SSID Authentication Rule

This completes the creation of the authentication rule. The authorization policy is what determines which actions to take for the authentications that passed.

## Remote-Access VPN

Very often, authentications for a remote-access VPN connection get routed to an OTP server, such as an RSA SecureID server. For this example, let's build a rule for remote-access VPN authentications and configure it to do the following:

- Only match authentications coming from the VPN device
- Route that authentication to the OTP server

From the ISE GUI, perform the following steps:

**Step 1.** Navigate to **Work Centers > Network Access > Policy Sets > Default**.

**Step 2.** In the Authentication Policy section, insert a new rule above the preconfigured Dot1X rule.

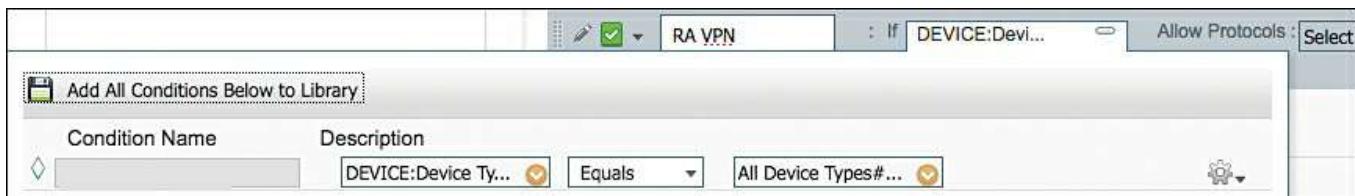
**Step 3.** Provide a name for the rule. For purposes of this example, name it **RA VPN**.

**Step 4.** For the condition, choose **DEVICE:Device Type**.

**Step 5.** Set the operator to **Equals**.

**Step 6.** Choose the Network Device Group VPN.

[Figure 13-19](#) shows the selection of the conditions.



**Figure 13-19** Device Type Equals VPN

**Step 7.** For this example, set the Allow Protocols field to **Default Network Access**.

**Step 8.** For the identity store, the OTP server was selected that was previously configured in **Administration > Identity Management > External Identity Sources > RADIUS Token (ATWOTP)**.

**Step 9.** Leave the default options.

**Step 10.** Click **Done**.

**Step 11.** Click **Save**.

[Figure 13-20](#) shows the completed RA VPN rule.



**Figure 13-20** Completed RA VPN Authentication Rule

## Alternative ID Stores Based on EAP Type

In this modern day of BYOD and mobility, it is common to have multiple user and device types connecting to the same wireless SSID. In scenarios like this, often times, the corporate users with corporate laptops authenticate using EAP-FAST with EAP chaining while BYOD-type devices need to use certificates and EAP-TLS. Anyone authenticating with PEAP is recognized as a non-corporate and non-registered asset and sent to a device registration portal instead of being permitted network access.

For this example, let's modify the preconfigured Dot1X rule by creating subrules for each EAP type. This rule will be configured to

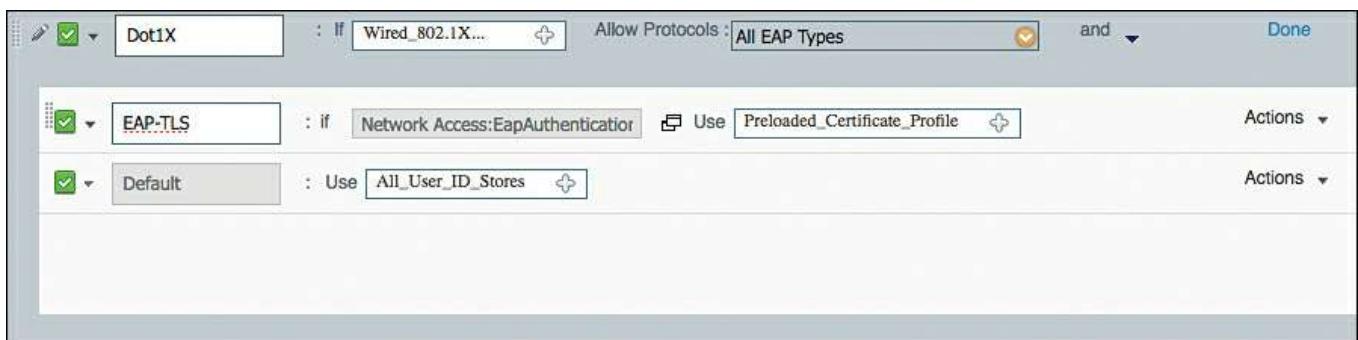
- Match wired or wireless 802.1X
- Route EAP-TLS authentications to a Certificate Authentication Profile (CAP)
- Route PEAP authentications to an LDAP server
- Route EAP-FAST to Active Directory
- Route EAP-MD5 to internal endpoints for host-lookup as a MAB request

From the ISE GUI, perform the following steps:

- Step 1.** Navigate to **Work Centers > Network Access > Policy Sets > Default**.
- Step 2.** Click **Edit** to edit the preconfigured Dot1X rule.
- Step 3.** Create a new allowed protocol object that only allows EAP authentications.  
Select the drop-down for allowed protocols.
- Step 4.** Click the cog icon in the upper-right corner and choose **Create a New Allowed Protocol**.
- Step 5.** Provide a name. For purposes of this example, name it **All EAP Types**.
- Step 6.** (Optional) Provide a description.
- Step 7.** Working top-down in the Allowed Protocols list, ensure that all EAP types are enabled (checked), except for LEAP (unless you need LEAP for backward compatibility).
- Step 8.** Check the **EAP Chaining** check box, as you did previously in the wireless SSID exercise.
- Step 9.** Click **Save**.
- Step 10.** Insert a new subrule above the Default identity store subrule and name it **EAP-**

**TLS.**

**Step 11.** For the condition, choose **Network Access > EapAuthentication EQUALS EAP-TLS** (as shown in [Figure 13-21](#)).



**Figure 13-21** Condition Set to Network Access:EapAuthentication EQUALS EAP-TLS

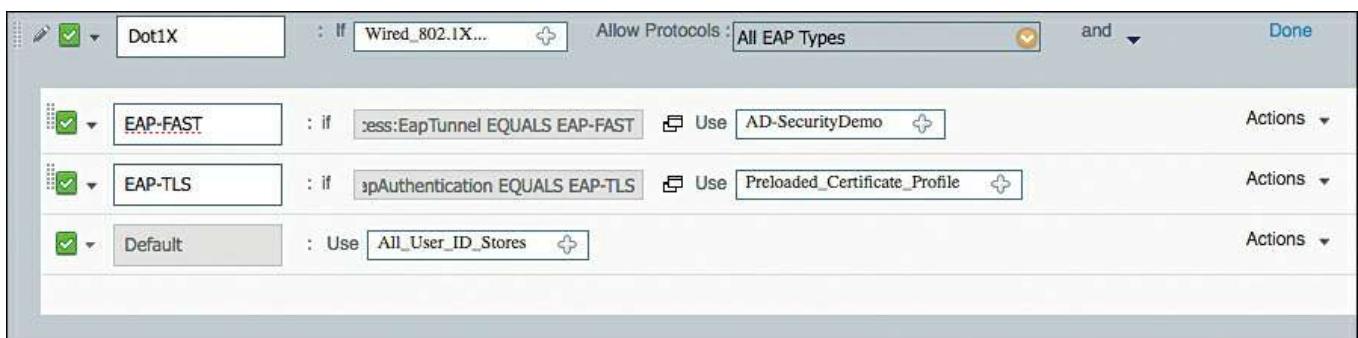
**Step 12.** For the identity source, choose the preconfigured Certificate Authentication Profile (CAP) named **Preloaded\_Certificate\_Profile**.

**Step 13.** Insert a new row above the EAP-TLS row to insert EAP-FAST. You place EAP-FAST above EAP-TLS because EAP-TLS may be used as an inner method of EAP-FAST.

**Step 14.** Choose **Network Access > EapTunnel EQUALS EAP-FAST** for the condition.

**Step 15.** Select the Active Directory object for the identity source.

[Figure 13-22](#) shows the rules so far.



**Figure 13-22** Condition Set to Network Access: EapTunnel EQUALS EAP-FAST

**Step 16.** Insert a new row above the EAP-TLS row to insert PEAP.

**Step 17.** Choose **Network Access > EapTunnel EQUALS PEAP** for the condition.

**Step 18.** Select the LDAP object for the identity source.

**Step 19.** Insert a new row below the EAP-TLS row to insert EAP-MD5.

**Step 20.** Choose **Network Access > EapAuthentication EQUALS EAP-MD5** for the

condition.

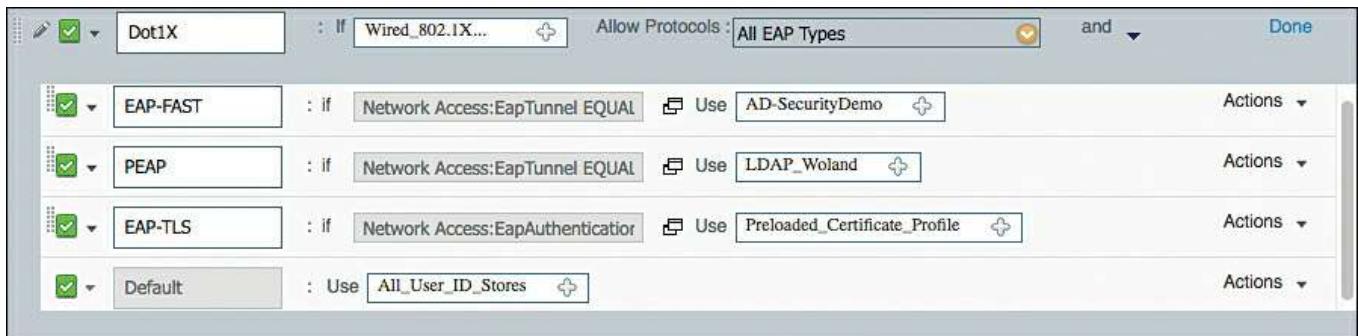
**Step 21.** Select internal endpoints for the identity source.

**Step 22.** Change the default identity store (bottom row) to **Deny Access**.

**Step 23.** Click **Done**.

**Step 24.** Click **Save**.

[Figure 13-23](#) shows the completed rule and subrules.



**Figure 13-23** Completed Authentication Rule and Subrules

This completes the authentication section of this chapter. The next section takes an in-depth look at authorization policies and common authorization rules.

## Authorization Policies

The ultimate goal of an authentication policy is to determine if the identity credential is valid or not; however, success or failure in the authentication policy may not necessarily determine whether the user or device is actually permitted access to the network. The authorization rules make that determination.

## Goals of Authorization Policies

Authorization policies have one main goal: to examine conditions in order to send an authorization result (sometimes called permissions) to the network access device (NAD). What conditions? Well, what did you have in mind?

Common conditions could include internal and external attributes, like Active Directory group membership or internal group membership within ISE. Policies can be built using attributes like location, time, if a device was registered, whether a mobile device has been jail-broken...nearly any attribute imaginable. Even the authentication is an attribute: was authentication successful; which authentication protocol was used; and what is the content of specific fields of the certificate that was used?

The authorization policy compares these conditions with the explicit goal of providing an authorization result. The result may be a standard RADIUS Access-Accept or Access-Reject message, but it can also include more advanced items, like VLAN

assignment, dACLs, Security Group Tag (SGT), URL redirection, and more. The result allows or denies access to the network, and when it is allowed, it can include any and all restrictions for limiting network access for the user or endpoint.

## Understanding Authorization Policies

Now that you understand the fundamental responsibilities of the authorization policy, it will be easier to understand the exercises in this section. To understand authorization policies even more, let's examine a few.

Basic authorization policy rules are logically organized in this manner:

IF conditions THEN AssignThesePermissions

Just like the authentication policy, authorization policy rules are processed in a top-down, first-match order. So, if the conditions do not match, the authentication is compared to the next rule in the policy.

As previously mentioned, ISE is preconfigured with rules that we call smart defaults. There is a rule for blacklisted devices, named Wireless Black List Default, another for Profiled Cisco IP Phones, and yet another for Profiled Non Cisco IP Phones. There are also some preconfigured rules that are disabled out of the box but can be used for BYOD onboarding and guest access. We will examine those rules in the relevant chapters for those topics.

Let's examine the Cisco IP Phone and Wireless Black List Default rules in order to dig into authorization rules and how they work. If you have a live ISE system, it may help to follow along with the text.

From the ISE GUI, perform the following steps:

### Step 1. Navigate to Work Centers > Network Access > Policy Sets > Default.

In the Authorization Policy section, you should notice an immediate difference between the authorization policy and the authentication policy examined earlier in this chapter. The authorization policy attempts to display the rule logic in plain English. The bold text designates an identity group, while the standard font is a normal attribute. The operator is always AND when both identity group and other conditions are used in the same rule.

[Figure 13-24](#) displays the default authorization policy.

Authorization Policy					
Exceptions (0)					
Standard					
Status	Rule Name	Conditions (identity groups and other conditions)		Permissions	
<input checked="" type="checkbox"/>	Wireless Black List Default	If <b>Blacklist AND Wireless_Access</b>	then	Blackhole_Wireless_Access	
<input checked="" type="checkbox"/>	Profiled Cisco IP Phones	If <b>Cisco-IP-Phone</b>	then	Cisco_IP_Phones	
<input checked="" type="checkbox"/>	Profiled Non Cisco IP Phones	If <b>Non_Cisco_Profiled_Phones</b>	then	Non_Cisco_IP_Phones	
<input type="checkbox"/>	Compliant_Devices_Access	If <b>(Network_Access_Authentication_Passed AND Compliant_Devices )</b>	then	PermitAccess	
<input type="checkbox"/>	Employee_EAP-TLS	If <b>(Wireless_802.1X AND BYOD_Is_Registered AND EAP-TLS AND MAC_in_SAN )</b>	then	PermitAccess AND BYOD	
<input type="checkbox"/>	Employee_Onboarding	If <b>(Wireless_802.1X AND EAP-MSCHAPv2 )</b>	then	NSP_Onboard AND BYOD	
<input type="checkbox"/>	Wi-Fi_Guest_Access	If <b>(Guest_Flow AND Wireless_MAB )</b>	then	PermitAccess AND Guests	
<input type="checkbox"/>	Wi-Fi_Redirect_to_Guest_Login	If <b>Wireless_MAB</b>	then	Cisco_WebAuth	
<input checked="" type="checkbox"/>	Basic_Authenticated_Acces	If <b>Network_Access_Authentication_Passed</b>	then	PermitAccess	
<input checked="" type="checkbox"/>	Default	If no matches, then		DenyAccess	

**Figure 13-24** Default Authorization Policy

**Step 2.** Click **Edit** to edit the rule named Profiled Cisco IP Phones.

Notice the identity group is a separate list than the other conditions. In this rule, there is an identity group named Cisco-IP-Phone. The next field is where other conditions are selected.

This particular rule is a prebuilt rule that permits any device that was profiled as a Cisco IP Phone, sending an Access-Accept that also sends an attribute-value pair (AVP) that permits the phone into the voice VLAN. [Figure 13-25](#) shows an identity group of Cisco-IP-Phone.

Authorization Policy					
Exceptions (0)					
Standard					
Status	Rule Name	Conditions (identity groups and other conditions)		Permissions	
<input checked="" type="checkbox"/>	Wireless Black List Default	If <b>Blacklist AND Wireless_Access</b>		Blackhole_Wireless_Access	
<input checked="" type="checkbox"/>	Profiled Cisco IP Phones	If <b>Cisco-IP-Phone</b>		Cisco_IP_Phones	
<input checked="" type="checkbox"/>	Profiled Non Cisco IP Phones	If <b>Non_Cisco_Profiled_Phones</b>		Non_Cisco_IP_Phones	

**Figure 13-25** Profiled Cisco IP Phones Rule

**Step 3.** Examine the permissions (result) that is sent. Navigate to **Work Centers > Network Access > Policy Elements > Results > Authorization Profiles**.

An authorization profile is a set of authorization results that should be sent together. [Figure 13-26](#) displays the default authorization profiles.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes links for Home, Context Visibility, Operations, Policy, Administration, Work Centers, and License. Below the navigation is a secondary menu with Network Access, Guest Access, TrustSec, BYOD, Profiler, Posture, Device Administration, and PassiveID. Under Network Access, Overview, Identities, Id Groups, Ext Id Sources, Network Resources, Policy Elements (which is selected and highlighted in blue), Policy Sets, Troubleshoot, Reports, Settings, and Dictionaries are listed. On the left, a sidebar has sections for Conditions and Results, with Allowed Protocols, Authorization Profiles, and Downloadable ACLs. The main content area is titled "Standard Authorization Profiles" and contains a table with the following data:

Name	Profile	Description
Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless devices. Ensure that you can see the device in the Blacklist tab.
Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
Cisco_WebAuth	Cisco	Default Profile used to redirect users to the CWA portal.
NSP_Onboard	Cisco	Onboard the device with Native Suplicant Provisioning
Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
DenyAccess		Default Profile with access type as Access-Reject
PermitAccess		Default Profile with access type as Access-Accept

**Figure 13-26 Default Authorization Profiles**

#### Step 4. Click **Cisco\_IP\_Phones** Authorization Profiles.

The authorization result needs to be RADIUS attributes. To make that easier for the users of ISE, Cisco has included a Common Tasks section that presents the options in more of a “plain English” format, as shown in [Figure 13-27](#) for the default Cisco\_IP\_Phones authorization profile. Further down, the Attributes Details section, shown in [Figure 13-28](#), displays the raw RADIUS result that is sent.

Authorization Profiles > **Cisco\_IP\_Phones**

**Authorization Profile**

\* Name

Description

\* Access Type

Network Device Profile  Cisco

Service Template

Track Movement  

Passive Identity Tracking  

**▼ Common Tasks**

DACL Name

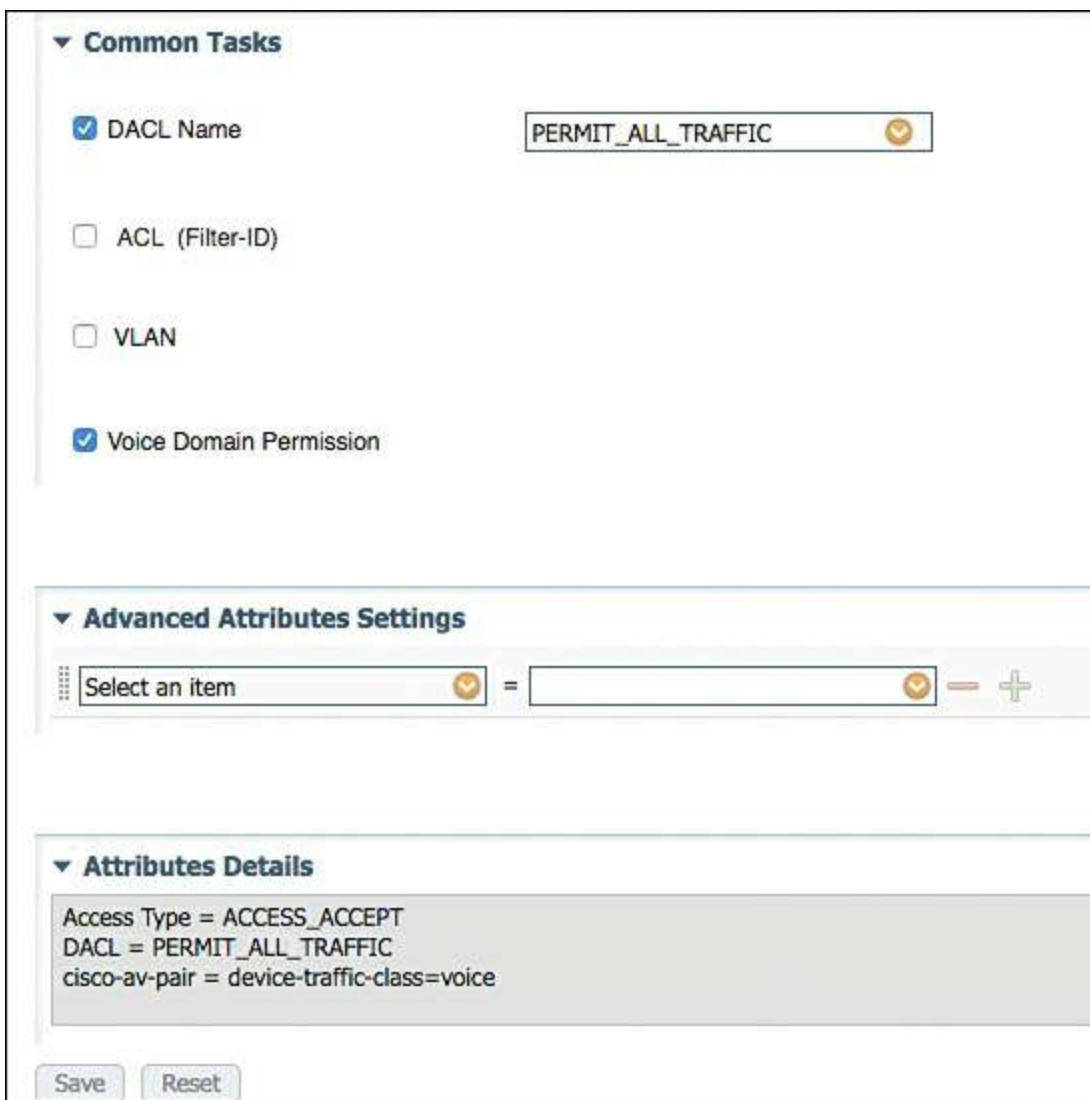


ACL (Filter-ID)

VLAN

Voice Domain Permission

**Figure 13-27 Cisco\_IP\_Phones Authorization Profile**



**Figure 13-28** Cisco\_IP\_Phones Authorization Profile Attributes Details

In [Figure 13-27](#), note the DACL Name task includes a drop-down box where you select a downloadable access list that is created and stored in ISE. Checking the Voice Domain Permission check box is required for the switch to allow the phone into the voice VLAN on the switch.

[Figure 13-28](#) shows the lower portion of the UI screen, where the Attributes Details section previously mentioned appears. This is the raw RADIUS result that will be sent to the NAD. Notice in this figure that the Voice Domain Permission check box actually translates to cisco-av-pair = device-traffic-class=voice.

Next, examine the Wireless Black List Default rule:

**Step 1.** Navigate to **Work Centers > Network Access > Policy Sets > Default**.

**Step 2.** Edit the rule named **Wireless Black List Default**.

Again, notice the identity group is a separate list from the other conditions. In this rule, there is an identity group named **Blacklist**. The next field is populated with

a prebuilt condition specifying wireless connections. This particular rule is built to prevent devices that have been marked lost or stolen from accessing the network.

**Step 3.** Examine the authorization condition being used. Navigate to **Work Centers > Network Access > Policy Elements > Conditions > Authorization Compound Conditions**.

[Figure 13-29](#) shows the default list of compound conditions.

Authorization Compound Conditions			
For Policy Export go to <a href="#">Administration &gt; System &gt; Backup &amp; Restore &gt; Policy Export Page</a>			
<a href="#">Edit</a> <a href="#">Add</a> <a href="#">Duplicate</a> <a href="#">Delete</a>			
Name	Profile	Description	
<a href="#">BYOD_is_Registered</a>		Default condition for BYOD flow for any device that has passed the NSP process	
<a href="#">Catalyst_Switch_Local_We...</a>		Default condition used to match authentication requests for Local Web Authentication	
<a href="#">Compliant_Devices</a>		Default condition for compliant devices	
<a href="#">EAP-MSCHAPv2</a>		Default condition for BYOD Onboarding flow	
<a href="#">EAP-TLS</a>		Default condition for BYOD flow for any device that has passed the NSP process	
<a href="#">Guest_Flow</a>		Default condition for guest flow	
<a href="#">MAC_in_SAN</a>		Default condition for BYOD flow for any device that has passed the NSP process	
<a href="#">Network_Access_Authentic...</a>		Default condition used for basic Network Access requiring that authentication was	
<a href="#">Non_Cisco_Profiled_Phones</a>		Default condition used to match Non Cisco IP Phones	
<a href="#">Switch_Web_Authentication</a>	All Profiles	A condition to match requests for web authentication from switches, according to	
<a href="#">WLC_Web_Authentication</a>	All Profiles	A condition to match requests for web authentication from wireless LAN controllers	
<a href="#">Wired_802.1X</a>	All Profiles	A condition to match 802.1X based authentication requests from switches, accordi	
<a href="#">Wired_MAB</a>	All Profiles	A condition to match MAC Authentication Bypass service based authentication requ	
<a href="#">Wireless_802.1X</a>	All Profiles	A condition to match 802.1X based authentication requests from wireless LAN con	
<a href="#">Wireless_Access</a>		Default condition used to match any authentication request from Cisco Wireless LA	
<a href="#">Wireless_MAB</a>	All Profiles	A condition to match MAC Authentication Bypass service based authentication requ	

**Figure 13-29** Prebuilt Authorization Compound Conditions

**Step 4.** Click on **Wireless\_Access**.

As shown in [Figure 13-30](#), the **Wireless\_Access** compound condition references the RADIUS attribute of NAS-Port-Type Equals Wireless-IEEE 802.11.

Authorization Compound Condition List > [Wireless\\_Access](#)

### Authorization Compound Conditions

* Name	Wireless_Access
Description	Default condition used to match any authentication request from Cisco Wireless LAN Controller.

\*Condition Expression

Condition Name	Description
<input type="text"/> tadius:NAS-Port-Type	<input type="radio"/> Equals <input type="radio"/> Contains <input type="radio"/> Starts With <input type="radio"/> Ends With <input type="radio"/> Is Null <input type="radio"/> Is Not Null
<input type="text"/> Wireless - IEEE 8...	<input checked="" type="checkbox"/>

**Save** **Reset**

**Figure 13-30** Wireless\_Access Compound Condition

**Step 5.** Examine the authorization result that is being sent for this authorization rule.

    Navigate to **Work Centers > Network Access > Policy Elements > Results > Authorization Profiles**.

**Step 6.** Select **Blackhole\_Wireless\_Access**.

As shown in the composite image [Figure 13-31](#), the Blackhole\_Wireless\_Access authorization profile does not use any of the common tasks. Instead, it employs the Advanced Attribute Settings fields to send a URL-Redirect and URL-Redirect-ACL result to the WLC, along with an Access-Accept. So, this result allows the devices onto the network, but forces all traffic to redirect to a web page describing that the device is blacklisted.

Authorization Profiles > **Blackhole\_Wireless\_Access**

**Authorization Profile**

* Name	Blackhole_Wireless_Access
Description	Default profile used to blacklist wireless devices. Ensure that you configure a BLACKHOLE ACL on the Wireless LAN Controller.
* Access Type	ACCESS_ACCEPT
Network Device Profile	Cisco

**Advanced Attributes Settings**

- [Cisco:cisco-av-pair] = url-redirect=https://ip:port/black..
- [Cisco:cisco-av-pair] = url-redirect-acl=BLACKHOLE

**Attributes Details**

```

Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect=https://ip:port/blacklistportal/gateway?portal=a0b94090-8c01-11e6-996c-525400b48521
cisco-av-pair = url-redirect-acl=BLACKHOLE

```

**Buttons:** Save | Reset

**Figure 13-31 Blackhole\_Wireless\_Access Authorization Profile**

These two authorization rules demonstrate a variety of rules. This chapter examines a few common authorization policies in later sections.

## Role-Specific Authorization Rules

The end goal of a Secure Access deployment is to provide very specific permissions to any authorization. However, that should always be handled in a staged approach to limit the impact to the end users.

[Chapter 20, “Deployment Phases,”](#) is dedicated to discussing the staged approach for authorizations.

## Authorization Policy Example

This section provides an example of an authorization policy made up of numerous rules based on a common use case. This use case was selected to show multiple aspects of the authorization policy and help to solidify your working knowledge of the parts of an authorization policy and the workflows associated with creating the policy.

For this example, let’s configure three authorization rules: one that assigns full access to an employee that authenticated successfully with EAP chaining; one that assigns more

limited access to the same employee authenticating with a non-corporate machine; and one that assigns Internet-only access to the same employee authenticating on a mobile device.

## **Employee and Corporate Machine Full-Access Rule**

In this rule, assign full-access permissions to an employee who is authenticating from a valid corporate asset. From the ISE GUI, perform the following steps:

**Step 1.** Navigate to **Work Centers > Network Access > Policy Sets > Default**.

**Step 2.** In the Authorization Policy section, insert a new rule above the rule named **Basic\_Authenticated\_Access**.

The default configuration of ISE is to allow any successful authentication to access the network, making it easier to install and test. The **Basic\_Authenticated\_Access** rule is what enables that behavior. As you roll out ISE into your environment and look toward role-specific access, you will want to disable this rule.

**Step 3.** For this example, name the new rule **Employee and CorpMachine**.

**Step 4.** For the other conditions drop-down, where it says Select Attribute, click the + sign and select **Create New Condition**.

**Step 5.** Choose **Network Access > EapChainingResult**.

**Step 6.** Choose **Equals**.

**Step 7.** Select **User and Machine Both Succeeded**.

**Step 8.** Click the cog icon on the right side and choose **Add Attribute/Value**.

**Step 9.** Select **AD1 > External Groups Equals “Employees”** (or another AD group of your choosing).

**Step 10.** For the AuthZ Profiles, click the + sign.

**Step 11.** Click the cog icon in the upper-right corner and choose **Add New Standard Profile**.

**Step 12.** In the Name text box, name the new authorization profile **Employee Full Access**.

**Step 13.** (Optional) Add a description.

**Step 14.** From the Access Type drop-down list, choose **ACCESS\_ACCEPT**.

**Step 15.** Check the **DACL Name** check box and choose **PERMIT\_ALL\_TRAFFIC** from the drop-down list.

[Figure 13-32](#) shows the Employee Full Access authorization profile.

**Add New Standard Profile**

**Authorization Profile**

* Name	Employee Full Access
Description	
* Access Type	ACCESS_ACCEPT

Network Device Profile Cisco +

Service Template

Track Movement  ⓘ

Passive Identity Tracking  ⓘ

**Common Tasks**

<input checked="" type="checkbox"/> DACL Name	PERMIT_ALL_TRAFFIC <input checked="" type="checkbox"/>
<input type="checkbox"/> ACL (Filter-ID)	
<input type="checkbox"/> VLAN	

**Figure 13-32 Employee Full Access Authorization Profile**

**Step 16.** Click **Save**.

**Step 17.** Click **Done** to finish editing the rule.

**Step 18.** Click **Save** to save the authorization policy.

[Figure 13-33](#) shows the completed authorization rule.

Employee and CorpMachine	If Network Access:EapChainingResult EQUALS User and machine both succeeded AND AD-SecurityDemo:ExternalGroups EQUALS securitydemo.net/Users/Employees	then Employee Full Access	Edit   ▾
Basic_Authenticated_Access	If Network_Access_Authentication_Passed	then PermitAccess	Edit   ▾

**Figure 13-33 Completed Employee and CorpMachine Rule**

## Internet Only for Mobile Devices

Now that the rule for employees with corporate devices has been created, you need to

create the rule below it that provides Internet access only to employee authentications on mobile devices.

To begin this rule, first create a new DACL that is applied to switches, create the authorization result, and then go back into the authorization policy and build the rule:

**Step 1.** Navigate to **Work Centers > Network Access > Policy Elements > Results > Downloadable ACLs**.

**Step 2.** Click **Add**.

**Step 3.** In the Name text field, name the ACL **Internet-Only**.

**Step 4.** (Optional) Provide a description.

**Step 5.** In the DACL Content pane, provide an ACL that permits required traffic for Internet access and denies traffic destined to the corporate network. [Figure 13-34](#) shows an example.

The screenshot shows the Cisco Identity Services Engine (ISE) interface for creating a new Downloadable ACL named "Internet-Only". The "DACL Content" pane displays the following rules:

```
1 permit udp any any eq 68
2 permit udp any any eq 53
3 deny ip any 172.26.0.0 0.0.3.255
4 deny ip any 192.168.0.0 0.0.255.255
5 deny ip any 10.0.0.0 0.0.0.255
6 permit ip any any
7
8
9
10
```

The "Check DACL Syntax" section indicates that the DACL is valid.

### **Figure 13-34 Internet-Only DACL**

#### **Step 6. Click Submit.**

Now that the DACL is created, it's time to create the authorization profile:

#### **Step 1.** Navigate to **Work Centers > Network Access > Policy Elements > Results > Authorization Profiles.**

#### **Step 2.** Click **Add**.

#### **Step 3.** In the Name field, name the authorization profile **Internet Only**.

#### **Step 4.** (Optional) Provide a description.

#### **Step 5.** From the Access Type drop-down list, choose **ACCESS\_ACCEPT**.

#### **Step 6.** Check the **DACL Name** check box and choose **Internet-Only** from the drop-down list.

#### **Step 7.** (Optional) Check the **VLAN** check box and provide a guest VLAN.

Keep in mind this VLAN Name or ID is used for both wired and wireless devices. An alternative is to create separate rules for wired and wireless, so the user is assigned VLAN on wireless but not wired.

#### **Step 8.** Select **Airspace ACL Name** and fill in the name of the ACL on the controller that provides Internet-only access.

#### **Step 9.** Click **Submit**.

[Figure 13-35](#) shows the completed authorization profile.

Authorization Profiles > New Authorization Profile

### Authorization Profile

* Name	Internet Only
Description	
* Access Type	ACCESS_ACCEPT
Network Device Profile	Cisco
Service Template	<input type="checkbox"/>
Track Movement	<input type="checkbox"/> <a href="#">i</a>
Passive Identity Tracking	<input type="checkbox"/> <a href="#">i</a>

**Common Tasks**

<input checked="" type="checkbox"/> DACL Name	Internet-Only
<input type="checkbox"/> ACL (Filter-ID)	
<input checked="" type="checkbox"/> VLAN	Tag ID: 1
	<a href="#">Edit Tag</a> <a href="#">ID/Name</a> GUEST
<input type="checkbox"/> Voice Domain Permission	

**Advanced Attributes Settings**

Select an item	=		<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Add</a>
----------------	---	--	----------------------	------------------------	---------------------

**Attributes Details**

Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:GUEST
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6
DACL = Internet-Only
Airespace-ACL-Name = Internet-Only

**Buttons**

Submit Cancel

**Figure 13-35 Internet Only Authorization Profile**

Before you build the authorization policy, take a look at a pre-existing logical profile that is designed to encompass all mobile devices out of the box. We will leverage this in your authorization policy, as it makes the policy building much easier and provides a reusable policy object:

**Step 1.** Navigate to **Work Centers > Profiler > Profiling Policies > Logical Profiles**.

[Figure 13-36](#) shows the pre-existing logical profiles.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes links for Home, Context Visibility, Operations, Policy, Administration, and Work Centers. Below the navigation is a secondary menu with items like Network Access, Guest Access, TrustSec, BYOD, Profiler, Posture, Device Administration, and PassiveID. The main content area is titled "Profiling" and contains a sidebar with sections for Profiling Policies and Logical Profiles. Under Logical Profiles, there are categories for Cameras, Gaming Devices, Home Network Dev, IP-Phones, Infrastructure Netw, Medical Devices, Mobile Devices, and Printers. To the right is a table titled "Logical Profiles" with columns for Logical Profiles, System Type, and Description. The table lists several default profiles: Cameras (Cisco Provided), Gaming Devices (Cisco Provided), Home Network Devices (Cisco Provided), IP-Phones (Cisco Provided), Infrastructure Network Dev... (Cisco Provided), Medical Devices (Cisco Provided), Mobile Devices (Cisco Provided), and Printers (Cisco Provided). A red arrow points to the "Mobile Devices" row in the table.

**Figure 13-36** Logical Profiles

**Step 2.** Examine the Mobile Devices logical profile by clicking its name (not its check box). This grouping of profiles, shown in [Figure 13-37](#), consists of endpoint profiles such as Apple-iPad, Android, Samsung-Phone, and others.

The screenshot shows the "Logical Profiles List > Mobile Devices" configuration page. At the top, there is a "Logical Profile" section with fields for "Name" (set to "Mobile Devices") and "Description" (set to "Default logical profile for mobile devices"). Below this is a "Policy Assignment" section. On the left, under "Available Policies", a list of policies is shown: 2Wire-Device, 3Com-Device, Astra-Device, Astra-IP-Phone, Aerohive-Access-Point, Aerohive-Device, American-Power-Conversion-Device, and Android-Amazon. On the right, under "Assigned Policies", a list of policies is shown: Android, Apple-iPad, Apple-iPhone, Apple-iPod, BlackBerry, HP-TouchPad-Tablet, HTC-Device, and Microsoft-Surface-Tablet. Between these two lists are four buttons: a single right-pointing arrow (>), a double left-pointing arrow (<<), a double right-pointing arrow (>>), and a double left-pointing arrow (<<<<).

**Figure 13-37** Mobile Devices Logical Profile

Finally, it is now time to create the authorization rule:

**Step 1.** Navigate to **Work Centers > Network Access > Policy Sets > Default**.

**Step 2.** In the Authorization Policy section, insert a new rule above the `Basic_Authenticated_Access` rule.

**Step 3.** Name the rule **Employee Mobile Devices**.

**Step 4.** Click the + sign for conditions, and choose **Endpoints > LogicalProfile**.

**Step 5.** Choose **Equals**.

**Step 6.** Select **Mobile Devices**.

**Step 7.** Click the cog icon on the right side and choose **Add Attribute/Value**.

**Step 8.** Select **AD-SecurityDemo > External Groups Equals “Employees”** (or another AD group of your choosing).

**Step 9.** For the AuthZ Profiles, click the + sign.

**Step 10.** Choose **Standard > Internet Only**.

**Step 11.** Click **Done**.

**Step 12.** Click **Save**.

The completed authorization rule is displayed in [Figure 13-38](#).

<input checked="" type="checkbox"/> Employee and CorpMachine	If Network Access:EapChainingResult EQUALS User and machine both succeeded	then Employee Full Access	Edit   ▾
<input checked="" type="checkbox"/> Employee Mobile Devices	If EndPoints:LogicalProfile EQUALS Mobile Devices AND AD-SecurityDemo:ExternalGroups EQUALS securitydemo.net/Users/Employees	then Internet Only	Edit   ▾
<input checked="" type="checkbox"/> Basic_Authenticated_Access	If Network_Access_Authentication_Passed	then PermitAccess	Edit   ▾
<input checked="" type="checkbox"/> Default	If no matches, then DenyAccess		Edit   ▾

**Figure 13-38** Employee Mobile Devices Authorization Rule

## Employee Limited Access Rule

Now that the rule for employees connecting with mobile devices has been created, you need to create the rule below it that only provides limited access to employee authentications on any other device.

To begin this rule, first create a new DACL that is applied to switches, create the authorization result, and then go back into the authorization policy and build the rule:

**Step 1.** Navigate to **Work Centers > Network Access > Policy Elements > Results > Downloadable ACLs**.

**Step 2.** Click **Add**.

**Step 3.** In the name text box, name the ACL **EmployeeLimited**.

**Step 4.** (Optional) Provide a description.

**Step 5.** In the DACL Content pane, provide an ACL that permits required traffic and denies traffic destined to the corporate network. For this example, allow traffic to reach your virtual desktop infrastructure and essential services, like DNS only.

[Figure 13-39](#) shows the example EmployeeLimited DACL.

Downloadable ACL List > New Downloadable ACL

### Downloadable ACL

* Name	<input type="text" value="EmployeeLimited"/>
Description	Permit Access to the VDI environment only
* DACL Content	<pre> 1 permit udp any any eq 68 2 permit udp any any eq 53 3 permit tcp any host 10.1.100.222 eq 3389 4 permit tcp any host 10.1.100.222 eq 443 5 permit tcp any host 10.1.100.222 eq 80 6 7 8 9 10 </pre>
<b>▼ Check DACL Syntax</b>	
<input type="button" value="Recheck"/> <input type="button" value="&lt;"/> <input type="button" value="&gt;"/> DACL is valid	
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

**Figure 13-39 EmployeeLimited DACL**

**Step 6. Click Submit.**

Now that the DACL is created, build the authorization policy to permit network access and apply that DACL:

**Step 1.** Navigate to **Work Centers > Network Access > Policy Elements > Results > Authorization Profiles.**

**Step 2.** Click **Add**.

**Step 3.** In the Name text box, name the authorization profile **Employee Limited**.

**Step 4.** (Optional) Provide a description.

**Step 5.** From the Access Type drop-down list, choose **ACCESS\_ACCEPT**.

**Step 6.** Check the **DACL Name** check box and choose **EmployeeLimited** from the drop-down list.

**Step 7.** Do not assign a different VLAN for this authorization.

**Step 8.** Select **Airespace-ACL-Name** and fill in the name of the ACL on the controller that provides Internet-only access.

**Step 9.** Click **Submit**.

[Figure 13-40](#) shows the completed authorization profile.

* Name	<input type="text" value="Employee Limited"/>
Description	<input type="text"/>
* Access Type	<input type="text" value="ACCESS_ACCEPT"/>
Network Device Profile	Cisco
Service Template	<input type="checkbox"/>
Track Movement	<input type="checkbox"/>
Passive Identity Tracking	<input type="checkbox"/>
<b>Common Tasks</b>	
<input checked="" type="checkbox"/> DACL Name	<input type="text" value="EmployeeLimited"/>
<input type="checkbox"/> ACL (Filter-ID)	
<input type="checkbox"/> VLAN	
<input type="checkbox"/> Voice Domain Permission	
<b>Advanced Attributes Settings</b>	
Select an item	= <input type="text"/>
<b>Attributes Details</b>	
Access Type = ACCESS_ACCEPT DACL = EmployeeLimited Airespace-ACL-Name = EmployeeLimited	
<input type="button" value="Submit"/>	<input type="button" value="Cancel"/>

**Figure 13-40** Employee Limited Authorization Profile

Now, create the authorization policy rule to assign that authorization profile:

**Step 1.** Navigate to **Work Centers > Network Access > Policy Sets > Default**.

**Step 2.** In the Authorization Policy section, insert a new rule above the **Basic\_Authenticated\_Access** rule.

**Step 3.** Name the Rule **Employee VDI Only**.

**Step 4.** Click the + sign for conditions.

**Step 5.** Select **AD-SecurityDemo > External Groups Equals “Employees”** (or another AD group of your choosing).

**Step 6.** For the AuthZ Profiles, click the + sign.

**Step 7.** Choose **Standard > Employee Limited**.

**Step 8.** Click **Done**.

**Step 9.** Click **Save**.

[Figure 13-41](#) shows the completed Employee VDI Only authorization rule.

<input checked="" type="checkbox"/> Employee and CorpMachine	if Network Access:EapChainingResult EQUALS User and machine both succeeded	then Employee Full Access	Edit   ▾
<input checked="" type="checkbox"/> Employee Mobile Devices	if (EndPoint:LogicalProfile EQUALS Mobile Devices AND AD-SecurityDemo:ExternalGroups EQUALS securitydemo.net/Users/Employees)	then Internet Only	Edit   ▾
<input checked="" type="checkbox"/> Employee VDI Only	if AD-SecurityDemo:ExternalGroups EQUALS securitydemo.net/Users/Employees	then Employee Limited	Edit   ▾

**Figure 13-41** Employee VDI Only Authorization Rule

**Note** The ordering of rules is very important. They are processed in a top-down manner. Therefore, you must always ensure that the most-specific rules are above the less-specific rules. In the example shown in [Figure 13-41](#), if the Employee VDI Only rule were above the Employee Mobile Devices rule, then mobile devices would also be limited to VDI only, which is not the intended result.

## Saving Attributes for Reuse

ISE offers the ability to save conditions to the library to make it much easier to reuse them in other policies. To show this, let's go back into your example authorization policy and save a few of the conditions.

From the ISE GUI, perform the following steps:

**Step 1.** Navigate to **Work Centers > Network Access > Policy Sets > Default**.

**Step 2.** In the Authorization Policy section, **Edit** the Employee and CorpMachine rule.

**Step 3.** Expand the conditions by clicking the + sign.

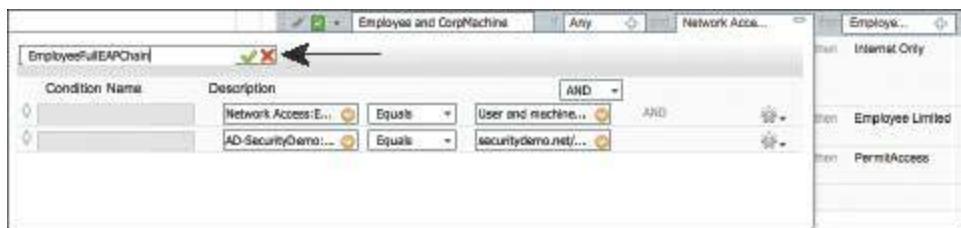
**Step 4.** Click **Add All Conditions Below to Library**, as shown in [Figure 13-42](#). This adds the full set of conditions, including the AND operator.



**Figure 13-42 Add All Conditions Below to Library**

**Step 5.** Provide a name for this new saved condition, such as **EmployeeFullEAPChain** for this example.

**Step 6.** Click the green check mark, as shown in [Figure 13-43](#), and finish editing the rule.



**Figure 13-43 Add All Conditions Below to Library Check Mark**

**Step 7.** Click Save.

As shown in [Figure 13-44](#), the authorization policy text is simplified now with the name of the saved compound condition instead of the raw attributes.



**Figure 13-44 Authorization Policy After Saving Conditions to Library**

Next, save the Employees group for AD as a condition:

**Step 1.** Navigate to **Work Centers > Network Access > Policy Sets > Default**.

**Step 2.** In the Authorization Policy section, click **Edit** to edit the Employee Mobile Devices rule.

**Step 3.** Expand the conditions by clicking the + sign.

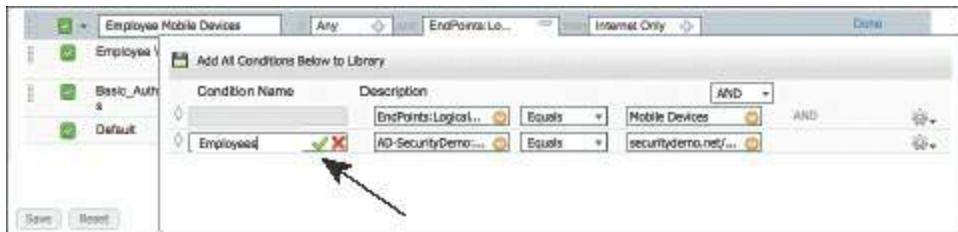
**Step 4.** Click the cog icon on the right side of the line where the Employee Active Directory group is used.

**Step 5.** Choose **Add Condition to Library**.

**Step 6.** Name the condition **Employees**.

**Step 7.** Click the green check mark.

[Figure 13-45](#) displays the saving of Employees to the Conditions library.



**Figure 13-45** Saving Employees to Library

**Step 8.** Click **Done** to finish editing the rule.

**Step 9.** Click **Save**.

[Figure 13-46](#) shows the final authorization policy.



**Figure 13-46** Final Authorization Policy

## Summary

This chapter examined the relationship between authentication and authorization and how to build policies for each. It described a few common authentication policies and authorization policies to help solidify your knowledge of how to work with these policy constructs. [Chapter 20](#) will focus on specific configurations of these policies to help in the actual deployment of ISE and the Secure Access solution.

[Chapter 14, “Guest Lifecycle Management,”](#) examines web authentication, guest access, and the full lifecycle management of guest users.

# Chapter 14 Guest Lifecycle Management

This chapter covers the following topics:

- Overview of guest services
  - Hotspot guest portal configuration
  - Sponsored guest portal configuration
  - Authentication and authorization guest policies
  - Guest sponsor portal configuration
  - Guest sponsor portal usage
- Configuration of network devices for guest CWA

Cisco Identity Services Engine provides a complete solution for guest network access. A guest is defined as someone who needs temporary and restricted access to your network. This is usually a visitor or temporary contractor. The access provided to guests is usually limited to Internet access. But, as you will learn in this chapter, this can be opened up or closed down as you see fit. Guest sponsors, employees who have the rights to create guest accounts, typically create and distribute guest usernames/passwords to their visitors. This is a common function of the front-desk receptionist who already has the job of checking in visitors. As visitors arrive, the receptionist checks them in and provides them with guest access, if required, while they are on the premises.

To configure ISE guest services quickly, read [Chapter 6](#), “Quick Setup of an ISE Proof of Concept,” to learn about the Wireless Setup Wizard. This chapter guides you through the non-wizard steps to set up ISE guest service in its many shapes and colors. ISE guest services support both wired and wireless access methods. Guest authentication takes two general forms: non-authenticated guest and authenticated guest. Non-authenticated guest provides just a web redirect to a guest portal page and allows the guest to click through to gain access. Authenticated guest requires the guest to enter unique credentials on the guest portal page before being allowed access to the network. Regardless, guest services [Table 14-1](#) shows the differences.

<b>Local Web Auth (LWA)</b>	<b>Central Web Auth (CWA)</b>
Web pages are delivered by the network device.	Web pages are redirected to ISE and delivered by ISE centrally.
Guest authentication is performed by the network device.	Guest authentication is handled by ISE.
Does not allow/support Change of Authorization.	Allows/supports CoA. This allows posture and profiling services for guests. It also allows VLAN enforcement.
Authorization enforcement uses ACLs only.	Authorization enforcement uses ACLs and VLANs.
Requires complete local web auth configuration on each NAD (switch or WLC).	Configuration for web auth is performed in ISE.
Each device has its own web portal files, web server, customization, etc.	Web portals and portal customization are performed inside of ISE centrally.

**Table 14-1** Central Versus Local Web Authentication

As you have probably already deduced, Central Web Auth is by far the most popular and easiest method. In almost all cases, you will want to deploy CWA. As a result, most of this chapter focuses on CWA, with limited LWA discussion. Check the ISE release notes on [Cisco.com](https://www.cisco.com) for the latest versions required.

Figure 14-1 shows the Local Web Authentication flow.

## LWA – Session Flow

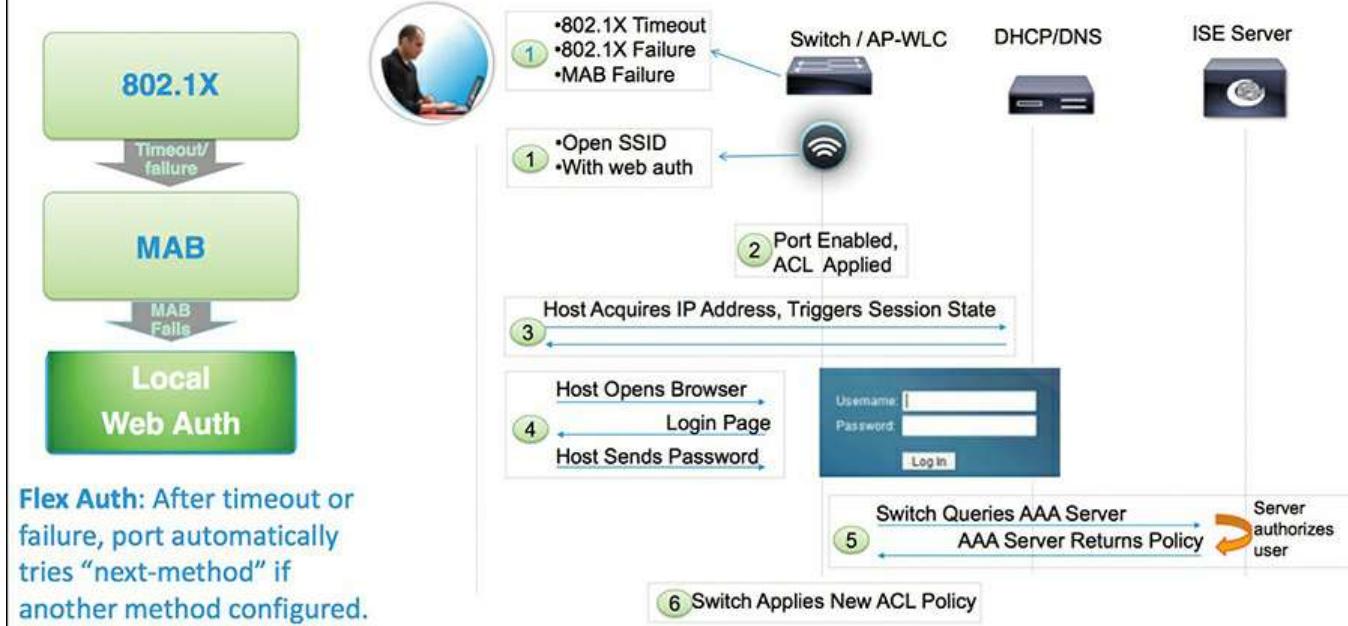


Figure 14-1 Local Web Auth Flow

Figure 14-2 shows the flow for Central Web Authentication

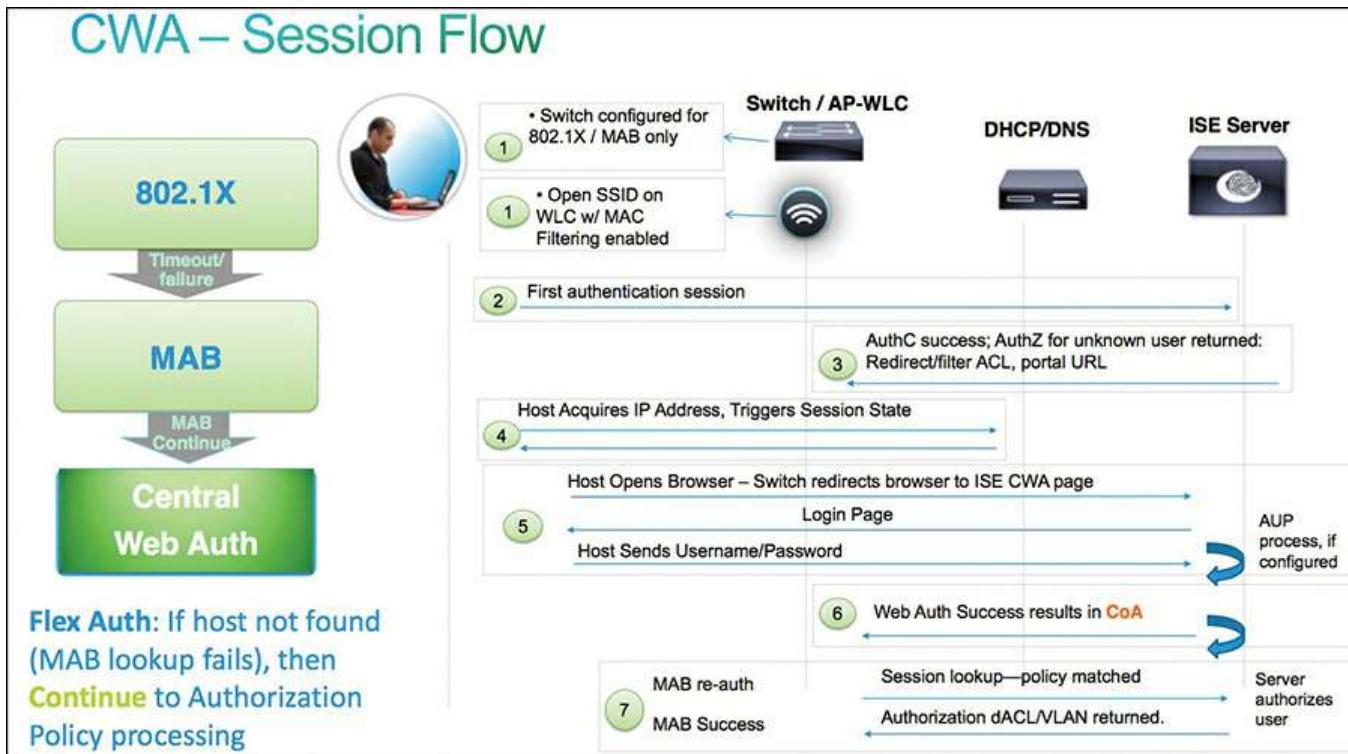


Figure 14-2 Central Web Auth Flow

The ISE guest services are available using the ISE Base license. If you decide to use posture or profiling for guests, then additional licensing applies. The ISE Policy Service Node (PSN) persona runs the guest services and web portal services.

Cisco ISE provides several methods of guest access. There are non-authenticated guest and authenticated guest options. Non-authenticated guest access is useful when you just want to provide your visitors with a hassle-free way to obtain access to the Internet. It typically involves a custom guest portal page that shows your acceptable use policy (AUP) and provides a button to click to get on the network.

Authenticated guest access requires all guests to have a username and password to gain access. These credentials are created by a guest sponsor who is typically an employee or receptionist of the company. The sponsor can select the access rights, time duration, and several other authorization guest privileges when creating the guest account. Cisco ISE also supports the creation of mass numbers of guest accounts quickly. This is useful for conferences, large meetings, and so on.

## Overview of ISE Guest Services

Cisco ISE provides the following three types of guest end-user services that you can customize. These options run on the ISE PSNs in your network.

- **Hotspot guest portal:** All visitors are redirected to a Welcome web page. They usually have to click an Accept button for an AUP to proceed, but that is configurable. ISE supports the creation of multiple customized guest portals that are selected based on criteria you specify. For example, you can create a portal for long-term contractors that is different from a visitor guest portal. Hotspot is the most popular guest portal method in use.
- **Sponsor guest portal:** Sponsored guests obtain their credentials from a sponsor. This is typically someone from the company, but can be anyone who has valid credentials to the sponsor portal in ISE. Sponsors can deliver guest account details to their visitors via email, printing, or SMS. All guest account management is handled using the sponsor web portal.
- **Self-registered guest portal:** This portal allows guests to obtain network access by creating their own accounts. The guest is presented with a registration page to fill out, which typically includes an AUP that they must accept to proceed. You can combine self-registration with sponsor approval if needed.

Each guest account must be associated with a guest type. Guest types allow a sponsor to assign different levels of access and different network connection times to a guest account. You can create your own guest types or use the following three built-in types that ISE includes:

- **Daily:** Short-term guests of less than 1 day up to 5 days
- **Weekly:** Guests of one to two weeks
- **Contractor:** Long-term guests of up to a year

Guest credentials can take many forms in ISE. The hotspot type doesn't require any credentials from guests. For the other portal types, you can choose from the following options:

- **Username/password:** Provided either by a sponsor or using self-registration. The username and password requirements are defined in the ISE guest username and guest password policies.
- **Access code:** A single shared code typically given to a group of visitors for temporary guest access. The access code can be written on the whiteboard of a classroom or handed out in printed form. Access codes can be used within all three portal types, including hotspot.
- **Registration code:** Similar to an access code except the code is for use during guest self-registration. A guest must enter a correct code to complete registration. If you want to collect some information from your guests but not allow them to self-register without some kind of credential, this method comes in handy.

## Hotspot Guest Portal Configuration

The ISE hotspot guest is the easiest method to configure and the easiest for your guest users to navigate. Hotspot guest portals do not require any user authentication; they use open mode on Wi-Fi and usually present the guest with an AUP. Here are the general steps to configure a hotspot guest portal:

**Step 1. Configure the hotspot portal:** ISE defaults are usually sufficient, with the exception of the customization necessary for the AUP and the support information page. To configure the portal, go to **Work Centers > Guest Access > Portals & Components > Guest Portals > Hotspot Guest Portal > Edit**.

**Step 2. Configure the authorization profile:** Configure a profile for web redirection to your newly created portal. Go to **Work Centers > Guest Access > Policy Elements > Results > Authorization Profiles** and click **Add**. See [Figure 14-3](#) for an example.

The screenshot shows the ISE interface under the 'Policy Elements' tab. On the left, a sidebar lists 'Conditions', 'Results', 'Allowed Protocols', 'Authorization Profiles', and 'Downloadable ACLs'. The main area is titled 'Authorization Profiles > New Authorization Profile' and contains the following fields:

- Name:** guests
- Description:** (empty)
- Access Type:** ACCESS\_ACCEPT
- Network Device Profile:** Cisco
- Service Template:** (checkbox)
- Track Movement:** (checkbox)
- Passive Identity Tracking:** (checkbox)
- Common Tasks:**
  - Voice Domain Permission (checkbox)
  - Web Redirection (CWA, MDM, NSP, CPP)** (checkbox) (selected)
- Hot Spot:** (dropdown) Hot Spot
- ACL:** (dropdown) guests
- Value:** Hotspot Guest Portal (default)

**Figure 14-3 Hotspot Authorization Profile**

**Step 3. Configure the authorization rule in your policy sets:** You need to create two rules to activate the hotspot. The first rule matches after a user successfully goes through the guest portal process. The second rule triggers the guest portal process. See [Figure 14-4](#) for an example of the rules you need to create.

▼ Authorization Policy					
▶ Exceptions (0)					
Standard					
Status	Rule Name	Conditions (identity groups and other conditions)			Permissions
	Allow_guest	AND			then Guests
	guest_portal				then guest-access

**Figure 14-4 Guest Hotspot Authorization Rules**

**Note** For information on how to configure the Cisco Wireless LAN Controller (WLC) to use ISE for guest access, see “Configure ISE Wireless CWA and Hotspot Flows with AireOS and Next Generation WLCs,” at <http://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-21/200565-Configure-ISE-Wireless-CWA-and-Hotspot-F.html>.

# Sponsored Guest Portal Configuration

The first step in configuring ISE for sponsored guest services is to define how ISE authenticates users. ISE guest services includes two special kinds of user accounts: sponsors and guests. Sponsors are employees or ISE users who have the rights to create guest accounts for visitors. You define the access method, privileges, and feature support for sponsors inside of ISE but can use an external identity source such as Active Directory. Sponsors authenticate to the sponsor portal to create guest accounts. ISE supports multiple types of authentication methods. The sections that follow outline the procedures to set up your guest sponsor portal:

- Create an Active Directory identity store
- Create ISE guest types
- Create guest sponsor groups

## Create an Active Directory Identity Store

If it has not already been created, create an Active Directory identity store. AD is the most popular ID store for sponsors, but you can skip this step and use RADIUS or internal ISE users instead.

**Step 1.** Go to **Administration > Identity Management > External Identity Sources > Active Directory**.

**Step 2.** Configure and join ISE to your Active Directory. See [Chapter 6](#) for details on joining AD.

**Step 3.** Choose or create a group in AD that will be used to specify who is a sponsor. For example, create a group called ISE Guest Sponsors and add the members who you want to be sponsors. Select and add that group to ISE as shown in [Figure 14-5](#).

The screenshot shows the 'External Identity Sources' configuration page. On the left, under 'Active Directory > AD1', there is a list of identity sources: Certificate Authentication Profile, Active Directory (selected), LDAP, RADIUS Token, and RSA SecurID. On the right, the 'Groups' tab is selected, showing a list of available Active Directory groups. The 'Add' button is highlighted, and a dropdown menu shows 'ISE Guest Sponsors' as the selected group. The list of groups includes: ise.local/Users/Contractors, ise.local/Users/Domain Admins, ise.local/Users/Domain Computers, ise.local/Users/Domain Users, ise.local/Users/Employees, ise.local/Users/Enterprise Admins, ise.local/Users/HR, ise.local/Users/ISE Administrators, and ise.local/Users/ISE Guest Sponsors.

**Figure 14-5 AD Group for Sponsors**

**Step 4.** Configure an Identity Source Sequence that includes AD. Go to **Administration > Identity Management > Identity Source Sequences**. Note the built-in group called **Sponsor\_Portal\_Sequence**, as shown at the bottom of the list in [Figure 14-6](#). Edit that group. [Figure 14-7](#) depicts making AD the first choice in the list followed by local ISE users.

The screenshot shows the 'Identity Source Sequences' page. The top navigation bar includes 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', 'pxGrid Services', 'Feed Service', and 'Threat Centric NAC'. Below this, a secondary navigation bar has links for 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences' (which is highlighted in blue), and 'Settings'. The main content area is titled 'Identity Source Sequences' with a sub-instruction 'For Policy Export go to Administration > System > Backup & Restore > Policy Export Page'. Below this is a toolbar with icons for 'Edit', 'Add', 'Duplicate', and 'Delete'. A table lists several identity sequences:

Name	Description	Identity Stores
All_User_ID_Stores	A built-in Identity Sequence to include all User Identity Stores	Preloaded_Certificate_Profile,Internal Users,All_AD_Join_Point...
Certificate_Request_Sequence	A built-in Identity Sequence for Certificate Request APIs	Internal Users,All_AD_Join_Points
Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Internal Users,Guest Users,All_AD_Join_Points
MyDevices_Portal_Sequence	A built-in Identity Sequence for the My Devices Portal	Internal Users,All_AD_Join_Points
Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal	Internal Users,All_AD_Join_Points

**Figure 14-6 Sponsor Portal Sequence List**

The screenshot shows the configuration of the 'Sponsor\_Portal\_Sequence'. The top navigation bar is identical to Figure 14-6. The main content area starts with 'Identity Source Sequences List > Sponsor\_Portal\_Sequence'. Below this is a section titled 'Identity Source Sequence' with a sub-section 'Identity Source Sequence'. It contains fields for 'Name' (set to 'Sponsor\_Portal\_Sequence') and 'Description' (set to 'A built-in Identity Sequence for the Sponsor Portal'). There is also a checkbox for 'Select Certificate Authentication Profile' which is unchecked. The next section is 'Certificate Based Authentication', which is collapsed. Below this is 'Authentication Search List', which is also collapsed. When expanded, it shows a list of available authentication sources: 'Internal Endpoints', 'Guest Users', and 'AD-SecDemo'. To the right, under 'Selected', are 'All\_AD\_Join\_Points' and 'Internal Users', with 'All\_AD\_Join\_Points' being the currently selected item. A double-headed arrow button is between the 'Available' and 'Selected' lists.

## Figure 14-7 Sponsor Portal Sequence Edit

**Step 5.** Apply the ID sequence as your sponsor authentication source. Go to **Administration > Web Portal Management > Settings > Sponsor > Authentication Source**. Select your sequence.

## Create ISE Guest Types

You need to create guest types before you create your sponsor groups because the guest types are used in the sponsor groups. Guest types provide different levels of access to different guest accounts. Sponsors must assign a guest type to a guest when creating an account, but they cannot make changes to the profiles themselves. An ISE administrator does that.

To add a custom guest type, navigate to **Work Centers > Guest Access > Portals & Components > Guest Types** and click **Create** or **Duplicate**. Fill out the information as appropriate for your needs. [Figures 14-8](#) through [14-10](#) show an example of creating a daily guest type profile.

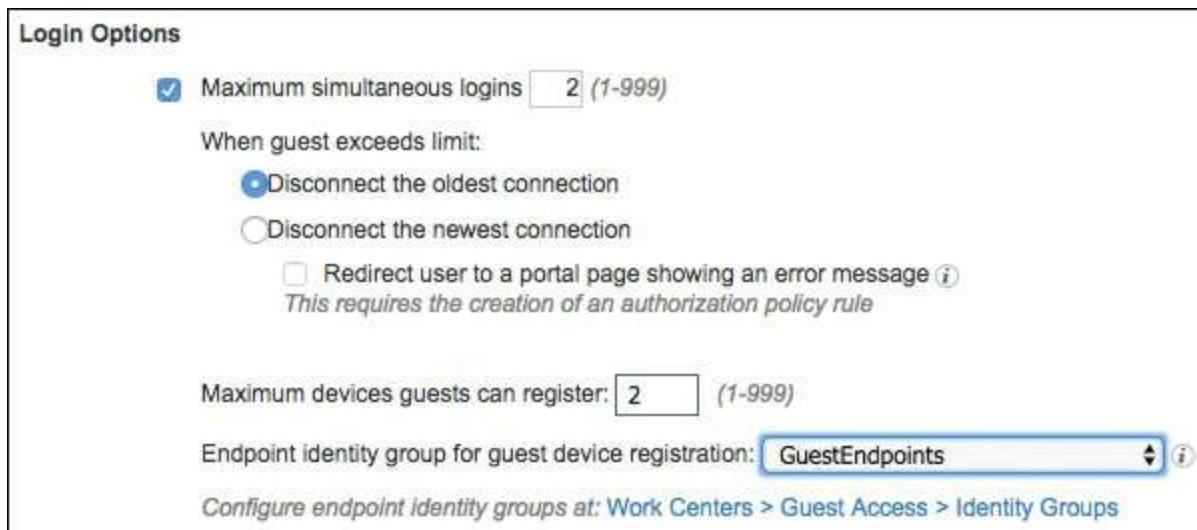
As shown in the Maximum Access Time section of [Figure 14-8](#), you can apply restrictions to both the account duration and the time period and days of week during which access is allowed. These settings can help you to ensure that visitors assigned to this basic guest type cannot use their credentials after hours or on weekends. Many businesses set the times to match their reception desk hours.

The screenshot shows the 'Guest Type' configuration page with the following fields:

- Guest type name:** \* Daily Corp Guest
- Description:** Use this for Daily corp guests
- Language File:** Language File ▾
- Collect Additional Data:** Custom Fields...
- Mobile Phone:** Mobile Phone  Required
- Tip:** Enter 7 digit phone number
- Maximum Access Time:**
  - Account duration starts:
    - From first login
    - From sponsor-specified date (or date of self-registration, if applicable)
  - Maximum account duration:
    - 10 hours Default 1 (1-999)
  - Allow access only on these days and times:
    - From 7:00 AM To 6:00 PM
    - Sun  Mon  Tue  Wed  Thu  Fri  Sat

**Figure 14-8** Guest Type Customization: Maximum Access Time

[Figure 14-9](#) shows your login options, such as the maximum number of simultaneous logins and the maximum number of guest devices that can be registered. In [Figure 14-9](#), both options are set to two. You also set the endpoint identity group to which guest devices should be added after they have registered. The default GuestEndpoints group is used in the example.



**Figure 14-9** Guest Type Customization: Login Options

[Figure 14-10](#) shows the settings available to you for notifying your guests that their account is going to expire soon. These settings are useful for weekly or long-term guest accounts. Because the present example is for creating a guest type for daily guests, there is no need to set up any notifications. [Figure 14-10](#) also shows you the sponsor accounts that are authorized to use this guest type.

**Account Expiration Notification**

Send account expiration notification  days  before account expires

View messages in: English - English

Email

Use customization from: [Self-Registered Guest Portal \(default\)](#)

Messages:

Your account is going to expire in 3 days. Please notify your sponsor to extend your account now to avoid any delays.

Send test email to me at:

Configure SMTP server at: [Work Centers > Guest Access > Administration > SMTP server](#)

SMS

Messages:

Your account is going to expire in 3 days. Please notify your sponsor to extend your account now to avoid any delays.

(160 character limit per message)\* Over 160 characters requires multiple messages.

Send test SMS to me at:  phone number

Configure SMS service provider at: [Work Centers > Guest Access > Administration > SMS Gateway Providers](#)

These sponsor groups can create this guest type:

Sponsor Groups: [ALL ACCOUNTS \(default\)](#) [GROUP ACCOUNTS \(default\)](#)

**Figure 14-10** Guest Type Customization: Expiration Notification and Sponsor Groups Assignment

## Create Guest Sponsor Groups

Now that you have created or customized the guest types, you can create sponsor groups. A sponsor is assigned the permissions from all of the groups they are members of.

ISE uses the following logic for multiple matching of sponsor groups (essentially, it adds the permissions together and defaults to the least restrictive permissions when a conflict is detected):

1. An individual permission such as “Delete guests’ accounts” is granted if it is enabled in any of the matching groups.
2. The sponsor can create guests using the guest types in any of the matching groups.
3. The sponsor can create guests at the locations in any of the matching groups.
4. For a numeric value such as a batch size limit, the largest value from the matching groups is used.

Guest sponsor configuration is accomplished in two parts: create the sponsor groups, and then create the sponsor group policies.

The following three built-in sponsor groups are available, as illustrated in [Figure 14-11](#):

- **ALL\_ACCOUNTS:** This is the super-admin group equivalent for sponsors. It allows a sponsor in this group to manage all guest accounts in the ISE network.
- **GROUP\_ACCOUNTS:** Sponsors can manage guest accounts from other sponsors in the same sponsor group.
- **OWN\_ACCOUNTS:** Sponsors can manage only the guest accounts that they have created.

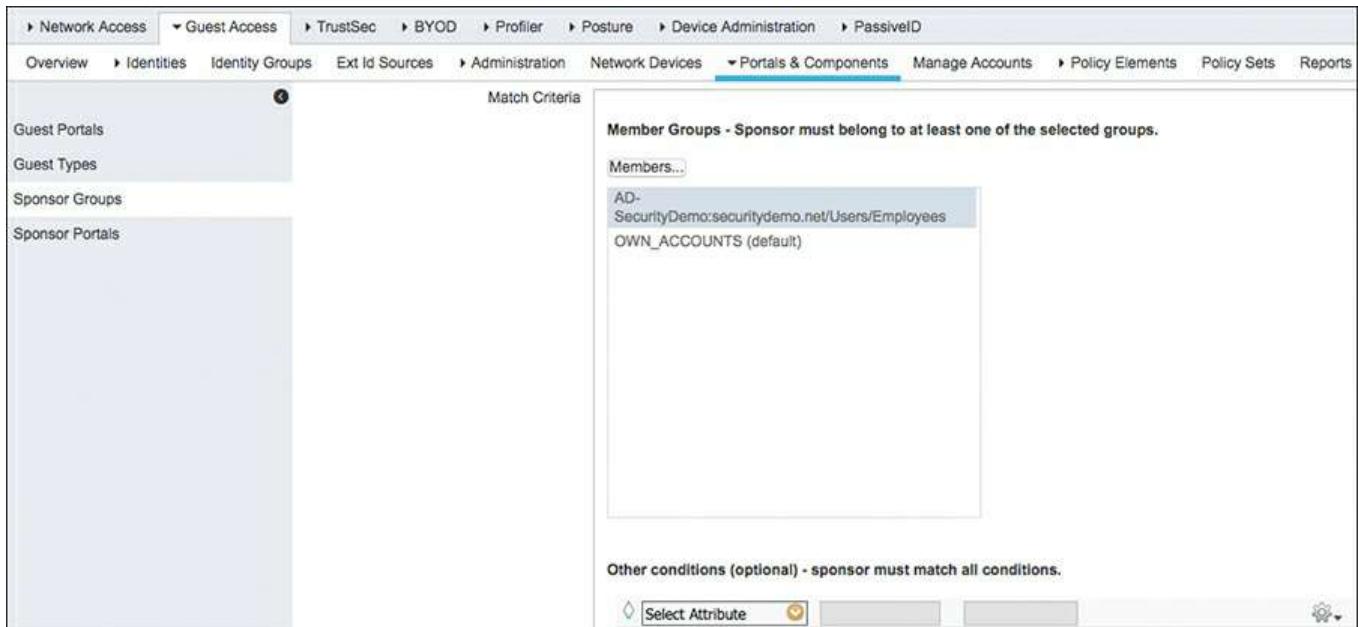
Enabled	Name	Member Groups	Other Conditions
✓	ALL_ACCOUNTS (default) Sponsors assigned to this group can manage all guest user accounts. By default, users in the ALL_ACCOUNTS user identity group are members of this sponsor group.	ALL_ACCOUNTS (default)	
✓	GROUP_ACCOUNTS (default) Sponsors assigned to this group can manage just the guest accounts created by sponsors from the same sponsor group. By default, users in the GROUP_ACCOUNTS user identity group are members of this sponsor group.	GROUP_ACCOUNTS (default)	
✓	OWN_ACCOUNTS (default) Sponsors assigned to this group can manage only the guest accounts that they have created. By default, users in the OWN_ACCOUNTS user identity group are members of this sponsor group.	OWN_ACCOUNTS (default)	

**Figure 14-11** Guest Sponsor Group Defaults

To create a new sponsor group, follow these steps from the ISE GUI:

**Step 1.** Navigate to **Work Centers > Guest Access > Portals & Components > Sponsor Groups** and click **Create** or **Duplicate**.

**Step 2.** Enter a descriptive name and description. Click **OK**. Enter the match criteria for this group. A sponsor must belong to at least one of the match criteria member groups. It is common to use an Active Directory group here. [Figure 14-12](#) shows an example of using an AD group named Employees. Optionally, you can add other conditions to the match criteria. This allows you to match just about any ISE criteria available.



**Figure 14-12** Guest Sponsor Group: Match Criteria

**Step 3.** In the Sponsor Permissions section, shown in [Figure 14-13](#), select the actions that members of the sponsor group are authorized to perform. This list represents the options that are available to the sponsor when they create a guest account.

## Sponsor Permissions

### Sponsor Can Create

- Multiple guest accounts assigned to specific guests (Import)  
Limit to batch of  (0 - 10000)
- Multiple guest accounts to be assigned to any guests (Random)  
Default username prefix:   
 Allow sponsor to specify a username prefix  
Limit to batch of:  (0 - 10000)
- Start date cannot be more than  (1 - 999) days into the future

### Sponsor Can Manage

- Only accounts sponsor has created
- Accounts created by members of this sponsor group
- All guest accounts

### Sponsor Can

- Update guests' contact information (email, Phone Number)
- View/print guests' passwords
- Send SMS notifications with guests' credentials
- Reset guests' account passwords
- Extend guest accounts
- Delete guests' accounts
- Suspend guests' accounts
  - Require sponsor to provide a reason
- Reinstate suspended guests' accounts
- Approve and view requests from self-registering guests
  - Any pending accounts
  - Only pending accounts assigned to this sponsor i
- Access Cisco ISE guest accounts using the programmatic interface (Guest REST API)

**Figure 14-13** Guest Sponsor Group: Authorization Levels

**Step 4.** Assign the guest types for which members of the sponsor group can create guest accounts. These roles can then be used in ISE authorization rules to determine guest privileges on the network. [Figure 14-14](#) shows that Daily and Weekly guest types are available to sponsors who match this group.



**Figure 14-14** Guest Sponsor Group: Guest Types

**Step 5.** Click **Save** when done.

## Authentication and Authorization Guest Policies

You now need to set up ISE for guest authentication and authorization policies. Just like in the hotspot guest configuration described previously, you need to configure ISE to trigger the guest process. Go to **Policy > Policy Sets** and select your policy. You should see a default MAC Authentication Bypass (MAB) rule in the authentication policy. The default MAB rule doesn't need any modifications for the majority of ISE customers.

## Guest Pre-Authentication Authorization Policy

If needed, refer to [Figure 14-2](#) for a refresher on the Central Web Auth flow. After successful web authentication by the guest, ISE sends a CoA to the network access device. The endpoint is then re-authenticated. This authentication results in a session lookup that now matches a policy. That policy is matched in an authorization rule in ISE, and the configured permissions are then deployed to the NAD.

You need to configure an authorization policy that matches the first time a guest connects to the network and before the guest is authenticated. The hotspot example earlier in the chapter showed how to create a policy rule to do this; in this example, use a different variation that uses the catch-all Default authorization rule instead. If none of the other rules is matched, then the Default rule is matched, as shown in [Figure 14-15](#). The example Default rule configuration initiates CWA via URL redirection of the guest to the ISE guest portal.

Authorization Policy				
Exceptions (0)				
Standard				
Status	Rule Name	Conditions (identity groups and other conditions)	then	Permissions
	Allow Guest	if <b>GuestEndpoints</b>	then	Guests
	Default	if no matches, then	Cisco_WebAuth	

**Figure 14-15** Default Authorization Policy: Guest Web Auth

The group Cisco\_WebAuth shown in [Figure 14-15](#) is a default ISE authorization profile. It is recommended that you modify this default by adding an ACL to it. This restricts guests' network access to only what is needed while they sign in.

For wired guests, create a downloadable ACL (dACL). Go to **Policy > Policy Elements > Results > Authorization > Downloadable ACLs**. Click **Add**. Create a pre-auth ACL, as shown in Example 14-1, to limit network traffic that can flow during the guest authentication process. Click **Submit**.

**Note** Downloadable ACLs are not supported on Cisco WLC. Configure an Airespace ACL name instead and preposition/preconfigure the ACL in [Example 14-1](#) on the WLC.

### Example 14-1 dACL for Wired Guests

[Click here to view code image](#)

```
permit udp any any eq bootps
permit udp any any eq domain
permit tcp any any eq domain
remark ping for troubleshooting
permit icmp any any echo
permit icmp any any echo-reply
remark allow web traffic to the ISE PSN 10.1.100.232
permit tcp any 10.1.100.232 eq 80
permit tcp any 10.1.100.232 eq 443
remark allow internet-only web traffic to kick off redirect
deny tcp any <Internal networks> eq 80
deny tcp any <Internal networks> eq 443
permit tcp any any eq 80
permit tcp any any eq 443
remark 10.1.100.232 is the ISE PSN for Guest Portal
permit tcp any host 10.1.100.232 eq 8443
permit tcp any host 10.1.100.232 eq 8905
permit tcp any host 10.1.100.232 eq 8909
permit udp any host 10.1.100.232 range 8905 8906
permit udp any host 10.1.100.232 eq 8909
deny ip any any
```

Port 8443 is used by the ISE guest portal by default. Ports 8905 and 8906 are used by the NAC Agent SWISS protocol. Port 8909 is used for client provisioning activity.

If deploying for wireless guests, be sure you enable the Airespace ACL name as part of your policy. ISE will call the ACL that is configured on the WLC. It does not download the ACL. The following are the steps to create an Authorization Policy.

**Step 1.** Go to **Policy > Policy Elements > Results > Authorization > Authorization Policies**. Edit the default Cisco\_WebAuth policy.

**Step 2.** Under Common Tasks, select your dACL name. The dACL will be downloaded to the NAD by ISE. If this is for wireless guests, then instead populate the Airespace ACL field with the name of the ACL you configured on the WLC.

**Step 3.** The default Cisco\_WebAuth policy references the web-redirect ACL name of ACL-WEBAUTH-REDIRECT. You need to pre-position this ACL on the switch

or WLC. For wired switches, the contents of ACL-WEBAUTH-REDIRECT should include the following (10.1.100.232=ISE PSN):

[Click here to view code image](#)

```
ip access-list extended ACL-WEBAUTH-REDIRECT
deny ip any host 10.1.100.232
permit tcp any any eq www
permit tcp any any eq 443
permit tcp any any eq 8443
remark be sure to include any proxy ports you have enabled
permit tcp any any eq 8080
```

On a switch, any ACL statement with a **permit** will force a URL redirect. This ACL does not permit and deny traffic; it only defines what ports kick off a URL redirect. For wireless, **deny** rules force a URL redirect. Rewrite the preceding wired ACL as necessary.

**Step 4.** Add your newly created authorization profile to the default authorization policy rule. Go to **Policy > Policy Sets > Authorization**. Click **Edit** on the last rule in the list called Default. Select your Cisco\_WebAuth policy, as shown previously in [Figure 14-15](#). Click **Done** and then **Save**.

## Guest Post-Authentication Authorization Policy

Once the guest successfully authenticates using their guest account credentials, ISE issues a Change of Authorization (CoA) request to the NAD. This time, the MAB session lookup matches. You need to configure an authorization policy in ISE to set the guest network permissions you want to allow. Go to **Policy > Policy Sets** and select your policy. Under Authorization Policy, click the down-arrow icon on the left side and follow these steps:

**Step 1.** Enter a descriptive rule name, such as Allow Guest.

**Step 2.** Select the identity groups that you want to match on. Common examples are GuestEndPoints, GuestType\_Daily, and GuestType\_Weekly. Remember that each identity group must match the guest type that the sponsor assigned to the guest account upon its creation. If you have multiple guest roles, then you need to create multiple authorization rules. Each rule provides different permissions to the guest.

**Step 3.** Assign the permissions, such as guest Internet only web. You can pick from your list of authorization profiles or create a new one by clicking the gear icon and selecting **Add New Standard Profile**. The most common permission elements are dACL, Airespace ACL, Security Group Tag, and VLAN. [Figure 14-16](#) shows an example.

Authorization Policy	
Exceptions (0)	
Standard	
Status	Rule Name
<input checked="" type="checkbox"/>	Allow Guest
	if <b>GuestEndpoints OR GuestType_Daily (default) OR GuestType_Weekly (default)</b>
	then Guests
<input checked="" type="checkbox"/>	Default
	if no matches, then Cisco_WebAuth

**Figure 14-16 Guest Authorization Rule**

Remember that authorization rules, by default, are processed from the top down until the first match. Be sure your guest rules are in the appropriate order. Your authenticated guest access rule needs to precede the WebAuth redirection rule.

## Guest Sponsor Portal Configuration

Sponsors are responsible for creating guest accounts for authorized visitors who need limited network or Internet-only connectivity while onsite. Typically, sponsors are allowed to create, send, and manage guest accounts. You need to configure the sponsor portal to allow sponsors to create guest accounts. ISE includes a default sponsor portal for you to use as well.

Set up the method you will use to authenticate your sponsors. This was covered previously in the “Create an Active Directory Identity Store” section but is mentioned here for a refresher. In most cases, Active Directory is used. Go to **Work Centers > Guest Access > Identities > Identity Source Sequences**. The built-in sequence is called **Sponsor\_Portal\_Sequence** and includes the identity stores Internal Users and **All\_AD\_Join\_Points**. You can use this sequence or create your own.

## Guest Portal Interface and IP Configuration

It is a best practice to configure your guest portal on its own ISE physical interface with its own IP address. This drastically reduces the security risk of an ISE compromise. Separating the admin portal from the guest portal provides some of this added security. You can specify the port used for each web portal, allowing you to use different ports for the end-user portals, such as Sponsor, Guest (also Client Provisioning), My Devices, and Blacklist. The Blacklist portal should be kept all alone on its own interface with its own IP address. This is also true for the admin configuration portal, which always uses Ethernet0 and a default port of HTTPS/443. To configure a sponsor portal or edit the default, go to **Work Centers > Guest Access > Portals & Components > Sponsor Portals**.

## Sponsor and Guest Portal Customization

The ISE sponsor portal can be completely customized to fit your organization's needs. Every button, label, icon, and text can be customized. ISE lets you customize the sponsor portal in just about any way you can dream up. Also covered in this section is "Guest Portal Behavior and Flow Settings," "Guest Portal Page Customization," and "Creating Multiple Guest Portals. The Sponsor Settings and Customization configuration screen located at **Work Centers > Guest Access > Portals & Components > Sponsor Portals** has two pages:

- Portal Behavior and Flow Settings
- Portal Page Customization

### Sponsor Portal Behavior and Flow Settings

The Portal Behavior and Flow Settings page has a bunch of settings you can configure. [Figure 14-17](#) depicts the various sections available. The most commonly used sections are Portal Settings, Login Settings, and AUP Page Settings.

Under Portal Settings, it is typical to input a vanity URL in the Fully Qualified Domain Names (FQDN) and Host Names field. This makes it easier for your employees/sponsors to remember where they go to register guests. Be sure to configure the DNS server so that it resolves the FQDN to the sponsor portal IP address. [Figure 14-17](#) shows it populated with sponsors.acme.com.

TrustSec > BYOO > Profiler > Posture > Device Administration > PassivID

Ext Id Sources > Administration > Network Devices > Portals & Components > Manage Accounts > Policy Elements > Policy Sets > Reports > Custom Portal Files > Settings

**Portal & Page Settings**

**Portal Settings**

HTTPS port: 8445

Allowed: Make selections in one or both columns based on your PSN configurations.

Interfaces: If bonding is not configured ( ), on a PSN, use:

- Gigabit Ethernet 0
- Gigabit Ethernet 1
- Gigabit Ethernet 2
- Gigabit Ethernet 3
- Gigabit Ethernet 4
- Gigabit Ethernet 5

If bonding is configured ( ), on a PSN, use:

- Bond 0  
Uses Gigabit Ethernet 0 as primary, 1 as backup.
- Bond 1  
Uses Gigabit Ethernet 2 as primary, 3 as backup.
- Bond 2  
Uses Gigabit Ethernet 4 as primary, 5 as backup.

Certificate: Default Portal Certificate Group

group: Configure certificates at:  
tag: Work Centers > Guest Access > Administration > System Certificates

Fully qualified domain names: sponsors.acme.com (FQDN)

and host names:

Identity: Sponsor\_Portal\_Sequence

Source: Configure authentication methods at:  
sequence: Work Centers > Guest Access > Identities > Identity Source Sequences  
Work Centers > Guest Access > Ext Id Sources > SAML Identity Providers

Idle timeout: 10 (0-20 min)

Display: Use browser locale

language: Fallback language: English - English

Always use English - English

SSIDs available to sponsors:

**Login Settings**

Maximum failed login attempts before rate limiting: 5 (1 - 999)

Time between login attempts when rate limiting: 2 minutes(1 - 3000)

Include an AUP as link

Require acceptance

**Acceptable Use Policy (AUP) Page Settings**

Include an AUP page

Require scrolling to end of AUP

Show AUP:

- On first login only
- On every login
- Every 7 days (starting at first login)

**Sponsor Change Password Settings**

**Post-Login Banner Settings**

**Support Information Page Settings**

**Sponsor Portal Application Settings**

**Sponsor Flow (based on settings)**

```

graph TD
    LOGIN[LOGIN] --> AUP[AUP]
    AUP --> SP[Sponsor Home]
    SP --- SC[Sponsor Portal]
    SC --- AUTH[AUTHENTICATE (if required)]
    AUTH --- APPROVE[APPROVE/DENY (if required)]
  
```

The diagram illustrates the Sponsor Flow based on settings. It starts with a **LOGIN** step, followed by an **AUP** step, and finally the **Sponsor Home**. An optional **Sponsor Portal** step is shown above the flow. To the right, a **Single Click Approval** section shows a vertical flow: **AUTHENTICATE (if required)** leads to **APPROVE/DENY (if required)**.

Figure 14-17 Sponsor Portal Behavior and Flow Settings

Note the Sponsor Flow diagram to the right of the Portal Settings section. The diagram changes as you change your settings.

**Note** Ensure that any ISE PSN certificates that you have also include the vanity URL FQDN in their Subject Alternative Name. This prevents certificate mismatch warnings from popping up on the sponsor's browser.

## Sponsor Portal Page Customization

On the Portal Page Customization page, you can customize all aspects of the portal, including its text, color, theme, graphics, button, and so forth, as shown in [Figure 14-18](#). This page also allows you to customize the Acceptable Usage Policy (AUP) and guest notification messages, such as emails, SMS, and printed credentials. Typically, customizing the sponsor portal experience to your business requires that you spend some time here.

The screenshot shows the Oracle Identity Services Engine interface with the following navigation paths:

- Home > Context Validity > Operations > Policy > Administration > Work Centers
- Network Access > Guest Access > ShiroEBC > BYOD > Profile > Policies > Device Administration > PassiveID
- Overview > Identities > Identity Groups > Ext ID Sources > Administration > Network Devices > Ports & Components > Manage Accounts > Policy Elements > Policy Sets > Reports > Custom Portal Files > Settings

The main content area is titled "Sponsor Settings and Customization". It includes fields for "Portal Name" (Sponsor Portal) and "Description" (Default portal used by sponsors to create and manage accounts for authors). Buttons for "Save" and "Close" are available.

Two tabs are present: "Portal Behavior and Flow Settings" (selected) and "Portal Page Customization". The "Portal Page Customization" tab is described as "Customize portal pages by applying a theme and specifying their names and versions for deployment to work centers".

The "Global Page Customizations" section contains "Portal Theme" (Default Blue theme), "Test Site", "Advanced Customization", and "View In" (English - English).

The "Page Customizations" section lists various pages for customization, including:

- Portal Access:** Login, Acceptable Use Policy, Change Password, Support Information, Sponsor Portal Settings, Error.
- Create Accounts:** Guest Types, Create Account for Known Guests, Create Account for Random Guests, Create Account for Imported Guests, Guest Access Information.
- Notify Guests:** Notify Known Guests, Notify Random Guests, Notify Imported Guests (Desktop only).
- Email Notifications:** Email Notification (selected), SMS Notification, Print Notification.
- Manage & Approve:** Accounts, Account Details View, Edit Account (Pop-up), External Account (Pop-up), Reset Password (Pop-up), Suspend Account (Pop-up), Print, Delete, Resend, Reinstated.
- Pending Accounts:** Pending Accounts List View (Approve/Deny), Pending Account Details View (Approve/Deny), Notice List/Details, Authenticate Approver from Email Request.
- Message:** Account Actions Messages, General Sponsor Portal Messages.

The "Email Notification" configuration pane shows "Subject" (Your Guest Account Credentials), "Email Introduction Text" (with rich text editor controls), and a "Send" button. A checkbox for "Send username and password separately" is also present.

Figure 14-18 Sponsor Portal Page Customization

Once you click **Save**, the PSN automatically applies the changes so that they take effect immediately. However, the PSN continues its other services uninterrupted.

## **Guest Portal Behavior and Flow Settings**

The customization for the sponsored guest portal is very similar to the customization for the sponsor portal. Go to **Work Centers > Guest Access > Portals & Components > Guest Portals**. Select and edit the default Sponsored Guest Portal or create a new one. [Figure 14-19](#) shows the Portal Behavior and Flow Settings page with the most commonly modified sections expanded so you can see the settings. Configure the settings to meet your needs.

**Portal Settings and Customization**

Portal Name: \* Sponsored Guest Portal (default) Description: Sponsor's create guest accounts, and guests access the network using their portal URL.

Language File: \*

**Portal Behavior and Flow Settings**

Use these settings to specify the guest experience for the portal.

**Portal & Page Settings**

**Guest Flow (Based on settings)**

```

graph TD
    LOON[LOON] --> AUP[AUP]
    AUP --> MaxNetworkReached[Max Network Reached]
    MaxNetworkReached --> PostLoginBanner[Post Login Banner]
    PostLoginBanner --> Success[Success]
  
```

**Acceptable Use Policy (AUP) Page Settings**

- Include an AUP page
- Use different AUP for employees
- Skip AUP for employees
- Require scrolling to end of AUP

Show AUP

- On first login only
- On every login
- Every \_\_\_\_\_ days (starting at first login)

**Guest Change Password Settings**

**Guest Device Registration Settings**

- Automatically register guest devices

A message displays to guests when they reach the maximum number of supported devices.

**BYOD Settings**

**Guest Device Compliance Settings**

**Post-Login Banner Page Settings**

**VLAN DHCP Release Page Settings**

**Authentication Success Settings**

Once authenticated, take guest to:

- Original URL
- Authentication Success page
- URL: \_\_\_\_\_  
E.g. Cisco-Off, www.cisco.com or TSS.Cisco-Off

**Support Information Page Settings**

**Figure 14-19 Sponsored Guest Portal Behavior and Flow Settings**

## **Guest Portal Page Customization**

Like the sponsor portal page, you can customize the guest portal pages. It is very common to customize these pages so that the guest portal is branded to your business. The Portal Theme selection sets the colors, fonts, graphics, and so forth for all of the portal pages. [Figure 14-20](#) shows the various options available.

The screenshot shows the 'Portals Settings and Customization' page under 'Portals & Components'. At the top, there's a 'Portal Name' field set to 'Sponsored Guest Portal (default)' with a description: 'Sponsors create guest accounts, and guests access the network using their Portal test URL.' There are 'Save' and 'Close' buttons.

In the center, there are two main sections: 'Portal Behavior and Flow Settings' and 'Portal Page Customization'. The 'Portal Page Customization' section is expanded, showing 'Text Elements' (Banner title: 'Sponsored Guest Portal', Contact: 'Contact Support') and 'Footer Elements' (empty). Below this, there are tabs for 'Portal Theme' (Default Olive theme), 'Tweaks...', 'Advanced Customization...', and 'View In' (English - English).

On the left, there's a sidebar for 'Global Page Customizations' with sections for 'Images' (Logo (Mobile), Logo (Desktop), Banner Image, Background Image) and 'Text Elements' (Banner title, Contact). On the right, there's a 'Pages' sidebar with options like 'Pages', 'Login', 'Acceptable Use Policy', etc., and a 'Page Customizations' area for the 'Sign On' page, which includes a rich text editor and static text areas for content title and instructional text.

A preview window on the right shows the final look of the 'Sponsored Guest Po...' portal, featuring a 'Sign On' form with fields for 'Username' and 'Password' and a 'Sign On' button. There are also 'Refresh Preview' and 'Desktop Preview' buttons.

**Figure 14-20** Sponsored Guest Portal Page Customization

As shown in [Figure 14-20](#), you can upload your own logos and images from your local PC. All saved changes take effect immediately. To view your changes before you save, click the **Desktop Preview** hyperlink. This opens your browser to the portal so that you can see what it looks like.

Here are some of the tips for getting your theme right:

- Upload a .jpeg, .gif, or .png image file to use as the logo on the portal Login page for the Guest, Sponsor, and My Devices portals.
- When you upload an image, it is automatically resized to fit an image size required for that area. (See ISE help for details on image sizes.) To avoid distortion, resize your image to fit these dimensions:
  - Login logo and banner logo image size of 86 pixels (width) by 45 pixels (height).
  - Login background image size is 533 pixels (width) by 325 pixels (height).
  - Banner background image size is 133 pixels (height). The width is not controlled, and the banner background color displays to fill the remaining area.
- The post-login banner displays for 15 seconds.

## Creating Multiple Guest Portals

In some cases, you might want to create multiple portals for different uses. For example, you might have different business groups that each need their own name on the guest portal. Configuring multiple portals is fairly straightforward. Here are the steps required:

- Step 1.** Create one or more guest portals at **Work Centers > Guest Access > Portals & Components > Guest Portals**, as previously described.
- Step 2.** Create an authorization profile for each portal (**Work Centers > Guest Access > Policy Elements > Results > Authorization Profiles > Add**). For each element, select the Web Redirection value under Common Tasks to equal the portal name you created. Repeat this for each portal.
- Step 3.** Use the portal in an authorization policy rule. Go to **Policy > Policy Sets**. Select your policy and scroll down to the Authorization section. Add a new rule at the bottom, right above the Default rule. Specify the conditions for which you want this particular guest portal to be selected. You should also include a condition for endpoint=unknown. Then, add other conditions to specify where you want the portal to be used. [Figure 14-21](#) shows an example using location of the NAD.

Authorization Policy			
Exceptions (0)			
Standard			
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Allow Guest	If GuestEndpoints OR GuestType_Daily (default) OR GuestType_Weekly (default)	then Guests
<input type="checkbox"/> <input checked="" type="checkbox"/>	DeptA Guest Portal	If Unknown AND DEVICE:Location EQUALS All Locations#NorthAmerica#CLT	then Guest_deptA
<input checked="" type="checkbox"/>	Default	If no matches, then	Cisco_WebAuth

Figure 14-21 Multi-Portal Authorization Rule

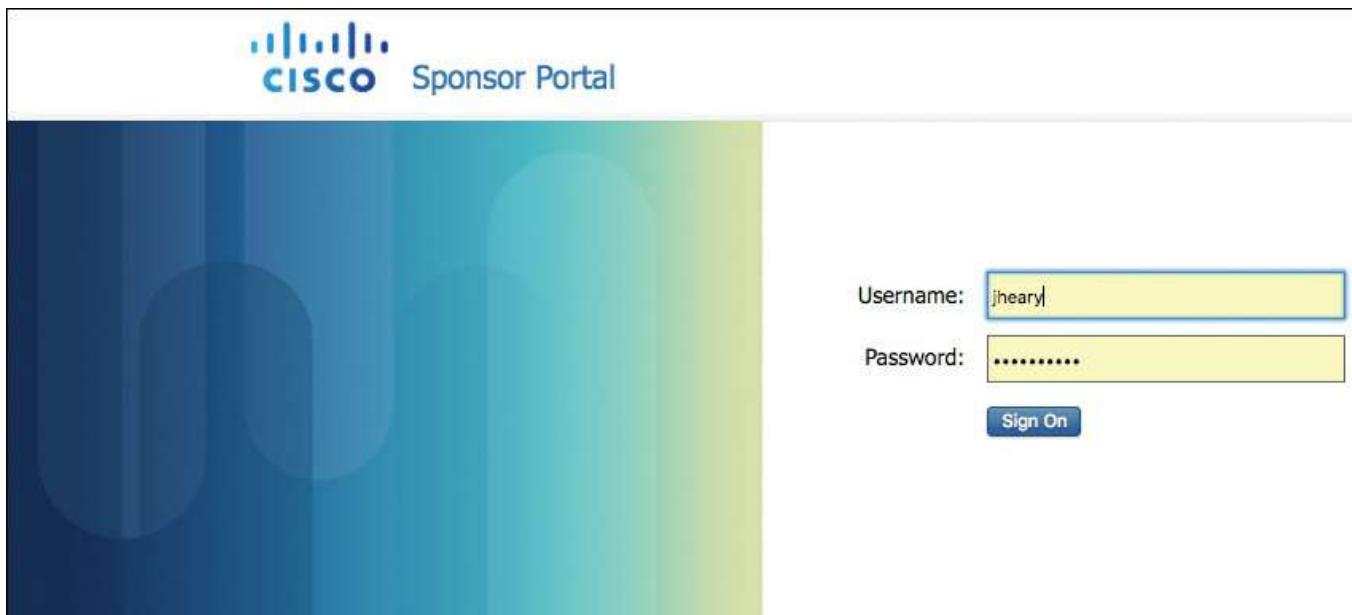
## Guest Sponsor Portal Usage

This section explains the usage of the sponsor portal. The main topics addressed are

- Portal layout
- Creating guest accounts
- Managing guest accounts

## Sponsor Portal Layout

To access the ISE sponsor portal, open your browser to the vanity URL you configured, such as [sponsors.acme.com](https://sponsors.acme.com), or go to `https://<IP address of ISE PSN with portal>:8443/sponsorportal/`. You will see the Sponsor Portal login page, along with any customization you have made to the portal. [Figure 14-22](#) shows an example Sponsor Portal login page.



**Figure 14-22** Sponsor Portal Login

At the bottom of the page is a link to help (not shown).

Once logged in, you see a page similar to [Figure 14-23](#). The options on your screen vary depending on the sponsor privileges you have. [Figure 14-23](#) depicts an account with restricted sponsor privileges.

Username	Status	First Name	Last Name	Email Address
jheary@appledreams.com	Awaiting Initial Login	Liam	Heary	jheary@appledreams.com

**Figure 14-23** Sponsor Portal Home Page

The first thing you should do is review/update your sponsor settings. Click **My Settings** in the top-right corner. Set up your email address as a minimum.

## Creating Guest Accounts

From the sponsor portal home page, there are three ways to create guest accounts:

- **Create Account:** Creates a single guest account
- **Import Accounts:** Uses an Excel spreadsheet to import multiple accounts. The spreadsheet template is available for download from this option.
- **Create Random Accounts:** Allows you to quickly generate a lot of guest accounts at once

To perform one of these options, just click its icon. [Figure 14-24](#) shows the form for Create Account.

## Create Account

\* First name: Liam

\* Last name: Heary

\* Email address: jheary@appledreams.com  Send email notification

\* Company: Appledreams

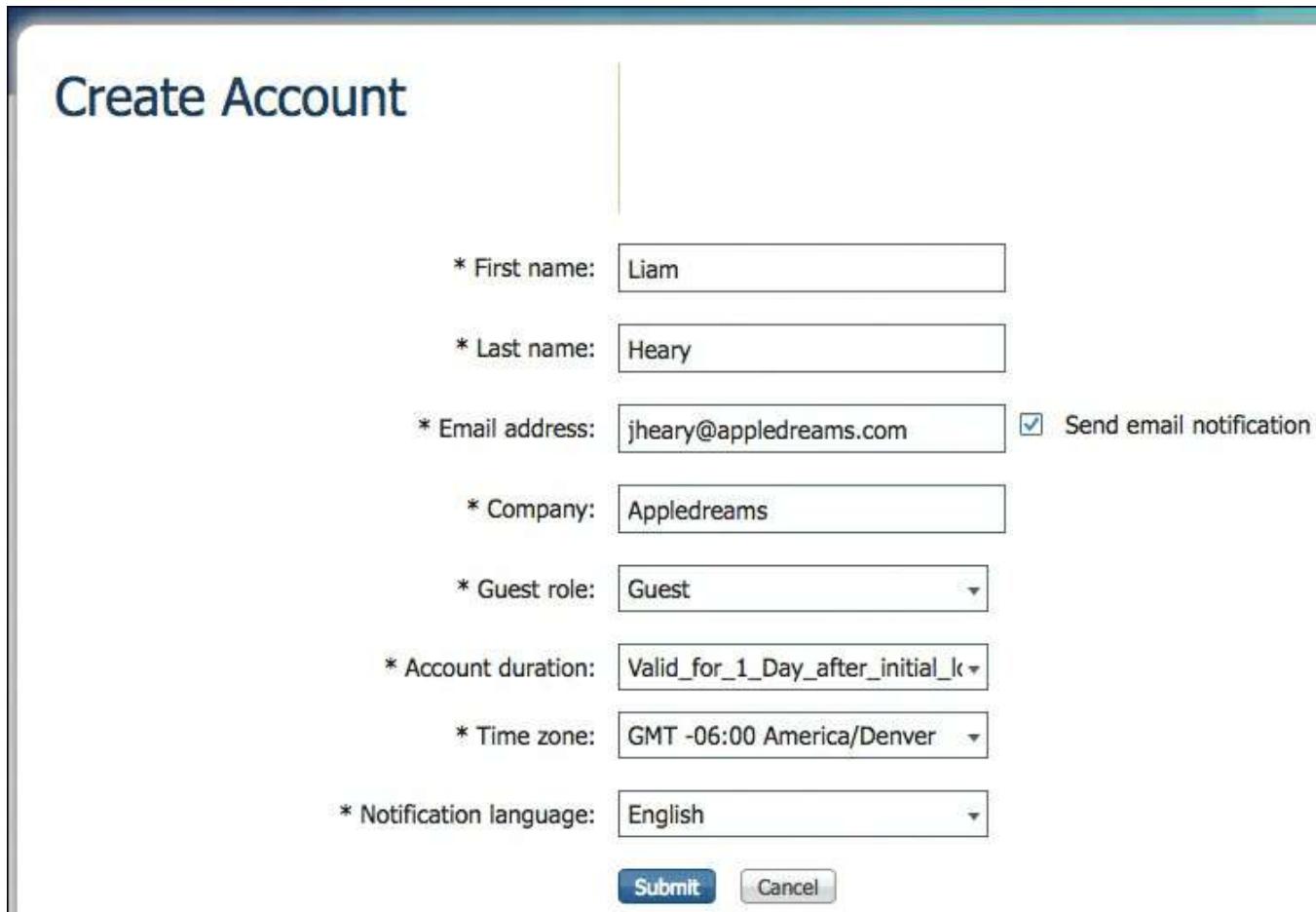
\* Guest role: Guest

\* Account duration: Valid\_for\_1\_Day\_after\_initial\_k

\* Time zone: GMT -06:00 America/Denver

\* Notification language: English

**Submit** **Cancel**



**Figure 14-24** Sponsor Portal: Guest Account Creation

Fill out the required fields and click **Submit**. The credentials are emailed to the guest. If you would like to print the credentials, go back to the sponsor portal home page, select the account, and click **Print**.

## Managing Guest Accounts

Your ability to manage guest accounts depends on the privileges of your sponsor account. You can perform the following actions on an existing guest account:

- Edit
- Notify (email, text, print)
- Reinstate (activates a previously suspended account)
- Suspend
- Delete
- Change account duration

To perform one of the actions, select an account and click the action (refer to [Figure 14-23](#)).

# Configuration of Network Devices for Guest CWA

With ISE ready to serve as your Central Web Auth source, the next step is to configure your switches and WLCs. This process is straightforward and simple.

## Wired Switches

This configuration assumes that you already have the switch configured to communicate with ISE. If not, see [Chapter 11, “Bootstrapping Network Access Devices,”](#) for details. This example demonstrates using an ACL that is configured directly on the switch instead of using a dACL from ISE, as was shown previously in this chapter. The most common method deployed for wired is dACL, so this example is presented here for completeness of your options.

There are three steps to enabling CWA on your switches:

**Step 1.** Configure a pre-authentication ACL on the switch. This determines what traffic is allowed to flow before authentication happens. Here is an example ACL:

[Click here to view code image](#)

```
ip access-list extended webauth
permit udp any any eq bootps
permit udp any any eq domain
permit tcp any any eq domain
remark ping for troubleshooting
permit icmp any any echo
permit icmp any any echo-reply
remark allow web traffic to kick off redirect
permit tcp any any eq www
permit tcp any any eq 443
remark 10.1.100.232 is the ISE PSN for Guest Portal
permit tcp any host 10.1.100.232 eq 8443
permit tcp any host 10.1.100.232 eq 8905
permit tcp any host 10.1.100.232 eq 8909
permit udp any host 10.1.100.232 range 8905 8906
permit udp any host 10.1.100.232 eq 8909
```

**Step 2.** Configure a redirect ACL on the switch. Any traffic that matches a **permit** statement is redirected to the guest URL. Here is a sample ACL:

[Click here to view code image](#)

```
ip access-list extended ACL-WEBAUTH-REDIRECT
deny ip any host 10.1.100.232
permit tcp any any eq www
permit tcp any any eq 443
```

```
permit tcp any any eq 8443
remark be sure to include any proxy ports you have enabled
permit tcp any any eq 8080
```

### Step 3. Configure your switch for HTTP and ports for MAB and apply ACLs:

[Click here to view code image](#)

```
ip http server
ip http secure-server
interface GigabitEthernet1/0/12
description ISE1 - dot1x clients - UCS Eth0
switchport access vlan 100
switchport mode access
ip access-group webauth in
authentication order mab
authentication priority mab
authentication port-control auto
mab
spanning-tree portfast
```

You can use the **show auth sess int gi1/12** switch command to see the session info.

## Wireless LAN Controllers

Configuring the Cisco WLC for CWA is a three-step process. These steps assume that you already have the basic WLC to ISE configuration completed. If not, see [Chapter 11](#) for more details. Follow these steps to get up and running:

**Step 1.** Ensure that the RADIUS server has Support for CoA set to Enabled, which is the default, as shown in [Figure 14-25](#).

The screenshot shows the Cisco Wireless LAN Controller (WLC) web interface. The top navigation bar includes links for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (which is highlighted in orange), and MANA. On the left, a sidebar under the 'Security' heading lists various AAA and EAP options. The main content area is titled 'RADIUS Authentication Servers > Edit'. It displays configuration settings for a RADIUS server:

Server Index	4
Server Address(Ipv4/Ipv6)	10.48.39.161
Shared Secret Format	ASCII ▾
Shared Secret	•••
Confirm Shared Secret	•••
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and r
Port Number	1812
Server Status	Enabled ▾
Support for CoA	Enabled ▾
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input type="checkbox"/> Enable
Management Retransmit Timeout	2 seconds
Realm List	
IPSec	<input type="checkbox"/> Enable

Figure 14-25 Support for CoA

**Step 2.** Select or create your guest WLAN and SSID. Edit the WLAN and go to **Security > Layer 2**. Enable **MAC Filtering**, as shown in [Figure 14-26](#).



Figure 14-26 WLC MAC Filtering

**Step 3.** Go to **Security > Layer 3**. From the Layer 3 Security drop-down list, choose **None** as shown in [Figure 14-27](#).

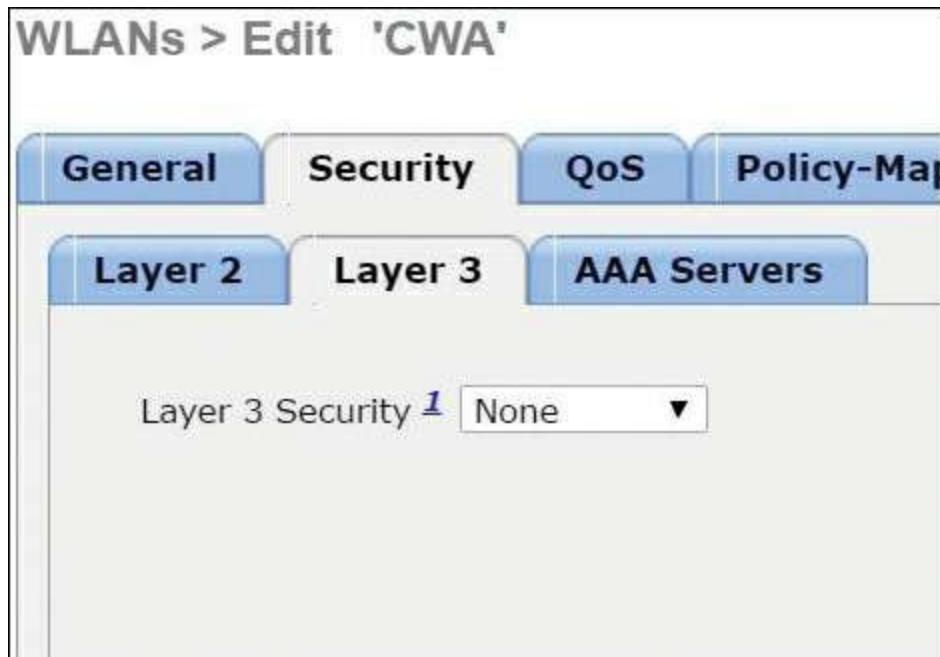
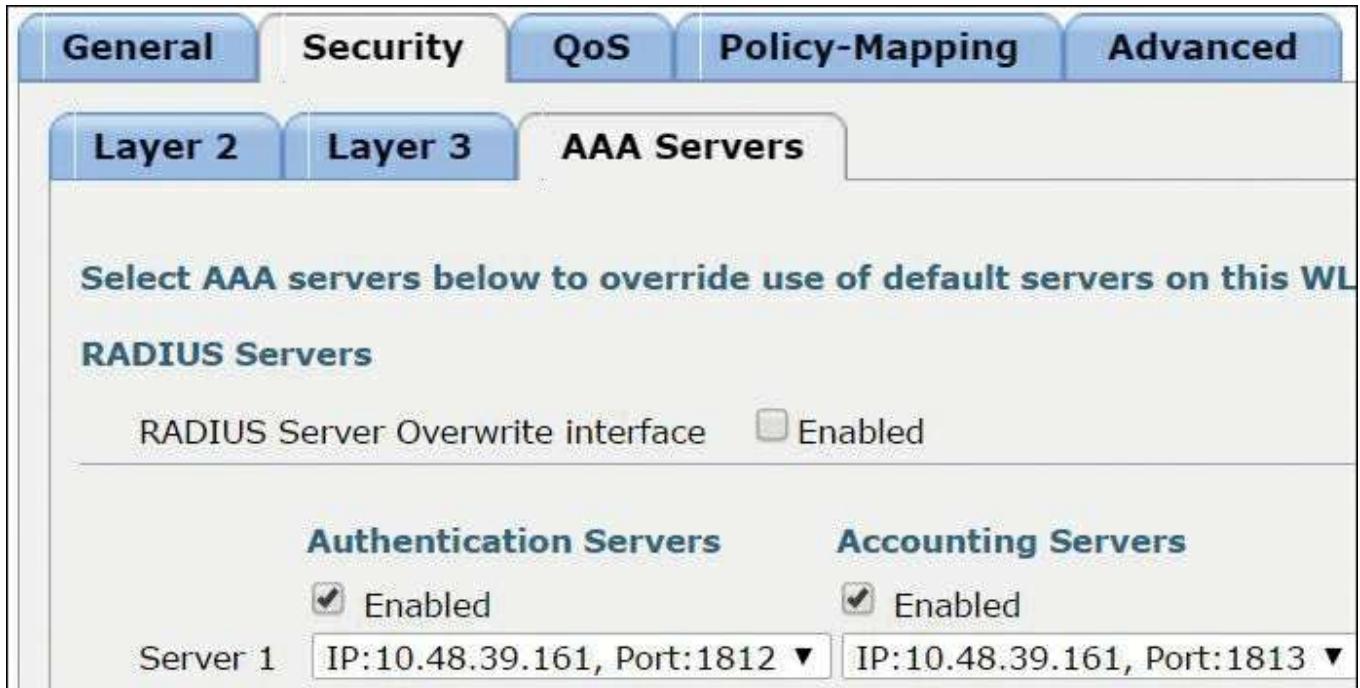


Figure 14-27 WLC Layer 3

**Step 4.** Go to **Security > AAA Servers**. Add ISE AAA, as shown in [Figure 14-28](#). When deploying ISE in your wireless network, do not configure a primary and secondary ISE server. Instead, configure high availability (HA) between the two ISE servers. Having a primary and secondary ISE setup requires a posture validation to happen before the client moves to the RUN state. If HA is configured, the client is automatically moved to the RUN state in the fallback ISE

server.

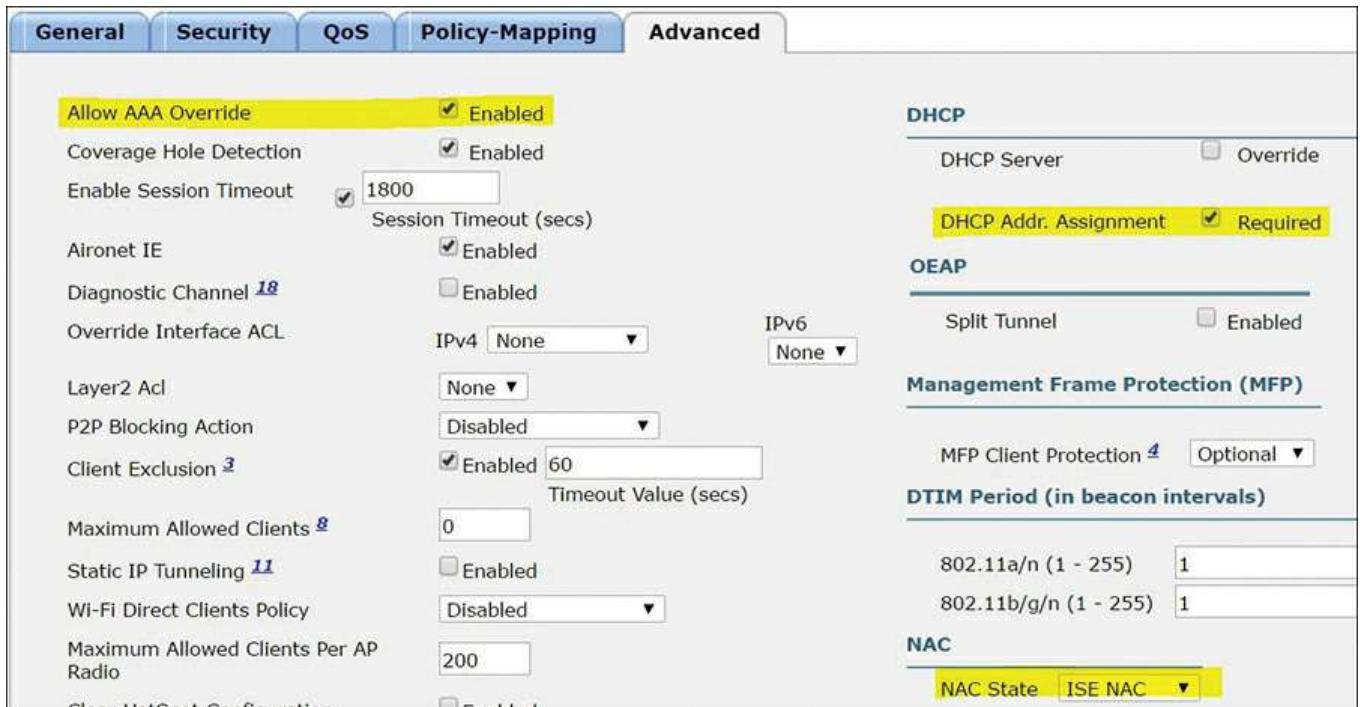


The screenshot shows the 'AAA Servers' tab under the 'Security' section of the WLC configuration. It displays settings for RADIUS servers, including authentication and accounting servers, and their respective IP addresses and ports.

Authentication Servers		Accounting Servers	
<input checked="" type="checkbox"/> Enabled		<input checked="" type="checkbox"/> Enabled	
Server 1	IP:10.48.39.161, Port:1812 ▾	IP:10.48.39.161, Port:1813 ▾	

Figure 14-28 WLC AAA Servers

**Step 5.** Click the **Advanced** tab. Enable the settings shown highlighted in [Figure 14-29](#).



The screenshot shows the 'Advanced' tab of the WLC configuration. It includes sections for Allow AAA Override, DHCP, OEAP, Management Frame Protection (MFP), DTIM Period (in beacon intervals), and NAC.

Allow AAA Override	<input checked="" type="checkbox"/> Enabled
Coverage Hole Detection	<input checked="" type="checkbox"/> Enabled
Enable Session Timeout	<input checked="" type="checkbox"/> 1800 Session Timeout (secs)
Aironet IE	<input checked="" type="checkbox"/> Enabled
Diagnostic Channel <a href="#">18</a>	<input type="checkbox"/> Enabled
Override Interface ACL	IPv4 <a href="#">None</a> IPv6 <a href="#">None</a>
Layer2 Acl	<a href="#">None</a>
P2P Blocking Action	<a href="#">Disabled</a>
Client Exclusion <a href="#">3</a>	<input checked="" type="checkbox"/> Enabled 60 Timeout Value (secs)
Maximum Allowed Clients <a href="#">8</a>	<a href="#">0</a>
Static IP Tunneling <a href="#">11</a>	<input type="checkbox"/> Enabled
Wi-Fi Direct Clients Policy	<a href="#">Disabled</a>
Maximum Allowed Clients Per AP Radio	<a href="#">200</a>
Clear HotSpot Configuration	<input type="checkbox"/> Enabled

**DHCP**  
DHCP Server  Override  
DHCP Addr. Assignment  Required

**OEAP**  
Split Tunnel  Enabled

**Management Frame Protection (MFP)**  
MFP Client Protection [4](#)  Optional

**DTIM Period (in beacon intervals)**  
802.11a/n (1 - 255) [1](#)  
802.11b/g/n (1 - 255) [1](#)

**NAC**  
NAC State [ISE NAC](#)

Figure 14-29 WLC Advanced Tab

**Step 6.** Create the web-redirection ALC. Be sure to use the same name as you used in the ISE configuration authorization profile web-redirect ACL. This ACL is referenced in the Access-Accept of the ISE and defines what traffic should be

redirected (denied by the ACL) and what traffic should not be redirected (permitted by the ACL). Here, you just prevent from redirection traffic toward the ISE. You might want to be more specific and only prevent traffic to/from the ISE on port 8443 (guest portal), but still redirect if a user tries to access the ISE on port 80/443. Go to **Security > Access Control Lists > Access Control Lists**. [Figure 14-30](#) shows an example, where 10.48.39.161 is the IP of ISE.

General									
Access List Name		cwa_redirect							
Deny Counters		0							
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCH	Direction	Number of Hits
<u>1</u>	Permit	0.0.0.0 0.0.0.0	/ 0.0.0.0 0.0.0.0	UDP	DNS	Any	Any	Any	836
<u>2</u>	Permit	0.0.0.0 0.0.0.0	/ 0.0.0.0 0.0.0.0	UDP	Any	DNS	Any	Any	2072
<u>3</u>	Permit	0.0.0.0 0.0.0.0	/ 10.48.39.161 255.255.255.255	/ Any	Any	Any	Any	Any	4895
<u>4</u>	Permit	10.48.39.161 255.255.255.255	/ 0.0.0.0 0.0.0.0	/ Any	Any	Any	Any	Any	7160
<u>5</u>	Deny	0.0.0.0 0.0.0.0	/ 0.0.0.0 0.0.0.0	/ Any	Any	Any	Any	Any	6587

**Figure 14-30** WLC ACL

## Step 7. Click Save.

## Summary

This chapter focused on creating a robust guest user environment. It covered everything from basic setup to full portal customization. The majority use case covered was Central Web Authentication with the sponsored guest type. Topics explored in this chapter include guest portals, sponsor portals, sponsor lifecycle, configuration of wired and wireless devices, guest authentication, and portal customization.

# Chapter 15 Client Posture Assessment

This chapter covers the following topics:

- ISE posture assessment flow
- Configure global posture and client provisioning settings
- Configure the AnyConnect and NAC client provisioning rules
- Configure the Client Provisioning Portal
- Configure posture elements
- Configure posture policy
- Configure host application visibility and context collection (optional)
- Enable posture client provisioning and assessment in your ISE authorization policies
- Posture reports and troubleshooting
- Enable posture assessment in the network

In short, this chapter shows you how to use ISE to answer, “Are my clients compliant with the company’s client/host security policy?”

Wouldn’t it be great if you could always be confident that all of your hosts are running up-to-date software with all the right patches and running up-to-date antivirus and antimalware software? Cisco ISE posture assessment helps you to ensure that your clients are in compliance with your host security policy. Posture assessment allows you to check the security health of your PC and Mac clients. This includes checking for the installation, running state, and last update for security software such as antivirus, antimalware, personal firewall, and so forth. It also includes checking to ensure that the hosts’ operating systems are patched appropriately. In addition, ISE posture policies can check for additional custom attributes such as files, processes, registry settings, and applications, just to name a few. Taken together, these features enable ISE to determine the security health of a client that is trying to access your network. ISE uses posture policies to determine the access rights and remediation options that should be provided to clients.

**Note** ISE posture functionality requires an ISE Apex license.

To ease the configuration process, ISE has a Work Center specifically for Posture. As shown in [Figure 15-1](#), the steps for configuring posture are broken down into three categories: Prepare, Define, and Go Live & Monitor.

**Prepare**

**1**

- Network Access Devices
- Updates
- Client Provisioning Resources
- Acceptable Use Policy
- Settings

**Define**

**2**

- Policy Elements
- Posture Policy
- Client Provisioning Portal

**Go Live & Monitor**

**3**

- Auditing
- Troubleshooting

**Figure 15-1** Posture Assessment Work Center

Here are the high-level steps, in the order I prefer, that are required to set up the ISE posture assessment feature:

1. Configure global posture and client provisioning settings:
  - a. Download to ISE the latest posture updates and the client provisioning packages.
  - b. Verify the default global posture settings meet your needs.
2. Configure the posture client provisioning policy.
3. Configure the Client Provisioning Portal.
4. Configure posture elements:
  - a. Configure posture conditions.
  - b. Configure posture remediation.
  - c. Configure posture requirements.
5. Configure posture policy.
6. Optionally, configure host application visibility and context collection.
7. Enable posture client provisioning and assessment in your ISE authorization policies.

## 8. Enable posture assessment on the network devices.

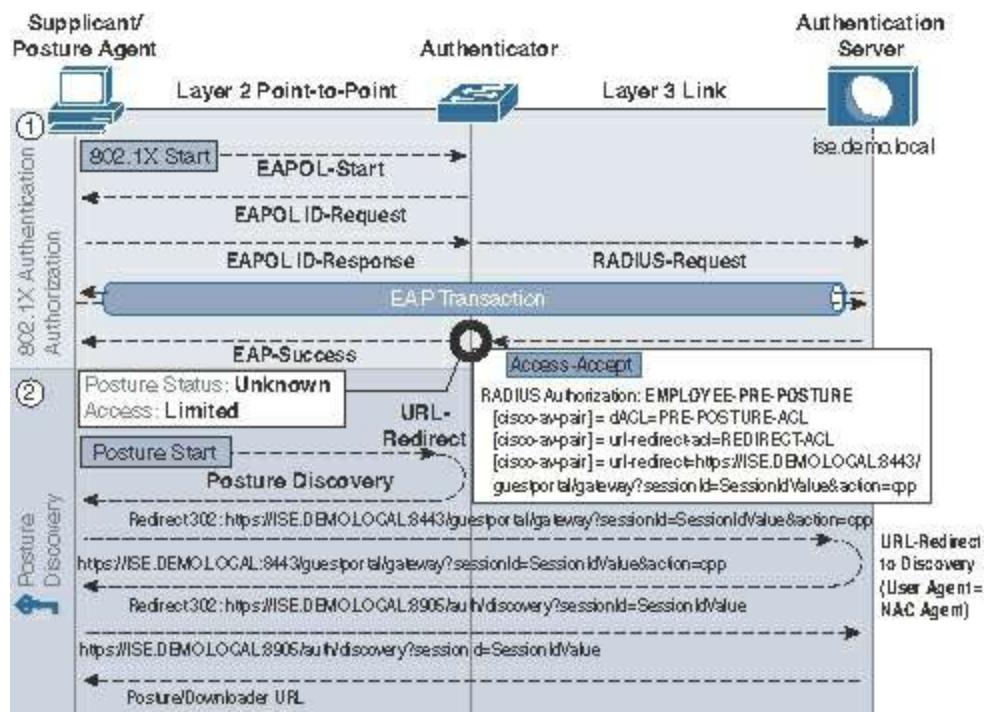
### ISE Posture Assessment Flow

It is important to understand where posture fits in the overall system flow of ISE. [Figure 15-2](#) illustrates the flow that ISE goes through when posture assessment is enabled.

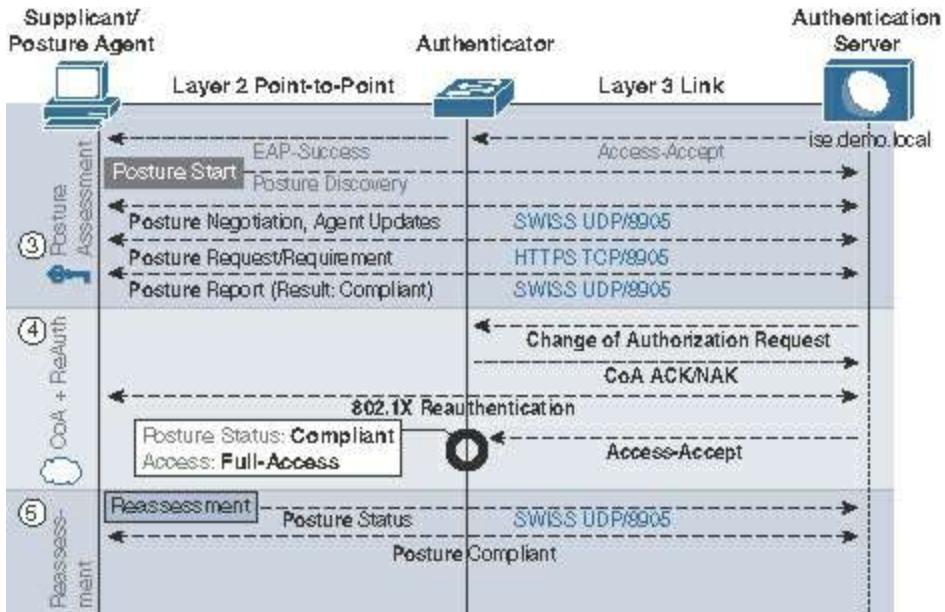


**Figure 15-2** ISE Flow When Poster Assessment Is Enabled

[Figures 15-3](#) and [15-4](#) depict the flow ISE goes through for an 802.1X end user with posture assessment.



**Figure 15-3 Posture Assessment 802.1X Flow Steps 1–2**



**Figure 15-4 Posture Assessment 802.1X Flow Steps 3–5**

Here is a brief description of what is happening at each step (1–5) shown in [Figures 15-2](#) and [15-3](#):

1. The client 802.1X supplicant talks to the access switch to start 802.1X. The EAP transaction takes place with the switch acting as the proxy between the client and ISE. If the authentication is successful, the posture status is set to Unknown.
2. ISE instructs the switch to redirect the client to an ISE URL for downloading the posture NAC Agent software or the dissolvable NAC Web Agent, depending on policy.
3. Now that the client has a NAC Agent, posture assessment proceeds through its flow. The NAC Agent uses the SWISS protocol to communicate with ISE. (SWISS is a proprietary UDP protocol created by Cisco.) At the end, a posture result is created.
4. ISE sends a Change of Authorization (CoA) request to the switch. This triggers an 802.1X reauthentication. A new authorization rule is matched given the new posture status of the client (compliant, noncompliant). The new access rights of the match authorization rule are downloaded to the switch.
5. If periodic reassessment is enabled, the client periodically goes through posture assessment to check for any changes. This happens without affecting the client communication. If the status changes, then a CoA is issued and the steps begin anew.

## Configure Global Posture and Client Provisioning Settings

In this section, you will enable the global settings required to turn on posture assessment. There are two parts: client provisioning setup and posture setup. Client provisioning deals with the NAC Agent software, its delivery, and other such settings. Posture setup deals with downloading the posture condition database and clients, keeping it up to date, posture reassessment, and other general settings.

## Posture Client Provisioning Global Setup

To begin client provisioning setup, you need to enable and download your posture resources. ISE posture assessment requires an agent to run. There are three major types of ISE posture agents for posture assessment, each of which supports Windows and macOS operating systems:

- Cisco AnyConnect with the compliance module
- Cisco NAC Agent
- NAC Web Agent

The NAC web agent is on-demand and dissolvable, meaning it is downloaded via the ISE Central Web Authentication page based on policy. It temporarily runs via the client's web browser as an ActiveX or Java applet. The NAC Web Agent is not permanent like the other NAC Agents are, and deletes itself once posture is complete. The AnyConnect and NAC Agents install permanently like any other agent software would.

Here is a list of all the client provisioning resource types:

- Persistent and temporal posture agents:
  - Windows and Mac OS X Cisco AnyConnect Agents with the ISE compliance module installed
  - Windows and Mac OS X Cisco NAC Agents
  - Cisco NAC Web Agent
  - Agent compliance modules
  - Agent customization packages

The following resources are also available but are not used for ISE posture assessment. They are used for the provisioning of the clients' 802.1X supplicant and are covered in [Chapter 16, “Supplicant Configuration.”](#)

- Native supplicant profiles
- Native supplicant provisioning/installation wizards

To enable and download the posture resources, go to **Administration > System > Settings > Client Provisioning**. [Figure 15-5](#) shows the various settings available here,

as described in the following list. Before you make any changes, ensure that you have your ISE proxy settings configured, if required for your environment.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes links for Home, Context Visibility, Operations, Policy, Administration, Work Centers, System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, Threat C, Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Backup & Restore, Admin Access, and Settings. The left sidebar has sections for Client Provisioning, FIPS Mode, Alarm Settings, Posture, Profiling, Protocols, Proxy, and SMTP Server. The main content area is titled 'Client Provisioning' and contains the following configuration options:

- \* Enable Provisioning: Set to 'Enable'.
- \* Enable Automatic Download: Set to 'Enable'.
- \* Update Feed URL: Set to <https://www.cisco.com/web/secure/pmbu/provisioning-update.xml>.
- \* Native Supplicant Provisioning Policy Unavailable: Set to 'Allow Network Access'.

At the bottom of the form are 'Save' and 'Reset' buttons.

**Figure 15-5** Global Client Provisioning Settings

**Step 1.** Enable client provisioning.

**Step 2a.** (Optional) Enable automatic download. This downloads any and all client files from Cisco.com. Select the exact files you want, as covered following this list.

**Step 2b.** If you choose to enable automatic download, use the default feed URL or set up your own client repository site. As of ISE version 2.2, the default URL is <https://www.cisco.com/web/secure/pmbu/provisioning-update.xml>.

**Step 3.** In most cases, keep the default setting of **Allow Network Access** for the Native Supplicant Provisioning Policy Unavailable.

**Step 4.** Click **Save**. Expect to wait a few minutes while ISE downloads the client files if you enabled automatic download.

To select just the client files you need for your environment, go to **Policy > Policy Elements > Results > Client Provisioning > Resources**, as shown in [Figure 15-6](#). (You can also get there via **Work Centers > Posture > Client Provisioning > Resources**.) This screen shows you all of the agents and other ISE resources you have downloaded already. To add more, click **Add** and choose either to add them from [Cisco.com](#) or to add them from your local PC. If you choose to add them from Cisco.com, you will see a list of available agents and software. Select what you want and click **Save**. The software is downloaded, which can take several minutes. [Figure 15-7](#) shows the [Cisco.com](#) software select screen. To see the complete Description field, grab the column separator and drag it larger, similar to what you would do in

Excel to make a column wider.

The screenshot shows the 'Client Provisioning' section of the Cisco ISE interface. Under 'Resources', there is a table listing various client provisioning components. The columns are: Name, Type, Version, Last Update, and Description. The table includes entries for AgentCustomizationPackage, AnyConnectComplianceModuleOSX, AnyConnectComplianceModuleWindows, ComplianceModule, MACComplianceModule, MacOsXAgent, MacOsXSPWizard, and NACAgent. A note at the bottom right of the table says 'Show All'.

Name	Type	Version	Last Update	Description
AgentCustomizationPackage 1.1.1.6	AgentCustomizationPackage	1.1.1.6	2017/03/03 17:47:45	This is the NACAgent Customization Package v1.1.1.6 for Windows
AnyConnectComplianceModuleOSX 4.2.749.0	AnyConnectComplianceModule	4.2.749.0	2017/03/03 17:47:22	AnyConnect OSX Compliance Module v4.2.749.0
AnyConnectComplianceModuleWindows 4.2.520.0	AnyConnectComplianceModule	4.2.520.0	2017/03/03 17:54:48	AnyConnect Windows Compliance Module v4.2.520.0
AnyConnectDesktopWindows 4.4.1054.0	AnyConnectDesktopWindows	4.4.1054.0	2017/03/03 17:54:00	AnyConnect Secure Mobility Client for Windows
Win_posture	AnyConnectProfile	Not Applicable	2017/03/03 17:44:44	
ComplianceModule 3.6.11098.2	ComplianceModule	3.6.11098.2	2017/03/03 17:47:11	NACAgent ComplianceModule v3.6.11098.2
MACComplianceModule 3.6.11098.2	MACComplianceModule	3.6.11098.2	2017/03/03 17:47:26	MACAgent ComplianceModule v3.6.11098.2
MacOsXAgent 4.9.5.3	MacOsXAgent	4.9.5.3	2017/03/03 17:47:41	NAC Posture Agent for Mac OSX v4.9.5.3
MacOsXSPWizard 2.1.0.42	MacOsXSPWizard	2.1.0.42	2017/01/25 18:43:42	Suplicant Provisioning Wizard for Mac OSX v2.1.0.42
NACAgent 4.9.5.10	NACAgent	4.9.5.10	2017/03/05 13:20:07	NAC Windows Agent - ISE 1.2.1 above

Figure 15-6 Client Provisioning Resources

The screenshot shows a modal dialog titled 'Download Remote Resources'. It lists various resources with checkboxes next to their names. One resource, 'AnyConnectComplianceModuleOSX 4...', has a checked checkbox. At the bottom of the list, there is a note about downloading AnyConnect software from Cisco.com. There are 'Save' and 'Cancel' buttons at the bottom right.

Name	Description
AgentCustomizationPackage 1.1.1.6	This is the NACAgent Customization Package v1.1.1.6 for Windows
AnyConnectComplianceModuleOSX 3...	AnyConnect OS X Compliance Module 3.6.11098.2
<input checked="" type="checkbox"/> AnyConnectComplianceModuleOSX 4...	AnyConnect OSX Compliance Module 4.2.749.0
AnyConnectComplianceModuleWindo...	AnyConnect Windows Compliance Module 3.6.11098.2
AnyConnectComplianceModuleWindo...	AnyConnect Windows Compliance Module 4.2.520.0
ComplianceModule 3.6.11098.2	NACAgent ComplianceModule v3.6.11098.2 for Windows
MACComplianceModule 3.6.11098.2	MACAgent ComplianceModule v3.6.11098.2 for MAC OSX
MacOsXAgent 4.9.0.1006	NAC Posture Agent for Mac OSX (ISE 1.2 release)
MacOsXAgent 4.9.0.1007	NAC Posture Agent for Mac OSX v4.9.0.1007 (with CM 3.6.7873.2)- ISE 1.2 release
MacOsXAgent 4.9.0.655	NAC Posture Agent for Mac OSX (ISE 1.1.1 or later)
MacOsXAgent 4.9.0.661	NAC Posture Agent for Mac OS X v4.9.0.661 with CM v3.5.7371.2 (ISE 1.1.3 Release)
MacOsXAgent 4.9.4.3	NAC Posture Agent for Mac OSX v4.9.4.3 - ISE 1.2 , ISE 1.1.3 and Above releases
MacOsXAgent 4.9.5.3	NAC Posture Agent for Mac OSX v4.9.5.3 - ISE 1.2 Patch 12, ISE 1.3 release and Ab...
MacOsXSPWizard 1.0.0.18	Suplicant Provisioning Wizard for Mac OSX 1.0.0.18 (ISE 1.1.3 Release)
MacOsXSPWizard 1.0.0.21	Suplicant Provisioning Wizard for Mac OSX 1.0.0.21 (for ISE 1.2 release)
MacOsXSPWizard 1.0.0.27	Suplicant Provisioning Wizard for Mac OSX 1.0.0.27 (for ISE 1.2 release with Patch ...)
MacOsXSPWizard 1.0.0.29	Suplicant Provisioning Wizard for Mac OSX 1.0.0.29 (for ISE 1.2 release with Patch ...)

For AnyConnect software, please download from <http://cisco.com/go/anyconnect>. Use the "Agent resource from local disk" add option, to import into ISE

Figure 15-7 Adding Client Provisioning Resources from Cisco.com

The note at the bottom of [Figure 15-7](#) tells you that, as of ISE version 2.2, you cannot download the full AnyConnect Agent through ISE. You can, however, download the AnyConnect compliance module that fits inside the full AnyConnect client. To obtain the full AnyConnect Agent, you must download it from Cisco.com/go/AnyConnect; hover your mouse pointer over Support, enter **AnyConnect Secure Mobility Client** in the search field, click **Find**, and click the latest version in the search results. Download the

AnyConnect Headend Deployment Package (.pkg) file(s) for your operating system(s). See [Figure 15-8](#) for an example. Once downloaded, next upload the file into ISE as shown in [Figure 15-9](#).

The screenshot shows the 'AnyConnect Secure Mobility Client v4.x' software download page. On the left, there's a sidebar with a search bar, an 'Expand All' link, and a collapse all link. Below that is a tree view of releases: Latest (4.4.01054), All Releases (4.3.05017, WebSecurityCert, Translations, ISEComplianceModule, AppSelector-2.0, Hostscan, 4.4, 4.3), and a detailed view of Release 4.4.01054. The main content area displays the release details for 'Release 4.4.01054'. It includes a star rating of 5 stars, a summary stating 'AnyConnect 4.4 is available to customers with active AnyConnect Apex, Plus or VPN Only term/contracts. See the AnyConnect Ordering Guide for options Software Download problems?', and a table of files. The table has columns for 'File Information', 'Release Date', and 'Size'. It lists four files: 'Language localization transform Headend Deployment (Windows)' (anyconnect-win-4.4.01054-core-vpn-lang-webdeploy-k9.zip), 'AnyConnect Pre-Deployment Package (Windows) - includes individual MSI files' (anyconnect-win-4.4.01054-predeploy-k9.zip), 'Application Programming Interface [API] (Windows)' (anyconnect-win-4.4.01054-vpnapi.zip), and 'AnyConnect Headend Deployment Package (Windows)' (anyconnect-win-4.4.01054-webdeploy-k9.pkg). Each file row has 'Download', 'Add to cart', and 'Publish' buttons.

**Figure 15-8** AnyConnect Agent Package Files

The screenshot shows the 'Client Provisioning' tab in the Cisco ISE interface. On the left, there's a sidebar with 'Overview', 'Network devices', 'Client Provisioning' (which is selected and highlighted in blue), 'Policy Elements', 'Posture Policy', 'Policy Sets', 'Troubleshoot', 'Reports', and 'Setting'. Under 'Client Provisioning', it says 'Client Provisioning Policy' and 'Resources'. In the main content area, it says 'Agent Resources From Local Disk > Agent Resources From Local Disk'. Below that is a section titled 'Agent Resources From Local Disk'. It has a 'Category' dropdown set to 'Cisco Provided Packages'. There's a 'Choose File' button with the path 'anyconnect-...ploy-k9.pkg' highlighted. At the bottom, there's a section titled 'AnyConnect Uploaded Resources' with a table showing one entry: 'Name' (AnyConnectDesktopWindows 4.4.1054...) and 'Type' (AnyConnectDesktopWindows).

**Figure 15-9** Add AnyConnect to ISE

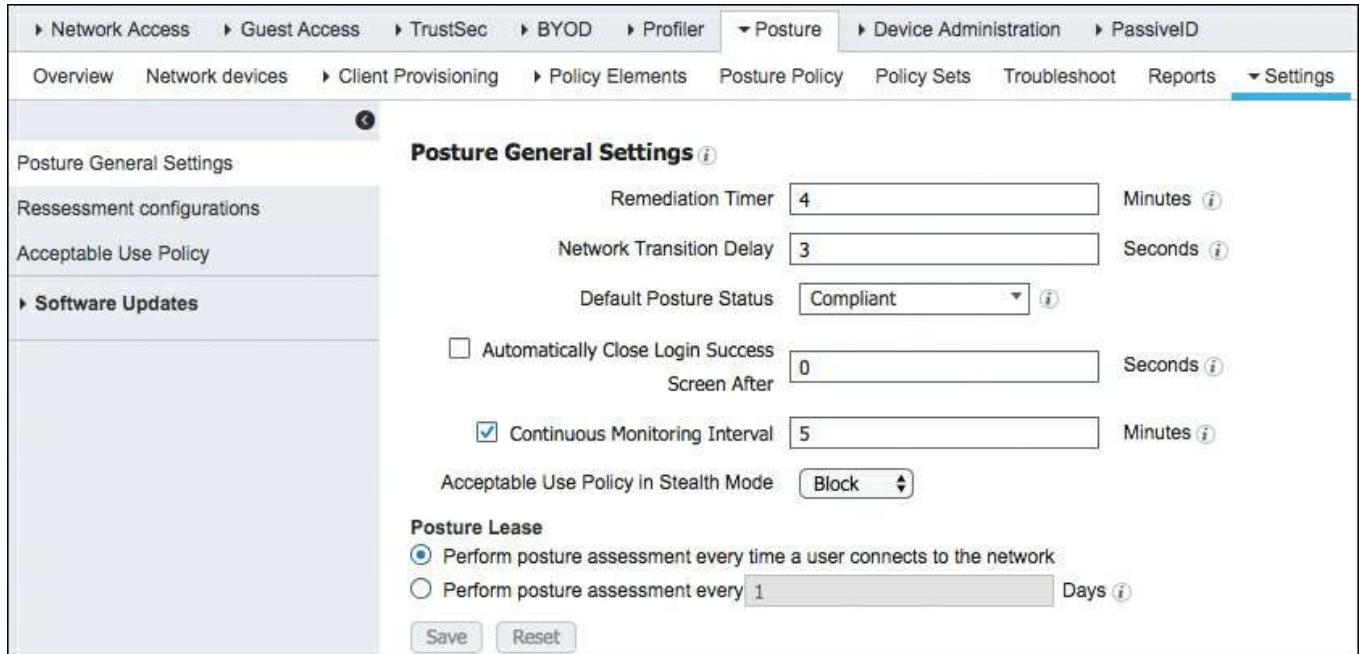
## Posture Global Setup

This section steps you through how to set up the global settings for ISE posture assessment. The various timer settings should be adjusted to meet the needs of your

organization.

## Posture General Settings

To begin, ensure that the basic posture settings are correct for your environment. Go to **Administration > System > Settings > Posture > General Settings**, or go to **Work Centers > Posture > Settings > Posture General Settings**. [Figure 15-10](#) shows the settings.



**Figure 15-10** Posture General Settings

These global settings take effect only if there is not a more specific posture profile in effect. The Default Posture Status field provides posture status for non-Agent devices (for example, Linux-based operating systems) and endpoints for which no NAC Agent installation policy applies. It is a best practice to enable **Automatically Close Login Success Screen After** and set it to **0** seconds. This disables display of the login success screen, which enhances the end-user experience in most organizations. You can also set the Posture Lease behavior of ISE. The option to perform posture assessment based on the number of days since the last posture scan is a great new feature; however, it only works with the Cisco AnyConnect compliance module and not with the NAC Agent or Web Agent.

## Posture Reassessments

If you would like to periodically recheck the posture of your endpoints, you can enable it via **Posture > Settings > Reassessment Configurations**. It works on a per-user identity group basis or is enabled for all. [Figure 15-11](#) shows the reassessment settings.

The screenshot shows the 'Reassessment Configuration' page in the Cisco ISE interface. The configuration name is 'Employees' and the description is 'Reassessment for employees'. The 'Use Reassessment Enforcement?' checkbox is checked. The 'Enforcement Type' dropdown is set to 'continue'. The 'Interval' field is set to 120 minutes. The 'Grace Time' field is set to 5 minutes. Below these fields, there is a list of 'Group Selection Rules' with the following points:

1. Each configuration must have a unique group or a unique combination of groups.
2. No two configurations may have any group in common.
3. If a config already exists with a group of 'Any', then no other configs can be created unless -
  - i. the existing config with a group of 'Any' is updated to reflect a group (or groups) other than 'Any', or
  - ii. the existing config with a group of 'Any' is deleted
4. If a config with a group of 'Any' must be created, delete all other configs first.

\* Select User Identity Groups Employee or RegisteredDevices +

**Figure 15-11 Posture Reassessment**

Ensure that you consider the ramifications of enabling certain enforcement types in your configurations. Options for the Enforcement Type setting include the following:

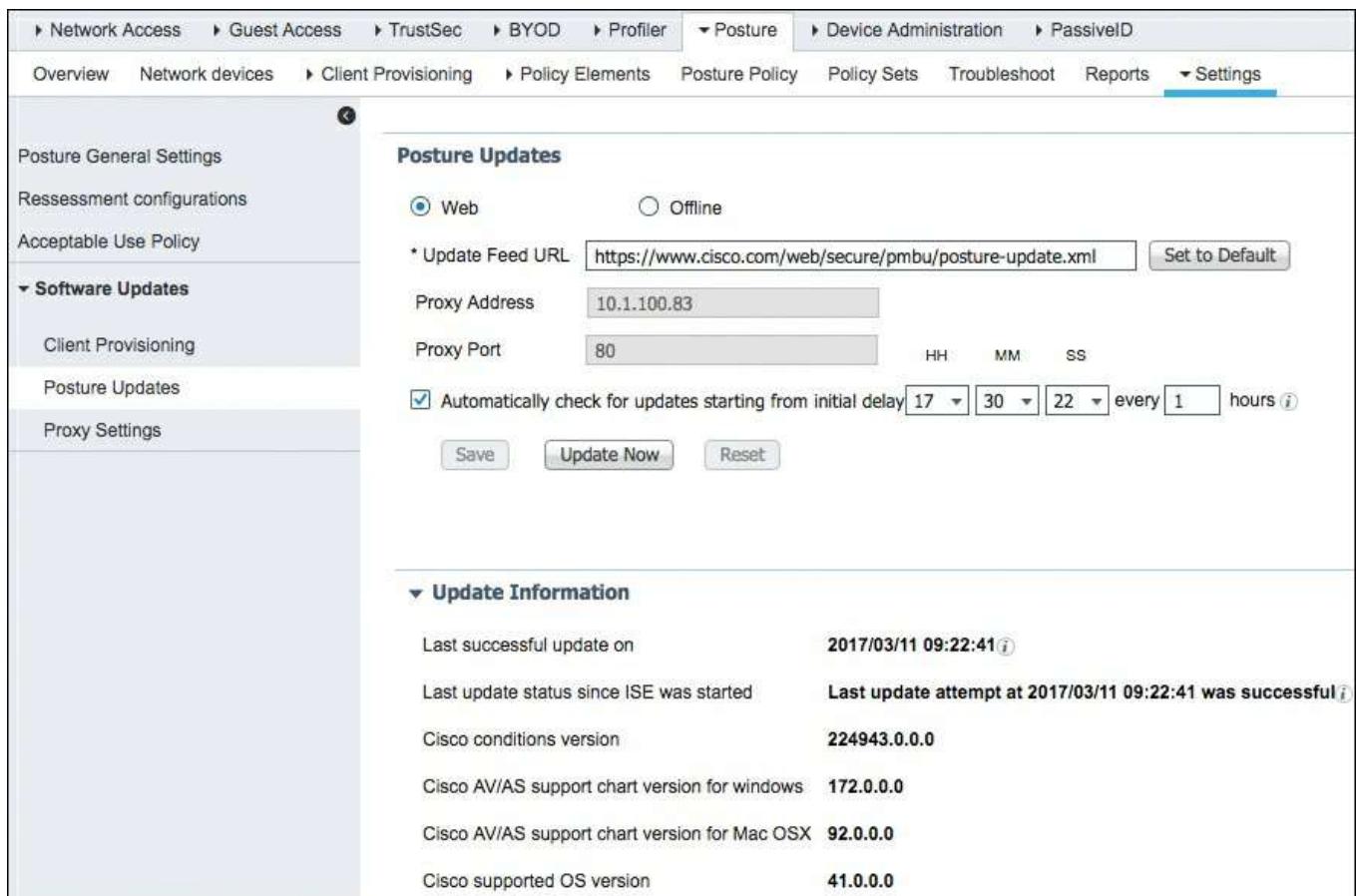
- **continue:** Irrespective of the posture reassessment compliance status, the user continues with the same privileged access. No remediation takes place.
- **logoff:** If the client posture is not compliant, the user is forced to log off from the network. When the client logs in again, the compliance status is reset to Unknown. ISE then runs through its normal authorization steps for a new client.
- **remediate:** If the client is not compliant, the agent waits for a specified time for the remediation to complete. Once the client has remediated, the agent sends the reassessment report to the Policy Service Node (PSN). If the remediation is ignored on the client, then the agent sends a logoff request to the PSN to force the client to log off from the network.

As you can see from [Figure 15-11](#), ISE uses the following group selection rules:

1. Each configuration must have a unique group or a unique combination of groups.
2. No two configurations may have any group in common.
3. If a config already exists with a group of 'Any', then no other configs can be created unless
  - a. the existing config with a group of 'Any' is updated to reflect a group (or groups) other than 'Any', or
  - b. the existing config with a group of 'Any' is deleted
4. If a config with a group of 'Any' must be created, delete all other configs first.

## Posture Updates

Cisco provides a posture update service to ensure that ISE has the latest information regarding posture check information. It is a best practice to set up auto-updates for posture. To do this, navigate to **Work Centers > Posture > Settings > Software Updates > Posture Updates**, as shown in [Figure 15-12](#). Configure ISE to retrieve posture updates either from [Cisco.com](#) or from an internal server you maintain. In almost all cases, you should enable **Automatically Check for Updates**. Enter the start time in 24-hour format, such as 4:30:00; the repeat time is in hours, such as 2. Ensure that you have configured any necessary proxy settings in ISE before attempting an update. If this is your first time updating, click the **Update Now** button and ensure that it completes successfully.



**Figure 15-12** Posture Updates

## Acceptable Use Policy Enforcement

ISE provides the ability to enforce the acceptance of an acceptable use policy (AUP) after a successful login and compliant posture assessment completes. After login and successful posture assessment of clients, the client agent displays a temporary network access screen that contains a link to an AUP. To proceed, users must click the link, which redirects them to a page that displays the AUP, where they must acknowledge that they have read the AUP and accept its network-usage terms and conditions. Unlike guest

access, where AUP enforcement is widely used, posture-triggered AUP enforcement is not a widely used or popular ISE feature, for two reasons: it interrupts the network login of the user and requires the user to accept the policy before they are granted network access, which impacts productivity, and it often is redundant, because most postured hosts are being used by users who have already accepted a corporate AUP as part of their employment contract.

When the feature is used, each AUP configuration must have a unique user identity group, or a unique combination of user identity groups. Cisco ISE finds the AUP for the first matched user identity group and communicates that to the client agent, which displays the AUP. These settings apply to AnyConnect ISE Posture and NAC Agents for Windows. This AUP does not apply to guest users; you must use guest portal settings instead. The configuration is group-based, like the posture reassessment. If AUP is enabled for a group, members of that group see a pop-up from their NAC Agent each time they log in. They have to click Accept before being allowed to log in. Because this happens at each login, it is typically enabled only where required, such as for high-risk user groups, non-employees, temporary workers, or other groups that haven't signed a contractual network AUP already. Another tactic is to enable the AUP for all network users once a year for a short period of time. This ensures that everyone is aware of your network AUP and accepts it yearly. To set up AUP enforcement, navigate to **Work Centers > Posture > Settings > Acceptable Use Policy**. [Figure 15-13](#) depicts the AUP settings screen.

The screenshot shows the 'Acceptable use policy Configurations List > New Acceptable use policy Configurations' screen. The 'Acceptable User Policy' section contains the following fields:

- \* Configuration Name: Employee AUP
- Configuration Description: Employee AUP
- Show AUP to Agent users:
- Use URL for AUP message
- Use file for AUP message (Please upload a zip file. The zip file must include index.html at the top level, i.e., not under any subdirectory.)
- \* AUP URL: internal.acme.com/aup.html

Below these fields is a list of Group Selection Rules:

1. Posture AUP is not applicable for guest portal login (use guest portal settings).
2. Each configuration must have a unique group or a unique combination of groups.
3. No two configurations may have any group in common.
4. If a config already exists with a group of 'Any', then no other configs can be created unless the existing config with a group of 'Any' is deleted.
5. If a config with a group of 'Any' must be created, delete all other configs first.

\* Select User Identity Groups: Employee or RegisteredDevices

**Figure 15-13** Acceptable Use Policy Settings

## Configure the AnyConnect and NAC Client Provisioning Rules

ISE allows you to granularly control which client and client profiles are provisioned to a host. ISE has two agents: the AnyConnect Agent with the compliance module installed and the NAC Agent. Going forward, Cisco is migrating in favor of the AnyConnect

Agent, so if you have a new deployment, you should opt to deploy the AnyConnect Agent.

## AnyConnect Agent with ISE Compliance Module

This section walks you through configuring the AnyConnect Agent for use with ISE posture assessment. The AnyConnect client provisioning requires four different resources to be in place before it can be used in a client provisioning policy:

- AnyConnect Secure Mobility Client software
- AnyConnect Windows/OS X compliance module
- AnyConnect Posture Profile file
- AnyConnect configuration file

Cisco provides the first two resources. You need to create the last two resources inside of ISE (first the Posture Profile and then the configuration file). [Figure 15-14](#) shows an example of the four required resources for AnyConnect.

The screenshot shows a table titled 'Resources' with columns: Name, Type, Version, Last Update, and Description. There are six rows listed, with the second, third, fourth, and fifth rows being checked (indicated by a blue checkmark icon). The table includes standard navigation buttons like Edit, Add, Duplicate, and Delete at the top, and a 'Selected 4 | Total 6' status indicator.

Name	Type	Version	Last Update	Description
anyconnect				
AnyConnectComplianceModuleOSX 4.2.749.0	AnyConnectComplianceModuleOSX	4.2.749.0	2017/03/03 17:47:22	AnyConnect OSX Compliance Module 4.2.749.0
AnyConnectComplianceModuleWindows 4.2.520.0	AnyConnectComplianceModuleWindows	4.2.520.0	2017/03/11 11:47:21	AnyConnect Windows Compliance Module 4.2.520.0
AnyConnectDesktopWindows 4.4.1054.0	AnyConnectDesktopWindows	4.4.1054.0	2017/03/11 12:08:38	AnyConnect Secure Mobility Client for Windows 4.4.1054.0
AnyConnect Windows	AnyConnectProfile	Not Applicable	2017/03/11 12:14:49	4.4
AnyConnect Configuration Windows	AnyConnectConfig	Not Applicable	2017/03/11 12:08:18	4.4.1054
AnyConnectDesktopOSX 4.4.1054.0	AnyConnectDesktopOSX	4.4.1054.0	2017/03/11 12:32:35	AnyConnect Secure Mobility Client for OS X 4.4.1054

**Figure 15-14** AnyConnect Required Resources

**Note** As previously discussed, ISE, as of version 2.2, cannot download the AnyConnect client package directly from Cisco.com. Thus, it is necessary for you to download the AnyConnect Headend Deployment Package file to your computer and then upload it manually into the ISE client provisioning resources. Packages are available for Windows, OS X, and Linux. However, the Linux package does not support posture assessment.

## AnyConnect Posture Profile Creation

The Posture Profile defines the AnyConnect Agent behaviors and is used in the AnyConnect configuration file. To configure it, go to **Work Centers > Posture > Client Provisioning > Resources**, click **Add**, and select **NAC Agent or AnyConnect Posture Profile**. Next, from the **Posture Agent Profile Settings** drop-down list, choose **AnyConnect**, as shown in [Figure 15-15](#). Enter a descriptive name for your

profile. The profile settings are broken into three sections:

- Agent Behavior
- IP Address Change
- Posture Protocol

[Figure 15-15](#) shows the Agent Behavior section. Typically, the default values are fine for most deployments.

The screenshot shows the 'Posture Agent Profile Settings' section for a new profile named 'AnyConnect 4.4 Profile Win'. The 'Agent Behavior' table contains the following configuration:

Parameter	Value	Notes	Description
Enable debug log	No		Enables the debug log on the agent.
Operate on non-802.1X wireless	No		Enables the agent to operate on non-802.1X wireless networks.
Enable signature check	No	OSX: N/A	Enables signature checking of executables before the agent will run them.
Log file size	5 MB		The maximum agent log file size
Remediation timer	4 mins	The default is empty which means use the global setting. The default of global setting is 4.	The time the user has for remediation before they will be tagged as non-compliant
Stealth Mode	Disabled		AnyConnect can act as either clientless or standard mode. When stealth mode is enabled, it runs as a service without any user interface.

**Figure 15-15** Profile Settings: Agent Behavior Section

[Figure 15-16](#) shows the IP Address Change section. If you will be changing VLANs as part of your permission and remediation settings, then you need to tweak these settings.

[Figure 15-16](#) shows some example settings for this; however, if you are not changing the client's VLAN, the defaults will work fine for most deployments.

The screenshot shows the 'IP Address Change' table for the same profile. The configuration is as follows:

Parameter	Value	Notes	Description
Enable agent IP refresh	Yes	Enables VLAN change detection	Sets the Vlan change detection flag on the server, to transmit the configured dhcp release delay, and the dhcp renew delay values from the server to the client.
VLAN detection interval	5 secs	0 means VLAN detection is disabled	The interval at which the agent will check for a VLAN change
Ping or ARP	Ping	0=Ping, 1=ARP, 2=Ping then ARP	Method for detecting IP address change.
Maximum timeout for ping	1 secs		Ping timeout.
DHCP renew delay	1 secs		
DHCP release delay	4 secs		
Network transition delay	3 secs	The default is empty which means uses the global setting. The default of global setting is 3.	The period for which the agent suspends network monitoring so it can wait for a planned IP change to happen

**Figure 15-16** Profile Settings: IP Address Change Section

[Figure 15-17](#) shows the Posture Protocol section. You should set the discovery host, server name rules, and call home list.

Posture Protocol			
Parameter	Value	Notes	Description
PRA retransmission time	120 secs		This is the agent retry period if there is a Passive Reassessment communication failure.
Discovery host	psn.acme.com		The server that the agent should connect to
* Server name rules	*.acme.com	need to be blank by default to force admin to enter a value. *** means agent will connect to all	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. *.cisco.com
Call Home List	psn1.acme.com,psn2.acr	List of IP addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPAddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)	A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer	30 secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.	Anyconnect agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

**Figure 15-17 Profile Settings: Posture Protocol Section**

## AnyConnect Configuration File Creation

The AnyConnect configuration file defines which AnyConnect software and its associated configuration files are used. This configuration can be used in the client provisioning policy that allows users to download and install AnyConnect resources on the clients.

**Note** If you use both ISE and an ASA to deploy AnyConnect, then the configurations must match on both.

To create your configuration file, go to **Work Centers > Posture > Client Provisioning > Resources**. Click **Add** and select **AnyConnect Configuration**. The configuration is separated into five sections:

- AnyConnect Package Info
- AnyConnect Module Selection
- Profile Selection
- Deferred Update
- Installation Options

Fill out the first three sections with the values for your organization. [Figure 15-18](#) shows some example values.

* Select AnyConnect Package:	AnyConnectDesktopWindows 4.4.1054.0
* Configuration Name:	AnyConnect Configuration Windows 4.4.1054
Description:	Windows 4.4.1054
<b>DescriptionValue</b>	
* Compliance Module:	AnyConnectComplianceModuleWindows 4.2.520.0
<b>AnyConnect Module Selection</b>	
ISE Posture	<input checked="" type="checkbox"/>
VPN	<input checked="" type="checkbox"/>
Network Access Manager	<input type="checkbox"/>
Web Security	<input type="checkbox"/>
AMP Enabler	<input type="checkbox"/>
ASA Posture	<input type="checkbox"/>
Network Visibility	<input type="checkbox"/>
Umbrella Roaming Security	<input type="checkbox"/>
Start Before Logon	<input type="checkbox"/>
Diagnostic and Reporting Tool	<input type="checkbox"/>
<b>Profile Selection</b>	
* ISE Posture	AnyConnect 4.4 Profile Windows
VPN	<input type="checkbox"/>
Network Access Manager	<input type="checkbox"/>
Web Security	<input type="checkbox"/>
AMP Enabler	<input type="checkbox"/>
Network Visibility	<input type="checkbox"/>
Umbrella Roaming Security	<input type="checkbox"/>
Customer Feedback	<input type="checkbox"/>

**Figure 15-18** AnyConnect Sample Configuration for First Three Sections

The fourth section defines the settings for allowing or disallowing the end user to defer a client update. [Figure 15-19](#) shows an example of allowing deferral of the agent software update but not allowing deferral of a compliance module update. Under Installation Options, the Uninstall Cisco NAC Agent check box will uninstall any existing NAC agents on the client after a successful AnyConnect posture module install. This should be checked; the AnyConnect posture module and the Cisco NAC agent should NOT both be installed on the same host.

Customization Bundle:

Localization Bundle:

**Deferred Update**

Allowed for AnyConnect Software:

Minimum Version Required for AnyConnect Software:

Allowed for Compliance Module:

Minimum Version Required for Compliance Module:

Prompt Auto Dismiss Timeout:

Prompt Auto Dismiss Default Response:

If set to 'Yes', the end user can defer the update as long as they already meet the minimum version in the setting below, for all required AnyConnect modules.  
Format is 'n.n.n'. '0.0.0' means no minimum version is required. '3' means minimum version is 3.0.0. '3.2' means minimum is 3.2.0.

If set to 'Yes', the end user can defer the update as long as they already meet the minimum version in the setting below.  
Format is 'n.n.n.n'. '0.0.0.0' means no minimum version is required. '3' means minimum version is 3.0.0.0. '3.6' means minimum is 3.6.0.0, and so on.

The number of seconds that the deferred update prompt is displayed before being dismissed automatically. 'None' means the prompt can only be dismissed by the user. A '0' value and a 'defer' value for the response setting below will force a deferral of the software update.

The action taken when the prompt is automatically dismissed.

**Installation Options**

Uninstall Cisco NAC Agent

Uninstalls Cisco NAC Agent after successful installation of ISE Posture.

**Figure 15-19** AnyConnect Configuration: Deferred Update

## AnyConnect Client Provisioning Policy

Now that you have the four required resources for AnyConnect, you can create a provisioning policy. Client provisioning policy rules determine which users and endpoints receive which resources (agents, agent compliance modules, and/or agent customization packages/profiles) from Cisco ISE after authentication. Define the client provisioning policy to determine what users will receive upon login and user session initiation. For Agent configuration, this includes version of agent, agent profile, agent compliance module, and/or agent customization package.

Navigate to **Work Centers > Posture > Client Provisioning > Client Provisioning Policy**. Click the drop-down arrow at the right end of a policy row and choose **Insert New Policy**. There are two results per rule: Native supplicant and Agent configuration. We cover only the Agent rules here. Typically, you create at least one rule per operating system. An example is shown in [Figure 15-20](#).

Rule Name:	Identity Groups:	Operating Systems:	Other Conditions:	Results:
<input checked="" type="checkbox"/> Windows - Employee	If Any	and Windows 10 (All)	and AD-SecurityDemo\ExternalGroups EQUALS securitydemo.net\Users\Employees	then AnyConnect Configuration Windows 4.4.1054 <a href="#">Edit</a>

**Figure 15-20** AnyConnect Client Provisioning Rule

Each rule has the following settings:

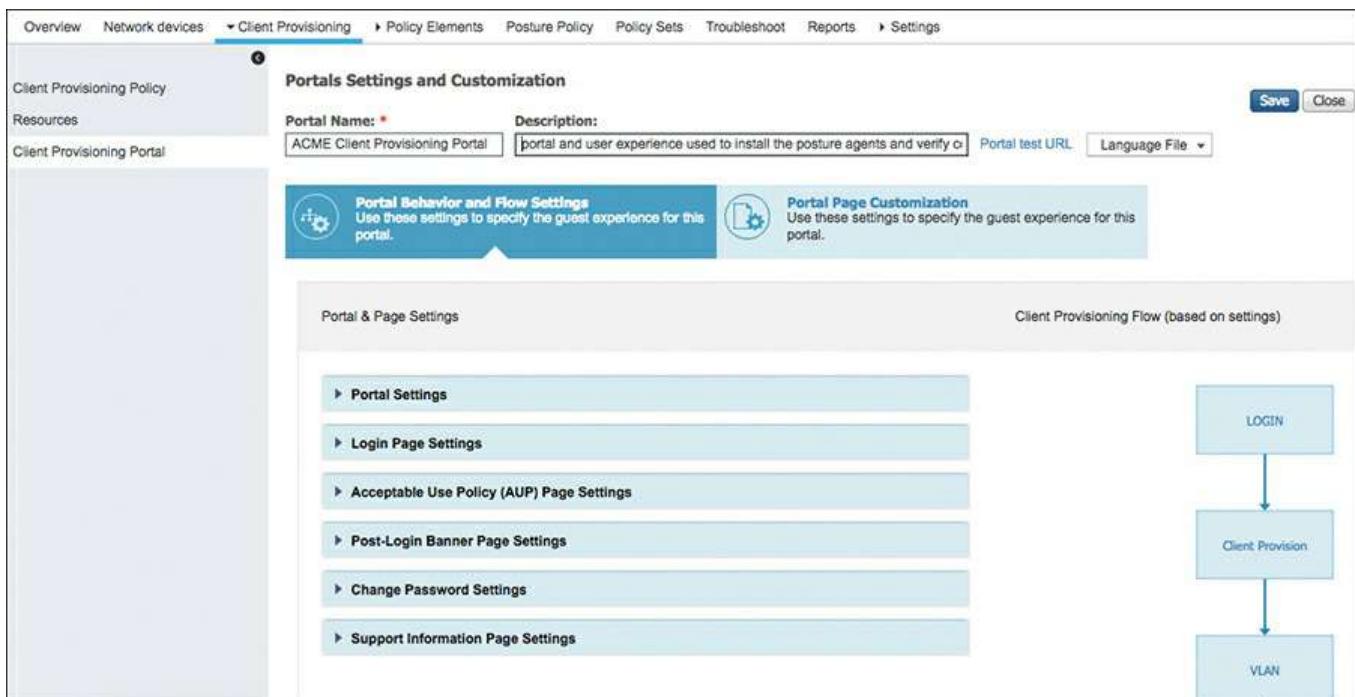
- **Status:** This is the green check box in [Figure 15-20](#). Options are Enable, Disable, or Monitor. Monitor disables the policy and just “watches” and logs the client provisioning requests.
- **Rule Name:** Use a descriptive name that includes the key conditions you are matching, such as windows10-employees.

- **Identity Groups:** Not typically used.
- **Operating Systems:** This setting is a requirement for a proper rule base. You should at a minimum have a Windows policy and a Mac policy.
- **Other Conditions:** Includes AD group selection.
- **Results:** Agent and supplicant configuration selection.

## Configure the Client Provisioning Portal

ISE posture assessment requires an agent to be installed on the endpoint. You can install that agent using ISE, ASA, or your own software provisioning system. If you use ISE, then you must configure the Client Provisioning Portal. After users successfully authenticate and request network access, ISE can route them to a Client Provisioning web portal to provide them with the posture agent for download. The posture agent downloads, installs, and runs and provides a posture verdict back to ISE.

To set up the portal, go to **Work Centers > Posture > Client Provisioning > Client Provisioning Portal**, select the **Default** portal, and click **Duplicate**. On the Portal Settings and Customization page, shown in [Figure 15-21](#), give your new portal a descriptive name and, optionally, add a description. Click **Portal Settings**, and change the port and your interfaces as appropriate for your deployment. If you have multiple PSNs, the interfaces and ports chosen will be the same on all PSNs. At this point you are done unless you want to customize the page using the other sections shown in [Figure 15-21](#).



**Figure 15-21** Client Provisioning Portal

**Note** If users will access your portal page directly (not through the usual URL redirect mechanism), or if the redirect single sign-on (SSO) fails for any reason, you must configure the **Portal Settings > Authentication Method** section and authorized groups appropriately—for example, users accessing the portal page via an AnyConnect VPN session. In the authentication method section, change this to whichever user database should be used to authenticate users to the portal.

Next, select **Authorized Groups**. The FQDN of the Client Provisioning Portal needs to be specified next. This FQDN should be resolvable to ISE PSN IPs. Caution: Make sure you don't specify the exact same FQDN of an ISE standalone admin login page; otherwise, you will lose your admin page. Users need to be instructed to enter the FQDN URL in the web browser to visit the portal during their first connection attempt.

## Configure Posture Elements

Posture elements are the building blocks for your posture requirements. There are three major categories of posture policy elements you need to configure: Conditions, Remediations, and Requirements. [Figure 15-22](#) shows these categories of elements, located at **Work Centers > Posture > Policy Elements**.

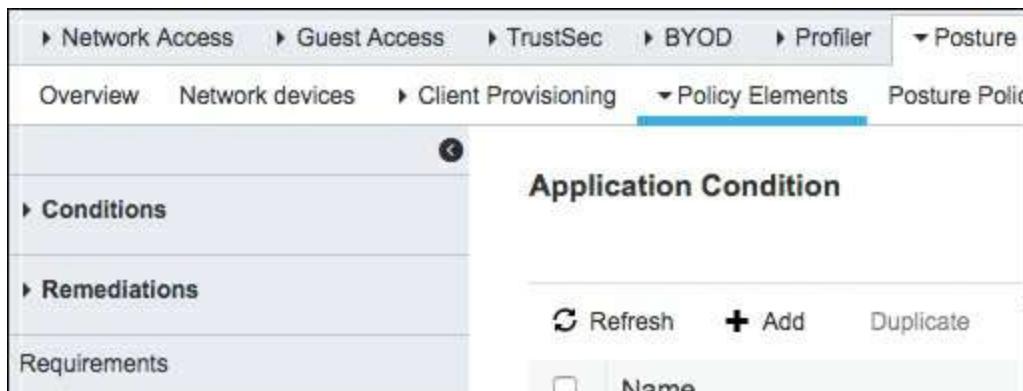
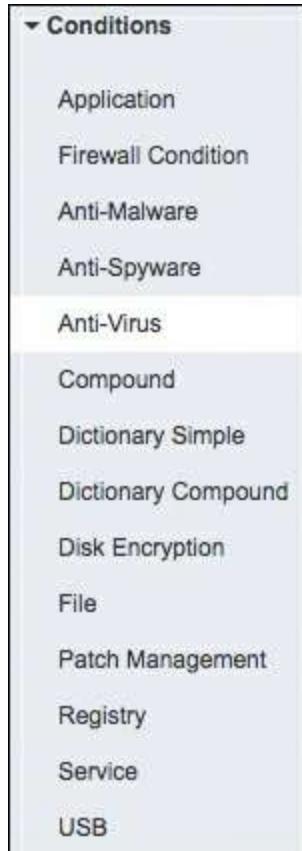


Figure 15-22 Categories of Posture Elements

## Configure Posture Conditions

There are many types of posture conditions, as shown in [Figure 15-23](#). To configure the conditions, go to posture **Work Centers > Posture > Policy Elements > Conditions**.



**Figure 15-23** Posture Condition Types

The good news is that many of these condition types are prepopulated from the [Cisco.com](#) posture update process that you configured earlier. Updates continue to flow in as they are available, always keeping your conditions up to date. There are some condition types that, as of ISE 2.2, are not supported on Macs. The list seems to shrink with each AnyConnect release, so check the latest ISE release notes for details. Posture assessment is not supported at all on Linux.

ISE has many predefined conditions that help speed configuration and deployment. Cisco-defined simple conditions have pc\_ as their prefixes and compound conditions have pr\_ as their prefixes. You cannot delete or edit Cisco-defined posture conditions, but you can duplicate them and edit the duplicate. [Figure 15-24](#) shows an example predefined compound condition. This condition checks to ensure that all Windows 7 x64 critical hotfixes are installed. As new hotfixes are released by Microsoft, this rule is auto-updated by Cisco ISE.

The screenshot shows the 'Policy Elements' tab selected in the navigation bar. On the left, a sidebar lists various condition types under 'Conditions'. The 'Compound' type is currently selected. The main pane displays a 'Compound Condition' configuration for a policy element named 'pr\_Win7\_64\_Hotfixes'. The configuration includes:

- Name:** pr\_Win7\_64\_Hotfixes
- Description:** Cisco Predefined Rule: Windows 7 Hotfixes
- Operating System:** Windows 7 (All)
- Compliance Module:** Any version
- Condition Details:** A large text area contains a complex logical expression: `(pc_Win7_32)|((pc_W7_SP1|pc_W7_SP1_int)&pc_W7_64_KB3197868_MS16-130&pc_W7_64_KB3197868_MS16-131&pc_W7_64_KB3170455_MS16-087&pc_W7_64_KB3184122_MS16-116&pc_W7_64_KB3146963_MS16-040&pc_W7_64_KB3108670_MS15-130&pc_W7_64_KB3080446_MS15-109&pc_W7_64_KB3078601_MS15-080&pc_W7_64_KB3042553_MS15-034&pc_W7_64_KB3033889_MS15-020&pc_W7_64_KB2992611_MS14-066&pc_W7_64_KB3000061_MS14-058&pc_W7_64_KB2893294_MS13-098&pc_W7_64_KB2892074_MS13-099&pc_W7_64_KB2876331_MS13-089&pc_W7_64_KB2864058_MS13-083&pc_W7_64_KB2685939_MS12-036&pc_W7_64_KB2681578_MS12-034&pc_W7_64_KB2653956_MS12`

**Figure 15-24** Windows 7 Compound Condition

[Figures 15-25](#) through [15-30](#) provide example screenshots of some of the other condition types, in the following order: Registry, Application, Disk Encryption, Firewall, and Anti-Virus (both predefined and manual).

The screenshot shows the 'Registry Conditions List' screen for a policy element named 'pc\_W7\_SP1'. The configuration includes:

- Name:** pc\_W7\_SP1
- Description:** Cisco Predefined Check
- Operating System:** Windows 7 (All)
- Compliance Module:** Any version
- Registry Type:** RegistryValue
- Registry Root Key:** HKLM
- Sub Key:** Windows NT\CurrentVersion\
- Value Name:** CSDVersion
- Value DataType:** String
- Value Operator:** contains
- Value Data:** Service Pack 1

**Figure 15-25** Registry Condition Settings

Application Condition > pc_Symantec_Norton_App-Corporate	
Name *	pc_Symantec_Norton_App-Corporate
Description	Cisco Predefined Check
Operating System *	Windows All
Check By *	Process
Compliance module	Any version
Process Name *	rtvscan.exe
Application Operator *	Running

**Figure 15-26** Application Condition Settings

**Note** You can use the command-line tool **tasklist** to find all running Windows applications.

**Disk Encryption Condition**

\* Name

Description

\* Operating System  

\* Compliance Module

\* Vendor Name

**▼ Products for Selected Vendor**

	Product Name	Version	Encryption State Check	Minimum Compliant Module Support
<input checked="" type="checkbox"/>	BitLocker Drive Encryption	10.x	YES	4.2.520.0
<input type="checkbox"/>	BitLocker Drive Encryption	6.x	YES	4.2.520.0

Encryption State 

Location:   Is Fully Encrypted OR  Pending Encryption OR  Partially Encrypted  

**Figure 15-27 Disk Encryption Condition Settings**

Firewall Conditions > Firewall Condition  
Input fields marked with an asterisk (\*) are required.

Name *	Windows10_Firewall_Settings
Description	Windows 10 Firewall Enabled Check
Compliance module *	4.x or later
Operating System *	Windows 10 (All) <input type="button" value="+"/>
Vendor *	Microsoft Corporation
<input checked="" type="checkbox"/> Enable	
<b>At least one product must be selected *</b>	
1 Selected	Rows/Page <input type="button" value="3"/>
<input type="button" value="Refresh"/>	
<input type="checkbox"/> Product Name	Version
<input checked="" type="checkbox"/> Windows Firewall	10.x

**Figure 15-28 Firewall Condition Settings**

The Anti-Virus (AV), Anti-Malware (AM), and Anti-Spyware (AS) compound conditions are similar. By default, ISE provides a check for any AV, AM, or AS installed on Windows and Mac. Also included is a check for any AV or AS definition file that is 5 days old or older than the latest file date for Windows and Mac. [Figure 15-29](#) shows a predefined AV condition.

Anti-virus Conditions List > ANY\_av\_win\_def

### Anti-Virus Condition

* Name	ANY_av_win_def			
Description	Any AV definition check on Windo			
Compliance Module	3.x or earlier <i>i</i>			
* Operating System	Windows All <i>+</i>			
Vendor	ANY <i>▼</i>			
Check Type	<input type="radio"/> Installation <input checked="" type="radio"/> Definition			
<input type="radio"/> Check against latest AV definition file version if available. Otherwise check against latest definition file date. <input checked="" type="radio"/> Allow virus definition file to be <input type="text"/> 5 days older than <input checked="" type="radio"/> latest file date <input type="radio"/> current system date				
<b>▼ Products for Selected Vendor</b>				
Product Name	Version	Remediation Support	Definition Check	Latest Definition Date
<input checked="" type="checkbox"/> ANY	ANY	N/A	YES	

**Figure 15-29** Predefined AV Definition Up to Date Condition

An ISE custom AV or AS condition can check for either the definition or the installation of the software. Use a compound condition to combine them into a single condition. Creating a custom AV rule is typically done when a corporation has standard AV software set up on its corporate PCs and Macs. [Figure 15-30](#) shows an example of a custom AV condition. This AV vendor also supports automatic remediation by ISE, allowing ISE to trigger an AV signature update action.

Anti-Virus Condition

* Name	Corp_mcafee_AV					
Description	EST 10.x					
Compliance Module	3.x or earlier <i>i</i>					
* Operating System	Windows 7 (All) <i>+</i>					
Vendor	McAfee, Inc. <i>▼</i>					
Check Type	<input type="radio"/> Installation <input checked="" type="radio"/> Definition					
<input checked="" type="radio"/> Check against latest AV definition file version if available. Otherwise check against latest definition file date. <input type="radio"/> Allow virus definition file to be <input type="text"/> 0 days older than <input checked="" type="radio"/> latest file date <input type="radio"/> current system date						
<b>▼ Products for Selected Vendor</b>						
Product Name	Version	Remediation Support	Definition Check	Latest Definition Date	Latest Definition Version	Minimum Compliance M
<input checked="" type="checkbox"/> McAfee Endpoint Security Threat...	10.x	YES	YES	03/12/2017	2916.0	Installation 3.6.9038.2
						Definition Date 3.6.9038.2

**Figure 15-30** Custom AV Definition Up to Date Condition

## Configure Posture Remediations

Now that you have created your various conditions, the next step is to configure client remediation actions. These are actions that the AnyConnect Agent, NAC Agent, and/or

end user can perform to fix any failed conditions and thus come into posture compliance. For example, you could set up ISE to automatically update a host's antivirus definition file. Like the Conditions category, the Remediations category has various types in ISE, as shown in [Figure 15-31](#).



**Figure 15-31** Remediation Types

[Table 15-1](#) outlines the available remediation actions, as of ISE version 2.2, listed by supported agent type.

	<b>Windows AnyConnect Posture Agent/NAC Agent</b>	<b>Web Agent for Windows</b>	<b>Mac OS X AnyConnect Posture Agent/NAC Agent</b>
Message Text (Local Check)	Supported	Supported	Supported
URL Link (Link Distribution)	Supported (manual and automatic)	Supported (manual)	Supported (manual)
Launch Program	Supported (manual and automatic)	Not Supported	Not supported
File Distribution	Supported	Supported	Not supported
Antivirus Definition Update	Supported (manual and automatic)	Not supported	Supported
Antispyware Definition Update	Supported (manual and automatic)	Not supported	Supported
Windows Update	Supported (manual and automatic)	Not supported	Not supported
WSUS	Supported (manual and automatic)	Not supported	Not supported
Patch Management	Supported (manual and automatic)	Not supported	Not supported
Host Firewall Enabled	Supported (manual and automatic)	Not supported	Supported (manual and automatic)
Block USB storage devices	Supported (automatic)	Not supported	Not supported
Application Uninstall or Kill	Supported (manual and automatic)	Not supported	Supported (manual and automatic)

**Table 15-1** ISE Version 2.2 Remediation Actions

If a remediation action is manual, the end user sees a NAC Agent popup with instructions to click it to perform the action. If the action is automatic, the end user doesn't have to perform any action. The NAC agent performs the action automatically.

To create or edit remediation actions, following these steps:

**Step 1.** Navigate to **Work Centers > Posture > Policy Elements > Remediations**.

**Step 2.** Select the type of remediation you want to create.

**Step 3.** Fill in the fields.

[Figure 15-32](#) provides an example of the Cisco predefined AV remediation action configured to occur automatically.

Anti-Virus Remediations List > [AnyAVDefRemediationWin](#)

### Anti-Virus Remediation

\* Name: AnyAVDefRemediationWin [i](#)

Description: Remediation for any AV

Operating System:  Windows  Mac

Compliance Module: 3.x or earlier [i](#)

Remediation Type: Automatic

\* Interval: 20 (in secs)

\* Retry Count: 1 (Valid Ra

\* Anti-Virus Vendor Name: ANY

[Save](#) [Reset](#)

**Figure 15-32** AV Remediation Action

In addition to creating a corporate AV remediation rule, it is also common to create a Patch Management rule. Patch management is only supported on Windows OSs. [Figure 15-33](#) shows a typical Windows System Center Configuration Manager (SCCM) update rule example. ISE remediation natively supports over 20 patch management vendors.

Patch Management Remediations List > [SCCM\\_Install\\_Missing\\_patches](#)

### Patch Management Remediation

\* Name: SCCM\_Install\_Missing\_patches [i](#)

Description: Important & Critical lvl

Operating System: Windows

Compliance Module: 4.x or later

Remediation Type: Automatic

\* Interval: 0 (Valid Range 0 to 9999)

\* Retry Count: 0 (Valid Range 0 to 99)

\* Patch Management Vendor Name: Microsoft Corporation

Remediation Option:  Enable  Install missing patches  Activate patch management software GUI

Check patches installed: Important & critical

**Products for Selected Vendor**

Product Name	Version	Enabled Remediation Support	Update Remediation Support	Show UI Remediation Support
Microsoft Intune Client	5.x	NO	NO	YES
System Center Configuration Ma...	5.x	YES	YES	YES

**Figure 15-33** Windows SCCM Patch Auto-Remediation

Another very common Windows remediation rule is the Windows Server Update Services (WSUS) rule. This remediation action allows the AnyConnect or NAC Agent to talk with the client's WSUS agent to ensure the client is patched correctly. [Figure 15-34](#) shows an example WSUS remediation action using severity level with a Microsoft Server. The Validate Windows Update Using option enables you to choose to trust the severity settings on your WSUS server (Severity Level radio button) or trust the Cisco rules that are downloaded to ISE. If you choose Cisco Rules, you can then select specific rules to check for in the corresponding posture requirement rule. These rules are ignored if you select the Severity Level option.

Windows Server Update Services Remediations List > [New Windows Server Update Services Remediation](#)

**Windows Server Update Services Remediation**

\* Name: WSUS\_Remediaion [i](#)

Description:

Compliance Module: Any version

Remediation Type: Automatic

Interval: 0 (in secs) (Valid Range 0 to 9999)

Retry Count: 0 (Valid Range 0 to 99)

Validate Windows updates using:  Cisco Rules  Severity Level

Windows Updates Severity Level: Express

Update to latest OS Service Pack

Windows Updates Installation Source:  Microsoft Server  Managed Server

Installation Wizard Interface Setting:  Show UI  No UI

**Submit** **Cancel**

**Figure 15-34** WSUS Remediation Action

When using the Severity Level option, you must choose the pr\_WSUSRULE compound condition in the corresponding posture requirement rule. When the posture requirement fails, the NAC Agent enforces the WSUS remediation action based on the severity level that you defined in the WSUS remediation action.

You also need to check the Update to Latest OS Service Pack check box if you want to force a Service Pack update on the client if one is available. Use this with care, because Windows Service Pack upgrades can be time-consuming and error-prone.

For the Windows Updates Installation Source setting, choose either Microsoft Server or

Managed Server. A Microsoft server is hosted by Microsoft in the Internet, whereas a managed server is a WSUS server that you administer internally.

If you choose the Show UI radio button for the Installation Wizard Interface Setting option, your users must have administrator access to their Windows client for it to operate. The UI shows the WSUS update progress.

ISE can also uninstall or stop an application from running on Windows or Mac. Use an Application remediation rule to get this done. Say, for example, that you want to uninstall all versions of a vulnerable program, kill a malicious application running, or uninstall any prohibited applications. You can do this using ISE Application remediation rules. [Figures 15-35](#) and [15-36](#) show an example of uninstalling BitTorrent on Mac OS X.

Application Remediation > Application Remediation  
Input fields marked with an asterisk (\*) are required.

Name *	Uninstall_bitTorrent
Description	Remove bittorrent from corp Macs
Operating System	Mac OSX +
Compliance module	4.x or later
Remediation Type *	Automatic
Interval *	0
Retry Count *	0
Remediation Option	<input checked="" type="radio"/> Uninstall <input type="radio"/> Kill Process

**Figure 15-35** Application Remediation Action

The screenshot shows the 'Remediation Option' section with 'Uninstall' selected. Below it, under 'Category', there is a checked checkbox. A list of categories follows:

<input type="checkbox"/> Unclassified	<input type="checkbox"/> Browser
<input type="checkbox"/> Encryption	<input type="checkbox"/> Anti-Malware
<input type="checkbox"/> Messenger	<input type="checkbox"/> Data Loss Prevention
<input type="checkbox"/> Backup	<input type="checkbox"/> Antiphishing
<input type="checkbox"/> Virtual Machine	<input checked="" type="checkbox"/> Public File Sharing
<input type="checkbox"/> Data Storage	<input type="checkbox"/> Patch Management
<input type="checkbox"/> VPN Client	<input type="checkbox"/> Firewall
<input type="checkbox"/> Health Agent	

Below this is a 'Vendor Name' field containing 'BitTorrent, Inc.' with a dropdown arrow.

At the bottom left, it says '1 Selected'. To the right are 'Rows/Page' (set to 2), navigation arrows, page number '1', and a total count '11'.

A 'Refresh' button is located below the vendor name field.

Product Name	Version
<input type="checkbox"/> BitTorrent	7.x
<input checked="" type="checkbox"/> BitTorrent	ANY

Figure 15-36 Application Remediation Action (Continued)

## Configure Posture Requirements

Now that you have configured or reviewed all of the pieces, the next step is to put them together in a series of posture requirements. A posture requirement is a set of compound conditions with an associated remediation action that can be linked with a role and an operating system. All the clients connecting to your network must meet mandatory requirements during posture evaluation to become compliant on the network. Several requirements come predefined in ISE and cover the AV, AM, USB, and AS use cases. In addition to these, you typically want to create a patch management or Windows update requirement. The requirements that you create are used as a part of your posture policies in the next section.

To create a posture requirement from the ISE GUI:

**Step 1.** Go to Work Centers > Posture > Policy Elements > Requirements.

**Step 2.** Click the drop-down arrow at the right end of a row and select **Insert New Requirement** or **Duplicate** to duplicate an existing one.

[Figure 15-37](#) depicts an example requirement.

Requirements					
Name	Operating Systems	Compliance Module	Stealth Mode	Conditions	Remediation
Actions					
USB_Block	for Windows All	using 4.x or later	using Disabled	met if USB_Check	then
USB_Block					Edit   ▾
Any_AM_Definition_Mac	for Mac OSX	using 4.x or later	using Disabled	met if ANY_am_mac_def	then
AnyAMDefRemediationMac					Edit   ▾
Windows Up-to-date	for Windows 10 (All)	using 4.x or later	using Disabled	met if pr_AutoUpdateCheck_Rule	then
WSUS_Remediation					Edit   ▾

**Figure 15-37** Windows Update Posture Requirement

The requirement in [Figure 15-37](#) called Windows Up-to-date applies to all Windows 10 endpoints and is met if the condition pr\_AutoUpdateCheck\_Rule is true. Otherwise, the remediation action of WSUS\_Remediation is executed. Create the requirements that you need for your environment and host security policy.

You can deploy the AnyConnect 4.4+ Agent in stealth mode to monitor and enforce Cisco ISE posture policies. Stealth mode allows posture to be run as a service without any user agent or interaction allowed.

You can configure the following remediations in stealth mode (must be set to Automatic mode):

- Create Anti-Malware Remediation
- Create Launch Program Remediation
- Create Patch Management Remediation
- Create USB Remediation
- Create Windows Server Update Services Remediation
- Create Windows Update Remediation

You cannot configure the following remediations in stealth mode:

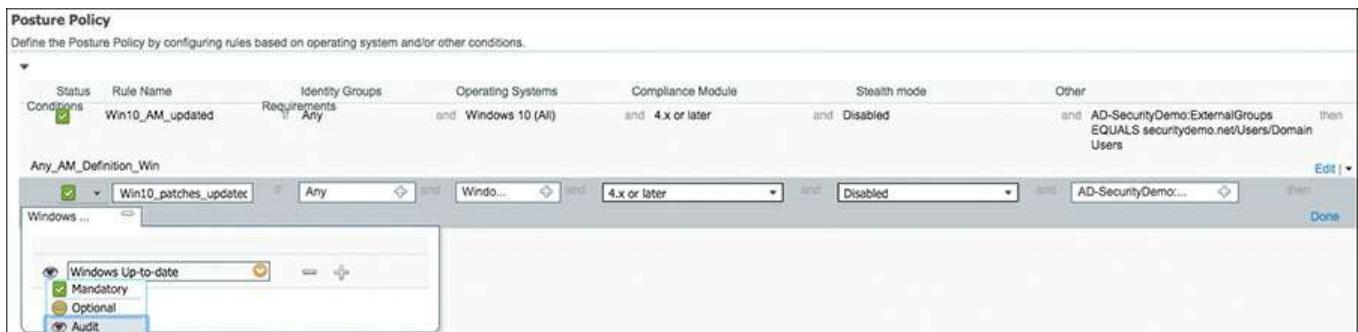
- Manual Remediation
- Link Remediation
- File Remediation
- Windows Server Update Services (WSUS) Remediation
- Patch Management Remediation—Activate Patch Management Software GUI (Remediation Option)
- AUP Policy

## Configure Posture Policy

Up to now, you have configured items to support the policies you will create in this section. This section enacts the posture assessment process within ISE.

To configure posture policy, navigate to **Work Centers > Posture > Posture Policy**. A posture policy maps posture requirements to selection criteria such as operating system, identity or external group, or other conditions. This allows you to define different posture policy rules, which you can individually enable or disable, for the various client and user types. Each requirement listed within a posture policy rule has its own status setting of Mandatory, Optional, or Audit ([Figure 15-38](#) shows the options). Mandatory means that the requirement must be met in order for the endpoint to be allowed on the network. Optional means that if the endpoint fails the requirement, it still passes onto the network but any automatic remediation actions are executed. Audit only logs the requirement result and does not affect the client's ability to access the network nor execute any automatic remediation actions. Audit requirements are transparent to the end user.

[Figure 15-38](#) shows the posture policy table along with an example policy. No policies are configured by default. If you have created policies, to add a new one just click the drop-down arrow at the far right of a rule and select either **Duplicate** or **Insert**.



**Figure 15-38** Posture Policy Table

The example policies shown in [Figure 15-38](#) are in Audit mode. It is highly recommended that you use Audit first to test that your policies work as expected. The first example policy ensures that all Windows 10 endpoints with Domain Users logged in have an up-to-date antimalware program. If the requirement fails, then the assigned remediation action kicks off an AM client definition file that updates automatically. Let's step through the setup of this policy:

**Step 1.** Set the status to **Enabled** (default) or **Disabled**.

**Step 2.** Provide a name to the policy that describes its purpose.

**Step 3.** Select the identity group that you want the policy to match against. You can set this to **Any** or to a specific group like **Employee** or **Contractor**. The example

sets it to **Any**, which is typical.

**Step 4.** Select the operating system to match this policy against. The example selects Windows 10, so any Windows 10 operating system will match it. You can select multiple operating systems within the same type but cannot mix operating systems of different types. For example, Windows 7 (All) or Windows 8 (All) is acceptable, but Windows 7 (All) or Mac OS X does not work.

**Step 5.** Select the version of the AnyConnect or NAC Agent compliance module. New installs should use version 4.x or higher.

**Step 6.** Set Stealth Mode to **Enabled** or **Disabled**.

**Step 7.** Setting Other conditions is optional but useful. An Other condition to consider is an initial posture condition. This means the policy only matches if the endpoint is going through its initial posture assessment and not a period reassessment. In this example, the Other condition defined that the user had to be a member of AD domain users to match this rule.

**Step 8.** Finally, define the requirement(s) when a rule is matched. Essentially, if all of the defined conditions are true, check the endpoint against certain posture requirements. In the example, there is just one requirement, Windows Up-to-date. This is a built-in ISE requirement you can use. What the policy doesn't show is the status of these requirements: Mandatory, Optional, or Audit. To edit or view the status, edit the policy and click the plus sign next to the requirements box. You can see the options in [Figure 15-38](#).

It is highly recommended that, in a production environment, all requirements start with a status of either Audit or Optional. This lessens the impact on your user community, helpdesk staff, and yourself. Because the posture reports in ISE provide you with a good idea of the impact your policies are having while in Audit or Optional status, you will know when the time is right to move them to Mandatory status. For example, you write a policy that requires AV to be installed and initially set it to Audit status. After a week, you check the ISE reports and determine that only 5% of your endpoints are failing the policy. At this time, you could move it to Optional status with automatic remediation. When you check back the following week, you see 99% of endpoints are passing, so you move the status to Mandatory to catch the last 1%.

[Figure 15-38](#) depicts another common posture policy, for monitoring that the Windows Update Service is running and, if it is not, automatically turning it on. You can see the fine detail of a requirement by editing the policy rule, clicking in the requirements box, and clicking the target symbol next to a requirement. This opens up additional detailed dialog boxes as shown in [Figure 15-39](#).



**Figure 15-39 Posture Policy Windows Update Detail**

The policy checks to ensure WSUS is running and is set to automatically enable updates if not. This policy affects AD Domain Users and Windows 10 (All) endpoints. The remediation action, in Audit mode, does not override the user's settings with the requirements settings of auto download and notify. The remediation action takes effect only after you move the policy to Optional or Mandatory status.

It is a best practice not to burden clients with an excessive amount of posture policy requirements. Doing so can adversely affect the user's network experience and login times. Keep it to a handful of your top security requirements per operating system.

## Configure Host Application Visibility and Context Collection (Optional)

ISE with AnyConnect is capable of providing you with a running record of all the applications installed, version information, and running processes on your hosts. This works for both Windows and Mac operating systems. AnyConnect collects information about installed applications only with the 4.x (or later) compliance module. ISE populates this data in the **Context Visibility > Endpoints** dashboard. This data can then be used by you to better understand the various applications installed and running on your endpoints. [Figure 15-40](#) shows an example.

Application Name	Version	Vendor	Running process	Category	Install Path
Windows Defender	6.1.7600.16385	Microsoft Corporation		AntiMalware	C:\Program Files\Win...
McAfee VirusScan Enterprise	8.8.0	McAfee, Inc.		AntiMalware	C:\Program Files (x86...
Cisco Advanced Malware Protection for En...	4.4.2.10200-93872e5	Cisco Systems, Inc.		AntiMalware	C:\Program Files\Sou...
Internet Explorer	11.0.9600.18537	Microsoft Corporation		AntiPhishing, Browser	C:\Program Files\Inte...
Google Chrome	56.0.2924.87	Google Inc.		AntiPhishing, Browser	C:\Program Files (x86...
Mozilla Firefox	51.0.1	Mozilla Corporation	2	AntiPhishing, Browser	C:\Program Files (x86...

**Figure 15-40 Endpoint Application Visibility and Context**

The Endpoint Applications list shows the following attributes:

- Application name.
- Application version.
- Vendor.
- Running processes for the application. If blank, that means the application was not running at the time of the audit. For each process, you are shown the Process Name, Hash, and Process ID.
- Category.
- Install path.

To set up ISE to start collecting endpoint application data, perform the following three steps:

**Step 1. Create an Application Condition.** Typically, this condition is set to collect Everything, but you can set it to collect just certain applications or categories of applications. See [Figure 15-41](#) for an example of collecting everything.

Application Condition > New	
Name *	Win_Apps_Collection
Description	AnyConnect will collect info on all Apps running on a host
Operating System *	Windows All <a href="#">+</a>
Check By *	Application
Compliance module	4.x or later
Application State *	<input checked="" type="checkbox"/> Installed <input checked="" type="checkbox"/> Running
Provision by	Everything

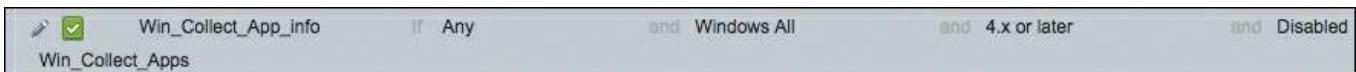
**Figure 15-41** Endpoint Application Visibility Condition

**Step 2. Create a Posture Requirement** for the condition in Step 1. Set the action to **Message Text Only** and input some text. This text is not displayed to your users. [Figure 15-42](#) provides an example.



**Figure 15-42** Endpoint Application Visibility Posture Requirement

**Step 3.** Finally, create a **Posture Policy Rule** that executes your requirement on the hosts you want it to gather information from. Ensure that you set your rule requirement to **Audit** mode. [Figure 15-43](#) provides an example.



**Figure 15-43** Endpoint Application Visibility Posture Policy Rule

## Enable Posture Client Provisioning and Assessment in Your ISE Authorization Policies

At this stage, all of the building blocks required to enable both posture client provisioning and authorization based on posture compliance are in place.

### Posture Client Provisioning

This section walks you through an example of how to enable posture client provisioning to detect when a user does not have AnyConnect with the compliance module installed and redirect the user to the necessary files for download and installation. Here are the steps:

**Step 1.** On the network device CLI or GUI, create an ACL named **redirect-acl**. You will enter this ACL name in the ISE authorization profile that you create in Step 3. This ACL defines what traffic type triggers a redirect action on the NAD. A redirect ACL should not trigger on traffic to and from ISE PSNs, DNS, and DHCP, at a minimum. You can set up your ACL to trigger on all other IP traffic or just on HTTP and HTTPS traffic.

**Note** Cisco Wireless LAN Controllers and switches interpret their redirect ACLs oppositely. On a Cisco WLC, a permit ACL rule defines traffic that will not trigger a redirect and a deny rule match triggers a redirect. Conversely, on a Cisco switch, a permit ACL rule match triggers a redirect and a deny ACL rule defines traffic that will not trigger a redirect.

**Step 2. (Optional)** Create a dACL in ISE to restrict users' access to your network during client provisioning. Ensure that you allow DNS plus HTTP/S and client access to all Cisco Provisioning Portal (CPP) pages' IP address and port.

**Step 3.** Create an authorization profile for client provisioning. Go to **Work Centers >**

**Posture > Policy Elements > Authorization Profiles.** Click **Add**. At a minimum, fill in the following profile form entries (also shown in [Figure 15-44](#)):

- In the Name text box, provide a meaningful name.
- From the Access Type drop-down list, choose **ACCESS\_ACCEPT**.
- Expand **Common Tasks**, check the **Web Redirection** check box, and choose **Client Provisioning (Posture)** from the drop-down list. Enter the name of the ACL you created in Step 1 and set **Value** to the provisioning portal you created earlier.
- Optionally, check the **DACL Name** check box and enter a name for it.

The screenshot shows the 'Authorization Profiles > AnyConnect\_CPP' section. Under 'Authorization Profile', the 'Name' is 'Posture\_CPP', 'Description' is 'Client Provisioning Portal redirect for AnyConnect posture agent', and 'Access Type' is 'ACCESS\_ACCEPT'. Below this, under 'Network Device Profile', there is a dropdown set to 'Cisco'. Under 'Common Tasks', the 'DACL Name' is checked and set to 'Limited\_Traffic'. The 'Web Redirection (CWA, MDM, NSP, CPP)' checkbox is also checked. A dropdown for 'Client Provisioning (Posture)' is set to 'redirect-acl', and the 'Value' dropdown is set to 'ACME Client Provisioning Porta'. At the bottom, a summary box displays the following:  
Access Type = ACCESS\_ACCEPT  
DACL = Limited\_Traffic  
cisco-av-pair = url-redirect-acl=redirect-acl  
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=148d25f0-0767-11e7-aa0e-0242982dc559&action=cpp

**Figure 15-44** Authorization Profile for Posture Client Provisioning

## Authorization Based On Posture Compliance

At this point, ISE is collecting posture information from your hosts and performing the remediation actions, if any, that you specified. Now you need to add authorization rules (at least two) that change a user's network permissions based on their posture compliance. You also must designate a posture agent for automatic installation if the client doesn't already have one. This will be done using the CPP set up previously.

**Tip** It is a good idea to initially set your posture authorization rules to Audit mode. Then set them to Mandatory or Optional after you have verified they function as expected.

Here are the steps to complete:

**Step 1.** Create a Posture provisioning redirect authorization policy rule that matches when a host doesn't have a posture client to respond to ISE with. This rule redirects them to the Client Provisioning Portal page so that they can get the NAC Agent. Go to **Work Centers > Posture > Policy Sets** and select the relevant policy set. In the Authorization Rules section, select **Insert New Rule**. [Figure 15-45](#) shows the result after selecting Insert New Rule and completing the task.

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
●	Posture_Compliant	If Session:PostureStatus EQUALS Compliant	then PermitAccess
●	Posture_NonCompliant	If Session:PostureStatus EQUALS NonCompliant	then Quarantined
●	Posture_Provisioning_Redirect	If Session:PostureStatus NOT_EQUALS Compliant	then Posture_CPP

**Figure 15-45** Authorization Rules for Posture

**Step 2.** Insert a Posture\_Compliant authorization rule above the Posture\_Provisioning\_Redirect rule in Step 1. This rule matches when a host returns posture status equals compliant, meaning the host passes all of your posture requirements. The permissions of this rule should match the network access permission you want to assign to your compliant hosts. Because the authorization rules are processed top down, first match, the redirect rule will never execute. See [Figure 15-45](#) for an example.

**Step 3.** Finally, insert a Posture\_NonCompliant authorization rule above the Posture\_Provisioning\_Redirect rule in Step 1 that puts the host in Quarantine so that posture remediation can start. You need to define which permissions are allowed while in quarantine, but they should include access to any remediation resources that you want the client to access. See [Figure 15-45](#) for an example.

## Posture Reports and Troubleshooting

ISE has several reports for posture. To view the relevant reports available, go to **Work Centers > Posture > Reports**. The best reports for posture are Client Provisioning, Posture Assessment by Condition, Posture Assessment by Endpoint, and Current Active Sessions. You can schedule these reports or run them on demand.

For troubleshooting, ISE has a built-in Posture Troubleshooting tool, located at **Work Centers > Posture > Troubleshoot**. The Posture Troubleshooting tool helps you to find the cause of a posture-check failure by identifying the following:

- Which endpoints were successful in posture and which were not
- If an endpoint failed in posture, what steps failed in the posture process
- Which mandatory and optional checks passed and failed

ISE logs are also helpful for detailed posture troubleshooting. Go to **Administration > System > Logging > Debug Log Configuration**. For posture troubleshooting, the following ISE log components need to be in debug mode on the ISE nodes where the posture process happens:

- **client-webapp:** Component responsible for agent provisioning. Target log files guest.log and ise-psc.log.
- **guestaccess:** Component responsible for Client Provisioning Portal component and session owner lookup. Target log file guest.log.
- **provisioning:** Component responsible for client provisioning policy processing. Target log file guest.log.
- **posture:** All posture-related events. Target log file ise-psc.log.

For the AnyConnect compliance module (client side) troubleshooting, you can use

- **acisensa.log:** In case of a client provisioning failure on the client side, this file is created in the same folder from which the NAC Agent or AnyConnect software installation was run (the Downloads directory for Windows, normally).
- **AnyConnect\_ISEPosture.txt:** This file can be found in the DART bundle in directory Cisco AnyConnect ISE Posture Module. All information about ISE PSN discovery and general steps of posture flow are logged into this file.

## Enable Posture Assessment in the Network

You need to ensure that your endpoints are allowed the proper communication rights while in quarantine and performing posture assessment and remediation activities.

Ensure that the access switch pre-posture/limited access ACL allows HTTPS and SWISS communication between the Cisco ISE Policy Service Node(s) and the endpoint. Here is an example ACL showing the ports needed for posture assessment to work:

[Click here to view code image](#)

```
remark Allow DHCP
permit udp any eq bootpc any eq bootps
remark Allow DNS
```

```

permit udp any any eq domain
remark Allow ping to ISE PSN and any other devices necessary
permit icmp any host <ISE PSN IP>
! This is for URL redirect
permit tcp any host <ISE PSN IP> eq 443
! This is for URL redirect
permit tcp any host <ISE PSN IP> eq www
! This is for guest portal
permit tcp any host <ISE PSN IP> eq 8443
! This is for posture
! Communication between NAC agent and ISE (SWISS ports)
permit tcp any host <ISE PSN IP> eq 8905
! This is for posture
! Communication between NAC agent and ISE (SWISS ports)
permit udp any host <ISE PSN IP> eq 8905
deny ip any any

```

Ensure that you create a similar quarantine ACL for the posture-noncompliant endpoints with these rights plus rights to access the remediation IPs.

Finally, ensure that nothing in the traffic path—such as firewalls, ACLs, and so on—is preventing the traffic from flowing.

**Note** During posture assessment of a Windows endpoint using a login script, the endpoint user may encounter a delay in accessing the desktop. The reason might be that Windows is trying to restore the file server drive letter mappings before providing the user access to the desktop. The following are best practices to avoid the delay during posture:

- Use Windows Group Policy Preference (GPP) drive mappings instead of a login script. GPP has a reconnect setting.
- If you have to use login scripts, then set your drive mappings to nonpersistent, such as net use S: \\server\share /persistent:no.
- Allow endpoints to reach the Active Directory server so the file server drive letter can be mapped properly. When posture (with AnyConnect ISE Posture Agent) triggers, it blocks access to AD, causing a delay in login. Use Posture Remediation ACLs to provide access to AD servers before posture is completed.
- Set a delay for the login script until posture completes and set the drive mapping Persistence attribute to **NO**. Windows tries to reconnect all the network drives during login, and this cannot be done until the AnyConnect ISE Posture Agent gains full network access.

## **Summary**

This chapter covered the details of configuring posture assessment on the Cisco ISE. Here are the high-level steps that were covered in this chapter:

- 1.** Configure your network devices to connect users.
- 2.** Configure client provisioning:
  - a.** Download to ISE the latest posture updates and the client provisioning packages.
  - b.** Verify the default global posture settings meet your needs.
  - c.** Configure the posture client provisioning policy.
  - d.** Configure the Client Provisioning Portal.
- 3.** Configure posture elements:
  - a.** Configure posture conditions.
  - b.** Configure posture remediation.
  - c.** Configure posture requirements.
- 4.** Configure posture policy.
- 5.** Optionally, configure host application visibility and context collection.
- 6.** Optionally, configure ISE posture integration with Microsoft SCCM.
- 7.** Enable posture client provisioning and assessment in your ISE authorization policies.
- 8.** Enable posture assessment in the network.

When used correctly, ISE posture assessment can greatly increase the host visibility and security throughout your organization. Plus, you'll sleep better knowing only security-compliant endpoints are allowed to attach to your network.

# Chapter 16 Supplicant Configuration

This chapter covers the following topics:

- Comparison of popular supplicants
- Configuring common supplicants

The client 802.1X supplicant is a critical part of any Identity Services deployment. What is a supplicant? A client supplicant is simply the piece of software that the operating system uses to connect to networks, both wired and wireless. All of the major operating systems (such as Windows, Mac OS X, Android, iOS, Linux) and many network devices (such as Cisco IP Phones, IP cameras, and so on) include a built-in supplicant. The network access devices (NAD) interact with the client's supplicant upon connection to the wired or wireless network. The 802.1X transactions are performed between supplicant and the NAD. The NAD then talks RADIUS to Cisco ISE.

Cisco ISE has a very nice feature called native supplicant provisioning. This feature allows you to remove the burden from the end users of configuring their own supplicant; instead, it does it automatically for them via an ISE supplicant provisioning wizard. This feature is highly recommended because of its ability to simplify the deployment of ISE. It only works with the native built-in supplicants in the following operating systems:

- Android
- Mac OS X
- Apple iOS (for Apple iPhones and iPads)
- Microsoft Windows Vista, 7, 8/8.1, and 10

**Note** If you are using one of these OSs, it is highly recommended that you skip this chapter and instead read [Chapter 17, “BYOD: Self-Service Onboarding and Registration,”](#) which covers client provisioning in detail.

If you will not be using the native supplicants or would prefer not to use the ISE client provisioning wizards, this chapter is for you. It covers the configuration steps for the following client supplicants:

- Cisco AnyConnect Network Access Manager (NAM) for Windows
- Windows 7 Native Supplicant
- Mac OS X 10.8.2 Native Supplicant

The configuration steps focus solely on the wired network portion of their configuration.

There is a lot of knowledge and readily available information for wireless configuration already out there, so including it here would be redundant.

## Comparison of Popular Supplicants

There are only a handful of popular supplicants on the market today and a bunch of niche supplicants. The most popular ones for wired are the following:

- Windows Native Supplicant
- Mac OS X Native Supplicant
- Android/iOS Native Supplicants
- Cisco AnyConnect Secure Mobility NAM Client
- Linux Native Supplicants (wpa\_supplicant)

When deciding on which supplicant to use, answer these basic questions:

1. What is the dominant OS going to be in my ISE deployment?
2. Are most of my clients members of Active Directory?
3. Which Extensible Authentication Protocol (EAP) type(s) will be required (PEAP, EAP-TLS, EAP-FAST, EAP-MSCHAPv2, etc.)?
4. Do I require an all-in-one client?
5. Will I be using the ISE native supplicant provisioning?
6. Is EAP-chaining required? EAP-chaining provides differentiated access based on enterprise and non-enterprise assets. It also has the ability to validate users and devices in a single EAP transaction and to perform both machine authentication and user authentication simultaneously.

You must consider several other deciding factors, depending on the complexity of your ISE deployment, but these are the most common ones. After you answer the preceding questions, you will be able to match your answers with the available supplicants and their requirements. It is space-prohibitive, and highly susceptible to becoming quickly outdated, to list all the supplicants and their supported features here. Instead, you should check the websites of the supplicant vendors for these details.

**Note** In general, the native OS supplicants are sufficient for your ISE deployment. If you are using either Microsoft Active Directory Group Policy or Cisco ISE native client provisioning, you must choose the native supplicant.

## Configuring Common Supplicants

This section deals with the manual configuration steps for some of the most common supplicants. Specifically, it covers Windows 7 Native, Mac OS X Native, and Cisco AnyConnect NAM. Only Wired 802.1X configuration is covered.

## Mac OS X 10.8.2 Native Supplicant Configuration

In versions 10.8+ of OS X, Apple changed the wired 802.1X configuration steps. The good news is that the change made it a zero configuration setup for the vast majority of wired 802.1X ISE deployments. Upon connecting to the Ethernet network, the 802.1X authentication process is started automatically and the user is presented with a popup message to log in to the network.

**Note** By default, during 802.1X authentication, OS X requires that the name in the server's certificate must match its DNS hostname. So, ensure that your ISE server-side certificate complies.

If the default setting for autoconnect, as shown in [Figure 16-1](#), has been modified, you can reenable it by following these steps:

**Step 1.** Click **System Preferences** and select **Network** under **Internet and Wireless**.

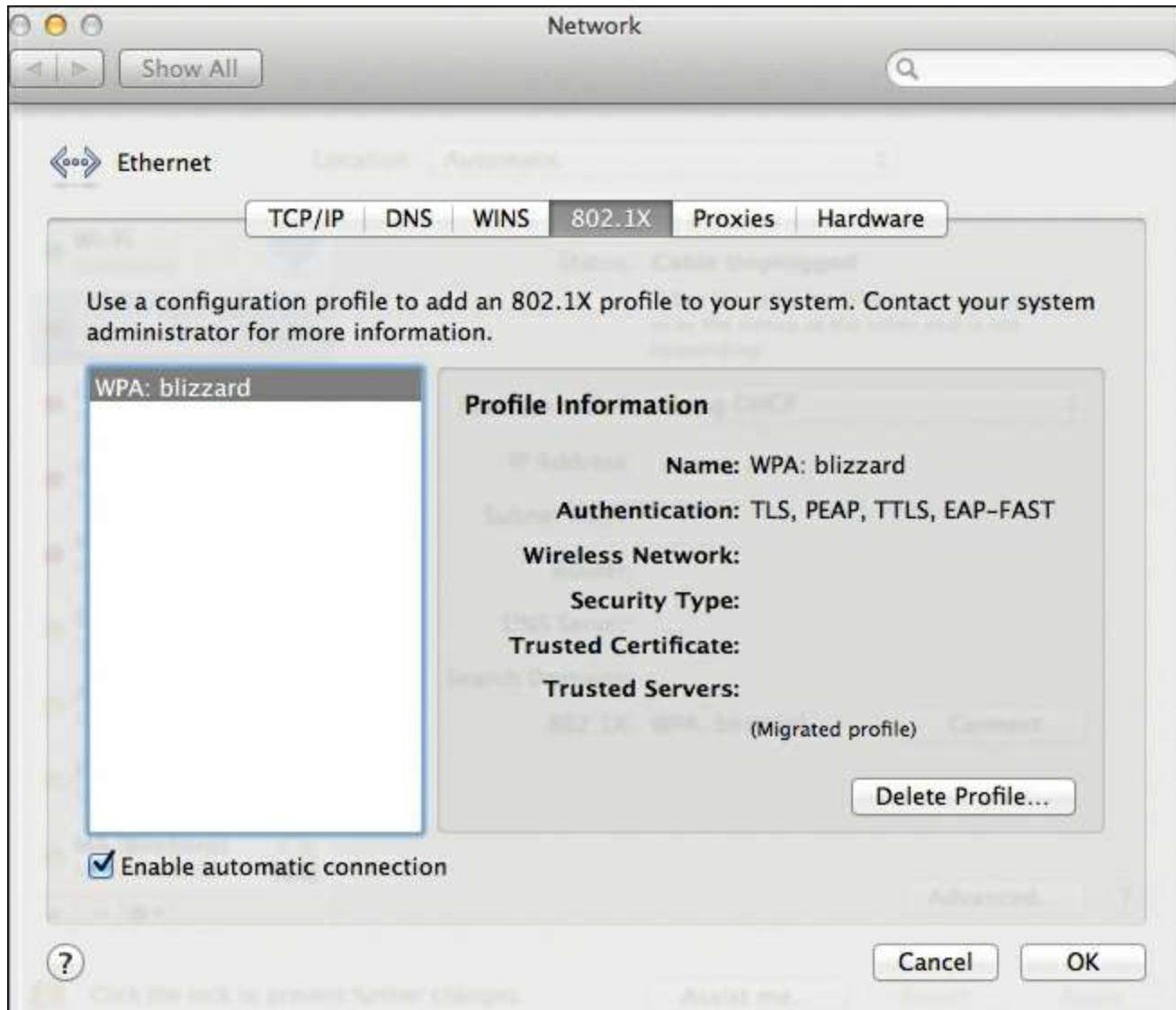


**Figure 16-1** Network—Ethernet

**Step 2.** Click **Ethernet** and click **Advanced**.

**Step 3.** Click the **802.1X** tab.

**Step 4.** Check the **Enable Automatic Connection** check box, as shown in [Figure 16-2](#).



**Figure 16-2** Network—Ethernet 802.1X

To access networks that cannot be joined with the method shown in [Figure 16-2](#), or to use a login window mode or a system mode profile, you need to create and distribute a .mobileconfig file to clients that contains the correct network configuration information. You can create a .mobileconfig file by using the Profile Manager service provided in macOS Server. See Apple's support site for detailed information.

## Windows GPO Configuration for Wired Suplicant

Windows 2008r2 or newer includes the capability to use Group Policy Objects (GPO) to configure clients' wired and wireless 802.1X settings. For complete instructions, go to <https://technet.microsoft.com/en-us/library/cc733169.aspx>.

Here are the common steps for configuring wired GPO 802.1X settings using EAP-TLS with certificates and single sign-on (SSO). This assumes you have already delivered the full certificate chain for your CA and machine and identity certificates to the client,

hopefully using GPO for that as well.

**Step 1.** Open the Group Policy Management console, as shown in [Figure 16-3](#).



**Figure 16-3** GPO Management Console

**Step 2.** Select your domain. Either create a new Group Policy Object or select an

existing one. Right-click and select **Edit**. This opens the Group Policy Management Editor, as shown in [Figure 16-4](#).



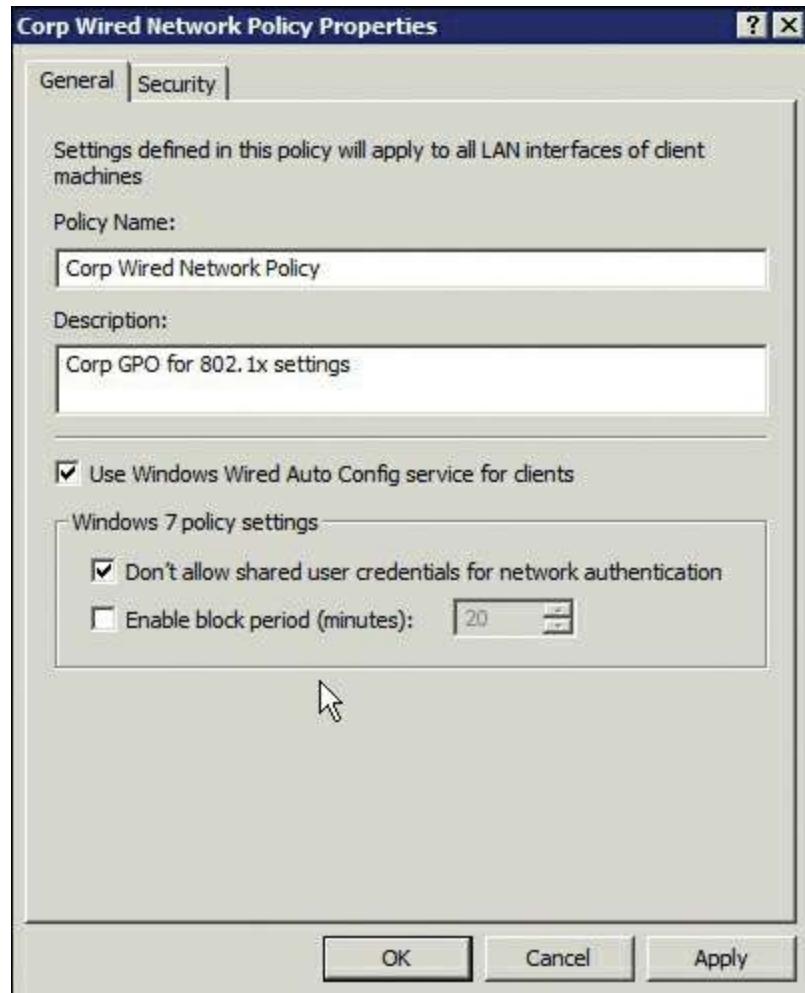
**Figure 16-4** GPO Management Editor

**Step 3.** Create a new wired network policy. To do this, go to **Computer Configuration > Policies > Windows Settings > Security Settings > Wired Network Policies**. Right-click and select **Create a New Wired Network Policy for Windows Vista and Later Releases**, as shown in [Figure 16-5](#).



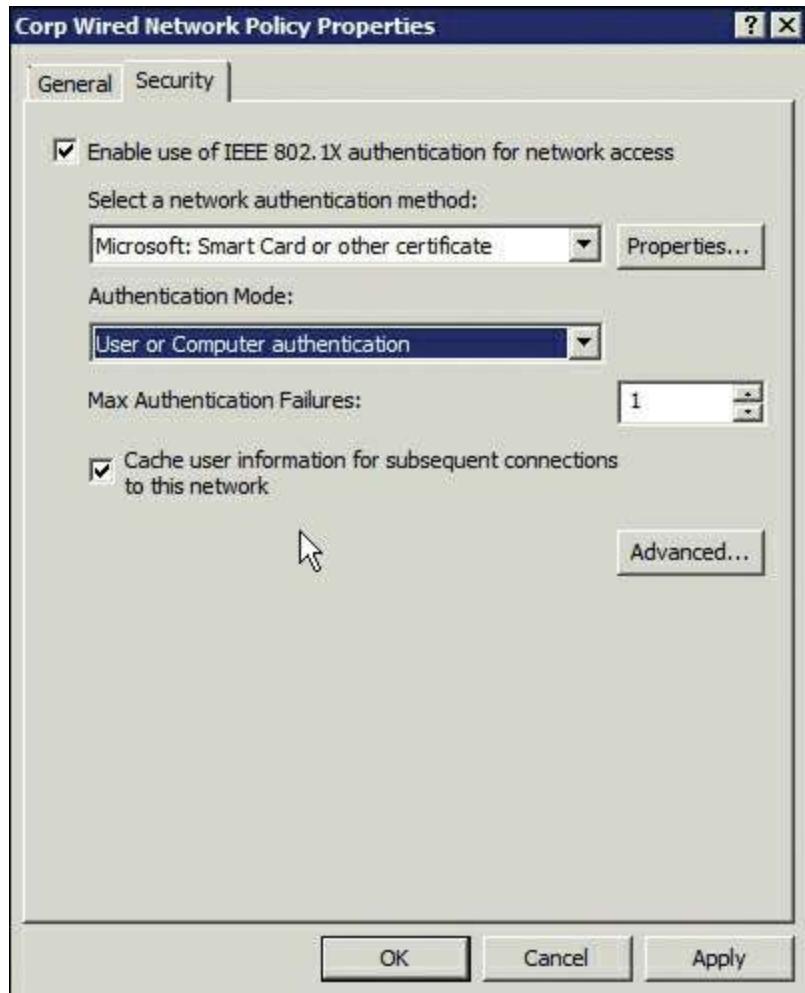
**Figure 16-5** Wired Network Policy Creation

**Step 4.** Fill in the policy name and description. Be sure to check **Use Windows Wired Auto Config Service for Clients**. Optionally, check **Don't Allow Shared User Credentials for Network Authentication**. See [Figure 16-6](#) for an example.



**Figure 16-6** Wired Network Policy—General Settings

**Step 5.** Click the **Security** tab, shown in [Figure 16-7](#). Check the **Enable Use of IEEE 802.1X Authentication for Network Access** check box.

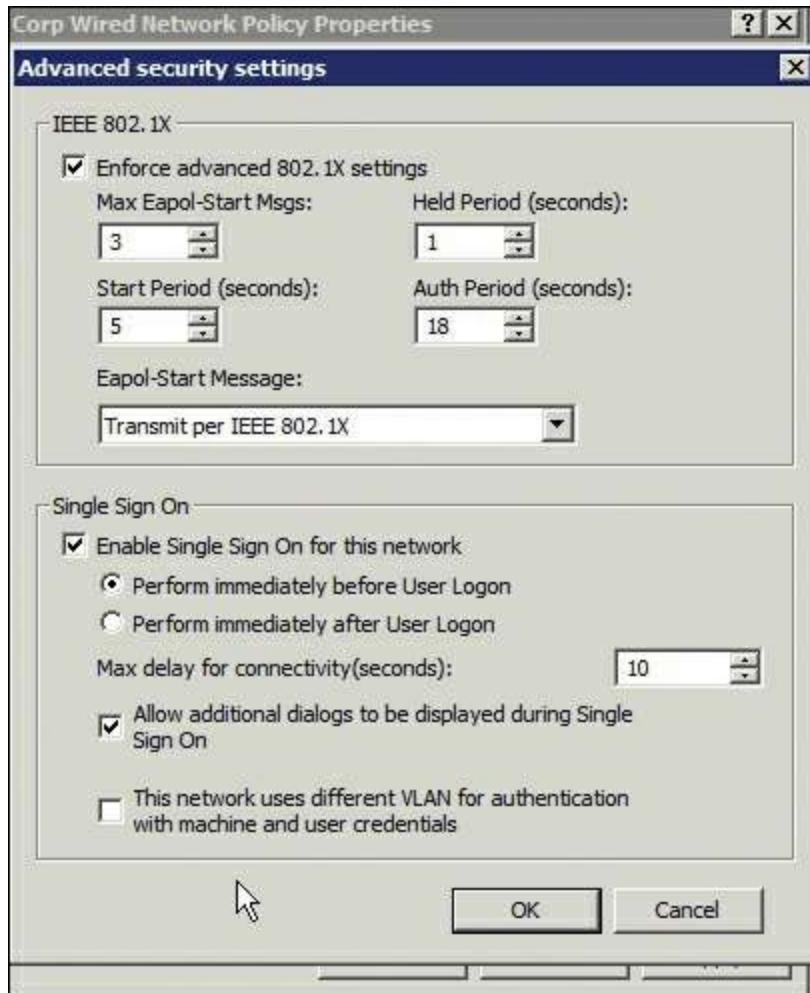


**Figure 16-7** Wired Network Policy—Security Settings

**Step 6.** From the Select a Network Authentication Method drop-down list, choose **Microsoft: Smart Card or Other Certificate**.

**Step 7.** Check the **Cache User Information for Subsequent Connections to this Network** check box.

**Step 8.** Click the **Advanced** button. In the Advanced Security Settings dialog box, shown in [Figure 16-8](#), check the **Enforce Advanced 802.1X Settings** check box. You can leave the defaults or change for your environment.



**Figure 16-8** Wired Network Policy—Advanced Security Settings

**Step 9.** Check **Enable Single Sign On**. The most common setting is **Perform Immediately Before User Logon**. This allows the user to log on to the domain and run logon scripts.

**Step 10.** Check **Allow Additional Dialogs to Be Displayed During Single Sign On**.

**Step 11.** If you will be using ISE to change the wired switchport VLAN between machine logon and user logon, check **This Network Uses Different VLAN for Authentication with Machine and User Credentials**.

**Step 13.** Click **OK**. The Advanced Security Settings dialog box closes, returning you to the Security tab. On the Security tab, click **Properties**. The Smart Card or other Certificate Properties dialog box opens, shown in [Figure 16-9](#).



**Figure 16-9** Wired Network Policy—Certificate Settings

**Step 14.** Click the **Use a Certificate on This Computer** radio button and check the **Use Simple Certificate Selection** check box.

**Step 15.** Check **Validate Server Certificate**.

**Step 16.** Check **Connect to These Servers** and type the name of each ISE policy server, exactly as it appears in the Subject field of the ISE server's certificate. Use semicolons to specify multiple ISE server names.

**Step 17.** Leave everything else disabled. For higher security settings, see the Microsoft documentation. Click **OK** and **OK** to close this all out.

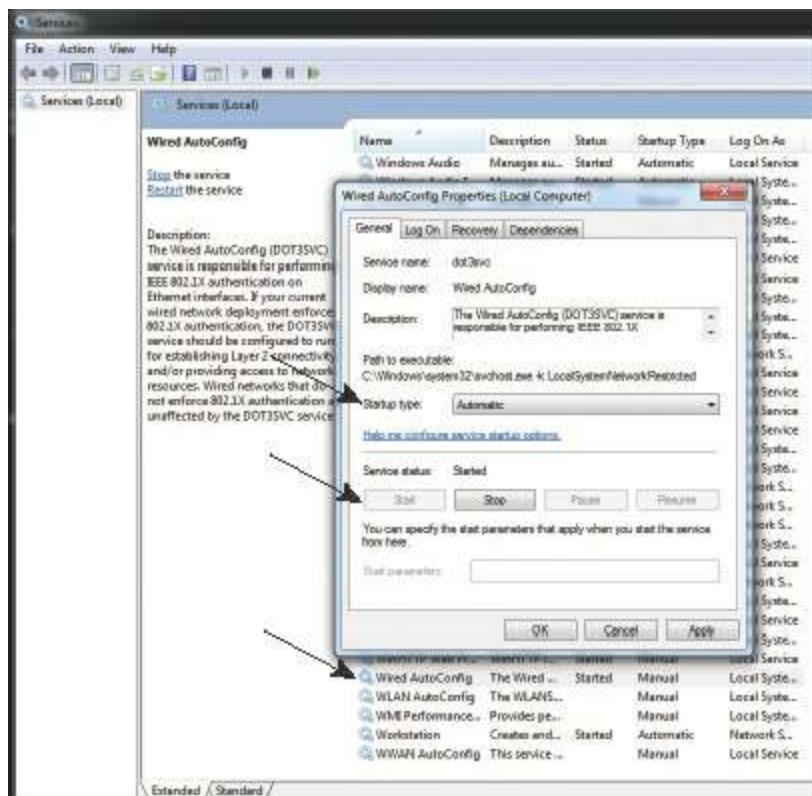
Your new policy will be pushed out to your clients the next time they do a GPO update.

## Windows 7, 8/8.1, and 10 Native Suplicant Configuration

Microsoft disables wired 802.1X by default on Windows 7, 8/8.1, and 10. The following steps show you how to enable and configure wired 802.1X on Windows 7. You must be logged in as an administrator to complete these steps.

**Step 1.** Open Windows Services. Go to **Start > Search**, type in **services**, and click **Services** in the search results under Programs. This opens the Services Management Console.

**Step 2.** Select and double-click **Wired AutoConfig**. In the dialog box that opens, from the Startup Type drop-down list, choose **Automatic**, as shown in [Figure 16-10](#). Click **Start** to start the service. Click **OK**. The 802.1X service is now enabled by default.



**Figure 16-10** Enable 802.1X Permanently

**Step 3.** Open the Control Panel and choose **Network and Internet > Network Connections**. Select your wired interface, right-click, and choose **Properties**. See [Figure 16-11](#) for details.



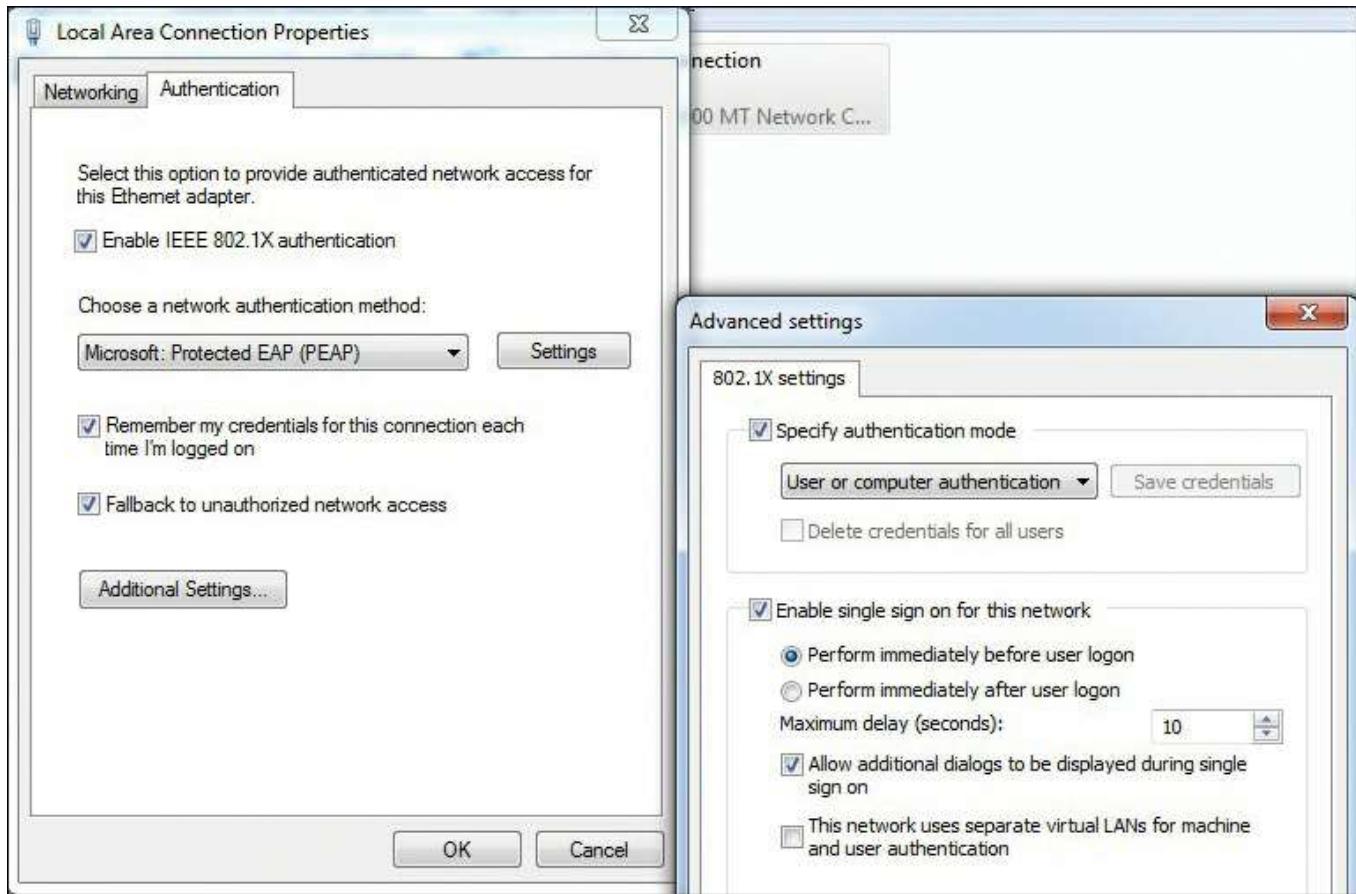
**Figure 16-11** Set Up Wired 802.1X

**Step 4.** Click the **Authentication** tab (this appears only if you have enabled the Wired AutoConfig service). Check **Enable IEEE 802.1X authentication**. Choose your authentication method; Protected EAP (PEAP) is the most popular, because it uses your AD username and password by default. See [Figure 16-12](#) for details.



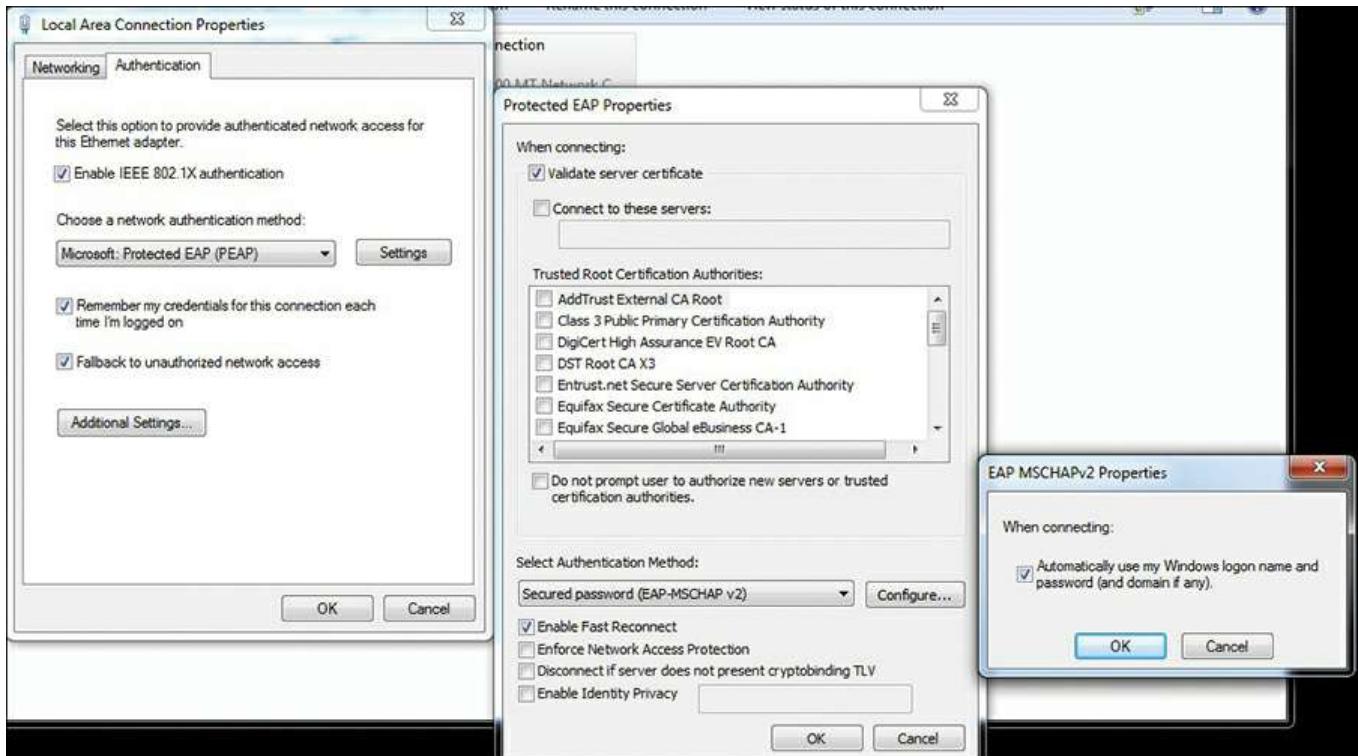
**Figure 16-12** Set Up Wired 802.1X Authentication

**Step 5.** Click **Additional Settings**. In the Advanced Settings dialog box, shown in [Figure 16-13](#), specify your authentication mode. Also, enable single sign-on. Click **OK**.



**Figure 16-13** Configure Wired 802.1X Advanced Settings

**Step 6. (Optional) Click **Settings**.** Depending on the authentication method you chose, you may or may not have to configure settings. If you chose PEAP, the defaults are fine in most cases. If you want to use PEAP but not have it automatically use your Windows logon name and password, click **Configure** next to Secured Password (EAP-MSCHAPv2) and uncheck the box. See [Figure 16-14](#) for an example.



**Figure 16-14 Configure Wired 802.1X PEAP Properties**

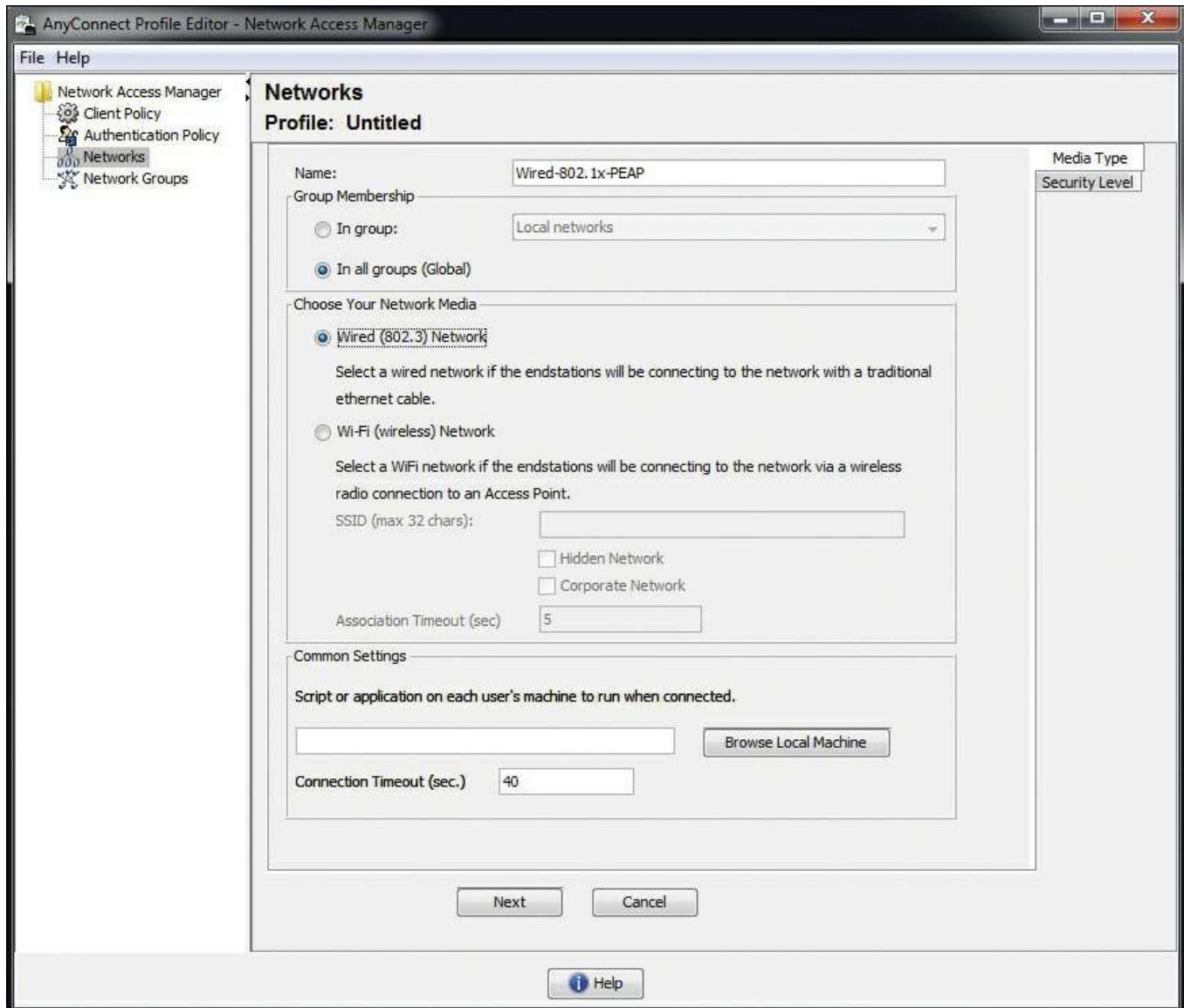
**Step 5.** Click **OK** until you close out all the dialog boxes.

Your Windows 7 client is now ready to connect to a wired 802.1X protected network.

## Cisco AnyConnect Secure Mobility Client NAM

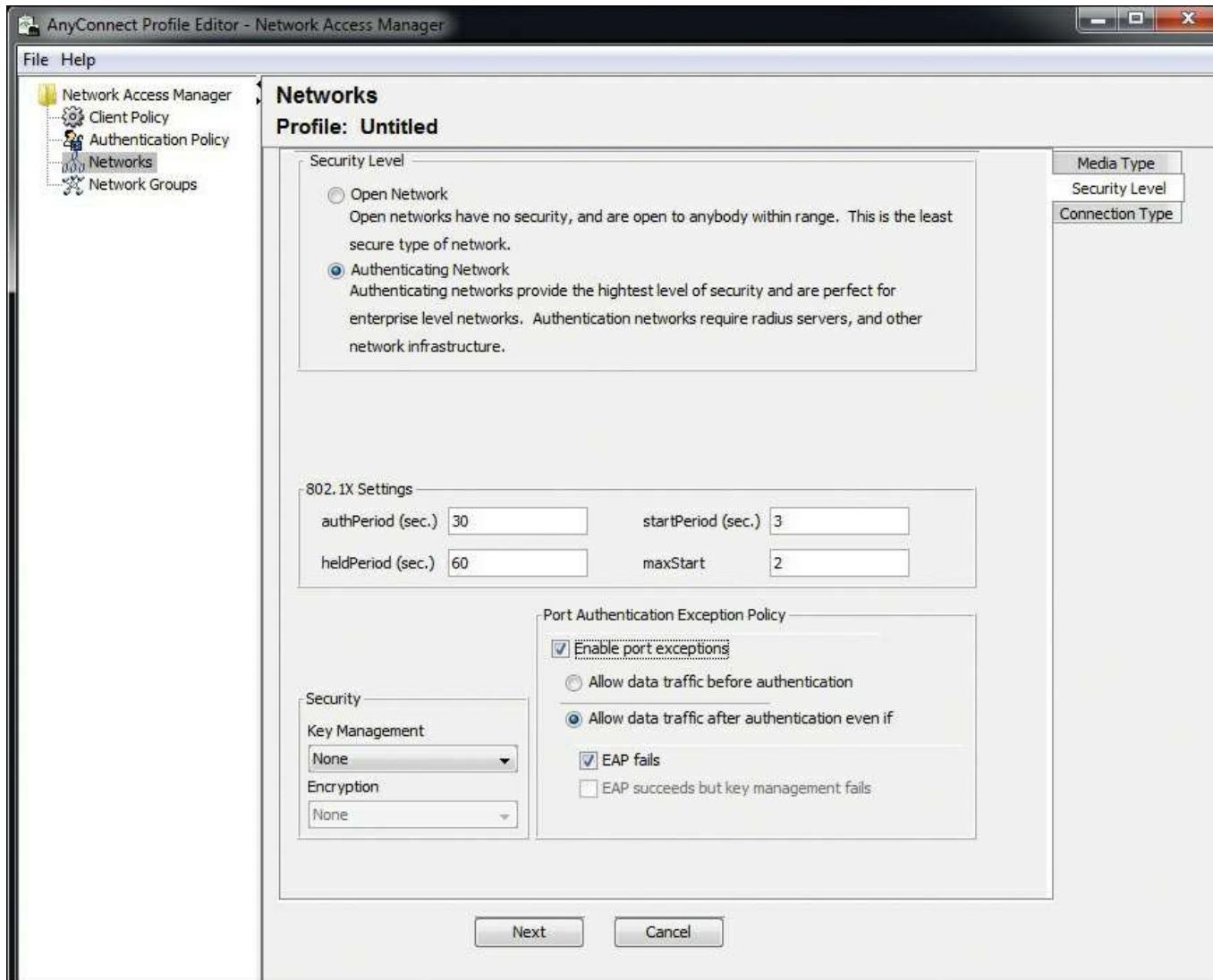
This section walks through how to set up the Cisco AnyConnect client for wired PEAP 802.1X authentication. To start, you must download the standalone AnyConnect Profile Editor from [Cisco.com](http://Cisco.com) or use the profile editor inside of Cisco Adaptive Security Device Manager (ASDM) or Cisco Security Manager (CSM). Once you have a profile editor installed, proceed with these steps:

**Step 1.** Open AnyConnect Profile Editor and select **Networks**. Click **Add** to launch the wizard shown in [Figure 16-15](#). Provide a name. Change Group Membership to **In All Groups (Global)**. Select **Wired** under Choose Your Network Media. Click **Next**.



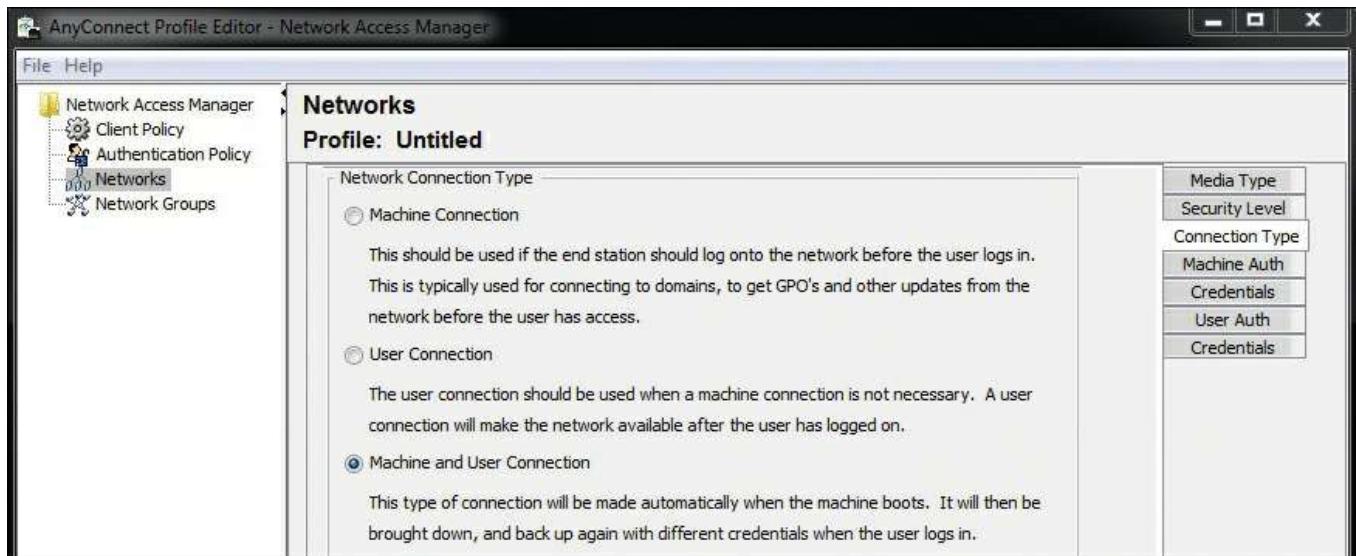
**Figure 16-15** AnyConnect NAM 802.1X Wired Profile

**Step 2.** On the Security Level wizard page, shown in [Figure 16-16](#), click the **Authenticating Network** radio button. If you are running in 802.1X open mode, do the following: check **Enable Port Exceptions**, click **Allow Data Traffic After Authentication Even If**, and check **EAP Fails**. In open mode, you want to ensure that your clients still access the network even if they have a failure, and this setting accomplishes that. Once you move away from open mode, you need to disable this setting. Click **Next**.



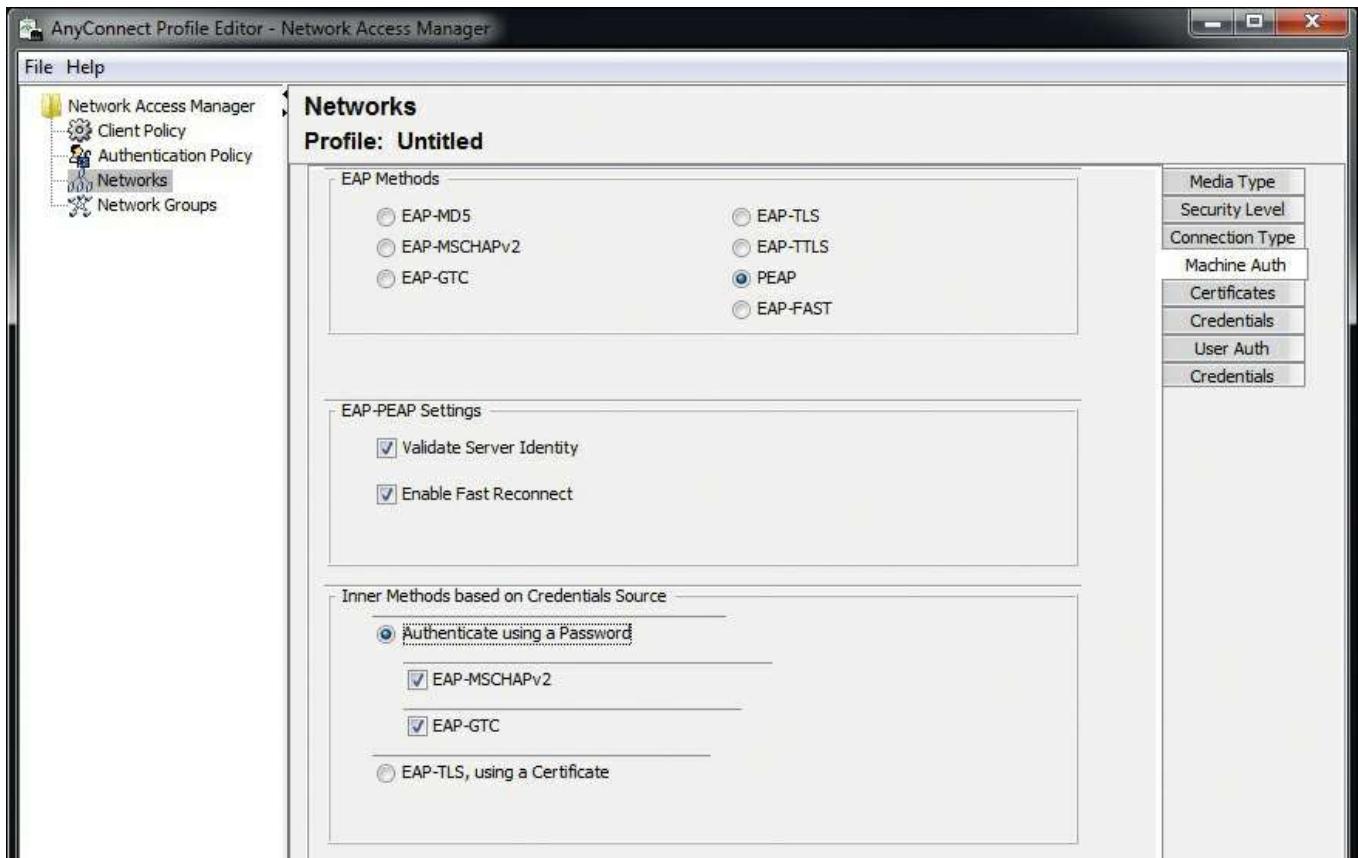
**Figure 16-16** AnyConnect NAM Profile Security Level

**Step 3.** On the Connection Type page, shown in [Figure 16-17](#), select **Machine and User Connection** (or the setting of your choice). Click **Next**.



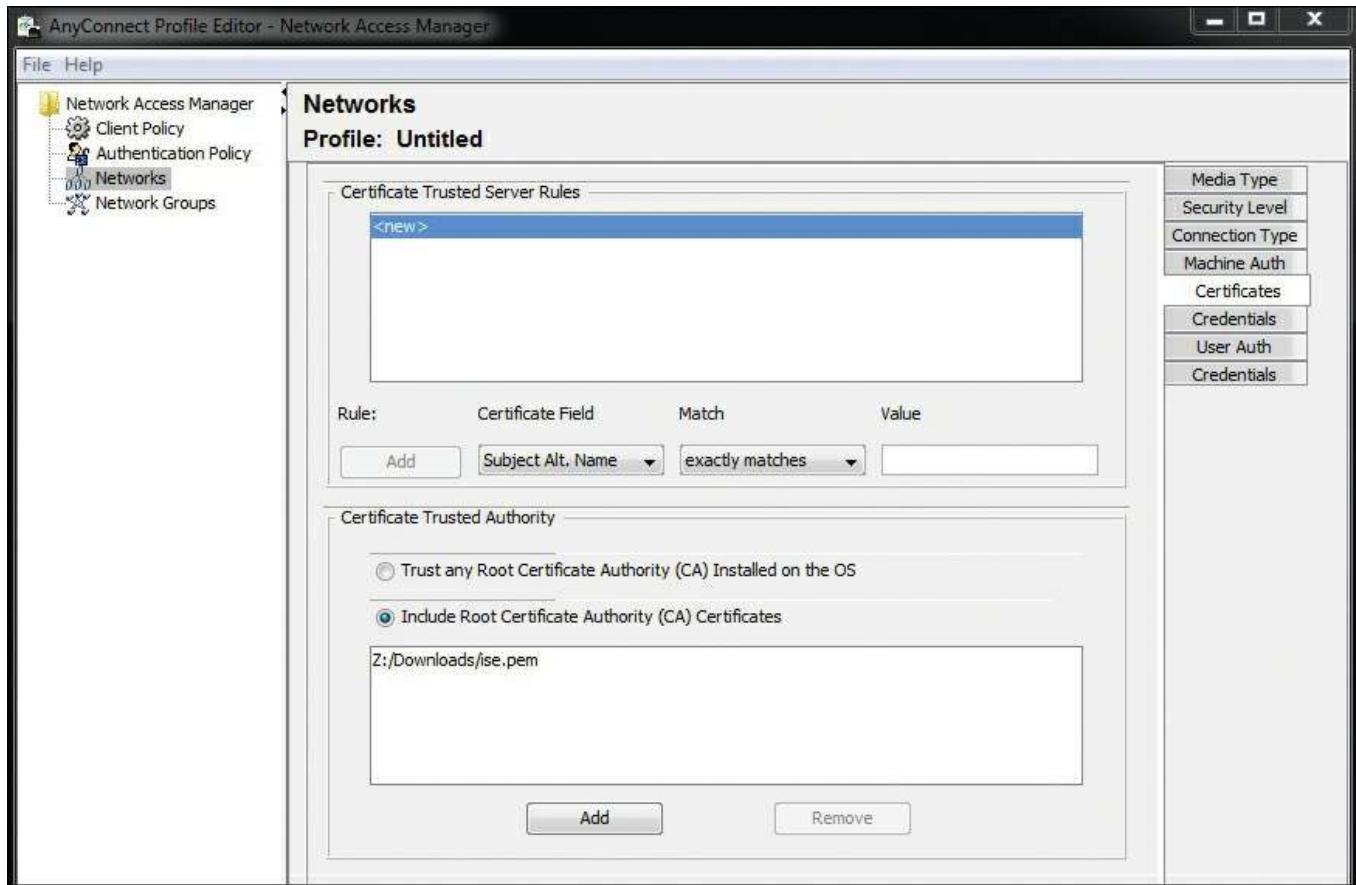
**Figure 16-17 AnyConnect NAM Profile Connection Type**

**Step 4.** On the Machine Auth page, enable **PEAP**, as shown in [Figure 16-18](#). The default settings are usually not changed. Click **Next**.



**Figure 16-18** AnyConnect NAM Profile Machine Auth

**Step 5.** On the Certificates page, you have the option to upload root certificates as part of the profile. If you need to do this (i.e., you are using your own CA server), add them here as shown in [Figure 16-19](#). Click **Next**.



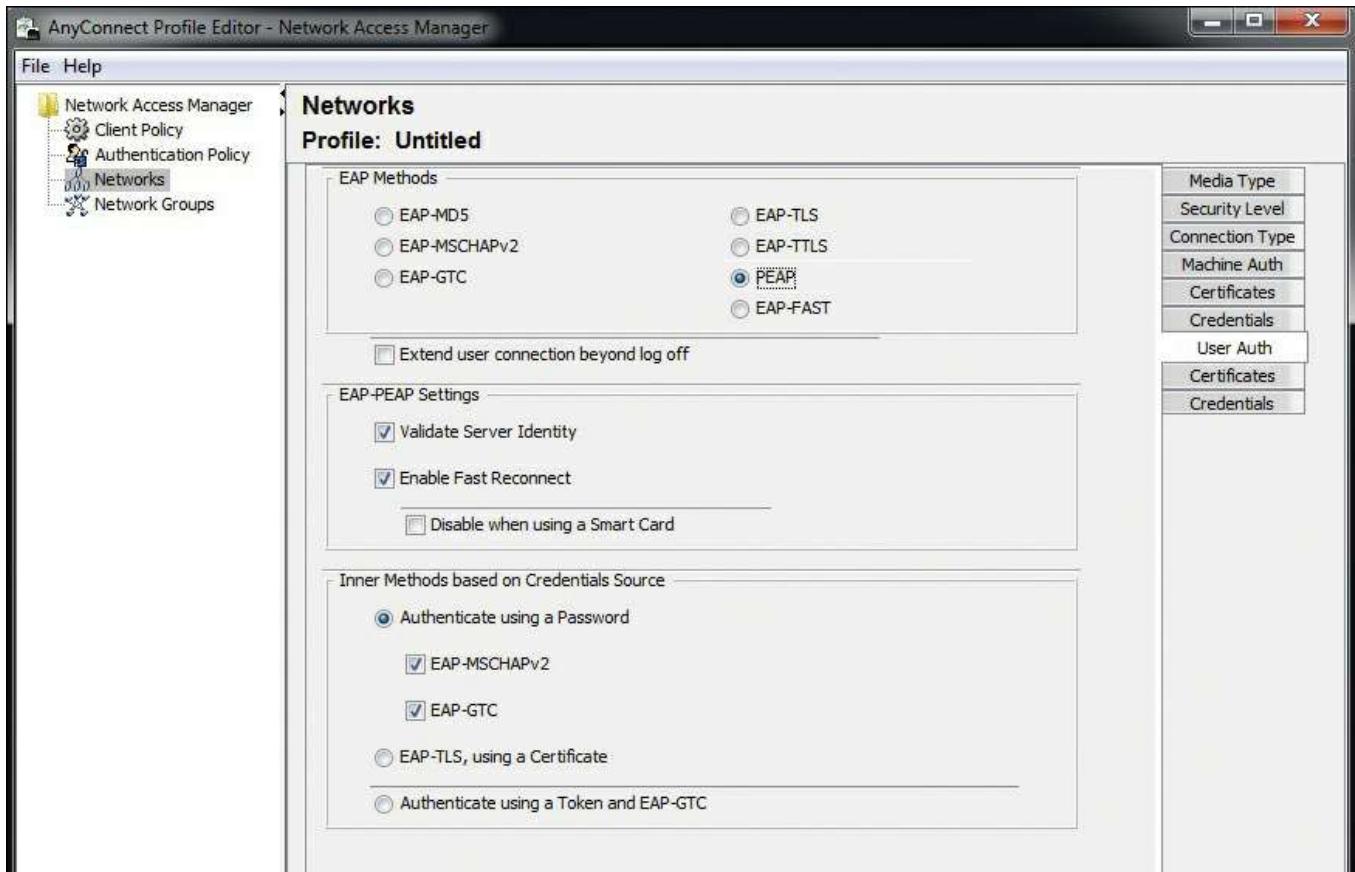
**Figure 16-19** AnyConnect NAM Profile Machine Auth Certificates

**Step 6.** Set the credentials that the machine should use. Normally, the defaults are fine.

Click **Next**.

**Step 7.** For User Auth, select **PEAP** or your choice of authentication methods.

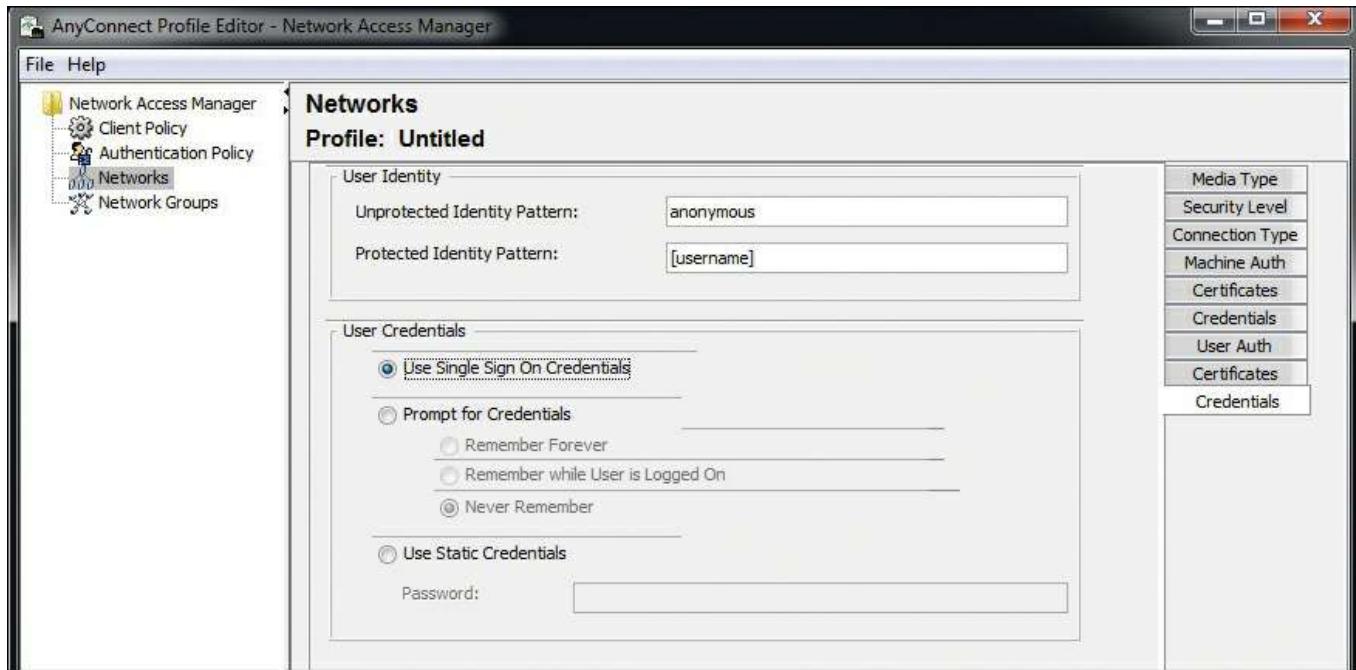
Normally, the defaults are fine. Click **Next**. See [Figure 16-20](#) for an example.



**Figure 16-20** AnyConnect NAM Profile User Auth

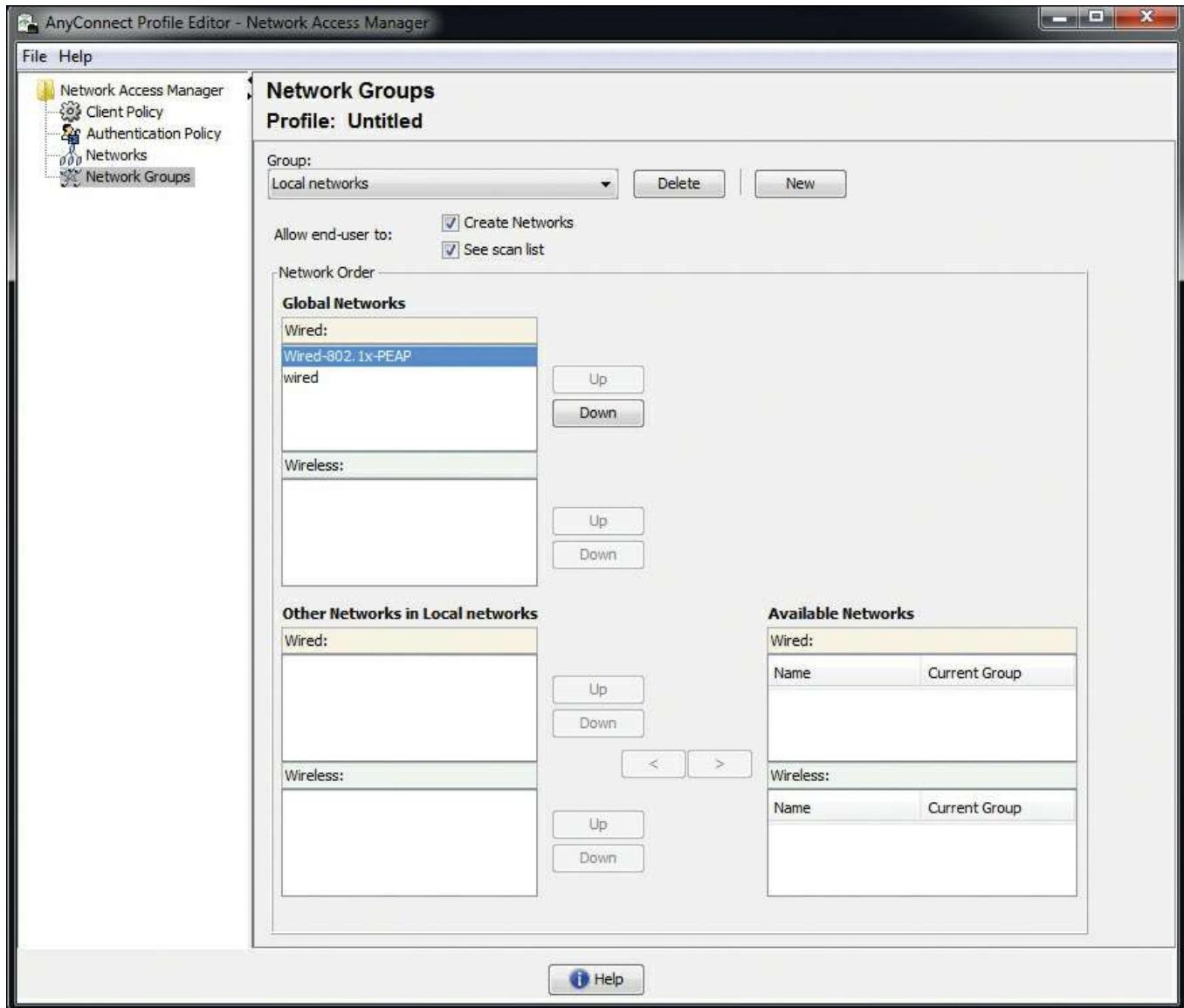
**Step 8.** The second Certificates page is for user certificate checking. Repeat what you did for machine certificates in Step 5. Click **Next**.

**Step 9.** On the final page, Credentials for user authorization, click **Use Single Sign On Credentials** (or select the settings appropriate for your deployment). Click **Done**. See [Figure 16-21](#).



**Figure 16-21** AnyConnect NAM Profile User Credentials

**Step 10.** On the AnyConnect Profile Editor screen, select **Network Groups** in the navigation pane on the left, as shown in [Figure 16-22](#). Under Global Networks: Wired, make sure that your policy is at the top of the list. If it isn't, select it and click the **Up** button.



**Figure 16-22** AnyConnect NAM Profile Network Groups

- Step 11.** Save the Profile file. On the top menu, click **File** and then **Save As**.
- Step 12.** You must save the configuration with the filename **configuration.xml** in the  
  `\\ProgramData\\Application Data\\Cisco\\Cisco AnyConnect Secure Mobility  
  Client\\Network Access Manager\\newConfigFiles` directory.
- Step 13.** To apply this new configuration, right-click the AnyConnect icon in the system  
  tray and choose **Network Repair**. This forces the Cisco AnyConnect NAM to  
  restart its services. A service restart causes NAM to search the newConfigFiles  
  directory for a configuration.xml file.
- Step 14.** You're finished!

## Summary

This chapter discussed 802.1X supplicants, with a particular focus on wired 802.1X

suplicant configuration. It covered the setup of Windows 7, Mac OS X, and Cisco AnyConnect supplicants. It also discussed the use of Microsoft Active Directory GPO as a supplicant configuration tool.

# Chapter 17 BYOD: Self-Service Onboarding and Registration

This chapter covers the following topics:

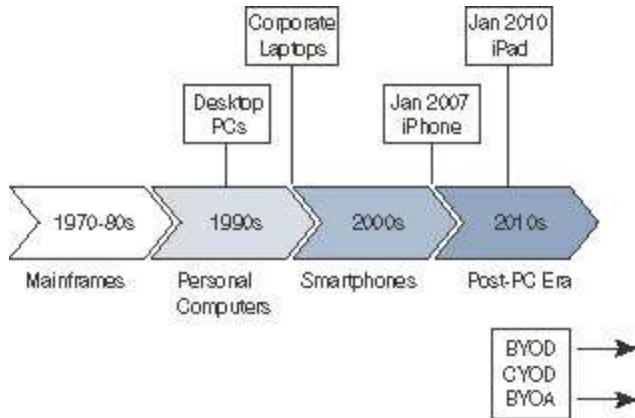
- BYOD challenges
- Onboarding process
- The opposite of BYOD: identify corporate systems

Back in January 2007, Steve Jobs introduced the iPhone and suggested that Apple was shooting for 1% of the mobile device market. The device had a revolutionary multi-touch screen interface, boasted a “real” browser instead of the cut-down versions on mobile devices to that point, and arguably “changed the game” for the experience that users expected from their mobile devices from that point on. In January 2010, the iPad was released. In June 2010, I was at Cisco Live in Las Vegas presenting a session on network access control (NAC).

In that session, I asked the audience if their company would allow users to bring in iPhones and iPad-type devices and connect to the corporate network for purposes of doing work from those devices. The few hundred people in my sample size responded with about 90% “no-way” responses and only 10% affirmative responses.

At that same conference, Cisco announced the Cius, which was designed to be a “corporate tablet,” a device to provide that wonderful user experience along with the security and guarantees that IT departments required. Fast forward 18 months, and Cisco announced the end-of-sale of the Cius, due to lack of adoption. In June 2012, when asked the same question about allowing personal devices, the result was 90% affirmative and only 10% said their organizations would not allow personal devices. What a difference two years makes! Bring Your Own Device (BYOD) has become an absolute reality. In today’s business world, it is no longer a question of if a company will allow the use of these devices, but a question of what level of support the end users will get with those devices.

As shown in [Figure 17-1](#), we are moving into an era of BYOD, Choose Your Own Device (CYOD), and even a Bring Your Own App (BYOA) type of model. Employees are demanding the use of the devices that make them most productive, with native applications running on those platforms that provide the user experience they have become accustomed to. This introduces a new paradigm for security, especially the identification of the user, the device, the location of the user, and much more.

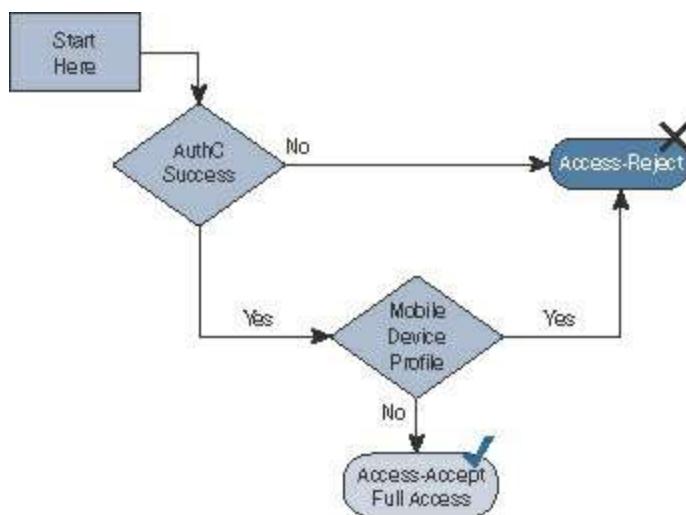


**Figure 17-1** BYOD Timeline

## BYOD Challenges

Because user identity is typically based on a single identity credential, IT does not possess the ability to create and enforce a rigorous secure access policy. Although the user might be authorized, the device, location, time, and access media can pose a company policy violation or even regulatory compliance violation that cannot be adequately detected or enforced.

This chapter focuses on the technical challenges of providing a secure BYOD access model. One of the most common challenges is referred to as onboarding. A user buys a new tablet or device and decides to connect it to the corporate Wi-Fi network and be productive on that consumer device. It has the challenge of identifying the device as a non-corporate device and providing a limited set of access to the device. This was originally what many companies used Cisco ISE to do. [Figure 17-2](#) illustrates the flow of these original policies.

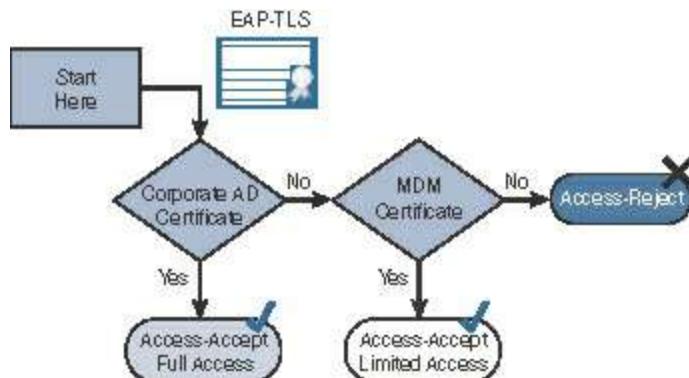


**Figure 17-2** Old-Style Policy

Then, mobile device management (MDM) solutions came into play. They were able to manage these mobile platforms to some extent. MDM policies ensured that devices had

security enabled, such as encryption, remote wipe capabilities, screen lock (pin lock), and so forth. The MDM could provision certificates down to the device and supplicant profiles to preconfigure the device to have network access. Then, ISE would provide the correct level of access for the devices based on the certificate the device had.

[Figure 17-3](#) illustrates a policy that uses certificates to differentiate access.



**Figure 17-3** Using Certificates to Differentiate Access

MDM systems typically cost money per device, and many companies were only looking for a good way to provision certificates and configure the device supplicant to use that certificate with 802.1X. The MDM cost was often prohibitive. The main objective was to provision the certificate and get the device on the network. Cisco customers were looking for a much easier and cheaper way to accomplish the onboarding aspect of network access.

## Onboarding Process

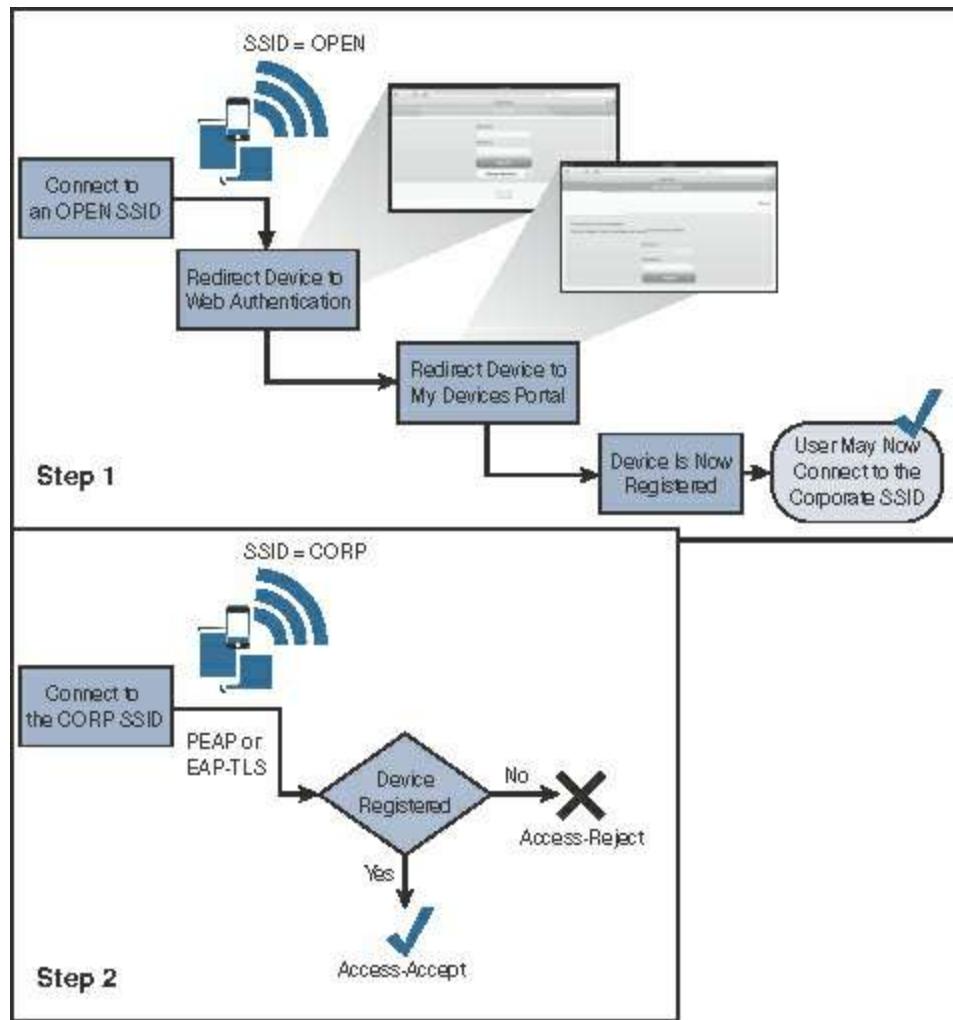
This chapter focuses on two types of onboarding. The first is what Cisco calls BYOD onboarding, which includes registering the device with ISE, provisioning the certificate to the device, and configuring the device's supplicant. BYOD onboarding uses the native supplicant within the operating system. It does not install a new supplicant. The second type is MDM onboarding, which is the process of registering the device with the MDM, installing the MDM client software, and enforcing the security policy on that device. The key to successful onboarding within a company is to make it self-service and not require involvement of IT.

## BYOD Onboarding

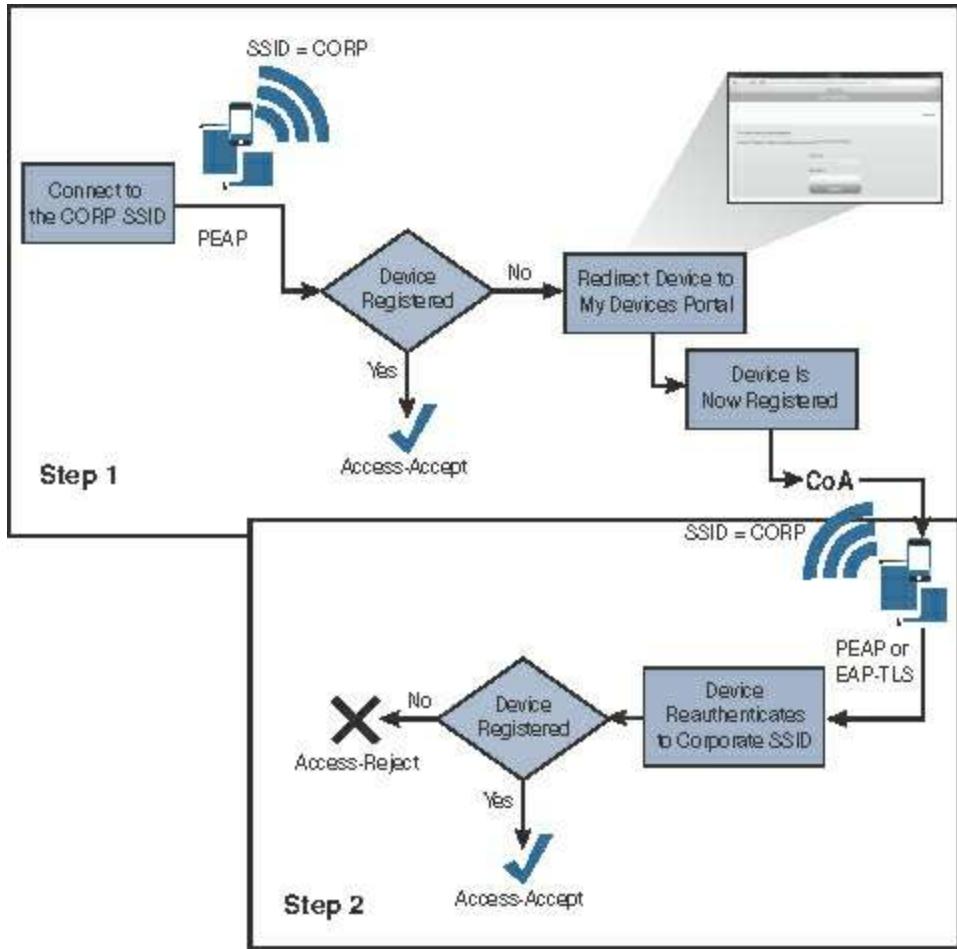
ISE provides the My Devices Portal, which allows users to register devices and manage those devices that have been registered. A device may simply be registered, which may provide one level of authorization, such as Internet-only access. Or the device may go through the full-blown onboarding and provisioning process where the supplicant configuration is installed into the device along with the optional certificate used for EAP-TLS connectivity.

Regardless of your choice to use device registration only or to use the full onboarding process, you can choose a single-SSID approach or dual-SSID approach to the onboarding, plus wired access (of course).

[Figure 17-4](#) depicts the dual-SSID approach, while [Figure 17-5](#) depicts the single-SSID approach. A quick comparison of the approaches follows.



**Figure 17-4** Dual-SSID Flow



**Figure 17-5 Single-SSID Flow**

## Dual SSID

The dual-SSID model of onboarding operates as follows (see [Figure 17-4](#)):

- Employee does not need to configure the supplicant on the device.
- Employee authenticates to a web form.
- Employee connects to the open SSID before the provisioning process, and the employee must connect to the corporate SSID after the process.

## Single SSID

The single-SSID model of onboarding operates as follows (see [Figure 17-5](#)):

- Employee must configure the supplicant on the device to connect to the corporate SSID.
- The authentication used to connect to the corporate SSID is used for single sign-on to the onboarding and provisioning process.
- A Change of Authorization (CoA) is used to provide full access after the

provisioning process without requiring the employee to reconnect to the network.

## Configuring NADs for Onboarding

Dual-SSID onboarding uses an open WLAN configured for NAC RADIUS, CoA, and MAC filtering (wireless MAC Authentication Bypass [MAB]). You likely created this network already based on [Chapter 14, “Guest Lifecycle Management,”](#) but this section briefly reviews the WLC settings.

### Review of the WLC Configuration

This section briefly reviews the configuration for the Cisco Wireless LAN Controller (WLC).

The General tab of the WLAN should provide an SSID and profile name, as shown in [Figure 17-6](#).

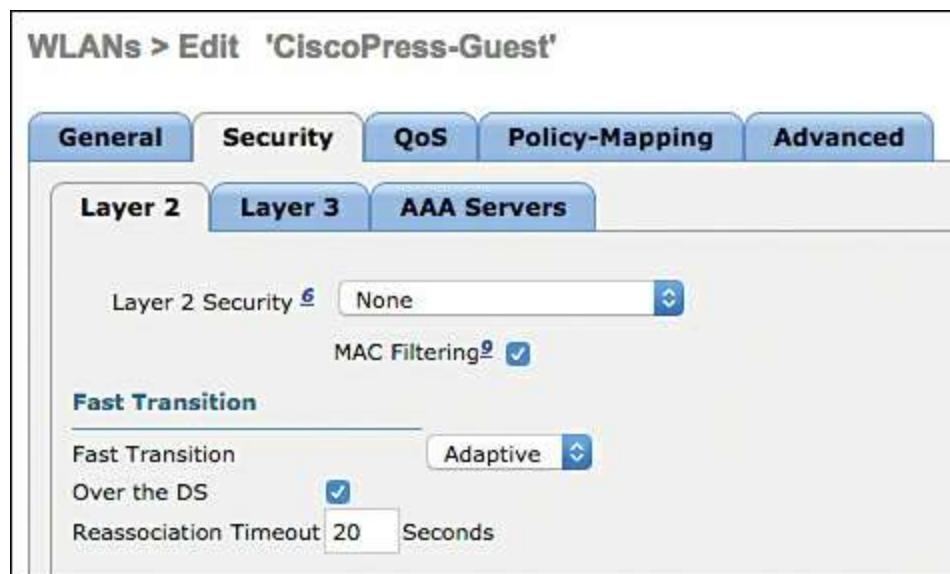
WLANS > Edit 'CiscoPress-Guest'

General		Security	QoS	Policy-Mapping	Advanced
Profile Name	CiscoPress-Guest				
Type	WLAN				
SSID	CiscoPress-Guest				
Status	<input type="checkbox"/> Enabled				
Security Policies	[WPA2][Auth(802.1X)] <small>(Modifications done under security tab will appear after</small>				
Radio Policy	All				
Interface/Interface Group(G)	guest				
Multicast Vlan Feature	<input type="checkbox"/> Enabled				
Broadcast SSID	<input checked="" type="checkbox"/> Enabled				
NAS-ID	none				

**Figure 17-6** Open WLAN General Tab Configuration for CiscoPress-Guest

Under **Security > Layer 2**, the Layer 2 Security field should be set to **None** and the MAC Filtering check box should be checked, as displayed in [Figure 17-7](#).

**Note** Beginning with WLC version 8.4, the controller supports using WPA2-PSK on a guest network, but that's not what we are doing in this example.



**Figure 17-7** Layer 2 Security Subtab Configuration for CiscoPress-Guest

Under **Security > Layer 3**, the Layer 3 Security field should be set to **None**, as shown in [Figure 17-8](#).



**Figure 17-8** Layer 3 Security Subtab Configuration for CiscoPress-Guest

Under **Security > AAA Servers**, the ISE Policy Service Node(s) should be selected for authentication and accounting servers, as shown in [Figure 17-9](#).

**WLANS > Edit 'CiscoPress-Guest'**

**General Security QoS Policy-Mapping Advanced**

**Layer 2 Layer 3 AAA Servers**

Select AAA servers below to override use of default servers on this WLAN

**RADIUS Servers**

RADIUS Server Overwrite interface  Enabled

Authentication Servers		Accounting Servers	
<input checked="" type="checkbox"/> Enabled		<input checked="" type="checkbox"/> Enabled	
Server 1	IP:10.1.100.231, Port:1812	IP:10.1.100.231, Port:1813	
Server 2	None	None	
Server 3	None	None	
Server 4	None	None	
Server 5	None	None	
Server 6	None	None	

**RADIUS Server Accounting**

Interim Update  Interim Interval 0 Seconds

**LDAP Servers**

**Figure 17-9** AAA Servers Security Subtab Configuration for CiscoPress-Guest

On the Advanced tab, the **Enabled** check box for Allow AAA Override should be checked, and the NAC State field should be set to **ISE NAC**, as shown in [Figure 17-10](#).

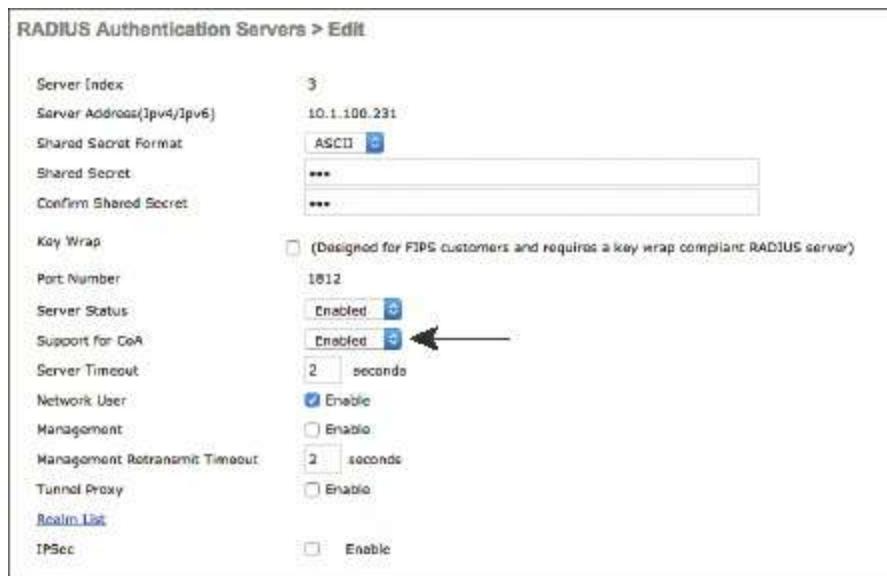
**WLANS > Edit 'CiscoPress-Guest'**

**General Security QoS Policy-Mapping Advanced**

Allow AAA Override <input checked="" type="checkbox"/>	DHCP
Coverage Hole Detection <input checked="" type="checkbox"/>	DHCP Server <input type="checkbox"/> Override
Enable Session Timeout <input checked="" type="checkbox"/>	DHCP Addr. Assignment <input type="checkbox"/> Required
1800 Session Timeout (secs)	DEAP
Aironet IE <input checked="" type="checkbox"/>	Split Tunnel <input type="checkbox"/> Enabled
Diagnostic Channel <input checked="" type="checkbox"/>	Management Frame Protection (MFP)
Override Interface ACL: IPv4: None IPv6: None	NFP Client Protection # <input type="checkbox"/> Optional
Layer2_Acl: None	DTIM Period (in beacon intervals)
URL ACL: None	802.11a/n (1 - 255) <input type="checkbox"/> 1
P2P Blocking Action: Disabled	802.11b/g/n (1 - 255) <input type="checkbox"/> 1
Client Exclusion: <input checked="" type="checkbox"/> Enabled 60 Timeout Value (secs)	NAC
Maximum Allowed Clients: 0	NAC State <input type="checkbox"/> ISE NAC
Static IP Tunneling <input type="checkbox"/> Enabled	Load Balancing and Band Select
Wi-Fi Direct Clients Policy: Disabled	
Maximum Allowed Clients Per AP Radio: 200	

**Figure 17-10** Advanced Tab Configuration for CiscoPress-Guest

Navigate to **Security > RADIUS > Authentication** and double-check that the RADIUS server definition is configured to allow CoA; the Support for CoA drop-down list box should be set to **Enabled**, as shown in [Figure 17-11](#).



**Figure 17-11** Enabling Support for CoA on RADIUS Authentication Servers

## Required ACLs

You should have an ACL on the switches and the wireless controllers already named **ACL\_WEBAUTH\_REDIRECT** that permits DHCP, DNS, and traffic to ISE and denies most other traffic. This configuration was discussed and added in [Chapter 14](#), and it also matches the preconfigured authorization policies within ISE 2.0 and newer.

When onboarding with iOS, Windows, and macOS, the endpoint need only communicate with ISE. Apple iOS uses its native Over the Air (OTA) provisioning process.

Windows and macOS both use a native application that is downloaded from ISE through the device's browser. Because the communication is limited to just ISE, the **ACL\_WEBAUTH\_REDIRECT** ACL is sufficient to be repurposed for the onboarding ACL as well.

However, Android is a different story altogether. Android devices inherently do not trust apps being installed from an app store other than those trusted during the factory install, which includes Google Play. Therefore, ISE would not be allowed to host an app for Android devices by default. To keep the process simple for the end user, you have to either open the ACL to allow access to a range of addresses for Google Play or use the DNS ACL capabilities of the WLC.

The Google Play app store (<https://play.google.com>) is a cloud service, and the addresses it uses may change regularly. This presents a challenge to permit access to those address ranges. The current solution is to permit a series of blocks of addresses that are known to be used by Google Play, as shown here:

- 74.125.0.0/16
- 173.194.0.0/16
- 173.227.0.0/16
- 206.111.0.0/16

This ACL is used for both single- and dual-SSID onboarding. To read a Google support thread where Google discusses how to identify the current list of Google IP addresses, go to <http://support.google.com/a/bin/answer.py?hl=en&answer=60764>.

When adding the DNS names to the ACL, keep in mind there may be different URLs for different countries or regions. Additionally, there may be images or other ads that are displayed in Google Play that come from other places.

In our experience, the following two URLs will work in the United States and generally provide a good end-user experience:

- android.clients.google.com
- google.com

The DNS ACLs on the WLC are also known as URL Lists. When you add a URL, an implicit wildcard is added in front of whatever you enter. So, if you enter google.com, it is actually equal to \*.google.com. Keep in mind that wildcards in FQDNs are specific to the level. So, for example, \*.google.com would not include android.clients.google.com, which is why it is listed separately.

DNS ACLs work on the access points themselves, where they snoop DNS traffic, record the DNS results that match the URL list, and send those results to the controller to be appended as implicit permit entries in the ACL.

### Add the URLs to ACL\_WEBAUTH\_REDIRECT

To add the URLs to ACL\_WEBAUTH\_REDIRECT, from the WLC GUI, navigate to **Security > Access Control Lists**, hover your mouse over the blue and white arrow icon next to ACL\_WEBAUTH\_REDIRECT, and then click **Add-Remove URL**, as shown in [Figure 17-12](#).



**Figure 17-12** Add-Remove URL Pop-Up Option

This takes you to the URL List, as shown in [Figure 17-13](#), where you can add up to 20 URLs per ACL. To configure the list shown in [Figure 17-13](#), if you are in the United

States, type **google.com** and click **Add**, and then type **android.clients.google.com** and click **Add**. If you are based outside the United States, it might benefit you to use a wildcard after google in your entries: **google.\*** and **android.clients.google.\***.

The screenshot shows a web-based configuration interface for an URL list. The title bar reads "ACL > ACL-WEBAUTH-REDIRECT > URL List". Below the title, there is a form with a "URL String Name" input field and an "Add" button. A table lists two URLs: "google.com" and "android.clients.google.com".

URL Name
google.com
android.clients.google.com

**Figure 17-13 URL List**

As with anything as dynamic as cloud services, you might need to alter these URLs for continued success. New URLs may become necessary and old URLs may become obsolete.

## ISE Configuration for Onboarding

With the NADs prepared for the onboarding process, it's time to build the logic within the ISE authorization policy for both the dual- and single-SSID onboarding models.

The easier model to set up and understand first is the single-SSID model. It assumes that if a user or endpoint has been successfully admitted to the network, the user or endpoint must have authenticated with a certificate via EAP-TLS. If an authentication occurs with only a username and password (say, MsCHAPv2 inner method), you know the device must still need to be onboarded.

For example, suppose an employee shows up to work with his new mobile device. He decides to try and connect to the corporate Wi-Fi network and it prompts him for a username and password. The employee enters his Active Directory credentials (as would be expected), and when he opens the browser on the mobile device, he is redirected to the My Devices Portal, where he can begin the onboarding process. This process is simple, quick, and intuitive to most end users nowadays.

Beginning with ISE version 2.0, there is a preconfigured “smart-default” client provisioning policy. Aside from a single, small change, that default policy and its settings will be used in the following examples.

## End-User Experience

To fully understand the configuration of ISE, it is best that you experience the end-user experience for both single- and dual-SSID onboarding. That will aid you in your

understanding of each policy that is required, and each choice you will have to make. To demonstrate multiple user experiences, the following examples use Apple iOS for the first example, which demonstrates single-SSID onboarding, and Android for the second example, which demonstrates dual-SSID onboarding. However, each onboarding method could be used with any of the supported clients (iOS, Android, Mac OS X, and Windows).

For the examples, we will be leveraging a default, out-of-the-box policy set. The biggest difference is that we enabled the relevant rules for BYOD, as shown in [Figure 17-14](#). Additionally, we changed the SSID in the default profile to be CiscoPress instead of the default one, which is named ISE.

Default Policy Set			
Authentication Policy			
<input checked="" type="checkbox"/>	MAB	: If <code>Wired_MAB OR Wireless_MAB</code>	Allow Protocols : Default Network Access
	<input checked="" type="checkbox"/> Default	:use Internal Endpoints	
<input checked="" type="checkbox"/>	Dot1X	: If <code>Wired_802.1X OR Wireless_802.1X</code>	Allow Protocols : Default Network Access
	<input checked="" type="checkbox"/> Default	:use All_User_ID_Stores	
<input checked="" type="checkbox"/>	Default Rule (If no match)	: Allow Protocols : Default Network Access	and use : All_User_ID_Stores
Authorization Policy			
Exceptions (0)			
Standard			
Status	Rule Name	Conditions (Identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Wireless Black List Default	If <code>Blacklist AND Wireless_Access</code>	then Blackhole_Wireless_Access
<input checked="" type="checkbox"/>	Profiled Cisco IP Phones	If <code>Cisco-IP-Phone</code>	then Cisco_IP_Phones
<input checked="" type="checkbox"/>	Profiled Non Cisco IP Phones	If <code>Non_Cisco_Profiled_Phones</code>	then Non_Cisco_IP_Phones
<input checked="" type="checkbox"/>	Compliant_Devices_Access	If <code>(Network_Access_Authentication_Passed AND Compliant_Devices )</code>	then PermitAccess
<input checked="" type="checkbox"/>	Employee_EAP-TLS	If <code>(Wireless_802.1X AND BYOD_is_Registered AND EAP-TLS AND MAC_in_SAN )</code>	then PermitAccess AND BYOD
<input checked="" type="checkbox"/>	Employee_Onboarding	If <code>(Wireless_802.1X AND EAP-MSCHAPv2 )</code>	then NSP_Onboard AND BYOD
<input checked="" type="checkbox"/>	Wi-Fi_Guest_Access	If <code>(Guest_Flow AND Wireless_MAB )</code>	then PermitAccess AND Guests
<input checked="" type="checkbox"/>	Wi-Fi_Redirect_to_Guest_Login	If <code>Wireless_MAB</code>	then Cisco_WebAuth
<input checked="" type="checkbox"/>	Basic_Authenticated_Access	If <code>Network_Access_Authentication_Passed</code>	then PermitAccess
<input checked="" type="checkbox"/>	Default	If no matches, then	DenyAccess

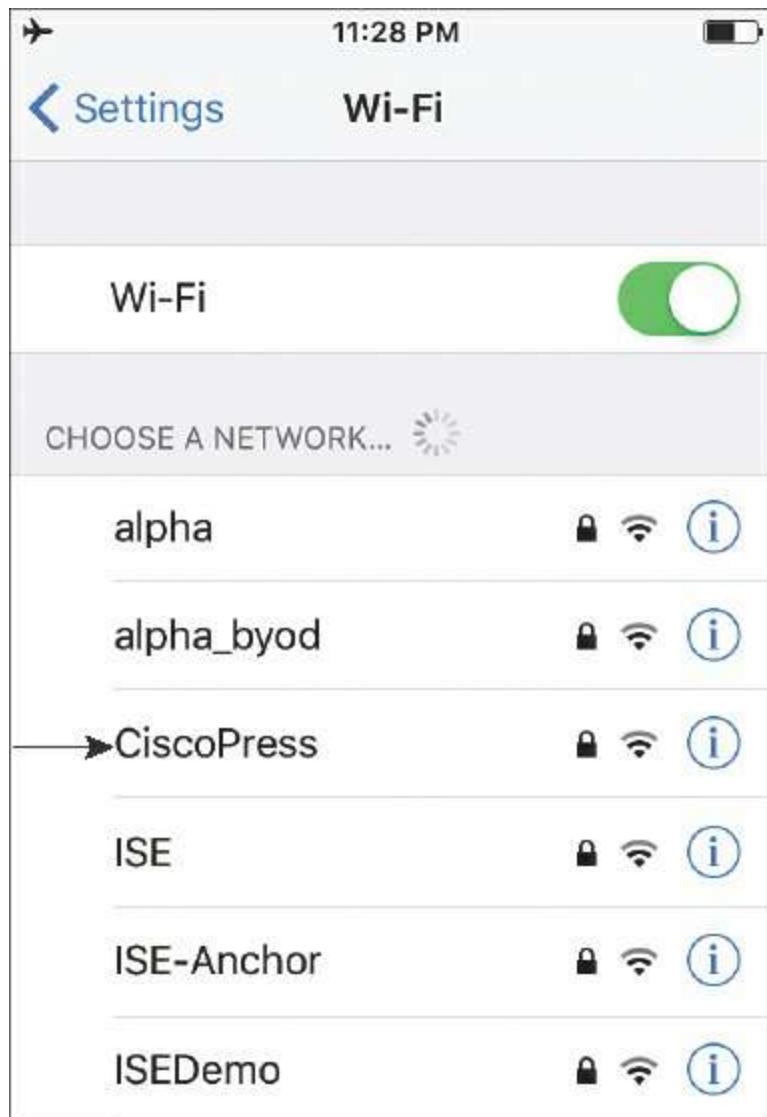
**Figure 17-14 Default Policy Set with Enabled BYOD Rules**

Beginning with ISE version 2.0, there are default policies commonly referred to as “smart defaults” to aid you in going from install to BYOD onboarding in 30 minutes or less. Don’t worry too much about understanding this policy set just yet; we will go through it together after you focus on the end-user experience.

### Single-SSID Onboarding with Apple iOS Example

The following steps are designed to follow the end-user experience with single-SSID onboarding using an Apple iOS device in a corporate setting:

**Step 1.** On your iOS device, choose **Settings > Wi-Fi**, enable Wi-Fi (as shown in [Figure 17-15](#)), and connect to the corporate Wi-Fi (CiscoPress in this example).



**Figure 17-15** Choosing a Wi-Fi Network on an iOS Device

**Step 2.** You are prompted to input a username and password. An employee would use

their Active Directory username and password, similar to what is shown in [Figure 17-16](#).



11:32 PM



Enter the password for "CiscoPress"

Cancel

Enter Password

Join

Username employee1

Password

••••••••|

1 2 3 4 5 6 7 8 9 0

- / : ; ( ) \$ &amp; @ "

#+=

.

,

?

!

'



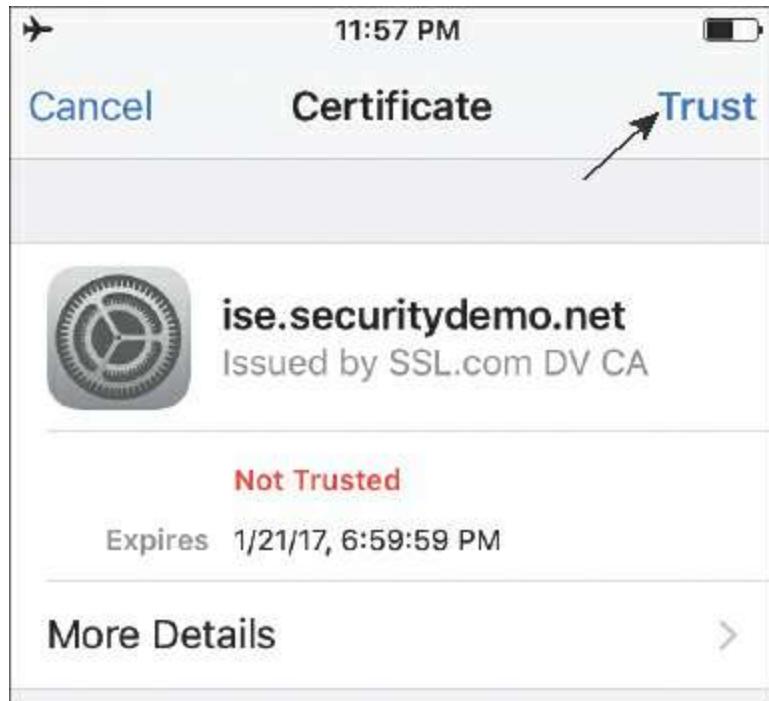
ABC

space

return

Figure 17-16 iOS: Enter Credentials

**Step 3.** Because you are manually joining a secured network instead of joining a network that was provisioned to your device by an MDM, you are prompted to accept (trust) ISE's EAP certificate, as shown in [Figure 17-17](#).



**Figure 17-17** iOS: Trust ISE Certificate

**Step 4.** After you are successfully connected to the corporate network, you see the Wi-Fi symbol and can view your IP address, as shown in [Figure 17-18](#). However, you do not see anything indicating that your access is actually limited.



**Figure 17-18** iOS: Connected to Corporate Wi-Fi

**Step 5.** Open a web browser, and you are redirected to the BYOD portal, where you are stepped through entering some information about the device and then beginning the OTA provisioning process. [Figure 17-19](#) shows the welcome screen for the BYOD portal.

10:29 PM

atw-ise231.securitydemo.net

**CISCO BYOD Portal**

1 2 3

## BYOD Welcome

Welcome to the BYOD portal.

Access to this network requires your device to be configured for enhanced security. Click **Start** to provide device information before components are installed on your device.

pronipiteda. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will be posted on Cisco System's website and will be effective as to existing users 30 days after posting.

**Start**

**Figure 17-19 iOS: BYOD Portal Welcome Screen**

**Step 6.** Tap **Start**.

**Step 7.** Step 2 within the BYOD portal is to provide a device name for the endpoint and, optionally, a description, as shown in [Figure 17-20](#). Type in the requested information and tap **Continue**.



10:32 PM



atw-ise231.securitydemo.net



## BYOD Portal

2

3

4

### Device Information

Enter the device name and optional description for this device so you can manage it using the My Devices Portal.

**Device name:** \*

ATW iPhone6

**Description:**

That wasn't good enough?

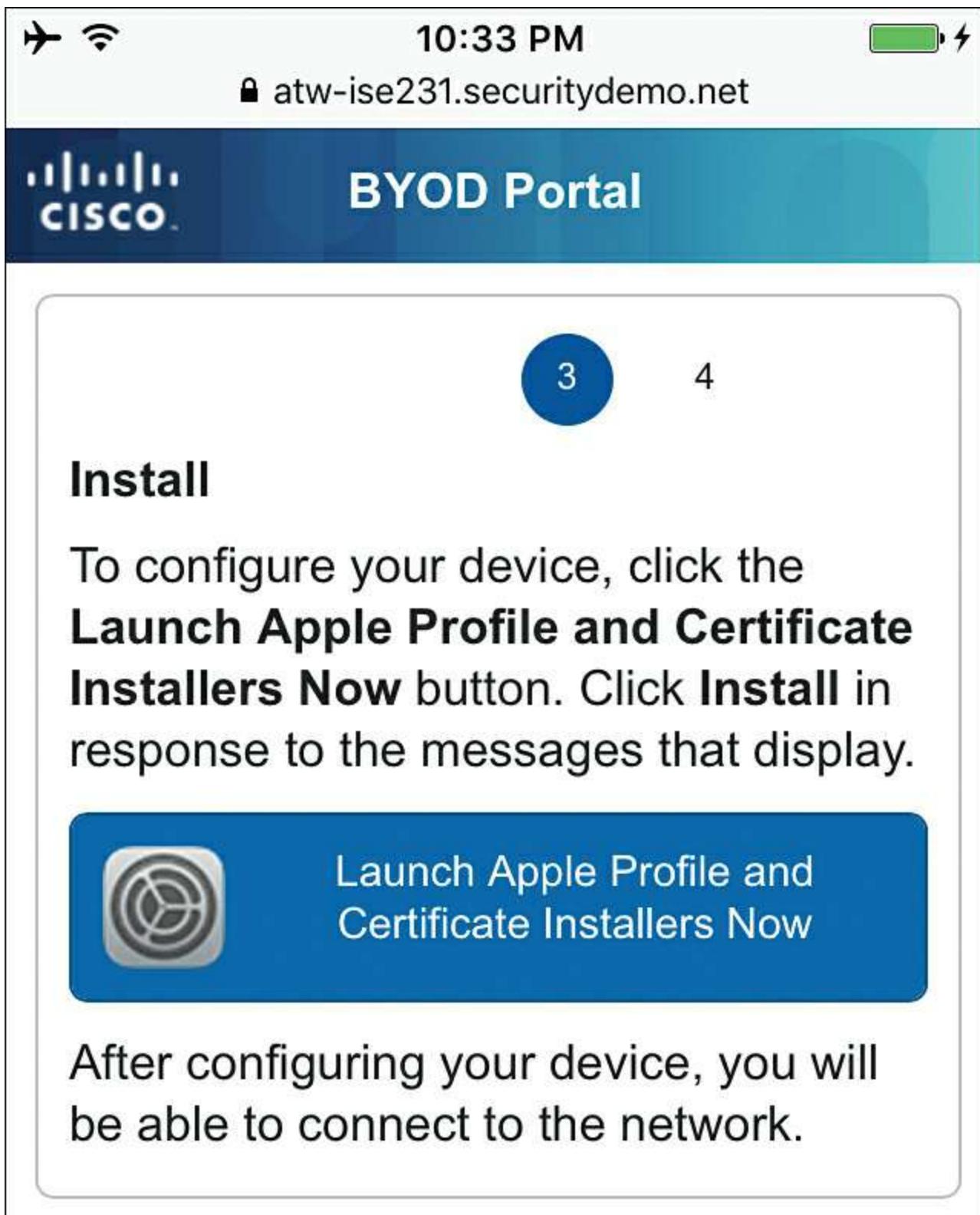
**Device ID:** D4:F4:6F:A9:55:0E

**Continue**



**Figure 17-20** iOS: BYOD Portal Device Information

**Step 8.** Tap the **Launch Apple Profile and Certificate Installers Now** button to launch the Apple OTA provisioning, as shown in [Figure 17-21](#).

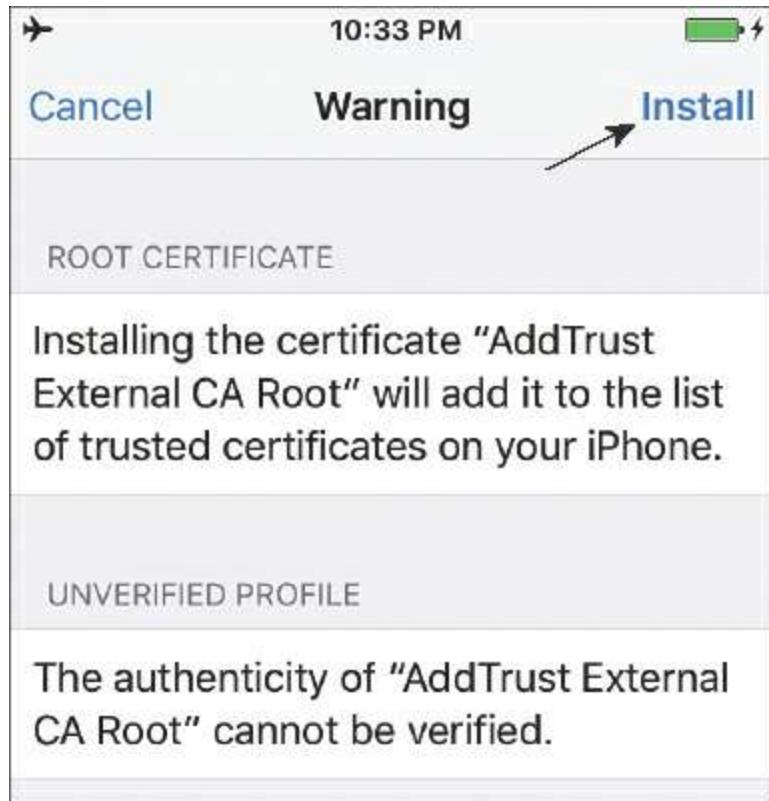


**Figure 17-21** iOS: BYOD Portal Install Screen

**Step 9.** For OTA to work correctly, the OTA profile must be signed by a trusted certificate authority (CA). This is often handled by an MDM; however, because this is a BYOD flow, you have to trust that CA manually. As part of the OTA process, ISE sends the public certificate of the CA that signed its admin certificate, as shown in [Figure 17-22](#). You can tap **More Details** to see more about the usage of the certificate that you are installing, as shown in [Figure 17-23](#). You are installing a profile that consists of a CA root certificate.

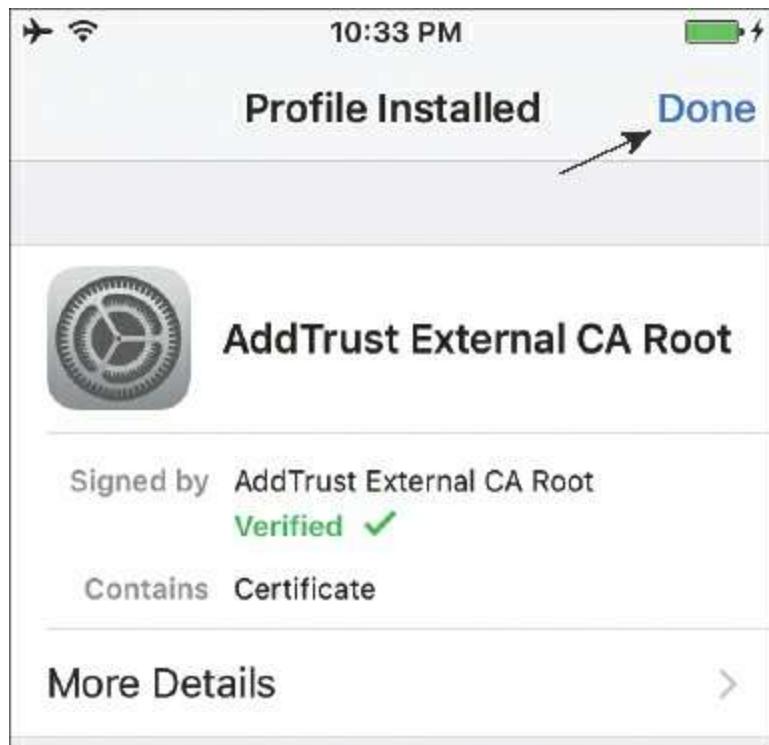


**Figure 17-22** iOS: Installing OTA Signing CA Certificate



**Figure 17-23** iOS: Viewing More Details About the CA Certificate

**Step 10.** Tap **Install**. The root CA certificate is now marked as verified, as shown in [Figure 17-24](#). Tap **Done**.



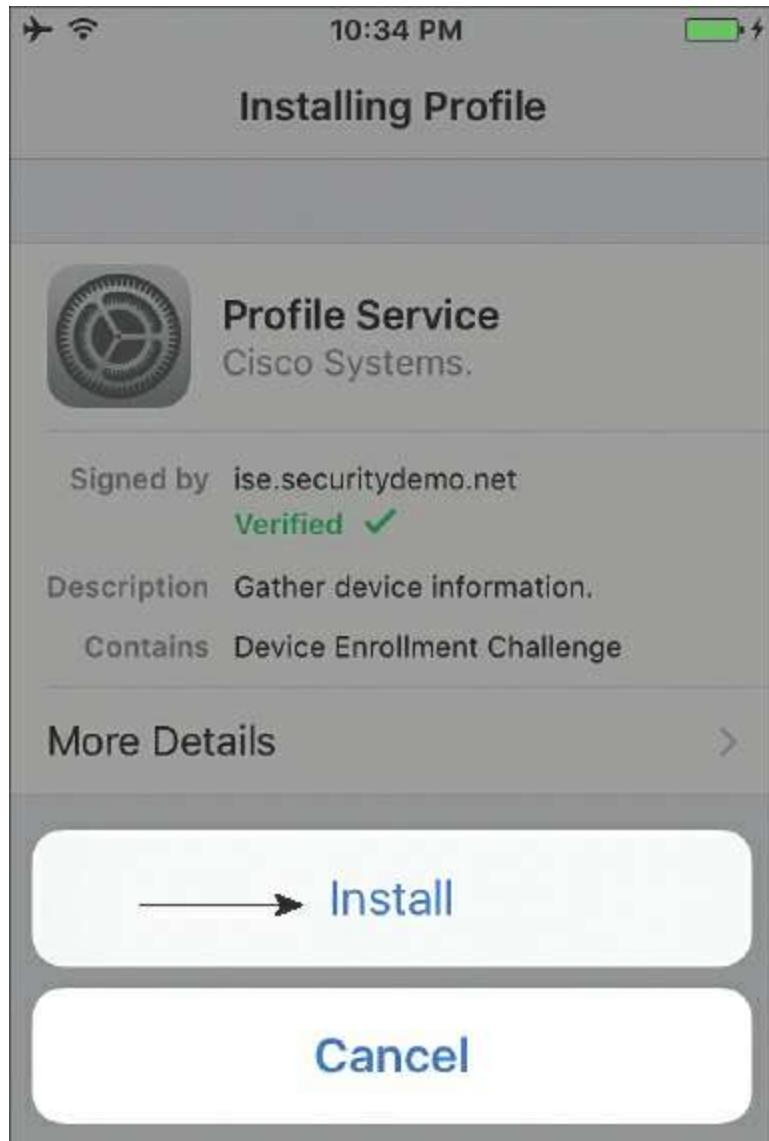
**Figure 17-24** iOS: OTA Signing CA Certificate Installed

**Step 11.** After you tap **Done**, the Install Profile screen changes a bit. It now shows that you are installing a Profile Service. It is signed by your ISE node's admin certificate, which is marked verified (it is trusted), as shown in [Figure 17-25](#). The signed profile is trusted because you trusted the root CA in Step 10. Tap **Install**.



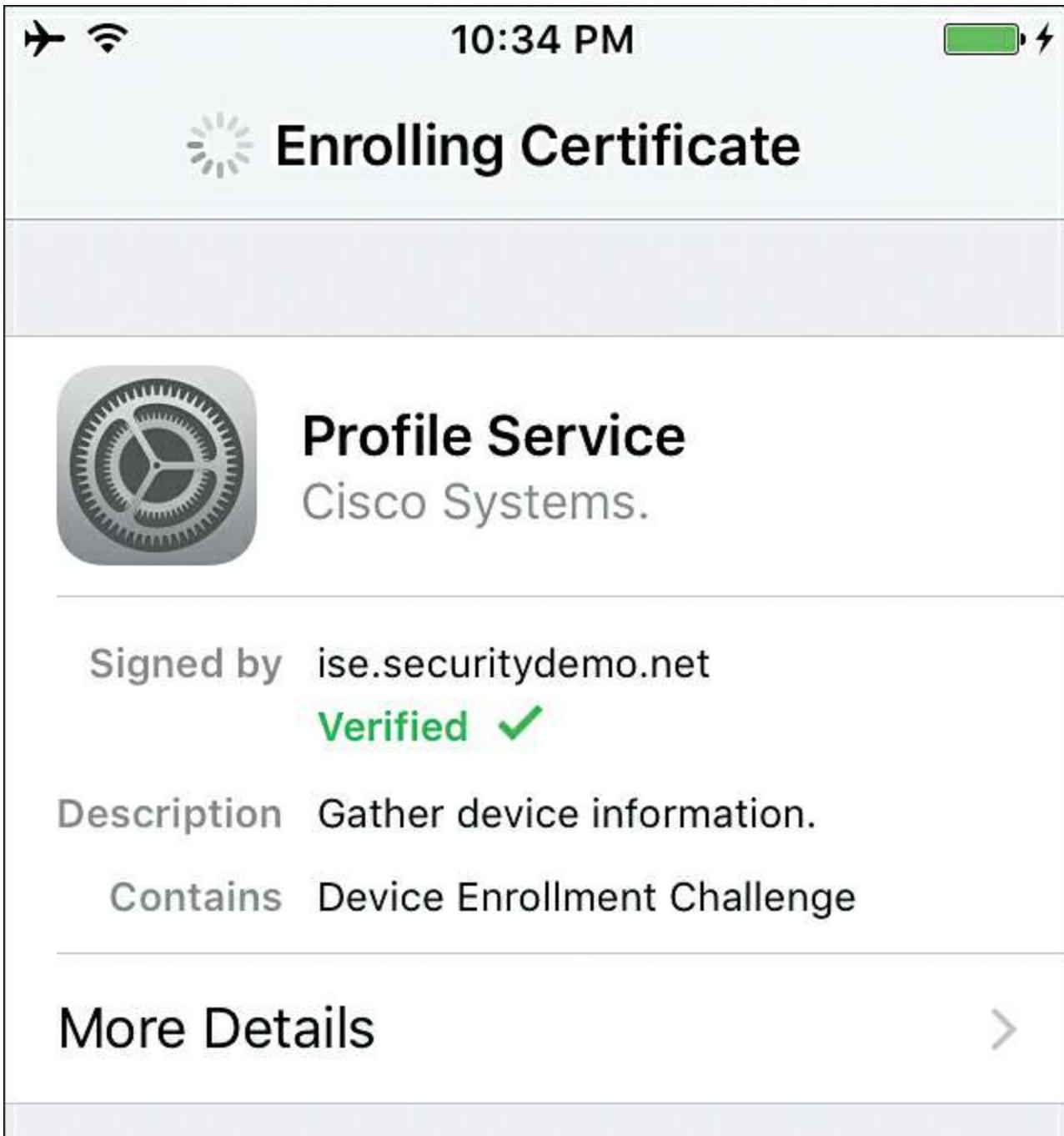
**Figure 17-25** iOS: Installing a Profile Service

**Step 12.** The screen changes to the Installing Profile screen, as shown in [Figure 17-26](#). Tap **Install**.

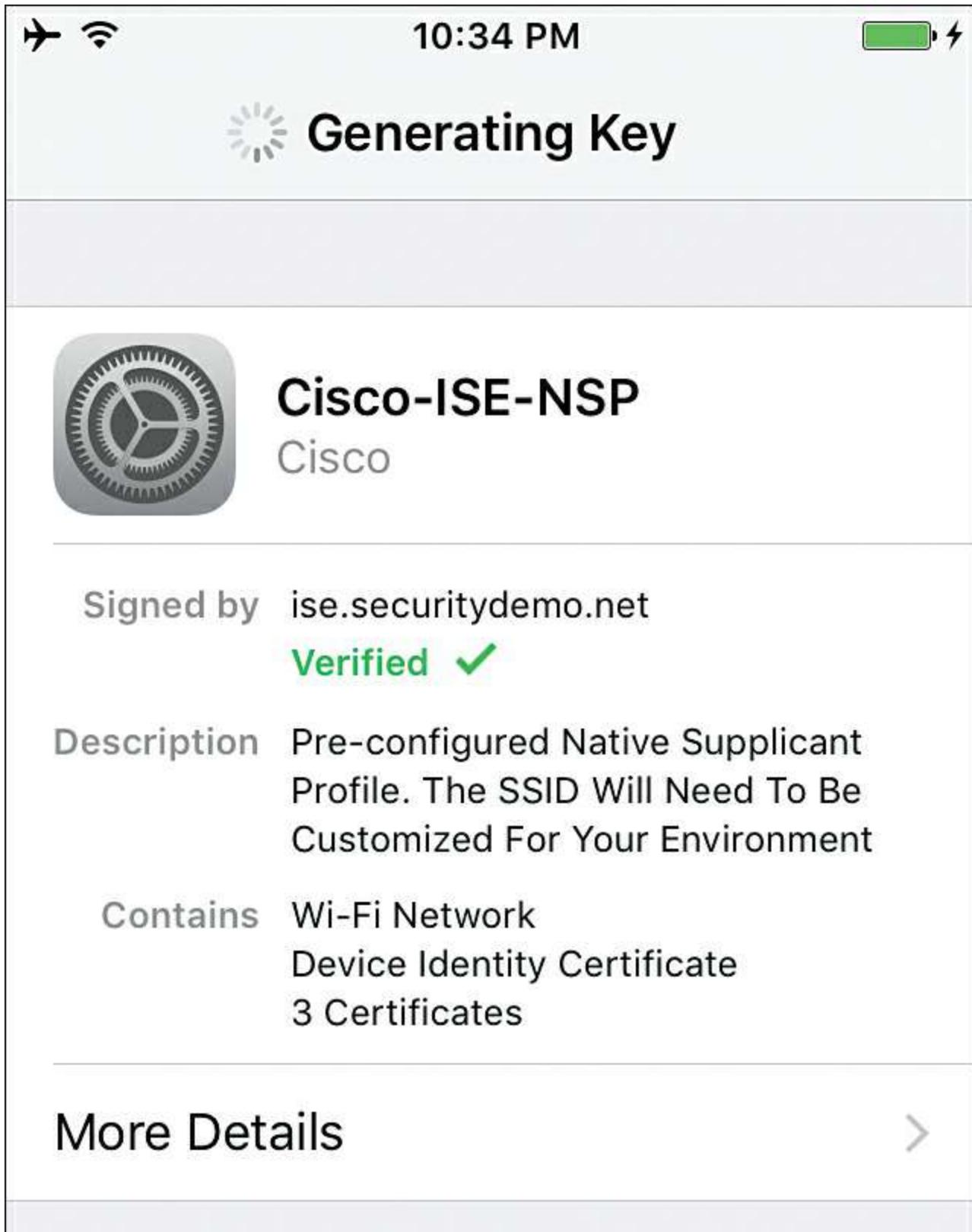


**Figure 17-26** iOS: Installing Profile

**Step 13.** The screen updates itself several times without requiring any user interaction. You are notified that the OTA service is enrolling certificates and generating keys (see [Figures 17-27](#) through [17-29](#)), and then finally shown the end state with the profile installed, as shown in [Figure 17-30](#).



**Figure 17-27** iOS: Enrolling Certificate for Device



**Figure 17-28** iOS: Generating Key

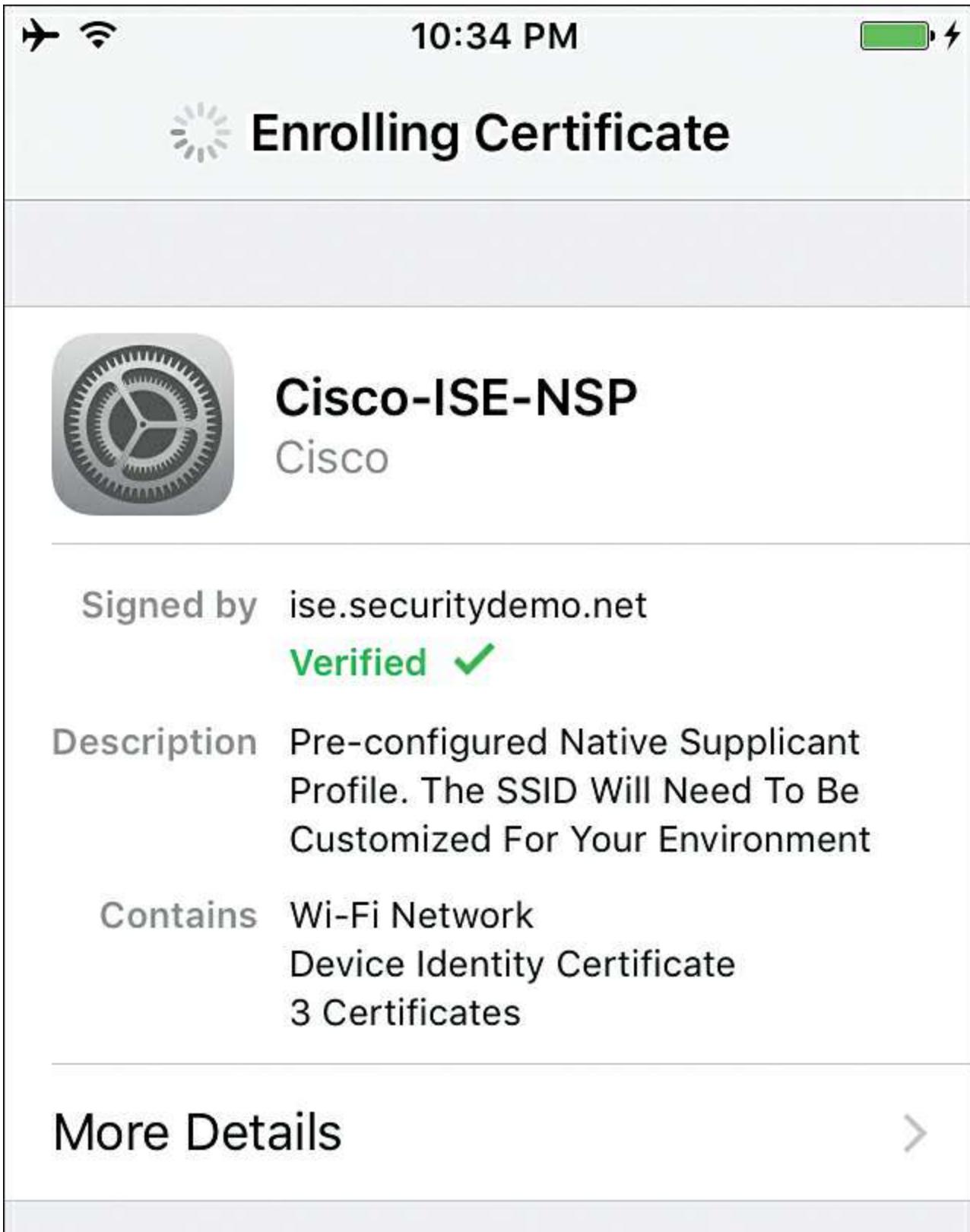
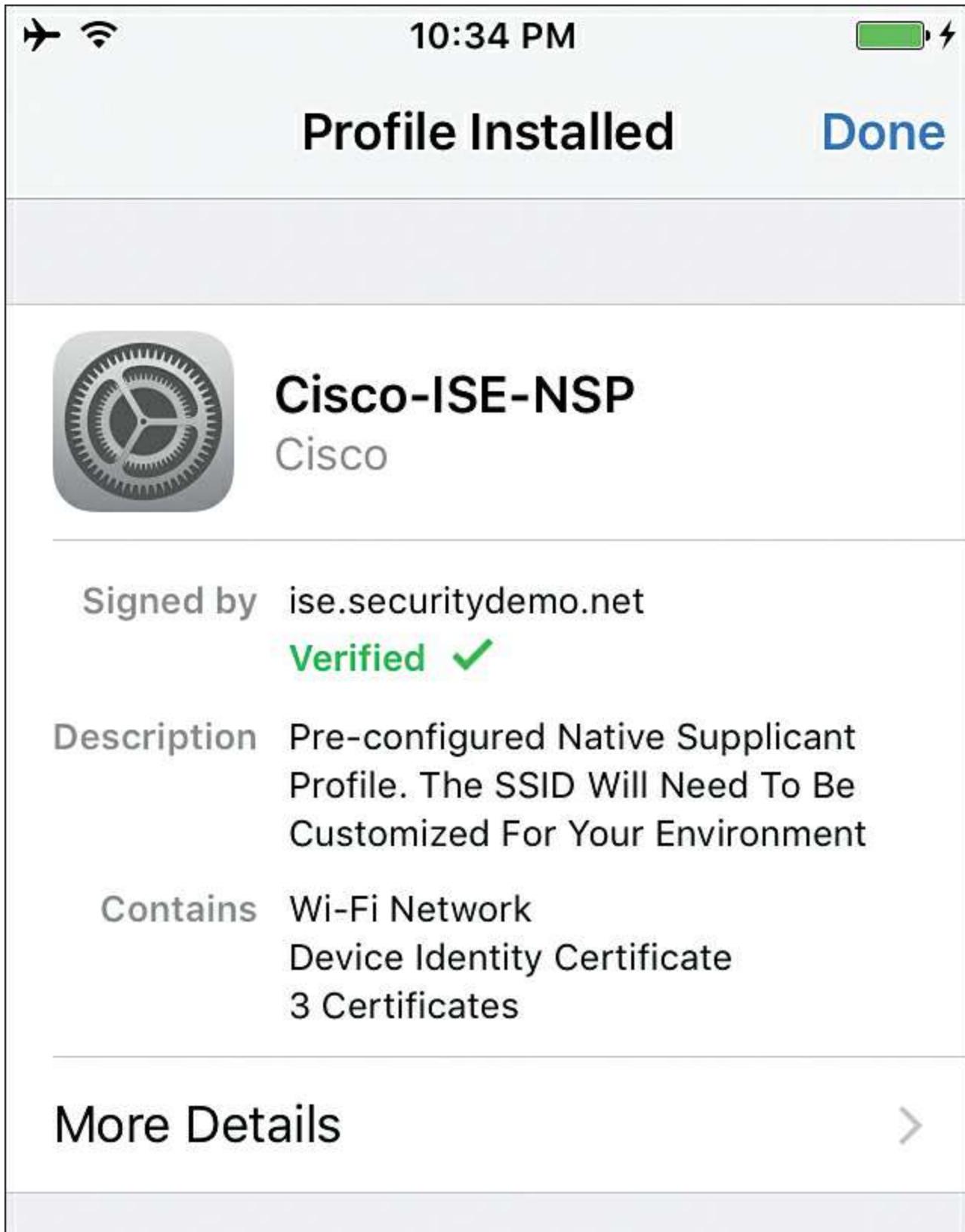
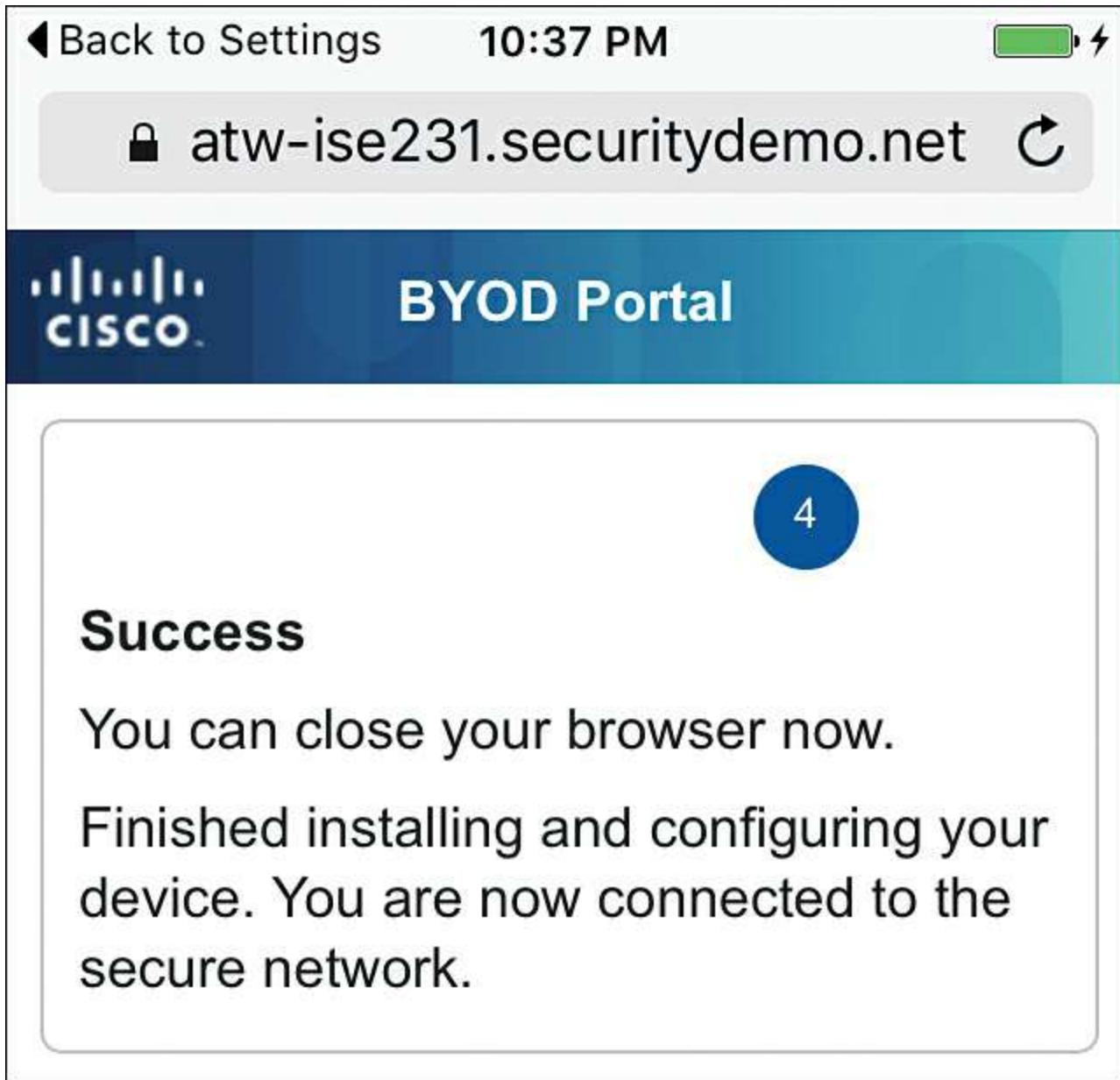


Figure 17-29 iOS: Enrolling Certificate for User



**Figure 17-30** iOS: Profile Installed

**Step 14.** When the profile is installed, tap **Done** and your web browser will refresh with the success message, as shown in [Figure 17-31](#). It takes only a few minutes for the entire process if the end user is paying attention to the prompts.



**Figure 17-31** iOS: Success

**Step 15.** You are now able to browse resources on the network. The IOS device authenticates using the certificate you just installed, and the device no longer remembers the username and password that were typed in when this device first joined the wireless SSID.

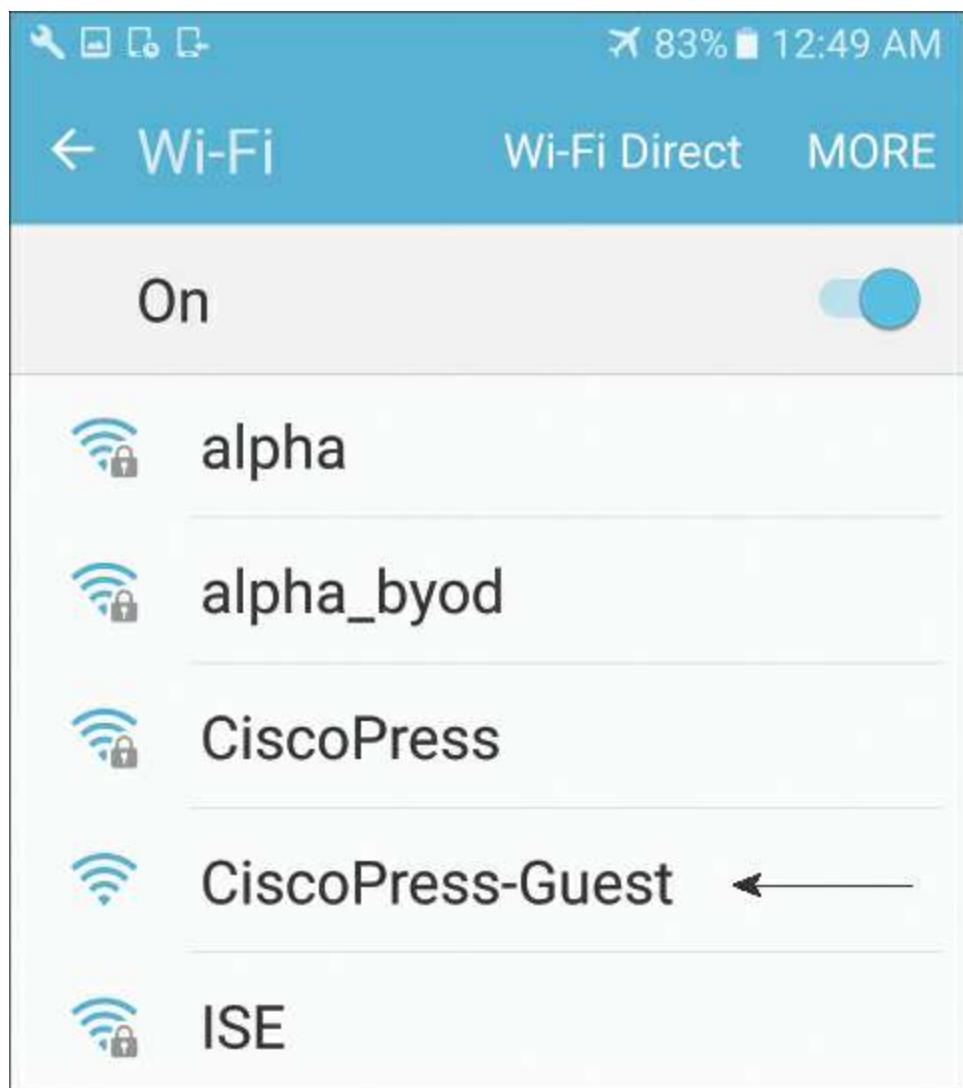
That concludes the onboarding process for iOS with a single SSID. Next, let's examine the user experience with dual SSID by using an Android example.

### Dual-SSID Onboarding with Android Example

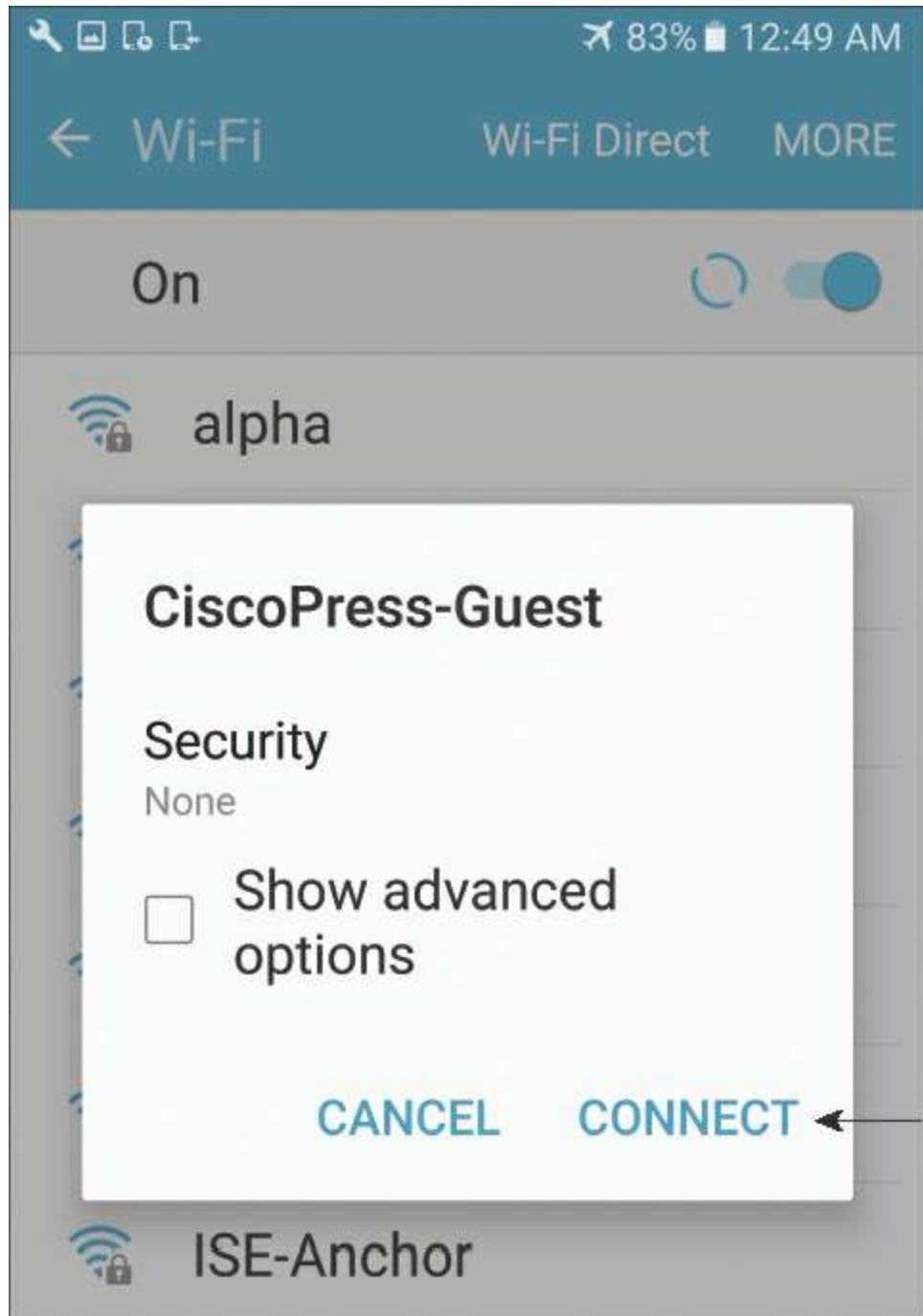
The user experience with dual SSIDs is a bit different from the single-SSID experience. In this type of onboarding, the user first joins an open SSID or a guest SSID and, after being logged in to the web authentication portal as an employee, then begins the

onboarding process. The following steps are designed to follow the end-user experience with dual-SSID onboarding using an Android-based device in a corporate setting:

**Step 1.** On your Android device, choose **Settings > Wi-Fi** and connect to the guest Wi-Fi. In our example, we are connecting to an open WLAN named CiscoPress-Guest, as shown in [Figure 17-32](#). Depending on your Android version, you may have to tap **Connect** after choosing the network, as shown in [Figure 17-33](#). This is an extra precaution since you are joining an open (unsecured) SSID. If you aren't sure why open WLANs are a problem, just google "freesheep."

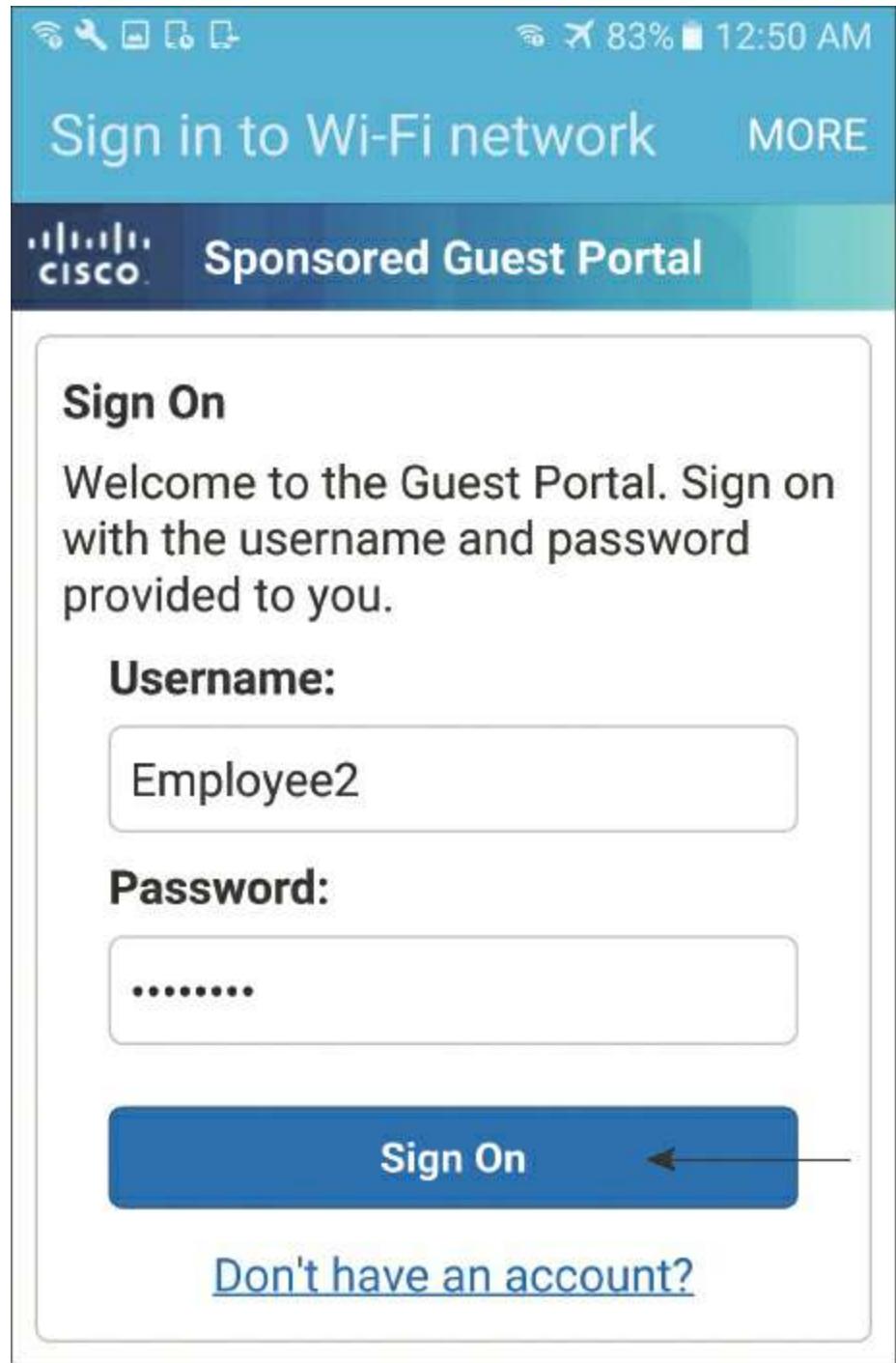


**Figure 17-32** Android: Choose a Wi-Fi Network



**Figure 17-33** Android: Tap Connect

**Step 2.** Because you protected the guest Wi-Fi by requiring a login (Guest or Active Directory), you are redirected to the Web Authentication (WebAuth) portal, as shown in [Figure 17-34](#). Keep in mind that these portals are fully customizable, so you can make it look any way you would like. Take note that the portal is a Guest portal: this is because ISE has no way of knowing if you are a guest or an employee until you provide your identity—in other words, until you log in.



**Figure 17-34** Android: WebAuth Portal

**Step 3.** After you log in through the WebAuth portal, you are seamlessly redirected to the BYOD portal, as shown in [Figure 17-35](#). The BYOD portal steps you through the onboarding process.

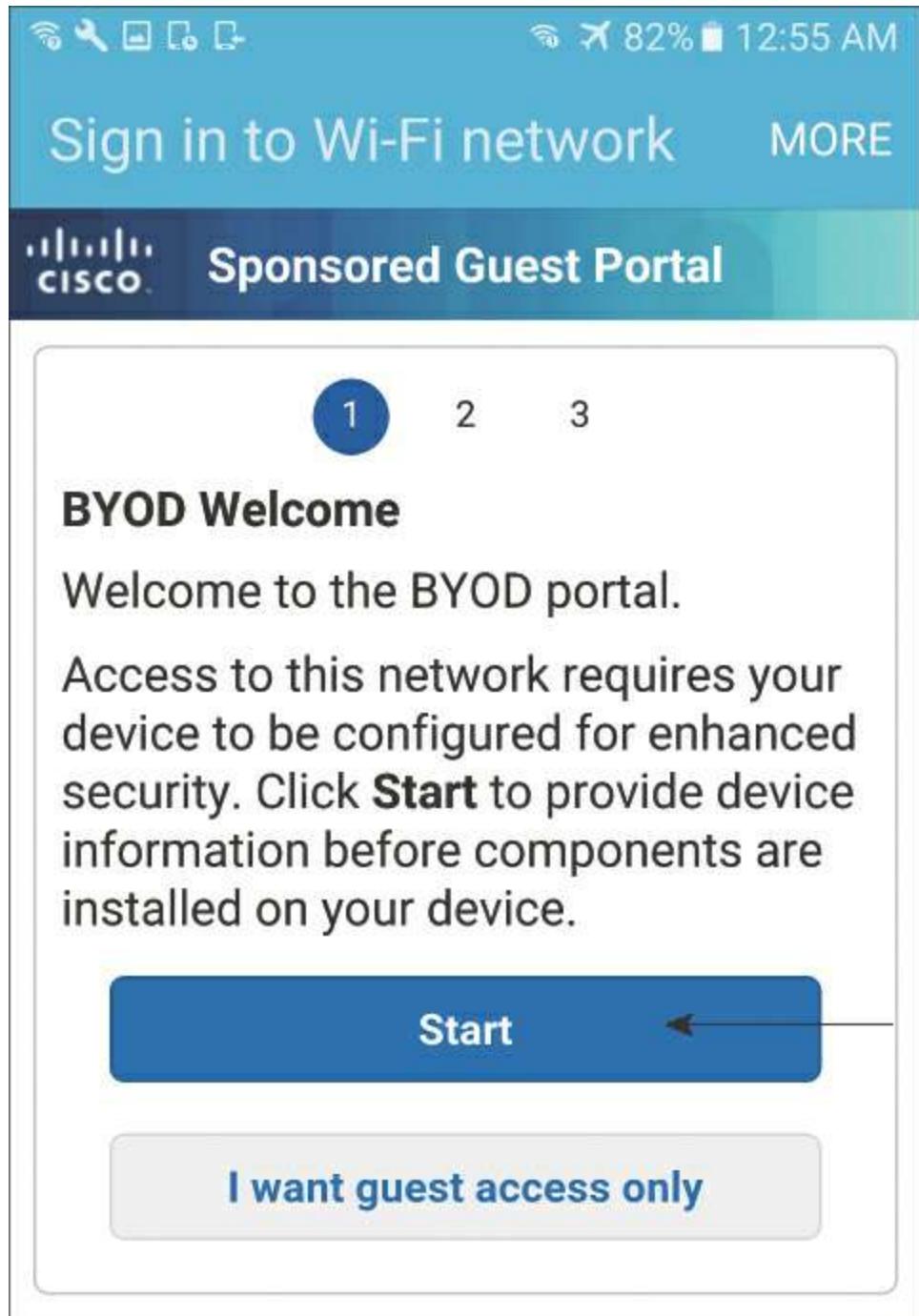
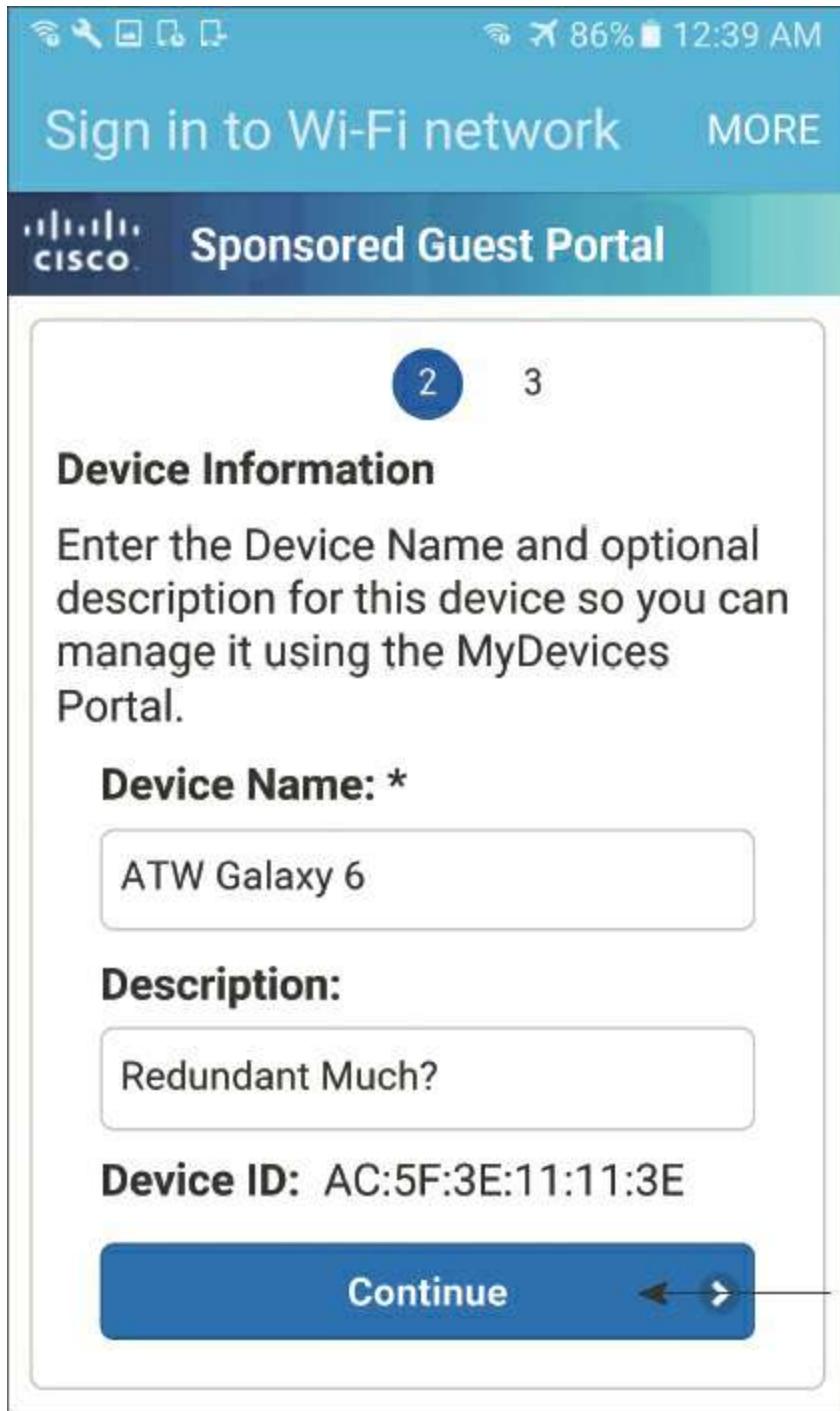


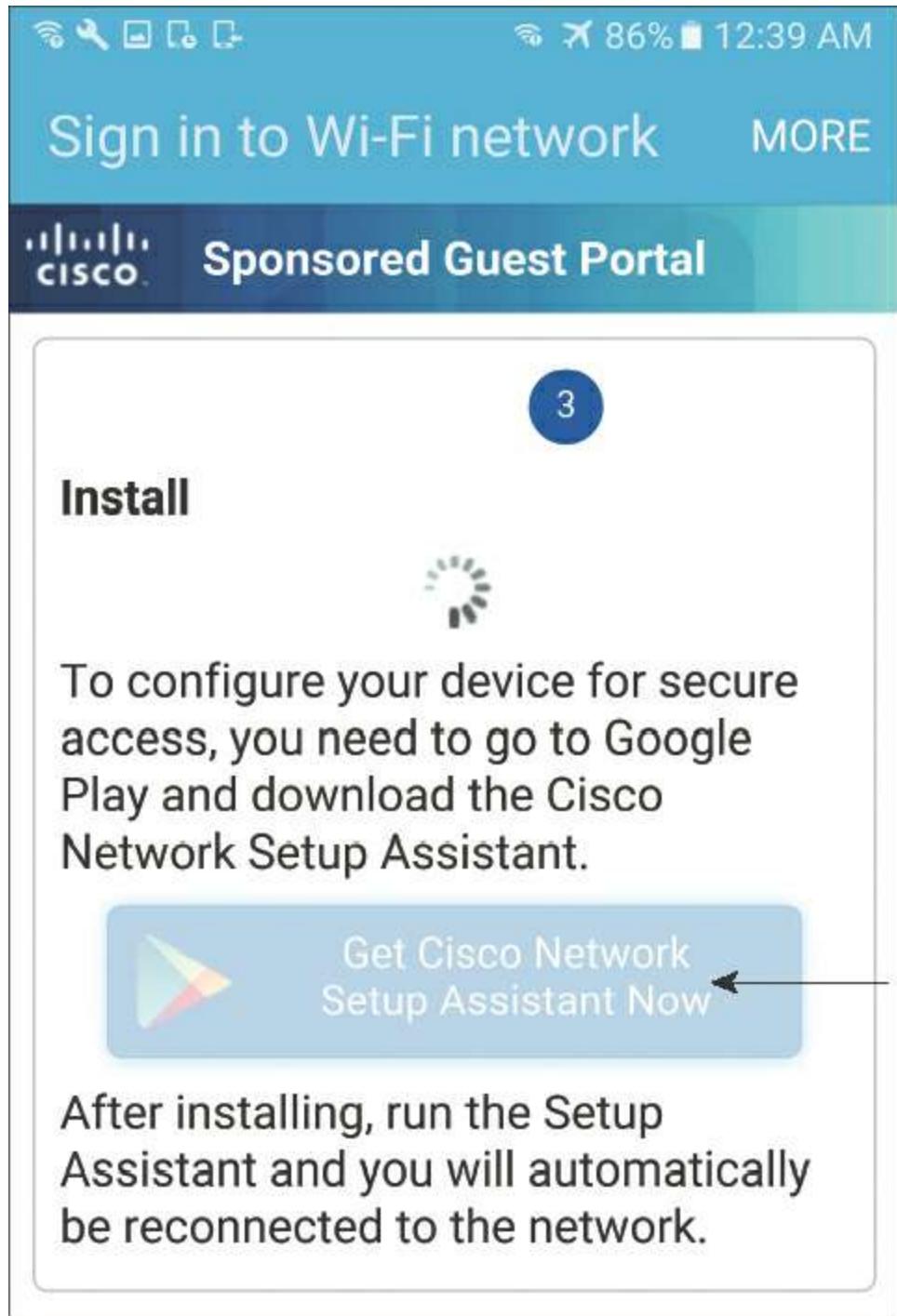
Figure 17-35 Android: BYOD Portal Welcome Page

**Step 4.** Tap **Start**. You move to step 2 of the BYOD portal, which is where device information is captured. As you can see in [Figure 17-36](#), you must enter a name that helps you to identify this device, and an optional description. The device ID (MAC address) is optionally displayed at the bottom.



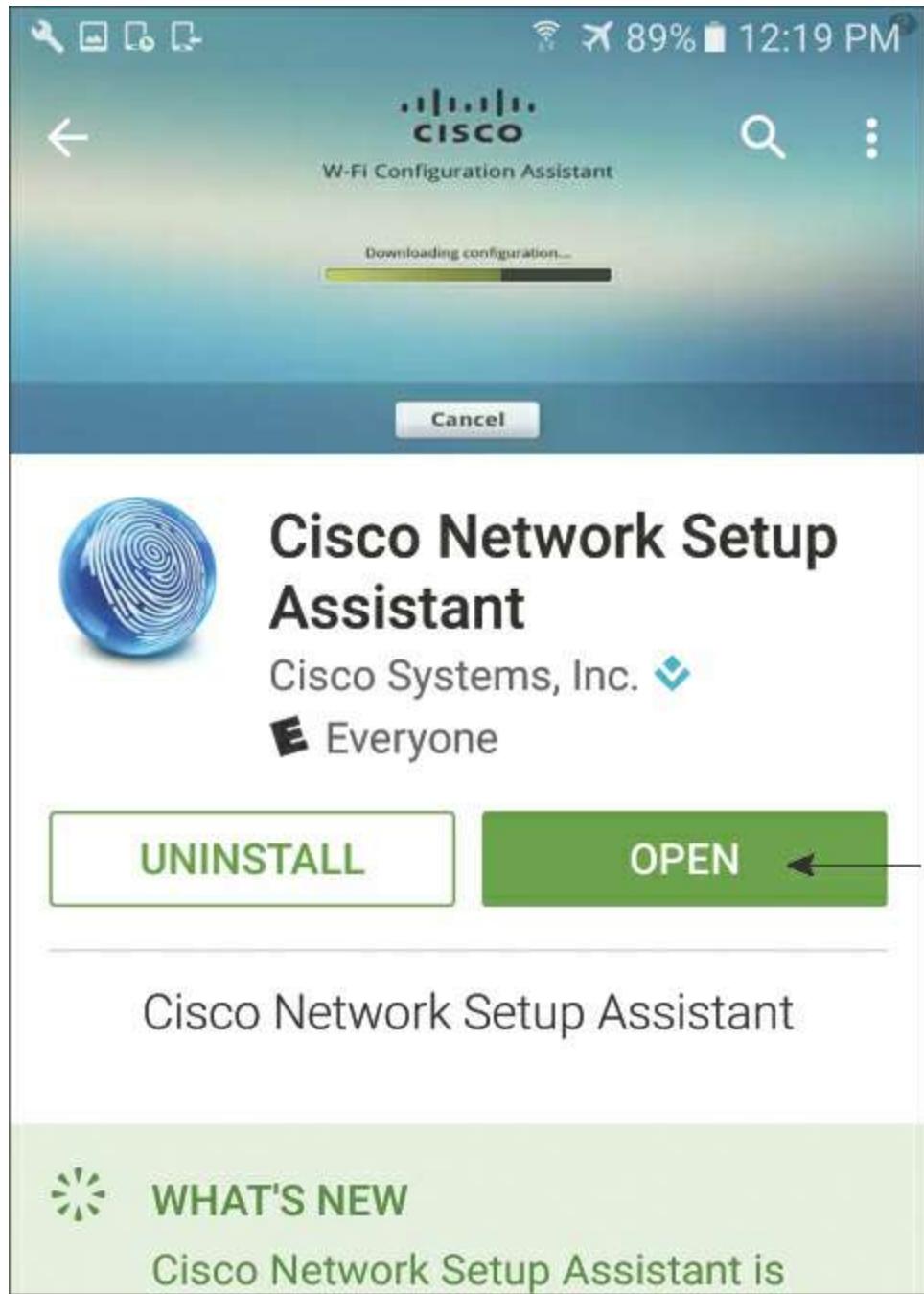
**Figure 17-36** Android: Device Information

**Step 5.** Enter the required device name and then tap **Continue**. You are advanced to step 3 of the BYOD portal, where you must tap the button to reach out to Google Play and download the Cisco Network Setup Assistant app, as shown in [Figure 17-37](#). Depending on your personal device settings, you may be given the choice between the Internet and the Google Play app.



**Figure 17-37** Android: Connect to Google Play

**Step 6.** Download or open the app from Google Play, as shown in [Figure 17-38](#).



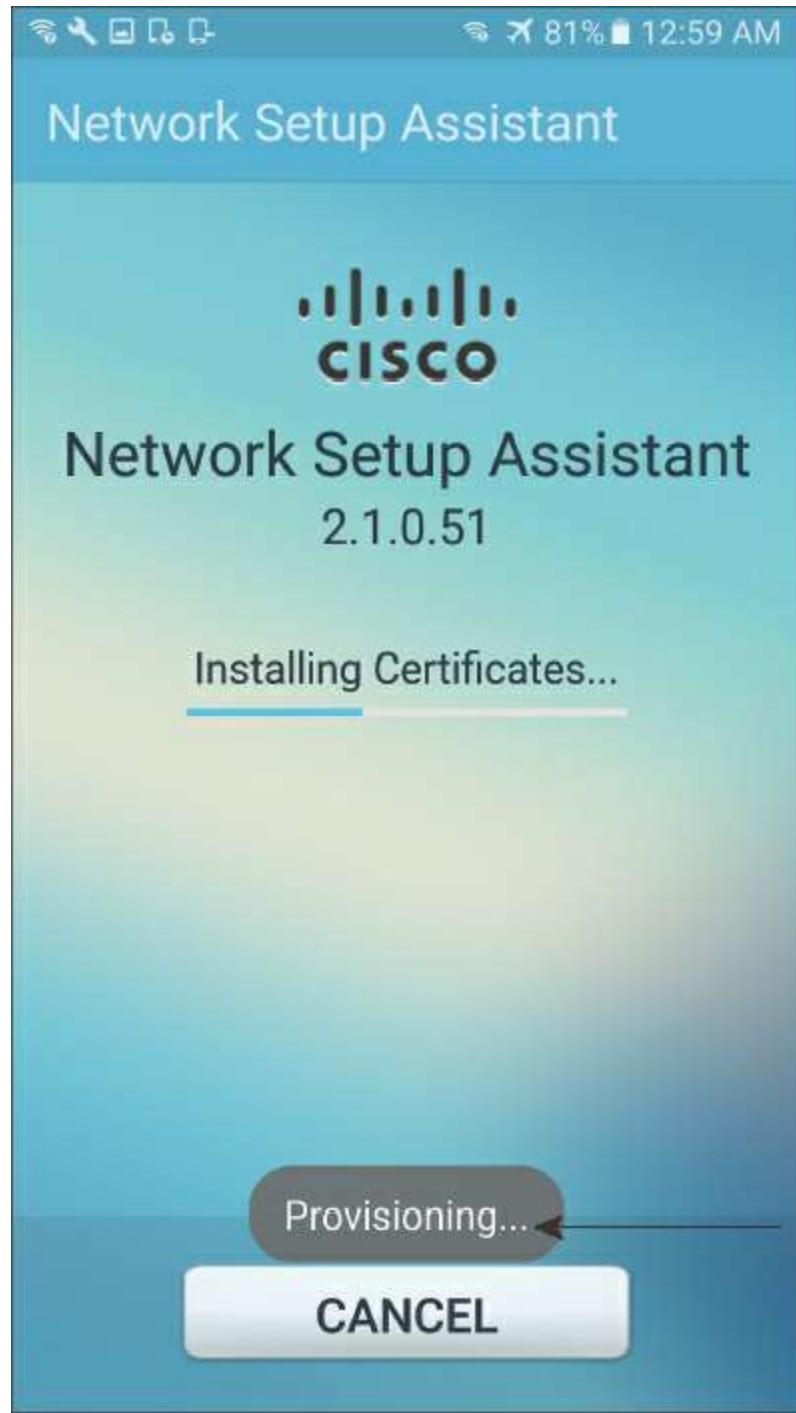
**Figure 17-38** Android: Download Cisco Network Setup Assistant

**Step 7.** Run the app and tap **Start**, as shown in [Figure 17-39](#).



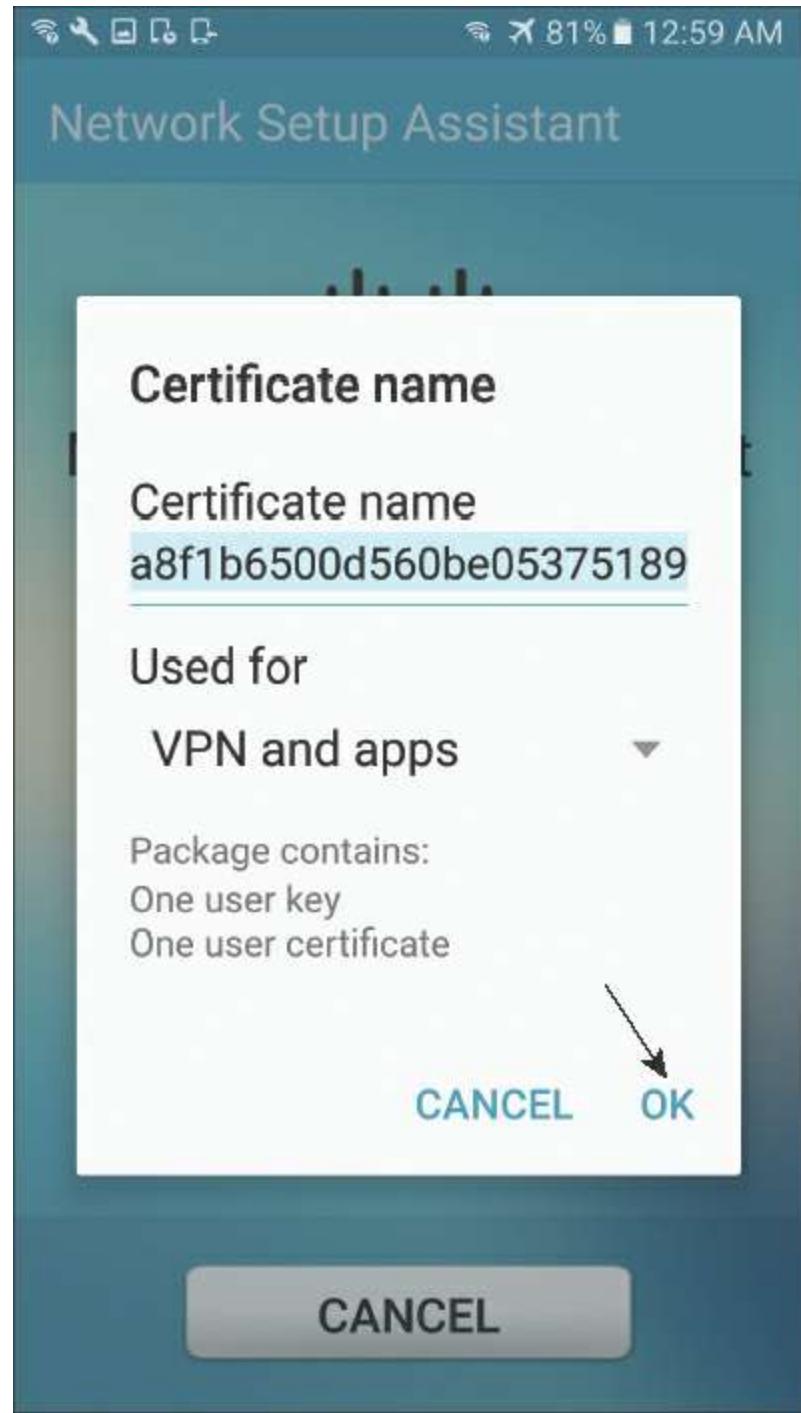
**Figure 17-39** Android: Run the NSA App

**Step 8.** The NSA app downloads the profile from ISE, as shown in [Figure 17-40](#).



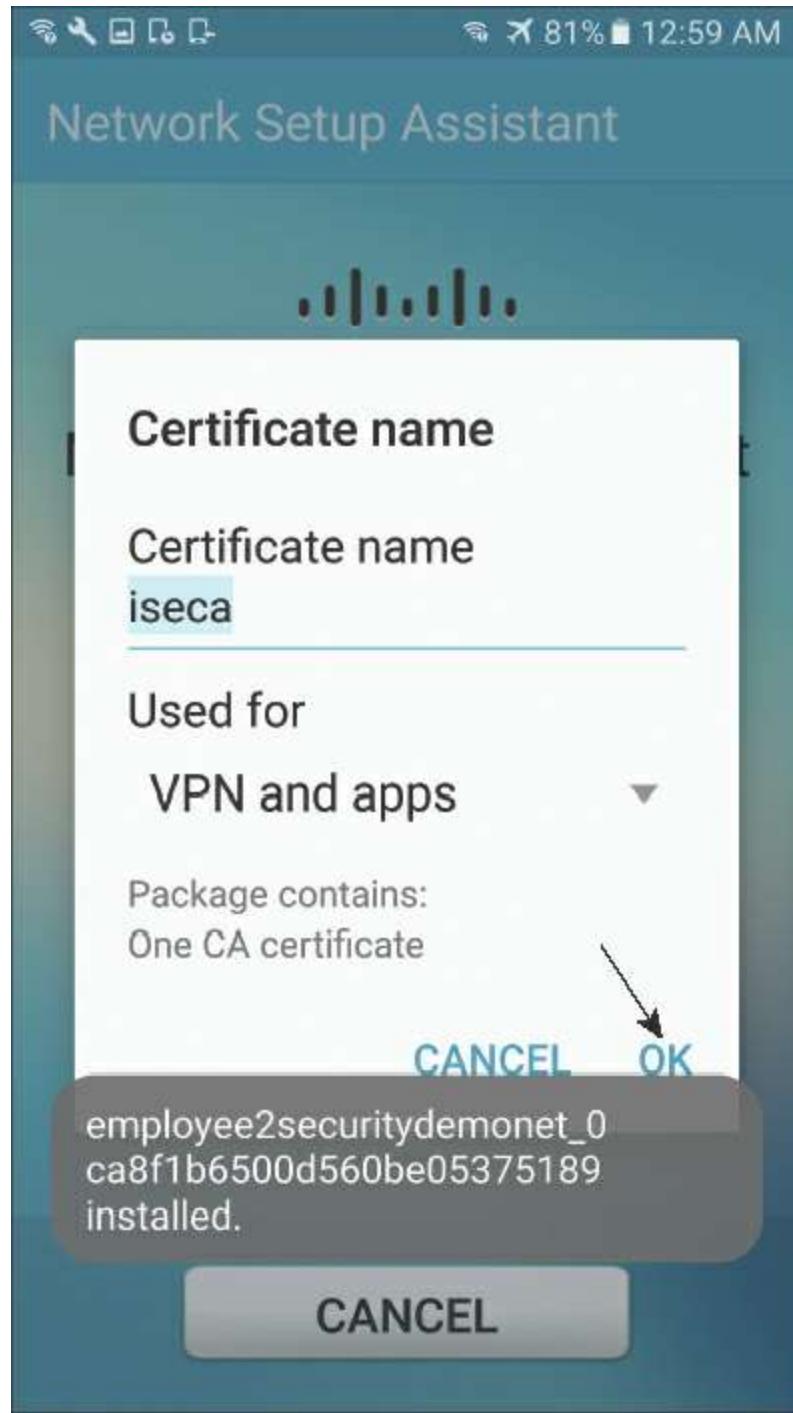
**Figure 17-40** Android: NSA App Downloading Profile

**Step 9.** Name and save your certificate, as shown in [Figure 17-41](#).



**Figure 17-41** Android: Name and Save the Certificate

**Step 10.** Name and save the CA certificate, as shown in [Figure 17-42](#).



**Figure 17-42** Android: Name and Save the CA Certificate

**Step 11.** The NSA app automatically changes the network connection to the corporate SSID and authenticates with the new certificate using EAP-TLS, as shown in [Figure 17-43](#) and [Figure 17-44](#). Your Android device is now ready to be used regularly on the corporate network. The onboarding was a one-time thing.

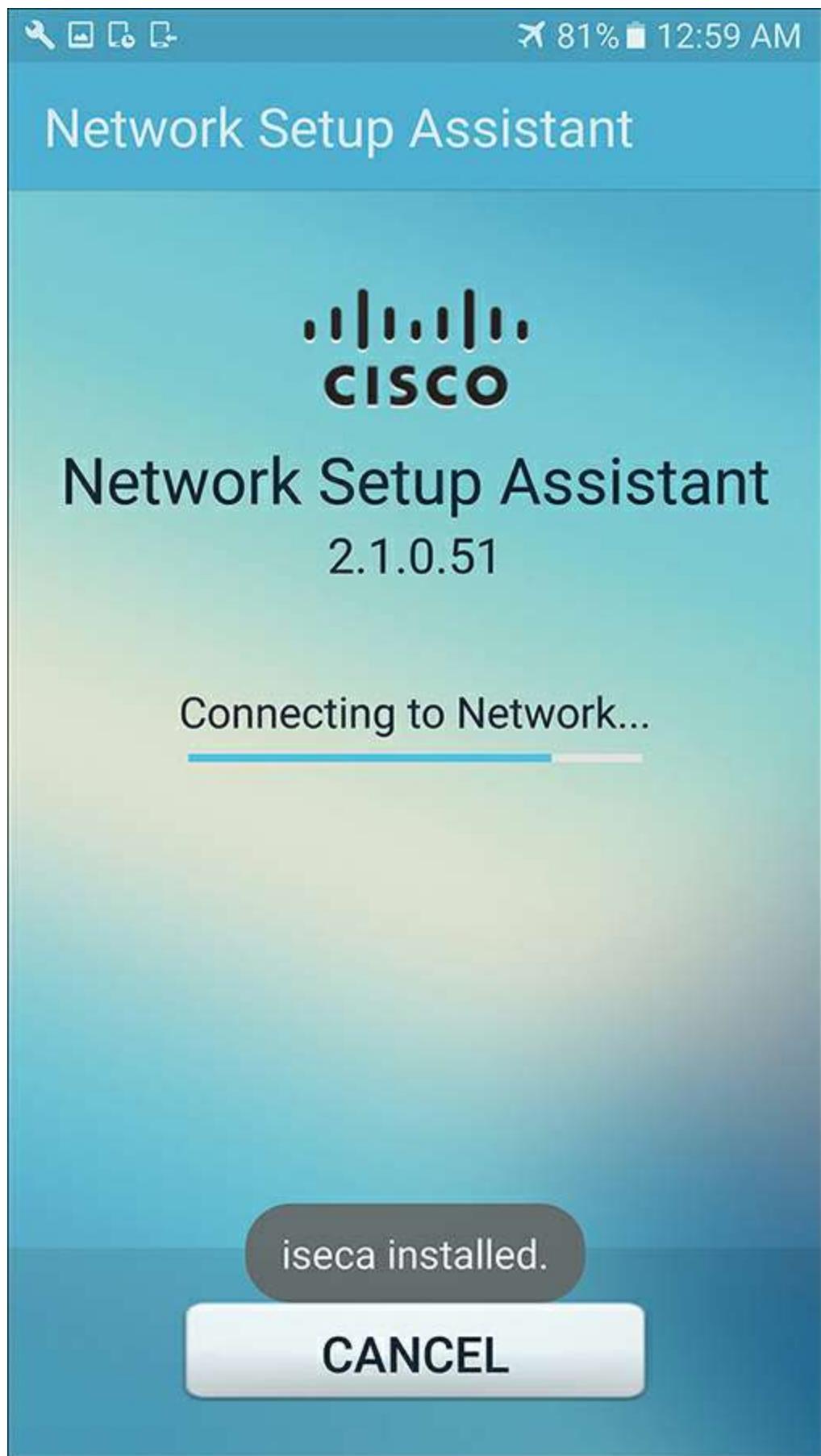


Figure 17-43 Android: Connect to the Corporate SSID

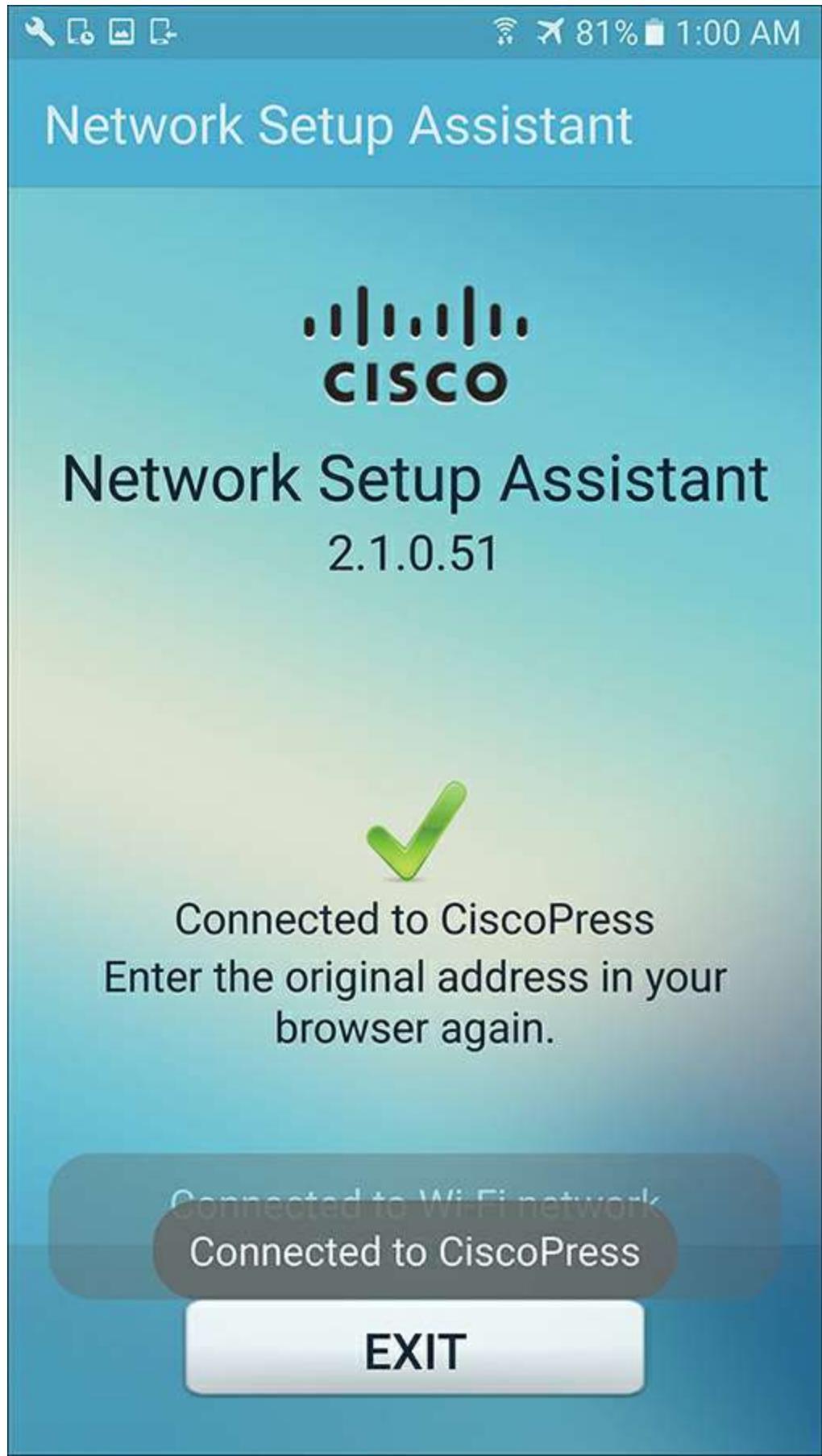


Figure 17-44 Android: Connected

## Configuring ISE for Onboarding

As you saw in the previous section, the end-user experience is designed to be straightforward and easy for a typical user to be able to follow without any interaction with the IT department. It is always advisable to keep the end-user experience as simple and easy as possible, and to put the administrative burden on yourself—the administrator—instead. To keep that end-user experience simple, you need to do some up-front work on the configuration side. A lot of it is completed for you out of the box in ISE version 2.0 and newer, but this section covers the entire configuration, default or not, so that you are familiar with it.

### Configure the Native Suplicant Profile

The native supplicant profile (NSP) defines the network settings for the endpoints that will go through onboarding.

The native supplicant profile defines the following:

- One or more wireless SSIDs
- EAP type to use (PEAP or EAP-TLS)
- Key size for certificates
- Level of wireless security
- If it applies to wired, wireless, or both
- Proxy configuration, if any
- Whether or not to connect to the SSID if not broadcasting

Beginning with ISE 2.0, ISE comes with the NSPs preinstalled. The following steps guide you through adding the latest client provisioning resources from the Cisco site (if necessary), and then editing the prebuilt native supplicant profile.

**Step 1.** Navigate to **Work Centers > BYOD > Client Provisioning > Resources**.

Examine the preinstalled resources, as shown in [Figure 17-45](#).

<input type="checkbox"/> Name	Type	Version	Last Update	Description
<input type="checkbox"/> WinSPWizard 2.1.0.51	WinSPWizard	2.1.0.51	2016/10/06 13:01:12	Supplicant Provisioning Wizard
<input type="checkbox"/> MacOsXSPWizard 2.1.0.41	MacOsXSPWizard	2.1.0.41	2016/10/06 13:01:12	Supplicant Provisioning Wizard
<input type="checkbox"/> Cisco-ISE-Chrome-NSP	Native Supplicant Profile	Not Applicable	2016/10/06 13:01:12	Pre-configured Native Supplicant Profile
<input type="checkbox"/> Cisco-ISE-NSP	Native Supplicant Profile	Not Applicable	2016/11/22 20:59:20	Pre-configured Native Supplicant Profile

**Figure 17-45 Preinstalled Agent Resources**

- Step 2.** To download newer or additional resources, choose **Add > Agent Resources from Cisco Site**. Note that this communication requires Internet access, which may require you to configure a proxy server to successfully communicate.
- Step 3.** The list of all versions of the clients and wizards is displayed, as shown in [Figure 17-46](#). Select any that you want to download and click **Save**.

Name	Description
<input type="checkbox"/> AgentCustomizationPackage 1.1.1.6	This is the NACAgent Customization Package v1.1.1.6 for Windows
<input type="checkbox"/> AnyConnectComplianceModuleOSX 3.6....	AnyConnect OS X Compliance Module 3.6.10881.2
<input type="checkbox"/> AnyConnectComplianceModuleOSX 4.2....	AnyConnect OSX Compliance Module 4.2.721.0
<input type="checkbox"/> AnyConnectComplianceModuleWindow...	AnyConnect Windows Compliance Module 3.6.10881.2
<input type="checkbox"/> AnyConnectComplianceModuleWindow...	AnyConnect Windows Compliance Module 4.2.488.0
<input type="checkbox"/> ComplianceModule 3.6.10853.2	NACAgent ComplianceModule v3.6.10853.2 for Windows
<input type="checkbox"/> MACComplianceModule 3.6.10853.2	MACAgent ComplianceModule v3.6.10853.2 for MAC OSX
<input type="checkbox"/> MacOsXAgent 4.9.0.1006	NAC Posture Agent for Mac OSX (ISE 1.2 release)
<input type="checkbox"/> MacOsXAgent 4.9.0.1007	NAC Posture Agent for Mac OSX v4.9.0.1007 (with CM 3.6.7873.2)- ISE 1.2 release
<input type="checkbox"/> MacOsXAgent 4.9.0.655	NAC Posture Agent for Mac OSX (ISE 1.1.1 or later)
<input type="checkbox"/> MacOsXAgent 4.9.0.661	NAC Posture Agent for Mac OS X v4.9.0.661 with CM v3.5.7371.2 (ISE 1.1.3 Release)
<input type="checkbox"/> MacOsXAgent 4.9.4.3	NAC Posture Agent for Mac OSX v4.9.4.3 - ISE 1.2 , ISE 1.1.3 and Above releases
<input type="checkbox"/> MacOsXAgent 4.9.5.3	NAC Posture Agent for Mac OSX v4.9.5.3 - ISE 1.2 Patch 12, ISE 1.3 release and Above
<input type="checkbox"/> MacOsXSPWizard 1.0.0.18	Supplicant Provisioning Wizard for Mac OsX 1.0.0.18 (ISE 1.1.3 Release)
<input type="checkbox"/> MacOsXSPWizard 1.0.0.21	Supplicant Provisioning Wizard for Mac OsX 1.0.0.21 (for ISE 1.2 release)
<input type="checkbox"/> MacOsXSPWizard 1.0.0.27	Supplicant Provisioning Wizard for Mac OsX 1.0.0.27 (for ISE 1.2 release with Patch 11 and ...)
<input type="checkbox"/> MacOsXSPWizard 1.0.0.29	Supplicant Provisioning Wizard for Mac OsX 1.0.0.29 (for ISE 1.2 release with Patch 12 and ...)

For AnyConnect software, please download from <http://cisco.com/go/anyconnect>. Use the "Agent resource from local disk" add option, to import into ISE

**Save** **Cancel**

**Figure 17-46** Agent Resources from Cisco Site

Remember, with BYOD, you are not installing a network manager or a supplicant onto the device. Instead, you are configuring the endpoint for the end user. To help accomplish that, NSPs are used to configure the networking on the endpoints that are onboarded. In other words, the NSPs are the configuration instructions for the supplicants that exist in the endpoint operating systems.

An NSP contains configurations identifying which wireless SSID the client should connect to (if there is more than one wireless network), which security those wireless networks require to connect, whether the endpoint should also authenticate to wired networks, and whether to use user or machine authentication—truly a slew of configuration choices for the supplicant native to the endpoint OS.

**Step 4.** On the Resources screen, select the preconfigured NSP named **Cisco-ISE-NSP** and click **Edit**. Your screen should have a preconfigured wireless network with an SSID of ISE. [Figure 17-47](#) shows the contents of Cisco-ISE-NSP—the one in our figure has a second wireless SSID named CiscoPress.

The screenshot shows the 'Native Suplicant Profile > Cisco-ISE-NSP' page. At the top, there's a 'Native Suplicant Profile' section with fields for Name (Cisco-ISE-NSP), Description (Pre-configured Native Suplicant Profile. The SSID Will Need To Be Customized For Your), and Operating System (ALL). Below this is a 'Wireless Profile(s)' section. It contains a table with two rows:

SSID Name	Proxy Auto-Config File ...	Proxy Host/IP	Port	Security	Allowed Protocol	Certificate Template
CiscoPress				WPA2 Enterprise	TLS	EAP_Authentication_Certi
ISE				WPA2 Enterprise	TLS	EAP_Authentication_Certi

Below the table, there's a 'Wired Profile' section with dropdown menus for Allowed Protocol (PEAP) and Certificate Template (Not Required). At the bottom are 'Submit' and 'Cancel' buttons.

**Figure 17-47** Cisco-ISE-NSP

**Step 5.** Select **ISE** and click **Edit** to see the preconfigured wireless profile. As shown

in [Figure 17-48](#), this out-of-the-box profile is designed to use an SSID named ISE with WPA2 and TLS that leverages the EAP\_Authentication\_Certificate\_Template and will connect even if the network is not broadcasting.

The screenshot shows the 'Wireless Profile' configuration page. At the top, it says 'SSID Name \*' followed by a text input field containing 'ISE'. Below that are fields for 'Proxy Auto-Config File URL' and 'Proxy Host/IP', both with information icons. There are also fields for 'Proxy Port', 'Security \*' (set to 'WPA2 Enterprise'), 'Allowed Protocol \*' (set to 'TLS'), and 'Certificate Template' (set to 'EAP\_Authentication\_Certificate\_Template'). A section titled 'Optional Settings' is expanded, showing 'Windows Settings' with 'Authentication Mode' set to 'User or Computer'. Under 'Windows Settings', there are three checkboxes: 'Do not prompt user to authorize new servers or trusted certification authorities' (unchecked), 'Use a different user name for the connection' (unchecked), and 'Connect even if the network is not broadcasting its name (SSID)' (checked). Below this is an 'iOS Settings' section with a single checkbox 'Enable if target network is hidden' (unchecked). At the bottom right are 'Submit' and 'Cancel' buttons.

**Figure 17-48** ISE Wireless Profile

## Examine the Certificate Template

As you just learned, NSPs are the network configurations sent to the endpoints. EAP-TLS is the most common deployment, and when TLS is used, a certificate must be issued to the endpoint. The certificate template defines the content or fields of the certificate, the certificate strength, and even which CA should be used to issue the certificates.

Examine the default EAP\_Authentication\_Certificate\_Template that is used in the default Cisco-ISE-NSP native supplicant profile by following these steps:

**Step 1.** Navigate to Work Centers > BYOD > Portals & Components > Certificates > Certificate Templates and select EAP\_Authentication\_Certificate\_Template, as shown in [Figure 17-49](#), and then click Edit.

The screenshot shows the Cisco Identity Services Engine interface. The top navigation bar includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. Under Work Centers, the sub-navigation includes Network Access, Guest Access, TrustSec, BYOD, Profiler, Posture, Device Administration, and PassiveID. The main menu has sections for Overview, Identities, Identity Groups, Network devices, Ext Id Sources, Client Provisioning, Portals & Components (which is selected and highlighted in blue), and Policy Elements. On the left, a sidebar lists BYOD Portals, My Devices Portals, Blacklist Portal, Certificates (which is expanded to show Internal CA Settings, Certificate Templates, and External CA Templates), and pxGrid\_Certificate\_Template. The main content area is titled "Certificate Templates" and contains a table with the following data:

Template Name	Description	Key Type	Key Size	Curve Type
CA_SERVICE_Certificate_Template	This template will be us...	RSA	2048	N/A
EAP_Authentication_Certificate_Template	This template will be us...	RSA	2048	N/A
pxGrid_Certificate_Template	This template will be us...	RSA	2048	N/A

**Figure 17-49** Certificate Templates

**Step 2.** As shown in [Figure 17-50](#), the certificate template is configured with a fixed common name (CN) set to the \$UserName\$ variable. This is automatically substituted with the username of the employee performing the onboarding. The other portions of the subject, such as organization (O) and organizational unit (OU), are filled with placeholders that you can modify to suit your own needs.

**Edit Certificate Template**

* Name	EAP_Authentication_Certificate_Template	
Description	This template will be used to issue certificates for EAP Authentication	
<b>Subject</b>		
Common Name (CN)	\$UserName\$ <small>(i)</small>	
Organizational Unit (OU)	Example unit	
Organization (O)	Company name	
City (L)	City	
State (ST)	State	
Country (C)	US	
Subject Alternative Name (SAN)		
<input type="button" value="..."/> MAC Address		
Key Type	RSA	
Key Size	2048	
* SCEP RA Profile	ISE Internal CA	
Valid Period	730	Day(s) (Valid Range 1 - 730)
Extended Key Usage <input checked="" type="checkbox"/> Client Authentication <input type="checkbox"/> Server Authentication		
<input type="button" value="Save"/> <input type="button" value="Reset"/>		

**Figure 17-50 EAP\_Authentication\_Certificate\_Template**

**Step 3.** Continuing with [Figure 17-50](#), notice the Subject Alternative Name (SAN) field. The drop-down box has only one choice, which is MAC Address; because this cannot be changed or removed, it seems to be a bit of a UI mistake. The UI components are used to someday allow extending the template for other items in the template, but alas—those other options are not available yet.

**Step 4.** Still referencing [Figure 17-50](#), you can see that the default template is configured to use RSA as the key type. The other choice is to use elliptic curve cryptography (ECC). ECC should only be used with total planning, because not all devices support it, for now. The default RSA key size is 2048, but that size can be changed to 1024 or 4096.

**Step 5.** The purpose of the SCEP RA Profile field in [Figure 17-50](#) is to configure which CA should be used to sign the certificates. The default configuration is to use the

internal CA; if an external CA is configured in ISE, it will also be in the drop-down list.

**Step 6.** The Valid Period setting determines how long the certificate is “warranted” by the CA, meaning how long the CA is responsible for publishing the revocation state of the certificate.

**Step 7.** The default setting for Extended Key Usage (EKU) of an endpoint certificate is Client Authentication only. Server authentication is available for you to configure if you need it, but it should not be required for a BYOD certificate.

## Examine the Client Provisioning Policy

The NSPs are the network configurations sent to the endpoints, and they include the choice of which certificate template to use, which, in turn, decides which CA to use and which key sizes.

You still need a policy to determine which NSP to send to clients, which is completed in the client provisioning policy (CPP). The CPP dictates the software and profiles that should be downloaded and installed based on the operating system of the endpoint and a multitude of other possible attributes. For example, you might configure a policy for Android to be provisioned for the CORP-SSID wireless network when an employee is going through the provisioning process and configure another policy for Android to be provisioned for the CONTRACTOR-SSID wireless network for all vendors and contractors who are also working through the provisioning process.

Out of the box, there is one client provisioning policy per OS using the preinstalled native supplicant wizards, native supplicant profiles, and certificate templates. To examine these preconfigured policies, navigate to **Work Centers > BYOD > Client Provisioning**, as shown in [Figure 17-51](#).

Client Provisioning Policy						
Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation: For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package. For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.						
Rule Name	Identity Groups	Operating Systems	Other Conditions	Results		
IOS	If Any	and Apple iOS All	and Condition(s)	then	Cisco-ISE-NSP	
Android	If Any	and Android	and Condition(s)	then	Cisco-ISE-NSP	
Windows	If Any	and Windows All	and Condition(s)	then	WinSPWizard 2.1.0.51 And Cisco-ISE-NSP	
MAC OS	If Any	and Mac OSX	and Condition(s)	then	MacOsXSPWizard 2.1.0.41 And Cisco- ISE-NSP	
Chromebook	If Any	and Chrome OS All	and Condition(s)	then	Cisco-ISE-Chrome-NSP	

**Figure 17-51** Client Provisioning Policy

First, examine the client provisioning policy for Apple iOS:

**Step 1.** Click **Edit** at the right end of the row for the rule named IOS.

**Step 2.** Note that a rule can apply to specific user or endpoint identity groups, specific operating systems, and a slew of other conditions that are exposed to the CPP.

**Step 3.** Click the plus symbol in the Results column. The result choices vary based on the OS chosen. For iOS, notice that only the profile is selectable, as shown in [Figure 17-52](#). The ISE BYOD portal automatically uses the OTA provisioning process that is native to Apple iOS. There is no need to specify anything else here.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
IOS	If Any + and	Apple iOS All + and	Condition(s) + then	Cisco-ISE-NSP
Android	If Any			
Windows	If Any			
MAC OS	If Any			

**Figure 17-52** Client Provisioning Policy for iOS

Next, examine the client provisioning policy for Android:

**Step 1.** Click **Edit** at the right end of the row for the rule named Android.

**Step 2.** Click the plus symbol in the Results column to see the configuration options, as shown in [Figure 17-53](#). Again, the result choices vary based on the OS chosen. The only selection available for Android is the NSP because the ISE client BYOD portal automatically redirects Android devices to Google Play to download the Network Setup Assistant app, as you saw previously in the chapter. There is no option to specify a different app store.

Next, examine the client provisioning policy for Windows:

**Step 1.** Click **Edit** at the right end of the row for the rule named Windows.

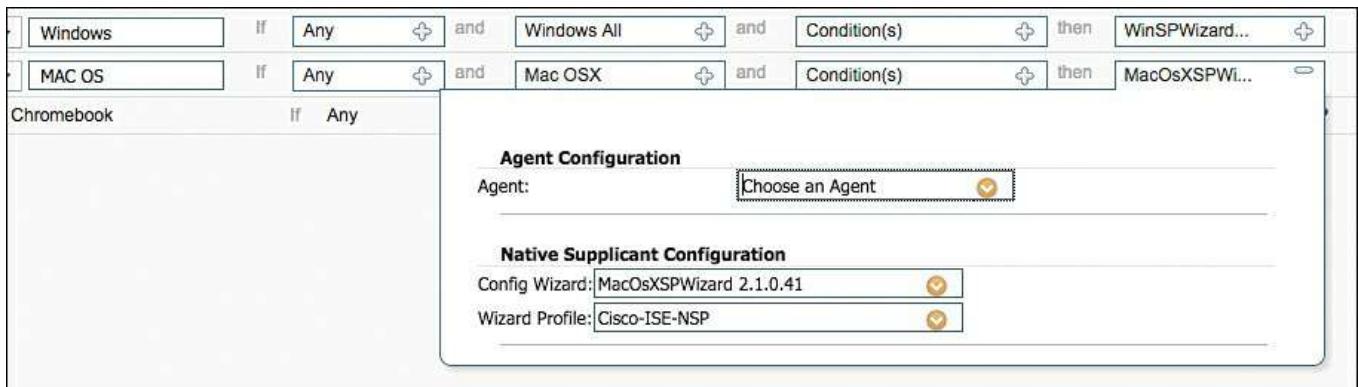
**Step 2.** Click the plus symbol in the Results column. For Windows, the drop-down box provides more possibilities than are available for iOS or Android, as shown in [Figure 17-53](#). The upper portion of the results configuration is for posture, while the lower half is for BYOD provisioning. Focusing on BYOD, you see that it is preconfigured to use the preinstalled Windows program to implement the provisioning, and that must be specified here.



**Figure 17-53** Client Provisioning Policy for Windows and Android

Next, examine the client provisioning policy for Mac OS X:

- Step 1.** Click **Edit** at the right end of the row for the rule named MAC OS.
- Step 2.** Click the plus symbol in the results column. Like Windows, the drop-down box for Mac OS X provides more possibilities than are available for iOS and Android, as shown in [Figure 17-54](#). The upper portion of the results configuration is for posture, while the lower half is for BYOD provisioning. Focusing on BYOD, you see that it is preconfigured to use the preinstalled MAC OS program to implement the provisioning, and that must be specified here.



**Figure 17-54** Client Provisioning Policy for MAC OS

Finally, examine the client provisioning policy for Chromebooks:

- Step 1.** Click **Edit** at the right end of the row for the rule named Chromebook.
- Step 2.** Click the plus symbol in the Results column. The result choices vary based on the OS chosen. Chrome OS onboarding is very different from the other BYOD platforms, and is actually a managed endpoint strategy, not a BYOD strategy at all. It gets its own NSP, separate from the other OSs, and requires that the devices be managed by Google domain registration and device licenses. The NSA must be pre-pushed to the device by the Google cloud.

## BYOD and WebAuth Portals

Now that you have seen the client provisioning policies, you can take a look at the portals that the end users will see. You saw these portals yourself during the client experience review section and in figures such as [Figure 17-19](#) and [17-34](#). The BYOD portal is used in single-SSID provisioning, while the WebAuth portal is used during the dual-SSID flow.

Let's start with the BYOD portal:

**Step 1.** Navigate to **Work Centers > BYOD > Portals & Components > BYOD Portals**.

**Step 2.** Edit the preconfigured **BYOD Portal (default)**, as shown in [Figure 17-55](#).

## Portal Settings and Customization

Portal Name: \*

BYOD Portal (default)

Description:

Default portal and user experience used when employees register a person:

Port



### Portal Behavior and Flow Settings

Use these settings to specify the guest experience for this portal.



### Portal Page Customization

Customize portal pages by applying a template to field names and messages displayed to guests.

## Portal & Page Settings

### ▼ Portal Settings

HTTPS

port:

8443 (8000 - 8999)

Allowed Make selections in one or both columns based on your PSN configurations.

interfaces: If bonding is **not** configured i on a PSN, use:

Gigabit Ethernet 0

Gigabit Ethernet 1

Gigabit Ethernet 2

Gigabit Ethernet 3

Gigabit Ethernet 4

Gigabit Ethernet 5

If bonding is configured i on a PSN, use:

Bond 0

Uses Gigabit Ethernet 0 as **primary**, 1 as **backup**.

Bond 1

Uses Gigabit Ethernet 2 as **primary**, 3 as **backup**.

Bond 2

Uses Gigabit Ethernet 4 as **primary**, 5 as **backup**.

Certificate

Default Portal Certificate Group ▾

group tag:

Configure certificates at:

[Administration > System > Certificates > System Certificates](#)

Endpoint

RegisteredDevices ▾

Identity

Configure endpoint identity groups at:

group: \* [Work Centers > BYOD > Identity Groups](#)

The endpoints in this group will be purged according to the policies defined in:

[Administration > Identity Management > Settings > Endpoint purge](#)

Display  Use browser locale

language:

Fallback language: English - English ▾

Always use: English - English ▾

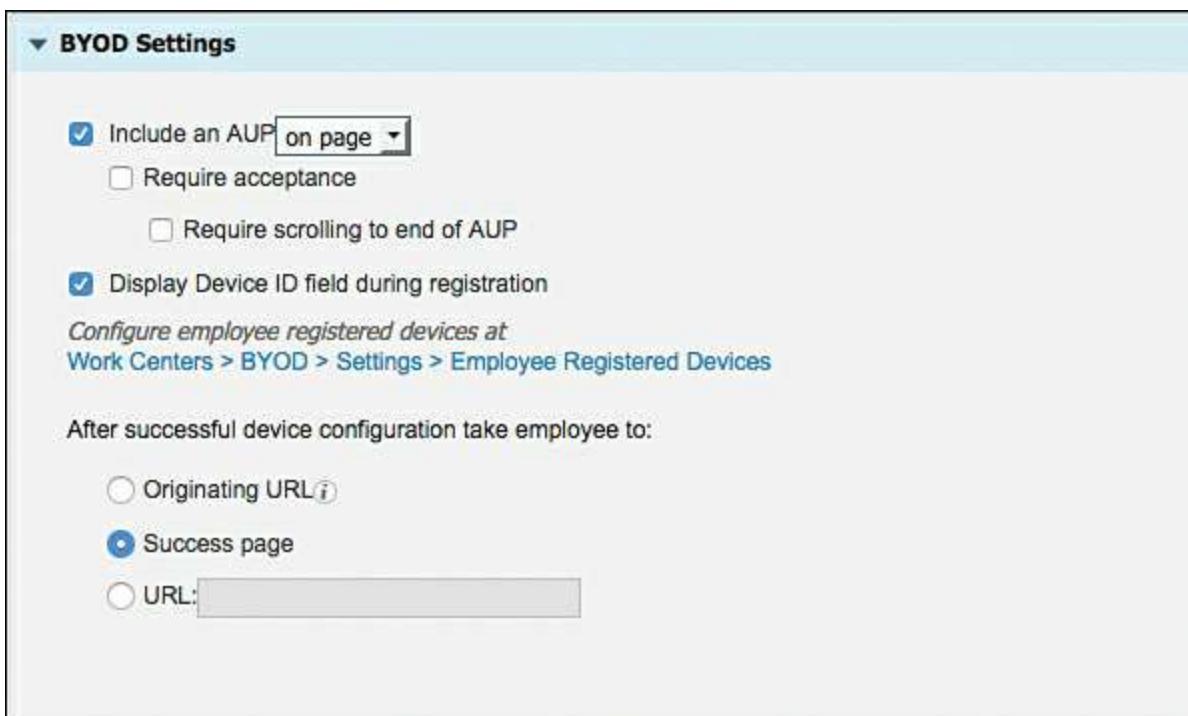
**Figure 17-55** BYOD Portal—Configuring Portal Settings

**Step 3.** Expand the **Portal Settings** section, which is used to configure the following:

- The TCP ports and interfaces for the portal to operate on. The default is to operate on the Gigabit Ethernet 0 interface or the Bond 0 interface for those Policy Service Nodes (PSN) configured with network interface card (NIC) bonding, and to operate on port 8443.
- The Certificate Group Tag drop-down list is used to pick which certificate should be used to identify the web service and secure the HTTPS connection. The default certificate group tag is used with an out-of-the-box configuration.
- The Endpoint Identity Group option is preconfigured to leverage the RegisteredDevices group. This means that any endpoints going through the BYOD process are added to this RegisteredDevices group. It is configurable per portal, so different users or endpoint types can be added to different endpoint identity groups.

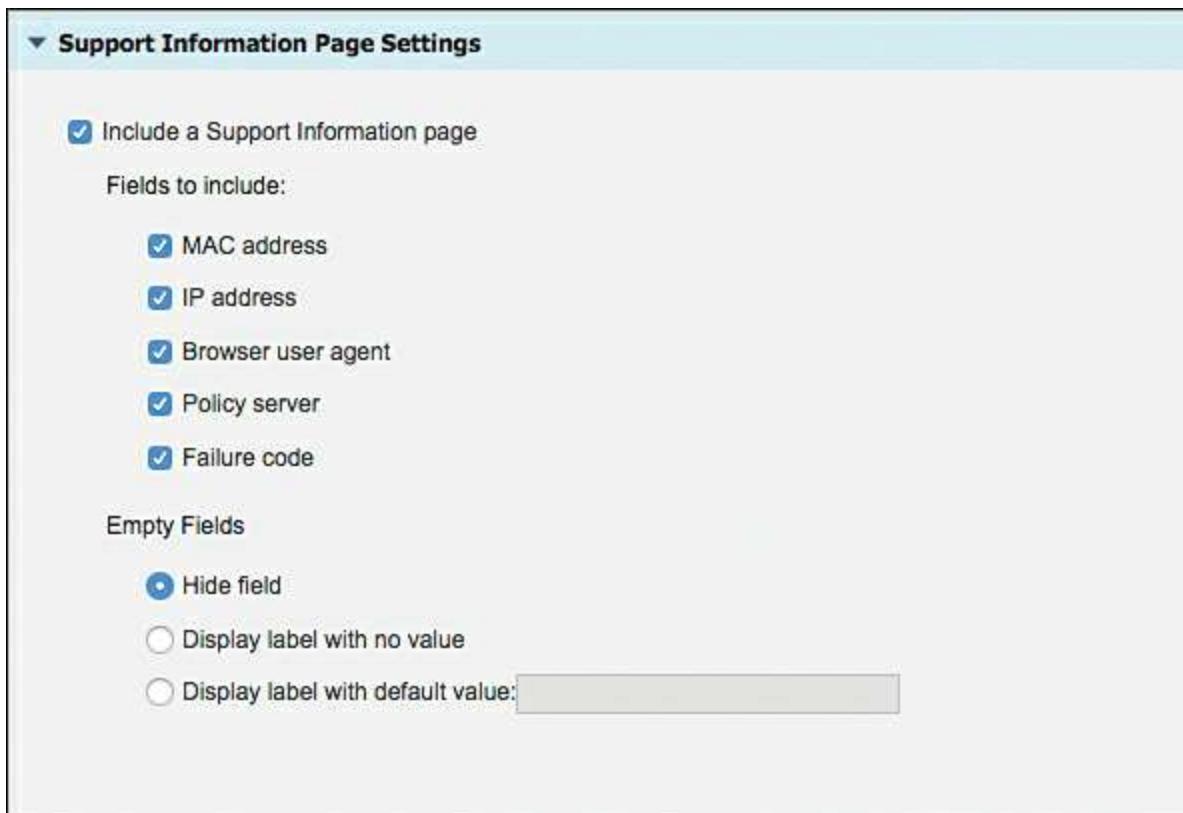
**Step 4.** Expand the **BYOD Settings** section, which is used to configure a few options, as shown in [Figure 17-56](#):

- Whether to require the employee to agree to an acceptable use policy (AUP).
- Whether to display the Device ID (MAC Address) field during registration, which is very useful for an IT admin, but perhaps not so useful for the end user unless he or she needs to leverage the help desk.



**Figure 17-56** BYOD Portal—Configuring BYOD Settings

**Step 5.** Expand the **Support Information Settings** section, which is used to display certain information to the employee that can aid the help desk, should a need arise to call them. [Figure 17-57](#) shows the support information.



**Figure 17-57** BYOD Portal—Configuring Support Information Settings

Now examine the WebAuth portal, which is the portal end users see in a dual-SSID onboarding flow.

There is a plethora of options when it comes to Web Authentication and supplicant provisioning. For instance, it is absolutely possible to configure different web portals based on a number of attributes available from the authentication request (such as source SSID). This way, you can enable the device registration and supplicant provisioning to occur per use case, if you so choose.

For simplicity, examine the default rule named `Wi-Fi_Redirect_to_Guest_Login`:

**Step 1.** Navigate to **Work Centers > BYOD > Policy Sets > Default**, as shown in [Figure 17-58](#). Notice that this is the exact same policy set screen that you have used before in the Network Access Work Center. That's the beauty of a Work Center: it is designed to provide access to all the portions of the UI required to complete your task. Also notice that this rule will match any incoming wireless MAB requests and leverage the preconfigured result of `Cisco_WebAuth`.

Authorization Policy					
Exceptions (0)		Conditions (Identity groups and other conditions)		Permissions	
Status	Role Name	Condition	then	Permissions	Action
Active	Wireless_Block_List_Default	If: Blacklist AND Wireless_Access	then:	Blockhole_Wireless_Access	Edit   +
Active	Profiled Cisco IP Phones	If: Cisco_IP_Phone	then:	Cisco_IP_Phones	Edit   +
Active	Profiled Non Cisco IP Phone	If: Non_Cisco_Profiled_Phones	then:	Non_Cisco_IP_Phones	Edit   -
Active	Compliant_Devices_Access	If: Network_Access_Authentication_Passed AND Compliant_Devices	then:	PermitAccess	Edit   +
Active	Employee_EAP-TLS	If: Wireless_802.1X AND BYOD_is_Registered AND EAP-TLS AND MAC_in_BAN	then:	PermitAccess AND BYOD	Edit   +
Active	Employee_Onboarding	If: Wireless_802.1X AND EAP-MSCHAPv2	then:	NSP_Onboard AND BYOD	Edit   +
Active	Wi-Fi_Guest_Access	If: Guest_Flow AND Wireless_MAB	then:	PermitAccess AND Guests	Edit   +
Active	Wi-Fi_Redirect_to_Guest_Login	If: Wireless_MAB	then:	Cisco_WebAuth	Edit   +
Active	Basic_Authenticated_Access	If: Network_Access_Authentication_Passed	then:	PermitAccess	Edit   +
Active	Default	If no matches, then:		DenyAccess	Edit   +

Figure 17-58 Default Policy Set

**Step 2.** Navigate to Work Centers > BYOD > Policy Elements > Results > Authorization Profiles > Cisco\_WebAuth, as shown in [Figure 17-59](#). Here you can see under the common tasks and the Attribute Details that Centralized Web Authentication has been preconfigured to use Self-Registered Guest Portal (default).

Authorization Profiles > **Cisco\_WebAuth**

**Authorization Profile**

* Name	Cisco_WebAuth
Description	Default Profile used to redirect users to the CWA portal.
* Access Type	ACCESS_ACCEPT
Network Device Profile	Cisco
Service Template	<input type="checkbox"/>
Track Movement	<input type="checkbox"/> i
Passive Identity Tracking	<input type="checkbox"/> i

**Common Tasks**

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

Centralized Web Auth	ACL	ACL_WEBAUTH_REDIRECT	Value
			Self-Registered Guest Portal (de)

**Attributes Details**

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=ACL_WEBAUTH_REDIRECT
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=a03877d0-8c01-11e6-996c-525400b48521&action=cwa
```

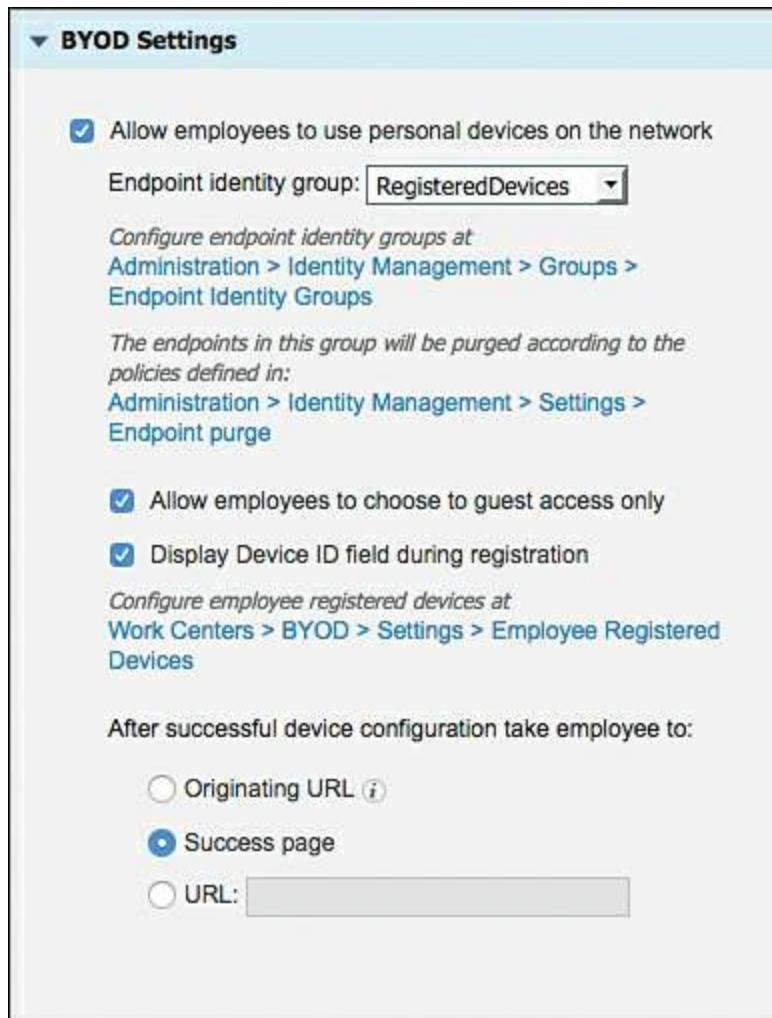
Figure 17-59 Cisco\_WebAuth

Now examine the Self-Registered Guest Portal to see how a guest portal ties into the BYOD flow:

**Step 1.** Navigate to Work Centers > Guest Access > Portals & Components > Guest Portals > Self-Registered Guest Portal (default).

**Step 2.** As shown in [Figure 17-60](#), the BYOD Settings section has a few items of note:

- Allow Employees to Use Personal Devices on the Network is the “make it work” option. In other words, it is what enables the BYOD flow for any non-guest users who authenticate to the WebAuth portal.
- Just as with the BYOD portal, the Endpoint Identity Group setting configures which endpoint identity group to automatically assign any endpoints to who go through this particular BYOD flow.
- Allow Employees to Choose to Guest Access Only provides an option for employees to click a button to choose guest-level access instead of going through the BYOD onboarding process. You saw this option back in [Figure 17-35](#) in the example of the Android device going through the dual-SSID flow.



**Figure 17-60** Self-Registered Guest Portal (Default): BYOD Settings

## Verify Default Unavailable Client Provisioning Policy Action

To address such situations, navigate to **Work Centers > BYOD > Settings > Client Provisioning** and click the Native Supplicant Provisioning Policy Unavailable drop-down list, as shown in [Figure 17-61](#). ISE offers two options:

- **Allow Network Access:** Users are allowed to register their device through the My Devices Portal and gain network access without having to install and launch a native supplicant wizard. This assumes the user will have to interact and configure the supplicant independently. This option is attractive if the end users are capable of requesting and installing their own certificates.
- **Apply Defined Authorization Policy:** Basically, this option leaves the client in the current state, which is a state of limited access. This is also the default setting.



**Figure 17-61** Default Unavailable Client Provisioning Policy Action

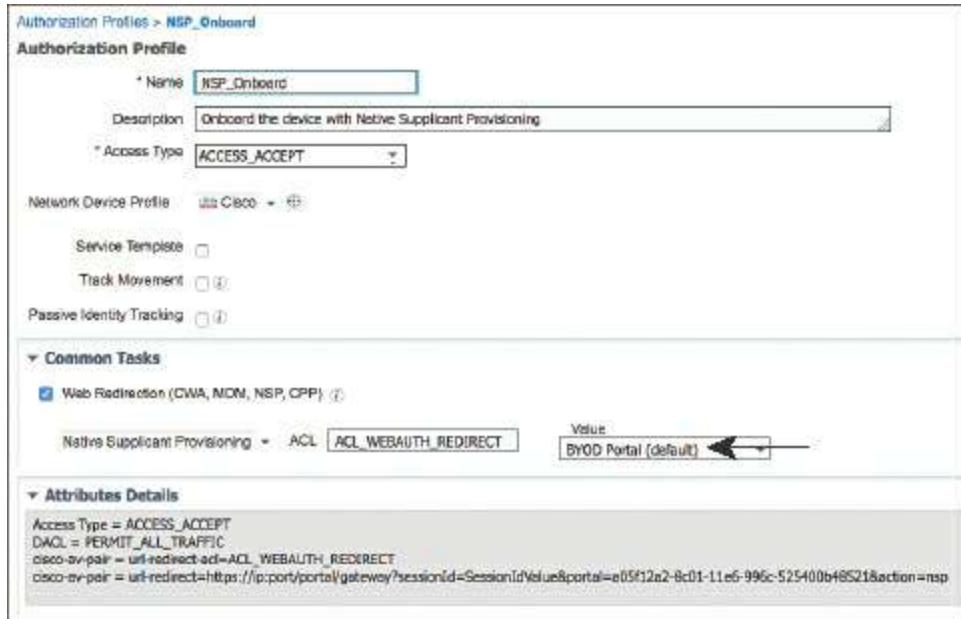
### Examine the Authorization Profiles

Although having the client provisioning policy is required, the authorization policy is still mission-critical. Without the properly configured authorization policy, there is no call to action that sends the endpoint over to the client provisioning portal. Of course, an authorization rule needs an authorization profile that includes that call to action.

Out of the box, there are two authorization profiles that contain the needed calls to action: NSP\_Onboard for the single-SSID flow and Cisco\_WebAuth for the dual-SSID flow. You have already examined the Cisco\_WebAuth authorization profile in the “BYOD and WebAuth Portals” section (refer to [Figure 17-59](#)), so now examine NSP\_Onboard:

**Step 1.** Navigate to **Work Centers > BYOD > Policy Elements > Results > Authorization > Authorization Profiles**.

**Step 2.** Edit the **NSP\_Onboard** authorization profile, as shown in [Figure 17-62](#). Note that this authorization profile is still using web authentication, but the portal is set to the BYOD Portal.



**Figure 17-62** NSP\_Onboard Authorization Profile

## Examine the Authorization Policy Rules

Now that you have seen the authorization profiles, take a look at all the relevant authorization rules that use those profiles for results. Out of the box, you can leverage the following three rules in the default authorization policy, shown in [Figure 17-63](#) and numbered for purposes of discussion:

Status	Rule Name	Conditions (Identity groups and other conditions)	Permissions	
Enabled	Wireless Black List Default	If: Blacklist AND Wireless_Access	Then: Blackhole_Wireless_Access	Edit   ▾
Enabled	Profiled Cisco IP Phones	If: Cisco_IP_Phone	Then: Cisco_IP_Phones	Edit   ▾
Enabled	Profiled Non Cisco IP Phone	If: Non_Cisco_Profiled_Phones	Then: Non_Cisco_IP_Phones	Edit   ▾
Enabled	Compliant_Devices_Access	If: Network_Access_Authentication_Passed AND Compliant_Devices	Then: PermitAccess	Edit   ▾
3	Employee_EAP-TLS	If: Wireless_802.1X AND BYOD_is_Registered AND EAP-TLS AND MAC_in_SAN	Then: PermitAccess AND BYOD	Edit   ▾
1	Employee_Onboarding	If: (Wireless_802.1X AND EAP-MSCHAPv2)	Then: NSP_Onboard AND BYOD	Edit   ▾
2	Wi-Fi_Guest_Access	If: Guest_Flow AND Wireless_MAB	Then: PermitAccess AND Guests	Edit   ▾
2	Wi-Fi_Redirect_to_Guest_Login	If: Wireless_MAB	Then: Cisco_WebAuth	Edit   ▾
Enabled	Basic_Authenticated_Access	If: Network_Access_Authentication_Passed	Then: PermitAccess	Edit   ▾
Enabled	Default	If no matches, then DenyAccess		Edit   ▾

**Figure 17-63** Default Authorization Policy

- The Employee\_Onboarding rule (1) is used for single-SSID onboarding. As shown in [Figure 17-63](#), the rule takes any incoming authorization where the method is wireless 802.1X and EAP-MSCHAPv2 and then sends that user to the BYOD portal to be onboarded. Once the onboarding is complete, ISE sends a CoA to trigger a reauthentication, and the new authentication from the endpoint uses the certificate (EAP-TLS), thereby landing on the Employee\_EAP-TLS rule (3), which provides full access.
- The Wi\_Fi\_Redirect\_to\_Guest\_Login rule (2) is the rule for dual-SSID

onboarding, as well as general guest access. As shown in [Figure 17-63](#), the rule takes any incoming authorization where wireless MAB is used, and sends the user to the guest portal. If the user who logs into that WebAuth portal is an employee, that user is sent through the BYOD flow as described earlier in the chapter. Once the onboarding is complete, ISE sends a CoA to trigger a reauthentication, and the new authentication from the endpoint uses the certificate (EAP-TLS), thereby landing on the Employee\_EAP-TLS rule (3), which provides full access.

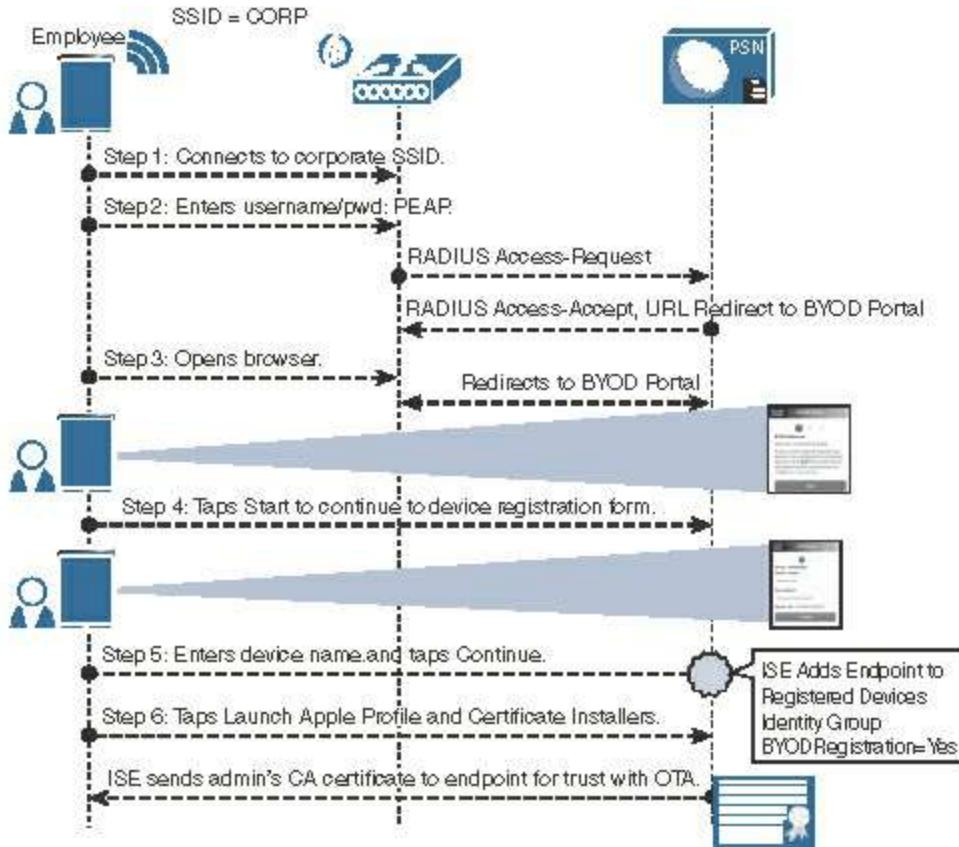
- The Employee\_EAP-TLS rule (3) is the final rule in the onboarding process. It is the end result of rules 1 and 2. As shown in [Figure 17-63](#), the rule has conditions set to match authorizations where wireless 802.1X with EAP-TLS is used, where the endpoint object in ISE's database has the BYOD registered flag enabled, and the endpoint's MAC address is also in the subject alternative name (SAN) field of the certificate. Only if all those conditions are met is the employee granted full access.

## **BYOD Onboarding Process Detailed**

Yes, this chapter is getting long, but there's a good chance you will find all of this information useful if you ever find yourself in a spot where you need to do troubleshooting of this process. You have seen that the user experience is simple and straightforward; the process behind the scenes, however, is complex.

## **iOS Onboarding Flow**

To examine, in detail, the experience with iOS devices and onboarding, the following onboarding flow focuses on a single SSID onboarding experience. The end user should have to complete only a few actions, as noted in [Figure 17-64](#), but all the items that occur behind the scenes are included to give you the full scope of the process.



**Figure 17-64** iOS Phase 1: Device Registration

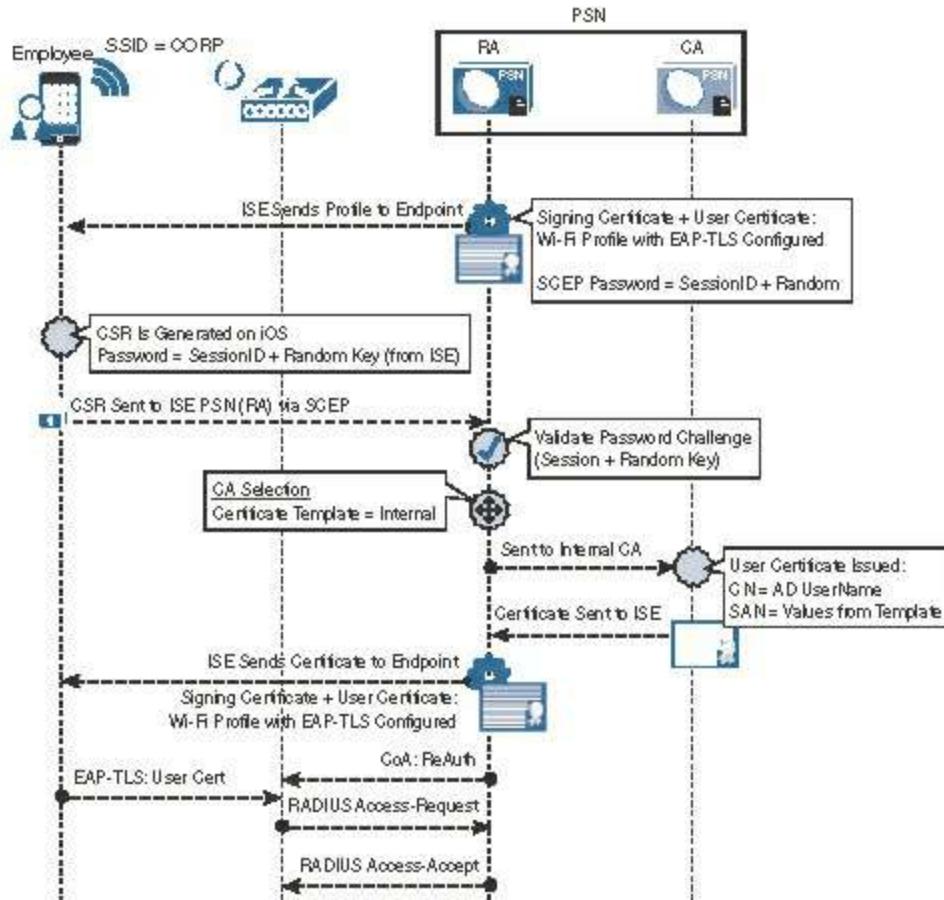
## Phase 1: Device Registration

1. A user joins the corporate SSID via his iOS device, and the iOS device prompts the user for credentials.
2. The user enters his AD username and password.
3. The EAP login request is sent to the wireless controller, which wraps the request in a RADIUS access-request packet to ISE.
4. The authorization result from ISE includes a URL redirection to the BYOD portal.
5. The user opens his web browser, which is redirected to the BYOD portal on ISE. The end user must tap Start to begin the onboarding process.
6. On the device registration page, the user completes the Device Name field and, optionally, the Description field. The user taps Continue, which causes ISE to do the following:
  - Set the BYODRegistration flag for the endpoint identity to Yes
  - Add the endpoint to the RegisteredDevices identity group
  - Send the admin's root CA certificate to the IOS device for it to trust for OTA provisioning
7. The user taps Launch Apple Profile and Certificate Installers Now.

## Phase 2: Device Enrollment and Provisioning

1. The device registration flag is set on the endpoint record in ISE's database.
2. ISE sends a profile to the iOS endpoint via OTA.
3. The profile instructs iOS to generate a certificate signing request (CSR) using the employee's credentials (given to iOS by ISE via the OTA service) as the certificate's common name in the subject, and the endpoint's MAC address as the Subject Alternative Name (SAN) field:
  - CN=Username
  - SAN=MAC-Address
4. The CSR is sent to ISE via SCEP, which is received by the registration authority (RA) function of the PSN. Since the request is for the internal CA, the RA uses an internal API to pass the certificate enrollment request to the endpoint CA function of the PSN.
5. The internal endpoint CA automatically issues the certificate.
6. The certificate is sent back to ISE, which sends it to the device through the OTA service. Included in that OTA profile is the Wi-Fi configuration, which details the SSID and to use EAP-TLS.
7. ISE sends a CoA to the NAD of the type ReAuth, which causes a new authentication.
8. The endpoint authenticates to the corporate SSID using the certificate via EAP-TLS.

[Figure 17-65](#) illustrates the transactions in Phase 2.



**Figure 17-65 iOS Phase 2: Device Enrollment**

## Android Flow

To detail the flow of onboarding with Android, the following onboarding flow uses the dual-SSID approach. Android is certainly capable of doing a single-SSID approach as well. The end user should have to complete only a few actions, as noted in [Figure 17-66](#), but all the items that occur behind the scenes are included to give you the full scope of the process.

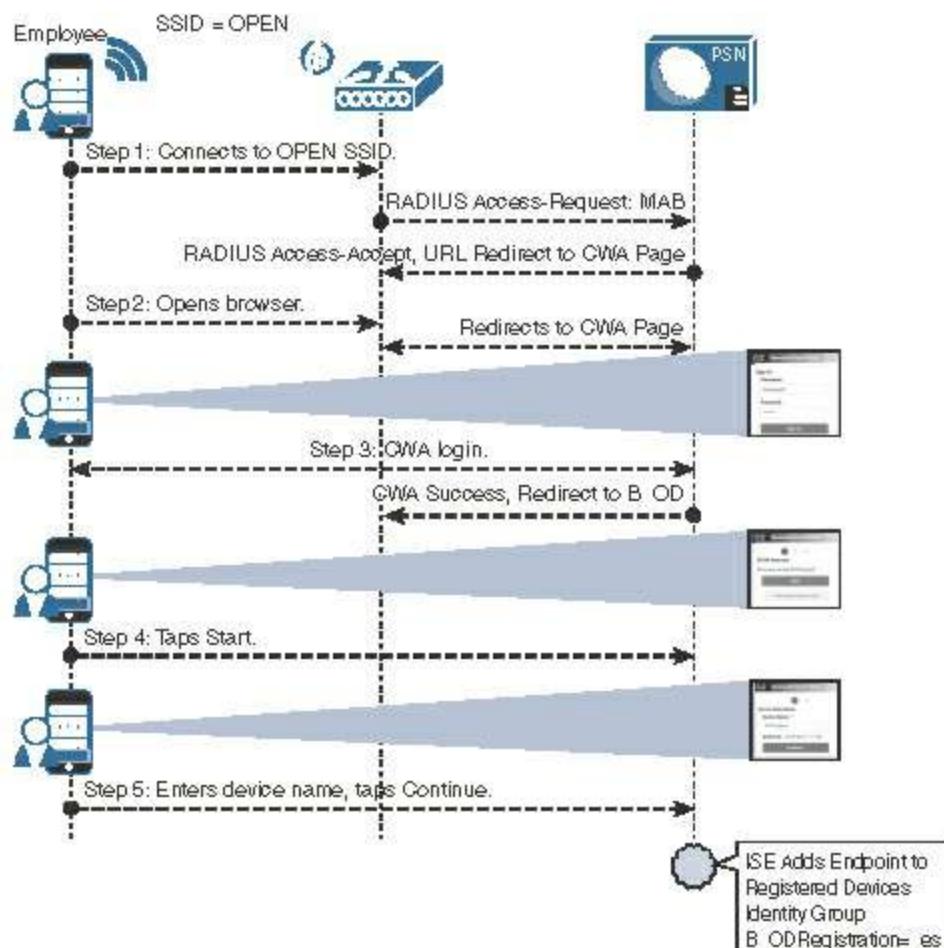
### Phase 1: Device Registration

1. A user joins the open SSID via her Android device, and the WLC sends a MAB request to ISE.
2. ISE sends a redirection to the Centralized Web Authentication portal.
3. The user opens a browser and is redirected to the CWA portal.
4. The user enters her AD username and password.
5. The successful WebAuth triggers a redirection, and the web page changes to the BYOD portal flow.
6. The user taps Start on the BYOD portal to begin the registration.
7. On the device registration page, the user completes the Device Name field and,

optionally, the Description field. The user taps Continue, which causes ISE to do the following:

- Set the BYODRegistration flag for the endpoint identity to Yes
- Add the endpoint to the RegisteredDevices identity group
- Set the Session:Device-OS attribute to Android (a temporary attribute used only for the provisioning process)
- Send a CoA to the WLC to apply the correct ACL that allows Google Play to access the Android device

[Figure 17-66](#) illustrates the transactions in Phase 1.



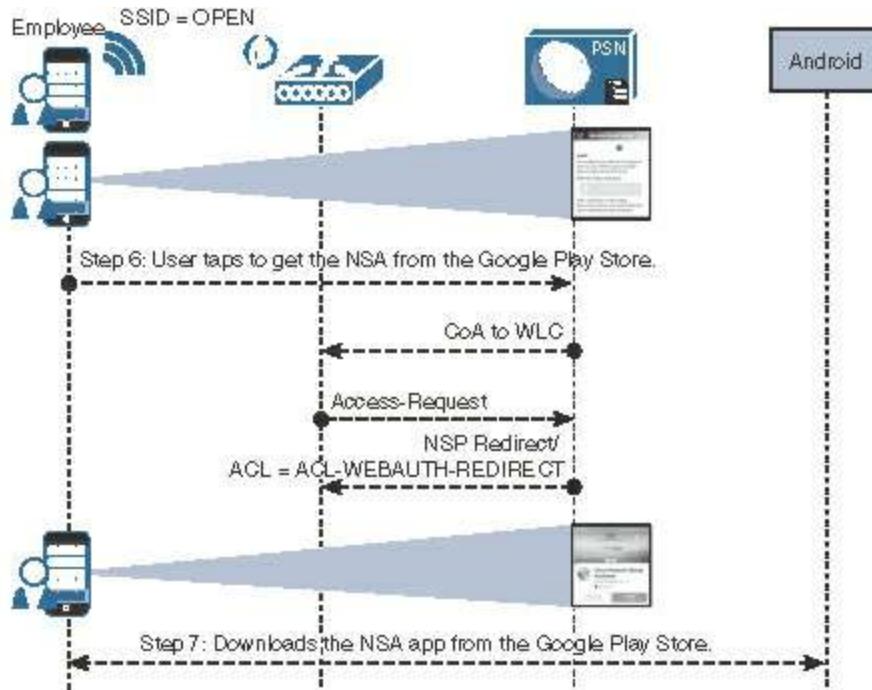
**Figure 17-66** Android Phase 1: Device Registration

## Phase 2: Download the NSA App

1. The CoA from phase 1 applied an ACL that permits traffic to Google Play.
2. The browser was automatically sent to Google Play and the Android device prompts the user to choose the Internet or Google Play to complete the request.
3. The user may be prompted to log in to Google Play.

- The user taps a button to install and/or open the Cisco Network Setup Assistant app.

[Figure 17-67](#) illustrates the transactions in Phase 2.



**Figure 17-67** Android Phase 2: Download NSA

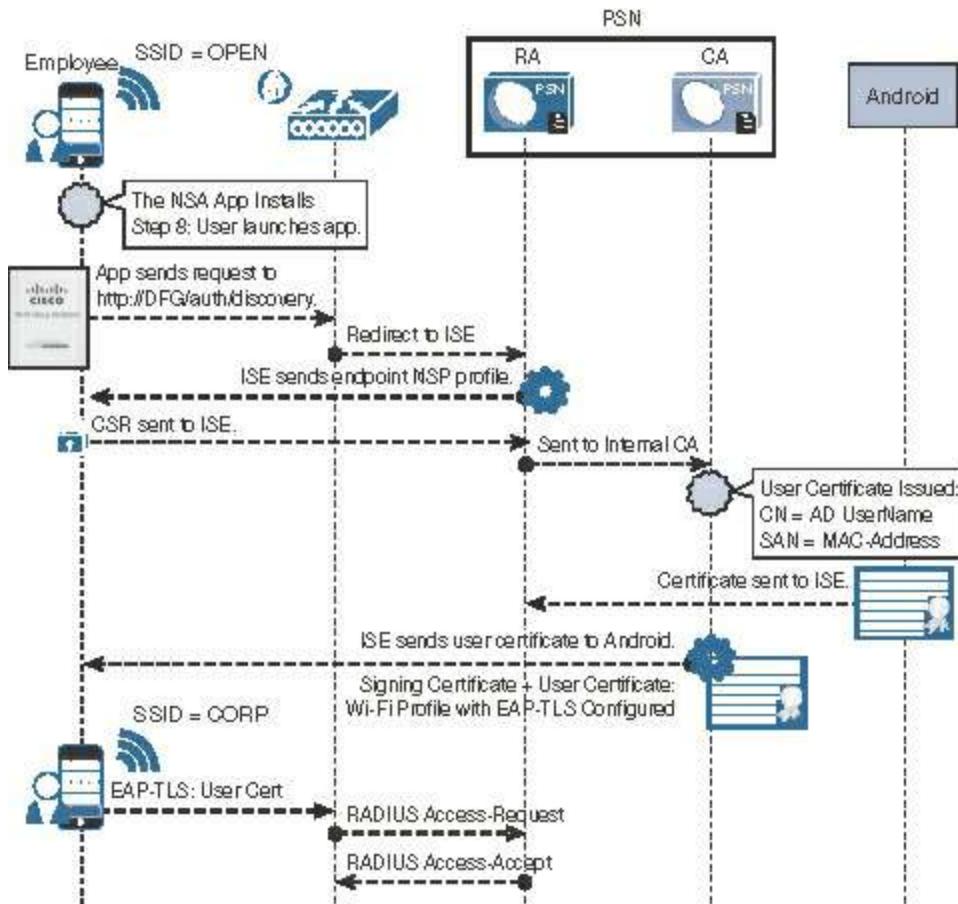
### Phase 3: Device Provisioning

- The Network Setup Assistant installs, and the user runs it.
- The NSA sends a discovery message to <http://default-gateway/auth/discovery>.
- The WLC redirects that HTTP message to the ISE native supplicant provisioning portal based on the URL-REDIRECT result within the authorization from ISE.
- ISE sends the Android profile based on the native supplicant profile to the endpoint.
- NSA generates the certificate signing request (CSR), using the employee's credentials as the certificate's subject, and the MAC address as the Subject Alternative Name (SAN) field:
  - CN=Username
  - SAN=MAC-Address
- The CSR is sent to the ISE PSN's registration authority (RA) function, which in turn sends the certificate enrollment request to the endpoint CA function.
- The CA automatically issues the certificate.
- The certificate is sent back to ISE, which sends it to the NSA app. Included in the

NSA profile is the Wi-Fi configuration, which details the SSID and to use EAP-TLS.

9. The NSA app connects the endpoint to the corporate SSID and ISE sends a CoA to the NAD of the type ReAuth, which also causes a new authentication.
  10. The endpoint authenticates to the corporate SSID using the certificate via EAP-TLS.

[Figure 17-68](#) illustrates the transactions in Phase 3.



**Figure 17-68** Android Phase 3: Device Provisioning

# Windows and Mac OS X Flow

Mac OS X and Windows both use a wizard to accomplish the onboarding and provisioning. It is downloaded as a Microsoft Installer (.msi) file for Windows and a disk image (.dmg) file containing a native application for macOS. Both are named the Cisco native supplicant provisioning wizard. The wizard takes care of triggering the CSR from the OS and installing the supplicant profile, and it works very similarly to the way Android provisioning functions. One key difference is that the wizard downloads directly from ISE for Windows and macOS.

## MDM Onboarding

Many organizations use mobile device management (MDM) solutions. These solutions provide endpoint management for a plethora of devices. They help enforce specific security requirements, such as endpoint encryption, PIN lock, jail-break detection, remote wipe capabilities, application whitelisting, application blacklisting, and more. Many MDMs even provision supplicants and certificates to devices as part of their management package.

In the past, the MDM solutions had some drawbacks. With a typical solution, a user who brought in a mobile device and wanted to gain access to the network had to call the help desk and receive instructions on how to onboard the device with the MDM solution. There were some significant downsides to this process, such as:

- Users were required to manually connect to the MDM solution to begin the onboarding process.
- It lacked enforcement to help “steer” the user toward that solution.
- An MDM license was required for every device the organization would provision and allow to have network access, which often was cost-prohibitive.

Cisco and the MDM vendors recognized these drawbacks presented a beneficial and strategic opportunity. The MDM vendors possessed the mobile device-management capabilities, and Cisco had the onboarding, network access policy, and enforcement mechanisms. Since ISE 1.2, ISE has integrated with the industry’s leading MDM vendors. Solutions include, but are not limited to

- Cisco Meraki Systems Manager
- VMware AirWatch
- MobileIron
- Citrix ZenMobile
- Good Technology (acquired by BlackBerry in October 2016)
- Jamf
- SAP Afaria

All 20 or so supported vendors have implemented an API written by Cisco to enable scalable bidirectional communication between their solutions and ISE.

## Integration Points

The API enables ISE to use MDM attributes in the authorization policies. The authorization can either use a macro-level attribute stating that the device is in compliance with the MDM policy or use micro-level attributes, such as jail break

status, PIN lock, or even endpoint encryption.

[Table 17-1](#) documents the possible MDM attribute values, provides a definition of each value, and lists the possible values for each attribute.

MDM Attribute	Definition	Possible Values
DeviceRegisterStatus	Indicates whether the device is registered with the MDM.	Unregistered Registered
DeviceComplianceStatus	Macro-level attribute that indicates whether the device meets the security policy of the MDM.	NonCompliant Compliant
DiskEncryptionStatus	Indicates whether encryption is enabled on the storage of the device.	On Off
PinLockStatus	Specifies whether the device has an automatic lock, requiring a PIN or password to unlock the device.	On Off
JailBrokenStatus	Indicates whether the device been jail broken.	Unbroken Broken
Manufacturer	Identifies the manufacturer of the device.	Text field or can be compared to attribute from AD/LDAP
Model	Identifies the model of the device.	Text field or can be compared to attribute from AD/LDAP
IMEI	Identifies the unique ID of the device.	Text field or can be compared to attribute from AD/LDAP
SerialNumber	Identifies the serial number of the device.	Text field or can be compared to attribute from AD/LDAP
OSVersion	Identifies the version of the operating system.	Text field or can be compared to attribute from AD/LDAP
PhoneNumber	Identifies the phone number.	Text field or can be compared to attribute from AD/LDAP

DaysSinceLastCheckIn	Indicates how many days have passed since the endpoint has called home to the MDM.	Text field or can be compared to attribute from AD/LDAP
MDMServerReachable	Defines the MDM status which may be used as part of policy evaluation, so that endpoints may fall through to a rule if MDM is not reachable.	Drop-down selection, Reachable or Unreachable
MDMFailureReason	Identifies the reason that an MDM server might not be reached. The reason for the failure can be leveraged in a policy decision.	Text field or can be compared to attribute from AD/LDAP
MDMServerName	Identifies which MDM server was leveraged. Because ISE may connect to multiple MDMs simultaneously, this attribute can be used to uniquely identify a specific connection.	Drop-down list of configured MDMs

**Table 17-1** MDM Attributes

## Configuring MDM Integration

Before you configure ISE to communicate with the MDM, ISE needs to trust the certificate of the MDM for the SSL-encrypted communications. You can accomplish this by using the following steps:

**Step 1.** Navigate to **Administration > System > Certificates**.

**Step 2.** Choose **Trusted Certificates**.

**Step 3.** Import the certificate of the MDM as a trusted certificate, as shown in [Figure 17-69](#), and click **Submit**.

**Import a new Certificate into the Certificate Store**

* Certificate File	<input type="button" value="Browse..."/> *.meraki.com.crt
Friendly Name	Meraki EMM Certificate
Trusted For: <small>(i)</small>	
<input checked="" type="checkbox"/> Trust for authentication within ISE	
<input type="checkbox"/> Trust for client authentication and Syslog	
<input type="checkbox"/> Trust for authentication of Cisco Services	
<input type="checkbox"/> Validate Certificate Extensions	
Description	<input type="text"/>
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

**Figure 17-69** Importing the MDM Certificate

Now that the certificate is trusted, add the MDM server to ISE. You can configure and use multiple MDMs. For example, you may have an operation in Germany that requires its own MDM instance, separate from the ones that the rest of the company uses. To add an MDM to ISE:

**Step 4.** Navigate to **Administration > Network Resources > External MDM**.

**Step 5.** Click **Add**.

**Step 6.** In the Name field, enter a name for the connection to the MDM.

**Step 7.** From the Server Type drop-down list, choose **Mobile Device Management**.

**Step 8.** From the Authentication Type drop-down list, choose **Basic**.

**Step 9.** In the Host Name/IP Address field, enter the hostname of the server.

**Step 10.** In the Port field, set the port to **443**, unless otherwise instructed by your MDM vendor.

**Step 11.** (Optional) In the Instance Name field, if the vendor is multitenant-aware, enter the instance name.

**Step 12.** In the Username and Password fields, enter the username and password for the MDM API authentication.

**Step 13.** (Optional) Add a description.

**Step 14.** Set the Polling Interval to **240** minutes.

**Step 15.** Click **Test Connection** to test the connectivity.

**Step 16.** Click **Save**.

[Figure 17-70](#) shows the successful addition of the MDM.

The screenshot shows the 'MDM Servers > MerakiEMM' configuration page. The form fields are as follows:

- Name: MerakiEMM
- Server Type: Mobile Device Manager
- Authentication Type: Basic
- Host Name / IP Address: n196.meraki.com
- Port: 443 (max length: 5)
- Instance Name: (empty)
- Username: 895b69483e7ca4f0eea93933810007d5
- Password: (redacted)
- Description: Meraki EMM
- Polling Interval: 240 (minutes)
- Status: Enabled

At the bottom are 'Test Connection' and 'Save' buttons.

**Figure 17-70** Adding an MDM

## Configuring MDM Onboarding Policies

The MDM onboarding is configured much like the ISE BYOD onboarding. The authorization rules need to be configured to redirect the endpoint to MDM onboarding if it meets specific requirements.

One example of where to place an MDM onboarding policy is just below the BYOD onboarding rules but above the rule that would permit final access. Some organizations

do not want to send all devices to the MDM, but prefer that specific devices be included. One way to achieve this is to maintain a separate list of MAC addresses belonging to corporate-owned assets and add that list to an endpoint identity group. The example shown in [Figure 17-71](#) does not use identity groups, but it represents a policy that has been used in production at a number of installs.

	Emp_TLS_MDM_OnBoard	If (Wireless_802.1X AND BYOD_Is_Registered AND EAP-TLS AND MAC_In_SAN AND MDM:DeviceRegisterStatus EQUALS UnRegistered AND MDM:MDMServerReachable EQUALS Reachable)	Then MerakiOnboard AND BYOD	←
	Employee_EAP-TLS	If (Wireless_802.1X AND BYOD_Is_Registered AND EAP-TLS AND MAC_In_SAN)	Then PermitAccess AND BYOD	
	Employee_Onboarding	If (Wireless_802.1X AND EAP-MSCHAPv2)	Then NSP_Onboard AND BYOD	

**Figure 17-71** MDM Authorization Rule Example

The first step is to create the authorization profile that redirects the endpoint to the MDM for onboarding:

**Step 1.** Navigate to **Work Centers > BYOD > Policy Elements > Results > Authorization Profiles**.

**Step 2.** In the Name field, enter a name for the new authorization profile ([Figure 17-72](#) uses the example MerakiOnboard).

Authorization Profiles > **MerakiOnboard**

**Authorization Profile**

* Name	<input type="text" value="MerakiOnboard"/>
Description	<input type="text"/>
* Access Type	<input type="button" value="ACCESS_ACCEPT"/>
Network Device Profile	Cisco <input type="button" value="+"/>
Service Template	<input type="checkbox"/>
Track Movement	<input type="checkbox"/>
Passive Identity Tracking	<input type="checkbox"/>

**Common Tasks**

Web Redirection (CWA, MDM, NSP, CPP)

MDM Redirect	<input type="button" value="ACL"/> <input type="text" value="ACL_WEBAUTH_REDIRECT"/>	Value <input type="button" value="MDM Portal (default)"/>	MDM Server <input type="text" value="MerakiEMM"/>
--------------	--	---	---

**Attributes Details**

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-aci=ACL_WEBAUTH_REDIRECT
cisco-av-pair = url-redirect=https://ip:port/mdmportal/gateway?sessionId=SessionIdValue&portal=a0931af0-8c01-11e6-996c-525400b48521&
mdmServerId=f7f1ff20-b774-11e6-b67a-0242dc74a909&action=mdm
```

**Figure 17-72** MerakiOnboard Authorization Profile

**Step 3.** From the Access Type drop-down list, choose **Access-Accept**.

**Step 4.** From the Web Redirection drop-down list, choose **MDM Redirect**.

**Step 5.** For the Web Redirection ACL, reference an ACL that permits access to the MDM and ISE, but denies access to the rest of the Internet.

**Step 6.** Click **Save**.

Now, create an authorization rule to send endpoints to the MDM for onboarding:

**Step 1.** Navigate to **Work Centers > Network Access > Policy Sets**.

**Step 2.** Duplicate the Employee\_EAP-TLS rule above the original rule.

**Step 3.** Name the rule (our example is named Emp\_TLS\_MDM\_OnBoard).

**Step 4.** Add the conditions, as follows:

- MDM:DeviceRegistrationStatus EQUALS Unregistered
- MDM: MDMServerReachable EQUALS Reachable

**Step 5.** Set the result to the **MDM Onboard Authorization Profile**.

**Step 6.** Click **Done**.

Duplicate the rule below so that it permits access to devices that are registered and meet the MDM compliance.

**Step 7.** Navigate to **Work Centers > Network Access > Policy Sets**.

**Step 8.** Duplicate the rule below it that permits access to devices that are registered and meet the MDM compliance.

**Step 9.** Name the rule **MDM Permit**.

**Step 10.** Modify the MDM:DeviceRegistrationStatus to be **Registered**.

**Step 11.** Add the condition MDM:DeviceComplianceStatus EQUALS Compliant.

**Step 12.** Set the Result to **Permit Access**.

**Step 13.** Click **Done**.

**Step 14.** Click **Save**. [Figure 17-73](#) shows the final authorization policy.

<input checked="" type="checkbox"/> Emp_TLS_MDM_OnBoard	if	(Wireless_802.1X AND BYOD_is_Registered AND EAP-TLS AND MAC_in_SAN AND MDM:DeviceRegisterStatus EQUALS UnRegistered AND MDM:MDMServerReachable EQUALS Reachable )	then	MerakiOnboard AND BYOD
<input checked="" type="checkbox"/> Emp_TLS_MDM_Compliant	if	(Wireless_802.1X AND BYOD_is_Registered AND EAP-TLS AND MAC_in_SAN AND MDM:DeviceRegisterStatus EQUALS Registered AND MDM:MDMServerReachable EQUALS Reachable AND MDM:DeviceCompliantStatus EQUALS Compliant )	then	PermitAccess AND BYOD
<input checked="" type="checkbox"/> Employee_EAP-TLS	if	(Wireless_802.1X AND BYOD_is_Registered AND EAP-TLS AND MAC_in_SAN )	then	PermitAccess AND BYOD

**Figure 17-73 MDM Rules in the Authorization Policy**

## The Opposite of BYOD: Identify Corporate Systems

For many years, customers have voiced their business need to identify the machine as an authorized asset, in addition to the user being an authorized user. Given that Microsoft Windows has both a user and a machine state, it allows the device to be authenticated to the network with what is commonly known as machine auth, as well as the ability to have the interactive user authenticated to the network.

The issue is that EAP was always designed to transport a single credential. The machine authentication occurs when there is no interactive user or if the supplicant profile is configured to only issue the machine's credentials. When the user logs into the system, it changes to a user state and issues the credentials associated to the user. With standard RADIUS and standard EAP, there was no way to join those authentications together.

To answer the issue, Cisco enhanced EAP-FAST with the capability to do EAP chaining. EAP chaining is the ability to authenticate both the machine and the user within the same authentication session. EAP-FASTv2 is being standardized on and should be known as EAP-TEAP when it finalizes standardization.

## EAP Chaining

With EAP-FASTv2 and EAP chaining, both the machine and the user are issued a Protected Access Credential (PAC), similar to a secure cookie. So, ISE may request the machine PAC during the user authentication process, and the authorization policy is capable of using the results of either or both authentications.

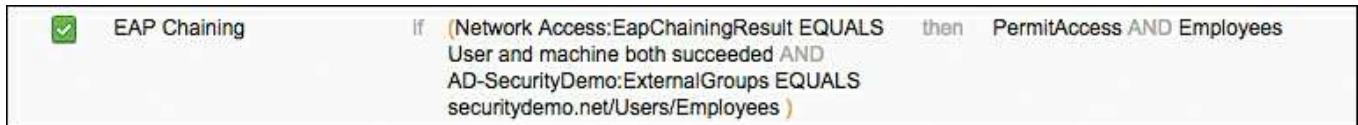
The authorization condition is NetworkAccess:EAPChainingResult, and the options are as follows:

- No chaining
- User and machine both failed
- User and machine both succeeded

- User failed and machine succeeded
- User succeeded and machine failed

With that level of flexibility and authorization, a result may be provided that permits limited access to remediate a single failure, no access if neither succeeds, and full access if both succeed.

[Figure 17-74](#) shows an example authorization rule that uses EAP chaining.



**Figure 17-74** EAP Chaining Authorization Rule Example

A practical example from a customer was to use EAP chaining to identify corporate-owned and-managed devices. The authorization rule acted like this:

If  
 the device and user authentication both succeed  
 and the endpoint posture is compliant  
 and the user is a member of the PCI group in Active Directory  
 and the location of the endpoint is on a corporate campus  
 Then  
 permit full access  
 and assign the PCI Security Group Tag (SGT)

That authorization rule allows only those devices to communicate to the servers housing credit card data.

EAP chaining is part of RFC 7170 (TEAP) along with a slew of other secure networking enhancements. As of this writing, many vendors are in the process of incorporating TEAP into their products, but none were in production.

## Summary

This chapter took an in-depth look at BYOD onboarding and MDM integration. It provided a brief look at identifying corporate assets and users with EAP chaining. The next chapter focuses on distributed ISE deployments.

# Chapter 18 Setting Up and Maintaining a Distributed ISE Deployment

This chapter covers the following topics:

- Configuring ISE nodes in a distributed environment
- Understanding the HA options available
- Using load balancers
- IOS load balancing
- Maintaining ISE deployments

[Chapter 5](#), “[Making Sense of the ISE Deployment Design Options](#),” discussed the many options within ISE design. At this point, you should have an idea of which type of deployment will be the best fit for your environment, based on the number of concurrent endpoints and the number of Policy Service Nodes (PSN) that will be used in the deployment. This chapter focuses on the configuration steps required to deploy ISE in a distributed design. It also covers the basics of using a load balancer and includes a special bonus section on a very cool high-availability (HA) configuration that uses Anycast routing, and covers patching distributed ISE deployments.

## Configuring ISE Nodes in a Distributed Environment

All ISE nodes are installed in a standalone mode by default. When in a standalone mode, the ISE node is configured to run all personas by default. That means that the standalone node runs Administration, Monitoring, and Policy Service personas. Also, all ISE standalone nodes are configured as their own root certificate authority (CA).

It is up to you, the ISE administrator, to promote the first node to be a primary administration node and then join the additional nodes to this new deployment. At the time of joining, you also determine which services will run on which nodes; in other words, you determine which persona the node will have.

You can join more than one ISE node together to create a multinode deployment, known commonly in the field as an ISE cube. It is important to understand that before any ISE nodes can be joined together, they must trust each other’s administrative certificate. Without that trust, you will receive a communication error stating that the “node was unreachable,” but the root cause is the lack of trust.

Similar to a scenario of trying to connect to a secure website that is not using a trusted certificate, you would see an SSL error in your web browser. This is just like that, only it is based on Transport Layer Security (TLS).

If you are still using the default self-signed certificates in ISE, you’ll be required to import the public certificate of each ISE node into each other ISE node’s

**Administration > System > Certificates > Trusted Certificates** screen, because they are all self-signed (untrusted) certificates and each ISE node needs to trust the primary node, and the primary node needs to trust each of the other nodes.

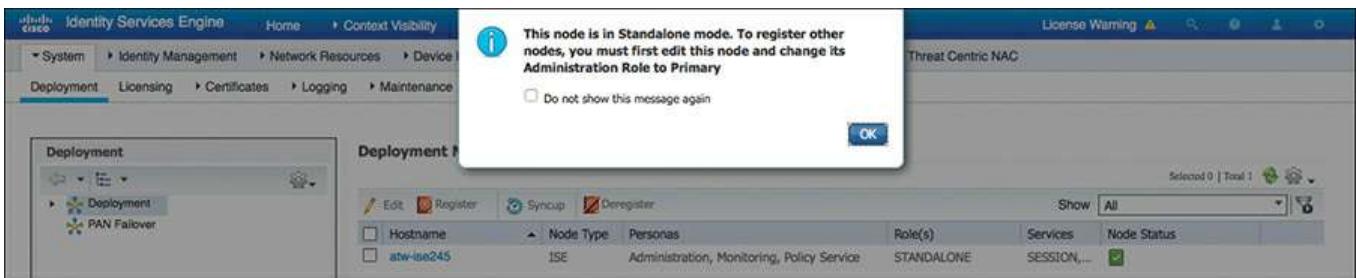
Instead of dealing with all this public key import for these self-signed certificates, the best practice is to always use certificates issued from the same trusted source. In that case, only the root certificates need to be added to the Trusted Certificates list.

## Make the Policy Administration Node a Primary Device

Because all ISE nodes are standalone by default, you must first promote the ISE node that will become the Primary Policy Administration Node (PAN) to be a primary device instead of a standalone.

From the ISE GUI, perform the following steps:

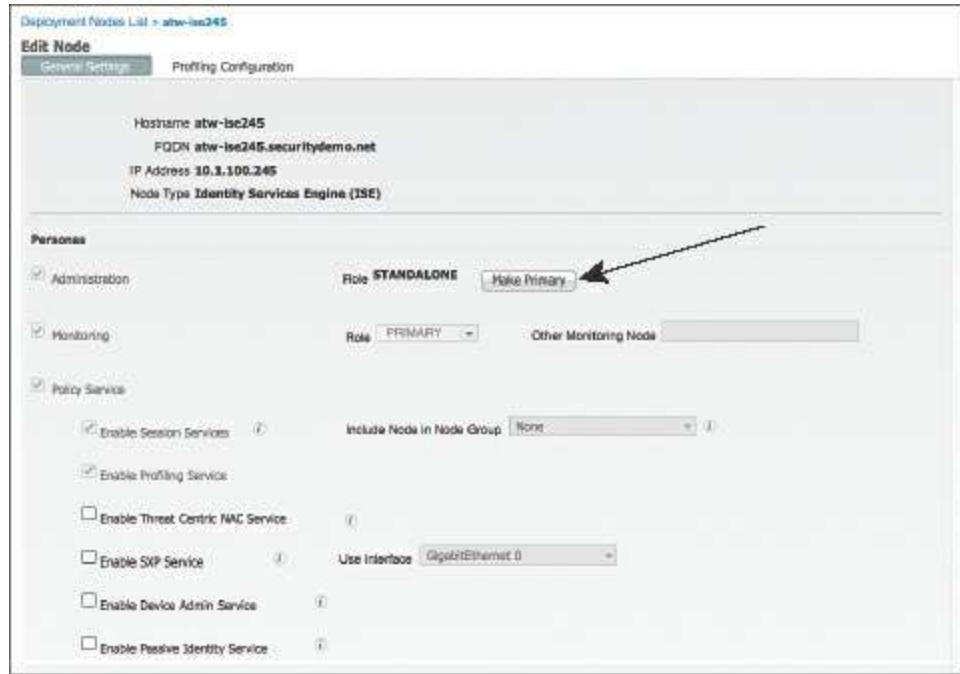
**Step 1.** Choose **Administration > System > Deployment**. [Figure 18-1](#) shows an example of the Deployment screen.



**Figure 18-1** Deployment Screen

**Step 2.** Select the ISE node (there should only be one at this point).

**Step 3.** Click the **Make Primary** button, as shown in [Figure 18-2](#).



**Figure 18-2** Make Primary Button

**Step 4.** At this point, the Monitoring and Policy Service check boxes on the left have become selectable. If the primary node will not also be providing any of these services, uncheck them now. (You can always return later and make changes.)

**Step 5. Click Save.**

After saving the changes, the ISE application restarts itself. This is a necessary process, as the sync services are started and the node prepares itself to handle all the responsibilities of the primary PAN persona. Once the application server has restarted, reconnect to the GUI, log in again, and proceed to the next section.

**Note** You can monitor the status of the application server by using the **show application status ise** command from the command-line interface through either the console or a Secure Shell (SSH) session to the ISE node, as shown in Example 18-1. When the application server state changes from initializing to running, then ISE will be ready for you to log in to.

**Example 18-1** **show application status ise** Command Output

[Click here to view code image](#)

```
atw-ise245/admin# show application status ise
```

ISE PROCESS NAME	STATE	PROCESS ID
Database Listener	running	5851
Database Server	running	75 PROCESSES
Application Server	initializing	
Profiler Database	running	6975
ISE Indexing Engine	running	1821
AD Connector	running	10338
M&T Session Database	running	1373
M&T Log Collector	running	2313
M&T Log Processor	running	2219
Certificate Authority Service	disabled	
EST Service	disabled	
SXP Engine Service	disabled	
TC-NAC Docker Service	disabled	
TC-NAC MongoDB Container	disabled	
TC-NAC RabbitMQ Container	disabled	
TC-NAC Core Engine Container	disabled	
VA Database	disabled	
VA Service	disabled	
pxGrid Infrastructure Service	disabled	
pxGrid Publisher Subscriber Service	disabled	
pxGrid Connection Manager	disabled	
pxGrid Controller	disabled	
PassiveID Service	disabled	
DHCP Server (dhcpd)	disabled	
DNS Server (named)	disabled	

```
atw-ise245/admin#
```

## Register an ISE Node to the Deployment

Now that there is a primary PAN, you can implement a multinode deployment. From the GUI on the primary PAN, you will register and assign personas to all ISE nodes.

From the ISE GUI on the primary PAN, perform the following steps:

**Step 1.** Choose **Administration > System > Deployment**.

**Step 2.** Choose **Register > Register an ISE Node**, as shown in [Figure 18-3](#).

**Note** As with all other operations with ISE, DNS is a critical component.



**Figure 18-3** Choosing to Register an ISE Node

**Step 3.** In the Host FQDN field, enter the IP address or DNS name of the first ISE node you will be joining to the deployment, as shown in [Figure 18-4](#).

A screenshot of a registration form titled 'Register ISE Node - Step 1: Specify Node Host FQDN (hostname.domain-name) and Credentials'. The form has three input fields: 'Host FQDN' containing 'atw-ise244.securitydemo.net', 'User Name' containing 'admin', and 'Password' (redacted). Below the fields are 'Next' and 'Cancel' buttons.

**Figure 18-4** Specifying Hostname and Credentials

**Step 4.** In the User Name and Password fields, enter the administrator name (admin by default) and password.

**Step 5.** Click **Next**.

**Note** If you have not installed valid certificates from a trusted root, you will receive an error. You'll be required to install the certificate of each ISE node as a trusted root, because they are all self-signed certificates. Best practice is to always use certificates issued from a trusted source.

**Step 6.** On the Configure Node screen, shown in [Figure 18-5](#), you can pick the main

persona of the ISE node, including enabling of profiling services. You cannot, however, configure which probes to enable yet. Choose the persona for this node. [Figure 18-5](#) shows adding a secondary Administration and Monitoring node, while [Figure 18-6](#) shows adding a Policy Service Node.

Deployment Nodes List > **Configure Node**  
Register ISE Node - Step 2: Configure Node  
**General Settings**

Hostname **atw-ise244**  
FQDN **atw-ise244.securitydemo.net**  
IP Address **10.1.100.244**  
Node Type **Identity Services Engine (ISE)**

**Personas**

Administration      Role **SECONDARY**

Monitoring      Role **SECONDARY** ▾      Other Monitoring Node **atw-ise245**

Policy Service

Enable Session Services      ⓘ      Include Node in Node Group **None** ▾ ⓘ

Enable Profiling Service

Enable Threat Centric NAC Service      ⓘ

Enable SXP Service      ⓘ      Use Interface **GigabitEthernet 0** ▾ ⓘ

Enable Device Admin Service      ⓘ

Enable Passive Identity Service      ⓘ

pxGrid      ⓘ

**Submit** **Cancel**

**Figure 18-5** Configure Node Screen Secondary Admin and MnT Addition

18

Deployment Nodes List > **Configure Node**

Register ISE Node - Step 2: Configure Node

**General Settings**

Hostname **atw-ise246**  
FQDN **atw-ise246.securitydemo.net**  
IP Address **10.1.100.246**  
Node Type **Identity Services Engine (ISE)**

**Personas**

Administration      Role **SECONDARY**

Monitoring      Role **SECONDARY** ▾      Other Monitoring Node

Policy Service

Enable Session Services (i)      Include Node in Node Group  ▾ (i)

Enable Profiling Service

Enable Threat Centric NAC Service (i)

Enable SXP Service (i)      Use Interface  ▾ (i)

Enable Device Admin Service (i)

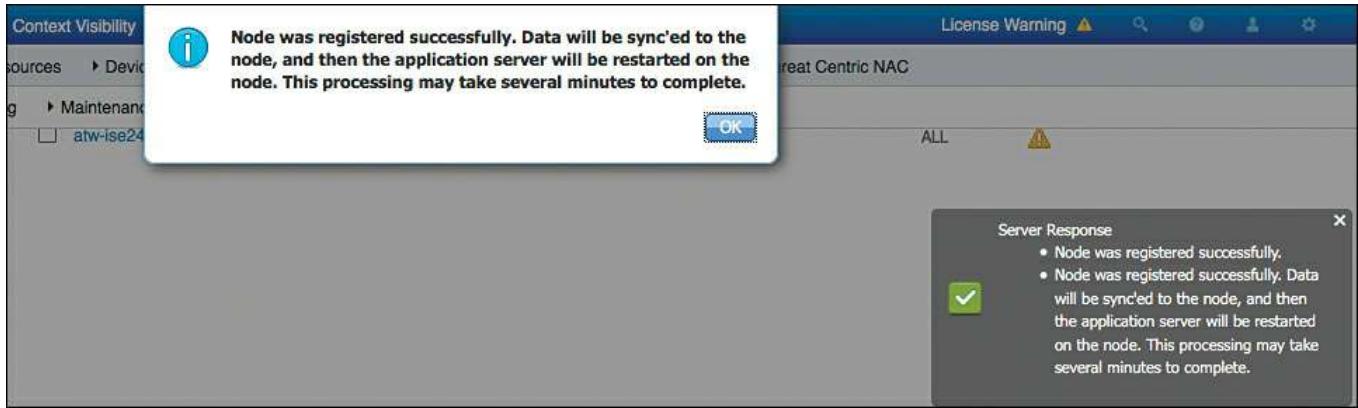
Enable Passive Identity Service (i)

pxGrid (i)

**Submit** **Cancel**

**Figure 18-6** Configure Node Screen Policy Service Node Addition

**Step 7.** Click **Submit**. At this point, the Policy Administration Node syncs the entire database to the newly joined ISE node, as you can see in [Figure 18-7](#).



**Figure 18-7 Sync Initiated**

**Step 8.** Repeat these steps for all the ISE nodes that should be joined to the same deployment.

## Ensure the Persona of All Nodes Is Accurate

Now that all of your ISE nodes are joined to the deployment, you can ensure that the correct personas are assigned to the appropriate ISE nodes. [Table 18-1](#) shows the ISE nodes in the sample deployment and the associated persona(s) that will be assigned.

[Figure 18-8](#) shows the final Deployment screen, after the synchronization has completed for all nodes (a check mark in the Node Status column indicates a node that is healthy and in sync).

Deployment Nodes						
	Hostname	Node Type	Personas	Role(s)	Services	Node Status
<input type="checkbox"/>	atw-ise244	ISE	Administration, Monitoring	SEC(A), SEC(M)	NONE	<input checked="" type="checkbox"/>
<input type="checkbox"/>	atw-ise245	ISE	Administration, Monitoring	PRI(A), PRI(M)	NONE	<input checked="" type="checkbox"/>
<input type="checkbox"/>	atw-ise246	ISE	Policy Service		ALL	<input checked="" type="checkbox"/>
<input type="checkbox"/>	atw-ise247	ISE	Policy Service		IDENTITY MAPPING, SESSION, PROFILER, DEVICE ADMIN	<input checked="" type="checkbox"/>

**Figure 18-8 Final Personas and Roles**

**Note** This is also a good time to double-check that all the desired probes are enabled on the PSNs.

ISE Node	Persona
atw-ise244	Administration, Monitoring
atw-ise245	Administration, Monitoring
atw-ise246	Policy Service
atw-ise247	Policy Service

**Table 18-1** ISE Nodes and Personas

## Understanding the HA Options Available

There are many different items to note when it comes to high availability (HA) within a Secure Access deployment. There are the concerns of communication between the PANs and the other ISE nodes for database replications and synchronization, and communication between the PSNs and Monitoring nodes for logging. There is also the issue of authentication sessions from the network access devices (NAD) reaching the PSNs in the event of a WAN outage, as well as a NAD recognizing that a PSN may no longer be active, and sending authentication requests to the active PSN instead.

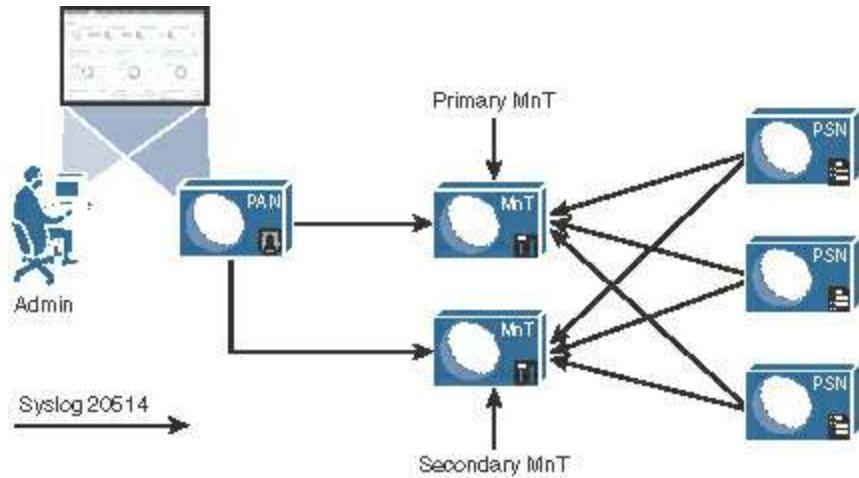
## Primary and Secondary Nodes

PANs and Monitoring & Troubleshooting (MnT) nodes both employ the concept of primary and secondary nodes, but they operate very differently. Let's start with the easiest one first, the MnT node.

## Monitoring & Troubleshooting Nodes

As you know, the MnT node is responsible for the logging and reporting functions of ISE. All PSNs will send their logging data to the MnT node as syslog messages (UDP port 20514).

When there are two monitoring nodes in an ISE deployment, all ISE nodes send their audit data to both monitoring nodes at the same time. [Figure 18-9](#) displays this logging flow.



**Figure 18-9 Logging Flows**

The active/active nature of the MnT nodes can be viewed easily in the administrative console, as the two MnTs get defined as LogCollector and LogCollector2. [Figures 18-10](#) and [18-11](#) display the log collector definitions and the logging categories, respectively.

Name	IP Address	Port	Type	Description	Status
LogCollector	10.1.100.245	20514	UDP SysLog	Syslog Target for Log Collector	<input checked="" type="checkbox"/> Enabled
LogCollector2	10.1.100.244	20514	SysLog	Second Syslog Target for Log Collector	<input checked="" type="checkbox"/> Enabled
ProfilerRadiusProbe	127.0.0.1	30514	Profiler SysLog	Syslog Target for Profiler RADIUS Probe	<input checked="" type="checkbox"/> Enabled
TCPLogCollector	10.1.100.245	1468	TCP SysLog	TCP SysLog collector	<input type="checkbox"/> Disabled

**Figure 18-10 Logging Targets**

Logging Categories					
Selected 0   Total 28					
		Category	Targets	Severity	Local Log Level
<input type="radio"/>	AAA Audit	AAA Audit	LogCollector,LogCollector2	INFO	enable
<input type="radio"/>		Failed Attempts	LogCollector,ProfilerRadiusProbe,Log...	INFO	enable
<input type="radio"/>		Passed Authentications	LogCollector,ProfilerRadiusProbe,Log...	INFO	disable
<input type="radio"/>	AAA Diagnostics	AAA Diagnostics	LogCollector,LogCollector2	WARN	enable
<input type="radio"/>		Administrator Authentication and Authorization		WARN	enable
<input type="radio"/>		Authentication Flow Diagnostics		WARN	enable
<input type="radio"/>		Identity Stores Diagnostics		WARN	enable
<input type="radio"/>		Policy Diagnostics		WARN	enable
<input type="radio"/>		RADIUS Diagnostics		WARN	enable
<input type="radio"/>		Guest	LogCollector,LogCollector2	INFO	enable
<input type="radio"/>		MyDevices	LogCollector,LogCollector2	INFO	enable
<input type="radio"/>		AD Connector	LogCollector,LogCollector2	INFO	enable
<input type="radio"/>		TACACS Diagnostics	LogCollector,LogCollector2	WARN	enable
<input type="radio"/>	Accounting	Accounting	LogCollector,LogCollector2	INFO	enable
<input type="radio"/>		RADIUS Accounting	LogCollector,ProfilerRadiusProbe,Log...	INFO	enable
<input type="radio"/>		TACACS Accounting	LogCollector,LogCollector2	INFO	enable
<input type="radio"/>		Administrative and Operational Audit	LogCollector,LogCollector2	INFO	enable
<input type="radio"/>	External MDM	External MDM	LogCollector,LogCollector2	INFO	enable
<input type="radio"/>		PassiveID	LogCollector,LogCollector2	INFO	enable
<input type="radio"/>		Posture and Client Provisioning Audit	ProfilerRadiusProbe,LogCollector,Log...	INFO	enable
<input type="radio"/>		Posture and Client Provisioning Diagnostics	LogCollector,LogCollector2	WARN	enable

**Figure 18-11 Logging Categories**

Upon an MnT failure, all nodes continue to send logs to the remaining MnT node. Therefore, no logs are lost. The PAN retrieves all log and report data from the secondary MnT node, so there is no administrative function loss, either. However, the log database is not synchronized between the primary and secondary MnT nodes. Therefore, when the MnT node returns to service, a backup and restore of the monitoring node is required to keep the two MnT nodes in complete sync.

**Note** The best practice for logging is to also send logging data to a security information and event manager (SIEM) tool, for long-term data archiving and reporting.

## Policy Administration Nodes

The PAN is responsible for providing not only an administrative GUI for ISE but also the critical function of database synchronization of all ISE nodes. All ISE nodes maintain a full copy of the database, with the master database existing on the primary PAN.

A PSN may receive data about a guest user, and when that occurs it must sync that data to the primary PAN. The primary PAN then synchronizes that data out to all the ISE nodes in the deployment.

Because the functionality is so arduous, and having only a single source of truth for the

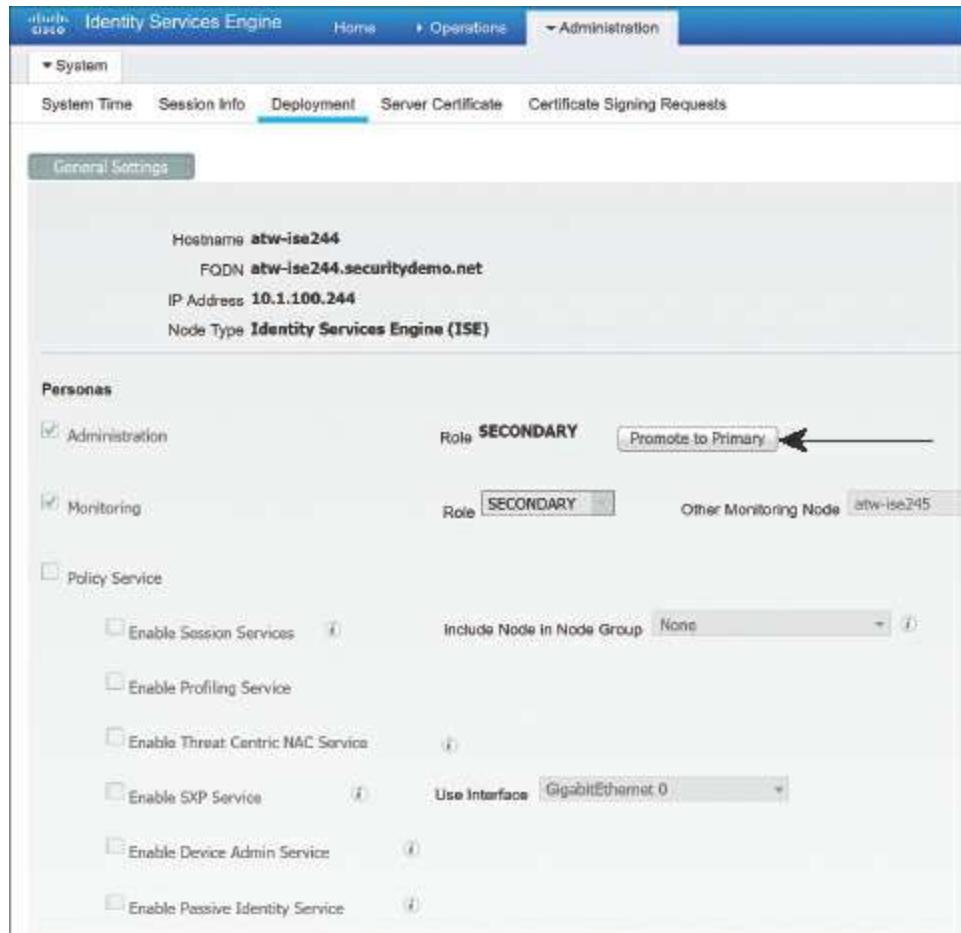
data in the database is so critical, failing over to the secondary PAN is usually a manual process. In the event of the primary PAN going offline, no synchronizations occur until the secondary PAN is promoted to primary. Once it becomes the primary, it takes over all synchronization responsibility. This is sometimes referred to as a “warm spare” type of HA.

## Promote the Secondary PAN to Primary

To promote the secondary PAN to primary, connect to the GUI on the secondary PAN and perform the following steps:

**Step 1.** Choose **Administration > System > Deployment**.

**Step 2.** Click **Promote to Primary**. [Figure 18-12](#) illustrates the Promote to Primary option available on the secondary node.

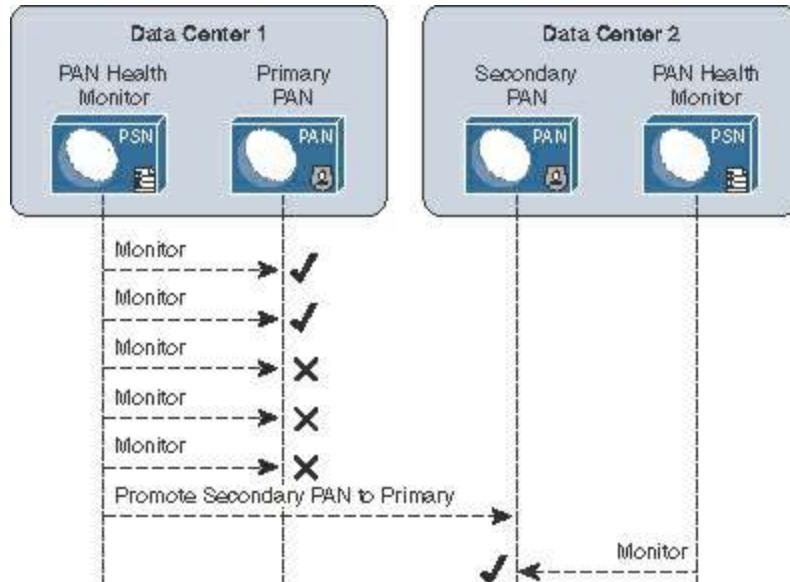


**Figure 18-12** Promoting a Secondary PAN to Primary

## Auto PAN Failover

An automated promotion function was added to ISE beginning with version 1.4. It requires there to be two admin nodes (obviously) and at least one other non-admin node in the deployment.

The non-admin node will act as a health check function for the admin node(s), probing the primary admin node at specified intervals. The Health Check Node will promote the secondary admin node when the primary fails a configurable number of probes. Once the original secondary node is promoted, it is probed. [Figure 18-13](#) illustrates the process.



**Figure 18-13** Promoting a Secondary PAN to Primary with Automated Promotion

As of ISE version 2.1, there is no ability to automatically sync the original primary PAN back into the ISE cube. That is still a manual process.

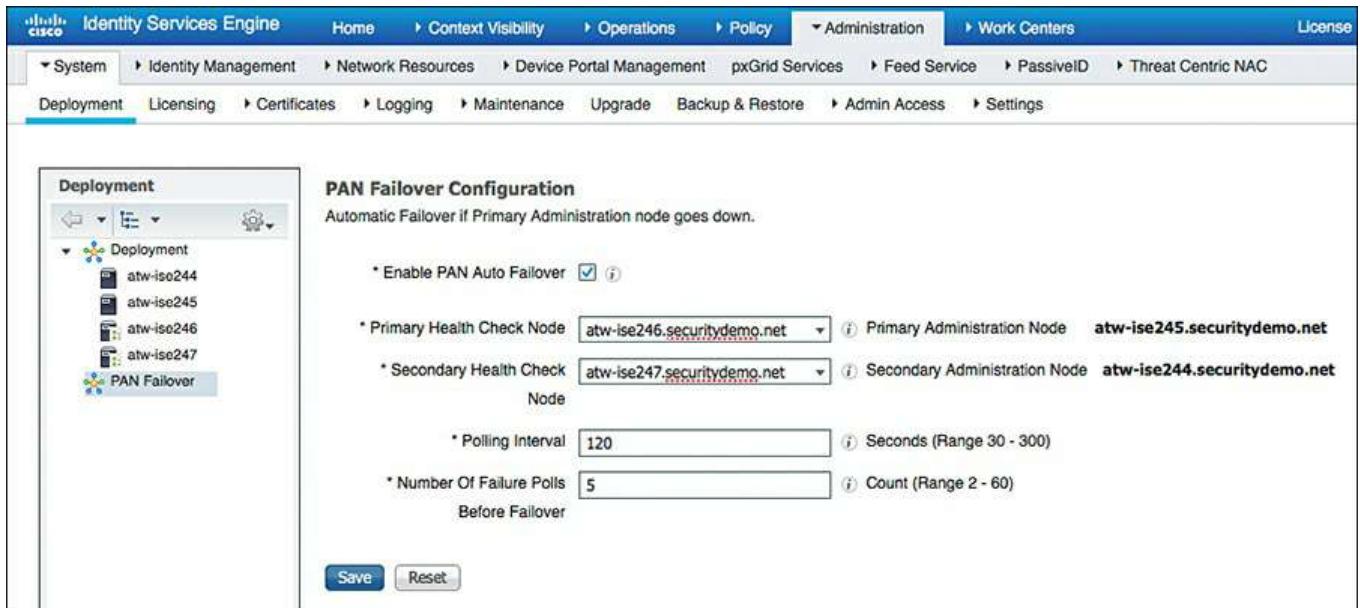
### Configure Automatic Failover for the Primary PAN

For the configuration to be available, there must be two PANs and at least one non-PAN in the deployment.

From the ISE GUI, perform the following steps:

**Step 1.** Navigate to **Administration > System > Deployment**.

**Step 2.** Click **PAN Failover** in the left pane, as shown in [Figure 18-14](#).



**Figure 18-14** PAN Failover

**Step 3.** Check the **Enable PAN Auto Failover** check box.

**Step 4.** Select the **Health Check Nodes** from the drop-down lists. Notice the primary PAN and secondary are listed to the right of the selected Health Check Nodes, as shown in [Figure 18-14](#).

**Step 5.** In the **Polling Interval** field, set the polling interval. The interval is in seconds and can be set between **30** and **300** (5 minutes).

**Step 6.** In the **Number of Failure Polls Before Failover** field, enter the number of failed probes that have to occur before failover is initiated. Valid range is anywhere from **2–60** consecutive failed probes.

**Step 7.** Click **Save**.

## Policy Service Nodes and Node Groups

PSNs do not necessarily need to have an HA type of configuration. Every ISE node maintains a full copy of the database, and the NADs have their own detection of a “dead” RADIUS server, which triggers the NAD to send AAA communication to the next RADIUS server in the list.

However, ISE has the concept of a node group. Node groups are made up of PSNs, where the PSNs maintain a heartbeat with each other. Beginning with ISE 1.3, the PSNs can be in different subnets or can be Layer 2 adjacent. In older ISE versions, the PSNs required the use of multicast, but starting in version 1.3 they use direct encrypted TCP-based communication instead:

- **TCP/7800:** Used for peer communication
- **TCP/7802:** Used for failure detection

If a PSN goes down and orphans a URL-redirected session, one of the other PSNs in the node group sends a Change of Authorization (CoA) to the NAD so that the endpoint can restart the session establishment with a new PSN.

Node groups do have another function, which is entirely related to data replication. ISE used a serial replication model in ISE 1.0, 1.1, and 1.1.x, meaning that all data had to go through the primary PAN and it sent the data objects to every other node, waiting for an acknowledgement for each piece of data before sending the next one in line.

Beginning with ISE 1.2 and moving forward, ISE begins to use a common replication framework known as JGroups (<http://bfy.tw/5vYC>). One of the benefits of JGroups is the way it handles replications in a group or segmented fashion. JGroups enables replications with local peers directly without having to go back through a centralized master, and node groups are used to define those segments or groups of peers.

So, when a member of a node group learns endpoint attributes (profiling), it is able to send the information directly to the other members of the node group directly. However, when that data needs to be replicated globally (to all PSNs), then the JGroups communication must still go through the primary PAN, which in turn replicates it to all the other PSNs.

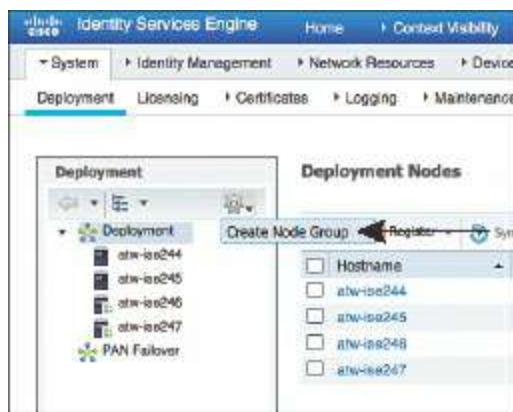
Node groups are most commonly used when deploying the PSNs behind a load balancer; however, there is no reason node groups could not be used with regionally located PSNs. You would not want to use a node group with PSNs that are geographically and logically separate.

## Create a Node Group

To create a node group, from the ISE GUI, perform the following steps:

**Step 1.** Choose **Administration > System > Deployment**.

**Step 2.** In the Deployment pane on the left side of the screen, click the cog icon and choose **Create Node Group**, as shown in [Figure 18-15](#).



**Figure 18-15** Choosing to Create a Node Group

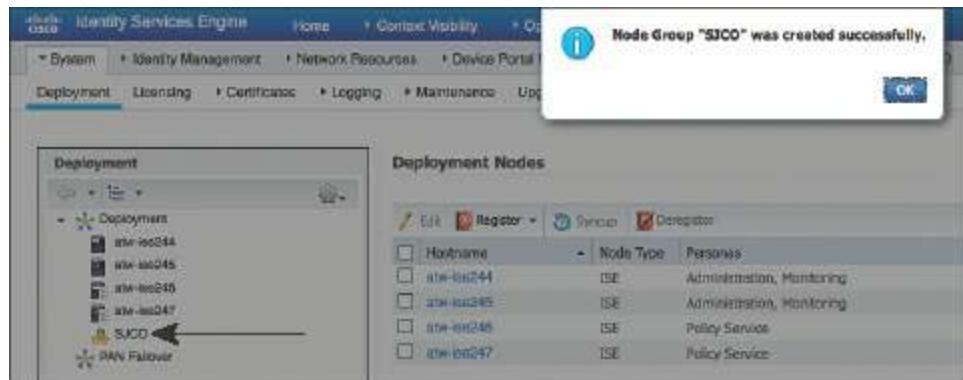
**Step 3.** On the Create Node Group screen, shown in [Figure 18-16](#), enter in the Node Group Name field a name for the node group. Use a name that also helps describe the location of the group. In this example, SJCO was used to represent San Jose, Building O.

The form has a title 'Create Node Group'. It contains two input fields: 'Node Group Name' with the value 'SJCO' and 'Description' with the value 'PSNs in Building O'. At the bottom are 'Submit' and 'Reset' buttons.

**Figure 18-16** Node Group Creation

**Step 4.** (Optional) In the Description field, enter a more detailed description that helps to identify exactly where the node group is (for example, PSNs in Building O). Click **Submit**.

**Step 5.** Click **OK** in the success popup window, as shown in [Figure 18-17](#). Also notice the appearance of the node group in the left pane.



**Figure 18-17** Success Popup

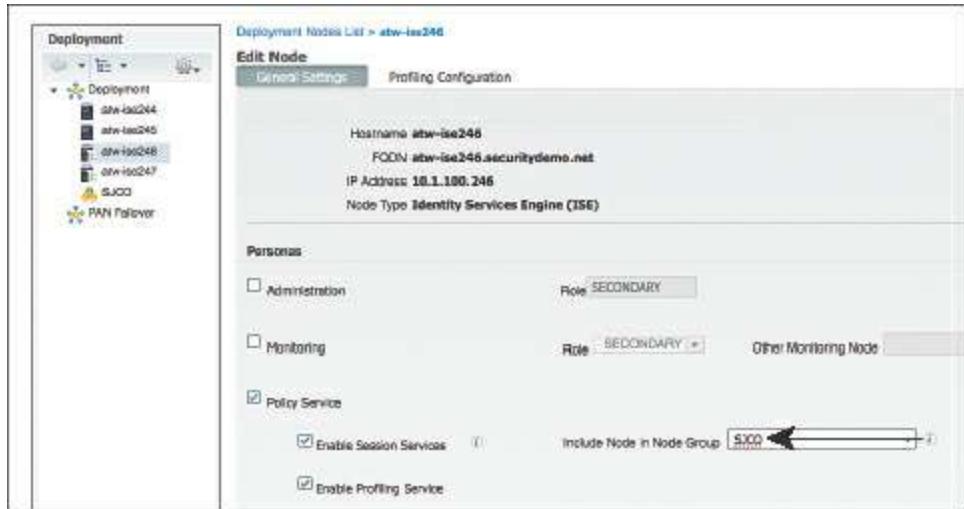
## Add the Policy Service Nodes to the Node Group

To add the PSNs to the node group, from the ISE GUI, perform the following steps:

**Step 1.** Choose **Administration > System > Deployment**.

**Step 2.** Select one of the PSNs to add to the node group.

**Step 3.** Click the **Include Node in Node Group** drop-down arrow and select the newly created group, as shown in [Figure 18-18](#).



**Figure 18-18** Assigning a Node Group

**Step 4.** Click Save.

**Step 5.** Repeat the preceding steps for each PSN that should be part of the node group.

[Figure 18-19](#) shows the reorganization of the PSNs within the node group in the Deployment navigation pane on the left side.

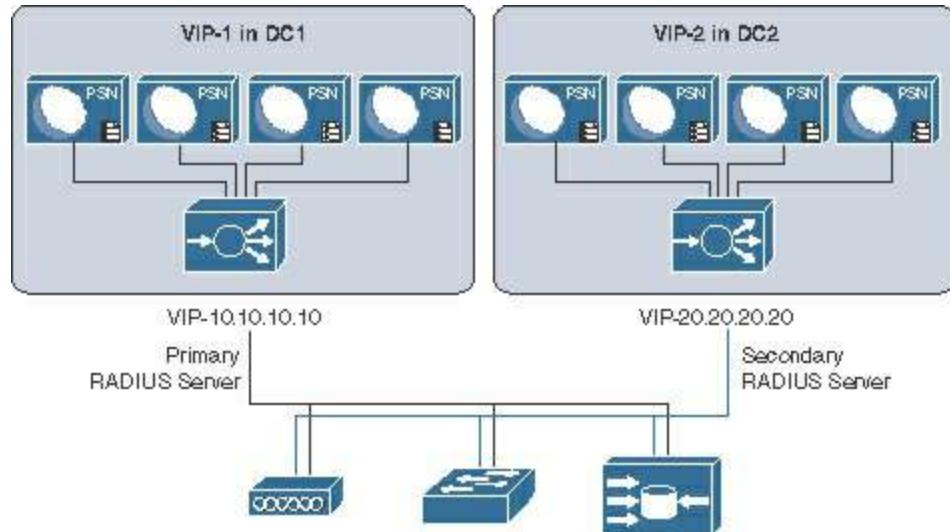
Hostname	Node Type	Personas
atw-ise244	ISE	Administration, Monitoring
atw-ise245	ISE	Administration, Monitoring
atw-ise246	ISE	Policy Service
atw-ise247	ISE	Policy Service

**Figure 18-19** Reorganized Deployment Navigation Pane

## Using Load Balancers

One high-availability option that is growing in popularity for Cisco ISE deployments is the use of load balancers. Load balancer adoption with ISE deployments has skyrocketed over the years because it can significantly simplify administration and designs in larger deployments. As [Figure 18-20](#) illustrates, with load balancing, the

NADs have to be configured with only one IP address per set of ISE PSNs, removing a lot of the complexity in the NAD configuration. The load balancer itself takes care of monitoring the ISE PSNs and removing them from service if they are down and allows you to scale more nodes behind the virtual IP (VIP) without ever touching the network device configuration again.



**Figure 18-20** Load-Balanced PSN Clusters

Craig Hyps, a Principal Technical Marketing Engineer for ISE at Cisco, has written what is considered to be the definitive guide on load balancing with ISE, “How To: Cisco & F5 Deployment Guide: ISE Load Balancing Using BIG-IP.” Craig wrote the guide based on using F5 load balancers, but the principles are identical regardless of which load balancer you choose to implement. You can find his guide here: <https://communities.cisco.com/docs/DOC-68198>.

Instead of replicating that entire large and detailed guide in this chapter, this section simply focuses on the basic principles that must be followed when using ISE with load balancers.

## General Guidelines

When using a load balancer, you must ensure the following:

- Each PSN must be reachable by the PAN/MnT directly, without having to go through Network Address Translation (NAT). This sometimes is referred to as routed mode or pass-through mode.
- Each PSN must also be reachable directly from the endpoint.
  - When the PSN sends a URL-Redirection to the NAD, it uses the fully qualified domain name (FQDN) from the configuration, not the virtual IP (VIP) address.
  - You might want to use Subject Alternative Names (SAN) in the certificate to

include the FQDN of the load-balancer VIP.

- The same PSN is used for the entire session. User persistence, sometimes called needs to be based on Calling-Station-ID.
- The VIP gets listed as the RADIUS server of each NAD for all 802.1X-related AAA.
  - Includes both authentication and accounting packets.
  - Some load balancers use a separate VIP for each protocol type.
- The list of RADIUS servers allowed to perform dynamic-authorizations (also known as Change of Authorization [CoA]) on the NAD should use the real IP addresses of the PSNs, not the VIP.

The VIP could be used for the CoAs, if the load balancer is performing source NAT (SNAT) for the CoAs sent from the PSNs.

**Note** ISE uses the device's Layer 3 address to identify the NAD, not the NAS-IP-Address in the RADIUS packet. This is another reason to avoid SNAT for the incoming RADIUS requests.

- Load balancers should be configured to use test probes to ensure the PSNs are still "alive and well."
  - A probe should be configured to ensure RADIUS is responding.
  - HTTPS should also be checked.
  - If either probe fails, the PSN should be taken out of service.
  - A PSN must be marked dead and taken out of service in the load balancer before the NAD's built-in failover occurs.
- Since the load balancer(s) should be configured to perform health checks of the RADIUS service on the PSN(s), the load balancer(s) must be configured as NADs in ISE so their test authentications may be answered correctly.

## Failure Scenarios

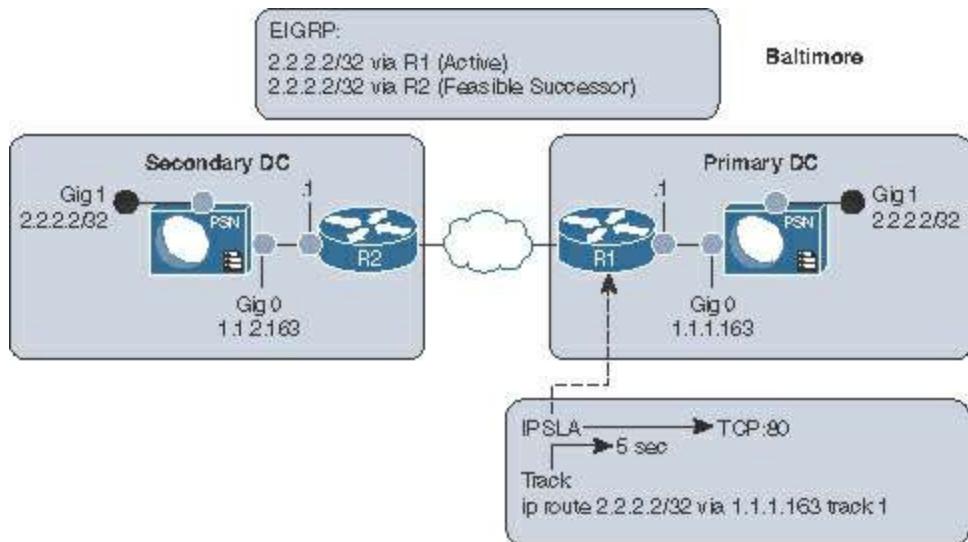
If a single PSN fails, the load balancer takes that PSN out of service and spreads the load over the remaining PSNs. When the failed PSN is returned to service, the load balancer adds it back into the rotation. By using node groups along with a load balancer, another of the node group members issues a CoA-reauth for any sessions that were establishing. This CoA causes the session to begin again. At this point, the load balancer directs the new authentication to a different PSN.

NADs have some built-in capabilities to detect when the configured RADIUS server is

“dead” and automatically fail over to the next RADIUS server configured. When using a load balancer, the RADIUS server IP address is actually the VIP address. So, if the entire VIP is unreachable (for example, the load balancer has died), the NAD should quickly fail over to the next RADIUS server in the list. That RADIUS server could be another VIP in a second data center or another backup RADIUS server.

## Anycast HA for ISE PSNs

This section exists thanks to a friend of the author who is also one of the most talented and gifted technologists roaming the earth today. E. Pete Karelis, CCIE No. 8068, designed this high-availability solution for a small ISE deployment that had two data centers. [Figure 18-21](#) illustrates the network architecture.

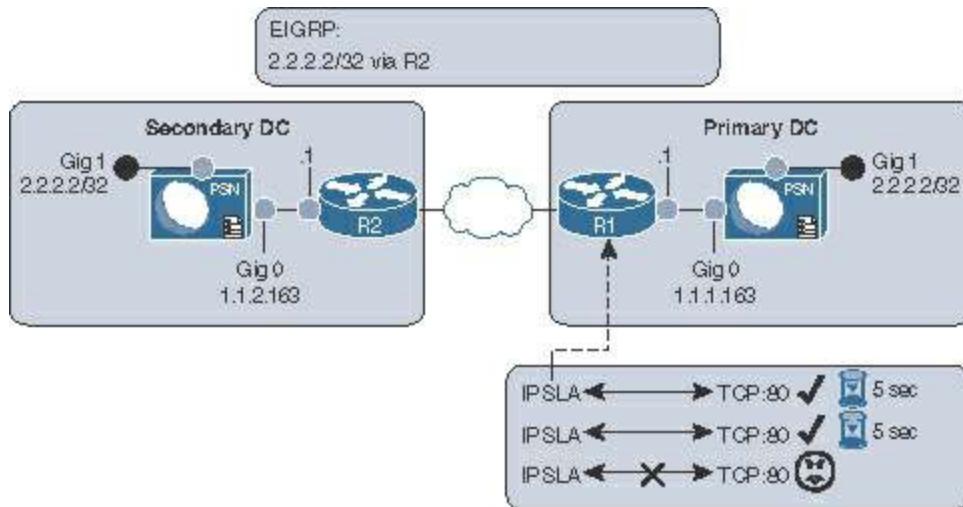


**Figure 18-21** Network Drawing and IPSLA

Anycast is a networking technique where the same IP address exists in multiple places within the network. In this case, the same IP address (2.2.2.2) is assigned to the Gig1 interfaces on all the PSNs, which is connected to an isolated VLAN (or port group in VMware), so that the PSN sees the interface as “up” and connected with the assigned IP address (2.2.2.2). Each default gateway (router) in each data center is configured with a static route to 2.2.2.2/32 with the Gig0 IP address of the PSN as the next hop. Those static routes are redistributed into the routing protocol; in this case EIGRP is used. Anycast relies on the routing protocols to ensure that traffic destined to the Anycast address (2.2.2.2) is sent to the closest instance of that IP address.

After setting up Anycast to route 2.2.2.2 to the ISE PSN, Pete used EIGRP metrics to ensure that all routes preferred the primary data center, with the secondary data center route listed as the feasible successor (FS). With EIGRP, there is less than a 1-second delay when a route (the successor) is replaced with the backup route (the feasible successor).

Now, how do we make the successor route drop from the routing table when the ISE node goes down? Pete configured an IP service-level agreement (IPSLA) on the router that checked the status of the HTTP service on the ISE PSN in the data center every 5 seconds. If the HTTP service stops responding on the active ISE PSN, then the route is removed and the FS takes over, causing all the traffic for 2.2.2.2 to be sent to the PSN in the secondary data center. [Figure 18-22](#) illustrates the IPSLA function, and when it occurs the only route left in the routing table is to the router at the secondary data center.



**Figure 18-22** IPSLA in Action

All network devices are configured to use the Anycast address (2.2.2.2) as the only RADIUS server in their configuration. The RADIUS requests will always be sent to whichever ISE node is active and closest. Authentications originating within the secondary data center go to the local PSN.

**Note** The dynamic-authorization configuration of the NAD must still use the Gig0 interface IP addresses, as those will be the source when ISE sends a CoA to the switch.

[Example 18-2](#) shows the interface configuration on the ISE PSN. The Gig0 interface is the actual routable IP address of the PSN, while Gig1 is in a VLAN to nowhere using the Anycast IP address.

### Example 18-2 ISE Interface Configuration

[Click here to view code image](#)

```
interface gig 0
    !Actual IP of Node
    ip address 1.1.1.163 255.255.255.0

interface gig 1
    !Anycast VIP assigned to all PSN nodes on G1
    ip address 2.2.2.2 255.255.255.255

ip default-gateway [Real Gateway for Gig0]
!note no static routes needed.
```

[Example 18-3](#) shows the IPSLA configuration on the router, to test port 80 on the PSN every 5 seconds but to timeout after 1000 msec. When that timeout occurs, the IP SLA object will be marked as “down,” which causes changed object tracking to remove the static route from the route table.

### Example 18-3 IPSLA Configuration

[Click here to view code image](#)

```
ip sla 1
    !Test TCP to port 80 to the actual IP of the node.
    !"control disable" is necessary, since you are connecting to an
    !actual host instead of an SLA responder

tcp-connect 1.1.1.163 80 control disable
    ! Consider the SLA as down if response takes longer than 1000msec

threshold 1000
    ! Timeout after 1000 msec.
timeout 1000
    !Test every 5 Seconds:
frequency 5

ip sla schedule 1 life forever start-time now
track 1 ip sla 1
ip route 2.2.2.2 255.255.255.255 1.1.1.163 track 1
```

[Example 18-4](#) shows the route redistribution configuration where the EIGRP metrics are applied. Pete was able to use the metrics that he chose specifically because he was very familiar with his network. His warning to others attempting the same thing is to be familiar with your network or to test thoroughly when identifying the metrics that would work for you.

Remember, you must avoid equal-cost, multiple-path routes, as this state could potentially introduce problems if RADIUS requests are not sticking to a single node. Furthermore, this technique is not limited to only two sites; Pete has since added a third location to the configuration and it works perfectly.

**Note** There is an obvious, albeit rare, flaw in the design. With this design, we are using HTTP to validate the status of the node, rather than validating the state of the RADIUS service itself, since the status of the RADIUS service cannot be queried by IOS Changed Object Tracking. This works very well in most cases, but in the rare event that the HTTP service on a PSN is operational and the RADIUS service is not operational, it could theoretically cause issues.

[Example 18-4 Route Redistribution](#)

[Click here to view code image](#)

```
router eigrp [Autonomous-System-Number]
 redistribute static route-map STATIC-TO-EIGRP
 route-map STATIC-TO-EIGRP permit 20
 match ip address prefix-list ISE_VIP
 !Set metrics correctly
 set metric 1000000 1 255 1 1500
 ip prefix-list ISE_VIP seq 5 permit 2.2.2.2/32
```

## Cisco IOS Load Balancing

Cisco network devices have a lot of intelligence built into them to aid in an intelligent access layer for policy and policy enforcement. One such intelligence level is the capability to perform local load balancing of RADIUS servers. This does not mean using a Cisco switch as a server load balancer instead of a dedicated appliance. Instead, it refers to the capability of the access layer switch to load-balance the outbound authentication requests for endpoints that are authenticated to the switch itself. Enabling IOS RADIUS server load balancing only takes one additional command. After all the PSNs are defined as AAA servers in the switch, use the **radius-server load-balance** global configuration command to enable it.

[Example 18-5](#) shows use of a **show** command to verify that multiple ISE servers are configured.

### Example 18-5 Verifying All ISE PSNs Are Configured on Switch

[Click here to view code image](#)

```
3750-X# show aaa server | include host
RADIUS: id 4, priority 1, host 10.1.100.232, auth-port 1812, acct-port
1813
RADIUS: id 5, priority 2, host 10.1.100.233, auth-port 1812, acct-port
1813
RADIUS: id 6, priority 3, host 10.1.100.234, auth-port 1812, acct-port
1813
```

[Example 18-6](#) shows how to enable IOS load balancing

### Example 18-6 Enabling IOS Load Balancing

[Click here to view code image](#)

```
3750-X(config)# radius-server load-balance method least-outstanding  
batch-size 5
```

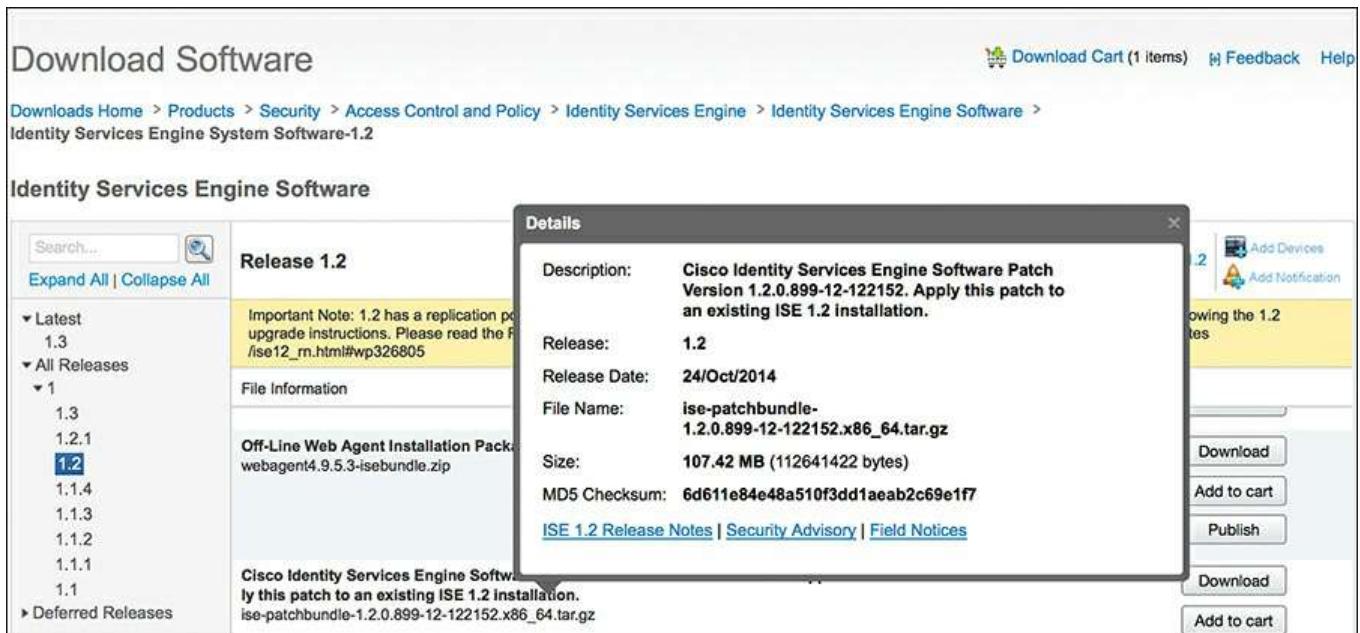
# Maintaining ISE Deployments

Having a distributed deployment and load-balanced architecture are certainly critical items to scaling the deployment and ensuring it is highly available, but there are also critical basic maintenance items that should always be considered to ensure the most uptime and stability. That means having a patching strategy and a backup and restore strategy.

# Patching ISE

Cisco releases ISE patches on a semi-regular basis. These patches contain bug fixes and, when necessary, security fixes. Think about the Heartbleed and Poodle vulnerabilities that were discovered with SSL. To ensure that bug fixes are applied, security vulnerabilities are plugged, and the solution works as seamlessly as possible, always have a planned patching strategy.

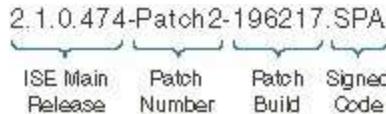
Patches are downloaded from Cisco.com, under **Downloads > Products > Security > Access Control and Policy > Identity Services Engine > Identity Services Engine Software**, as shown at the top of [Figure 18-23](#).



## **Figure 18-23 ISE Downloads Page**

Search the list of software available for your specific version of ISE. [Figure 18-24](#)

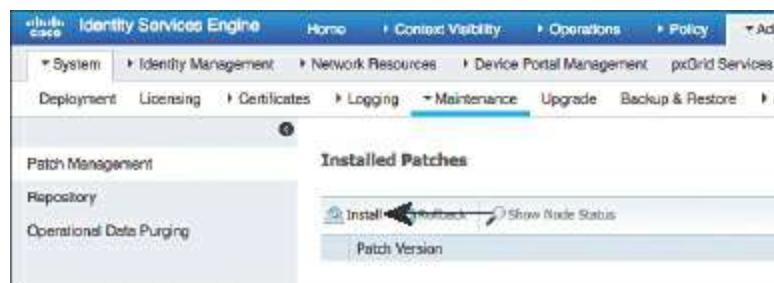
illustrates the naming convention for ISE patches. Cisco ISE patches are normally cumulative, meaning that installing 1.2 patch 12 will include all the fixes in patches 1 through 11 as well.



**Figure 18-24** Anatomy of ISE Patch Nomenclature

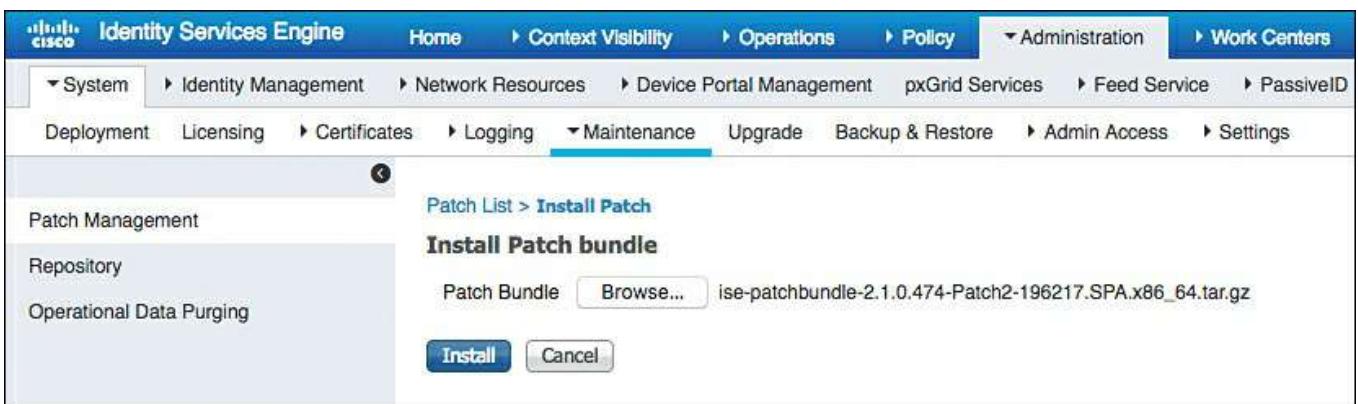
After identifying the correct patch file, follow these steps:

- Step 1.** Download the required patch.
- Step 2.** From the ISE GUI, navigate to **Administration > System > Maintenance > Patch Management**.
- Step 3.** Click the **Install** button, as shown in [Figure 18-25](#).



**Figure 18-25** Patch Management Screen

- Step 4.** Click **Browse**, select the downloaded patch, and click **Install**, as shown in [Figure 18-26](#).



**Figure 18-26** Installing the Selected Patch

As the patch is installed on the PAN, you are logged out of the GUI and the patch is distributed from the PAN to all nodes in the ISE cube. After the patch is successfully installed on the PAN, it is applied to all nodes in the cube one at a time, in alphabetical order.

You can log back into the PAN when it's finished restarting services or rebooting. Click the **Show Node Status** button shown previously in [Figure 18-25](#) to verify the progress of the patching. [Figure 18-27](#) shows the resulting status of each node's progress for the patch installation.

**Note** PAN Auto Failover must be disabled before upgrading, and can be re-enabled after the upgrade is completed.

Node Status for Patch: 2	
Nodes	Patch Status
atw-ise244.securitydemo.net	Installation in Progress
atw-ise245.securitydemo.net	Installed
atw-ise246.securitydemo.net	Not Installed
atw-ise247.securitydemo.net	Not Installed

**Figure 18-27** Node Status

## Backup and Restore

Another key strategy to assuring the availability of ISE in the environment is having a solid backup strategy. There are two types of ISE backups: configuration backup and operational backup. These two types are most easily related to backing up the product databases (configuration) and backing up the MnT data (operational).

[Figure 18-28](#) shows the backup screen in ISE, located at **Administration > System > Backup & Restore**.

**Configuration Backup**

Status:

- Backup Name: - Start Date: -
- Repository Name: - Status: -
- Scheduled: - Progress Percent: -
- Triggered From: - Progress Message: -
- Execute On: -

Schedule:

Frequency: - Start and End: - Execute At: - [Create](#)

History for Repository: [NAS](#)

File Name	Modified Time	... File ...
Weekly_Configuration_Backup-CFG-160130-0000.tar.gpg	Sat Jan 30 01:42:49 2016	NAS 201 MB <a href="#">Restore</a>
Weekly_Configuration_Backup-CFG-160213-0000.tar.gpg	Sat Feb 13 01:43:39 2016	NAS 206 MB <a href="#">Restore</a>
Weekly_Configuration_Backup-CFG-151107-0000.tar.gpg	Sat Nov 7 01:40:10 2015	NAS 154 MB <a href="#">Restore</a>
Weekly_Configuration_Backup-CFG10-151107-0000.tar.gpg	Sat Nov 7 01:35:51 2015	NAS 105 MB <a href="#">Restore</a>
... Monthly_Configuration_Backup...	Mon Nov 14 01:35:40 2015	NAS 108 MB <a href="#">Restore</a>

**Operational Backup**

Status:

- Backup Name: - Start Date: -
- Repository Name: - Status: -
- Scheduled: - Progress Percent: -
- Triggered From: - Progress Message: -
- Execute On: -

Schedule:

Frequency: - Start and End: - Execute At: - [Create](#)

History for Repository:

File Name	Modified Time	R... File...
Monthly_Operational_Backup-OPS10-160201-0000.tar.gpg	Mon Feb 1 01:37:01 2016	NAS 14 MB <a href="#">Restore</a>
Monthly_Operational_Backup-OPS10-160201-0000.tar.gpg	Mon Feb 1 01:36:28 2016	NAS 3 MB <a href="#">Restore</a>
Monthly_Operational_Backup-OPS10-160101-0000.tar.gpg	Fri Jan 1 01:35:55 2016	NAS 13 MB <a href="#">Restore</a>
Monthly_Operational_Backup-OPS10-151101-0000.tar.gpg	Sun Nov 1 01:34:31 2015	NAS 12 MB <a href="#">Restore</a>
Monthly_Operational_Backup-OPS10-160101-0000.tar.gpg	Fri Jan 1 01:35:43 2016	NAS 5 MB <a href="#">Restore</a>
Monthly_Operational_Backup-OPS10-151201-0000.tar.gpg	Tue Dec 1 01:35:14 2015	NAS 13 MB <a href="#">Restore</a>

**Figure 18-28** Backup & Restore Screen

As shown in [Figure 18-28](#), the backups are stored in a repository, and can be restored from the same repository. You can schedule backups to run automatically or you can run them manually on demand. You can view the status of a backup from either the GUI or the CLI, but you can view the status of a restore only from the CLI.

## Summary

This chapter reviewed the basic principles of deploying distributed ISE nodes, high availability for ISE Policy Administration and Monitoring & Troubleshooting nodes. It examined the pillars of successful load balancing with ISE Policy Service Nodes, failover selection on Cisco Catalyst switches, and IOS load balancing.

This chapter also emphasized the importance of having regular backups in addition to a highly available design, and described where to configure those backups in addition to patching an ISE deployment.

# Chapter 19 Remote Access VPN and Cisco ISE

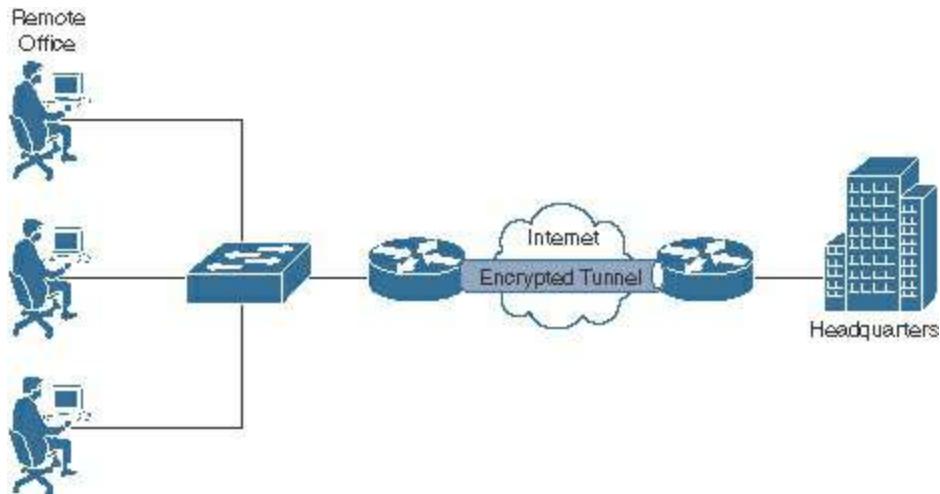
This chapter covers the following topics:

- Introduction to VPNs
- Client-Based remote access VPN
- Remote access VPN and posture
- Extending the ASA remote access VPN capabilities

You have read all about ISE and how it's a policy server for wired, wireless, and VPN; however, VPN has not been covered yet. While wired and wireless communicate in similar ways, remote-access VPN is vastly different; therefore, the way ISE integrates is also vastly different behind the scenes.

## Introduction to VPNs

There are many different types of virtual private networks (VPN). A VPN can be used to connect two or more networks together, extending them almost like a wide-area network (WAN), except that a VPN uses an encrypted tunnel across public infrastructure (the Internet) to connect the networks instead of requiring the dedicated infrastructure of a WAN. This type of VPN is known as a site-to-site VPN, and is illustrated in [Figure 19-1](#).



**Figure 19-1** Site-to-Site Virtual Private Network

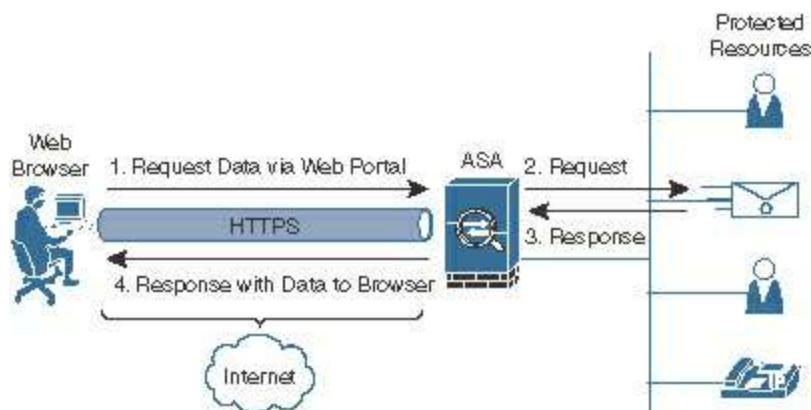
Because site-to-site VPNs simply join disparate networks into a single logical internetwork, ISE may still authenticate users and endpoints at the edge switch in the remote location. In other words, the site-to-site VPN is ultimately transparent to ISE, and the end users are treated the same as if they were connected to an access layer switch at the corporate headquarters.

Alternatively, virtual private networking also replaced dial-up networking in being the

primary means of remote access to corporate networks directly from an endpoint. This type of VPN is known as a remote access VPN (RA-VPN).

To further classify VPN types, an RA-VPN can be clientless or client-based. A clientless RA-VPN is most commonly a method of providing access to internal data that uses a reverse-proxy mechanism, such that the endpoint never actually communicates directly to the corporate network. The VPN headend acts as a reverse proxy by publishing links to certain applications or data to the end user within an HTTPS secured portal that the user accesses through his or her web browser. When the end user attempts to access that published data, the VPN headend initiates the traffic and presents it to the end user through the secure web portal.

[Figure 19-2](#) illustrates a clientless RA-VPN and demonstrates how it is a reverse proxy in nature.



**Figure 19-2 Clientless Remote Access VPN**

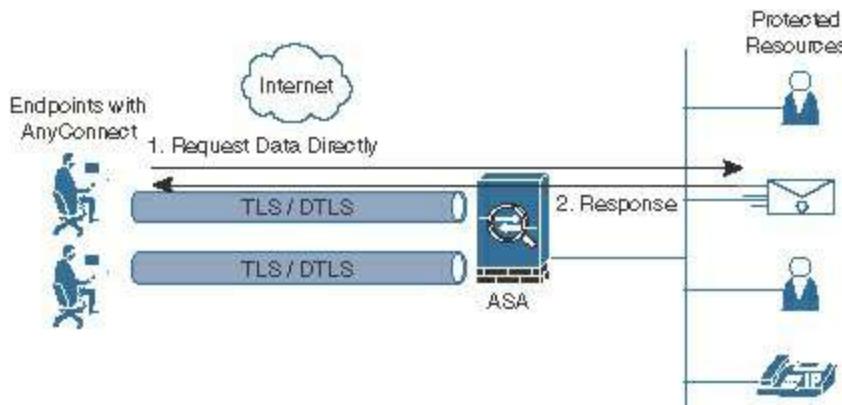
Cisco Adaptive Security Appliances (ASA) and Cisco Firepower Threat Defense (FTD) Next-Generation Firewalls (NGFW) are common headends for clientless RA-VPNs. However, because the end user's endpoint never really communicates directly within the corporate network, traditional posture assessment is a technical improbability. Therefore, ISE integration is limited to traditional authentication, authorization, accounting (AAA) of the end-user logins; consequently, this chapter does not focus much on clientless VPNs.

The primary focus of this chapter is the client-based RA-VPN. It establishes the encrypted tunnel between software on the endpoint itself to the VPN headend, which could be located anywhere where there is a need to protect servers or data, such as the corporate headquarters or even in a cloud. Originally, this type of RA-VPN leveraged IP Security (IPsec) to provide the encrypted tunnel, but the industry moved quite hastily to using Secure Sockets Layer (SSL) as the encryption mechanism of choice. The primary reason for the move was ease of use—many environments do not allow IP protocols 50-51 and UDP port 500, which are required for the IPsec VPN to exit through their firewalls, but normally do not stop TCP/443 (SSL and TLS) or UDP/443.

(dynamic TLS).

In truth, SSL has not really been used in years, and most of what you think is SSL is actually Transport Layer Security (TLS). Cisco AnyConnect uses TLS, and can use Datagram Transport Layer Security (DTLS) simultaneously for the VPN encryption. The overall VPN technology is still commonly referred to as “SSL-VPN,” although it would be most accurate to refer to the client-based RA-VPN as “TLS-VPN” instead.

[Figure 19-3](#) illustrates a client-based RA-VPN and demonstrates how the tunnel is formed between the VPN client and the VPN headend.



**Figure 19-3** Client-based Remote Access VPN

An additional driver away from IPsec VPNs to SSL/TLS-based VPNs was the complexity and rigidity of the traditional IPsec configuration, key negotiation, and the static profiles for the endpoint client.

Now, let's add one more twist. IPsec uses Internet Key Exchange (IKE) for the exchange of encryption keys, and IKE version 2 (IKEv2) allows for a much more simplified VPN setup. The availability of the IKEv2 capabilities has revived the use of IPsec VPNs to some extent. In fact, Cisco AnyConnect Secure Mobility Client has support for IKEv2-based IPsec VPNs in addition to TLS VPNs.

Hopefully, this brief history and vocabulary lesson have been valuable to you. Virtual private networking is a broad topic that could easily fill its own book, and (as you know) this is an ISE book, not a VPN book.

## Client-Based Remote Access VPN

As its name suggests, with this form of VPN, you must have a software client on the endpoint to establish the encrypted tunnel to a headend. The headend device could be located within your corporate data center, or even in the cloud—anywhere your organization has resources that need to be accessed and protected. For purposes of this discussion, the headend is a Cisco ASA or FTD NGFW. The endpoint software is the Cisco AnyConnect Secure Mobility Client (AnyConnect), which is deployed on more than 150 million endpoints around the world, making it far and away the number one

RA-VPN client in the world.

At its core, AnyConnect is a VPN client, but it is also much more. The AnyConnect client is modular, allowing other Cisco security services modules to be fitted to the client. Many modules exist today, and more will be added in the future. Here are a few examples:

- **ISE Posture module:** Also referred to as the ISE compliance module, and also referred to as System Scan. This is the replacement for the older Cisco NAC Agent to provide posture. See [Chapter 15](#), “[Client Posture Assessment](#),” for more details.
- **Umbrella Roaming module:** Connects endpoints to the Cisco Umbrella Secure Internet Gateway (SIG) service.
- **Network Access Manager (NAM) module:** An enterprise-class supplicant and network manager to handle wired and wireless connections along with the 802.1X authentications.
- **AMP Enabler module:** Reaches out to a distribution point and installs the Advanced Malware Protection (AMP) client.

So, how do you deploy AnyConnect onto the corporate endpoints? There are a number of installation options, but mostly they can be broken down into two installation models:

- **Pre-Deploy:** This mode enables enterprises to leverage their existing software distribution systems and push the client out to the managed assets before they need to connect to the VPN.
- **Web-Deploy:** This mode has the AnyConnect client staged on the headend. The end user can log in to the web portal on the ASA and have the client installed automatically through an ActiveX or Java applet, or the user can download from the web portal.

**Note** In some cases, the Pre-Deploy package is used for the initial push, and Web-Deploy is used for updates going forward.

So, you need to install a client on the endpoint and set up a headend. In the typical fashion of this book, you’ll learn as you configure.

## Configuring a Client-Based RA-VPN on the Cisco ASA

You have several choices of tools to use to configure the ASA for a remote access VPN. You could use the command-line interface, the ASA Device Manager (ASDM) graphical user interface, or even Cisco Security Manager (CSM). This chapter shows you how to leverage ASDM for the configuration.

ASDM has several built-in wizards that you can use to configure the VPN. However, to learn the process, you need to step through the configuration manually. After that, you will understand what the wizards are doing behind the curtains. Here is an overview of the configuration steps:

**Step 1.** Download the latest AnyConnect headend packages.

**Step 2.** Prepare the headend.

**Step 3.** Add an AnyConnect connection profile.

**Step 4.** Add the ISE PSNs to the AAA server group.

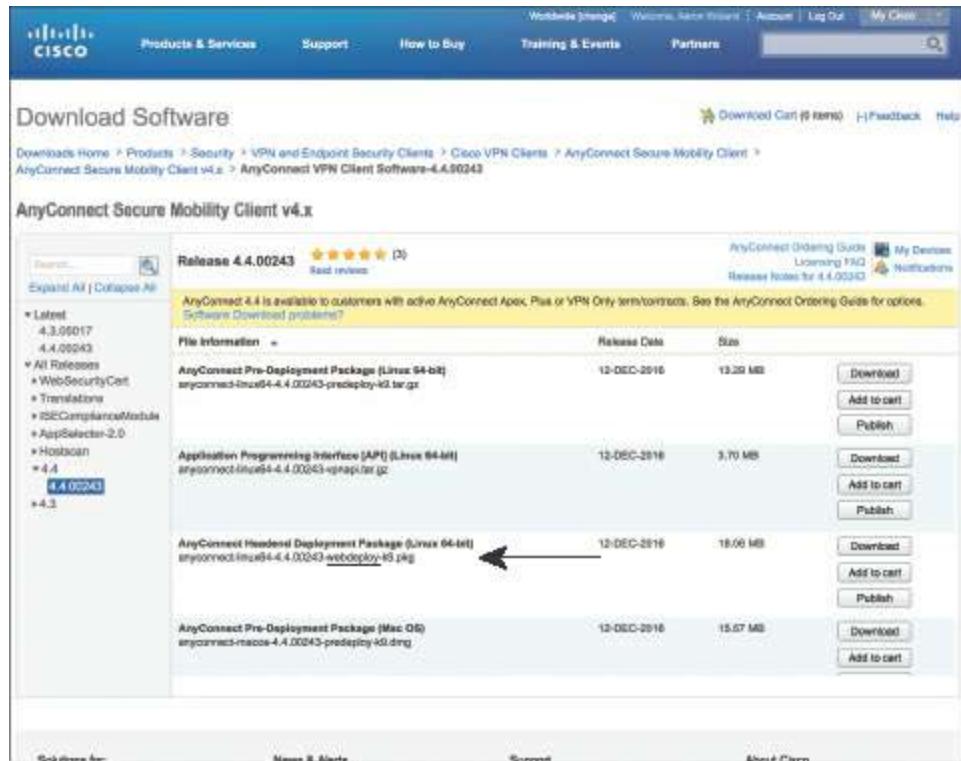
**Step 5.** Add a client address pool.

**Step 6.** Perform network reachability tasks.

You could create each of the required items individually and then tie them together in the connection profile. However, ASDM brilliantly allows you to configure each of the items on the fly, which is what you are going to do in this section.

## **Download the Latest AnyConnect Headend Packages**

Before focusing on ASDM and configuring the remote access VPN itself, download the latest AnyConnect packages from [Cisco.com](#) by navigating to **Support > All Downloads > Security > VPN and Endpoint Security Clients > Cisco VPN Clients > AnyConnect Secure Mobility Client > AnyConnect Secure Mobility Client v4.x**, as shown in [Figure 19-4](#).



**Figure 19-4** Downloading AnyConnect from Cisco.com

As you can see in [Figure 19-4](#), locating the correct package is a bit daunting because there are so many folders listed and so many choices. With AnyConnect, you typically want to download the latest version (4.4.00243 at the time of this writing). When looking for the packages to load into the ASA, keep in mind that the names include the deployment method described previously in this chapter: Pre-Deploy packages are for downloading and installing manually or through a software management system, and the Web-Deploy packages are for loading into the ASA. The word Headend is also in the title, as indicated in [Figure 19-4](#). Download all three Headend packages: Windows, Mac OS, and Linux. After you've downloaded the three AnyConnect packages, log in to ASDM; it is time to start configuring.

## Prepare the Headend

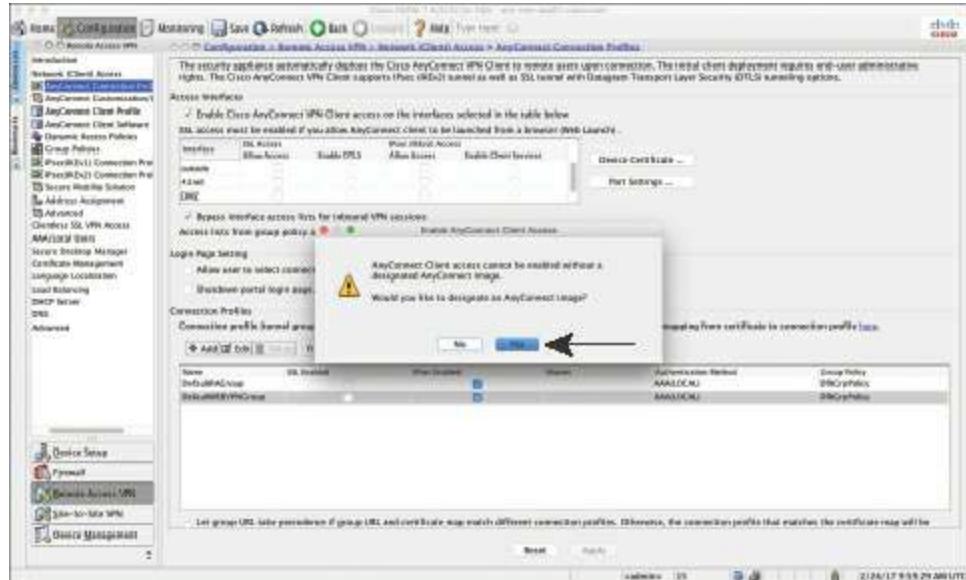
After logging in to ASDM, follow these steps to prepare the headend:

**Step 1.** Navigate to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**.

**Step 2.** Check the **Enable Cisco AnyConnect VPN Client Access on the Interfaces Selected in the Table Below** check box.

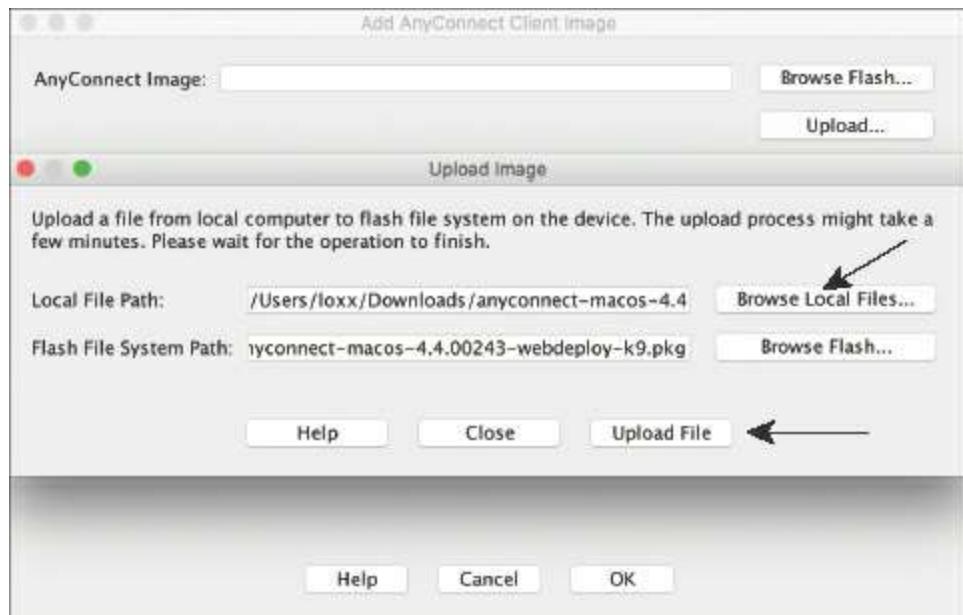
If you do not have any AnyConnect packages loaded, you are prompted with “AnyConnect Client access cannot be enabled without a designated AnyConnect image. Would you like to designate an AnyConnect image?” (see [Figure 19-5](#)). If

you do not receive this message, it means you already have AnyConnect packages installed on the ASA. In that case, navigate to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Software** and click **Add** to follow along.



**Figure 19-5** Warning to Designate an AnyConnect Image

**Step 3.** If you receive the prompt shown in [Figure 19-5](#), click **Yes** to open the Add AnyConnect Client Image dialog box, shown in [Figure 19-6](#).



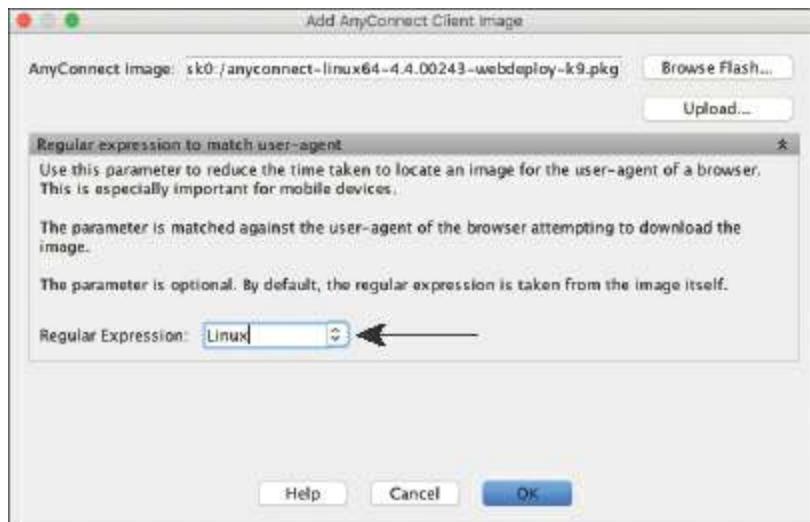
**Figure 19-6** Uploading an AnyConnect Package to the ASA

**Step 4.** Click **Upload**, click **Browse Local Files**, and select one of the packages you downloaded, as shown in [Figure 19-6](#).

**Step 5.** Click **Upload File**.

**Step 6.** Select the operating system regular expression to match the operating system type of the uploaded package, as shown in [Figure 19-7](#).

The ASA expects the Windows client software to be the default, and therefore requires you to point out the operating system to match to the other images for Linux and Mac.



**Figure 19-7** Selecting the Operating System Regular Expression

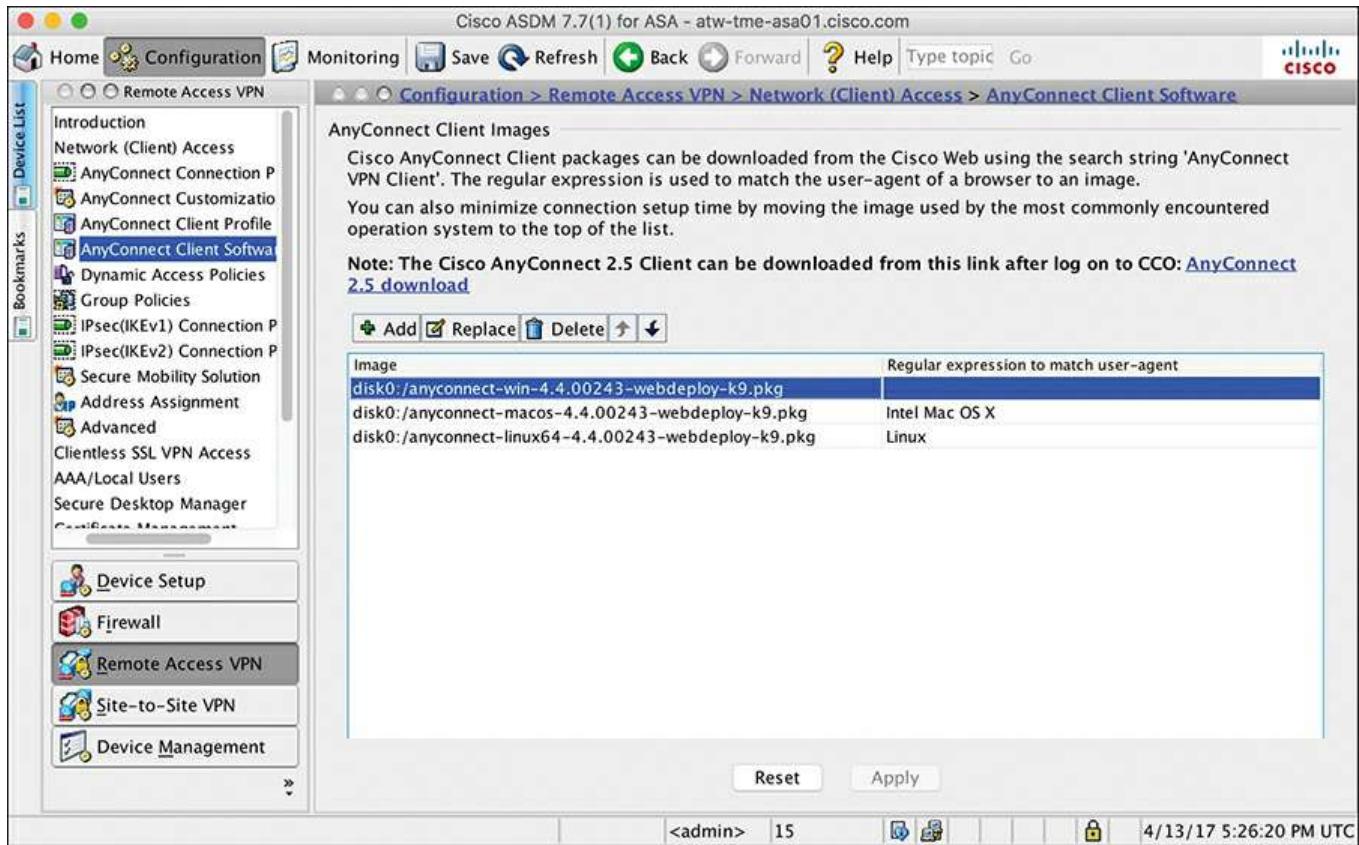
**Step 7.** Click **OK** to complete the upload and mapping.

**Step 8.** Repeat Steps 3 through 6 until Windows, Mac OS, and Linux are all uploaded.  
Skip Step 5 for Windows.

**Step 9.** Click **Apply** to save the configuration changes to the running configuration.

**Step 10.** Click **Save** to save the configuration to the startup configuration.

[Figure 19-8](#) shows the final uploaded packages.



**Figure 19-8 Final Uploaded Packages**

## Add an AnyConnect Connection Profile

Back on the AnyConnect Connection Profile screen, follow these steps to add an AnyConnect connection profile:

- Step 1.** Check the **Enable Cisco AnyConnect VPN Client Access on the Interfaces Selected in the Table Below** check box.
- Step 2.** In the interfaces table, choose the interface that you want to use for VPN access. Typically, the outside interface is used. In that case, check the **Allow Access** check boxes under SSL Access and IPsec (IKEv2) for the outside interface.
- Step 3.** Check the **Enable DTLS** and **Enable Client Services** check boxes.

**Note** Enabling DTLS allows AnyConnect to establish an SSL/TLS VPN using two tunnels simultaneously, a TLS tunnel and a DTLS tunnel. DTLS reduces the impact of latency on the VPN session and helps improve the performance of real-time applications, such as IP telephony, which are quite sensitive to delays.

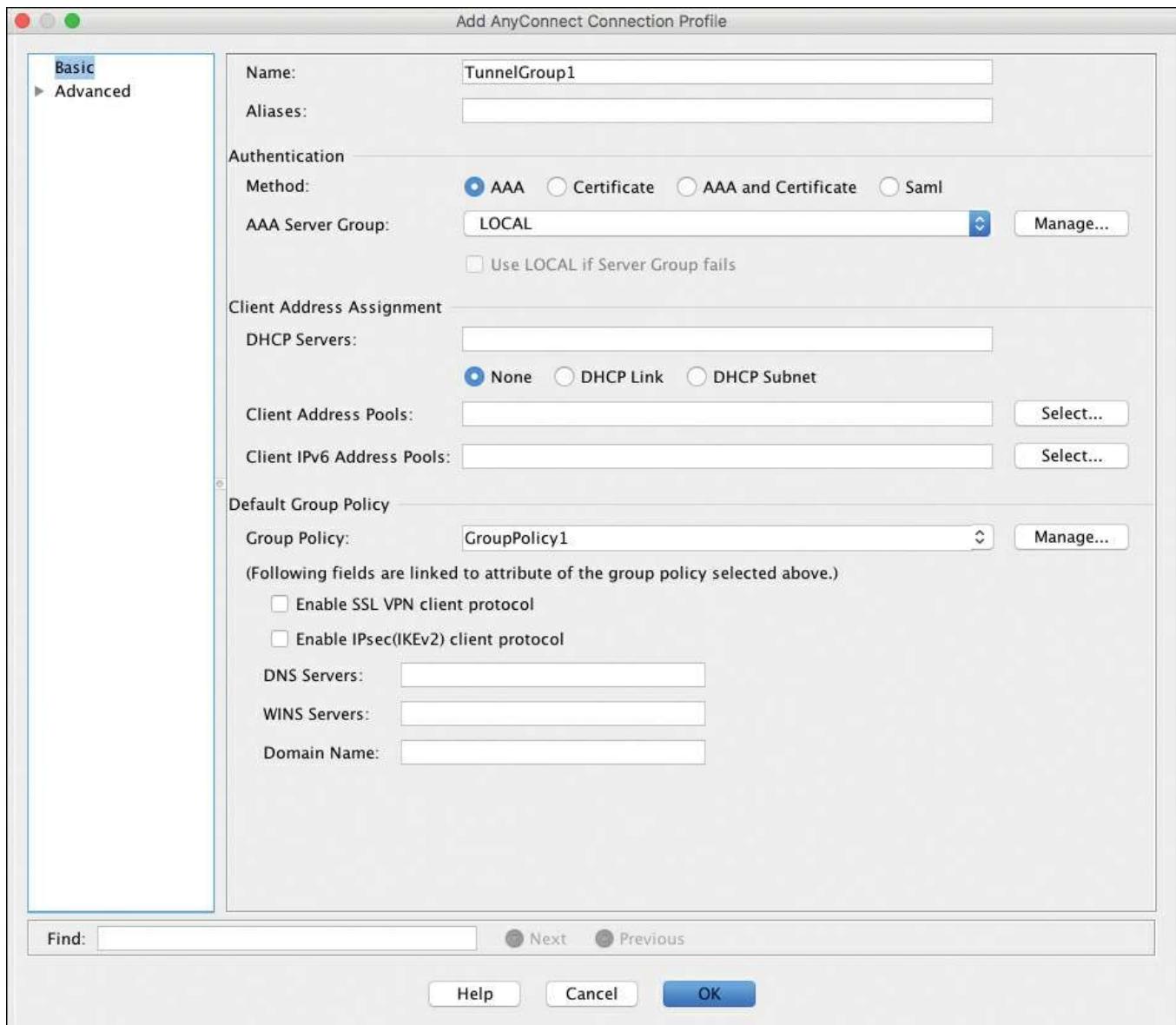
- Step 4.** Below the table, check the **Bypass Interface Access Lists for Inbound VPN Sessions** check box, which prevents the ACL from having to account for what

traffic is permitted from the VPN users to the inside network. This is, of course, specific to your needs in the deployment.

**Step 5. (Optional) Check the Allow User to Select Connection Profile on the Login Page** check box if appropriate for your production VPN deployment.

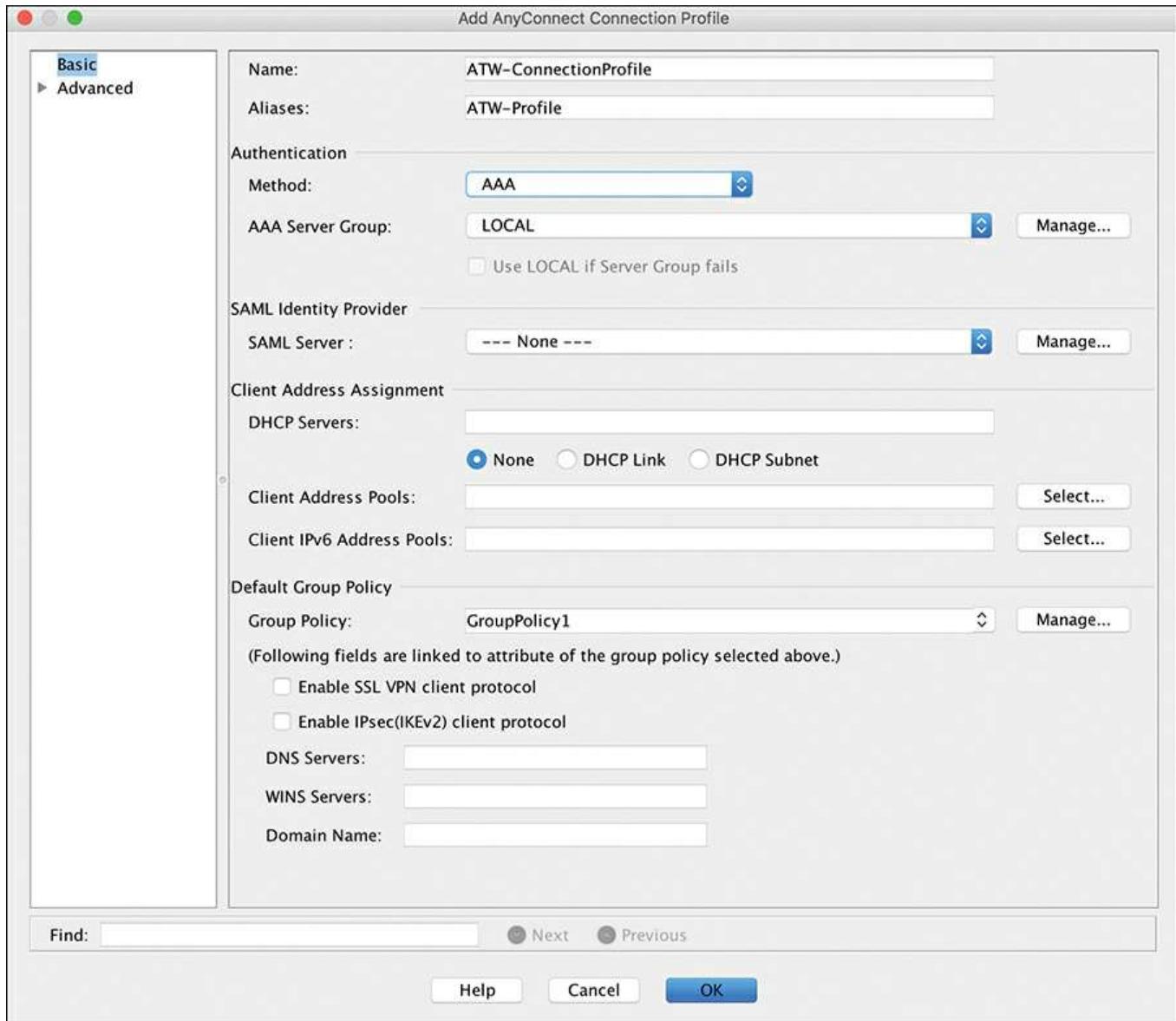
Now that remote access with AnyConnect is enabled on the outside interface of the ASA, the next logical step is to add a new connection profile.

**Step 6. Click Add to add a new connection profile.** The Add AnyConnect Connection Profile screen appears, as shown in [Figure 19-9](#).



**Figure 19-9** Add AnyConnect Connection Profile Screen

**Step 7. Rename the connection profile from TunnelGroup1 to something that makes sense to you and your users. For purposes of this example, use ATWConnectionProfile, as shown in [Figure 19-10](#).**



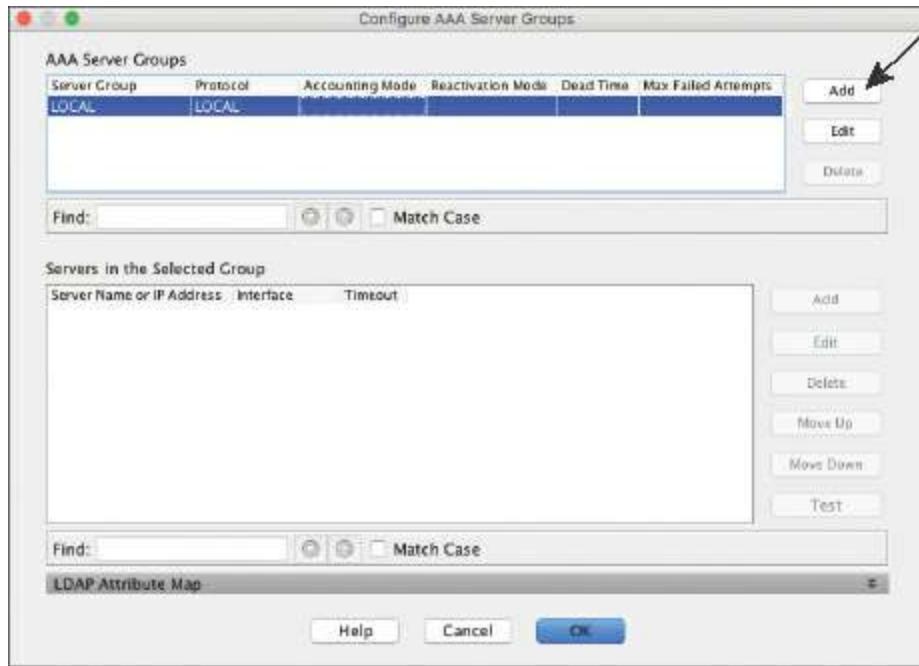
**Figure 19-10** Naming the AnyConnect Connection Profile and the Alias

**Step 8.** In the Aliases text box, provide an alias. This sometimes can be used by the end user to select from the drop-down list when connecting, and can be used for URL matching. For this example, use **ATW-Profile**, as shown in [Figure 19-10](#).

**Step 9.** In the Authentication Section, select AAA in the Method field and click **Manage**.

The VPN requires a mechanism to authenticate the users and authorize them to connect. (See [Chapter 2, “Fundamentals of AAA,”](#) for a refresher on authentication, authorization, and accounting.) By default, the ASA uses a local user database. Obviously, this is a configuration faux pas that you must remedy immediately.

[Figure 19-11](#) shows the Configure AAA Server Groups window.



**Figure 19-11 Configure AAA Server Groups**

**Step 10.** Click **Add** to create a new AAA server group.

This group serves as a placeholder for multiple RADIUS servers (ISE PSNs).

**Step 11.** In the Add AAA Server Group dialog box, shown in [Figure 19-12](#), provide a descriptive name that helps identify the servers that will be in this group. In the example, the group is named ISE231-232 because it will contain two ISE PSNs: atw-ise231 and atw-ise232. In retrospect, a better name would be SJC-ISE, describing the location (San Jose) and the server types (ISE), which considers the possibility of more PSNs being added in the future.

**Step 12.** From the Protocol drop-down list, choose **RADIUS**.

**Step 13.** Leave the Accounting Mode setting at the default, **Single**.

This is important. Single mode sends the accounting packet to the active RADIUS server only, whereas simultaneous mode sprays the accounting packets to all the RADIUS servers in the group. This is not a good idea, especially with RADIUS servers that track session state, like ISE does, and can have unwanted results.

**Step 14.** Leave the Reactivation Mode setting at the default, **Depletion**, the Dead Time at the default of **10** minutes, and the Max Failed attempts at the default of **3**.

With these settings, a RADIUS server will be marked unresponsive (dead) after three authentication attempts are not responded to. Reactivation refers to the method in which unresponsive (dead) RADIUS servers are brought back into service on the ASA. Depletion mode will not bring a dead server back until all the servers in the group have been depleted. Even so, it will wait 10 minutes by

default (Dead Time).

**Step 15.** Check the **Enable Interim Accounting Update** check box.

**Step 16.** Check the **Update Interval** check box and leave the default value of **24** hours.

Interim accounting is important to ISE because it helps maintain that a user is still connected and the network session is still alive.

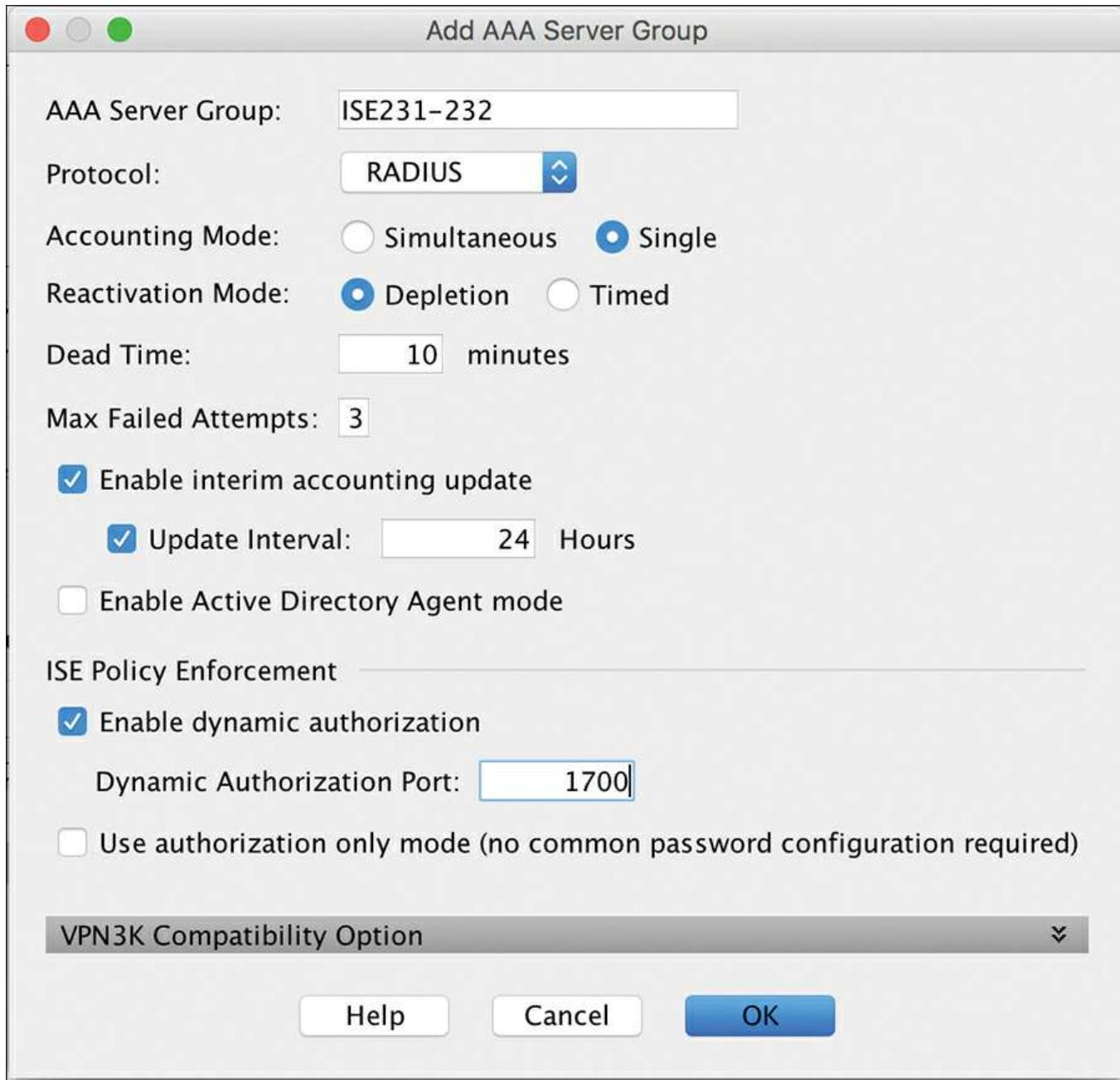
**Step 17.** In the ISE Policy Enforcement section, check the **Enable Dynamic Authorization** check box and leave the Dynamic Authorization Port setting at its default value of **1700**.

As you most likely know from reading the first 18 chapters of this book, dynamic authorization is the official name for Change of Authorization (CoA), which the ASA does a bit differently than the network devices that you have been configuring to this point in the book. For most of the use cases that you have seen within this book, a reauthentication CoA (CoA-ReAuth) is used.

Conversely, the ASA only uses a policy push type of CoA (CoA-Push). Here's the difference:

- **CoA-ReAuth:** When a CoA is sent to the network access device (NAD), it in turn sends a request to the endpoint to authenticate again, in which case a full authentication and authorization process occurs again, with a new authorization result sent to the NAD.
- **CoA-Push:** When a CoA is sent to the ASA, the CoA packet already contains the new authorization result. In the case of the ASA, that means a new ACL is being sent. More details on this method are provided later in the chapter.

[Figure 19-12](#) shows the completed AAA server group.



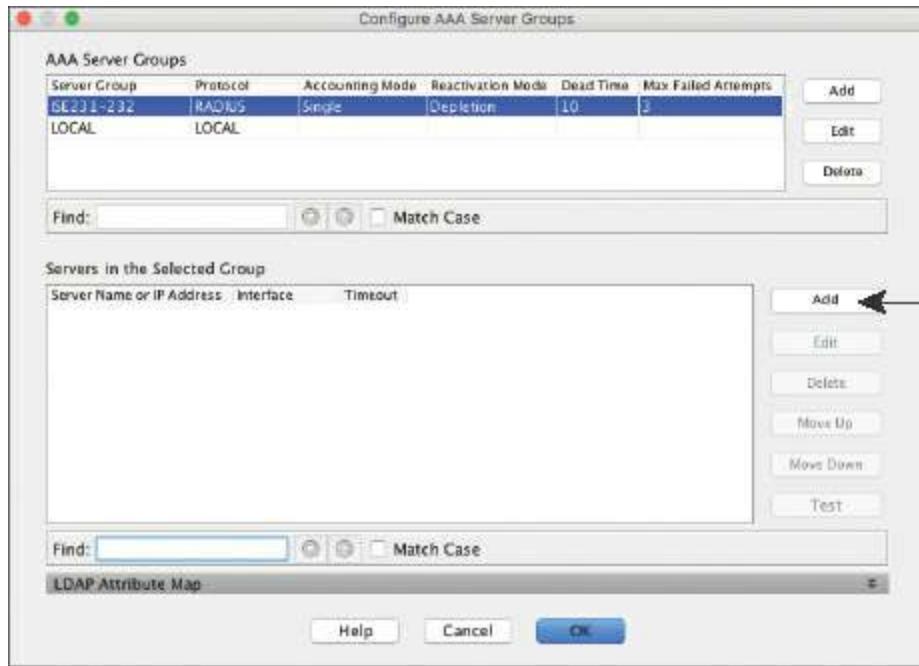
**Figure 19-12** Completed AAA Server Group

**Step 18.** Click **OK**. Leave the Configure AAA Server Groups window open to proceed with the configuration in the next section.

### Add the ISE PSNs to the AAA Server Group

Now that you have created an AAA server group, you are ready to add the PSNs to the group. With the newly created server group (ISE231-232 in the example) selected in the Configure AAA Server Groups window, as shown in [Figure 19-13](#), follow these steps:

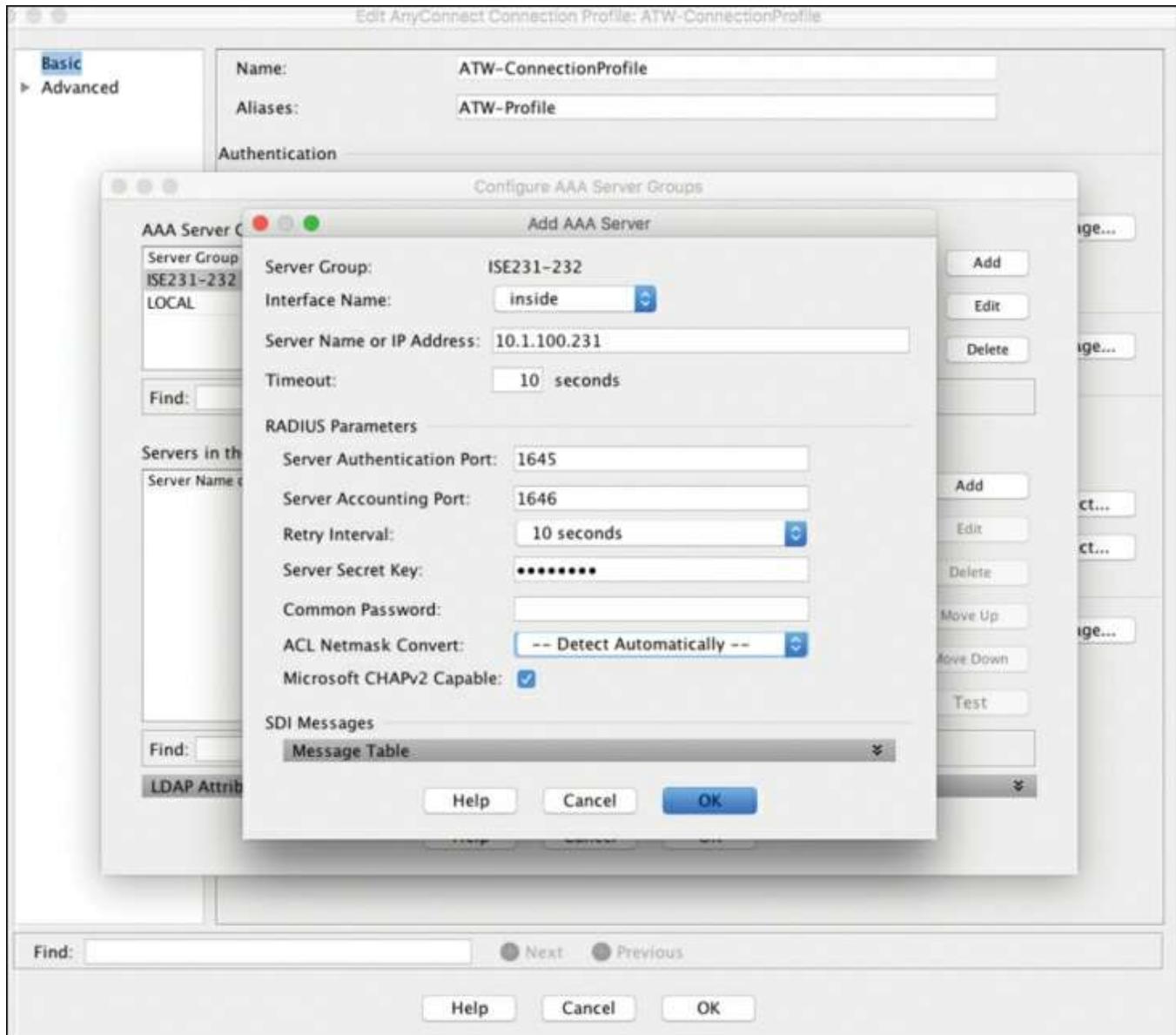
**Step 1.** To the right of the Servers in the Selected Group pane, click **Add** to create a RADIUS server object.



**Figure 19-13** Configure AAA Server Groups Window with New Server Group Selected

- Step 2.** In the Add AAA Server dialog box, shown in [Figure 19-14](#), choose for the Interface Name the correct interface that is closest to the ISE PSNs. In the example, it is the **inside** interface.
- Step 3.** In the Server Name or IP Address field, enter the first PSN's DNS name or IP address, and leave the Timeout value at the default **10** seconds.
- Step 4.** Leave the Server Authentication Port and Server Accounting Port fields at their default values of **1645** and **1646**, respectfully.
- Step 5.** Leave the Retry Interval at the default of **10** seconds.
- Step 6.** In the Server Secret Key field, provide the RADIUS shared secret that is being used between the ASA and ISE. It must be the same as what is configured in the NAD object definition within ISE.
- Step 7.** From the ACL Netmask Convert drop-down list, choose **Detect Automatically**. This is an interesting setting. Whereas ACLs for Cisco Catalyst switches use a wildcard mask in the ACL instead of a standard netmask, the ASA uses a standard netmask for its ACL configuration. Because the ASA can accept the downloadable ACLs (dACL) that are sent from ISE, those dACLs could be configured for either the wildcard or the standard netmask method. The RADIUS server definition in the ASA can be configured for either, or to automatically detect which is being sent. Brilliant!

[Figure 19-14](#) shows the final configuration for the RADIUS server.

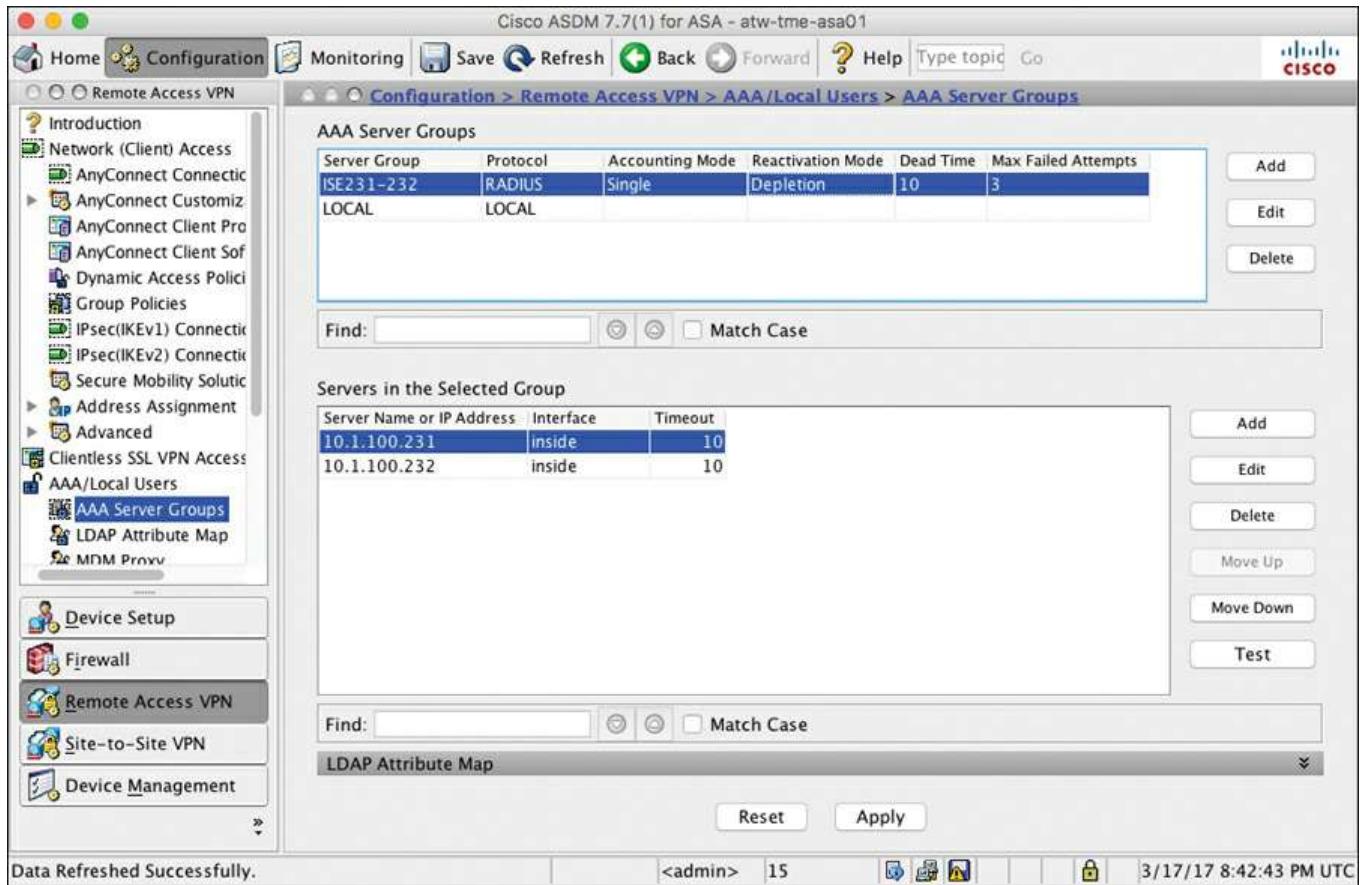


**Figure 19-14** Completed AAA Server Object

**Step 8.** Click **OK**.

**Step 9.** Repeat Steps 1 through 8 for each of the PSNs.

[Figure 19-15](#) shows the completed AAA server group.



**Figure 19-15** Completed AAA Server Group

**Step 10.** Click **Apply**.

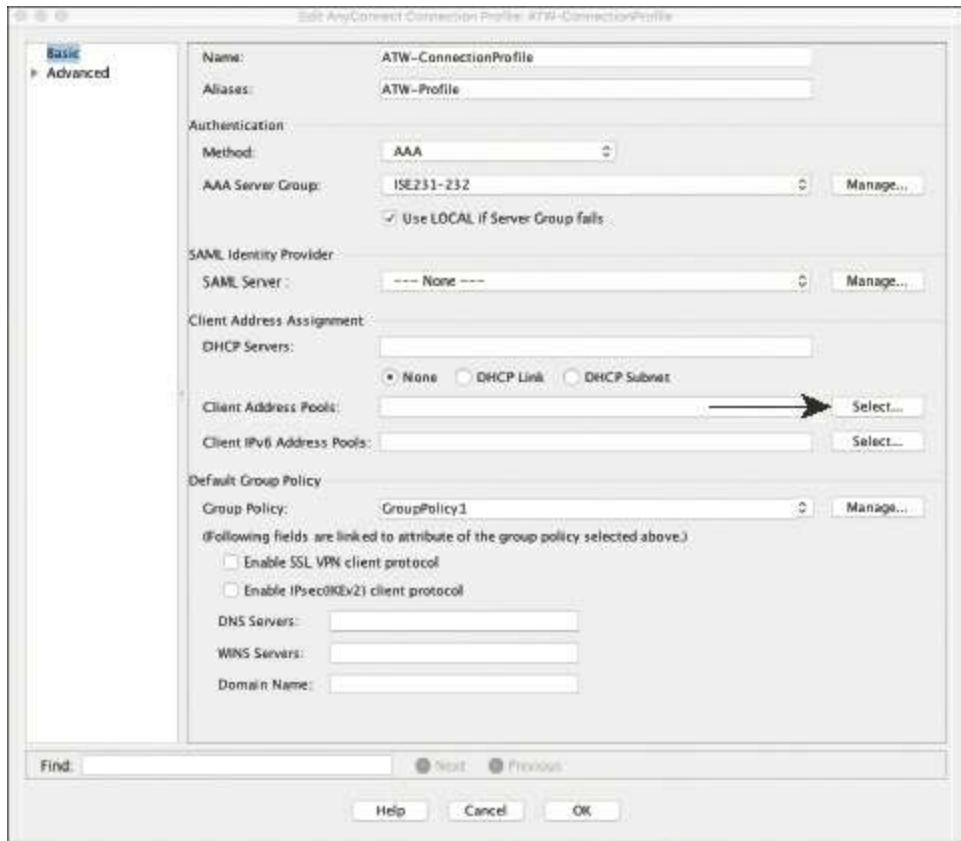
**Step 11.** Click **Save**.

After clicking Save, you are returned to the AnyConnect Connection Profile window. You may choose to check the **Use LOCAL If Server Group Fails** check box if you prefer to fall back to the local user database if the ISE PSNs are unavailable, as shown in [Figure 19-16](#).

The next step is to configure client address assignment.

## Add a Client Address Pool

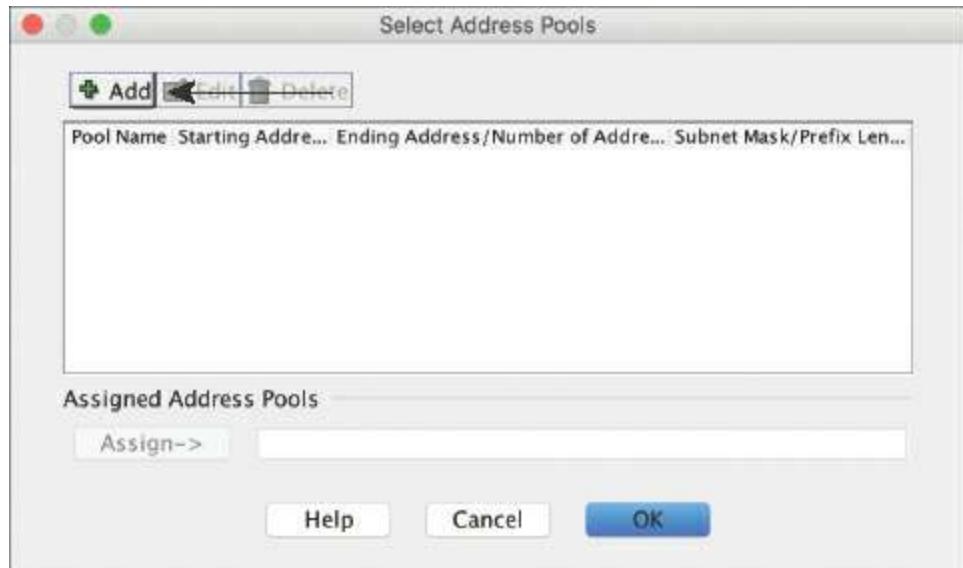
[Figure 19-16](#) shows the connection profile after the AAA server group has been configured. The next item down in the configuration is the SAML Identity Provider section. This doesn't apply to the present ISE configuration example, so leave the SAML Server field set to None.



**Figure 19-16** Connection Profile in Progress After the AAA Server Group Configuration

You do need to be able to assign an IP address to the clients when they connect to the VPN. As shown in the Client Address Assignment section of [Figure 19-16](#), you can configure the connection profile to use an external DHCP server to assign IP addresses to the connecting endpoints, or you can use a pool of addresses configured locally on the ASA. This example uses the latter. The following steps demonstrate how to use a pool of addresses:

**Step 1.** Click **Select** to the right of Client Address Pools, as pointed out in [Figure 19-16](#), to open the Select Address Pools dialog box, shown in [Figure 19-17](#).



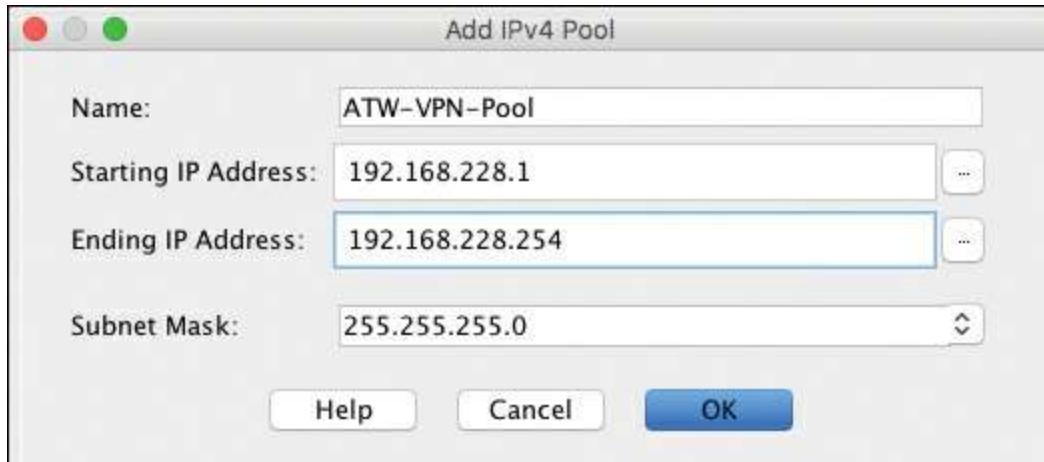
**Figure 19-17** Select Address Pool

**Step 2.** Click **Add** to open the Add IPv4 Pool dialog box, shown in [Figure 19-18](#).

**Step 3.** Provide a self-descriptive name for the address pool. For purposes of the example, use **ATW-VPN-Pool**.

**Step 4.** Enter the starting and ending IP addresses, along with the subnet mask.

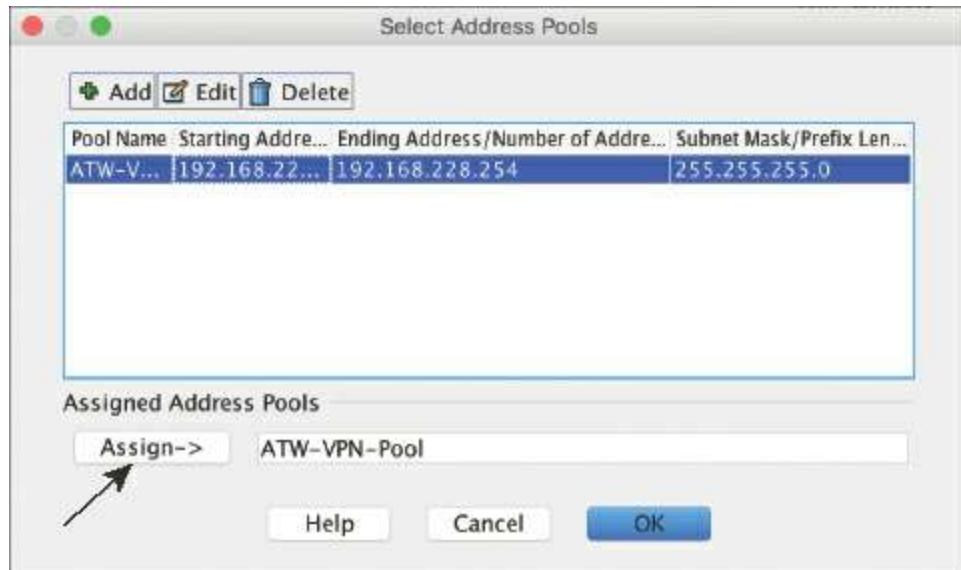
[Figure 19-18](#) shows the configured IPv4 address pool.



**Figure 19-18** Add IPv4 Pool

**Step 5.** Click **OK** to return to the Select Address Pools dialog box.

**Step 6.** Select the newly created IPv4 address pool and click **Assign**, as shown in [Figure 19-19](#).



**Figure 19-19** Selecting the Address Pool

**Step 7.** Click **OK**. You are returned to the Connection Profile screen, with the address pool assigned.

The next logical step would be to configure a group policy, but that is not necessary for the goals of this chapter, so leave the default of **GroupPolicy1**, as shown in [Figure 19-20](#).

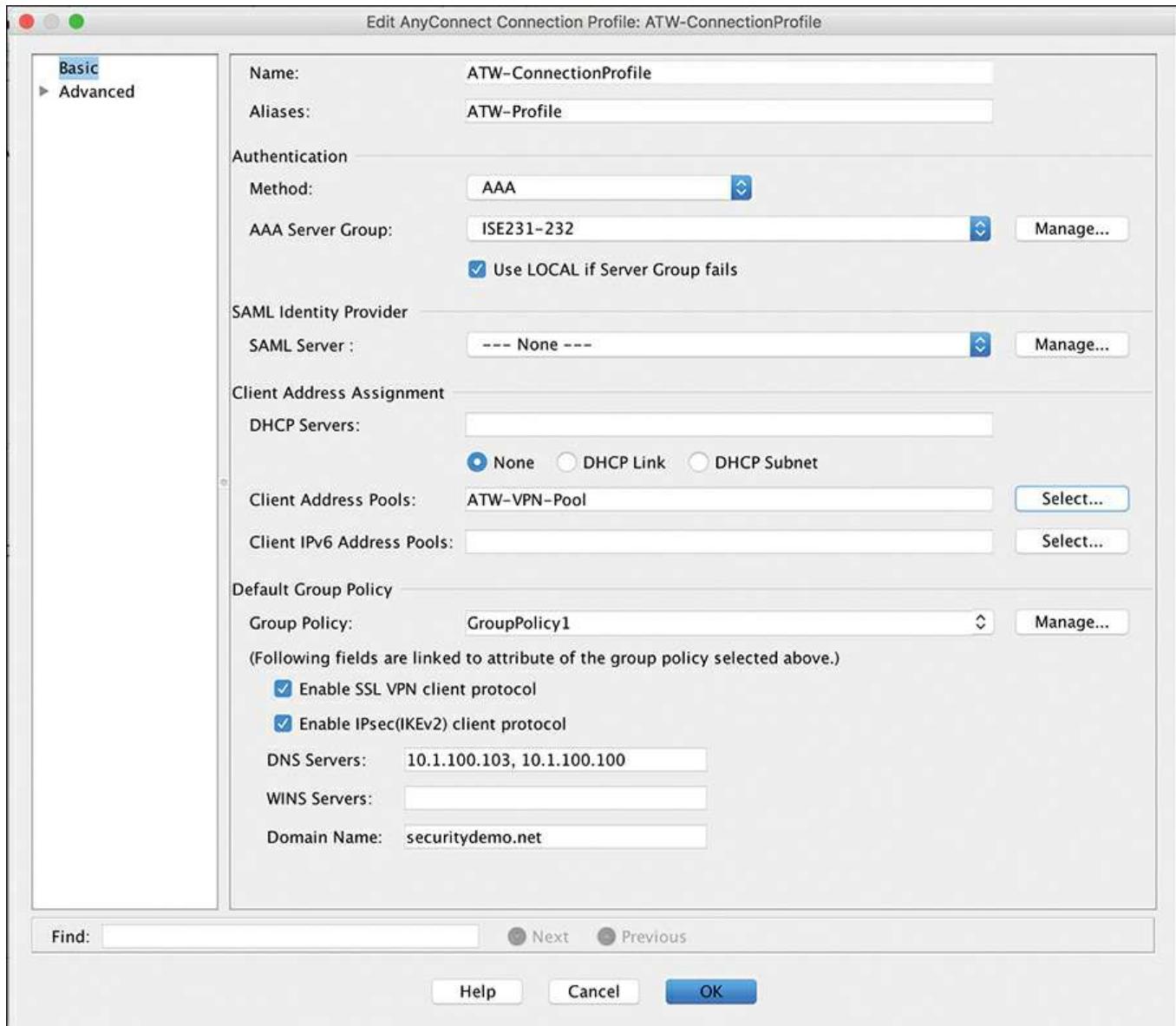
**Step 8.** Check the **Enable SSL VPN Client Protocol** check box.

**Step 9.** Check the **Enable IPsec(IKEv2) Client Protocol** check box.

**Step 10.** In the DNS Servers field, provide the DNS servers to be used for the connected clients.

**Step 11.** In the Domain Name field, provide the DNS domain name to be assigned to the clients.

[Figure 19-20](#) shows the configured connection profile.



**Figure 19-20** Fully Configured AnyConnect Connection Profile

**Step 12.** Click **OK**.

**Step 13.** Click **Apply**.

**Step 14.** Click **Save**.

The AnyConnect connection profile now is fully configured, with an address pool from which to assign client IP addresses, ready to respond to SSL (TLS, actually) and IPsec(IKEv2) requests. However, you are not yet ready to have your clients join the VPN.

## Perform Network Reachability Tasks

There are a few very important steps required to ensure that the VPN-connected endpoints can communicate to and from the other hosts in the network. These steps are

often overlooked, leaving administrators scrambling to figure out why their VPN is not working. This section covers those steps.

Other hosts on the network need to know how to return traffic to addresses that are coming from the VPN pool. There are several ways to accomplish this task, the choice of which depends on the preference of your network team and whether you are running dynamic routing protocols on your ASA:

- If you are running a dynamic routing protocol, such as OSPF or EIGRP, you can redistribute the route for the address pool into that routing protocol.

**Note** If you are running a dynamic routing protocol such as OSPF or EIGRP, you can also use reverse-route injection, as described in the Cisco document “ASA/PIX: Configure and Troubleshoot the Reverse Route Injection (RRI)” (<http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/107596-asa-reverseroute.html>).

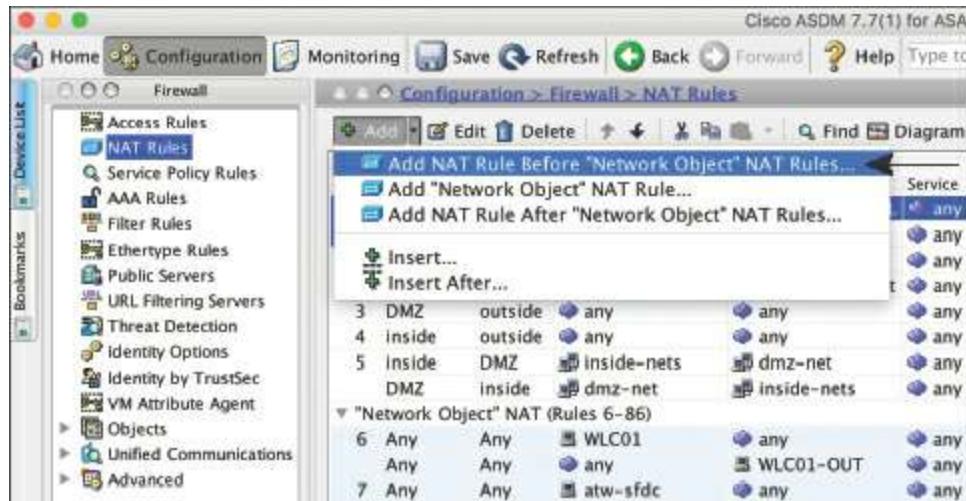
- You can add a static route in the network that sends all traffic for the VPN pool to the ASA.
- Use the ASA as the default gateway. This option is common in smaller deployments, such as branch offices. In that scenario, the return traffic is already sent to the ASA.

The ASA in this example is the default gateway for this environment, and therefore the third option is used.

With the routing sorted out, the next step is to ensure that traffic to and from the VPN is exempted from network address translation (NAT). To accomplish this task, follow these steps:

**Step 1.** Navigate to **Configuration > Firewall > NAT Rules**.

**Step 2.** Click the drop-down arrow next to Add and choose **Add NAT Rule Before “Network Object” NAT Rules**, as shown in [Figure 19-21](#). This ensures that the rule is processed correctly.



**Figure 19-21** Add NAT Rule Before “Network Object” NAT Rules

**Step 3.** In the Match Criteria: Original Packet section at the top of the Add NAT Rule dialog box, choose the **inside** interface of the Source Interface drop-down list, as shown in [Figure 19-22](#).

**Step 4.** Leave the Destination Interface field set to **Any**.

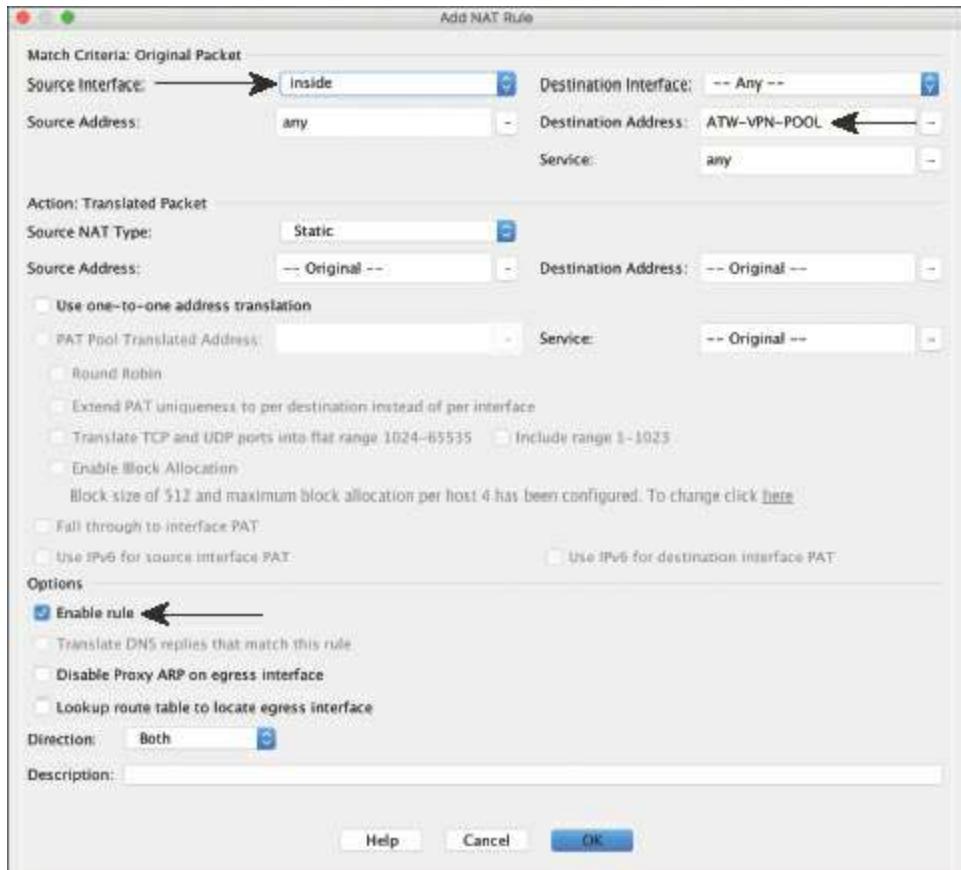
**Step 5.** Change the Destination Address to be the addresses in your client address pool. You can use the network or create a network object.

**Step 6.** In the Action: Translated Packet section, leave the Source NAT Type field set to **Static** and the Source Address field set to **Original**.

**Step 7.** In the Options section, check the **Enable Rule** check box.

**Step 8.** Set the Direction field to **Both**, which ensures that the NAT rule is created for the return traffic as well.

[Figure 19-22](#) shows the completed NAT rule configuration.



**Figure 19-22** Completed NAT Rule

### Step 9. Click OK.

[Figure 19-23](#) shows the completed NAT rule in the NAT table. Ensure that it is at the top of the list, as shown by using the up and down arrows.

#	Match Criteria: Original Packet	Action: Translated Packet					
	Source Intf	Dest Intf	Source	Destination	Service	Source	Destination
1	Inside	any	any	ATW-VPN-POOL	any	-- Original -- (S)	-- Original --
2	DMZ	outside	any	atw-anchor	any	-- atw-anchor-out-- (S)	-- atw-anchor--
3	DMZ	outside	any	any	any	-- atw-anchor-out-- (S)	-- atw-anchor--
4	Inside	outside	any	any	any	-- Outside IP (S)	-- Original --
5	Inside	DMZ	any	dmz-net	any	-- Outside IP (S)	-- Original --
6	DMZ	inside	any	dmz-net	any	-- Original -- (S)	-- Original --
	* Network Object* NAT (Rules 6-86)						
	Any	Any	WLC01	any	any	WLC01-OUT (S)	-- Original --

**Figure 19-23** Completed NAT Rule at Top of NAT Table

### Step 10. Click Apply.

### Step 11. Click Save.

## Configure ISE for the ASA VPN

At this point, all the required configuration in the ASA is complete, and it is time to move to the required configurations in ISE.

The ASA is an access-layer device when it acts as a VPN headend. Instead of an end user plugging in to a Catalyst switch port, or associating to the Wi-Fi SSID of the WLC, the user establishes a tunnel to the ASA.

Exactly like the switches and the WLCs, the ASA is the RADIUS client, and ISE is the RADIUS server. As such, you must ensure that ISE has a configured NAD object for the ASA under **Work Centers > Network Access > Network Resources > Network Devices**, and you must ensure that the RADIUS shared secret matches what was configured in the AAA server object in the ASA configuration. [Figure 19-24](#) shows the configured NAD object in ISE.

Network Devices List > **ATW-TME-5515**

**Network Devices**

\* Name

Description

\* IP Address:  /

\* Device Profile  Cisco

\* Network Device Group

Device Type

IPSEC

Location

Stage

**RADIUS Authentication Settings**

**RADIUS UDP Settings**

Protocol	RADIUS
* Shared Secret	<input type="text" value="*****"/> <input type="button" value="Show"/>
CoA Port	<input type="text" value="1700"/> <input type="button" value="Set To Default"/>

**Figure 19-24** ASA NAD Object in ISE

Next, you need to configure the policy for remote access (go to **Work Centers >**