



SECURITY

## Cisco ISE for BYOD and Secure Unified Access

[ciscopress.com](http://ciscopress.com)

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

FREE SAMPLE CHAPTER



SHARE WITH OTHERS

# Cisco ISE for BYOD and Secure Unified Access

---

Aaron T. Woland, CCIE No. 20113

Jamey Heary, CCIE No. 7680

**Cisco Press**

800 East 96th Street

Indianapolis, IN 46240

# Cisco ISE for BYOD and Secure Unified Access

Aaron Woland

Jamey Heary

Copyright© 2013 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 1 2 3 4 5 6 7 8 9 0

First Printing June 2013

Library of Congress Cataloging-in-Publication Number: 2013938450

ISBN-13: 978-1-58714-325-0

ISBN-10: 1-58714-325-9

## Warning and Disclaimer

This book is designed to provide information about Cisco Identity Services Engine. 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.

## Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact **U.S. Corporate and Government Sales** 1-800-382-3419, [corpsales@pearsontechgroup.com](mailto:corpsales@pearsontechgroup.com).

For sales outside of the U.S., please contact **International Sales** [international@pearsoned.com](mailto:international@pearsoned.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.

**Publisher:** Paul Boger

**Business Operation Manager, Manager Global Certification:**  
Cisco Press: Jan Cornelssen

**Associate Publisher:** Dave Dusthimer

**Senior Development Editor:** Christopher Cleveland

**Executive Editor:** Brett Bartow

**Development Editor:** Marianne Bartow

**Managing Editor:** Sandra Schroeder

**Technical Editors:** Brad Spencer, Chad Sullivan

**Project Editor:** Mandie Frank

**Editorial Assistant:** Vanessa Evans

**Copy Editor:** Sheri Replin

**Indexer:** Lisa Stumpf

**Proofreader:** Sarah Kearns

**Composition:** Jake McFarland

**Cover Designer:** Mark Shirar



**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).

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Stadium/Vision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0812R)

## About the Authors

**Aaron Woland**, CCIE No. 20113, is a Senior Secure Access Engineer at Cisco Systems and works with Cisco's largest customers all over the world. His primary job responsibilities include secure access and ISE deployments, solution enhancements, futures, and escalations. Aaron joined Cisco in 2005 and is currently a member of numerous security advisory boards. Prior to joining Cisco, he spent 12 years as a consultant and technical trainer. His areas of expertise include network and host security architecture and implementation, regulatory compliance, and routing and switching. Aaron is the author of many white papers and design guides, including the *TrustSec 2.0 Design and Implementation Guide* and the *NAC Layer 3 OOB Using VRFs for Traffic Isolation* design guide. He is also a distinguished speaker at Cisco Live for topics related to identity and is a security columnist for *Network World*, where he blogs on all things related to identity. Additional certifications include CCSP, CCNP, CCDP, Certified Ethical Hacker, MCSE, and many other industry certifications.

**Jamey Heary**, CCIE No. 7680, is a Distinguished Systems Engineer at Cisco Systems, where he works as a trusted security advisor to Cisco customers and business groups. He is also a featured security columnist for *Network World*, where he blogs on all things security. Jamey sits on the PCI Security Standards Council-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 pending on a new DDoS mitigation technique. Jamey sits on numerous security advisory boards for Cisco Systems and is a founding member of the Colorado Healthcare InfoSec Users Group. His other certifications include CISSP, and he is a Certified HIPAA Security Professional. He has been working in the IT field for 19 years and in IT security for 15 years.

## About the Technical Reviewers

**Brad Spencer**, CCIE No. 25971 (Security), has worked as a senior security engineer and architect in a consulting capacity for multiple fortune 100 companies since 1997. In the last 16 years, Brad has concentrated on Cisco Security products through consulting as being a Cisco Certified Systems Instructor (CCSI). Brad is currently the Program Manager of Identity Solutions at Priveon, with the primary focus on Cisco Security and Identity products.

**Chad Sullivan** is CEO and co-owner of Priveon, Inc., a networking and security consulting organization that works with customers globally to deploy and integrate various solutions into customer environments. Prior to starting Priveon, Chad was a Security Consulting Systems Engineer (CSE) at Cisco Systems in Atlanta, GA. Chad holds many certifications, including a triple CCIE (Route-Switch, SNA/IP, and Security). Chad is known across the networking and security industries for his experience, which also includes endpoint security where he has written two books (Cisco Security Agent). Chad has also assisted by contributing to other books as well, by providing content for a NAC Appliance book available from Cisco Press. Today, Chad spends most of his professional time consulting with customers, researching current security trends, and speaking at various public events and seminars.

## Dedications

This book is dedicated first to my Mom and Dad, who have always believed in me and supported me in everything I've ever done, encouraged me to never stop learning, taught me the value of hard work, and to pursue a career in something I love. Secondly to my wife, Suzanne, without her continued love, support, guidance, wisdom, encouragement, and patience, this book would surely not exist. To my two awesome children—Eden and Nyah—who are my inspiration, my pride and joy, and who continue to make me want to be a better man. Lastly, to my grandparents, who have taught me what it means to be alive and the true definition of courage and perseverance.

—Aaron

This book is dedicated to my loving wife and two incredible sons, Liam and Conor. Without your support and sacrifice, this book would not have been possible. Thanks for putting up with the late nights and weekends I had to spend behind the keyboard instead of playing games, Legos, soccer, or some other fun family activity. You are all the greatest!

—Jamey

# Acknowledgments

## From Aaron:

To Thomas Howard and Allan Bolding from Cisco for their continued support, encouragement, and guidance. I could not have done it without you.

To Craig Hyps, a Senior Technical Marketing Engineer at Cisco, for his deep technical knowledge on absolutely everything and his guidance on content found throughout this book. Craig, you are a true inspiration and you drive me to be better every day.

To Jamey Heary, Distinguished Systems Engineer: Thank you for being crazy enough to agree to take the plunge with me. You've been a terrific writing partner and friend.

To Christopher Heffner, a Technical Marketing Engineer at Cisco, for convincing me to step up and take a swing at this book. Without his words of encouragement and guidance, this book would not exist.

To Paul Forbes, a Product Owner at Cisco, who sets an example to aspire to. Without Paul's continued passion, focus, dedication, and drive to make ISE the best product ever, none of us would have this amazing solution to work with.

To Darrin Miller and Nancy Cam-Winget, Distinguished Engineers who set the bar so incredibly high. You are both truly inspirational people to look up to, and I appreciate all the guidance you give me.

To the original cast members of the one and only SSU, especially Jason Halpern, Danelle Au, Mitsunori Sagae, Fay-Ann Lee, Pat Calhoun, Jay Bhansali, AJ Shipley, Joseph Salowey, Thomas Howard, Darrin Miller, Ron Tisinger, Brian Gonsalves, and Tien Do.

To Jonny Rabinowitz, Mehdi Bouzouina, Eddie Mendonca, Pramod Badjate, and all the other members of the world's greatest engineering team. You guys continue to show the world what it means to be "world class."

To my colleagues Naasief Edross, Jeremy Hyman, Kevin Sullivan, Mason Harris, David Anderson, Luc Billot, Jesse Dubois, Jay Young Taylor, Hsing-Tsu Lai, Dave White Jr., Nevin Absher, Ned Zaldivar, Mark Kassem, Greg Tillett, Chuck Parker, Jason Frazier, Shelly Cadora, Ralph Schmieder, Corey Elinburg, Scott Kenewell, Larry Boggis, Chad Sullivan, Dave Klein, and so many more! The contributions you make to this industry inspire me.

To the technical reviewers, Chad Sullivan and Brad Spencer, who provided excellent technical coverage and kept this book accurate and easy to navigate. Your suggestions and guidance are evidenced on nearly every page!

Finally, to the Cisco Press team: Brett Bartow, the executive editor, for seeing the value and vision provided in the original proposal and believing enough to provide me the opportunity to build this book. In addition, Marianne Bartow (Neil), Christopher Cleveland, Mandie Frank, and Sheri Replin, who have put up with my inability to utilize the English language in the manner deemed appropriate by Cisco Press, and who have



been there every step of the way. Your guidance, perseverance, and ability to constantly remind Jamey and I of our deadlines are much appreciated! Lastly, everyone else in the Cisco Press team who spent countless hours normalizing the manuscript, its technical drawings and content; their effort can be seen throughout this book pertaining to my ideas, words, and pictures, presented in ways that I could never have imagined.

### **From Jamey:**

I echo Aaron's sentiments, which are previously shown. So many people have made it possible for this book to exist, and for that matter, for this most excellent solution to exist to write about in the first place. Great job to SAMPG, your tireless efforts are bearing fruit. Thank you.

Thank you to Aaron Woland, for pushing the idea of us writing this 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. Lastly, a huge thanks for picking up my slack when things got crazy, thus allowing us to publish this on time. It was a fun ride.

Thank you, Tony Kelly and John Graham. Without your coaching, backing, and support as my manager, this book wouldn't have happened. Thanks for making it possible.

Thank you to Greg Edwards, for your mentorship and advice as I transitioned into the DSE role and contemplated whether writing another book was a good fit. You got it right again; it was a good idea and good fit.

Thank you to the tech editors and Cisco Press team. As Aaron stated, your contributions and tireless efforts are supremely appreciated.

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

# Contents at a Glance

Introduction xxvi

## **Section I The Evolution of Identity Enabled Networks**

- Chapter 1 Regain Control of Your IT Security 1
- Chapter 2 Introducing Cisco Identity Services Engine 7

## **Section II The Blueprint, Designing an ISE Enabled Network**

- Chapter 3 The Building Blocks in an Identity Services Engine Design 15
- Chapter 4 Making Sense of All the ISE Deployment Design Options 29
- Chapter 5 Following a Phased Deployment 37

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

- Chapter 6 Building a Cisco ISE Network Access Security Policy 47
- Chapter 7 Building a Device Security Policy 67
- Chapter 8 Building an ISE Accounting and Auditing Policy 83

## **Section IV Configuration**

- Chapter 9 The Basics: Principal Configuration Tasks for Cisco ISE 95
- Chapter 10 Profiling Basics 127
- Chapter 11 Bootstrapping Network Access Devices 169
- Chapter 12 Authorization Policy Elements 205
- Chapter 13 Authentication and Authorization Policies 215
- Chapter 14 Guest Lifecycle Management 249
- Chapter 15 Device Posture Assessment 279
- Chapter 16 Supplicant Configuration 301
- Chapter 17 BYOD: Self-Service Onboarding and Registration 319
- Chapter 18 Setting Up a Distributed Deployment 377
- Chapter 19 Inline Posture Node 391

## **Section V Deployment Best Practices**

- Chapter 20 Deployment Phases 395
- Chapter 21 Monitor Mode 411
- Chapter 22 Low-Impact Mode 443
- Chapter 23 Closed Mode 459

## **Section VI Advanced Secure Unified Access Features**

- Chapter 24 Advanced Profiling Configuration 475
- Chapter 25 Security Group Access 495
- Chapter 26 MACSec and NDAC 547
- Chapter 27 Network Edge Authentication Topology 569

## **Section VII Monitoring, Maintenance, and Troubleshooting**

- Chapter 28 Understanding Monitoring and Alerting 577
- Chapter 29 Troubleshooting 589
- Chapter 30 Backup, Patching, and Upgrading 619
- Appendix A Sample User Community Deployment Messaging Material 635
- Appendix B Sample ISE Deployment Questionnaire 639
- Appendix C Configuring the Microsoft CA for BYOD 645
- Appendix D Using a Cisco IOS Certificate Authority for BYOD Onboarding 669
- Appendix E Sample Switch Configurations 675
- Index 689

# Contents

**Introduction xxvi**

## **Section I The Evolution of Identity Enabled Networks**

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

Security: A Weakest-Link Problem with Ever More Links 2

Cisco Identity Services Engine 3

Sources for Providing Identity and Context Awareness 4

Unleash the Power of Centralized Policy 5

Summary 6

### **Chapter 2 Introducing Cisco Identity Services Engine 7**

Systems Approach to Centralized Network Security Policy 7

What Is the Cisco Identity Services Engine? 9

ISE Authorization Rules 12

Summary 13

## **Section II The Blueprint, Designing an ISE Enabled Network**

### **Chapter 3 The Building Blocks in an Identity Services Engine Design 15**

ISE Solution Components Explained 15

Infrastructure Components 16

Policy Components 20

Endpoint Components 20

ISE Personas 21

ISE Licensing, Requirements, and Performance 22

ISE Licensing 23

ISE Requirements 23

ISE Performance 25

ISE Policy-Based Structure Explained 27

Summary 28

### **Chapter 4 Making Sense of All the ISE Deployment Design Options 29**

Centralized Versus Distributed Deployment 29

Centralized Deployment 30

Distributed Deployment 32

Summary 35

**Chapter 5 Following a Phased Deployment 37**

Why Use a Phased Deployment Approach? 37

Monitor Mode 38

Choosing Your End-State Mode 40

End-State Choice 1: Low-Impact Mode 42

End-State Choice 2: Closed Mode 44

Transitioning from Monitor Mode into an End-State Mode 45

Summary 46

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

**Chapter 6 Building a Cisco ISE Network Access Security Policy 47**

What Makes Up a Cisco ISE Network Access Security Policy? 47

Network Access Security Policy Checklist 48

Involving the Right People in the Creation of the Network Access Security Policy 49

Determining the High-Level Goals for Network Access Security 51

Common High-Level Network Access Security Goals 52

Defining the Security Domains 55

Understanding and Defining ISE Authorization Rules 57

Commonly Configured Rules and Their Purpose 58

Establishing Acceptable Use Policies 59

Defining Network Access Privileges 61

Enforcement Methods Available with ISE 61

Commonly Used Network Access Security Policies 62

Summary 65

**Chapter 7 Building a Device Security Policy 67**

Host Security Posture Assessment Rules to Consider 67

Sample NASP Format for Documenting ISE Posture Requirements 72

Common Checks, Rules, and Requirements 74

Method for Adding Posture Policy Rules 74

*Research and Information 75*

*Establishing Criteria to Determine the Validity of a Security Posture Check, Rule, or Requirement in Your Organization 76*

*Method for Determining Which Posture Policy Rules a Particular Security Requirement Should Be Applied To 77*

*Method for Deploying and Enforcing Security Requirements* 78

ISE Device Profiling 79

ISE Profiling Policies 80

ISE Profiler Data Sources 81

Using Device Profiles in Authorization Rules 82

Summary 82

## **Chapter 8 Building an ISE Accounting and Auditing Policy 83**

Why You Need Accounting and Auditing for ISE 83

Using PCI DSS as Your ISE Auditing Framework 84

ISE Policy for PCI 10.1: Ensuring Unique Usernames and Passwords 87

ISE Policy for PCI 10.2 and 10.3: Audit Log Collection 89

ISE Policy for PCI 10.5.3, 10.5.4, and 10.7: Ensure the Integrity and Confidentiality of Log Data 90

ISE Policy for PCI 10.6: Review Audit Data Regularly 91

Cisco ISE User Accounting 92

Summary 94

## **Section IV Configuration**

### **Chapter 9 The Basics: Principal Configuration Tasks for Cisco ISE 95**

Bootstrapping Cisco ISE 95

Using the Cisco ISE Setup Assistant Wizard 98

Configuring Network Devices for ISE 106

Wired Switch Configuration Basics 106

Wireless Controller Configuration Basics 109

Completing the Basic ISE Setup 113

Install ISE Licenses 113

ISE Certificates 114

Installing ISE Behind a Firewall 116

Role-Based Access Control for Administrators 121

RBAC for ISE GUI 121

*RBAC: Session and Access Settings and Restrictions* 121

*RBAC: Authentication* 123

*RBAC: Authorization* 124

Summary 126

**Chapter 10 Profiling Basics 127**

Understanding Profiling Concepts	127
Probes	130
<i>Probe Configuration</i>	130
<i>Deployment Considerations</i>	133
DHCP	134
<i>Deployment Considerations</i>	135
NetFlow	137
<i>Deployment Considerations</i>	137
RADIUS	137
<i>Deployment Considerations</i>	138
Network Scan (NMAP)	138
<i>Deployment Considerations</i>	139
DNS	139
<i>Deployment Considerations</i>	139
SNMP	140
<i>Deployment Considerations</i>	140
IOS Device-Sensor	141
Change of Authorization	142
CoA Message Types	142
<i>Configuring Change of Authorization in ISE</i>	143
Infrastructure Configuration	144
DHCP Helper	145
SPAN Configuration	145
VLAN Access Control Lists (VACL)	146
VMware Configurations to Allow Promiscuous Mode	148
Best Practice Recommendations	149
Examining Profiling Policies	152
Endpoint Profile Policies	152
Cisco IP Phone 7970 Example	155
Using Profiles in Authorization Policies	161
Endpoint Identity Groups	161
EndPointPolicy	163
Logical Profiles	164
Feed Service	166
Configuring the Feed Service	166
Summary	168

**Chapter 11 Bootstrapping Network Access Devices 169**

Bootstrap Wizard 169

Cisco Catalyst Switches 170

Global Configuration Settings for All Cisco IOS 12.2 and 15.x  
Switches 170*Configure Certificates on a Switch* 170*Enable the Switch HTTP/HTTPS Server* 170*Global AAA Commands* 171*Global RADIUS Commands* 172*Create Local Access Control Lists* 174*Global 802.1X Commands* 175*Global Logging Commands (Optional)* 175*Global Profiling Commands* 177

Interface Configuration Settings for All Cisco Switches 179

*Configure Interfaces as Switch Ports* 179*Configure Flexible Authentication and High Availability* 179*Configure Authentication Settings* 182*Configure Authentication Timers* 184*Apply the Initial ACL to the Port and Enable Authentication* 184

Cisco Wireless LAN Controllers 184

Configure the AAA Servers 185

*Add the RADIUS Authentication Servers* 185*Add the RADIUS Accounting Servers* 186*Configure RADIUS Fallback (High Availability)* 187

Configure the Airespace ACLs 188

*Create the Web Authentication Redirection ACL* 188*Create the Posture Agent Redirection ACL* 191

Create the Dynamic Interfaces for the Client VLANs 193

*Create the Employee Dynamic Interface* 193*Create the Guest Dynamic Interface* 194

Create the Wireless LANs 195

*Create the Guest WLAN* 195*Create the Corporate SSID* 199

Summary 202



**Chapter 12 Authorization Policy Elements 205**

- Authorization Results 206
  - Configuring Authorization Downloadable ACLs 207
  - Configuring Authorization Profiles 209
- Summary 212

**Chapter 13 Authentication and Authorization Policies 215**

- Relationship Between Authentication and Authorization 215
- Authentication Policies 216
  - Goals of an Authentication Policy 216
  - Accept Only Allowed Protocols* 216
  - Route to the Correct Identity Store* 216
  - Validate the Identity* 217
  - Pass the Request to the Authorization Policy* 217
- Understanding Authentication Policies 217
  - Conditions 218
  - Allowed Protocols* 220
  - Identity Store* 224
  - Options* 224
  - Common Authentication Policy Examples 224
    - Using the Wireless SSID* 225
    - Remote-Access VPN* 228
    - Alternative ID Stores Based on EAP Type* 230
- Authorization Policies 232
  - Goals of Authorization Policies 232
  - Understanding Authorization Policies* 233
  - Role-Specific Authorization Rules* 237
  - Authorization Policy Example 237
    - Employee and Corporate Machine Full-Access Rule* 238
    - Internet Only for iDevices* 240
    - Employee Limited Access Rule* 243
- Saving Attributes for Re-Use 246
- Summary 248

**Chapter 14 Guest Lifecycle Management 249**

- Guest Portal Configuration 251
  - Configuring Identity Source(s) 252
- Guest Sponsor Configuration 254
  - Guest Time Profiles 254

Guest Sponsor Groups	255
Sponsor Group Policies	257
Authentication and Authorization Guest Policies	258
Guest Pre-Authentication Authorization Policy	258
Guest Post-Authentication Authorization Policy	262
Guest Sponsor Portal Configuration	263
Guest Portal Interface and IP Configuration	264
Sponsor and Guest Portal Customization	264
<i>Customize the Sponsor Portal</i>	264
<i>Creating a Simple URL for Sponsor Portal</i>	265
<i>Guest Portal Customization</i>	265
<i>Customizing Portal Theme</i>	266
<i>Creating Multiple Portals</i>	268
Guest Sponsor Portal Usage	271
Sponsor Portal Layout	271
Creating Guest Accounts	273
Managing Guest Accounts	273
Configuration of Network Devices for Guest CWA	274
Wired Switches	274
Wireless LAN Controllers	275
Summary	277

## **Chapter 15 Device Posture Assessment 279**

ISE Posture Assessment Flow	280
Configure Global Posture and Client Provisioning Settings	283
Posture Client Provisioning Global Setup	283
Posture Global Setup	285
<i>General Settings</i>	285
<i>Reassessments</i>	286
<i>Updates</i>	287
<i>Acceptable Use Policy</i>	287
Configure the NAC Agent and NAC Client Provisioning Settings	288
Configure Posture Conditions	289
Configure Posture Remediation	292
Configure Posture Requirements	295
Configure Posture Policy	296
Enabling Posture Assessment in the Network	298
Summary	299

## **Chapter 16 Supplicant Configuration 301**

- Comparison of Popular Supplicants 302
- Configuring Common Supplicants 303
  - Mac OS X 10.8.2 Native Supplicant Configuration 303
  - Windows GPO Configuration for Wired Supplicant 305
  - Windows 7 Native Supplicant Configuration 309
  - Cisco AnyConnect Secure Mobility Client NAM 312
- Summary 317

## **Chapter 17 BYOD: Self-Service Onboarding and Registration 319**

- BYOD Challenges 320
- Onboarding Process 322
  - BYOD Onboarding 322
    - Dual SSID* 322
    - Single SSID* 323
    - Configuring NADs for Onboarding* 324
    - ISE Configuration for Onboarding* 329
    - End-User Experience* 330
    - Configuring ISE for Onboarding* 347
    - BYOD Onboarding Process Detailed* 357
  - MDM Onboarding 367
    - Integration Points* 367
    - Configuring MDM Integration* 368
    - Configuring MDM Onboarding Policies* 369
- Managing Endpoints 372
  - Self Management 373
  - Administrative Management 373
- The Opposite of BYOD: Identify Corporate Systems 374
  - EAP Chaining 375
- Summary 376

## **Chapter 18 Setting Up a Distributed Deployment 377**

- Configuring ISE Nodes in a Distributed Environment 377
  - Make the Policy Administration Node a Primary Device 377
  - Register an ISE Node to the Deployment 379
  - Ensure the Persona of All Nodes Is Accurate 381
- Understanding the HA Options Available 382
  - Primary and Secondary Nodes 382

<i>Monitoring and Troubleshooting Nodes</i>	382
Policy Administration Nodes	384
Promoting the Secondary PAN to Primary	385
Node Groups	385
Create a Node Group	386
Add the Policy Services Nodes to the Node Group	387
Using Load Balancers	388
General Guidelines	388
Failure Scenarios	389
Summary	390

## **Chapter 19 Inline Posture Node 391**

Use Cases for the Inline Posture Node	391
Overview of IPN Functionality	392
IPN Configuration	393
IPN Modes of Operation	393
Summary	394

## **Section V Deployment Best Practices**

### **Chapter 20 Deployment Phases 395**

Why Use a Phased Approach?	395
A Phased Approach	397
Authentication Open Versus Standard 802.1X	398
Monitor Mode	399
Prepare ISE for a Staged Deployment	401
<i>Create the Network Device Groups</i>	401
<i>Create the Policy Sets</i>	403
Low-Impact Mode	404
Closed Mode	406
Transitioning from Monitor Mode to Your End State	408
Wireless Networks	409
Summary	410

### **Chapter 21 Monitor Mode 411**

Endpoint Discovery	412
SNMP Trap Method	413
<i>Configuring the ISE Probes</i>	414

<i>Adding the Network Device to ISE</i>	416
<i>Configuring the Switches</i>	418
RADIUS with SNMP Query Method	420
<i>Configuring the ISE Probes</i>	420
<i>Adding the Network Device to ISE</i>	421
<i>Configuring the Switches</i>	422
Device Sensor Method	424
<i>Configuring the ISE Probes</i>	425
<i>Adding the Network Device to ISE</i>	425
<i>Configuring the Switches</i>	426
Using Monitoring to Identify Misconfigured Devices	428
Tuning the Profiling Policies	428
Creating the Authentication Policies for Monitor Mode	430
Creating Authorization Policies for Non-Authenticating Devices	433
<i>IP-Phones</i>	433
<i>Wireless APs</i>	435
<i>Printers</i>	436
Creating Authorization Policies for Authenticating Devices	438
<i>Machine Authentication (Machine Auth)</i>	438
<i>User Authentications</i>	439
<i>Default Authorization Rule</i>	440
Summary	441

## **Chapter 22 Low-Impact Mode 443**

Transitioning from Monitor Mode to Low-Impact Mode	445
Configuring ISE for Low-Impact Mode	446
Set Up the Low-Impact Mode Policy Set in ISE	446
<i>Duplicate the Monitor Mode Policy Set</i>	446
<i>Create the Web Authentication Authorization Result</i>	448
<i>Configure the Web Authentication Identity Source Sequence</i>	451
<i>Modify the Default Rule in the Low-Impact Policy Set</i>	451
Assign the WLCs and Switches to the Low-Impact Stage NDG	452
Modify the Default Port ACL on the Switches That Will Be Part of Low-Impact Mode	453
Monitoring in Low-Impact Mode	454
Tightening Security	454
Creating AuthZ Policies for the Specific Roles	454

- Change Default Authentication Rule to Deny Access 456
- Moving Switch Ports from Multi-Auth to Multi-Domain 457
- Summary 458

## **Chapter 23 Closed Mode 459**

- Transitioning from Monitor Mode to Closed Mode 461
- Configuring ISE for Closed Mode 461
  - Set Up the Closed Mode Policy Set in ISE 461
  - Duplicate the Monitor Mode Policy Set* 462
  - Create the Web Authentication Authorization Result* 463
  - Configure the Web Authentication Identity Source Sequence* 466
  - Modify the Default Rule in the Closed Policy Set* 467
- Assign the WLCs and Switches to the Closed Stage NDG 468
- Modify the Default Port ACL on the Switches That Will Be Part of Closed Mode 469
- Monitoring in Closed Mode 469
- Tightening Security 469
  - Creating Authorization Policies for the Specific Roles 470
  - Change Default Authentication Rule to Deny Access 472
  - Moving Switch Ports from Multi-Auth to MDA 473
- Summary 474

## **Section VI Advanced Secure Unified Access Features**

### **Chapter 24 Advanced Profiling Configuration 475**

- Creating Custom Profiles for Unknown Endpoints 475
  - Identifying Unique Values for an Unknown Device 476
  - Collecting Information for Custom Profiles 478
  - Creating Custom Profiler Conditions 479
  - Creating Custom Profiler Policies 480
- Advanced NetFlow Probe Configuration 481
  - Commonly Used NetFlow Attributes 483
  - Example Profiler Policy Using NetFlow 483
  - Designing for Efficient Collection of NetFlow Data 484
  - Configuration of NetFlow on Cisco Devices 485
- Profiler COA and Exceptions 488
  - Types of CoA 489
  - Creating Exceptions Actions 489

Configuring CoA and Exceptions in Profiler Policies	490
Profiler Monitoring and Reporting	491
Summary	494

## **Chapter 25 Security Group Access 495**

Ingress Access Control Challenges	495
VLAN Assignment	495
Ingress Access Control Lists	498
What Is Security Group Access?	499
So, What Is a Security Group Tag?	500
<i>Defining the SGTs</i>	501
<i>Classification</i>	504
<i>Dynamically Assigning SGT via 802.1X</i>	504
<i>Manually Assigning SGT at the Port</i>	506
<i>Manually Binding IP Addresses to SGTs</i>	506
<i>Access Layer Devices That Do Not Support SGTs</i>	507
Transport: Security Group eXchange Protocol (SXP)	508
SXP Design	508
<i>Configuring SXP on IOS Devices</i>	509
<i>Configuring SXP on Wireless LAN Controllers</i>	511
<i>Configuring SXP on Cisco ASA</i>	513
Transport: Native Tagging	516
Configuring Native SGT Propagation (Tagging)	517
<i>Configuring SGT Propagation on Cisco IOS Switches</i>	518
<i>Configuring SGT Propagation on a Catalyst 6500</i>	520
<i>Configuring SGT Propagation on a Nexus Series Switch</i>	522
Enforcement	523
SGACL	524
<i>Creating the SG-ACL in ISE</i>	526
<i>Configure ISE to Allow the SGACLs to Be Downloaded</i>	531
<i>Configure the Switches to Download SGACLs from ISE</i>	532
<i>Validating the PAC File and CTS Data Downloads</i>	533
Security Group Firewalls	535
<i>Security Group Firewall on the ASA</i>	535
<i>Security Group Firewall on the ISR and ASR</i>	543
Summary	546

**Chapter 26 MACSec and NDAC 547**

MACSec 548

Downlink MACSec 549

*Switch Configuration Modes* 551*ISE Configuration* 552*Uplink MACSec* 553

Network Device Admission Control 557

Creating an NDAC Domain 558

*Configuring ISE* 558*Configuring the Seed Device* 562*Adding Non-Seed Switches* 564*Configuring the Switch Interfaces for Both Seed and Non-Seed* 566

MACSec Sequence in an NDAC Domain 567

Summary 568

**Chapter 27 Network Edge Authentication Topology 569**

NEAT Explained 570

Configuring NEAT 571

Preparing ISE for NEAT 571

*Create the User Identity Group and Identity* 571*Create the Authorization Profile* 572*Create the Authorization Rule* 573

Access Switch (Authenticator) Configuration 574

Desktop Switch (Supplicant) Configuration 574

Summary 575

**Section VII Monitoring, Maintenance, and Troubleshooting****Chapter 28 Understanding Monitoring and Alerting 577**

ISE Monitoring 577

Live Authentications Log 578

Monitoring Endpoints 580

Global Search 581

Monitoring Node in a Distributed Deployment 584

Device Configuration for Monitoring 584

ISE Reporting 585

Data Repository Setup 586

ISE Alarms 587

Summary 588



**Chapter 29 Troubleshooting 589**

- Diagnostics Tools 589
  - RADIUS Authentication Troubleshooting 589
  - Evaluate Configuration Validator 591
  - TCP Dump 594
- Troubleshooting Methodology 596
  - Troubleshooting Authentication and Authorization 596
    - Option 1: No Live Log Entry Exists* 597
    - Option 2: An Entry Exists in the Live Log* 603
  - General High-Level Troubleshooting Flowchart 605
  - Troubleshooting WebAuth and URL Redirection 605
  - Active Directory Is Disconnected 610
  - Debug Situations: ISE Logs 611
    - The Support Bundle* 611
- Common Error Messages and Alarms 613
  - EAP Connection Timeout 613
  - Dynamic Authorization Failed 615
  - WebAuth Loop 617
  - Account Lockout 617
- ISE Node Communication 617
- Summary 618

**Chapter 30 Backup, Patching, and Upgrading 619**

- Repositories 619
  - Configuring a Repository 619
- Backup 625
- Restore 628
  - Patching 629
  - Upgrading 632
- Summary 634

**Appendix A Sample User Community Deployment Messaging Material 635**

**Appendix B Sample ISE Deployment Questionnaire 639**

**Appendix C Configuring the Microsoft CA for BYOD 645**

**Appendix D Using a Cisco IOS Certificate Authority for BYOD Onboarding 669**

**Appendix E Sample Switch Configurations 675**

**Index 689**

## 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 Unified 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 the device type, location, management status, operating-system patch level, and ensuring anti-malware software is running and up to date.

This book addresses the complete lifecycle of protecting a modern borderless network using Cisco Secure Unified 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, and Security Group Access 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.

## Objectives of This Book

This book helps the reader understand, design, and deploy the next-generation of Network Access Control: Cisco's Secure Unified Access system. This system combines 802.1X, profiling, posture assessments, device onboarding, and Guest Lifecycle management. Cisco ISE for Secure Unified Access teaches readers about the business cases that an identity solution can help solve. It examines identifying users, devices, security policy compliance (posture), and the technologies that make all this possible. This book details the Secure Unified Access solution and how to plan and design a network for this next

generation of access control, and all it can offer a customer environment, from device isolation to protocol-independent network segmentation. This book gives readers a single reference to find the complete configuration for an integrated identity solution. All sections of this book use both best practices and real-world examples.

## Who Should Read This Book?

The 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's ISE and 802.1X, as well as Bring Your Own Device (BYOD) or Choose Your Own Device (CYOD) information-technology models.

## How This Book Is Organized

This book is organized into 30 chapters distributed across 7 sections. Although it can be read cover to cover, readers can move between chapters and sections, covering only the content that interests them. The seven sections on the book are

**Section I, “The Evolution of Identity-Enabled Networks”:** 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 section covers 802.1X, NAC framework, NAC appliance, the evolution into Secure Unified Access, and the creation of the 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.

**Section II, “The Blueprint, Designing an ISE-Enabled Network”:** Covers the high-level design phase of a Secure Unified Access project. Solution diagrams are included. This section covers the different functions available on the ISE, how to distribute these functions, and the rollout phases of the solution: Monitor Mode, Low-Impact Mode, and Closed Mode. Additionally, the solution taxonomy is explained. 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 sections.

**Section 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 access project. This section 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 section to aid in the readers' understanding of the process, how communication occurs and in what order, as well as how to configure the miscellaneous device supplicants.

**Section IV, “Configuration”:** Details the step-by-step configuration of the ISE, the network access devices, and supplicants. The goal of this section is to have the entire infrastructure and policy management configured and ready to begin the actual deployment in Section V.

**Section V, “Deployment Best Practices”:** Walks readers through a phased deployment. It starts by explaining the different phases of deployment and how to ensure zero downtime. This section begins with a description followed by the actual step-by-step deployment guides, how to use the monitoring tools to build out the correct policies and profiling tuning, and how to move from phase to phase. This section provides the reader with insight into the best practices, caveats, common mistakes, deployment lessons learned, tricks of the trade, and rules to live by.

**Section VI, “Advanced Secure Unified Access Features”:** Details some of the more advanced solution features that truly differentiate Secure Unified Access as a system.

**Section VII, “Monitoring, Maintenance, and Troubleshooting”:** Examines the maintenance of ISE, backups, and upgrades. It covers how to troubleshoot not only ISE, but the entire Secure Unified Access system, and how to use the tools provided in the ISE solution. Common monitoring and maintenance tasks, as well as troubleshooting tools, are explained from a help-desk support technician's point of view.

Here is an overview of each of the 30 chapters:

- **Chapter 1, “Regain Control of Your IT Security”:** 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, “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 new product and provides an overview of its functions and capabilities.
- **Chapter 3: “The Building Blocks in an Identity Services Engine Design”:** This chapter covers the components of the Secure Unified Access solution, including ISE personas, licensing model, and the policy structure.
- **Chapter 4: “Making Sense of All the ISE Deployment Design Options”:** This chapter examines all the available personas in ISE and design options with the combination of those personas.
- **Chapter 5: “Following a Phased Deployment”:** Implementing secure access with a phased approach to deployment is critical to the success of the project. Cisco provided three modes to assist with this phased approach: Monitor Mode,

Low-Impact Mode, and Closed Mode. This chapter briefly summarizes the importance of following this phased approach to deployment.

- **Chapter 6: “Building a Cisco ISE Network Access Security Policy”:** 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 enforces that policy network-wide. This chapter focuses on the creation of that NASP.
- **Chapter 7: “Building a Device Security Policy”:** This chapter explores Host Security Posture Assessment and Device Profiling features in some detail in order to disclose the different ways in which ISE identifies device types and determines their security posture.
- **Chapter 8: “Building an ISE Accounting and Auditing Policy”:** This chapter delves into the creation of accounting and audit policies, including administrator configuration changes, ISE system health, processing of ISE rules, and full logging of authentication and authorization activities.
- **Chapter 9: “The Basics: Principal Configuration Tasks for Cisco ISE”:** This chapter provides a high-level overview of the ISE personas, walks the reader through the initial configuration (called bootstrapping) of ISE itself, and role-based access control (RBAC).
- **Chapter 10: “Profiling Basics”:** 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 network access devices (NAD) themselves and focuses on best practices to ensure a successful ongoing deployment.
- **Chapter 12: “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, the pieces that make up the policy, and provides examples of how to create a policy in ISE that enforces the logical policies created out of 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: “Device Posture Assessments”:** 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: “Supplicant 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 Bring Your Own Device (BYOD) concepts, policies, and flows. Both the user and administrative experiences are detailed, as well as introducing the new integration between ISE and third-party MDM vendors.
- **Chapter 18: “Setting Up a Distributed Deployment”:** Cisco ISE can be deployed in a scalable distributed model as well as a standalone device. This chapter examines the way ISE may be deployed in this distributed model, and the caveats associated, as well as detailing high availability (HA) with technologies such as load balancing.
- **Chapter 19: “Inline Posture Node”:** This chapter overviews the Inline Posture Node and its deployment into a network.
- **Chapter 20: “Deployment Phases”:** This key chapter builds on Chapter 5, going into more detail and beginning the foundational configuration for a phased deployment approach.
- **Chapter 21: “Monitor Mode”:** This chapter details the configuration and the flow during the Monitor Mode phase of deployment to ensure zero downtime for the end users.
- **Chapter 22: “Low-Impact Mode”:** This chapter examines the configuration and the flow for the Low-Impact Mode end-state of deployment.
- **Chapter 23: “Closed Mode”:** This chapter details the configuration and the flow for the Low-Impact Mode end-state of deployment.
- **Chapter 24: “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 25: “Security Group Access”:** This chapter introduces the next-generation tagging enforcement solution, examining classification, transport, and enforcement.
- **Chapter 26: “MACSec and NDAC”:** This chapter covers the layering of Layer 2 encryption on top of the deployment to secure the traffic flows and the Security Group Tags from Chapter 25. It also examines the network device admission control features that provide access control for network devices and forms domains of trusted network devices.
- **Chapter 27: “Network Edge Access Topology”:** This chapter discusses the concept and configuration of this unique capability for extending secure access networks beyond the wiring closet.
- **Chapter 28: “Understanding Monitoring and Alerting”:** This chapter explains

the extensive and redesigned monitoring, reporting, and alerting mechanisms built into the ISE solution.

- **Chapter 29: “Troubleshooting”:** This chapter aids the reader when having to troubleshoot the Secure Unified Access system and its many moving parts.
- **Chapter 30: “Backup, Patching, and Upgrading”:** Provides a detailed discussion and procedural walk-through on the available backup, restore, patching, and upgrading of ISE.
- **Appendix A: Sample User Community Deployment Messaging Material**
- **Appendix B: Sample ISE Deployment Questionnaire**
- **Appendix C: Configuring the Microsoft CA for BYOD**
- **Appendix D: Using a Cisco IOS Certificate Authority for BYOD Onboarding**
- **Appendix E: Sample Switch Configurations**



*This page intentionally left blank*

## Authentication and Authorization Policies

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 those authorization results, such as Downloadable Access Lists and Authorization Profiles to accommodate the enforcement of that “paper policy.”

These authorization results 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 12. 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 wireless backgrounds, tend to confuse these terms and what they actually do. Wireless is used as an example here, because it went through such tremendous growth over the last few years, and with that growth, appeared increased security. 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 were to go into a bank and request a withdrawal from an account, it 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 United States or a Military ID)?

Let's say, for conversations sake, that you handed them 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.

## Authentication Policies

Authentication policies have a few goals, but the ultimate end goal of an Authentication Policy is to determine if the identity credential is valid or not.

### Goals of an Authentication Policy

Authentication Policies have a few goals:

1. Drop traffic that isn't allowed and prevent it 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 over 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 Policy Service nodes down and use the Authentication Protocol to help choose the right identity store.

### Route to the Correct Identity Store

Once the authentication is accepted, ISE makes a routing decision. The identity store that should be checked is based on the incoming authentication. Obviously, if a certificate is being presented, ISE should not try and validate that certificate against the internal users 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

Once the correct identity store has been identified, ISE confirms the credentials are valid. If it's a username/password, do those match what is in the directory store? If it's a certificate, does ISE trust the certificate signer? Was that certificate revoked?

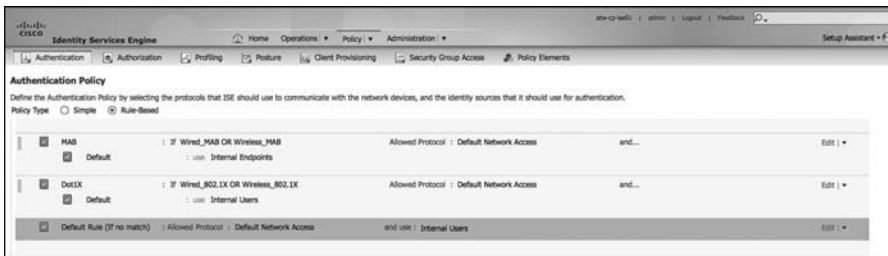
## Pass the Request to the Authorization Policy

If the authentication failed, the policy can reject the request without wasting the CPU cycles comparing 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. To understand Authentication Policies even more, let's examine a few.

From the ISE GUI, navigate to **Policy > Authentication**. Notice the default, as displayed in Figure 13-1.



**Figure 13-1** *Default Authentication Policy*

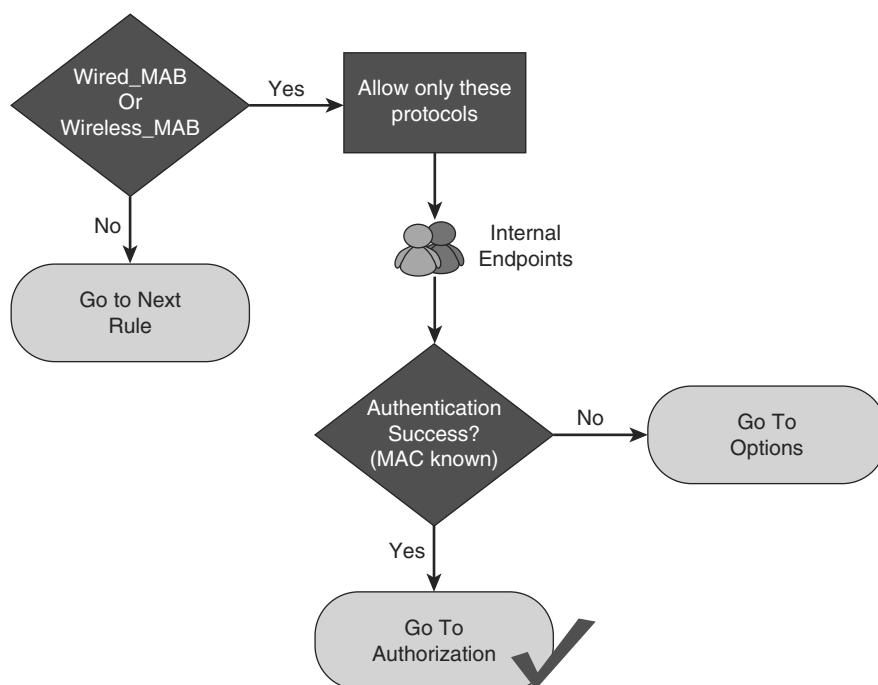
Basic Authentication Policy rules are logically organized in this manner:

IF *conditions* THEN ALLOW PROTOCOLS IN LIST *AllowedProtocolList*  
AND CHECK THE IDENTITY STORE IN LIST *IdentityStore*

Rules are processed in a top-down, first-match order; just like a firewall policy. So, if the conditions do not match, the authentication is compared to the next rule in the policy.

As shown in Figure 13-1, 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 13-2 demonstrates the MAB rule in flowchart format.



**Figure 13-2** MAB Rule Flow Chart

## Conditions

The conditions of this rule state, “If the authentication request is Wired\_MAB or Wireless\_MAB, it will match this rule.” You can expand these conditions by mousing over the conditions and clicking the target icon that appears or by looking directly at the authentication conditions shown in the following steps:

1. Navigate to **Policy > Policy Elements > Conditions > Authentication > Compound Conditions**.
2. Select **Wired\_MAB**.

As you can see in Figure 13-3, Wired\_MAB is looking for the RADIUS Service-Type to be Call-Check and the NAS-Port-Type to be Ethernet. This combination of attributes from the RADIUS authentication packet notifies ISE that it is a MAB request from a switch.

Figure 13-4 highlights these key attributes in a packet capture of the MAB authentication request.



Figure 13-3 *Wired\_MAB Condition*

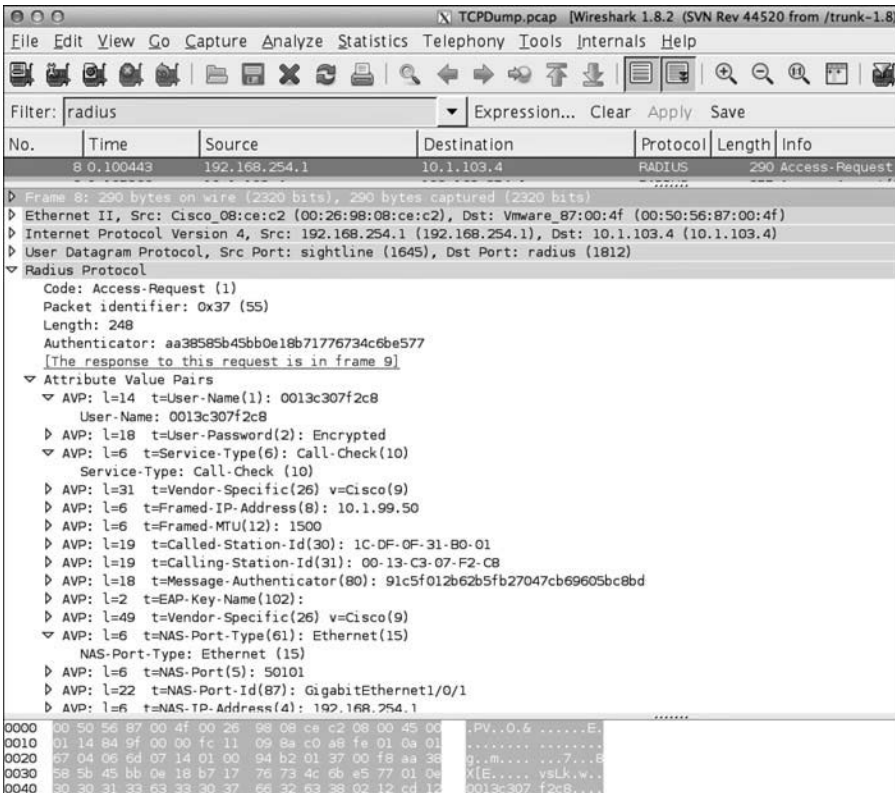


Figure 13-4 *Packet Capture of Wired MAB*

3. Navigate to Policy > Policy Elements > Conditions > Authentication > Compound Conditions.
4. Select Wireless\_MAB.

As shown in Figure 13-5, wireless MAB is similar. 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.



**Figure 13-5** *Wireless\_MAB Condition*

## 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:

1. Navigate to Policy > Policy Elements > Results > Authentication > Allowed Protocols.
2. Select Default Network Access.

As you can see in Figure 13-6, 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.

Allowed Protocols Services List > Default Network Access

**Allowed Protocols**

Name: Default Network Access

Description: Default Allowed Protocol Service

▼ Allowed Protocols

- Process Host Lookup
- Authentication Protocols**
  - Allow PAP/ASCII
    - Detect PAP as Host Lookup
  - Allow CHAP
    - Detect CHAP as Host Lookup
    - Allow MS-CHAPv1
    - Allow MS-CHAPv2
  - Allow EAP-MD5
    - Detect EAP-MD5 as Host Lookup
  - Allow EAP-TLS
  - Allow LEAP
  - Allow PEAP
    - PEAP Inner Methods
      - Allow EAP-MS-CHAPv2
        - Allow Password Change Retries  (Valid Range 0 to 3)
        - Allow EAP-GTC
          - Allow Password Change Retries  (Valid Range 0 to 3)
        - Allow EAP-TLS
    - Allow EAP-FAST
      - EAP-FAST Inner Methods
        - Allow EAP-MS-CHAPv2
          - Allow Password Change Retries  (Valid Range 1 to 3)
        - Allow EAP-GTC
          - Allow Password Change Retries  (Valid Range 1 to 3)
        - Allow EAP-TLS
      - Use PACs  Don't Use PACs
- Tunnel PAC Time To Live:  Days
- Proactive PAC update will occur after  % of PAC Time To Live has expired
- Allow Anonymous In-Band PAC Provisioning
- Allow Authenticated In-Band PAC Provisioning
  - Server Returns Access Accept After Authenticated Provisioning
  - Accept Client Certificate For Provisioning
- Allow Machine Authentication
  - Machine PAC Time To Live:  Weeks
- Enable Stateless Session Resume

**Figure 13-6** *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 Figure 13-6, from 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.

The check box for Detect PAP as Host Lookup allows PAP authentications to access the internal endpoints database. Without this check box selected, MAB would 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.

The check box for Detect CHAP as Host Lookup allows CHAP authentications to access the internal endpoints database. Without this check box selected, MAB does not work.

### 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 one has its own benefit and downside. As an interesting sidenote, 802.1X defines EAP over LAN:

- **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 is validating 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 it is also possible that some switches send MAB requests within EAP-MD5. The check box for Detect EAP-MD5 as Host Lookup allows EAP-MD5 authentications to access the internal endpoints database. Without this check box selected, MAB does not work.
- **EAP-TLS:** Uses Transport Layer Security (TLS) to provide the secure identity transaction. This is similar to 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 is quickly becoming the EAP type of choice when supporting BYOD in the enterprise.

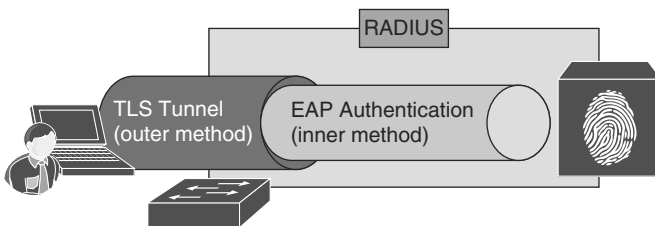
### Tunneled EAP Types

The EAP types previously described transmit their credentials immediately. These next two EAP types (see Figure 13-7) form encrypted tunnels first and then transmit the credentials within the tunnel:

- **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 another EAP type as an “inner method,” authenticating the client using EAP within the outer tunnel.

- **EAP-MSCHAPv2:** When using this inner method, the client’s credentials are sent to the server encrypted within an MSCHAPv2 session. This is the most common inner-method, as it allows for simply 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 (GTC). This inner method was created by Cisco as an alternative to MSCHAPv2 that allows generic authentications to virtually any identity store, including One-Time-Password (OTP) token servers, LDAP, Novell E-Directory and more.
- **EAP-TLS:** Although rarely used and not widely known, PEAP is capable of using EAP-TLS as an inner method.



**Figure 13-7** Tunnelled EAP Types (PEAP and FAST)

- **EAP-FAST:** Flexible Authentication via Secure Tunnel (FAST) is similar to PEAP. FAST was created by Cisco as an alternative to PEAP that allows for faster re-authentications 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 the 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-MSCHAPv2:** When using this inner method, the client’s credentials are sent to the server encrypted within an MSCHAPv2 session. This is the most common inner method, as it allows for simply 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 (GTC). This inner method was created by Cisco as an alternative to MSCHAPv2 that allows generic authentications to virtually any identity store, including One-Time-Password (OTP) token servers, LDAP, Novell E-Directory, 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 publishing this book, it was to be referred to as EAP-TEAP (tunneled EAP), which should eventually be supported by all major vendors.

## Identity Store

After processing the allowed protocols, the authentication request is then authenticated against the chosen identity store, or in this case with 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. This is covered in Chapter 21, “Monitor Mode.”

## Options

Every authentication rule has a set of options that are 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.

See Chapters 20–23 for more details on when to use these options.

## Common Authentication Policy Examples

This section considers a few quick examples of Authentication Policies, based on common use-case or simply because they were interesting.

## Using the Wireless SSID

One of the most common Authentication Policy requests that I 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. The attribute you need to use is called-station-id. That is the field that describes the wireless SSID name.

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

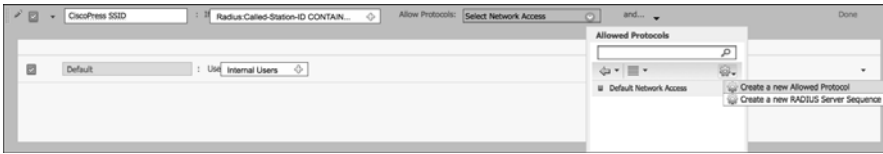
From the ISE GUI, perform the following steps:

1. Navigate to **Policy > Authentication**.
2. Insert a new rule above the preconfigured Dot1X rule.
3. Provide a name for the rule. In this case, we named it CiscoPress SSID.
4. For the condition, choose **RADIUS > Called-Station-ID**.
5. Select **Contains**.
6. Type in the SSID Name in the text box. Figure 13-8 shows the condition.



**Figure 13-8** *Called-Station-ID Contains CiscoPress*

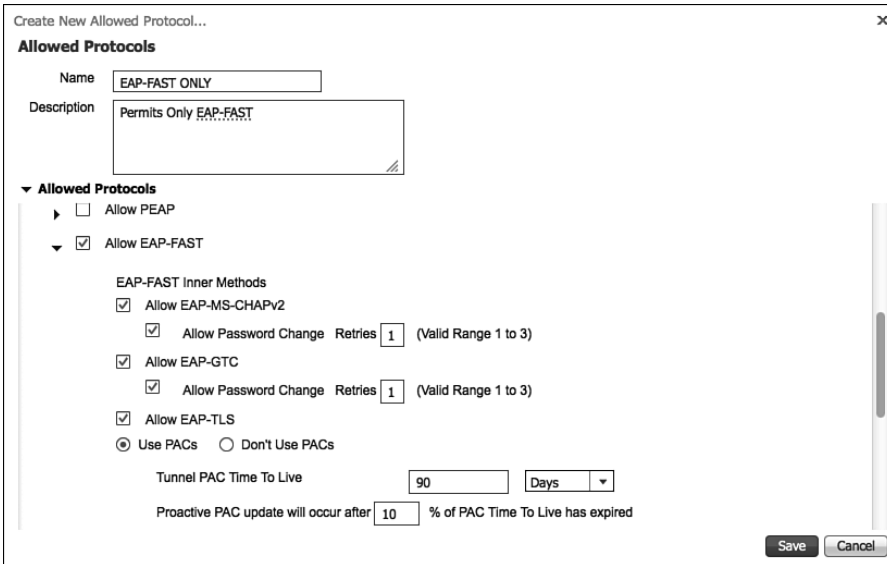
7. Create a new allowed protocol object that only allows EAP-FAST, as shown in Figure 13-9. Select the drop-down for Allowed Protocols.
8. Click the cog in the upper-right corner and choose Create a New Allowed Protocol.



**Figure 13-9** *Create a New Allowed Protocol*

9. Provide a name. In this case, it was named it EAP-FAST ONLY.
10. Optionally, provide a description.
11. Working top-down, ensure that all the check boxes are unchecked until you reach Allow EAP-FAST.
12. Confirm that Allow EAP-FAST is enabled.
13. For ease of use, enable EAP-MS-CHAPv2, EAP-GTC, and EAP-TLS for inner methods.
14. Select Use PACs for faster session re-establishment, and to allow EAP chaining.

Figure 13-10 shows the EAP-FAST settings for the new Allowed Protocols definition.



**Figure 13-10** *Allowed Protocols*

15. For ease of deployment, select Allow Anonymous In-Band PAC Provisioning and Allow Authenticated In-Band PAC Provisioning.

16. Check the boxes for Server Sends Access-Accept After Authenticated Provisioning and Accept Client Certificate for Provisioning.
17. Enable Allow Machine Authentication.
18. Select Enable Stateless Session Resume.
19. Select Enable EAP chaining, as shown in Figure 13-11.

Create New Allowed Protocol...

**Allowed Protocols**

Name:

Description:

▼ Allowed Protocols

Proactive PAC update will occur after  % of PAC Time To Live has expired

Allow Anonymous In-Band PAC Provisioning

Allow Authenticated In-Band PAC Provisioning

Server Returns Access Accept After Authenticated Provisioning

Accept Client Certificate For Provisioning

Allow Machine Authentication

Machine PAC Time To Live:

Enable Stateless Session Resume

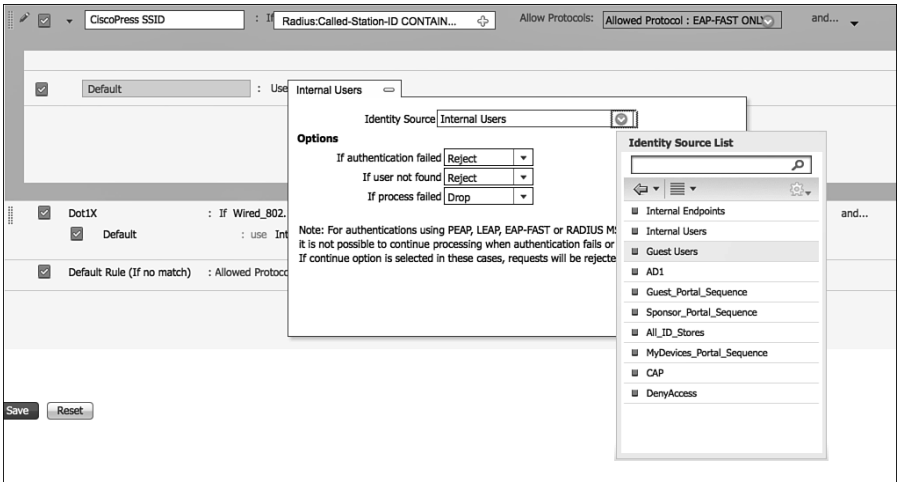
Authorization PAC Time To Live:   ⓘ

Enable EAP Chaining

Preferred EAP Protocol:

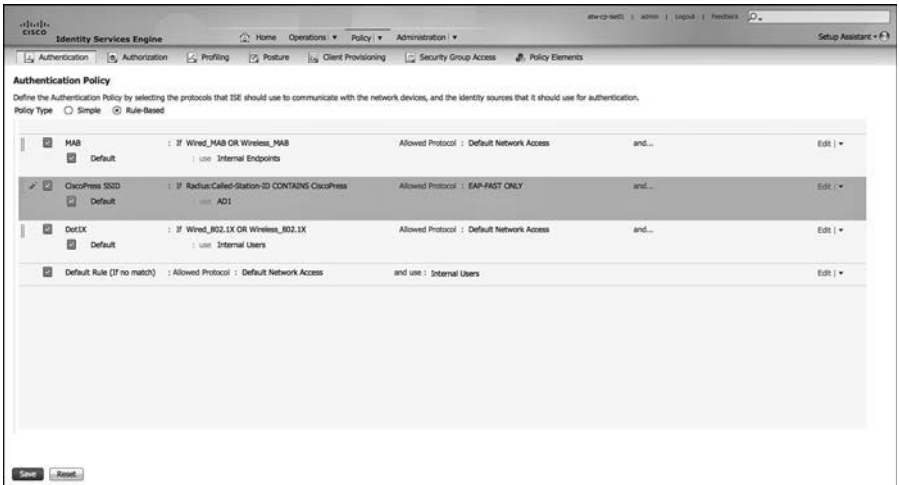
**Figure 13-11** *Allowed Protocols, Continued*

20. Because you are only allowing one protocol, there is no need to set a preferred EAP Protocol.
21. Click **Save**.
22. Select the drop-down for the identity source (currently set for Internal Users), as shown in Figure 13-12.
23. Select your Active Directory source. In this case, the name is AD1.
24. Leave the default options.
25. Click **Done**.
26. Click **Save**.



**Figure 13-12** *Selecting the AD Identity Source*

Figure 13-13 shows the completed authentication rule.



**Figure 13-13** *Completed Authentication Rule*

This completes the creation of the authentication rule. Determining what actions to take for the authentications that passed is handled in the Authorization Policy.

### Remote-Access VPN

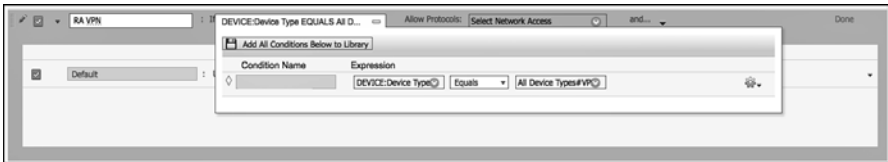
Very often, authentications for a remote-access VPN connection get routed to an OTP server, like RSAs SecureID. For this example, let's build a rule for remote-access VPN authentications. This rule will be configured to

- Only match authentications coming from the VPN device
- Route that authentication to the OTP server

From the ISE GUI, perform the following steps:

1. Navigate to **Policy > Authentication**.
2. Insert a new rule above the preconfigured Dot1X rule.
3. Provide a name for the rule. In this case, it was named RA VPN.
4. For the condition, choose **DEVICE > Device Type**.
5. Set the operator to Equals.
6. Choose the Network Device Group VPN.

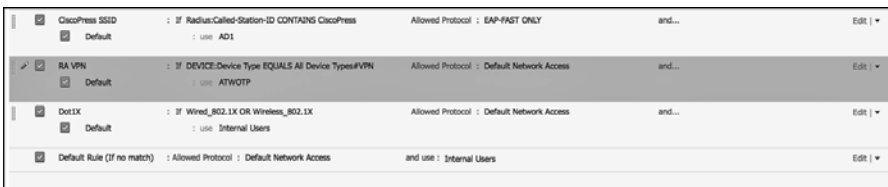
Figure 13-14 shows the selection of the conditions.



**Figure 13-14** *Device Type Equals VPN*

7. For this example, just use the allowed protocol of Default Network Access.
8. For the identity store, the OTP server was selected that was previously configured in **Administration > Identity Management > External Identity Sources > RADIUS Token (ATWOTP)**.
9. Leave the default options.
10. Click **Done**.
11. Click **Save**.

Figure 13-15 shows the completed RA VPN rule.



**Figure 13-15** *Completed Authentication Rule*



## Alternative ID Stores Based on EAP Type

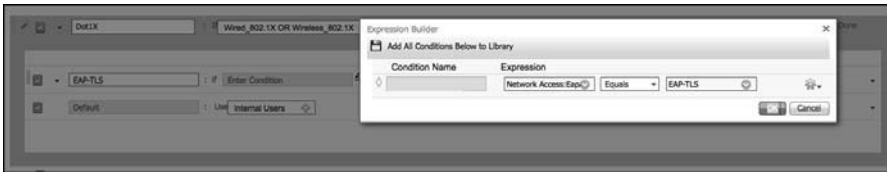
In this modern day of BYOD and mobility, it is common to have multiple user and device types connecting to the same wireless SSID. In scenarios like this, often times, the corporate users with corporate laptops authenticate using EAP-FAST with EAP chaining while BYOD-type devices need to use certificates 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:

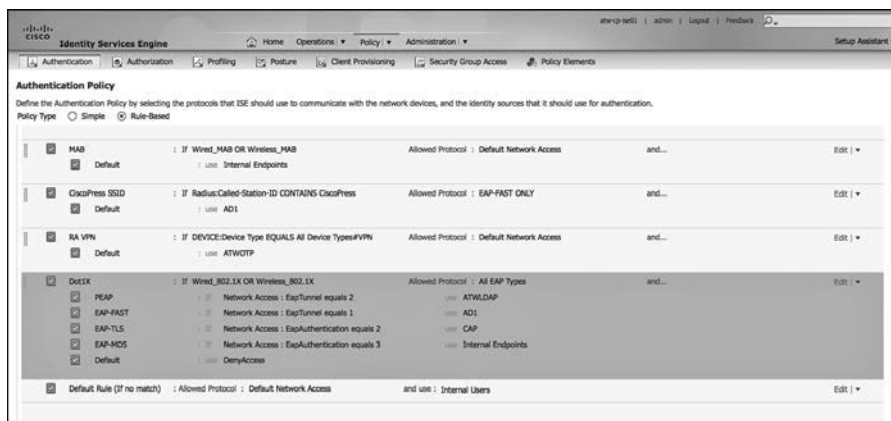
1. Navigate to **Policy > Authentication**.
2. Edit the preconfigured Dot1X rule.
3. Create a new allowed protocol object that only allows EAP authentications. Select the drop-down for allowed protocols.
4. Click the cog in the upper-right corner and choose Create a New Allowed Protocol.
5. Provide a name. In this case, it is named All EAP Types.
6. Optionally, provide a description.
7. Working top-down, ensure all EAP types are enabled, except for LEAP (unless you need LEAP for backward compatibility).
8. Enable EAP chaining, as done previously in the wireless SSID exercise.
9. Click **Save**.
10. Insert a new subrule above the Default Identity Store subrule and name it EAP-TLS.
11. For the condition, choose **Network Access > EapAuthentication equals EAP-TLS** (as shown in Figure 13-16).



**Figure 13-16** *Network Access:EapAuthentication Equals EAP-TLS*

12. For the identity source, choose the preconfigured Certificate Authentication Profile (CAP). This was configured at **Administration > Identity Management > External Identity Sources > Certificate Authentication Profile**.
13. Insert a new row above the EAP-TLS row to insert EAP-FAST. Place EAP-FAST above EAP-TLS, because EAP-TLS may be used as an inner-method of EAP-FAST.
14. Choose **Network Access > EapTunnel Equals EAP-FAST** for the condition.
15. Select the Active Directory object for the identity source.
16. Insert a new row above the EAP-TLS row to insert PEAP.
17. Choose **Network Access > EapTunnel Equals PEAP** for the condition.
18. Select the LDAP object for the identity source.
19. Insert a new row below the EAP-TLS row to insert EAP-MD5.
20. Choose **Network Access > EapAuthentication Equals EAP-MD5** for the condition.
21. Select internal endpoints for the identity source.
22. Change the default identity store (bottom row) to be Deny Access.
23. Click **Done**.
24. Click **Save**.

Figure 13-17 shows the completed rule and subrules.



**Figure 13-17** *Completed Authentication Rule and Sub Rules*

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 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 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, downloadable Access-Lists (dACL), Security Group Tag, 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.

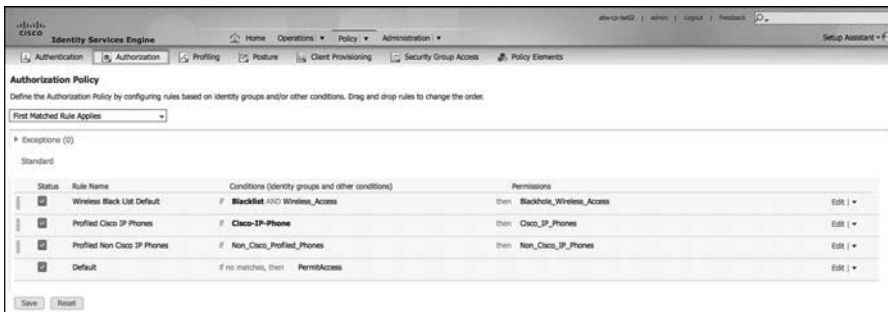
ISE is preconfigured with a default rule for blacklisted devices, named Wireless Blacklist Default, Profiled Cisco IP-Phones, and Profiled Non Cisco IP-Phones. Let's examine the Cisco IP-Phone and blacklist rules in order to dig into authorization rules and how they work. If you have a live ISE system, it may help to follow along with the text.

From the ISE GUI, perform the following steps:

1. Navigate to **Policy > Authorization**.

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 13-18 displays the default Authorization Policy.



**Figure 13-18** *Default Authorization Policy*

2. Edit the rule named 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-Phones. 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 13-19 shows an identity group of Cisco-IP-Phone.

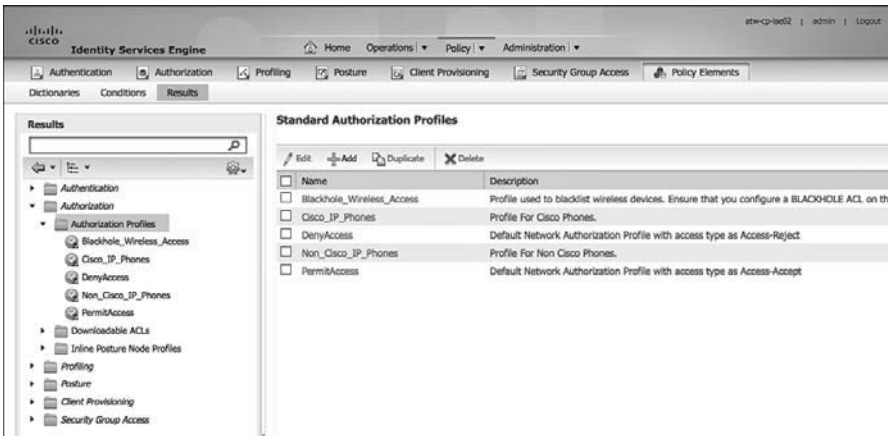


**Figure 13-19** *Profiled Cisco IP Phones*

3. Examine the permissions (result) that is sent. Navigate to **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.

Authorization Profiles are a set of authorization results that should be sent together. Notice that there are two other categories of authorization results: Downloadable ACLs and Inline Posture Node Profiles.

Figure 13-20 displays the default Authorization Profiles.

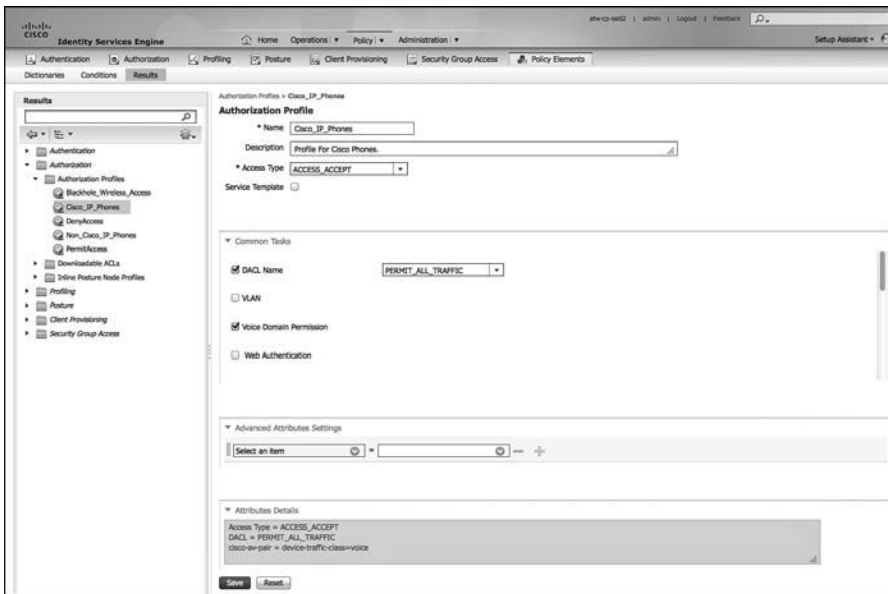


**Figure 13-20** *Default Authorization Profiles*

4. Select the **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. The Attributes Details section at the bottom displays the raw RADIUS result that is sent.

Figure 13-21 shows the common tasks, using the default Cisco\_IP\_Phones authorization profile as the example.



**Figure 13-21** Cisco\_IP\_Phones Authorization Profile

In Figure 13-21, note the DAACL name is a drop-down box where you select a downloadable access list that is created and stored in ISE. The Voice Domain Permission check box is required for the switch to allow the phone into the voice VLAN on the switch.

5. Notice in the Attributes Detail section, this authorization result sends a RADIUS result with an access-accept, a DAACL that permits all traffic, and the voice-domain VSA to permit the phone to join the voice VLAN.

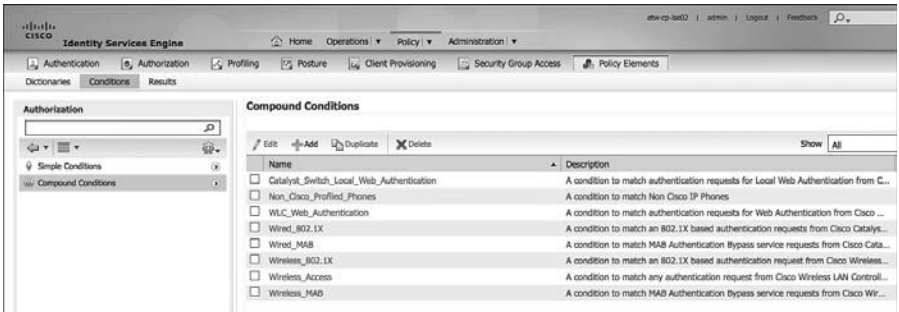
Next, examine the Wireless Blacklist Default Rule:

1. Navigate to Policy > Authorization.
2. Edit the rule named Wireless Black List Default.

Notice the Identity Group is a separate list than the other conditions. In this rule, there is an Identity Group named “Blacklist”. The next field is populated with a pre-built condition specifying wireless connections. This particular rule is built to prevent devices that have been marked lost or stolen from accessing the network.

3. Examine the authorization condition being used. Navigate to Policy > Policy Elements > Conditions > Authorization > Compound Conditions.

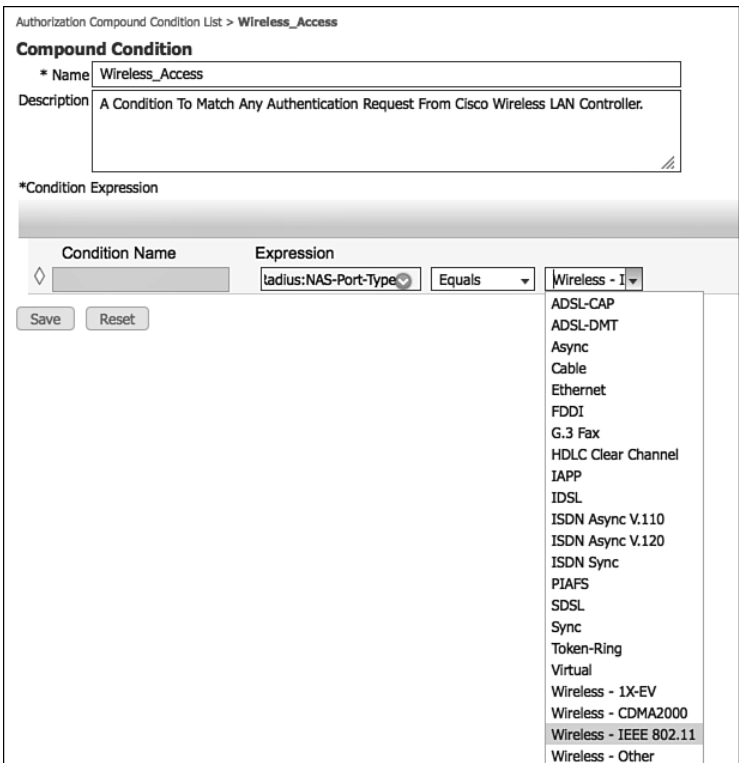
Figure 13-22 shows the default list of compound conditions.



**Figure 13-22** Pre-Built Authorization Compound Conditions

4. Select **Wireless\_Access**.

As shown in Figure 13-23, the **Wireless\_Access** compound condition references the **RADIUS** attribute of **NAS-Port-Type Equals Wireless – IEEE 802.11**.



**Figure 13-23** Wireless\_Access Compound Condition

5. Examine the authorization result that is being sent for this Authorization Rule. Navigate to **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.
6. Select **Blackhole\_Wireless\_Access**.

As shown in Figure 13-24, the **Blackhole\_Wireless\_Access** Authorization Profile does not use any of the common tasks. Instead, it employs the Advanced Attribute settings 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 was blacklisted.



**Figure 13-24** *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. In Chapter 6, “Building a Cisco ISE Network Access Security Policy,” you learned all about the specific results and how to create those authorizations. However, that should always be handled in a staged approach in order to limit the impact to the end users.

Part V is dedicated to this phased approach.

## 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 the parts/pieces of an Authorization Policy and the workflows associated with creating the policies.

For this example, let’s configure three authorization rules: one that assigns full access to an employee that authenticated successfully with EAP chaining followed by a rule that assigns more limited access to the same employee authenticating with a non-corporate machine. The last rule created 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 that is authenticating from a valid corporate asset. From the ISE GUI, perform the following steps:

1. Navigate to **Policy > Authorization**.
2. Insert a new rule above the default rule.
3. Name the new rule **Employee and CorpMachine**.
4. For the other conditions drop-down, where it says **Select Attribute**, click the **+** and select **Create New Condition**.
5. Choose **Network Access > EapChainingResult**.
6. Choose **Equals**.
7. Select **User and Machine Both Succeeded**.
8. Click the cog on the right-hand side > **Add Attribute/Value**.
9. Select **AD1 > External Groups Equals "Employees"** (or another AD group of your choosing).
10. For the AuthZ Profiles, click the **+** sign.
11. Click the cog in the upper-right corner > **Add New Standard Profile**.
12. Name the new Authorization Profile **Employee Full Access**.
13. Optionally add a description.
14. Access Type = **Access\_Accept**.
15. Select **DACL Name > Permit\_ALL\_TRAFFIC**.  
Figure 13-25 shows the Employee Full Access authorization profile.
16. Click **Save**.
17. Click **Done** to finish editing the rule.
18. Click **Save** to save the Authorization Policy.

Figure 13-26 shows the completed authorization rule.

Add New Standard Profile x

**Authorization Profile**

\* Name

Description

\* Access Type

Service Template

---

▼ Common Tasks

DACL Name

VLAN

Voice Domain Permission

Web Authentication

---

▼ Advanced Attributes Settings

Select an item =  - +

---

▼ Attributes Details

Access Type = ACCESS\_ACCEPT  
 DACL = PERMIT\_ALL\_TRAFFIC

**Figure 13-25** *Employee Full Access Authorization Profile*

Identity Services Engine #10-102 | admin | Logout | Feedback

Authentication | **Authorization** | Profiling | Posture | Client Provisioning | Security Group Access | Policy Elements

**Authorization Policy**

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

Exceptions (0)

Standard

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	Edit   ▼
<input checked="" type="checkbox"/>	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones	Edit   ▼
<input checked="" type="checkbox"/>	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones	Edit   ▼
<input checked="" type="checkbox"/>	Employee and CorpMachine	if (Network_Access:EapChainingResult EQUALS User and machine both succeeded AND) AND: ExternalGroups EQUALS (e.local/Users/Employees)	then Employee Full Access	Edit   ▼
<input checked="" type="checkbox"/>	Default	if no matches, then	PermAccess	Edit   ▼

**Figure 13-26** *Completed Employee and CorpMachine Rule*

## Internet Only for iDevices

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:

1. Navigate to **Policy > Policy Elements > Results > Authorization > Downloadable ACLs**.
2. Click **Add**.
3. Name the ACL **Internet Only**.
4. Optionally provide a description.
5. Within **DACL Content**, provide an ACL that permits required traffic for Internet access and denies traffic destined to the corporate network.

Figure 13-27 is just an example.

Downloadable ACL List > New Downloadable ACL

**Downloadable ACL**

\* Name:

Description:

\* DACL Content: 

```
permit udp any any eq 68
permit udp any any eq 53
deny ip any 172.16.0.0 0.0.3.255
deny ip any 192.168.0.0 0.0.255.255
deny ip any 10.0.0.0 0.0.0.255
permit ip any any
```

**DACL Check**

DACL is valid

**Figure 13-27** *Internet Only DACL*

6. Click **Submit**.

Now that the DACL is created, it's time to create the Authorization Profile:

1. Navigate to **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.
2. Click **Add**.
3. Name the Authorization Profile **Internet Only**.
4. Optionally provide a description.
5. Access Type is **ACCESS\_ACCEPT**.
6. Select **DACL Name** and select **Internet Only**.
7. Optionally 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.

8. Select **Airspace ACL Name** and fill in the name of the ACL on the controller that provides Internet Only Access.
9. Click **Submit**.

Figure 13-28 shows the completed Authorization Profile.

The screenshot shows the configuration page for an Authorization Profile. The breadcrumb navigation is "Authorization Profiles > Internet Only". The profile name is "Internet Only" and the description is "AuthZ Profile To Provide Internet Only Access". The access type is set to "ACCESS\_ACCEPT".

Under the "Common Tasks" section, the "DACL Name" is set to "Internet Only" and the "VLAN" section shows "Tag ID 1" and "ID/Name GUEST".

The "Advanced Attributes Settings" section is currently empty, showing a "Select an item" dropdown.

The "Attributes Details" section at the bottom lists the following attributes:
 

- Access Type = ACCESS\_ACCEPT
- Tunnel-Private-Group-ID = 1:GUEST
- Tunnel-Type=1:13
- Tunnel-Medium-Type=1:6
- DACL = Internet Only
- Airspace-ACL-Name = InternetOnly

**Figure 13-28** *Internet Only Authorization Profile*

Before you build the Authorization Policy, create a logical profiling policy that encompasses all mobile devices. This makes the policy building much easier and provides a reusable policy object:

1. Navigate to **Policy > Profiling > Logical Profiles**.
2. Click **Add**.
3. Name the Logical Policy **iDevices**.
4. Optionally provide a description.
5. Select all the mobile platforms from the Available Devices side, and click the **>** to move them to the Assigned Policies side.
6. Click **Submit**.

Figure 13-29 shows the **iDevices** Logical Profile.



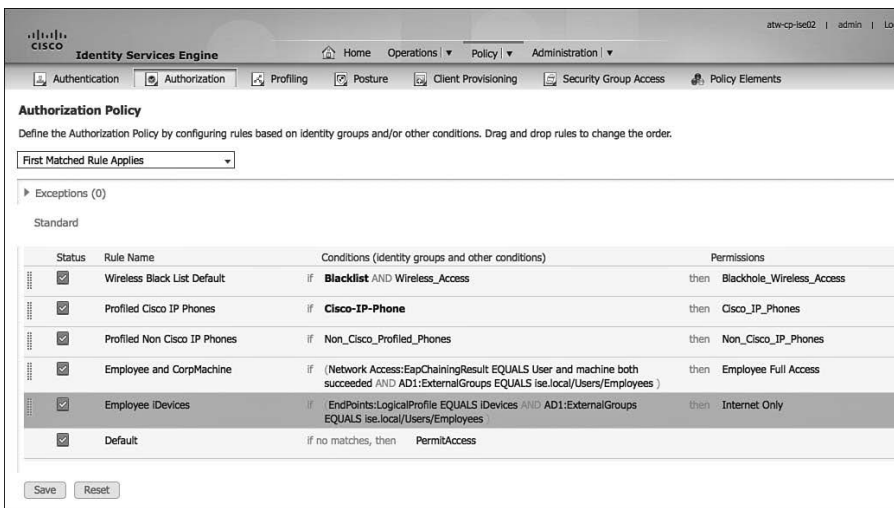
**Figure 13-29** *iDevices* Logical Profile

Finally, it is now time to create the authorization rule:

1. Navigate to **Policy > Authorization**.
2. Insert a new rule above the default rule.
3. Name the Rule **Employee iDevices**.
4. Select the **+** sign for conditions, and select **Endpoints > LogicalProfile**.
5. Choose **Equals**.
6. Select **iDevices**.
7. Click the cog on the right-hand side **> Add Attribute/Value**.

8. Select **AD1 > External Groups Equals “Employees”** (or another AD group of your choosing).
9. For the AuthZ Profiles, click the **+** sign.
10. Select **Standard > Internet Only**.
11. Click **Done**.
12. Click **Save**.

The completed authorization rule is displayed in Figure 13-30.



The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring an Authorization Policy. The page title is "Authorization Policy" and it includes a sub-header "Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order." Below this, there is a dropdown menu for "First Matched Rule Applies" and a section for "Exceptions (0)". The main part of the page is a table of rules under the "Standard" category. The table has columns for "Status", "Rule Name", "Conditions (identity groups and other conditions)", and "Permissions". The rule "Employee iDevices" is highlighted in grey, indicating it is the selected rule. Below the table are "Save" and "Reset" buttons.

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Wireless Black List Default	if <b>Blacklist</b> AND Wireless_Access	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 Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones
<input checked="" type="checkbox"/>	Employee and CorpMachine	if (Network Access:EapChainingResult EQUALS User and machine both succeeded AND AD1:ExternalGroups EQUALS ise.local/Users/Employees )	then Employee Full Access
<input checked="" type="checkbox"/>	Employee iDevices	if EndPoints:LogicalProfile EQUALS iDevices AND AD1:ExternalGroups EQUALS ise.local/Users/Employees	then Internet Only
<input checked="" type="checkbox"/>	Default	if no matches, then	PermitAccess

**Figure 13-30** *Employee iDevices Authorization Rule*

## Employee Limited Access Rule

Now the rule for employees connecting with mobile devices is created, you need to create the rule below it that provides limited access only 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:

1. Navigate to **Policy > Policy Elements > Results > Authorization > Downloadable ACLs**.
2. Click **Add**.
3. Name the ACL **Employee Limited**.
4. Optionally provide a description.

5. Within DACL Content, provide an ACL that permits required traffic and denies traffic destined to the corporate network. For this example, allow traffic to reach our virtual desktop infrastructure and essential services, like DNS only.

Figure 13-31 shows the Employee Limited dACL.

Downloadable ACL List > New Downloadable ACL

**Downloadable ACL**

\* Name: Employee Limited

Description: permit traffic to VDI servers only

\* DACL Content:

```

permit udp any any eq 68
permit udp any any eq 53
permit tcp any host 10.1.100.222 eq 3389
permit tcp any host 10.1.100.222 eq 443
permit tcp any host 10.1.100.222 eq 80

```

▼ DACL Check

Recheck Clear Verbose

DACL is valid

Submit Cancel

**Figure 13-31** Employee Limited DACL

6. Click **Submit**.

Now that the DACL is created, build the Authorization Policy to permit network access and apply that DACL:

1. Navigate to Policy > Policy Elements > Results > Authorization > Authorization Profiles.
2. Click **Add**.
3. Name the Authorization Profile Employee Limited.
4. Optionally provide a description.
5. Access Type is ACCESS\_ACCEPT.
6. Select **DACL Name** and select **Employee Limited**.
7. Do not assign a different VLAN for this authorization.

8. Select **Airspace ACL Name** and fill in the name of the ACL on the controller that provides Internet-only access.

9. Click **Submit**.

Figure 13-32 shows the completed Authorization Profile.

Authorization Profiles > New Authorization Profile

**Authorization Profile**

\* Name

Description

\* Access Type

Service Template

▼ Common Tasks

PMLSEC Policy

NEAT

Web Authentication (Local Web Auth)

Airespace ACL Name

ASA VPN

▼ Advanced Attributes Settings

Select an item =  - +

▼ Attributes Details

Access Type = ACCESS\_ACCEPT  
 DACL = Employee Limited  
 Airespace-ACL-Name = EmployeeLimited

**Figure 13-32** *Employee Limited Authorization Profile*

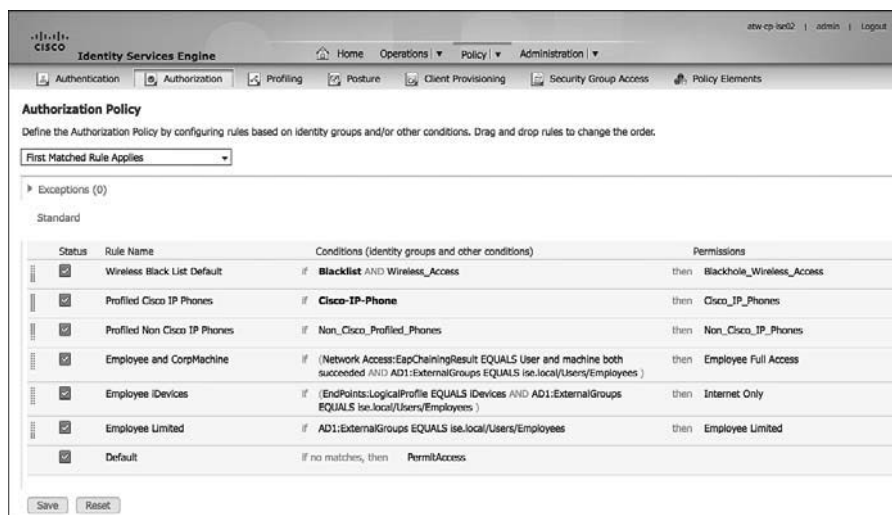
Now, create the Authorization Policy rule to assign that Authorization Profile:

1. Navigate to **Policy > Authorization**.
2. Insert a new rule above the default rule.
3. Name the Rule **Employee Limited**.
4. Select the **+** sign for conditions.
5. Select **AD1 > External Groups Equals "Employees"** (or another AD group of your choosing).



6. For the AuthZ Profiles, click the + sign.
7. Select **Standard > Employee Limited**.
8. Click **Done**.
9. Click **Save**.

Figure 13-33 shows the completed Employee Limited authorization rule.



**Figure 13-33** *Employee Limited Authorization Rule*

## Saving Attributes for Re-Use

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:

1. Navigate to **Policy > Authorization**.
2. Edit the Employee and CorpMachine rule.
3. Expand the conditions.
4. Click **Add All Conditions Below to Library**, as shown in Figure 13-34.

This is adding the full set of conditions, including the AND operator.



**Figure 13-34** Add All Conditions Below to Library

5. Provide a name for this new saved condition, such as EmployeeFullEAPChain.
6. Finish editing the rule.
7. Click Save.

As shown in Figure 13-35, the Authorization Policy text is simplified now with the name of the saved conditions instead of the raw attributes.

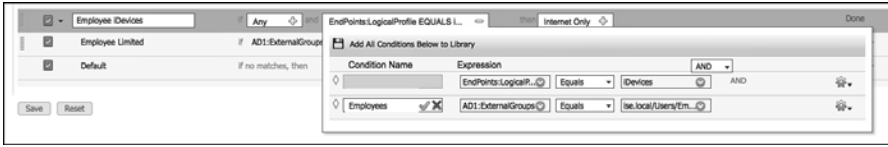
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Wireless Black List Default	if <b>Blacklist</b> AND Wireless_Access	then Blackhole_Wireless_Access
<input checked="" type="checkbox"/>	Profiled Cisco IP Phones	if <b>Cisco-IP-Phone</b>	then Cisco_IP_Phones
<input checked="" type="checkbox"/>	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones
<input checked="" type="checkbox"/>	Employee and CorpMachine	if EmployeeFullEAPChain	then Employee Full Access
<input checked="" type="checkbox"/>	Employee iDevices	if (EndPoints:LogicalProfile EQUALS iDevices AND AD1:ExternalGroups EQUALS ise.local/Users/Employees )	then Internet Only
<input checked="" type="checkbox"/>	Employee Limited	if AD1:ExternalGroups EQUALS ise.local/Users/Employees	then Employee Limited
<input checked="" type="checkbox"/>	Default	if no matches, then PermitAccess	

**Figure 13-35** Authorization Policy After Saving Conditions to Library

Next, save the Employees group for AD as a condition:

1. Navigate to Policy > Authorization.
2. Edit the Employee iDevices Rule.
3. Expand the conditions.
4. Click the cog on the right-hand side of the Employees line.
5. Choose Add Condition to Library.
6. Name the condition Employees.
7. Click the green check mark.

Figure 13-36 displays the saving of Employees to the Conditions library.



**Figure 13-36** Saving Employees to Library

8. Click Done to finish editing the rule.
9. Click Save.

Figure 13-37 shows the final Authorization Policy.

Status	Rule Name	Conditions (Identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Wireless Black List Default	if <b>Blacklist</b> AND Wireless_Access	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 Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones
<input checked="" type="checkbox"/>	Employee and CorpMachine	if EmployeeFullEAPChain	then Employee Full Access
<input checked="" type="checkbox"/>	Employee ID Devices	if (EndPoint:LogicalProfile EQUALS IDDevices AND Employees )	then Internet Only
<input checked="" type="checkbox"/>	Employee Limited	if AD1:ExternalGroups EQUALS ise.local/Users/Employees	then Employee Limited
<input checked="" type="checkbox"/>	Default	if no matches, then PermitAccess	

**Figure 13-37** 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. Chapters 20 to 23 focus on specific configurations of these policies to help in the actual deployment of ISE and the Secure Unified Access Solution.

Chapter 14, “Guest Lifecycle Management,” examines web authentication, guest access, and the full lifecycle management of guest users.

# Index

## Symbols

---

802.1X, 4, 9, 10-11

assigning SGT via, 504-505

binary behavior of 802.1X, 41

Closed Mode, 44-45

global commands, switches, 175

intended behavior, 395

Monitor Mode, phased deployment,  
38-39

posture assessment, 280-282

802.1X supplicant/agent, 20

## A

---

AAA (authentication, authorization,  
and accounting), 584

switches, 171-172

AAA servers, configuring, 185-187

RADIUS accounting servers, 186-  
187

RADIUS authentication servers, 185-  
186

RADIUS fallback, 187

acceptable use policies (AUP), 59-60  
posture global setup, 287

access, guest access, 4, 11-12

access control, 50

access control lists, creating local on  
switches, 174-175

Access Control Server. *See* ACS  
(Access Control Server)

access enablement, 50

access layer devices that do not sup-  
port SGTs, 506

access session settings, RBAC (role-  
based access control), ISE GUI,  
121-123

access switches, NEAT (Network  
Edge Authentication Topology),  
574

account lockout, error messages, 617

account roles, Active Directory, 646

accounting

reasons for, 83-84

user accounting, 92-93

ACL, pre-posture, 298

ACLs (access control lists)

BYOD onboarding, 328

- creating on switches, 329*
- creating on wireless LAN controllers, 328*
- ingress, 498
- ingress access control, 498
- posture agent redirection ACL, 191-192
- web authentication redirection ACL, 188-191
- ACL-WEBAUTH-REDIRECT, 261**
- ACS (Access Control Server), 7-8**
- Active Directory**
  - account roles, 646
  - Cisco ISE Policy Setup Assistant wizard, 99
  - Identity Source Sequence, 252
  - troubleshooting disconnections, 610
- Active Directory Certificate Services, installing, 647-659**
- adding**
  - network devices
    - Device Sensor method, 425-426*
    - RADIUS with SNMP Query method, 421*
    - SNMP Trap method, 416-418*
  - non-seed switches, NDAC (Network Device Admission Control), 564-566
  - policy services nodes to node groups, 387-388
  - posture policy rules, 74-75
- ADE-OS (Application Development Environment Operating System), 96**
- Administration, 21**
- Administration node, 34-35**
- administrative management, endpoints, 372-374**
- Advanced licenses, 23**
- aggregated services router (ASR), 356**
- Airespace ACLs, configuring, 188**
  - posture agent redirection ACL, 191-192
  - web authentication redirection ACL, 188-191
- alarms, 587-588**
- Allow Network Access, 352**
- allowed protocols, conditions, authentication policies, 220**
- alternative ID stores based on EAP type, authentication policies, 230-232**
- Android, 328**
  - BYOD onboarding, 361-364
  - dual SSID, 340-345
- antispymware programs, 74**
- antivirus programs, 74**
- Apple, 319**
- Apple iOS, single-SSID, 330-340**
- Apple iPad, profiler conditions, 80-81**
- Application Condition settings, 290**
- Application Development Environment Operating System (ADE-OS), 96**
- Apply Defined Authorization Policy, 352**
- AS condition, 292**
- ASA**
  - identity firewall, 11
  - security group firewalls, 535-536
- ASR (aggregated services router), 356**
  - security group firewalls, 543-544
- assigning**
  - SGT (Security Group Tag)
    - at the port, 506*
    - via 802.1X, 504-505*

- switches to Low-Impact Stage network Device Group (NDG), 452-453
- WLC (Wireless LAN Controller) and switches, to Closed Stage NDG, 468-469
- WLCs to Low-Impact Stage network Device Group (NDG), 452-453
- Attribute Value Pairs (AVP), 572**
- attributes**
  - endpoints, 476-478
  - MDM, 367
  - NetFlow, 483
  - saving for re-use, 246-248
- atw-cp-ise02, 382**
- atw-cp-ise03, 382**
- atw-cp-ise04, 382**
- ATW-ISE-12, 382**
- audit data, reviewing, 91-92**
- auditing, reasons for, 83-84**
- AUP (acceptable use policy), 59-60**
- authenticated guest access, 251**
- authenticating devices, authorization policies for, 438**
  - default authorization profiles, 440-441
  - machine authentication, 438-439
  - user authentications, 439-440
- authentication**
  - versus authorization, 215-216
  - RADIUS, 11
  - RBAC (role-based access control), ISE GUI, 123-124
  - troubleshooting, 596-597
    - entries exist in the live log, 603-604*
    - no live log entry exists, 597-602*
  - VPN authentication, 4
  - web authentication, 11
- authentication and authorization guest policies, 258**
  - guest post-authentication authorization policies, 262-263
  - guest pre-authentication authorization policy, 258-262
- authentication policies, 216**
  - alternative ID stores based on EAP type, 230-232
  - conditions, 218-220
    - allowed protocols, 220*
    - authentication protocol primers, 221-222*
    - EAP (Extensible authentication protocol) types, 222*
    - identity store, 224*
    - options, 224*
    - tunneled EAP types, 222-224*
  - examples, wireless SSID, 225-228
  - goals, 216-217
  - NASP (network access security policy), 48
  - remote-access VPN, 228-229
- authentication protocol primers, 221-222**
- authentication settings, configuring, 182-183**
- authentication timers, configuring, 184**
- authenticator switches, 574**
- authorization**
  - versus authentication, 215-216
  - RBAC (role-based access control), ISE GUI, 124-125

- troubleshooting, 596-597
    - entries exist in the live log*, 603-604
    - no live log entry exists*, 597-602
  - authorization dACLs, configuring**, 207
  - authorization policies, 232-237**
    - for authenticating devices, 438
      - default authorization profiles*, 440-441
      - machine authentication*, 438-439
      - user authentications*, 439-440
    - Closed Mode, creating for specific roles, 470-472
    - examples, 237
      - employee and corporate machine full-access rule*, 238
      - employee limited access rule*, 243-246
      - Internet only for iDevices*, 240-243
    - goals, 232
    - NASP (network access security policy), 48
    - for non-authenticating devices, 433
      - IP-Phones*, 433-434
      - printers*, 436-437
      - wireless APs*, 435
    - probes, Logical Profiles, 164-165
    - profiles, 161
      - endpoint identity groups*, 161-163
      - EndPointPolicy*, 163-164
    - role-specific authorization rules, 237
    - saving conditions to library, 247
  - authorization policy elements, 205-206**
  - authorization policy rules, creating**, 354-356
  - authorization profiles**
    - configuring, 209-211
    - creating, 353-354
      - for NEAT*, 572
    - Downlink MACSec, 549
  - Authorization Results, 206-216**
    - configuring
      - authorization dACLs*, 207
      - authorization profiles*, 209-211
  - authorization rules, 12, 58-59**
    - creating for NEAT, 573-574
    - device profiling, 82
    - employee authorization rule, 64
    - guest authorization rules, 62
    - NASP (network access security policy), 57-58
    - permissions, 62
  - AuthZ policies, creating for specific roles**, 454-456
  - AV condition**, 292
  - AV Remediation action**, 292-294
  - AVP (Attribute Value Pairs)**, 572
- 
- ## B
- Backup and Restore screen**, 626
  - backup progress**, 626
  - backups, 625-628**
    - CLI (command-line interface), 627
    - scheduling, 628
  - bandwidth requirements, 27**
    - centralized deployment, 32
    - distributed deployment, 34
  - best practices, profiling**, 149-152
  - binary behavior of 802.1X**, 41

binding IP addresses to SGTs, 506

Blackberry, unsupported mobile devices, 346-347

Blackhole Wireless Access Authorization Profile, 237

Blacklist portal, 264

bootstrapping, 169  
ISE, 95-97

bridged mode, IPN (Inline Posture Node), 393

BYOA (Bring Your Own App), 319

BYOD (Bring Your Own Device), 319  
challenges, 320-321

BYOD onboarding, 322  
Android, 361-364  
authorization policy rules, creating, 354-356  
authorization profiles, creating, 353-354  
client provisioning policy, configuring, 349-351  
configuring ISE for, 347  
configuring NADs for, 324  
creating ACLs on wireless LAN controllers, 328  
creating ACLs on the switch, 329  
creating native supplicant profiles, 347-349  
dual SSID, 322  
*Android*, 340-345  
endpoints, 372-373  
end-user experience, 330  
iOS onboarding flow, 357  
*device enrollment*, 359  
*device provisioning*, 359-360  
*device registration*, 358-357  
ISE configuration for, 329-330  
MDM onboarding, 367

*configuring MDM integration*, 368-369  
*configuring policies*, 369-372  
*integration points*, 367  
required ACLs, 328  
SCEP, configuring, 356-357  
single SSID, 322-323  
single-SSID with Applied iOS, 330-340  
unsupported mobile devices, Blackberry, 346-347  
verifying default unavailable client provisioning policy action, 352  
WebAuth, configuring, 351  
Windows and Mac-OSX flow, 364-366  
WLC configuration, 324-327

## C

---

CA (Certificate Authority), 645-646  
enabling, 671-672  
requirements for, 645  
setting lifetimes of, 672

CA insurer names, configuring, 672

CA servers, CDP (Certificate Distribution Point), 673

campus LANs, security domains, 56

Catalyst 6500, 507  
IP Helper, 420

Catalyst 6500 Seed Device, configuring, 564

Catalyst 6500 Supervisor 2T, verifying tagging, 522

CDP (Certificate Distribution Point), CA servers, 673

CD-ROM, repositories, 623

central Web Authentication, 249-250



- central Web Authentication flow, 249-251
- centralized deployment, 29-31
- centralized network security policy, 7-9
- centralized policies, 5-6
- Certificate Distribution Point (CDP), 673
- Certificate Enrollment Web Service, 645
- Certificate Revolution List. *See* CRL (Certificate Revocation List)
- certificate servers, generating/exporting for certificate servers (RSA key pairs), 670-671
- certificate templates
  - configuring, 659-663
  - publishing, 665
- certificate-signing requests, 114
- certificates, 114-116
  - configuring on switches, 170
- Change of Authorization. *See* CoA (Change of Authorization)
- changing default authentication rule to deny access, 456-457
- CHAP (Challenge Handshake Authentication Protocol), 222
- checklist, NASP (network access security policy), 48-49
- choosing end-state mode, phased deployment, 40-45
- CIMC (Cisco Integrated Management Controller), 95
- Cisco 3750X switch configuration, 106-109
- Cisco AnyConnect Secure Mobility Client NAM, supplicants, 312-316
- Cisco ASA (Adaptive Security Appliance), SXP (Security Group eXchange Protocol), configuring, 513-515
- Cisco Catalyst Switches. *See* switches
- Cisco devices, configuration of NetFlow, 485-487
- Cisco Integrated Management Controller (CIMC), 95
- Cisco IOS 12.2, 170
- Cisco IOS 15.x, 170
- Cisco IP Phone 7970, endpoint profile policies, 155-161
- Cisco ISE Policy Setup Assistant wizard, 97-104
  - Configure Network Access Service page, 100
  - Identify Policy Requirements page, 99
  - Select Network Device Types wizard page, 102-103
  - Setup Assistant wizard, 113
  - Wireless Network Controller settings, 103
- Cisco NAC Agent, 21, 67
- Cisco NAC Framework, 7
- Cisco NAC Guest Server, 8
- Cisco NAC Manager, 9
- Cisco NAC Profiler, 8
- Cisco NAC Server, 9
- Cisco Secure Unified Access system, 170
- Cisco Security Intelligence Operations, 76
- Cisco Setup Assistant Wizard, 169
- Cisco TrustSec, 9
- Cisco wireless LAN controller configuration, 109-113
- Cisco.com Download Center, 629
- Cisco-Device profiling policy, 157
- Cisco-IP-Phone 7970 profile, 160
- Cisco-IP-Phone profiling policy, 160

CIUS, 319

classification, SGT (Security Group Tag), 504

CLI (command-line interface), 95-96

backups, 627

restoring, 629

client provisioning

NAC client provisioning, configuring, 288-289

posture client provisioning global setup, 283-285

client provisioning policy, configuring, 349-351

client supplicants, 301

Closed Mode, 44-45, 459-460

authorization policies, creating for specific roles, 470-472

changing (default authentication rules to deny access), 472-473

deployment phases, 406-408

modifying default port ACL on switches, 469

monitoring, 469

moving switch ports from multi-auth to MDA, 473-474

Policy Set, 461

*assigning WLCs and switches to Closed stage NDG, 468-469*

*duplicating Monitor Mode Policy Set, 462*

*modifying the default rule, 467*

*web authentication authorization results, 463-466*

*web authentication identity source sequence, 466*

transitioning from Monitor Mode, 461

CoA (Change of Authorization), 488-489, 565

configuring in profiler policies, 490

profiling, 133-142

*configuring, 143-144*

*message types, 142-143*

types of, 489

collecting information for custom profiles, 478-479

command-line interface (CLI), 95

common checks, ISE solution, 74

comparing supplicants, 302-303

conditions, 205

authentication policies, 218-220

*allowed protocols, 220*

*authentication protocol primers, 221-222*

*EAP (Extensible authentication protocol) types, 222*

*identity store, 224*

*options, 224*

*tunneled EAP types, 222-224*

creating custom profiler conditions, 479-480

posture, 289-292

conference room network access, 569

Configure Network Access Service page, Cisco ISE Policy Setup Assistant wizard, 100

configuring

AAA servers, 185-187

*RADIUS accounting servers, 186-187*

*RADIUS authentication servers, 185-186*

*RADIUS fallback, 187*

- Airespace ACLs, 188-192
  - posture agent redirection ACL, 191-192*
  - web authentication redirection ACL, 188-191*
- authentication settings, 182-183
- authentication timers, 184
- authorization dACLs, 207
- authorization profiles, 209-211
- CA insurer names, 672
- certificate templates, 659-663
- certificates on switches, 170
- client provisioning policy, 349-351
- CoA (Change of Authorization), 143-144, 490
- domain names, 669-670
- exceptions in profiler policies, 490
- feed service, 166-167
- flexible authentication and high availability, 179-182
- guest portals, 251
  - identity sources, 252-253*
- guest sponsor portals, 263-264
  - guest portal interface and IP configuration, 264*
- guest sponsors, 254
  - guest sponsor groups, 255-256*
  - guest time profiles, 254-255*
  - sponsor group policies, 257*
- guest time profiles, 254-255
- hostnames, 669-670
- HTTP servers, 669-670
- identity sources, 252-253
- interfaces as switch ports, 179
- ISE
  - NDAC (Network Device Admission Control), 558-561*
  - for onboarding, 347*
  - ISE probes, SNMP Trap method, 414*
  - ISE to allow SGACLs to be downloaded, 531-532*
  - Low-Impact Mode, 446*
  - Mac OS X 10.8.2 native supplicant, 303*
  - MDM integration, 368-369*
  - MDM onboarding, policies, 369-372*
  - NAC agents, 288-289*
  - NAC client provisioning, 288-289*
  - NADs for onboarding, 324*
  - native SGT propoagation, 517*
  - native tagging*
    - SGT Popagation on Cisco IOS switches, 518-520*
    - SGT propagation on Nexus series switches, 522-523*
    - SGT propagation on a catalyst 6500, 520-522*
  - NDAC (Network Device Admission Control), switch interfaces, 566-567*
- network devices
  - wired switch configuration basics, 106-109*
  - wireless controller configuration basics, 109-113*
- network devices for guest CWA
  - wired switches, 274-275*
  - wireless LAN controllers, 275*
- posture conditions, 289-292
- posture policy, 296-298
- posture remediation actions, 292-295
- posture requirements, 295-296
- probes
  - Device Sensor method, 425*
  - NetFlow, 481-483*

- profiling, 130-132*
  - RADIUS with SNMP Query method, 420-421*
  - repositories, 619-625
  - SCEP, 356-357
  - security group firewalls, TrustSec
    - downloads from ISE via ASDM, 536-541
  - seed devices, NDAC (Network Device Admission Control), 562-564
  - SG-FW on an ASR and ISR, 544-546
  - SG-FW policies via ASDM, 542
  - SMS text messaging, 264
  - switches
    - Device Sensor method, 426-428 to download SGACLs from ISE, 532*
    - RADIUS with SNMP Query method, 422-424*
    - SNMP Trap method, 418-420*
  - SXP (Security Group eXchange Protocol)
    - on Cisco ASA, 513-515*
    - on iOS devices, 509-511*
    - on WLC, 511-513*
  - Uplink MACSec, 553-555
  - web authentication identity source sequence, 451
  - WebAuth, 351
  - Windows 7 native supplicant, 309-312
  - Windows GPO for wired supplicant, 305-309
  - context awareness, 5
  - corporate SSID, creating, 199-202
  - corporate systems, identifying, 374-375
    - EAP chaining, 375-376
    - criteria, establishing to determine validity of security posture checks, rules, or requirements, 76-77
  - CRL (Certificate Revocation List), 672-673
  - CTS data downloads, validating, 533-535
  - Custom AV condition, 292
  - custom default portals, 268
  - custom device web authorization portal, 268
  - custom profiler conditions, creating, 479-480
  - custom profiler policies, creating, 480-481
  - custom profiles
    - collecting information for, 478-479
    - for unknown endpoints, 475-476
  - customizing
    - guest portals, 265-266
    - portal themes, 266-267
    - sponsor portals, 264
  - CYOD (Choose Your Own Device), 319
- ## D
- 
- dACL (downloadable ACL), 259, 448, 454
    - authorization dACLs, configuring, 207
    - AuthZ policies, creating for specific roles, 454-456
    - Closed Mode, 44
    - Low-Impact Mode, 43
    - Web Auth dACL, 259
  - dACL syntax checker, 209
  - dashlet, 577

data repositories, 586

Data Security Standard. *See* DSS

data sources, device profiling, 81-82

database levels, enabling, 671-672

debug situations, troubleshooting,  
611-612

default authentication rule, changing  
to deny access, 456-457, 472-473

default authorization profiles, 234,  
440-441

default port ACL on switches, modi-  
fying (Closed Mode), 469

default port ACL on switches,  
modifying (Low-Impact Mode),  
453-454

default portals, 268

default rule in Closed Policy Set,  
modifying, 467

default unavailable client provisioning  
policy action, verifying, 352

deny access

changing default authentication rule,  
456-457

changing default authentication  
rules, 472-473

deploying security requirements,  
78-79

deployment

centralized deployment, 29-31

centralized versus distributed, 29-30

distributed deployment. *See* distrib-  
uted deployment

phased deployment, 37-38

*choosing end-state mode, 40-45*

*Monitor Mode, 38-39*

probes

*DHCP (Dynamic Host  
Configuration Protocol),  
135-137*

*DNS, 139*

*HTTP, 133-134*

*NetFlow, 137*

*NMAP, 139*

*RADIUS, 138*

*SNMP, 140-141*

deployment phases, 397

authentication open versus standard  
802.1X, 398-399

Closed Mode, 406-408

Low-Impact Mode, 404-406

Monitor Mode, 399-401

*preparing for staged deploy-  
ment, 401-404*

reasons for using, 395-397

transitioning from Monitor Mode to  
end state, 408-409

wireless networks, 409

design, SXP (Security Group  
eXchange Protocol), 508-509

designing NetFlow, efficient collec-  
tion of data, 484-485

desktop switches, NEAT (Network  
Edge Authentication Topology),  
574-575

device configuration, for monitoring,  
584-585

device enrollment, iOS onboarding  
flow, 359

device posture assessment, 67

device profiling, 79-80

authorization rules, 82

data sources, 81-82

profiling policies, 80

device profiling policy, 48

device provisioning, iOS onboarding  
flow, 359-360

device registration, iOS onboarding flow, 358-357

device registration portal, 251

Device Sensor method, 424

adding network devices, 425-426

configuring

*probes*, 425

*switches*, 426-428

Device Sensors, switches, 177-178

device web authorization portal, 268

DHCP (Dynamic Host Configuration Protocol)

Device Sensors, 177

infrastructure configuration, profiling, 145

probes, deployment, 135-137

dhcp-class-identifier, 477

dictionaries, 205-206

disconnections, Active Directory, troubleshooting, 610

distributed deployment, 32-35, 377

ISE nodes, 377

*ensuring the persona of nodes is accurate*, 381

*making the Policy*

*Administration Node a primary device*, 377-378

*registering nodes to deployment*, 379-381

DNS, probes, 139

domain names, configuring, 669-670

domains, NDAC (Network Device Admission Control)

configuring ISE to allow SGACLs to be downloaded, 558-561

MACSec sequence, 567-568

Downlink MACSec, 549-550

authorization profiles, 549

ISE configuration, 552

policies, 549

policy switch CLI, 550

switch configuration modes, 551-552

downloadable ACL. *See* dACL

DSS (Data Security Standard), 84

dual SSID, BYOD onboarding, 322

Android, 340-345

duplicating Monitor Mode Policy Set, 446-447, 462

dVLAN (dynamic VLAN)

Closed Mode, 44

Low-Impact Mode, 43

Dynamic Authorization Failed, 615-616

dynamic interfaces for client VLANs, creating, 193

employee dynamic interfaces, 193

guest dynamic interfaces, 194-195

## E

EAP (Extensible authentication protocol) types, 222

EAP chaining, 375-376

EAP chaining with EAP-FASTv2, 224

EAP Connection Timeout, 613-614

EAP-FAST (Flexible Authentication via Secure Tunnel), 223

EAP-GTC (Generic Token Card), 223

EAP-MD5, 222

EAP-MSCHAPv2, 223

EAP-TLS, 222, 223

East-West, SGACL, 525

editing Registry, 665-667

employee and corporate machine full-access rule, 238

employee authorization rule, 64

**employee dynamic interfaces, creating**, 193

**employee limited access rule**, 243-246

**employee posture policies**, 73

**enabling**

CA (Certificate Authority), 671-672

database levels, 671-672

HTTP/HTTPS servers on switches, 170-171

posture assessment in the network, 298-299

**endpoint components, ISE solutions**, 20-21

**Endpoint Discovery, Monitor Mode**, 412-413

Device Sensor method. *See* Device Sensor method

SNMP Trap method. *See* SNMP Trap method

**endpoint identity groups, authorization policies, profiles**, 161-163

**Endpoint Profile Changes Report**, 493

**endpoint profile policies**, 150-154

Cisco IP Phone 7970, 155-161

**EndPointPolicy**, 163-164

**endpoints**

attributes, 476-478

filtering, 476

managing, 372-373

*administrative management*, 372-374

*self management*, 372

monitoring, 580-581

**end-state mode**

choosing, 40-45

Closed Mode, 44-45

Low-Impact Mode, 42-44

transitioning from Monitor Mode, 45-46, 408-409

**end-user experience, BYOD onboarding**, 330

**enforcement**

SGA (Security Group Access), 523-524

*SGACL*, 524-525

SGA, security group firewalls. *See* security group firewalls

**enforcement methods, network access privileges**, 61-62

**enforcement types**

Closed Mode, 44

Low-Impact Mode, 43

**enforcing**

AUP (acceptable use policy), 60

security requirements, 78-79

**error messages**

account lockout, 617

Dynamic Authorization Failed, 615-616

EAP Connection Timeout, 613-614

WebAuth Loop, 617

**establishing criteria to determine validity of security posture checks, rules, or requirements**, 76-77

**Evaluate Configuration Validator**, 591-593

**examples**

authentication policies, wireless SSID, 225-228

authorization policies, 237

*employee and corporate*

*machine full-access rule*, 238

*employee limited access rule*, 243-246

*Internet only for iDevices*, 240-243

exception actions, 489-490  
 exceptions  
     configuring in profiler policies, 490  
     profilers, 488-489  
 exporter configurations, NetFlow, 486  
 exporting RSA key pairs, 670-671

## F

---

failure scenarios, load balancers, 389  
 feed service, 166  
     configuring, 166-167  
 File Condition settings, posture conditions, 290  
 Filter-ID  
     Closed Mode, 44  
     Low-Impact Mode, 43  
 filtering endpoints, 476  
 firewalls  
     ASA identity firewall, 11  
     installing ISE, 116-118  
     security group firewalls. *See* security group firewalls  
 flexible authentication, configuring, 179-182  
 flow, posture assessment, 280-282  
 FTP (File Transfer Protocol), 620-621

## G

---

global AAA commands, switches, 171-172  
 global configuration settings, switches, 170  
 global logging commands, switches, 175-177  
 global profiling commands, switches, 177  
 global RADIUS commands, switches, 172-174  
 GNU Privacy Guard (GPG), 625  
 goals  
     authentication policies, 216-217  
     authorization policies, 232  
     for NASP (network access security policy), 51-52  
     of NASP (network access security policy), high-level goals, 52-55  
 Google Play app store, 328  
 groups, guest sponsor groups, 255-256  
 guest access, 4, 11-12  
 guest accounts  
     creating for guest sponsor portals, 273  
     managing for guest sponsor portals, 273  
 guest authentication, 249  
 guest authorization rules, 62  
 guest dynamic interfaces, 194-195  
 guest email notification, 265  
 guest portal interface and IP configuration, 264  
 guest portals  
     configuring, 251  
         *identity sources*, 252-253  
     customizing, 265-266



- guest post-authentication authorization policies, authentication and authorization guest policies, 262-263
- guest pre-authentication authorization policy, authentication and authorization guest policies, 258-262
- guest sponsor groups, 255-256
- guest sponsor portals
  - configuring, 263-264
    - guest portal interface and IP configuration*, 264
  - guest accounts
    - creating*, 273
    - managing*, 273
  - sponsor portal layout, 271-272
- guest sponsors, configuring, 254
  - guest sponsor groups, 255-256
  - guest time profiles, 254-255
  - sponsor group policies, 257
- guest time profiles, configuring, 254-255
- guest web portal, 251
- Guest WLANs, creating, 195-198
- guests, security domains, 56

## H

---

- high availability, 381
    - configuring, 179-182
    - PANs (Policy Administration Nodes), 384-385
    - primary and secondary nodes, 381
    - promoting Secondary PAN to Primary, 385
  - high-level troubleshooting flowchart, 605
  - Home Dashboard, 491-492
  - host posture assessment policy, 48
  - hostname, 478
  - hostnames, configuring 669-670
  - hot fixes, Microsoft 646
  - HTTP
    - probes, profiling, 132-133
    - repositories, 624-625
  - HTTP servers, configuring 669-670
  - HTTP/HTTPS servers, enabling on switches, 170-171
- █
- Identify Policy Requirements page, Cisco ISE Policy Setup Assistant wizard, 99
  - identifying
    - corporate systems, 374-375
      - EAP chaining*, 375-376
    - misconfigured devices, 428
      - authorization policies*, 433
      - profiling policies*, 428-429
    - unique values for unknown devices, 476-478
  - identities, creating for NEAT, 571
  - identity awareness, 4-5
  - identity firewall, ASA, 11
  - Identity Services Engine
    - sample letter to students, 638
    - sample notice for bulletin board/poster, 636-638
    - sample requirement change notification email, 635-636
  - identity sources, 252-253
  - identity store, authentication policies, 224

- IEEE 802.1X, 9
- information, collecting for custom profiles, 478-479
- infrastructure components, ISE solutions, 16-20
- infrastructure configuration, profiling, 144-145
  - DHCP (Dynamic Host Configuration Protocol), 145
  - SPAN (Switched Port Analyzer), 145-146
  - VACL (VLAN Access Control Lists), 146-148
  - VMware (promiscuous mode), 148-149
- ingress access control, 495
  - lists, 498
  - VLAN assignments, 495-497
- ingress reflector mode, 520
- Inline Posture Node (IPN), 22
- installing
  - Active Directory Certificate Services, 647-659
  - ISE, behind firewalls, 116-118
  - licenses, 113-114
  - patches, 630-631
- Integrated Services Routers. *See* ISR (Integrated Services Router)
- integration points, MDM onboarding, 367
- Intel Hyper-Threading Technology, 25
- interface configuration, NetFlow, 487
- interface configuration settings, switches, 179
  - applying ACL to the port and enabling authentication, 184
  - configuring
    - authentication timers*, 184
    - flexible authentication and high availability*, 179-182
    - interfaces as switch ports*, 179
- Interface probe, 141
- interfaces, configuring as switch ports, 179
- Internet, security domains, 56
- Internet only for iDevices, 240-243
- IOS CA SCEP RA configuration, 673
- IOS Device-Sensor, probes, 141-142
- iOS devices, configuring SXP (Security Group eXchange Protocol), 509-511
- iOS onboarding flow, 357
  - device enrollment, 359
  - device provisioning, 359-360
  - device registration, 358-357
- ip address-helper, 145
- IP addresses, binding to SGTs, 506
- ip helper-address, 136
- IPEVENT, 584
- IPN (Inline Posture Node), 22, 383, 391
  - configuring, 393
  - modes of operation, 393-394
  - overview, 392
- IP-Phones, authorization policies, 433-434
- ISE (Identity Services Engine), 3-4, 249
  - bootstrapping, 95-97
  - installing behind firewalls, 116-118
  - overview, 9-12
  - rules and requirements structure, 70

**ISE Accounting**, 83  
**ISE Auditing**, 83  
**ISE Certificate Store**, 116  
**ISE certificates**, 114-116  
**ISE Client Provisioning service**, 68  
**ISE configuration**  
     for BYOD onboarding, 329-330  
     Downlink MACSec, 552  
**ISE Dashboard**, 578-577  
**ISE file condition**, 68  
**ISE guest services**, 249  
**ISE Guest Sponsors**, 252  
**ISE GUI**  
     configuring (SGACL), 526-530  
     RBAC (role-based access control),  
         121  
         *access session settings*, 121-123  
         *authentication*, 123-124  
         *authorization*, 124-125  
         *passwords*, 124  
**ISE licensing**, 23  
**ISE logs, debug situations**, 611-612  
**ISE nodes**, 22  
     distributed deployment, 377  
         *ensuring the persona of nodes  
         is accurate*, 381  
         *making the Policy  
         Administration Node a pri-  
         mary device*, 377-378  
         *registering nodes to deploy-  
         ment*, 379-381  
     Policy Administration Node,  
         377-378  
     registering to deployment, 379-381  
**ISE performance**, 25-27  
**ISE policy-based structure, overview**,  
     25

**ISE posture assessment process**, 70  
**ISE requirements**, 23-25  
**ISE solutions**, 15  
     endpoint components, 20-21  
     infrastructure components, 16-20  
     policy components, 20  
**ISR (integrated services routers)**, 356,  
     669  
     security group firewalls, 543-544

## J-K

---

Jobs, Steve, 319

## L

---

**licenses, installing**, 113-114  
**licensing**, 23  
**lifetimes**, 672  
**Live Authentications Alternate view**,  
     579  
**Live Authentications CoA action**, 580  
**Live Authentications Log**, 578-580  
**Live Authentications screen**, 491  
**load balancers**, 388  
     failure scenarios, 389  
     guidelines for, 388-389  
**local access control lists, creating on  
 switches**, 174-175  
**local Web Authentication**, 249-250  
**local Web Authentication flow**, 249  
**log data, ensuring integrity and confi-  
 dentiality of**, 90  
**logging commands, global logging  
 commands, switches**, 175-177  
**Logical Profiles**, 164-165

**Low-Impact Mode, 42-44, 443-444**

- configuring, 446
- deployment phases, 404-406
- enforcement types, 43
- modifying default port ACL on switches, 453-454
- monitoring, 454
- Policy Set, 446
  - configuring web authentication identity source sequences, 451*
  - creating web authentication authorization results, 448-449*
  - duplicating Monitor Mode Policy Set, 446-447*
  - modifying the default rule, 451-452*
- transitioning from Monitor Mode, 445-446

**Low-Impact Mode Policy Set, 457**

low-impact policy set, modifying, 451-452

Low-Impact Stage Network Device Group (NDG), assigning WLCs and switches, 452-453

## M

---

MAB (MAC Authentication Bypass), 11, 128, 258

MAC address authentication, 4

MAC address, profiling policies, 128

MAC Authentication Bypass (MAB), 11, 258

Mac OS X 10.8.2 native supplicant, configuring, 303

Mac-OSX, BYOD onboarding, 364-366

machine authentication, authorization policies, 438-439

**MACSec, 548**

- Downlink MACSec, 549-550
  - authorization profiles, 549*
  - ISE configuration, 552*
  - policies, 549*
  - policy switch CLI, 550*
  - switch configuration modes, 551-552*
- MDA Mode, 551
- Multi-Authentication Mode, 551
- Multi-Host Mode, 551
  - sequence in NDAC domains, 567-568
- Uplink MACSec, 553
  - configuring, 553-555*
  - verifying configuration, 556-557*

MACSec Layer 2 Hop-by-Hop encryption, 547

managing endpoints, 372-373

- administrative management, 372-374
- self management, 372

**mapping**

- subnets to SGTs, 507
- VLANs to SGTs, 507-508

MDA Mode, MACSec, 551

MDM (mobile device management), 320-321

attributes, 367

MDM integration, configuring, 368-369

MDM onboarding, 367

- configuring
  - MDM integration, 368-369*
  - policies, 369-372*
- integration points, 367

message types, CoA (Change of Authorization), 142-143

Metasploit, 76

Microsoft, hotfixes, 646

Microsoft Certificate Authority (CA), 645-646

requirements for, 645

Microsoft Security Bulletins, 75

Microsoft TechNet Security Center, 75

misconfigured devices, identifying, 428

authorization policies, 433

profiling policies, 428-429

mobile device management.  
*See* MDM

Mobile Device On-Boarding, 9

modes of operation, IPN (Inline Posture Node), 393-394

modifying

default port ACL on switches

*Closed Mode*, 469

*Low-Impact Mode*, 453-454

default rule in Closed Policy Set, 467

low-impact policy set, 451-452

monitor configuration, NetFlow, 486-487

Monitor Mode, 411-412

default authorization profiles, 440-441

deployment phases, 399-401

*preparing for staged deployment*, 401-404

Endpoint Discovery, 412-413

*Device Sensor method*. *See*  
*Device Sensor method*

*RADIUS with SNMP Query method*. *See* RADIUS,  
*SNMP Query method*

*SNMP Trap method*. *See*  
*SNMP Trap method*

identifying misconfigured devices, 428

*authorization policies*, 433

*profiling policies*, 428-429

phased deployment, 38-39

transitioning, to end state, 408-409

transitioning to Closed Mode, 461

transitioning to end-state mode, 45-46

transitioning to Low-Impact Mode, 445-446

Monitor Mode Policy Set, duplicating, 446-447, 462

monitor session, SPAN (Switched Port Analyzer), 145-146

monitoring, 577

Closed Mode, 469

device configuration for, 584-585

endpoints, 580-581

Global Search, 581-582

Live Authentications Log, 578-580

Low-Impact Mode, 454

nodes in distributed deployment, 584

primary and secondary nodes, 381-383

profilers, 491-493

Monitoring persona, 21

moving switch ports

from multi-auth to MDA, 473-474

from multi-auth to multi-domain, 457-458

multi-auth switch ports, 457-458

**Multi-Authentication Mode, MACSec, 551**  
**multi-domain switch ports, 457-458**  
**Multi-Host Mode, MACSec, 551**  
**multiple portals, creating, 268-270**

## N

---

**NAC (Network Access Control), 319**  
**NAC Agent for Mac OS X**  
 posture checks, 71  
 posture remediation actions, 70  
**NAC Agent for Windows**  
 posture checks, 71  
 posture remediation actions, 70  
**NAC agents, 21**  
 configuring, 288-289  
**NAC Appliance, posture assessment, 280**  
**NAC client provisioning, 288-289**  
**NAC Framework, 7**  
**NAC Guest Server, 8**  
**NAC Manager, 9**  
**NAC Profiler, 8**  
**NAC Server, 9**  
**NAC web agent, 285**  
**NAD (Network Access Devices), 29**  
**NASP (network access security policy), 47**  
 AUP (acceptable use policy), 59-60  
 authorization rules, 57-58  
 checklist, 48-49  
 determining goals for, 51-52  
 high-level goals, 52-55  
 including the right people when creating, 49-51  
 network access privileges, defining, 61  
 overview, 47-48  
 security domains, defining, 55-57  
**NASP format for documenting ISE posture requirements, samples, 72**  
**National Cyber Awareness System, 75**  
**National Vulnerability Database, 76**  
**native supplicant profiles, creating, 347-349**  
**native supplicant provisioning, 301**  
**native tagging, 516-517**  
 configuring  
*native SGT propagation, 517*  
*SGT Propagation on Cisco IOS switches, 518-520*  
*SGT propagation on Nexus series switches, 522-523*  
*SGT propagation on a catalyst 6500, 520-522*  
**NDAC (Network Device Admission Control), 557**  
 adding non-seed switches, 564-566  
 configuring switch interfaces, 566-567  
 domains, configuring ISE to allow SGACLs to be downloaded, 558-561  
 MACSec sequence in domains, 567-568  
 seed devices, configuring, 562-564  
**NDES (Network Device Enrollment Services), 645-646, 356**  
**NEAT (Network Edge Authentication Topology), 569**  
 access switches, 574  
 desktop switches, 574-575  
 overview, 570-571  
 preparing ISE for, 571

- authorization rules, 573-574*
- creating authorization profiles, 572*
- creating user identity group and identity, 571*

**NetFlow, 34**

- attributes, 483
- configuration on Cisco devices, 485-487
- designing for efficient collection of data, 484-485
- probes, 137
  - configuring, 481-483*
  - deployment considerations, 137*
- profiler policy, examples, 483

**Network Access Devices. *See* NAD (Network Access Devices)**

**network access privileges, defining, 61**

**network access security policy. *See* NASP**

**Network Device Admission Control. *See* NDAC (Network Device Admission Control)**

**Network Device Groups, creating, 401-402**

**network devices**

- adding
  - Device Sensor method, 425-426*
  - RADIUS with SNMP Query method, 421*
  - SNMP Trap method, 416-418*
- configuring
  - wired switch configuration basics, 106-109*
  - wireless controller configuration basics, 109-113*

**network devices for guest CWA, configuring**

- wired switches, 274-275
- wireless LAN controllers, 275

**Network Edge Authentication Topology. *See* NEAT (Network Edge Authentication Topology)**

**Network File System (NFS), 623**

**networks, enabling posture assessment, 298-299**

**Nexus 7000, enabling tagging, 523**

**Nexus 7000 Seed Device, configuring, 563-564**

**NFS (Network File System), 623**

**NMAP, probes, 138**

- deployment, 139

**node communications, 617**

**node groups, 385-386**

- adding policy services nodes to, 387-388
- creating, 386-387

**node types, functions, 22**

**nodes. *See also* ISE nodes**

- Administration node, 34-35

- IPN (Inline Posture Node). *See* IPN (Inline Posture Node)

- primary and secondary nodes, 381
  - monitoring and troubleshooting, 381-383*

- PSNs (Policy Service Nodes), adding to node groups, 387-388

**nodes in distributed deployment, monitoring, 584**

**non-authenticating devices, authorization policies for**

- IP-Phones, 433-434

- printers, 436-437

- wireless APs, 435

non-seed switches, adding, NDAC (Network Device Admission Control), 564-566

North-South, SGACL, 525

## O

---

On Demand Backup, 626

onboarding, BYOD (Bring Your Own Device). *See* BYOD onboarding

OOB management, security domains, 56

options, authentication policies, 224

OTA (Over the Air), 328

## P

---

PAC (Protected Access Credential) files, 533-535

PAC files, validating, 533-535

Packet Captures, 594

PANs, 632

PANs (Policy Administration Nodes), high availability, 384-385

PAP (Password Authentication Protocol), 221

Parker, Chuck, 569

passwords, RBAC (role-based access control), ISE GUI, 124

patches, installing, 630-631

patching, 629-631

PCI (Payment Card Industry), 84

PCI 10.1: Ensuring unique usernames and passwords, 84-89

PCI 10.2: Audit log collection, 89

PCI 10.3: Audit log collection, 89

PCI 10.5.3: Ensuring the integrity and confidentiality of log data, 90

PCI 10.5.4: Ensuring the integrity and confidentiality of log data, 90

PCI 10.6: Reviewing audit data regularly, 91-92

PCI 10.7: Ensuring the integrity and confidentiality of log data, 90

PCI DSS

10.1: Ensuring unique usernames and passwords, 84-89

10.2 and 10.3, Audit log collection, 89

10.5.3, 10.5.4, and 10.7: Ensuring the integrity and confidentiality of log data, 90

10.6: Reviewing audit data regularly, 91-92

as auditing framework, 84

PCI DSS 2.0 requirement 10, 85

PEAP (Protected EAP), 223

Perfigo, 7

performance, 25-27

Permit Access Authorization result, 454

Permit-All-Traffic, 454

personas, 21-22

Administration, 21

ensuring accuracy for all nodes, 381

Monitoring, 21

Policy Service, 21

phased deployment, 37-38

choosing end-state mode, 40-45

Monitor Mode, 38-39

physical appliance specifications, ISE GUI, 24

policies

centralized policies, 5-6

custom profiler policies, creating, 480-481



- Downlink MACSec, 549
- MDM onboarding, 369-372
- profiling, endpoint profile policies, 150-154
- POLICY\_APP\_FAILURE, 584**
- POLICY\_APP\_SUCCESS, 584**
- Policy Administration Node, as a primary device, 377-378
- policy components, ISE solutions, 20
- Policy Service, 21
- Policy Service Nodes. *See* PSNs
- policy services nodes to node groups, adding to node groups, 387-388
- Policy Set
  - Closed Mode, 461
    - assigning WLCs and switches to Closed stage NDG, 468-469*
    - duplicating Monitor Mode Policy Set, 462*
    - modifying the default rule, 467*
    - web authentication authorization results, 463-466*
    - web authentication identity source sequence, 466*
  - creating, 403-404
  - Low-Impact Mode, 446
    - configuring web authentication identity source sequences, 451*
    - creating web authentication authorization results, 448-449*
    - duplicating Monitor Mode Policy Set, 446-447*
    - modifying the default rule, 451-452*
- policy switch CLI, Downlink MACSec, 550
- policy-based structure, overview, 25
- portal themes, customizing, 266-267
- portals, multiple portals, creating, 268-270
- ports
  - assigning SGT (Security Group Tag), 506
  - behavior with open authentication, 399
- posture, conditions, 289-292
- posture agent redirection ACL, 191-192
- posture assessment, 279-280
  - enabling in the network, 298-299
  - flow, 280-282
  - NAC Appliance, 280
  - posture client provisioning global setup, 283-285
  - posture global setup, 285-287
- posture checks, 71
- posture client provisioning global setup, 283-285
- posture global setup, 285-287
- Posture Policy, 68
- posture policy rules
  - adding, 74-75
  - determining which rules a security requirement should be applied to, 77-78
- posture policy, configuring, 296-298
- posture remediation actions, 70
  - configuring, 292-295
- posture requirements, configuring, 295-296
- preboot execution environment (PXE), 42
- pre-built authorization compound conditions, 235

**preparing**

ISE for NEAT, 571

*authorization rules, 573-574*

*creating authorization profiles, 572*

*creating user identity group and identity, 571*

for staged deployment, Monitor Mode, 401-404

**primary devices, Policy**

Administration Node, 377-378

**primary nodes, 381**

monitoring and troubleshooting, 381-383

**printers, authorization policies, 436-437****privileges, network access privileges, defining, 61****probes, 475-476**

authorization policies, Logical Profiles, 164-165

configuring

*Device Sensor method, 425*

*RADIUS with SNMP Query method, 420-421*

*SNMP Trap method, 414*

Interface probe, 141

NetFlow, configuring, 481-483

profiling, 130

*configuring, 130-132*

*DHCP (Dynamic Host Configuration Protocol), 134*

*DNS, 139*

*HTTP, 132-133*

*HTTP, deployment considerations, 133-134*

*IOS Device-Sensor, 141-142*

*NetFlow, 137*

*NMAP, 138*

*RADIUS, 137-138*

*SNMP, 140-141*

System probe, 140

**Profiled Endpoints Summary Report, 493****profiler data sources, 81-82****profiler policies**

configuring

*CoA (Change of Authorization), 490*

*exceptions, 490*

NetFlow, examples, 483

**profiler reports, 493****profilers**

CoA (Change of Authorization), 488-489

exceptions, 488-489

monitoring and reporting, 491-493

**profiles**

authorization policies, 161

*endpoint identity groups, 161-163*

*EndPointPolicy, 163-164*

custom profiler conditions, creating, 479-480

custom profiler policies, creating, 480-481

Logical Profiles, 164-165

**profiling, 127-130**

best practices, 149-152

CoA (Change of Authorization), 133-142

*configuring, 143-144*

*message types, 142-143*

creating custom profiles for unknown endpoints, 475-476

infrastructure configuration, 144-145  
     *DHCP (Dynamic Host Configuration Protocol)*, 145  
     *SPAN (Switched Port Analyzer)*, 145-146  
     *VACL (VLAN Access Control Lists)*, 146-148  
     *VMware (promiscuous mode)*, 148-149  
 policies, endpoint profile policies, 150-154  
 probes, 130  
     *configuring*, 130-132  
     *DHCP (Dynamic Host Configuration Protocol)*, 134  
     *DNS*, 139  
     *HTTP*, 132-133  
     *HTTP, deployment considerations*, 133-134  
     *IOS Device-Sensor*, 141-142  
     *NetFlow*, 137  
     *NMAP*, 138  
     *RADIUS*, 137-138  
     *SNMP*, 140-141  
 profiling commands, global profiling commands, switches, 177  
 profiling policies, 80  
     identifying misconfigured devices, 428-429  
 promoting Secondary PAN to Primary, high availability, 385  
 protocols  
     CHAP (Challenge Handshake Authentication Protocol), 222  
     EAP (Extensible authentication protocol) types, 222  
     PAP (Password Authentication Protocol), 221

    SXP (Security Group eXchange Protocol), 508  
     tunneled EAP types, 222-224  
 PSNs (Policy Service Nodes), 29, 632  
 publishing certificate templates, 665  
 PXE (preboot execution environment), 42

## Q

---

questionnaires, sample ISE deployment questionnaire, 639-641

## R

---

**RADIUS**, 83  
     probes, 137-138  
         *deployment*, 138  
     SNMP query method, 420  
         *adding network devices*, 421  
         *configuring probes*, 420-421  
         *configuring switches*, 422-424  
**RADIUS accounting servers**, 186-187  
**RADIUS authentication**, 11, 185-186  
**RADIUS Authentication Troubleshooting**, 589-591  
**RADIUS commands, switches**, 172-174  
**RADIUS fallback**, 187  
**RBAC (role-based access control)**, 121  
     ISE GUI, 121  
         *access session settings*, 121-123  
         *authentication*, 123-124  
         *authorization*, 124-125  
         *passwords*, 124  
 reassessments, posture global setup, 286

record configuration, NetFlow, 485-486

registering ISE nodes to deployment, 379-381

Registry, editing, 665-667

Registry Condition settings, 290

relationships, authentication and authorization, 215-216

remediation actions, posture, 293

remote access, security domains, 56

remote-access VPN, authentication policies, 228-229

report groups, 585

reporting, 585

- data repositories, 586
- profilers, 491-493

reports

- profiler reports, 493
- running, 586

repositories, 619

- CD-ROM, 623
- configuring, 619-625
- FTP (File Transfer Protocol), 620-621
- host keys, 622
- HTTP, 624
- HTTPS, 624-625
- Network File System (NFS), 623
- SFTP (Secure File Transfer Protocol), 620-621
- TFTP, 622
- types of, 619-620

requirements

- ISE solution, 74
- for Microsoft Certificate Authority (CA), 645

requirements for ISE, 23-25

research, sources for, 75-76

restoring, 628-629

- patching, 629-631
- upgrading, 632-634

results, 206

re-using attributes, saving, 246-248

reviewing audit data, 91-92

RFC 2196, 51

role-based access control. *See* RBAC (role-based access control)

role-specific authorization rules, 237

routed mode, IPN (Inline Posture Node), 393-394

RSA key pairs, generating/exporting for certificate servers, 670-671

rules

- authorization rules, 12
- ISE solution, 74
- posture policy rules, adding, 74-75

rules and requirements structure, ISE, 70

running reports, 586

## S

---

sample ISE deployment questionnaire, 639-641

sample letter to students, Identity Services Engine, 638

sample notice for bulletin board/poster, Identity Services Engine, 636-638

sample requirement change notification email, Identity Services Engine, 635-636

samples

- NASP format for documenting ISE posture requirements, 72

- switch configurations
  - Catalyst 3000 Series, 12.2 (55) SE, 675-678*
  - Catalyst 3000 Series, 15.00(2) SE, 678-682*
  - Catalyst 4500 Series, IOS-XE 3.3.0/15.a(a)SG, 682-685*
  - Catalyst 6500 Series, 12.2(33) SXJ, 686-688*
- saving attributes for re-use, 246-248
- SCEP, configuring, 356-357
- scheduling backups, 628
- SecLists.org Security Mailing List Archive, 75
- secondary nodes, 381
  - monitoring and troubleshooting, 381-383
- Secondary PAN First (SPF), 632
- security, 2-3
  - AuthZ policies, creating for specific roles, 454-456
  - changing default authentication rule to deny access, 456-457
  - Permit Access Authorization result, 454
- security domains, defining, 55-57
- Security Group Access. *See* SGA (Security Group Access)
- Security Group eXchange Protocol. *See* SXP
- security group firewalls, 535
  - ASA, 535-536
  - ASR (aggregated services router), 543-544
  - configuring
    - SG-FW on an ASR and ISR, 544-546*
    - SG-FW policies via ASDM, 542*
    - TrustSec downloads from ISE via ASDM, 536-541*
  - ISR (integrated services routers), 543-544
  - validating TrustSec communication, 541
- Security Group Tags. *See* SGT
- security posture, establishing criteria to determine validity of checks, rules, and requirements, 76-77
- security requirements
  - deploying, 78-79
  - enforcing, 78-79
- SecurityFocus, 75
- seed devices, NDAC (Network Device Admission Control), configuring, 562-564
- Select Network Device Types wizard page, Cisco ISE Policy Setup Assistant wizard, 102-103
- self management, endpoints, 372
- Service Condition settings, 291
- Session Reauthentication, 143
- Session Terminate, 143
- Session Terminate with Port-Bounce, 143
- Setup Assistant, 169
- Setup task, 113
- SFTP (Secure File Transfer Protocol), 620-621
- SGA (Security Group Access), 495, 499-500
  - enforcement, 523-524
    - SGACL, 524-525*
- SGA, enforcement, security group firewalls. *See* security group firewalls
- SGACL, 524-525
  - configuring ISE to allow SGACLs to be downloaded, 531-532
  - configuring switches to download SGACLs from ISE, 532

- creating in ISE, 526-530
  - East-West, 525
  - North-South, 525
  - validating PAC file and CTS data downloads, 533-535
- SG-FW on an ASR and ISR, configuring, 544-546**
- SG-FW policies via ASDM, configuring, 542**
- SGT (Security Group Tag), 500-503**
  - access layer devices that do not support, 506
  - binding IP addresses to, 506
  - classification, 504
  - Closed Mode, 44
  - dynamically assigning via 802.1X, 504-505
  - Low-Impact Mode, 43
  - manually assigning at the port, 506
  - mapping subnets to, 507
  - mapping VLANs, 507-508
- SGT Propagation on Cisco IOS switches, configuring, 518-520**
- SGT propagation on Nexus series switches, configuring, 522-523**
- SGT propagation on a catalyst 6500, configuring, 520-522**
- show cts environment-data, 534**
- show cts interface, 556**
- show cts pac, 533**
- show cts role-based access-lists, 534**
- show cts role-based policy, 534**
- show cts role-based sgt-map, 535**
- show repository, 625**
- Simple Dictionary Condition settings, 290**
- single mode, MACSec, 551**
- single SSID, BYOD onboarding, 322-323**
  - with Applied iOS, 330-340
- SMS text messaging, configuring, 264**
- SNMP, probes, 140-141**
  - deployment, 140-141
- SNMP query method, RADIUS**
  - adding network devices, 421
  - configuring probes, 420-421
  - configuring switches, 422-424
- SNMP Trap method, 413**
  - adding network devices to ISE, 416-418
  - configuring
    - ISE probes, 414*
    - switches, 418-420*
- SNMPQuery, 140**
- SNMPTrap, 140**
- sources for providing identity and context awareness, 4-5**
- sources of research and information, 75-76**
- SPAN (Switched Port Analyzer), 595**
  - infrastructure configuration, 145-146
- SPAN-based collection methods, 34, 133**
- SPF (Secondary PAN First), 632**
- sponsor group policies, 257**
- sponsor portal layout, guest sponsor portals, 271-272**
- sponsor portals**
  - creating simple URLs for, 265
  - customizing, 264
- sponsor web portals, 251**
- staged deployment, preparing for (Monitor Mode), 401-404**
- subnets, mapping to SGTs, 507**
- Supervisor 2T, 520**

**supplicant, 301**

**supplicant switches, NEAT (Network Edge Authentication Topology), 574-575**

**supplicants**

Cisco AnyConnect Secure Mobility Client NAM, 312-316

comparing, 302-303

Mac OS X 10.8.2 native supplicant, configuring, 303

Windows 7 native supplicant, configuring, 309-312

Windows GPO for wired supplicant, configuring, 305-309

**support bundles, 611-612****switch configuration modes,**

**Downlink MACSec, 551-552**

**switch configurations, samples**

Catalyst 3000 Series, 12.2 (55)SE, 675-678

Catalyst 3000 Series, 15.00(2)SE, 678-682

Catalyst 4500 Series, IOS-XE 3.3.0/15.a(a)SG, 682-685

Catalyst 6500 Series, 12.2(33)SXJ, 686-688

**switch interfaces, configuring NDAC (Network Device Admission Control), 566-567**

**switch ports, moving**

from multi-auth to MDA, 473-474

from multi-auth to multi-domain, 457-458

**Switched Port Analyzer (SPAN), 595**

**switches, 170****assigning**

*to Closed Stage NDG, 468-469*

*to Low-Impact Stage network Device Group (NDG), 452-453*

**configuring**

*certificates, 170*

*Device Sensor method, 426-428*  
*to download SGACLs from ISE, 532*

*RADIUS with SNMP Query method, 422-424*

*SNMP Trap method, 418-420*

creating ACLs, 329

creating local access control lists, 174-175

desktop switches, NEAT (Network Edge Authentication Topology), 574-575

with Device Sensor capabilities, 177-178

enabling HTTP/HTTPS servers, 170-171

global 802.1X commands, 175

global AAA commands, 171-172

global configuration settings, 170

global logging commands, 175-177

global profiling commands, 177

global RADIUS commands, 172-174

interface configuration settings, 179

*applying ACL to the port and enabling authentication, 184*

*configuring authentication settings, 182-183*

*configuring authentication timers, 184*

*configuring flexible authentication and high availability, 179-182*

*configuring interfaces as switch ports, 179*

modifying default port ACL, Low-Impact Mode, 453-454

without Device Sensor capabilities, 178

**SXP (Security Group eXchange Protocol), 508**

## configuring

*on Cisco ASA, 513-515**on iOS devices, 509-511**on WLC, 511-513*

## design, 508-509

**System probe, 140****T**

---

**Task Navigator, 113****TCAM (Ternary CAM), 498****TCP Dump, 594****Ternary CAM (TCAM), 498****TFTP, 622****themes, customizing portal themes, 266-267****tools, troubleshooting**

Evaluate Configuration Validator, 591-593

RADIUS Authentication  
Troubleshooting, 589-591

TCP Dump, 594

**Top Authorization By User Report, 93****transitioning**from Monitor Mode to Closed  
Mode, 461

from Monitor Mode to end state, 408-409

from Monitor Mode to Low-Impact  
Mode, 445-446  
*to end-state mode, 45-46***troubleshooting**

Active Directory, disconnections, 610

authentication and authorization, 596-597

*entries exist in the live log, 603-604**no live log entry exists, 597-602*

debut situations, 611-612

high-level troubleshooting flowchart, 605

primary and secondary nodes, 381-383

support bundles, 611-612

**tools***Evaluate Configuration  
Validator, 591-593**RADIUS Authentication  
Troubleshooting, 589-591**TCP Dump, 594*

WebAuth and URL redirection, 605-609

**TrustSec, 9****TrustSec communication, validating, 541****TrustSec downloads from ISE via ASDM, configuring, 536-541****tunneled EAP types, 222-224****U**

---

**UDI (Unique Device Identifier), 97****unique values for unknown devices, identifying for unknown devices, 476-478****unknown devices, identifying unique values, 476-478****unknown endpoints, custom profiles for, 475-476**



- Unknown NAD alarms, 598
- unsupported mobile devices, BYOD
  - onboarding, Blackberry, 346-347
- updates, posture global setup, 287
- upgrading, 632-634
- Uplink MACSec, 553
  - configuring, 553-555
  - verifying configuration, 556-557
- URL redirection, troubleshooting, 605-609
- URL-Redirection
  - Closed Mode, 44
  - Low-Impact Mode, 43
- URLs, creating for sponsor portals, 265
- US-CERT, 76
- user accounting, 92-93
- User Authentication Summary Report, 92
- user authentications, authorization policies, 439-440
- user identity groups, creating for NEAT, 571
- user-agent string, 477

## V

---

- VACL (VLAN Access Control Lists), 146-148
- validating
  - PAC files and CTS data downloads, 533-535
  - TrustSec communication, 541
- VDI (virtual desktop infrastructure), 42
- verifying
  - configurations, Uplink MACSec, 556-557
  - default unavailable client provisioning policy action, 352
- virtual desktop infrastructure (VDI), 42
- virtual machine (VM), 25
- VLAN Access Control Lists (VACL), 146-148
- VLAN assignments, ingress access control, 495-497
- VLANs, mapping to SGTs, 507-508
- VM (virtual machine), 25
- VMware (promiscuous mode), 148-149
- VPN authentication, 4, 11

## W-X-Y-Z

---

- Web Agent for Windows
  - posture checks, 71
  - posture remediation actions, 70
- Web Auth, 258
- Web Auth dACL, 259
- Web Authentication, 11
  - central Web Authentication, 249-250
  - central Web Authentication flow, 249-251
  - local Web Authentication, 249-250
  - local Web Authentication flow, 249
- web authentication authorization results
  - Closed Mode, 463-466
  - creating, 448-449
- web authentication identity source sequence
  - Closed Mode, 466
  - configuring, 451
- web authentication redirection ACL, 188-191

web redirect, 4

## WebAuth

authorization profile, 262

configuring, 351

troubleshooting, 605-609

WebAuth Authorization Profile, 449

WebAuth Loop, 617

WEP (Wired Equivalency Protection), 547

Windows, BYOD onboarding, 364-366

Windows 7 native supplicant, configuring, 309-312

Windows Automatic Update, 294

Windows GPO for wired supplicant, configuring, 305-309

Windows Update Remediation action, 294

Windows Update service, posture policy, 297

wired switch configuration basics, 106-109

wired switches, configuring for network devices for guest CWA, 274-275

wired URL Redirection, 606-607

wireless, 215

security domains, 56

wireless APs, authorization policies, 435

wireless controller configuration basics, 109-113

Wireless Equivalency, 547

Wireless LAN Controller. *See* WLC

wireless LANs, 195

creating

*corporate SSID, 199-202*

*Guest WLANs, 195-198*

Wireless Network Controller settings, Cisco ISE Policy Setup Assistant wizard, 103

wireless networks, deployment phases, 409

wireless redirection, 607

wireless SSID, authentication policies, 225-228

wireless\_access compound condition, 236

## wizards

Cisco ISE Policy Setup Assistant wizard, 97-104

Cisco Setup Assistant Wizard, 169

WLC (Wireless Lan Controller), 184-185, 495

assigning to Closed Stage NDG, 468-469

assigning to Low-Impact Stage Network Device Group (NDG), 452-453

configuring AAA servers, 185-187

configuring Airespace ACLs, 188-192

configuring for network devices for guest CWA, 275

creating ACLs, BYOD onboarding, 328

dynamic interfaces for client VLANs, 193-195

SXP (Security Group eXchange Protocol), configuring, 511-513

wireless LANs, 195-202

WLC configuration, BYOD onboarding, 324-327

WSUS remediation action, 295

WSUS rule, 294