



Practice Tests



Flash Cards



Study Planner



Video Training



Review Exercises

# Official Cert Guide

Advance your IT career with hands-on learning

# CCNP Security Identity Management

## SISE 300-715

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

**AARON WOLAND**, CCIE® No. 20113  
**KATHERINE McNAMARA**, CCIE® No. 50931

FREE SAMPLE CHAPTER  
SHARE WITH OTHERS



# **CCNP Security Identity Management SISE 300-715**

**Official** Cert Guide

**Enhance Your Exam Preparation**

## **Save 80% on Premium Edition eBook and Practice Test**

The *CCNP Security Identity Management SISE 300-715 Official Cert Guide Premium Edition and Practice Test* provides three eBook files (PDF, EPUB, and MOBI/Kindle) to read on your preferred device and an enhanced edition of the Pearson Test Prep practice test software. You also receive two additional practice exams with links for every question mapped to the PDF eBook.

**See the card insert in the back of the book for your Pearson**

**CCNP  
Security  
Identity  
Management  
SISE 300-715  
Official Cert Guide**

**AARON WOLAND, CCIE No. 20113**

**KATHERINE MCNAMARA, CCIE No. 50931**

**Cisco Press**

# CCNP Security Identity Management SISE 300-715 Official Cert Guide

Aaron Woland

Katherine McNamara

Copyright© 2021 Cisco Systems, Inc.

Published by:  
Cisco Press

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit [www.pearson.com/permissions](http://www.pearson.com/permissions).

No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ScoutAutomatedPrintCode

Library of Congress Control Number: 2020913602

ISBN-10: 0-13-664294-2

ISBN-13: 978-0-13-664294-7

## Warning and Disclaimer

This book is designed to provide information about the Implementing and Configuring Cisco Identity Services Engine (SISE 300-715) exam. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

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

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

## Trademark Acknowledgments

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

## Special Sales

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

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

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

## Feedback Information

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

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

We greatly appreciate your assistance.

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

**Copy Editor:** Kitty Wilson

**Alliances Manager, Cisco Press:** Arezou Gol

**Technical Editor:** Akhil Behl

**Director, ITP Product Management:** Brett Bartow

**Editorial Assistant:** Cindy Teeters

**Executive Editor:** James Manly

**Designer:** Chuti Prasertsith

**Managing Editor:** Sandra Schroeder

**Composition:** codeMantra

**Development Editor:** Christopher A. Cleveland

**Indexer:** Erika Millen

**Project Editor:** Mandie Frank

**Proofreader:** Donna Mulder



**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV Amsterdam,  
The Netherlands

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

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

## Credits

Figure Number	Attribution/Credit Line
Figure 2-7	Screenshot of ISE LDAP Identity Source Configuration © Microsoft 2020
Figure 2-11	Screenshot of Authy One-Time Password Soft Token App © 2020 Twilio, Inc.
Figure 3-6	Screenshot of Windows Services Control Applet © Microsoft 2020
Figure 3-7	Screenshot of Wired AutoConfig Properties © Microsoft 2020
Figure 3-8	Screenshot of Local-Area Connection Properties © Microsoft 2020
Figure 3-9	Screenshot of Authentication Tab © Microsoft 2020
Figure 3-10	Screenshot of Protected EAP Properties Dialog © Microsoft 2020
Figure 3-11	Screenshot of EAP MSCHAPv2 Properties Dialog © Microsoft 2020
Figure 3-12	Screenshot of EAP MSCHAPv2 Properties Dialog © Microsoft 2020
Figure 3-13	Screenshot of Back to the Protected EAP Properties © Microsoft 2020
Figure 3-14	Screenshot of Back to the Authentication Tab © Microsoft 2020
Figure 3-15	Screenshot of Advanced Settings Tab © Microsoft 2020
Figure 3-16	Screenshot of Authentication Mode Choices © Microsoft 2020
Figure 15-16	Screenshot of Connecting to a CA's Website © Microsoft 2020
Figure 15-17	Screenshot of Downloading a Public Certificate © Microsoft 2020
Figure 21-66	Screenshot of Launching DART from the Start Menu © Microsoft 2020
Figure 23-10	Screenshot of Users Must Be Part of the Security Manager Role in Tenable.SC © 2020 Tenable, Inc.
Figure 23-12	Screenshot of Tenable.SC Repositories © 2020 Tenable, Inc.
Figure 23-13	Screenshot of Tenable.SC Scan Results © 2020 Tenable, Inc.
Figure 23-29	Screenshot of Tenable.SC Scan Results © 2020 Tenable, Inc.

## Contents at a Glance

Introduction xxxvi

### **Part I Authentication, Authorization, and Accounting**

- Chapter 1 Fundamentals of AAA 2
- Chapter 2 Identity Management 18
- Chapter 3 Extensible Authentication Protocol (EAP) over LAN: 802.1X 38
- Chapter 4 Non-802.1X Authentication 76
- Chapter 5 Introduction to Advanced Concepts 92

### **Part II Cisco Identity Services Engine**

- Chapter 6 Cisco Identity Services Engine Architecture 104
- Chapter 7 A Guided Tour of the Cisco ISE Graphical User Interface (GUI) 122
- Chapter 8 Initial Configuration of Cisco ISE 174
- Chapter 9 Authentication Policies 206
- Chapter 10 Authorization Policies 232

### **Part III Implementing Secure Network Access**

- Chapter 11 Implement Wired and Wireless Authentication 258
- Chapter 12 Web Authentication 306
- Chapter 13 Guest Services 334
- Chapter 14 Profiling 402

### **Part IV Advanced Secure Network Access**

- Chapter 15 Certificate-Based Authentication 460
- Chapter 16 Bring Your Own Device 482
- Chapter 17 TrustSec and MACSec 548
- Chapter 18 Posture Assessment 626

## **Part V Safely Deploying in the Enterprise**

Chapter 19 Deploying Safely 714

Chapter 20 ISE Scale and High Availability 734

Chapter 21 Troubleshooting Tools 764

## **Part VI Extending Secure Access Control**

Chapter 22 ISE Context Sharing and Remediation 818

Chapter 23 Threat Centric NAC 868

## **Part VII Device Administration AAA**

Chapter 24 Device Administration AAA with ISE 906

Chapter 25 Configuring Device Administration AAA with Cisco IOS 930

Chapter 26 Configuring Device Admin AAA with the Cisco WLC 968

## **Part VIII Final Preparation**

Chapter 27 Final Preparation 988

## **Part IX Appendixes**

Glossary of Key Terms 991

Appendix A Answers to the “Do I Know This Already?” Quizzes and Q&A Sections 1002

Appendix B CCNP Security Implementing and Configuring Cisco Identity Services Engine (SISE 300-715) Exam Updates 1032

Appendix C Sample Switch Configurations 1034

Index 1062

## **Online Element**

Appendix D Study Planner

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

## Contents

	Introduction	xxxvi
<b>Part I</b>	<b>Authentication, Authorization, and Accounting</b>	
<b>Chapter 1</b>	<b>Fundamentals of AAA</b>	<b>2</b>
	“Do I Know This Already?” Quiz	3
	Foundation Topics	5
	Comparing and Selecting AAA Options	5
	Device Administration AAA	6
	Network Access AAA	7
	TACACS+	7
	TACACS+ Authentication Messages	9
	TACACS+ Authorization and Accounting Messages	10
	RADIUS	12
	AV Pairs	15
	Change of Authorization (CoA)	16
	Comparing RADIUS and TACACS+	16
	Exam Preparation Tasks	16
	Review All Key Topics	16
	Define Key Terms	17
	Q&A	17
<b>Chapter 2</b>	<b>Identity Management</b>	<b>18</b>
	“Do I Know This Already?” Quiz	18
	Foundation Topics	20
	What Is an Identity?	20
	Identity Stores	20
	Internal Identity Stores	21
	<i>Internal User Identities</i>	21
	<i>User Identity Groups</i>	22
	<i>Endpoint Groups</i>	22
	External Identity Stores	23
	<i>Active Directory</i>	24
	LDAP	25
	<i>Multifactor Authentication</i>	26
	<i>One-Time Password (OTP) Services</i>	29
	<i>Smart Cards</i>	29
	<i>Certificate Authorities</i>	30

	<i>Has the Digital Certificate Been Signed by a Trusted CA?</i>	31
	<i>Has the Certificate Expired?</i>	32
	<i>Has the Certificate Been Revoked?</i>	33
	Identity Source Sequences	34
	Special Identity Sources	35
	SAML IdPs	35
	Social Login	35
	Exam Preparation Tasks	36
	Review All Key Topics	36
	Define Key Terms	36
	Q&A	36
<b>Chapter 3</b>	<b>Extensible Authentication Protocol (EAP) over LAN: 802.1X</b>	<b>38</b>
	“Do I Know This Already?” Quiz	38
	Foundation Topics	41
	Extensible Authentication Protocol	41
	EAP over LAN (802.1X)	41
	EAP Types	42
	<i>Native EAP Types (Non-Tunneled EAP)</i>	43
	<i>Tunneled EAP Types</i>	44
	<i>All Tunneled EAP Types</i>	47
	<i>EAP Authentication Type Identity Store Comparison</i>	49
	Network Access Devices	49
	Supplicant Options	50
	Windows Native Supplicant	50
	<i>User Authentication</i>	58
	<i>Machine Authentication (Computer Authentication)</i>	58
	Cisco AnyConnect NAM Supplicant	59
	<i>Client Policy</i>	61
	<i>Authentication Policy</i>	62
	<i>Networks</i>	62
	<i>Network Groups</i>	71
	<i>Implementing AnyConnect NAM Profiles</i>	71
	<i>EAP Chaining</i>	73
	Exam Preparation Topics	73
	Review All Key Topics	73
	Define Key Terms	74
	Q&A	74

**Chapter 4 Non-802.1X Authentication 76**

- “Do I Know This Already?” Quiz 76
- Foundation Topics 79
- Devices Without a Supplicant 79
- MAC Authentication Bypass 80
- Web Authentication 83
  - Local Web Authentication 84
  - Local Web Authentication with a Centralized Portal 84
  - Centralized Web Authentication 85
  - Centralized Web Authentication with Third-Party Network Device Support 87
- Remote-Access Connections 88
- EasyConnect 89
- Exam Preparation Tasks 90
- Review All Key Topics 90
- Define Key Terms 91
- Q&A 91

**Chapter 5 Introduction to Advanced Concepts 92**

- “Do I Know This Already?” Quiz 92
- Foundation Topics 95
- Change of Authorization 95
- Automating MAC Authentication Bypass (MAB) 96
- Posture Assessment 99
- Mobile Device Management (MDM) 101
- Exam Preparation Tasks 102
- Review All Key Topics 102
- Define Key Terms 102
- Q&A 103

**Part II Cisco Identity Services Engine**

**Chapter 6 Cisco Identity Services Engine Architecture 104**

- “Do I Know This Already?” Quiz 104
- Foundation Topics 106
- What Is Cisco ISE? 106
- Personas 108
  - Administration Persona 109
  - Monitoring Persona 109

Policy Services Persona	110	
pxGrid Persona	111	
Physical or Virtual Appliances	111	
ISE Deployment Scenarios	113	
Single-Node Deployment	113	
Two-Node Deployment	114	
Distributed Deployments	116	
Exam Preparation Tasks	120	
Review All Key Topics	120	
Define Key Terms	120	
Q&A	120	
<b>Chapter 7</b>	<b>A Guided Tour of the Cisco ISE Graphical User Interface (GUI)</b>	<b>122</b>
“Do I Know This Already?” Quiz	123	
Foundation Topics	125	
Logging in to ISE	125	
Initial Login	125	
ISE Home Dashboards	132	
Administration Portal	137	
<i>Global Search for Endpoints</i>	139	
<i>Help Menu</i>	140	
<i>ISE Setup Wizards</i>	141	
<i>Settings Menu</i>	142	
Organization of the ISE GUI	142	
Context Visibility	143	
Operations	143	
RADIUS	144	
<i>Threat-Centric NAC Live Logs</i>	146	
<i>TACACS Live Log</i>	147	
<i>Troubleshoot</i>	147	
<i>Adaptive Network Control</i>	148	
<i>Reports</i>	150	
Policy	150	
<i>Policy Sets</i>	150	
<i>Profiling</i>	152	
<i>Posture</i>	152	
<i>Client Provisioning</i>	153	
<i>Policy Elements</i>	154	

Administration	155
System	155
Identity Management	161
Network Resources	163
Device Portal Management	166
pxGrid Services	169
Feed Service	169
Threat Centric NAC	170
Work Centers	170
Types of Policies in ISE	171
Authentication	171
Authorization	171
Profiling	172
Posture	172
Client Provisioning	172
TrustSec	172
Exam Preparation Tasks	173
Review All Key Topics	173
Define Key Term	173
Q&A	173
<b>Chapter 8 Initial Configuration of Cisco ISE</b>	<b>174</b>
“Do I Know This Already?” Quiz	174
Foundation Topics	177
Cisco Identity Services Engine Form Factors	177
Bootstrapping Cisco ISE	177
Where Are Certificates Used with Cisco Identity Services Engine?	181
Self-Signed Certificates	181
CA-Signed Certificates	182
Network Devices	192
Network Device Groups	192
Network Access Devices	192
ISE Identity Stores	194
Local User Identity Groups	194
Local Endpoint Groups	195
Local Users	195
External Identity Stores	196
Active Directory	196

	<i>Prerequisites for Joining an Active Directory Domain</i>	196
	<i>Joining an Active Directory Domain</i>	197
	Certificate Authentication Profile (CAP)	202
	Identity Source Sequences	202
	Exam Preparation Topics	204
	Review All Key Topics	204
	Define Key Terms	204
	Q&A	205
<b>Chapter 9</b>	<b>Authentication Policies</b>	<b>206</b>
	“Do I Know This Already?” Quiz	207
	Foundation Topics	209
	The Relationship Between Authentication and Authorization	209
	Authentication Policy	210
	Goal 1: Accept Only Allowed Protocols	210
	Goal 2: Select the Correct Identity Store	210
	Goal 3: Validate the Identity	211
	Goal 4: Pass the Request to the Authorization Policy	211
	Understanding Policy Sets	211
	Allowed Protocols	213
	Understanding Authentication Policies	216
	Conditions	217
	Identity Store	219
	Options	220
	Common Authentication Policy Examples	220
	Using the Wireless SSID	220
	Remote Access VPN	223
	Alternative ID Stores Based on EAP Type	224
	More on MAB	227
	Restore the Authentication Policy	229
	Exam Preparation Tasks	230
	Review All Key Topics	230
	Q&A	230
<b>Chapter 10</b>	<b>Authorization Policies</b>	<b>232</b>
	“Do I Know This Already?” Quiz	232
	Foundation Topics	235
	Authentication Versus Authorization	235

- Authorization Policies 235
  - Goals of Authorization Policies 235
  - Understanding Authorization Policies* 236
  - Role-Specific Authorization Rules* 241
  - Authorization Policy Example 241
  - Employee Full Access Rule* 241
  - Internet Only for Smart Devices Rule* 243
  - Employee Limited Access Rule* 246
- Saving Conditions for Reuse 249
  - Combining AND with OR Operators 252
- Exam Preparation Tasks 256
- Review All Key Topics 256
- Define Key Terms 256
- Q&A 256

### **Part III Implementing Secure Network Access**

#### **Chapter 11 Implement Wired and Wireless Authentication 258**

- “Do I Know This Already?” Quiz 259
- Foundation Topics 261
- Authentication Configuration on Wired Switches 261
  - Global Configuration AAA Commands 261
  - Global Configuration RADIUS Commands 262
  - IOS 12.2.x* 262
  - IOS 15.x and IOS XE* 263
  - IOS 12.2.x, 15.x, and IOS XE* 264
  - Global 802.1X Commands* 266
  - Device Tracking in IOS XE 16.x and Later* 267
  - Creating Local Access Control Lists* 268
- Interface Configuration Settings for All Cisco Switches 269
  - Configure Interfaces as Switch Ports* 269
  - Configure Flexible Authentication and High Availability* 269
  - Host Mode of the Switch Port* 272
  - Configure Authentication Settings* 274
  - Configure Authentication Timers* 275
  - Apply the Initial ACL to the Port and Enable Authentication* 275
- Authentication Configuration on WLCs 276
  - Configure the AAA Servers 276
  - Add the RADIUS Authentication Servers* 277

<i>Add the RADIUS Accounting Servers</i>	278
<i>Configure RADIUS Fallback (High Availability)</i>	279
Configure the Airespace ACLs	280
<i>Create the Web Authentication Redirection ACL</i>	280
<i>Add Google URLs for ACL Bypass</i>	282
<i>Create the Posture Agent Redirection ACL</i>	283
Create the Dynamic Interfaces for the Client VLANs	284
<i>Create the Employee Dynamic Interface</i>	284
<i>Create the Guest Dynamic Interface</i>	285
Create the Wireless LANs	286
<i>Create the Guest WLAN</i>	287
<i>Create the Corporate WLAN</i>	291
Verifying Dot1x and MAB	295
Endpoint Supplicant Verification	295
Network Access Device Verification	296
<i>Verifying Authentications with Cisco Switches</i>	296
<i>Sending Syslog to ISE</i>	299
<i>Verifying Authentications with Cisco WLCs</i>	300
Cisco ISE Verification	302
<i>RADIUS Live Log</i>	302
Live Sessions	303
Looking Forward	303
Exam Preparation Tasks	303
Review All Key Topics	303
Define Key Terms	304
Q&A	304
<b>Chapter 12 Web Authentication</b>	<b>306</b>
“Do I Know This Already?” Quiz	306
Foundation Topics	309
Web Authentication Scenarios	309
Local Web Authentication (LWA)	310
Centralized Web Authentication (CWA)	311
Configuring Centralized Web Authentication	313
Cisco Switch Configuration	313
<i>Configure Certificates on the Switch</i>	313
<i>Enable the Switch HTTP/HTTPS Server</i>	314
<i>Verify the URL-Redirect ACL</i>	314

Cisco WLC Configuration	315
<i>Validate That MAC Filtering Is Enabled on the WLAN</i>	315
<i>Validate That ISE NAC Is Enabled on the WLAN</i>	315
<i>Validate That the URL-Redirection ACL Is Configured</i>	316
Configure ISE for Centralized Web Authentication	317
<i>Configure MAB Continue for the Authentication</i>	318
<i>Verify the Web Authentication Identity Source Sequence</i>	319
<i>Configure a dACL for Pre-WebAuth Authorization</i>	319
<i>Configure an Authorization Profile</i>	320
Building CWA Authorization Policies	322
Create the Rule to Redirect Users to the CWA Portal	323
Create the Rules to Authorize Users Who Authenticate via CWA	323
Verifying Centralized Web Authentication	324
Check the Experience from the Client	324
Verify CWA Through the ISE UI	327
<i>Check Live Log</i>	327
Check the NAD	327
<i>show Commands on the Wired Switch</i>	328
<i>Viewing the Client Details on the WLC</i>	329
Exam Preparation Tasks	331
Review All Key Topics	331
Define Key Terms	331
Q&A	332

## **Chapter 13 Guest Services 334**

“Do I Know This Already?” Quiz	334
Foundation Topics	337
Guest Services Overview	337
Portals, Portals, and More Portals!	341
Guest Portal Types	341
<i>Hotspot Guest Portal</i>	342
<i>Self-Registered Guest Portal</i>	342
<i>Sponsored Guest Portal</i>	342
Guest Types	343
<i>Contractor</i>	344
<i>Daily</i>	346
<i>Weekly</i>	347
<i>Social</i>	348
Guest Portals and Authorization Policy Rules	348

Configuring Guest Portals and Authorization Rules	351
Configuring a Hotspot Guest Portal	351
<i>Portal Behavior and Flow Settings</i>	351
<i>Portal Page Customization</i>	358
<i>Authorization Rule Configuration</i>	362
Configuring a Self-Registered Guest Portal	365
<i>Portal Settings</i>	366
<i>Login Page Settings</i>	367
<i>Registration Form Settings</i>	368
<i>Self-Registration Success</i>	371
<i>Guest Change Password Settings and Guest Device Registration Settings</i>	371
<i>BYOD Settings</i>	372
<i>Guest Device Compliance Settings</i>	373
<i>Authorization Rule Configuration</i>	373
Configuring a Sponsored Guest Portal	380
Sponsors	381
Sponsor Groups	381
Sponsor Portals	384
<i>Portal Settings</i>	385
<i>Login Settings and AUP Page Settings</i>	386
<i>The Remaining Settings</i>	387
Notification Services	388
<i>SMTP Servers</i>	388
<i>SMS Gateway Providers</i>	388
Provisioning Guest Accounts from a Sponsor Portal	389
SAML Authentication	394
Call to Action	400
Exam Preparation Tasks	400
Review All Key Topics	400
Define Key Terms	401
Q&A	401
<b>Chapter 14 Profiling</b>	<b>402</b>
“Do I Know This Already?” Quiz	402
Foundation Topics	404
ISE Profiler	404
Anomalous Behaviour	406
Cisco ISE Probes	409

<i>Probe Configuration</i>	409
<i>DHCP and DHCPSPAN</i>	411
<i>RADIUS</i>	414
<i>Network Scan (Nmap)</i>	415
<i>DNS</i>	417
<i>SNMPQUERY and SNMPTRAP</i>	417
<i>NETFLOW</i>	419
<i>HTTP Probe</i>	420
<i>Active Directory Probe</i>	422
<i>pxGrid Probe</i>	423
Infrastructure Configuration	424
DHCP Helper	424
SPAN Configuration	424
VLAN Access Control Lists (VACLs)	425
Device Sensor	426
VMware Configurations to Allow Promiscuous Mode	427
Profiling Policies	429
Profiling Feed Service	429
<i>Configuring the Profiler Feed Service</i>	429
<i>Verifying the Profiler Feed Service</i>	429
Endpoint Profile Policies	431
Logical Profiles	441
ISE Profiler and CoA	442
Global CoA	442
Per-Profile CoA	443
Global Profiler Settings	444
Configure SNMP Settings for Probes	444
Endpoint Attribute Filtering	444
Custom Attributes for Profiling	445
Publishing Endpoint Probe Data on pxGrid	450
Profiles in Authorization Policies	450
Endpoint Identity Groups	450
EndPointPolicy	453
Verify Profiling	454
The Dashboard	454
Global Search	454
Endpoint Identities	455
Device Sensor show Commands	457

Exam Preparation Topics 458

Review All Key Topics 458

Define Key Terms 458

Q&A 458

## **Part IV      Advanced Secure Network Access**

### **Chapter 15    Certificate-Based Authentication    460**

“Do I Know This Already?” Quiz 460

Foundation Topics 463

Certificate Authentication Primer 463

    Determine If a Trusted Authority Has Signed the Digital Certificate 463

    Examine Both the Start and End Dates to Determine If the Certificate Has Expired 465

    Verify If the Certificate Has Been Revoked 466

    Validate That the Client Has Provided Proof of Possession 468

A Common Misconception About Active Directory 469

EAP-TLS 470

Configuring ISE for Certificate-Based Authentications 470

    Validate Allowed Protocols 470

    Certificate Authentication Profile 471

    Verify the Authentication Policy Is Using the CAP 472

    Authorization Policies 474

    Ensure the Client Certificates Are Trusted 475

*Import the Certificate Authority’s Public Certificate* 476

*Configure Certificate Status Verification (Optional)* 478

Exam Preparation Tasks 479

Review All Key Topics 479

Define Key Terms 480

Q&A 480

### **Chapter 16    Bring Your Own Device    482**

“Do I Know This Already?” Quiz 483

Foundation Topics 485

BYOD Challenges 485

Onboarding Process 487

    BYOD Onboarding 487

*Dual SSID* 487

*Single SSID* 488

Configuring NADs for Onboarding	489
Configuring a WLC for Dual SSID Onboarding	489
<i>Review of the WLAN Configuration</i>	490
<i>Verify the Required ACLs</i>	492
ISE Configuration for Onboarding	495
The End-User Experience	496
<i>Single SSID with Apple iOS Example</i>	496
<i>Dual SSID with Android Example</i>	503
<i>Unsupported Mobile Device: BlackBerry Example</i>	508
Configuring ISE for Onboarding	510
<i>Creating the Native Supplicant Profile</i>	510
<i>Configure the Client Provisioning Policy</i>	512
<i>Configure the WebAuth</i>	514
<i>Verify Default Unavailable Client Provisioning Policy Action</i>	515
<i>Create the Authorization Profiles</i>	516
<i>Create the Authorization Rules for Onboarding</i>	517
<i>Create the Authorization Rules for the EAP-TLS Authentications</i>	518
ISE as a Certificate Authority	519
Configuring SCEP	520
Configuring ISE as an Intermediate CA	521
BYOD Onboarding Process Detailed	523
iOS Onboarding Flow	523
<i>Phase 1: Device Registration</i>	523
<i>Phase 2: Device Enrollment</i>	525
<i>Phase 3: Device Provisioning</i>	526
Android Flow	526
<i>Phase 1: Device Registration</i>	526
<i>Phase 2: NSP App Download App</i>	528
<i>Phase 3: Device Provisioning</i>	529
Windows and macOS Flow	531
<i>Phase 1: Device Registration</i>	531
<i>Phase 2: Device Provisioning</i>	532
Verifying BYOD Flows	534
RADIUS Live Logs	534
Reports	534
Identity Group	535

MDM Onboarding	535
Integration Points	536
Configuring MDM Integration	537
Configuring MDM Onboarding Rules	539
<i>Create the Authorization Profile</i>	539
<i>Create the Authorization Rules</i>	540
Managing Endpoints	542
Self-Management	543
Administrative Management	545
The Opposite of BYOD: Identify Corporate Systems	545
Exam Preparation Topics	546
Review All Key Topics	547
Define Key Terms	547
Q&A	547
<b>Chapter 17 TrustSec and MACsec</b>	<b>548</b>
“Do I Know This Already?” Quiz	548
Foundation Topics	551
Ingress Access Control Challenges	551
VLAN Assignment	551
Ingress Access Control Lists	553
East–West Segmentation	554
What Is TrustSec?	555
What Is a Security Group Tag?	556
What Is the TrustSec Architecture?	557
TrustSec-Enabled Network Access Devices	558
Defining the TrustSec Settings for a Network Access Device	559
Configuring an IOS XE Switch for TrustSec	560
Configuring an ASA for TrustSec	564
Network Device Admission Control (NDAC)	566
Configuring the Seed Device	566
Configuring the Non-Seed Device	567
Defining the SGTs	572
Classification	575
Dynamically Assigning SGT via 802.1X	577
Manually Assigning SGTs to a Port	577
Manually Binding IP Addresses to SGTs in ISE	578
Access-Layer Devices That Do Not Support SGTs	580

<i>Mapping a Subnet to an SGT</i>	580
<i>Mapping a VLAN to an SGT</i>	580
Transport: SGT Exchange Protocol (SXP)	581
SXP Design	582
Configuring SXP on ISE	584
Configuring SXP on IOS Devices	587
Configuring SXP on Wireless LAN Controllers	590
Configuring SXP on Cisco ASA	591
Verifying SXP Connections in ASDM	592
Transport: Native Tagging	593
Configuring Native SGT Propagation (Tagging)	594
Configuring Manual SGT Propagation on Cisco IOS XE Switches	595
Enforcement	597
SGACL	597
<i>Configuring Security Group ACLs</i>	601
TrustSec Policy Matrix	604
<i>Configuring the TrustSec Policy Matrix</i>	605
Security Group Firewalls	611
<i>Security Group Firewall on the ASA</i>	612
<i>Security Group Firewall on the Firepower</i>	612
<i>Security Group Firewall on the ISR and ASR</i>	613
Software-Defined Access (SD-Access)	613
MACsec	614
Downlink MACsec	616
<i>Switch Configuration Modes</i>	618
<i>ISE Configuration</i>	619
Uplink MACsec	619
<i>Manually Configuring Uplink MACsec</i>	620
<i>Verifying the Manual Configuration</i>	622
Exam Preparation Tasks	623
Review All Key Topics	623
Define Key Terms	623
Q&A	624
<b>Chapter 18 Posture Assessment</b>	<b>626</b>
“Do I Know This Already?” Quiz	626
Foundation Topics	629

Posture Assessment with ISE	629
A Bit of a History Lesson	629
ISE Posture Flows	633
Configuring Posture	636
Update the Compliance Modules	637
Configure Client Provisioning	638
<i>Protect Your Sanity</i>	638
<i>Download AnyConnect</i>	640
<i>Upload AnyConnect Headend Deployment Packages to ISE</i>	642
<i>Configure the Client Provisioning Portal</i>	650
<i>Configure the Client Provisioning Policy</i>	652
Configuring Posture Policy Elements	653
<i>Conditions</i>	654
<i>Remediations</i>	679
<i>Requirements</i>	687
Configure Posture Policies	688
Other Important Posture Settings	690
<i>Posture Lease</i>	691
<i>Cache Last Known Posture Compliant Status</i>	691
<i>Reassessment Configurations</i>	691
Authorization Rules	693
<i>Create an Authorization Profile for Redirection</i>	693
<i>Create the Authorization Rules</i>	694
The Endpoint Experience	695
Scenario 1: AnyConnect Not Installed on Endpoint Yet	696
Scenario 2: AnyConnect Already Installed, Endpoint Not Compliant	700
Scenario 3: Stealth Mode	703
Scenario 4: Temporal Agent and Posture Compliant	705
Mobile Posture	707
Create Mobile Posture Authorization Conditions	709
Create Mobile Posture Authorization Rules	710
Exam Preparation Tasks	713
Review All Key Topics	713
Define Key Terms	713
Q&A	713

**Part V Safely Deploying in the Enterprise**

**Chapter 19 Deploying Safely 714**

“Do I Know This Already?” Quiz 714  
Foundation Topics 717  
Why Use a Phased Approach? 717  
Comparing authentication open to Standard 802.1X 719  
Prepare ISE for a Staged Deployment 720  
Monitor Mode 722  
Low-Impact Mode 725  
Closed Mode 728  
Transitioning from Monitor Mode to Your End State 730  
Wireless Networks 731  
Exam Preparation Tasks 731  
Review All Key Topics 731  
Q&A 732

**Chapter 20 ISE Scale and High Availability 734**

“Do I Know This Already?” Quiz 734  
Foundation Topics 737  
Configuring ISE Nodes in a Distributed Environment 737  
    Make the First Node a Primary Device 738  
    Registering an ISE Node to the Deployment 739  
    Ensure That the Persona of Each Node Is Accurate 742  
Understanding the High Availability Options Available 743  
    Primary and Secondary Nodes 743  
    *Monitoring and Troubleshooting Nodes* 743  
    Policy Administration Nodes 745  
    *Promoting the Secondary PAN to Primary* 745  
    *Auto PAN Switchover* 745  
    *Configuring Automatic Failover for the Primary PAN* 746  
    *Licensing in a Multi-Node ISE Cube* 747  
Node Groups 748  
    *Add the Policy Services Nodes to the Node Group* 750  
Using Load Balancers 751  
    General Guidelines 752  
    Failure Scenarios 753  
    Anycast High Availability for ISE PSNs 753  
    IOS Load Balancing 756

Maintaining ISE Deployments	757
Patching ISE	757
Backup and Restore	759
Exam Preparation Tasks	761
Review All Key Topics	761
Define Key Term	761
Q&A	762
<b>Chapter 21 Troubleshooting Tools</b>	<b>764</b>
“Do I Know This Already?” Quiz	764
Foundation Topics	766
Logging	766
Live Log	766
<i>Advanced Filtering</i>	771
<i>Authentication Details Report</i>	771
<i>The Blank Lines</i>	774
Live Sessions	776
Logging and Remote Logging	777
<i>Logging Targets</i>	777
<i>Logging Categories</i>	778
Debug Logs	779
<i>Downloading Debug Logs from the GUI</i>	780
<i>Viewing Log Files from the CLI</i>	781
<i>Support Bundles</i>	782
Diagnostic Tools	785
RADIUS Authentication Troubleshooting Tool	785
Execute Network Device Command	787
Evaluate Configuration Validator	788
Posture Troubleshooting	794
Endpoint Debug	796
TCP Dump	798
Session Trace Tests	801
Troubleshooting Methodology	804
<i>Log De-duplication</i>	805
<i>The USERNAME User</i>	807
Troubleshooting Outside of ISE	808
Endpoint Diagnostics	809
<i>Cisco AnyConnect Diagnostics and Reporting Tool (DART)</i>	809

- Supplicant Provisioning Logs* 812
- Network Device Troubleshooting 812
- Show Authentication Session Interface* 812
- Viewing Client Details on the WLC* 813
- Debug Commands* 815

Exam Preparation Tasks 815

Review All Key Topics 815

Q&A 816

## **Part VI Extending Secure Access Control**

### **Chapter 22 ISE Context Sharing and Remediation 818**

“Do I Know This Already?” Quiz 818

Foundation Topics 820

Integration Types in the ISE Ecosystem 820

- MDM Integration 820

- Rapid Threat Containment 821

- Platform Exchange Grid 824

pxGrid 825

- pxGrid in Action 826

- Context-In 827

- Configuring ISE for pxGrid 828

- Configuring pxGrid Participants 831

- Configuring Firepower Management Center for Identity with pxGrid* 831

- Configuring the Web Security Appliance* 850

- Integrating Stealthwatch and ISE* 857

Exam Preparation Tasks 867

Review All Key Topics 867

Define Key Terms 867

Q&A 867

### **Chapter 23 Threat Centric NAC 868**

“Do I Know This Already?” Quiz 868

Foundation Topics 871

Vulnerabilities and Threats, Oh My! 871

Integrating Vulnerability Assessment Sources 872

- TC-NAC Flows 873

- Enable TC-NAC 874

	Configure the Integration with a Vulnerability Assessment Vendor	878
	Authorization Profile and Authorization Rules	884
	Seeing TC-NAC with Vulnerability Scanners in Action	887
	Verifying What Happened	888
	Integrating with Threat Sources	890
	Cognitive Threat Analytics (CTA)	890
	<i>Create a CTA STIX/TAXII API Account</i>	892
	<i>Create a CTA Integration for TC-NAC</i>	894
	<i>Using CTA with Authorization</i>	896
	AMP for Endpoints	897
	<i>Normalized Events</i>	899
	<i>Configuring the AMP Adapter</i>	900
	Exam Preparation Tasks	904
	Review All Key Topics	904
	Define Key Terms	905
	Q&A	905
<b>Part VII</b>	<b>Device Administration AAA</b>	
<b>Chapter 24</b>	<b>Device Administration AAA with ISE</b>	<b>906</b>
	“Do I Know This Already?” Quiz	906
	Foundation Topics	909
	Device Administration AAA Refresher	909
	Device Administration in ISE	910
	Device Administration Design	911
	<i>Large Deployments</i>	912
	<i>Medium Deployments</i>	913
	<i>Small Deployments</i>	913
	Enabling TACACS+ in ISE	914
	Network Devices	916
	Device Administration Global Settings	917
	Connection Settings	918
	Password Change Control	918
	Session Key Assignment	918
	Device Administration Work Center	919
	Identities	920
	Network Resources	921
	Policy Elements	922

*TACACS Command Sets* 922

*TACACS Profiles* 923

Policy Sets 925

Reports 927

Exam Preparation Tasks 928

Review All Key Topics 928

Q&A 928

## **Chapter 25 Configuring Device Administration AAA with Cisco IOS 930**

“Do I Know This Already?” Quiz 930

Foundation Topics 932

Overview of IOS Device Administration AAA 932

*TACACS Profile* 932

*TACACS+ Command Sets* 934

Configure ISE and an IOS Device for Device Administration AAA 936

*Prepare ISE for IOS Device Administration AAA* 937

*Ensure That the Device Administration Service Is Enabled* 937

*Prepare the Network Device* 937

Prepare the Policy 939

*Configure the TACACS Profiles* 939

*Configure the TACACS Command Sets* 941

*Configure the Policy Set* 943

IOS Configuration for TACACS+ 946

*Configure TACACS+ Authentication and Fallback* 946

*Configure TACACS+ Command Authorization* 948

*Configure TACACS+ Command Accountings* 951

Testing and Troubleshooting 951

Testing and Troubleshooting in ISE 952

Troubleshooting at the IOS Command Line 954

Exam Preparation Tasks 966

Review All Key Topics 966

Define Key Terms 967

Q&A 967

## **Chapter 26 Configuring Device Admin AAA with the Cisco WLC 968**

“Do I Know This Already?” Quiz 968

Foundation Topics 971

Overview of WLC Device Administration AAA 971

Configure ISE and the WLC for Device Administration AAA	972
Prepare ISE for WLC Device Administration AAA	972
<i>Prepare the Network Device</i>	972
<i>Prepare the Policy Results</i>	974
<i>Configure the Policy Set</i>	977
Adding ISE to the WLC TACACS+ Servers	979
Testing and Troubleshooting	981
Exam Preparation Tasks	986
Review All Key Topics	986
Q&A	987

## **Part VIII Final Preparation**

### **Chapter 27 Final Preparation 988**

Hands-on Activities	988
Suggested Plan for Final Review and Study	988
Summary	989

## **Part IX Appendixes**

Glossary of Key Terms	991
Appendix A Answers to the “Do I Know This Already?” Quizzes and Q&A Sections	1002
Appendix B CCNP Security Implementing and Configuring Cisco Identity Services Engine (SISE 300-715) Exam Updates	1032
Appendix C Sample Switch Configurations	1034
Index	1062

## **Online Element**

Appendix D Study Planner	
--------------------------	--

## About the Authors

**Aaron Woland, CCIE No. 20113**, is a Principal Engineer in Cisco's Advanced Threat Security & Integrations group and works with Cisco's Largest Customers all over the world. His primary job responsibilities include security design, solution enhancements, standards development, advanced threat solution design, endpoint security, and futures.

Aaron joined Cisco in 2005 and is currently a member of numerous security advisory boards and standards body working groups. Prior to joining Cisco, Aaron spent 12 years as a Consultant and Technical Trainer.

Aaron's other publications include *Integrated Security Technologies and Solutions*, Volume I; both Volumes I and II of the *Cisco ISE for BYOD and Secure Unified Access* book; the *All-in-one Cisco ASA Firepower Services, NGIPS and AMP* book; the *CCNP Security SISAS 300-208 Official Cert Guide*; the *CCNA Security 210-260 Complete Video Course*; and many published white papers and design guides.

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

You can follow Aaron on Twitter: @aaronwoland.

**Katherine McNamara, CCIE No. 50931**, is a Cybersecurity Technical Solutions Architect at Cisco Systems and has worked with large enterprise and public sector customers.

Katherine joined Cisco in 2014 and has worked in IT since 2007 in multiple networking and security roles. She graduated with a Bachelor of Science in IT Security and a Master of Science in Information Security and Assurance. Her many certifications include CCIE Data Center, CCIE Security, MCSE, VCP, CISSP, CCNP, CCDP, and more.

Outside of her day job, she runs a blog called network-node.com, which provides training articles and videos about Cisco Security products. She also helps co-organize the largest Cisco study Meetup group in the world named Router gods.

You can follow Katherine on Twitter: @kmcnam1

## About the Technical Reviewer

**Akhil Behl**, CCIE No. 19564, is a passionate IT executive with a key focus on cloud and security. He has more than 16 years of experience in the IT industry working in several leadership, advisory, consultancy, and business development profiles with various organizations. His technology and business specialization includes cloud, security, infrastructure, data center, and business communication technologies.

Akhil is a published author. Over the span of the past few years, Akhil authored multiple titles on security and business communication technologies. He has contributed as technical editor for over a dozen books on security, networking, and information technology. He has published several research papers in national and international journals, including *IEEE Xplore*, and presented at various IEEE conferences, as well as other prominent ICT, security, and telecom events. Writing and mentoring are his passion and a part of his life.

He holds CCIE (Collaboration and Security), CCSK, CHFI, PMP, ITIL, VCP, TOGAF, CEH, ISM, CCDP, and many other industry certifications. He has Bachelor in Technology and Masters in Business Administration degrees.

## Dedications

**From Aaron and Katherine:** This book was written largely during the rise of the COVID-19 worldwide pandemic. We spent some of this time not knowing if there was going to be a world to live in, much less if there was going to be any readers to learn from this material. So, this book is dedicated to all the people of the world who did not survive the ordeal, to our friends, family, and colleagues who did contract the virus and pulled through, and the many of us who survived the trials and tribulations of the quarantines.

**From Aaron:** This book is dedicated to my amazing best friend, fellow adventurer, and wife, Suzanne. Thank you for your continued support, encouragement, and patience and for putting up with all the long nights I had to be writing while you let the twins have a “sleepover” in our room, and let me sleep in to make up for it and for always believing in me and supporting me. You are beyond amazing.

To Mom and Pop. You have always believed in me and supported me in absolutely everything I’ve ever pursued and showed pride in my accomplishments (no matter how small). I hope I can continue to fill your lives with pride, happiness, “nachas”; and if I succeed in my endeavors to make you proud, it will still only be a fraction of what you deserve.

To my four absolutely incredible daughters, Eden, Nyah, Netanya, and Cassandra: You girls are my inspiration, pride, and joy! I can only hope that one day you will look back at the ridiculous man that raised you and feel a level of pride.

—Aaron

**From Katherine:** This book is dedicated to my wonderful, amazing, and supportive wife, Dianne. This book is as much yours as it is mine. I could not have done it without the support and love you gave me through it all. Thank you for being so amazing every day. I know life with me has been a crazy rollercoaster of adventures but there is truly no one else I’d rather have by my side though all of life’s surprises. The luckiest day of my life was the day I saw you walking toward me in Colorado all those years ago. You’re my foundation, rock, muse, and soulmate. I love you forever. Also, Brock is your cat.

I also want to dedicate this book to my parents—Robert and Evelyne McNamara—and my siblings—Ryan, Jack, Cai, Mimi, Grace, Molly, and Little Bob. I love you all, and I can’t wait until the time we can see each other again in person.

To Raket—It’s been a crazy few years. You have had the monumental job of putting up with me for which I am thankful for all you do. Thank you for grounding me so many times when I needed it and always being a listening ear (or text message). As far as I’m concerned, you are a part of my tribe. Thanks for being my Jiminy Cricket. I wish you all the lavender, crackpie, stressballs, monster salads, hot yoga, travel, love, and happiness in the world.

To Gordon—Who will never see this. You wanted me to be a better person and gave me another chance at life. I hope if you were still here, you would be proud of me.

To my Secret Ninja Pirates—Dustin Schuemann, Tim McConnaughy, Matthew McGee, Joel Sprague, Hieu Phan, Renee Kostreva, Steven McNutt, Anthony Sytnik, Brad Johnson,

Joshua Burget, JP Cedeno, and even David Gaytan—thank you for the many laughs and vent sessions.

I want to thank Bill Boyles Jr., Amanda Boyles, Jessica Rojas, Lily Speerbrecker, Marshall DuVal, Simone Hirsekorn, Jenna Bulis, Chelsea Filer, James Ziegenbalg, and Amanda La Ford. You guys are my real-life superheroes and inspiration to push myself in so many ways.

I want to give thanks to my very awesome SWS team who has made me feel so welcomed in this amazing team/family. Thank you, Isabella Yani, Oli Laurent, Greg Evans, Blake Fletcher, Cristin Beckendorf, Dani Hemmings, Glen Oltmanns, James Nolan, Jeff Hubbell, Jeremy Stephens, Jerod Atkins, Tammy McKeever, Patrick Taylor, Matt Rhebeck, Shane Hanner, Dan Turner, and Thomas Archuleta.

To Miguel de Zubeldia: You're an amazing work partner. Thanks to you I can never look at spicy tacos the same again. Thank you for the all the amazing work, laughs, and accepting me as the other half of this pant-less dynamic duo.

Thank you to everyone in RouterGods and in Cisco who supported me along the way—especially Humphrey Cheung, Dmitry Figol, James Schallau, Nicole Wajer, Lindsay Simancek, Nick Russo, Francois Caen, Alex Shkolnik, Brad Edgeworth, Carolina Terrazas, John Behen, David Peñaloza, Joe Astorino, Kyle Winters, Joey Muniz, Moses Frost, Russell Pope, Jeff Denton, and so many more.

To my amazing professional mentors—my amazing co-author Aaron Woland who honored me so much by choosing me as a co-author. Jeff Fanelli who always gives me amazing advice and encouragement. You make me feel like I can do anything I set my mind to. Thank you for taking a chance with me at Cisco Live and I'll always strive to never let you down. Denise Fishburne who has been an awesome friend in the last few years. You always offer great and wise advice and I am always thankful for your insight. Willow Young—your bravery and wit always inspire me. Jeff Moncrief who should never shave his beard off and who vouched for me to make the transition to a security specialist. You're my favorite furry, and I'm honored to call you friend. Neno Spasov, who got me interested in ISE in the first place, has always been patient with all my questions and literally was in the trenches with me. I love you, big guy.

## Acknowledgments

**From Aaron:** to my co-author, Katherine. Since you joined me at Cisco, you have reinvigorated my passion for ISE and security. I truly treasure our professional and personal relationships and I especially love seeing Dianne's and your fun interactions online. Thank you for agreeing to do the lion's share of the work for this book; it's been a true honor collaborating with you on this book and it is also an honor to call you a colleague and even more so to call you a friend.

To Chris Cleveland, you and I have worked on so many projects together at this point, it is like we know each other on a personal level, even though we've never met in person. You are an amazing editor and Pearson is truly blessed to have you! As soon as we can meet in person, my friend, the drinks are on me!

**From Aaron and Katherine:**

To editors Chris Cleveland, Mandie Frank, and Kitty Wilson: You are amazing. I hope the readers appreciate how much you all have done to make this book what it is today: correcting all the mistakes we made and keeping us aligned with the Cisco Press requirements for style and content. It must have been like herding cats!

To the technical editor, Akhil Behl, you have amazing insights into the security industry, and we look forward to reading your doctoral thesis someday.

To our employer, Cisco: You really are the greatest place to work in the world. Not only are we both passionate for your technology, but also we are patinate about the place we call home. Chuck's leadership in the community and in the company is second to none.

## 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

The Cisco Certified Network Professional (CCNP) certification program has several technology tracks including Enterprise, Security, Data Center, Service Provider, and, last but not least, Collaboration. This book will focus on one of the optional concentration exams to achieve your CCNP Security certification – Implementing and Configuring Cisco Identity Services Engine (SISE 300-715).

You may already have other Cisco certifications in other networking technologies or this may be your first foray into the Cisco certification process. You may instead be reading this book to enrich your skillset for your job and not even take the exam. Whichever the case, you have chosen a great resource to further your learning and we wish you the best of luck in your studies.

## CCNP Security Certification Overview

Security is an ever evolving and growing networking technology—a technology that will likely be needed for generations to come. As the protocols, applications, and user base that communicate over a network change and evolve, so must the security approach that is implemented. Network security requires a holistic approach whereby a single chink in the security armor can equal a significant compromise of intellectual property and may result in costly network downtime.

The CCNP Security certification track provides a solid basis in core Cisco security technologies and optional concentration exams that focus on operating a variety of security technologies and concepts – Email Security Appliance, Next-Generation Firewall/IPS, Web Security, Virtual Private Networks (VPN), Identity Services Engine, and automation for Cisco Security Solutions. As highlighted above, the focus of this book will be on the implementation and configuration of Identity Services Engine (Cisco Certification 300-715 SISE). Table I-1 lists the optional concentration exams one may take in addition to the 300-701 SCOR exam in order to receive the CCNP Security Certification.

**Table I-1** CCNP Security Concentration Exams

Concentration Exam(s)	Recommended Training
300-715 SNCF	Securing Networks with Cisco Firepower Next-Generation Firewall (SSNGFW) Securing Networks with Cisco Firepower Next-Generation IPS (SSFIPS)
300-720 SESA	Securing Email with Cisco Email Security Appliance (SESA)
300-715 SISE	Implementing and Configuring Cisco Identity Services Engine (SISE)
300-725 SWSA	Securing the Web with Cisco Web Security Appliance (SWSA)
300-730 SVPN	Implementing Secure Solutions with Virtual Private Networks (SVPN)
300-735 SAUTO	Implementing Automation for Cisco Security Solutions (SAUI)

By educating yourself in these areas of the Cisco security solutions portfolio, you will be well equipped to implement a well-rounded security infrastructure onto your network.

## Contents of the CCNP Security SISE Exam

In order to study effectively for an exam, it is important to know what is actually going to be on the exam. Cisco fully understands this need and provides a “blueprint” for each of its certification exams. These blueprints give a high-level overview as to what is going to be covered on the exam. By diving deeper into each of these blueprint topics, you will become better prepared for your certification exam.

To view the blueprints for the complete CCNP exam certification tracks, you can browse to <http://www.cisco.com/go/ccnp>. This webpage contains links to each of the CCNP certification tracks – including the CCNP Security track. The link to go directly to the CCNP Security certification track is <https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/professional/ccnp-security-v2.html>.

To drill down specifically to the SISE exam blueprint, click the link under the “Concentration exams (choose one)” corresponding to the SISE exam. On this page, you will find several links that provide a high-level description of the SISE exam, Exam Topics, Exam Policies, and sample exam questions. As you review the blueprint (under Exam Topics) and other content pertaining to the SISE exam, you may find that some topics overlap with other Cisco certifications – namely, the CCNA. You may choose to enhance your studies by reviewing some of the topics covered in these other exams to refresh your core knowledge.

The topics contained on the CCNP Security SISE exam are provided in Table I-2.

**Table I-2** CCNP Security SISE Exam (300-715) Topics

Certification Guide Chapter	Exam Domain/Topic
	Architecture and Deployment (10% of exam)
8, 18, 20–21, 22–24	Configure Personas
6, 20, 24	Describe Deployment Options
	Policy Enforcement (25% of exam)
8	Configure native AD and LDAP
2, 13	Describe identity store options
11	Configure wired/wireless 802.1x network access
19	Configure 802.1x phasing deployment
11	Configure network access devices
11	Implement MAB
17	Configure Cisco TrustSec

<b>Certification Guide Chapter</b>	<b>Exam Domain/Topic</b>
9–18, 23	Configure policies including authentication and authorization profiles
	Web Auth and Guest Services (15% of exam)
12	Configure web authentication
13	Configure guest access services
13	Configure sponsor and guest portals
	Profiler (15% of exam)
14	Implement profiler services
14	Implement probes
14	Implement CoA
14–16, 18	Configure endpoint identity management
	BYOD (15% of exam)
16	Describe Cisco BYOD functionality
16	Configure BYOD device onboarding using internal CA with Cisco switches and Cisco wireless LAN controllers
15–16	Configure certificates for BYOD
16	Configure blacklist/whitelist
	Endpoint Compliance (10% of exam)
18	Describe endpoint compliance, posture services, and client provisioning
18	Configure posture conditions and policy and client provisioning
18	Configure the compliance module
18	Configure Cisco ISE posture agents and operational modes
1	Describe supplicant, supplicant options, authenticator, and server
	Network Access Device Management (10% of exam)
1, 24	Compare AAA protocols
24–26	Configure TACACS+ device administration and command authorization

Besides the training resources provided on the SISE exam page, you might also find additional study resources at the links provided in Table I-3. Other unofficial texts, video, and online training resources can also be found via your favorite online search engine.

**Table 1-3** Additional Training Resources

Resource	URL
The Cisco Learning Network SISE page	<a href="https://www.cisco.com/c/en/us/training-events/training-certifications/exams/current-list/sise-300-715.html">https://www.cisco.com/c/en/us/training-events/training-certifications/exams/current-list/sise-300-715.html</a>
Cisco Support Forums	<a href="https://supportforums.cisco.com">https://supportforums.cisco.com</a>
Cisco Press	<a href="http://www.ciscopress.com">http://www.ciscopress.com</a>
Cisco ISE for BYOD and Secure Unified Access	<a href="http://www.ciscopress.com/store/cisco-ise-for-byod-and-secure-unified-access-9781587144738">http://www.ciscopress.com/store/cisco-ise-for-byod-and-secure-unified-access-9781587144738</a>
BYOD Networking LiveLessons	<a href="http://www.ciscopress.com/store/cisco-bring-your-own-device-byod-networking-livelessons-9781587144219">http://www.ciscopress.com/store/cisco-bring-your-own-device-byod-networking-livelessons-9781587144219</a>

## How to Take the SISE Exam

To take the CCNP Security SISE Exam, browse to <https://www.cisco.com/go/ccnp>. Click on the link for the CCNP Security certification and then the link for SISE. You will find information about the exam including the languages in which the exam will be offered, duration of the exam, as well as a link to register for the exam. At the time of publication of this book, the only approved testing vendor for the SISE exam is Pearson VUE ([www.vue.com](http://www.vue.com)). To register, click on the Pearson VUE link, create an account, and register for the 300-715 SISE exam. You will then be allowed to select a time and testing center that is most convenient to you.

## Who Should Take This Exam and Read This Book?

The SISE 300-715 Exam is just one piece of the CCNP Security certification track. For this reason, the primary audience for this book is those people who are working toward the CCNP Security certification. Furthermore, this book can either be used as the totality of the study material or supplement other study resources (other texts, videos, instructor-led training, online training). Whether you are participating in formalized training for the SISE exam or studying on your own, this text is for you.

Those who take the CCNP Security certification or other CCNP exams are often those individuals who require this level of expertise in their job or their intended career path. Sometimes, the CCNP-level exams are the pinnacle of an individual's intended training—once their CCNP certification is achieved, the recipient chooses to not pursue additional certifications. Other times, the CCNP exams are used as a stepping-stone to higher certifications. In this latter case, the next step in the certification progression is to take the CCIE in the relevant discipline. If the CCNA is the bachelor's degree equivalent of the certification hierarchy and the specialist certifications are a minor in a particular discipline, the CCNP of that discipline is a master's degree. If we were to continue this analogy, the CCIE would be the PhD of the specific technology. See Table I-4 for a comparison chart.

**Table I-4 Security Certification Comparison Chart**

Certification Name	Years of Experience	Job Role	Product/Technology	Number of Exams	Prerequisites
CCNA	1-3	Network Specialist, Network Support Engineer	Network fundamentals, Network access, IP connectivity, IP services, Security fundamentals, Automation and programmability	1	None
CCNP Security	3-5	Network Security Engineer	Network security, Cloud security, Endpoint protection and detection, Security network access, Visibility and enforcement, Next-Generation Firewall/IPS (Optional), Identity Services Engine (Optional), Email Security Appliance (Optional), Web Security Appliance (Optional), VPN (Optional), C	2	None
CCIE Security	7+	Network Security Engineer	Cisco Adaptive Security Appliance (ASA) Firewall, Firepower Threat Defense (FTD), Firepower Management Center (FMC), Cisco IOS Security, Virtual Private Networks (VPN), LAN Security, Identity Services Engine (ISE), Web Security Appliance (WSA), Email Security Appliance (ESA), AnyConnect, Advanced Malware Protection (AMP), Umbrella, Cognitive Threat Analytics (CTA), Cisco Threat Response (CTR), Security automation and programmability	2	None

Certification Name	Years of Experience	Job Role	Product/Technology	Number of Exams	Prerequisites
<b>Security Specialists</b>					
Cisco Certified Specialist – Network Security Firewall	1–3	Security Administrators, Security Consultants, Network Administrators	Cisco Firewall Threat Defense and Firewall 7000 and 8000 Series virtual appliances	1	None
Cisco Certified Specialist – Security Identity Management Implementation	1–3	Network Security Engineers, ISE Administrators, Wireless Network Security Engineers	Identity Services Engine (ISE)	1	None
Cisco Certified Specialist – Email Content Security	1–3	Enterprise Messaging Managers, Email System Designers, System Administrators	Email Security Appliance (ESA)	1	None
Cisco Certified Specialist – Web Content Security	1–3	Security Architects, System Designers, Network Administrators, Operations Engineers, Security Technicians	Web Security Appliance (WSA)	1	None
Cisco Certified Specialist – Network Security VPN Implementation	1–3	Network Security Engineers, Network Engineers, Network Administrators	Virtual Private Networks (VPN) including GETVPN, DMVPN, FlexVPN, Site-to-Site VPN, Clientless VPN, Remote Access VPN	1	None
Cisco Certified DevNet Specialist – Security Automation and Programmability	1–3	Security Engineers, DevOps Engineers, Network Engineers	Programming concepts, RESTful APIs, Data Models	1	None

## Format of the CCNP Security SISE Exam

If you have taken other Cisco Certification Exams, this exam format will not be much different. After registering for the SISE exam, you will have a date and location where you will take your exam. It is recommended that you arrive at the testing center 15–20 minutes ahead of your testing schedule. You will then be asked to present two forms of personal identification—a government-issued picture ID and a second that has at least your signature. You will then be asked to put all of your personal effects into a locker or other secure area as you walk into the testing room. As all Cisco Certification Exams are “closed book,” you will not be allowed to take any study materials into the exam room.

The testing room contains a number of testing PCs—often isolated in their own cubicle to encourage privacy and to minimize any interruptions between those who are taking exams. Your testing proctor will escort you into the testing room. You will be provided earplugs and two sheets of writing material (front and back of each sheet is usually available). Oftentimes, these are laminated sheets with a white-erase marker and eraser—allowing you to reuse the sheets as often as you require during your exam. Further details about your testing experience will be provided at the base of the Confirmation Letter as you schedule your exam.

When you start your exam, you will be given the option of taking a sample quiz. This sample quiz will allow you to become familiar with the exam’s format. If you are familiar with using a computer, the sample quiz test engine, and that of the actual exam, will likely be easy to navigate.

The CCNP-level exams follow the same format and construction as the CCNA and include the following question types:

- Multiple-Choice
  - Single-Answer
  - Multiple-Answer
- Drag and Drop
- Fill-in-the-Blank
- Testlet
- Simlet
- Simulated Lab

With the multiple-choice questions, these can take on one of two formats—single-answer and multiple-answer. With the single-answer, multiple-choice questions, you will be given a question with several options for the correct answer. You will be asked to select only one of these options using a round radio button to the left of the chosen answer—pointing your mouse icon at the radio button and left-clicking the mouse. For the multiple-answer, multiple-choice questions, you will still be given a question with several options for the correct answer. However, you will usually be asked to select a prescribed number of correct answers—for instance, “Choose 3.” These will be selected

using a square radio button to the left of the chosen answers. If you attempt to choose too many answers, you will be prompted to choose only the prescribed amount.

Drag and Drop questions will test your ability to match or put into order a number of words/concepts. You will select one option by left-clicking the option and then, while still maintaining the left-click, move the option to another part of the screen. Often, you will be matching an option from one side of the screen to a related option on the other side of the screen. At times, there may be more “answers” on the left than there are slots to fill on the right. In this case, you have to narrow down your choices to those answers that best match the slots on the right.

Although very uncommon, the Cisco certification testing environment does allow for the Fill-in-the-Blank question format. In this type of question, a question is asked and the tester is expected to input the correct answer into the Fill-in-the-Blank box.

A Testlet is a question whereby a scenario is given. The examinee is given multiple choices to choose from to address the given scenario.

The Simlet questions will provide a simulated scenario. With this scenario, you will be asked a number of questions—usually multiple-choice questions. After answering all of the multiple-choice questions, you can submit your collective answer from the Simlet. Be sure that you have answered all of the multiple-choice answers before submitting the Simlet.

The final question format is a Simulated Lab. The exam software has the ability to emulate a number of different Cisco devices interconnected in a simulated network. As part of this Simulated Lab question type, you will be asked to configure the relevant network devices. You will interact with the simulated device in a manner similar to how you would interact with the device in a real-live network. If a graphical user interface (GUI) is the normal method of configuring the test device, you will need to use the GUI to affect the configuration and behavior of the affected device. If you normally use the command-line interface (CLI) to configure a device, the CLI may be the best way to configure the device during your exam. In this Simulated Lab environment, not all commands are going to be available and the standard ‘?’ context-sensitive help available on Cisco Routers and Switches or Tab-completion for commands may not be available. However, all commands that are needed to complete the question adequately should be available.

Again, the format of the CCNP-level tests is very similar to the format of the CCNA. There are examples of the question formats available on Cisco’s Learning Network. The direct link to this Exam Tutorial can be found at [http://www.cisco.com/web/learning/wwtraining/certprog/training/cert\\_exam\\_tutorial.html](http://www.cisco.com/web/learning/wwtraining/certprog/training/cert_exam_tutorial.html).

## **CCNP Security SISE 300-715 Official Certification Guide**

As you review the contents of this book, take every opportunity you can to apply the information to your daily job, your studies, and any supplemental training that you may do. By applying the information within this book whenever possible, it will help to reinforce the material—making it more relevant to your particular application and, hopefully, making it easier to remember when you take the actual certification exam.

In Part I of the book, the focus will be on Identity Management and Secure Access. In this part, we will be discussing how to manage the users as well as how to allow them secure access to the network. The chapters in Part I help present the basis of Authentication, Authorization, and Accounting—AAA. We'll cover the management of users—leveraging the internal user database of Cisco's Identity Services Engine (ISE)—as well as third-party enterprise databases. The verification of the user via one of these databases—internal or external—is called Authentication.

There are a number of methods that can be used to authenticate users when they are joining the network. We'll cover a number of these authentication methods and the underlying protocols during this first part of the book. We'll cover how to authenticate a wired and wireless user using 802.1X, MAC Authentication Bypass, as well as non-standard flows including Local and Centralized Web Authentication.

Once we've authenticated the user, we'll need to dictate the level of access that the user will be given on the network. This process is called authorization. Authorization often-times leverages the authentication step—providing differentiated access to each endpoint based as much on the user who owns the device as the device itself.

We'll round out this part of the book by discussing some advanced concepts—diving more deeply into some of the details of how ISE and the supporting network infrastructure accomplish what needs to be accomplished. By the end of this first section, you should have a pretty good overview of the end-to-end AAA process.

Part II of the book will focus on Cisco's Identity Services Engine (ISE) and its configuration. We'll discuss the specific roles that each persona plays in the ISE architecture and several common deployment scenarios. After this overview of ISE architecture, we'll walk you through the ISE GUI and do some initial configuration of ISE including certificate generation and assignment as well as identity stores—those internal and external databases that provide us the authentication function.

After we have firmly established a complete understanding of AAA concepts and constructs, we'll consider the policy on ISE for both authentication and authorization. We'll walk you step-by-step through how ISE is configured for authentication policies and authorization policies—highlighting all of the building blocks that are required for a typical enterprise deployment.

Depending on the method of access (for example, wired versus wireless), the manner in which we enforce the level of access may change. For instance, the enforcement mechanisms (VLANs, Access Control Lists, Security Group Access, etc.) may be different depending on the method of access. By combining the authentication method (802.1X, MAB, and so on), the method of access (wired versus wireless), endpoint posturing, and profiling, we'll be able to leverage ISE to granularly apply differentiated access to each endpoint individually.

Part III of the book will move most of its focus away from ISE and onto the individual network devices that form the network infrastructure—the switches and wireless LAN controllers. We'll review how to configure the various Switching and Wireless platforms to put our AAA policy into action—leveraging 802.1X, MAB, as well as Local and Centralized Web Authentication.

We'll finish off Part III by reviewing some special use cases—how to configure guest services within ISE as well as how to profile devices as they try to join the network. Configuring guest services can be essential to an enterprise deployment—either by providing basic Internet access to employees or access to vendors and visitors. Profiling is a process whereby ISE can make an intelligent guess as to what type of device is joining the network—making granular authorization decisions based on device type. By the end of Part III, you should have a pretty solid understanding of how to secure your network leveraging ISE as the AAA server and the infrastructure devices to enforce the ISE's policy.

As we get into the Part IV of the book, *Advanced Secure Network Access*, we'll start to apply more of our knowledge in an advanced manner. Up to this point, we were doing basic configuration and basic policy enforcement. In the chapters in Part IV, we'll incorporate certificate-based user authentication—authenticating a user based on an X.509 certificate, either issued by ISE or by a third-party device. The ability to use certificates to validate a user can greatly enhance the level of security in the authentication process.

Bring your own device (BYOD) is also an advanced topic that we'll cover in this part of the book. BYOD is a process and security infrastructure that allows a user to bring her personal smart device onto the corporate network. The BYOD onboarding process allows a user to self-manage his device and registers the device to the corporate network. There are a number of special portals and configurations that are required to allow for an effective BYOD deployment. To ensure that this personal device doesn't adversely affect the network or gain access to unauthorized resources, ISE can provide differentiated access to the endpoint based on a number of key factors.

The next advanced topic that we'll review in Part IV is TrustSec and MACSec. We'll do a quick overview of these two topics and highlight some of benefits as well as the constructs and configurations that affect the Security Group Access configuration and enforcement both on the device and within ISE.

The final topic that we'll address in Part IV is Posture Assessment. Posturing and profiling are sometimes used interchangeably, but that is not accurate. Profiling often leverages information that is readily available via protocols that run over the network—including protocols such as RADIUS, DHCP, HTTP, as well as MAC addresses that are provided within the RADIUS exchange protocol. By replicating or otherwise sending this data to ISE as a client joins the network, profiling is able to make an intelligent decision as to what device is trying to join the network—without ever actively probing the device. Posturing is a little more entrenched at the client/endpoint level. Posturing will leverage information that is contained deep in the configuration of the endpoint—requiring a posturing agent to be run on the endpoint. Once key information is read from the endpoint via this agent, the ISE will make a decision as to whether the device/user is compliant to be allowed access to the network and, if so, what level of access the user should be given.

Part V of this book is geared toward the operational aspects of having ISE. As part of this chapter, we'll discuss how to slowly roll out your ISE deployment to minimize network outages. By leveraging deployment phasing, a network administrator can be in “monitor mode” whereby a device will not be denied access to the network but simply a log is thrown if the user doesn't match an available policy. This allows network administrators

to fully discover and understand the endpoints on their network—without having an adverse effect on the users. Once the network administrators are confident that they have reasonably triaged any unknown endpoints, they can gradually increase the level of policy enforcement.

A second important topic covered in Part V is ISE scale and high availability. This part will highlight how to configure and deploy a distributed ISE architecture in order to accommodate additional load, demand, and possible additional features. Each instance of ISE has an upper limit based on the platform and particular software that it is running on. By providing a distributed deployment architecture, the ISE deployment can grow as a company grows—incorporating a new ISE appliance whenever needed.

As we round out Part V of the CCNP-Security SISE 300-715 Official Certification Guide, we'll provide you with some tips and tricks to troubleshoot ISE. Some of these tools include a configuration validator, Live Logs, as well as a TCP dump. In the right hands, these tools can provide all of the necessary information to isolate any quality or network issues.

In Part VI of the book, we'll dive into turning ISE into the center of a full security ecosystem and extending the access control with other security products using the platform exchange grid (pxGrid) and adding some much needed security operations value to posture by extending network access control with threat and vulnerability data using threat-centric NAC.

Part VII rounds out the exam learning topics of the book with the other half of authentication, authorization, and accounting (AAA) device administration. This is the ability to control access to the network devices like Cisco routers, switches, and wireless controllers.

In the final section, Part VIII, we'll describe the steps that you'll need to take in order to prepare for the CCNP Security SISE.

## Objectives and Methods

This book uses several key methodologies to help you discover the exam topics on which you need more review, to help you fully understand and remember those details, and to help you prove to yourself that you have retained your knowledge of those topics. This book does not try to help you pass the exam only by memorization; it seeks to help you to truly learn and understand the topics. This book is designed to help you pass the Security Identity Management SISE (300-715) exam by using the following methods:

- Helping you discover which exam topics you have not mastered
- Providing explanations and information to fill in your knowledge gaps
- Supplying exercises that enhance your ability to recall and deduce the answers to test questions
- Providing practice exercises on the topics and the testing process via test questions on the companion website

## Book Features

To help you customize your study time using this book, the core chapters have several features that help you make the best use of your time:

- **Foundation Topics:** These are the core sections of each chapter. They explain the concepts for the topics in that chapter.
- **Exam Preparation Tasks:** After the “Foundation Topics” section of each chapter, the “Exam Preparation Tasks” section lists a series of study activities that you should do at the end of the chapter:
- **Review All Key Topics:** The Key Topic icon appears next to the most important items in the “Foundation Topics” section of the chapter. The Review All Key Topics activity lists the key topics from the chapter, along with their page numbers. Although the contents of the entire chapter could be on the exam, you should definitely know the information listed in each key topic, so you should review these.
- **Define Key Terms:** Although the PenTest+ exam may be unlikely to ask a question such as “Define this term,” the exam does require that you learn and know a lot of pentest-related terminology. This section lists the most important terms from the chapter, asking you to write a short definition and compare your answer to the glossary at the end of the book.
- **Review Questions:** Confirm that you understand the content that you just covered by answering these questions and reading the answer explanations.
- **Web-based practice exam:** The companion website includes the Pearson Cert Practice Test engine that allows you to take practice exam questions. Use it to prepare with a sample exam and to pinpoint topics where you need more study.

## The Companion Website for Online Content Review

All the electronic review elements, as well as other electronic components of the book, exist on this book’s companion website.

To access the companion website, which gives you access to the electronic content with this book, start by establishing a login at [www.ciscopress.com](http://www.ciscopress.com) and register your book.

To do so, simply go to [www.ciscopress.com/register](http://www.ciscopress.com/register) and enter the ISBN of the print book: 9780136642947. After you have registered your book, go to your account page and click the **Registered Products** tab. From there, click the **Access Bonus Content** link to get access to the book’s companion website.

Note that if you buy the *Premium Edition eBook and Practice Test* version of this book from Cisco Press, your book will automatically be registered on your account page. Simply go to your account page, click the **Registered Products** tab, and select **Access Bonus Content** to access the book’s companion website.

Please note that many of our companion content files can be very large, especially image and video files.

If you are unable to locate the files for this title by following the steps at left, please visit [www.pearsonITcertification.com/contact](http://www.pearsonITcertification.com/contact) and select the **Site Problems/ Comments** option. Our customer service representatives will assist you.

## How to Access the Pearson Test Prep (PTP) App

You have two options for installing and using the Pearson Test Prep application: a web app and a desktop app. To use the Pearson Test Prep application, start by finding the registration code that comes with the book. You can find the code in these ways:

- **Print book:** Look in the cardboard sleeve in the back of the book for a piece of paper with your book's unique PTP code.
- **Premium Edition:** If you purchase the Premium Edition eBook and Practice Test directly from the Cisco Press website, the code will be populated on your account page after purchase. Just log in at [www.ciscopress.com](http://www.ciscopress.com), click **account** to see details of your account, and click the **digital purchases** tab.
- **Amazon Kindle:** For those who purchase a Kindle edition from Amazon, the access code will be supplied directly from Amazon.
- **Other Bookseller E-books:** Note that if you purchase an e-book version from any other source, the practice test is not included because other vendors to date have not chosen to vend the required unique access code.

**NOTE** Do not lose the activation code because it is the only means with which you can access the QA content with the book.

Once you have the access code, to find instructions about both the PTP web app and the desktop app, follow these steps:

- Step 1.** Open this book's companion website, as was shown earlier in this Introduction under the heading "How to Access the Companion Website."
- Step 2.** Click the **Practice Exams** button.
- Step 3.** Follow the instructions listed there both for installing the desktop app and for using the web app.

Note that if you want to use the web app only at this point, just navigate to [www.pearsontestprep.com](http://www.pearsontestprep.com), establish a free login if you do not already have one, and register this book's practice tests using the registration code you just found. The process should take only a couple of minutes.

**NOTE** Amazon eBook (Kindle) customers: It is easy to miss Amazon's email that lists your PTP access code. Soon after you purchase the Kindle eBook, Amazon should send an email. However, the email uses very generic text and makes no specific mention of PTP or practice exams. To find your code, read every email from Amazon after you purchase the book. Also do the usual checks for ensuring your email arrives like checking your spam folder.

**NOTE** Other eBook customers: As of the time of publication, only the publisher and Amazon supply PTP access codes when you purchase their eBook editions of this book.

## Customizing Your Exams

Once you are in the exam settings screen, you can choose to take exams in one of three modes:

- **Study mode:** Allows you to fully customize your exams and review answers as you are taking the exam. This is typically the mode you would use first to assess your knowledge and identify information gaps.
- **Practice Exam mode:** Locks certain customization options, as it is presenting a realistic exam experience. Use this mode when you are preparing to test your exam readiness.
- **Flash Card mode:** Strips out the answers and presents you with only the question stem. This mode is great for late-stage preparation when you really want to challenge yourself to provide answers without the benefit of seeing multiple-choice options. This mode does not provide the detailed score reports that the other two modes do, so you should not use it if you are trying to identify knowledge gaps.

In addition to these three modes, you will be able to select the source of your questions. You can choose to take exams that cover all of the chapters or you can narrow your selection to just a single chapter or the chapters that make up specific parts in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, simply deselect all the chapters and then select only those on which you wish to focus in the Objectives area.

You can also select the exam banks on which to focus. Each exam bank comes complete with a full exam of questions that cover topics in every chapter. The two exams printed in the book are available to you as well as two additional exams of unique questions. You can have the test engine serve up exams from all four banks or just from one individual bank by selecting the desired banks in the exam bank area.

There are several other customizations you can make to your exam from the exam settings screen, such as the time of the exam, the number of questions served up, whether to randomize questions and answers, whether to show the number of correct answers for multiple-answer questions, and whether to serve up only specific types of questions. You can also create custom test banks by selecting only questions that you have marked or questions on which you have added notes.

## Updating Your Exams

If you are using the online version of the Pearson Test Prep software, you should always have access to the latest version of the software as well as the exam data. If you are using the Windows desktop version, every time you launch the software while connected to the Internet, it checks if there are any updates to your exam data and automatically downloads any changes that were made since the last time you used the software.

Sometimes, due to many factors, the exam data may not fully download when you activate your exam. If you find that figures or exhibits are missing, you may need to manually update your exams. To update a particular exam you have already activated and downloaded, simply click the **Tools** tab and click the **Update Products** button. Again, this is only an issue with the desktop Windows application.

If you wish to check for updates to the Pearson Test Prep exam engine software, Windows desktop version, simply click the **Tools** tab and click the **Update Application** button. This ensures that you are running the latest version of the software engine.

*This page intentionally left blank*



## CHAPTER 12

# Web Authentication

### This chapter covers the following topics:

- Web Authentication scenarios
- Configuring Centralized Web Authentication
- Building CWA authorization rules
- Verifying Centralized Web Authentication

As discussed in Chapter 4, “Non-802.1X Authentications,” just because there is no configured supplicant on an endpoint does not mean the user of that endpoint does not need to authenticate. Consider the use cases of guests or visitors, or maybe just a misconfiguration or an expired credential for an end user. The user may still require access to the network.

Enter *Web Authentication*, commonly referred to as just *WebAuth*. With WebAuth, an authenticator can send a user to a locally hosted web page—that is, a web page hosted on the local device itself (the switch, wireless controller, or even the firewall or VPN concentrator) where a user can submit a username and password.

As mentioned in Chapter 4, there are multiple types of WebAuth, and Centralized WebAuth (CWA) is the type used with Cisco Secure Access and ISE. CWA is the focus of the Implementing and Configuring Cisco Identity Services Engine SISE 300-715 exam and, therefore, the main focus of this book.

**NOTE** This chapter was written based on the assumption that the switches and WLCs have been configured as described in Chapter 11, “Implement Wired and Wireless Authentication.” If you have not already configured your network devices for authentication, none of the configuration in this chapter will work, and you should revisit Chapter 11.

## “Do I Know This Already?” Quiz

The “Do I Know This Already?” quiz allows you to assess whether you should read this entire chapter thoroughly or jump to the “Exam Preparation Tasks” section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 12-1 lists the major headings in this chapter and their corresponding “Do I Know This Already?” quiz questions. You can find the answers in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes and Q&A Sections.”

**Table 12-1** “Do I Know This Already?” Section-to-Question Mapping

Foundation Topics Section	Questions
Web Authentication Scenarios	5
Configuring Centralized Web Authentication	1, 3–6
Building CWA Authorization Policies	3
Verifying Centralized Web Authentication	2, 7–10

**CAUTION** The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Before a Cisco switch can generate a self-signed certificate, what configuration is required?
  - a. The internal CA must be enabled.
  - b. An IPv6 address must be configured.
  - c. A Cisco switch cannot generate a self-signed certificate.
  - d. A domain name must be configured.
2. Which statement about URL-Redirect ACLs is true?
  - a. A URL redirection ACL can be downloaded from ISE to a NAD.
  - b. A URL redirection must be preconfigured locally on the NAD, and ISE applies it through the use of RADIUS attribute/value pairs (AV pairs).
  - c. There is no ACL needed for URL redirection.
  - d. A URL redirection ACL and its ACEs must be configured both in ISE and on the NAD.
3. Which of the following settings is required for a WLAN to support CWA on the Cisco WLC?
  - a. SNMP NAC
  - b. Layer 3 authentication
  - c. ISE NAC
  - d. Fast transition
4. For wired and wireless MAB, which option must be configured for unknown identities?
  - a. Drop
  - b. Continue
  - c. Reject
  - d. Pass

5. Which of the following rule types need to be created for CWA? (Choose two.)
  - a. A WebAuth authentication rule must be created for the authentication through the web portal.
  - b. An authorization rule must be created to redirect the user to the CWA portal.
  - c. An authentication rule must be created to permit access to users who have successfully authorized through the CWA portal.
  - d. An authorization rule must be created to permit access to users who have successfully authenticated through the CWA portal.
  - e. A WebAuth authentication rule must be created to redirect the end user to the CWA portal.
6. Which statement is true regarding network segmentation and Web Authentication?
  - a. Network segmentation should never be used with Web Authentication; they are mutually exclusive technologies.
  - b. VLAN changes may be used, and TrustSec SGTs may be used, but VLAN changes and SGTs can never be used together.
  - c. Only TrustSec SGTs can be used with Web Authentication to provide segmentation.
  - d. VLAN changes should only be used with devices that can recognize a change and request a new DHCP address.
7. Which of the following statements about CWA is true?
  - a. CWA is configured exactly the same for both wired and wireless NADs.
  - b. CWA must leverage different policy sets when configured for wired and wireless.
  - c. With CWA, the switch isn't aware of the Web Authentication and only identifies the session as using MAB.
  - d. CWA stands for Cisco Wide-area Authorization.
8. Which command on a NAD displays information about a URL-redirectioned session, including the MAC address, IP address, dACL, URL-Redirect ACL, and the URL the end user is being redirected to?
  - a. `show epm redirection`
  - b. `show authentication sessions`
  - c. `show epm authentication | include redirection`
  - d. `show authentication session interface [interface-name]`
9. Which of the following locations in the ISE GUI is the best one to examine to validate that CWA is working?
  - a. Policy > Policy Elements > Results > Authorization
  - b. Operations > RADIUS > Live Log
  - c. Policy > Policy Elements > Results > Authentication
  - d. Operations > Results

10. Which of the following statements most accurately describes the use of Change of Authorization (CoA) in relation to CWA?
- The CoA-Reauth causes the NAD to reauthenticate the endpoint within the same session, and ISE is then able to tie together the MAB and CWA authentications.
  - The CoA sends a Packet of Disconnect (PoD) to the NAD, which starts a new session based on the web credentials.
  - The CoA-Reauth causes the NAD to reauthenticate the endpoint, which starts a new session based on the web credentials.
  - The CoA sends a PoD to the NAD, and ISE is able to tie the original MAB session to the new Web Authentication session by correlating the MAC addresses from both authentication sessions.

## Foundation Topics

### Web Authentication Scenarios

There are a number of reasons that a company may choose to implement a WebAuth strategy. One of the most common reasons is to provide Internet access to visitors (also known as guests), as detailed in Chapter 13, “Guest Services.” In addition, as newer versions of ISE come out, many companies are looking to add interactive logins to capture usernames and passwords as additional credentials to certificate-based authentication (think two-factor authentication).

The end user is presented with a web portal to input a username and password. The credentials are then sent from the authenticator to ISE in a standard RADIUS Access-Request packet. So, in a very similar fashion to what occurs with MAC Authentication Bypass (MAB), the switch sends the request for the endpoint, and the endpoint itself does not participate in authentication. Figure 12-1 illustrates the WebAuth concept.

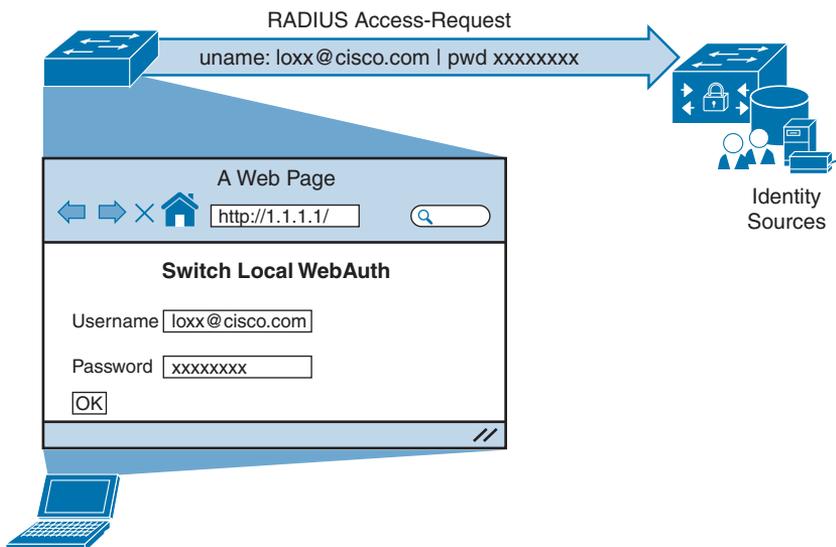


Figure 12-1 Web Authentication

The credential that gets submitted through the WebAuth page could be the Active Directory credentials of an employee. The credentials could be guest credentials for someone who is only temporarily allowed to have Internet access (and no other access). The use of WebAuth is really not limited to any specific type of user account.

Keep in mind that WebAuth is only an effective authentication method for a device that has an interactive user. In other words, it would not make sense to try to use WebAuth for a printer as there would be no user to interact with the web portal, enter credentials, and click Submit.

Like MAB, WebAuth is not a standard. There are multiple ways to perform WebAuth, with benefits and downsides to each one.

**NOTE** It is important not to confuse the term *WebAuth* with the term *WebAuthN*. WebAuthN refers to a new Internet standard for Web Authentication and the use of Web Authentication pages in combination with authentication protocols such as FIDO2 with tokens like YubiKeys, Windows Hello, and Apple's Touch ID. These topics are beyond the scope of the SISE 300-715 exam and, therefore, this book.

## Local Web Authentication (LWA)

*Local Web Authentication (LWA)* is the original WebAuth. With LWA, the authenticator redirects web browser traffic to a locally hosted web portal where a user can enter a username and password.

### Key Topic

The credentials are submitted through the switch or wireless controller, which sends the RADIUS Access-Request to the authentication server, using the username and password from the web portal's form. It is key to remember that any time the switch is sending the credentials for the user, it is considered Local Web Authentication.

On a Cisco Catalyst switch, the locally hosted web pages are not very customizable. Many companies require that web portals be customized to match the corporate branding. For those companies, traditional LWA is not usually an acceptable solution—at least not for WebAuth with wired connections.

In addition, when using LWA with Cisco switches, there is no native support for advanced services such as the following:

- Acceptable use policy acceptance pages
- Client provisioning
- Password-changing capabilities
- Self-registration

- Device registration
- BYOD onboarding

For advanced capabilities like these, a company truly needs to consider using Centralized Web Authentication.

**NOTE** For more details on LWA, see Chapter 4.

## Centralized Web Authentication (CWA)

Cisco ISE uses *Centralized Web Authentication (CWA)* almost exclusively. While Cisco ISE is capable of supporting LWA methods, those methods are typically reserved for non-Cisco network devices.

Like other forms of Web Auth, CWA is only for interactive users with web browsers, who need to manually enter usernames and passwords.

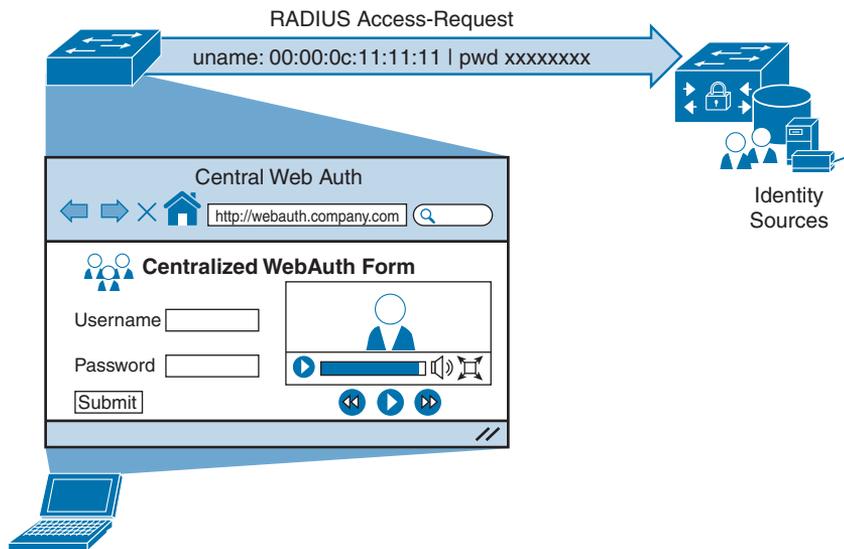
Change of Authorization (CoA) works fully with CWA, which contributes to support for all the authorization results, such as ACL and VLAN authorization. Keep in mind that any time you change VLANs on an endpoint, the endpoint must be able to detect the VLAN change and trigger an IP address renewal. With 802.1X, the supplicant takes care of the VLAN change detection and address renewal. However, when using WebAuth, a supplicant does not typically exist on the endpoint. Therefore, the DHCP scope length must be set to renew the address quickly, or the portal must use an ActiveX or Java applet to handle the renewal of the IP address after the VLAN assignment, which is not a popular option due to the security concerns related to using Java or ActiveX applets.

CWA also supports advanced services such as the following:

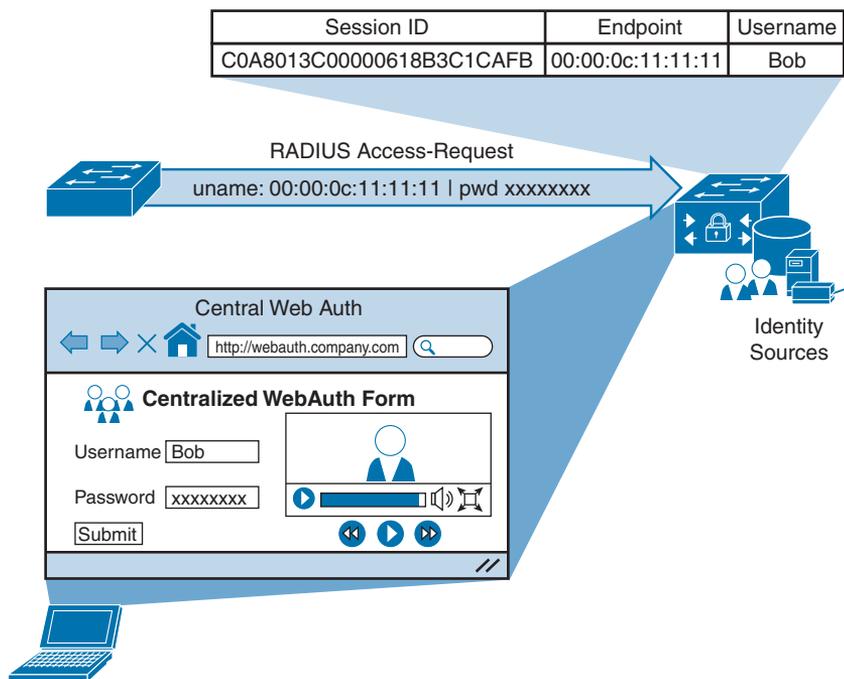
- Client provisioning
- Posture assessments
- Acceptable use policies (AUPs)
- Password changing
- Self-registration
- Device registration
- BYOD onboarding



As described in Chapter 4, a switch or wireless controller only sees MAB, and the rest is handled on the authentication server (ISE). Figure 12-2 shows the MAB occurring with a redirection to the centralized portal, and Figure 12-3 shows how the switch still sees only a MAB request, with ISE maintaining the user authentication.



**Figure 12-2** *URL-Redirected MAC Authentication Bypass*



**Figure 12-3** *Credentials Never Sent to the Authenticator*

The following steps detail what occurs in Figures 12-2 and 12-3:

- Step 1.** The endpoint entering the network does not have a supplicant.
- Step 2.** The authenticator performs MAB, sending the RADIUS Access-Request to Cisco ISE (the authentication server).

- Step 3.** The authentication server (ISE) sends the RADIUS result, including a URL redirection, to the centralized portal on the ISE server.
- Step 4.** The end user enters credentials into the centralized portal. Unlike the LWA options, the credentials are never sent to the switch; instead, they are stored within the ISE session directory and tied together with the MAB coming from the switch.
- Step 5.** ISE sends a reauthentication Change of Authorization (CoA-reauth) to the switch. This causes the switch to send a new MAB request with the same SessionID to ISE, and it is processed.
- Step 6.** ISE sends the final authorization result to the switch for the end user.

CWA and the URL-redirection capability in the switches and wireless devices are the basis for many of the other solutions in ISE, including Device Registration WebAuth, BYOD onboarding, MDM onboarding, and posture assessment.

## Configuring Centralized Web Authentication

Multiple devices need to be configured to enable CWA. The network access device (NAD) requires some special configuration, such as a redirection ACL; in addition, ISE needs authentication and authorization rules set up for CWA. The following sections look at these configurations.

### Cisco Switch Configuration

With secure network access using ISE, the switch performs the URL redirection for Web Authentication and also redirects the discovery traffic from the posture agent to the ISE policy service node.

Performing URL redirection at the Layer 2 access (edge) device is a vast improvement over previous NAC solutions, which requires an appliance (such as the inline device) to capture web traffic and perform redirection to a Web Authentication page. URL redirection at the Layer 2 access device simplifies Web Authentication deployment, device onboarding, and the posture agent discovery process.

### Configure Certificates on the Switch

In order to redirect HTTPS traffic, there is a prerequisite for the switch to have its own certificate. To configure a certificate, perform the following tasks in global configuration mode on a switch:

**NOTE** Cisco IOS does not allow for certificates or even self-generated keys to be created and installed until a DNS domain name is defined on the device.

- Step 1.** To set the DNS domain name on the switch, type `ip domain-name domain-name` at the global configuration prompt. Now that the domain name is configured, and the keys can be generated.
- Step 2.** To generate keys to be used for HTTPS, type `crypto key generate rsa general-keys mod 2048` at the global configuration prompt.

## Enable the Switch HTTP/HTTPS Server

The embedded HTTP/HTTPS server in IOS is used to grab HTTP traffic from the user and redirect that user's browser to the Centralized Web Authentication portal or to a device registration portal or even to the mobile device management onboarding portal. This same function is used for redirecting the posture agent's traffic to the Policy Services node. Follow these steps to enable the switch HTTP/HTTPS server:

- Step 1.** Enable the HTTP server by entering the following command in global configuration mode:

```
C3850(config)# ip http server
```

- Step 2.** Enable the HTTP secure server by entering the following command:

```
C3850(config)# ip http secure-server
```

### Key Topic

Many organizations need to ensure that this redirection process, which is using the switch's internal HTTP server, is decoupled from the management of the switch itself. To disconnect the HTTP management process from the URL-redirection process, run the following two commands in global configuration mode:

```
C3850(config)# ip http active-session-modules none
```

```
C3850(config)# ip http secure-active-session-modules none
```

## Verify the URL-Redirect ACL

In Chapter 11, you created an access list named ACL-WEBAUTH-REDIRECT, which is used to determine what traffic is redirected to the CWA portal with the **permit** statement. Any traffic that is denied is not redirected.

### Key Topic

Contrary to the way a wireless LAN controller works, the URL-Redirect ACL on a switch is used only to determine what traffic is redirected and what traffic is not redirected. If network traffic is denied from redirection, it is not necessarily denied the ability to traverse the network. The traffic-filtering capability comes from the downloadable ACL (dACL) that is sent to the switch from ISE as part of the authorization result.

The use of dual ACLs is limited to IOS-based wired and wireless devices. (The Aireospace wireless controllers behave differently and are covered later in this chapter.) Follow these steps to verify the URL-Redirect ACL:

- Step 1.** Validate whether the ACL-WEBAUTH-REDIRECT ACL is configured on the NAD by entering the following command:

```
C3850# show ip access-list ACL-WEBAUTH-REDIRECT
```

```
Extended IP access list ACL-WEBAUTH-REDIRECT
```

```
10 deny udp any any eq domain
```

```
20 permit tcp any any eq www
```

```
30 permit tcp any any eq 443
```

If the ACL is not there or needs to be modified, continue to step 2.

**Step 2.** Add the following ACL to be used for URL redirection with Web Authentication:

```
C3850(config)# ip access-list ext ACL-WEBAUTH-REDIRECT
C3850(config-ext-nacl)# remark explicitly deny DNS from
being redirected to address a bug
C3850(config-ext-nacl)# deny udp any any eq 53
C3850(config-ext-nacl)# remark redirect all applicable
traffic to the ISE Server
C3850(config-ext-nacl)# permit tcp any any eq 80
C3850(config-ext-nacl)# permit tcp any any eq 443
C3850(config-ext-nacl)# remark all other traffic will be
implicitly denied from the redirection
```

## Cisco WLC Configuration

Cisco switches are responsible for redirecting web browser traffic to the centralized portal(s), and Cisco WLCs must do the same thing.

**NOTE** As stated in the introduction to this chapter, you are expected to have already configured the WLC according to the directions in Chapter 11. In Chapter 11, you should have created an “open” WLAN with MAC filtering enabled and the NAC state configured for ISE NAC. In addition, you created an access list named ACL-WEBAUTH-REDIRECT.

## Validate That MAC Filtering Is Enabled on the WLAN

The MAC Filtering option for an open wireless network configures a WLAN for wireless MAB. This is necessary to ensure that an authentication is sent from the WLC to ISE, so ISE can return the URL redirection in the authorization result.

From the WLC’s GUI, navigate to the WLANs tab, examine the list of WLANs, and ensure that MAC Filtering is listed in the Security Policies column, as shown for the CiscoPress-Guest SSID in Figure 12-4.

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
2	WLAN	CiscoPress	CiscoPress	Enabled	[WPA2][Auth(802.1X)]
5	WLAN	CiscoPress-Guest	CiscoPress-Guest	Disabled	MAC Filtering

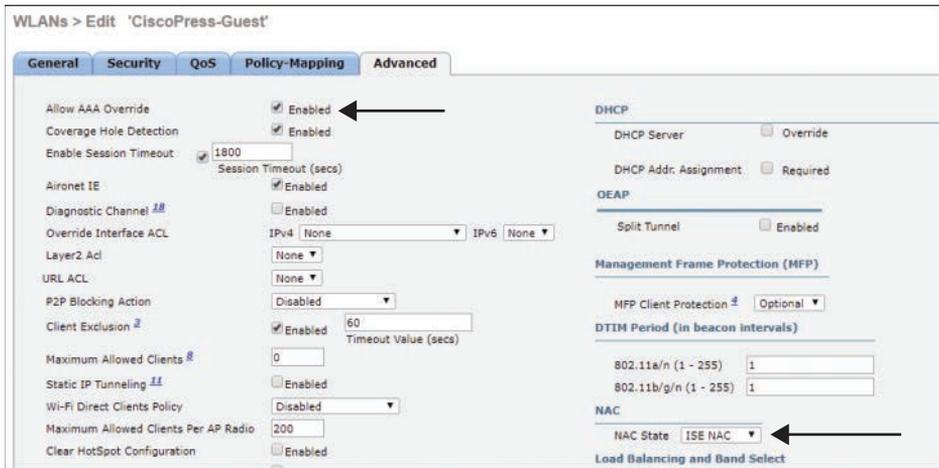
**Figure 12-4** MAC Filtering on an Open SSID

## Validate That ISE NAC Is Enabled on the WLAN

The ISE NAC feature is a very important setting. It is critical to allow for URL redirection, Centralized Web Authentication, posture assessment, native supplicant provisioning, and more.

From the WLC GUI, follow these steps:

- Step 1.** Navigate to **WLANs >** and select your open SSID.
- Step 2.** Click on the **Advanced** tab.
- Step 3.** Ensure that NAC State is forest to **ISE NAC**, as shown in Figure 12-5. In the same screen, ensure that Allow AAA Override is set to **Enabled**.



**Figure 12-5** ISE NAC Setting

### Validate That the URL-Redirection ACL Is Configured

The last critical item you need to ensure exists in the WLC configuration is an ACL to use for URL redirections. In Chapter 11, you created an ACL named ACL-WEBAUTH-REDIRECT, which is used to determine what traffic is redirected to the CWA portal with the **deny** statement. Any traffic that is permitted is not redirected.

#### Key Topic

Unlike IOS-based NADs, AireospaceOS-based wireless controllers use a single ACL to determine which traffic to redirect and which traffic to permit through. In other words, both redirection and traffic filtering are handled by a single ACL. Therefore, the logistics of which traffic is redirected are not the same as with IOS-based devices. With Cisco WLCs, a **deny** statement means that traffic should be redirected. A **permit** statement allows the traffic through the WLC and bypasses the redirection.

In the WLC GUI, follow these steps:

- Step 1.** Navigate to **Security > Access-Control-Lists > Access-Control Lists**. Ensure that the ACL-WEBAUTH-REDIRECT ACL is in the list, as shown in Figure 12-6.
- Step 2.** Click this access list and ensure that the entries for your environment are there, as shown in Figure 12-7.

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT

### Access Control Lists

Enable Counters

Name	Type
<a href="#">ACL-WEBAUTH-REDIRECT</a>	IPv4
<a href="#">HR-ACL</a>	IPv4
<a href="#">NSP-ACL</a>	IPv4
<a href="#">ACL-AGENT-REDIRECT</a>	IPv4
<a href="#">ACL-GUEST-ACCESS</a>	IPv4
<a href="#">BLACKHOLE</a>	IPv4
<a href="#">Android-Marketplace</a>	IPv4
<a href="#">Internet-Only</a>	IPv4
<a href="#">Restricted</a>	IPv4
<a href="#">ACL-MDM-REDIRECT</a>	IPv4
<a href="#">Employee_Limited</a>	IPv4
<a href="#">AD-KeyServicesOnly-ACL</a>	IPv4
<a href="#">ACL_WEBAUTH_REDIRECT</a>	IPv4
<a href="#">Test-ACL</a>	IPv4
<a href="#">TestRBAC</a>	IPv4
<a href="#">SECURITYDEMO-CPU-ACL</a>	IPv4

**Foot Notes**  
1. Counter configuration is global for acl, urlacl and layer2acl.

Figure 12-6 Access Control Lists

### Access Control Lists > Edit

**General**

Access List Name: ACL-WEBAUTH-REDIRECT

Deny Counters: 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	0.0.0.0 0.0.0.0	/ 0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound
2	Permit	0.0.0.0 0.0.0.0	/ 0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any
3	Permit	0.0.0.0 0.0.0.0	/ 0.0.0.0 / 0.0.0.0	TCP	Any	HTTPS	Any	Any
4	Permit	0.0.0.0 0.0.0.0	/ 0.0.0.0 / 0.0.0.0	UDP	DHCP Client	DHCP Server	Any	Inbound
5	Permit	0.0.0.0 0.0.0.0	/ 10.1.100.0 255.255.255.0	Any	Any	Any	Any	Inbound
6	Permit	0.0.0.0 0.0.0.0	/ 10.1.103.0 255.255.255.0	Any	Any	Any	Any	Inbound
7	Deny	0.0.0.0 0.0.0.0	/ 0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Inbound

Figure 12-7 ACL-WEBAUTH-REDIRECT Contents

## Configure ISE for Centralized Web Authentication

When you're sure the key elements of the network devices are configured correctly, it's time to ensure that ISE is configured correctly, too. A key change must be made in the authentication policy: An identity source sequence that uses all the appropriate identity stores and the appropriate traffic-filtering dACLs need to be configured. In addition, you need to create the appropriate authorization rules for both before and after Web Authentication.

**NOTE** Beginning with ISE Version 2.0, ISE contains “smart default” policies. These are preconfigured policies that help customers deploy things like CWA, BYOD, and posture. Due to a communication error between the software developers and Aaron Woland (the man who drove the idea behind smart defaults), those smart defaults include using an ACL named `ACL_WEBAUTH_REDIRECT`. Notice the underscore instead of the dash. This section does not use the prebuilt rules but shows how to create new rules.

The sections that follow describe the key steps in configuring ISE for Centralized Web Authentication:

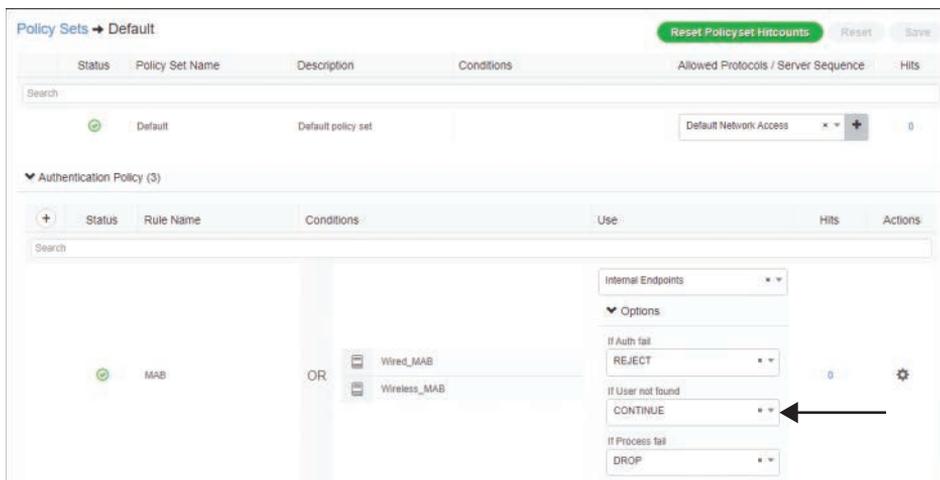
- Step 1.** Configure MAB Continue for the Authentication.
- Step 2.** Verify the Web Authentication identity source sequence.
- Step 3.** Configure a dACL for pre-WebAuth authorization.
- Step 4.** Configure an authorization profile.

### Configure MAB Continue for the Authentication

WebAuth is often used for guest access, which means an endpoint is likely to be unknown to ISE when a guest attaches to the network. It is therefore critical to set the identity options to continue when the MAC address is unknown. This has been the default for MAB since ISE Version 2.0, but we examine it anyway to better understand the situation.

In the ISE GUI, follow these steps (see Figure 12-8):

- Step 1.** Navigate to **Work Centers > Network Access > Policy Sets**.
- Step 2.** Select the **Default** policy set.
- Step 3.** Expand the **Authentication Policy** section.
- Step 4.** In the MAB rule, click **Options** underneath Internal Endpoints.
- Step 5.** Ensure that If User Not Found is set to **CONTINUE**.

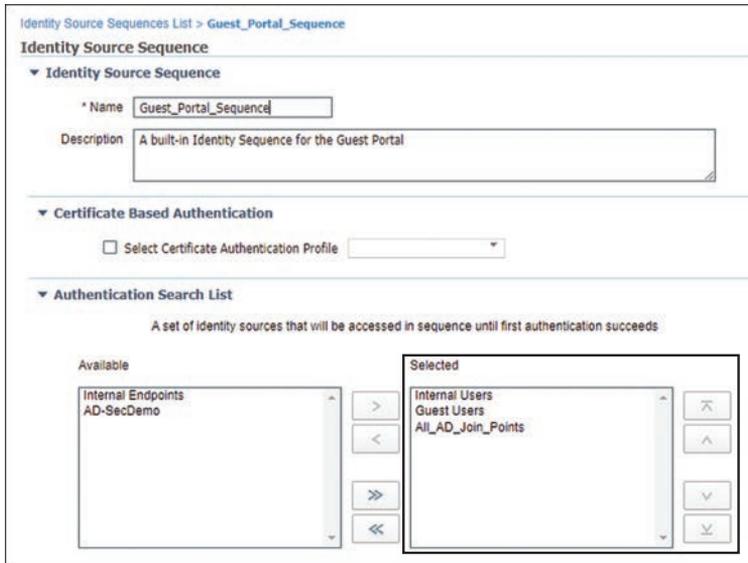


**Figure 12-8** MAB Continue

## Verify the Web Authentication Identity Source Sequence

There is a preconfigured identity source sequence (ISS) named `Guest_Portal_Sequence`. The default Web Authentication portal is configured to use this ISS. It is configured by default to check Internal Users, Guest Users, and All\_AD\_Join\_Points—in that order.

There is no configuration change required. This sequence, and all the preconfigured sequences since ISE Version 2.0, are ready to use as is. However, just to be sure it does what you need, in the ISE GUI, navigate to Work Centers > Network Access > Identities > Identity Source Sequence and select the `Guest_Portal_Sequence`, as shown in Figure 12-9.



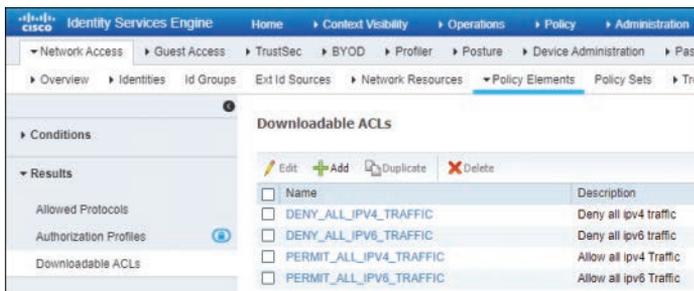
**Figure 12-9** Identity Source Sequences

## Configure a dACL for Pre-WebAuth Authorization

Before a device can reach the CWA portal, it first has to be permitted onto the network. Full network access is not desirable in most cases. For IOS-based devices, a dACL can and should be used to limit the network access.

In the ISE GUI, follow these steps:

- Step 1.** Navigate to Work Centers > Network Access > Policy Elements > Results > Downloadable ACLs, as shown in Figure 12-10.



**Figure 12-10** Downloadable ACLs

- Step 2.** Click **Add**.
- Step 3.** Name the new dACL **WebAuth**.
- Step 4.** Add a description.
- Step 5.** Configure the ACL to permit traffic to the ISE policy service nodes but deny access to the remainder of the internal network. Figure 12-11 shows what this might look like.

The screenshot displays the configuration page for a Downloadable ACL named 'WebAuth'. The description is 'A downloadable ACL used for traffic control during web authentication phases'. The IP version is set to IPv4. The ACL content is as follows:

```

1 permit ip any host 10.1.100.241
2 permit ip any host 10.1.100.242
3 permit ip any host 10.1.100.243
4 permit ip any host 10.1.100.244
5 deny ip any 10.0.0.0 0.0.0.255
6 deny ip any 172.16.0.0 0.15.255.255
7 deny ip any 192.168.0.0 0.0.255.255
8
9
10

```

The 'Check DACL Syntax' section shows a 'Recheck' button and navigation arrows. Below it, a message states 'DACL is valid'.

**Figure 12-11** Sample WebAuth dACL

- Step 6.** Click **Submit**.

## Configure an Authorization Profile

At this point, you are ready to build the authorization profile to allow the end user onto the network, apply the URL redirection to the default CWA portal with the correct URL-Redirect ACL, and apply the dACL to limit network traffic.

In the ISE GUI, follow these steps:

- Step 1.** Navigate to **Work Centers > Network Access > Policy Elements > Results > Authorization Profiles**, as shown in Figure 12-12.
- Step 2.** Click **Add**.
- Step 3.** Name the new Authorization Profile **CWA**.
- Step 4.** Select the **WebAuth** dACL.
- Step 5.** Select the **Web Redirection** checkbox and choose **Centralized Web Auth** from the first dropdown. In the ACL text box, type **ACL-WEBAUTH-REDIRECT**. You are using a default WebAuth portal, so ensure that **Sponsored Guest Portal (default)** is selected from the Value dropdown.

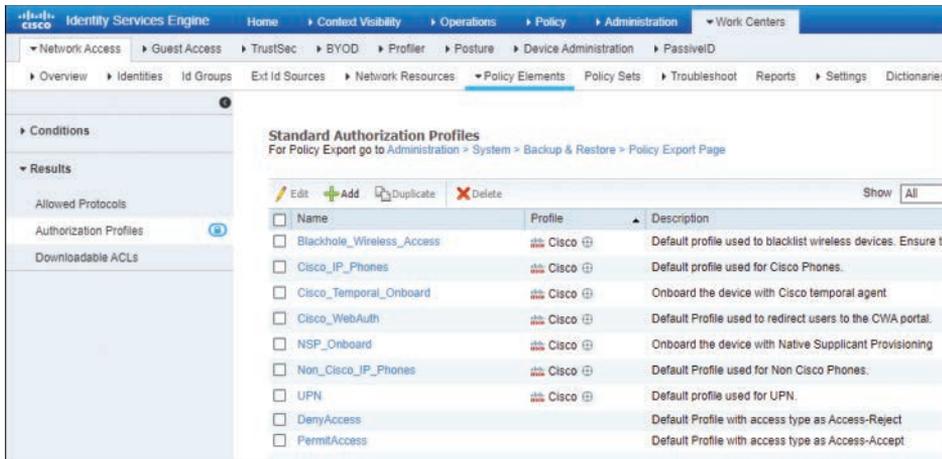


Figure 12-12 Downloadable ACLs

Figure 12-13 is a composite image that shows all the key parts in one graphic, including the complete authorization profile.

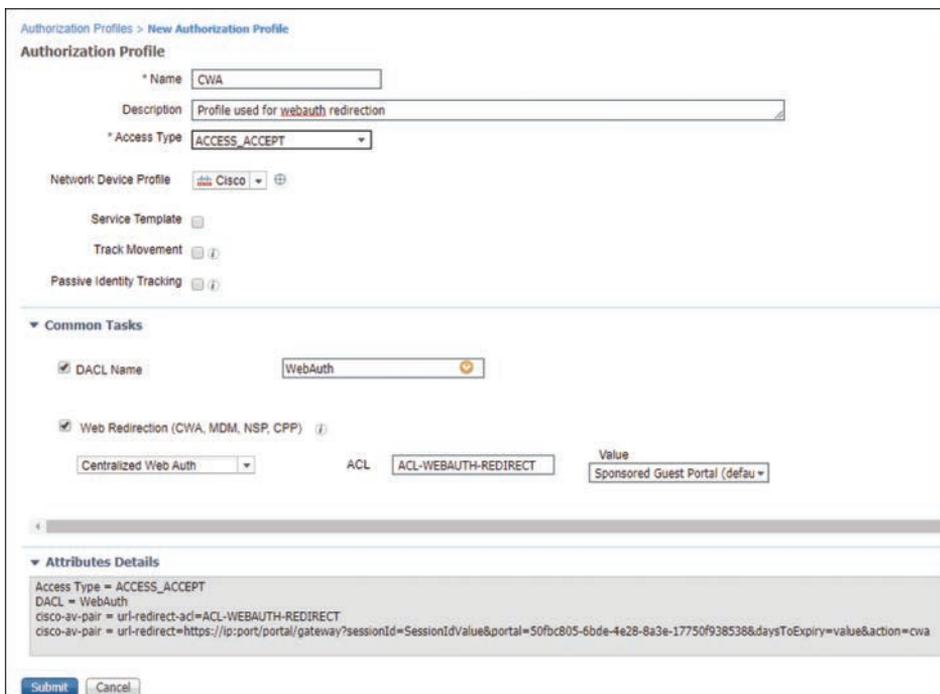


Figure 12-13 Complete CWA Authorization Profile



Many organizations implement segmentation with ISE, as it is a security best practice. After all, this is a major use case for ISE and probably a big reason you are reading this book now. With segmentation, users and devices that have an 802.1X supplicant and perform strong authentication should be admitted to the network and kept separate (segmented) from users and devices that have not gone through strong authentication.

If you are going to use VLANs for segmentation, go for it. However, you don't want to change VLANs on a device that is not using a supplicant unless you absolutely have no other choice.

A supplicant detects VLAN changes and renews its IP address in the new VLAN. Most devices that are not using a supplicant don't detect that change of VLAN, and they therefore hold on to the wrong IP address, effectively ensuring that the device will be unable to communicate on the network at all.

Some tricks of the trade can be employed here. (Some in the industry like to call it network gymnastics.) Java and ActiveX applets can be used with WebAuth, and you can play tricks with the DHCP scope in the initial VLAN. The DHCP option is one of the better ones, as a lease can be issued for a very short time, such as 5 minutes. The rules of DHCP client behavior dictate that a client will try to renew its IP address at 50% of the lease time (in this case, 2.5 minutes). ISE has a built-in DHCP server for just such use cases.

However, the recommendation from most implementors is to change VLANs only on clients who use supplicants. Therefore, the default VLAN of your switch ports should remain in a common network segment for guest users and the like, while an authorization profile for employees who gain access via 802.1X should include the VLAN change, and an employee who gains access via CWA should land in the default VLAN of the switch.

## Building CWA Authorization Policies

Configuring the authorization policy for centralized Web Authentication is ultimately a two-rule process. This section shows how to create two different authorization rules that will exist toward the end of your authorization policy. They appear at the end of the policy because of the top-down nature of ISE policies and to ensure that CWA is leveraged only when a more specific authorization rule does not apply. If an explicit authorization does not occur, ISE uses the CWA rule to redirect the user to the CWA portal.

The second rule must exist above the redirection rule because this rule is used to assign the right level of access to a user who successfully authenticates to the CWA portal. The second rule must exist above the first rule, or the user will end up in a CWA loop.

Cisco has included preconfigured authorization rules with ISE for wireless guest access Web Authentication. These rules, which are shown in Figure 12-14, are disabled by default.



**Figure 12-14** Preconfigured Web Authentication Rules

You can leverage these prebuilt rules, but how would that help you learn and prepare for the SISE 300-715 exam? Instead of leveraging those prebuilt rules, which could shorten your configuration time dramatically, in the following sections you will see how to build your own rules.

## Create the Rule to Redirect Users to the CWA Portal

The first rule to create is one that redirects unauthenticated users to the CWA portal, where they are required to authenticate interactively.

In the ISE GUI, follow these steps:

- Step 1.** Navigate to **Work Centers > Network Access > Policy Sets**.
- Step 2.** Drill down into your default policy set (or the policy set that is in use for your deployment at this time).
- Step 3.** Insert a new rule above the `Basic_Authenticated_Access` rule and name the new rule **WebAuth**, as shown in Figure 12-15.
- Step 4.** For the conditions, select two existing compound conditions from the library: **Wired\_MAB** and **Wireless\_MAB**. Ensure that the **OR** operator is used with the conditions, as shown in Figure 12-15.
- Step 5.** Use the **CWA** authorization profile you created previously for the result, as shown in Figure 12-15.
- Step 6.** Click **Save**.

Figure 12-15 shows the completed **WebAuth** authorization rule.



**Figure 12-15** Completed *WebAuth* Authorization Rule

## Create the Rules to Authorize Users Who Authenticate via CWA

The second rule needs to allow a user who authenticates via **WebAuth** to have specific access to the network. The number of rules created depends on the needs of your organization. For the purposes of this chapter, you will create only one rule, for employees. (Guest users are covered in Chapter 13.)

In this case, you need to construct a new authorization rule that will allow employees (users who are members of the **Employees** group in **Active Directory**) who have successfully authenticated through the web portal to have network access.

To accomplish this task, you can use a dictionary item named *Guest Flow* in your rule. ISE uses this dictionary item to identify when an authentication has occurred via an ISE web portal.

Technically, you are not required to use the **Guest Flow** attribute in your conditions, and an employee logging in through **CWA** will still land on any rule that matches your employee condition. However, for good security practice, you should be specific and construct an authorization rule that allows employees (users who belong to the **Active Directory** group named **Employees**) who have successfully authenticated through the web portal to have Internet-only network access.

In the ISE GUI, follow these steps:

- Step 1.** Navigate to **Work Centers > Network Access > Policy Sets**.
- Step 2.** Drill down into your default policy set (or the policy set that is in use for your deployment at this time).
- Step 3.** Insert a new rule above the WebAuth rule and name it **Employee CWA**.
- Step 4.** Use **GuestFlow** as the first condition for the rule.
- Step 5.** Add another condition with the **AND** operator.
- Step 6.** Select the Active Directory group named **Employees** as the second condition.
- Step 7.** Use the previously created authorization profile named **Internet-Only**.
- Step 8.** Select the **Employees** security group tag.
- Step 9.** Click **Save**.

Figure 12-16 shows the completed Employee\_CWA rule.



**Figure 12-16** Completed Employee\_CWA Rule

**NOTE** It is impossible to stress enough times that you should not leverage VLAN assignment with CWA. The authors of this book have met with countless customers who have deployed ISE and have helped many of them deal with exactly that problem.

## Verifying Centralized Web Authentication

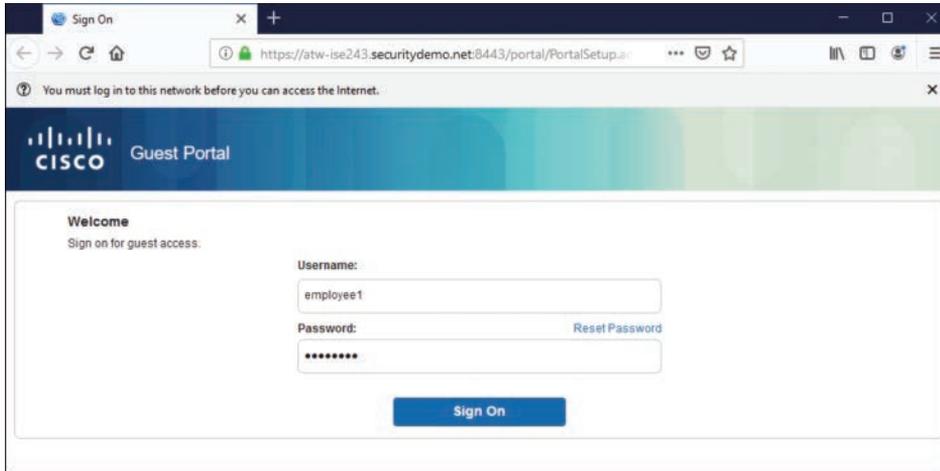
You've already gone through a fair bit of configuration in this chapter. Now that you've completed the CWA configurations, you're ready to see it all in action.

There are a number of locations to verify the actions. You can examine the effect the user experiences on the client, check Live Log in ISE, run **show** commands on the wired switch, or even examine the client details on the WLC.

### Check the Experience from the Client

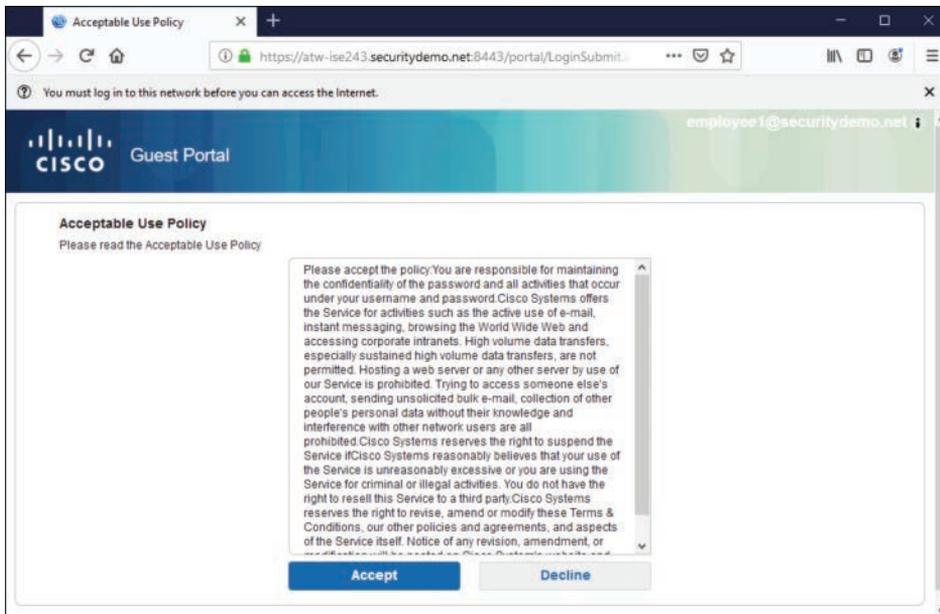
A quick way to see if your configuration is working is to try opening a web browser on the client machine and see if the browser is redirected to a portal.

Figure 12-17 shows the client experience on a wired Windows client being redirected to the CWA portal and the user entering credentials in the login form.



**Figure 12-17** *Browser Redirected to the CWA Portal*

Figure 12-18 displays the acceptable use policy that is shown to a user who submits valid authentication credentials. Figures 12-19 and 12-20 show the screens that follow, which indicate that it is now possible for the user to access the Internet. Finally, Figure 12-21 shows the successful connection to the Internet, as the user browses to <http://www.cisco.com>.



**Figure 12-18** *Acceptable Use Policy*

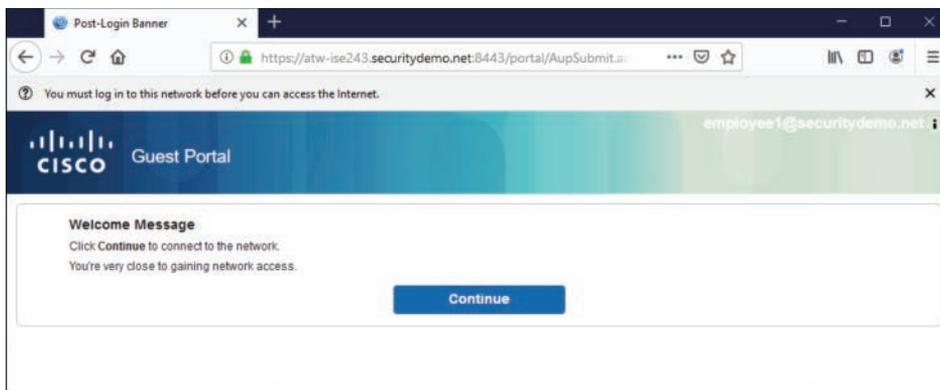


Figure 12-19 *Browser Redirected to the CWA Portal*



Figure 12-20 *Success*

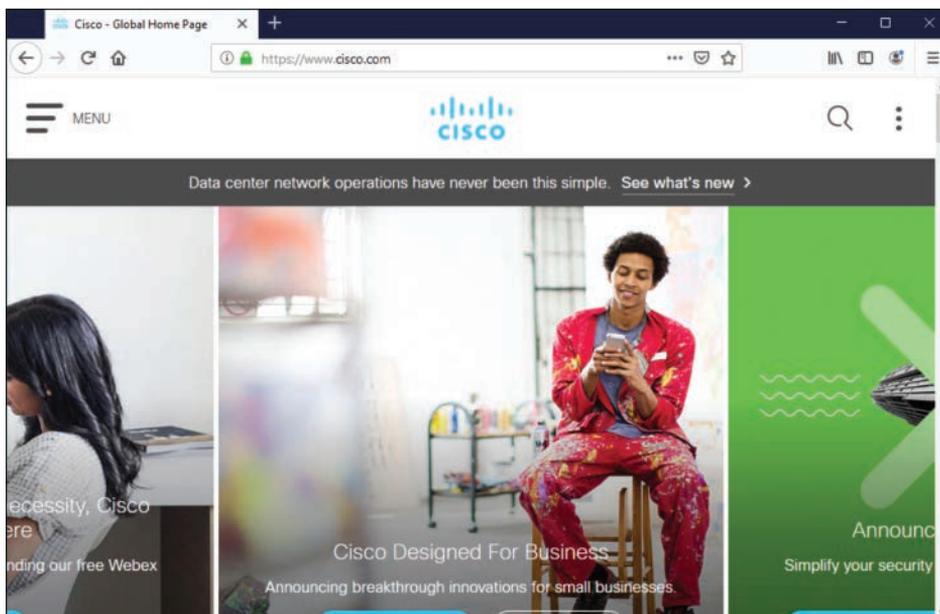


Figure 12-21 *Successfully Browsing the Internet*

## Verify CWA Through the ISE UI

A logical way to verify WebAuth configuration would be to look at the centralized policy server. ISE has a number of tools that can be used to verify WebAuth. The most common is Live Log, but many other tools can be used, including TCPDump (although this chapter covers only Live Log). For more on those other tools, see Chapter 21, “Troubleshooting Tools.”

### Check Live Log

Cisco ISE has a phenomenally useful built-in tool called Live Log. Live Log provides a near-real-time view of all incoming authentications, Change of Authorization (CoA), and more. In this section, you will follow the client experience from the ISE management console.

#### Key Topic

Figure 12-22 highlights the process.

Status	Details	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorizati...	IP Address	Network Device
X		Identity	Endpoint ID	Endpoint Prof	Authenticator	Authorization	Authorization	IP Address	Network Device
		employee1@secu...	00:50:56:A1:1E:3A	Windows10...	Default	Default == E...	Employees.I...	10.1.10.51	
		#ACSACL#-IP-Int	00:50:56:A1:1E:3A						3750-X
		employee1@secu...	00:50:56:A1:1E:3A	Windows10...		Default == E...	Employees.I...	10.1.10.51	3750-X
			00:50:56:A1:1E:3A						3750-X
			00:50:56:A1:1E:3A						3750-X
		employee1@secu...	00:50:56:A1:1E:3A					10.1.10.51	
		#ACSACL#-IP-We...	00:50:56:A1:1E:3A						3750-X
			00:50:56:A1:1E:3A	VMWare-De...	Default == M...	Default == ...	CWA	10.1.10.51	

Figure 12-22 Live Log

The following points correspond to the numbers in the figure:

1. The initial MAB has been assigned the CWA authorization result.
2. Immediately following the successful authorization, you see the successful download of the dACL.
3. After the end user enters credentials and clicks Submit, those credentials are recorded.
4. Immediately after the credentials are authenticated, a CoA-ReAuth is sent to the switch. The CoA is a key function that causes the switch to reauthenticate the endpoint without starting a new session.
5. That reauthentication means the switch sends another MAB request to ISE, where the Web Authentication from the centralized portal is bound to the MAB request from the switch.
6. Due to the correlation of the centralized Web Authentication to the MAB authentication request, the employee is assigned the Internet\_Only authorization profile, which is followed immediately by the successful download of the Internet\_Only dACL.
7. Finally, a RADIUS accounting packet is sent from the switch to ISE, confirming the full session establishment.

### Check the NAD

Checking the device that is performing the enforcement should be a good way to confirm that CWA is working. In this section, you will see how to examine the authorization result on a Cisco switch and a Cisco WLC.

## show Commands on the Wired Switch

The go-to command on a Cisco switch is **show authentication session interface** [*interface-name*]. This provides a lot of valuable information. Example 12-1 shows the command and its output for the endpoint as it was being redirected to the CWA portal.

Highlighted in this example are the MAC address, IP address, dACL (listed as an ACS ACL), URL-Redirect ACL, and the URL the end user is being redirected to. Notice that the username is the MAC address of the endpoint, which is a clear sign that the authentication performed was really a MAB. At the end of the screen output, you also see that MAB has the state Authc Success.

### Example 12-1 *show authentication session interface g1/0/3 Command Output*

```

3750-X#show authen sessions int g1/0/1
      Interface: GigabitEthernet1/0/1
      MAC Address: 0050.56a1.1e3a
      IP Address: 10.1.10.51
      User-Name: 00-50-56-A1-1E-3A
      Status: Authz Success
      Domain: DATA
      Security Policy: Should Secure
      Security Status: Unsecure
      Oper host mode: multi-auth
      Oper control dir: both
      Authorized By: Authentication Server
      Vlan Policy: N/A
      ACS ACL: xACSACLx-IP-WebAuth-5e2a155e
      URL Redirect ACL: ACL-WEBAUTH-REDIRECT
      URL Redirect: https://atw-ise243.securitydemo.net:8443/portal/gateway?sessionId=C0A8FE0100000271FEF432A8&portal=50fbc805-6bde-4e28-8a3e-17750f938538&action=cwa&token=b296cdf51b7985efc8adace571ce4c29
      Session timeout: N/A
      Idle timeout: N/A
      Common Session ID: C0A8FE0100000271FEF432A8
      Acct Session ID: 0x000003AE
      Handle: 0xBF000272

Runnable methods list:

      Method   State
      mab      Authc Success
      dot1x    Not run

```

Example 12-2 shows the command and its output for the endpoint after the user has successfully completed the Web Authentication.

**Example 12-2** *show authentication session interface g1/0/3 Command Output*

```

3750-X#show authen sessions int g1/0/1
      Interface: GigabitEthernet1/0/1
      MAC Address: 0050.56a1.1e3a
      IP Address: 10.1.10.51
      User-Name: employee1@securitydemo.net
      Status: Authz Success
      Domain: DATA
      Security Policy: Should Secure
      Security Status: Unsecure
      Oper host mode: multi-auth
      Oper control dir: both
      Authorized By: Authentication Server
      Vlan Policy: N/A
      ACS ACL: xACSACLx-IP-Internet_Only-5e606c90
      SGT: 0004-00
      Session timeout: N/A
      Idle timeout: N/A
      Common Session ID: COA8FE0100000271FEF432A8
      Acct Session ID: 0x000003AE
      Handle: 0xBF000272

Runnable methods list:
      Method   State
      mab      Authc Success
      dot1x    Not run

```

**Key Topic**

Notice the differences between Examples 12-1 and 12-2. Specifically, notice that in Example 12-2, the username is filled in (and no longer listed as the device's MAC address), and there is no longer any redirection happening. However, the authentication method for mab is still listed as Authc Success. This is because a switch still considers CWA to be MAB rather than a separate authentication. ISE is responsible for binding the username to the MAB session.

**Viewing the Client Details on the WLC**

With the WLC, you can navigate to Monitor > Clients to see a list of all clients currently associated to that controller. Clicking the MAC address brings up the details about the client and its association, including authentication information such as the redirection and run state.

**Key Topic**

When you implement ISE, in addition to needing to know how ISE works, it is especially important to have a clear understanding of how the network devices work with ISE.

Figure 12-23 is a screenshot from the WLC GUI that shows the details for a client that is currently being redirected to a CWA portal, with a cropped focus on the Security Information section.

Security Information	
Security Policy Completed	No
Policy Type	N/A
Auth Key Mgmt	N/A
Encryption Cipher	None
EAP Type	N/A
SNMP NAC State	Access
Radius NAC State	CENTRAL_WEB_AUTH
CTS Security Group Tag	Unknown(0)
AAA Override ACL Name	ACL-WEBAUTH-REDIRECT
AAA Override ACL Applied Status	Yes
AAA Override Flex ACL	none
AAA Override Flex ACL Applied Status	Unavailable
Redirect URL	https://atw-ise243.securitydemo.net:8443/portal/gateway?sessio
IPv4 ACL Name	none
FlexConnect ACL Applied Status	Unavailable
IPv4 ACL Applied Status	Unavailable

**Figure 12-23** Security Information Section of Client Details – CWA

Figure 12-23 highlights the important sections:

- The RADIUS NAC state is set to **CENTRAL\_WEB\_AUTH**.
- The Security Policy Completed state is currently **No**.
- There is an AAA override ACL named **ACL-WEBAUTH-REDIRECT**.
- The redirect URL contains the dynamic URL of the active ISE PSN for this client's session.

Figure 12-24 is a screenshot from the WLC GUI that shows the details for the same client after it has gone through a successful Web Authentication. The screenshot has a cropped focus on the Security Information section.

Security Information	
Security Policy Completed	Yes
Policy Type	N/A
Auth Key Mgmt	N/A
Encryption Cipher	None
EAP Type	N/A
SNMP NAC State	Access
Radius NAC State	RUN
CTS Security Group Tag	Not Applicable
AAA Override ACL Name	none
AAA Override ACL Applied Status	Unavailable
AAA Override Flex ACL	none
AAA Override Flex ACL Applied Status	Unavailable
Redirect URL	none
IPv4 ACL Name	Internet-Only
IPv4 ACL Applied Status	Yes

**Figure 12-24** Security Information Section of Client Details – Run State

Figure 12-24 highlights the important sections:

- The RADIUS NAC state is now **RUN**. This is a key setting: The redirection will never work if the state is RUN since RUN is the final state.
- The Security Policy Completed state is currently **Yes**.
- There is no AAA override ACL in the RUN state.
- There is no redirect URL in the RUN state.
- There is an Internet-only ACL applied.

## Exam Preparation Tasks

As mentioned in the section “How to Use This Book” in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter 27, “Final Preparation,” and the exam simulation questions in the Pearson Test Prep software online.

## Review All Key Topics

Review the most important topics in the chapter, noted with the key topics icon in the outer margin of the page. Table 12-2 lists these key topics and the page number on which each is found.

**Key  
Topic**

**Table 12-2** Key Topics

Key Topic Element	Description	Page
Paragraph	Local Web Authentication	310
Paragraph	Disconnecting management traffic from the web server in order to isolate and protect a switch	311
Paragraph	Using MAB with CWA	314
Paragraph	Traffic filtering and traffic matching	314
Paragraph	Traffic filtering and traffic matching combined with the WLC	316
Paragraph	Segmentation	321
Figure 12-22	The steps involved with CWA	327
Paragraph	A switch recognizing CWA as a MAB flow	329
Paragraph	The steps involved with CWA on the WLC	329

## Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

Web Authentication (WebAuth), Local Web Authentication (LWA), Centralized Web Authentication (CWA), Guest Flow

## Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep software online.

1. What is the final state of a client connected to a Cisco wireless LAN controller?
2. What capability in a Cisco NAD enables the client to be sent to a Web Authentication portal?
3. What authentication method is displayed on a switch for a user who has successfully authenticated via CWA?
4. Where is the URL-Redirect ACL created?
5. What is different about URL redirection when comparing how a switch uses ACLs to how a WLC uses ACLs?



# Index

## SYMBOLS

\* (asterisk), 494, 922

2FA (two-factor authentication), 26, 1000

802.1Q, 284

802.1X, 7. *See also* EAP (Extensible Authentication Protocol)

authentication. *See* authentication

Cisco AnyConnect NAM supplicant, 59–73

- AnyConnect* NAM profiles, 71–72
- Authentication Policy* view, 60, 62
- Client Policy* view, 60, 61–62
- EAP chaining*, 73
- Network Groups* view, 60, 71
- Networks* view, 60, 62–70
- overview of*, 59–60

definition of, 993

FlexAuth (Flexible Authentication)

- configuration*, 269–272
- definition of*, 994
- FAST (Flexible Authentication via Secure Tunneling)*, 45, 48–49, 215

global 802.1X commands, 266–267

history of, 38

identity stores. *See* identity stores

NADs (network access devices). *See* NADs (network access devices)

overview of, 41–42, 719–720

phased deployment

- advantages of*, 717–718
- closed mode*, 728–730
- default port behavior*, 719

- low-impact mode*, 725–727
- monitor mode*, 722–725, 730–731
- preparation for*, 720–721
- transitioning to end state*, 730–731
- wireless networks*, 731

SGT (security group tag) assignment with, 577

supplicants. *See* supplicants

## A

AAA (authentication, authorization, and accounting). *See* accounting; authentication; authorization

### aaa commands

aaa accounting commands 1 default start-stop group ISE-TACACS, 951

aaa accounting commands 15 default start-stop group ISE-TACACS, 951

aaa accounting dot1x default start-stop group ise-group, 562

aaa accounting dot1x default start-stop group radius, 262, 567

aaa accounting exec default start-stop group ISE-TACACS, 951

aaa accounting system default start-stop group ise-group, 562

aaa accounting system default start-stop group radius, 567

aaa authentication dot1x default group ise-group, 562

aaa authentication dot1x default group radius, 262, 567

aaa authentication enable default group ISE-TACACS enable, 947

- aaa authentication login, 947
- aaa authorization commands, 949
- aaa authorization config-commands, 949
- aaa authorization console, 948
- aaa authorization exec, 948
- aaa authorization network cts-list group
  - ise-group, 562
- aaa authorization network cts-list group
  - radius, 567
- aaa group server radius ise-group, 561
- aaa group server tacacs+ ISE-TACACS, 947
- aaa new-model, 261, 561, 567, 947
- aaa server radius dynamic-author, 265, 563
- AAA Identity Management Security*, 6
- AAA Servers** tab
  - corporate WLAN, 293–294
  - guest WLAN, 289–290
- ABSOLUTE\_PATH** file path option, 669
- ACCEPT** message, 9
- acceptable use policy (AUP) page settings
  - hotspot guest portals, 354–356
  - sponsored guest portals, 386
- Acceptable Use Policy in Stealth Mode
  - setting (Posture General Settings), 691
- access control entries (ACEs), 553
- Access Control List option (TACACS
  - profile), 933
- access control lists. *See* ACLs (access
  - control lists)
- Access Control Server (ACS), 8, 630, 909,
  - 910
- access levels, Admin group roles, 127–132
- access policy
  - for FMC (Firepower Management Center),
    - 840–844
  - for WSA (Web Security Appliance),
    - 855–856
- Access-Accept message, 13
- Access-Challenge message, 13
- access-layer devices. *See* NADs (network
  - access devices)
- Access-Reject message, 13
- Access-Request message, 13, 88
- Account Expiration Notification settings,
  - 346
- accounting
  - configuration
    - RADIUS accounting servers*,
      - 278–279
    - RADIUS fallback*, 279–280
  - device administration AAA with Cisco
    - IOS, 951
  - messages
    - RADIUS*, 13
    - TACACS+*, 11
- Accounting-Request message, 14
- Accounting-Response message, 14
- accounts
  - CTA STIX/TAXII API, 892–893
  - guest
    - contractors*, 344–346
    - daily*, 344–346
    - overview of*, 341, 343
    - provisioning from sponsor portals*,
      - 389–394
    - social*, 348
    - weekly*, 347
  - sponsor groups, 381–382
- ACEs (access control entries), 553
- ACL-MDM-REDIRECT, 539–540
- ACLs (access control lists)
  - ACEs (access control entries), 553
  - ACL-MDM-REDIRECT, 539–540
  - ACL-WEBAUTH-REDIRECT, 280–282,
    - 314–315, 330, 492, 693
  - configuration for BYOD onboarding,
    - 492–495
    - DNS ACLs*, 494
    - NSP ACL*, 493, 495
  - dACLs (downloadable access control lists),
    - 236, 237, 553
    - configuration for pre-WebAuth
 
      - authorization*, 319–320
    - creating*, 246–249

- DNS (Domain Name System), 494, 993
- ingress, 553–554
- local, 268–269
- named, 244
- pACLs (port-based ACLs), 725
- SGACLs (security group ACLs), 597–604
  - definition of*, 998
  - Deny\_All SGACL*, 601–602
  - east-west deployment of*, 598–599
  - egress policy*, 597–598, 600–601
  - north-south deployment of*, 598–599
  - Permit\_HTTP\_HTTPS SGACL*, 601–602
  - Permit\_ICMP SGACL*, 602–603
  - Permit\_Mgmt SGACL*, 601
  - Permit\_SRC\_HTTP\_HTTPS SGACL*, 603–604
  - Permit\_WEB\_RDP SGACL contents*, 598
  - syntax*, 599–600
- URL-redirect
  - configuration for Cisco switch*, 314–315
  - configuration for WLC*, 316
- wireless authentication, 280–284
  - Google URLs for ACL Bypass*, 282–283
  - Posture Agent Redirection ACL*, 283–284
  - Web Authentication Redirection ACL*, 280–282
- ACL-WEBAUTH-REDIRECT access list, 280–282, 314–315, 330, 492, 693
- ACS (Access Control Server), 8, 630, 909, 910
- Active Directory. *See* AD (Active Directory)
- active users, viewing in FMC (Firepower Management Center), 844–845
- ActiveX, 85–86, 153, 322, 356
- AD (Active Directory), 23, 24–25, 196–202
  - Active Directory probe, 422
  - CA (certificate authority), 469
  - definition of, 991
  - domains, 24
  - forests, 24
  - joining, 197–202
  - MDM support for, 101
  - objects, 24
  - prerequisites for, 196
- Adaptive Network Control (ANC), 148–149, 156, 822–823, 864–866
- Adaptive Security Appliances. *See* ASA (Adaptive Security Appliance)
- Adaptive Security Device Manager. *See* ASDM (Adaptive Security Device Manager)
- Add Dashlet(s) command, 134
- Add Directory dialog, 838
- Add New Dashboard option, 134
- Add New Realm dialog, 838
- Add New Rule command, 282, 283
- Add-Remove URL command, 283
- address ipv4 command, 264
- Address Resolution Protocol (ARP), 646
- addresses, MAC (Media Access Control). *See* MAC (Media Access Control) addresses
- AD-Host-Exists attribute (Active Directory), 422
- adi\_cli session command, 844–845
- AD-Join-Point attribute (Active Directory), 422
- Admin Access tab (System), 160–161
- Administration persona, 109, 737
- Administration portal, 137–142
  - Admin group roles, 127–132
  - global search for endpoints, 139–140
  - Help menu, 138, 140–141
  - initial login, 125–126
  - ISE Setup Wizards, 141
  - Settings menu, 142
  - tabs, 137–139
- Administration profile, 940–941

- Administration screen, 142, 155–170**
  - Device Portal Management tab, 166–169
    - Blacklist portal, 166*
    - Certificate Provisioning portal, 166–167*
    - Client Provisioning portal, 166–167, 650–651*
    - Custom Portal Files portal, 168*
    - Mobile Device Management portal, 168*
    - My Devices portal, 168*
    - Settings, 169*
  - Feed Service tab, 169
  - Identity Management tab, 161–163
    - External Identity Sources tab, 162*
    - Groups tab, 162*
    - Identities tab, 161*
    - Identity Source Sequences tab, 163*
    - Settings tab, 163*
  - Network Resources tab, 163–166
    - External MDM tab, 165*
    - External RADIUS Servers tab, 165*
    - Location Services tab, 166*
    - NAC Managers tab, 165*
    - Network Device Groups tab, 164–165*
    - Network Device Profiles tab, 165*
    - Network Devices tab, 163–164*
    - RADIUS Server Sequences tab, 165*
  - PassiveID Setup option, 138
  - pxGrid Services tab, 169
  - Search icon, 138
  - System Activities option, 139
  - System tab, 155–161
    - Admin Access tab, 160–161*
    - Backup & Restore tab, 160*
    - Certificates tab, 158*
    - Deployment tab, 155*
    - Licensing tab, 155–158*
    - Logging tab, 159*
    - Maintenance tab, 159*
    - Settings tab, 161*
    - Upgrade tab, 160*
  - Threat Centric NAC tab, 170
  - Visibility Setup option, 138
  - Wireless Setup (BETA) option, 139
- Administration tab (Guest Access work center), 340–341**
- AD-Operating-System attribute (Active Directory), 422**
- AD-OS-Version attribute (Active Directory), 422**
- AD-Service-Pack attribute (Active Directory), 422**
- Advance Filter, 771**
- Advanced Malware Protection. *See* AMP (Advanced Malware Protection) for Endpoints**
- Advanced Settings tab, Windows native supplicant, 57**
- Advanced tab**
  - corporate WLAN, 294–295
  - guest WLAN, 289–290
- agents, temporal, 999**
- Aggregation Services Router. *See* ASR (Aggregation Services Router)**
- Airwatch, 708**
- Alarms dashlet, 134**
- ALL role, 972**
- ALL\_ACCOUNTS sponsor group, 381**
- All\_User\_ID\_Stores, 472–474**
- alternative ID stores based on EAP type, 224–227**
  - EapAuthentication equals EAP-TLS, 225
  - EapTunnel equals EAP-FAST, 226–227
  - EapTunnel equals PEAP, 226
- AMP (Advanced Malware Protection) for Endpoints, 897–904**
  - adapter configuration, 900–904
  - capabilities of, 897–898
  - incidents, 899–900, 991
  - indicators, 899
- AMP Enabler profile, 642**

- ANC (Adaptive Network Control),  
148–149, 156, 822–823, 864–866, 991
- AND operator, 252–256
- Android devices. *See also* BYOD (bring your own device) onboarding; MDM (mobile device management)
- BYOD (bring your own device)
  - onboarding, 526–530
    - device provisioning*, 529–530
    - device registration*, 526–528
    - NSP app download*, 528–529
  - fingerprint technology, 27
  - mobile posture, 707–712
    - authorization conditions*, 709–710
    - authorization rules*, 710–712
    - supported device managers*, 707–709
- Anomalous Behaviour Detection,  
406–408, 991
- anti-malware, 100, 661–663, 681–682
- anti-spyware, 100, 663, 681–682
- anti-virus, 100, 663, 681–682, 753–756
- Anycast high availability
  - IP SLAs (service-level agreements), 754–756
  - network architecture, 753–754
  - route redistribution, 755–756
- AnyConnect Diagnostics and Reporting Tool. *See* DART (AnyConnect Diagnostics and Reporting Tool)
- AnyConnect ISE agent, 992
- AnyConnect ISE Posture Module, 99–100
- AnyConnect NAM (Network Access Manager) supplicant, 59–73, 809
- AnyConnect NAM profiles, 71–72
- Authentication Policy view, 60, 62
- Client Policy view, 60, 61–62
- EAP chaining, 73
- Network Groups view, 60, 71
- Networks view, 60, 62–70
  - Certificates tab*, 67
  - Connection Type tab*, 66
  - Credentials tab*, 68–70
  - Machine Auth tab*, 66
  - PAC Files tab*, 67–68
  - Security Level tab*, 64–66
  - User Auth tab*, 68–70
- overview of, 59–60
- profiles, 71–72
- AnyConnect posture assessment endpoint scenarios
  - AnyConnect already installed, endpoint not compliant, 700–702
  - AnyConnect not installed on endpoint yet, 696–700
  - stealth mode, 645, 703
  - temporal agent and posture compliant, 705
- AnyConnect Secure Mobility Client,  
640–649
  - AnyConnect configuration, 648–649
  - AnyConnect posture profile configuration, 644–648
  - client provisioning resource configuration, 640–642
  - downloading, 640
  - headend deployment packages, uploading to ISE, 642–644
- AnyConnect System Scan. *See* posture assessment
- Apex license packages, 156
- APIs (application programming interfaces)
  - license packages, 156
  - MDM (mobile device management), 821
- Apple iOS. *See also* MDM (mobile device management)
  - BYOD (bring your own device), 523–526. *See also* BYOD (bring your own device) onboarding
    - device enrollment*, 523–524
    - device provisioning*, 526–527
    - device registration*, 523–524
  - faceprint technology, 27
  - iPad, 482
  - iPCU (iPhone Configuration Utility), 812
  - mobile posture, 707–712
    - authorization conditions*, 709–710

- authorization rules*, 710–712
- supported device managers*, 707–709
- Push Notification, 101
- Touch ID, 310
- application conditions, 100, 655–660
- application provisioning, 101
- application remediations, 680
- Application tab (Context Visibility screen), 143
- architecture (ISE). *See* ISE (Identity Services Engine) architecture
- ARP (Address Resolution Protocol), 646
- ASA (Adaptive Security Appliance)
  - ASDM (Adaptive Security Device Manager), 592–593
  - configuration for TrustSec, 564–565
  - DAP (Dynamic Access Policy), 629
  - SGFW (security group firewall) on, 612
  - SXP (SGT Exchange Protocol) configuration on, 591–592
- ASDM (Adaptive Security Device Manager), 592–593
- Ask a Question option (Help menu), 141
- ASR (Aggregation Services Router), 613
- assertions, SAML (Security Assertion Markup Language), 35, 395, 998
- assetConnectedLinks attribute (pxGrid), 423
- assetCustomAttributes attribute (pxGrid), 423
- assetDeviceType attribute (pxGrid), 423
- assetHwRevision attribute (pxGrid), 423
- assetId attribute (pxGrid), 423
- assetIpAddress attribute (pxGrid), 423
- assetMacAddress attribute (pxGrid), 423
- assetName attribute (pxGrid), 423
- assetProductId attribute (pxGrid), 423
- assetProtocol attribute (pxGrid), 423
- assetSerialNumber attribute (pxGrid), 423
- assetSwRevision attribute (pxGrid), 423
- assetVendor attribute (pxGrid), 423
- assignment
  - SGTs (security group tags)
    - dynamically*, 577
    - manually*, 577–578
  - VLAN (virtual LAN), 551–553
- asterisk (\*), 494, 922
- attribute/value (AV) pairs, 13, 15, 107
- Audit reports, 150
- AUP (acceptable use policy) page settings
  - hotspot guest portals, 354–356
  - sponsored guest portals, 386
- authentication, 13–14. *See also* certificate-based authentication; CWA (Centralized Web Authentication); posture assessment
  - 2FA (two-factor authentication), 26, 1000
  - authentication open versus 802.1X, 719–720
  - authentication servers, 41, 991
  - authenticators, 41, 991
  - authorization compared to, 209–210, 235
  - communications in, 42
  - definition of, 206
  - device administration AAA with Cisco IOS
    - device administration AAA with Cisco IOS*, 946–948
    - TACACS+ command accounting*, 951
    - TACACS+ command authorization*, 948–950
  - devices without a supplicant, 79–80
  - EasyConnect, 89–90, 993
  - FlexAuth (Flexible Authentication)
    - configuration*, 269–272
    - definition of*, 994
    - FAST (Flexible Authentication via Secure Tunneling)*, 45, 48–49, 215
  - flows for, 804–805
  - importance of, 5
  - MAB (MAC Authentication Bypass)
    - authentication with*, 80–82, 227–228
    - configuration*, 265, 270–274, 318
    - definition of*, 717, 995

- MAB rule flowchart*, 217
  - overview of*, 96–99
  - profiling*, 96–99
  - role-specific authorization rules*, 241
  - wireless*, 489
- messages
  - RADIUS*, 13–14
  - TACACS+*, 9
- MFA (multifactor authentication), 26–29
- Multi-Auth (Multiauthentication), 995
- policies and policy sets, 151
  - allowed protocols*, 210, 213–216
  - for alternative ID stores based on EAP type*, 224–227
  - authorization compared to*, 209–210, 235
  - for certificate-based authentication*, 472–474
  - conditions*, 217–219
  - default*, 216–217
  - definition of*, 171
  - for device administration AAA with Cisco IOS*, 944
  - goals of*, 206–207, 210–211
  - identity stores*, 210–211, 219–220
  - identity validation*, 211
  - for MAB (MAC Authentication Bypass)*, 227–228
  - options*, 220
  - for remote access VPN*, 223–224
  - restoring*, 229
  - for wireless SSID*, 220–223
- remote access connections, 88–89
- SAML (Security Assertion Markup Language), 394–400
  - assertions*, 395, 998
  - guest portal logins*, 368, 394–400
  - IdPs (identity providers)*, 35, 394–400, 998
  - SPs (service providers)*, 394, 998
  - support for*, 23
- sponsored guest portals, 342, 380–381
  - AUP (acceptable use policy) page settings*, 386
  - configuration flowchart*, 380–381
  - default sponsor portal*, 384
  - login settings*, 386
  - other settings*, 387
  - portal settings*, 385–386
  - provisioning guest accounts from*, 389–394
- timers, 275
- Web Authentication. *See* WebAuth (Web Authentication)
- Windows native supplicant
  - machine authentication*, 58–59
  - user authentication*, 58
- wired, 261–276
  - Cisco ISE verification*, 302–303
  - endpoint supplicant verification*, 295–296
  - global configuration AAA commands*, 261–262
  - global configuration RADIUS commands*, 262–269
  - interface configuration settings*, 269–276
  - NAC (network access device) verification*, 296–302
- wireless
  - AAA servers*, 276–280
  - airespace ACLs (access control lists)*, 280–284
  - Cisco ISE verification*, 302–303
  - dynamic interfaces for client VLANs*, 284–286
  - endpoint supplicant verification*, 295–296
  - NAC (network access device) verification*, 296–302
  - wireless LANs*, 286–295
- authentication event fail action command, 271

- authentication event server alive action
  - reinitialize command, 272
- authentication event server dead action
  - authorize vlan command, 272
- authentication event server dead action
  - authorize voice command, 272
- authentication event server dead action
  - reinitialize vlan command, 272
- authentication host-mode multi-auth
  - command, 273
- authentication linksec policy command, 617
- authentication open command, 275, 718, 719–720, 722, 725
- authentication order dot1x mab command, 271
- Authentication Policy view, Cisco
  - AnyConnect NAM supplicant, 60, 62
- authentication port-control auto command, 276
- authentication priority dot1x mab
  - command, 271
- authentication servers, 41, 991
- authentication success settings, hotspot
  - guest portals, 357–358
- Authentication tab, Windows native
  - supplicant, 53, 56–57
- authentication timers, 275
- authentication violation restrict command, 273
- authentication VLAN, 87–88
- Authentications dashlet, 134
- authenticators, 41, 991
- authorization. *See also* ACLs (access control lists)
  - authentication compared to, 209–210, 235
  - for certificate-based authentication, 474–475
  - Cisco CTA (Cognitive Threat Analytics), 896–897
  - CoA (Change of Authorization)
    - CWA (*Centralized Web Authentication*) and, 85–86, 311
    - definition of, 16, 95–96, 992
    - enabling, 265, 277
    - ISE Profiler and, 442–444
    - messages, 110, 748
  - definition of, 209, 232
  - for device administration AAA with Cisco IOS, 948–950
  - flows for, 804–805
  - messages
    - RADIUS, 13
    - TACACS+, 10–11
  - mobile posture
    - authorization conditions, 709–710
    - authorization rules, 710–712
  - policies and policy sets, 151
    - authentication compared to, 209–210, 235
    - Blackhole\_Wireless\_Access, 240–241
    - for certificate-based authentication, 474–475
    - Cisco\_IP\_Phones, 237–241
    - compound conditions, 239, 251–256, 992
    - condition blocks, 252–256
    - configuration of, 241–249
    - default, 236–241
    - definition of, 171
    - for device administration AAA with Cisco IOS, 945–946
    - goals of, 235–241
    - for guest portals, 348–351
    - for MDM (mobile device management), 536–537
    - organization of, 216, 236
    - profile assignment in, 450–453
    - role-specific authorization rules, 241
    - rule processing for, 236–241
    - saving conditions for reuse in, 249–251
    - simple conditions, 239, 251, 999
  - profiles, 450–453
    - assignment of, 450–452, 453

- for BYOD (bring your own device) onboarding, 516*
    - configuration, 320–322*
    - Downlink MACsec, 616*
    - Employee Full Access, 241–243*
    - Employee\_Limited, 246–249*
    - for hotspot guest portals, 362–364*
    - Internet\_Only, 243–246*
    - MDM Onboard, 539–540*
    - for posture assessment, 693*
    - for self-registered guest portals, 373–380*
    - for TC-NAC (Threat Centric Network Access Control), 884–886*
  - rules, 236–241, 693–694
    - AND/OR operators in, 252–256*
    - for BYOD (bring your own device) onboarding, 517, 518*
    - for device administration AAA with Cisco WLC (Wireless LAN Controller), 977–979*
    - Employee and CorpMachine, 242–243*
    - employee full access, 241–243*
    - employee limited access, 246–249*
    - Internet-only access, 243–246*
    - IT Users Access, 252–256*
    - for MDM onboarding, 539–542*
    - PERMIT\_ALL\_IPV4\_TRAFFIC, 241–243*
    - role-specific, 241*
    - for self-registered guest portals, 373–380*
    - for TC-NAC (Threat Centric Network Access Control), 884–886*
    - Wireless Black List Default, 239*
  - security context, 232, 235
  - TrustSec, 559
  - Authorization Policy column, Live Log, 767**
  - Authorization Profiles column, Live Log, 768**
  - Authy, 29**
  - Auto Command option (TACACS profile), 933**
  - auto PAN switchover, 745–746**
  - automate-tester username command, 264**
  - automatic failover, 746**
  - auto-source command, 267**
  - AV (attribute/value) pairs, 13, 15, 107**
- ## B
- Backup & Restore tab (System), 160**
  - backup and restore, 101, 160, 759–761**
  - backup interface GigabitEthernet 3 command, 352**
  - backup-logs command, 783–784**
  - Base license packages, 156**
  - Base64-encoded files, 477**
  - BlackBerry, 508–509, 708**
  - Blackhole\_Wireless\_Access authorization profile, 240–241**
  - Blacklist portal, 166**
  - blocks, condition, 252–256**
  - bootstrapping ISE (Identity Services Engine), 177–180**
  - bring your own device. *See* BYOD (bring your own device) onboarding**
  - browsers**
    - requirements for, 125
    - Softerra LDAP, 26
    - support for, 122–123
  - BYOD (bring your own device) onboarding. *See also* MDM (mobile device management)**
    - Android onboarding flow, 526–530*
    - device provisioning, 529–530*
    - device registration, 526–528*
    - NSP app download, 528–529*
  - challenges of, 485–487
  - definition of, 487
  - dual SSID versus single SSID, 487–488, 993, 999
  - end-user experience

- Blackberry example*, 508–509
  - dual SSID with Android example*, 503–508
  - single SSID with Apple iOS example*, 496–503
  - history of, 482
  - iOS onboarding flow, 523–526
    - device enrollment*, 523–524
    - device provisioning*, 526–527
    - device registration*, 523–524
  - ISE configuration for, 495–496
    - authorization profiles*, 516
    - authorization rules for EAP-TLS authentications*, 518
    - authorization rules for onboarding*, 517
    - client provisioning policy configuration*, 512–514
    - default unavailable client provisioning policy action*, 515
    - ISE as certificate authority*, 519–520, 521–523, 994
    - native supplicant profile*, 510–512
    - SCEP (Simple Certificate Enrollment Protocol)*, 520–521, 999
    - WebAuth configuration*, 514–515
  - overview of, 487
  - self-registered guest portal settings, 372
  - verification of BYOD flows, 534–535
    - endpoint identity groups database*, 535
    - RADIUS Live Logs*, 534
    - reports*, 534–535
  - Windows and Mac onboarding flow, 531–533
    - device provisioning*, 532–533
    - device registration*, 531
  - WLC (Wireless LAN Controller) configuration, 489–495
    - ACLs (access control lists)*, 492–495
    - WLAN configuration*, 490–491
  - BYOD Endpoints dashlet, 134
- ## C
- C (Country) field, 184
  - C3PL (Common Classification Policy Language), 789
  - CA\_SERVICE\_Certificate\_Template, 520
  - Cache Last Known Posture Compliance setting, 691
  - CACs (Common Access Cards), 992
  - Call Home List setting (AnyConnect posture profile), 647
  - Call-Check for Service-Type, 228
  - Called-Station-Id attribute (RADIUS), 414
  - Calling-Station-Id attribute (RADIUS), 414
  - Calling-Station-Id field (RADIUS), 97
  - CAPs (certificate authentication profiles), 23, 202, 469, 471–472, 991
  - cards, smart, 29
  - career limiting events (CLEs), 717
  - CAs (certificate authorities). *See also* certificate-based authentication
    - AD (Active Directory), 469
    - CA-signed certificates, 182–191
    - characteristics of, 30–33
    - CSR (certificate signing requests), 182–191
      - binding certificates*, 189–191
      - certificate subject fields*, 183–184
      - downloading and importing certificates*, 188–191
      - exporting certificates*, 191
      - PEM files*, 186–187
      - submitting*, 186–187
      - wildcard certificates*, 184
    - definition of, 992
    - ISE as, 519–520, 521–523, 994
    - signatures, 31–32
    - trusted, 31–32, 475–479
      - certificate status verification*, 478–479
      - public certificates*, 476–477
      - role in authentication process*, 463–465

- Catalyst 3000 Series, 12.2(55)SE switch configuration, 1034–1038
- Catalyst 3000 Series, 15.0(2)SE switchconfiguration, 1038–1044
- Catalyst 4500 Series, IOS-XE 3.3.0 / 15.1(1)SG switchconfiguration, 1053–1057
- Catalyst 6500 Series, 12.2(33)SXJ switchconfiguration, 1058–1061
- Catalyst 9000 Series, 16.9.5 switchconfiguration, 1044–1052
- categories, logging, 778–779
- CCP (client provisioning policy), 515
- CDA (Context Directory Agent), 469
- CDP (Cisco Discovery Protocol), 98, 273, 418, 991
- centralized portal, LWA (Local Web Authentication) with, 84–85
- Centralized Web Authentication. *See* CWA (Centralized Web Authentication)
- certificate authentication profiles. *See* CAPs (certificate authentication profiles)
- certificate authorities. *See* CAs (certificate authorities)
- Certificate Authority Certificates menu (ISE Certificate Authority), 520
- Certificate Provisioning portal, 166–167
- certificate revocation lists (CRLs), 33, 466, 992
- certificate signing requests. *See* CSRs (certificate signing requests)
- Certificate Templates menu (ISE Certificate Authority), 520
- certificate-based authentication, 158. *See also* PKI (public key infrastructure)
  - CAPs (certificate authentication profiles), 23, 202, 469, 471–472, 991
  - CAs. *See* CAs (certificate authorities)
  - concept of, 30–31
  - CRLs (certificate revocation lists), 466, 992
  - CSRs (certificate signing requests), 182–191, 521–523
    - binding certificates*, 189–191
    - definition of*, 992
    - downloading and importing certificates from*, 188–191
    - exporting certificates*, 191
    - ISE (Identity Services Engine)*, 521–523
    - PEM files*, 186–187
    - submitting*, 186–187
    - wildcard certificates*, 184
- CWA (Centralized Web Authentication) configuration, 313
  - definition of, 463
- EAP-TLS (EAP Transport Layer Security), 470
  - expired certificates, 32–33, 465
  - guest services, 340–341
- ISE configuration for, 181–191, 470–479
  - authentication policies*, 472–474
  - authorization policies*, 474–475
  - CAPs (certificate authentication profiles)*, 471–472
  - certificate status verification*, 478–479
  - overview of*, 470
  - principal username X.509 attribute*, 470
  - protocols verification*, 470–471
  - public certificates, importing*, 476–477
  - trusted CAs (certificate authorities)*, 475–479
- popularity of, 460
- public certificates, 476–477
- purpose of, 181
- pxGrid certificates. *See* pxGrid (Platform Exchange Grid)
- RAs (registration authorities), 998
- revoked certificates, 33
  - checking for*, 466–467
  - CRLs (certificate revocation lists)*, 33
  - CRLs (certificate revocation lists)*, 33, 466

- OCSP (*Online Certificate Status Protocol*), 33, 466, 996
  - validity period, 467
- self-signed certificates, 181–182
- trusted certificates, 537–538
- Certificates tab
  - Cisco AnyConnect NAM supplicant, 67
  - System, 158
- chaining, EAP, 73, 216
- Challenge Handshake Authentication Protocol. *See* CHAP (Challenge Handshake Authentication Protocol)
- Change of Authorization. *See* CoA (Change of Authorization)
- CHAP (Challenge Handshake Authentication Protocol), 7, 46, 214, 215
- chip cards, 29
- Chrome, support for, 122
- Cisco Access Control Server (ACS), 909, 910
- Cisco Access Registrar, 8
- Cisco AnyConnect Diagnostics and Reporting Tool. *See* DART (AnyConnect Diagnostics and Reporting Tool)
- Cisco AnyConnect ISE agent, 992
- Cisco AnyConnect ISE Posture Module. *See* AnyConnect ISE Posture Module
- Cisco AnyConnect Network Access Manager. *See* AnyConnect NAM (Network Access Manager) supplicant
- Cisco Cognitive Threat Analytics. *See* CTA (Cognitive Threat Analytics)
- Cisco Context Directory Agent (CDA), 469
- Cisco Discovery Protocol (CDP), 98, 418
- Cisco Duo Security, 27–29
- Cisco Firepower Management Center. *See* FMC (Firepower Management Center) configuration
- Cisco Identity Services Engine architecture. *See* ISE (Identity Services Engine) architecture
- Cisco Industrial Network Director (IND), 827
- Cisco IOS. *See* IOS (Internetwork Operating System)
- Cisco ISE for BYOD and Secure Unified Access (Woland and Heary), 859
- Cisco ISE (Identity Services Engine) architecture. *See* ISE (Identity Services Engine) architecture
- Cisco Meraki Systems Manager (Meraki SM), 708
- Cisco Meta Data (CMD) field, 593, 616
- Cisco NAC (Network Admission Control), 626, 630
- Cisco Network Setup Assistant app, 492, 507
- Cisco Platform Exchange Grid. *See* pxGrid (Platform Exchange Grid)
- Cisco Secure Access Control Server (ACS), 8
- Cisco Secure Network Server (SNS), 177
- Cisco Security Agent (CSA) service, 676
- Cisco Software-Defined Access (SD-Access), 613–614
- Cisco Stealthwatch. *See* Stealthwatch
- Cisco Supplicant Provisioning Wizard, 513
- Cisco Temporal Agent, 99–100
- Cisco Umbrella, 640
- Cisco Wireless LAN Controller. *See* WLC (Wireless LAN Controller)
- Cisco IP Phones authorization profile, 237–241
- cisco-av-pair command, 576
- CiscoPress SSID policy set, 518
- CiscoPress-TLS, 513–514
- Citrix XenMobile, 708
- Class (RADIUS attribute 25) VSA, 266
- Class-Identifier attribute (DHCP), 411
- Clean Machines, 631
- CLEs (career limiting events), 717
- CLI (command-line interface), 992. *See also specific commands*
- CLI Setup Wizard, 178–179
- Client Messaging servers, 101

- Client Policy view, Cisco AnyConnect NAM supplicant, 60, 61–62
- client provisioning policy. *See* CPP (client provisioning policy)
- Client Provisioning portal, 166–167, 650–651
- Client Provisioning tab (Policy page), 153
- Client Stopped Responding counter, 768
- Client Supplicant Not Capable of MACsec policy, 617
- client VLANs, dynamic interfaces for, 284–286
  - employee dynamic interface, 284–285
  - guest dynamic interface, 285–286
- Client-FQDN attribute (DHCP), 411
- client/server communication, 7–8
- closed mode, 728–730
- CMD (Cisco Meta Data) field, 593, 616
- CN (common name), 183, 833
- CoA (Change of Authorization)
  - CWA (Centralized Web Authentication) and, 85–86, 311
  - definition of, 16, 992
  - enabling, 265, 277
  - ISE Profiler and, 442–444
    - global CoA*, 442–443, 994
    - per-profile CoA*, 443–444
  - messages, 110, 748
- CoA Type setting, hotspot guest portals, 354
- Coa-Events report, 888–889
- Cognitive Intelligence. *See* CTA (Cognitive Threat Analytics)
- Cognitive Threat Analytics. *See* CTA (Cognitive Threat Analytics)
- command sets
  - definition of, 992
  - device administration AAA with Cisco IOS, 934–936
  - TACACS+, 934–936, 941–943
- command-line interface (CLI), 992. *See also specific commands*
  - COMMANDS role, 971
  - comma-separated values (CSV) files, 194
  - Common Access Cards (CACs), 992
  - Common Classification Policy Language (C3PL), 789
  - common name (CN), 183, 833
  - Common Port option, Nmap, 416
  - Common Task Type option, TACACS profile, 933
  - Common Vulnerabilities and Exposures (CVE), 873, 992
  - Common Vulnerability Scoring System (CVSS), 873, 992
  - compliance. *See* posture assessment
  - compliance modules, updating, 637–638
  - compound conditions, 239, 251–256, 664–665, 677–678, 992
  - Compromised Endpoints Over Time dashlet, 137
  - conditions
    - authentication policy, 217–219
    - authorization policy
      - blocks*, 252–256
      - compound*, 239, 251–256, 664–665, 677–678, 992
      - definition of*, 235
      - EmployeeFullEAPChain*, 249–250
      - mobile posture*, 709–710
      - saving for reuse*, 249–251
      - simple*, 239, 251, 999
    - posture policy, 654–679
      - anti-malware*, 661–663
      - anti-spyware*, 663
      - anti-virus*, 663
      - application*, 655–660
      - compound*, 677–678
      - dictionary compound*, 664–665
      - dictionary simple*, 663–664
      - disk encryption*, 665–666
      - file*, 667–673
      - firewall*, 660–661
      - hardware attributes*, 655

- patch management*, 673–675
- Registry*, 675
- USB*, 679
- Wired\_802.1X, 242, 254
- Wired\_MAB, 242
- Conditions Studio, 217–219
- Conditions tab (Policy Elements), 154
- conf t command, 621
- configure command, 922
- configure terminal command, 963
- Connection Settings (Device Administration), 918
- Connection Type tab (Cisco AnyConnect NAM supplicant), 66
- Console application, 812
- context
  - brokering, 992
  - definition of, 992
  - sharing
    - EPS (Endpoint Protection Services)*, 821–822
    - MDM integration*, 820–821
    - need for*, 818
    - pxGrid*. *See pxGrid (Platform Exchange Grid)*
    - Rapid Threat Containment*, 821–823, 993, 998
- Context Directory Agent (CDA), 469
- Context Visibility screen, 137, 142, 143
- Context-In, 827, 992
- Context-Out, 827, 993
- CONTINUE message, 9, 11
- Continue option
  - authentication policy, 220
  - posture reassessment, 692
- Continuous Monitoring Interval setting (Posture General Settings), 691
- contractors, 344–346
- CONTROLLER role, 971
- Core Files support bundles, 783
- Corporate Wipe option, 543
- corporate WLAN configuration, 291–295
  - AAA Servers tab, 293–294
  - Advanced tab, 294–295
  - General tab, 292
  - Layer 2 Security tab, 292–293
  - Layer 3 Security tab, 293
- correlation policy, 845–847
- correlation rules, 845–847
- Country (C) field, 184
- CPP (client provisioning policy), 172, 637–638
  - AnyConnect Secure Mobility Client, 640–649
    - AnyConnect configuration, building*, 648–649
    - AnyConnect posture profile*, 644–648
    - client provisioning resource configuration*, 640–642
    - headend deployment packages, uploading to ISE*, 642–644
  - BYOD (bring your own device) onboarding
    - client provisioning policies*, 512–514
    - default unavailable client provisioning policy action*, 515
- Client Provisioning portal, 153, 166–167, 650–651
  - default client provisioning policy, 652
  - order of operations, 637–638
  - rules, creating, 652–653
- CRC32 file type, 672
- credentials, 20
- Credentials tab (Cisco AnyConnect NAM supplicant), 68
- CRLs (certificate revocation lists), 33, 466, 992
- Cropped Portal Page Customization screen, 358
- crypto key generate rsa general-keys mod 2048 command, 313
- crypto key generate rsa modulus 2048 command, 946

- CSA (Cisco Security Agent) service, 676
- CSRs (certificate signing requests), 182–191, 521–523
  - binding certificates, 189–191
  - definition of, 992
  - downloading and importing certificates from, 188–191
  - exporting certificates, 191
  - ISE (Identity Services Engine), 521–523
  - PEM files, 186–187
  - submitting, 186–187
  - wildcard certificates, 184
- CSV (comma-separated values) files, 194
- CTA (Cognitive Threat Analytics), 890–897
  - authorization with, 896–897
  - CTA STIX/TAXII API account creation, 892–893
  - dashboard, 890–892
  - integration for TC-NAC, 894–896
- CTD (Cyber Threat Defense), 857
- CTI (cyber threat intelligence), 890, 993
- cts authorization list cts-list command, 562
- cts credentials id Sw01 password Cisco123 command, 561
- cts manual command, 595, 621
- cts manualN7K-DIST command, 578
- cts role-based enforcement command, 562, 595, 596
- cts role-based sgt-map command, 580
- cts role-based sgt-map vlan-list command, 580
- cts sxp connection peer command, 588, 589
- cts sxp default password command, 588
- cts sxp default source-ip command, 588
- cts sxp enable command, 588–589
- cubes, ISE
  - definition of, 109, 737, 995
  - joining, 182
  - licensing in, 747–748
- Current, Chip, 337
- Custom Attribute option (TACACS profile), 933
- Custom Portal Files portal, 168
- Custom Ports option (Nmap), 416
- custom profiling attributes, 445–448
- Customization admin role, 127
- CVE (Common Vulnerabilities and Exposures), 873, 992
- CVSS (Common Vulnerability Scoring System), 873, 992
- CWA (Centralized Web Authentication), 730–731. *See also* sponsored guest portals
  - authentication process, 85–87
  - authorization policies, 322–324
    - custom authorization rules, 323–324*
    - Guest Flow attribute, 323–324, 994*
    - preconfigured authorization rules, 322*
- Cisco switch configuration, 313–315
  - certificates, 313*
  - HTTP/HTTPS server, 314*
  - URL-redirect ACL, 314–315*
- CoA (Change of Authorization) and, 311
  - definition of, 991
  - dual SSID onboarding and, 496
  - ISE (Identity Services Engine)
    - configuration, 317–322
      - authorization profiles, 320–322*
      - dACLs (downloadable access control lists), 319–320*
      - Guest\_Portal\_Sequence ISS (identity source sequence), 319*
      - MAB (MAC Authentication Bypass), 96–99, 318*
  - services supported by, 311
  - with third-party network device support, 87–88
- URL-redirected MAC authentication bypass, 311–313
- verification from client, 324–326
- verification on NAD (network access device), 327–331

- client details, viewing on WLC,*  
329–331
- show commands on wired switch,*  
328–329
- WLC (Wireless LAN Controller)
  - configuration, 98, 315–316, 329–331
  - ISE NAC feature, 315–316
  - MAC Filtering option, 315
  - URL-redirect ACL, 316
- Cyber Threat Defense (CTD), 857
- cyber threat intelligence (CTI), 890, 993

## D

- dACLs (downloadable access control lists),  
13, 236, 237, 246–249,  
319–320, 548, 553
- daily guest accounts, 344–346
- DAP (Dynamic Access Policy), 629
- DART (AnyConnect Diagnostics and  
Reporting Tool), 59, 809–811, 991
- dashboard, 132–137
  - Dashboard Settings menu, 134
  - Endpoints tab, 134–135
  - Guests tab, 135–136
  - Summary tab, 134
  - Threat tab, 137
  - verifying profiling with, 454
  - Vulnerability tab, 136
- Dashboard Settings menu, 134
- dashlets
  - Alarms, 134
  - Authentications, 134
  - BYOD Endpoints, 134
  - Compromised Endpoints Over Time, 137
  - Endpoint Categories, 135, 454
  - Endpoint Categories dashlet, 135
  - Endpoints, 134, 135
  - Failure Reason, 136
  - Guest Status, 136
  - Guest Type, 136
  - Location, 136
  - Metrics, 134
  - Network Devices, 134, 135
  - Status, 134
  - System Summary, 134
  - Threat Watchlist, 137
  - Top Threats, 137
  - Top Vulnerability, 136
  - Total Compromised Endpoints, 137
  - Total Vulnerable Endpoints, 136
  - Vulnerability Watchlist, 136
  - Vulnerable Endpoints Over Time, 136
- databases, 994
  - endpoint identity groups, 535
  - endpoints, 455–456
  - internal endpoint, 22, 994
  - internal user, 994
- Datagram Transport Layer Security  
(DTLS), 190
- DaysSinceLastCheckIn attribute, 537
- debug aaa authentication command, 955
- debug aaa authorization command,  
955–958
- debug aaa tacacs enable command, 985
- debug authentication command, 815
- debug client command, 302, 815
- debug commands, 815
- debug dot1x command, 302, 815
- debug epm command, 815
- debug interface command, 815
- debug ip tcp transactions command, 966
- debug logs, 779–784
  - configuration, 779–780
  - downloading from GUI, 780
  - support bundles, 782–784
    - categories of, 782–783
    - creating from CLI, 783–784
    - creating from GUI, 783
    - definition of, 782
    - viewing from CLI, 781–782
- Debug Logs support bundles, 783

- debug tacacs command, 958–961
- debug tacacs packet command, 963–965
- decryption policy, 857
- Dedicated MNT, 742
- de-duplication of logs, 805–807
- default authorization policies, 236–241
- default client provisioning policy, 652
- default policy sets, 211
- Default Posture Status setting (Posture General Settings), 691
- Default Privilege option (TACACS profile), 933
- default sponsor portals, 384
- defense-in-depth, 241
- Delete option (endpoint management), 543
- deny statement, 280, 316
- Deny\_All SGACL, 601–602
- DenyAllCommands command, 941
- deployment
  - AnyConnect headends
    - AnyConnect configuration, building*, 648–649
    - package upload to ISE*, 642–644
    - posture profile configuration*, 644–648
  - device administration AAA, 911–913
    - large deployments*, 912
    - medium deployments*, 913
    - small deployments*, 913
  - high availability, 743
    - Anycast high availability*, 753–756
    - backup and restore*, 759–761
    - failure scenarios*, 753
    - general guidelines for*, 752–753
    - licensing in multi-mode ISE cube*, 747–748
    - load balancing*, 751–752, 756–757
    - MnT (Monitoring and Troubleshooting) nodes*, 109–110, 743–744
    - node groups*, 748–750
    - PAN (Policy Administration node)*, 109, 743–744
    - patches*, 757–759
- ISE (Identity Services Engine)
  - distributed*, 116–119
  - hybrid*, 116–117
  - overview of*, 113
  - physical versus virtual*, 111–113
  - scale limits for*, 118–119
  - single-node*, 113
  - two-node*, 114–116
- ISE nodes in distributed environment, 737–742
  - ISE cubes*, 737
  - ISE persona types*, 737
  - node personas*, 742
  - PPAN (Policy Administration Node)*, 738–739
  - primary devices*, 738–739
  - registration of ISE nodes*, 739–742
- phased approach to
  - advantages of*, 717–718
  - authentication open versus 802.1X*, 719–720
  - closed mode*, 728–730
  - low-impact mode*, 725–727
  - monitor mode*, 722–725, 730–731
  - preparation for*, 720–721
  - transitioning to end state*, 730–731
  - wireless networks*, 731
- Deployment tab (Administration), 155
- design
  - for device administration, 911–913
    - large deployments*, 912
    - medium deployments*, 913
    - small deployments*, 913
  - SXP (SGT Exchange Protocol), 582–583
- Desktop Preview (portal page customization), 358
- destination tree view (TrustSec policy matrix), 553

Details icon, Live Log, 768

device administration AAA, 478–479

concept of, 6

configuring with Cisco IOS, 930

*device administration service, enabling, 937*

*network device preparation, 937–939*

*overview of, 932*

*policy preparation, 939–946*

*privilege levels, 932–933, 997*

*TACACS profiles, 932–934*

*TACACS+ authentication and fallback, 946–948*

*TACACS+ command accounting, 951*

*TACACS+ command authorization, 948–950*

*TACACS+ command sets, 934–936, 992*

*testing and troubleshooting in ISE, 952–954*

*troubleshooting at IOS command line, 954–966*

configuring with Cisco WLC (Wireless LAN Controller)

*ISE configuration on WLC TACACS+ servers, 979–980*

*network device preparation, 972*

*policy results preparation, 974–977*

*policy sets, 977–979*

*testing and troubleshooting, 981–986*

*top-level menus, 971–972*

definition of, 2, 993

design and deployment, 911–913

*large deployments, 912*

*medium deployments, 913*

*small deployments, 913*

device administration service, enabling, 937

device backup, 101

device enrollment, 523–524

device tracking in IOS Xe 16.x and later, 267

devices without a supplicant, 79–80

graphical illustration of, 6, 909

interactive nature of, 909–910

license packages, 157

MDM (mobile device management), 108, 820–821. *See also* BYOD (bring your own device) onboarding

*definition of, 995*

*overview of, 101–102*

*posture assessment with, 108*

*supported features, 101–102*

*vendors, 101–102*

NAD (network access device)

configuration, 917

*connection settings, 918*

*identities, 920*

*network resources, 921–922*

*overview of, 916–917*

*password change control, 918*

*policy elements, 922–924*

*policy sets, 925–927*

*reports, 927*

*session key assignment, 918*

*UI navigation for, 919–920*

network device troubleshooting, 812–815

*client details, viewing on WLC, 813–814*

*debug commands, 815*

*show authentication interface command, 812–813*

policies, 922–924, 939–946

*policy sets, 943–946*

*roles, 939*

*TACACS command sets, 922–923, 941–943*

*TACACS profiles, 923–924, 939–941*

purpose of, 909–910

RADIUS. *See* RADIUS (Remote Access Dial-In User Service)

- reports, 150
- resources for, 6
- security context, 232, 235
- smart devices
  - employee limited access*, 246–249
  - Internet-only access for*, 243–246
- TACACS+. *See* TACACS+ (Terminal Access Controller Access Control System)
- Device Administration Policy Set**, 943–944
- Device Portal Management tab (Administration screen)**, 166–169
  - Blacklist portal, 166
  - Certificate Provisioning portal, 166–167
  - Client Provisioning portal, 166–167, 650–651
  - Custom Portal Files portal, 168
  - Mobile Device Management portal, 168
  - My Devices portal, 168
  - Settings, 169
- device provisioning**
  - Android onboarding flow, 529–530
  - iOS onboarding flow, 526–527
  - Windows and Mac onboarding flow, 532–533
- device registration**
  - Android onboarding flow, 526–528
  - iOS onboarding flow, 523–524
  - Windows and Mac onboarding flow, 531
- Device Sensor**, 98, 267, 426–427, 457–458
- DeviceComplianceStatus** attribute, 536
- DeviceCompliantStatus** attribute, 712
- DeviceRegisterStatus** attribute, 536
- device-sensor accounting** command, 427
- device-sensor filter-list cdp list** command, 427
- device-sensor filter-list dhcp list** command, 426
- device-sensor filter-list lldp list** command, 427
- device-sensor filter-spec cdp include list** command, 427
- device-sensor filter-spec dhcp include list** command, 427
- device-sensor filter-spec lldp include list** command, 427
- device-sensor notify all-changes** command, 427
- device-tracking attach-policy** command, 267
- device-tracking policy** command, 267
- device-tracking tracking auto-source** command, 267
- DHCP (Dynamic Host Configuration Protocol)**
  - DHCP helper, 424–427
  - DHCP probe, 411–414
  - DHCPSPAN probe, 411–414
  - profiling, 97, 98
- diagnostic tools**
  - Endpoint Debug, 796–798
  - endpoint diagnostics, 809–812
    - Cisco AnyConnect Diagnostics and Reporting Tool (DART)*, 59, 809–811
    - supplicant provisioning logs*, 812
  - Evaluate Configuration Validator, 788–793
  - Execute Network Device Command, 787–789
  - network device troubleshooting, 812–815
    - client details, viewing on WLC*, 813–814
    - debug commands*, 815
    - show authentication interface command*, 812–813
  - Posture Troubleshooting, 794–795
  - RADIUS Authentication Troubleshooting tool, 785–786
  - Session Trace, 801–804
  - TCP Dump, 798–801
  - troubleshooting methodology, 804–808
    - authentication and authorization flows*, 804–805
    - log de-duplication*, 805–807
    - USERNAME user*, 807

- Diagnostics and Reporting Tool. *See* DART (AnyConnect Diagnostics and Reporting Tool)
- Diagnostics reports, 150
- diagrams, monitor mode flow, 7, 723–724
- dial-up networking, 88
- Dictionaries tab (Policy Elements), 154
- dictionary compound conditions, 664–665
- dictionary simple conditions, 100, 663–664
- digital certificates. *See* certificate-based authentication
- disable command, 932
- Disable UAC Prompt setting (AnyConnect posture profile), 646
- Discovery host setting (AnyConnect posture profile), 647
- disk encryption conditions, posture policy, 665–666
- DiskEncryptionStatus attribute, 536
- Display Language setting, hotspot guest portals, 354
- distributed ISE deployment, node configuration in, 116–119, 737–742
  - ISE cubes, 737
  - ISE persona types, 737
  - node personas, 742
  - PPAN (Policy Administration Node), 738–739
  - primary devices, 738–739
  - registration of ISE nodes, 739–742
- Distribution Points, CRL, 467
- DNS (Domain Name System), 196
  - ACLs (access control lists)
    - for BYOD onboarding, 494
    - definition of, 993
  - DNS probe, 417
  - snooping, 494
- Domain Name System (DNS), 196, 417
- Domain-Name attribute (DHCP), 411
- domains
  - AD (Active Directory), 24
    - joining, 197–202
    - prerequisites for joining, 196
  - TrustSec, 557, 1000
- Dot1x. *See* 802.1X
- dot1x pae authenticator command, 275
- dot1x system-auth-control command, 266, 563
- dot1x timeout tx-period 10 command, 275
- Downlink MACsec, 616–619
  - authorization profile, 616
  - ISE (Identity Services Engine) configuration, 619
  - policies, 616–618
  - switch configuration modes, 618–619
- downloadable access control lists (dACLs), 13, 236, 237, 246–249, 319–320, 553
- downloadable ACLs (dACLs), 548
- downloading
  - AnyConnect Secure Mobility Client, 640
  - debug logs, 780
- Drop option, authentication policy, 220
- DTLS (Datagram Transport Layer Security), 190
- dual SSID onboarding, 487–488, 993
  - definition of, 993
  - ISE (Identity Services Engine) configuration, 495–496, 510–523
    - authorization profiles, 516
    - authorization rules for EAP-TLS authentications, 518
    - authorization rules for onboarding, 517
    - client provisioning policy configuration, 512–514
    - default unavailable client provisioning policy action, 515
    - dual SSID with Android example, 503–508
    - ISE as certificate authority, 519–520, 521–523, 994
    - native supplicant profile, 510–512
    - SCEP (Simple Certificate Enrollment Protocol), 520–521, 999
    - WebAuth configuration, 514–515

- verification of BYOD flows, 534–535
    - endpoint identity groups database*, 535
    - RADIUS Live Logs*, 534
    - reports*, 534–535
  - WLC (Wireless LAN Controller)
    - configuration, 489–495
    - ACLs (access control lists)*, 492–495
    - WLAN configuration*, 490–491
  - Dubois, Jesse, 772
  - “dumb” devices, 96
  - Duo Security, 27–29
  - Dynamic Access Policy (DAP), 629
  - Dynamic Host Configuration Protocol. *See* DHCP (Dynamic Host Configuration Protocol)
  - dynamically assigning SGTs (security group tags), 577
- ## E
- EAP (Extensible Authentication Protocol), 7, 42–49, 73, 214, 545–546
    - alternative ID stores based on, 224–227
    - comparison of, 47–49
    - definition of, 993
    - EAP-FAST, 45, 48–49, 215
    - EAP-GTC, 43, 45, 215
    - EAP-MD5, 43, 46, 214
    - EAP-MS-CHAPv2, 43, 45, 46, 215
    - EAPoL (EAP over LAN). *See* 802.1X
    - EAPoL-Proxy-Logoff, 273, 993
    - EAPoL-Start (EAP over LAN Start), 270
    - EAP-TLS, 43, 45, 214, 215
    - EAP-TTLS, 45–46, 48–49
    - identity store comparison, 49
    - native types, 43–44, 996
    - PEAP, 44–45, 48–49, 53–54, 55–56, 108, 215
    - TEAP, 46–47, 48–49, 73
    - tunneled, 44–49, 1000
  - EAP MSCHAPv2 Properties dialog, 54
  - EAP\_Authentication\_Certificate\_Template, 520
  - EAPChainingResult, 546
  - EAP-Identity-Request messages, 270
  - east-west segmentation, 554–555
  - east-west SGACL deployment, 598–599
  - EasyConnect, 89–90, 993
  - Edge, support for, 122
  - editors, Conditions Studio, 218
  - EDR (endpoint detection and response), 661, 897–898
  - eduroam initiative, 46
  - egress enforcement, of SGTs (security group tags), 555–556
  - EKU (extended key usage), 211
  - Elevated system admin role, 131
  - Employee and CorpMachine authorization rule, 242–243
  - employee dynamic interface, 284–285
  - employee full access rule, 241–243
  - employee limited access, 246–249
  - Employee profile, 977
  - Employee\_Limited dACL, 246–249
  - EmployeeFullEAPChain condition, 249–250
  - Enable agent IP refresh setting (AnyConnect posture profile), 646
  - enable command, 932
  - Enable notifications in stealth mode setting (AnyConnect posture profile), 645
  - Enable Rescan Button setting (AnyConnect posture profile), 645
  - enable secret ISEc0ld command, 947
  - Enable signature check setting (AnyConnect posture profile), 645
  - encryption, posture policy conditions for, 665–666
  - end state, transitioning to, 730–731
  - Endpoint Assignment tab (Adaptive Network Control), 149
  - endpoint attribute filtering, 444–445
  - Endpoint Categories dashlet, 135, 454

- Endpoint Debug tool, 796–798
- Endpoint ID column (Live Log), 767
- endpoint identity groups, 22, 354, 450–452
- endpoint identity groups database, 535
- Endpoint list, 454
- Endpoint Profile column (Live Log), 767
- Endpoint Profile Policies, 431–441
- endpoint protection platform (EPP), 661, 897–898
- Endpoint Protection Services (EPS), 821–822, 993
- EndPointPolicy, 453
- endpoints
  - diagnostics, 809–812
    - Cisco AnyConnect Diagnostics and Reporting Tool (DART)*, 809–811
    - supplicant provisioning logs*, 812
  - EDR (endpoint detection and response), 661, 897–898
  - endpoint attribute filtering, 444–445
  - endpoint diagnostics, 809–812
    - Cisco AnyConnect Diagnostics and Reporting Tool (DART)*, 59, 809–811
    - supplicant provisioning logs*, 812
  - endpoint identity groups, 22, 354, 450–452
  - endpoint identity groups database, 535
  - EndPointPolicy, 453
  - endpoints database, 455–456
  - EPP (endpoint protection platform), 661, 897–898
  - EPS (Endpoint Protection Services), 993
  - global search for, 139–140
  - guest access, 338
  - health of. *See* posture assessment
  - internal endpoint database, 22, 994
  - local endpoint groups, 195
  - MDM (mobile device management), 542–543
  - onboarding, 153
  - posture assessment, 695–705
    - AnyConnect already installed, endpoint not compliant*, 700–702
    - AnyConnect not installed on endpoint yet*, 696–700
    - redirected state*, 695–696
    - stealth mode*, 645, 703
    - temporal agent and posture compliant*, 705
  - profile policies for, 431–441
  - purge policies for, 345
  - supplicant verification, 295–296
- Endpoints and Users reports, 150
- Endpoints dashlet, 134, 135
- Endpoints tab
  - Context Visibility screen, 143
  - Home page, 134–135
- Endpoints widget, 454
- enforcement, traffic
  - SGACLs (security group ACLs), 597–604, 998
    - Deny\_All* SGACL, 601–602
    - east-west deployment of*, 598–599
    - egress policy*, 597–598, 600–601
    - north-south deployment of*, 598–599
    - Permit\_HTTP\_HTTPS* SGACL, 601–602
    - Permit\_ICMP* SGACL, 602–603
    - Permit\_Mgmt* SGACL, 601
    - Permit\_SRC\_HTTP\_HTTPS* SGACL, 603–604
    - Permit\_WEB\_RDP* SGACL *contents*, 598
    - syntax*, 599–600
  - SGFWs (security group firewalls), 611–613
    - on ASA (Adaptive Security Appliances)*, 612
    - on ASR (Aggregation Services Router)*, 613
    - definition of*, 999
    - on Firepower*, 612–613
    - on ISR (Integrated Services Router)*, 613

- TrustSec policy matrix, 604–609
  - configuration of*, 605–609
  - views of*, 604–605
- environment data, 558, 993
- epm logging command, 299
- EPP (endpoint protection platform), 661, 897–898
- EPS (Endpoint Protection Services), 821–822, 993
- EPStatus condition, 821–822
- eradication, 896
- ERROR message, 9, 11
- ERS (External RESTful Services), 131, 850–851
- Evaluate Configuration Validator, 788–793
- Evaluation license, 155, 157
- exam preparation, 988–989
  - exam updates, 1032–1033
  - final study and review, 988–989
  - hands-on activities, 988–989
- Execute Network Device Command tool, 787–789
- Executive SGT (Security Group Tag), 555
- ExernalBlue, 868
- exit command, 932
- expanding policy sets, 211
- expired certificates, 32–33, 465
- exploits, definition of, 872, 993
- Export command (Dashboard settings), 134
- Ext Id Sources tab (Guest Access work center), 340
- extended key usage (EKU), 211
- Extensible Authentication Protocol.
  - See* EAP (Extensible Authentication Protocol)
- Extensible Communication Platform (XCP) server, 825
- Extensible Messaging and Presence Protocol (XMPP), 825
- External CA Settings, 520
- external data source condition, 100

- External Identity Sources tab (Identity Management), 162
- external identity stores, 23–33, 993. *See also* certificate-based authentication
  - AD (Active Directory), 24–25
  - configuration, 196
  - definition of, 23, 993
  - LDAP (Lightweight Directory Access Protocol), 25–26
  - MFA (multifactor authentication), 26–29
  - OTP (one-time password) services, 29
  - smart cards, 29
- External MDM tab (Network Resources), 165
- External RADIUS Servers tab (Network Resources), 165
- External RESTful Services (ERS), 131, 850–853

## F

- faceprint technology, 27
- Fail Live Log status, 767
- FAIL message, 10
- Failure Reason dashlet, 136
- fallback, TACACS+, 946–948
- FAST (Flexible Authentication via Secure Tunneling)
  - EAP chaining, 216
  - EAP-FAS, 215
  - EAP-FAST, 45, 48–49
- FDM (Firepower Device Management), 832
- Feed Service tab (Administration screen), 169
- FIDO2, 310
- files
  - CRC32, 672
  - file conditions, 100, 667–673
  - FileDate, 669–671
  - FileExistence, 671–678
  - FileVersion, 672
  - ise-2.7.0.356.SPA.x86\_64.iso, 112

- ISE-2.70.356-virtual-SNS3615-SNS3655-300.ova, 112
  - ISE-2.70.356-virtual-SNS3655-SNS3695-1200.ova, 112
  - ISE-2.70.356-virtual-SNS3695-2400.ova, 112
  - paths for, 669-670
  - policy for, 612
  - remediations for, 682
  - SHA-256, 672
  - FileVersion file type, 672**
  - filtering**
    - endpoint attributes, 444-445
    - Live Log, 771
  - Finance SGT (Security Group Tag), 555**
  - fingerprint technology, 27**
  - Firefox, support for, 122**
  - Firepower**
    - FDM (Firepower Device Management), 832
    - FTD (Firepower Threat Defense), 629
    - SGFW (security group firewall) on, 612-613
  - firewalls, 611**
    - conditions for, 100, 660-661
    - posture policy conditions, 660-661
    - remediations, 682
    - SGFWs (security group firewalls), 611-613
      - on ASA (Adaptive Security Appliances), 612*
      - on ASR (Aggregation Services Router), 613*
      - definition of, 999*
      - on Firepower, 612-613*
      - on ISR (Integrated Services Router), 613*
  - FlexAuth (Flexible Authentication)**
    - configuration, 269-272
    - definition of, 994
    - FAST (Flexible Authentication via Secure Tunneling)
      - EAP chaining, 216*
      - EAP-FAS, 215*
      - EAP-FAST, 45, 48-49*
  - FMC (Firepower Management Center) configuration, 831-850**
    - access rules, 840-844
    - active users, viewing, 844-845
    - FDM (Firepower Device Management), 832
    - pxGrid integration, 832-837
    - Rapid Threat Containment, 845-850
    - realms, 837-840
  - FOLLOW message, 11**
  - Forbes, Paul, 633**
  - forests, AD (Active Directory), 24**
  - form factors**
    - ISE (Identity Services Engine), 177
    - SNS (Secure Network Server) appliances, 111-112
  - FQDN (fully qualified domain name), 416, 833**
  - Framed-IP-Address attribute (RADIUS), 265, 414**
  - FTD (Firepower Threat Defense), 629**
  - Full Configuration Database support bundles, 782**
  - Full Wipe option (endpoint management), 543**
  - fully qualified domain name (FQDN), 416, 833**
  - Funk Software, 45**
- G**
- gateway providers, SMS (Short Message Service), 388-389**
  - GCL (pxGrid common library), 825**
  - General tab**
    - corporate WLAN, 292
    - guest WLAN, 287-288
  - Generic Token Card (GTC), 43, 45, 215**
  - global CoA (Change of Authorization), 442-443, 994**

- global configuration AAA commands, 261–262
- global configuration RADIUS commands, 262–269
  - device tracking in IOS Xe 16.x and later, 267
  - global 802.1X commands, 266–267
  - IOS 12.2.x, 262–263, 264–266
  - IOS 15.x, 263–266
  - IOS XE, 263–266
  - local ACL (access control list) creation, 268–269
- Global Page Customizations (portal page customization), 361
- global profiler settings, 444–445
- global search for endpoints, 139–140
- Global Search tool, verifying profiling with, 454–455
- Good Technology, 708
- Google Chrome, 122
- Google Client Messaging servers, 101
- Google Play Store, 282, 492–493, 506
- Google URLs for ACL Bypass, 282–283
- graphical user interface. *See* GUI (graphical user interface)
- GROUP\_ACCOUNTS sponsor group, 381
- groups
  - Admin group roles, 127–132
  - endpoint, 22
  - endpoint identity, 22, 354, 450–452, 535
  - local endpoint, 195
  - local user identity, 194
  - NDGs (network device groups), 720–721, 996
  - node, 748–750, 996
  - user identity, 22, 339–340, 840–844, 1000
- Groups tab (Identity Management), 162
- GRTC (Generic Token Card), 43, 45
- GTC (Generic Token Card), 43, 215
- Guest Access work center
  - Administration tab, 340–341
  - Ext Id Sources tab, 340
- Identities tab
  - endpoints, 338
  - ISS (identity source sequence), 339
  - user identity groups, 339–340
- overview page, 337–338
- Portals & Components tab, 341
  - guest portals, 341–342
  - guests, 341, 343–348
  - overview of, 341
  - sponsor portals, 341
- guest dynamic interface, 285–286
- Guest Exceeds Limit setting, contractor accounts, 345
- Guest Flow attribute, 323–324, 994
- guest location setting, 369–371, 994
- Guest management license packages, 156
- guest portals, 341–342
  - authorization policies for, 348–351
  - definition of, 341–342
  - hotspot, 351–358
    - AUP (acceptable use policy) page settings, 354–356
    - authentication success settings, 357
    - authorization rule configuration, 362–365
    - configuration flowchart for, 351
    - definition of, 342
    - interface bonding, 352–353
    - portal page customization, 358–362
    - portal settings, 352–354
    - post-access banner page settings, 355–356
    - support information page settings, 357–358
    - VLAN DHCP release page settings, 355–356
- self-registered
  - authorization rule configuration, 373–380
  - BYOD settings, 372
  - configuration flowchart, 365–366
  - definition of, 342

- guest change password settings, 371–372*
  - guest device compliance settings, 373*
  - guest device registration settings, 371–372*
  - guest location setting, 369–371, 994*
  - login page settings, 367–368*
  - portal settings, 366–367*
  - registration form settings, 368–371*
  - self-registration success, 371*
- sponsored, 380–381
  - AUP (acceptable use policy) page settings, 386*
  - configuration flowchart, 380–381*
  - default sponsor portal, 384*
  - definition of, 342*
  - login settings, 386*
  - other settings, 387*
  - portal settings, 385–386*
  - provisioning guest accounts from, 389–394*
- Guest reports, 150**
- guest services, 337–341**
  - administration, 340–341
  - authorization policies for, 348–351
  - guests, 343–348
    - contractors, 344–346*
    - daily, 346–347*
    - definition of, 341*
    - overview of, 343*
    - provisioning from sponsor portals, 389–394*
    - social, 348*
    - sponsor, 341*
    - weekly, 347*
  - hotspot guest portals, 351–365
    - AUP (acceptable use policy) page settings, 354–356*
    - authentication success settings, 357*
    - authorization rule configuration, 362–365*
    - configuration flowchart for, 351*
    - definition of, 341–342*
    - interface bonding, 352–353*
    - portal page customization, 358–362*
    - portal settings, 352–354*
    - post-access banner page settings, 355–356*
    - support information page settings, 357–358*
    - VLAN DHCP release page settings, 355–356*
  - identities, 338–340
  - importance of, 334
  - notification services, 388–389
    - SMS gateway providers, 388–389*
    - SMTP servers, 388*
  - overview of, 337–341
  - SAML (Security Assertion Markup Language) authentication, 394–400
  - self-registered guest portals
    - authorization rule configuration, 373–380*
    - BYOD settings, 372*
    - configuration flowchart, 365–366*
    - definition of, 342*
    - guest change password settings, 371–372*
    - guest device compliance settings, 373*
    - guest device registration settings, 371–372*
    - guest location setting, 369–371, 994*
    - login page settings, 367–368*
    - portal settings, 366–367*
    - registration form settings, 368–371*
    - self-registration success, 371*
  - sponsored guest portals, 380–381
    - AUP (acceptable use policy) page settings, 386*
    - configuration flowchart, 380–381*
    - default sponsor portal, 384*
    - definition of, 342*

- login settings*, 386
- other settings*, 387
- portal settings*, 385–386
- provisioning guest accounts from*, 389–394
- sponsors
  - definition of*, 381, 999
  - sponsor groups*, 381–382
- Guest Status dashlet**, 136
- Guest Type dashlet**, 136
- guest WLAN configuration**, 287–290
  - AAA Servers tab, 289–290
  - Advanced tab, 290
  - General tab, 287–288
  - Layer 2 Security tab, 288
  - Layer 3 Security tab, 289
- Guest\_Portal\_Sequence ISS**, 319, 339
- guests**, 343–348
  - contractors, 344–346
  - daily, 344–346
  - definition of, 341, 994
  - overview of, 343
  - provisioning from sponsor portals, 389–394
  - social, 348
  - weekly, 347
- Guests tab (Home page)**, 135–136
- GUI (graphical user interface)**
  - Admin group roles, 127–132
  - Administration portal, 137–142
    - global search for endpoints*, 139–140
    - Help menu*, 138, 140–141
    - ISE Setup Wizards*, 141
    - Settings menu*, 142
    - tabs*, 137–139
  - Administration screen, 142, 155–170
    - Device Portal Management tab*, 166–169
    - Feed Service tab*, 169
    - Identity Management tab*, 161–163
    - Network Resources tab*, 163–166
  - PassiveID Setup option*, 138
  - pxGrid Services tab*, 169
  - Search icon*, 138
  - System Activities option*, 139
  - System tab*, 155–161
  - Threat Centric NAC tab*, 170
  - Visibility Setup option*, 138
  - Wireless Setup (BETA) option*, 139
- browser requirements for, 125
- Context Visibility screen, 137, 142, 143
- definition of, 994
- downloading, 780
- Home dashboards, 132–137
- initial login, 125–126
- Operations screen, 142, 143–150
  - ANC (Adaptive Network Control) component*, 147–148, 991
  - RADIUS tab*, 144–146
  - Reports tab*, 150
  - TACACS Live Log tab*, 147
  - Threat-Centric NAC Live Logs tab*, 146
  - Troubleshoot tab*, 147–148
- Policy page, 138, 142, 150–154
  - Client Provisioning tab*, 153
  - Policy Elements tab*, 154
  - Policy Sets tab*, 150–151
  - Posture tab*, 152
  - Profiling tab*, 152
- support bundles, 783
- supported browsers, 122–123
- Work Centers screen, 142, 170–171

## H

- HA (high availability)**
  - configuration, 269–272
  - RADIUS fallback, 279–280
- hardware attributes condition**, 100, 655
- headends, AnyConnect**
  - configuration of, 640–642

- deployment packages
  - AnyConnect configuration, building*, 648–649
  - posture profile configuration*, 644–648
  - uploading to ISE*, 642–644
- number of, 640
- Hello (Windows), 27
- help command, 932
- Help menu, Administration portal, 138, 140–141
- Helpdesk admin role, 127
- HelpDesk command set, 941–942
- helpdesk group, 945
- HelpDesk profile, 939, 940, 976
- high availability (HA), 743
  - Anycast, 753–756
    - IP SLAs (service-level agreements)*, 754–756
    - network architecture*, 753–754
    - route redistribution*, 755–756
  - backup and restore, 759–761
  - configuration, 269–272
  - failure scenarios, 753
  - general guidelines for, 752–753
  - licensing in multi-mode ISE cube, 747–748
  - load balancing
    - IOS (Internetwork Operating System)*, 756–757
    - PSNs (Public Services Networks)*, 751–752
  - MnT (Monitoring and Troubleshooting) nodes, 109–110, 743–744
    - logging categories*, 744
    - logging flows*, 743
    - logging targets*, 743–744
  - node groups, 748–750
  - PAN (Policy Administration node), 109, 743–744
  - patches, 757–759
  - RADIUS fallback, 279–280
- high-security mode. *See* closed mode
- Home dashboards, 132–137
  - Dashboard Settings menu, 134
  - Endpoints tab, 134–135
  - Guests tab, 135–136
  - Summary tab, 134
  - Threat tab, 137
  - Vulnerability tab, 136
- hop-by-hop encryption, 548
- host mode, switch port, 272–274
- Host-Name attribute (DHCP), 411
- hostname command, 946
- HostScan, 629
- hotspot guest portals, 342, 351–358
  - AUP (acceptable use policy) page settings, 354–356
  - authentication success settings, 357
  - authorization rule configuration, 362–365
  - configuration flowchart for, 351
  - interface bonding, 352–353
  - portal page customization, 358–362
  - portal settings, 352–354
  - post-access banner page settings, 355–356
  - support information page settings, 357–358
  - VLAN DHCP release page settings, 355–356
- “HowTo: Cisco and F5 Deployment Guide-ISE Load Balancing Using BIG-IP” (Hyps), 752
- HR SGT (Security Group Tag), 555
- hrDeviceDescr option (Nmap), 416
- HTTP (Hypertext Transfer Protocol)
  - HTTP probe, 420–421
  - HTTP/HTTPS servers, enabling, 314
  - HTTPS (HTTP Secure), 126, 180
  - POST method, 84–85
- hybrid ISE deployment, 116–117
- Hyper-V, 113
- Hyps, Craig, 633, 752

- I**
- IBM MaaS360, 708**
- IBM Tivoli Identity Manager (TIM), 25**
- identification profiles, WSA (Web Security Appliance), 855–857**
- Identities tab**
  - Device Administration, 920
  - Guest Access work center
    - endpoints*, 338
    - ISS (identity source sequence)*, 339
    - user identity groups*, 339–340
  - Identity Management, 161
- Identity admin role, 127**
- Identity column, Live Log, 767**
- Identity Management tab (Administration screen), 161–163**
  - External Identity Sources tab, 162
  - Groups tab, 162
  - Identities tab, 161
  - Identity Source Sequences tab, 163
  - Settings tab, 163
- identity providers. *See* IdPs (identity providers)**
- Identity Services Engine. *See* ISE (Identity Services Engine) architecture**
- Identity Source Sequences tab (Identity Management), 163**
- identity sources, 34, 35**
- identity stores, 21–33, 993**
  - authentication policy for, 219–220
  - CAPs (certificate authentication profiles), 202
  - definition of, 20–21
  - EAP (Extensible Authentication Protocol). *See* EAP (Extensible Authentication Protocol)
  - external
    - Active Directory. See AD (Active Directory)*
    - certificates. See certificate-based authentication configuration*, 196
    - definition of*, 23, 993
    - LDAP (Lightweight Directory Access Protocol)*, 25–26
    - MFA (multifactor authentication)*, 26–29
    - OTP (one-time password) services*, 29
    - smart cards*, 29
  - identity sources, 21, 994
  - identity validation, 211
  - internal, 21–22
    - endpoint groups*, 22
    - user identity groups*, 22, 1000
  - ISS (identity source sequence), 34, 202–204, 218, 319, 339, 472, 994
  - local endpoint groups, 195
  - local user identity groups, 194
  - local users, 195–196
  - selection of, 210–211
- Idle Timeout option (TACACS profile), 933**
- IdPs (identity providers), 35, 394–400, 998**
- IEEE 802.1X. *See* 802.1X**
- IETF (Internet Engineering Task Force), 12**
  - NEA (Network Endpoint Assessment), 626
  - RADIUS. *See* RADIUS (Remote Access Dial-In User Service)
- IF.THEN policy rules, 154**
  - in authentication policies, 216
  - in authorization policies, 236
- IMEI attribute, 537**
- importing public certificates, 476–477**
- incidents, 899–900**
- Include Service Version Information option (Nmap), 416**
- IND (Industrial Network Director), 827**
- indicators of compromise (IoCs), 899, 994**
- Industrial Network Director (IND), 827**
- Informational Live Log status, 767**
- infrastructure configuration**
  - DHCP helper, 424–427
  - IOS Device Sensor, 426–427
  - SPAN (Switched Port Analyzer), 424–425

- VACLs (VLAN Access Control Lists), 425–426
- VMware vSwitches, 427
- ingress access controls**
  - ACLs (access control lists), 553–554
  - east-west segmentation, 554–555
  - VLAN assignment, 551–553
- int eth1/3N7K-DIST command**, 578
- int GigabitEthernet 2 command**, 352
- Integrated Services Router. *See* ISR (Integrated Services Router)**
- integration**
  - definition of, 820, 994
  - MDM (mobile device management), 820–821
    - administrative management*, 545
    - configuration*, 537–538
    - endpoint management*, 542–543
    - integration points*, 536–537
    - onboarding rules*, 539–542
    - self-management*, 543–544
  - Rapid Threat Containment, 821–823
    - ANC (Adaptive Network Control)*, 822–823
    - definition of*, 998
    - EPS (Endpoint Protection Services)*, 821–822, 993
- interface bonding, hotspot guest portals**, 352–353
- interface configuration**, 269–276
  - application of initial ACL to port, 275–276
  - authentication settings, 274–275
  - authentication timers, 275
  - configuration of interfaces as switch ports, 269
  - FlexAuth (Flexible Authentication), 269–272
  - HA (high availability), 269–272
  - host mode of switch port, 272–274
- interface g1/0/1 command**, 267
- interface range command**, 269
- intermediate CAs (certificate authorities)**, 521–523
- internal blocking**, 896
- Internal CA Settings menu (ISE Certificate Authority)**, 520
- internal endpoint database**, 22, 994
- internal identity stores**, 21–22
  - endpoint groups, 22
  - user identity groups, 22, 1000
- internal user database**, 994
- Internet Engineering Task Force. *See* IETF (Internet Engineering Task Force)**
- Internet Explorer**, 122
- Internet-only access for smart devices**, 243–246
- intrusion prevention systems (IPs)**, 661, 818
- IoCs (indicators of compromise)**, 899, 994
- iOS. *See* Apple iOS**
- IOS (Internetwork Operating System)**
  - device administration AAA with, 930
    - device administration service, enabling*, 937
    - network device preparation*, 937–939
    - overview of*, 932
    - policy preparation*, 939–946
    - privilege levels*, 932–933, 997
    - TACACS profiles*, 932–934
    - TACACS+ authentication and fallback*, 946–948
    - TACACS+ command accounting*, 951
    - TACACS+ command authorization*, 948–950
    - TACACS+ command sets*, 934–936, 992
    - testing and troubleshooting in ISE*, 952–954
    - troubleshooting at IOS command line*, 954–966

- Device Sensor feature, 426–427
- global configuration RADIUS commands
  - device tracking in IOS Xe 16.x and later*, 267
  - IOS 12.2.x*, 262–263, 264–266
  - IOS 15.x*, 263–266
  - IOS XE*, 263–266
  - local ACL (access control list) creation*, 268–269
- IOS XE switches
  - configuration for TrustSec*, 560–563
  - global configuration RADIUS commands*, 263–266
  - manual SGT (security group tag) propagation on*, 595–597
- IOS-based NADs, 495
- load balancing, 756–757
- SXP (SGT Exchange Protocol)
  - configuration on, 588–590
- IOS\_Network\_CS, 943
- IOS\_Admin\_Privilege profile, 940–941
- IOS\_HelpDesk\_CS, 941–942
- IOS\_HelpDesk\_Privilege profile, 940
- IOS\_Security\_CS, 942–943
- IoT SGT (Security Group Tag), 555
- ip access-group ACL-ALLOW command, 276
- ip access-list ext ACL-AGENT-REDIRECT command, 269
- ip access-list ext ACL-DEFAULT command, 268
- ip access-list ext ACL-WEBAUTH-REDIRECT command, 268, 315
- ip access-list extended ACL-ALLOW command, 268
- ip access-list extended command, 425, 948
- IP Address column, Live Log, 768
- ip device tracking command, 266, 298
- ip device tracking probe auto-source command, 267
- ip domain-name command, 313, 946
- ip helper-address command, 412–413, 424
- ip http active-session-modules none command, 314
- ip http secure-server command, 314
- ip http server command, 314
- ip radius source-interface command, 266
- IP SLAs (service-level agreements), 754–756
- ip ssh version 2 command, 947
- iPad, 482. *See also* Apple iOS
- iPCU (iPhone Configuration Utility), 812
- iPhone, 482. *See also* Apple iOS
- iPhone Configuration Utility (iPCU), 812
- IPs (intrusion prevention systems), 612, 661, 818
- ISE (Identity Services Engine) architecture, 6. *See also* profiling
  - Anomalous Behaviour Detection, 406–408, 991
  - configuration for BYOD onboarding, 495–496, 510–523
    - authorization profiles*, 516
    - authorization rules for EAP-TLS authentications*, 518
    - authorization rules for onboarding*, 517
    - Blackberry example*, 508–509
    - client provisioning policy configuration*, 512–514
    - default unavailable client provisioning policy action*, 515
    - dual SSID with Android example*, 503–508
    - ISE as certificate authority*, 519–520, 521–523, 994
    - native supplicant profile*, 510–512
    - SCEP (Simple Certificate Enrollment Protocol)*, 520–521, 999
    - single SSID with Apple iOS example*, 496–503
    - WebAuth configuration*, 514–515
  - configuration for CWA (Centralized Web Authentication), 317–322, 327
    - authorization profiles*, 320–322
    - dACLs (downloadable access control lists)*, 319–320

- Guest\_Portal\_Sequence ISS (identity source sequence)*, 319
- MAB (MAC Authentication Bypass)*, 96–99, 318
- configuration for MACsec, 619
- configuration for pxGrid, 828–831
- cubes, 182
  - definition of*, 109, 737, 995
  - licensing in*, 747–748
- deployment
  - distributed*, 116–119, 737–742
  - hybrid*, 116–117
  - overview of*, 113
  - physical versus virtual*, 111–113
  - scale limits for*, 118–119
  - single-node*, 113
  - two-node*, 114–116
- device administration AAA with Cisco IOS
  - device administration service, enabling*, 937
  - network device preparation*, 937–939
  - policy preparation*, 939–946
  - TACACS+ authentication and fallback*, 946–948
  - TACACS+ command accounting*, 951
  - TACACS+ command authorization*, 948–950
- Endpoint Profile Policies, 431–441
- form factors, 177
- GUI (graphical user interface). *See* GUI (graphical user interface)
- high availability, 743
  - Anycast high availability*, 753–756
  - backup and restore*, 759–761
  - failure scenarios*, 753
  - general guidelines for*, 752–753
  - licensing in multi-mode ISE cube*, 747–748
  - load balancing*, 751–752, 756–757
  - MnT (Monitoring and Troubleshooting) node*, 109–110, 743–744
  - node groups*, 748–750
  - PAN (Policy Administration node)*, 109, 743–744
  - patches*, 757–759
- initial configuration, 174
  - AD (Active Directory)*, 196–202
  - bootstrapping*, 177–180
  - CAPs (certificate authentication profiles)*, 202
  - certificates*, 181–191
  - external identity stores*, 196, 993
  - form factors*, 177
  - installation guides*, 177
  - ISS (identity source sequence)*, 202–204, 994
  - local endpoint groups*, 195
  - local user identity groups*, 194
  - local users*, 195–196
  - NADs (network access devices)*, 192
  - NDGs (network device groups)*, 192–194
  - SSL (Secure Sockets Layers)*, 181
  - TLS (Transport Layer Security)*, 181–182
- ISE NAC feature, 315–316
- ISE nodes in distributed environment, 737–742
  - ISE cubes*, 737
  - ISE persona types*, 737
  - node personas*, 742
  - PPAN (Policy Administration Node)*, 738–739
  - primary devices*, 738–739
  - registration of ISE nodes*, 739–742
- licensing
  - in multi-mode ISE cube*, 747–748
  - packages*, 155–158
- Live Log, 327
- NADs (network access devices), 113
- network probes, 409–423
  - Active Directory*, 422
  - configuration*, 409–411

- DHCP and DHCPSPAN*, 411–414
- DNS*, 417
- HTTP*, 420–421
- NETFLOW*, 419–420
- Nmap (network scan)*, 415–417
- publishing endpoint probe data on*, 450
- pxGrid*, 423
- RADIUS*, 414–415
- SNMPQUERY and SNMPTRAP*, 417–419
- nodes
  - configuration in distributed environment*, 737–742
  - definition of*, 109
  - MnT (Monitoring and Troubleshooting)*, 109–110, 743–744
  - node groups*, 748–750
  - PAN (Policy Administration node)*, 109, 745–748
  - PSN (Policy Services node)*, 110
  - single-node ISE deployment*, 113
  - two-node ISE deployment*, 114–116
- overview of, 106–108
- personas
  - Administration*, 109, 737
  - definition of*, 108–109
  - Monitoring*, 109–110, 737
  - Policy Services*, 110, 737
  - pxGrid*, 111, 737
  - types of*, 737
- posture assessment. *See* posture assessment
- Profiler Feed Service, 404–406, 429–430
  - CoA (Change of Authorization) with*, 442–444
  - configuration*, 429
  - verification of*, 429–430
- SXP (SGT Exchange Protocol)
  - configuration on*, 584–586
- troubleshooting. *See* troubleshooting tools
  - verification of*, 302–303
  - Live Sessions*, 303
  - RADIUS Live Log*, 302–303
- version scalability, 118–119
- virtual appliances, 177
- WLC device administration AAA
  - ISE configuration on WLC TACACS+ servers*, 979–980
  - network device preparation*, 972
  - policy results preparation*, 974–977
  - policy sets*, 977–979
- ISE Community Page option (Help menu), 141
- ISE Documentation option (Help menu), 141
- ISE on Cisco.com option (Help menu), 141
- ISE Partner Ecosystem option (Help menu), 141
- ISE Passive Identity Connector (ISE-PIC), 157, 858
- ISE Portal Builder option (Help menu), 141
- ISE Profiler. *See* profiling
- ISE Setup Wizards, 141
- ISE Software Downloads option (Help menu), 141
- ISE YouTube Channel option (Help menu), 141
- ise-2.70.356.SPA.x86\_64.iso file, 112
- ISE-2.70.356-virtual-SNS3615-SNS3655–300.ova file, 112
- ISE-2.70.356-virtual-SNS3655-SNS3695–1200.ova file, 112
- ISE-2.70.356-virtual-SNS3695–2400.ova file, 112
- ISE-PIC (ISE Passive Identity Connector), 157, 858
- ISR (Integrated Services Router), 613
- ISS (identity source sequence), 34, 202–204, 218, 319, 339, 472, 994
- Issued Certificates menu (ISE Certificate Authority), 520
- IT Users Access authorization rule, 252–256

**J**

Jabber, 825  
 JailBrokenStatus attribute, 536  
 Jamf Pro, 673, 708  
 Java applets, 85–86, 153, 322, 356  
 JGroups, 748  
 Jobs, Steve, 482  
 joining AD (Active Directory) domains, 197–202  
 Juniper, 45

**K**

Karelis, E. Peter, 753  
 Kerberos, 196, 469  
 key command, 264  
 keys. *See also* PKI (public key infrastructure)  
   EKU (extended key usage), 211  
   key pairs, 468–469, 995  
   MKA (MAC Security Key Agreement), 616  
   private, 468–469  
   public, 468–469, 998  
 Kpasswd, 196

**L**

L (Locality) field, 183  
 Lancope Stealthwatch. *See* Stealthwatch  
 LANs (local area networks)  
   EAP over LAN. *See* 802.1X  
   VLANs (virtual LANs), 726  
     assignment of, 551–553, 726  
     authentication VLAN, 87–88  
     dynamic interfaces for, 284–286  
     mapping to SGTs (security group tags), 580  
     segmentation with, 322  
   VACLs (VLAN Access Control Lists), 424, 425–426

Launch Page Level Help option (Help menu), 140  
 launch program remediations, 683  
 Layer 2 Security tab  
   corporate WLAN, 292–293  
   guest WLAN, 288  
 Layer 3 Security tab  
   corporate WLAN, 293  
   guest WLAN, 289  
 Layout Template command (Dashboard settings), 134  
 LDAP (Lightweight Directory Access Protocol), 23, 25–26, 196, 995  
 lease, posture, 691  
 left-zero-padded keyword, 621  
 library, Conditions Studio, 218  
 library conditions, 708  
 licensing, 155–158, 747–748  
 Lightweight Directory Access Protocol. *See* LDAP (Lightweight Directory Access Protocol)  
 Lightweight Directory Access Protocol (LDAP), 23, 25–26, 196, 995  
 Line-of-Business-1 SGT (Security Group Tag), 555  
 Line-of-Business-2 SGT (Security Group Tag), 555  
 Link encryption (MACsec), 156  
 Link Layer Discovery Protocol (LLDP), 98, 418  
 link remediations, 684  
 Linux KVM, 113  
 lists  
   ACLs (access control lists). *See* ACLs (access control lists)  
   CRLs (certificate revocation lists), 33, 466  
 Live Log, 766–771  
   Actions menu, 770  
   advanced filtering, 771  
   authentication details report, 771–774  
   Authorization Policy column, 767  
   Authorization Profiles column, 768

- blank lines in, 774–775
- Cisco ISE verification with, 302–303
- Client Stopped Responding counter, 768
- CWA (Centralized Web Authentication) verification from, 327
- Details icon, 768
- device administration AAA with Cisco IOS, 952–954
- Endpoint ID column, 767
- Endpoint Profile column, 767
- Identity column, 767
- IP Address column, 768
- MDM Server column, 768
- Misconfigured Network Devices counter, 768
- Misconfigured Supplicants counter, 768
- Network Device column, 768
- Quick Filters counter, 769
- RADIUS (Remote Access Dial-In User Service), 144–146
- RADIUS Drops counter, 768
- Record Selector, 770
- Refresh counter, 770
- Repeat counter, 767, 769
- Server column, 768
- status types, 767
- TACACS+, 147, 982–983
- Threat-Centric NAC, 146
- Time Selector, 770
- verification of BYOD flows with, 534
- Live Sessions, 776**
  - Cisco ISE verification with, 303
  - RADIUS (Remote Access Dial-In User Service), 145–146
- LLDP (Link Layer Discovery Protocol), 98, 418**
- load balancing**
  - IOS (Internetwork Operating System), 756–757
  - PSNs (Public Services Networks), 751–752
- LOBBY role, 972**
- local ACLs (access control lists), 268–269**
- local endpoint groups, 195**
- Local Logs support bundles, 783**
- local user identity groups, 194**
- local users, 195–196**
- Local Web Authentication. *See* LWA (Local Web Authentication)**
- Locality (L) field, 183**
- Location dashlet, 136**
- Location Services tab (Network Resources), 166**
- Log %temp%\spwProfileLog.txt command, 812**
- logging categories, 778–779**
- logging host command, 299**
- logging in to ISE (Identity Services Engine), 125–132**
  - Admin group roles, 127–132
  - Administration portal, 137–142
    - global search for endpoints, 139–140*
    - Help menu, 138, 140–141*
    - ISE Setup Wizards, 141*
    - Settings menu, 142*
    - tabs, 137–139*
  - daily guest accounts, 347
  - Home dashboards, 132–137
  - initial login, 125–126
  - self-registered guest portals, 367–368
  - social, 35
  - sponsored guest portals, 386
- logging monitor informational command, 299**
- logging origin-id ip command, 299**
- logging source-interface command, 299**
- logging synchronous command, 947**
- Logging tab (System), 159**
- logging targets, 743–744, 777–778**
- logical profiles, 441–442, 995**
- login authentication command, 947**
- Login Page Settings (Client Provisioning portal), 651–652**

**Logoff option, posture reassessment, 692**

**logout command, 932**

**logs, 159, 766–785**

debug, 779–784

*configuration, 779–780*

*downloading from GUI, 780*

*support bundles, 782–784*

*viewing from CLI, 781–782*

de-duplication of, 805–807

Live Log. *See* Live Log

Live Sessions, 776

logging categories, 744, 778–779

logging flows for, 743

logging targets for, 743–744, 777–778

**Lost option (endpoint management), 543**

**low-impact mode, 725–727**

**LWA (Local Web Authentication), 310–311**

with centralized portal, 84–85

definition of, 995

when to use, 84

## M

**MaaS360, 708**

**MAB (MAC Authentication Bypass)**

authentication with, 80–82, 227–228

configuration, 265, 270–274, 318

definition of, 717, 995

MAB rule flowchart, 217

overview of, 96–99

profiling, 96–99

*DHCP (Dynamic Host Configuration Protocol), 97*

*RADIUS (Remote Access Dial-In User Service), 97*

role-specific authorization rules, 241

wireless, 489

**MAC (Media Access Control) addresses**

identity management with, 20

MAB (MAC Authentication Bypass), 80–82, 995

*authentication with, 227–228*

*configuration, 265, 318*

*definition of, 717*

*MAB rule flowchart, 217*

*overview of, 96–99*

*profiling, 96–99*

*role-specific authorization rules, 241*

*wireless, 489*

Mac filtering on WLCs, 315

MACsec, 995

MAM (MAC Address Management)  
model, 451

MKA (MAC Security Key Agreement),  
616

URL-redirected MAC authentication  
bypass, 311–313

**MAC Filtering option, WLC (Wireless LAN Controller), 315**

**Mac OSX**

Console application, 812

onboarding flow, 531–533

*device provisioning, 532–533*

*device registration, 531*

**Machine Access Restriction (MAR), 472**

**Machine Authentication, 66, 545–546**

**macro-segmentation, 613**

**MACsec, 995**

definition of, 548

Downlink MACsec, 616–619

*authorization profile for, 616*

*ISE (Identity Services Engine)  
configuration, 619*

*policies, 616–618*

*switch configuration modes,  
618–619*

history of, 614–616

Multi-Hosts mode, 273, 298, 618, 995

Uplink MACsec, 619–623

**Maintenance tab (System), 159**

**Make Primary button, 738**

- malware**
  - anti-malware posture policy conditions, 661–663
  - anti-malware remediations, 681–682
- MAM (MAC Address Management) model, 451**
- Manage Dashboards command (Dashboard settings), 134**
- MANAGEMENT role, 971**
- manual SGT (security group tag) propagation, 595–597**
- manually assigning SGTs (security group tags), 577–578**
- Manufacturer attribute, 536**
- mapping**
  - subnets to SGTs (security group tags), 580
  - VLANs to SGTs (security group tags), 580
- MAR (Machine Access Restriction), 472**
- matrix view (TrustSec policy matrix), 553**
- Maximum Access Time setting**
  - contractor accounts, 344
  - daily guest accounts, 347
  - weekly guest accounts, 347
- Maximum Privilege option (TACACS profile), 933**
- Maximum Simultaneous Logins setting, 345**
- MD5 algorithm, 43, 46, 214**
- MDA (Multidomain Authentication), 273, 298, 618, 995**
- MDM (mobile device management), 820–821. *See also* BYOD (bring your own device) onboarding**
  - definition of, 995
  - dictionary, 708–709
  - onboarding
    - administrative management, 545*
    - advantages of, 535–536*
    - attributes in authorization policies, 536–537*
    - definition of, 487*
    - endpoint management, 542–543*
    - integration configuration, 537–538*
    - onboarding rule configuration, 539–542*
    - self-management, 543–544*
  - overview of, 101–102
  - posture assessment with, 108
  - supported features, 101–102
  - vendors, 101–102
- MDM Server column (Live Log), 768**
- MDM\_Compliant authorization rule, 709, 711**
- MDM\_Detailed\_Posture condition, 710**
- MDM\_NotCompliant authorization rule, 711**
- MDM\_NotCompliant condition, 709–710**
- MDM\_NotReachable authorization rule, 710**
- MDMFailureReason attribute, 537**
- MDMServerName attribute, 537**
- MDMServerReachable attribute, 537, 712**
- Media Access Control. *See* MAC (Media Access Control) addresses**
- MEID attribute, 537**
- Meraki Systems Manager (Meraki SM), 708**
- meshed SXP (SGT Exchange Protocol), 582–583**
- messages**
  - CoA (Change of Authorization), 110, 311
  - RADIUS, 13–14
    - accounting messages, 13*
    - authentication messages, 13*
    - authorization messages, 13*
  - syslog, 299–300
  - TACACS+
    - accounting messages, 11*
    - authentication messages, 9*
    - authorization messages, 10–11*
    - communication flows, 12*
- Metrics dashlet, 134**
- MFA (multifactor authentication), 26–29**
- micro-segmentation, 614**

- Microsoft Active Director. *See* AD (Active Directory)
- Microsoft CHAP. *See* MS-CHAP (Microsoft CHAP)
- Microsoft Edge, 122
- Microsoft Hyper-V, 113
- Microsoft Internet Explorer, 122
- Microsoft Intune, 673, 708
- Microsoft Remote Procedure Call (MSRPC), 196
- Miller, Darrin, 633
- Misconfigured Network Devices counter, 768
- Misconfigured Suppliants counter, 768
- MKA (MAC Security Key Agreement), 616
- MnT (Monitoring and Troubleshooting)
  - admin role, 127
- MnT (Monitoring and Troubleshooting) nodes, 109–110, 743–744, 912
  - Dedicated MNT, 742
  - definition of, 995
  - logging categories, 744
  - logging flows, 743
  - logging targets, 743–744
  - sending syslog messages to, 299
- mobile device management. *See* MDM (mobile device management)
- Mobile Device Management portal, 168
- Mobile Iron UEM, 708
- mobile posture, 707–712
  - authorization conditions, 709–710
  - authorization rules, 710–712
  - supported device managers, 707–709
- Mobile Preview pane (portal page customization), 358
- Mobility license packages, 156
- Mobility Upgrade license packages, 157
- Model attribute, 537
- modes
  - closed, 728–730
  - low-impact, 725–727
  - monitor, 722–725
    - flow diagram*, 723–724
    - operational flow*, 722–723
    - policy set creation*, 724–725
    - transitioning to end state*, 730–731
- modify device capabilities, 101
- modules, compliance, 637–638
- monitor mode, 722–725
  - flow diagram*, 723–724
  - operational flow*, 722–723
  - policy set creation*, 724–725
  - transitioning to end state*, 730–731
- MONITOR role, 972
- monitor session command, 425
- Monitoring and Reporting Logs support bundles, 783
- Monitoring and Troubleshooting nodes. *See* MnT (Monitoring and Troubleshooting) nodes
- Monitoring persona, 109–110, 737
- Mozilla Firefox, 122
- MS-CHAP (Microsoft CHAP), 43, 45, 46
- MSE integration, 156
- MSRPC (Microsoft Remote Procedure Call), 196
- Multi-Auth (Multiauthentication), 273, 298, 618, 995
- Multidomain Authentication (MDA), 273, 298, 618, 995
- multifactor authentication (MFA), 26–29
- multi-hop, 582
- Multi-Hosts mode (MACsec), 273, 298, 618, 995
- multi-node deployment. *See* cubes, ISE
- Multiple Hosts (Multi-Hosts), 273, 298
- must-not-secure policy (MACsec), 616, 618
- must-secure policy (MACsec), 616, 618
- My Devices portal, 168, 543–544
- MyDevices\_Portal\_Sequence, 544

## N

- NAC (network access control) projects, 258. *See also* AAA (authentication, authorization, and accounting)
- NAC (Network Admission Control), 626, 630
  - NAC Appliance, 631–633
  - “NAC Framework” solution, 630
- NAC Managers tab (Network Resources), 165
- NADs (network access devices), 7, 107. *See also* authorization
  - configuration, 917
    - ACLs (*access control lists*), 492–495
    - for BYOD onboarding, 489–495
    - connection settings, 918
    - identities, 920
    - network resources, 921–922
    - overview of, 916–917
    - password change control, 918
    - policy elements, 922–924
    - policy sets, 925–927
    - reports, 927
    - Session Key Assignment, 918
    - UI navigation for, 919–920
    - WLAN configuration, 490–491
  - CWA (Centralized Web Authentication) verification, 327–331
    - client details, viewing on WLC, 329–331
    - show commands on wired switch, 328–329
  - definition of, 113, 996
  - enforcement types for, 50
  - ISE initial configuration, 192
  - role of, 49–50
  - TrustSec-enabled
    - defining TrustSec settings for, 559
    - PACs (*Protected Access Credentials*), 558–559
  - verification of, 296–302
    - with Cisco switches, 296–299
    - with Cisco WLC (*Wireless LAN Controller*), 300–302
    - with syslog messages, 299–300
- NAM (Network Access Manager), 991
- named ACLs, 244
- NAP (Network Access Protection), 626
- NAS-Port-Id attribute (RADIUS), 415
- NAS-Port-Type attribute (RADIUS), 415
- National Security Agency, 868
- native EAP (Extensible Authentication Protocol), 43–44, 996
- native SGT (security group tag) propagation, 593–597
- native supplicant profile, 510–512, 642
- native tagging, 593–597
  - configuration on IOS XE switches, 595–597
  - Layer 2 frame format with, 593–594
  - pervasive tagging, 594
- NDAC (Network Device Admission Control), 566, 996
- NDES (Network Device Enrollment Services), 520
- NDGs (network device groups), 192–194, 720–721, 996
- NDS (Novell Directory Services), 25
- NEA (Network Endpoint Assessment), 626
- net-admin group, 945
- NetAdmin profile, 974–975
- NETFLOW probe, 419–420
- NetIQ eDirectory. *See* AD (Active Directory)
- netsh ras set tracing \* enable command, 296
- network access AAA, 3, 7, 996
- network access control (NAC) projects, 258. *See also* AAA (authentication, authorization, and accounting)
- network access devices. *See* NADs (network access devices)
- Network Access Manager (NAM), 809, 991
- Network Access Protection (NAP), 626

- network access users, 21
- Network Administrator command set, 943
- Network Administrator role, 939
- Network Admission Control. *See* NAC (Network Admission Control)
- Network device admin role, 128
- Network Device Admission Control (NDAC), 566, 996
- Network Device column (Live Log), 768
- Network Device Enrollment Services (NDES), 520
- network device groups (NDGs), 720–721, 996
- Network Device Groups tab (Network Resources), 164–165
- Network Device Profiles tab (Network Resources), 165
- network device troubleshooting, 812–815. *See also* device administration AAA
  - client details, viewing on WLC, 813–814
  - debug commands, 815
  - show authentication interface command, 812–813
- Network Devices dashlet, 134, 135
- Network Devices tab, 143, 163–164
- Network Devices widget, 454
- Network Endpoint Assessment (NEA), 626
- Network Groups view, Cisco AnyConnect NAM supplicant, 60, 71
- Network Infrastructure SGT (Security Group Tag), 555
- network interface cards (NICs), 97
- network probes. *See* probes
- Network Resources tab (Administration screen), 163–166
  - External MDM tab, 165
  - External RADIUS Servers tab, 165
  - Location Services tab, 166
  - NAC Managers tab, 165
  - Network Device Groups tab, 164–165
  - Network Device Profiles tab, 165
  - Network Devices tab, 163–164
  - RADIUS Server Sequences tab, 165
- Network Resources tab (Device Administration), 921–922
- network scan (Nmap), 415–417
- Network Services Platform. *See* NSP (Network Services Platform)
- Network Services SGT (Security Group Tag), 555
- Network Setup Assistant app, 282, 507
- Network Time Protocol (NTP), 32, 196, 465, 996
- Networks view, Cisco AnyConnect NAM supplicant, 60, 62–70
  - Certificates tab, 67
  - Connection Type tab, 66
  - Credentials tab, 68–70
  - Machine Auth tab, 66
  - PAC Files tab, 67–68
  - Security Level tab, 64–66
  - User Auth tab, 68–69
- NGFWs (next-generation firewalls), 818
- NICs (network interface cards), 97
- Nmap (network scan), 415–417
- No Escape option (TACACS profile), 933
- nodes
  - configuration in distributed environment, 737–742
    - ISE cubes*, 737
    - ISE persona types*, 737
    - node personas*, 742
    - PPAN (Policy Administration Node)*, 738–739
    - primary devices*, 738–739
    - registration of ISE nodes*, 739–742
  - definition of, 109, 996
  - MnT (Monitoring and Troubleshooting), 109–110, 743–744
    - Dedicated MNT*, 742
    - definition of*, 995
    - logging categories*, 744

- logging flows*, 743
  - logging targets*, 743–744
  - sending syslog messages to*, 299
  - node groups, 748–750, 996
  - PAN (Policy Administration node), 109, 745–748
    - auto PAN switchover*, 745–746
    - automatic failover for*, 746
    - definition of*, 997
    - promoting to primary*, 745
  - PSN (Policy Services node), 110, 633, 874–876
  - single-node ISE deployment, 113
  - two-node ISE deployment, 114–116
  - non-802.1X authentication**
    - devices without a supplicant, 79–80
    - EasyConnect, 89–90, 993
    - MAB (MAC Authentication Bypass). *See* MAB (MAC Authentication Bypass)
    - need for, 76
    - remote access connections, 88–89
    - Web Authentication. *See* WebAuth (Web Authentication)
  - non-seed devices**, 567–571, 996
  - non-tunneled EAP (Extensible Authentication Protocol)**, 43–44
  - north-south SGACL deployment**, 598–599
  - Not MACsec capable**, 617–618
  - notification services**, 388–389
    - SMS gateway providers, 388–389
    - SMTP servers, 388
  - Novell Directory Services (NDS)**, 25
  - NSP (Network Services Platform)**
    - NSP ACL (access control list), 493, 495
    - NSP app download, 528–529
  - NTP (Network Time Protocol)**, 32, 196, 465, 996
- O**
- O (Organization) field**, 183
  - objects, AD (Active Directory)**, 24
  - OCSP (Online Certificate Status Protocol)**, 33, 466, 519, 996
  - onboarding**. *See* BYOD (bring your own device) onboarding; MDM (mobile device management)
  - one-time password (OTP)**, 29, 88, 996
  - Online Certificate Status Protocol (OCSP)**, 33, 466, 519, 996
  - open virtual appliances (OVAs)**, 112
  - Operate on non-802.1X wireless networks setting (AnyConnect posture profile)**, 645
  - Operations screen**, 142, 143–150
    - ANC (Adaptive Network Control) component, 147–148, 991
    - RADIUS tab, 144–146
    - Reports tab, 150
    - TACACS Live Log tab, 147
    - Threat-Centric NAC Live Logs tab, 146
    - Troubleshoot tab, 147–148
  - operators**
    - AND, 252–256
    - OR, 252–256
  - option name host-name command**, 426
  - OR operator**, 252–256
  - Oracle Identity Manager**, 25
  - Organization (O) field**, 183
  - organizational units (OUs)**, 25, 183
  - organizationally unique identifiers (OUIs)**, 97
  - OS option (Nmap)**, 416
  - OSCP (Online Certificate Status Protocol)**, 519
  - OSVersion attribute**, 537
  - OTA (over-the-air) provisioning**, 492
  - OTP (one-time password)**, 29, 88, 996
  - OUIs (organizationally unique identifiers)**, 97
  - OUs (organizational units)**, 25, 183
  - OVAs (open virtual appliances)**, 112
  - over-the-air (OTA) provisioning**, 492
  - Overview menu (ISE Certificate Authority)**, 520
  - OWN\_ACCOUNTS sponsor group**, 382

## P

- PAC Files tab (Cisco AnyConnect NAM supplicant), 67–68
- packages
  - AnyConnect headend deployment
    - AnyConnect configuration, building*, 648–649
    - posture profile configuration*, 644–648
    - uploading to ISE*, 642–644
  - licensing, 155–158
- pACLs (port-based ACLs), 725
- PACs (Protected Access Credentials), 45, 546, 558–559, 997
- PAN (Policy Administration node), 109, 519, 738–739, 745–748
  - auto PAN switchover, 745–746
  - automatic failover for, 746
  - definition of, 997
  - promoting to primary, 745
- PAP (Password Authentication Protocol), 7, 46, 214
- Parameter-Request-List attribute (DHCP), 411
- Pass Live Log status, 767
- PASS\_ADD message, 10–11
- PASS\_REPL message, 11
- passive identity service, 110
- PassiveID Setup option (Admin portal), 138
- pass-through mode, 752
- Password Authentication Protocol (PAP), 46, 214
- Password Change Control (Device Administration), 918
- passwords
  - guest change password settings, 371–372
  - OTP (one-time password), 29, 88, 996
- patch management, 685, 757–759
  - conditions for, 100, 673–675
  - remediations, 685
- PCI (Payment Card Industry), 551
- PEAP (Protected EAP), 44–45, 48–49, 53–54, 55–56, 108, 215
- Pearson Test Prep software, 989
- peering, 582
- PEM (Privacy Enhanced Electronic Mail) format, 186–187, 833
- Perfigo, 631
- permit statement, 280, 314, 316
- PERMIT\_ALL\_IPV4\_TRAFFIC authorization rule, 241–243
- Permit\_HTTP\_HTTPS SGACL, 601–602, 607
- Permit\_ICMP SGACL, 602–603
- Permit\_Mgmt SGACL, 601, 607
- Permit\_SRC\_HTTP\_HTTPS SGACL, 603–604
- Permit\_WEB\_RDP SGACL, 598
- per-profile CoA (Change of Authorization), 443–444
- personas
  - Administration, 109, 737
  - definition of, 108–109, 997
  - ISE nodes and, 742
  - Monitoring, 109–110, 737
  - Policy Services, 110, 737
  - pxGrid, 111, 737
  - types of, 737
- pervasive tagging, 594
- phased deployment, 717–718
  - authentication open versus 802.1X, 719–720
  - closed mode, 728–730
  - low-impact mode, 725–727
  - monitor mode, 722–725
    - flow diagram*, 723–724
    - operational flow*, 722–723
    - policy set creation*, 724–725
    - transitioning to end state*, 730–731
  - preparation for, 720–721
  - transitioning to end state, 730–731
  - wireless networks, 731

- PhoneNumber attribute, 537
- physical ISE appliances, 111–113
  - form factors for, 111–112
  - scalability of, 112–113
- PIN Lock option (endpoint management), 543
- ping, 646
- PinLockStatus attribute, 536
- PKI (public key infrastructure), 519. *See also* certificate-based authentication
  - definition of, 463, 998
  - encryption with, 468–469
  - key pairs, 468–469, 995
  - prevalence of, 460
  - public versus private keys in, 468–469
  - RAs (registration authorities), 998
  - signatures, 31–32
  - smart cards, 29
- Platform Exchange Grid. *See* pxGrid (Platform Exchange Grid)
- Plus license packages, 156
- Point-to-Point Protocol. *See* PPP (Point-to-Point Protocol)
- Point-to-Point Protocol (PPP), 12
- policies and policy sets. *See also* posture assessment; profiles
  - ANC (Adaptive Network Control), 148–149, 156, 822–823, 864–866
  - AUP (acceptable use policy)
    - hotspot guest portals, 354–356
    - sponsored guest portals, 386
- authentication, 151
  - allowed protocols, 210, 213–216
  - for alternative ID stores based on EAP type, 224–227
  - authorization compared to, 209–210, 235
  - for certificate-based authentication, 472–474
  - conditions, 217–219
  - default, 216–217
  - definition of, 171
  - device administration, 944
  - for device administration AAA with Cisco IOS, 944
  - goals of, 206–207, 210–211
  - identity stores, 210–211, 219–220
  - identity validation, 211
  - for MAB (MAC Authentication Bypass), 227–228
  - options, 220
  - for remote access VPN, 223–224
  - restoring, 229
  - for wireless SSID, 220–223
- authorization, 151
  - authentication compared to, 209–210, 235
  - Blackhole\_Wireless\_Access, 240–241
  - for certificate-based authentication, 474–475
  - Cisco\_IP\_Phones, 237–241
  - compound conditions, 239, 251–256, 992
  - condition blocks, 252–256
  - configuration of, 241–249
  - for CWA (Centralized Web Authentication), 322–324
  - default, 236–241
  - definition of, 171
  - device administration, 945–946
  - for device administration AAA with Cisco IOS, 945–946
  - goals of, 235–241
  - for guest portals, 348–351
  - for MDM (mobile device management), 536–537
  - organization of, 216, 236
  - profile assignment in, 450–453
  - role-specific authorization rules, 241
  - rule processing for, 236–241
  - saving conditions for reuse in, 249–251
  - simple conditions, 239, 251, 999

- BYOD (bring your own device) onboarding
  - client provisioning policy*, 512–514
  - default unavailable client provisioning policy*, 515
- Cisco AnyConnect NAM supplicant
  - Authentication Policy view*, 60, 62
  - Client Policy view*, 60, 61–62
- Cisco WLC (Wireless LAN Controller), 974–979
- CiscoPress SSID, 518
- closed mode, 730
- correlation, 845–847
- CPP (client provisioning policy), 637–638
  - AnyConnect Secure Mobility Client*, 640–649
  - Client Provisioning portal*, 153, 166–167, 650–651
  - default client provisioning policy*, 652
  - definition of*, 172
  - for ISE for BYOD onboarding*, 512–514, 515
  - order of operations*, 637–638
  - rules, creating*, 652–653
- default, 211
- device administration, 922–924, 925–927, 939–946
  - policy sets*, 943–946
  - roles*, 939
  - TACACS command sets*, 922–923, 941–943
  - TACACS profiles*, 923–924, 939–941
- Endpoint Profile Policies, 431–441
- endpoint purge, 345
- expanding, 211
- for hotspot guest portals, 362–364
- low-impact mode, 727
- MACsec, 616–618
- monitor mode, 724–725
- for self-registered guest portals, 373–380
- SGTs (security group tags), 577, 612
- “smart default”, 318
- top-level rules of, 212
- TrustSec
  - egress policy*, 597–598
  - policy matrix*, 600–601, 604–609
- WSA (Web Security Appliance), 855–857
  - access policy*, 855–856
  - decryption policy*, 857
- Policy admin role**, 128
- Policy Administration node**. *See* PAN (Policy Administration node)
- policy configuration support bundles**, 783
- Policy List tab**, 149
- Policy page**, 138, 142, 150–154
  - Client Provisioning tab, 153
  - Policy Elements tab, 154, 922–924
  - Policy Sets tab, 150–151
  - Posture tab, 152
  - Profiling tab, 152
- Policy Service nodes (PSNs)**, 110, 210, 519, 633
- Policy Services persona**, 110, 737
- Policy Sets tab**, 150–151, 925–927
- policy static sgt command**, 578, 595, 596
- portals**
  - Administration, 137–142
    - global search for endpoints*, 139–140
    - Help menu*, 138, 140–141
    - ISE Setup Wizards*, 141
    - Settings menu*, 142
    - tabs*, 137–139
  - authorization policies for, 348–351
  - definition of, 997
  - guest types, 341–342
    - contractors*, 344–346
    - daily*, 344–346
    - overview of*, 343
    - social*, 348
    - weekly*, 347
  - hotspot, 341–342, 351–358

- AUP (acceptable use policy) page settings*, 354–356
- authentication success settings*, 357
- authorization rule configuration*, 362–365
- configuration flowchart for*, 351
- definition of*, 342
- portal page customization*, 358–362
- portal settings*, 352–354
- post-access banner page settings*, 355–356
- support information page settings*, 357–358
- VLAN DHCP release page settings*, 355–356
- overview of, 341
- self-registered, 366–367
  - authorization rule configuration*, 373–380
  - BYOD settings*, 372
  - configuration flowchart*, 365–366
  - definition of*, 342
  - guest change password settings*, 371–372
  - guest device compliance settings*, 373
  - guest device registration settings*, 371–372
  - guest location setting*, 369–371, 994
  - login page settings*, 367–368
  - portal settings*, 366–367
  - registration form settings*, 368–371
  - self-registration success*, 371
- sponsored, 380–381, 385–386
  - AUP (acceptable use policy) page settings*, 386
  - configuration flowchart*, 380–381
  - default sponsor portal*, 384
  - definition of*, 342
  - login settings*, 386
  - other settings*, 387
  - portal settings*, 385–386
  - provisioning guest accounts from*, 389–394
- Portals & Components tab (Guest Access work center)**. *See* portals
- port-control command**, 276
- ports**
  - 802.1X default port behavior, 719
  - application of initial ACL to, 275–276
  - assigning SGTs (security group tags) to, 577–578
  - configuring interfaces as, 269
  - host mode, 272–274
  - pACLs (port-based ACLs), 725
  - ports, 273
  - security, 273, 997
  - switch
    - configuring interfaces as*, 269
    - host mode*, 272–274
- TCP**
  - port 49*, 8
  - port 389*, 25
  - port 636*, 25
  - port 64999*, 580
- UDP**, 32
- POST method**, 84–85
- post-access banner page settings**, 355–356
- Posture Agent Redirection ACL**, 283–284
- posture assessment**. *See also* posture policy
  - authorization rules, 693–694
  - centralization of, 629
  - compliance module updates, 637–638
  - conditions for, 99–100, 997
  - CPP (client provisioning policy)
    - configuration, 637–638
    - AnyConnect Secure Mobility Client*, 640–649
    - Client Provisioning portal*, 650–651
    - default client provisioning policy*, 652
    - order of operations*, 637–638
    - rules, creating*, 652–653

- definition of, 172, 626, 997
- endpoint experience, 695–705
  - AnyConnect already installed, endpoint not compliant*, 700–702
  - AnyConnect not installed on endpoint yet*, 696–700
  - redirected state*, 695–696
  - stealth mode*, 645, 703
  - temporal agent and posture compliant*, 705
- history of, 629–633
- ISE posture flows, 107–110, 633–636
- license packages, 156
- mobile posture, 707–712
  - authorization conditions*, 709–710
  - authorization rules*, 710–712
  - supported device managers*, 707–709
- overview of, 99–101
- Posture General Settings, 690–691
- posture lease concept, 691
- posture requirements, 997
- Posture Troubleshooting tool, 794–795
- Posture work center
  - Cache Last Known Posture Compliance setting*, 691
  - Posture General Settings*, 690–691
  - posture lease*, 691
  - posture reassessment*, 691–692
- profiling versus, 402
- remediation, 997
- posture policy, 653–688**
  - conditions, 654–679
    - anti-malware*, 661–663
    - anti-spyware*, 663
    - anti-virus*, 663
    - application*, 655–660
    - compound*, 677–678
    - dictionary compound*, 664–665
    - dictionary simple*, 663–664
    - disk encryption*, 665–666
    - file*, 667–673
    - firewall*, 660–661
    - hardware attributes*, 655
    - patch management*, 673–675
    - Registry*, 675
    - USB*, 679
  - configuration, 688–689
  - relationships between elements of, 653
  - remediations, 679–686
    - anti-malware*, 681–682
    - anti-spyware*, 681–682
    - anti-virus*, 681–682
    - application*, 680
    - definition of*, 679–680
    - file*, 682
    - firewall*, 682
    - launch program*, 683
    - link*, 684
    - patch management*, 685
    - USB*, 686
    - WSUS (Windows Server Update Services)*, 685
  - requirements, 687–688
- posture profiles, 644–648**
- Posture tab (Policy page), 152
- PoV (proof of value) service, 138
- PPAN (Policy Administration Node), 738–739
- PPP (Point-to-Point Protocol), 12
- PRA retransmission time setting, 647
- Preboot Execution Environment (PXE), 725
- primary devices, 738–739
- primary PAN (Policy Administration node), 745
- principle username X.509 attribute, 470, 997
- Privacy Enhanced Electronic Mail (PEM) format, 186–187, 833
- private keys, 468–469, 997
- privilege levels, 932–933, 997
- probe delay command, 267

**probes, 409–423**

- Active Directory, 422
- configuration, 409–411
- DHCP and DHCPSPAN, 411–414
- DNS, 417
- HTTP, 420–421
- NETFLOW, 419–420
- Nmap, 415–417
- publishing endpoint probe data on pxGrid, 450
- pxGrid, 423
- RADIUS, 414–415
- SNMPQUERY and SNMPTRAP, 417–419

**Process Host Lookup, 214****Profiled Cisco IP Phones rule, 237****Profiler Feed Service, 429–430**

- configuration, 429
- verification of, 429–430

**profiles, 884–886, 923–924. See also profiling**

- AMP Enabler, 642
- AnyConnect NAM, 71–72
- assignment in authorization policies, 450
  - endpoint identity groups, 450–452*
  - EndPointPolicy, 453*
- BYOD (bring your own device)
  - onboarding, 510–512, 516
- CAPs (certificate authentication profiles), 23, 202, 469, 471–472, 991
- Cisco WLC (Wireless LAN Controller)
  - Employee, 977*
  - Helpdesk, 976*
  - NetAdmin, 974–975*
  - predefined TACACS profiles, 974*
  - SecAdmin, 975–976*
- configuration, 320–322
- device administration AAA with Cisco IOS, 932–934, 939–941
  - Administration profile, 940–941*
  - HelpDesk profile, 940*
- Downlink MACsec, 616

- Employee Full Access, 241–243

- Employee\_Limited, 246–249

- for hotspot guest portals, 362–364

- Internet\_Only, 243–246

- license packages, 156

- logical, 441–442, 995

- MDM Onboard, 539–540

- native supplicant, 642

- for posture assessment, 693

- for self-registered guest portals, 373–380

- verification of

- dashboard, 454*

- Device Sensor show commands, 457–458*

- endpoints database, 455–456*

- Global Search tool, 454–455*

- WSA (Web Security Appliance), 855–857

**profiling, 107, 404–406. See also profiles**

- Anomalous Behaviour Detection, 406–408

- Cisco ISE probes, 409–423

- Active Directory, 422*

- configuration, 409–411*

- DHCP and DHCPSPAN, 411–414*

- DNS, 417*

- HTTP, 420–421*

- NETFLOW, 419–420*

- Nmap, 415–417*

- publishing endpoint probe data on pxGrid, 450*

- pxGrid, 423*

- RADIUS, 414–415*

- SNMPQUERY and SNMPTRAP, 417–419*

- CoA (Change of Authorization) and, 442–444

- global CoA, 442–443, 994*

- per-profile CoA, 443–444*

- custom attributes, 445–448

- definition of, 172, 995

- DHCP (Dynamic Host Configuration Protocol), 98

- evolution of, 404–406
- global settings for, 444–445
  - endpoint attribute filtering*, 444–445
  - SNMP*, 444
- infrastructure configuration, 424–427
  - DHCP helper*, 424
  - IOS Device Sensor*, 426–427
  - SPAN (Switched Port Analyzer)*, 424–425
  - VACLs (VLAN Access Control Lists)*, 425–426
  - VMware vSwitches*, 427
- MAB (MAC Authentication Bypass), 80–82, 96–99
  - DHCP (Dynamic Host Configuration Protocol)*, 97
  - RADIUS (Remote Access Dial-In User Service)*, 97
- posture versus, 402
- Profiler Feed Service, 429–430
  - configuration*, 429
  - verification of*, 429–430
- Profiling tab (Policy page)**, 152
- Promote to Primary option**, 745
- proof of value (PoV) service**, 138
- Protected Access Credentials (PACs)**, 45, 546, 558–559, 997
- Protected EAP (PEAP)**, 44–45, 48–49, 53–54, 55–56, 215
- provisioning**. *See also* **CPP (client provisioning policy)**
  - PACs (Protected Access Credentials), 558–559
  - supplicant provisioning reports, 534–535
- PSNs (Policy Service nodes)**, 110, 210, 519, 633, 874–876
- PSNs (Public Services Networks)**, 210, 519
  - for large deployments, 912
  - load balancing, 751–752
  - for medium deployments, 913
  - for small deployments, 913
- public certificates, importing**, 476–477
- public key infrastructure**. *See* **PKI (public key infrastructure)**
- public keys**, 468–469, 998
- Public Services Networks**. *See* **PSNs (Public Services Networks)**
- publish and subscribe (pub/sub) communication bus**, 111
- publishers**, 824, 998
- purge policies, endpoint**, 345
- Push Notification (Apple)**, 101
- PXE (Preboot Execution Environment)**, 725
- pxGrid (Platform Exchange Grid)**, 169, 190
  - communication between participants, 826–827
  - components of, 824, 825
  - Context-In, 827, 992
  - Context-Out, 827, 993
  - definition of, 998
  - FMC (Firepower Management Center)
    - configuration, 831–850
    - access rules*, 840–844
    - active users, viewing*, 844–845
    - FDM (Firepower Device Management)*, 832
    - pxGrid integration*, 832–837
    - Rapid Threat Containment*, 845–850
    - realms*, 837–840
  - GCL (pxGrid common library), 825
  - ISE (Identity Services Engine)
    - configuration, 828–831
  - license packages, 156
  - overview of, 824–825
  - password-based account creation, 837
  - persona, 111, 737
  - publishing endpoint probe data on, 450
  - pxGrid probe, 423
  - Stealthwatch, 857–866
    - capabilities of*, 858
    - ISE integration*, 862–866
    - pxGrid client identity certificate, importing*, 859–862

- version history, 825
- WSA (Web Security Appliance)
  - configuration, 850–857
    - access policy*, 855–856
    - decryption policy*, 857
    - ERS (External RESTful Services)*, 850–853
    - identification profiles*, 855–857
    - integration with pxGrid and ISE*, 850–855
    - policies*, 855–857

- pxGrid common library (GCL), 825
- pxGrid Services tab (Administration screen), 169
- pxGrid\_Certificate\_Template, 520

## Q

- Quarantine action (EPS), 821
- Quick Filters counter, 769

## R

- RADIUS (Remote Access Dial-In User Service), 12–14
  - AV (attribute/value) pairs, 15
  - CoA (Change of Authorization)
    - CWA (Centralized Web Authentication) and*, 311
    - definition of*, 16, 95–96
    - messages*, 110
  - definition of, 998
  - for device administration, 927
  - Drops counter, 768
  - fallback, 279–280
  - global configuration commands, 262–269
    - device tracking in IOS Xe 16.x and later*, 267
    - global 802.1X commands*, 266–267
    - IOS 12.2.x*, 262–263, 264–266
    - IOS 15.x*, 263–266

- IOS XE*, 263–266
  - local ACL (access control list) creation*, 268–269
- Layer 2 EAP communication with, 12–13
- Live Log. *See* Live Log
- Live Sessions, 145–146, 303
- message types, 13–14
- profiling, 97
- RADIUS Authentication Troubleshooting tool, 785–786
- RADIUS over Datagram Transport Layer Security (DTLS), 190
- RADIUS probe, 414–415
  - with remote-access VPN, 88
  - role of, 107
  - server configuration
    - accounting servers*, 278–279
    - authentication servers*, 277–278
  - service-type values, 13
  - TACACS+ compared to, 13, 16
  - token servers, 23
- radius server command, 263, 561
- RADIUS Server Sequences tab (Network Resources), 165
- RADIUS tab (Operations screen), 144–146
- radius-server attribute command, 264, 265
- radius-server dead-criteria time 5 tries 3 command, 264
- radius-server host command, 263
- radius-server load-balance command, 757
- radius-server vsa send accounting command, 265, 562, 567
- radius-server vsa send authentication command, 265, 562, 567
- ransomware, WannaCry, 554–555, 868
- Rapid Threat Containment, 821–823
  - ANC (Adaptive Network Control), 822–823
  - configuration, 845–850
  - definition of, 998
  - EPS (Endpoint Protection Services), 821–822, 993

- RAs (registration authorities), 998
- RBAC (role-based access control), 128, 934, 971. *See also* WLC (Wireless LAN Controller)
- Read-only admin role, 129
- Realm Directory configuration, 838
- realms, configuration in FMC (Firepower Management Center), 837–840
- reassessment, posture, 691–692
- Record Selector, 770
- redirected state, 695–696
- redistribute static route-map STATIC-TO-EIGRP command, 756
- Refresh counter, 770
- Registrar, 8
- registration authorities (RAs), 998
- registration form, self-registered guest portals, 368–371
- Registry conditions, 100, 675
- RegistryKey option, 675–676
- RegistryValue option, 675
- RegistryValueDefault option, 675–676
- Reinstate option (endpoint management), 543
- REJECT message, 9
- Reject option, authentication policy, 220
- reload command, 946
- remediation
  - posture, 679–686, 692, 997
    - anti-malware*, 681–682
    - anti-spyware*, 681–682
    - anti-virus*, 681–682
    - application*, 680
    - definition of*, 679–680
    - file*, 682
    - firewall*, 682
    - launch program*, 683
    - link*, 684
    - patch management*, 685
    - USB*, 686
    - WSUS (Windows Server Update Services)*, 685
  - Rapid Threat Containment, 845–850
    - ANC (Adaptive Network Control)*, 822–823
    - EPS (Endpoint Protection Services)*, 821–822, 993
- remediation timer, 645, 691
- remote access connections, 88–89
- Remote Access Dial-In User Service. *See* RADIUS (Remote Access Dial-In User Service)
- remote access VPN (virtual private network), 223–224
- Repeat counter, 767, 769
- replication, 748
- REPLY message, 9
- reports
  - authentication details, 771–774
  - Device Administration, 927
  - supplicant provisioning, 534–535
  - TC-NAC (Threat Centric Network Access Control)
    - Coa-Events*, 888–889
    - TC-NAC Live Log*, 888–889
    - Threat-Events*, 888
    - Vulnerability Assessment*, 888
- Reports tab (Operations screen), 150
- repositories, Tenable.SC, 881–882
- REQUEST message, 10, 11
- requests for comments. *See* RFCs (requests for comments)
- RESPONSE message, 10, 11
- restore, 229, 759–761
- Results tab (Policy Elements), 154
- reuse, saving conditions for, 249–251
- revoked certificates, 33
  - checking for, 466–467
  - CRLs (certificate revocation lists), 33, 466
  - OCSP (Online Certificate Status Protocol), 33, 466, 996
  - validity period, 467
- RFCs (requests for comments)
  - RFC 5176, 106

- RFC 5281, 48
- RFC 6238, 29
- RFC 7170, 46–47, 48
- role-based access control (RBAC)**, 128, 934, 971. *See also* WLC (Wireless LAN Controller)
- roles**
  - Admin, 127–132
  - Cisco WLC (Wireless LAN Controller), 971–972
  - device administration AAA with Cisco IOS, 939
  - role-specific authorization rules, 241
- route redistribution**, 755–756
- routed mode**, 752
- RSA SecurID**, 23
- rules**, 239. *See also* policies and policy sets
  - authentication, 151
    - alternative ID stores based on EAP type*, 224–227
    - MAB rule flowchart*, 217
    - organization of*, 216
    - policy sets*, 211–212
    - remote access VPN*, 223–224
    - wireless SSIDs (service set identifiers)*, 220–223
  - authorization, 151
    - AND/OR operators in*, 252–256
    - for BYOD (bring your own device) onboarding*, 517, 518
    - for device administration AAA with Cisco WLC*, 977–979
    - Employee and CorpMachine*, 242–243
    - employee full access*, 241–243
    - employee limited access*, 246–249
    - for guest portals*, 348–358
    - Internet-only access*, 243–246
    - IT Users Access*, 252–256
    - MDM On-boarding*, 539–542
    - mobile posture*, 710–712
    - PERMIT\_ALL\_IPV4\_TRAFFIC*, 241–243

- for posture assessment*, 693–694
- role-specific*, 241
- for self-registered guest portals*, 373–380
- TC-NAC (Threat Centric Network Access Control)*, 884–886
- Wireless Black List Default*, 239
- correlation, 845–847
- CPP (client provisioning policy), 652–653
- CWA (Centralized Web Authentication)
  - custom authorization rules*, 323–324
  - Guest Flow attribute*, 323–324, 994
  - preconfigured authorization rules*, 322
- Profiled Cisco IP Phones, 237
- Run SMB Discovery Script option (Nmap)**, 416
- Russell, Paul**, 337

## S

- Sales SGT (Security Group Tag)**, 555
- SAML (Security Assertion Markup Language)**
  - assertions, 395, 998
  - guest portal logins, 368, 394–400
  - IdPs (identity providers), 35, 394–400, 998
  - SPs (service providers), 394, 998
  - support for, 23
- SANs (subject alternative names)**, 184–185, 752
- SAP (Security Association Protocol)**, 616
- sap mode-list no-encap command**, 566, 568
- sap pmk 26 mode-list gcm-encrypt command**, 621
- sap pmk pairwise-master-key mode-list gcm-encrypt command**, 621
- scalability**
  - ISE (Identity Services Engine), 118–119, 737–742
    - ISE cubes*, 737
    - ISE persona types*, 737

- node personas*, 742
- PPAN (Policy Administration Node)*, 738–739
- primary devices*, 738–739
- registration of ISE nodes*, 739–742
- SNS (Secure Network Server) appliances, 112–113
- scans, Tenable.SC, 882–883
- SCCM (System Center Configuration Manager), 673, 708
- SCEP (Simple Certificate Enrollment Protocol), 500, 520–521, 999
- SD-Access (Software-Defined Access), 613–614
- /sdcards/downloads/spw.log command, 812
- Search icon (Admin portal), 138
- sec-admin group, 945
- SecAdmin profile, 975–976
- Second Port Disconnect, CDP, 991
- secondary PAN (Policy Administration node)
  - auto PAN switchover, 745–746
  - automatic failover for, 746
  - promoting to primary, 745
- Secure Network Server. *See* SNS (Secure Network Server) appliances
- Secure Shell. *See* SSH (Secure Shell)
- Secure Sockets Layer. *See* SSL (Secure Sockets Layers)
- secure web gateways, 818
- Security Administrator command set, 942–943
- Security Administrators role, 939
- Security Assertion Markup Language. *See* SAML (Security Assertion Markup Language)
- Security Association Protocol (SAP), 616
- security context, 232, 235
- Security Group Access. *See* TrustSec
- security group ACLs. *See* SGACLs (security group ACLs)
- security group firewalls. *See* SGFWs (security group firewalls)
- security group tags. *See* SGTs (security group tags)
- security holes. *See* vulnerability assessment
- security information and event management (SIEM) systems, 818
- security information management (SIM), 744
- Security Level tab (Cisco AnyConnect NAM supplicant), 64–66
- security posturing, 101
- SECURITY role, 971
- seed devices, 566, 999
- self-management, MDM (mobile device management) onboarding, 543–544
- self-registered guest portals, 342, 515
  - authorization rule configuration, 373–380
  - BYOD settings, 372
  - configuration flowchart, 365–366
  - guest change password settings, 371–372
  - guest device compliance settings, 373
  - guest device registration settings, 371–372
  - guest location setting, 369–371, 994
  - login page settings, 367–368
  - portal settings, 366–367
  - registration form settings, 368–371
  - self-registration success, 371
- Self-Registration Success page, 371
- self-signed certificates, 181–182
- serial replication, 748
- SerialNumber attribute, 537
- Server column (Live Log), 768
- Server name rules setting (AnyConnect posture profile), 647
- servers, 276–280
  - authentication, 41, 277–278, 991
  - Cisco Access Control Server (ACS), 909, 910
  - HTTP/HTTPS, 314
  - RADIUS
    - accounting servers*, 278–279
    - authentication servers*, 277–278

- fallback*, 279–280
- token servers*, 23
- SMTP (Simple Mail Transfer Protocol), 388
- SNS (Secure Network Server) appliances, 177
- Sun Directory Server, 25
- XCP (Extensible Communication Platform), 825
- service providers, 35
- service set identifiers. *See* SSIDs (service set identifiers)
- service-level agreements (SLAs), 754–756
- Service-Type attribute (RADIUS), 96, 265, 415
- service-type values, 13
- session IDs, 97
- Session Key Assignment, 918
- Session Trace tool, 801–804
- Settings tab, 161, 163
- setup command, 178
- SGA (Security Group Access). *See* TrustSec
- SGACLs (security group ACLs), 597–604
  - definition of, 998
  - Deny\_All SGACL, 601–602
  - east-west deployment of, 598–599
  - egress policy, 597–598, 600–601
  - north-south deployment of, 598–599
  - Permit\_HTTP\_HTTPS SGACL, 601–602
  - Permit\_ICMP SGACL, 602–603
  - Permit\_Mgmt SGACL, 601
  - Permit\_SRC\_HTTP\_HTTPS SGACL, 603–604
  - Permit\_WEB\_RDP SGACL contents, 598
  - syntax, 599–600
- SGFWs (security group firewalls), 611–613
  - on ASA (Adaptive Security Appliances), 612
  - on ASR (Aggregation Services Router), 613
  - definition of, 999
  - on Firepower, 612–613
  - on ISR (Integrated Services Router), 613
- SGTs (security group tags), 13, 236, 822
  - access-layer devices that do not support, 580
  - classification of, 575–577
  - configuration, 572–574
  - definition of, 172, 556
  - dynamically assigning via 802.1X, 577
  - egress enforcement with, 555–556
  - manually assigning via 802.1X, 577–578
  - mapping subnets to, 580
  - mapping VLANs to, 580
  - native tagging, 593–597
    - configuration on IOS XE switches*, 595–597
    - Layer 2 frame format with*, 593–594
    - pervasive tagging*, 594
- SXP (SGT Exchange Protocol), 110, 303, 581–593
  - configuration on Cisco ASA*, 591–592
  - configuration on IOS devices*, 588–590
  - configuration on ISE (Identity Services Engine)*, 584–586
  - configuration on WLCs (wireless LAN controllers)*, 590–591
  - definition of*, 998
  - design*, 582–583
  - verification in ASDM (Adaptive Security Device Manager)*, 592–593
- SHA-256 file type, 672
- Shadow Brokers, 868
- sho cts interface command, 596
- sho run int command, 621
- Short Message Service. *See* SMS (Short Message Service)
- should-secure policy (MACsec), 616, 618
- show commands, 147, 457–458
  - show aaa server | incl host, 757
  - show aaa servers, 296–297
  - show application status ise, 741–742

- show authentication interface, 812–813
- show authentication session int g0/23, 696
- show authentication session interface, 297–299, 328–329
- show cts environment-data, 562, 568
- show cts interface, 571, 622–623
- show cts pac, 568
- show cts policy peer, 570
- show cts rbacl, 609
- show cts role-based permissions, 562, 609
- show cts sxp connections brief, 589, 591
- show cts sxp sgt-map brief, 590
- show device-sensor cache all, 457–458
- show device-tracking database details, 267
- show ip access-list ACL-WEBAUTH-REDIRECT, 314
- show ip device tracking all, 267
- show logging application, 781–782
- show logging system, 781–782
- show run, 11, 620
- show running-config, 952, 961–963
- show running-config aaa, 569
- show running-config all | inc ip, 266
- show running-config all | inc radius-server, 265
- show udi, 747–748
- show users, 955
- Shutdown action (EPS), 821**
- SIEM (security information and event management) systems, 818**
- signatures**
  - AnyConnect posture profile, 645
  - CAs (certificate authorities), 31–32
- SIM (security information management), 744**
- Simple Certificate Enrollment Protocol (SCEP), 500, 520–521, 999**
- simple conditions, 239, 251, 663–664, 999**
- Simple Mail Transfer Protocol. *See* SMTP (Simple Mail Transfer Protocol) servers**
- Simple Network Management Protocol. *See* SNMP (Simple Network Management Protocol)**
- single sign-on. *See* SSL (Secure Sockets Layers)**
- single SSID onboarding, 487–488**
  - Android onboarding flow, 526–530
    - device provisioning, 529–530*
    - device registration, 526–528*
    - NSP app download, 528–529*
  - definition of, 999
  - iOS onboarding flow, 523–526
    - device enrollment, 523–524*
    - device provisioning, 526–527*
    - device registration, 523–524*
  - ISE configuration, 495–496, 510–523
    - Apple iOS example, 496–503*
    - authorization profiles, 516*
    - authorization rules for EAP-TLS authentications, 518*
    - authorization rules for onboarding, 517*
    - Blackberry example, 508–509*
    - client provisioning policy configuration, 512–514*
    - default unavailable client provisioning policy action, 515*
    - ISE as certificate authority, 519–520, 521–523, 994*
    - native supplicant profile, 510–512*
    - SCEP (Simple Certificate Enrollment Protocol), 520–521, 999*
    - WebAuth configuration, 514–515*
  - verification of BYOD flows, 534–535
    - endpoint identity groups database, 535*
    - RADIUS Live Logs, 534*
    - reports, 534–535*
  - Windows and Mac onboarding flow, 531–533
    - device provisioning, 532–533*
    - device registration, 531*
  - WLC (Wireless LAN Controller) configuration, 489–495

- ACLs (access control lists)*, 492–495
  - WLAN configuration*, 490–491
- Single-Host mode, 272, 298, 618
- single-node ISE deployment, 113
- SISE 300–715 exam preparation, 988–989
  - final study and review, 988–989
  - hands-on activities, 988–989
- Skip NMAP Host Discovery option (Nmap), 416
- SLAs (service-level agreements), 754–756
- smart cards, 29
- smart default policies, 318
- smart devices
  - employee limited access, 246–249
  - Internet-only access, 243–246
  - SmartDevice logical profile, 245–246
- SMS (Short Message Service), 388–389
- SMTP (Simple Mail Transfer Protocol) servers, 388
- SNAT (Source NAT), 752
- SNMP (Simple Network Management Protocol)
  - global probe settings, 444
  - SNMP Ports option (Nmap), 416
  - SNMPQUERY and SNMPTRAP probes, 417–419
- snmp trap mac-notification change added command, 418
- snmp trap mac-notification change removed command, 418
- SNMPQUERY probe, 417–419
- snmp-server community command, 419
- snmp-server source-interface informs command, 266
- snmp-server trap-source command, 266
- SNMPTRAP probe, 417–419
- snooping, DNS, 494
- SNS (Secure Network Server) appliances, 177
  - form factors, 111–112
  - scalability, 112–113
- social guest accounts, 348
- social login, 23, 35
- Softerra LDAP browser, 26
- Software-Defined Access (SD-Access), 613–614
- Source NAT (SNAT), 752
- source SGT, 559
- source tree view (TrustSec policy matrix), 552
- sources, identity, 34, 35
- SPAN (Switched Port Analyzer)
  - configuration, 424–425
  - DHCPSPAN probe, 411–414
  - HTTP SPAN design, 420–421
- Sponsor Groups settings
  - contractor accounts, 346
  - weekly guest accounts, 348
- sponsored guest portals, 342, 380–381
  - AUP (acceptable use policy) page settings, 386
  - configuration flowchart, 380–381
  - default sponsor portal, 384
  - login settings, 386
  - other settings, 387
  - portal settings, 385–386
  - provisioning guest accounts from, 389–394
- sponsors
  - definition of, 341, 381, 999
  - sponsor groups, 381–382
- SPs (service providers), 35, 394, 998
- spyware
  - anti-spyware posture policy conditions, 663
  - anti-spyware remediations, 681–682
- SSH (Secure Shell), 6
- SSIDs (service set identifiers), 220–223, 487–488, 730–731, 999. *See also* dual SSID onboarding; single SSID onboarding
- SSL (Secure Sockets Layers), 25, 181
- SSO (single sign-on), 35

- ST (State) field, 184
- START message, 9, 11
- statements
  - deny, 280, 316
  - permit, 280, 314, 316
- status, Live Log, 767
- Status dashlet, 134
- stealth mode, 645, 703
- Stealthwatch
  - capabilities of, 858
  - configuration, 857–866
  - ISE integration, 862–866
  - pxGrid client identity certificate, importing, 859–862
- STIX (Structured Threat Information eXpression), 890, 892–893, 999
- STOP message, 11
- subject alternative names (SANs), 184–185, 752
- subnets, mapping to SGTs (security group tags), 580
- subordinate CAs (certificate authorities), 521–523
- subscribers, 824, 999
- SUCCESS message, 11
- Summary tab (Home page), 134
- Sun Directory Server, 25
- Super admin role, 130
- supplicants
  - authenticators, 719
  - Cisco AnyConnect NAM, 59–73
    - AnyConnect NAM profiles*, 71–72
    - Authentication Policy view*, 60, 62
    - Client Policy view*, 60, 61–62
    - EAP chaining*, 73
    - Network Groups view*, 60, 71
    - Networks view*, 60, 62–70
    - overview of*, 59–60
  - definition of, 41, 50, 999
  - devices without, 79–80
  - endpoint supplicant verification, 295–296
  - native supplicant profile, 510–512
  - policy for, 617
  - supplicant provisioning reports, 534–535
  - Windows native, 50–59
    - machine authentication*, 58–59
    - user authentication*, 58
    - Wired AutoConfig service*, 50–57
- support bundles, 782–784
  - categories of, 782–783
  - creating from CLI, 783–784
  - creating from GUI, 783
  - definition of, 782
- support information page settings, hotspot guest portals, 357–358
- Switched Port Analyzer. *See* SPAN (Switched Port Analyzer)
- switches. *See also* ports; WLC (Wireless LAN Controller)
  - authentication on, 261–276
    - AAA servers*, 276–280
    - Cisco ISE verification*, 302–303
    - endpoint supplicant verification*, 295–296
    - global configuration AAA commands*, 261–262
    - global configuration RADIUS commands*, 262–269
    - interface configuration settings*, 269–276
    - NAC (network access device) verification*, 296–302
- IOS XE
  - configuration for TrustSec*, 560–563
  - manual SGT (security group tag) propagation on*, 595–597
- MACsec, 618–619
- sample configurations, 1034–1061
  - Catalyst 3000 Series, 12.2(55)SE*, 1034–1038
  - Catalyst 3000 Series, 15.0(2)SE*, 1038–1044
  - Catalyst 4500 Series, IOS-XE 3.3.0 / 15.1(1)SG*, 1053–1057

*Catalyst 6500 Series, 12.2(33)SXJ, 1058–1061*

*Catalyst 9000 Series, 16.9.5, 1044–1052*

verifying authentications with, 296–299

- show aaa servers command, 296–297*
- show authentication session interface command, 297–299*
- test aaa command, 297*

WebAuth, 313–315

- certificates, 313*
- HTTP/HTTPS server, 314*
- URL-redirect ACL, 314–315*

switchport command, 269

SXP (SGT Exchange Protocol), 110, 303, 581–593

- configuration on Cisco ASA, 591–592
- configuration on IOS devices, 588–590
- configuration on ISE (Identity Services Engine), 584–586
- configuration on WLCs (wireless LAN controllers), 590–591
- definition of, 998
- design, 582–583
- overview of, 581–582
- verification in ASDM (Adaptive Security Device Manager), 592–593

sysContact option (Nmap), 416

sysDescr option (Nmap), 416

sysLocation option (Nmap), 416

syslog messages, 299–300

sysName option (Nmap), 416

System Activities option (Admin portal), 139

System admin role, 130

System Center Configuration Manager (SCCM), 673, 708

System Certificates settings, hotspot guest portals, 353

System logs support bundles, 783

System Scan module. *See* posture assessment

System Summary dashlet, 134

System tab (Administration screen), 155–161

- Admin Access tab, 160–161
- Backup & Restore tab, 160
- Certificates tab, 158
- Deployment tab, 155
- Licensing tab, 155–158
- Logging tab, 159
- Maintenance tab, 159
- Settings tab, 161
- Upgrade tab, 160

SYSTEM\_32 file path option, 669

SYSTEM\_DRIVE file path option, 669

SYSTEM\_PROGRAMS file path options, 669

SYSTEM\_ROOT file path option, 669

## T

TACACS Live Log tab (Operations screen), 147

TACACS+ (Terminal Access Controller Access Control System)

- accounting messages, 11
- admin role, 131
- authentication messages, 9
- authorization messages, 10–11
- Cisco WLC (Wireless LAN Controller) profiles
  - Employee, 977*
  - Helpdesk, 976*
  - ISE configuration on WLC TACACS+ servers, 979–980*
  - NetAdmin, 974–975*
  - predefined, 974*
  - SecAdmin, 975–976*
- client/server communication, 7–8
- command sets, 922–923
- communication flows, 12
- device administration AAA with Cisco IOS
  - policy sets, 943–946*

- TACACS *command sets*, 941–943
- TACACS *profiles*, 932–934, 939–941
- TACACS+ *authentication and fallback*, 946–948
- TACACS+ *command accounting*, 951
- TACACS+ *command authorization*, 948–950
- TACACS+ *command sets*, 934–936, 992
- enabling, 910–911, 914–915
- Live Log. *See* Live Log
- profiles, 923–924
- RADIUS compared to, 13, 16
- support for, 8
- tags, security group.** *See* SGTs (security group tags)
- targets, logging**, 743–744, 777–778
- TAXII (Trusted Automated eXchange of Intelligence Information)**, 890, 892–893, 999
- TCAM (Ternary CAM)**, 554
- TC-NAC (Threat Centric Network Access Control)**, 110, 886
  - AMP (Advanced Malware Protection) for Endpoints, 897–904
    - adapter configuration*, 900–904
    - capabilities of*, 897–898
    - incidents*, 899–900
    - indicators*, 899
  - authorization profiles/rules, 884–886
  - capabilities of, 871–873
  - Coa-Events report, 888–889
  - CTA (Cognitive Threat Analytics), 890–897
    - authorization with*, 896–897
    - CTA STIX/TAXII API account creation*, 892–893
    - dashboard*, 890–892
    - integration for TC-NAC*, 894–896
  - CVE (Common Vulnerabilities and Exposures), 873, 992
  - CVSS (Common Vulnerability Scoring System), 873, 992
  - enabling, 874–878
  - endpoint transition on network with TC-NAC, 887
  - exploits, definition of, 872, 993
  - flows for, 873–874
  - goals of, 868
  - integration with threat sources, 890
  - integration with vulnerability assessment vendor, 878–883
    - advanced settings*, 881
    - basic setup*, 880
    - configured vendor instances*, 883
    - Tenable.SC repositories*, 881–882
    - Tenable.SC scans*, 882–883
    - users*, 880
  - license packages, 156
  - TC-NAC Live Log, 888–889
  - Threat-Events report, 888
  - Vulnerability Assessment report, 888
  - vulnerability-based access control, 873–874
- TCP (Transmission Control Protocol)**
  - port 49, 8
  - port 389, 25
  - port 636, 25
  - port 64999, 580
  - TCP/7800, 748
  - TCP/7802, 748
- TCPDump**, 327, 798–801
- TEAP (Tunnel EAP)**, 46–47, 48–49, 73, 216
- temporal agents**, 99–100, 999
- Tenable.SC repositories**, 881–882
- Tenable.SC scans**, 882–883
- Terminal Access Controller Access Control System.** *See* TACACS+ (Terminal Access Controller Access Control System)
- Ternary CAM (TCAM)**, 554
- test aaa command**, 297
- testing**
  - device administration AAA with Cisco IOS
    - at IOS command line*, 954–966

- in ISE (Identity Services Engine), 952–954*
- device administration AAA with Cisco WLC, 981–986
- themes, hotspot guest portals, 361
- Threat Centric NAC reports, 150
- Threat Centric NAC tab (Administration screen), 170
- Threat Centric Network Access Control. *See* TC-NAC (Threat Centric Network Access Control)
- threat sources, TC-NAC integration with, 890
- Threat tab (Home page), 137
- Threat Watchlist dashlet, 137
- Threat-Centric NAC Live Logs tab (Operations screen), 146
- Threat-Events report, 888
- TIM (IBM Tivoli Identity Manager), 25
- Time Selector, 770
- Timeout option (TACACS profile), 933
- timers
  - authentication, 275
  - remediation, 645, 691
- Tivoli Identity Manager (TIM), 25
- TLS (Transport Layer Security), 43, 45, 181–182, 214, 215, 235, 470, 737
- token servers, 23
- Top Threats dashlet, 137
- Top Vulnerability dashlet, 136
- topics (pxGrid), 824, 999
- Total Compromised Endpoints dashlet, 137
- Total Vulnerable Endpoints dashlet, 136
- Touch ID, 310
- tracking enable command, 267
- Transmission Control Protocol. *See* TCP (Transmission Control Protocol)
- transport
  - native tagging, 593–597
  - SXP (SGT Exchange Protocol), 303, 581–593
  - configuration on Cisco ASA, 591–592*
  - configuration on IOS devices, 588–590*
  - configuration on ISE (Identity Services Engine), 584–586*
  - configuration on WLCs (wireless LAN controllers), 590–591*
  - design, 582–583*
  - overview of, 581–582*
  - verification in ASDM (Adaptive Security Device Manager), 592–593*
- Transport Layer Security. *See* TLS (Transport Layer Security)
- Transportation Security Administration (TSA), 2
- Troubleshoot tab (Operations screen), 147–148
- “Troubleshooting Cisco’s ISE without TAC” (Woland), 815
- troubleshooting tools
  - for device administration, 981–986
    - at IOS command line, 954–966*
    - in ISE (Identity Services Engine), 952–954*
  - Endpoint Debug, 796–798
  - endpoint diagnostics, 809–812
    - Cisco AnyConnect Diagnostics and Reporting Tool (DART), 59, 809–811*
    - supplicant provisioning logs, 812*
  - Evaluate Configuration Validator, 788–793
  - Execute Network Device Command, 787–789
  - logs, 766–785
    - debug logs, 779–784*
    - de-duplication of, 805–807*
    - Live Log, 327, 766–775*
    - Live Sessions, 776*
    - logging categories, 744, 778–779*
    - logging flows, 743*
    - logging targets, 743–744, 777–778*

- network device troubleshooting, 812–815
  - client details, viewing on WLC, 813–814*
  - debug commands, 815*
  - show authentication interface command, 812–813*
- Posture Troubleshooting, 794–795
- RADIUS Authentication Troubleshooting tool, 785–786
- Session Trace, 801–804
- support bundles, 782–784
  - categories of, 782–783*
  - creating from CLI, 783–784*
  - creating from GUI, 783*
  - definition of, 782*
- TCP Dump, 798–801
- troubleshooting methodology, 804–808
  - authentication and authorization flows, 804–805*
  - log de-duplication, 805–807*
  - USERNAME user, 807*
- trusted authorities, 999**
- Trusted Automated eXchange of Intelligence Information (TAXII), 890, 892–893, 999**
- trusted CAs (certificate authorities), 31–32, 475–479**
  - certificate status verification, 478–479
  - public certificates, 476–477
  - role in authentication process, 463–465
- trusted certificates, 188, 537–538**
- Trusted for Client Auth field, 463**
- TrustSec**
  - architecture of, 557–558
  - Cisco Software-Defined Access (SD-Access), 613–614
  - configuration
    - ASA (Adaptive Security Appliances), 564–565*
    - IOS XE switches, 560–563*
    - NAD (network access devices) settings, 559*
    - PACs (Protected Access Credentials), 558–559*
  - definition of, 172, 548, 555–556
  - domains, 557, 1000
  - environment data, 558, 993
  - goals of, 555
  - license packages, 156
  - native tagging, 593–597
    - configuration on IOS XE switches, 595–597*
    - Layer 2 frame format with, 593–594*
    - pervasive tagging, 594*
  - NDAC (Network Device Admission Control), 566, 996
    - non-seed devices, 567–571, 996*
    - seed devices, 566, 999*
  - policy matrix, 604–609
    - configuration of, 605–609*
    - views of, 604–605*
  - reports, 150
  - SGACLs (security group ACLs), 597–604, 998
    - Deny\_All SGACL, 601–602*
    - east-west deployment of, 598–599*
    - egress policy, 597–598, 600–601*
    - north-south deployment of, 598–599*
    - Permit\_HTTP\_HTTPS SGACL, 601–602*
    - Permit\_ICMP SGACL, 602–603*
    - Permit\_Mgmt SGACL, 601*
    - Permit\_SRC\_HTTP\_HTTPS SGACL, 603–604*
    - Permit\_WEB\_RDP SGACL contents, 598*
    - syntax, 599–600*
  - SGFWs (security group firewalls), 611–613
    - on ASA (Adaptive Security Appliances), 612*
    - on ASR (Aggregation Services Router), 613*
    - definition of, 999*
    - on Firepower, 612–613*

on ISR (Integrated Services Router),  
613

SGTs (security group tags)

*access-layer devices that do not  
support, 580*

*classification of, 575–577*

*defining, 572–574*

*definition of, 556*

*dynamically assigning via 802.1X,  
577*

*egress enforcement with, 555–556*

*manually assigning via 802.1X,  
577–578*

*mapping subnets to, 580*

*mapping VLANs to, 580*

*native tagging, 593–597*

*SXP (SGT Exchange Protocol),  
581–593*

TrustSec-enabled NADs (network access  
devices)

*defining TrustSec settings for, 559*

*PACs (Protected Access Credentials),  
558–559*

**TSA (Transportation Security  
Administration), 2**

**TTLS (Tunneled Transport Layer Security)**

EAP-TTLS, 45–46, 48–49, 216

TEAP, 216

**Tunnel EAP (Tunnel EAP), 46–47, 48–49,  
73, 216**

**tunneled EAP (Extensible Authentication  
Protocol) types, 44–49, 214–216, 1000**

EAP chaining, 216

EAP-FAS, 215

EAP-FAST, 48–49

EAP-GTC, 215

EAP-MS-CHAPv2, 215

EAP-TLS, 215

EAP-TTLS, 48–49, 216

PEAP, 44–45, 48–49, 215

TEAP, 46–47, 73, 216

**Tunneled Transport Layer Security (TTLS),  
45–46, 48–49, 216**

**two-factor authentication (2FA), 26, 1000**

**two-node ISE deployment, 114–116**

## U

**UDID attribute, 537**

**UDP (User Datagram Protocol) port 123,  
32**

**Umbrella, 640**

**Unquarantine action (EPS), 821**

**unsupported devices, onboarding, 508–509**  
**updates**

to Cisco Identity Services Engine (SISE  
300–715) Exam, 1034–1061

*Catalyst 3000 Series, 12.2(55)SE,  
1034–1038*

*Catalyst 3000 Series, 15.0(2)SE,  
1038–1044*

*Catalyst 4500 Series, IOS-XE 3.3.0 /  
15.1(1)SG, 1053–1057*

*Catalyst 6500 Series, 12.2(33)SXJ,  
1058–1061*

*Catalyst 9000 Series, 16.9.5,  
1044–1052*

to compliance modules, 637–638

**Upgrade tab (System), 160**

**upgrades, 160**

**Uplink MACsec, 619–623**

**uploading AnyConnect deployment  
packages, 642–644**

**URL policy, 612**

**URL redirection, 236**

**URL-redirect ACL**

configuration for Cisco switch, 314–315

configuration for WLC, 316

**URL-redirected MAC authentication  
bypass, 311–313**

**USB condition, 100, 679**

**USB remediations, 686**

**user agents (SAML), 35**

User Auth tab (Cisco AnyConnect NAM supplicant), 68–69

user authentication. *See* authentication

User Datagram Protocol (UDP) port 123, 32

user identities, 920, 921–922

user identity groups, 22

- definition of, 1000
- FDM (Firepower Device Management), 840–844
- Guest Access work center, 339–340

user interface, Device Administration work center, 919–920

user persistence, 752

USER\_DESKTOP file path option, 669

USER\_PROFILE file path option, 670

user-experience (UX), 337. *See also* guest services

username command, 263

username cts-user privilege command, 561

UserNotified attribute, 537

users, 807

- internal, 21–22, 994
- local, 195–196
- network access, 21
- TC-NAC (Threat Centric Network Access Control), 880
- viewing in FMC (Firepower Management Center), 844–845

Users tab (Context Visibility screen), 143

UX (user-experience), 337. *See also* guest services

## V

VACLs (VLAN Access Control Lists), 424, 425–426

Validate Server Certificate checkbox (Windows native supplicant), 53

validity period, for certificate, 467

vendors

- MDM (mobile device management), 101–102

- TC-NAC integration with, 878–883
  - advanced settings*, 881
  - basic setup*, 880
  - configured vendor instances*, 883
  - Tenable.SC repositories*, 881–882
  - Tenable.SC scans*, 882–883
  - users*, 880
- VSAs (vendor-specific attributes), 265–266, 1000

virtual ISE appliances, 111–113, 177

virtual private networks. *See* VPNs (virtual private networks)

viruses

- anti-virus posture policy conditions, 663
- anti-virus remediations, 681–682

Visibility Setup option (Admin portal), 138

vlan access-map command, 426

VLAN detection interval setting (AnyConnect posture profile), 646

VLAN DHCP release page settings, hotspot guest portals, 355–356

VLANs (virtual LANs)

- assignment of, 551–553, 726
- authentication VLAN, 87–88
- dynamic interfaces for, 284–286
  - employee dynamic interface*, 284–285
  - guest dynamic interface*, 285–286
- mapping to SGTs (security group tags), 580
- segmentation with, 322
- VACLs (VLAN Access Control Lists), 424, 425–426

VMware

- ISE support for, 113
- vSwitches, 427
- Workspace One, 708

VPNs (virtual private networks), 7

- provisioning, 101
- remote access, 88, 223–224

VRF instances, 548

VSAs (vendor-specific attributes), 265–266, 1000

vSwitches, 427

vulnerabilities, definition of, 872, 1000

vulnerability assessment

exploits

*CVE (Common Vulnerabilities and Exposures)*, 873, 992

*CVSS (Common Vulnerability Scoring System)*, 873, 992

definition of, 872, 993

TC-NAC (Threat Centric Network Access Control)

capabilities of, 871–873

*Coa-Events report*, 888–889

enabling, 874–878

endpoint transition on network with TC-NAC, 887

flows for, 873–874

integration with threat sources, 890

integration with vulnerability assessment vendor, 878–883

TC-NAC Live Log, 888–889

*Threat-Events report*, 888

*Vulnerability Assessment report*, 888

vulnerability-based access control, 873–874

Vulnerability Assessment report, 888

Vulnerability tab (Home page), 136

Vulnerability Watchlist dashlet, 136

Vulnerable Endpoints Over Time dashlet, 136

Vulnerable-LimitAccess authorization rule, 886

## W

WannaCry ransomware, 554–555

Web Authentication. *See* WebAuth (Web Authentication)

Web Authentication Redirection ACL, 280–282

WebAuth (Web Authentication)

configuration for BYOD onboarding, 514–515

CWA (Centralized Web Authentication), 730–731. *See also* sponsored guest portals

authentication process, 85–87

authorization policies, 322–324

Cisco switch configuration, 313–315

CoA (*Change of Authorization*) and, 311

definition of, 991

dual SSID onboarding and, 496

ISE (*Identity Services Engine*) configuration, 317–322

services supported by, 311

with third-party network device support, 87–88

URL-redirected MAC authentication bypass, 311–313

verification from client, 324–326

verification from ISE UI, 327

verification on NAD (*network access device*), 327–331

WLC (*Wireless LAN Controller*) configuration, 98, 315–316, 329–331

definition of, 306, 1000

guests, 309

LWA (*Local Web Authentication*), 310–311

with centralized portal, 84–85

definition of, 995

when to use, 84

overview of, 83

scenarios for, 309–310

WebAuthN, 310

weekly guest accounts, 347

WEP (*Wired Equivalency Protection*), 614

Wi-Fi Protected Access (WPA/WPA2), 615

wildcard certificates, 184

- Windows BYOD (bring your own device)**
  - onboarding, 531–533
  - device provisioning, 532–533
  - device registration, 531
- Windows Hello, 27, 310**
- Windows native supplicant, 50–59**
  - machine authentication, 58–59
  - user authentication, 58
- Wired AutoConfig service**
  - Advanced Settings tab, 57*
  - Authentication tab, 53, 56–57*
  - EAP MSCHAPv2 Properties dialog, 54*
  - local area connection properties, 52–53*
  - Protected EAP Properties page, 53–54, 55–56*
  - Windows services control applet, 51–52*
- Windows Server Update Services (WSUS) remediations, 685**
- Windows Update Agent, 673**
- WinSPWizard, 513**
- wired authentication, 261–276**
  - Cisco ISE verification, 302–303
    - Live Sessions, 303*
    - RADIUS Live Log, 302–303*
  - endpoint supplicant verification, 295–296
  - global configuration AAA commands, 261–262
  - global configuration RADIUS commands, 262–269
    - device tracking in IOS Xe 16.x and later, 267*
    - global 802.1X commands, 266–267*
    - IOS 12.2.x, 262–263, 264–266*
    - IOS 15.x, 263–266*
    - IOS XE, 263–266*
    - local ACL (access control list) creation, 268–269*
  - interface configuration settings, 269–276
    - application of initial ACL to port, 275–276*
    - authentication settings, 274–275*
    - authentication timers, 275*
    - configuration of interfaces as switch ports, 269*
    - FlexAuth (Flexible Authentication), 269–272*
    - HA (high availability), 269–272*
    - host mode of switch port, 272–274*
  - NAC (network access device) verification, 296–302
    - with Cisco switches, 296–299*
    - with Cisco WLC (Wireless LAN Controller), 300–302*
    - with syslog messages, 299–300*
- Wired AutoConfig service**
  - Advanced Settings tab, 57
  - Authentication tab, 53, 56–57
  - EAP MSCHAPv2 Properties dialog, 54
  - local area connection properties, 52–53
  - Protected EAP Properties page, 53–54, 55–56
  - Windows services control applet, 51–52
- Wired Equivalency Protection (WEP), 614**
- Wired\_802.1X condition, 242, 254**
- Wired\_MAB condition, 242**
- wireless authentication, 731**
  - airespace ACLs (access control lists), 280–284
    - Google URLs for ACL Bypass, 282–283*
    - Posture Agent Redirection ACL, 283–284*
    - Web Authentication Redirection ACL, 280–282*
  - RADIUS, 276–280
    - accounting servers, 278–279*
    - authentication servers, 277–278*
    - fallback, 279–280*
- Wireless Black List Default rule, 239**

- Wireless LAN Controller. *See* WLC (Wireless LAN Controller)
- wireless LANs. *See* WLAN (wireless LAN) configuration
- wireless MAB, 489
- WIRELESS role, 971
- Wireless Setup (BETA) option (Admin portal), 139
- wireless SSIDs, authentication policy for, 220–223
  - AD identity source, 223
  - allowed protocols, 221–222
  - completed authentication rule, 223
  - SSID name, 221
- wizards, 179
  - Cisco Supplicant Provisioning Wizard, 513
  - CiscoPress-TLS, 513
  - CLI Setup Wizard, 178–179
  - ISE Setup Wizards, 141
  - WinSPWizard, 513
- WLAN (wireless LAN) configuration, 286–295, 971
  - for BYOD onboarding, 490–491
  - corporate WLAN, 291–295
  - guest WLAN, 287–290
- WLC (Wireless LAN Controller), 329–331
  - authentication configuration on
    - AAA servers, 276–280
    - airespace ACLs (access control lists), 280–284
    - Cisco ISE verification, 302–303
    - dynamic interfaces for client VLANs, 284–286
    - endpoint supplicant verification, 295–296
    - NAC (network access device) verification, 296–302
    - wireless LANs, 286–295
  - configuration, 315–316, 329–331
    - for BYOD onboarding, 489–495
    - ISE NAC feature, 315–316
    - MAC Filtering option, 315
    - URL-redirect ACL, 316
  - device administration AAA configuration
    - ISE configuration on WLC TACACS+ servers, 979–980
    - network device preparation, 972
    - policy results preparation, 974–977
    - policy sets, 977–979
    - testing and troubleshooting, 981–986
    - top-level menus, 971–972
  - Device Sensor feature, 98
  - DHCP probes with, 413
  - HTTP POST method, 84–85
  - SXP (SGT Exchange Protocol) configuration on, 590–591
  - verifying authentications with, 300–302
    - current clients, 300–302
    - debug clients, 302
  - viewing client details on, 813–814
- Woland, Aaron, 482, 633
- Work Centers, Device Administration, 918
  - Identities tab, 920
  - Network Resources tab, 921–922
  - Password Change Control settings, 918
  - Policy Elements tab, 922–924
  - Policy Sets tab, 925–927
  - Reports, 927
  - Session Key Assignment settings, 918
  - UI navigation for, 919–920
- Work Centers screen, 142, 170–171
- Workspace One, 708
- WPA (Wi-Fi Protected Access), 548, 615
- WSA (Web Security Appliance) configuration, 850–857
  - access policy, 855–856
  - decryption policy, 857
  - ERS (External RESTful Services), 850–853

identification profiles, 855–857  
integration with pxGrid and ISE, 850–855  
policies, 855–857  
WSUS (Windows Server Update Services)  
remediations, 685

## **X**

X.509 certificates. *See* certificate-based authentication

XCP (Extensible Communication Platform)  
server, 825  
XenMobile, 708  
XMPP (Extensible Messaging and Presence  
Protocol), 825

## **Y-Z**

YubiKeys, 310  
ZBF (zone-based firewall), 611

# **CCNP Security Identity Management SISE 300-715 Official Cert Guide Companion Website**

---

Access interactive study tools on this book's companion website, including practice test software, memory tables, review exercises, Key Term flash card application, study planner, and more!

To access the companion website, simply follow these steps:

1. Go to [www.ciscopress.com/register](http://www.ciscopress.com/register).
2. Enter the print book ISBN: 9780136642947.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the **Registered Products** tab.
6. Under the book listing, click on the **Access Bonus Content** link.

If you have any issues accessing the companion website, you can contact our support team by going to [pearsonitp.echelp.org](http://pearsonitp.echelp.org).