Cisco ISE for BYOD and Secure Unified Access

Second Edition

Aaron T. Woland, CCIE No. 20113

Jamey Heary, CCIE No. 7680

Cisco Press

800 East 96th Street

Indianapolis, Indiana 46240 USA

Cisco ISE for BYOD and Secure Unified Access
Second Edition

Aaron T. Woland

Jamey Heary

Copyright© 2017 Cisco Systems, Inc.

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

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

Printed in the United States of America

First Printing June 2017

Library of Congress Control Number: 2017938614

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

ISBN-10: 1-58714-473-5

Warning and Disclaimer

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

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

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

Trademark Acknowledgments

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

Special Sales

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

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact 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. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Editor-in-Chief: Mark Taub

Alliances Manager, Cisco Press: Ron Fligge

Executive Editor: Mary Beth Ray

Managing Editor: Sandra Schroeder

Development Editor: Christopher Cleveland

Senior Project Editor: Tonya Simpson

Copy Editor: Bill McManus

Technical Editor: Pete Karelis

Editorial Assistant: Vanessa Evans

Cover Designer: Chuti Prasertsith

Composition: codeMantra

Indexer: Erika Millen

Proofreader: Sasirekha Durairajan

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

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. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

About the Authors

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

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

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

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

About the Technical Reviewer

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

Dedications

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

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

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

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

To my sister, Anna: If I hadn't always had to compete with you for our parents' attention and to keep my things during our "garage sales," I would probably have grown up very naive and vulnerable. You drove me to think outside the box and find new ways to accomplish the things I wanted to do. Seeing you succeed in life and in school truly had a profound effect on my life. Thank you for marrying Eddie, my brilliant brother-in-law. Eddie convinced me that I could actually have a career in this technology stuff, and without his influence, I would probably be in law enforcement or under the hood of car.

To my grandparents, Jack, Lola, Herb, and Ida: You have taught me what it means to be alive and the true definition of courage, survival, perseverance, hard work, and never giving up.

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

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

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

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

Acknowledgments

From Aaron:

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

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

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

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

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

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

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

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

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

To the world's greatest Engineering Team, and of course I mean the people who spend their days writing and testing the code that makes up Cisco ISE. You guys continue to show the world what it means to be "world-class."

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

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

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

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

From Jamey:

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

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

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

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

Contents at a Glance

Introduction xxix

Part I Identity-Enabled Network: Unite!

Chapter 1 Regain Control of Your IT Security 1

Chapter 2 Fundamentals of AAA 9

Chapter 3 Introducing Cisco Identity Services Engine 23

Part II The Blueprint, Designing an ISE-Enabled Network

Chapter 4 The Building Blocks in an Identity Services Engine Design 35

Chapter 5 Making Sense of the ISE Deployment Design Options 51

Chapter 6 Quick Setup of an ISE Proof of Concept 59

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

Chapter 7 Building a Cisco ISE Network Access Security Policy 77

Chapter 8 Building a Device Security Policy 107

Chapter 9 Building an ISE Accounting and Auditing Policy 117

Part IV Let's Configure!

Chapter 10 Profiling Basics and Visibility 133

Chapter 11 Bootstrapping Network Access Devices 195

Chapter 12 Network Authorization Policy Elements 247

Chapter 13 Authentication and Authorization Policies 257

Chapter 14 Guest Lifecycle Management 299

Chapter 15 Client Posture Assessment 327

Chapter 16 Supplicant Configuration 365

Chapter 17 BYOD: Self-Service Onboarding and Registration 383

Chapter 18 Setting Up and Maintaining a Distributed ISE Deployment 439

Chapter 19 Remote Access VPN and Cisco ISE 465

Chapter 20 Deployment Phases 521

Part V Advanced Secure Access Features

Chapter 21 Advanced Profiling Configuration 537

Chapter 22 Cisco TrustSec AKA Security Group Access 557

Chapter 23 Passive Identities, ISE-PIC, and EasyConnect 593

Chapter 24 ISE Ecosystems: The Platform eXchange Grid (pxGrid) 631

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

Chapter 25 Understanding Monitoring, Reporting, and Alerting 659

Chapter 26 Troubleshooting 673

Chapter 27 Upgrading ISE 705

Part VII Device Administration

Chapter 28 Device Administration Fundamentals 721

Chapter 29 Configuring Device Admin AAA with Cisco IOS 739

Chapter 30 Configuring Device Admin AAA with Cisco WLC 759

Chapter 31 Configuring Device Admin AAA with Cisco Nexus Switches 777

Part VIII Appendixes

Appendix A Sample User Community Deployment Messaging Material 785

Appendix B Sample ISE Deployment Questionnaire 789

Appendix C Sample Switch Configurations 793

Appendix D The ISE CA and How Cert-Based Auth Works 807

Index 831

Contents

Introduction xxix

Part I Identity-Enabled Network: Unite!

Chapter 1 Regain Control of Your IT Security 1

Security: Still a Weakest-Link Problem 2

Cisco Identity Services Engine 3

Sources for Providing Identity and Context Awareness 5

Unleash the Power of Centralized Policy 6

Summary 8

Chapter 2 Fundamentals of AAA 9

Triple-A 10

Compare and Select AAA Options 10

Device Administration 11

Network Access 12

TACACS+ 13

TACACS+ Authentication Messages 14

TACACS+ Authorization and Accounting Messages 15

RADIUS 17

AV Pairs 20

Change of Authorization 20

Comparing RADIUS and TACACS+ 21

Summary 21

Chapter 3 Introducing Cisco Identity Services Engine 23

Architecture Approach to Centralized and Dynamic Network Security Policy Enforcement 23

Cisco Identity Services Engine Features and Benefits 26

ISE Platform Support and Compatibility 30

Cisco Identity Services Engine Policy Construct 30

ISE Authorization Rules 33

Summary 34

Part II The Blueprint, Designing an ISE-Enabled Network

Chapter 4 The Building Blocks in an Identity Services Engine Design 35

ISE Solution Components Explained 35

Infrastructure Components 36

Policy Components 42

Endpoint Components 42

ISE Personas 43

ISE Licensing, Requirements, and Performance 45

ISE Licensing 45

ISE Requirements 46

ISE Performance 47

ISE Policy-Based Structure Explained 48

Summary 49

Chapter 5 Making Sense of the ISE Deployment Design Options 51

Centralized Versus Distributed Deployment 52

Centralized Deployment 52

Distributed Deployment 55

Summary 58

Chapter 6 Quick Setup of an ISE Proof of Concept 59

Deploy ISE for Wireless in 15 Minutes 59

Wireless Setup Wizard Configuration 60

Guest Self-Registration Wizard 61

Secure Access Wizard 65

Bring Your Own Device (BYOD) Wizard 67

Deploy ISE to Gain Visibility in 15 Minutes 69

Visibility Setup Wizard 69

Configuring Cisco Switches to Send ISE Profiling Data 73

Summary 75

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

Chapter 7 Building a Cisco ISE Network Access Security Policy 77

Components of a Cisco ISE Network Access Security Policy 78

Network Access Security Policy Checklist 79

Involving the Right People in the Creation of the Network Access Security Policy 79

Determining the High-Level Goals for Network Access Security 81

Common High-Level Network Access Security Goals 82

Network Access Security Policy Decision Matrix 84

Defining the Security Domains 85

Understanding and Defining ISE Authorization Rules 87
Commonly Configured Rules and Their Purpose 88
Establishing Acceptable Use Policies 89
Host Security Posture Assessment Rules to Consider 91
Sample NASP Format for Documenting ISE Posture Requirements 96
Common Checks, Rules, and Requirements 97
Method for Adding Posture Policy Rules 98
Research and Information 98
Establishing Criteria to Determine the Validity of a Security Posture Check, Rule, or Requirement in Your Organization 99
Method for Determining What Posture Policy Rules a Particular Security Requirement Should Be Applied To 100
Method for Deploying and Enforcing Security Requirements 101
Defining Dynamic Network Access Privileges 102
Enforcement Methods Available with ISE 102
Commonly Used Network Access Policies 103
Summary 105

Chapter 8 Building a Device Security Policy 107
ISE Device Profiling 107
ISE Profiling Policies 109
ISE Profiler Data Sources 110
Using Device Profiles in Authorization Rules 111
Threat-Centric NAC 111
Using TC-NAC as Part of Your Incident Response Process 113
Summary 116

Chapter 9 Building an ISE Accounting and Auditing Policy 117
Why You Need Accounting and Auditing for ISE 117
Using PCI DSS as Your ISE Auditing Framework 118
ISE Policy for PCI 10.1: Ensuring Unique Usernames and Passwords 126
ISE Policy for PCI 10.2 and 10.3: Audit Log Collection 128
ISE Policy for PCI 10.5.3, 10.5.4, and 10.7: Ensure the Integrity and Confidentiality of Audit Log Data 129
ISE Policy for PCI 10.6: Review Audit Data Regularly 130
Cisco ISE User Accounting 131
Summary 132

Part IV Let's Configure!

Chapter 10 Profiling Basics and Visibility 133

Understanding Profiling Concepts 133

ISE Profiler Work Center 137

ISE Profiling Probes 137

Probe Configuration 138

DHCP and DHCPSPAN Probes 140

RADIUS Probe 142

Network Scan (NMAP) Probe 143

DNS Probe 147

SNMPQUERY and SNMPTRAP Probes 148

Active Directory Probe 149

HTTP Probe 150

HTTP Profiling Without Probes 152

NetFlow Probe 152

Infrastructure Configuration 153

DHCP Helper 153

SPAN Configuration 156

VLAN ACL Captures 157

Device Sensor 157

VMware Configurations to Allow Promiscuous Mode 159

Profiling Policies 160

Profiler Feed Service 160

Configuring the Profiler Feed Service 160

Verifying the Profiler Feed Service 162

Offline Manual Update 164

Endpoint Profile Policies 167

Context Visibility 169

Logical Profiles 178

ISE Profiler and CoA 179

Global CoA 180

Per-Profile CoA 181

Global Profiler Settings 182

Configure SNMP Settings for Probes 182

Endpoint Attribute Filtering 182

NMAP Scan Subnet Exclusions 183

Profiles in Authorization Policies 183
Endpoint Identity Groups 183
EndPointPolicy 187
Importing Profiles 187
Verifying Profiling 189
The Dashboard 189
Endpoints Dashboard 189
Context Visibility 190
Device Sensor Show Commands 191
Triggered NetFlow: A Woland-Santuka Pro Tip 191
Summary 194

Chapter 11 Bootstrapping Network Access Devices 195

Cisco Catalyst Switches 195
Global Configuration Settings for Classic IOS and IOS 15.x Switches 196
Configure Certificates on a Switch 196
Enable the Switch HTTP/HTTPS Server 197
Global AAA Commands 198
Global RADIUS Commands 199
Create Local Access Control Lists for Classic IOS and IOS 15.x 202
Global 802.1X Commands 204
Global Logging Commands (Optional) 204
Global Profiling Commands 205
Interface Configuration Settings for Classic IOS and IOS 15.x Switches 207
Configure Interfaces as Switch Ports 208
Configure Flexible Authentication and High Availability 208
Configure Authentication Settings 211
Configure Authentication Timers 212
Apply the Initial ACL to the Port and Enable Authentication 213
Configuration Settings for C3PL Switches 213
Why Use C3PL? 213
Global Configuration for C3PL 216
Global RADIUS Commands for C3PL 217
Configure Local ACLs and Local Service Templates 219
Global 802.1X Commands 220
C3PL Fundamentals 221
Configure the C3PL Policies 222

Cisco Wireless LAN Controllers 225

AireOS Features and Version History 225

Configure the AAA Servers 226

Add the RADIUS Authentication Servers 226

Add the RADIUS Accounting Servers 227

Configure RADIUS Fallback (High Availability) 229

Configure the Airespace ACLs 229

Create the Web Authentication Redirection ACL 230

Add Google URLs for ACL Bypass 231

Create the Dynamic Interfaces for the Client VLANs 232

Create the Employee Dynamic Interface 233

Create the Guest Dynamic Interface 234

Create the Wireless LANs 236

Create the Guest WLAN 236

Create the Corporate SSID 240

Summary 245

Chapter 12 Network Authorization Policy Elements 247

ISE Authorization Policy Elements 247

Authorization Results 251

Configuring Authorization Downloadable ACLs 251

Configuring Authorization Profiles 253

Summary 256

Chapter 13 Authentication and Authorization Policies 257

Relationship Between Authentication and Authorization 257

Enable Policy Sets 258

Authentication Policy Goals 261

Accept Only Allowed Protocols 261

Route to the Correct Identity Store 261

Validate the Identity 261

Pass the Request to the Authorization Policy 262

Understanding Authentication Policies 262

Conditions 263

Allowed Protocols 266

Authentication Protocol Primer 268

Identity Store 271

Options 272

Common Authentication Policy Examples 272

Using the Wireless SSID 272

Remote-Access VPN 277

Alternative ID Stores Based on EAP Type 278

Authorization Policies 280

Goals of Authorization Policies 280

Understanding Authorization Policies 280

Role-Specific Authorization Rules 286

Authorization Policy Example 286

Employee and Corporate Machine Full-Access Rule 286

Internet Only for Mobile Devices 288

Employee Limited Access Rule 292

Saving Attributes for Reuse 295

Summary 297

Chapter 14 Guest Lifecycle Management 299

Overview of ISE Guest Services 301

Hotspot Guest Portal Configuration 302

Sponsored Guest Portal Configuration 304

Create an Active Directory Identity Store 304

Create ISE Guest Types 305

Create Guest Sponsor Groups 307

Authentication and Authorization Guest Policies 310

Guest Pre-Authentication Authorization Policy 310

Guest Post-Authentication Authorization Policy 312

Guest Sponsor Portal Configuration 313

Guest Portal Interface and IP Configuration 313

Sponsor and Guest Portal Customization 313

Sponsor Portal Behavior and Flow Settings 313

Sponsor Portal Page Customization 315

Guest Portal Behavior and Flow Settings 316

Guest Portal Page Customization 317

Creating Multiple Guest Portals 318

Guest Sponsor Portal Usage 318

Sponsor Portal Layout 319

Creating Guest Accounts 320

Managing Guest Accounts 320

Configuration of Network Devices for Guest CWA 321

Wired Switches 321

Wireless LAN Controllers 322

Summary 325

Chapter 15 Client Posture Assessment 327

ISE Posture Assessment Flow 329

Configure Global Posture and Client Provisioning Settings 331

Posture Client Provisioning Global Setup 331

Posture Global Setup 335

Posture General Settings 335

Posture Reassessments 336

Posture Updates 337

Acceptable Use Policy Enforcement 338

Configure the AnyConnect and NAC Client Provisioning Rules 339

AnyConnect Agent with ISE Compliance Module 339

AnyConnect Posture Profile Creation 340

AnyConnect Configuration File Creation 341

AnyConnect Client Provisioning Policy 343

Configure the Client Provisioning Portal 343

Configure Posture Elements 345

Configure Posture Conditions 345

Configure Posture Remediations 349

Configure Posture Requirements 353

Configure Posture Policy 355

Configure Host Application Visibility and Context Collection (Optional) 357

Enable Posture Client Provisioning and Assessment in Your ISE Authorization Policies 359

Posture Client Provisioning 359

Authorization Based On Posture Compliance 360

Posture Reports and Troubleshooting 361

Enable Posture Assessment in the Network 362

Summary 363

Chapter 16 Supplicant Configuration 365

Comparison of Popular Supplicants 366

Configuring Common Supplicants 367

Mac OS X 10.8.2 Native Supplicant Configuration 367

Windows GPO Configuration for Wired Supplicant 369

Windows 7, 8/8.1, and 10 Native Supplicant Configuration 373

Cisco AnyConnect Secure Mobility Client NAM 377

Summary 382

Chapter 17 BYOD: Self-Service Onboarding and Registration 383

BYOD Challenges 384

Onboarding Process 386

BYOD Onboarding 386

Dual SSID 387

Single SSID 387

Configuring NADs for Onboarding 388

ISE Configuration for Onboarding 392

End-User Experience 393

Configuring ISE for Onboarding 408

BYOD Onboarding Process Detailed 423

MDM Onboarding 429

Integration Points 430

Configuring MDM Integration 431

Configuring MDM Onboarding Policies 433

The Opposite of BYOD: Identify Corporate Systems 435

EAP Chaining 436

Summary 437

Chapter 18 Setting Up and Maintaining a Distributed ISE Deployment 439

Configuring ISE Nodes in a Distributed Environment 439

Make the Policy Administration Node a Primary Device 440

Register an ISE Node to the Deployment 442

Ensure the Persona of All Nodes Is Accurate 445

Understanding the HA Options Available 446

Primary and Secondary Nodes 446

Monitoring & Troubleshooting Nodes 446

Policy Administration Nodes 448

Policy Service Nodes and Node Groups 450

Create a Node Group 451

Add the Policy Service Nodes to the Node Group 452

Using Load Balancers 453

General Guidelines 454

Failure Scenarios 455

Anycast HA for ISE PSNs 456

Cisco IOS Load Balancing 459

Maintaining ISE Deployments 460

Patching ISE 460

Backup and Restore 462

Summary 463

Chapter 19 Remote Access VPN and Cisco ISE 465

Introduction to VPNs 465

Client-Based Remote Access VPN 468

Configuring a Client-Based RA-VPN on the Cisco ASA 469

Download the Latest AnyConnect Headend Packages 470

Prepare the Headend 471

Add an AnyConnect Connection Profile 473

Add the ISE PSNs to the AAA Server Group 478

Add a Client Address Pool 481

Perform Network Reachability Tasks 484

Configure ISE for the ASA VPN 487

Testing the Configuration 488

Perform a Basic AAA Test 488

Log In to the ASA Web Portal 490

Connect to the VPN via AnyConnect 492

Remote Access VPN and Posture 494

RA-VPN with Posture Flows 495

Adding the Access Control Lists to ISE and the ASA 496

Adding Posture Policies to the VPN Policy Set 499

Watching It Work 501

Extending the ASA Remote Access VPN Capabilities 507

Double Authentication 507

Certificate-Based Authentication 509

Provisioning Certificates 509

Authenticating the VPN with Certificates 515

Connecting to the VPN via CertProfile 518

Summary 519

Chapter 20 Deployment Phases 521

Why Use a Phased Approach? 521

A Phased Approach 523
Authentication Open Versus Standard 802.1X 524
Monitor Mode 526
Prepare ISE for a Staged Deployment 527
Create the Network Device Groups 528
Create the Policy Sets 529
Low-Impact Mode 530
Closed Mode 532
Transitioning from Monitor Mode to Your End State 534
Wireless Networks 535
Summary 535
Part V Advanced Secure Access Features
Chapter 21 Advanced Profiling Configuration 537
Profiler Work Center 537
Creating Custom Profiles for Unknown Endpoints 538
Identifying Unique Values for an Unknown Device 539
Collecting Information for Custom Profiles 541
Creating Custom Profiler Conditions 542
Creating Custom Profiler Policies 543
Advanced NetFlow Probe Configuration 544
Commonly Used NetFlow Attributes 546
Example Profiler Policy Using NetFlow 546
Designing for Efficient Collection of NetFlow Data 547
Configuration of NetFlow on Cisco Devices 548
Profiler CoA and Exceptions 550
Types of CoA 551
Creating Exceptions Actions 552
Configuring CoA and Exceptions in Profiler Policies 552
Profiler Monitoring and Reporting 553
Summary 556
Chapter 22 Cisco TrustSec AKA Security Group Access 557
Ingress Access Control Challenges 558
VLAN Assignment 558
Ingress Access Control Lists 560
What Is TrustSec? 562
So, What Is a Security Group Tag? 562

Defining the SGTs 564
Classification 565
Dynamically Assigning an SGT via 802.1X 566
Manually Assigning an SGT at the Port 567
Manually Binding IP Addresses to SGTs 568
Access Layer Devices That Do Not Support SGTs 569
Transport: SGT eXchange Protocol (SXP) 569
SXP Design 570
Configuring SXP on IOS Devices 572
Configuring SXP on Wireless LAN Controllers 573
Configuring SXP on Cisco ASA 576
Configuring SXP on ISE 578
Transport: pxGrid 579
Transport: Native Tagging 580
Configuring Native SGT Propagation (Tagging) 581
Configuring SGT Propagation on Cisco IOS Switches 582
Configuring SGT Propagation on a Catalyst 6500 584
Configuring SGT Propagation on a Nexus Series Switch 586
Enforcement 587
Traffic Enforcement with SGACLs 588
Creating TrustSec Matrices in ISE 590
Traffic Enforcement with Security Group Firewalls 591
Security Group Firewall on the ASA 591
Security Group Firewall on the ISR and ASR 592
Summary 592

Chapter 23 Passive Identities, ISE-PIC, and EasyConnect 593
Passive Authentication 594
Identity Sharing 596
Tenet 1: Learn 598
Active Directory 598
Syslog Sources 611
REST API Sources 614
Learning More Is Critical 615
Tenet 2: Share 615
pxGrid 616
CDA-RADIUS 617

Tenet 3: Use 617

Integration Details 618

Integration Summary 623

Tenet 4: Update 623

Logoff Detection with the Endpoint Probe 623

WMI Update Events 625

Session Timeouts 625

ISE Passive Identity Connector 626

EasyConnect 628

Summary 630

Chapter 24 ISE Ecosystems: The Platform eXchange Grid (pxGrid) 631

The Many Integration Types of the Ecosystem 632

MDM Integration 632

Rapid Threat Containment 632

Platform Exchange Grid 635

pxGrid in Action 637

Configuring ISE for pxGrid 639

Configuring pxGrid Participants 642

Configuring Firepower Management Center for pxGrid 642

Configuring the Web Security Appliance for pxGrid 649

Configuring Stealthwatch for pxGrid 652

Summary 658

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

Chapter 25 Understanding Monitoring, Reporting, and Alerting 659

ISE Monitoring 660

Cisco ISE Home Page 660

Context Visibility Views 663

RADIUS Live Logs and Live Sessions 666

Global Search 667

Monitoring Node in a Distributed Deployment 669

Device Configuration for Monitoring 669

ISE Reporting 670

Data Repository Setup 671

ISE Alarms 672

Summary 672

Chapter 26 Troubleshooting 673

Diagnostic Tools 674

RADIUS Authentication Troubleshooting 674

Evaluate Configuration Validator 675

TCP Dump 678

Endpoint Debug 680

Session Trace 682

Troubleshooting Methodology 685

Troubleshooting Authentication and Authorization 685

Log Deduplication 686

Active Troubleshooting 688

Option 1: No Live Logs Entry Exists 689

Option 2: An Entry Exists in the Live Logs 694

General High-Level Troubleshooting Flowchart 697

Troubleshooting WebAuth and URL Redirection 697

Debug Situations: ISE Logs 701

The Support Bundle 702

Summary 703

Chapter 27 Upgrading ISE 705

The Upgrade Process 705

Repositories 708

Configuring a Repository 708

Repository Types and Configuration 708

Performing the Upgrade 714

Command-Line Upgrade 718

Summary 720

Part VII Device Administration

Chapter 28 Device Administration Fundamentals 721

Device Administration in ISE 723

Large Deployments 724

Medium Deployments 725

Small Deployments 726

Enabling TACACS+ in ISE 726

Network Devices 727

Device Administration Global Settings 728

Connection Settings 729

Password Change Control 729

Session Key Assignment 729

Device Administration Work Center 730

Overview 730

Identities 731

Network Resources 733

Policy Elements 733

Device Admin Policy Sets 736

Reports 738

Summary 738

Chapter 29 Configuring Device Admin AAA with Cisco IOS 739

Preparing ISE for Incoming AAA Requests 739

Preparing the Policy Results 739

Create the Authorization Results for Network Administrators 740

Create the Authorization Results for Network Operators 742

Create the Authorization Results for Security Administrators 743

Create the Authorization Results for the Helpdesk 745

Preparing the Policy Set 747

Configuring the Network Access Device 749

Time to Test 752

Summary 758

Chapter 30 Configuring Device Admin AAA with Cisco WLC 759

Overview of WLC Device Admin AAA 759

Configuring ISE and the WLC for Device Admin AAA 761

Preparing ISE for WLC Device Admin AAA 761

Prepare the Network Device 761

Prepare the Policy Results 762

Configure the Policy Set 766

Adding ISE to the WLC TACACS+ Servers 768

Testing and Troubleshooting 770

Summary 775

Chapter 31 Configuring Device Admin AAA with Cisco Nexus Switches 777

Overview of NX-OS Device Admin AAA 777

Configuring ISE and the Nexus for Device Admin AAA 778

Preparing ISE for Nexus Device Admin AAA 778

Prepare the Network Device 778

Prepare the Policy Results 779

Configure the Policy Set 782

Preparing the Nexus Switch for TACACS+ with ISE 783

Enable TACACS+ and Add ISE to NX-OS 784

Summary 784

Part VIII Appendixes

Appendix A Sample User Community Deployment Messaging Material 785

Sample Identity Services Engine Requirement Change Notification Email 785

Sample Identity Services Engine Notice for a Bulletin Board or Poster 786

Sample Identity Services Engine Letter to Students 788

Appendix B Sample ISE Deployment Questionnaire 789

Appendix C Sample Switch Configurations 793

Catalyst 3000 Series, 12.2(55)SE 793

Catalyst 3000 Series, 15.0(2)SE 796

Catalyst 4500 Series, IOS-XE 3.3.0 / 15.1(1)SG 800

Catalyst 6500 Series, 12.2(33)SXJ 804

Appendix D The ISE CA and How Cert-Based Auth Works 807

Certificate-Based Authentication 808

Has the Digital Certificate Been Signed by a Trusted CA? 808

Has the Certificate Expired? 810

Has the Certificate Been Revoked? 811

Has the Client Provided Proof of Possession? 813

So, What Does Any of This Have to Do with Active Directory? 814

ISE's Internal Certificate Authority 815

Why Put a CA into ISE? 815

ISE CA PKI Hierarchy 815

The Endpoint CA 818

Reissuing CA Certificates 819

Configuring ISE to be a Subordinate CA to an Existing PKI 820

Backing Up the Certificates 823

Issuing Certificates from the ISE CA 826

Index 831

Reader Services

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

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

Command Syntax Conventions

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

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

Introduction

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

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

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

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

Who Should Read This Book?

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

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

How This Book Is Organized

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

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

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

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

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

Part V, "Advanced Secure Access Features": Dives into some of the more advanced solution features that truly differentiate the ISE secure access system. This part covers advanced configurations of the ISE profiling engine, Cisco TrustSec, high availability, backups, passive identity capabilities, EasyConnect, and context sharing with the Platform eXchange Grid (pxGrid).

Part VI, "Monitoring, Maintenance, and Troubleshooting for Network Access AAA": Examines the maintenance of ISE, backups, and upgrades. It covers how to troubleshoot not only ISE, but the entire secure access system, and how to use the tools provided in the ISE product. Common monitoring and maintenance tasks, as well as troubleshooting tools, are explained from a help-desk support technician's point of view.

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

Here is an overview of each of the 31 chapters:

- **Chapter 1, "Regain Control of Your IT Security":** This chapter introduces the concepts that brought us to the current evolutionary stage of network access security. It discusses the explosion of mobility, virtualization, social networking, and ubiquitous network access coupled with the consumerization of information technology.
- **Chapter 2, "Fundamentals of AAA":** This chapter reviews the critical security concept of authentication, authorization, and accounting (AAA); compares and contrasts the two main AAA types of network access and device administration; and dives into the foundations of RADIUS and TACACS+.
- **Chapter 3, "Introducing Cisco Identity Services Engine":** Cisco ISE makes up the backbone of Cisco's next-generation, context-aware, identity-based security policy solution. This chapter introduces this revolutionary product and provides an overview of its functions and capabilities.
- **Chapter 4, "The Building Blocks in an Identity Services Engine Design":** This chapter covers the components of the secure access solution, including ISE personas, licensing model, and the policy structure.
- **Chapter 5, "Making Sense of the ISE Deployment Design Options":** This chapter examines all the available personas in ISE and design options with the combination of those personas.
- **Chapter 6, "Quick Setup of an ISE Proof of Concept":** This chapter provides a high-level overview of the ISE personas, walks you through the initial configuration (called bootstrapping) of ISE itself, and introduces role-based access control (RBAC).
- **Chapter 7, "Building a Cisco ISE Network Access Security Policy":** This chapter guides you through the process of creating a comprehensive network access security policy (NASP) that you can use in an environment that is safeguarded by Cisco ISE.
- **Chapter 8, "Building a Device Security Policy":** This chapter explores ISE device profiling and Threat-Centric NAC features in some detail. The goal is to disclose the different ways in which ISE can identify device types and other contextual information about devices for use in an ISE policy.
- **Chapter 9, "Building an ISE Accounting and Auditing Policy":** This chapter covers why you need accounting and auditing for ISE; using PCI DSS as your ISE auditing

framework; and Cisco ISE user accounting. Understanding and keeping track of what is happening inside the network and inside of ISE is critical to achieving a successful ISE deployment.

- **Chapter 10, "Profiling Basics and Visibility":** This chapter introduces the concepts of profiling and configuration choices needed to create a foundation to build upon. It examines the different profiling mechanisms and the pros and cons related to each, discussing best practices and configuration details.
- **Chapter 11, "Bootstrapping Network Access Devices":** This key chapter examines the configuration of the NADs themselves and focuses on best practices to ensure a successful ongoing deployment.
- **Chapter 12, "Network Authorization Policy Elements":** This chapter examines the logical roles within an organization and how to create authorization results to assign the correct level of access based on that role.
- **Chapter 13, "Authentication and Authorization Policies":** This chapter explains the distinct and important difference between authentication and authorization policies, presents the pieces that make up the policies, and provides examples of how to create a policy in ISE that enforces the logical policies created in Chapter 12.
- **Chapter 14, "Guest Lifecycle Management":** Guest access has become an expected resource at companies in today's world. This chapter explains the full secure guest lifecycle management, from Web Authentication (WebAuth) to sponsored guest access and self-registration options.
- **Chapter 15, "Client Posture Assessment":** This chapter examines endpoint posture assessment and remediation actions, the configuration of the extensive checks and requirements, and how to tie them into an authorization policy.
- **Chapter 16, "Supplicant Configuration":** This chapter looks at configuration examples of the most popular supplicants.
- **Chapter 17, "BYOD: Self-Service Onboarding and Registration":** This critical chapter goes through a detailed examination of BYOD concepts, policies, and flows. Both the user and administrative experiences are detailed, as well as the integration between ISE and third-party MDM vendors and ISE's internal certificate authority (CA).
- **Chapter 18, "Setting Up and Maintaining a Distributed ISE Deployment":** Cisco ISE can be deployed in a scalable distributed model or as a standalone device. This chapter examines how ISE can be deployed in this distributed model, and the caveats associated. It also details high availability (HA) with technologies such as load balancing.
- **Chapter 19, "Remote Access VPN and Cisco ISE":** This chapter details the integration of ISE with remote access VPNs using the Cisco ASA.

- **Chapter 20, "Deployment Phases":** This chapter explains the best practices related to phasing in a secure network access deployment. The chapter goes through the phases of Monitor Mode, Low-Impact Mode, and Closed Mode deployments.
- **Chapter 21, "Advanced Profiling Configuration":** This chapter builds on what was learned and configured in Chapter 10, examining how to profile unknown endpoints and looking deeper into the profiling policies themselves.
- **Chapter 22, "Cisco TrustSec AKA Security Group Access":** This chapter introduces the next-generation policy model known as Cisco TrustSec and Security Group Tags.
- **Chapter 23, "Passive Identities, ISE-PIC, and EasyConnect":** Brand new for this second edition, this chapter compares and contrasts active versus passive identities, and the EasyConnect method of network access control.
- **Chapter 24, "ISE Ecosystems: The Platform eXchange Grid (pxGrid)":** Also brand new for this edition, this chapter discusses the use of ISE as the center of a security ecosystem, the importance of context sharing, and the best practices for deploying the Platform eXchange Grid (pxGrid).
- **Chapter 25, "Understanding Monitoring, Reporting, and Alerting":** This chapter explains the extensive and redesigned monitoring, reporting, and alerting mechanisms built into the ISE solution.
- **Chapter 26, "Troubleshooting":** This chapter aids the reader when having to troubleshoot the ISE identity-enabled network and its many moving parts.
- **Chapter 27, "Upgrading ISE":** This chapter focuses on the upgrading of ISE nodes using both the graphical tool and the command line, with a heavy focus on the secondary PAN first (SPF) method of upgrade.
- **Chapter 28, "Device Administration Fundamentals":** This chapter details the integration of device administration AAA and TACACS+ into the ISE solution and the design options for deploying it in parallel or in conjunction with network access AAA.
- **Chapter 29, "Configuring Device Admin AAA with Cisco IOS":** Building on Chapter 29, this chapter details the configuration of ISE and Cisco IOS–based Catalyst switches for the purposes of device administration AAA with TACACS+.
- **Chapter 30, "Configuring Device Admin AAA with Cisco WLC:** This chapter details the configuration of ISE and Cisco Wireless LAN Controllers for the purposes of device administration AAA with TACACS+.
- **Chapter 31, "Configuring Device Admin AAA with Cisco Nexus Switches":** This chapter details the configuration of ISE and Cisco Wireless LAN Controllers for the purposes of device administration AAA with TACACS+.

Chapter 18

Setting Up and Maintaining a Distributed ISE Deployment

This chapter covers the following topics:

- Configuring ISE nodes in a distributed environment
- Understanding the HA options available
- Using load balancers
- IOS load balancing
- Maintaining ISE deployments

Chapter 5, “Making Sense of the ISE Deployment Design Options,” discussed the many options within ISE design. At this point, you should have an idea of which type of deployment will be the best fit for your environment, based on the number of concurrent endpoints and the number of Policy Service Nodes (PSN) that will be used in the deployment. This chapter focuses on the configuration steps required to deploy ISE in a distributed design. It also covers the basics of using a load balancer and includes a special bonus section on a very cool high-availability (HA) configuration that uses Anycast routing, and covers patching distributed ISE deployments.

Configuring ISE Nodes in a Distributed Environment

All ISE nodes are installed in a standalone mode by default. When in a standalone mode, the ISE node is configured to run all personas by default. That means that the standalone node runs Administration, Monitoring, and Policy Service personas. Also, all ISE standalone nodes are configured as their own root certificate authority (CA).

It is up to you, the ISE administrator, to promote the first node to be a primary administration node and then join the additional nodes to this new deployment. At the time of joining, you also determine which services will run on which nodes; in other words, you determine which persona the node will have.

You can join more than one ISE node together to create a multinode deployment, known commonly in the field as an *ISE cube*. It is important to understand that before any ISE nodes can be joined together, they must trust each other's administrative certificate. Without that trust, you will receive a communication error stating that the "node was unreachable," but the root cause is the lack of trust.

Similar to a scenario of trying to connect to a secure website that is not using a trusted certificate, you would see an SSL error in your web browser. This is just like that, only it is based on Transport Layer Security (TLS).

If you are still using the default self-signed certificates in ISE, you'll be required to import the public certificate of each ISE node into each other ISE node's **Administration > System > Certificates > Trusted Certificates** screen, because they are all self-signed (untrusted) certificates and each ISE node needs to trust the primary node, and the primary node needs to trust each of the other nodes.

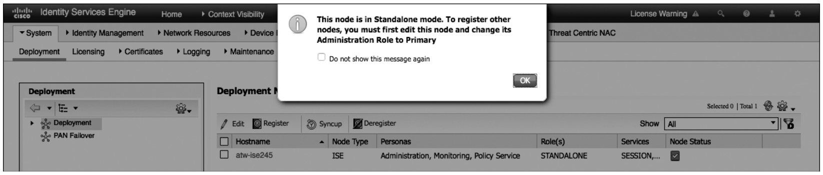
Instead of dealing with all this public key import for these self-signed certificates, the best practice is to always use certificates issued from the same trusted source. In that case, only the root certificates need to be added to the Trusted Certificates list.

Make the Policy Administration Node a Primary Device

Because all ISE nodes are standalone by default, you must first promote the ISE node that will become the Primary Policy Administration Node (PAN) to be a primary device instead of a standalone.

From the ISE GUI, perform the following steps:

Step 1. Choose **Administration > System > Deployment**. Figure 18-1 shows an example of the Deployment screen.



This node is in Standalone mode. To register other nodes, you must first edit this node and change its Administration Role to Primary

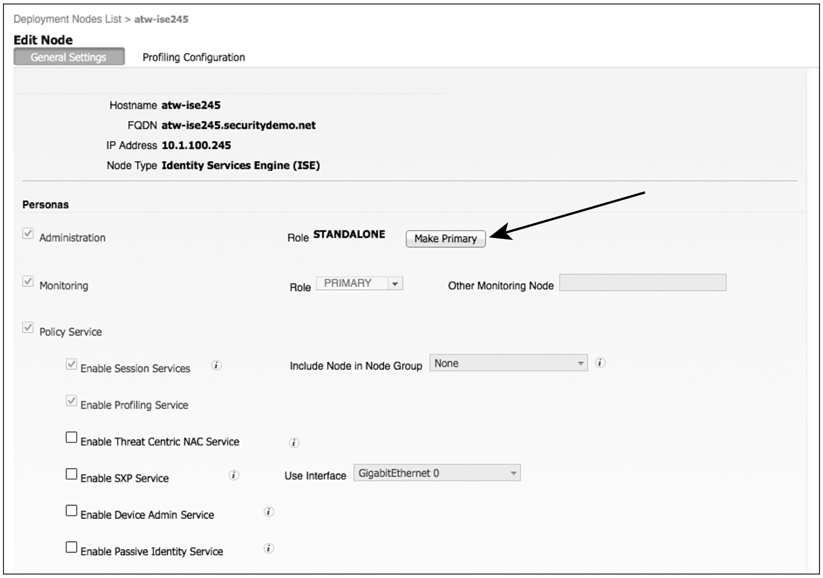
□ Do not show this message again

□	Hostname	Node Type	Personas	Role(s)	Services	Node Status
□	atw-ise245	ISE	Administration, Monitoring, Policy Service	STANDALONE	SESSION,...	☑

Figure 18-1 *Deployment Screen*

Step 2. Select the ISE node (there should only be one at this point).

Step 3. Click the **Make Primary** button, as shown in Figure 18-2.



Deployment Nodes List > atw-ise245

Edit Node

General Settings | Profiling Configuration

Hostname **atw-ise245**
FQDN **atw-ise245.securitydemo.net**
IP Address **10.1.100.245**
Node Type **Identity Services Engine (ISE)**

Personas

☑ Administration — Role **STANDALONE** [Make Primary]

☑ Monitoring — Role PRIMARY — Other Monitoring Node

☑ Policy Service

- ☑ Enable Session Services — Include Node in Node Group: None
- ☑ Enable Profiling Service
- ☐ Enable Threat Centric NAC Service
- ☐ Enable SXP Service — Use Interface: GigabitEthernet 0
- ☐ Enable Device Admin Service
- ☐ Enable Passive Identity Service

Figure 18-2 *Make Primary Button*

Step 4. At this point, the Monitoring and Policy Service check boxes on the left have become selectable. If the primary node will not also be providing any of these services, uncheck them now. (You can always return later and make changes.)

Step 5. Click **Save**.

After saving the changes, the ISE application restarts itself. This is a necessary process, as the sync services are started and the node prepares itself to handle all the responsibilities of the primary PAN persona. Once the application server has restarted, reconnect to the GUI, log in again, and proceed to the next section.

Note You can monitor the status of the application server by using the **show application status ise** command from the command-line interface through either the console or a Secure Shell (SSH) session to the ISE node, as shown in Example 18-1. When the application server state changes from initializing to running, then ISE will be ready for you to log in to.

Example 18-1 show application status ise *Command Output*

```
atw-ise245/admin# show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          5851
Database Server                        running          75 PROCESSES
Application Server                     initializing
Profiler Database                      running          6975
ISE Indexing Engine                    running          1821
AD Connector                           running          10338
M&T Session Database                   running          1373
M&T Log Collector                      running          2313
M&T Log Processor                      running          2219
Certificate Authority Service          disabled
EST Service                            disabled
SXP Engine Service                     disabled
TC-NAC Docker Service                  disabled
TC-NAC MongoDB Container               disabled
TC-NAC RabbitMQ Container              disabled
TC-NAC Core Engine Container           disabled
VA Database                            disabled
VA Service                             disabled
pxGrid Infrastructure Service          disabled
pxGrid Publisher Subscriber Service    disabled
pxGrid Connection Manager              disabled
pxGrid Controller                      disabled
PassiveID Service                      disabled
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled

atw-ise245/admin#
```

Register an ISE Node to the Deployment

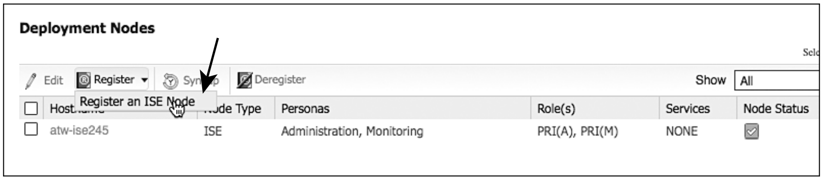
Now that there is a primary PAN, you can implement a multinode deployment. From the GUI on the primary PAN, you will register and assign personas to all ISE nodes.

From the ISE GUI on the primary PAN, perform the following steps:

Step 1. Choose **Administration > System > Deployment**.

Step 2. Choose **Register > Register an ISE Node**, as shown in Figure 18-3.

Note As with all other operations with ISE, DNS is a critical component.

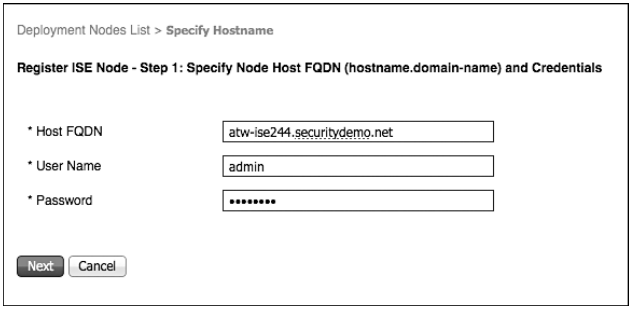


Deployment Nodes

□	Host	de Type	Personas	Role(s)	Services	Node Status
□	atw-ise245	ISE	Administration, Monitoring	PRI(A), PRI(M)	NONE	☑

Figure 18-3 *Choosing to Register an ISE Node*

Step 3. In the Host FQDN field, enter the IP address or DNS name of the first ISE node you will be joining to the deployment, as shown in Figure 18-4.



Deployment Nodes List > **Specify Hostname**

Register ISE Node - Step 1: Specify Node Host FQDN (hostname.domain-name) and Credentials

* Host FQDN: atw-ise244.securitydemo.net

* User Name: admin

* Password: ••••••••

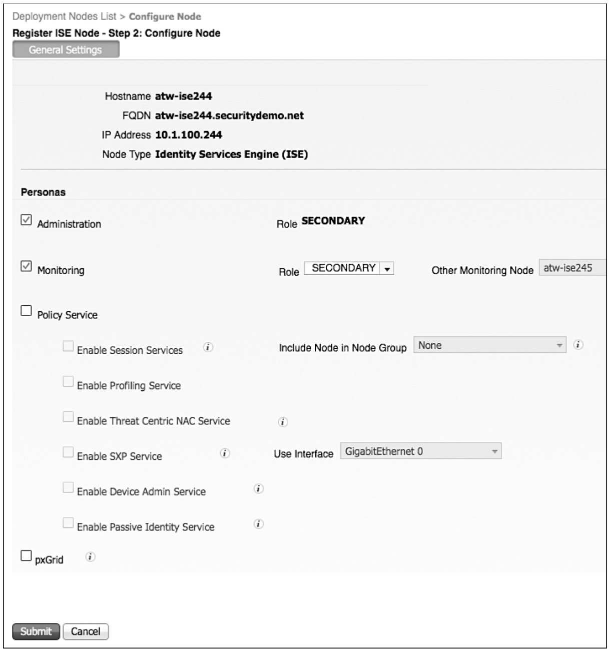
Figure 18-4 *Specifying Hostname and Credentials*

Step 4. In the User Name and Password fields, enter the administrator name (admin by default) and password.

Step 5. Click **Next**.

Note If you have not installed valid certificates from a trusted root, you will receive an error. You'll be required to install the certificate of each ISE node as a trusted root, because they are all self-signed certificates. Best practice is to always use certificates issued from a trusted source.

Step 6. On the Configure Node screen, shown in Figure 18-5, you can pick the main persona of the ISE node, including enabling of profiling services. You cannot, however, configure which probes to enable yet. Choose the persona for this node. Figure 18-5 shows adding a secondary Administration and Monitoring node, while Figure 18-6 shows adding a Policy Service Node.



Deployment Nodes List > **Configure Node**

Register ISE Node - Step 2: Configure Node

General Settings

Hostname **atw-ise244**
FQDN **atw-ise244.securitydemo.net**
IP Address **10.1.100.244**
Node Type **Identity Services Engine (ISE)**

Personas

☑ Administration — Role **SECONDARY**

☑ Monitoring — Role SECONDARY ▾ — Other Monitoring Node atw-ise245

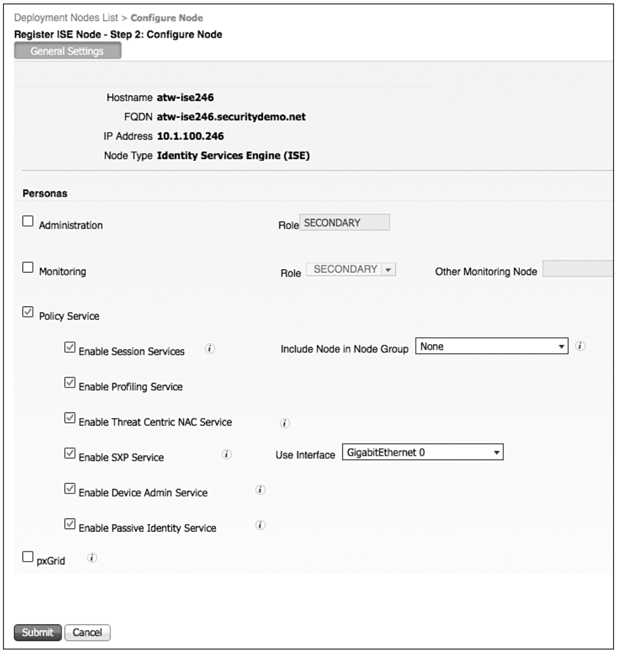
□ Policy Service

- □ Enable Session Services — Include Node in Node Group None ▾
- □ Enable Profiling Service
- □ Enable Threat Centric NAC Service
- □ Enable SXP Service — Use Interface GigabitEthernet 0 ▾
- □ Enable Device Admin Service
- □ Enable Passive Identity Service

□ pxGrid

Submit Cancel

Figure 18-5 *Configure Node Screen Secondary Admin and MnT Addition*



Deployment Nodes List > **Configure Node**

Register ISE Node - Step 2: Configure Node

General Settings

Hostname **atw-ise246**
FQDN **atw-ise246.securitydemo.net**
IP Address **10.1.100.246**
Node Type **Identity Services Engine (ISE)**

Personas

□ Administration — Role SECONDARY

□ Monitoring — Role SECONDARY ▾ — Other Monitoring Node

☑ Policy Service

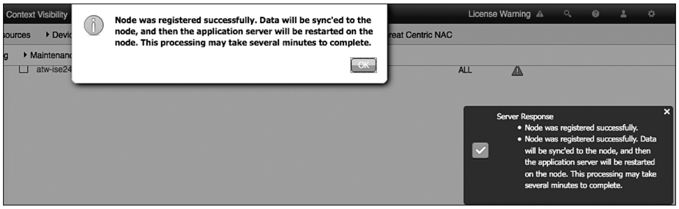
- ☑ Enable Session Services — Include Node in Node Group None ▾
- ☑ Enable Profiling Service
- ☑ Enable Threat Centric NAC Service
- ☑ Enable SXP Service — Use Interface GigabitEthernet 0 ▾
- ☑ Enable Device Admin Service
- ☑ Enable Passive Identity Service

□ pxGrid

Submit Cancel

Figure 18-6 *Configure Node Screen Policy Service Node Addition*

Step 7. Click **Submit.** At this point, the Policy Administration Node syncs the entire database to the newly joined ISE node, as you can see in Figure 18-7.



Node was registered successfully. Data will be sync'ed to the node, and then the application server will be restarted on the node. This processing may take several minutes to complete.

Server Response

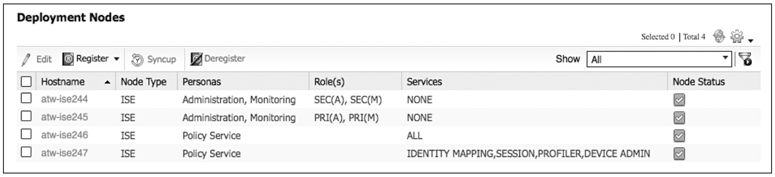
- Node was registered successfully.
- Node was registered successfully. Data will be sync'ed to the node, and then the application server will be restarted on the node. This processing may take several minutes to complete.

Figure 18-7 *Sync Initiated*

Step 8. Repeat these steps for all the ISE nodes that should be joined to the same deployment.

Ensure the Persona of All Nodes Is Accurate

Now that all of your ISE nodes are joined to the deployment, you can ensure that the correct personas are assigned to the appropriate ISE nodes. Table 18-1 shows the ISE nodes in the sample deployment and the associated persona(s) that will be assigned. Figure 18-8 shows the final Deployment screen, after the synchronization has completed for all nodes (a check mark in the Node Status column indicates a node that is healthy and in sync).



Deployment Nodes

Selected 0 | Total 4

Show All

□	Hostname	Node Type	Personas	Role(s)	Services	Node Status
□	atw-ise244	ISE	Administration, Monitoring	SEC(A), SEC(M)	NONE	☑
□	atw-ise245	ISE	Administration, Monitoring	PRI(A), PRI(M)	NONE	☑
□	atw-ise246	ISE	Policy Service		ALL	☑
□	atw-ise247	ISE	Policy Service		IDENTITY MAPPING,SESSION,PROFILER,DEVICE ADMIN	☑

Figure 18-8 *Final Personas and Roles*

Note This is also a good time to double-check that all the desired probes are enabled on the PSNs.

Table 18-1 *ISE Nodes and Personas*

ISE Node	Persona
atw-ise244	Administration, Monitoring
atw-ise245	Administration, Monitoring
atw-ise246	Policy Service
atw-ise247	Policy Service

Understanding the HA Options Available

There are many different items to note when it comes to high availability (HA) within a Secure Access deployment. There are the concerns of communication between the PANs and the other ISE nodes for database replications and synchronization, and communication between the PSNs and Monitoring nodes for logging. There is also the issue of authentication sessions from the network access devices (NAD) reaching the PSNs in the event of a WAN outage, as well as a NAD recognizing that a PSN may no longer be active, and sending authentication requests to the active PSN instead.

Primary and Secondary Nodes

PANs and Monitoring & Troubleshooting (MnT) nodes both employ the concept of primary and secondary nodes, but they operate very differently. Let's start with the easiest one first, the MnT node.

Monitoring & Troubleshooting Nodes

As you know, the MnT node is responsible for the logging and reporting functions of ISE. All PSNs will send their logging data to the MnT node as syslog messages (UDP port 20514).

When there are two monitoring nodes in an ISE deployment, all ISE nodes send their audit data to both monitoring nodes at the same time. Figure 18-9 displays this logging flow.

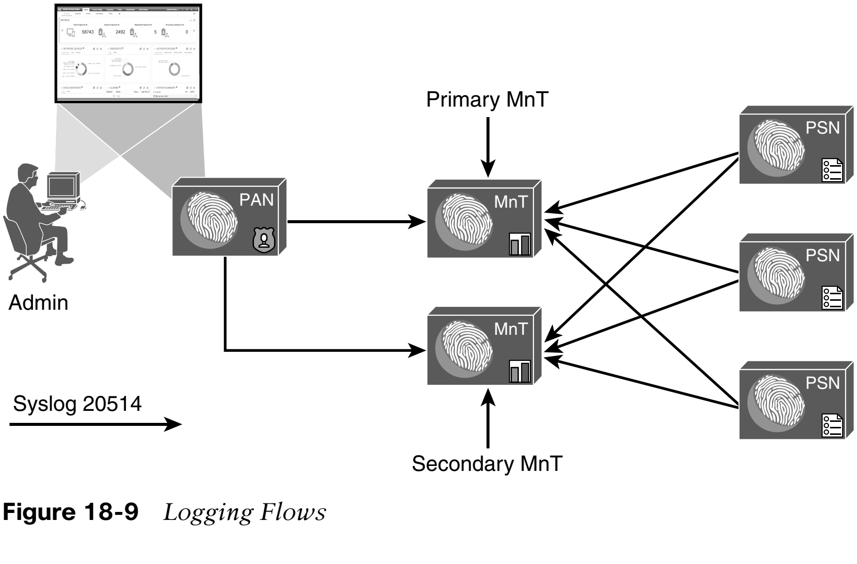
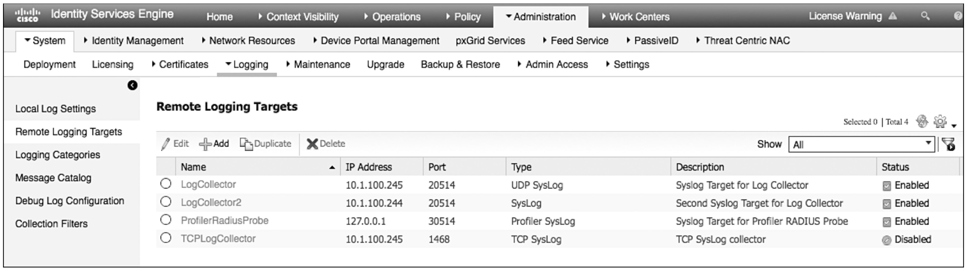


Figure 18-9 *Logging Flows*

The active/active nature of the MnT nodes can be viewed easily in the administrative console, as the two MnTs get defined as LogCollector and LogCollector2. Figures 18-10 and 18-11 display the log collector definitions and the logging categories, respectively.

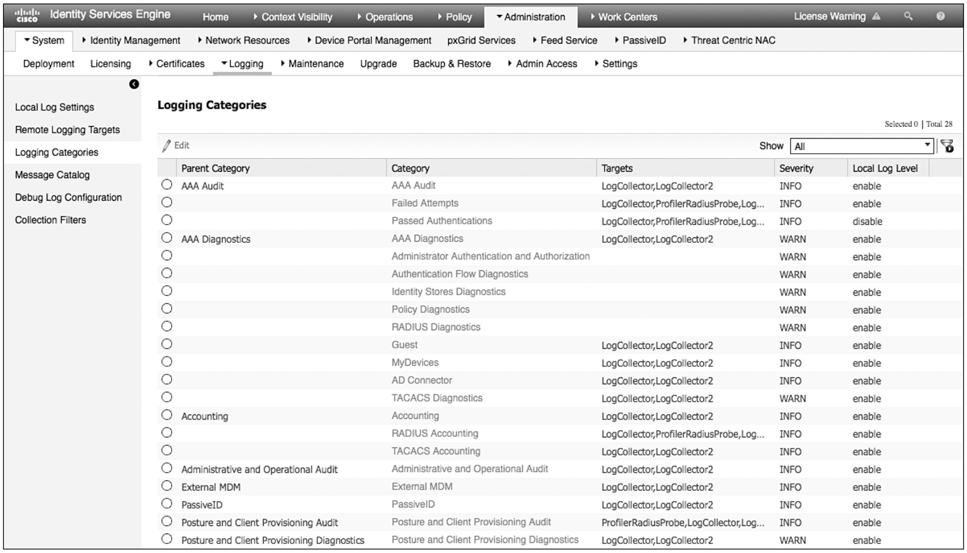


Remote Logging Targets

Selected 0 | Total 4

	Name	IP Address	Port	Type	Description	Status
○	LogCollector	10.1.100.245	20514	UDP SysLog	Syslog Target for Log Collector	☑ Enabled
○	LogCollector2	10.1.100.244	20514	SysLog	Second Syslog Target for Log Collector	☑ Enabled
○	ProfilerRadiusProbe	127.0.0.1	30514	Profiler SysLog	Syslog Target for Profiler RADIUS Probe	☑ Enabled
○	TCPLogCollector	10.1.100.245	1468	TCP SysLog	TCP SysLog collector	⊘ Disabled

Figure 18-10 *Logging Targets*



Logging Categories

Selected 0 | Total 28

	Parent Category	Category	Targets	Severity	Local Log Level
○	AAA Audit	AAA Audit	LogCollector,LogCollector2	INFO	enable
○		Failed Attempts	LogCollector,ProfilerRadiusProbe,Log...	INFO	enable
○		Passed Authentications	LogCollector,ProfilerRadiusProbe,Log...	INFO	disable
○	AAA Diagnostics	AAA Diagnostics	LogCollector,LogCollector2	WARN	enable
○		Administrator Authentication and Authorization		WARN	enable
○		Authentication Flow Diagnostics		WARN	enable
○		Identity Stores Diagnostics		WARN	enable
○		Policy Diagnostics		WARN	enable
○		RADIUS Diagnostics		WARN	enable
○		Guest	LogCollector,LogCollector2	INFO	enable
○		MyDevices	LogCollector,LogCollector2	INFO	enable
○		AD Connector	LogCollector,LogCollector2	INFO	enable
○		TACACS Diagnostics	LogCollector,LogCollector2	WARN	enable
○	Accounting	Accounting	LogCollector,LogCollector2	INFO	enable
○		RADIUS Accounting	LogCollector,ProfilerRadiusProbe,Log...	INFO	enable
○		TACACS Accounting	LogCollector,LogCollector2	INFO	enable
○	Administrative and Operational Audit	Administrative and Operational Audit	LogCollector,LogCollector2	INFO	enable
○	External MDM	External MDM	LogCollector,LogCollector2	INFO	enable
○	PassiveID	PassiveID	LogCollector,LogCollector2	INFO	enable
○	Posture and Client Provisioning Audit	Posture and Client Provisioning Audit	ProfilerRadiusProbe,LogCollector,Log...	INFO	enable
○	Posture and Client Provisioning Diagnostics	Posture and Client Provisioning Diagnostics	LogCollector,LogCollector2	WARN	enable

Figure 18-11 *Logging Categories*

Upon an MnT failure, all nodes continue to send logs to the remaining MnT node. Therefore, no logs are lost. The PAN retrieves all log and report data from the secondary MnT node, so there is no administrative function loss, either. However, the log database is not synchronized between the primary and secondary MnT nodes. Therefore, when the MnT node returns to service, a backup and restore of the monitoring node is required to keep the two MnT nodes in complete sync.

Note The best practice for logging is to also send logging data to a security information and event manager (SIEM) tool, for long-term data archiving and reporting.

Policy Administration Nodes

The PAN is responsible for providing not only an administrative GUI for ISE but also the critical function of database synchronization of all ISE nodes. All ISE nodes maintain a full copy of the database, with the master database existing on the primary PAN.

A PSN may receive data about a guest user, and when that occurs it must sync that data to the primary PAN. The primary PAN then synchronizes that data out to all the ISE nodes in the deployment.

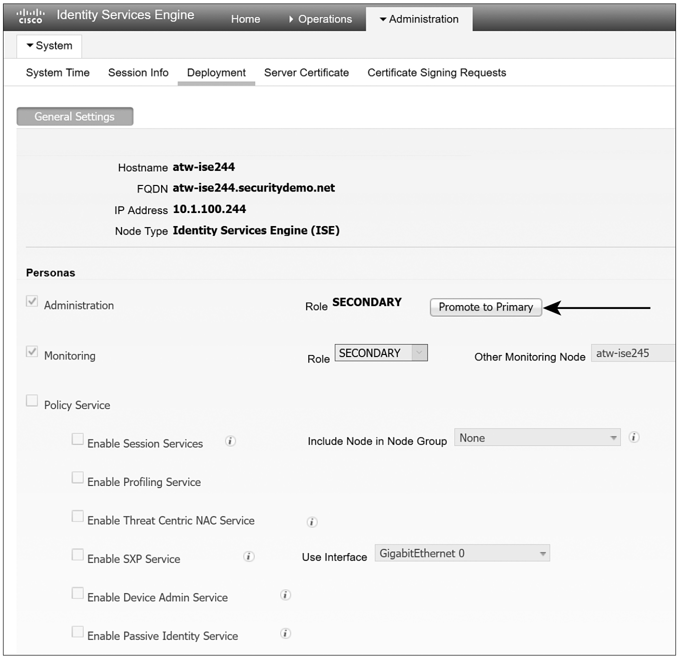
Because the functionality is so arduous, and having only a single source of truth for the data in the database is so critical, failing over to the secondary PAN is usually a manual process. In the event of the primary PAN going offline, no synchronizations occur until the secondary PAN is promoted to primary. Once it becomes the primary, it takes over all synchronization responsibility. This is sometimes referred to as a "warm spare" type of HA.

Promote the Secondary PAN to Primary

To promote the secondary PAN to primary, connect to the GUI on the secondary PAN and perform the following steps:

Step 1. Choose **Administration > System > Deployment**.

Step 2. Click **Promote to Primary**. Figure 18-12 illustrates the Promote to Primary option available on the secondary node.



Hostname **atw-ise244**
FQDN **atw-ise244.securitydemo.net**
IP Address **10.1.100.244**
Node Type **Identity Services Engine (ISE)**

Personas

☑ Administration — Role **SECONDARY**

☑ Monitoring — Role SECONDARY — Other Monitoring Node atw-ise245

□ Policy Service

□ Enable Session Services — Include Node in Node Group None

□ Enable Profiling Service

□ Enable Threat Centric NAC Service

□ Enable SXP Service — Use Interface GigabitEthernet 0

□ Enable Device Admin Service

□ Enable Passive Identity Service

Figure 18-12 *Promoting a Secondary PAN to Primary*

Auto PAN Failover

An automated promotion function was added to ISE beginning with version 1.4. It requires there to be two admin nodes (obviously) and at least one other non-admin node in the deployment.

The non-admin node will act as a health check function for the admin node(s), probing the primary admin node at specified intervals. The Health Check Node will promote the secondary admin node when the primary fails a configurable number of probes. Once the original secondary node is promoted, it is probed. Figure 18-13 illustrates the process.

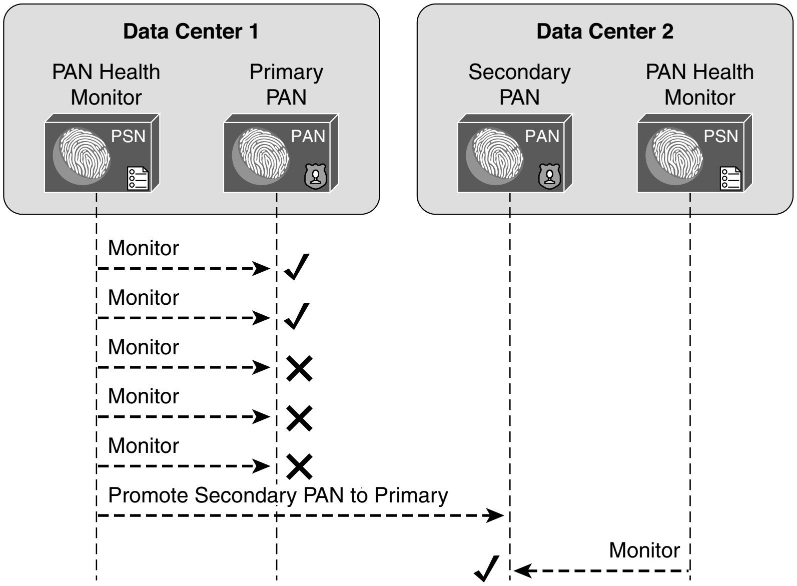


Figure 18-13 *Promoting a Secondary PAN to Primary with Automated Promotion*

As of ISE version 2.1, there is no ability to automatically sync the original primary PAN back into the ISE cube. That is still a manual process.

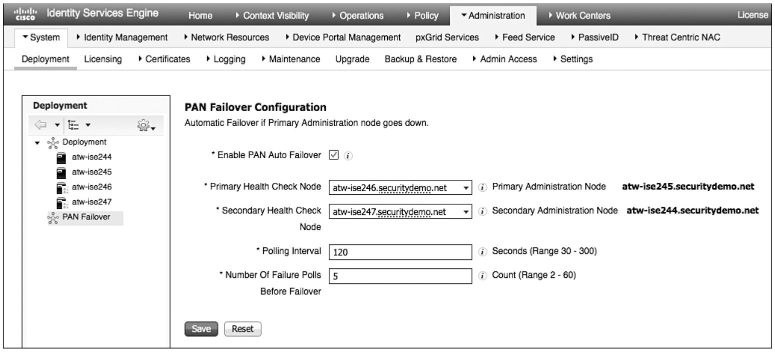
Configure Automatic Failover for the Primary PAN

For the configuration to be available, there must be two PANs and at least one non-PAN in the deployment.

From the ISE GUI, perform the following steps:

Step 1. Navigate to **Administration > System > Deployment**.

Step 2. Click **PAN Failover** in the left pane, as shown in Figure 18-14.



PAN Failover Configuration

Automatic Failover if Primary Administration node goes down.

* Enable PAN Auto Failover ☑

* Primary Health Check Node: atw-ise246.securitydemo.net — Primary Administration Node **atw-ise245.securitydemo.net**

* Secondary Health Check Node: atw-ise247.securitydemo.net — Secondary Administration Node **atw-ise244.securitydemo.net**

* Polling Interval: 120 — Seconds (Range 30 - 300)

* Number Of Failure Polls Before Failover: 5 — Count (Range 2 - 60)

Figure 18-14 *PAN Failover*

Step 3. Check the **Enable PAN Auto Failover** check box.

Step 4. Select the **Health Check Nodes** from the drop-down lists. Notice the primary PAN and secondary are listed to the right of the selected Health Check Nodes, as shown in Figure 18-14.

Step 5. In the Polling Interval field, set the polling interval. The interval is in seconds and can be set between **30** and **300** (5 minutes).

Step 6. In the Number of Failure Polls Before Failover field, enter the number of failed probes that have to occur before failover is initiated. Valid range is anywhere from **2–60** consecutive failed probes.

Step 7. Click **Save**.

Policy Service Nodes and Node Groups

PSNs do not necessarily need to have an HA type of configuration. Every ISE node maintains a full copy of the database, and the NADs have their own detection of a “dead” RADIUS server, which triggers the NAD to send AAA communication to the next RADIUS server in the list.

However, ISE has the concept of a *node group*. Node groups are made up of PSNs, where the PSNs maintain a heartbeat with each other. Beginning with ISE 1.3, the PSNs can be in different subnets or can be Layer 2 adjacent. In older ISE versions, the PSNs required the use of multicast, but starting in version 1.3 they use direct encrypted TCP-based communication instead:

- **TCP/7800:** Used for peer communication
- **TCP/7802:** Used for failure detection

If a PSN goes down and orphans a URL-redirected session, one of the other PSNs in the node group sends a Change of Authorization (CoA) to the NAD so that the endpoint can restart the session establishment with a new PSN.

Node groups do have another function, which is entirely related to data replication. ISE used a serial replication model in ISE 1.0, 1.1, and 1.1.x, meaning that all data had to go through the primary PAN and it sent the data objects to every other node, waiting for an acknowledgement for each piece of data before sending the next one in line.

Beginning with ISE 1.2 and moving forward, ISE begins to use a common replication framework known as JGroups (http://bfy.tw/5vYC). One of the benefits of JGroups is the way it handles replications in a group or segmented fashion. JGroups enables replications with local peers directly without having to go back through a centralized master, and node groups are used to define those segments or groups of peers.

So, when a member of a node group learns endpoint attributes (profiling), it is able to send the information directly to the other members of the node group directly. However, when that data needs to be replicated globally (to all PSNs), then the JGroups communication must still go through the primary PAN, which in turn replicates it to all the other PSNs.

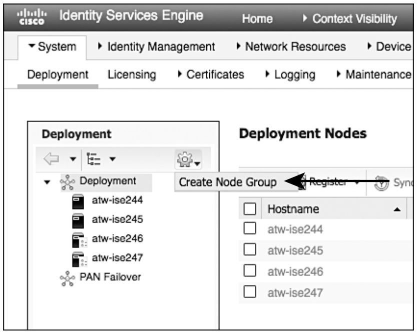
Node groups are most commonly used when deploying the PSNs behind a load balancer; however, there is no reason node groups could not be used with regionally located PSNs. You would not want to use a node group with PSNs that are geographically and logically separate.

Create a Node Group

To create a node group, from the ISE GUI, perform the following steps:

Step 1. Choose **Administration > System > Deployment.**

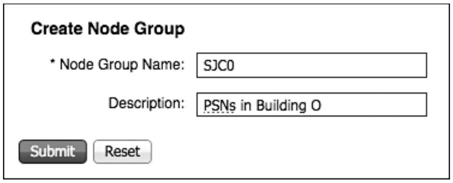
Step 2. In the Deployment pane on the left side of the screen, click the cog icon and choose **Create Node Group**, as shown in Figure 18-15.



☐ Hostname
☐ atw-ise244
☐ atw-ise245
☐ atw-ise246
☐ atw-ise247

Figure 18-15 *Choosing to Create a Node Group*

Step 3. On the Create Node Group screen, shown in Figure 18-16, enter in the Node Group Name field a name for the node group. Use a name that also helps describe the location of the group. In this example, SJCO was used to represent San Jose, Building O.



Create Node Group

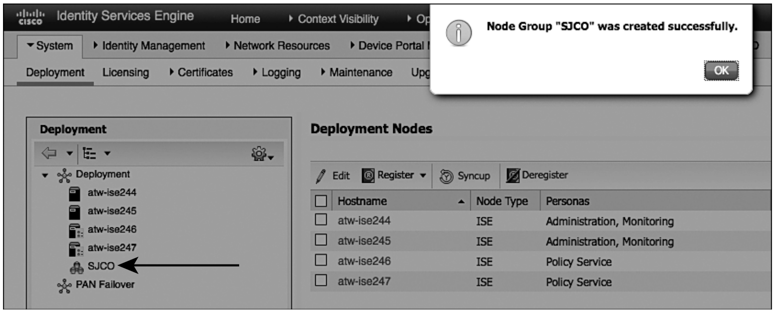
* Node Group Name: SJC0

Description: PSNs in Building O

Figure 18-16 *Node Group Creation*

Step 4. (Optional) In the Description field, enter a more detailed description that helps to identify exactly where the node group is (for example, PSNs in Building O). Click **Submit.**

Step 5. Click **OK** in the success popup window, as shown in Figure 18-17. Also notice the appearance of the node group in the left pane.



Node Group "SJCO" was created successfully.

Deployment Nodes

☐	Hostname	Node Type	Personas
☐	atw-ise244	ISE	Administration, Monitoring
☐	atw-ise245	ISE	Administration, Monitoring
☐	atw-ise246	ISE	Policy Service
☐	atw-ise247	ISE	Policy Service

Figure 18-17 *Success Popup*

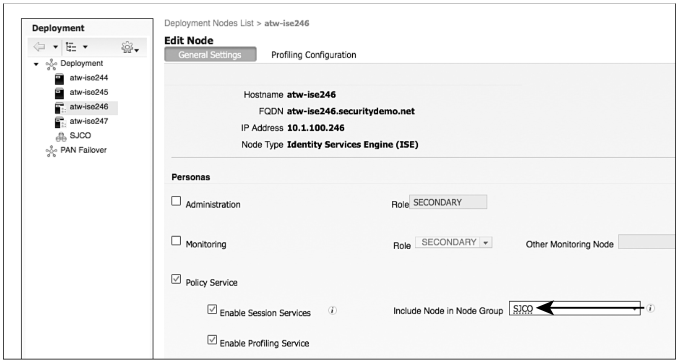
Add the Policy Service Nodes to the Node Group

To add the PSNs to the node group, from the ISE GUI, perform the following steps:

Step 1. Choose **Administration > System > Deployment.**

Step 2. Select one of the PSNs to add to the node group.

Step 3. Click the **Include Node in Node Group** drop-down arrow and select the newly created group, as shown in Figure 18-18.



Edit Node

Hostname **atw-ise246**
FQDN **atw-ise246.securitydemo.net**
IP Address **10.1.100.246**
Node Type **Identity Services Engine (ISE)**

Personas

□ Administration Role SECONDARY

□ Monitoring Role SECONDARY Other Monitoring Node

☑ Policy Service

☑ Enable Session Services Include Node in Node Group SJCO

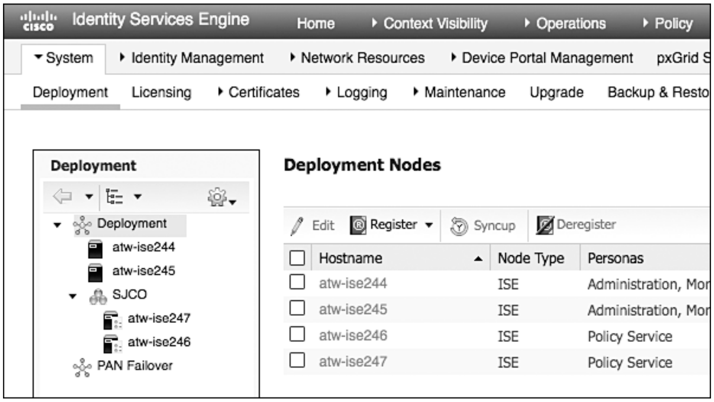
☑ Enable Profiling Service

Figure 18-18 *Assigning a Node Group*

Step 4. Click **Save**.

Step 5. Repeat the preceding steps for each PSN that should be part of the node group.

Figure 18-19 shows the reorganization of the PSNs within the node group in the Deployment navigation pane on the left side.



Deployment Nodes

□	Hostname	Node Type	Personas
□	atw-ise244	ISE	Administration, Mor
□	atw-ise245	ISE	Administration, Mor
□	atw-ise246	ISE	Policy Service
□	atw-ise247	ISE	Policy Service

Figure 18-19 *Reorganized Deployment Navigation Pane*

Using Load Balancers

One high-availability option that is growing in popularity for Cisco ISE deployments is the use of load balancers. Load balancer adoption with ISE deployments has skyrocketed over the years because it can significantly simplify administration and designs in larger deployments. As Figure 18-20 illustrates, with load balancing, the NADs have to be configured with only one IP address per set of ISE PSNs, removing a lot of the complexity in the NAD configuration. The load balancer itself takes care of monitoring the ISE PSNs and removing them from service if they are down and allows you to scale more nodes behind the virtual IP (VIP) without ever touching the network device configuration again.

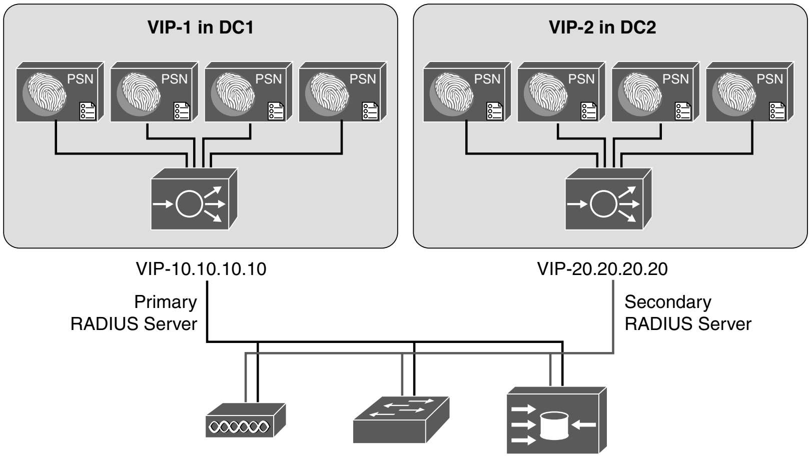


Figure 18-20 *Load-Balanced PSN Clusters*

Craig Hyps, a Principal Technical Marketing Engineer for ISE at Cisco, has written what is considered to be the definitive guide on load balancing with ISE, "How To: Cisco & F5 Deployment Guide: ISE Load Balancing Using BIG-IP." Craig wrote the guide based on using F5 load balancers, but the principles are identical regardless of which load balancer you choose to implement. You can find his guide here: https://communities.cisco.com/docs/DOC-68198.

Instead of replicating that entire large and detailed guide in this chapter, this section simply focuses on the basic principles that must be followed when using ISE with load balancers.

General Guidelines

When using a load balancer, you must ensure the following:

- Each PSN must be reachable by the PAN/MnT directly, without having to go through Network Address Translation (NAT). This sometimes is referred to as *routed mode* or *pass-through mode*.
- Each PSN must also be reachable directly from the endpoint.
  - When the PSN sends a URL-Redirection to the NAD, it uses the fully qualified domain name (FQDN) from the configuration, not the virtual IP (VIP) address.
  - You might want to use Subject Alternative Names (SAN) in the certificate to include the FQDN of the load-balancer VIP.
- The same PSN is used for the entire session. User persistence, sometimes called needs to be based on Calling-Station-ID.

- The VIP gets listed as the RADIUS server of each NAD for all 802.1X-related AAA.
    - Includes both authentication and accounting packets.
    - Some load balancers use a separate VIP for each protocol type.
- The list of RADIUS servers allowed to perform dynamic-authorizations (also known as Change of Authorization [CoA]) on the NAD should use the real IP addresses of the PSNs, not the VIP.

  The VIP could be used for the CoAs, if the load balancer is performing source NAT (SNAT) for the CoAs sent from the PSNs.

Note ISE uses the device's Layer 3 address to identity the NAD, not the NAS-IP-Address in the RADIUS packet. This is another reason to avoid SNAT for the incoming RADIUS requests.

- Load balancers should be configured to use test probes to ensure the PSNs are still "alive and well."
    - A probe should be configured to ensure RADIUS is responding.
    - HTTPS should also be checked.
    - If either probe fails, the PSN should be taken out of service.
    - A PSN must be marked dead and taken out of service in the load balancer before the NAD's built-in failover occurs.
- Since the load balancer(s) should be configured to perform health checks of the RADIUS service on the PSN(s), the load balancer(s) must be configured as NADs in ISE so their test authentications may be answered correctly.

Failure Scenarios

If a single PSN fails, the load balancer takes that PSN out of service and spreads the load over the remaining PSNs. When the failed PSN is returned to service, the load balancer adds it back into the rotation. By using node groups along with a load balancer, another of the node group members issues a CoA-reauth for any sessions that were establishing. This CoA causes the session to begin again. At this point, the load balancer directs the new authentication to a different PSN.

NADs have some built-in capabilities to detect when the configured RADIUS server is "dead" and automatically fail over to the next RADIUS server configured. When using a load balancer, the RADIUS server IP address is actually the VIP address. So, if the entire VIP is unreachable (for example, the load balancer has died), the NAD should quickly fail over to the next RADIUS server in the list. That RADIUS server could be another VIP in a second data center or another backup RADIUS server.

Anycast HA for ISE PSNs

This section exists thanks to a friend of the author who is also one of the most talented and gifted technologists roaming the earth today. E. Pete Karelis, CCIE No. 8068, designed this high-availability solution for a small ISE deployment that had two data centers. Figure 18-21 illustrates the network architecture.

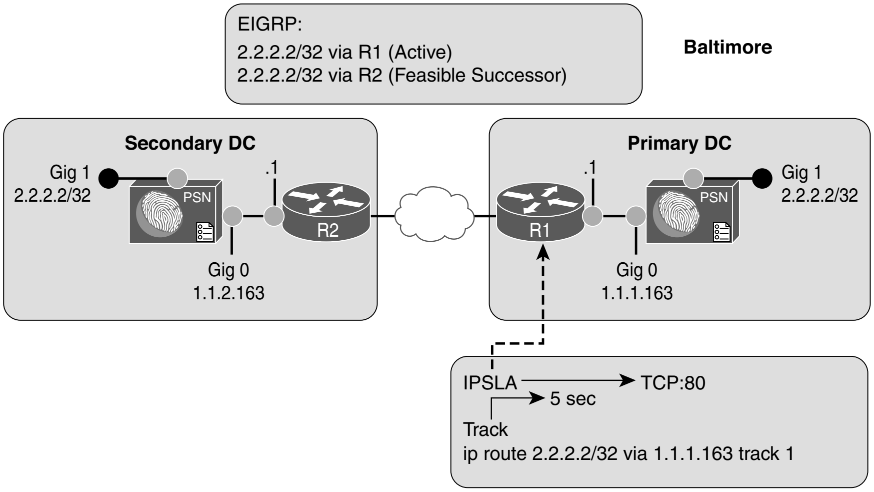


Figure 18-21 *Network Drawing and IPSLA*

Anycast is a networking technique where the same IP address exists in multiple places within the network. In this case, the same IP address (2.2.2.2) is assigned to the Gig1 interfaces on all the PSNs, which is connected to an isolated VLAN (or port group in VMware), so that the PSN sees the interface as "up" and connected with the assigned IP address (2.2.2.2). Each default gateway (router) in each data center is configured with a static route to 2.2.2.2/32 with the Gig0 IP address of the PSN as the next hop. Those static routes are redistributed into the routing protocol; in this case EIGRP is used. Anycast relies on the routing protocols to ensure that traffic destined to the Anycast address (2.2.2.2) is sent to the closest instance of that IP address.

After setting up Anycast to route 2.2.2.2 to the ISE PSN, Pete used EIGRP metrics to ensure that all routes preferred the primary data center, with the secondary data center route listed as the feasible successor (FS). With EIGRP, there is less than a 1-second delay when a route (the successor) is replaced with the backup route (the feasible successor).

Now, how do we make the successor route drop from the routing table when the ISE node goes down? Pete configured an IP service-level agreement (IPSLA) on the router that checked the status of the HTTP service on the ISE PSN in the data center every 5 seconds. If the HTTP service stops responding on the active ISE PSN, then the route is removed and the FS takes over, causing all the traffic for 2.2.2.2 to be sent to the PSN in the secondary data center. Figure 18-22 illustrates the IPSLA function, and when it occurs the only route left in the routing table is to the router at the secondary data center.

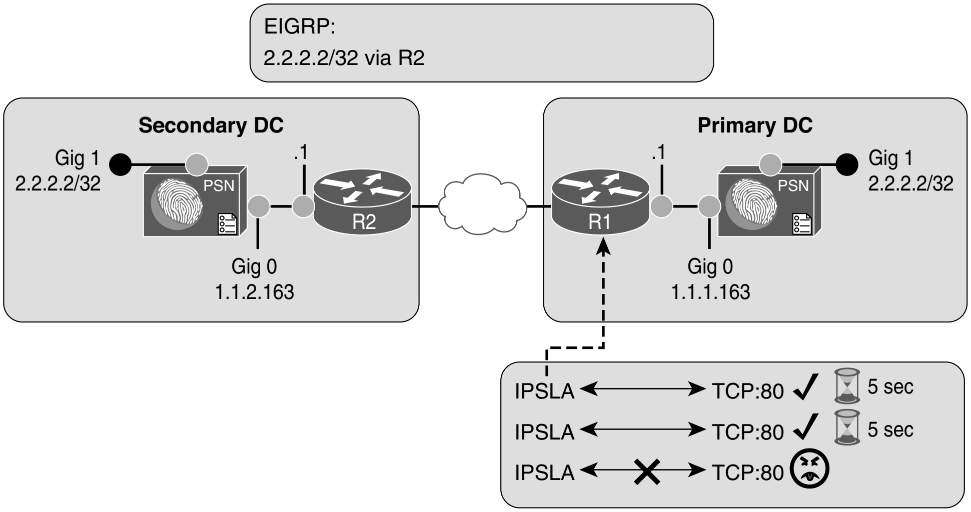


Figure 18-22 *IPSLA in Action*

All network devices are configured to use the Anycast address (2.2.2.2) as the only RADIUS server in their configuration. The RADIUS requests will always be sent to whichever ISE node is active and closest. Authentications originating within the secondary data center go to the local PSN.

Note The dynamic-authorization configuration of the NAD must still use the Gig0 interface IP addresses, as those will be the source when ISE sends a CoA to the switch.

Example 18-2 shows the interface configuration on the ISE PSN. The Gig0 interface is the actual routable IP address of the PSN, while Gig1 is in a VLAN to nowhere using the Anycast IP address.

Example 18-2 *ISE Interface Configuration*

```
interface gig 0
  !Actual  IP of Node
  ip address 1.1.1.163 255.255.255.0
interface gig 1
  !Anycast VIP assigned to all PSN nodes on G1
  ip address 2.2.2.2 255.255.255.255

ip default-gateway [Real Gateway for Gig0]
!note no static routes needed.
```

Example 18-3 shows the IPSLA configuration on the router, to test port 80 on the PSN every 5 seconds but to timeout after 1000 msec. When that timeout occurs, the IP SLA object will be marked as "down," which causes changed object tracking to remove the static route from the route table.

Example 18-3 *IPSLA Configuration*

```
ip sla 1
  !Test TCP to port 80 to the actual IP of the node.
  !"control disable" is necessary, since you are connecting to an
  !actual host instead of an SLA responder

  tcp-connect 1.1.1.163 80 control disable
  ! Consider the SLA as down if response takes longer than 1000msec

    threshold 1000
    ! Timeout after 1000 msec.
    timeout 1000
    !Test every 5 Seconds:
    frequency 5

ip sla schedule 1 life forever start-time now
track 1 ip sla 1
ip route 2.2.2.2 255.255.255.255 1.1.1.163 track 1
```

Example 18-4 shows the route redistribution configuration where the EIGRP metrics are applied. Pete was able to use the metrics that he chose specifically because he was very familiar with his network. His warning to others attempting the same thing is to be familiar with your network or to test thoroughly when identifying the metrics that would work for you.

Remember, you must avoid equal-cost, multiple-path routes, as this state could potentially introduce problems if RADIUS requests are not sticking to a single node. Furthermore, this technique is not limited to only two sites; Pete has since added a third location to the configuration and it works perfectly.

Note There is an obvious, albeit rare, flaw in the design. With this design, we are using HTTP to validate the status of the node, rather than validating the state of the RADIUS service itself, since the status of the RADIUS service cannot be queried by IOS Changed Object Tracking. This works very well in most cases, but in the rare event that the HTTP service on a PSN is operational and the RADIUS service is not operational, it could theoretically cause issues.

Example 18-4 *Route Redistribution*

```
router eigrp [Autonomous-System-Number]
  redistribute static route-map STATIC-TO-EIGRP

route-map STATIC-TO-EIGRP permit 20
  match ip address prefix-list ISE_VIP
  !Set metrics correctly
  set metric 1000000 1 255 1 1500

ip prefix-list ISE_VIP seq 5 permit 2.2.2.2/32
```

Cisco IOS Load Balancing

Cisco network devices have a lot of intelligence built into them to aid in an intelligent access layer for policy and policy enforcement. One such intelligence level is the capability to perform local load balancing of RADIUS servers. This does not mean using a Cisco switch as a server load balancer instead of a dedicated appliance. Instead, it refers to the capability of the access layer switch to load-balance the outbound authentication requests for endpoints that are authenticated to the switch itself.

Enabling IOS RADIUS server load balancing only takes one additional command. After all the PSNs are defined as AAA servers in the switch, use the **radius-server load-balance** global configuration command to enable it.

Example 18-5 shows use of a **show** command to verify that multiple ISE servers are configured.

Example 18-5 *Verifying All ISE PSNs Are Configured on Switch*

```
3750-X# show aaa server | include host
RADIUS: id 4, priority 1, host 10.1.100.232, auth-port 1812, acct-port 1813
RADIUS: id 5, priority 2, host 10.1.100.233, auth-port 1812, acct-port 1813
RADIUS: id 6, priority 3, host 10.1.100.234, auth-port 1812, acct-port 1813
```

Example 18-6 shows how to enable IOS load balancing

Example 18-6 *Enabling IOS Load Balancing*

```
3750-X(config)# radius-server load-balance method least-outstanding
  batch-size 5
```

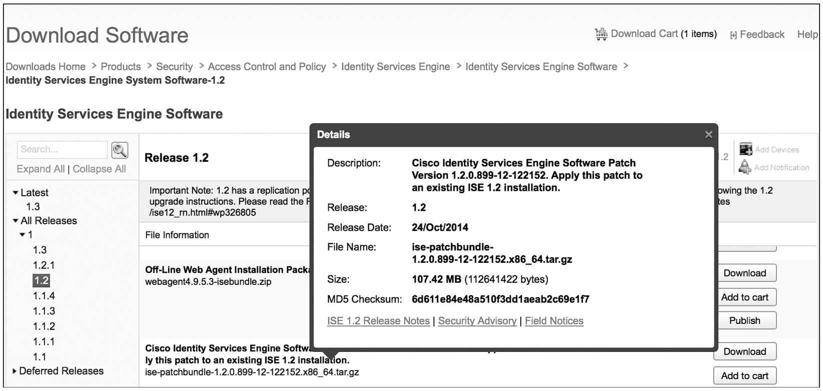
Maintaining ISE Deployments

Having a distributed deployment and load-balanced architecture are certainly critical items to scaling the deployment and ensuring it is highly available, but there are also critical basic maintenance items that should always be considered to ensure the most uptime and stability. That means having a patching strategy and a backup and restore strategy.

Patching ISE

Cisco releases ISE patches on a semi-regular basis. These patches contain bug fixes and, when necessary, security fixes. Think about the Heartbleed and Poodle vulnerabilities that were discovered with SSL. To ensure that bug fixes are applied, security vulnerabilities are plugged, and the solution works as seamlessly as possible, always have a planned patching strategy.

Patches are downloaded from Cisco.com, under **Downloads > Products > Security > Access Control and Policy > Identity Services Engine > Identity Services Engine Software**, as shown at the top of Figure 18-23.



Download Software

Downloads Home > Products > Security > Access Control and Policy > Identity Services Engine > Identity Services Engine Software >
Identity Services Engine System Software-1.2

Identity Services Engine Software

Release 1.2

Important Note: 1.2 has a replication po… owing the 1.2
upgrade instructions. Please read the F… tes
/ise12_rn.html#wp326805

File Information

Off-Line Web Agent Installation Packa…
webagent4.9.5.3-isebundle.zip

Cisco Identity Services Engine Softwa…
ly this patch to an existing ISE 1.2 installation.
ise-patchbundle-1.2.0.899-12-122152.x86_64.tar.gz

Details

Description: Cisco Identity Services Engine Software Patch Version 1.2.0.899-12-122152. Apply this patch to an existing ISE 1.2 installation.

Release: 1.2

Release Date: 24/Oct/2014

File Name: ise-patchbundle-1.2.0.899-12-122152.x86_64.tar.gz

Size: 107.42 MB (112641422 bytes)

MD5 Checksum: 6d611e84e48a510f3dd1aeab2c69e1f7

ISE 1.2 Release Notes | Security Advisory | Field Notices

Figure 18-23 *ISE Downloads Page*

Search the list of software available for your specific version of ISE. Figure 18-24 illustrates the naming convention for ISE patches. Cisco ISE patches are normally cumulative, meaning that installing 1.2 patch 12 will include all the fixes in patches 1 through 11 as well.

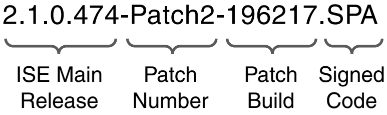


Figure 18-24 *Anatomy of ISE Patch Nomenclature*

After identifying the correct patch file, follow these steps:

Step 1. Download the required patch.

Step 2. From the ISE GUI, navigate to **Administration > System > Maintenance > Patch Management**.

Step 3. Click the **Install** button, as shown in Figure 18-25.

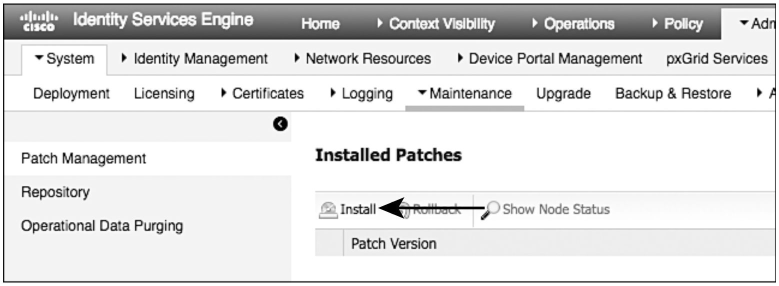
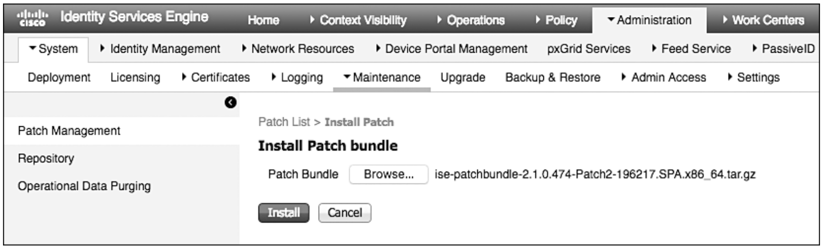


Figure 18-25 *Patch Management Screen*

Step 4. Click **Browse**, select the downloaded patch, and click **Install**, as shown in Figure 18-26.



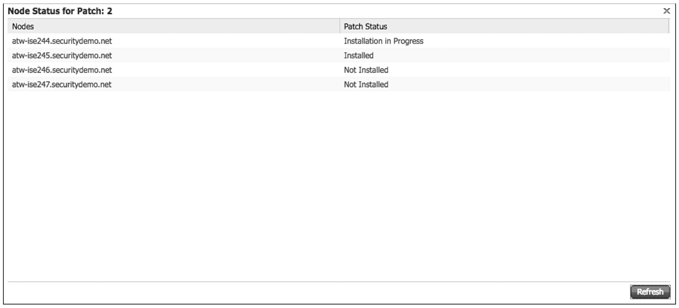
Patch Bundle Browse... ise-patchbundle-2.1.0.474-Patch2-196217.SPA.x86_64.tar.gz

Figure 18-26 *Installing the Selected Patch*

As the patch is installed on the PAN, you are logged out of the GUI and the patch is distributed from the PAN to all nodes in the ISE cube. After the patch is successfully installed on the PAN, it is applied to all nodes in the cube one at a time, in alphabetical order.

You can log back into the PAN when it's finished restarting services or rebooting. Click the **Show Node Status** button shown previously in Figure 18-25 to verify the progress of the patching. Figure 18-27 shows the resulting status of each node's progress for the patch installation.

Note PAN Auto Failover must be disabled before upgrading, and can be re-enabled after the upgrade is completed.



Node Status for Patch: 2

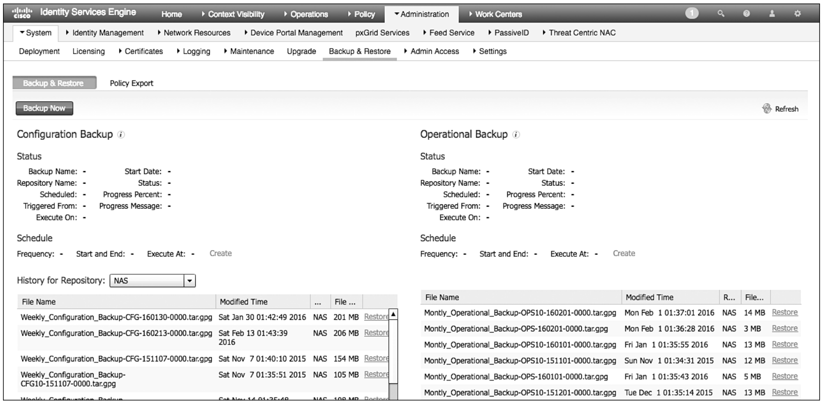
Nodes	Patch Status
atw-ise244.securitydemo.net	Installation in Progress
atw-ise245.securitydemo.net	Installed
atw-ise246.securitydemo.net	Not Installed
atw-ise247.securitydemo.net	Not Installed

Figure 18-27 *Node Status*

Backup and Restore

Another key strategy to assuring the availability of ISE in the environment is having a solid backup strategy. There are two types of ISE backups: configuration backup and operational backup. These two types are most easily related to backing up the product databases (configuration) and backing up the MnT data (operational).

Figure 18-28 shows the backup screen in ISE, located at **Administration > System > Backup & Restore**.



Configuration Backup

Status

Backup Name: - Start Date: -
Repository Name: - Status: -
Scheduled: - Progress Percent: -
Triggered From: - Progress Message: -
Execute On: -

Schedule

Frequency: - Start and End: - Execute At: - Create

History for Repository: NAS

File Name	Modified Time	...	File ...	
Weekly_Configuration_Backup-CFG-160130-0000.tar.gpg	Sat Jan 30 01:42:49 2016	NAS	201 MB	Restore
Weekly_Configuration_Backup-CFG-160213-0000.tar.gpg	Sat Feb 13 01:43:39 2016	NAS	206 MB	Restore
Weekly_Configuration_Backup-CFG-151107-0000.tar.gpg	Sat Nov 7 01:40:10 2015	NAS	154 MB	Restore
Weekly_Configuration_Backup-CFG10-151107-0000.tar.gpg	Sat Nov 7 01:35:51 2015	NAS	105 MB	Restore
Weekly_Configuration_Backup-	Sat Nov 14 01:35:48	NAS	108 MB	Restore

Operational Backup

Status

Backup Name: - Start Date: -
Repository Name: - Status: -
Scheduled: - Progress Percent: -
Triggered From: - Progress Message: -
Execute On: -

Schedule

Frequency: - Start and End: - Execute At: - Create

File Name	Modified Time	R...	File...	
Montly_Operational_Backup-OPS10-160201-0000.tar.gpg	Mon Feb 1 01:37:01 2016	NAS	14 MB	Restore
Montly_Operational_Backup-OPS-160201-0000.tar.gpg	Mon Feb 1 01:36:28 2016	NAS	3 MB	Restore
Montly_Operational_Backup-OPS10-160101-0000.tar.gpg	Fri Jan 1 01:35:55 2016	NAS	13 MB	Restore
Montly_Operational_Backup-OPS10-151101-0000.tar.gpg	Sun Nov 1 01:34:31 2015	NAS	12 MB	Restore
Montly_Operational_Backup-OPS-160101-0000.tar.gpg	Fri Jan 1 01:35:43 2016	NAS	5 MB	Restore
Montly_Operational_Backup-OPS10-151201-0000.tar.gpg	Tue Dec 1 01:35:14 2015	NAS	13 MB	Restore

Figure 18-28 *Backup & Restore Screen*

As shown in Figure 18-28, the backups are stored in a repository, and can be restored from the same repository. You can schedule backups to run automatically or you can run them manually on demand. You can view the status of a backup from either the GUI or the CLI, but you can view the status of a restore only from the CLI.

Summary

This chapter reviewed the basic principles of deploying distributed ISE nodes, high availability for ISE Policy Administration and Monitoring & Troubleshooting nodes. It examined the pillars of successful load balancing with ISE Policy Service Nodes, failover selection on Cisco Catalyst switches, and IOS load balancing.

This chapter also emphasized the importance of having regular backups in addition to a highly available design, and described where to configure those backups in addition to patching an ISE deployment.

Index

Numbers

802.1X, 5, 31, 36
- agents, 42–43
- configuration
  - *on C3PL switches, 220–221*
  - *on Classic IOS/IOS 15.x switches, 204*
- global commands
  - *for C3PL switches, 220–221*
  - *for Classic IOS/IOS 15.x switches, 204*
- phased deployment, 524–525
- supplicants
  - *choosing, 366–367*
  - *Cisco AnyConnect Secure Mobility Client NAM, 377–381*
  - *comparison of popular supplicants, 366–367*
  - *configuration, 365–366*
  - *definition of, 32, 42–43, 524*
  - *Mac OS X C10.8.2 native supplicant, 367–369*
  - *native supplicant provisioning, 365*
  - *Windows 7, 8/8.1, and 10 native supplicants, 373–377*
  - *Windows GPO configuration for wired supplicant, 369–373*

A

AAA (authentication, authorization, and accounting), 4, 9–10, 28. *See also* **auditing policy; authentication; authorization; device administration**
- AAA tests, 488–490
- AV (attribute-value) pairs, 20
- configuration on switches, 198–199
- credentials, 10
- global commands, 198–199
- network access, 12
- RADIUS, 17–20, 32
  - *AV (attribute-value) pairs, 20*
  - *C3PL switch configuration, 217–219*
  - *Classic IOS switch configuration, 199–201*
  - *CoA (Change of Authorization), 20–21*
  - *compared to TACACS+21*
  - *global commands, 199–203, 217–220*

IOS 15.x switch configuration, 201–202

Live Logs, 666–667, 686–696

Live Sessions views, 666–667

messages, 18–20

RADIUS probe, 74

RADIUS probes, 142–143

service types, 18

use cases, 17–18

WLC (Wireless LAN Controller) configuration, 226–229

TACACS+13–21

command sets, 733–734

enabling, 726–727

profiles, 734–736

troubleshooting, 685

active troubleshooting, 688–696

high-level troubleshooting flowchart, 697

ISE logs, 701–703

log deduplication, 686–688

WebAuth and URL redirection, 697–701

aaa authorization config-commands command, 751

AAA message, 670

ACCEPT packet, 14

acceptable use policy (AUP), 89–90

access control, 27

access control entries (ACE), 251–253

access control lists. ***See*** **ACLs (access control lists)**

Access Control Server (ACS), 13

Access Registrar, 13

Access Type field (authorization profiles), 254

Access-Accept messages, 18

Access-Challenge messages, 19

Access-Reject messages, 19

Access-Request messages, 18

accounting, 128–129. ***See also*** **AAA (authentication, authorization, and accounting)**

accounting messages, 15–17, 19

importance of, 117–118

user accounting, 131–132

Accounting-Request messages, 19

Accounting-Response messages, 20

accounts

administrator accounts, 126–127

guest accounts

creating, 320

managing, 320–321

ACE (access control entries), 251–253

ACLs (access control lists), 7

ACL bypass, 231–232

Airespace ACLs, 229–232

BYOD onboarding, 390–391

creating

for C3PL switches, 219–220

for Classic IOS/IOS 15.x switches, 202–203

dACLs (downloadable access control lists), 18, 36

configuration, 251–253

creating, 496–499

syntax checker, 253

for wired guests, 310–311

ingress ACLs, 560–561

RA-VPN with posture flows, 496–499

SGACLs, traffic enforcement with, 588–591

VLAN ACL capture configuration, 157

ACS (Access Control Server), 13

active authentication. ***See*** **authentication**

Active Directory. ***See*** **AD (Active Directory)**

Active Directory Run Time (ADRT) connector, 149

active troubleshooting

existing entry in Live Logs, 694–696

no Live Log entries exist, 689–694

steps for, 686–689

AD (Active Directory)

identity stores, 304–305

multi-forest Active Directory support, 29
passive identities, learning about, 598–599
ISE-PIC (Passive Identity Connector), 603–610
Kerberos sniffing via SPAN, 610–611
WMI (Windows Management Instrumentation), 599–603
probes, 149–150
Adapter Status report, 115
Adaptive Network Control (ANC), 634–635, 664
Adaptive Security Appliance (ASA), 32, 467, 621–622
addresses (MAC). ***See*** **MAC addresses**
AD-Host-Exists attribute, 149
AD-Join-Point attribute, 149
Admin nodes, 55
administration. ***See*** **device administration**
Administration persona, 43
administrator accounts, creating, 126–127
Administrator Change Configuration Audit report, 130
AD-Operating-System attribute, 150
AD-OS-Version attribute, 150
ADRT (Active Directory Run Time) connector, 149
AD-Service-Pack attribute, 150
Advanced Malware Protection (AMP), 6, 663
agent configuration file (ISE-PIC), 609
agents, 42–43
AireOS features (WLCs), 225–226
Airespace ACLs, 229–232
alarms, 672. ***See also*** **monitoring tools**
ALL role, 760
ALL_ACCOUNTS group, 308
AMP (Advanced Malware Protection), 6, 663
AMP Enabler module, 469
ANC (Adaptive Network Control), 634–635, 664
Android
BYOD onboarding, 401–408
onboarding flow, 425–428
Anycast HA (high availability), 456–459, 614
AnyConnect
AnyConnect Agent with ISE Compliance Module, 339
client provisioning policy, 343
configuration file creation, 341–342
Apex license, 45–46
Compliance Module, 43
connection profiles, 473–478
Headend packages, 469–470
Posture Agent, 91–95
Secure Mobility Client NAM, 377–381
Apex license, 45–46
Apple iOS onboarding, 394–401
application upgrade cleanup command, 719
application upgrade prepare command, 719
application upgrade proceed command, 719–720
architecture (ISE), 23. ***See also*** **deployment; ISE-enabled network design**
authorization rules, 33–34
centralized policy control operation, 23–26
endpoint components, 42–43
features and benefits, 3–5, 26–30
infrastructure components
feature-to-functionality mapping, 37
functionality of, 36–37
recommended components, 41
role of, 35–36
supported components, list of, 37–41
ISE personas, 43–45
licensing, 45–46

node types, 43–45

performance, 47–48

platform support and compatibility, 30

policy components, 42

policy construct, 30–33

policy-based structure, 48–49

requirements, 46–47

ASA (Adaptive Security Appliance), 32, 467, 621–622

assigning

SGTs (Security Group Tags), 566–568

VLANs, 558–560

attributes

for access control entries (ACE), 251–253

AD-Host-Exists, 149

AD-Join-Point, 149

AD-Operating-System, 150

AD-OS-Version, 150

AD-Service-Pack, 150

endpoint attributes, filtering, 182–183

EndPointPolicy, 187

MDM (mobile device management), 430–431

NetFlow probes, 546

saving for reuse, 295–297

attribute-value (AV) pairs, 253

auditing policy

audit logs

collection of, 128–129

ensuring integrity and confidentiality of, 129

logging categories, 128

regular audit data review, 129

remote logging targets, 129

importance of, 117–118

PCI DSS (Payment Card Industry Data Security Standard), 118–126

simplification of, 25

unique username and password enforcement, 126–128

user accounting, 128–129

AUP (acceptable use policy), 89–90, 338

authenticated guest access, 33

authentication, 4, 9–10, 28, 258–261. *See also* AAA (authentication, authorization, and accounting); passive authentication; supplicants

authenticated guest access, 33

authentication servers, 32

authenticators, 32

AV (attribute-value) pairs, 20

certificate-based

authenticating VPN with certificates, 515–518

connecting to VPN via CertProfile, 518–519

provisioning certificates, 509–515

compared to authorization, 257–258

configuration on switches, 211–213

credentials, 10

definition of, 10

device administration, 11, 28

double authentication, 507–508

Flex-Auth (Flexible Authentication), 208–211

network access, 12

open authentication, 524–525

policies, 310

allowed protocols, 266–271

alternative ID stores based on EAP type, 278–280

conditions, 263–266

definition of, 78

goals of, 261–262

guest post-authentication, 312

guest pre-authentication, 310–312

identity store, 271–272

policy sets, 258–260

processing of, 262–263

RA-VPN example, 277

wireless SSID example, 272–276

troubleshooting, 685

active troubleshooting, 688–696

high-level troubleshooting flowchart, 697

ISE logs, 701–703

log deduplication, 686–688

WebAuth and URL redirection, 697–701

VPNs (virtual private networks), 5

web authentication, 32, 36

authentication display legacy command, 213

authentication messages, 14–15

authentication open command, 523, 526, 530

authentication servers, 32

Authentications Summary report, 131

authenticators, 32. *See also* supplicants

authorization. *See also* AAA (authentication, authorization, and accounting); CoA (Change of Authorization)

authorization profiles

configuration, 253–255

RA-VPN with posture flows, 499–500

Authorization Results, 251–255

compared to authentication, 257–258

definition of, 10

device admin AAA with Cisco IOS

Helpdesk profile, 745–746

NetAdmin profile, 740–742

NetOps profile, 742–743

policy sets, 747–749

policies, 78, 247–251, 310

authorization based on posture compliance, 360–361

authorization profiles, 253–255

Authorization Results, 251

BYOD onboarding, 422–423

conditions, 249–250

dACLs (downloadable access control lists), 251–253

employee and corporate machine full-access rule, 286–288

employee limited access rule, 292–295

goals of, 280

guest post-authentication, 312

guest pre-authentication, 310–312

Internet only for mobile devices, 288–292

policy rules, 247–251

policy sets, 247–248

posture client provisioning, 359–360

processing of, 280–286

profiles in, 183–187

RA-VPN with posture flows, 501

rules, 286

saving attributes for reuse, 295–297

profiles, 421–422

roles, 111

rules, 33–34, 87–89

TACACS+ messages, 15–17

troubleshooting, 685

active troubleshooting, 688–696

high-level troubleshooting flowchart, 697

ISE logs, 701–703

log deduplication, 686–688

WebAuth and URL redirection, 697–701

Authorization Results, 251

authorization profiles, 253–255

dACLs (downloadable access control lists), 251–253

auto PAN (Policy Administration Node) failover, 449–450

AV (attribute-value) pairs, 20, 253

B

backups, 462

bandwidth

centralized deployment, 54

distributed deployment, 56–57

Base license, 45–46

benefits of Cisco ISE (Identity Services Engine), 3–5, 26–30

Blacklist Identity Group, 185–186

bootstrapping. *See* configuration

Bring Your Own Device (BYOD) Wizard, 67–69

business-based access, 25

business-policy enforcement, 26

BYOD onboarding, 27, 386

accelerating, 25

Android onboarding flow, 425–428

dual SSID, 387

end-user experience, 393–394

dual-SSID onboarding with Android, 401–408

single-SSID onboarding with Apple iOS, 394–401

iOS onboarding flow, 423–425

ISE configuration, 392–393

authorization policy rules, 422–423

authorization profiles, 421–422

certificate template, 411–413

client provisioning policy, 413–415

default unavailable client provisioning policy action, 420–421

native supplicant profile, 408–411

WebAuth portals, 415–420

NADs (network access devices)

required ACLs (access control lists), 390–391

URLs, adding to ACL_WEBAUTH_REDIRECT, 392

WLC (Wireless LAN Controller) configuration, 388–390

single SSID, 387–388

Windows and Mac OS onboarding flow, 428–429

BYOD Wizard, 67–69

C

C3PL switch configuration, 196, 213–215

ACLs (access control lists), 219–220

certificates, 216–217

differentiated authentication, 214

global 802.X commands, 220–221

global RADIUS commands, 217–219

local service templates, 219–220

policies, 222–224

CA (certificate authority), 4, 28, 439, 638

capabilities of Cisco ISE (Identity Services Engine), 3–5, 23–26

Catalyst switches. *See* switches

CDA (Context Directory Agent), 594, 616

CDA-RADIUS, 617

CD-ROM repositories, 712

Central Web Authentication. *See* CWA (Central Web Authentication)

centralized deployment

bandwidth guidance, 54

considerations for, 53

diagram of, 52–53

centralized management, 26

centralized policy

advantages of, 6–7

Cisco ISE operation, 23–26

certificate authority. *See* CA (certificate authority)

certificates

certificate-based authentication

authenticating VPN with certificates, 515–518 *connecting to VPN via CertProfile, 518–519*

provisioning certificates, 509–515

configuration

for C3PL switches, 216–217

on Classic IOS/IOS 15.x switches, 196–197

importing, 440

provisioning, 509–515

renewing for EAP-TLS, 271

templates, 411–413

certifications, 30

CertProfile, 518–519

chaining (EAP), 436–437

Challenge Handshake Authentication Protocol (CHAP), 12

Change Configuration Audit report, 162

Change of Authorization. *See* CoA (Change of Authorization)

CHAP (Challenge Handshake Authentication Protocol), 12, 268

Cisco Access Registrar, 13

Cisco Adaptive Security Appliance. *See* ASA (Adaptive Security Appliance)

Cisco Advanced Malware Protection. *See* AMP (Advanced Malware Protection)

Cisco AnyConnect. *See* AnyConnect

Cisco Catalyst switches. *See* switches

Cisco Context Directory Agent (CDA), 594, 616

Cisco Firepower Management Center (FMC). *See* FMS (Firepower Management Center)

Cisco Firepower Threat Defense (FTD), 467

Cisco IOS. *See* IOS (Cisco)

Cisco ISE (Identity Services Engine). *See* ISE-enabled network design

Cisco NAC Appliance, 24

Cisco NGFW, 6

Cisco Platform Exchange Grid. *See* pxGrid (Platform Exchange Grid)

Cisco Rapid Threat Containment, 29, 632–635

Cisco Secure Access Control Server (ACS), 13

Cisco Stealthwatch. *See* Stealthwatch

Cisco Terminal Services (TS) Agent, 615

Cisco TrustSec. *See* TrustSec

Cisco Wireless LAN Controller. *See* WLCs (Wireless LAN Controllers)

classes, control, 222–223

Classic IOS switch configuration, 196

ACLs (access control lists), 202–203

authentication settings, 211–212

authentication timers, 212

certificates, 196–197

Flex-Auth (Flexible Authentication), 208–211

global 802.X commands, 204

global AAA commands, 198–199

global logging commands, 204–205

global profiling commands, 205–207

global RADIUS commands, 199–202

HTTP/HTTPS server, 197

Monitor Mode, 213

native SGT propagation, 582–584

switch port interfaces, 208

classification of SGTs (Security Group Tags), 565–566

client address pools, assigning, 481–484

client posture assessment. *See* posture assessment

client provisioning policy

configuration, 413–415

default unavailable client provisioning policy action, 420–421

client provisioning portal, 343–344

client supplicants. *See* supplicants

client-based remote access VPNs

configuration

AnyConnect connection profiles, 473–478

AnyConnect Headend packages, 469–470

client address pool, 481–484

configuration tools, 469–470

Headend preparation, 471–473

ISE configuration, 487–488

network reachability tasks, 484–487

PSNs (Policy Service Nodes), 478–481

security services modules, 468–469

connecting to, 490–491

overview of, 467–468

testing

AAA test, 488–490

connecting to VPN, 492–494

logging in to web portal, 490–491

clientless remote access VPNs, 466–467

Closed Mode, 532–534

CoA (Change of Authorization), 20–21, 36, 179–180

COA Events report, 115

CoA menu, 663–665

CoA-Push, 477, 496

CoA-ReAuth, 477

conditions producing, 550–551

configuration, 552–553

exceptions, 552

global CoA, 180–181

per-profile CoA, 181

types of, 551–552

Cognitive Threat Analysis (CTA), 663

CollectData SGT (Security Group Tag), 194

command sets, 21, 733–734

commands

802.1X commands, 204, 220–221

aaa authorization config-commands, 751

AAA commands, 198–199

application upgrade cleanup, 719

application upgrade prepare, 719

application upgrade proceed, 719–720

authentication display legacy, 213

authentication open, 523, 526, 530

cts role-based sgt-map, 569

cts role-based sgt-map vlan-list, 569

epm logging, 669

interface range, 208

ip dhcp relay ISE_PSN_address, 75

ip domain-name, 197

ip helper-address, 153–156

ip helper-address ISE_PSN_address, 74

ip http secure-server, 197

ip http server, 197

ip radius source-interface, 669, 690, 693

ip tacacs source-interface, 669

logging commands, 204–205

logging source-interface, 669

monitor session, 156

nslookup, 700

ping, 700

profiling commands, 205–207

RADIUS commands, 199–203, 217–220

radius-server load-balance, 459

service-policy, 224

show aaa server, 459

show application status ise, 441–442

show authentication session interface, 691–692, 693–694, 698

show device-sensor, 191

show ip access-list interface, 700

show ip interface brief, 692

show privilege, 756

show repository, 713

show role feature, 778

show role feature-group, 778

show running-config, 710–711

show tech-support, 702

show vpn-sessiondb detail anyconnect, 503–506

source-interface, 669

switchport, 208

test aaa, 752

username, 751

COMMANDS role, 760

committees (NASP), 79–81

Common Classification Policy Language switches. *See* C3PL switch configuration

Common Criteria, 30

Common Ports scan (NMAP), 146

Common Vulnerability Scoring System (CVSS), 111, 662

compliance, simplification of, 25

compound conditions, 249

conditions

authentication policy, 263–266

authorization policy, 249–250

ISE profiler, 108–109

posture conditions, 345–349

confidentiality of audit logs, 129

configuration. *See also* NASP (network access security policy); onboarding; profiling

802.1X supplicants, 365–366

Cisco AnyConnect Secure Mobility Client NAM, 377–381

comparison of popular supplicants, 366–367

Mac OS X C10.8.2 native supplicant, 367–369

Windows 7, 8/8.1, and 10 native supplicants, 373–377

Windows GPO configuration for wired supplicant, 369–373

alarms, 672

authorization policy, 247

authorization profiles, 253–255

Authorization Results, 251

conditions, 249–250

dACLs (downloadable access control lists), 251–253

policy rules, 247–251

policy sets, 247–248

authorization profiles, 253–255

auto PAN (Policy Administration Node) failover, 449–450

C3PL switches, 213–215

ACLs (access control lists), 219–220

certificates, 216–217

differentiated authentication, 214

global 802.X commands, 220–221

global RADIUS commands, 217–219

local service templates, 219–220

policies, 222–224

Classic IOS/IOS 15.x switches

ACLs (access control lists), 202–203

authentication settings, 211–212

authentication timers, 212

certificates, 196–197

Flex-Auth (Flexible Authentication), 208–211

global 802.X commands, 204

global AAA commands, 198–199

global logging commands, 204–205

global profiling commands, 205–207

global RADIUS commands, 199–202

HTTP/HTTPS server, 197

Monitor Mode, 213

switch port interfaces, 208

client-based remote access VPNs

AnyConnect connection profiles, 473–478

AnyConnect Headend packages, downloading, 469–470

client address pool, 481–484

configuration tools, 469–470

Headend preparation, 471–473

ISE configuration, 487–488

network reachability tasks, 484–487

PSNs (Policy Service Nodes), 478–481

security services modules, 468–469

testing, 488–494

CoA (Change of Authorization), 552–553

dACLs (downloadable access control lists), 251–253

device admin AAA with Cisco IOS

Helpdesk profile, 745–746

NAD (network access device) configuration, 749–752

NetAdmin profile, 740–742

NetOps profile, 742–743

overview of, 739

policy sets, 747–749

testing and troubleshooting, 752–758

user roles, 739–740

device admin AAA with Cisco Nexus switches, 777

Helpdesk profile, 781–782

NetAdmin profile, 779–780

NetOps profile, 780–781

network device preparation, 778–779

policy sets, 782–783

SecAdmin profile, 781

TACACS+, enabling, 783–784

user roles, 777–778

device admin AAA with Cisco WLC

Employee profile, 765–766

Helpdesk profile, 765

NetAdmin profile, 763–764

network device preparation, 761–762

overview of, 759–760

policy sets, 766–768

SecAdmin profile, 764

TACACS+, enabling, 768–770

testing and troubleshooting, 770–775

Device Administration Work Center, 728–729

Connection settings, 729

Device Admin Policy Sets, 736–738

Ext ID Sources, 732

Identities, 731–732

navigation UI, 730–731

Network Resources, 733

Password Change Control settings, 729

Policy Elements, 733–736

Reports, 738

Session Key Assignment settings, 729–730

User Identity Groups, 731–732

device configuration for monitoring, 669–670

guest services

guest accounts, 320–321

guest post-authentication authorization policy, 312

guest pre-authentication authorization policy, 310–312

hotspot guest portals, 302–303

sponsored guest portals, 302–318

ISE for wireless, 59–60

BYOD (Bring Your Own Device) Wizard, 67–69

Guest Self-Registration Wizard, 61–65

Secure Access Wizard, 65–67

Wireless Setup Wizard home page, 59–60

ISE nodes in distributed environment, 439–440
node personas and roles, 445
node registration, 442–445
primary PANs, 440–442
ISE to gain visibility, 69
DHCP probe, 74–75
RADIUS probe, 74
SNMPQUERY probe, 73–74
Visibility Setup Wizard, 69–73
NetFlow probes, 548–550
Network Device Groups, 528–529
node groups, 451–453
policy sets, 529–530, 736–738
posture assessment
AnyConnect Agent with ISE Compliance Module, 339–343
AUP (acceptable use policy) enforcement, 338
authorization policies, 359–361
client provisioning portal, 343–344
enabling in network, 362–363
host application visibility and context collection, 357–358
posture client provisioning global setup, 331–335
posture conditions, 345–349
posture elements, 345
posture general settings, 335–336
posture policy, 355–357
posture reassessments, 336–337
posture remediations, 349–353
posture requirements, 353–355
posture updates, 337
probes, 138–139
AD (Active Directory) probes, 149–150
DHCP and DHCPSPAN probes, 141–142
HTTP probes, 151
NMAP probes, 144–147
RADIUS probes, 142–143
SNMPQUERY probe, 148–149
SNMPTRAP probes, 148–149
pxGrid (Platform Exchange Grid)
ISE, 639–642
Stealthwatch, 652–657
WSA (Web Security Appliance), 649–652
remote logging targets, 129
repositories, 671–672, 708–713
SGTs (Security Group Tags)
native tagging on Catalyst 6500, 584–586
native tagging on Cisco IOS switches, 582–584
native tagging on Nexus series switch, 586–587
SXP (SGT Exchange Protocol)
on Cisco ASA, 576–577
on IOS devices, 572–573
on ISE, 578–579
on wireless LAN controllers, 573–575
Syslog providers, 612–614
TACACS+726–727
triggered NetFlow, 191–194
WLCs (Wireless LAN Controllers), 225
AireOS features, 225–226
Airespace ACLs, 229–232
Corporate SSID, 240–245
dynamic interfaces for client VLANs, 233–235
Guest WLAN, 236–240
RADIUS accounting servers, 227–228
RADIUS authentication servers, 226–227
RADIUS fallback, 229
WMI (Windows Management Instrumentation), 599–603

configuration files, AnyConnect Agent, 341–342

Configure WMI process, 599–603

Connection Settings (Device Administration), 729

context

context collection, 357–358

context visibility

Context Visibility views, 663–665

device profiling, 107–108, 169–178

verification of, 190–191

context-based access, 25

contextual information, 6

definition of, 31

Context Directory Agent (CDA), 594, 616

Context In integration, 632

Context Sharing integration, 632

CONTINUE packet, 14–16

control classes, 222–223

control policies

applying to interfaces, 224

configuration, 223–224

CONTROLLER role, 760

controllers, pxGrid (Platform Exchange Grid), 635

Corporate SSID, 240–245

corporate system identification, 436–437

credentials, 10

Critical MAB, 214

CTA (Cognitive Threat Analysis), 663

cts role-based sgt-map command, 569

cts role-based sgt-map vlan-list command, 569

Custom Ports scan (NMAP), 146

customization. *See* configuration

CVSS (Common Vulnerability Scoring System), 111, 662

CWA (Central Web Authentication), 299–301, 321–325

D

dACLs (downloadable access control lists), 18, 36

configuration, 251–253

creating, 496–499

syntax checker, 253

for wired guests, 310–311

dashboards

Summary, 660–661

Threat, 663

verification of profiles, 189–190

Vulnerability, 662

Data Access permissions, 127

data repositories. *See* repositories

data sources for device profiling, 110–111

Datagram Transport Layer Security (DTLS), 467

debugging. *See* troubleshooting

decision matrix (NASP), 84–85

deduplication of logs, 686–688

Default Rule policies, 249

deny statement, 230

deployment

centralized

bandwidth guidance, 54

considerations for, 53

diagram of, 52–53

device administration

large deployments, 724–725

medium deployments, 725

small deployments, 726

distributed, 55–57, 439

Anycast HA, 456–459

backup and restore, 462

bandwidth requirements, 56–57

Cisco IOS load balancing, 459

HA (high-availability) options, 446–453

ISE node configuration in, 439–445

load balancers, 453–455

maintaining, 460–462

Monitoring nodes in, 669

patches, 460–462

sample model, 55–56

when to use, 55

host security posture assessment rules, 101

ISE-PIC (Passive Identity Connector) Agent, 604–607

phased approach, 521

802.1X, 524–525

advantages of, 521–523

Closed Mode, 532–534

deployment process, 523–524

Low-Impact Mode, 530–532

Monitor Mode, 526–527

open authentication, 524–525

preparation for, 527–530

transition from Monitor Mode to end state, 534–535

wireless networks, 535

Description field (authorization profiles), 254

design. *See* ISE-enabled network design

device admin license, 723

Device Admin Policy Sets (Device Administration), 736–738

device administration, 11, 28, 721–724. *See also* device profiling

device admin AAA with Cisco IOS

Helpdesk profile, 745–746

NAD (network access device) configuration, 749–752

NetAdmin profile, 740–742

NetOps profile, 742–743

overview of, 739

policy sets, 747–749

testing and troubleshooting, 752–758

user roles, 739–740

device admin AAA with Cisco Nexus switches, 777

Helpdesk profile, 781–782

NetAdmin profile, 779–780

NetOps profile, 780–781

network device preparation, 778–779

policy sets, 782–783

SecAdmin profile, 781

TACACS+, enabling, 783–784

user roles, 777–778

device admin AAA with Cisco WLC

Employee profile, 765–766

Helpdesk profile, 765

NetAdmin profile, 763–764

network device preparation, 761–762

overview of, 759–760

policy sets, 766–768

SecAdmin profile, 764

TACACS+, enabling, 768–770

testing and troubleshooting, 770–775

device admin license, 723

device onboarding, 27

device-profile feed service, 29

large deployments, 724–725

medium deployments, 725

monitoring, 669–670

NADs (network access devices), 727–728

security policy, 107

small deployments, 726

TACACS+, enabling, 726–727

TC-NAC (Threat-Centric Network Access Control)

authorization conditions, 112–113

in incident response process, 113–116

reports, 115–116

software support, 111–112

Work Center, 728–729

Connection settings, 729

Device Admin Policy Sets, 736–738

Ext ID Sources, 732

Identities, 731–732

navigation UI, 730–731

Network Resources, 733

Password Change Control settings, 729

Policy Elements, 733–736

Reports, 738

Session Key Assignment settings, 729–730

User Identity Groups, 732

Device Administration license, 45–46

Device Logical Profiles, 110

device posture, 6

Device Profile Information worksheet, 541

device profiling, 28

authorization policy based on, 135–136, 183

endpoint Identity Groups, 183–186

EndPointPolicy, 187

in authorization roles, 111

CoA (Change of Authorization), 179–180

global CoA, 180–181

per-profile CoA, 181

context visibility, 107–108

data sources, 110–111

evolution of, 136

global profiler settings

endpoint attribute filtering, 182–183

NMAP Scan Subnet Exclusions, 183

SNMP settings for probes, 182

how it works, 134–135

HTTP profiling without probes, 152

importance of, 133–134

importing profiles, 187–188

infrastructure configuration, 153

device sensor, 157–159

DHCP helper, 153–156

ip helper-address commands, 153–156

SPAN, 156

VLAN ACL captures, 157

VMware Promiscuous Mode vSwitch setting, 159

least-privilege strategy, 136

logical profiles, 110, 178–179

policies, 109–110, 160

context visibility, 169–178

definition of, 78

endpoint profile policies, 167–169

logical profiles, 178–179

profiler feed service, 160–166

probes

AD (Active Directory) probes, 149–150

configuration, 138–139

definition of, 137

DHCP probes, 140–142

DHCPSPAN probes, 140–142

DNS probes, 147

HTTP probes, 150–152

NetFlow probes, 152–153

NMAP probes, 142–143

RADIUS probes, 142–143

SNMPQUERY probes, 148–149

SNMPTRAP probes, 148–149

profiler conditions, 108–109

profiler feed service

configuration, 160–161

offline manual update, 164–166

verification, 162–163

Profiler Work Center, 137

triggered NetFlow, 191–194

verification of profiles, 189

context visibility, 190–191

dashboard, 189–190

device sensor show commands, 191

device sensor, 205–207

configuration, 157–159

show commands, 191

device-profile feed service, 29

DHCP (Dynamic Host Configuration Protocol)

DHCP probes, 74–75

Cisco WLC considerations, 141

configuration, 141–142

overview of, 140

DHCPSPAN probes

Cisco WLC considerations, 141

configuration, 141–142

overview of, 140–141

infrastructure configuration, 153–156

diagnostic tools, 674

Endpoint Debug, 680–682

Evaluate Configuration Validator, 675–678

RADIUS Authentication Troubleshooting, 674–675

Session Trace, 682–685

TCP Dump, 678–680

DIAMETER, 12

dictionaries, 249–250

differentiated authentication, 214

DIRECTION attribute, 546

disk repositories, 709

disk space requirements (ISE), 47

distinguished name (DN), 615

distributed deployment

Anycast HA, 456–459

backup and restore, 462

bandwidth guidance, 56–57

Cisco IOS load balancing, 459

HA (high-availability) options, 446

MnT (Monitoring & Troubleshooting) nodes, 446–447

node groups, 451–453

PANs (Policy Administration Nodes), 446–447

PSNs (Policy Service Nodes), 450–451

ISE node configuration, 439–440

node personas and roles, 445

node registration, 442–445

primary PANs, 440–442

load balancers, 453–455

maintaining, 460–462

Monitoring nodes in, 669

patches, 460–462

sample model, 55–56

when to use, 55

DN (distinguished name), 615

DNS (Domain Name System) probes, 147

DNS probes, 147

documentation, posture requirements for, 96–97

domains, security, 85–87

double authentication, 507–508

downloadable access control lists. ***See*** **dACLs (downloadable access control lists)**

downloading

AnyConnect Headend packages, 469–470

ISE logs, 702–703

DTLS (Datagram Transport Layer Security), 467

dual-SSID onboarding

with Android, 401–408

overview of, 387

Dubois, Jesse, 680, 682

dynamic network access privileges, 102

E

EAP (Extensible Authentication Protocol), 12, 268

alternative ID stores based on EAP type, 278–280

EAP chaining, 436–437

EAP-FAST, 269

EAP-FASTv2, 436–437

EAP-MD5, 268

EAP-TLS, 268–269, 271

EAP-TTLS, 269

PEAP (Protected EAP), 269

EAPoL (Extensible Authentication Protocol over LAN), 42–43

Easy Connect, 5, 27

ECC (elliptic curve cryptography), 412

ecosystems. *See* ISE ecosystems

elliptic curve cryptography (ECC), 412

EMM (enterprise mobility management)

partners, 25

triggered NetFlow, 192–194

employee and corporate machine full-access rule, 286–288

employee authorization rule, 104–105

employee dynamic interface, 233–234

employee limited access rule, 292–295

Employee profile, 765–766

Endpoint Classification page (Visibility Setup Wizard), 72

Endpoint Debug, 680–682

Endpoint Protection Services (EPS), 632

EndPointPolicy attribute, 187

endpoints

Advanced Malware Protection (AMP) for Endpoints, 663

components, 42–43

context visibility, 169–178

custom profiles for, 538

collecting information for, 541–542

profiler conditions, 542–543

profiler policies, 543–544

unique values for unknown devices, 539–541

endpoint attribute filtering, 182–183

Endpoint Debug, 680–682

endpoint probe, 623–624

EndPointPolicy, 187

Endpoints view, 663–664

finding, 667–669

Identity Groups, 183–186

posture service, 29

profile policies, 167–169

Endpoints view, 663–664

end-user experience, 393–394

dual-SSID onboarding with Android, 401–408

single-SSID onboarding with Apple iOS, 394–401

enforcement

AUP (acceptable use policy), 338

host security posture assessment rules, 98–101

NASP (network access security policy), 102–103

TrustSec, 587–588

with security group firewalls, 591–592

with SGACLs, 588–591

unique usernames and passwords, 126–128

Enforcement Policy Module (EPM), 669

enterprise mobility

accelerating, 25

EMM (enterprise mobility management), 25

EPM (Enforcement Policy Module), 669

epm logging command, 669

EPS (Endpoint Protection Services), 632

ERROR packet, 14, 16

Evaluate Configuration Validator, 675–678

Exception policies, 248

exceptions for CoA (Change of Authorization), 552

Ext ID Sources screen (Device Administration), 732

Extensible Authentication Protocol. *See* EAP (Extensible Authentication Protocol)

Extensible Authentication Protocol over LAN (EAPoL), 42–43

Extensible Communication Platform (XCP), 636

Extensible Messaging and Presence Protocol (XMPP), 636

EZ Connect, 628–630

F

FAIL packet, 16

failover, 449–450

features of Cisco ISE (Identity Services Engine), 26–30

Federal Information Processing Standard (FIPS) 2, 30, 140

feed service (profiler), 160

- configuration, 160–161
- offline manual update, 164–166
- verification, 162–163

fields for authorization profiles, 254–255

File Transfer Protocol repositories, 709

files

- AnyConnect Agent configuration files, 341–342
- audit logs
  - *collection of, 128–129*
  - *ensuring integrity and confidentiality of, 129*
  - *logging categories, 128*
  - *regular audit data review, 129*
  - *remote logging targets, 129*
- ISE-PIC (Passive Identity Connector) Agent
  - *agent configuration, 609*
  - *nodes, 608*

filtering

- endpoint attributes, 182–183
- Live Logs, 666

finding endpoints, 667–669

FIPS (Federal Information Processing Standard) 140–2, 30

Firepower Management Center. *See* FMC (Firepower Management Center)

Firepower Threat Defense (FTD), 467

firewalls

- IDFW (identity firewalling), 32
- traffic enforcement with, 591–592

Flex-Auth (Flexible Authentication), 208–211

FlexConnect, 41

flow diagrams

- Closed Mode, 533
- high-level troubleshooting flowchart, 697
- Low-Impact Mode, 531
- Monitor Mode, 526, 527
- phased deployment, 524

FMC (Firepower Management Center), 619–620, 642–648

FMS (Firepower Management Center), 615, 619–620

FOLLOW packet, 16

forwarding logs, 610

FQDN (fully qualified domain name), 147, 454

FTD (Firepower Threat Defense), 467

FTP (File Transfer Protocol) repositories, 709

fully qualified domain name (FQDN), 147, 454

G

Gash, Douglas, 682, 723–724

global CoA (Change of Authorization), 180–181

global search, 667–669

global settings
Device Administration Work Center, 728–729
Connection settings, 729
Device Admin Policy Sets, 736–738
Ext ID Sources, 732
Identities, 731–732
navigation UI, 730–731
Network Resources, 733
Password Change Control settings, 729
Policy Elements, 733–736
Reports, 738
Session Key Assignment settings, 729–730
User Identity Groups, 731–732
posture assessment
posture client provisioning global setup, 331–335
posture general settings, 335–336
posture reassessments, 336–337
posture updates, 337
profiler
endpoint attribute filtering, 182–183
NMAP Scan Subnet Exclusions, 183
SNMP settings for probes, 182
Go Live button (Guest Self-Registration Wizard), 65
Google Play app store, 391
Google URLs, adding for ACL bypass, 231–232
government certifications, 30
GPOs (Group Policy Objects)
phased deployment, 523
Windows GPO configuration for wired supplicant, 369–373
GROUP_ACCOUNTS group, 308
groups
guest sponsor groups, 307–309
Identity Groups, 183–186
NDGs (Network Device Groups)
creating, 528–529
phased deployment, 527
node groups, 451–453
guest accounts
creating, 320
managing, 320–321
guest authorization rule, 105
Guest domain, 86
guest portals
hotspot guest portals, 302–303
sponsored guest portals, 313
Active Directory identity stores, 304–305
guest sponsor groups, 307–309
guest types, 305–307
multiple guest portals, 318
overview of, 304
portal page customization, 315
sponsor portal behavior and flow settings, 313–314
Guest Self-Registration Wizard, 61–65
Guest Server, 33
guest services, 5, 33, 299–302
CWA (Central Web Authentication)
compared to LWA (Local Web Authorization), 299–301
wired switches, 321–322
WLCs (Wireless LAN Controllers), 322–325
dynamic interface, 234–235
guest accounts
creating, 320
managing, 320–321
guest experience, 25
guest sponsors, 299, 307–309

guest types, 305–307

hotspot guest portal configuration, 302–303

lifecycle management, 27

LWA (Local Web Authorization), 299–301

policies, 310

guest post-authentication authorization policy, 312

guest pre-authentication authorization policy, 310–312

sponsored guest portals, 313

Active Directory identity stores, 304–305

guest sponsor groups, 307–309

guest types, 305–307

layout, 319

multiple guest portals, 318

overview of, 304

portal page customization, 315

sponsor portal behavior and flow settings, 313–314

Guest WLAN, creating, 236–240

H

HA (high-availability) options, 43, 446

Anycast HA, 456–459

configuration on Classic IOS/IOS 15.x switches, 208–211

MnT (Monitoring & Troubleshooting) nodes, 446–447

node groups, 451–453

PANs (Policy Administration Nodes)

auto PAN failover, 449–450

HA (high-availability) options, 446–447

promoting, 448

PSNs (Policy Service Nodes), 450–453

RADIUS fallback, 227–228

hardware addresses. *See* MAC addresses

Headend packages

downloading, 469–470, 471–473

preparing, 471–473

Helpdesk profile

device admin AAA with Cisco IOS, 745–746, 747–752

device admin AAA with Cisco Nexus switches, 781–782

device admin AAA with Cisco WLC, 765

high-availability options. *See* HA (high-availability) options

high-level goals (NASP), 81–84

high-level troubleshooting flowchart, 697

High-Security Mode. *See* Closed Mode

Holla, Hariprasad, 222

host application visibility, 357–358

host keys, adding to SFTP repository, 710–711

host security posture assessment rules

adding, 98–101

common checks, rules, and requirements, 97

definition of, 78

deployment, 98–101

determining validity of, 99–100

documentation of posture requirements, 96–97

enforcement, 98–101

examples of, 89–90

posture assessment options, 93–94, 95

HostScan, 494

hotspot guest portal configuration, 302–303

"How To: Cisco and F5 Deployment Guide-ISE Load Balancing Using BIG-IP" (Hyps), 454

HREAP (Hybrid Remote Edge Access Point) mode, 41

HTTP/HTTPS
enabling on Classic IOS/IOS 15.x switches, 197
probes
HTTP probes, 150–152
HTTP profiling without probes, 152
repositories, 712–713,
Hybrid Remote Edge Access Point (HREAP) mode, 41
Hypertext Transfer Protocol. *See* HTTP/HTTPS
Hyper-Threading Technology, 46
Hyps, Craig, 153, 188, 454

I

Identities screen (Device Administration), 731–732
identity awareness
contextual information, 6
definition of, 5
identity consumers
ASA (Adaptive Security Appliance), 621–622
FMS (Firepower Management Center), 619–620
Stealthwatch, 618–619
Web Security Appliance, 620–621
identity firewalling (IDFW), 32
identity gathering, 31–33
Identity Groups, 183–186
Identity Services Engine. *See* ISE-enabled network design
identity sharing
Active Directory identities, learning about, 598–599
ISE-PIC (Passive Identity Connector), 603–610
Kerberos sniffing via SPAN, 610–611
WMI (Windows Management Instrumentation), 599–603
Active Directory identity stores, 304–305
ASA (Adaptive Security Appliance), 621–622
CDA-RADIUS, 617
EZ Connect, 628–630
FMS (Firepower Management Center), 619–620
ISE-PIC (Passive Identity Connector), 603–604, 626–628
logoff detection with endpoint probe, 623–624
metadata API, 617–618
pxGrid (Platform Exchange Grid), 616–617
session timeouts, 625
Stealthwatch, 618–619
Syslog sources, 611–615
Web Security Appliance, 620–621
identity store, 271–272
Active Directory identity stores, 304–305
alternative ID stores based on EAP type, 278–280
IDFW (identity firewalling), 32
IETF RFC 2196, 82
IKE (Internet Key Exchange), 468
importing profiles, 187–188
Incident Response policy, 113–116
Include Service Version Information scan (NMAP), 147
infrastructure components
feature-to-functionality mapping, 37
functionality of, 36–37
recommended components, 41
role of, 35–36
supported components, list of, 37–41
infrastructure configuration. *See* configuration
ingress access control challenges, 558–561
Inline Posture Node, 44

integration

identity sharing

ASA (Adaptive Security Appliance), 621–622

FMS (Firepower Management Center), 619–620

metadata API, 617–618

Stealthwatch, 618–619

Web Security Appliance, 620–621

integration types, 632

MDM (mobile device management), 632

integration configuration, 431–433

integration points, 430–431

Rapid Threat Containment, 632–635

integrity of audit logs, ensuring, 129

Intel Hyper-Threading Technology, 46

interface range command, 208

Interface SNMPQUERY probe, 148

interfaces

configuration on Classic IOS/IOS 15.x switches, 208

dynamic interfaces for client VLANs, 233–235

Internal Administrator Summary report, 130

internal CA (certificate authority), 28

Internet Access domain, 86

Internet Key Exchange (IKE), 468

Internet of Things (IoT), 2

Internet only for mobile devices authorization rule, 288–292

Internet service providers (ISPs), 12

iOS (Apple), onboarding, 394–401

IOS (Cisco)

BYOD onboarding, 394–401

Classic IOS switches, 196

ACLs (access control lists), 202–203

authentication settings, 211–212

authentication timers, 212

certificates, 196–197

Flex-Auth (Flexible Authentication), 208–211

global 802.X commands, 204

global AAA commands, 198–199

global logging commands, 204–205

global profiling commands, 205–207

global RADIUS commands, 199–202

HTTP/HTTPS server, 197

Monitor Mode, 213

native SGT propagation, 582–584

switch port interfaces, 208

device admin AAA

Helpdesk profile, 745–746

NAD (network access device) configuration, 749–752

NetAdmin profile, 740–742

NetOps profile, 742–743

overview of, 739

policy sets, 747–749

testing and troubleshooting, 752–758

user roles, 739–740

Device Sensor, 37

IOS 15.x switches

ACLs (access control lists), 202–203

authentication settings, 211–212

authentication timers, 212

certificates, 196–197

characteristics of, 196

Flex-Auth (Flexible Authentication), 208–211

global 802.X commands, 204

global AAA commands, 198–199

global logging commands, 204–205

global profiling commands, 205–207

global RADIUS commands, 199–202

HTTP/HTTPS server, 197

Monitor Mode, 213

native SGT propagation, 582–584

switch port interfaces, 208

load balancing, 459

onboarding flow, 423–425

SXP (SGT Exchange Protocol) configuration, 572–573

IoT (Internet of Things), 2

IP address management (IPAM), 612

IP addresses, binding to SGTs, 568

ip dhcp relay ISE_PSN_address command, 75

ip domain-name command, 197

ip helper-address commands, 153–156

ip helper-address ISE_PSN_address command, 74

ip http secure-server command, 197

ip http server command, 197

ip radius source-interface command, 669, 690, 693

IP service-level agreement (IPSLA), 456

ip tacacs source-interface command, 669

IPAM (IP address management), 612

IPEVENT message, 670

IPSLA (IP service-level agreement), 456

IPv4_DST_ADDR attribute, 546

IPv4_SRC_ADDR attribute, 546

IR (Incident Response) policy, TC-NAC in, 113–116

ISE ecosystems

integration types, 632

MDM integration, 632

overview of, 631

pxGrid (Platform Exchange Grid)

CA (certificate authority), 638

controllers, 635

FMC (Firepower Management Center) configuration, 642–648

full mesh of trust, 637–638

ISE configuration for, 639–642

overview of, 635–637

publishers, 635

Stealthwatch configuration, 652–657

subscribers, 635

WSA (Web Security Appliance) configuration, 649–652

Rapid Threat Containment, 632–635

ISE Home Page, 660–663

ISE Posture module, 469

ISE-enabled network design, 23. ***See also*** **security policy; upgrades (ISE)**

authorization rules, 33–34

centralized policy control operation, 23–26

deployment

centralized, 52–54

distributed, 55–57

endpoint components, 42–43

features and benefits, 3–5, 26–30

infrastructure components

feature-to-functionality mapping, 37

functionality of, 36–37

recommended components, 41

role of, 35–36

supported components, list of, 37–41

ISE for wireless, 59–60

BYOD (Bring Your Own Device) Wizard, 67–69

Guest Self-Registration Wizard, 61–65

Secure Access Wizard, 65–67

Wireless Setup Wizard home page, 59–60

ISE personas, 43–45

ISE to gain visibility, 69

DHCP probe, 74–75

RADIUS probe, 74

SNMPQUERY probe, 73–74
Visibility Setup Wizard, 69–73
licensing, 45–46
node types, 43–45
performance, 47–48
platform support and compatibility, 30
policy components, 42
policy construct, 30–33
policy-based structure, 48–49
requirements, 46–47
ISE-PIC (Passive Identity Connector) Agent, 603–604, 626–628
agent configuration file, 609
Agent screen, 603–604
deploying, 604–607
design options, 610
log forwarding, 610
nodes file, 608
ISO 27001, 30
ISPs (Internet service providers), 12

J–K

Jobs, Steve, 383
Karelis, E. Pete, 456, 614
Kerberos sniffing, 610–611
Keren, Eyal, 682
keywords. *See also* **commands**
log, 252
smartlog, 252

L

L4_DST_PORT attribute, 546
L4_SRC_PORT attribute, 546
large deployments, 724–725
layout of sponsored guest portals, 319
Learn tenet (passive identification), 598, 615
least-privilege strategy, 136
licensing
device admin license, 723
ISE (Identity Services Engine), 45–46
listeners, 569
Live Logs, 666–667
filtering, 666
troubleshooting
existing entry in Live Logs, 694–696
no Live Log entries exist, 689–694
steps for, 686–689
Live Sessions views, 666–667
load balancing
Cisco IOS load balancing, 459
failure scenarios, 455
general guidelines, 454–455
load balancers, 453–455
LOBBY role, 760
local service templates, 219–220
Local Web Authentication (LWA), 36
log deduplication, 686–688
log keyword, 252
logging source-interface command, 669
logical profiles, 110, 178–179
logoff detection with endpoint probe, 623–624
logs
audit logs
collection of, 128–129
ensuring integrity and confidentiality of, 129
logging categories, 128
regular audit data review, 129
remote logging targets, 129
configuration on Classic IOS/IOS 15.x switches, 204–205
deduplication, 686–688
forwarding, 610
global logging commands, 204–205
ISE logs, 701–703

Live Logs, 666–667
filtering, 666
troubleshooting, 688–696
MnT (Monitoring & Troubleshooting) nodes, 446–447
support bundle, 702–703
TACACS+660
TC-NAC, 660
Low-Impact Mode, 530–532
LWA (Local Web Authentication), 36, 299–301

M

MAB (MAC Authentication Bypass), 5, 36, 134, 214
MAC addresses
MAB (MAC Authentication Bypass), 5, 32, 36, 134, 214
MAM (MAC address management) model, 185
Mac OS onboarding flow, 428–429
Mac OS X C10.8.2 native supplicants, 367–369
maintenance of distributed deployments, 460–462
MAM (MAC address management) model, 185
management API, 617–618
MANAGEMENT role, 760
MDA (Multi-Domain Authentication), 210
MDM (mobile device management) onboarding, 429
attributes, 430–431
integration, 632
integration configuration, 431–433
integration points, 430–431
policies, 433–435
medium deployments, 725
Menu Access permissions, 127–128
messages
AAA, 670
IPEVENT, 670
POLICY_APP_FAILURE, 670
POLICY_APP_SUCCESS, 670
RADIUS, 18–20
TACACS+
accounting messages, 15–17
authentication messages, 14–15
authorization messages, 15–17
metadata API, 617–618
Metasploit, 99
Microsoft CHAP (MS-CHAP), 12
Microsoft Security Bulletin, 98
Microsoft TechNet Security Center, 98
MnT (Monitoring & Troubleshooting) nodes, 43–44, 117
HA (high-availability) options, 446–447
in large deployments, 724
upgrading, 705–708
mobile device management. ***See*** **MDM (mobile device management) onboarding**
Monitor Mode
configuration on Classic IOS/IOS 15.x switches, 213
operational flow, 526–527
transition to end state, 534–535
MONITOR role, 760
monitor session command, 156
Monitoring & Troubleshooting nodes. ***See*** **MnT (Monitoring & Troubleshooting) nodes**
Monitoring nodes, 55, 669
Monitoring persona, 43–44
monitoring tools, 30, 659–660. ***See also*** **profiling**
Context Visibility views, 663–665
data repository setup, 671–672

device configuration for monitoring, 669–670

global search, 667–669

ISE alarms, 672

ISE Home Page, 660–663

ISE reporting, 670–671

Monitoring nodes, 669

RADIUS Live Logs and Live Sessions views, 666–667

MS-CHAP (Microsoft CHAP), 12

Multi-Auth (Multiple Authentication), 210

Multi-Domain Authentication (MDA), 210

multi-forest Active Directory support, 29

multiple guest portals, creating, 318

N

NAC (Network Access Control), 23–24, 112–116

NADs (network access devices), 12, 51, 99. *See also* device administration

BYOD onboarding

ACLs (access control lists), 390–391

URLs, adding to ACL_WEBAUTH_REDIRECT, 392

WLC (Wireless LAN Controller) configuration, 388–390

C3PL switch configuration, 196, 213–215

ACLs (access control lists), 219–220

certificates, 216–217

differentiated authentication, 214

global 802.X commands, 220–221

global RADIUS commands, 217–219

local service templates, 219–220

policies, 222–224

Classic IOS/IOS 15.x switch configuration, 195–196

ACLs (access control lists), 202–203

authentication settings,

211–212

authentication timers, 212

certificates, 196–197

Flex-Auth (Flexible Authentication), 208–211

global 802.X commands, 204

global AAA commands, 198–199

global logging commands, 204–205

global profiling commands, 205–207

global RADIUS commands, 199–202

HTTP/HTTPS server, 197

Monitor Mode, 213

switch port interfaces, 208

WLC (Wireless LAN Controller) configuration, 225

AireOS features, 225–226

Airespace ACLs, 229–232

Corporate SSID, 240–245

dynamic interfaces for client VLANs, 233–235

Guest WLAN, 236–240

RADIUS accounting servers, 227–228

RADIUS authentication servers, 226–227

RADIUS fallback, 229

NAM (Network Access Manager), 377–381, 469

Name field (authorization profiles), 254

NAS (network access server), 17

NASP (network access security policy). *See also* policy sets

AnyConnect client provisioning policy, 343

auditing policy

audit log collection, 128–129

audit log integrity and confidentiality, 129

PCI DSS (Payment Card Industry Data Security Standard), 118–126

regular audit data review, 129

unique usernames and passwords, 126–128

user accounting, 131–132

AUP (acceptable use policy), 89–90, 338

authentication policies

allowed protocols, 266–271

alternative ID stores based on EAP type, 278–280

conditions, 263–266

goals, 261–262

identity store, 271–272

processing of, 262–263

RA-VPN example, 277

wireless SSID example, 272–276

authorization policies

authorization based on posture compliance, 360–361

BYOD onboarding, 422–423

employee and corporate machine full-access rule, 286–288

employee limited access rule, 292–295

goals of, 280

Internet only for mobile devices, 288–292

posture client provisioning, 359–360

processing of, 280–286

profiles in, 183–187

RA-VPN with posture flows, 501

rules, 286

saving attributes for reuse, 295–297

authorization policy, 247

authorization profiles, 253–255

Authorization Results, 251

conditions, 249–250

dACLs (downloadable access control lists), 251–253

policy rules, 247–251

policy sets, 247–248

authorization rules, 87–89

centralized policy

advantages of, 6–7

Cisco ISE operation, 23–26

checklist, 79

client provisioning policy

configuration, 413–415

default unavailable client provisioning policy action, 420–421

commonly used policies, 103–105

components of, 78–79

configuration on C3PL switches, 222–224

control policies

applying to interfaces, 224

configuration, 223–224

custom policies, 543–544

decision matrix, 84–85

definition of, 77

device profiling policy, 160

context visibility, 169–178

endpoint profile policies, 167–169

logical profiles, 178–179

profiler feed service, 160–166

device security policy, 107

device profiling, 107–111

TC-NAC (Threat-Centric Network Access Control), 111–116

dynamic network access privileges, 102

enforcement, 102–103

guest policies, 310

guest post-authentication authorization policy, 312

guest pre-authentication authorization policy, 310–312

high-level goals for, 81–84

host security posture assessment rules, 91–101

adding, 98–101

common checks, rules, and requirements, 97

deployment, 98–101

determining validity of, 99–100

documentation of posture requirements, 96–97

enforcement, 98–101

examples of, 89–90

posture assessment options, 93–94

posture remediation options, 95

IR (Incident Response) policy, 113–116

MDM onboarding policies, 433–435

NASP committees, 79–81

policy components, 42

policy construct, 30–33

policy sets, 48, 247–248

creating, 529–530, 736–738

device admin AAA with Cisco IOS, 747–749

device admin AAA with Cisco WLC, 766–768

enabling, 258–261

ISE for Nexus device admin AAA, 782–783

policy-based structure, 48–49

posture policy, 355–357

security domains, 85–87

software-defined segmentation policy, 25

NAT (Network Address Translation), 454

National Cyber Awareness System, 99

National Vulnerability Database, 99

native supplicants

comparison of popular supplicants, 366–367

configuration

Mac OS X C10.8.2 native supplicant, 367–369

Windows 7, 8/8.1, and 10 native supplicants, 373–377

profiles, configuring for onboarding, 408–423

provisioning, 365

native tagging, 580–581

navigation UI (Device Administration), 730–731

NDGs (Network Device Groups)

creating, 528–529

device administration, 727–728

phased deployment, 527

NetAdmin profile

device admin AAA with Cisco IOS, 740–742

device admin AAA with Cisco Nexus switches, 779–780

device admin AAA with Cisco WLC, 763–764

NetFlow

probes, 152–153, 544–545

attributes, 546

configuration, 548–550

efficient data collection, 547–548

example profile policy using, 546–547

triggered NetFlow, 191–194

NetOps profile

device admin AAA with Cisco IOS, 742–743

device admin AAA with Cisco Nexus switches, 780–781

Network Access Control (NAC), 23–24

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

Network Access Manager (NAM) module, 469

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

network access server (NAS), 17

Network Address Translation (NAT), 454

network authorization policy, 247

- authorization profiles, 253–255
- Authorization Results, 251
- conditions, 249–250
- dACLs (downloadable access control lists), 251–253
- policy rules, 247–251
- policy sets, 247–248

network design. ***See*** **ISE-enabled network design**

Network Device Groups (NDGs)

- creating, 528–529
- device administration, 727–728
- phased deployment, 527

Network Devices view, 665

network reachability tasks, 484–487

Network Resources screen (Device Administration), 733

Network Scan probes. ***See*** **NMAP probes**

network visibility, gaining, 25

network-admin user role, 777

network-operator user role, 777

next-generation firewalls (NGFW), 4, 467

Nexus switches

- configuring device admin AAA with, 777
  - *Helpdesk profile, 781–782*
  - *NetAdmin profile, 779–780*
  - *NetOps profile, 780–781*
  - *network device preparation, 778–779*
  - *policy sets, 782–783*
  - *SecAdmin profile, 781*
  - *TACACS+, enabling, 783–784*
  - *user roles, 777–778*
- native SGT propagation for, 586–587

NFS (Network File System) repositories, 712

NGFW (next-generation firewalls), 4, 6, 467

NMAP probes

- configuration, 144–147
- considerations for, 144
- NMAP Scan Subnet Exclusions, 183
- overview of, 143–144

No CoA setting, 180

node types (ISE), 43–45

nodes. ***See also*** **PANs (Policy Administration Nodes)**

- Admin, 55
- configuration in distributed environment, 439–440
  - *node personas and roles, 445*
  - *node registration, 442–445*
  - *primary PANs, 440–442*
- MnT (Monitoring & Troubleshooting), 117
  - *in large deployments, 724*
  - *upgrading, 705–708*
- Monitoring, 55, 669
- node groups, 451–453
- personas, verifying, 445
- PSNs (Policy Service Nodes), 51–52
  - *adding to AAA server group, 478–481*
  - *upgrading, 705–708*
- registering to deployment, 442–445

nodes files, 608

nslookup command, 700

NX-OS device admin AAA, 777

- Helpdesk profile, 781–782
- NetAdmin profile, 779–780
- NetOps profile, 780–781
- network device preparation, 778–779
- policy sets, 782–783
- SecAdmin profile, 781
- TACACS+, enabling, 783–784
- user roles, 777–778

O

offline manual update (profiler feed service), 164–166

onboarding. *See* BYOD onboarding; MDM (mobile device management) onboarding

one-time password (OTP), 507

OOB Management domain, 86

Open Authentication, 211

open authentication, 524–525

OS scan (NMAP), 146

OTA (Over the Air) provisioning, 391

OTP (one-time password), 507

OWN_ACCOUNTS group, 308

P

PANs (Policy Administration Nodes), 55, 128–129

auto PAN failover, 449–450

configuring as primary devices, 440–442

HA (high-availability) options, 446–447

promoting, 448

S-PAN (Secondary PAN), 705–708

PAP (Password Authentication Protocol), 12, 268

PASS_ADD packet, 16

PASS_REPL packet, 16

passive authentication

compared to active authentication, 594–595

definition of, 593

EZ Connect, 628–630

identity sharing

Active Directory identities, 598–599

ASA (Adaptive Security Appliance), 621–622

CDA-RADIUS, 617

FMS (Firepower Management Center), 619–620

input and outputs, 596

logoff detection with endpoint probe, 623–624

metadata API, 617–618

pxGrid (Platform Exchange Grid), 616–617

REST (representational state transfer) API sources, 614–615

session timeouts, 625

Stealthwatch, 618–619

Syslog sources, 611–614

Web Security Appliance, 620–621

ISE-PIC (Passive Identity Connector), 603–604, 626–628

PassiveID Work Center, 596–597

tenets of, 596–597

Learn, 598, 615

Share, 615–616

Update, 623

Use, 617–618

passive identities

Active Directory identities, learning about, 598–599

ISE-PIC (Passive Identity Connector), 603–610

Kerberos sniffing via SPAN, 610–611

WMI (Windows Management Instrumentation), 599–603

ASA (Adaptive Security Appliance), 621–622

CDA-RADIUS, 617

definition of, 593

EZ Connect, 628–630

FMS (Firepower Management Center), 619–620

ISE-PIC (Passive Identity Connector), 603–604, 626–628 logoff detection with endpoint probe, 623–624

metadata API, 617–618

pxGrid (Platform Exchange Grid), 616–617

REST (representational state transfer) API sources, 614–615

session timeouts, 625

Stealthwatch, 618–619

Syslog sources, 611–614

Web Security Appliance, 620–621

Passive Identity Connector (PIC), 603–604, 626–628

Passive Identity Tracking field (authorization profiles), 255

PassiveID Work Center, 596–597

Password Authentication Protocol (PAP), 12, 268

Password Change Control (Device Administration), 729

password enforcement, 126–128

patches, 460–462

PCI-DSS (Payment Card Industry Data Security Standard), 1, 118–126, 558

PEAP (Protected EAP), 269

Perfigo, acquisition by Cisco, 24

performance of ISE (Identity Services Engine), 47–48

permissions, administrator, 127

permit statement, 230

per-profile CoA (Change of Authorization), 181

personas, 43–45, 445

phased deployment, 521

802.1X, 524–525

advantages of, 521–523

Closed Mode, 532–534

deployment process, 523–524

Low-Impact Mode, 530–532

Monitor Mode, 526–527

open authentication, 524–525

preparation for

Network Device Groups, 528–529

policy sets, 529–530

transition from Monitor Mode to end state, 534–535

wireless networks, 535

physical addresses. *See* MAC addresses

PIC (Passive Identity Connector), 603–604, 626–628

PICAgent.exe.config file, 609

ping command, 700

plain old telephone service (POTS), 12

Platform Exchange Grid (pxGrid), 4, 25, 44, 579–580, 616–617

platform support and compatibility, 30

Plus license, 45–46

Point-to-Point Protocol (PPP), 17

policies. *See* NASP (network access security policy)

Policy Administration Nodes. *See* PANs (Policy Administration Nodes)

policy authoring API, 617–618

Policy Elements screen (Device Administration), 733–736

TACACS+ command sets, 733–734

TACACS+ profiles, 734–736

Policy Service Nodes. *See* PSNs (Policy Service Nodes)

Policy Service persona, 43

policy sets, 48, 247–248

creating, 529–530, 736–738

device admin AAA with Cisco IOS, 747–749

device admin AAA with Cisco WLC, 766–768

enabling, 258–261

ISE for Nexus device admin AAA, 782–783

POLICY_APP_FAILURE message, 670

POLICY_APP_SUCCESS message, 670

policy-based structure, 48–49

Port Bounce CoA (Change of Authorization), 180–181

Portal Behavior and Flow Settings page, 313–314

Portal Customization (Guest Self-Registration Wizard), 63

Portal Notifications (Guest Self-Registration Wizard), 63

Portal Page Customization page, 315

Portal Pages (Guest Self-Registration Wizard), 63

portals. ***See*** **client provisioning portal; sponsored guest portals**

ports. ***See also*** **802.1X; supplicants**
- Closed Mode, 532–534
- configuration on Classic IOS/IOS 15.x switches, 208
- Low-Impact Mode, 530–532

posture assessment. ***See also*** **posture flows**
- configuration
  - *AnyConnect Agent with ISE Compliance Module, 339–343*
  - *AUP (acceptable use policy) enforcement, 338*
  - *authorization policies, 359–361*
  - *client provisioning portal, 343–344*
  - *host application visibility and context collection, 357–358*
  - *posture client provisioning global setup, 331–335*
  - *posture conditions, 345–349*
  - *posture elements, 345*
  - *posture general settings, 335–336*
  - *posture policy, 355–357*
  - *posture reassessments, 336–337*
  - *posture remediations, 349–353*
  - *posture requirements, 353–355*
  - *posture updates, 337*
- enabling in network, 362–363
- overview of, 327–329
- Posture Assessment Work Center, 328–329
- reports, 361–362
- rules
  - *adding, 98–101*
  - *common checks, rules, and requirements, 97*
  - *deployment, 98–101*
  - *determining validity of, 99–100*
  - *documentation of posture requirements, 96–97*
  - *enforcement, 98–101*
  - *examples of, 89–90*
  - *posture assessment options, 93–94*
  - *posture remediation options, 95*
- troubleshooting, 361–362

Posture Assessment by Condition report, 556

Posture Assessment Work Center, 328–329

posture flows
- overview of, 329–331
- RA-VPNs with, 495–496
  - *ACLs (access control lists), 496–499*
  - *authorization policies, 501*
  - *authorization profiles, 499–500*
  - *sample session, 501–506*

POTS (plain old telephone service), 12

PPP (Point-to-Point Protocol), 17

Preboot Execution Environment (PXE), 211, 530

Pre-Deploy mode, 469

primary nodes
- MnT (Monitoring & Troubleshooting) nodes, 446–447
- PANs (Policy Administration Nodes), 448–450

primary PANs (Policy Administration Nodes), 440–442

privileges

administrator accounts, 126–127

dynamic network access privileges, 102

probes

AD (Active Directory) probes, 149–150

configuration, 138–139

definition of, 137

DHCP, 74–75

Cisco WLC considerations, 141

configuration, 141–142

overview of, 140

DHCPSPAN

Cisco WLC considerations, 141

configuration, 141–142

overview of, 140–141

DNS, 147

endpoint probe, logoff detection with, 623–624

HTTP, 150–152

NetFlow, 152–153, 544–545

attributes, 546

configuration, 548–550

efficient data collection, 547–548

example profile policy using, 546–547

NMAP

configuration, 144–147

considerations for, 144

overview of, 143–144

RADIUS, 74, 142–143

SNMPQUERY, 73–74, 148–149

SNMPTRAP, 148–149

Profiled Endpoints Summary Report report, 556

profiler. ***See also*** **profiling**

CoA (Change of Authorization), 179–180

global CoA, 180–181

per-profile CoA, 181

custom conditions, 542–543

custom policies, 543–544

feed service, 160

configuration, 160–161

offline manual update, 164–166

verification, 162–163

global profiler settings

endpoint attribute filtering, 182–183

NMAP Scan Subnet Exclusions, 183

SNMP settings for probes, 182

monitoring, 553–556

reports, 553–556

Profiler Work Center, 137, 537–538

profiling, 28. ***See also*** **profiler**

AnyConnect connection profiles, 473–478

authorization policy based on, 135–136, 183

endpoint Identity Groups, 183–186

EndPointPolicy, 187

authorization profiles

BYOD onboarding, 421–422

configuration, 253–255

RA-VPN with posture flows, 499–500

in authorization roles, 111

on Classic IOS/IOS 15.x switches, 205–207

CoA (Change of Authorization), 179–180

conditions producing, 550–551

configuration, 552–553

exceptions, 552

global CoA, 180–181

per-profile CoA, 181

types of, 551–552

context visibility, 107–108

custom profiles, 538

collecting information for, 541–542

profiler conditions, 542–543

profiler policies, 543–544

unique values for unknown devices, 539–541 data sources, 110–111

Employee profile, 765–766

evolution of, 136

global commands, 205–207

global profiler settings

endpoint attribute filtering, 182–183

NMAP Scan Subnet Exclusions, 183

SNMP settings for probes, 182

Helpdesk profile

device admin AAA with Cisco IOS, 745–746

device admin AAA with Cisco Nexus switches, 781–782

device admin AAA with Cisco WLC, 765

how it works, 134–135

HTTP profiling without probes, 152

importance of, 133–134

importing profiles, 187–188

infrastructure configuration, 153

device sensor, 157–159

DHCP helper, 153–156

ip helper-address commands, 153–156

SPAN, 156

VLAN ACL captures, 157

VMware Promiscuous Mode vSwitch setting, 159

least-privilege strategy, 136

logical profiles, 110, 178–179

monitoring, 553–556

native supplicant profiles, 408–423

NetAdmin profile

device admin AAA with Cisco IOS, 740–742

device admin AAA with Cisco Nexus switches, 779–780

device admin AAA with Cisco WLC, 763–764

NetOps profile

device admin AAA with Cisco IOS, 742–743

device admin AAA with Cisco Nexus switches, 780–781

policies, 109–110, 160

context visibility, 169–178

endpoint profile policies, 167–169

logical profiles, 178–179

profiler feed service, 160–166

probes

AD (Active Directory) probes, 149–150

configuration, 138–139

definition of, 137

DHCP probes, 140–142

DHCPSPAN probes, 140–142

DNS probes, 147

HTTP probes, 150–152

NetFlow probes, 152–153, 544–545

NMAP probes, 143–147

RADIUS probes, 142–143

SNMPQUERY probes, 148–149

SNMPTRAP probes, 148–149

profiling instrastructure, 153

device sensor, 157–159

DHCP helper, 153–156

feed service, 160–166

ip helper-address commands, 153–156

SPAN, 156

VLAN ACL captures, 157

VMware Promiscuous Mode vSwitch setting, 159

pxGrid (Platform Exchange Grid), 642–648

reports, 553–556

SecAdmin profile

device admin AAA with Cisco Nexus switches, 781

device admin AAA with Cisco WLC, 764

TACACS+ profiles, 734–736

triggered NetFlow, 191–194

verification of, 189

context visibility, 190–191

dashboard, 189–190

device sensor show commands, 191

Profiling Configuration tab (Visibility Setup Wizard), 73

Promiscuous Mode, 159

promoting PANs (Policy Administration Nodes), 448

proof of concept

ISE for wireless, 59–60

BYOD (Bring Your Own Device) Wizard, 67–69

Guest Self-Registration Wizard, 61–65

Secure Access Wizard, 65–67

Wireless Setup Wizard home page, 59–60

ISE to gain visibility, 69

DHCP probe, 74–75

RADIUS probe, 74

SNMPQUERY probe, 73–74

Visibility Setup Wizard, 69–73

Protected EAP (PEAP), 269

providers (Syslog), 612–614

provisioning certificates, 509–515

provisioning policy

configuration, 413–415

default unavailable client provisioning policy action, 420–421

proxy server, profiler feed service setting, 163

PSNs (Policy Service Nodes), 43, 51–52, 117

adding to AAA server group, 478–481

Anycast HA, 456–459

HA (high-availability) options, 450–451

node groups, 451–453

upgrading, 705–708

publishers, 635

PXE (Preboot Execution Environment), 211, 530

PXE (Preboot Execution Environments), 579–580

pxGrid (Platform Exchange Grid), 4, 25, 44, 616–617, 733–734

CA (certificate authority), 638

controllers, 635

FMC (Firepower Management Center) configuration, 642–648

full mesh of trust, 637–638

ISE configuration for, 639–642

overview of, 635–637

publishers, 635

Stealthwatch configuration, 652–657

subscribers, 635

WSA (Web Security Appliance) configuration, 649–652

Q–R

quarantine action, 632

RADIUS (Remote Authentication Dial-In User Service), 17–20, 32

AV (attribute-value) pairs, 20

C3PL switch configuration, 217–219

CDA-RADIUS, 617

Classic IOS switch configuration, 199–201

CoA (Change of Authorization), 20–21

compared to TACACS+21

global commands

for C3PL switches, 217–220

for Classic IOS/IOS 15.x switches, 199–203

IOS 15.x switch configuration, 201–202

Live Logs, 666–667, 686–696

Live Sessions views, 666–667

messages, 18–20

RADIUS probe, 74, 142–143

service types, 18
use cases, 17–18
WLC (Wireless LAN Controller) configuration
RADIUS accounting servers, 227–228
RADIUS authentication servers, 226–227
RADIUS fallback, 229

RADIUS Authentication Troubleshooting tool, 674–675

radius-server load-balance command, 459

Rapid Threat Containment, 29, 632–635

RA-VPNs (remote access VPNs)
authentication policy, 277
client-based RA-VPN configuration
AnyConnect connection profiles, 473–478
AnyConnect Headend packages, downloading, 469–470
client address pool, 481–484
configuration tools, 469–470
Headend preparation, 471–473
ISE configuration, 487–488
network reachability tasks, 484–487
PSNs (Policy Service Nodes), 478–481
security services modules, 468–469
testing, 488–494
connecting to, 490–491
overview of, 466–467
with posture flows, 495–496
ACLs (access control lists), 496–499
authorization policies, 501
authorization profiles, 499–500
sample session, 501–506

RBAC (role-based access control), 759

realms, 619

reassessments, posture, 336–337

Reauth CoA (Change of Authorization), 181

recommended infrastructure components, 41

redirect to web portal, 5

redundancy, syslog providers, 614

registering nodes to deployment, 442–445

REJECT packet, 14

remediation, posture, 95, 349–353

Remote Access domain, 86

remote access VPNs. *See* RA-VPNs (remote access VPNs)

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

remote logging targets, 129

REPLY packet, 14

reports, 670–671
Adapter Status, 115
Administrator Change Configuration Audit, 130
Authentications Summary, 131
Change Configuration Audit, 162
COA Events, 115
Device Administration, 738
Internal Administrator Summary, 130
posture assessment, 361–362
Posture Assessment by Condition, 556
Profiled Endpoints Summary, 556
profiler, 553–556
Scheduled Admin Change Configuration, 131
Threat Events, 115
Top Authorizations by User, 132
Vulnerability Assessment, 116

repositories, 708
CD-ROM, 712
configuration, 708–713
creating, 671–672

disk, 709

FTP, 709

HTTP, 712–713

HTTPS, 713

NFS, 712

SFTP, 710–711

TFTP, 711

validation, 713

REQUEST packet, 15–16

researching host security posture assessment rules, 98–99

RESPONSE packet, 16

REST (representational state transfer) API, 614–615

restore, 462

results

Authorization Results, 251

authorization profiles, 253–255

dACLs (downloadable access control lists), 251–253

definition of, 251

reviewing audit data, 129

role-based access control (RBAC), 759

roles (WLC), 760

rules

authorization, 87–89, 286

host security posture assessment rules

adding, 98–101

common checks, rules, and requirements, 97

deployment, 98–101

determining validity of, 99–100

documentation of posture requirements, 96–97

enforcement, 98–101

examples of, 89–90

posture assessment options, 93–94

posture remediation options, 95

network authorization policy, 247

Run SMB Discovery Script scan (NMAP), 147

S

SAN (Subject Alternative Names), 454

SANS policy site, 90

Santuka, Vivek, 191, 682

saving attributes for reuse, 295–297

scans, NMAP (network scan) probes, 143–147

SCEP (Simple Certificate Enrollment Protocol), 509–515

Scheduled Admin Change Configuration report, 131

searching, 667–669

SecAdmin profile

device admin AAA with Cisco Nexus switches, 781

device admin AAA with Cisco WLC, 764

SecLists.Org mailing lists, 98

secondary nodes

MnT (Monitoring & Troubleshooting) nodes, 446–447

PANs (Policy Administration Nodes), 448–450

Secondary PAN First (SPF) flow, 705–708

Secure Access, definition of, 23

Secure Access Wizard, 65–67

Secure File Transfer Protocol repositories, 710–711

Secure Sockets Layer (SSL), 467

security domains, 85–87

Security Group Access. *See* TrustSec

Security Group Tags. *See* SGTs (Security Group Tags)

security information and event manager (SIEM), 447

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

security risks, 2–3

SECURITY role, 760

security services modules, 468–469

SecurityFocus, 98

segmentation policy, software-defined, 25

self-registration, 61–65

self-service onboarding. *See* onboarding

self-signed certificates, importing, 440

servers

authentication servers, 32

Guest Server, 33

HTTP/HTTPS servers, 197

RADIUS accounting servers, 227–228

RADIUS authentication servers, 226–229

service set identifier (SSID), 5, 526

Service Template field (authorization profiles), 255

service templates, 219–220

service types, 18

service-policy command, 224

services of Cisco ISE (Identity Services Engine), 3–5

Session Key Assignment (Device Administration), 729–730

session timeouts, 625

Session Trace, 682–685

SFTP (Secure File Transfer Protocol) repositories, 710–711

SFUA (Source Fire User Agent), 594, 619

SGA (Security Group Access). *See* TrustSec

SGACLs, traffic enforcement with, 588–591

SGTs (Security Group Tags), 7, 18, 33, 37, 562–563. *See also* SXP (SGT Exchange Protocol)

assigning, 566–568

binding IP addresses to, 568

classification, 565–566

CollectData, 194

defining, 564–565

mapping subnets to, 569

mapping VLANs to, 569

native tagging

on Catalyst 6500, 584–586

on Cisco IOS switches, 582–584

on Nexus series switch, 586–587

Share tenet (passive identification), 615–616

sharing identity. *See* identity sharing

show aaa server command, 459

show application status ise command, 441–442

show authentication session interface command, 691–692, 693–694, 698

show device-sensor commands, 191

show ip access-list interface command, 700

show ip interface brief command, 692

show privilege command, 756

show repository command, 713

show role feature command, 778

show role feature-group command, 778

show run command, 16

show running-config command, 710–711

show tech-support command, 702

show vpn-sessiondb detail anyconnect command, 503–506

SIEM (security information and event manager), 447

Simple Certificate Enrollment Protocol (SCEP), 509–515

simple conditions, 249

Simple Network Management Protocol (SNMP), 24

single-SSID onboarding

with Apple iOS, 394–401

overview of, 387–388

site-to-site VPNs (virtual private networks), 465–466

Skip NMAP Host Discover scan (NMAP), 147

small deployments, 726

smartlog keyword, 252

SNAT (source NAT), 455

sniffing, 610–611

SNMP (Simple Network Management Protocol), 24

global profiler settings, 182

SNMP Port scan, 146

SNMPQUERY probe, 74

SNMPQUERY probes, 148–149

SNMPTRAP probes, 148–149

software-defined segmentation policy, 25

solution components (ISE)

endpoint components, 42–43

infrastructure components

feature-to-functionality mapping, 37

functionality of, 36–37

recommended components, 41

role of, 35–36

supported components, list of, 37–41

policy components, 42

Source Fire User Agent (SFUA), 594, 619

source NAT (SNAT), 455

source-interface command, 669

S-PAN (Secondary PAN), 705–708

SPAN (Switched Port Analyzer)

configuration, 156

Kerberos sniffing via, 610–611

SPF (Secondary PAN First) flow, 705–708

sponsored guest portals, 313

Active Directory identity stores, 304–305

guest sponsor groups, 307–309

guest types, 305–307

layout, 319

multiple guest portals, 318

overview of, 304

portal page customization, 315

sponsor portal behavior and flow settings, 313–314

SSID (service set identifier), 5, 526

Corporate SSIDs, creating, 240–245

dual-SSID onboarding, 387, 401–408

single-SSID onboarding, 387–388, 394–401

SSL (Secure Sockets Layer), 467

staged deployment. ***See*** **phased deployment**

Standard policies, 249

START packet, 14–16

statements

deny, 230

permit, 230

Stealthwatch, 6, 618–619, 652–657

STOP packet, 16

Subject Alternative Names (SAN), 454

subnets

mapping to SGTs, 569

NMAP Scan Subnet Exclusions, 183

subscribers, 635

SUCCESS packet, 16

Summary dashboard, 660–661

super administrator accounts, 126–127

supplicant-less network access, 27

supplicants

choosing, 366–367

comparison of, 366–367

configuration, 365–366

Cisco AnyConnect Secure Mobility Client NAM, 377–381

Mac OS X C10.8.2 native supplicant, 367–369

Windows 7, 8/8.1, and 10 native supplicants, 373–377

Windows GPO configuration for wired supplicant, 369–373

definition of, 32, 42–43

native supplicants, 365, 408–423

support bundle, 702–703

supported infrastructure components, list of, 41

Switched Port Analyzer. *See* SPAN (Switched Port Analyzer)

switches. *See also* device administration

C3PL switch configuration, 196, 213–215

ACLs (access control lists), 219–220

certificates, 216–217

differentiated authentication, 214

global 802.X commands, 220–221

global RADIUS commands, 217–219

local service templates, 219–220

policies, 222–224

Classic IOS/IOS 15.x switch configuration, 195–196

ACLs (access control lists), 202–203

authentication settings, 211–212

authentication timers, 212

certificates, 196–197

Flex-Auth (Flexible Authentication), 208–211

global 802.X commands, 204

global AAA commands, 198–199

global logging commands, 204–205

global profiling commands, 205–207

global RADIUS commands, 199–202

HTTP/HTTPS server, 197

Monitor Mode, 213

switch port interfaces, 208

configuring device admin AAA with, 777

Helpdesk profile, 781–782

NetAdmin profile, 779–780

NetOps profile, 780–781

network device preparation, 778–779

policy sets, 782–783

SecAdmin profile, 781

TACACS+, enabling, 783–784

user roles, 777–778

device admin AAA with Cisco Nexus switches, 777

Helpdesk profile, 781–782

NetAdmin profile, 779–780

NetOps profile, 780–781

network device preparation, 778–779

policy sets, 782–783

SecAdmin profile, 781

TACACS+, enabling, 783–784

user roles, 777–778

guest CWA (Central Web Authentication), 321–322

native SGT propagation

Catalyst 6500, 584–586

Classic IOS/IOS 15.x switches, 582–584

Nexus series, 586–587

switchport command, 208

SXP (SGT Exchange Protocol), 569

configuration

on Cisco ASA, 576–577

on IOS devices, 572–573

on ISE, 578–579

on wireless LAN controllers, 573–575

design, 570–572

support for, 27

Syslog

passive identities, 611–615

providers, 612–614

System SNMPQUERY probe, 148

T

TACACS+

accounting messages, 15–17

authentication messages, 14–15

authorization messages, 15–17

client-server communication, 13–14

command sets, 733–734

compared to RADIUS, 21
enabling, 726–727
device admin AAA with Cisco WLC, 768–770
ISE for Nexus device admin AAA, 783–784
logs, 660
profiles, 734–736
support for, 26

TC-NAC (Threat-Centric Network Access Control)
authorization conditions, 112–113
in incident response process, 113–116
logs, 660
reports, 115–116
software support, 111–112

TCP Dump, 678–680

templates
certificate templates, 411–413
service templates, 219–220

tenets of passive identification, 596–597
Learn, 598, 615
Share, 615–616
Update, 623
Use, 617–618

Terminal Access Controller Access-Control System. *See* TACACS+

Terminal Services (TS) Agent, 615

test aaa command, 752

testing. *See also* troubleshooting
client-based remote access VPNs
AAA test, 488–490
connecting to VPN, 490–491
logging in to web portal, 490–491
device admin AAA with Cisco IOS, 752–758
device admin AAA with Cisco WLC, 770–775

TFTP repositories, 711

Threat dashboard, 663

Threat Events report, 115

Threat-Centric Network Access Control. *See* TC-NAC (Threat-Centric Network Access Control)

threats, 2–3
Cisco Rapid Threat Containment, 29
CVSS (Common Vulnerability Scoring System), 111
TC-NAC (Threat-Centric Network Access Control)
authorization conditions, 112–113
in incident response process, 113–116
software support, 111–112
Threat dashboard, 663

timeouts, session, 625

timers, 212

TLS (Transport Layer Security), 440, 467

tools. *See also* commands
diagnostic tools, 674
Endpoint Debug, 680–682
Evaluate Configuration Validator, 675–678
RADIUS Authentication Troubleshooting, 674–675
Session Trace, 682–685
TCP Dump, 678–680
monitoring tools
Context Visibility views, 663–665
data repository setup, 671–672
device configuration for monitoring, 669–670
global search, 667–669
ISE alarms, 672
ISE Home Page, 660–663
ISE reporting, 670–671
Monitoring nodes, 669
RADIUS Live Logs and Live Sessions views, 666–667

Top Authorizations by User report, 132

Track Movement field (authorization profiles), 255

transition from Monitor Mode to end state, 534–535

Transport Layer Security (TLS), 440, 467

triggered NetFlow, 191–194

Triple-A. *See* AAA (authentication, authorization, and accounting)

troubleshooting, 30, 673

authentication and authorization, 685

active troubleshooting, 688–696

high-level troubleshooting flowchart, 697

ISE logs, 701–703

log deduplication, 686–688

WebAuth and URL redirection, 697–701

device admin AAA with Cisco IOS, 752–758

device admin AAA with Cisco WLC, 770–775

diagnostic tools, 674

Endpoint Debug, 680–682

Evaluate Configuration Validator, 675–678

RADIUS Authentication Troubleshooting, 674–675

Session Trace, 682–685

TCP Dump, 678–680

posture assessment, 361–362

trust, pxGrid (Platform Exchange Grid) and, 637–638

TrustSec, 4, 557–558

definition of, 562

enforcement, 587–588

with security group firewalls, 591–592

with SGACLs, 588–591

ingress access control challenges, 558–561

pxGrid (Platform Exchange Grid), 579–580

Security Group Tags (SGTs), 33

SGTs (Security Group Tags), 562–563

assigning, 566–568

binding IP addresses to, 568

classification, 565–566

defining, 564–565

mapping subnets to, 569

mapping VLANs to, 569

native tagging, 580–587

SXP (SGT Exchange Protocol), 569

configuration on Cisco ASA, 576–577

configuration on IOS devices, 572–573

configuration on ISE, 578–579

configuration on wireless LAN controllers, 573–575

design, 570–572

TS (Terminal Services) Agent, 615

tunneled EAP, 269–270

U

Umbrella Roaming module, 469

unauthenticated guest access, 33

unavailable client provisioning policy action, 420–421

Unified Capabilities Approved Product List, 30

unique usernames and passwords, enforcing, 126–128

unknown endpoints, custom profiles for, 538

collecting information for, 541–542

profiler conditions, 542–543

profiler policies, 543–544

unique values for unknown devices, 539–541

unquarantine action, 632

untrusted certificates, importing, 440

Update Report Page link (profiler feed service), 162

Update tenet (passive identification), 623

updates, posture, 337

upgrades (ISE)

command-line upgrade, 718–720

GUI upgrade tool, 714–718

repositories, 708–713

Secondary PAN First (SPF) flow, 705–708

upgrade process, 705–708

UPN (user principle name), 615

URLs

adding for ACL bypass, 231–232

adding to ACL_WEBAUTH_REDIRECT, 392

redirection, 697–701

U.S. Computer readiness team, 99

Use tenet (passive identification), 617–618

user accounting, 131–132

User Identity Groups screen (Device Administration), 731–732

user principle name (UPN), 615

username command, 751

usernames, unique, 126–128

Users view, 665

V

VACL (VLAN ACL), 157, 610

validating repositories, 713

validity of posture rules, 99–100

vdc-admin user role, 777

vdc-operator user role, 777

verification of profiles, 189

context visibility, 190–191

dashboard, 189–190

device sensor show commands, 191

profiler feed service, 162–163

views

Context Visibility, 663–665

Live Sessions, 666–667

VIP (virtual IP), 155

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

visibility

context visibility, 169–178, 190–191

ISE deployment, 69

DHCP probe, 74–75

RADIUS probe, 74

SNMPQUERY probe, 73–74

Visibility Setup Wizard, 69–73

Visibility Setup Wizard, 69–73

DHCP probe, 74–75

RADIUS probe, 74

SNMPQUERY probe, 73–74

VLAN ACL (VACL), 157, 610

VLANs

assignment, 558–560

dynamic interfaces for, 233–235

mapping to SGTs, 569

wireless LANs

Corporate SSID, 240–245

Guest WLAN, 236–240

VMware Promiscuous Mode, 159

VPNs (virtual private networks)

authentication, 5, 32

certificate-based authentication

authenticating VPN with certificates, 515–518

connecting to VPN via CertProfile, 518–519

provisioning certificates, 509–515

client-based RA-VPN configuration

AnyConnect connection profiles, 473–478

AnyConnect Headend packages, downloading, 469–470

client address pool, 481–484

configuration tools, 469–470

Headend preparation, 471–473

ISE configuration, 487–488

network reachability tasks, 484–487

PSNs (Policy Service Nodes), 478–481

security services modules, 468–469

testing, 488–494

clientless remote access VPNs, 466–467

connecting to, 490–491

double authentication, 507–508

overview of, 465–468

RA-VPN with posture flows, 495–496

ACLs (access control lists), 496–499

authorization policies, 501

authorization profiles, 499–500

sample session, 501–506

vSwitch Promiscuous Mode, 159

Vulnerability Assessment report, 116

Vulnerability dashboard, 662

W

web authentication, 32, 36, 415–420. *See also* CWA (Central Web Authentication)

Web Authentication Redirection ACL, 230–231

web portals

logging in to, 490–491

redirect to, 5

Web Security Appliance. *See* WSA (Web Security Appliance)

WebAuth

portals, 415–420

troubleshooting, 697–701

Web-Deploy mode, 469

Windows 7 supplicants

native supplicant configuration, 373–377

Windows GPO configuration for wired supplicant, 373–377

Windows 8/8.1 supplicants

native supplicant configuration, 373–377

Windows GPO configuration for wired supplicant, 373–377

Windows 10 supplicants

native supplicant configuration, 373–377

Windows GPO configuration for wired supplicant, 373–377

Windows GPO, 369–373

Windows Management Instrumentation. *See* WMI (Windows Management Instrumentation)

Windows onboarding, 428–429

Wired domain, 86

wired supplicants, Windows GPO configuration for, 369–373

wired switches, guest CWA (Central Web Authentication) for, 321–322

Wireless domain, 87

Wireless LAN Controller. *See* WLCs (Wireless LAN Controllers)

wireless networks. *See also* WLCs (Wireless LAN Controllers)

Corporate SSID, 240–245

Guest WLAN, 236–240

ISE deployment, 59–60

BYOD (Bring Your Own Device) Wizard, 67–69

Guest Self-Registration Wizard, 61–65

Secure Access Wizard, 65–67

Wireless Setup Wizard home page, 59–60

phased deployment, 535

WIRELESS role, 760

Wireless Setup Wizard

BYOD (Bring Your Own Device) Wizard, 67–69

Guest Self-Registration Wizard, 61–65

home page, 60–61

Secure Access Wizard, 65–67

startup, 59–60

wireless SSID, 272–276

wizards

Visibility Setup Wizard, 69–73

DHCP probe, 74–75

RADIUS probe, 74

SNMPQUERY probe, 73–74

Wireless Setup Wizard

BYOD (Bring Your Own Device) Wizard, 67–69

Guest Self-Registration Wizard, 61–65

home page, 60–61

Secure Access Wizard, 65–67

startup, 60–61

WLAN role, 760

WLCs (Wireless LAN Controllers), 59

AireOS features, 225–226

BYOD onboarding, 388–390

configuration, 225

Airespace ACLs, 229–232

Corporate SSID, 240–245

dynamic interfaces for client VLANs, 233–235

Guest WLAN, 236–240

RADIUS accounting servers, 227–228

RADIUS authentication servers, 226–227

RADIUS fallback, 229

roles, 760

SXP (SGT Exchange Protocol) configuration, 573–575

device admin AAA

Employee profile, 765–766

Helpdesk profile, 765

NetAdmin profile, 763–764

network device preparation, 761–762

overview of, 759–760

policy sets, 766–768

SecAdmin profile, 764

TACACS+, enabling, 768–770

testing and troubleshooting, 770–775

DHCP probe considerations, 141

guest CWA (Central Web Authentication), 322–325

WMI (Windows Management Instrumentation)

benefits of, 599

configuration, 599–603

Work Centers

Device Administration Work Center, 728–729

Connection settings, 729

Device Admin Policy Sets, 736–738

Ext ID Sources, 731–732

Identities, 731–732

navigation UI, 730–731

Network Resources, 733

Password Change Control settings, 729

Policy Elements, 733–736

Reports, 738

Session Key Assignment settings, 729–730

User Identity Groups, 731–732

PassiveID Work Center, 596–597

Posture Assessment Work Center, 328–329

Profiler Work Center, 137, 537–538

WSA (Web Security Appliance), 649–652

X–Y–Z

XCP (Extensible Communication Platform), 636

XMPP (Extensible Messaging and Presence Protocol), 636