



# Official Cert Guide

Learn, prepare, and practice for exam success



# CCNP Security SISAS 300-208

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

AARON T. WOLAND, CCIE NO. 20113  
KEVIN REDMON

FREE SAMPLE CHAPTER



SHARE WITH OTHERS

# **CCNP Security SISAS 300-208**

Official Cert Guide

---

Aaron T. Woland, CCIE No. 20113

Kevin Redmon

**Cisco Press**

800 East 96th Street

Indianapolis, IN 46240

# **CCNP Security SISAS 300-208 Official Cert Guide**

Aaron T. Woland  
Kevin Redmon

Copyright © 2015 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.

First Printing April 2015

Library of Congress Control Number: 2015936634

ISBN-13: 978-1-58714-426-4

ISBN-10: 1-58714-426-3

## **Warning and Disclaimer**

This book is designed to provide information about network security. 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 authors and are not necessarily those of Cisco Systems, Inc.

## **Trademark Acknowledgments**

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

## Corporate and Government Sales

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

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

## Feedback Information

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

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

We greatly appreciate your assistance.

<b>Publisher:</b> Paul Boger	<b>Business Operation Manager, Cisco Press:</b> Jan Cornelissen
<b>Associate Publisher:</b> Dave Dusthimer	<b>Executive Editor:</b> Mary Beth Ray
<b>Development Editor:</b> Eleanor C. Bru	<b>Copy Editor:</b> Megan Wade-Taxter
<b>Managing Editor:</b> Sandra Schroeder	<b>Technical Editors:</b> Tim Abbott, Konrad Reszka
<b>Project Editor:</b> Seth Kerney	<b>Proofreader:</b> Jess DeGabriele
<b>Editorial Assistant:</b> Vanessa Evans	<b>Indexer:</b> Tim Wright
<b>Cover Designer:</b> Mark Shirar	
<b>Composition:</b> Bumpy Design	



**Americas Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

**Asia Pacific Headquarters**  
Cisco Systems, Inc.  
168 Robinson Road  
#28-01 Capital Tower  
Singapore 068912  
[www.cisco.com](http://www.cisco.com)  
Tel: +65 6317 7777  
Fax: +65 6317 7799

**Europe Headquarters**  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
[www-europe.cisco.com](http://www-europe.cisco.com)  
Tel: +31 0 800 020 0791  
Fax: +31 0 20 357 1100

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

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)

## About the Authors

**Aaron T. Woland, CCIE No. 20113**, is a principal engineer within Cisco's technical marketing organization 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, and futures. Aaron joined Cisco in 2005 and is currently a member of numerous security advisory boards and standards body working groups. Prior to joining Cisco, Aaron spent 12 years as a consultant and technical trainer. His areas of expertise include network and host security architecture and implementation, regulatory compliance, virtualization, as well as route-switch and wireless. Technology is certainly his passion, and Aaron currently has two patents in pending status with the United States Patent and Trade Office.

Aaron is the author of the Cisco *ISE for BYOD and Secure Unified Access* book (Cisco Press) and many published whitepapers and design guides. Aaron is one of the first six members of the Hall of Fame for Distinguished Speakers at Cisco Live and is a security columnist for *Network World*, where he blogs on all things related to identity. In addition to being a proud holder of a CCIE-Security, his other certifications include GCIH, GSEC, CEH, MCSE, VCP, CCSP, CCNP, CCDP, and many other industry certifications.

**Kevin Redmon** is the youngest of 12 siblings and was born in Marion, Ohio. Since joining Cisco in October 2000, Kevin has worked closely with several Cisco design organizations; as a firewall/VPN customer support engineer with the Cisco Technical Assistant Center; as a systems test engineer in BYOD Smart Solutions Group; and now as a systems test engineer in the IoT Vertical Solutions Group in RTP, NC with a focus on the connected transportation systems.

Besides co-authoring this book with Aaron Woland, Kevin is also the author of the Cisco Press Video Series titled *Cisco Bring Your Own Device (BYOD) Networking LiveLessons*. He has a bachelor of science in computer engineering from Case Western Reserve University and a master of science in information security from East Carolina University, as well as several Cisco certifications. Kevin enjoys presenting on network security-related topics and Cisco's latest solutions. He has presented several times at Cisco Live, focusing on network security-related topics and has achieved the honor of Distinguished Speaker.

Kevin enjoys innovating new ideas to keep his mind fresh and currently has a patent listed with the United States Patent and Trade Office. He spends his free time relaxing with his wife, Sonya, and little girl, Melody, in Durham, North Carolina.

## About the Technical Reviewers

**Tim Abbott** is a technical marketing engineer at Cisco Systems who works with Cisco customers all over the world. He holds a bachelor's degree from the University of Texas at San Antonio. His primary responsibilities at Cisco include ISE deployment design and writing solution guides for Cisco customers and partners. Tim has held CCNA and CCNP certifications and was also named Distinguished Speaker at Cisco Live. He has more than 10 years of IT experience in areas such as network security, routing and switching, remote access, and data center technologies.

**Konrad Reszka** is a software engineer at Cisco Systems specializing in designing and validating end-to-end solutions. He has contributed to many architectures and design guides spanning multiple technologies, including data center, security, wireless, and Carrier Ethernet. He is a distinguished speaker at Cisco Live, where you can catch him giving talks on the Internet of Everything, BYOD, and MPLS VPNs. Konrad holds a degree in computer science from the University of North Carolina at Chapel Hill.

## Dedications

**Aaron Woland:** 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 love, support, guidance, wisdom, encouragement, and patience, as well as the occasional reminder that I need to “get it done.” Thank you for putting up with all the long nights and weekends I had to be writing. I doubt that I could be as patient and understanding with the bright laptop and the typing next to me while I tried to sleep. You are 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, and engrained in me the value of hard work and 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 two awesome and brilliant children, Eden and Nyah: 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 16 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 using that power to change the world. Maybe that power will be used within marine biology, or maybe you will follow in my footsteps. I can’t wait to see it for myself.

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 rambled on in the 12-minute wedding speech, you 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 Bradley’s 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.

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 not just 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 certainly would not be where I am today.

Lastly, 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.

—Aaron

**Kevin Redmon:** There are a number of people who, without them, my coauthoring this book would not be possible.

To my lovely wife, Sonya, and daughter, Melody: You both demonstrated an amazing amount of love, patience, and support throughout this book process, allowing me to spend numerous weekends and late nights in isolation to write. Sonya, you are my all, and I love you. I'm the luckiest man alive to have you as my co-pilot in life. Melody, thank you for being the beautiful princess that you are—Daddy loves you so much! Now that this book is done, my time again belongs to you both! Thank you both—with big hugs and kisses! I love you with all of my heart!

To my mom, Helen, and my brother, Jeffrey: Through the years, you both have provided me the tools, confidence, and financial support to achieve my dreams and go to college, enabling me to achieve my long career at Cisco and to, eventually, write this book. You have always been there to remind me that I can do whatever I put my mind to and to never quit—and, when I doubted that, you kept me in check. You both deserve all the riches that this world can give you, and then some. I love you, Mom! I love you, Bro!

To Adam Meiggs: You have been an inspiration, a rock, and an amazing friend. You helped me get over stage fright, allowing me to get in front of people, and to never say “I can’t!” Thanks for being there for me, Kid! I miss you, and there is rarely a day that goes by that I don’t think of you!

To Mr. Rick Heavner: Thank you for taking me under your wing in 4th grade and instilling in me humility and a love for computers. This was truly a turning point in my personal and, eventually, professional development. From the bottom of my heart, THANK YOU!!!

To Mrs. Joyce Johnston: Thank you for being you and helping me to recognize the intellectual gifts that I have been given. You helped me see my untapped talent and that I can achieve excellence with a little bit of hard work. From your Algebra King, thanks!

To Mr. Donald Wolfe: Thank you for being such a great friend and driving me to my scholarship interview in Columbus during my senior year. I didn’t get the scholarship, but that rejection gave me the fire in my belly to fight, kick, and scream through my undergrad at CWRU. Defeat was never an option. From one Baldy to another, thank you!

To my teachers from Glenwood Elementary, Edison Middle School, and Marion Harding High School in Marion, Ohio: I know that being a teacher can be a thankless career at times, but I do want to change that and say THANK YOU!!! Because of your dedication to teaching, I was able to achieve more than a man of my humble beginnings could ever dream of! Thank you for helping me achieve these dreams; without you, this would not have been possible.

To all of my friends: Thank you for being there through the years to support me. I know it was a tough job at times. Most of all, thank you for helping to make me who I am.

## Acknowledgments

### Aaron Woland:

There are so many 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 from Cisco, 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, a senior technical marketing engineer at Cisco. "Senior" doesn't do you justice, my friend. 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, an engineer at Cisco, for convincing me to step up and take a swing at being an author and for twisting my arm to put "pen to paper" a second time. Without your encouragement and enthusiasm, this book would not exist.

I am honored to work with so many brilliant and talented people every day. Among those: Jesse Dubois, Vivek Santuka, Christopher Murray, Doug Gash, Chad Mitchell, Jamie Sanbower, Louis Roggo, Kyle King, Tim Snow, Chad Sullivan, and Brad Spencer. You guys truly amaze me.

Chip Current and Paul Forbes: You guys continue to show the world what it means to be a real product owner and not just a PM. I have learned so much from you both, and I'm not referring only to vocabulary words.

To my world-class TME team: Hosuk Won, Tim Abbott, Hsing-Tsu Lai, Imran Bashir, Ziad Saredine, John Eppich, Fay-Ann Lee, Jason Kunst, Paul Carco, and Aruna Yerragudi. *World-class* is not a strong enough word 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.

Jonny Rabinowitz, Mehdi Bouzouina, and Christopher Murray: You three guys continue to set a high bar and somehow move that bar higher all the time. All three of you have a fight in you to never lose, and it's completely infectious. Chris, your constant enthusiasm, energy, brilliance, and expertise impresses me and inspires me.

Lisa Lorenzin, Cliff Cahn, Scott Pope, Steve Hannah, and Steve Venema: What an amazing cast of people who are changing the world one standard at a time. It has been an honor and a privilege to work with you.

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

Max Pritkin, I think you have forgotten more about certificates and PKI than most experts will ever know. 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's ISE. You guys continue to show the world what it means to be "world-class."

My colleagues: Naasief Edross, Andrae Middleton, Russell Rice, Dalton Hamilton, Tom Foucha, Matt Robertson, 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, Jason Frazier, Shelly Cadora, Ralph Schmieder, Corey Elinburg, Scott Kenewell, Larry Boggis, Chad Sullivan, Dave Klein, Nelson Figueroa, Kevin Redmon, Konrad Reszka, and so many more! The contributions you make to this industry inspire me.

#### **Kevin Redmon:**

First and foremost, I would like to give my utmost respect and recognition to my coauthor, Aaron Woland. When it comes to Cisco Identity Services Engine (ISE) and Cisco Secure Access, Aaron has been an indispensable resource. Without his expertise and support, the Cisco ISE community and the networking security industry at-large would be devoid of a huge knowledge base. To be in the same audience with a well-respected network security expert such as Aaron is truly an amazing feeling. Thank you for allowing me the honor to coauthor this book with you.

Special acknowledgements go to my former BYOD colleagues. During the two and a half years we shared on BYOD, I learned so much from each of you. By working closely with some of the brightest minds in solutions test and networking, I was able to learn so much in such a short time, giving me the knowledge, confidence, contacts, and tools to coauthor this book. Thank you for letting some random "security guy" wreck the ranks and become a part of the team. You guys are truly the best team that I've ever had the pleasure to work with!

I want to give a special shout-out to Nelson Figueroa and Konrad Reszka. You guys are just awesome—both as friends and colleagues. You both have become my brothers, and it's always a blast to collaborate with you both. I hope the Three Musketeers can continue to shake up the networking industry, one pint at a time.

I would also like to thank our two technical editors, Tim Abbott and Konrad Reszka. Writing a book is hard, but writing a good book would be impossible without some of the best technical editors around. Both of these guys are truly gifted network engineers in their own right. These guys help to keep me honest when I randomly drop words or overlook a key detail. Also, when my schedule slips, these guys help to make up for the lost time. Thanks guys—your help is truly appreciated!

## Contents at a Glance

### **Part I      The CCNP Certification**

Chapter 1      CCNP Security Certification    3

### **Part II      “The Triple A” (Authentication, Authorization, and Accounting)**

Chapter 2      Fundamentals of AAA    17

Chapter 3      Identity Management    35

Chapter 4      EAP Over LAN (Also Known As 802.1X)    53

Chapter 5      Non-802.1X Authentications    93

Chapter 6      Introduction to Advanced Concepts    109

### **Part III      Cisco Identity Services Engine**

Chapter 7      Cisco Identity Services Engine Architecture    123

Chapter 8      A Guided Tour of the Cisco ISE Graphical User Interface    151

Chapter 9      Initial Configuration of the Cisco ISE    197

Chapter 10      Authentication Policies    233

Chapter 11      Authorization Policies    261

### **Part IV      Implementing Secure Network Access**

Chapter 12      Implement Wired and Wireless Authentication    289

Chapter 13      Web Authentication    341

Chapter 14      Deploying Guest Services    379

Chapter 15      Profiling    441

### **Part V      Advanced Secure Network Access**

Chapter 16      Certificate-Based User Authentications    495

Chapter 17      Bring Your Own Device    523

Chapter 18      TrustSec and MACSec    597

Chapter 19      Posture Assessment    645

**Part VI     Safely Deploying in the Enterprise**

- Chapter 20    Deploying Safely    677
- Chapter 21    ISE Scale and High Availability    699
- Chapter 22    Troubleshooting Tools    723

**Part VII     Final Preparation**

- Chapter 23    Final Preparation    759

**Part VIII    Appendixes**

- Appendix A    Answers to the “Do I Know This Already?” Quizzes    773
- Appendix B    Configuring the Microsoft CA for BYOD    795
- Appendix C    Using the Dogtag CA for BYOD    821
- Appendix D    Sample Switch Configurations    845
- Glossary    861
- Index    868

# Contents

Introduction xxxi

## **Part I The CCNP Certification**

### **Chapter 1 CCNP Security Certification 3**

CCNP Security Certification Overview 3

Contents of the CCNP-Security SISAS Exam 4

How to Take the SISAS Exam 5

Who Should Take This Exam and Read This Book? 6

Format of the CCNP-Security SISAS Exam 9

CCNP-Security SISAS 300-208 Official Certification Guide 10

Book Features and Exam Preparation Methods 13

## **Part II “The Triple A” (Authentication, Authorization, and Accounting)**

### **Chapter 2 Fundamentals of AAA 17**

“Do I Know This Already?” Quiz 18

Foundation Topics 21

Triple-A 21

Compare and Select AAA Options 21

Device Administration 21

Network Access 22

TACACS+ 23

TACACS+ Authentication Messages 25

*TACACS+ Authorization and Accounting Messages* 26

RADIUS 28

AV-Pairs 31

Change of Authorization 31

Comparing RADIUS and TACACS+ 32

Exam Preparation Tasks 33

Review All Key Topics 33

Define Key Terms 33

### **Chapter 3 Identity Management 35**

“Do I Know This Already?” Quiz 35

Foundation Topics 38

What Is an Identity? 38

Identity Stores 38

Internal Identity Stores 39

External Identity Stores	41
Active Directory	42
LDAP	42
Two-Factor Authentication	43
One-Time Password Services	44
Smart Cards	45
<i>Certificate Authorities</i>	46
<i>Has the Certificate Expired?</i>	47
<i>Has the Certificate Been Revoked?</i>	48
Exam Preparation Tasks	51
Review All Key Topics	51
Define Key Terms	51

## **Chapter 4 EAP Over LAN (Also Known As 802.1X) 53**

“Do I Know This Already?” Quiz	53
Foundation Topics	56
Extensible Authentication Protocol	56
EAP over LAN (802.1X)	56
EAP Types	58
<i>Native EAP Types (Nontunneled EAP)</i>	58
<i>Tunneled EAP Types</i>	59
<i>Summary of EAP Authentication Types</i>	62
<i>EAP Authentication Type Identity Store Comparison Chart</i>	62
Network Access Devices	63
Supplicant Options	63
<i>Windows Native Supplicant</i>	64
<i>Cisco AnyConnect NAM Supplicant</i>	75
<i>EAP Chaining</i>	89
Exam Preparation Tasks	90
Review All Key Topics	90
Define Key Terms	90

## **Chapter 5 Non-802.1X Authentications 93**

“Do I Know This Already?” Quiz	93
Foundation Topics	97
Devices Without a Supplicant	97
MAC Authentication Bypass	98

	Web Authentication	100
	Local Web Authentication	101
	Local Web Authentication with a Centralized Portal	102
	Centralized Web Authentication	104
	Remote Access Connections	106
	Exam Preparation Tasks	107
	Review All Key Topics	107
	Define Key Terms	107
<b>Chapter 6</b>	<b>Introduction to Advanced Concepts</b>	<b>109</b>
	“Do I Know This Already?” Quiz	109
	Foundation Topics	113
	Change of Authorization	113
	Automating MAC Authentication Bypass	113
	Posture Assessments	117
	Mobile Device Managers	118
	Exam Preparation Tasks	120
	Review All Key Topics	120
	Define Key Terms	120
<b>Part III</b>	<b>Cisco Identity Services Engine</b>	
<b>Chapter 7</b>	<b>Cisco Identity Services Engine Architecture</b>	<b>123</b>
	“Do I Know This Already?” Quiz	123
	Foundation Topics	127
	What Is Cisco ISE?	127
	Personas	129
	Administration Node	129
	Policy Service Node	129
	Monitoring and Troubleshooting Node	130
	Inline Posture Node	130
	Physical or Virtual Appliance	131
	ISE Deployment Scenarios	133
	Single-Node Deployment	133
	Two-Node Deployment	135
	Four-Node Deployment	136
	Fully Distributed Deployment	137
	Communication Between Nodes	138

Exam Preparation Tasks	148
Review All Key Topics	148
Define Key Terms	148

## **Chapter 8 A Guided Tour of the Cisco ISE Graphical User Interface 151**

“Do I Know This Already?” Quiz	151
Foundation Topics	155
Logging In to ISE	155
Initial Login	155
Administration Dashboard	161
Administration Home Page	162
<i>Server Information</i>	162
<i>Setup Assistant</i>	163
<i>Help</i>	163
Organization of the ISE GUI	164
Operations	165
<i>Authentications</i>	165
<i>Reports</i>	169
<i>Endpoint Protection Service</i>	170
<i>Troubleshoot</i>	171
Policy	173
<i>Authentication</i>	173
<i>Authorization</i>	173
<i>Profiling</i>	174
<i>Posture</i>	175
<i>Client Provisioning</i>	175
<i>Security Group Access</i>	176
<i>Policy Elements</i>	177
Administration	178
<i>System</i>	178
<i>Identity Management</i>	183
<i>Network Resources</i>	186
<i>Web Portal Management</i>	189
<i>Feed Service</i>	191
Type of Policies in ISE	192
Authentication	192
Authorization	193

Profiling	193
Posture	193
Client Provisioning	193
Security Group Access	193
Exam Preparation Tasks	195
Review All Key Topics	195
Define Key Terms	195

## **Chapter 9 Initial Configuration of Cisco ISE 197**

“Do I Know This Already?” Quiz	197
Foundation Topics	201
Cisco Identity Services Engine Form Factors	201
Bootstrapping Cisco ISE	201
Where Are Certificates Used with the Cisco Identity Services Engine?	204
<i>Self-Signed Certificates</i>	206
<i>CA-Signed Certificates</i>	206
Network Devices	216
Network Device Groups	216
Network Access Devices	217
Local User Identity Groups	218
Local Endpoint Groups	219
Local Users	220
External Identity Stores	220
Active Directory	221
<i>Prerequisites for Joining an Active Directory Domain</i>	221
<i>Joining an Active Directory Domain</i>	222
Certificate Authentication Profile	226
Identity Source Sequences	227
Exam Preparation Tasks	230
Review All Key Topics	230

## **Chapter 10 Authentication Policies 233**

“Do I Know This Already?” Quiz	233
Foundation Topics	237
The Relationship Between Authentication and Authorization	237
Authentication Policy	237
Goals of an Authentication Policy	238

Goal 1—Accept Only Allowed Protocols	238
Goal 2—Select the Correct Identity Store	238
Goal 3—Validate the Identity	239
Goal 4—Pass the Request to the Authorization Policy	239
Understanding Authentication Policies	239
Conditions	241
Allowed Protocols	243
<i>Extensible Authentication Protocol Types</i>	245
<i>Tunneled EAP Types</i>	245
Identity Store	247
Options	247
Common Authentication Policy Examples	248
Using the Wireless SSID	248
Remote Access VPN	251
Alternative ID Stores Based on EAP Type	253
More on MAB	255
Restore the Authentication Policy	257
Exam Preparation Tasks	258
Review All Key Topics	258

## **Chapter 11 Authorization Policies 261**

“Do I Know This Already?” Quiz	261
Foundation Topics	265
Authentication Versus Authorization	265
Authorization Policies	265
Goals of Authorization Policies	265
<i>Understanding Authorization Policies</i>	266
<i>Role-specific Authorization Rules</i>	271
Authorization Policy Example	272
<i>Employee Full Access Rule</i>	272
<i>Internet Only for Smart Devices</i>	274
<i>Employee Limited Access Rule</i>	277
Saving Conditions for Reuse	279
Combining AND with OR Operators	281
Exam Preparation Tasks	287
Review All Key Topics	287
Define Key Terms	287

## **Part IV      Implementing Secure Network Access**

### **Chapter 12   Implement Wired and Wireless Authentication   289**

“Do I Know This Already?” Quiz	290
Foundation Topics	293
Authentication Configuration on Wired Switches	293
Global Configuration AAA Commands	293
Global Configuration RADIUS Commands	294
<i>IOS 12.2.X</i>	294
<i>IOS 15.X</i>	295
<i>Both IOS 12.2.X and 15.X</i>	296
<i>Global 802.1X Commands</i>	297
<i>Creating Local Access Control Lists</i>	297
Interface Configuration Settings for All Cisco Switches	298
<i>Configuring Interfaces as Switchports</i>	299
<i>Configuring Flexible Authentication and High Availability</i>	299
<i>Host Mode of the Switchport</i>	302
<i>Configuring Authentication Settings</i>	303
<i>Configuring Authentication Timers</i>	305
<i>Applying the Initial ACL to the Port and Enabling Authentication</i>	305
Authentication Configuration on WLCs	306
Configuring the AAA Servers	306
<i>Adding the RADIUS Authentication Servers</i>	306
<i>Adding the RADIUS Accounting Servers</i>	308
<i>Configuring RADIUS Fallback (High-Availability)</i>	309
<i>Configuring the Airespace ACLs</i>	310
<i>Creating the Web Authentication Redirection ACL</i>	310
<i>Creating the Posture Agent Redirection ACL</i>	313
Creating the Dynamic Interfaces for the Client VLANs	315
<i>Creating the Guest Dynamic Interface</i>	317
Creating the Wireless LANs	318
<i>Creating the Guest WLAN</i>	319
<i>Creating the Corporate SSID</i>	324
Verifying Dot1X and MAB	329
Endpoint Supplicant Verification	329
Network Access Device Verification	329
<i>Verifying Authentications with Cisco Switches</i>	329
<i>Sending Syslog to ISE</i>	332

*Verifying Authentications with Cisco WLCs* 334

Cisco ISE Verification 336

*Live Authentications Log* 336

Live Sessions Log 337

Looking Forward 338

Exam Preparation Tasks 339

Review All Key Topics 339

Define Key Terms 339

## **Chapter 13 Web Authentication 341**

“Do I Know This Already?” Quiz 341

Foundation Topics 345

Web Authentication Scenarios 345

Local Web Authentication 346

Centralized Web Authentication 346

Device Registration WebAuth 349

Configuring Centralized Web Authentication 350

Cisco Switch Configuration 350

*Configuring Certificates on the Switch* 350

*Enabling the Switch HTTP/HTTPS Server* 350

*Verifying the URL-Redirection ACL* 351

Cisco WLC Configuration 352

*Validating That MAC Filtering Is Enabled on the WLAN* 352

*Validating That Radius NAC Is Enabled on the WLAN* 352

*Validate That the URL-Redirection ACL Is Configured* 353

Captive Portal Bypass 354

Configuring ISE for Centralized Web Authentication 355

*Configuring MAB for the Authentication* 355

*Configuring the Web Authentication Identity Source Sequence* 356

*Configuring a dACL for Pre-WebAuth Authorization* 357

*Configuring an Authorization Profile* 359

Building CWA Authorization Policies 360

Creating the Rule to Redirect to CWA 360

Creating the Rules to Authorize Users Who Authenticate via CWA 361

*Creating the Guest Rule* 361

*Creating the Employee Rule* 362

Configuring Device Registration Web Authentication 363

Creating the Endpoint Identity Group 363

Creating the DRW Portal	364
Creating the Authorization Profile	365
Creating the Rule to Redirect to DRW	367
Creating the Rule to Authorize DRW-Registered Endpoints	368
Verifying Centralized Web Authentication	369
Checking the Experience from the Client	369
Checking on ISE	372
<i>Checking the Live Log</i>	372
<i>Checking the Endpoint Identity Group</i>	373
Checking the NAD	374
<i>show Commands on the Wired Switch</i>	374
<i>Viewing the Client Details on the WLC</i>	375
Exam Preparation Tasks	377
Review All Key Topics	377
<b>Chapter 14 Deploying Guest Services</b>	<b>379</b>
“Do I Know This Already?” Quiz	379
Foundation Topics	383
Guest Services Overview	383
Guest Services and WebAuth	383
<i>Portal Types</i>	384
Configuring the Web Portal Settings	389
<i>Port Numbers</i>	390
<i>Interfaces</i>	391
<i>Friendly Names</i>	391
Configuring the Sponsor Portal Policies	392
<i>Sponsor Types</i>	393
<i>Mapping Groups</i>	396
<i>Guest User Types</i>	398
Managing Guest Portals	398
<i>Portal Types</i>	399
Building Guest Authorization Policies	400
Provisioning Guest Accounts from a Sponsor Portal	416
<i>Individual</i>	416
<i>Random</i>	417
<i>Import</i>	418
Verifying Guest Access on the WLC/Switch	419

WLC 419

Exam Preparation Tasks 439

Review All Key Topics 439

Define Key Terms 439

## **Chapter 15 Profiling 441**

“Do I Know This Already?” Quiz 441

Foundation Topics 445

ISE Profiler 445

Cisco ISE Probes 447

Probe Configuration 447

*DHCP and DHCPSPAN* 449

*RADIUS* 452

*Network Scan* 453

*DNS* 454

*SNMPQUERY and SNMPTRAP* 455

*NETFLOW* 457

*HTTP Probe* 457

*HTTP Profiling Without Probes* 459

Infrastructure Configuration 459

DHCP Helper 459

SPAN Configuration 460

VLAN Access Control Lists 461

Device Sensor 462

VMware Configurations to Allow Promiscuous Mode 463

Profiling Policies 464

Profiler Feed Service 464

*Configuring the Profiler Feed Service* 465

*Verifying the Profiler Feed Service* 465

Endpoint Profile Policies 467

Logical Profiles 478

ISE Profiler and CoA 478

Global CoA 479

Per-profile CoA 480

Global Profiler Settings 481

*Endpoint Attribute Filtering* 482

Profiles in Authorization Policies	482
Endpoint Identity Groups	483
EndPointPolicy	486
Verify Profiling	486
The Dashboard	486
<i>Endpoints Drill-down</i>	487
<i>Global Search</i>	488
Endpoint Identities	489
Device Sensor Show Commands	491
Exam Preparation Tasks	492
Review All Key Topics	492

## **Part V      Advanced Secure Network Access**

### **Chapter 16   Certificate-Based User Authentications   495**

“Do I Know This Already?” Quiz	495
Foundation Topics	499
Certificate Authentication Primer	499
Determine Whether a Trusted Authority Has Signed the Digital Certificate	499
Examine Both the Start and End Dates to Determine Whether the Certificate Has Expired	501
Verify Whether the Certificate Has Been Revoked	502
Validate That the Client Has Provided Proof of Possession	504
A Common Misconception About Active Directory	505
EAP-TLS	506
Configuring ISE for Certificate-Based Authentications	506
Validate Allowed Protocols	507
Certificate Authentication Profile	508
Verify That the Authentication Policy Is Using CAP	509
Authorization Policies	511
Ensuring the Client Certificates Are Trusted	512
<i>Importing the Certificate Authority’s Public Certificate</i>	513
<i>Configuring Certificate Status Verification (optional)</i>	515
Verifying Certificate Authentications	516
Exam Preparation Tasks	520
Review All Key Topics	520
Define Key Terms	520

## **Chapter 17 Bring Your Own Device 523**

- “Do I Know This Already?” Quiz 524
- Foundation Topics 528
- BYOD Challenges 528
- Onboarding Process 529
  - BYOD Onboarding 529
    - Dual SSID* 530
    - Single SSID* 531
- Configuring NADs for Onboarding 532
  - Configuring the WLC for Dual-SSID Onboarding 532
    - Reviewing the WLAN Configuration* 532
    - Verifying the Required ACLs* 535
- ISE Configuration for Onboarding 538
  - The End User Experience 539
    - Single-SSID with Apple iOS Example* 539
    - Dual SSID with Android Example* 549
    - Unsupported Mobile Device—Blackberry Example* 555
  - Configuring ISE for Onboarding 557
    - Creating the Native Supplicant Profile* 557
    - Configuring the Client Provisioning Policy* 559
    - Configuring the WebAuth* 561
    - Verifying Default Unavailable Client Provisioning Policy Action* 562
    - Creating the Authorization Profiles* 563
    - Creating the Authorization Rules for Onboarding* 565
    - Creating the Authorization Rules for the EAP-TLS Authentications* 566
    - Configuring SCEP* 567
- BYOD Onboarding Process Detailed 570
  - iOS Onboarding Flow 570
    - Phase 1: Device Registration* 570
    - Phase 2: Device Enrollment* 571
    - Phase 3: Device Provisioning* 572
  - Android Flow 573
    - Phase 1: Device Registration* 573
    - Phase 2: Download SPW* 575
    - Phase 3: Device Provisioning* 576
  - Windows and Mac OSX Flow 577
    - Phase 1: Device Registration* 578
    - Phase 2: Device Provisioning* 579

Verifying BYOD Flows	581
Live Log	581
Reports	581
Identities	582
MDM Onboarding	583
Integration Points	583
Configuring MDM Integration	584
Configuring MDM Onboarding Rules	586
<i>Creating the Authorization Profile</i>	586
<i>Creating the Authorization Rules</i>	588
Managing Endpoints	590
Self Management	590
Administrative Management	593
The Opposite of BYOD: Identify Corporate Systems	593
Exam Preparation Tasks	595
Review All Key Topics	595
Define Key Terms	595

## **Chapter 18 TrustSec and MACSec 597**

“Do I Know This Already?” Quiz	597
Foundation Topics	601
Ingress Access Control Challenges	601
VLAN Assignment	601
Ingress Access Control Lists	603
What Is TrustSec?	605
What Is a Security Group Tag?	606
Defining the SGTs	607
Classification	609
Dynamically Assigning SGT via 802.1X	610
Manually Assigning SGT at the Port	611
Manually Binding IP Addresses to SGTs	611
Access Layer Devices That Do Not Support SGTs	612
<i>Mapping a Subnet to an SGT</i>	613
<i>Mapping a VLAN to an SGT</i>	613
Transport: Security Group Exchange Protocol	613
SXP Design	614
Configuring SXP on IOS Devices	615

Configuring SXP on Wireless LAN Controllers	617
Configuring SXP on Cisco ASA	619
Verifying SXP Connections in ASDM	620
Transport: Native Tagging	621
Configuring Native SGT Propagation (Tagging)	622
Configuring SGT Propagation on Cisco IOS Switches	623
Configuring SGT Propagation on a Catalyst 6500	625
Configuring SGT Propagation on a Nexus Series Switch	627
Enforcement	628
SGACL	629
Security Group Firewalls	631
<i>Security Group Firewall on the ASA</i>	632
<i>Security Group Firewall on the ISR and ASR</i>	632
MACSec	632
Downlink MACSec	634
<i>Switch Configuration Modes</i>	636
<i>ISE Configuration</i>	637
Uplink MACSec	638
<i>Manually Configuring Uplink MACSec</i>	638
<i>Verifying the Manual Configuration</i>	640
Exam Preparation Tasks	642
Review All Key Topics	642
Define Key Terms	642

## **Chapter 19 Posture Assessment 645**

“Do I Know This Already?” Quiz	645
Foundation Topics	648
Posture Service Overview	648
Posture Flow	649
Agent Types	650
Posture Conditions	652
CoA with Posture	654
Configuring Posture	655
Downloading CPP Resources	656
Client Provisioning Policy	657
Posture Policy Building Blocks	658
<i>Condition</i>	659

*Remediation* 661

*Requirement* 662

Modifying the Authorization Policy for CPP 663

Modifying the Authorization Policy for Compliance 666

Verifying Posture and Redirect 667

Exam Preparation Tasks 675

Review All Key Topics 675

Define Key Terms 675

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

### **Chapter 20 Deploying Safely 677**

“Do I Know This Already?” Quiz 677

Foundation Topics 680

Why Use a Phased Approach? 680

A Phased Approach 681

Comparing Authentication Open to Standard 802.1X 682

Preparing ISE for a Staged Deployment 683

Monitor Mode 685

Low-Impact Mode 689

Closed Mode 692

Transitioning from Monitor Mode to Your End State 695

Wireless Networks 695

Exam Preparation Tasks 696

Review All Key Topics 696

### **Chapter 21 ISE Scale and High Availability 699**

“Do I Know This Already?” Quiz 699

Foundation Topics 702

Configuring ISE Nodes in a Distributed Environment 702

Making the First Node a Primary Device 702

Registering an ISE Node to the Deployment 703

Ensuring the Personas of All Nodes Are Accurate 706

Licensing in a Multinode ISE Cube 706

Understanding the HA Options Available 707

Primary and Secondary Nodes 707

*Monitoring and Troubleshooting Nodes* 707

*Policy Administration Nodes* 709

Node Groups	710
Using Load Balancers	713
General Guidelines	713
Failure Scenarios	714
IOS Load Balancing	715
Maintaining ISE Deployments	716
Patching ISE	716
Backup and Restore	718
Exam Preparation Tasks	720
Review All Key Topics	720
Define Key Terms	720

## **Chapter 22 Troubleshooting Tools 723**

“Do I Know This Already?” Quiz	723
Foundation Topics	726
Logging	726
Live Log	726
Live Sessions Log	728
Logging and Remote Logging	729
<i>Logging Targets</i>	729
<i>Logging Categories</i>	730
Debug Logs	731
<i>Downloading Debug Logs from the GUI</i>	732
<i>Viewing Log Files from the CLI</i>	733
<i>Support Bundles</i>	734
Diagnostics Tools	735
Evaluate Configuration Validator	735
RADIUS Authentication Troubleshooting Tool	739
TCP Dump	741
Ensuring Live Log Displays All Events (Bypassing Suppression)	746
<i>Disabling Suppression</i>	747
Troubleshooting Outside of ISE	748
Endpoint Diagnostics	748
<i>AnyConnect Diagnostics and Reporting Tool</i>	748
<i>AnyConnect NAM Extended Logging</i>	751
<i>Microsoft Native Supplicant</i>	752
<i>Supplicant Provisioning Logs</i>	753

Network Device Troubleshooting	753
<i>The Go-To: show authentication session interface</i>	753
<i>Viewing Client Details on the WLC</i>	754
<i>Debug Commands</i>	755
Exam Preparation Tasks	756
Review All Key Topics	756

## **Part VII Final Preparation**

### **Chapter 23 Final Preparation 759**

Advice About the Exam Event	759
Learning the Question Types Using the Cisco Certification Exam Tutorial	759
Thinking About Your Time Budget Versus Number of Questions	760
A Suggested Time-Check Method	761
Miscellaneous Pre-Exam Suggestions	762
Exam-Day Advice	762
Exam Review	763
Taking Practice Exams	763
<i>Practicing Taking the SISAS Exam</i>	764
<i>Advice on How to Answer Exam Questions</i>	765
<i>Taking Other Practice Exams</i>	766
Finding Knowledge Gaps Through Question Review	767
Other Study Tasks	769
Final Thoughts	770

## **Part VIII Appendices**

### **Appendix A Answers to the “Do I Know This Already?” Quizzes 773**

### **Appendix B Configuring the Microsoft CA for BYOD 795**

CA Requirements	795
Other Useful Information	795
Microsoft Hotfixes	796
AD Account Roles	796
Configuration Steps	796
Installing the CA	796
Adding the Remaining Roles	804
Configuring the Certificate Template	809

Publishing the Certificate Template	814
Editing the Registry	816
Useful Links	819

## **Appendix C Using the Dogtag CA for BYOD 821**

What Is Dogtag, and Why Use It?	821
Prerequisites	821
<i>Installing 32-bit Fedora 15</i>	821
<i>Configuring Networking</i>	823
Installing Packages with yum	825
Configuring Proxy (if Needed)	825
Updating System Packages with yum	826
Installing and Configuring the NTP Service	826
Installing the LDAP Server	827
Installing the PHP Services	828
Installing and Configuring Dogtag	829
Modifying the Firewall Rules (iptables)	830
Creating a New CA Instance	830
Enabling and Configuring SCEP	840
Preparing Apache	841
Configuring ISE to Use the New Dogtag CA	842
Adding Dogtag to the SCEP RA Profiles	843

## **Appendix D Sample Switch Configurations 845**

Catalyst 2960/3560/3750 Series, 12.2(55)SE	845
Catalyst 3560/3750 Series, 15.0(2)SE	848
Catalyst 4500 Series, IOS-XE 3.3.0/15.1(1)SG	852
Catalyst 6500 Series, 12.2(33)SXJ	856

## **Glossary 861**

## **Index 868**

## Icons



AAA Client



AAA Server



Terminal User



Access Point



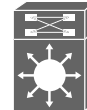
Local WLAN Controller

NAS  
AAA Client

Network User



ISE



Route/Switch Processor



Nexus 5000



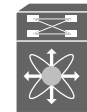
Workgroup Switch



Network Cloud



Policy Administration Node (PAN)



Nexus 7000



IntelliSwitch Stack



Monitoring Node (MnT)



Policy Service Node (PSN)



SSID



Cisco ASA 5500



Web Security Appliance

## 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).
- Italics indicate arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets [ ] indicate optional elements.
- Braces { } indicate a required choice.
- Braces within brackets [{ }] indicate a required choice within an optional element.

## Introduction

Welcome to the world of Cisco Career Certifications and the CCNP-Security. Moreover, welcome to the world of access control. Technology continues to evolve the way we do business, the types of devices that we use, the new threat vectors, and how we protect our valued assets. Through all these changes, organizations need intelligent solutions to enforce corporate policy in the access technologies that are deployed.

This book is designed to help you prepare for the Cisco CCNP Security 300-208 SISAS (Implementing Cisco Secure Access Solutions) certification exam, which is one of the four required exams to achieve the Cisco CCNP Security.

## Goals and Methods

This book will help the reader understand, design, and deploy Cisco's Secure Unified Access system. This system will combine 802.1X, profiling, posture assessments, device onboarding, and guest lifecycle management.

The reader will learn all the items that make up the SISAS 300-208 exam blueprint in a realistic method using building blocks of information. Each chapter builds on the knowledge learned in the previous chapters.

## How This Book Is Organized

Although you could read this book cover-to-cover, it is designed to be flexible and allow you to easily move between chapters and sections of chapters to cover only the material you need. If you do intend to read them all, the order in which they are presented is an excellent sequence.

Chapters 1–23 cover the following topics:

- **Chapter 1, “CCNP Security Certification,”** discusses the CCNP security certification with an overview and the contents of the SISAS 300-208 exam. It includes a discussion on how to take the SISAS exam and the exam's format. Additionally, features of the book and exam preparation methods are covered.
- **Chapter 2, “Fundamentals of AAA,”** builds a strong foundation for the concepts of authentication, authorization, and accounting (AAA). Comparisons and examples of the current AAA technologies and purposes are provided.
- **Chapter 3, “Identity Management,”** covers the many identity sources and how they work as related to secure network access.
- **Chapter 4, “EAP over LAN (also Known as 802.1X),”** discusses the IEEE standard for port-based network access control, its history, its progression, and the current state of the art.
- **Chapter 5, “Non-802.1X Authentications,”** details MAC authentication bypass (MAB) and the various types of web authentications. This chapter strengthens the

foundation built in the first four chapters and is reinforced by Chapters 6, 12, and 13.

- **Chapter 6, “Introduction to Advanced Concepts,”** builds on the strong foundation and starts to expand the reader’s knowledge base with an introduction into technologies such as profiling, posture, and BYOD.
- **Chapter 7, “Cisco Identity Services Engine Architecture,”** discusses the design of Cisco ISE, personas, and general deployment model.
- **Chapter 8, “A Guided Tour of the Cisco ISE Graphical User Interface,”** walks the reader through the many screens that make up the Cisco ISE graphical user interface.
- **Chapter 9, “Initial Configuration of Cisco ISE,”** guides the reader step-by-step through the bootstrapping and initial setup of Cisco ISE.
- **Chapter 10, “Authentication Policies,”** discusses the aspects of authentication policies, authentication methods, protocols, conditions, and results. The reader will learn about accessing the identity sources described in Chapter 3 to verify and validate the identity of the user or device attempting network access.
- **Chapter 11, “Authorization Policies,”** discusses the aspects of authorization policies, attribute sources, conditions, and results. The reader will learn about leveraging the identity learned in Chapter 11, accessing attributes of that identity, and utilizing those attributes to form the access control decision.
- **Chapter 12, “Implement Wired and Wireless Authentication,”** discusses the enabling of 802.1X and non-dot1x authentication and configuring the authorization policy to send the appropriate results.
- **Chapter 13, “Web Authentication,”** builds on the knowledge obtained in Chapter 5; this chapter puts the various web authentication mechanisms into play in the network access policies.
- **Chapter 14, “Deploying Guest Services,”** discusses extending the authentication and authorization policies with guest lifecycle services, including sponsored and self-registering guests.
- **Chapter 15, “Profiling,”** discusses the network configuration and ISE configuration related to profiling and profile data collection. Additionally, the chapter focuses on the profiling feed service and profile policies themselves.
- **Chapter 16, “Certificate-Based Authentications,”** discusses the use of end-entity certificates for authentication with EAP-Transport Layer Security (EAP-TLS). X.509 certificates, the signing of certificates, as well as the authentication process are examined in detail.
- **Chapter 17, “Bring Your Own Device,”** discusses the use of personal devices on the corporate network, differentiating between corporate and personal devices, and the onboarding of devices with Native Supplicant Provisioning (NSP). The ISE policies as well as the network device configuration are examined in detail.

- **Chapter 18, “TrustSec and MACSec,”** discusses the concepts and use of security group tags (SGTs), as well as the classification, propagation, and enforcement of those SGTs.
- **Chapter 19, “Posture Assessment,”** discusses endpoint compliance checking, the agents, and provisioning of the agents. The chapter dives into the posture policies themselves and integrating posture to the authorization policy.
- **Chapter 20, “Deploying Safely,”** examines a phased deployment approach that enables the administrator to implement ISE in the network environment in a safe and staged method using Monitor-Mode before moving a switch or location into Low-Impact Mode or Closed Mode.
- **Chapter 21, “ISE Scale and High Availability,”** describes how to configure ISE nodes in a distributed environment, installing ISE patches, using node groups, promotion of secondary to primary roles, and an introduction to the load-balancing of ISE PSNs.
- **Chapter 22, “Troubleshooting Tools,”** extends the validation and troubleshooting lessons learned throughout the book by describing and discussing the many troubleshooting tools within ISE and the network devices themselves.
- **Chapter 23, “Final Preparation,”** discusses the ways in which to prepare for the exam, from study methods to what to expect on exam day.

*This page intentionally left blank*



---

This chapter covers the following exam topics:

- Describe Identity Store Options (i.e., LDAP, AD, PKI, OTP, Smart Card, local)
- Implement Wired/Wireless 802.1X
- EAP Types
- Implement MAB
- Describe the MAB Process Within an 802.1X Framework
- ISE Authentication/Authorization Policies
- ISE Endpoint Identity Configuration

# Authentication Policies

---

An *authentication* is simply the validating of a credential. It is an important step in the process of performing any sort of secure network access control. When thinking about authentication, it often helps to relate the topic to something that occurs within your day-to-day life

Consider when a highway patrol officer has a driver pull his car over to the side of the road. The officer will walk up to the driver's window and ask for his driver's license and proof of insurance (at least that is what happens in the United States). The driver will hopefully hand over these documents for the officer to inspect.

The officer should examine the driver's license and determine whether it appears to be real. The hologram and watermarks in the driver's license are there, so it appears to be real. The picture on the license looks like the driver who handed over the license. The license hasn't expired. After going back to the squad car, the officer will perform a lookup into the Department of Motor Vehicles database to determine whether the license has been suspended.

All checks have passed. This is a valid ID. The "authentication" was successful.

Authentication policies have a few goals. They drop traffic that isn't allowed and prevent it from taking up any more processing power (the officer would immediately reject a library card because that is not an allowed form of ID for a driver). The policy will route authentication requests to the correct identity store (North Carolina DMV, or New York DMV, and so on and so on); validate the identity (was this a valid license for that driver); and finally "pass" successful authentications over to the authorization policy (was the driver allowed to exceed the speed limit and run other drivers off the road).

When thinking about authentication for network access, it often helps to relate the topic to an example such as this one, where it is something that occurs within your day-to-day life. Typically, the goals are similar, and it helps to understand the difference between authentication and authorization.

## "Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz enables you to assess whether you should read this entire chapter thoroughly or jump to the "Exam Preparation Tasks" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 10-1 lists the major headings in

this chapter and their corresponding “Do I Know This Already?” quiz questions. You can find the answers in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes.”

**Table 10-1** “Do I Know This Already?” Section-to-Question Mapping

Foundation Topics Section	Questions
Describe Identity Store Options	6
Implement Wired/Wireless 802.1X	6-7
AV Pairs	7-8
EAP Types	2
Implement MAB	1, 4
Describe the MAB Process Within an 802.1X Framework	1
ISE Authentication/Authorization Policies	3, 5, 9-10

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

1. Which of the following is required to perform MAB from a Cisco network device?
  - a. The RADIUS packet must have the `service-type` set to `login` and the `called-station-id` populated with the MAC address of the endpoint.
  - b. The RADIUS packet must have the `service-type` set to `Call-Check` and the `calling-station-id` populated with the MAC address of the endpoint.
  - c. The RADIUS packet must have the `service-type` set to `Call-Check` and the `called-station-id` populated with the MAC address of the endpoint
  - d. The RADIUS packet must have the `service-type` set to `login` and the `calling-station-id` populated with the MAC address of the endpoint
2. Which EAP type is capable of performing EAP chaining?
  - a. PEAP
  - b. EAP-FAST
  - c. EAP-TLS
  - d. EAP-MD5

3. Which of the following choices are purposes of an authentication policy?
  - a. To permit or deny access to the network based on the incoming authentication request
  - b. To apply access control filters, such as dACL or security group tags (SGTs), to the network device to limit traffic
  - c. To drop requests using an incorrect authentication method, route authentication requests to the correct identity store, validate the identity, and “pass” successful authentications over to the authorization policy
  - d. To terminate encrypted tunnels for purposes of remote access into the network
4. True or False? You must select Detect PAP as Host Lookup to enable MAB requests for Cisco nNetwork devices.
  - a. True
  - b. False
5. True or False? Policy conditions from attribute dictionaries can be saved as conditions inline while building authentication policies.
  - a. True
  - b. False
6. Which method will work effectively to allow a different Identity store to be selected for each EAP type used?
  - a. This is not possible because the first rule to match 802.1X will be used and no further rules can be used.
  - b. Create one authentication rule that matches a service type framed for each of the EAP protocols. Each authentication rule should have one subrule that matches the EapAuthentication (such as EAP-TLS, EAP-FAST, and so on).
  - c. This is only possible for the main EAP types. If there is an inner method of EAP-MSCHAPv2 with PEAP, it must be sent to the same identity store as the EAP-MSCHAPv2 inner method of EAP-FAST.
  - d. Create one sub-rule for each EAP type under the default 802.1X authentication rule that points to the appropriate identity store per rule.
7. Which RADIUS attribute is used to match the SSID?
  - a. `calling-station-ID`
  - b. `source-wireless-SSID`
  - c. `framed-station-ID`
  - d. `called-station-ID`

- 8.** Which RADIUS attribute contains the MAC address of the endpoint?
  - a.** `calling-station-ID`
  - b.** `source-wireless-SSID`
  - c.** `framed-station-ID`
  - d.** `called-station-ID`
- 9.** What is the purpose of the continue option of an authentication rule?
  - a.** The continue option is used to send an authentication down the list of rules in an authentication policy until there is a match.
  - b.** The continue option sends an authentication to the next sub-rule within the same authentication rule.
  - c.** The continue option is used to send an authentication to the authorization policy, even if the authentication was not successful.
  - d.** The continue option will send an authentication to the selected identity store.
- 10.** True or False? The Drop option for an authentication rule will allow ISE to act as if it were not “alive” so the network device will no longer send authentication requests to that ISE server.
  - a.** True
  - b.** False

---

## Foundation Topics

---

### The Relationship Between Authentication and Authorization

What is *authentication*, and what is *authorization*? Many IT professionals, especially those with wireless backgrounds (versus those with a security background), will tend to confuse these terms and what they actually do. Wireless was really the first place in the network where 802.1X took hold and is still the most prevalent use case of 802.1X authentication. With that in mind, the vast majority of wireless environments would provide a user with full network access as long as their usernames and passwords were correct (meaning that authentication was successful).

An authentication is simply the validating of credentials. If you were to go into a bank and request a withdrawal from an account, the teller would ask for your ID. You would pass your driver's license to the teller, and she would look the license over, going through a checklist of sorts:



- Is the license from a recognized authority (one of the United States or a military ID)?
- Does the picture on the ID look like the person in front of the teller?

Let's say for conversation's sake that you handed her a valid ID (authentication was successful). Does that mean you are *entitled* to the money you asked for?

The next step for the bank teller would be to check the account and ensure that the person requesting the withdrawal is entitled to complete that transaction. Perhaps you are allowed to withdraw up to \$1,000 but no more. This is the process of authorization. Just having a successful authentication does not prove entitlement.

This is why most of the time expended working within a product like Cisco ISE is spent setting up and tuning the authorization policy. Authorization is where the bulk of the decisions are made.

### Authentication Policy

Authentication policies are the first opportunity for Cisco ISE to interact with the RADIUS Access-Request coming from the network access device (NAD). The authentication policy has very specific goals, but ultimately the main goal is to process the authentication request quickly so it can be dropped (if invalid), denied immediately if the credentials were incorrect, or forwarded to be run through the authorization policies (if successful).

## Goals of an Authentication Policy

Authentication policies have a few goals:

1. Drop traffic that isn't allowed and prevent it from taking up any more processing power.
2. Route authentication requests to the correct identity store—sometimes called a policy information point (PIP).
3. Validate the identity.
4. Pass successful authentications over to the authorization policy.

### Goal 1—Accept Only Allowed Protocols

By default, ISE will allow nearly all supported authentication protocols; however, it would behoove the organization to lock this down to only the ones that are expected and supported. This serves a few purposes: It keeps the load on the Policy Service Nodes down and uses the authentication protocol to help choose the right identity store. For example, think of a corporation that wants to support only EAP-TLS for its corporate SSID. When an authentication comes in for a device attempting to join the corporate SSID, the allowed protocols could be set to allow only EAP-TLS and not waste time processing PEAP requests from device that are not configured with a certificate.

Keep in mind that a company is best served to have its security policy dictate which authentication protocols meet the security requirements of the organization. This is where the less secure protocols can be disabled, ensuring that any protocol that is more easily compromised is shut off.

Allowing only certain protocols defines which set of protocols should be permitted as well as the specific tuning of those protocols. For example, EAP-FAST can be in the allowed protocol list, but it also configures the options for EAP-FAST such as whether to allow in-band PAC provisioning or to use EAP chaining.

### Goal 2—Select the Correct Identity Store

After the authentication has been accepted, ISE must make an identity store selection decision; you can even consider it to be an identity routing decision. Based on the attributes of an incoming authentication, it must determine which identity store should be used. Obviously, if a certificate is being presented, ISE should not try to validate that certificate against the internal user database that is expecting usernames and passwords.

If your company has multiple lines of business, it can also have more than one Active Directory (AD) domain or more than one LDAP store. Using attributes in the authentication request, you can pick the correct domain or LDAP store.

### Goal 3—Validate the Identity

After the correct identity store has been identified, ISE must make sure the credentials are valid. In the case of password-based authentications, it must determine whether:

- The username is valid.
- The user's password matches what is in the Directory Store.

For certificate-based authentications, it must determine whether:

- The digital certificate has been issued and signed by a trusted certificate authority (CA).
- The certificate has expired (checks both the start and end dates).
- The certificate has been revoked.
- The client has provided proof of possession.
- The certificate presented has the correct key usage, critical extensions, and extended key usage values present.

### Goal 4—Pass the Request to the Authorization Policy

If the authentication failed, the policy can reject the request without wasting the CPU cycles comparing the request to the authorization policy. Also, if the request did not match any of the configured rules, should we send a reject message? However, when the request passes authentication, it is now time for the hand-off to the authorization policy.

## Understanding Authentication Policies

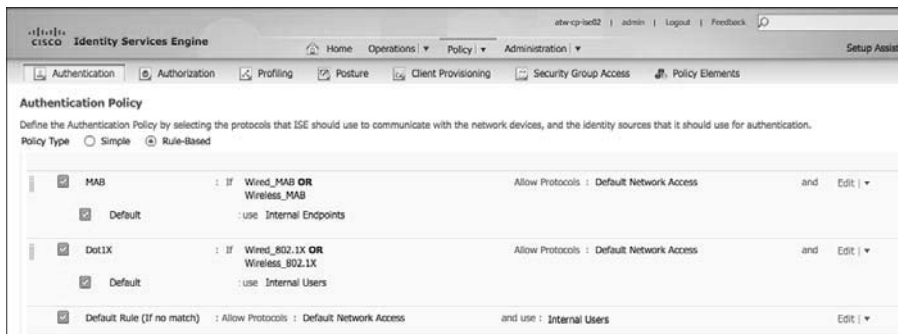
Now that you understand the four main responsibilities of the authentication policy, it will be easier to understand why you are doing the things we are introducing in this section.

To understand authentication policies even more, we will now examine a few.

From the ISE GUI, navigate to **Policy > Authentication**. You will notice the default rules as displayed in Figure 10-1. Basic authentication policy rules are logically organized in this manner:

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

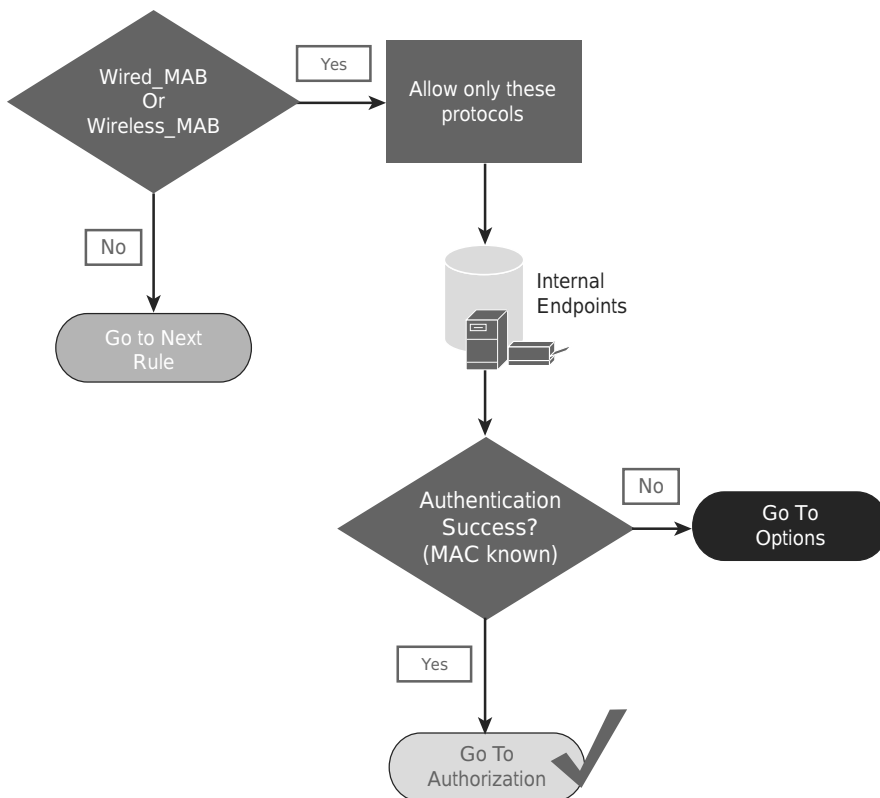
Rules are processed in a top-down, first-match order, just like a firewall policy. So if the conditions do not match, the authentication will be compared to the next rule in the policy.



**Figure 10-1** *Default authentication policy.*

As shown in Figure 10-1, ISE is preconfigured with a default rule for MAC Authentication Bypass (MAB). MAB is used for a number of things, such as allowing nonauthenticating endpoints onto the network, guest access, BYOD, and more, that will be covered in further chapters. For now, we are going to use this rule to dig into authentication rules and how they work. If you have a live ISE system, it can help to follow along with the text.

Figure 10-2 demonstrates the MAB rule in flow chart format.



**Figure 10-2** *MAB rule flow chart.*

# Conditions

The conditions of this rule state, “If the authentication request is Wired\_MAB or Wireless\_MAB, it will match this rule.” We can expand these conditions by mousing over the conditions and clicking the target icon that appears or by looking directly at the authentication conditions. Here’s how:

**Step 1.** Navigate to **Policy > Policy Elements > Conditions > Authentication > Compound Conditions**.

**Step 2.** Select **Wired\_MAB**.

As shown in Figure 10-3, Wired\_MAB is looking for the RADIUS Service-Type to be Call-Check and the NAS-Port-Type to be Ethernet. This combination of attributes from the RADIUS authentication packet tells ISE that it is a MABs (Service-type = Call-check) request from a switch (NAS-Port-Type = Ethernet).

Authentication Compound Condition List > Wired\_MAB

**Authentication Compound Conditions**

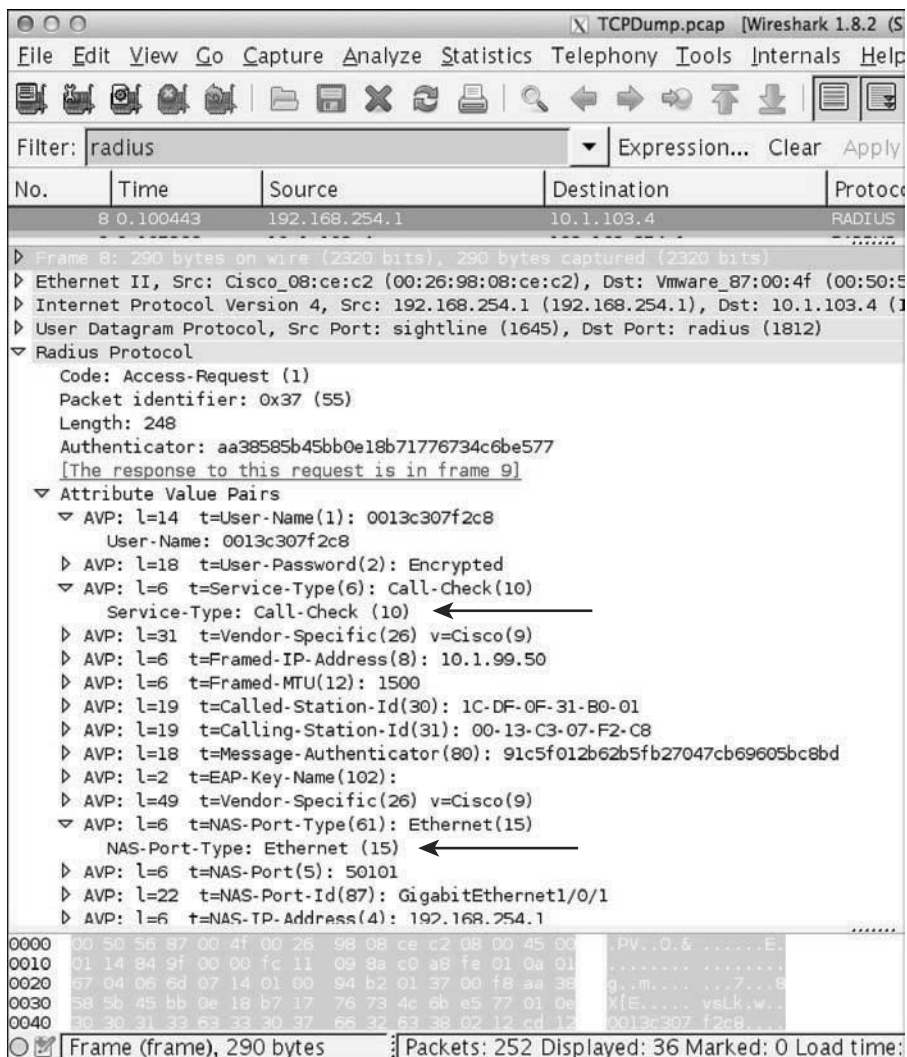
\* Name:

Description:

Condition Name	Expression	AND
<input type="text" value=""/>	Radius:Service-Type <input type="text" value="Equals"/> <input type="text" value="Call Check"/>	AND
<input type="text" value=""/>	Radius:NAS-Port-T... <input type="text" value="Equals"/> <input type="text" value="Ethernet"/>	

**Figure 10-3** *Wired\_MAB condition.*

Figure 10-4 highlights these key attributes in a packet capture of the MAB authentication request.



**Figure 10-4** Packet capture of wired MAB.

**Step 3.** Navigate back to Policy > Policy Elements > Conditions > Authentication > Compound Conditions.

**Step 4.** Select Wireless\_MAB.

Authentication Compound Condition List > Wireless\_MAB

**Authentication Compound Conditions**

\* Name:

Description:

Condition Name	Expression	AND
<input type="text" value="Radius:Service-Type"/>	<input type="text" value="Equals"/> <input type="text" value="Call Check"/>	AND
<input type="text" value="Radius:NAS-Port-T..."/>	<input type="text" value="Equals"/> <input type="text" value="Wireless - I"/>	

**Figure 10-5** *Wireless\_MAB condition.*

As shown in Figure 10-5, Wireless MAB is similar. However, it uses a NAS-Port-Type of Wireless - IEEE 802.11. This combination of attributes from the RADIUS authentication packet tells ISE that it is a MAB request from a wireless device.

## Allowed Protocols

After the conditions are matched, the rule now dictates which authentication protocols are permitted. Looking at the predefined MAB rule, this rule uses the Default Network Access list of allowed protocols (which is almost every supported authentication protocol). You can create multiple allowed protocols list, using a different one in each authentication policy rule.

Let's examine the default allowed protocols. From the ISE GUI, do the following:

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

As Figure 10-6 shows, the list of supported protocols and their options is very extensive. This default list is inclusive with the intention of making deployments work easily for customers, but security best practice is to lock this down to only the protocols needed for that rule. Be sure to elect the protocols that are consistent with your corporate security policy, ensuring that the most secure protocol is chosen for each particular application.



Allowed Protocols Services List > Default Network Access

**Allowed Protocols**

Name	Default Network Access
Description	Default Allowed Protocol Service

▼ **Allowed Protocols**

☒ Process Host Lookup

**Authentication Protocols**

▼ ☒ Allow PAP/ASCII

☒ Detect PAP as Host Lookup

▼ ☒ Allow CHAP

☒ Detect CHAP as Host Lookup

☐ Allow MS-CHAPv1

☐ Allow MS-CHAPv2

▼ ☒ Allow EAP-MD5

☒ Detect EAP-MD5 as Host Lookup

☒ Allow EAP-TLS

☐ Allow LEAP

▼ ☒ Allow PEAP

PEAP Inner Methods

☒ Allow EAP-MS-CHAPv2

☒ Allow Password Change Retries  (Valid Range 0 to 3)

☒ Allow EAP-GTC

☒ Allow Password Change Retries  (Valid Range 0 to 3)

☒ Allow EAP-TLS

▼ ☒ Allow EAP-FAST

EAP-FAST Inner Methods

☒ Allow EAP-MS-CHAPv2

☒ Allow Password Change Retries  (Valid Range 1 to 3)

☒ Allow EAP-GTC

☒ Allow Password Change Retries  (Valid Range 1 to 3)

☒ Allow EAP-TLS

☒ Use PACs ☐ Don't Use PACs

Tunnel PAC Time To Live  Days

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

☒ Allow Anonymous In-Band PAC Provisioning

☒ Allow Authenticated In-Band PAC Provisioning

☒ Server Returns Access Accept After Authenticated Provisioning

☐ Accept Client Certificate For Provisioning

☒ Allow Machine Authentication

Machine PAC Time To Live  Weeks

☒ Enable Stateless Session Resume

**Figure 10-6** *Default network access.*

Let's examine the main authentication (most common) protocols and their uses, so you will be able to create a more specific list of allowed protocols for your deployment. We will follow Figure 10-6, from top down:

- **PAP**—Password Authentication Protocol. Username is sent in the clear; password is optionally encrypted. PAP is normally used with MAB, and some devices use PAP for web authentications. We recommend you enable this for the MAB rule only

and disable PAP for any authentication rules for real authentications. The check box for Detect PAP as Host Lookup enables PAP authentications to access the Internal Endpoints Database. Without this check box selected, MAB would not work.

- **CHAP**—Challenge Handshake Authentication Protocol. Usernames and passwords are encrypted using a challenge sent from the server. Challenge Handshake Authentication Protocol (CHAP) is not often used with network access; however, some vendors will send MAB using CHAP instead of PAP. The check box for Detect CHAP as Host Lookup enables CHAP authentications to access the Internal Endpoints Database. Without this check box selected, MAB would not work.

## Extensible Authentication Protocol Types

Extensible Authentication Protocol (EAP) is an authentication framework providing for the transport and usage of identity credentials. EAP encapsulates the usernames, passwords, and certificates that a client is sending for purposes of authentication. There are many EAP types, each one with its own benefit and downside. As an interesting side note, 802.1X defines EAP over LAN. Here are the variations:

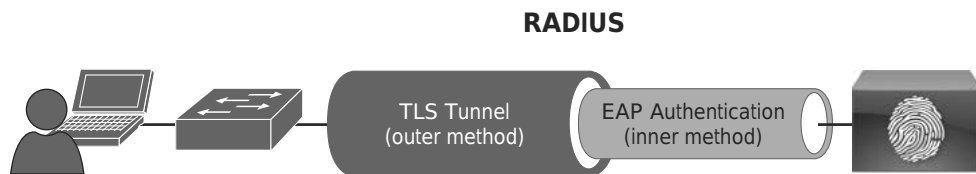
- **EAP-MD5**—Uses a message digest algorithm to hide the credentials in a HASH. The HASH is sent to the server where it is compared to a local hash to see whether the credentials were accurate. However, EAP-MD5 does not have a mechanism for mutual authentication. That means the server is validating the client, but the client does not authenticate the server (that is, it does not check to see whether it should trust the server). EAP-MD5 is common on some IP phones, and it is also possible that some switches will send MAB requests within EAP-MD5.

The check box for Detect EAP-MD5 as Host Lookup enables EAP-MD5 authentications to access the Internal Endpoints Database. Without this check box selected, MAB would not work.

- **EAP-TLS**—An EAP type that uses Transport Layer Security (TLS) to provide the secure identity transaction. This is similar to SSL and the way encryption is formed between your web browser and a secure website. EAP-TLS is considered universally supported. EAP-TLS uses X.509 certificates and provides the ability to support mutual authentication, where the client must trust the server's certificate, and vice versa. It is considered among the most secure EAP types because password capture is not an option; the endpoint must still have the private key. EAP-TLS is quickly becoming the EAP type of choice when supporting BYOD in the Enterprise.

## Tunneled EAP Types

The previously mentioned EAP types transmit their credentials immediately. These next two EAP types form encrypted tunnels first and then transmit the credentials within the tunnel. Figure 10-7 illustrates the tunneled EAP.



**Figure 10-7** *Tunnelled EAP types (PEAP and FAST).*

- **PEAP**—Protected EAP. Originally proposed by Microsoft, this EAP tunnel type has quickly become the most popular and widely deployed EAP method in the world. PEAP forms a potentially encrypted TLS tunnel between the client and server using the x.509 certificate on the server in much the same way the SSL tunnel is established between a web browser and a secure website. After the tunnel has been formed, PEAP uses another EAP type as an inner method authenticating the client using EAP within the outer tunnel.
- **EAP-MSCHAPv2**—Using this inner method, the client's credentials are sent to the server encrypted within an MSCHAPv2 session. This is the most common inner method because it enables simple transmission of usernames and passwords, or even computer names and computer passwords to the RADIUS server, which in turn will authenticate them to Active Directory.
- **EAP-GTC**—EAP-Generic Token Card (GTC). This inner method was created by Cisco as an alternative to MSCHAPv2 that allows generic authentications to virtually any identity store, including one-time-password (OTP) token servers, LDAP, Novell E-Directory, and more.
- **EAP-TLS**—While rarely used and not widely known, PEAP is capable of using EAP-TLS as an inner method.
- **EAP-FAST**—Flexible Authentication via Secure Tunnel (FAST) is similar to PEAP. FAST was created by Cisco as an alternative to PEAP that allows for faster reauthentications and support for faster wireless roaming. Just like PEAP, FAST forms a TLS outer tunnel and then transmits the client credentials within that TLS tunnel. Where FAST differs from the PEAP is the ability to use protected access credentials (PACs). A PAC can be thought of like a secure cookie, stored locally on the host as proof of a successful authentication.
- **EAP-MSCHAPv2**—Using this inner method, the client's credentials are sent to the server encrypted within an MSCHAPv2 session. This is the most common inner method because it enables simple transmission of usernames and passwords, or even computer names and computer passwords to the RADIUS server, which in turn will authenticate them to Active Directory.
- **EAP-GTC**—This inner method was created by Cisco as an alternative to MSCHAPv2 that allows generic authentications to virtually any identity store, including OTP token servers, LDAP, Novell E-Directory, and more.
- **EAP-TLS**—EAP-FAST is capable of using EAP-TLS as an inner method. This became quite popular with EAP chaining.

- **EAP Chaining with EAP-FASTv2**—As an enhancement to EAP-FAST, a differentiation was made to have a user PAC and a machine PAC. After a successful machine authentication, ISE will issue a machine PAC to the client. Then when processing a user authentication, ISE will request the machine PAC to prove that the machine was successfully authenticated, too. This is the first time in 802.1X history that multiple credentials have been able to be authenticated within a single EAP transaction; it is known as *EAP chaining*.

The IETF has recently published RFC 7170, a new open standard for Tunnel Extensible Authentication Protocol (TEAP), which is based on EAP-FASTv2. At the time of this book publishing, the RFC was brand-new and no known vendors have adopted TEAP yet. It is expected to take the industry by storm, providing the dual authentication for enterprises.

## Identity Store

After processing the allowed protocols, the authentication request is then authenticated against the chosen identity store, or in this case with MAB it is compared to the internal endpoints database (list of MAC addresses stored locally on ISE).

If the MAC Address is known, meaning it's present in the provided endpoint database, it is considered to be a successful MAB (notice this did not say successful “authentication”). MAB is exactly that—bypassing authentication—and it is not considered a secure authentication.

The selected identity source can also be an identity source sequence, which will try a series of identity stores in order. This is covered in more detail in Chapter 21, “ISE Scale and High Availability.”

## Options

Every authentication rule has a set of options that are stored with the identity store selection. These options tell ISE what to do if an authentication fails, if the user/device is unknown, or if the process fails. The options are Drop, Reject, and Continue:

- **Reject**—Send Access-Reject back to the NAD
- **Continue**—Continue to the authorization policy regardless of authentication pass/fail (used with web authentication)
- **Drop**—Do not respond to the NAD because NAD will treat as if RADIUS server is dead

Please see Chapters 20–23 for more on when to use these options.

## Common Authentication Policy Examples

In this section, you will see a few quick examples of authentication policies based on common use case, or simply because they were interesting.

### Using the Wireless SSID

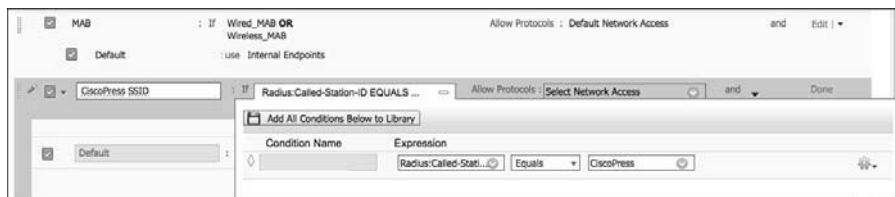
One of the most common authentication policy requests is to treat authentications differently based on the SSID of the wireless network. Creating the policy is not difficult; what becomes challenging is the identification of the attribute to use because “Source-SSI” is not a field in a RADIUS packet. The attribute we need to use is called-station-id. That is the field that describes the wireless SSID name.

For this example, we will build a rule for an SSID named CiscoPress. This rule will be configured to:

- Only match authentications coming from that SSID
- Allow only EAP-FAST authentications
- Utilize EAP chaining
- Authenticate against Active Directory

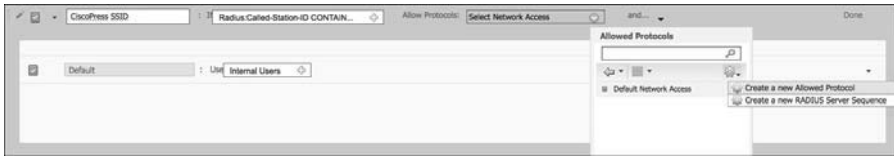
From the ISE GUI, do the following:

- Step 1.** Navigate to **Policy > Authentication**.
- Step 2.** Insert a new rule above the preconfigured Dot1X rule.
- Step 3.** Provide a name for the rule. In this case, we named it CiscoPress SSID.
- Step 4.** For the condition, select **RADIUS > Called-Station-ID**.
- Step 5.** Select **Contains**.
- Step 6.** Type the SSID name in the text box; Figure 10-8 shows the condition.



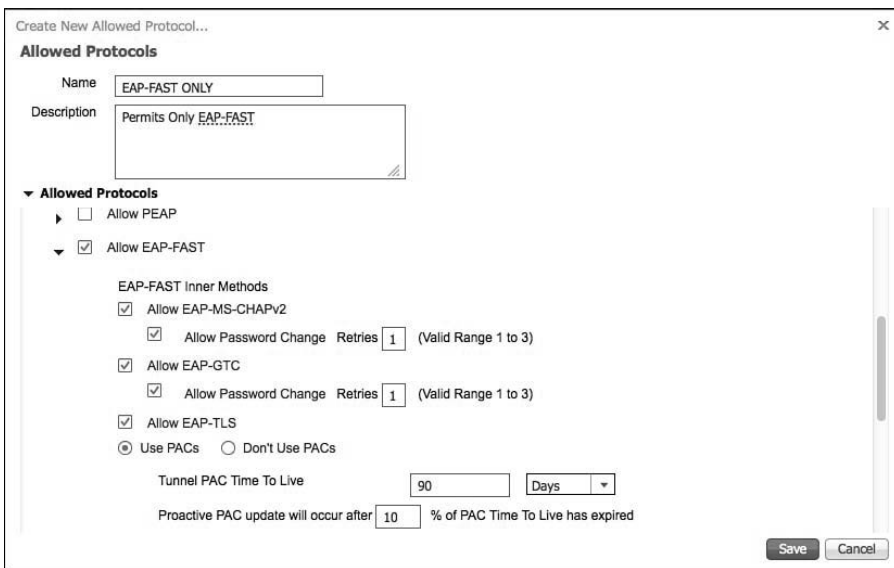
**Figure 10-8** Called-Station-ID contains CiscoPress.

- Step 7.** Next, we will create a new allowed protocol object that allows only EAP-FAST. Select the drop-down list for **Allowed Protocols**.
- Step 8.** Click the cog in the upper-right corner, and select **Create a new Allowed Protocol**, as shown in Figure 10-9.



**Figure 10-9** *Create a new allowed protocol.*

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



**Figure 10-10** *Allowed protocols.*

- Step 15.** For ease of deployment, select Allow Anonymous in-Band PAC Provisioning and Allow Authenticated in-Band PAC Provisioning.
- Step 16.** Check the boxes for Server Returns Access-Accept After Authenticated Provisioning and Accept Client Certificate for Provisioning.
- Step 17.** Enable Allow Machine Authentication.

**Step 18.** Select **Enable Stateless Session Resume**.

**Step 19.** Select **Enable EAP Chaining**.

Steps 15–19 are displayed in Figure 10-11.

Create New Allowed Protocol...

**Allowed Protocols**

Name: EAP-FAST ONLY

Description: Permits Only EAP-FAST

▼ **Allowed Protocols**

Proactive PAC update will occur after 10 % of PAC Time To Live has expired

☒ Allow Anonymous In-Band PAC Provisioning

☒ Allow Authenticated In-Band PAC Provisioning

☒ Server Returns Access Accept After Authenticated Provisioning

☒ Accept Client Certificate For Provisioning

☒ Allow Machine Authentication

Machine PAC Time To Live: 1 Weeks

☒ Enable Stateless Session Resume

Authorization PAC Time To Live: 1 Hours

☒ Enable EAP Chaining

☐ Preferred EAP Protocol: LEAP

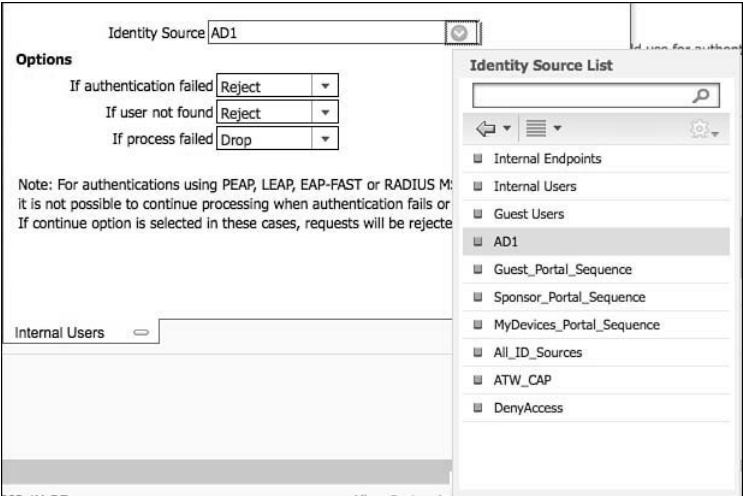
Save Cancel

**Figure 10-11** *Allowed protocols, continued.*

**Step 20.** Because we allowed only one protocol, there is no need to set a preferred EAP Protocol. Click **Save**.

**Step 21.** Even though we created the allowed protocol object for this specific authentication rule, it doesn't automatically select it from the drop-down list. Select the drop-down list for the identity source (currently set for Internal Users).

**Step 22.** Select your AD source; in this case, the name is **AD1**, as shown in Figure 10-12.

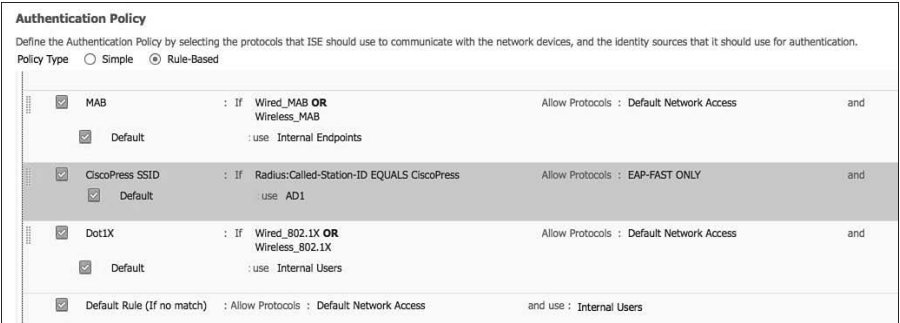


**Figure 10-12** *Selecting the AD identity source.*

**Step 23.** Leave the default Options, and click **Done**.

**Step 24.** Click **Save**.

Figure 10-13 shows the completed authentication rule.



**Figure 10-13** *Completed authentication rule.*

This completes the creation of the authentication rule. Determining which actions to take for the authentications that passed will be handled in the authorization policy.

## Remote Access VPN

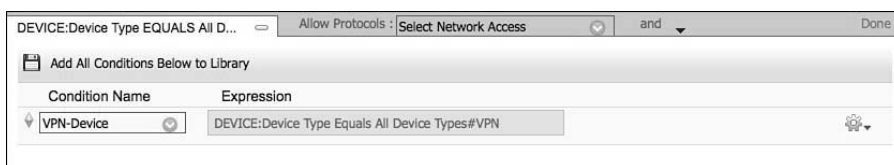
Often authentications for a remote access VPN connection get routed to an OTP server, such as RSAs SecureID. For this example, we will build a rule for remote access VPN authentications. This rule will be configured to:

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

From the ISE GUI, do the following:

- Step 1.** Navigate to **Policy > Authentication**.
- Step 2.** Insert a new rule above the preconfigured Dot1X rule.
- Step 3.** Provide a name for the rule. In this case, we named it RA VPN.
- Step 4.** For the condition, select **Create New Condition (Advanced Option) > DEVICE > Device Type**.
- Step 5.** Set the operator to Equals.
- Step 6.** Select the Network Device Group VPN.
- Step 7.** Save the selection as a condition by clicking the cog on the right side and then selecting **Add Condition to Library**. Name the condition **VPN-Device**.
- Step 8.** Click the green check mark.

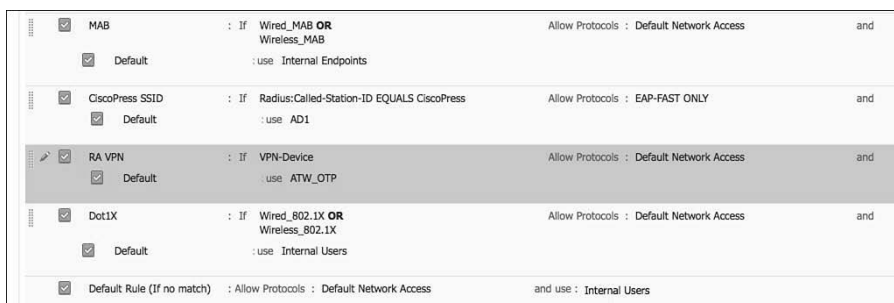
Figure 10-14 shows the completed condition.



**Figure 10-14** *Device type equals VPN.*

- Step 9.** For this example, we will just use the allowed protocol of Default Network Access. Click the drop-down list and select **Allowed Protocols** and then **Default Network Access**.
- Step 10.** For the identity store, we have selected the OTP server (previously configured) in **Administration > Identity Management > External Identity Sources > RADIUS Token (ATW\_OTP)**.
- Step 11.** We are leaving the default options; click **Done**.
- Step 12.** Click **Save**.

Figure 10-15 shows the completed authentication rule.



**Figure 10-15** *Completed authentication rule.*

## Alternative ID Stores Based on EAP Type

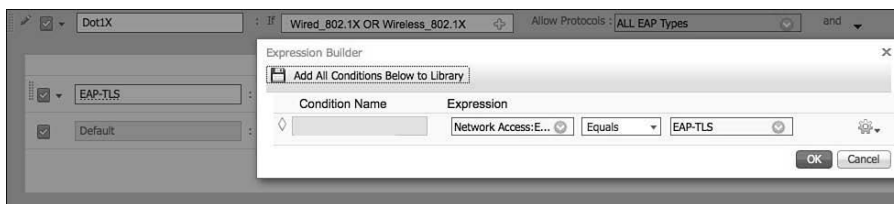
In this modern day of BYOD and mobility, it is common to have multiple user and device types connecting to the same wireless SSID. In scenarios like this, often the users with corporate laptops authenticate using EAP-FAST with EAP chaining; while BYOD-type devices must use certificates and EAP-TLS. Anyone authenticating with PEAP would be recognized as a noncorporate and nonregistered asset and be sent to a device registration portal instead of being permitted network access.

For this example, we will modify the preconfigured Dot1X rule by creating sub-rules for each EAP type. This rule will be configured to:

- Match wired or wireless 802.1X
- Route EAP-TLS authentications to a certificate authentication profile (CAP)
- Route PEAP authentications to an LDAP server
- Route EAP-FAST to Active Directory
- Route EAP-MD5 to internal endpoints for host lookup as a MAB request

From the ISE GUI, do the following:

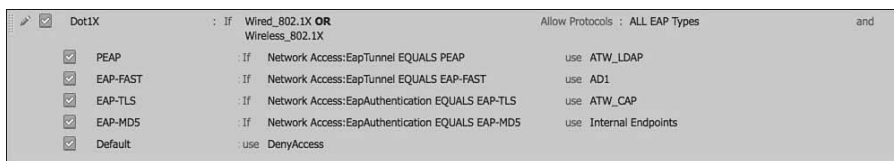
- Step 1.** Navigate to **Policy > Authentication**.
- Step 2.** Edit the preconfigured Dot1X rule.
- Step 3.** Next, we will create a new allowed protocol object that allows only EAP authentications. Select the drop-down list for **Allowed Protocols**.
- Step 4.** Click the cog in the upper-right corner, and select **Create a New Allowed Protocol**.
- Step 5.** Provide a name. In this case, we named it All EAP Types.
- Step 6.** Optionally, provide a description.
- Step 7.** Working top-down, ensure all EAP types are enabled, except for LEAP (unless you need LEAP for backward compatibility).
- Step 8.** Enable EAP chaining, as we did previously in the wireless SSID exercise.
- Step 9.** Click **Save**.
- Step 10.** Select the All EAP Types allowed protocol object for this authentication rule.
- Step 11.** Insert a new sub-rule above the Default identity store sub-rule, and name it EAP-TLS.
- Step 12.** For the condition, select **Create a New Condition (Advanced Option) > Network Access > EapAuthentication Equals EAP-TLS** (as shows in Figure 10-16).



**Figure 10-16** *Network access: EapAuthentication equals EAP-TLS.*

- Step 13.** For the identity source, we are choosing a preconfigured CAP. This was configured at **Administration > Identity Management > External Identity Sources > Certificate Authentication Profile**.
- Step 14.** Insert a new row above the EAP-TLS row, to insert EAP-FAST. We are placing EAP-FAST above EAP-TLS because EAP-TLS can be used as an inner method of EAP-FAST.
- Step 15.** Select **Network Access > EapTunnel Equals EAP-FAST** for the condition.
- Step 16.** Select the **Active Directory Object** for the identity source.
- Step 17.** Insert a new row above the EAP-TLS row to insert PEAP.
- Step 18.** Select **Network Access > EapTunnel Equals PEAP** for the condition.
- Step 19.** Select the **LDAP object** for the identity source.
- Step 20.** Insert a new row below the EAP-TLS row to insert EAP-MD5.
- Step 21.** Select **Network Access > EapAuthentication Equals EAP-MD5** for the condition.
- Step 22.** Select **Internal Endpoints** for the identity source.
- Step 23.** Change the default identity store (bottom row) to be **Deny Access**.
- Step 24.** Click **Done**.
- Step 25.** Click **Save**.

Figure 10-17 shows the completed rule and sub-rules.



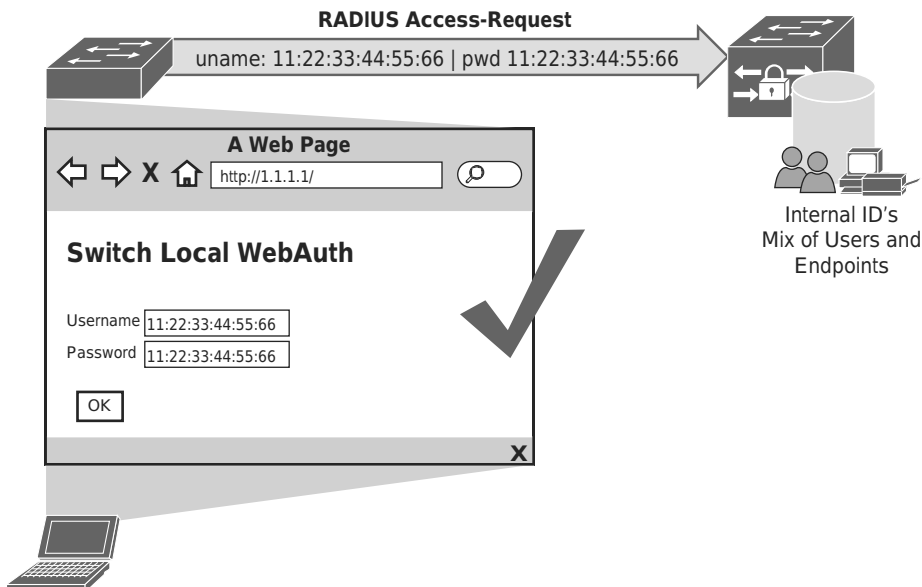
**Figure 10-17** *Completed authentication rule and Sub-rules.*

## More on MAB

One of the things that is often not understood, especially when looking to mix access device vendors, is MAB. There is no standard for MAB. Different vendors implement MAB in different ways. Ultimately, the goal is to allow the supplicant in the switch itself to run an authentication request for the endpoint because the endpoint obviously must not have a supplicant.

Some vendors send a RADIUS service-type of Login; some send a RADIUS service-type of Framed. Cisco uses a service-type of Call-Check for MAB. Why would Cisco use Call-Check if no other vendor does? Why does Cisco do MAB differently from everyone else? Quick answer: security.

Many years ago, before Cisco released Cisco ISE or the Cisco ACS 5.x server, there was a possible security vulnerability with MAB. That security vulnerability is still possible with other solutions and other network devices. The issue was/is the lack of differentiation between a MAB request and a local web authentication request. Both requests come from the network device with the same service type and the same format. There was no database separation of user IDs from endpoint IDs (MAC addresses). As displayed in Figure 10-18, a malicious user could enter a MAC address into the username and password fields of a web authentication or maybe even into the endpoint supplicant and gain access to the network.

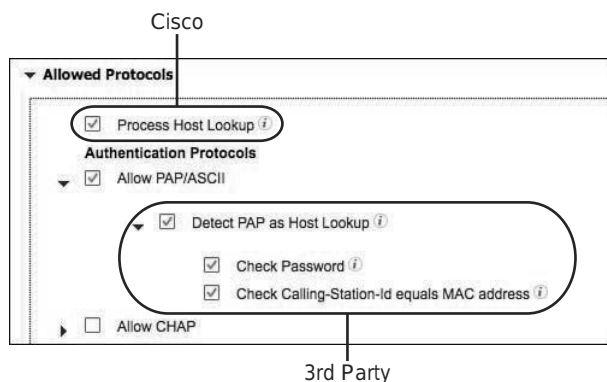


**Figure 10-18** Web authentication with MAC address instead of username.

In an effort to close this security hole and make MAB a bit more secure, Cisco changed the way it does MAB. The key differences are listed here:

- For authentication requests to be processed as MAB (by default), the service type must be Call-Check.
- RADIUS servers (ACS and ISE) maintain a separate endpoint database.
- The `calling-station-id` is the value that will be compared to the endpoint database, ignoring the username and password fields of the MAB request.

All supported Cisco NADs use a service type of Call-Check for MAB requests. They also ensure the `calling-station-id` is populated with the MAC address of endpoint. Lastly, Cisco ISE uses a simple check box within the allowed protocols configuration as another method to permit or deny the access into the endpoint database for the MAB request, as shown in Figure 10-19.



**Figure 10-19** *Process host lookup.*

As Figure 10-19 shows, the top selection for Process Host Lookup is the one for Cisco network devices. That check box allows RADIUS authentications with a service type of Call-Check to have the RADIUS `calling-station-id` value compared with the contents of the endpoints database. The selection for Process Host Lookup also exists under each of the individual authentication protocols (such as PAP, CHAP, and EAP-MD5). These are there for third-party support and are the reason there are two other check boxes: Check Password and Check Calling-Station-Id Equals MAC Address.

These check boxes make an insecure mechanism such as MAB a bit more insecure, so it is recommended that you secure it as much as possible by only allowing the network devices that must use MAB in the less secure manner to use it in that manner. This topic is discussed further in the successful deployment strategies section(s) of this book.

Keep in mind that MAB is inherently not a secure technology. When implementing MAB, you are bypassing the stronger security of 802.1X by allowing specific MAC addresses to gain access without authentication. When using MAB, always follow a defense-in-depth approach. This means a device that has been authorized to use the network from a MAB request should be granted access to the networks and services that

device is required to speak to only. In other words, don't provide full access to devices that have been MAB'd; instead provide them with an authorization that is more limited. This topic is covered in more detail in the next chapter where authorization policies are covered.

## Restore the Authentication Policy

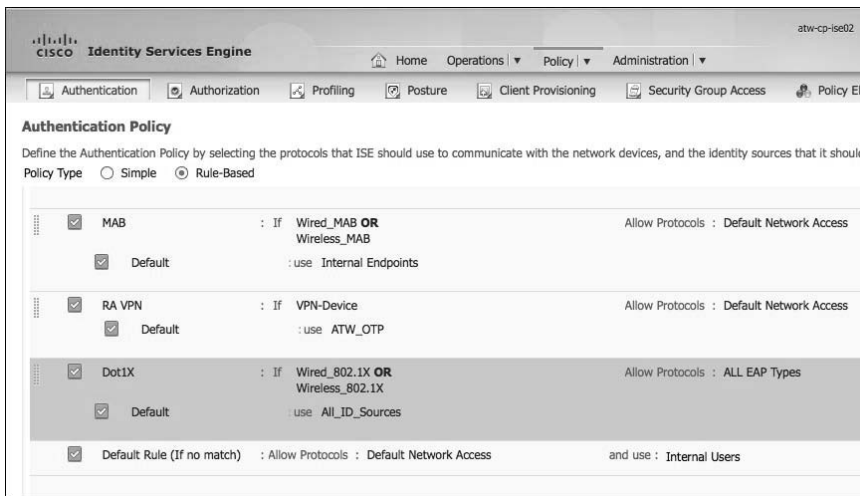
In this chapter, you have created a complex and specific authentication policy. This is useful for learning how authentication policies work, but it might make things a bit too complicated for you as you navigate through the future chapters.

To keep things simple, follow these steps to restore your authentication policy to something simple that will work for all use cases remaining in this book.

From the ISE GUI, do the following:

- Step 1.** Navigate to **Policy > Authentication**.
- Step 2.** Delete the rule named CiscoPress SSID.
- Step 3.** Edit the rule named Dot1X.
- Step 4.** Delete the PEAP, EAP-FAST, EAP-TLS, and EAP-MD5 rules.
- Step 5.** Change the Dot1X > Default rule from Deny Access to **All ID\_Sources**.

Figure 10-20 shows the final authentication policy that will enable you to support the use cases in the remainder of the book in an easy way.



**Figure 10-20** Simplified authentication policy.

This completes the authentication chapter. In the next chapter we take an in-depth look at authorization policies and common authorization rules.

---

## Exam Preparation Tasks

---

### Review All Key Topics

Review the most important topics in the chapter, noted with the key topics icon in the outer margin of the page. Table 10-2 lists a reference of these key topics and the page numbers on which each is found.



**Table 10-2** *Key Topics for Chapter 10*

Key Topic Element	Description	Page
Paragraph	Authentication and authorization	237
List	Allowed protocols	243
Paragraph	Matching an SSID	248
Paragraph	MAC authentication bypass	255

*This page intentionally left blank*

# Index

---

## Numerics

---

802.1X, 23, 56-58

- components, 56

- computer authentication, 73

- intended behavior of, 680-681

- NADs, 63

- supplicants, 63-89

  - Cisco AnyConnect NAM  
supplicant, 75-88*

  - devices without supplicants,  
97-98*

  - Windows native supplicant,  
64-72*

- user authentication, 72-73

## A

---

AAA (authentication, authorization,  
and accounting), 16, 21

- device administration, 16, 21-22

  - command sets, 22*

  - TACACS, 22*

- network access, 16, 22-32

  - RADIUS, 22, 28-32*

  - TACACS+, 23-27*

ACCEPT message (TACACS+), 25

access control

- ingress ACLs, 603-604

- VLAN assignment, 601-603

Access-Request message (RADIUS),  
29

accounting, 21

- RADIUS accounting servers, adding  
to WLC, 308-309

accuracy of personas, ensuring, 706

ACLs (access control lists)

- applying

  - to switchports, 305-306*

  - to WLCs, 310*

- DACLs,

- ingress ACLs, 603-604

- local ACLs, creating, 297-298

- number of ACEs, calculating, 603

- SGACLs, 629-632

- VACLs, 461-462

- web authentication redirection ACLs,  
creating, 310-313

ACS (Cisco Secure Access Control  
Server), 22

ActivatedGuests, 398

AD (Active Directory), 42, 221-226

- CA, 505-506

- computer authentication, 73

- domains, joining, 221-226

admin groups, Cisco ISE, 156

admin portal, 384

Administration Dashboard (Cisco  
ISE), 161-162

Administration node (Cisco ISE), 129

**Administration tab (Cisco ISE), 178-191**  
    Feed Service subcomponent, 191  
    Identity Management subcomponent, 183-186  
    Network Resources subcomponent, 186-189  
    System subcomponent, 178-182  
    Web Portal Management subcomponent, 189-190

**advanced functions, Cisco ISE, 127**  
    posturing, 128  
    profiling, 127

**Advanced license package (Cisco ISE), 178**

**agent types (NAC), 650-651**

**Alarms dashlet (Administration Dashboard), 162**

**alternative ID stores example, authentication policies, 253-254**

**AND operator, combining with OR operator, 281-286**

**Android device onboarding flow, 573-577**

**answering exam questions, 765-766**

**AnyConnect Diagnostics and Reporting tool, 748-750**

**AnyConnect Profile Editor, configuring Cisco AnyConnect NAM supplicant, 75-88**  
    Authentication Policy view, 78  
    Client Policy view, 76-78  
    Network Groups view, 87  
    Networks view, 79-86

**answers to “Do I Know This Already?” quizzes, 773-792**

**applying ACLs**  
    to switchports, 305-306  
    to WLCs, 310

**assessment options for posturing, 652-654**

**authentication servers, 56**

**authentication, 21, 233-232. *See also* authentication policies; WebAuth 802.1X**  
    *computer authentication, 73*  
    *intended behavior, 680-681*  
    *NADs, 63*  
    *supplicants, 63-89*  
    *user authentication, 72-73*

**and authorization, 237**

**certificate authentication**  
    *configuring, 506-516*  
    *EAP-TLS, 506*  
    *proof of possession, verifying, 504-505*  
    *revocation, verifying, 502-503*  
    *signing of certificates, verifying, 499-500*  
    *validity dates, verifying, 501*  
    *verifying, 516-519*

devices without supplicants, managing  
*MAB, 98-100, 115-116*  
*web authentication, 100-106*

## EAP

*802.1X, 56*  
*native types, 58-59*  
*tunneled types, 59-61*

failure types, 401

OTP services, 44-45

posturing, 117-118

two-factor authentication, 43-44

verifying

*on Cisco switches, 329-334*  
*on WLCs, 334-336*

WebAuth, 340-341

*CWA, 346-349*

*DRW, 349*

*LWA (local web authentication), 346*

on wired switches, configuring

*ACL, applying, 305-306*  
*creating local ACLs, 297-298*  
*Flex-Auth, 299-302*  
*global 802.1X commands, 297*  
*global configuration AAA commands, 293-294*  
*global configuration RADIUS commands, 294-297*

*HA, 299-302*

*host mode of switchport, setting, 302-303*

*settings, 303-305*

*switchports, 299*

*timers, 305*

on WLCs, configuring, 306-328

*ACLs, applying, 310*

*corporate SSID, creating, 324-328*

*dynamic interfaces for client VLAN, creating, 315*

*guest dynamic interface, creating, 317*

*guest WLAN, creating, 319-323*

*posture agent redirection ACL, creating, 313-314*

*RADIUS accounting servers, adding, 308-309*

*RADIUS authentication servers, adding, 306-308*

*RADIUS fallback, 309-310*

*web authentication redirection ACL, creating, 310-313*

**Authentication Live Log, 436-438**

**authentication policies**

allowed protocols, 243-247

conditions, 241-243

examples

*alternative ID stores example, 253-254*

*remote access VPN example, 251-252*

*wireless SSID example, 248-251*

goals, 238-239

identity store, 247

MAB, 255-257

MAB rule flow chart, 240

options, 247

restoring, 257

**Authentication Policy view (AnyConnect Profile Editor), 78**

**Authentication subcomponent (Cisco ISE), 173**

**Authentication subcomponent (Operations tab), 165-169**

**Authentications dashlet (Administration Dashboard), 162**

**authenticators, 56**

authorization, 21. *See also* authorization policies

and authentication, 237

CoA, 31-32, 113

*and Cisco ISE Profiler*, 478-482

*posturing*, 654-655

guest authorization, configuring,  
400-415

authorization policies, 265-279

building, 360-362

conditions, saving for reuse, 279-281

goals of, 265-266

profiles

*endpoint identity groups*, 483-485

*EndPointPolicy*, 486

rules, 266-279

*examples*, 272-279

*role-specific authorization rules*,  
271

Authorization subcomponent (Cisco ISE), 173

AV-pairs, 31

## B

---

backup and restore strategies, 718-719

bandwidth, requirements for Cisco ISE,  
139

Base license package (Cisco ISE), 178

bootstrapping Cisco ISE, 201-215

CA-signed certificates, 206-215

certificates

*locating*, 204-205

*self-signed certificates*, 206

building blocks for posturing, 658-659

BYOD (bring your own device)

challenges, 528-529

Dogtag, 821-825

*configuring*, 829-842

*installing*, 829-830

*installing packages with yum*, 825

*NTP service, configuring*, 826-827

*PHP services, installing*, 828-829

*prerequisites*, 821-825

EAP chaining, 593-594

LDAP server, installing, 827-828

Microsoft CA, configuring for BYOD,  
796-819

*requirements*, 795-796

onboarding process, 529-530

*Android onboarding flow*,  
573-577

*configuring on Cisco ISE*, 538-569

*device enrollment*, 571

*device registration*, 570

*dual-SSID approach*, 530

*flows, verifying*, 581-582

*iOS onboarding flow*, 570-573

*Mac OSX onboarding flow*,  
577-580

*NADs, configuring*, 532-538

*Windows device onboarding flow*,  
577-580

## C

---

CACs (common access cards), 45-46

calculating number of ACEs per ACL,  
603

CAP (certificate authentication profile),  
226-227

captive portal bypass, 354-355

CAs (certificate authorities), 46

AD, 505-506

CRLs, 49

- Dogtag, 821-825
  - configuring*, 830-842
  - configuring ISE for use*, 842-843
  - installing*, 829-830
  - LDAP server, installing*, 827-828
  - NTP service, configuring*, 826-827
  - PHP services, installing*, 828-829
- Microsoft CA, configuring for BYOD, 796-819
  - requirements*, 795-796
- CA-signed certificates, 206-215
- CCNP Security certification track, 2-4
- CDP (Cisco Discovery Protocol), 116
- certificate authentication
  - configuring, 506-516
    - allowed protocols, validating*, 507-508
    - authorization policies*, 511-512
    - CAP, verifying*, 508-511
    - ensuring trust*, 512-513
    - public certificate, importing*, 513-515
- EAP-TLS, 506
  - proof of possession, verifying, 504-505
  - revocation, verifying, 502-503
  - signing of certificates, verifying, 499-500
  - validity dates, verifying, 501
  - verifying, 516-519
- certificates, 180. *See also* certificate authentication
  - CAP, 226-227
  - CA-signed certificates, 206-215
  - CRLs, 49
  - locating, 204-205
  - OCSP, 49-50
  - self-signed certificates, 206
  - X.509 certificates, 46
    - revocation*, 48-49
    - validity dates*, 47-48
- certification
  - CCNP Security certification track, 2-4
  - security certifications, comparing, 6
- challenges to BYOD, 528-529
- CHAP (Challenge/Handshake Authentication Protocol), 23
- Cisco AnyConnect NAM supplicant, 87-88
  - AnyConnect NAM profiles, implementing, 87-88
  - AnyConnect Profile Editor
    - Authentication Policy view*, 78
    - Client Policy view*, 76-78
    - Network Groups view*, 87
    - Networks view*, 79-86
  - configuring, 75-88
  - EAP chaining, 89
- Cisco Certification Exam Tutorial, 759-760
- Cisco IOS 12.2.X, global configuration
  - RADIUS commands, 294
- Cisco IOS 15.X, global configuration
  - AAA commands, 295-297
- Cisco ISE (Identity Services Engine), 127-129
  - admin groups, 156
  - advanced functions, 127
  - authentication policies, 237-254
    - allowed protocols*, 243-247
    - alternative ID stores example*, 253-254
    - conditions*, 241-243
    - goals of*, 238-239
    - identity store*, 247
    - MAB*, 255-257
    - options*, 247

- remote access VPN example, 251-252*
- restoring, 257*
- wireless SSID example, 248-251*
- backup and restore strategies, 718-719
- bandwidth requirements, 139
- bootstrapping, 201-215
  - CA-signed certificates, 206-215*
  - locating certificates, 204-205*
  - self-signed certificates, 206*
- certificate authentication, configuring, 506-516
  - allowed protocols, validating, 507-508*
  - authorization policies, 511-512*
  - CAP, verifying, 508-511*
  - ensuring trust, 512-513*
  - public certificate, importing, 513-515*
  - verifying configuration, 516-519*
- CRLs, 49
- deploying, 133
  - four-node deployment, 136-137*
  - fully distributed deployment, 137*
  - single-node deployment, 133-135*
  - two-node deployment, 135-136*
- Dogtag, configuring, 842-843
- external identity stores, 41-50
  - AD, 42*
  - LDAP, 42-43*
  - smart cards, 45-46*
- form factors, 201
- Guest Services, 399-400. *See also* portals; WebAuth
- guest-level access, Cisco ISE, 128
- GUI, 150
  - Administration Dashboard, 161-162*
  - Administration Home page, 162-164*
  - Administration tab, 178-191*
  - Operations tab, 165-172*
  - Policy tab, 173-177*
- HA
  - MnT, 707-709*
  - node groups, 710-712*
  - PANs, 709-710*
- internal identity stores, 39-40
- licensing packages, 178
  - licensing in multinode cube, 706-707*
- logging events, 129
- logging in, 155-156
- network devices
  - NADs, 217-218*
  - NDGs, 216*
- nodes
  - communication between, 138-139*
  - configuring in distributed environment, 702-706*
  - load balancing, 713-715*
  - promoting to primary device, 702-703*
- onboarding process (BYOD), configuring, 538-569
- patching, 716
- personas, 129-131
  - Administration node, 129*
  - IPN, 130-131*
  - MnT, 130*
  - Policy Service Node, 129-130*
- phased deployment approach, 681-694
  - Closed Mode, 692-694*
  - Low-Impact Mode, 689-695*
  - Monitor Mode, 685-689*
  - preparing for, 683-685*

- transitioning to end state*, 695
- on wireless networks*, 695
- physical appliance specifications, 131
- policies, 192-194
  - authentication*, 233-232
- portals, 384-389
- posturing, 128, 648
  - assessment options*, 652-654
  - authorization policy for compliance, modifying*, 666-667
  - authorization policy for CPP, modifying*, 663-665
  - building blocks*, 658-659
  - CoA*, 654-655
  - conditions*, 659-660
  - functional components*, 648
  - NAC agent types*, 650-651
  - posture conditions*, 652-654
  - remediation*, 661
  - requirement function*, 662-663
  - verifying*, 667-674
- profiling, 127, 445-447
  - probes*, 447-459
- RADIUS, 127
- services, 138-139
- syslog, 332-334
- trusted-level access, 128
- user identity groups, 40
- virtual appliance specifications, 132
- web browser support, 150
- X.509 certificates, 46
  - revocation*, 48-49
  - validity dates*, 47-48
- Cisco ISE Profiler, 445-447. *See also***
  - and CoA, 478-482
    - global CoA*, 479-480
    - per-profile CoA*, 480-481
  - endpoint attribute filtering, 482
  - verifying profiling, 486-491
    - dashboard*, 486-487
    - Endpoints Drill-down tool*, 487-488
    - Global Search tool*, 488
- Cisco security certifications, comparing**, 6
- Client Policy view (AnyConnect Profile Editor)**, 76-78
- client provisioning**, 193
- Client Provisioning subcomponent (Cisco ISE)**, 175-176
- Closed Mode**, 692-694
- CoA (change of authorization)**, 31-32, 113
  - and Cisco ISE Profiler, 478-482
    - global CoA*, 479-480
    - per-profile CoA*, 480-481
  - posturing, 654-655
- collection filters**, 746-747
- combining AND with OR operators**, 281-286
- command sets**, 22
- commands**
  - debug commands, 336, 755
  - global 802.1X commands, 297
  - global configuration AAA commands, 293-294
  - global configuration RADIUS commands, 294-297
  - show aaa servers command, 329-330
  - show authentication session command, 331-332
  - show authentication sessions interface command, 668, 753-754
  - show device-sensor cache all command, 491
  - show monitor command, 460
  - test aaa command, 330-331

**communication between Cisco ISE nodes, 138-139**

**communication flows, RADIUS, 29-30**

**comparing**

authentication and authorization, 237, 265

EAP types, 62

RADIUS and TACACS+, 32

security certifications, 6

virtual versus physical Cisco ISE deployments, 131-133

**components of 802.1X, 56**

**computer authentication, 73**

**conditions, 241-243**

combining AND with OR operators, 281-286

saving for reuse, 279-281

**conditions (posture service), 117-118, 652-654, 659-660**

**configuration backups, 718-719**

**configuring**

authentication

*on wired switches, 293-306*

*on WLCs, 306-328*

**BYOD**

*Cisco ISE configuration, 538-569*

*onboarding, 532-538*

certificate authentication, 506-516

*allowed protocols, validating, 507-508*

*authorization policies, 511-512*

*CAP, verifying, 508-511*

*ensuring trust, 512-513*

Cisco AnyConnect NAM supplicant, 75-88

Dogtag, 829-842

Guest Services, guest authorization, 400-415

ISS, 356-357

MDM onboarding, 584-589

Microsoft CA for BYOD, 796-819

*requirements, 795-796*

nodes in distributed environment, 702-706

*ensuring accuracy of personas, 706*

*promoting node to primary device, 702-703*

*registering node to the deployment, 703-705*

NTP, 826-827

portals

*Friendly Names, 391-392*

*interfaces, 391*

*ports, 389-390*

posture service, 655-674

*conditions, 659-660*

*CPP, 657*

*remediation, 661*

*requirement function, 662-663*

profiling, 459-464

*device sensors, 462-463*

*DHCP helper, 459-460*

*SNMP settings, 481*

*SPAN, 460*

*VACLs, 461-462*

*VMware, 463-464*

sponsor portal

*policies, 392-393*

*sponsor groups, 394-396*

WebAuth

*CWA, 350-359*

*device registration, 363-368*

Windows native supplicant, 64-72

**CONTINUE packets (TACACS+), 25**

**controlling access to networks**

- ingress ACLs, 603-604

- VLAN assignment, 601-603

**CPP (client provisioning policy), 657**

- authorization policy, modifying, 663-665

- resources, downloading, 656-657

**creating**

- individual accounts, 416

- ISE cubes, 704-705

- local ACLs, 297-298

- random user accounts, 417

**CRLs (certificate revocation lists), 49****cubes (ISE)**

- creating, 704-705

- licensing, 706-707

- logging targets, 729-730

**customizing portals, 399-400****CWA (centralized web authentication), 104-106, 346-349**

- authorization policies, building, 360-362

- captive portal bypass, 354-355

- configuring, 350-359

- verifying, 369-375

**D****DACLs (downloadable access control lists),****dashboard, verifying profiling, 486-487****dashlets (Administration Dashboard), 162****databases**

- identity stores, 38-40

**databases, identity stores**

- external identity stores, 41-50

- internal identity stores, 39-40

**debug commands, 336, 755****debug logs, 731-732****deploying Cisco ISE, 133. *See also* phased deployment approach**

- four-node deployment, 136-137

- fully distributed deployment, 137

- single-node deployment, 133-135

- two-node deployment, 135-136

**device administration, 16, 21-22**

- command sets, 22

- TACACS, 22

**device sensors, configuring, 462-463****devices without supplicants, managing**

- MAB, 98-100

- DHCP profiling, 116*

- MAC addresses, 115-116*

- WebAuth, 100-106

**DHCP helper, 459-460****DHCP profiling, 116**

- probes, 449-452

**DHCPSPAN probes, 449-452****diagnostic tools, 735-747**

- AnyConnect Diagnostics and Reporting tool, 748-750

- collection filters, 746-747

- endpoint diagnostics, 748

- Evaluate Configuration Validator, 735-739

- RADIUS Authentication

- Troubleshooting tool, 739-740

- TCP Dump, 741-746

**DIAMETER, 23****distributed environments**

- nodes, configuring, 702-706

- ensuring accuracy of personas, 706*

- promoting node to primary device, 702-703*

*registering node to the  
deployment, 703-705*

**DNS probes, 454**

**Dogtag, 821-825**

configuring, 829-842

installing, 829-830

installing packages with yum, 825

LDAP server, installing, 827-828

NTP service, configuring, 826-827

PHP services, installing, 828-829

prerequisites for use, 821-825

**domains (AD), joining, 221-226**

**Dot1X. *See* 802.1X**

**Downlink MACSec, 634-635**

**downloading**

CPP resources, 656-657

debug logs, 732

**DRW (device registration WebAuth),  
349**

**dual-SSID onboarding, 530**

## E

---

**EAP (Extensible Authentication  
Protocol)**

802.1X, 56-58

native types, 58-59

tunneled types, 59-61

types of, comparing, 62

**EAP chaining, 89, 593-594**

**EAP-FAST, 60-61**

**EAP-GTC, 59**

**EAP-MD5, 58**

**EAP-MSCHAPv2, 59**

**EAPoL (EAP over LAN), 56-58**

components, 56

**EAP-TEAP, 89**

**EAP-TLS, 58-59**

certificate authentication, 506

**endpoint attribute filtering, 482**

**endpoint profile policies, 467-477**

**Endpoint Protection Service, 170**

**EndPointPolicy, 486**

**endpoints**

diagnostics, 748

identities, 489

local endpoint groups, 219

managing, 590-593

MDMs, 119

posturing, 117-118, 649

**Endpoints Drill-down tool, 487-488**

**enforcing traffic based on SGT,  
628-632**

**enrolling devices for BYOD, 571**

**ensuring accuracy of personas, 706**

**ERROR message (TACACS+), 25**

**ERS Admin role (Cisco ISE), 156**

**ERS Guest role (Cisco ISE), 156**

**Evaluate Configuration Validator,  
735-739**

**Evaluation license package (Cisco ISE),  
178**

**exam. *See* SISAS 300-208 exam;  
practice exams**

**examples**

of authentication policies

*alternative ID stores example,  
253-254*

*remote access VPN example,  
251-252*

*wireless SSID example, 248-251*

of authorization policies, 272-279

**extended logging, 751**

**external identity sources, 38**

**external identity stores, 41-50, 220-229**  
 AD, 42, 221-226  
     *domains, joining, 221-226*  
 CAP, 226-227  
 ISS, 227-229  
 LDAP, 42-43  
 smart cards, 45-46

## F

---

**failure types, authentication, 401**  
**features of MDMs, 119**  
**Fedora**  
     installing packages with yum, 825  
     proxy configuration, 825  
**Feed Service subcomponent (Cisco ISE), 191**  
**FIPS (Federal Information Processing Standard), 77**  
**Flex-Auth, configuring on wired switches, 299-302**  
**flows (onboarding), verifying, 581-582**  
**form factors for Cisco ISE, 201**  
**format of SISAS 300-208 exam, 9-10**  
**four-node deployment (Cisco ISE), 136-137**  
**Friendly Names, configuring on web portals, 391-392**  
**fully distributed deployment (Cisco ISE), 137**  
**functional components of posture service, 648**

## G

---

**global 802.1X commands, 297**  
**global CoA, 479-480**  
**global configuration AAA commands, 293-294**

**global configuration RADIUS commands, 294-297**

**Global Search tool, 488**

**goals**

    of authentication policies, 238-239  
     of authorization policies, 265-266

**groups**

    local endpoint groups, 219  
     local user identity groups, 218  
     NDGs, 216  
     node groups, HA, 709-710  
     sponsor groups

*configuring, 394-396*

*mapping, 396-397*

**guest accounts, provisioning, 416**

**Guest Services. *See also* WebAuth**

    guest accounts, provisioning, 416  
     guest authorization, configuring, 400-415

    guest user portal, screen elements, 386-389

    importing user accounts, 418

    individual accounts, creating, 416

    portals, 384-389

*customizing, 399-400*

    random user accounts, creating, 417

    verifying guest access

*on the switch, 428-438*

*on WLC, 419-427*

    web portals

*configuring, 391-392*

    web portals, configuring, 389-390

**guest user portal, 385**

    screen elements, 386-389

**guest user types, 398**

**guest-level access, Cisco ISE, 128**

**GUI (Cisco ISE), 150**

    admin groups, 156

Administration Dashboard, 161-162  
 Administration Home page, 162-164  
 Administration tab, 178-191

*Feed Service subcomponent*, 191

*Identity Management subcomponent*, 183-186

*Network Resources subcomponent*, 186-189

*System subcomponent*, 178-182

*Web Portal Management subcomponent*, 189-190

logging in, 155-156

Operations tab, 165-172

*Authentication subcomponent*, 165-169

*Reports subcomponent*, 169

*Troubleshoot subcomponent*, 171-172

Operations tab (Cisco ISE), Endpoint Protection Service, 170

Policy tab, 173-177

*Authentication subcomponent*, 173

*Authorization subcomponent*, 173

*Client Provisioning subcomponent*, 175-176

*Policy Elements subcomponent*, 177

*Posture subcomponent*, 175

*Profiling subcomponent*, 174-175

*Security Group Access subcomponent*, 176

guidelines for load balancing, 713-714

## H

---

### HA (high availability)

configuring on wired switches, 299-302  
 MnT, 707-709

node groups, 710-712

PANs, 709-710

RADIUS fallback, 309-310

hard tokens, 44

Help link (Administration Home page), 163-164

Helpdesk admin role (Cisco ISE), 156

host mode of switchport, setting, 302-303

hotfixes for Windows native supplicant, 752

HTTP probes, 457-459

## I

---

identifying knowledge gaps in exam topics, 767-769

identities, 38

Identity Admin role (Cisco ISE), 156

identity groups, local user identity groups, 218

identity management, 35-34

endoint identities, 489

OTP services, 44-45

two-factor authentication, 43-44

X.509 certificates, 46

CRLs, 49

validity dates, 47-48

Identity Management subcomponent (Cisco ISE), 183-186

identity source sequence, 38

identity stores, 38-40, 247

external identity stores, 41-50, 220-229

AD, 221-226

CAP, 226-227

LDAP, 42-43

identity source sequence, 38

internal identity stores, 39-40

- ISS, 227-229
- local endpoint groups, 219
- local users, 220
- IEEE 802.1X, 23, 56-58**
  - components, 56
  - computer authentication, 73
  - intended behavior, 680-681
  - NADs, 63
  - supplicants, 63-89
    - Cisco AnyConnect NAM supplicant*, 75-88
    - devices without supplicants*, 97-98
    - Windows native supplicant*, 64-72
  - user authentication, 72-73
- implementing AnyConnect NAM profiles, 87-88**
- importing**
  - public certificates, 513-515
  - user accounts, 418
- individual accounts, creating, 416**
- ingress access control**
  - ingress ACLs, 603-604
  - VLAN assignment, 601-603
- installing**
  - Dogtag, 829-830
  - LDAP server, 827-828
  - PHP services, 828-829
- intended audience for this book, 6**
- intended behavior of 802.1X, 680-681**
- interfaces**
  - configuring as switchports, 299
  - configuring on web portals, 391
  - dynamic interfaces for client VLAN, creating, 315
  - guest dynamic interface, creating, 317
- internal endpoint database, 40**
- internal identity stores, 39-40**

- iOS devices, onboarding flow, 570-573
- IOS load balancing, 715-716
- IPN (Inline Posture Node), 130-131
- ISE. *See* Cisco ISE (Identity Services Engine)
- ISS (identity source sequences), 227-229
  - configuring, 356-357

## J-K

---

- Jobs, Steve, 522
- joining AD domains, 221-226
- knowledge gaps in exam topics, identifying, 767-769

## L

---

- LDAP (Lightweight Directory Access Protocol), 42-43**
- licensing packages**
  - Cisco ISE, 178
  - licensing in multinode cube, 706-707
- Live Authentication Log, 726-728**
  - viewing, 336-337
- Live Sessions Log, 728**
  - viewing, 337
- LLDP (Link Layer Discovery Protocol), 116**
- load balancing, 713-715**
  - IOS load balancing, 715-716
- local ACLs, creating, 297-298**
- local user identity groups, 218**
- local users, 220**
- locating certificates, 204-205**
- logging**
  - Authentication Live Log, 436-438
  - categories, 730

- Cisco ISE, 129
- debug logs, 731-732
- extended logging, 751
- Live Authentication Log, 726-728
  - viewing*, 336-337
- Live Sessions Log, 728
  - viewing*, 337
- log files, viewing from CLI, 733-734
- supplicant provisioning logs, 753
- support bundles, 734
- syslog, 332-334
- targets, 729-730
- logging in to Cisco ISE, 155-156
- logical profiles, 478
- Low-Impact Mode, 689-695
- LWA (local web authentication), 101-102, 346
  - with centralized portal, 102-104

## M

---

- MAB (MAC Authentication Bypass), 98-100, 113-117
  - authentication policies, 255-257
  - authorization policy, 403-406
  - DHCP profiling, 116
  - MAC addresses, 115-116
  - rules, 240
- MAC addresses, 115-116
- Mac OSX device onboarding flow, 577-580
- MACSec, 632-641
  - Downlink MACSec, 634-635
  - Uplink MACSec, 638-640
- maintenance
  - backup strategies, 718-719
  - patching Cisco ISE, 716

- managing
  - devices without supplicants
    - MAB*, 98-100, 113-117
    - WebAuth*, 100-106
  - endpoints, 590-593
  - mobile devices, MDMs, 119
- mapping sponsor groups, 396-397
- MDM (mobile device management), 118-119
  - features, 119
  - onboarding process, 583-589
    - integration points*, 583
  - onboarding process (BYOD), configuring, 584-589
  - vendors, 119
- messages
  - RADIUS
    - accounting messages*, 30
    - authentication and authorization messages*, 29-30
  - TACACS+
    - authentication messages*, 25
    - authorization and accounting messages*, 26-27
- Metrics dashlet (Administration Dashboard), 162
- Microsoft Active Directory, 42
- Microsoft CA, configuring for BYOD, 796-819
  - requirements, 795-796
- MnT (Monitoring and Troubleshooting node), 130
  - HA, 707-709
- Mnt Admin role (Cisco ISE), 156
- mobile devices
  - BYOD
    - Android device onboarding flow*, 573-577

*challenges*, 528-529  
*configuring on Cisco ISE*, 538-569  
*iOS onboarding flow*, 570-573  
*Mac OSX device onboarding flow*,  
 577-580  
*onboarding flows, verifying*,  
 581-582  
*onboarding process*, 529-530,  
 570-571  
*single-SSID onboarding*, 531-530  
*Windows device onboarding flow*,  
 577-580

MDMs (mobile device managers), 119

#### modifying authorization policy

for compliance, 666-667

for CPP, 663-665

Monitor Mode, 685-689

MS-CHAP (Microsoft CHAP), 23

multinode cubes, licensing, 706-707

## N

### NAC (network admission control) agent

agent types, 650-651

posture assessment, 649

supported remediation types, 651

NADs (Network Access Devices), 23,  
 63, 217-218

configuring for onboarding, 532-538

verifying authentication, 329

NAM (Network Access Manager)  
 profiles, implementing, 87-88

native EAP types, 58-59

native tagging, 621-628

NDGs (network device groups), 216

NetFlow probes, 457

network access, 16, 22-32

RADIUS, 22, 28-32

*accounting messages*, 30

*authentication and authorization  
 messages*, 29-30

*AV-pairs*, 31

*CoA*, 31-32

*communication flows*, 29-30

*comparing to TACACS+*, 32

*service types*, 29

TACACS+, 23-27

*authentication messages*, 25

*authorization and accounting  
 messages*, 26-27

*comparing to RADIUS*, 32

Network Device Admin role (Cisco ISE),  
 156

### network devices

NADs, 217-218

NDGs, 216

Network Groups view (AnyConnect  
 Profile Editor), 87

Network Resources subcomponent  
 (Cisco ISE), 186-189

Networks view (AnyConnect Profile  
 Editor), 79-86

NMAP probes, 453-454

node groups, HA, 709-710

nodes (Cisco ISE), 129-131

Administration node, 129

communication between, 138-139

configuring in distributed environment,  
 702-706

*ensuring accuracy of personas*,  
 706

*promoting node to primary  
 device*, 702-703

*registering node to the  
 deployment*, 703-705

four-node deployment, 136-137

- IPN, 130-131
- load balancers, 713-715
- MnT, 130
  - HA, 707-709
- multinode cubes, licensing, 706-707
- PANs, HA, 709-710
- Policy Service Node, 129-130
- single-node deployment, 133-135
- two-node deployment, 135-136
- nontunneled EAP types, 58-59**
- NTP (Network Time Protocol), 48**
  - configuring, 826-827

## O

---

- OCSP (Online Certificate Status Protocol), 49-50**
- onboarding process (BYOD), 529-530.**
  - See also* onboarding process (MDM)
  - Android onboarding flow, 573-577
  - configuring on Cisco ISE, 538-569
  - device enrollment, 571
  - device registration, 570
  - dual-SSID approach, 530
  - flows, verifying, 581-582
  - iOS onboarding flow, 570-573
  - Mac OSX onboarding flow, 577-580
  - NADs, configuring, 532-538
  - single-SSID approach, 531-530
  - Windows device onboarding flow, 577-580
- onboarding process (MDM), 583-589**
  - configuring, 584-589
  - integration points, 583
- operational backups, 718-719**
- Operations tab (Cisco ISE), 165-172**
  - Authentication subcomponent, 165-169
  - Endpoint Protection Service, 170

- Reports subcomponent, 169
- Troubleshoot subcomponent, 171-172
- operators, combining AND with OR operators, 281-286**
- options**
  - assessment options for posturing, 652-654
  - for authentication policy rules, 247
- OR operator**
  - combining with AND operator, 281-286
- OTP (one-time password) services, 44-45**
- OUIs (organizationally unique identifiers), 115-116**

## P

---

- packages, updating with yum, 826
- PANs (policy administration nodes), HA, 709-710
- PAP (Password Authentication Protocol), 23**
- passwords, OTP services, 44-45
- patching Cisco ISE, 716
- PEAP (Protected EAP), 60**
- Pearson VUE, registering for SISAS 300-208 exam, 5-6**
- permitting promiscuous traffic, 463-464**
- per-profile CoA, 480-481**
- personas, 129-131**
  - Administration node, 129
  - communication between, 138-139
  - four-node deployment, 136-137
  - IPN, 130-131
  - nodes, configuring in distributed environment, 702-706
    - ensuring accuracy of personas, 706*

- multinode cubes, licensing, 706-707*
- promoting node to primary device, 702-703*
- registering node to the deployment, 703-705*
- Policy Service Node, 129-130
- single-node deployment, 133-135
- two-node deployment, 135-136
- phased deployment approach, 681-694**
  - Closed Mode, 692-694
  - Low-Impact Mode, 689-695
  - Monitor Mode, 685-689
  - preparing Cisco ISE for, 683-685
  - transitioning to end state, 695
  - on wireless networks, 695
- PHP services, installing, 828-829**
- physical appliance specifications (Cisco ISE), 131**
- PKI (Public Key Infrastructure), 180**
- Plus license package (Cisco ISE), 178**
- policies (Cisco ISE), 192-194**
  - authentication, 233-232
  - authentication policies, 237-254
    - allowed protocols, 243-247*
    - alternative ID stores example, 253-254*
    - conditions, 241-243*
    - goals of, 238-239*
    - identity store, 247*
    - MAB, 255-257*
    - MAB rule flow chart, 240*
    - options, 247*
    - remote access VPN example, 251-252*
    - restoring, 257*
    - wireless SSID example, 248-251*
  - authorization policies, 265-279
    - conditions, saving for reuse, 279-281*
    - examples, 272-279*
    - goals of, 265-266*
    - rules, 266-279*
- CPP, 657
  - resources, downloading, 656-657*
- guest authorization policies, configuring, 400-415
- profiling policies, 464-478
  - endpoint profile policies, 467-477*
  - logical profiles, 478*
  - profiler feed service, 464-466*
- Policy Admin role (Cisco ISE), 156**
- Policy Elements subcomponent (Cisco ISE), 177**
- Policy Service Node (Cisco ISE), 129-130**
- Policy tab (Cisco ISE), 173-177**
  - Authentication subcomponent, 173
  - Authorization subcomponent, 173
  - Client Provisioning subcomponent, 175-176
  - Policy Elements subcomponent, 177
  - Posture subcomponent, 175
  - Profiling subcomponent, 174-175
  - Security Group Access subcomponent, 176
- Port Bounce CoA, 480**
- portals, 384-389**
  - captive portal bypass, 354-355
  - customizing, 399-400
  - Friendly Names, configuring, 391-392
  - guest user portal, screen elements, 386-389
  - interfaces, configuring, 391
  - ports, configuring, 389-390

## sponsor portal

- guest accounts, provisioning, 416*
- guest user types, 398*
- policies, configuring, 392-393*
- sponsor groups, configuring, 394-396*
- sponsor groups, mapping, 396-397*
- types of sponsors, 393-396*

## ports

- communication between Cisco ISE nodes, 138-139
- configuring on web portals, 389-390

## Posture Compliance dashlet (Administration Dashboard), 162

## Posture subcomponent (Cisco ISE), 175

## posturing, 117-118, 128, 648

- assessment options, 652-654
- building blocks, 658-659
- CoA, 654-655
- compliance, modifying authorization policy, 666-667
- conditions, 659-660
- configuring, 655-674
- CPP, 657
  - authorization policy, modifying, 663-665*
- functional components, 648
- NAC
  - agent types, 650-651*
  - supported remediation types, 651*
- posture conditions, 652-654
- remediation, 661
- requirement function, 662-663
- verifying, 667-674

## POTS (plain old telephone service), 22

## PPP (Point-to-Point Protocol), 28

## practice exams, 763-767

## preparing

- Cisco ISE for phased deployment, 683-685
- for SISAS 300-208 exam, 759, 769-770
  - answering questions, 765-766*
  - Cisco Certification Exam Tutorial, 759-760*
  - exam-day advice, 762-763*
  - features of this book, 13-14*
  - knowledge gaps, identifying, 767-769*
  - practice exams, 766-767*
  - pre-exam suggestions, 762*
  - time management, 760-762*
  - topics covered, 4-5*

## probes, 447-459

- DHCP probes, 449-452
- DHCPSPAN probes, 449-452
- DNS probes, 454
- HTTP probes, 457-459
- NetFlow probes, 457
- NMAP probes, 453-454
- RADIUS probes, 452-453
- SNMP probes, 455-456
- SNMP settings, configuring, 481

## Profiler Activity dashlet (Administration Dashboard), 162

## profiler feed service, 464-466

## profiling, 127, 193, 445-447. *See also* profiling policies

- authorization policies
  - endpoint identity groups, 483-485*
  - EndPointPolicy, 486*
- endpoint attribute filtering, 482
- infrastructure, configuring, 459-464
  - device sensors, 462-463*
  - DHCP helper, 459-460*
  - SPAN, 460*
  - VACLs, 461-462*

- interfaces, VMware, 463-464
- NetFlow probes, 457
- probes, 447-459
  - DHCP probes*, 449-452
  - DHCPSPAN probes*, 449-452
  - DNS probes*, 454
  - HTTP probes*, 457-459
  - NMAP probes*, 453-454
  - RADIUS probes*, 452-453
  - SNMP probes*, 455-456
  - SNMP settings, configuring*, 481
- verifying, 486-491
  - dashboard*, 486-487
  - Endpoints Drill-down tool*, 487-488
  - Global Search tool*, 488
- profiling policies**
  - endpoint profile policies, 467-477
  - logical profiles, 478
  - profiler feed service, 464-466
- Profiling subcomponent (Cisco ISE)**, 174-175
- promiscuous traffic, permitting**, 463-464
- promoting nodes to primary device**, 702-703
- proof of possession for certificates, verifying**, 504-505
- provisioning**
  - client provisioning, 193
  - guest accounts from sponsor portal, 416
  - supplicant provisioning logs, 753
- pseudo-browsers**, 355
- PSNs (policy service nodes), probes**, 447-459
  - DHCP profiling, 449-452
  - DHCPSPAN probes, 449-452

- DNS probes, 454
- HTTP probes, 457-459
- NetFlow probes, 457
- NMAP probes, 453-454
- RADIUS probes, 452-453
- SNMP probes, 455-456

## Q-R

---

- RA (remote access)**, 106
- RADIUS (Remote Authentication Dial-In User Service)**, 22, 28-32, 127
  - accounting messages, 30
  - authentication and authorization messages, 29-30
  - AV-pairs, 31
  - CoA, 31-32, 113
  - communication flows, 29-30
  - comparing to TACACS+, 32
  - IOS load balancing, 715-716
  - probes, 452-453
  - service types, 29
- RADIUS Authentication Troubleshooting tool**, 739-740
- random user accounts, creating**, 417
- RBAC Admin role (Cisco ISE)**, 156
- Reauth CoA**, 480
- registering**
  - devices for BYOD, 570
  - nodes to ISE cube, 703-705
  - for SISAS 300-208 exam, 5-6
  - WebAuth devices, 363-368
- REJECT message (TACACS+)**, 25
- remediation**
  - NAC support for, 651
  - posture service, 661
- remote access VPN example, authentication policies**, 251-252

REPLY packets (TACACS+), 25  
 Reports subcomponent (Cisco ISE), 169  
 REQUEST message (TACACS+), 26-27  
 RESPONSE message (TACACS+), 26-27  
 responses to authentication failure, 402  
 restoring authentication policies, 257  
 reusing conditions, 279-281  
 revocation  
     OCSP, 49-50  
     verifying for certificates, 502-503  
     X.509 certificates, 48-49  
 role-specific authorization rules, 271  
 rules  
     802.1X authentication rule, 401  
     for authentication policies, 240  
         *conditions*, 241-243  
         *options*, 247  
     for authorization policies, 266-279  
         *examples*, 272-279  
         *role-specific authorization rules*,  
         271

## S

sample switch configurations  
     Catalyst 2960/3560/3750 Series,  
         12.2(55)SE, 845-848  
     Catalyst 3560/3750 Series, 15.0(2)SE,  
         848-852  
     Catalyst 4500 Series, IOS-XE  
         3.3.0/15.1(1)SG, 852-856  
     Catalyst 6500 Series, 12.2(33)SXJ,  
         856-858  
 saving conditions for reuse, 279-281  
 screen elements, guest user portal,  
     386-389  
 security certifications, comparing, 6  
 Security Group Access subcomponent  
     (Cisco ISE), 176  
 selecting EAP type, 62  
 self-signed certificates, 206  
 Server Information pop-up  
     (Administration Home page), 162  
 service types, 29  
 services (Cisco ISE), 138-139  
     posture service, 648  
         *assessment options*, 652-654  
         *authorization policy for*  
         *compliance, modifying*,  
         666-667  
         *authorization policy for CPP*,  
         *modifying*, 663-665  
         *building blocks*, 658-659  
         CoA, 654-655  
         *conditions*, 659-660  
         *configuring*, 655-674  
         CPP, 657  
         *functional components*, 648  
         NAC agent types, 650-651  
         *posture conditions*, 652-654  
         *remediation*, 661  
         *requirement function*, 662-663  
         *verifying*, 667-674  
 Setup Assistant link (Administration  
     Home page), 163  
 SGA (security group access), 193-194.  
     *See also* TrustSec  
     enforcement, 628-632  
     native tagging, 621-628  
     SGTs, 606-613  
     SXP, 613-621  
 SGACLs (Security Group ACLs),  
     629-632  
 SGTs (security group tags), 606-613  
     native tagging, 621-628  
 show aaa servers command, 329-330  
 show authentication session command,  
     331-332

- show authentication session interface command**, 753-754
- show authentication sessions interface command**, 668
- show device-sensor cache all command**, 491
- show monitor command**, 460
- signing of certificates, verifying**, 499-500
- single-node deployment (Cisco ISE)**, 133-135
- SISAS 300-208 exam**
  - answering questions, 765-766
  - exam-day advice, 762-763
  - format of exam, 9-10
  - knowledge gaps, identifying, 767-769
  - practice exams, 763-767
  - pre-exam suggestions, 762
  - preparing for, 759, 769-770
    - Cisco Certification Exam Tutorial*, 759-760
    - features of this book*, 13-14
  - registering for, 5-6
  - time management, 760-762
  - topics covered, 4-5
- smart cards**, 45-46
- SNMP probes**, 455-456
- soft tokens**, 44
- sponsor groups**
  - configuring, 394-396
  - mapping, 396-397
- sponsor portal**, 385
  - configuring, 392-393
  - guest accounts, provisioning, 416
  - guest user types, 398
  - sponsor groups
    - configuring*, 394-396
    - mapping*, 396-397
  - types of sponsors, 393-396
- SponsorAllAccounts group**, 394
- SponsorGroupGrpAccounts group**, 394
- SponsorGroupOwnAccounts group**, 394
- SSL (Secure Sockets Layer)**, 42
- standalone AnyConnect Profile Editor**, configuring Cisco AnyConnect NAM supplicant, 75-88
  - Authentication Policy view, 78
  - Client Policy view, 76-78
  - Network Groups view, 87
  - Networks view, 79-86
- START packets (TACACS+)**, 25
- Super Admin role (Cisco ISE)**, 156
- supplicants**, 56, 63-89
  - Cisco AnyConnect NAM supplicant, 75-88
    - AnyConnect NAM profiles, implementing*, 87-88
    - AnyConnect Profile Editor views*, 76-87
    - EAP chaining*, 89
  - devices without supplicants, managing, 97-98
    - MAB*, 98-100, 113-117
    - MAC addresses*, 115-116
    - WebAuth*, 100-106
  - supplicant provisioning logs, 753
  - Windows native supplicant, 64-72
    - hotfixes*, 752
- support bundles**, 734
- switches**
  - authentication, verifying, 329-334
  - guest access, verifying, 428-438
  - wired switches, configuring authentication
    - ACL, applying*, 305-306
    - creating local ACLs*, 297-298

*Flex-Auth*, 299-302  
*global 802.1X commands*, 297  
*global configuration AAA commands*, 293-294  
*global configuration RADIUS commands*, 294-297  
*HA*, 299-302  
*host mode of switchport, setting*, 302-303  
*settings*, 303-305  
*switchports*, 299  
*timers*, 305

## switchports

configuring on wired switches, 299  
 host mode, setting, 302-303

SXP (Security Group Exchange Protocol), 613-621

syslog, 332-334

System Admin role (Cisco ISE), 156

System subcomponent (Cisco ISE), 178-182

System Summary dashlet (Administration Dashboard), 162

# T

TACACS (Terminal Access Controller Access Control System), 22

TACACS+ (Terminal Access Controller Access Control System Plus), 23-27

authentication messages, 25

authorization and accounting messages, 26-27

comparing to RADIUS, 32

TCP Dump, 741-746

test aaa command, 330-331

time management, SISAS 300-208 exam, 760-762

timers, configuring on wired switches, 305

topics covered in SISAS exam, 4-5, 10-13

transitioning from Monitor Mode to end state, 695

Triple-A, 21

Troubleshoot subcomponent (Cisco ISE), 171-172

## troubleshooting tools

AnyConnect Diagnostics and Reporting tool, 748-750

diagnostic tools, 735-747

*collection filters*, 746-747

*Evaluate Configuration Validator*, 735-739

*RADIUS Authentication*

*Troubleshooting tool*, 739-740

*TCP Dump*, 741-746

## logging

*categories*, 730

*debug logs*, 731-732

*extended logging*, 751

*Live Authentication Log*, 726-728

*Live Sessions Log*, 728

*support bundles*, 734

*targets*, 729-730

trusted-level access, Cisco ISE, 128

TrustSec, 605-632

enforcement, 628-632

native tagging, 621-628

SGTs, 606-613

SXP, 613-621

tunneled EAP types, 59-61

two-factor authentication, 43-44

two-node deployment (Cisco ISE), 135-136

types of sponsors, 393-396

## U

---

### Uplink MACSec, 638-640

#### user accounts

- guest accounts, 416
- importing, 418
- individual accounts, creating, 416
- local users, 220
- random user accounts, creating, 417

#### user authentication, 72-73

## V

---

### VACLs (VLAN access control lists), 461-462

#### validity dates for certificates, 47-48

- verifying, 501

#### vendors of MDMs, 119

#### verifying

- authentication
  - on Cisco switches, 329-334*
  - on WLCs, 334-336*
- BYOD onboarding flows, 581-582
- certificate authentication, 516-519
- CWA, 369-375
- guest access
  - on the switch, 428-438*
  - on WLC, 419-427*
- posturing, 667-674
- profiling, 486-491
  - dashboard, 486-487*
  - Endpoints Drill-down tool, 487-488*
  - Global Search tool, 488*
- proof of possession for certificates, 504-505
- revocation of certificates, 502-503

- signing of certificates, 499-500
- validity dates of certificates, 501

#### viewing

- Live Authentication Log, 336-337
- Live Sessions Log, 337
- log files from CLI, 733-734
- WLC client details, 754

#### views (AnyConnect Profile Editor)

- Authentication Policy view, 78
- Client Policy view, 77
- Network Groups view, 87
- Networks view, 79-86

#### virtual appliance specifications (Cisco ISE), 132

#### VLAN assignment, controlling access to networks, 601-603

#### VMware, permitting promiscuous traffic, 463-464

#### VPNs (virtual private networks), RA, 106

## W

---

#### web authentication redirection ACLs, creating, 310-313

#### web browsers. *See also* GUI (Cisco ISE)

- Cisco ISE support for, 150
- pseudo-browsers, 355

#### Web Portal Management subcomponent (Cisco ISE), 189-190

#### web portals

- customizing, 399-400
- Friendly Names, configuring, 391-392
- guest user portal, screen elements, 386-389
- interfaces, configuring, 391
- ports, configuring, 389-390

## sponsor portal

- configuring*, 392-393
- guest accounts, provisioning*, 416
- guest user types*, 398
- sponsor groups, configuring*, 394-396
- sponsor groups, mapping*, 396-397
- sponsor types*, 393-396

**WebAuth, 100-106, 340-341**

- CWA, 104-106, 346-349
  - authorization policies, building*, 360-362
  - configuring*, 350-359
  - verifying*, 369-375
- device registration, configuring, 363-368

## DRW, 349

- guest accounts, provisioning, 416
- guest authorization, configuring, 400-415
- guest user portal, screen elements, 386-389

## individual accounts, creating, 416

## LWA, 101-102, 346

- with centralized portal*, 102-104

## portals, 384-389

- configuring*, 389-390
- customizing*, 399-400

## random user accounts, creating, 417

## web portals

- configuring*, 391-392

## web portals, configuring, 391

**Windows device onboarding flow, 577-580****Windows native supplicant**

- configuring, 64-72
- hotfixes, 752

**Wired AutoConfig, 64****wired switches, configuring authentication**

- ACL, applying, 305-306
- creating local ACLs, 297-298
- Flex-Auth, 299-302
- global 802.1X commands, 297
- global configuration AAA commands, 293-294
- global configuration RADIUS commands, 294-297
- HA, 299-302
- settings, 303-305
- switchports, 299
- timers, 305

**Wireless license package (Cisco ISE), 178****wireless networks**

- phased deployment approach, 695
- WLCs, configuring authentication, 306-328
  - ACLs, applying*, 310
  - corporate SSID, creating*, 324-328
  - dynamic interfaces for client VLAN, creating*, 315
  - guest dynamic interface, creating*, 317
  - guest WLAN, creating*, 319-323
  - posture agent redirection ACL, creating*, 313-314
  - RADIUS accounting servers, adding*, 308-309
  - RADIUS authentication servers, adding*, 306-308
  - RADIUS fallback*, 309-310
  - web authentication redirection ACL, creating*, 310-313

**wireless SSID example, authentication policies, 248-251**

**Wireless Upgrade license package  
(Cisco ISE), 178**

**WLANs (wireless LANs), creating guest  
WLAN, 319-323**

**WLCs (Wireless LAN Controllers)**

authentication, configuring, 306-328

*ACLs, applying, 310*

*corporate SSID, creating, 324-328*

*dynamic interfaces for client*

*VLAN, creating, 315*

*guest dynamic interface, creating,  
317*

*guest WLAN, creating, 319-323*

*posture agent redirection ACL,  
creating, 313-314*

*RADIUS accounting servers,  
adding, 308-309*

*RADIUS authentication servers,  
adding, 306-308*

*RADIUS fallback, 309-310*

*verifying authentication, 334-336*

*web authentication redirection  
ACL, creating, 310-313*

client details, viewing, 754

debug commands, 336

guest access, verifying, 419-427

**Woland, Aaron, 523**

## **X-Y-Z**

---

**X.509 certificates, 46**

revocation, 48-49

validity dates, 47-48

**yum**

installing Fedora packages, 825

updating system packages, 826

*This page intentionally left blank*



# ciscopress.com: Your Cisco Certification and Networking Learning Resource

Subscribe to the monthly Cisco Press newsletter to be the first to learn about new releases and special promotions.

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

While you are visiting, check out the offerings available at your finger tips.

—Free Podcasts from experts:

- OnNetworking
- OnCertification
- OnSecurity



View them at [ciscopress.com/podcasts](http://ciscopress.com/podcasts).

—Read the latest author **articles** and **sample chapters** at [ciscopress.com/articles](http://ciscopress.com/articles).

—Bookmark the Certification Reference Guide available through our partner site at [informit.com/certguide](http://informit.com/certguide).

Connect with Cisco Press authors and editors via Facebook and Twitter, visit [informit.com/socialconnect](http://informit.com/socialconnect).



## PEARSON IT CERTIFICATION

Browse by Exams ▼

Browse by Technology ▼

Browse by Format

Explore ▼

I'm New Here - Help!

Store

Forums

Safari Books Online

## Pearson IT Certification

THE LEADER IN IT CERTIFICATION LEARNING TOOLS

Visit [pearsonITcertification.com](http://pearsonITcertification.com) today to find:

- IT CERTIFICATION EXAM information and guidance for



CompTIA

Microsoft

vmware

Pearson is the official publisher of Cisco Press, IBM Press, VMware Press and is a Platinum CompTIA Publishing Partner—CompTIA's highest partnership accreditation

- EXAM TIPS AND TRICKS from Pearson IT Certification's expert authors and industry experts, such as

- *Mark Edward Soper* – CompTIA
- *David Prowse* – CompTIA
- *Wendell Odom* – Cisco
- *Kevin Wallace* – Cisco and CompTIA
- *Shon Harris* – Security
- *Thomas Erl* – SOACP



- SPECIAL OFFERS – [pearsonITcertification.com/promotions](http://pearsonITcertification.com/promotions)
- REGISTER your Pearson IT Certification products to access additional online material and receive a coupon to be used on your next purchase

Articles &amp; Chapters



Blogs



Books



Cert Flash Cards Online



eBooks



Mobile Apps



Newsletters



Podcasts



Question of the Day



Rough Cuts



Short Cuts



Software Downloads



Videos



## CONNECT WITH PEARSON IT CERTIFICATION

Be sure to create an account on [pearsonITcertification.com](http://pearsonITcertification.com) and receive members-only offers and benefits

