Video Training

Review Exercises

Official Cert Guide

Advance your IT career with hands-on learning

CCNP Security Identity Management

SISE 300-715

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

ciscopress.com

FREE SAMPLE CHAPTER

SHARE WITH OTHERS

CCNP Security Identity Management

SISE 300-715

Official Cert Guide

Enhance Your Exam Preparation

CCNP Security Identity Management

SISE 300-715

Official Cert Guide

AARON WOLAND, CCIE No. 20113

KATHERINE MCNAMARA, CCIE No. 50931

Cisco Press

CCNP Security Identity Management SISE 300-715 Official Cert Guide

Aaron Woland

Katherine McNamara

Published by:
Cisco Press

ScoutAutomatedPrintCode

Library of Congress Control Number: 2020913602

ISBN-10: 0-13-664294-2

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

Warning and Disclaimer

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

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

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

Trademark Acknowledgments

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

Special Sales

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

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

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Feedback Information

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

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

We greatly appreciate your assistance.

Editor-in-Chief: Mark Taub

Alliances Manager, Cisco Press: Arezou Gol

Director, ITP Product Management: Brett Bartow

Executive Editor: James Manly

Managing Editor: Sandra Schroeder

Development Editor: Christopher A. Cleveland

Project Editor: Mandie Frank

Copy Editor: Kitty Wilson

Technical Editor: Akhil Behl

Editorial Assistant: Cindy Teeters

Designer: Chuti Prasertsith

Composition: codeMantra

Indexer: Erika Millen

Proofreader: Donna Mulder

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

Credits

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

Contents at a Glance

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

Contents

About the Authors

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

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

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

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

You can follow Aaron on Twitter: @aaronwoland.

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

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

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

You can follow Katherine on Twitter: @kmcnam1

About the Technical Reviewer

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

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

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

Dedications

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

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

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

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

—Aaron

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

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

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

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

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

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

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

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

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

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

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

Acknowledgments

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

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

From Aaron and Katherine:

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

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

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

Command Syntax Conventions

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

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

Introduction

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

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

CCNP Security Certification Overview

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

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

Table I-1 CCNP Security Concentration Exams

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

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

Contents of the CCNP Security SISE Exam

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

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

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

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

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

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

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

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

Table 1-3 Additional Training Resources

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

How to Take the SISE Exam

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

Who Should Take This Exam and Read This Book?

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

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

Table I-4 Security Certification Comparison Chart

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

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

Format of the CCNP Security SISE Exam

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

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

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

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

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

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

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

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

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

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

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

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

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

CCNP Security SISE 300-715 Official Certification Guide

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Objectives and Methods

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

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

Book Features

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

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

The Companion Website for Online Content Review

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

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

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

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

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

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

How to Access the Pearson Test Prep (PTP) App

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

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

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

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

Step 1. Open this book's companion website, as was shown earlier in this Introduction under the heading "How to Access the Companion Website."

Step 2. Click the **Practice Exams** button.

Step 3. Follow the instructions listed there both for installing the desktop app and for using the web app.

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

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

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

Customizing Your Exams

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

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

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

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

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

Updating Your Exams

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

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

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

This page intentionally left blank

CHAPTER 12

Web Authentication

This chapter covers the following topics:

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

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

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

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

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

"Do I Know This Already?" Quiz

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

Table 12-1 "Do I Know This Already?" Section-to-Question Mapping

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

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

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

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

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

Foundation Topics

Web Authentication Scenarios

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

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

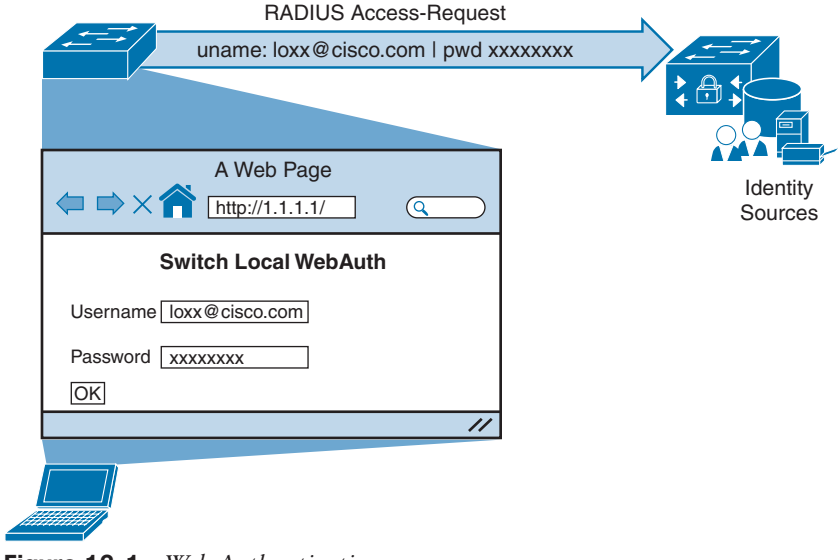

Figure 12-1 *Web Authentication*

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

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

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

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

Local Web Authentication (LWA)

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

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

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

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

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

- Device registration
- BYOD onboarding

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

NOTE For more details on LWA, see Chapter 4.

Centralized Web Authentication (CWA)

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

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

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

CWA also supports advanced services such as the following:

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

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

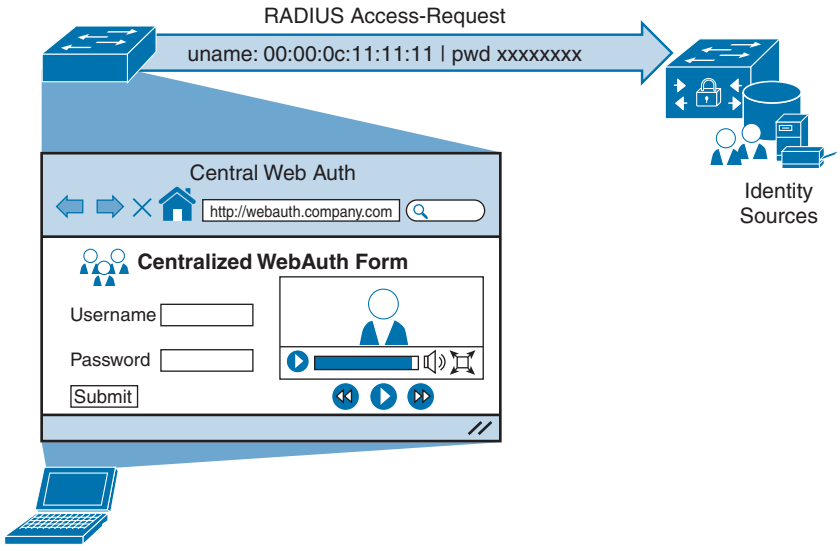

Figure 12-2 *URL-Redirected MAC Authentication Bypass*

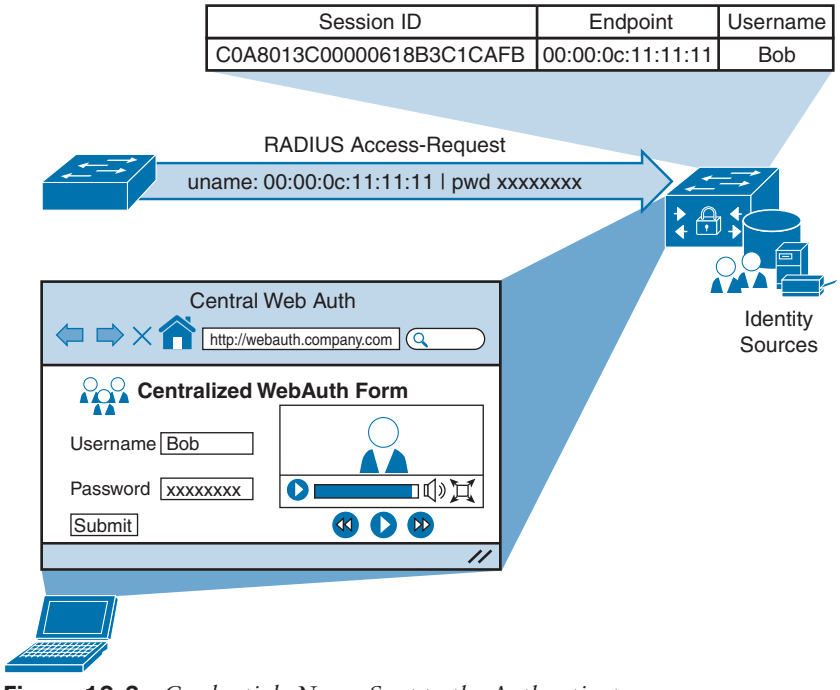

Figure 12-3 *Credentials Never Sent to the Authenticator*

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

Step 1. The endpoint entering the network does not have a supplicant.

Step 2. The authenticator performs MAB, sending the RADIUS Access-Request to Cisco ISE (the authentication server).

Step 3. The authentication server (ISE) sends the RADIUS result, including a URL redirection, to the centralized portal on the ISE server.

Step 4. The end user enters credentials into the centralized portal. Unlike the LWA options, the credentials are never sent to the switch; instead, they are stored within the ISE session directory and tied together with the MAB coming from the switch.

Step 5. ISE sends a reauthentication Change of Authorization (CoA-reauth) to the switch. This causes the switch to send a new MAB request with the same SessionID to ISE, and it is processed.

Step 6. ISE sends the final authorization result to the switch for the end user.

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

Configuring Centralized Web Authentication

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

Cisco Switch Configuration

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

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

Configure Certificates on the Switch

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

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

Step 1. To set the DNS domain name on the switch, type **ip domain-name** *domain-name* at the global configuration prompt. Now that the domain name is configured, and the keys can be generated.

Step 2. To generate keys to be used for HTTPS, type **crypto key generate rsa general-keys mod 2048** at the global configuration prompt.

Enable the Switch HTTP/HTTPS Server

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

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

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

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

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

Key Topic

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

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

Verify the URL-Redirect ACL

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

Key Topic

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

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

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

```
C3850# show ip access-list ACL-WEBAUTH-REDIRECT
Extended IP access list ACL-WEBAUTH-REDIRECT
 10 deny udp any any eq domain
 20 permit tcp any any eq www
 30 permit tcp any any eq 443
```

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

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

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

Cisco WLC Configuration

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

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

Validate That MAC Filtering Is Enabled on the WLAN

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

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

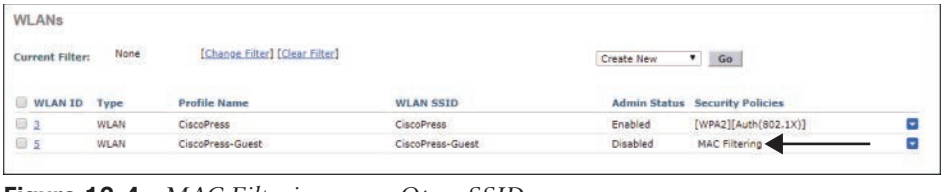

Figure 12-4 *MAC Filtering on an Open SSID*

Validate That ISE NAC Is Enabled on the WLAN

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

From the WLC GUI, follow these steps:

Step 1. Navigate to **WLANs >** and select your open SSID.

Step 2. Click on the **Advanced** tab.

Step 3. Ensure that NAC State is forest to **ISE NAC**, as shown in Figure 12-5. In the same screen, ensure that Allow AAA Override is set to **Enabled**.

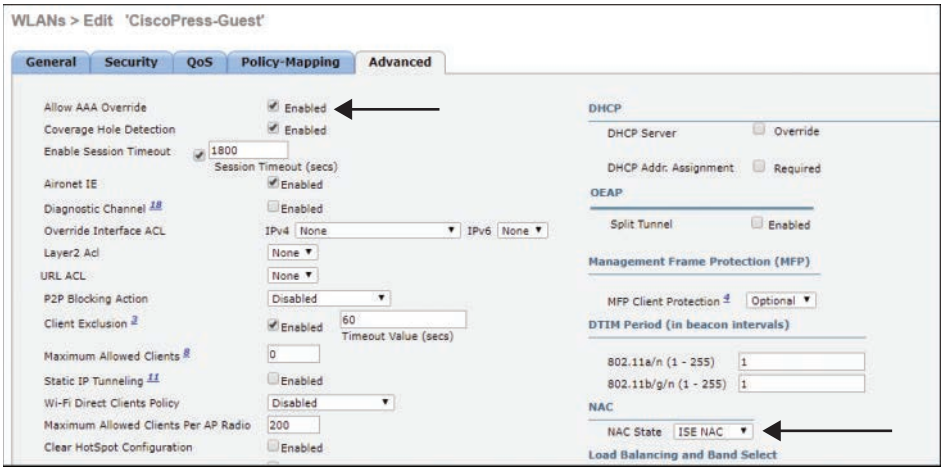

Figure 12-5 *ISE NAC Setting*

Validate That the URL-Redirection ACL Is Configured

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

Key Topic

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

In the WLC GUI, follow these steps:

Step 1. Navigate to **Security > Access-Control-Lists > Access-Control Lists**. Ensure that the ACL-WEBAUTH-REDIRECT ACL is in the list, as shown in Figure 12-6.

Step 2. Click this access list and ensure that the entries for your environment are there, as shown in Figure 12-7.

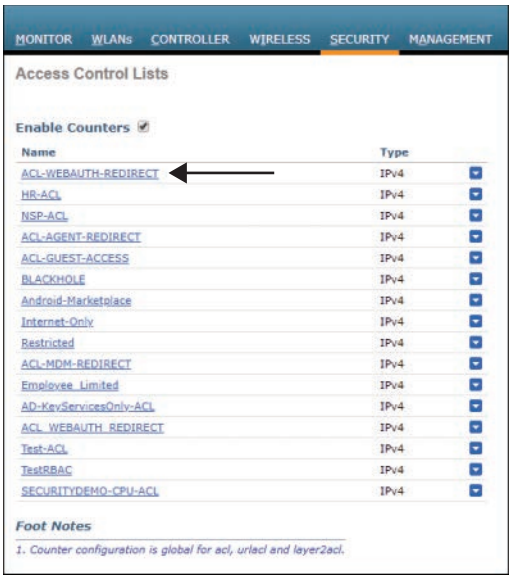

Figure 12-6 *Access Control Lists*

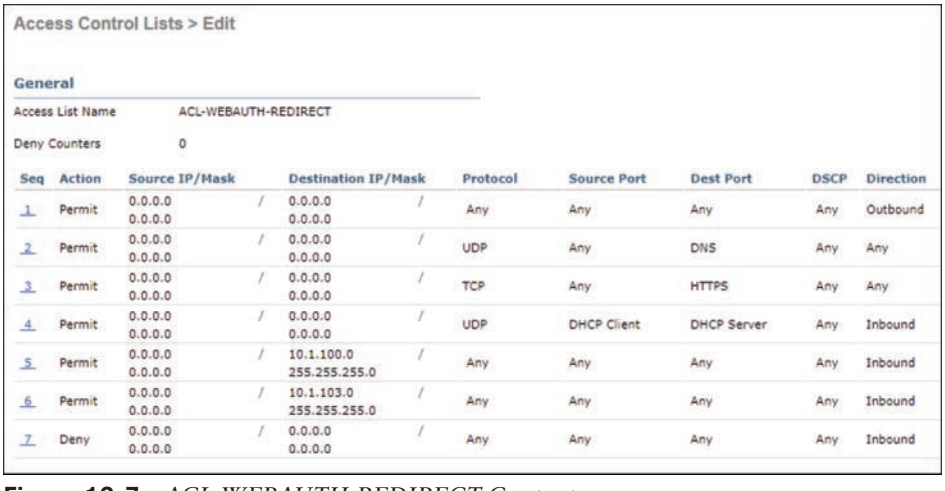

Figure 12-7 *ACL-WEBAUTH-REDIRECT Contents*

Configure ISE for Centralized Web Authentication

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

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

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

Step 1. Configure MAB Continue for the Authentication.

Step 2. Verify the Web Authentication identity source sequence.

Step 3. Configure a dACL for pre-WebAuth authorization.

Step 4. Configure an authorization profile.

Configure MAB Continue for the Authentication

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

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

Step 1. Navigate to **Work Centers > Network Access > Policy Sets**.

Step 2. Select the **Default** policy set.

Step 3. Expand the **Authentication Policy** section.

Step 4. In the MAB rule, click **Options** underneath Internal Endpoints.

Step 5. Ensure that If User Not Found is set to **CONTINUE**.

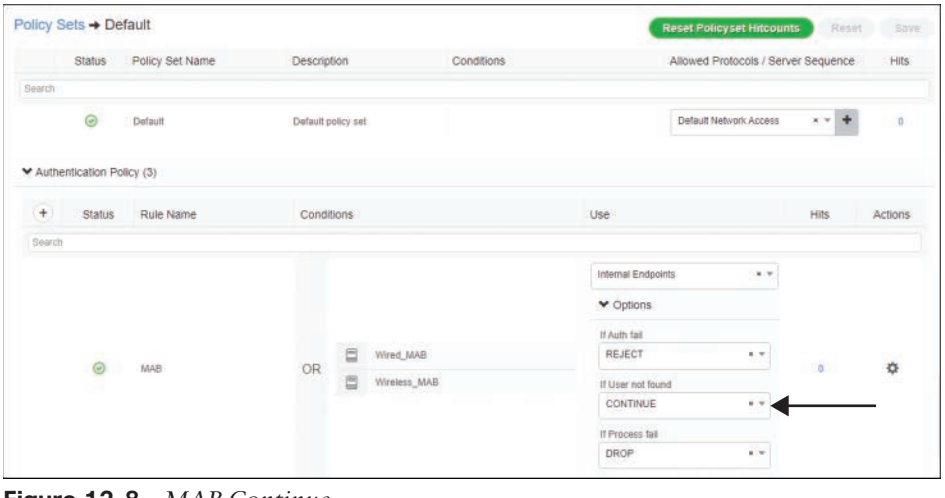

Figure 12-8 *MAB Continue*

Verify the Web Authentication Identity Source Sequence

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

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

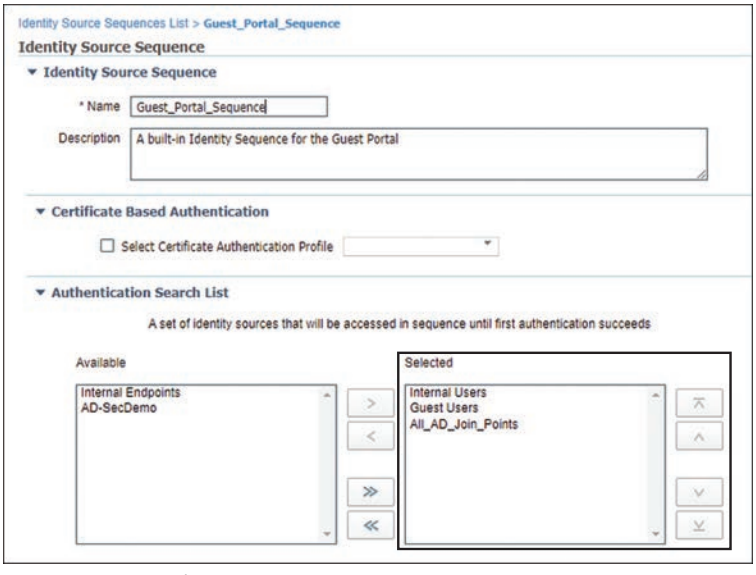

Figure 12-9 *Identity Source Sequences*

Configure a dACL for Pre-WebAuth Authorization

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

In the ISE GUI, follow these steps:

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

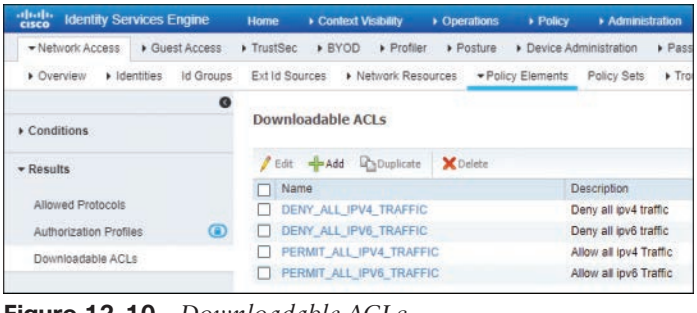

Figure 12-10 *Downloadable ACLs*

Step 2. Click **Add**.

Step 3. Name the new dACL **WebAuth**.

Step 4. Add a description.

Step 5. Configure the ACL to permit traffic to the ISE policy service nodes but deny access to the remainder of the internal network. Figure 12-11 shows what this might look like.

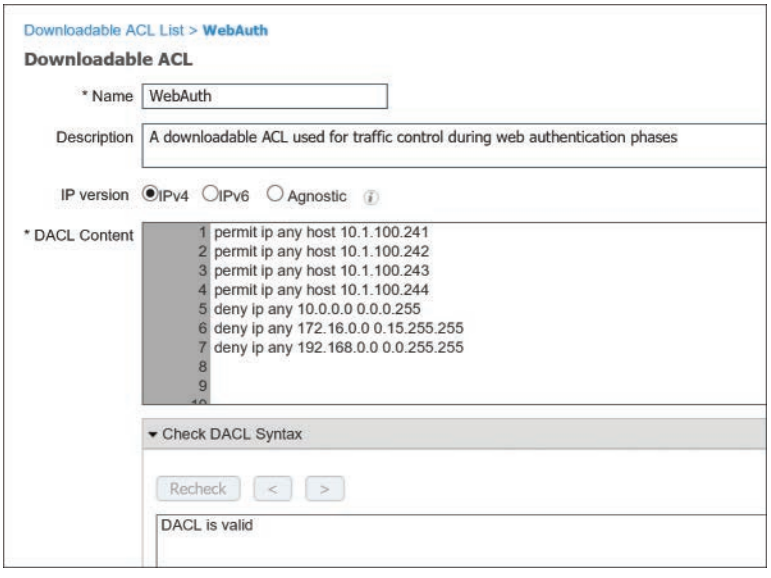

Figure 12-11 *Sample WebAuth dACL*

Step 6. Click **Submit**.

Configure an Authorization Profile

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

In the ISE GUI, follow these steps:

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

Step 2. Click **Add**.

Step 3. Name the new Authorization Profile **CWA**.

Step 4. Select the **WebAuth** dACL.

Step 5. Select the **Web Redirection** checkbox and choose **Centralized Web Auth** from the first dropdown. In the ACL text box, type **ACL-WEBAUTH-REDIRECT**. You are using a default WebAuth portal, so ensure that **Sponsored Guest Portal (default)** is selected from the Value dropdown.

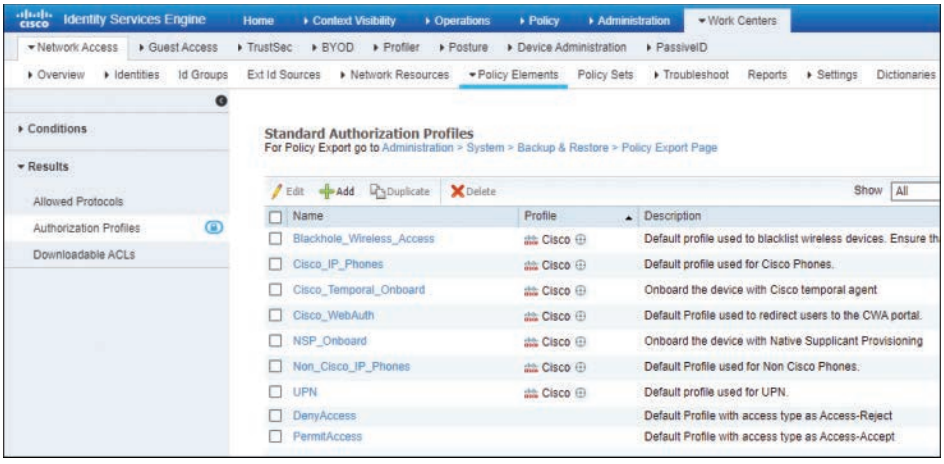

Figure 12-12 *Downloadable ACLs*

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

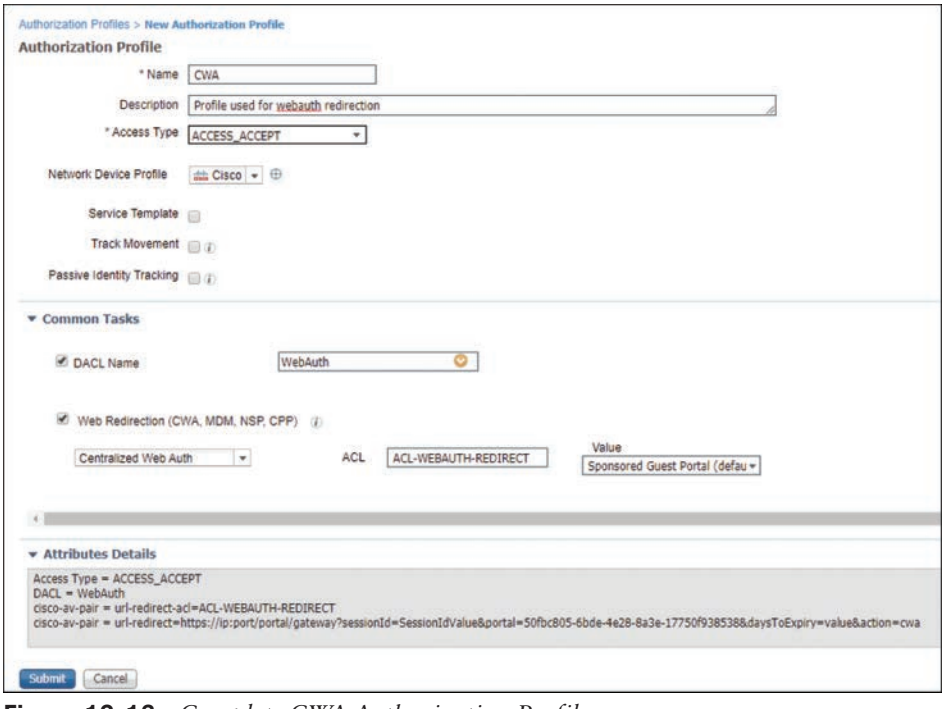

Figure 12-13 *Complete CWA Authorization Profile*

Key Topic

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

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

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

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

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

Building CWA Authorization Policies

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

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

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

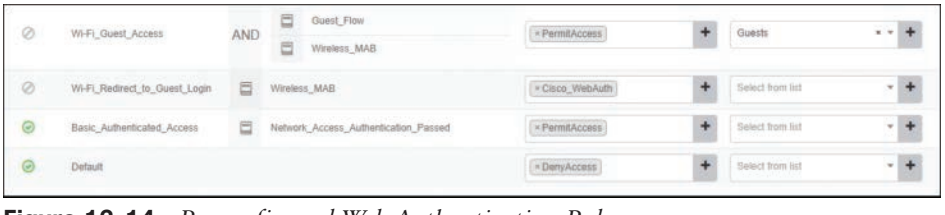

Figure 12-14 *Preconfigured Web Authentication Rules*

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

Create the Rule to Redirect Users to the CWA Portal

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

In the ISE GUI, follow these steps:

Step 1. Navigate to **Work Centers > Network Access > Policy Sets**.

Step 2. Drill down into your default policy set (or the policy set that is in use for your deployment at this time).

Step 3. Insert a new rule above the Basic_Authenticated_Access rule and name the new rule **WebAuth**, as shown in Figure 12-15.

Step 4. For the conditions, select two existing compound conditions from the library: **Wired_MAB** and **Wireless_MAB**. Ensure that the **OR** operator is used with the conditions, as shown in Figure 12-15.

Step 5. Use the **CWA** authorization profile you created previously for the result, as shown in Figure 12-15.

Step 6. Click **Save**.

Figure 12-15 shows the completed WebAuth authorization rule.

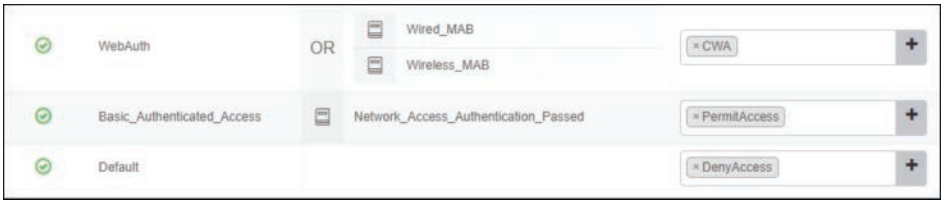

Figure 12-15 *Completed WebAuth Authorization Rule*

Create the Rules to Authorize Users Who Authenticate via CWA

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

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

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

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

In the ISE GUI, follow these steps:

Step 1. Navigate to **Work Centers > Network Access > Policy Sets**.

Step 2. Drill down into your default policy set (or the policy set that is in use for your deployment at this time).

Step 3. Insert a new rule above the WebAuth rule and name it **Employee CWA**.

Step 4. Use **GuestFlow** as the first condition for the rule.

Step 5. Add another condition with the **AND** operator.

Step 6. Select the Active Directory group named **Employees** as the second condition.

Step 7. Use the previously created authorization profile named **Internet-Only**.

Step 8. Select the **Employees** security group tag.

Step 9. Click **Save**.

Figure 12-16 shows the completed Employee_CWA rule.

Figure 12-16 *Completed Employee_CWA Rule*

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

Verifying Centralized Web Authentication

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

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

Check the Experience from the Client

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

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

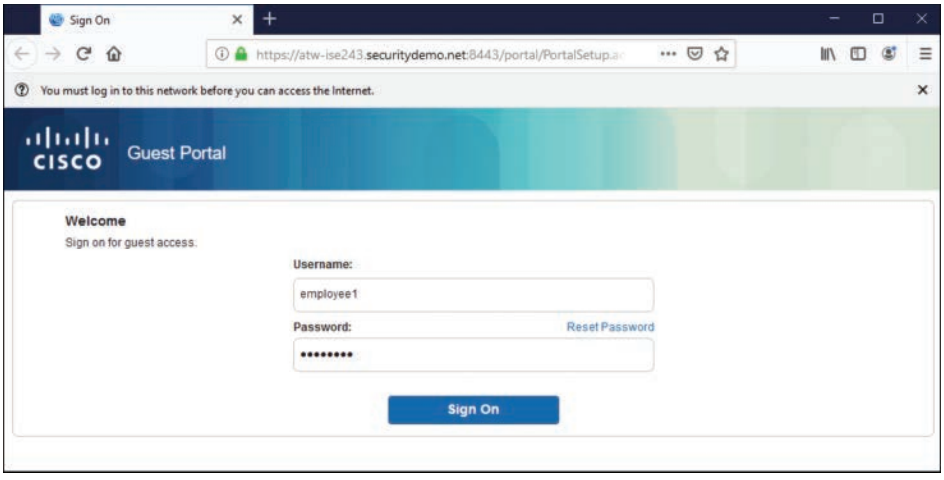

Figure 12-17 *Browser Redirected to the CWA Portal*

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

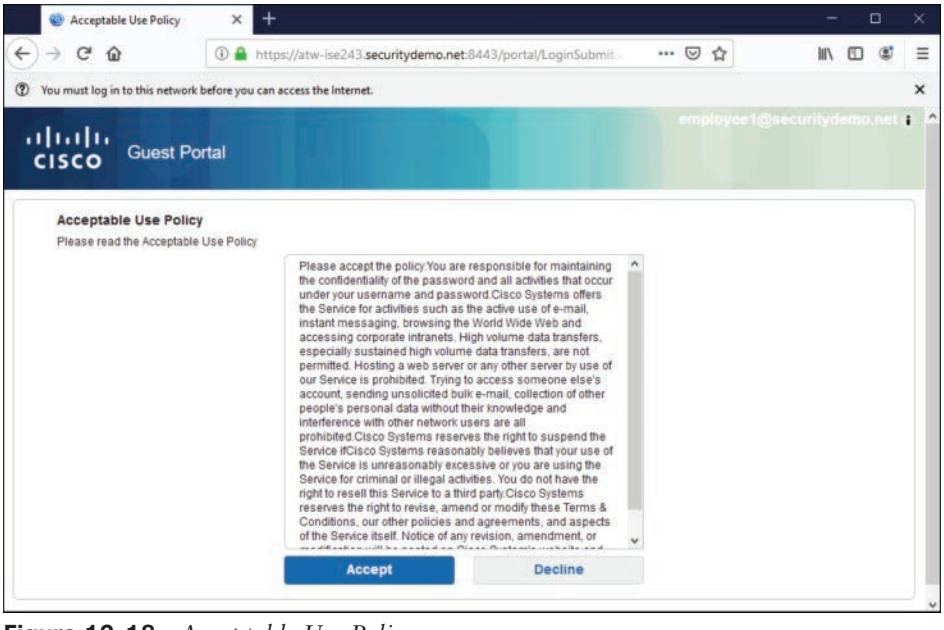

Figure 12-18 *Acceptable Use Policy*

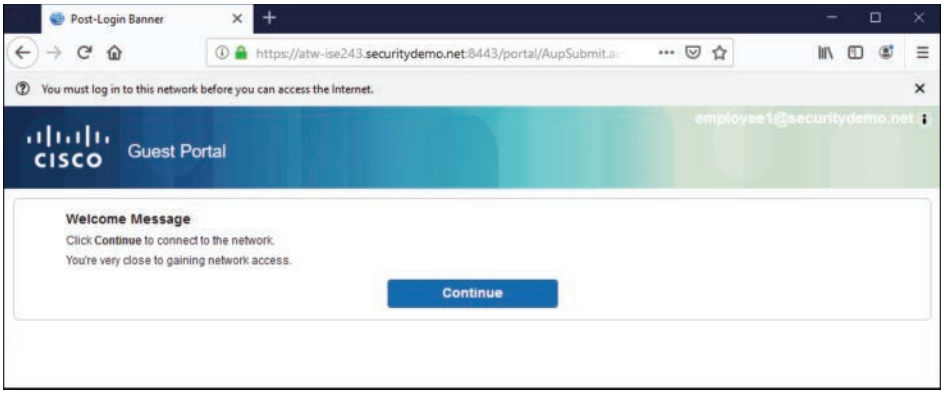

Figure 12-19 *Browser Redirected to the CWA Portal*

Figure 12-20 *Success*

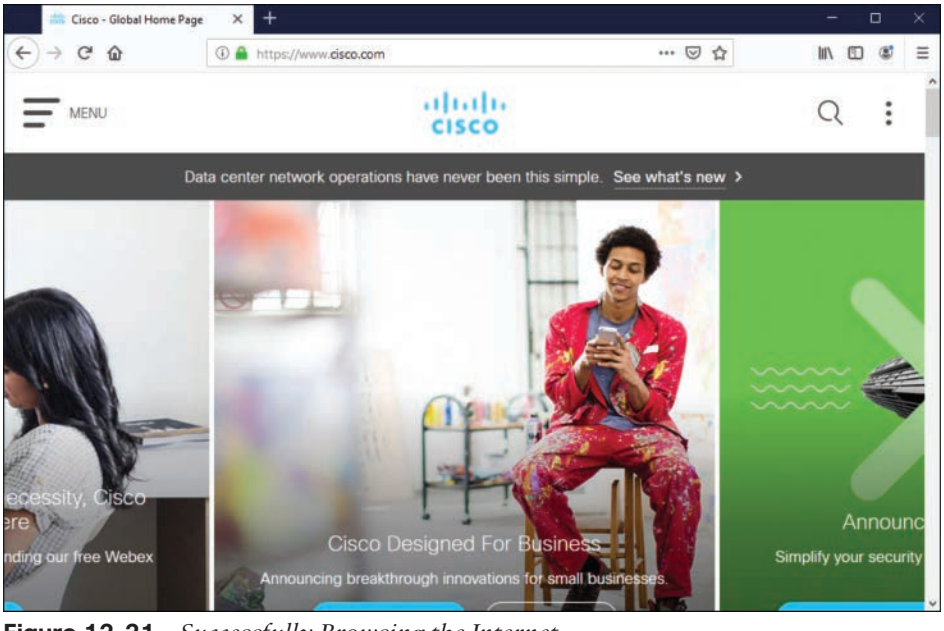

Figure 12-21 *Successfully Browsing the Internet*

Verify CWA Through the ISE UI

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

Check Live Log

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

Key Topic

Figure 12-22 highlights the process.

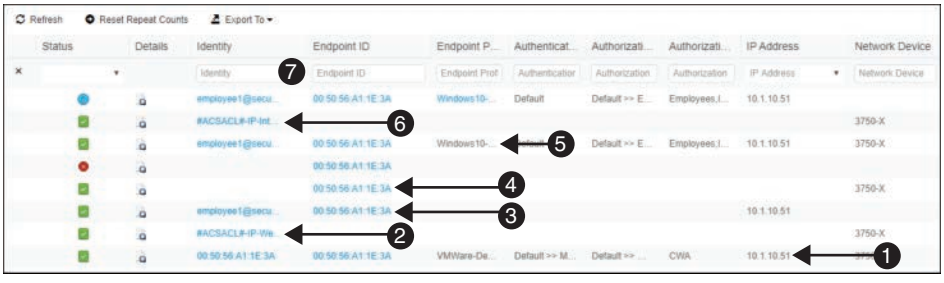

Figure 12-22 *Live Log*

The following points correspond to the numbers in the figure:

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

Check the NAD

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

show Commands on the Wired Switch

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

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

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

```
3750-X#show authen sessions int g1/0/1
            Interface:  GigabitEthernet1/0/1
          MAC Address:  0050.56a1.1e3a
           IP Address:  10.1.10.51
            User-Name:  00-50-56-A1-1E-3A
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
              ACS ACL:  xACSACLx-IP-WebAuth-5e2a155e
     URL Redirect ACL:  ACL-WEBAUTH-REDIRECT
         URL Redirect:  https://atw-ise243.securitydemo.net:8443/portal/
gateway?sessionId=C0A8FE0100000271FEF432A8&portal=50fbc805-6bde-4e28-8a3e-17750f9385
38&action=cwa&token=b296cdf51b7985efc8adace571ce4c29
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A8FE0100000271FEF432A8
      Acct Session ID:  0x000003AE
               Handle:  0xBF000272

Runnable methods list:

       Method   State
       mab      Authc Success
       dot1x    Not run
```

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

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

```
3750-X#show authen sessions int g1/0/1
            Interface:  GigabitEthernet1/0/1
          MAC Address:  0050.56a1.1e3a
           IP Address:  10.1.10.51
            User-Name:  employee1@securitydemo.net
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
              ACS ACL:  xACSACLx-IP-Internet_Only-5e606c90
                  SGT:  0004-00
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A8FE0100000271FEF432A8
      Acct Session ID:  0x000003AE
               Handle:  0xBF000272

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

Key Topic

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

Viewing the Client Details on the WLC

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

Key Topic

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

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

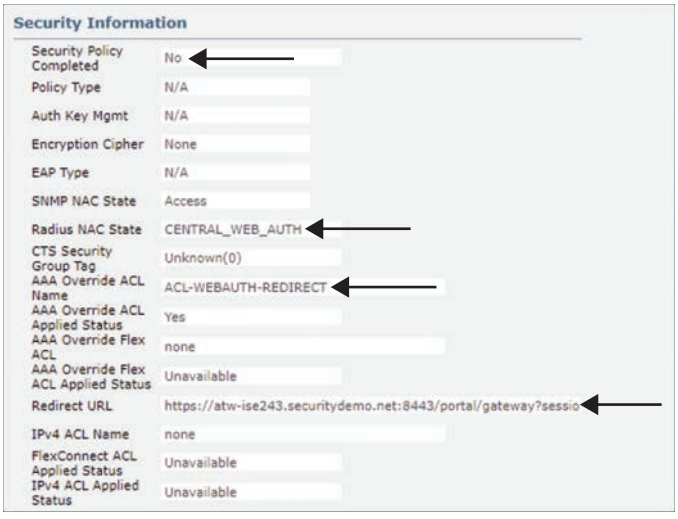

Figure 12-23 *Security Information Section of Client Details – CWA*

Figure 12-23 highlights the important sections:

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

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

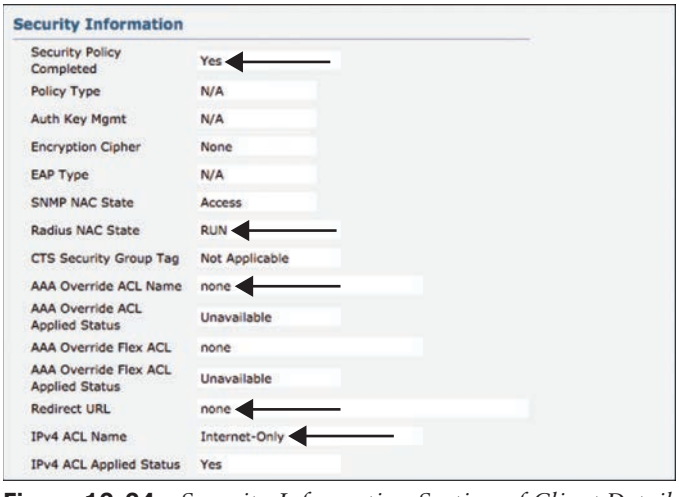

Figure 12-24 *Security Information Section of Client Details – Run State*

Figure 12-24 highlights the important sections:

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

Exam Preparation Tasks

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

Review All Key Topics

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

Key Topic

Table 12-2 Key Topics

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

Define Key Terms

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

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

Q&A

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

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

Index

SYMBOLS

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y-Z

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

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

To access the companion website, simply follow these steps:

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

If you have any issues accessing the companion website, you can contact our support team by going to **pearsonitp.echelp.org.**