NIST SPECIAL PUBLICATION 1800-35D

Implementing a Zero Trust Architecture

Volume D:

Functional Demonstrations

Oliver Borchert Alper Kerman **Scott Rose Murugiah Souppaya** National Institute of Standards and Technology

Gaithersburg, MD

Jason Ajmo Yemi Fashina Parisa Graveli **Joseph Hunt Jason Hurlburt** Nedu Irrechukwu Joshua Klosterman **Oksana Slivina Susan Symington Allen Tan** The MITRE Corporation McLean, VA

Peter Gallagher Aaron Palermo Appgate Coral Gables, FL

Adam Cerini Conrad Fernandes AWS (Amazon Web Services) Arlington, VA

Kyle Black Sunjeet Randhawa Broadcom Software San Jose, CA

Corey Lund Ivanti

December 2022

SECOND PRELIMINARY DRAFT

This publication is available free of charge from https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture

Aaron Rodriguez Micah Wilson Cisco Lookout Herndon, VA

Corey Bonnell Dean Coclin DiaiCert Lehi, UT

Ryan Johnson Dung Lam Seattle, WA

Neal Lucier Tom May Forescout San Jose, CA

Tim Knudsen Google Cloud Mill Valley, CA

Harmeet Singh Krishna Yellepeddy Armonk, NY

Farhan Saifudin South Jordan, UT

Hashim Khan Tim LeMaster Reston, VA

James Elliott **David Pricer** Mandiant Reston, VA

Joey Cruz **Carmichael Patton** Microsoft Redmond, WA

Vinu Panicker Okta San Francisco, CA

Andrew Keffalas Norman Wong Palo Alto Networks Santa Clara, CA

Rob Woodworth Shawn Higgins PC Matic Myrtle Beach, SC

Bryan Rosensteel Mitchell Lewars Ping Identity Denver, CO

Wade Ellery Don Coltrain Radiant Logic Novato, CA

Frank Briguglio **Rvan Tighe** SailPoint Austin, TX

Chris Jensen Joshua Moll Tenable Columbia, MD

Jason White Trellix. Public Sector Reston, VA

Jacob Rapp Paul Mancuso VMware Palo Alto, CA

Joe Brown Jim Kovach Zimperium Dallas, TX

Bob Smith Syed Ali Zscaler San Jose, CA



ח	SI	٦.	ΛΙ	M	F	R
		/		IVI	ы	1

1

- 2 Certain commercial entities, equipment, products, or materials may be identified by name or company
- 3 logo or other insignia in order to acknowledge their participation in this collaboration or to describe an
- 4 experimental procedure or concept adequately. Such identification is not intended to imply special
- 5 status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it
- 6 intended to imply that the entities, equipment, products, or materials are necessarily the best available
- 7 for the purpose.
- 8 While NIST and the NCCoE address goals of improving management of cybersecurity and privacy risk
- 9 through outreach and application of standards and best practices, it is the stakeholder's responsibility to
- 10 fully perform a risk assessment to include the current threat, vulnerabilities, likelihood of a compromise,
- and the impact should the threat be realized before adopting cybersecurity measures such as this
- 12 recommendation.
- 13 National Institute of Standards and Technology Special Publication 1800-35D, Natl. Inst. Stand. Technol.
- 14 Spec. Publ. 1800-35D, 123 pages, December 2022, CODEN: NSPUE2

15 **FEEDBACK**

- 16 You can improve this guide by contributing feedback. As you review and adopt this solution for your
- own organization, we ask you and your colleagues to share your experience and advice with us.
- 18 Comments on this publication may be submitted to: nccoe-zta-project@list.nist.gov.
- 19 Public comment period: December 21, 2022 through February 6, 2023
- 20 All comments are subject to release under the Freedom of Information Act.
- 21 National Cybersecurity Center of Excellence
 22 National Institute of Standards and Technology
 23 100 Bureau Drive
 24 Mailstop 2002
 25 Gaithersburg, MD 20899
 26 Email: nccoe@nist.gov

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

- 28 The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards
- and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and
- 30 academic institutions work together to address businesses' most pressing cybersecurity issues. This
- 31 public-private partnership enables the creation of practical cybersecurity solutions for specific
- industries, as well as for broad, cross-sector technology challenges. Through consortia under
- 33 Cooperative Research and Development Agreements (CRADAs), including technology partners—from
- 34 Fortune 50 market leaders to smaller companies specializing in information technology security—the
- 35 NCCoE applies standards and best practices to develop modular, adaptable example cybersecurity
- 36 solutions using commercially available technology. The NCCoE documents these example solutions in
- 37 the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework
- 38 and details the steps needed for another entity to re-create the example solution. The NCCoE was
- 39 established in 2012 by NIST in partnership with the State of Maryland and Montgomery County,
- 40 Maryland.

27

- To learn more about the NCCoE, visit https://www.nccoe.nist.gov/. To learn more about NIST, visit
- 42 https://www.nist.gov.

43 NIST CYBERSECURITY PRACTICE GUIDES

- 44 NIST Cybersecurity Practice Guides (Special Publication 1800 series) target specific cybersecurity
- 45 challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the
- 46 adoption of standards-based approaches to cybersecurity. They show members of the information
- 47 security community how to implement example solutions that help them align with relevant standards
- 48 and best practices, and provide users with the materials lists, configuration files, and other information
- 49 they need to implement a similar approach.
- 50 The documents in this series describe example implementations of cybersecurity practices that
- 51 businesses and other organizations may voluntarily adopt. These documents do not describe regulations
- or mandatory practices, nor do they carry statutory authority.

ABSTRACT

53

- A zero trust architecture (ZTA) focuses on protecting data and resources. It enables secure authorized
- 55 access to enterprise resources that are distributed across on-premises and multiple cloud environments,
- 56 while enabling a hybrid workforce and partners to access resources from anywhere, at any time, from
- 57 any device in support of the organization's mission. Each access request is evaluated by verifying the
- 58 context available at access time, including criteria such as the requester's identity and role, the
- requesting device's health and credentials, the sensitivity of the resource, user location, and user
- 60 behavior consistency. If the enterprise's defined access policy is met, a secure session is created to
- 61 protect all information transferred to and from the resource. A real-time and continuous policy-driven,

- 62 risk-based assessment is performed to establish and maintain the access. In this project, the NCCoE and
- 63 its collaborators use commercially available technology to build interoperable, open, standards-based
- 64 ZTA implementations that align to the concepts and principles in NIST Special Publication (SP) 800-207,
- 65 Zero Trust Architecture. This NIST Cybersecurity Practice Guide explains how commercially available
- technology can be integrated and used to build various ZTAs.

67 **KEYWORDS**

70

- 68 enhanced identity governance (EIG); identity, credential, and access management (ICAM); zero trust;
- 69 zero trust architecture (ZTA).

ACKNOWLEDGMENTS

71 We are grateful to the following individuals for their generous contributions of expertise and time.

Name	Organization
Quint Van Deman	Amazon Web Services
Jason Garbis	Appgate
Adam Rose	Appgate
Jonathan Roy	Appgate
Eric Michael	Broadcom Software
Ken Andrews	Cisco
Matthew Hyatt	Cisco
Leo Lebel	Cisco
Tom Oast	Cisco
Peter Romness	Cisco
Steve Vetter	Cisco
Daniel Cayer	F5

Name	Organization
David Clark	F5
Jay Kelley	F5
Tim Jones	Forescout
Yejin Jang	Forescout
Andrew Campagna	IBM
Adam Frank	IBM
Nalini Kannan	IBM
Priti Patil	IBM
Nikhil Shah	IBM
Mike Spisak	IBM
Vahid Esfahani	IT Coalition
Ebadullah Siddiqui	IT Coalition
Musumani Woods	IT Coalition
Tyler Croak	Lookout
Madhu Dodda	Lookout
Jeff Gilhool	Lookout
Ken Durbin	Mandiant
Earl Matthews	Mandiant

Name	Organization
Tarek Dawoud	Microsoft
Janet Jones	Microsoft
Hemma Prafullchandra	Microsoft
Brandon Stephenson	Microsoft
Clay Taylor	Microsoft
Sarah Young	Microsoft
Spike Dog	MITRE
Sallie Edwards	MITRE
Ayayidjin Gabiam	MITRE
Jolene Loveless	MITRE
Karri Meldorf	MITRE
Kenneth Sandlin	MITRE
Lauren Swan	MITRE
Jessica Walton	MITRE
Mike Bartock	NIST
Gema Howell	NIST
Douglas Montgomery	NIST
Kevin Stine	NIST

Name	Organization
Sean Frazier	Okta
Kelsey Nelson	Okta
Shankar Chandrasekhar	Palo Alto Networks
Sean Morgan	Palo Alto Networks
Seetal Patel	Palo Alto Networks
Zack Austin	PC Matic
Andy Tuch	PC Matic
Ivan Anderson	Ping Identity
Bill Baz	Radiant Logic
John Petrutiu	Radiant Logic
Rusty Deaton	Radiant Logic
Deborah McGinn	Radiant Logic
Lauren Selby	Radiant Logic
Peter Amaral	SailPoint
Jim Russell	SailPoint
Esteban Soto	SailPoint
Karen Scarfone	Scarfone Cybersecurity
Jeremiah Stallcup	Tenable

Name	Organization
Bill Stritzinger	Tenable
Andrew Babakian	VMware
Peter Bjork	VMware
Genc Domi	VMware
Keith Luck	VMware
Dennis Moreau	VMware*
Jeffrey Adorno	Zscaler
Jeremy James	Zscaler
Lisa Lorenzin	Zscaler*
Matt Moulton	Zscaler
Patrick Perry	Zscaler

- 72 * Former employee; all work for this publication was done while at that organization
- 73 The Technology Partners/Collaborators who participated in this build submitted their capabilities in
- 74 response to a notice in the Federal Register. Respondents with relevant capabilities or product
- 75 components were invited to sign a Cooperative Research and Development Agreement (CRADA) with
- NIST, allowing them to participate in a consortium to build this example solution. We worked with:

	Technology Collaborators	
<u>Appgate</u>	<u>IBM</u>	Ping Identity
<u>AWS</u>	<u>lvanti</u>	Radiant Logic
Broadcom Software	Lookout	<u>SailPoint</u>
Cisco	<u>Mandiant</u>	<u>Tenable</u>
<u>DigiCert</u>	<u>Microsoft</u>	<u>Trellix</u>
<u>F5</u>	<u>Okta</u>	<u>VMware</u>
<u>Forescout</u>	Palo Alto Networks	<u>Zimperium</u>
Google Cloud	PC Matic	<u>Zscaler</u>

DOCUMENT CONVENTIONS

77

85

99

100

101

102

- 78 The terms "shall" and "shall not" indicate requirements to be followed strictly to conform to the
- 79 publication and from which no deviation is permitted. The terms "should" and "should not" indicate that
- 80 among several possibilities, one is recommended as particularly suitable without mentioning or
- 81 excluding others, or that a certain course of action is preferred but not necessarily required, or that (in
- 82 the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms
- 83 "may" and "need not" indicate a course of action permissible within the limits of the publication. The
- 84 terms "can" and "cannot" indicate a possibility and capability, whether material, physical, or causal.

CALL FOR PATENT CLAIMS

- This public review includes a call for information on essential patent claims (claims whose use would be
- 87 required for compliance with the guidance or requirements in this Information Technology Laboratory
- 88 (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication
- or by reference to another publication. This call also includes disclosure, where known, of the existence
- 90 of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant
- 91 unexpired U.S. or foreign patents.
- 92 ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in
- 93 written or electronic form, either:
- a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not
- 95 currently intend holding any essential patent claim(s); or
- 96 b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring
- 97 to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft
- 98 publication either:
 - 1. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
 - 2. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.
- Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its
- behalf) will include in any documents transferring ownership of patents subject to the assurance,
- provisions sufficient to ensure that the commitments in the assurance are binding on the transferee,
- and that the transferee will similarly include appropriate provisions in the event of future transfers with
- the goal of binding each successor-in-interest.

- The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.
- Such statements should be addressed to: nccoe-zta-project@list.nist.gov

111 Contents

112	1	Inti	roduct	tion	1
113		1.1	How t	to Use this Guide	1
114	2	Fur	nction	al Demonstration Playbook	3
115		2.1	Defini	itions	3
116			2.1.1	Network IDs	3
117			2.1.2	Subject and Requested Resource Types	4
118			2.1.3	Resource and Querying Endpoint Compliance Classification	4
119			2.1.4	Desired Outcomes	4
120			2.1.5	Authentication Status	5
121		2.2	Gene	ral Configurations	6
122			2.2.1	Access Level	6
123			2.2.2	Access Profiles	6
124			2.2.3	Resources and Capabilities	7
125			2.2.4	User Profiles	8
126		2.3	Demo	nstration Methodology	8
127		2.4	Use C	ase A: Discovery and Identification of IDs, Assets, and Data Flows	10
128			2.4.1	Scenario A-1: Discovery and authentication of endpoint assets	10
129			2.4.2	Scenario A-2: Reauthentication of identified assets	12
130			2.4.3	Scenario A-3: Discovery of transaction flows	14
131		2.5	Use C	ase B: Enterprise ID Access	15
132			2.5.1	Scenario B-1: Full/limited resource access using an enterprise endpoint	15
133			2.5.2	Scenario B-2: Full/limited internet access using an enterprise endpoint	19
134			2.5.3	Scenario B-3: Stolen credential using an enterprise endpoint	22
135			2.5.4	Scenario B-4: Full/limited resource access using BYOD	27
136			2.5.5	Scenario B-5: Full/limited internet access using BYOD	31
137			2.5.6	Scenario B-6: Stolen credential using BYOD	33
138		2.6	Use C	ase C: Collaboration: Federated-ID Access	38
139			2.6.1	Scenario C-1: Full resource access using an enterprise endpoint	38

140			2.6.2	Scenario C-2: Limited resource access using an enterprise endpoint	39
141			2.6.3	Scenario C-3: Limited internet access using an enterprise endpoint	41
142			2.6.4	Scenario C-4: No internet access using an enterprise endpoint	41
143			2.6.5	Scenario C-5: Internet access using BYOD	42
144			2.6.6	Scenario C-6: Access resources using BYOD	43
145			2.6.7	Scenario C-7: Stolen credential using an enterprise endpoint	45
146			2.6.8	Scenario C-8: Stolen credential using BYOD	46
147		2.7	Use C	ase D: Other-ID Access	47
148			2.7.1	Scenario D-1: Full/limited resource access using an enterprise endpoint	47
149			2.7.2	Scenario D-2: Full/limited internet access using an enterprise endpoint	51
150			2.7.3	Scenario D-3: Stolen credential using BYOD or enterprise endpoint	54
151			2.7.4	Scenario D-4: Full/limited resource access using BYOD	59
152			2.7.5	Scenario D-5: Full/limited internet access using BYOD	63
153			2.7.6	Scenario D-6: Stolen credential using BYOD	66
154		2.8	Use C	ase E: Guest: No-ID Access	71
155			2.8.1	Scenario E-1: Guest requests public internet access	71
156		2.9	Use C	ase F: Confidence Level	71
157			2.9.1	Scenario F-1: User reauthentication fails during active session	71
158			2.9.2	Scenario F-2: Requesting endpoint reauthentication fails during active session	72
159			2.9.3	Scenario F-3: Resource reauthentication fails during active session	73
160			2.9.4	Scenario F-4: Compliance fails during active session	74
161			2.9.5	Scenario F-5: Compliance improves between requests	76
162	3	Fun	ction	al Demonstration Results	77
163		3.1	EIG Cr	awl Phase Demonstration Results	77
164			3.1.1	Enterprise 1 Build 1 (E1B1) Demonstration Results	77
165			3.1.2	Enterprise 2 Build 1 (E2B1) Demonstration Results	81
166			3.1.3	Enterprise 3 Build 1 (E3B1) Demonstration Results	86
167			3.1.4	Enterprise 4 Build 1 (E4B1) Demonstration Results	89
168		3.2	EIG Ru	un Phase Demonstration Results	89
169			3.2.1	Enterprise 1 Build 2 (E1B2) Demonstration Results	89

1/0	3.2.2	Enterprise 2 Build 2 (E2B2) Demonstration Results	96		
171	3.2.3	Enterprise 3 Build 2 (E3B2) Demonstration Results	97		
172	Appendix A	List of Acronyms	107		
173	Appendix B	References	109		
174	List of Tab	les			
175	Table 2-1 Auther	ntication Status Codes	5		
176	Table 2-2 Access	Levels	6		
177	Table 2-3 Access	Profiles	7		
178	Table 2-4 Resour	ces and Capabilities	7		
179	Table 2-5 User Pr	rofiles	8		
180	Table 2-6 Scenar	io A-1 Demonstrations	11		
181	Table 2-7 Scenar	io A-2 Demonstrations	13		
182	Table 2-8 Scenar	io A-3 Demonstrations	15		
183	Table 2-9 Scenar	io B-1 Demonstrations	16		
184	Table 2-10 Scena	ario B-2 Demonstrations	20		
185	Table 2-11 Scena	ario B-3 Demonstrations	22		
186	Table 2-12 Scena	ario B-4 Demonstrations	27		
187	Table 2-13 Scena	ario B-5 Demonstrations	31		
188	Table 2-14 Scena	ario B-6 Demonstrations	34		
189	Table 2-15 Scena	rio C-1 Demonstrations	39		
190	Table 2-16 Scena	ario C-2 Demonstrations	40		
191	Table 2-17 Scena	ario C-3 Demonstrations	41		
192	Table 2-18 Scena	ario C-4 Demonstrations	42		
193	Table 2-19 Scena	ario C-5 Demonstrations	43		
194	Table 2-20 Scena	rio C-6 Demonstrations	44		
195	Table 2-21 Scenario C-7 Demonstrations45				
196	Table 2-22 Scena	ario C-8 Demonstrations	46		

197	Table 2-23 Scenario D-1 Demonstrations	48
198	Table 2-24 Scenario D-2 Demonstrations	52
199	Table 2-25 Scenario D-3 Demonstrations	54
200	Table 2-26 Scenario D-4 Demonstrations	59
201	Table 2-27 Scenario D-5 Demonstrations	64
202	Table 2-28 Scenario D-6 Demonstrations	66
203	Table 2-29 Scenario E-1 Demonstrations	71
204	Table 2-30 Scenario F-1 Demonstrations	72
205	Table 2-31 Scenario F-2 Demonstrations	73
206	Table 2-32 Scenario F-3 Demonstrations	74
207	Table 2-33 Scenario F-4 Demonstrations	75
208	Table 2-34 Scenario F-5 Demonstrations	76
209	Table 3-1 Demonstration Results for E1B1 EIG Crawl Phase	77
210	Table 3-2 Demonstration Results for E2B1 EIG Crawl Phase	82
211	Table 3-3 Demonstration Results for E3B1 EIG Crawl Phase	86
212	Table 3-4 Demonstration Results for E1B2 EIG Crawl Phase	89
213	Table 3-5 Demonstration Results for E3B2 EIG Run Phase	97

1 Introduction

214

239

240

241

242

243244

245

215 To demonstrate the security characteristics supported by each zero trust architecture (ZTA) build that is 216 implemented as part of the NCCoE ZTA project, a variety of use cases have been defined, each of which 217 consists of numerous demonstrations that each have a specific expected outcome. The use cases are 218 designed to showcase ZTA security capabilities under a variety of conditions. 219 Section 2 of this document describes the use cases that have been defined. It also defines various types 220 of user IDs and endpoints, resources, user and access profiles, assumptions, and other information that 221 is required to fully describe the use cases. The purpose of this section of the document is to guide 222 operators as they perform each demonstration. 223 Section 3 of this document describes the results of performing these demonstrations using each of the 224 builds that have been implemented. 1.1 How to Use this Guide 225 226 This NIST Cybersecurity Practice Guide will help users develop a plan for migrating to ZTA. It 227 demonstrates a standards-based reference design for implementing a ZTA and provides users with the 228 information they need to replicate two different implementations of this reference design. Each of these 229 implementations, which are known as builds, are standards-based and align to the concepts and 230 principles in NIST Special Publication (SP) 800-207, Zero Trust Architecture. The reference design described in this practice guide is modular and can be deployed in whole or in part, enabling 231 232 organizations to incorporate ZTA into their legacy environments gradually, in a process of continuous 233 improvement that brings them closer and closer to achieving the ZTA goals that they have prioritized 234 based on risk, cost, and resources. 235 NIST is adopting an agile process to publish this content. Each volume is being made available as soon as 236 possible rather than delaying release until all volumes are completed. Work continues on implementing 237 the example solutions and developing other parts of the content. As a second preliminary draft, we will 238 publish at least one additional draft for public comment before it is finalized.

NIST SP 1800-35A: Executive Summary – why we wrote this guide, the challenge we address,

NIST SP 1800-35B: Approach, Architecture, and Security Characteristics – what we built and why

why it could be important to your organization, and our approach to solving this challenge

NIST SP 1800-35C: How-To Guides – instructions for building the example implementations,

including all the security-relevant details that would allow you to replicate all or parts of this

NIST SP 1800-35D: Implementing a Zero Trust Architecture

project

When complete, this guide will contain five volumes:

- NIST SP 1800-35D: Functional Demonstrations use cases that have been defined to showcase
 ZTA security capabilities and the results of demonstrating them with each of the example
 implementations (you are here)
- NIST SP 1800-35E: Risk and Compliance Management risk analysis and mapping of ZTA security
 characteristics to cybersecurity standards and recommended practices
- 251 Depending on your role in your organization, you might use this guide in different ways:
- 252 **Business decision makers, including chief security and technology officers,** will be interested in the
- 253 Executive Summary, NIST SP 1800-35A, which describes the following topics:
 - challenges that enterprises face in migrating to the use of ZTA
- 255 example solution built at the NCCoE
- benefits of adopting the example solution
- 257 **Technology or security program managers** who are concerned with how to identify, understand, assess,
- and mitigate risk will be interested in this part of the guide, NIST SP 1800-35B, which describes what we
- did and why.

- 260 Also, Section 3 of Risk and Compliance Management, NIST SP 1800-35E, will be of particular interest.
- 261 Section 3, ZTA Reference Architecture Security Mappings, maps logical components of the general ZTA
- 262 reference design to security characteristics listed in various cybersecurity guidelines and recommended
- 263 practices documents, including Framework for Improving Critical Infrastructure Cybersecurity (NIST
- 264 Cybersecurity Framework), Security and Privacy Controls for Information Systems and Organizations
- 265 (NIST SP 800-53), and Security Measures for "EO-Critical Software" Use Under Executive Order (EO)
- 266 *14028*.
- You might share the Executive Summary, NIST SP 1800-35A, with your leadership team members to help
- 268 them understand the importance of migrating toward standards-based ZTA implementations that align
- to the concepts and principles in NIST SP 800-207, Zero Trust Architecture [1].
- 270 IT professionals and operators who want to implement similar solutions will find the whole practice
- 271 guide useful. You can use the how-to portion of the guide, NIST SP 1800-35C, to replicate all or parts of
- the builds created in our lab. The how-to portion of the guide provides specific product installation,
- 273 configuration, and integration instructions for implementing the example solution. We do not re-create
- the product manufacturers' documentation, which is generally widely available. Rather, we show how
- 275 we incorporated the products together in our environment to create an example solution. Also, you can
- use NIST SP 1800-35D, which provides the use cases that have been defined to showcase ZTA security
- capabilities and the results of demonstrating them with each of the example implementations.
- 278 This guide assumes that IT professionals have experience implementing security products within the
- enterprise. While we have used a suite of commercial products to address this challenge, this guide does
- 280 not endorse these particular products. Your organization can adopt this solution or one that adheres to

- these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing
- parts of a ZTA. Your organization's security experts should identify the products that will best integrate
- 283 with your existing tools and IT system infrastructure. We hope that you will seek products that are
- 284 congruent with applicable standards and recommended practices.
- 285 A NIST Cybersecurity Practice Guide does not describe "the" solution, but example solutions. This is a
- second preliminary draft guide. As the project progresses, the second preliminary draft will be updated,
- and additional volumes will also be released for comment. We seek feedback on the publication's
- 288 contents and welcome your input. Comments, suggestions, and success stories will improve subsequent
- versions of this guide. Please contribute your thoughts to nccoe-zta-project@list.nist.gov.

2 Functional Demonstration Playbook

- 291 This section is intended to guide the operator through the set of ZTA scenarios and use cases that have
- been defined for demonstration in this project. To reduce the number of iterations, some potential
- 293 demonstrations have been omitted because they are not sufficiently different from another
- demonstration that has been included. For example, if the requester's access to a resource is blocked
- due to a non-compliant on-premises resource, then it is sufficient to demonstrate this once with an on-
- 296 premises-to-on-premises request; this demonstration does not need to be repeated making the request
- 297 from a branch office or remote access location because the location of the requester in this
- demonstration is irrelevant. The demonstration playbook is not exhaustive, and it does not capture all
- 299 possible demonstration cases.
- 300 This playbook is still under development. Additional scenarios and use cases will be included in the next
- 301 version as the implementations evolve and add capabilities. For this current draft of the document and
- 302 as discussed in Volume B of this guide, the scenarios are limited to on-premises resources or public
- internet resources with only enhanced identity governance (EIG) considered. Subject endpoints are
- located on-premises or at branch or remote locations. Only EIG approach solutions are currently present
- in the builds. Microsegmentation and software-defined perimeter (SDP) solutions are currently out of
- 306 scope.

307

290

2.1 Definitions

308 2.1.1 Network IDs

- 309 As defined in NIST SP 800-63, an *identity* is an attribute or set of attributes that uniquely identifies a
- 310 subject [2]. A network identity is used here simply as an identity that allows the subject to identify itself
- to all connected enterprise resources. The following definitions are used for network IDs:
- **Enterprise-ID:** A network ID issued and maintained by the enterprise. It is stored in one (or more) identity stores maintained by the enterprise.

321

325

326 327

328

329330

331332

333334

335

336

337

338

340 341

- Federated-ID: A network ID issued and maintained by another enterprise in a community of interest, and partner enterprises have a trusted means to authenticate the ID. This could include things such as a common PKI, etc.
- Other-ID: A network ID issued and maintained by another enterprise but known or registered by the first enterprise. Examples include contractors, customers, etc. The other enterprise has limited means to authenticate to the first enterprise.
 - **No-ID:** An anonymous network ID unknown to the enterprise that the enterprise would be unable to authenticate. This is also referred to as a "guest" to the enterprise.

322 2.1.2 Subject and Requested Resource Types

- In zero trust, all enterprise data, assets, etc. are considered resources. To clarify the actors (subject and requested resource) in the following scenarios, the following more detailed definitions are used:
 - Enterprise endpoint (EP): Owned and fully managed by the enterprise. The enterprise can inspect and modify any data on the endpoint. An EP is usually acting as the requesting subject but can be the target of a management utility.
 - **Enterprise resource (RSS):** Fully managed by the enterprise. The enterprise can inspect and modify the resource. An RSS is usually acting as the target of a request.
 - Bring Your Own Device (BYOD): Not owned by the enterprise and not fully managed. The enterprise can inspect the device but cannot directly manage or wipe the device. User agents, certificates, etc. may be pre-installed by a private owner, but the endpoint cannot be managed. A BYOD is usually acting as the requesting subject or as the target of a management utility.
 - **Guest device:** Not owned or managed by the enterprise and is opaque to the enterprise. The enterprise can only see what is emitted and received by its enterprise managed infrastructure. Examples include browser user agents and DNS queries. A guest device is usually acting as the requesting subject or as the target of a management utility.

2.1.3 Resource and Querying Endpoint Compliance Classification

- 339 The following definitions are used for endpoint and resource security compliance policies:
 - **(EIG) Endpoint Compliance:** Policy that requires the endpoint device to be uniquely identified and to conform to the enterprise security policy for the device.
- **(EIG) Resource Compliance:** Policy that requires the enterprise-managed resource to be identified and to conform to the enterprise security policy for the resource.

344 2.1.4 Desired Outcomes

345 The following definitions are used for desired outcomes:

350

351

352

353

354

355 356

357

358 359

360

361

362

363

364 365

366

367368

369

370

- Access to Network: Endpoint is allocated an address on enterprise infrastructure and
 enrolled/updated into any monitoring system in place. This result is only applicable to select on premises (or branch) demonstrations.
 - Access to Public Network: Endpoint is allocated an address, but only allowed access to the (public) internet; cannot reach/access non-public enterprise resources. This result is only applicable to select on-premises (or branch) demonstrations.
 - Limited Access to Network: Endpoint is allocated an address with strict traffic restrictions. This
 may include a quarantine state with only access to update/patch management system. This
 result is only applicable to select on-premises (or branch) demonstrations.
 - No Access to Network: Endpoint is not allocated an address and cannot send or receive communication. This result is only applicable to select on-premises (or branch) demonstrations.
 - Access (to Resource) Successful: Access to the resources that are specified in the profile is achieved.
 - Access (to Resource) Limited: Access to a subset, but not all, of the resources that are specified
 in the profile is achieved.
 - Access (to Resource) Not Successful: No access to the requested resource is achieved.
 - Keep Access (to Resource): Access remains at the previous state.
 - Max. Limited Access to Network: This outcome is specific for device-based assets that will be authenticated. This means that portions of the network or some RSS will not be available to be accessed by this subject.
 - **Terminate Access (to X):** The session is terminated or all access to the network is terminated (i.e., no longer allowed to send/receive communications).
 - Other Outcome: Some demonstrations use explicit text that informs of a desired action. Examples: "Terminate all sessions" or "Log API call."

2.1.5 Authentication Status

371 Table 2-1 explains the authentication status codes used in the demonstration use case tables below.

372 Table 2-1 Authentication Status Codes

Activity	Description	Examples	
A+	Authentication successful	All provided credentials matched	
A-	Authentication not successful	Password failure, MFA failure, account does not exist, account blocked, suspicions raised	
RA+	Successful re-authentication of a previously successful authentication	All provided credentials matched	

Activity	Description	Examples
RA-	Failed re-authentication of a previously successful authentication	Password failure, MFA failure, account does not exist, account blocked, suspicious activity
А	Actively authenticated	Previously authenticated but no need for reauthentication yet
	Not authenticated yet	

2.2 General Configurations

374 This section focuses on the configurations and specifications used within the demonstration use cases.

2.2.1 Access Level

Table 2-2 defines the access levels used in the demonstration scenarios. An *access level* specifies a set of available actions or access allowed to a subject. Downgrading an access level means the access level will be replaced by the new downgraded access level. For example, if a subject with access level "Full Access" gets downgraded to access level "Limited Access," this means the subject only has access to resources and/or functions that require at least "Limited Access." Similarly, if a subject with access level "Limited Access" gets downgraded, the subject will have no further access to anything. Downgraded access levels can be reversed to their original state.

383 Table 2-2 Access Levels

Access Level	Can Downgrade to	Description
Full Access	Limited Access	This allows the subject to use all functions available on the selected resource.
Limited Access	None	This allows the subject to use a subset of functions available on the selected resource.
None	None	No access

2.2.2 Access Profiles

<u>Table</u> 2-3 defines the access levels used in the demonstration scenarios. Access profiles provide the configuration and maximum access level that can be used. Access levels within the profile can be downgraded to the next lower level when the demonstration directs the operator to limit the access.

388 Table 2-3 Access Profiles

389

390

391

392

393

394

Access Profile	Maximum Access Level	Description
P_FULL	Full Access	This provides the capability to access all capabilities of each available resource.
P_LIMITED	Limited Access	This provides the capability to select a limited set of capabilities by the available resources.
P_NONE	none	No access

2.2.3 Resources and Capabilities

<u>Table</u> 2-4 defines the resources and capabilities used in the demonstration scenarios. Resources (RSS) and capabilities (CAP) specify items and actions used within the demonstrations. Access to them requires a minimum access level. For convenience, the *Access Profile* column lists the access profiles that will provide access to the given resource or capability. The *Example* column provides suggestions regarding resources and capabilities that the access level could be representing.

395 Table 2-4 Resources and Capabilities

Component	Туре	Minimum Access Level	Access Profile	Example	
RSS1	Resource	Full Access	P_FULL	GitLab only accessible by P_FULL	
RSS2	Resource	Limited Access	P_FULL, P_LIMITED	File server	
CAP1-RSS1	Capability	Full Access	P_FULL	Create and access repositories	
CAP2-RSS1	Capability	Full Access	P_FULL	Access repositories	
CAP1-RSS2	Capability	Full Access	P_FULL	Read and write access	
CAP2-RSS2	Capability	Limited Access	P_FULL, P_LIMITED	Read-only access to all or limited part of resource	
URL1	Resource	Full Access	P_FULL	https://www.nccoe.nist.gov	
URL2	Resource	Limited Access	P_FULL, P_LIMITED	https://www.nist.gov	

2.2.4 User Profiles

<u>Table</u> 2-5 contains the different user profiles (UP) used with an enterprise-ID (UP-E) or other-ID (UP-O) for the demonstrations. Some profiles might be redundant (e.g., UP-E1 and UP-E4). This is done to help keep the profile configuration simple because the demonstrations that the redundant profiles are used in utilize different resources.

Table 2-5 User Profiles

User Profile	Access Profile	Resource	Status	Downgrade Trigger Examples
UP-E1	P_FULL	RSS1	Active	Endpoint falls out of compliance
UP-O1		RSS2		
UP-E2	P_LIMITED	RSS2	Active	Endpoint falls out of compliance
UP-O2				
UP-E3	none	none	Deactivated	
UP-O3			or deleted	
UP-E4	P_FULL	URL1	Active	Endpoint falls out of compliance
UP-04		URL2		
UP-E5	P_LIMITED	URL1	Active	Endpoint falls out of compliance
UP-O5		URL2		Internet access only during specific times
UP-E6 UP-O6	P_FULL	RSS1	Active	Detection of multiple logins from different locations
				Detection of second login from enterprise- owned device not assigned to user
				Detection of login from location outside of the country
UP-E7	P_FULL	RSS1	Active	Account reported compromised
UP-O7				Using old MFA method (stolen PIV card)

2.3 Demonstration Methodology

We are leveraging two types of demonstration methodologies: manual and automated. Demonstrations that require human interaction (e.g., user performs multifactor authentication) must be performed manually. Demonstrations that do not require human interaction can be performed either manually or automated, or both. It is also possible to perform demonstrations in a hybrid manner in which the early part of a demonstration that requires user authentication is performed manually, followed by an

automated portion of the demonstration. This approach can be helpful for demonstrations that are complicated, yet nevertheless require human interaction.

We deployed Mandiant Security Validation (MSV) throughout the project's laboratory environment to enable us to monitor and verify various security characteristics of the builds. MSV automates a testing program that provides visibility and evidence of how security controls are performing by emulating attackers to safely process advanced cyberattack security content within production environments. It is designed so defenses respond to it as if an attack is taking place within the enterprise. Virtual machines (VMs) that are intended to operate as actors are deployed on each of the subnetworks in each of the enterprises. These actors can be used to initiate various actions for the purpose of verifying that security controls are working to support the objectives of zero trust. We also deployed three VMs that operate as directors, two of which function as applications within enterprise 1 and enterprise 3 that are used by those enterprises to monitor and audit their own traffic, and one of which is an overarching director that is located within the management and orchestration domain and used by the project team to demonstrate and audit operations that span multiple enterprises. (See Section 4.3 of NIST SP 1800-35B.)

This setup enabled the following dual-purpose MSV deployment:

- 1. A typical MSV deployment, in which each enterprise deploys MSV as an application within its own enterprise and uses it for self-auditing and testing. Each enterprise deploys a director and multiple actors that function as applications within the enterprise, enabling the enterprise to monitor and test its own enterprise security capabilities, verifying the protections it receives from the ZTA and its ability to operate as expected. In this capacity, MSV is treated just like any other application deployed within that enterprise. The components may be protected by PEPs according to enterprise policies, and directors and actors exchange traffic over the same data communications paths as other enterprise applications. Firewalls and policies within the ZTA must be configured to permit the communications that the MSV components send and receive, including traffic that is sent between actors and the director to control the actions that are performed to test various security controls.
- 2. The NCCoE project team, as testers, use MSV to monitor and audit enterprise and interenterprise actions. The project team deploys an overarching director and a management backchannel connecting that director to all actors throughout the laboratory environment. This overarching director is used as a tool to verify the security controls provided by each of the ZTAs in the various enterprises and to monitor and audit inter-enterprise interactions. In this capacity, MSV is not functioning as an application deployed or controlled by the enterprises, but rather as a tool being used to monitor and audit enterprise and inter-enterprise activity. Communications between the actors and this overarching director occur on a management channel that is separate from the data networks in each of the enterprises. Using a separate backchannel ensures that the tool being used to monitor and verify the various ZTA architectures is not itself impacting those architectures. Enabling the overarching MSV director

446

447

448

449

450

451

452

453

454

455

to control the actor VMs via a backchannel requires each of the actor VMs to have two network interface cards (NICs), one for enterprise data and one for MSV tool interoperation. Use of a separate backchannel ensures that enterprise ZTA policies and firewalls don't need to be modified to accommodate the overarching MSV testing by permitting traffic between the overarching director and the actors that would not normally be expected to transit any of the enterprise networks. Such policy and firewall modification would have been undesirable and would, in effect, have amounted to unauthorized channels into the enterprise networks.

- An MSV protective theater was also created in the lab. This is a virtualized system that allows destructive actions to be tested without adversely impacting the enterprise deployments themselves. For example, to understand the effects that malware might have on a specific system in one of the enterprises, that system could be imported into the protective theater and infected with malware to
- 456 test what the destructive effects of the malware might be.

457 2.4 Use Case A: Discovery and Identification of IDs, Assets, and Data Flows

- NIST SP 800-207 [1] discusses the discovery and cataloging of all enterprise IDs, assets, and data flows as
- 459 the initial step before migrating to a ZTA. An enterprise needs to identify and understand the workflows
- 460 used in business processes, the IDs used, and the resources involved. Then it can move on to creating
- 461 policies around those workflows. This use case covers this initial exercise.
- The following discovery use cases did not originally appear in the Project Description [3] but were
- subsequently included to reflect the full ZTA migration process described in NIST SP 800-207.

464 2.4.1 Scenario A-1: Discovery and authentication of endpoint assets

- 465 Discovery here is focused on detecting assets and flows on the network, mapping them to identified
- assets and flows, and providing access accordingly.
- 467 **Pre-Condition**: Enterprise-owned components (RSS and EP) have already undergone initial onboarding
- 468 for the enterprise, and BYODs have already registered with the enterprise. Any necessary agents,
- certificates, etc. have been installed. Non-onboarded enterprise-owned components as well as non-
- 470 registered BYODs are treated the same as unknown guest devices. BYOD devices must have a software
- agent installed that allows inspection of the devices to create a report of the device hygiene (e.g., look
- for accepted virus scanner and approved OS). The enterprise infrastructure is a macrosegmented local
- 473 network with an "enterprise" segment with resources that can only be accessed by authorized
- 474 enterprise IDs and a "guest" segment with access to the public internet only.
- 475 **Demonstration**: Connect the device to the network and demonstrate network connectivity.
- 476 **Purpose and Outcome**: This scenario demonstrates the capability to authenticate assets at a specific
- 477 location and provide enterprise network access.

478 Table 2-6 Scenario A-1 Demonstrations

Demo	ID	<u>Subj</u>	Onboarded/	<u>Auth</u>	Compl	Subj	Desired Outcome
	l	<u>Type</u>	Registered	<u>Stat</u>		Loc	
	а	RSS	Υ	A+	Υ		Access to Network
	b	RSS	Υ	A+	N		No Access to Network
	С	RSS	Υ	A-			No Access to Network
	d	RSS	N				No Access to Network
	е	EP	Υ	A+	Υ		Access to Network
	f	EP	Υ	A+	N		Max. Limited Access to Network
A 1 1	g	EP	Υ	A-		On-	No Access to Network
A-1.1	h	EP	N			Prem	Access to Public Network
	i	BYOD	Υ	A+	Υ		Access to Network
	j	BYOD	Υ	A+	N		Limited Access to Network
	k	BYOD	Υ	A-			No Access to Network
	I	BYOD	N				Access to Public Network
	m	Guest Dev.					Access to Public Network
	а	RSS	Υ	A+	Υ		Access to Network
	b	RSS	Υ	A+	N		No Access to Network
	С	RSS	Υ	A-			No Access to Network
	d	RSS	N				No Access to Network
A-1.2	е	EP	Υ	A+	Υ	Branch	Access to Network
	f	EP	Υ	A+	N		Limited Access to Network
	g	EP	Υ	A-			No Access to Network
	h	EP	N				Access to Public Network
	i	BYOD	Υ	A+	Υ		Access to Network

Demo	Demo ID		Onboarded/ Registered	Auth Stat	Compl	Subj Loc	<u>Desired Outcome</u>
	j	BYOD	Υ	A+	N		Limited Access to Network
	k	BYOD	Υ	A-			No Access to Network
	ı	BYOD	N				Access to Public Network
	m	Guest Dev.					Access to Public Network
	а	EP	Υ	A+	Υ		Access to Network
	b	EP	Υ	A+	N		Max. Limited Access to Network
	С	EP	Υ	A-			No Access to Network
A-1.3						Remot e	
	d	BYOD	Υ	A+	Υ		Access to Network
	е	BYOD	Υ	A+	N		Max. Limited Access to Network
	f	BYOD	Υ	A-			No Access to Network
	а	RSS	Υ	A+	Υ		Access to Network
	b	RSS	Υ	A+	N		No Access to Network
	С	RSS	Υ	A-			No Access to Network
	d	RSS	N				No Access to Network
A-1.4						Cloud	
	е	EP	Υ	A+	Υ		Access to Network
	f	EP	Υ	A+	N		Max. Limited Access to Network
	g	EP	Υ	A-			No Access to Network

2.4.2 Scenario A-2: Reauthentication of identified assets

- 480 Once an asset is identified and authenticated, continuous re-authentication is necessary.
- 481 **Pre-Condition:** The asset (user endpoint, resource) underwent previous authentication and is ready for operation.
- 483 **Demonstration:** The asset is reauthenticated and will either pass or fail reauthentication.

- Purpose and Outcome: This scenario demonstrates the proper reauthentication of an asset and
 performs the desired action accordingly.
 - **Table 2-7 Scenario A-2 Demonstrations**

Demo	ID	<u>Subj</u>	Onboarded/	Auth	Compl	Subj	Desired Outcome		
		<u>Type</u>	Registered	<u>Stat</u>		Loc			
	а	RSS	Υ	RA+	Υ		Keep Access to Network		
	b	RSS	Υ	RA+	N		Terminate Access to Network		
	С	RSS	Υ	RA-			Terminate Access to Network		
	d	EP	Υ	RA+	Υ		Keep Access to Network		
A-2.1	е	EP	Υ	RA+	N	On- Prem	Max. Limited Access to Network		
	f	EP	Υ	RA-		1 10111	Terminate Access to Network		
	g	BYOD	Υ	RA+	Υ		Keep Access to Network		
	h	BYOD	Υ	RA+	N		Max. Limited Access to Network		
	i	BYOD	Υ	RA-			Terminate Access to Network		
	а	RSS	Υ	RA+	Υ		Keep Access to Network		
	b	RSS	Υ	RA+	N		Terminate Access to Network		
	С	RSS	Υ	RA-			Terminate Access to Network		
	d	EP	Υ	RA+	Υ		Keep Access to Network		
A-2.2	е	EP	Υ	RA+	N	Branch	Max. Limited Access to Network		
	f	EP	Υ	RA-			Terminate Access to Network		
	g	BYOD	Υ	RA+	Υ		Keep Access to Network		
	h	BYOD	Υ	RA+	N		Max. Limited Access to Network		
	i	BYOD	Υ	RA-			Terminate Access to Network		
A-2.3	а	EP	Υ	RA+	Υ		Keep Access to Network		

Demo	ID	<u>Subj</u> <u>Type</u>	Onboarded/ Registered	Auth Stat	Compl	Subj Loc	<u>Desired Outcome</u>
	b	EP	Υ	RA+	N	Remot e	Max. Limited Access to Network
	С	EP	Υ	RA-			Terminate Access to Network
	d	BYOD	Υ	RA+	Υ		Keep Access to Network
	е	BYOD	Y	RA+	N	Max. Limited Access to Network	
	f	BYOD	Υ	RA-			Terminate Access to Network
	а	RSS	Υ	RA+	Υ		Keep Access to Network
	b	RSS	Υ	RA+	N		Terminate Access to Network
	С	RSS	Υ	RA-			Terminate Access to Network
A-2.4						Cloud	
, , , _ , ,	d	EP	Υ	RA+	Υ	Cioda	Keep Access to Network
	е	EP	Υ	RA+	N		Max. Limited Access to Network
	f	EP	Υ	RA-			Terminate Access to Network

2.4.3 Scenario A-3: Discovery of transaction flows

487

490

491

492

This scenario demonstrates the monitoring of transactions between endpoints. Transactions include user access to a resource or service-to-service communication.

Pre-Condition: User (Enterprise-ID or Other-ID) has a set of privileges to a resource and can successfully authenticate. Requesting endpoints are considered successfully authenticated. Some mechanism is present either on the endpoints or along the communication path that can observe and log actions.

493 **Demonstration**: Logs are produced that map user access requests, API calls, etc., between resources.
 494 The logs may be on a third resource.

495 **Purpose and Outcome:** This scenario demonstrates the discovery and recording of metadata of traffic
 496 flows between resources and user access requests/actions. The actual inspection of traffic is not
 497 necessary.

Table 2-8 Scenario A-3 Demonstrations

Demo	emo ID Endpoint Type		Req Loc	RSS Loc	Desired Outcome		
A-3.1	а	USER	On-Prem	On-Prem	User request and action is recorded		
A-3.1	b	RSS/Service	On-Prem	On-Prem	API call is recorded		
A-3.2	а	USER	On-Prem	Cloud	User request and action is recorded		
A-3.2	b	RSS/Service	On-Prem	Cloud	API call is recorded		
A-3.3	а	USER	Branch	On-Prem	User request and action is recorded		
A-3.3	b	RSS/Service	Didiicii	On-Prem	API call is recorded		
A-3.4	а	USER	Branch	Cloud	User request and action is recorded		
A-3.4	b	RSS/Service	Branch	Cloud	API call is recorded		
A-3.5	а	USER	Remote	On-Prem	User request and action is recorded		
A-3.6	а	USER	Remote	Cloud	User request and action is recorded		

2.5 Use Case B: Enterprise ID Access

Demonstrations in this use case deal with different scenarios using access to enterprise resources as well as non-enterprise resources located on-premises, in the cloud, and on the internet.

Each activity demonstrates the capability of authentication from within a given setting. The access is authenticated with an "enterprise-ID" using an enterprise-owned endpoint (EP) as well as a privately owned endpoint (BYOD). Each scenario provides a set of pre-conditions as well as multiple demonstrations.

2.5.1 Scenario B-1: Full/limited resource access using an enterprise endpoint

This scenario deals with a request using different enterprise ID profiles, one with access to all provided resources and one with access to a limited set of resources (e.g., only RSS1 but not RSS2), or limited functionality while accessing an enterprise-controlled resource (e.g., read-only vs. read/write).

Pre-Condition: The enterprise provides multiple user accounts with different access levels. The P_FULL access profile specifies access to all resources (RSS) within the enterprise and/or all capabilities (CAP) of resources within the enterprise. Additionally, the P_LIMITED access profile specifies access to a subset of the resources and/or only limited functionality of each resource. Both endpoints' compliance (Compl) is already verified, and systems are authenticated per demonstration policy.

Demonstration: Each requestor using an enterprise-ID will attempt to successfully access an enterprise resource or a functionality of an enterprise resource.

- Purpose and Outcome: This demonstration focuses on user privilege, authentication/re-authentication,
 the endpoint and RSS location, and the compliance of endpoints.
 - Table 2-9 Scenario B-1 Demonstrations

Demo	ID	<u>UP</u>	Location	<u>Au</u>	th St	at_	Access	Со	mpl	Desired Outcome
			Req. > RSS	User	EP	RSS		EP	RSS	
	а	E1		A+	Α	Α	RSS1	Υ	Υ	Access Successful
	b	E1		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	С	E1		A-	Α			Υ		Access Not Successful
	d	E2		A+	Α	Α	RSS1	Υ	Υ	Access Not Successful
	е	E2		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	f	E2		A-	Α			Υ		Access Not Successful
	g	E3		A-	Α			Υ		Access Not Successful
D 1 1	h	E1	On-Prem →	RA+	Α	Α	RSS1	Υ	Υ	Access Successful
B-1.1	B-1.1 i E	E1	→ On-Prem	RA-	Α			Υ		Access Not Successful
	j	E1		RA+	Α	Α	RSS1	N	Υ	Access Not Successful
	k	E1		RA+	Α	Α	RSS2	N	Υ	Access Limited
	I	E1		A+	Α	Α	RSS1	N	Υ	Access Not Successful
	m	E1		A+	Α	Α	RSS2	N	Υ	Access Limited
	n	E1		A+	Α	Α	RSS1	Υ	N	Access Not Successful
	0	E1		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	р	E2		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	а	E1		A+	Α	Α	RSS1	Υ	Υ	Access Successful
	b	E1		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	С	E1		A-	Α			Υ		Access Not Successful
B-1.2	d	E2	Branch →	A+	Α	Α	RSS1	Υ	Υ	Access Not Successful
B-1.2	е	E2	On-Prem	A+	Α	Α	RSS2	Υ	Υ	Access Successful
	f	E2		A-	Α			Υ		Access Not Successful
	g	E3		A-	Α			Υ		Access Not Successful

Demo	Demo ID		Location	Au	th St	<u>at</u>	Access	Со	mpl	Desired Outcome
			Req. > RSS	User	EP	RSS		EP	RSS	
	h	E1		RA+	Α	Α	RSS1	Υ	Υ	Access Successful
	i	E1		RA-	Α			Υ		Access Not Successful
	j	E1		RA+	Α	Α	RSS1	N	Υ	Access Not Successful
	k	E1		RA+	Α	Α	RSS2	N	Υ	Access Limited
	_	E1		A+	Α	Α	RSS1	N	Υ	Access Not Successful
	m	E1		A+	Α	Α	RSS2	N	Υ	Access Limited
	n	E1		A+	Α	Α	RSS1	Υ	N	Access Not Successful
	0	E1		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	р	E2		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	а	E1		A+	Α	Α	RSS1	Υ	Υ	Access Successful
	b	E1		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	С	E1		A-	Α			Υ		Access Not Successful
	d	E2		A+	Α	Α	RSS1	Υ	Υ	Access Not Successful
	е	E2		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	f	E2		A-	Α			Υ		Access Not Successful
	g	E3		A-	Α			Υ		Access Not Successful
D 1 2	h	E1	Remote	RA+	Α	Α	RSS1	Υ	Υ	Access Successful
B-1.3	i	E1	On-Prem	RA-	Α			Υ		Access Not Successful
	j	E1		RA+	Α	Α	RSS1	N	Υ	Access Not Successful
	k	E1		RA+	Α	Α	RSS2	N	Υ	Access Limited
	_	E1		A+	Α	Α	RSS1	N	Υ	Access Not Successful
	m	E1		A+	Α	Α	RSS2	N	Υ	Access Limited
	n	E1		A+	Α	Α	RSS1	Υ	N	Access Not Successful
	0	E1		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	р	E2		A+	Α	Α	RSS2	Υ	N	Access Not Successful
B-1.4	а	E1	On-Prem	A+	Α	Α	RSS1	Υ	Υ	Access Successful
D-1.4	b	E1	\rightarrow	A+	Α	Α	RSS2	Υ	Υ	Access Successful

Demo ID		<u>UP</u>	Location	Auth Stat		Access	Compl		Desired Outcome	
			Req. > RSS	User	EP	RSS		EP	RSS	
	С	E1	Cloud	A-	Α			Υ		Access Not Successful
	d	E2		A+	Α	Α	RSS1	Υ	Υ	Access Not Successful
	е	E2		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	f	E2		A-	Α			Υ		Access Not Successful
	g	E3		A-	Α			Υ		Access Not Successful
	h	E1		RA+	Α	Α	RSS1	Υ	Υ	Access Successful
	i	E1		RA-	Α			Υ		Access Not Successful
	j	E1		RA+	Α	Α	RSS1	N	Υ	Access Not Successful
	k	E1		RA+	Α	Α	RSS2	N	Υ	Access Limited
	ı	E1		A+	Α	Α	RSS1	N	Υ	Access Not Successful
	m	E1		A+	Α	Α	RSS2	N	Υ	Access Limited
	n	E1		A+	Α	Α	RSS1	Υ	N	Access Not Successful
	0	E1		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	р	E2		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	а	E1		A+	Α	Α	RSS1	Υ	Υ	Access Successful
	b	E1		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	С	E1		A-	Α			Υ		Access Not Successful
	d	E2		A+	Α	Α	RSS1	Υ	Υ	Access Not Successful
	е	E2		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	f	E2		A-	Α			Υ		Access Not Successful
D1E	g	E3	Branch >	A-	Α			Υ		Access Not Successful
B-1.5			Cloud							
	h	E1		RA+	Α	Α	RSS1	Υ	Υ	Access Successful
	i	E1		RA-	Α			Υ		Access Not Successful
	j	E1		RA+	Α	Α	RSS1	N	Υ	Access Not Successful
	k	E1		RA+	Α	Α	RSS2	N	Υ	Access Limited
	ı	E1		A+	Α	А	RSS1	N	Υ	Access Not Successful

Demo ID		<u>UP</u>	Location	Auth Stat		Access	Compl		Desired Outcome		
			Req. > RSS	User	EP	RSS		EP	RSS		
	m	E1		A+	Α	Α	RSS2	N	Υ	Access Limited	
	n	E1		A+	Α	Α	RSS1	Υ	N	Access Not Successful	
	0	E1		A+	Α	Α	RSS2	Υ	N	Access Not Successful	
	р	E2		A+	Α	Α	RSS2	Υ	N	Access Not Successful	
	а	E1		A+	Α	Α	RSS1	Υ	Υ	Access Successful	
	b	E1		A+	Α	Α	RSS2	Υ	Υ	Access Successful	
	С	E1		A-	Α			Υ		Access Not Successful	
	d	E2		A+	Α	Α	RSS1	Υ	Υ	Access Not Successful	
	е	E2		A+	Α	Α	RSS2	Υ	Υ	Access Successful	
	f	E2		A-	Α			Υ		Access Not Successful	
	g	E3		A-	Α			Υ		Access Not Successful	
B-1.6	h	E1	Remote	RA+	Α	Α	RSS1	Υ	Υ	Access Successful	
B-1.0	i	E1	Cloud	RA-	Α			Υ		Access Not Successful	
	j	E1	ciouu	RA+	Α	Α	RSS1	N	Υ	Access Not Successful	
	k	E1		RA+	Α	Α	RSS2	N	Υ	Access Limited	
	I	E1		A+	Α	Α	RSS1	N	Υ	Access Not Successful	
	m	E1		A+	Α	Α	RSS2	N	Υ	Access Limited	
	n	E1		A+	Α	Α	RSS1	Υ	N	Access Not Successful	
	0	E1		A+	Α	Α	RSS2	Υ	N	Access Not Successful	
	р	E2		A+	Α	Α	RSS2	Υ	N	Access Not Successful	

2.5.2 Scenario B-2: Full/limited internet access using an enterprise endpoint

This scenario deals with access from an enterprise-owned device to non-enterprise-managed internet resources using different enterprise ID profiles: one with access to the internet, one with limited access to the internet, and one with no access to the internet.

Pre-Condition: The enterprise provides multiple user accounts with different access levels to the internet. The internet access will be performed using an enterprise-owned endpoint. RSS types are OK for approved and not OK for not-approved internet resources. The approval depends on the user's policy. User endpoints are checked for compliance (Compl) per demonstration policy. "Out of Hours"

- refers to the request taking place outside of marked business hours, which would fall outside of normal access behaviors seen for the ID.
- 530 **Demonstration:** Each requestor using an Enterprise-ID will attempt to successfully access a non-
- 531 enterprise resource.
- Purpose and Outcome: This demonstration focuses on the endpoint location as well as the resource
- 533 location.

Table 2-10 Scenario B-2 Demonstrations

Demo ID		<u>UP</u>	UP Location		Auth Stat		Compl		<u>Desired Outcome</u>
			Req. > RSS	User	EP		EP	Out of Hours	
	а	E4		A+	Α	URL1	Υ	N	Access Successful
	b	E4		A+	Α	URL2	Υ	N	Access Successful
	С	E4		A+	Α	URL1	Υ	Υ	Access Successful
	d	E4		A+	Α	URL1	Υ	Υ	Access Successful
	е	E4		A-	Α		Υ		Access Not Successful
	f	E5		A+	Α	URL1	Υ	N	Access Not Successful
	g	E5		A+	Α	URL2	Υ	N	Access Successful
	h	E5		A+	Α	URL1	Υ	Υ	Access Not Successful
D 2.4	i	E5	On-Prem →	A+	Α	URL1	Υ	Υ	Access Not Successful
B-2.1	j	E5	Internet	A-	Α		Υ		Access Not Successful
							•		
	k	E4		RA+	Α	URL1	Υ		Access Successful
	I	E4		RA-	Α		Υ		Access Not Successful
		•			•				
	m	E4		A+	Α	URL1	N		Access Not Successful
	n	E4		A+	Α	URL2	N		Access Successful
	О	E5		A+	Α	URL1	N	N	Access Not Successful
	р	E5		A+	Α	URL2	N	N	Access Not Successful
	а	E4	Branch	A+	Α	URL1	Υ	N	Access Successful
B-2.2	b	E4	\rightarrow	A+	Α	URL2	Υ	N	Access Successful
	С	E4	Internet	A+	Α	URL1	Υ	Υ	Access Successful

Demo ID		<u>UP</u> Location		Auth Stat		Access	C	ompl	Desired Outcome
			Req. >	User	EP		EP	Out of	
	d	E4	RSS	A+	Α	URL1	Υ	Hours Y	Access Successful
	e	E4		A-	A		Y		Access Not Successful
	f					URL1			Access Not Successful
		E5		A+	Α		Υ	N	Access Not Successful
	g	E5		A+	Α	URL2	Y	N	Access Successful Access Not Successful
	h :	E5		A+	Α	URL1	Y	Y	
	i	E5		A+	Α	URL1	Υ		Access Not Successful
	j	E5		A-	Α		Υ		Access Not Successful
	1.	- A		DA.	Ι ,	LIDI 1			Acces Cuccesful
	k	E4		RA+	Α	URL1	Υ		Access Successful
	l	E4		RA-	Α		Υ		Access Not Successful
					Ι.	l	1		
	m	E4		A+	Α	URL1	N		Access Not Successful
	n	E4		A+	Α	URL2	N		Access Successful
	0	E5		A+	Α	URL1	N	N	Access Not Successful
	р	E5		A+	Α	URL2	N	N	Access Not Successful
	а	E4		A+	Α	URL1	Υ	N	Access Successful
	b	E4		A+	Α	URL2	Υ	N	Access Successful
	С	E4		A+	Α	URL1	Υ	Υ	Access Successful
	d	E4		A+	Α	URL1	Υ	Υ	Access Successful
	е	E4		A-	Α		Υ		Access Not Successful
	f	E5		A+	Α	URL1	Υ	N	Access Not Successful
D 2 2	g	E5	Remote →	A+	Α	URL2	Υ	N	Access Successful
B-2.3	h	E5	Internet	A+	Α	URL1	Υ	Υ	Access Not Successful
	i	E5	internet	A+	Α	URL1	Υ	Υ	Access Not Successful
	j	E5		A-	Α		Υ		Access Not Successful
	k	E4		RA+	Α	URL1	Υ		Access Successful
	I	E4		RA-	Α		Υ		Access Not Successful

538

539

540

541

542543

544

545

Demo ID UI		<u>UP</u>	Location	Auth Stat		Access	Compl		<u>Desired Outcome</u>
			Req. > RSS	User	EP		EP	Out of Hours	
	m	E4		A+	Α	URL1	N		Access Not Successful
	n	E4		A+	Α	URL2	N		Access Successful
	О	E5		A+	Α	URL1	N	N	Access Not Successful
	р	E5		A+	Α	URL2	N	N	Access Not Successful

2.5.3 Scenario B-3: Stolen credential using an enterprise endpoint

This scenario deals with a request using a stolen credential. It does not matter if the access is performed using an enterprise endpoint.

Pre-Condition: The requestor's credential is stolen and is used to attempt accessing the enterprise resource RSS1 using an enterprise endpoint. The endpoints are compliant and authenticated, and so is the resource.

Demonstration: Two requests for the same enterprise resource are performed using the same user credentials. The "Real Request" is performed using the latest credentials, which are modified/replaced after being reported stolen. The "Hostile Request" is performed using a stolen enterprise-ID. All authentication methods of the Hostile Request are compromised. Re-authentication always follows a previously successful authentication.

Purpose and Outcome: This demonstration focuses on the detection of a stolen requester's enterprise-ID and enforcement of isolation.

548 Table 2-11 Scenario B-3 Demonstrations

Demo ID		<u>UP</u>	Location Real	Auth Stat Real Hostile		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
			Hostile > RSS	Req	Req			
	а	E6		A+		N	Access Successful	
	b	E6	On-Prem	A-		N	Access Not Successful	
B-3.1	С	E6	On-Prem →	Α	A+	N	Change to Access Limited	Access Not Successful
	d	E6	On-Prem	Α	A-	N	Keep Access	Access Not Successful
	е	E6			A+	N		Access Successful

Demo	ID	<u>UP</u>	Location	Aut	h Stat	Rep.	Desired Outcome	Desired Outcome
			Real Hostile > RSS	Real Req	Hostile Req	Stolen	for Real Request	for Hostile Request
	f	E6			A-	N		Access Not Successful
	g	E6		A+ A N		N	Access Not Successful	Change to Access Limited
	h	E6		A-	А	N	Access Not Successful	Keep Access
	i	E7		A+		Υ	Access Successful	
	j	E7		Α	A-	Υ	Keep Access	Access Not Successful
	k	E7			A-	Υ		Access Not Successful
	Ι	E7		RA+		Υ	Access Successful	
	m	E7			RA-	Υ		Access Not Successful
	n	E7			A	Y		All Sessions Terminated
	0	E7		А		Y	All Sessions Terminated	
	а	E6		A+		N	Access Successful	
	b	E6		A-		N	Access Not Successful	
	С	E6	On-Prem	Α	A+	N	Change to Access Limited	Access Not Successful
B-3.2	d	E6	Branch	А	A-	N	Keep Access	Access Not Successful
	е	E6	On-Prem		A+	N		Access Successful
	f	E6			A-	N		Access Not Successful
	g	E6		A+	А	N	Access Not Successful	Change to Access Limited

Demo	ID	<u>UP</u>	Location	<u>Aut</u>	h Stat	Rep.	Desired Outcome	Desired Outcome
			Real Hostile > RSS	Real Req	Hostile Req	Stolen	for Real Request	for Hostile Request
	h	E6		A-	А	N	Access Not Successful	Keep Access
	i	E7		A+		Υ	Access Successful	
	j	E7		А	A-	Υ	Keep Access	Access Not Successful
	k	E7			A-	Υ		Access Not Successful
	I	E7		RA+		Υ	Access Successful	
	m	E7			RA-	Υ		Access Not Successful
	n	E7			А	Υ		Change to Access Limited
	0	E7		Α		Υ	Change to Access Limited	
	а	E6		A+		N	Access Successful	
	b	E6		A-		N	Access Not Successful	
	С	E6		А	A+	N	Change to Access Limited	Access Not Successful
	d	E6	Branch	Α	A-	N	Keep Access	Access Not Successful
D 2 2	е	E6	On-Prem		A+	N		Access Successful
B-3.3	f	E6	→ On-Prem		A-	N		Access Not Successful
	g	E6		A+	А	N	Access Not Successful	Change to Access Limited
	h	E6		A-	А	N	Access Not Successful	Keep Access
	i	E7		A+		Υ	Access Successful	

Demo	ID	<u>UP</u>	Location	<u>Aut</u>	h Stat	Rep.	Desired Outcome	Desired Outcome
			Real Hostile > RSS	Real Req	Hostile Req	Stolen	for Real Request	for Hostile Request
	j	E7		А	A-	Υ	Keep Access	Access Not Successful
	k	E7			A-	Υ		Access Not Successful
	I	E7		RA+		Υ	Access Successful	
	m	E7			RA-	Υ		Access Not Successful
	n	E7			А	Υ		Change to Access Limited
	0	E7		А		Υ	Change to Access Limited	
	а	E6		A+		N	Access Successful	
	b	E6		A-		N	Access Not Successful	
	С	E6		А	A+	N	Change to Access Limited	Access Not Successful
	d	E6		А	A-	N	Keep Access	Access Not Successful
	е	E6			A+	N		Access Successful
	f	E6	Remote		A-	N		Access Not Successful
B-3.4	g	E6	On-Prem → On-Prem	A+	А	N	Access Not Successful	Change to Access Limited
	h	E6	Oll-Freili	A-	А	N	Access Not Successful	Keep Access
	i	E7		A+		Υ	Access Successful	
	j	E7		А	A-	Υ	Keep Access	Access Not Successful
	k	E7			A-	Υ		Access Not Successful
	ı	E7		RA+		Υ	Access Successful	

Demo	ID	<u>UP</u>	Location	<u>Aut</u>	h Stat	Rep.	Desired Outcome	Desired Outcome
			Real Hostile > RSS	Real Req	Hostile Req	Stolen	for Real Request	for Hostile Request
	m	E7			RA-	Υ		Access Not Successful
	n	E7			А	Υ		Change to Access Limited
	0	E7		Α		Υ	Change to Access Limited	
	а	E6		A+		N	Access Successful	
	b	E6		A-		N	Access Not Successful	
	С	E6		Α	A+	N	Change to Access Limited	Access Not Successful
	d	E6		А	A-	N	Keep Access	Access Not Successful
	е	E6			A+	N		Access Successful
	f	E6			A-	N		Access Not Successful
	g	E6	On-Prem	A+	А	N	Access Not Successful	Change to Access Limited
B-3.5	h	E6	Remote → On-Prem	A-	А	N	Access Not Successful	Keep Access
			On-Prem					
	i	E7		A+	Y Acc		Access Successful	
	j	E7		А	A-	Υ	Keep Access	Access Not Successful
	k	E7			A-	Υ		Access Not Successful
	I	E7		RA+		Υ	Access Successful	
	m	E7	7		RA-	Υ		Access Not Successful
	n	E7			А	Υ		Change to Access Limited

Demo	ID	<u>UP</u>	Location	Auth Stat		Rep.	Desired Outcome	Desired Outcome	
			Real Hostile > RSS	Real Req	Hostile Req	Stolen	for Real Request	for Hostile Request	
	0	E7		Α		Υ	Change to Access Limited		

2.5.4 Scenario B-4: Full/limited resource access using BYOD

This scenario deals with requests using different enterprise ID profiles, one with access to all provided resources and one with access to a limited set of resources (e.g., only RSS1 but not RSS2) or limited functionality while accessing an enterprise-controlled resource (e.g., read-only vs. read/write). In this scenario, the device used is BYOD.

Pre-Condition: The enterprise provides multiple User accounts with different access levels. The P_FULL access profile specifies access to either all resources (RSS) within the enterprise and/or all capabilities (CAP) of resources within the enterprise. Additionally, the P_LIMITED access profile specifies access to either a subset of the resources and/or limited functionality of each resource. Both endpoints' compliance (Compl) is already verified, and systems are authenticated per demonstration policy.

Demonstration: Each requestor using an enterprise-ID will attempt to successfully access an enterprise resource or a functionality of an enterprise resource.

Purpose and Outcome: This demonstration focuses on user privilege, authentication/re-authentication, the endpoint and RSS location, and the compliance of endpoints.

563 Table 2-12 Scenario B-4 Demonstrations

Demo	ID	<u>UP</u>	Location	Auth Stat			Access	Compl		<u>Desired Outcome</u>
			Req. > RSS	User	EP	RSS		EP	RSS	
	а	E1		A+	Α	Α	RSS1	Υ	Υ	Access Successful
	b	E1		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	С	E1		A-	Α			Υ		Access Not Successful
	d	E2	On-Prem	A+	Α	Α	RSS1	Υ	Υ	Access Not Successful
B-4.1	е	E2	\rightarrow	A+	Α	Α	RSS2	Υ	Υ	Access Successful
	f	E2	On-Prem	A-	Α			Υ		Access Not Successful
	g	E3		A-	Α			Υ		Access Not Successful
	h	E1		RA+	Α	Α	RSS1	Υ	Υ	Access Successful

Demo	ID	<u>UP</u>	Location	Au	th St	at_	Access	Coi	mpl	Desired Outcome
			Req. > RSS	User	EP	RSS		EP	RSS	
	i	E1		RA-	Α			Υ		Access Not Successful
	j	E1		RA+	Α	Α	RSS1	N	Υ	Access Not Successful
	k	E1		RA+	Α	Α	RSS2	N	Υ	Access Limited
						•		•		
	ı	E1		A+	Α	Α	RSS1	N	Υ	Access Not Successful
	m	E1		A+	Α	Α	RSS2	N	Υ	Access Limited
	n	E1		A+	Α	Α	RSS1	Υ	N	Access Not Successful
	0	E1		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	р	E2		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	а	E1		A+	Α	Α	RSS1	Υ	Υ	Access Successful
	b	E1		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	С	E1		A-	Α			Υ		Access Not Successful
	d	E2		A+	Α	Α	RSS1	Υ	Υ	Access Not Successful
	е	E2		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	f	E2		A-	Α			Υ		Access Not Successful
	g	E3		A-	Α			Υ		Access Not Successful
B-4.2	h	E1	Branch →	RA+	Α	Α	RSS1	Υ	Υ	Access Successful
B-4.2	i	E1	On-Prem	RA-	Α			Υ		Access Not Successful
	j	E1		RA+	Α	Α	RSS1	N	Υ	Access Not Successful
	k	E1		RA+	Α	Α	RSS2	N	Υ	Access Limited
	I	E1		A+	Α	Α	RSS1	N	Υ	Access Not Successful
	m	E1		A+	Α	Α	RSS2	N	Υ	Access Limited
	n	E1		A+	Α	Α	RSS1	Υ	N	Access Not Successful
	О	E1		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	р	E2		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	а	E1	Remote	A+	Α	Α	RSS1	Υ	Υ	Access Successful
B-4.3	b	E1	→	A+	Α	Α	RSS2	Υ	Υ	Access Successful
	С	E1	On-Prem	A-	Α			Υ		Access Not Successful

Demo	ID	<u>UP</u>	Location	Au	th St	<u>at</u>	Access	Compl		Desired Outcome
			Req. > RSS	User	EP	RSS		EP	RSS	
	d	E2		A+	Α	Α	RSS1	Υ	Υ	Access Not Successful
	е	E2		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	f	E2		A-	Α			Υ		Access Not Successful
	g	E3		A-	Α			Υ		Access Not Successful
	h	E1		RA+	Α	Α	RSS1	Υ	Υ	Access Successful
	i	E1		RA-	Α			Υ		Access Not Successful
	j	E1		RA+	Α	Α	RSS1	N	Υ	Access Not Successful
	k	E1		RA+	Α	Α	RSS2	N	Υ	Access Limited
					•					
	I	E1		A+	Α	Α	RSS1	N	Υ	Access Not Successful
	m	E1		A+	Α	Α	RSS2	N	Υ	Access Limited
	n	E1		A+	Α	Α	RSS1	Υ	N	Access Not Successful
	О	E1		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	р	E2		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	а	E1		A+	Α	Α	RSS1	Υ	Υ	Access Successful
	b	E1		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	С	E1		A-	Α			Υ		Access Not Successful
	d	E2		A+	Α	Α	RSS1	Υ	Υ	Access Not Successful
	е	E2		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	f	E2		A-	Α			Υ		Access Not Successful
	g	E3	On-Prem	A-	Α			Υ		Access Not Successful
B-4.4			\rightarrow							
	h	E1	Cloud	RA+	Α	Α	RSS1	Υ	Υ	Access Successful
	i	E1		RA-	Α			Υ		Access Not Successful
	j	E1		RA+	Α	Α	RSS1	N	Υ	Access Not Successful
	k	E1		RA+	Α	Α	RSS2	N	Υ	Access Limited
	I	E1		A+	Α	Α	RSS1	N	Υ	Access Not Successful
	m	E1		A+	Α	Α	RSS2	N	Υ	Access Limited

Demo	ID	<u>UP</u>	Location	<u>Au</u>	th St	at_	Access	Co	mpl	Desired Outcome
			Req. > RSS	User	EP	RSS		EP	RSS	
	n	E1		A+	Α	Α	RSS1	Υ	N	Access Not Successful
	0	E1		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	р	E2		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	а	E1		A+	Α	Α	RSS1	Υ	Υ	Access Successful
	b	E1		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	С	E1		A-	Α			Υ		Access Not Successful
	d	E2		A+	Α	Α	RSS1	Υ	Υ	Access Not Successful
	е	E2		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	f	E2		A-	Α			Υ		Access Not Successful
	g	E3		A-	Α			Υ		Access Not Successful
					•					
D 4.5	h	E1	Branch →	RA+	Α	Α	RSS1	Υ	Υ	Access Successful
B-4.5	j	E1	Cloud	RA-	Α			Υ		Access Not Successful
	k	E1		RA+	Α	Α	RSS1	N	Υ	Access Not Successful
	I	E1		RA+	Α	Α	RSS2	N	Υ	Access Limited
	m	E1		A+	Α	Α	RSS1	N	Υ	Access Not Successful
	n	E1		A+	Α	Α	RSS2	N	Υ	Access Limited
	0	E1		A+	Α	Α	RSS1	Υ	N	Access Not Successful
	р	E1		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	q	E2		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	а	E1		A+	Α	Α	RSS1	Υ	Υ	Access Successful
	b	E1		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	С	E1		A-	Α			Υ		Access Not Successful
	d	E2	Remote	A+	Α	Α	RSS1	Υ	Υ	Access Not Successful
B-4.6	е	E2	→	A+	Α	Α	RSS2	Υ	Υ	Access Successful
	f	E2	Cloud	A-	Α			Υ		Access Not Successful
	g	E3		A-	Α			Υ		Access Not Successful
	h	E1		RA+	Α	Α	RSS1	Υ	Υ	Access Successful

Demo	ID	<u>UP</u>	Location	Au	th St	<u>at</u>	Access	Coi	mpl	<u>Desired Outcome</u>
			Req. > RSS	User	EP	RSS		EP	RSS	
	-	E1		RA-	Α			Υ		Access Not Successful
	j	E1		RA+	Α	Α	RSS1	N	Υ	Access Not Successful
	k	E1		RA+	Α	Α	RSS2	N	Υ	Access Limited
	_	E1		A+	Α	Α	RSS1	N	Υ	Access Not Successful
	m	E1		A+	Α	Α	RSS2	N	Υ	Access Limited
	n	E1		A+	Α	Α	RSS1	Υ	N	Access Not Successful
	0	E1		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	р	E2		A+	Α	Α	RSS2	Υ	N	Access Not Successful

2.5.5 Scenario B-5: Full/limited internet access using BYOD

This scenario deals with access from an enterprise-owned device to non-enterprise-managed internet resources using different enterprise ID profiles: one with access to the internet, one with limited access to the internet, and one with no access to the internet.

Pre-Condition: The enterprise provides multiple user accounts with different access levels to the internet. Internet access will be performed using an enterprise-owned endpoint. RSS types are OK for approved and not OK for not-approved internet resources. The approval depends on the user's policy. User endpoints are checked for compliance (Compl) per demonstration policy.

Demonstration: Each requestor using an enterprise-ID will attempt to successfully access a non-573 enterprise resource.

Purpose and Outcome: This demonstration focuses on the endpoint location and the resource location.

575 Table 2-13 Scenario B-5 Demonstrations

Demo	ID	<u>UP</u>	Location	<u>Auth</u>	<u>Stat</u>	Access	C	ompl	<u>Desired Outcome</u>
			Req. > RSS	User	EP		EP	Out of Hours	
	а	E4		A+	Α	URL1	Υ	N	Access Successful
	b	E4	On-Prem	A+	Α	URL2	Υ	N	Access Successful
B-5.1	С	E4	\rightarrow	A+	Α	URL1	Υ	Υ	Access Successful
	d	E4	Internet	A+	Α	URL1	Υ	Υ	Access Successful
	е	E4		A-	Α		Υ		Access Not Successful

Demo	ID	<u>UP</u>	Location	Auth	<u>Stat</u>	Access	C	ompl	Desired Outcome
			Req. > RSS	User	EP		EP	Out of Hours	
	f	E5		A+	Α	URL1	Υ	N	Access Not Successful
	g	E5		A+	Α	URL2	Υ	N	Access Successful
	h	E5		A+	Α	URL1	Υ	Υ	Access Not Successful
	i	E5		A+	Α	URL1	Υ	Υ	Access Not Successful
	j	E5		A-	Α		Υ		Access Not Successful
	k	E4		RA+	Α	URL1	Υ		Access Successful
	ı	E4		RA-	Α		Υ		Access Not Successful
	m	E4		A+	Α	URL1	N		Access Not Successful
	n	E4		A+	Α	URL2	N		Access Successful
	О	E5		A+	Α	URL1	N	N	Access Not Successful
	р	E5		A+	Α	URL2	N	N	Access Not Successful
	а	E4		A+	Α	URL1	Υ	N	Access Successful
	b	E4		A+	Α	URL2	Υ	N	Access Successful
	С	E4		A+	Α	URL1	Υ	Υ	Access Successful
	d	E4		A+	Α	URL1	Υ	Υ	Access Successful
	е	E4		A-	Α		Υ		Access Not Successful
	f	E5		A+	Α	URL1	Υ	N	Access Not Successful
	g	E5		A+	Α	URL2	Υ	N	Access Successful
B-5.2	h	E5	Branch →	A+	Α	URL1	Υ	Υ	Access Not Successful
B-5.2	i	E5	Internet	A+	Α	URL1	Υ	Υ	Access Not Successful
	j	E5	meernee	A-	Α		Υ		Access Not Successful
	k	E4		RA+	Α	URL1	Υ		Access Successful
	Ι	E4		RA-	Α		Υ		Access Not Successful
	m	E4		A+	Α	URL1	N		Access Not Successful
	n	E4		A+	Α	URL2	N		Access Successful

Demo	ID	<u>UP</u>	Location	Auth	<u>Stat</u>	Access	C	ompl	Desired Outcome
			Req. > RSS	User	EP		EP	Out of Hours	
	0	E5		A+	Α	URL1	N	N	Access Not Successful
	р	E5		A+	Α	URL2	N	N	Access Not Successful
	а	E4		A+	Α	URL1	Υ	N	Access Successful
	b	E4		A+	Α	URL2	Υ	N	Access Successful
	С	E4		A+	Α	URL1	Υ	Υ	Access Successful
	d	E4		A+	Α	URL1	Υ	Υ	Access Successful
	е	E4		A-	Α		Υ		Access Not Successful
	f	E5		A+	Α	URL1	Υ	N	Access Not Successful
	g	E5		A+	Α	URL2	Υ	N	Access Successful
	h	E5		A+	Α	URL1	Υ	Υ	Access Not Successful
B-5.3	i	E5	Remote	A+	Α	URL1	Υ	Υ	Access Not Successful
D-3.3	j	E5	Internet	A-	Α		Υ		Access Not Successful
	k	E4		RA+	Α	URL1	Υ		Access Successful
	I	E4		RA-	Α		Υ		Access Not Successful
	m	E4		A+	Α	URL1	N		Access Not Successful
	n	E4		A+	Α	URL2	N		Access Successful
	0	E5		A+	Α	URL1	N	N	Access Not Successful
	р	E5		A+	Α	URL2	N	N	Access Not Successful

2.5.6 Scenario B-6: Stolen credential using BYOD

This scenario deals with a request using a stolen credential. It does not matter if the access is performed using an enterprise endpoint or BYOD device.

Pre-Condition: The requestor's credential is stolen and is used to attempt accessing the enterprise resource RSS1 using an enterprise endpoint. The endpoints are compliant and authenticated, and so is the resource.

Demonstration: Two requests for the same enterprise resource are performed using the same user credentials. The "Real Request" is performed using the latest credentials, which are modified/replaced after being reported stolen, and that request can succeed. The "Hostile Request" is performed using a

588

589

stolen enterprise-ID. All authentication methods are compromised for the Hostile Request. Reauthentication always follows a previously successful authentication.

Purpose and Outcome: This demonstration focuses on the detection of a stolen requester's enterprise-ID and enforcement of isolation.

Table 2-14 Scenario B-6 Demonstrations

Demo	ID	<u>UP</u>	Location	Aut	h Stat	Rep.	Desired Outcome	Desired Outcome
			Real Hostile > RSS	Real Hostile Stol		Stol en	for Real Request	for Hostile Request
	а	E6		A+		N	Access Successful	
	b	E6		A-		N	Access Not Successful	
	С	E6		А	A+	N	Change to Access Limited	Access Not Successful
	d	E6		А	A-	N	Keep Access	Access Not Successful
	е	E6			A+	N		Access Successful
	f	E6			A-	N		Access Not Successful
	g	E6	On-Prem	A+	А	N	Access Not Successful	Change to Access Limited
B-6.1	h	E6	On-Prem → On-Prem	A-	А	N	Access Not Successful	Keep Access
			On-Frein					
	i	E6		A+		Υ	Access Successful	
	j			Α	A-	Υ	Keep Access	Access Not Successful
	k				A-	Υ		Access Not Successful
	I	E6		RA+		Υ	Access Successful	
	m	E6			RA-	Υ		Access Not Successful
	n	E6			А	Υ		All Sessions Terminated

Demo	ID	<u>UP</u>	Location Real	<u>Aut</u> Real	h Stat Hostile	Rep. Stol	Desired Outcome for Real Request	Desired Outcome for Hostile Request
			Hostile > RSS	Req	Req	en		
	0	E6		А		Υ	All Sessions Terminated	
	а	E6		A+		N	Access Successful	
	b	E6		A-		Z	Access Not Successful	
	С	E6		А	A+	N	Change to Access Limited	Access Not Successful
	d	E6		А	A-	N	Keep Access	Access Not Successful
	е	E6			A+	N		Access Successful
	f	E6			A-	N		Access Not Successful
	g	E6		A+	А	N	Access Not Successful	Change to Access Limited
B-6.2	h	E6	On-Prem Branch →	A-	А	N	Access Not Successful	Keep Access
			On-Prem					
	i	E7		A+		Υ	Access Successful	
	j	E7		А	A-	Υ	Keep Access	Access Not Successful
	k	E7			A-	Υ		Access Not Successful
	1	E7		RA+		Υ	Access Successful	
	m	E7			RA-	Υ		Access Not Successful
	n	E7			А	Υ		Change to Access Limited
	0	E7		А		Υ	Change to Access Limited	
	а	E6	Branch	A+		N	Access Successful	
B-6.3	b	E6	On-Prem →	A-		N	Access Not Successful	

Demo	ID	<u>UP</u>	Location	Aut	h Stat	Rep.	Desired Outcome	Desired Outcome
			Real Hostile > RSS	Real Req	Hostile Req	Stol en	for Real Request	for Hostile Request
	c E6 On-Prem		On-Prem	А	A+	N	Change to Access Limited	Access Not Successful
	d	E6		Α	A-	N	Keep Access	Access Not Successful
	е	E6			A+	N		Access Successful
	f	E6			A-	N		Access Not Successful
	g	E6		A+	А	N	Access Not Successful	Change to Access Limited
	h	E6		A-	А	N	Access Not Successful	Keep Access
	i	E7		A+		Υ	Access Successful	
	j	E7		А	A-	Υ	Keep Access	Access Not Successful
	k	E7			A-	Υ		Access Not Successful
	I	E7		RA+		Υ	Access Successful	
	m	E7			RA-	Υ		Access Not Successful
	n	E7			А	Υ		Change to Access Limited
	0	E7		А		Υ	Change to Access Limited	
	а	E6		A+		N	Access Successful	
	b	E6	Remote	A-		N	Access Not Successful	
B-6.4	С	E6	On-Prem →	А	A+	N	Change to Access Limited	Access Not Successful
	d	E6	On-Prem	A	A-	N	Keep Access	Access Not Successful
	е	E6			A+	N		Access Successful

Demo	ID	<u>UP</u>	Location	Aut	h Stat	Rep.	Desired Outcome	Desired Outcome
			Real Hostile > RSS	Real Req	Hostile Req	Stol en	for Real Request	for Hostile Request
	f E6				A-	N		Access Not Successful
	g	E6		A+	А	N	Access Not Successful	Change to Access Limited
	h	E6		A-	А	N	Access Not Successful	Keep Access
	i	E7		A+		Υ	Access Successful	
	j	E7		А	A-	Υ	Keep Access	Access Not Successful
	k	E7			A-	Y		Access Not Successful
	I	E7		RA+		Υ	Access Successful	
	m	E7			RA-	Υ		Access Not Successful
	n	E7			А	Υ		Change to Access Limited
	0	E7		Α		Υ	Change to Access Limited	
	а	E6		A+		N	Access Successful	
	b	E6		A-		N	Access Not Successful	
	С	E6	On-Prem	Α	A+	N	Change to Access Limited	Access Not Successful
B-6.5	d	E6	Remote →	A	A-	N	Keep Access	Access Not Successful
	е	E6	On-Prem		A+	N		Access Successful
	f	E6			A-	N		Access Not Successful
	g	E6		A+	А	N	Access Not Successful	Change to Access Limited

Demo	ID	<u>UP</u>	Location	Aut	h Stat	Rep.	Desired Outcome	Desired Outcome
			Real Hostile > RSS	Real Req	Hostile Req	Stol en	for Real Request	for Hostile Request
	h	E6		A-	А	N	Access Not Successful	Keep Access
	i	E7		A+		Υ	Access Successful	
	j	E7		Α	A-	Υ	Keep Access	Access Not Successful
	k	E7			A-	Υ		Access Not Successful
	I	E7		RA+		Υ	Access Successful	
	m	E7			RA-	Υ		Access Not Successful
	n	E7			А	Υ		Change to Access Limited
	0	E7		Α		Υ	Change to Access Limited	

2.6 Use Case C: Collaboration: Federated-ID Access

591 2.6.1 Scenario C-1: Full resource access using an enterprise endpoint

- This scenario deals with a request using a successfully authenticated federated ID accessing an enterprise-controlled resource. In this scenario, the maximum access configuration of the requester for
- the enterprise-managed resource is set to full access.

- 595 **Pre-Condition:** The requestor is identified and authenticated. Per configuration, the requestor is authorized with full access to the resource.
- 597 **Demonstration:** The requestor using a federated ID will attempt to access an enterprise resource using an enterprise-owned endpoint.
- 599 **Purpose and Outcome:** This demonstration focuses on the endpoint location with endpoint/resource compliance (Compl).

601 Table 2-15 Scenario C-1 Demonstrations

Demo	ID	Req EP Compl	Req Loc	RSS EP Compl	RSS Loc	<u>Desired Outcome</u>	
	а	Υ		Υ		Access Successful	
C 1 1	b	N	On Drawn	Υ	On Drawn	Access Not Successful	
C-1.1	С	Υ	On-Prem	N	On-Prem	Access Limited	
	d	N		N		Access Not Successful	
Comment: In this set of demonstrations, the desired outcome will be to deny access to the resource							

Comment: In this set of demonstrations, the desired outcome will be to deny access to the resource in case the endpoint is not compliant. If the endpoint is compliant but the resource is not compliant, the access is restricted.

tric acc	.033	13 1 63611666	J.			
C 1 2	а	Υ	Dranch	Υ	On Drom	Access Successful
C-1.2	b	N	Branch	Υ	On-Prem	Access Not Successful
C-1.3	Α	Υ	Domoto	Υ	On-Prem	Access Successful
C-1.5	b	N	Remote	Υ	On-Prem	Access Not Successful
	а	Υ		Υ		Access Successful
C-1.4	b	N	On-Prem	Υ	Cloud	Access Not Successful
C-1.4	С	Υ	On-Prem	N		Access Limited
	d	N		N		Access Not Successful
C-1.5	а	Υ	Branch	Υ	Cloud	Access Successful
C-1.5	b	Ν	DIGITOTI	Υ	Cloud	Access Not Successful
C-1.6	а	Υ	Pomoto	Υ	Cloud	Access Successful
C-1.0	b	N	Remote	Υ	Cloud	Access Not Successful

2.6.2 Scenario C-2: Limited resource access using an enterprise endpoint

This scenario deals with a request using a successfully authenticated federated ID accessing an enterprise-controlled resource. In this scenario, the maximum access configuration of the requester for the enterprise-managed resource is set to limited access.

602

603

604

- 606 **Pre-Condition:** The requestor is identified and authenticated. Per configuration, the requestor is authorized with limited access to the resource.
- 608 **Demonstration:** The requestor using a federated ID will attempt to access an enterprise resource using an enterprise-owned endpoint.
- Purpose and Outcome: This demonstration focuses on the endpoint location with endpoint/resource compliance (Compl).

Table 2-16 Scenario C-2 Demonstrations

612

Demo	ID	Req EP Compl	Req Loc	RSS EP Compl	RSS Loc	<u>Desired Outcome</u>
	а	Υ		Υ		Access Limited
C-2.1	b	Ν	On-Prem		Access Not Successful	
C-2.1	С	Υ	On-Prem	N	On-Prem	Access Limited
	d	N		N		Access Not Successful

Comment: In this set of demonstrations, the desired outcome will be to deny access to the resource in case the endpoint is not compliant. If the endpoint is compliant but the resource is not compliant, the access is restricted.

C 2 2	а	Υ	Dranch	Υ	On Drom	Access Limited
C-2.2	b	N	Branch	Υ	On-Prem	Access Not Successful
C-2.3	а	Υ	Domoto	Υ	On-Prem	Access Limited
C-2.5	b	N	Remote	Υ	On-Prem	Access Not Successful
	а	Υ		Υ		Access Limited
C-2.4	b	N	On Drom	Υ	Cloud	Access Not Successful
C-2.4	С	Υ	On-Prem	N		Access Limited
	d	N		N		Access Not Successful
C-2.5	а	Υ	Dranch	Υ	Cloud	Access Limited
C-2.5	b	Ν	Branch	Υ	Cloud	Access Not Successful
C-2.6	а	Υ	Pomoto	Υ	Cloud	Access Limited
C-2.0	b	N	Remote	Υ	Cioud	Access Not Successful

2.6.3 Scenario C-3: Limited internet access using an enterprise endpoint

- This scenario deals with a request using a successfully authenticated federated ID accessing a non-
- enterprise-controlled resource in the public internet using an enterprise-owned endpoint device with
- 616 limited internet access.
- 617 **Pre-Condition:** The requestor is identified and authenticated. Per configuration, the requestor is
- authorized with limited access to the Internet.
- 619 **Demonstration:** The requestor using a federated ID will attempt to access two resources located in the
- 620 public Internet. The resources are not controlled by the enterprise. One resource is allowed, the other
- 621 one is blocked.
- 622 **Purpose and Outcome:** This demonstration focuses on the endpoint resource compliance with access of
- 623 non-enterprise-controlled resources on the internet by a requester with internet access using an
- 624 enterprise-controlled resource.

625 Table 2-17 Scenario C-3 Demonstrations

Demo	ID	Req EP Req Loc Compl		RSS Access RSS Loc Policy		<u>Desired Outcome</u>
	а	Υ		Allowed RSS 1	latous et	Access Successful
C-3.1	b	N	On-	Allowed RSS 1		Access Not Successful
C-3.1	С	Υ	Prem	Blocked RSS 2	Internet	Access Not Successful
	d	N		Blocked RSS 2		Access Not Successful
	а	Υ		Allowed RSS 1		Access Successful
C-3.2	b	N	Branch	Allowed RSS 1	Internet	Access Not Successful
C-3.2	С	Υ	Branch	Blocked RSS 2	internet	Access Not Successful
	d	N		Blocked RSS 2		Access Not Successful
	а	Υ		Allowed RSS 1		Access Successful
C-3.3	b	N	Domoto	Allowed RSS 1	Intornat	Access Not Successful
C-3.3	С	Υ	Remote	Blocked RSS 2	Internet	Access Not Successful
d		N		Blocked RSS 2		Access Not Successful

2.6.4 Scenario C-4: No internet access using an enterprise endpoint

- 627 This scenario deals with a request using a successfully authenticated federated ID accessing a non-
- 628 enterprise-controlled resource in the public internet using an enterprise-owned endpoint device with
- 629 internet access disabled.

- 630 **Pre-Condition:** The requestor is identified and authenticated. Per configuration, the requestor is authorized with no access to the Internet.
- 632 **Demonstration:** The requestor using a federated ID will attempt to access two resources both located in 633 the public Internet. The resources are not controlled by the enterprise. One resource is allowed, the 634 other one is blocked.
- Purpose and Outcome: This demonstration focuses on the endpoint resource compliance with access of non-enterprise-controlled resources on the internet by a requester with no internet access.

637 Table 2-18 Scenario C-4 Demonstrations

Demo	ID	Req EP Compl	Req Loc	RSS Access Policy	RSS Loc	<u>Desired Outcome</u>
	а	n Y		Allowed RSS 1		Access Not Successful
C-4.1	b	N	On-	Allowed RSS 1	lusto un ot	Access Not Successful
C-4.1	С	Υ	Prem	Blocked RSS 2	Internet	Access Not Successful
	d	N		Blocked RSS 2		Access Not Successful
	а	Υ		Allowed RSS 1		Access Not Successful
C 4 2	b	N	Duomoh	Allowed RSS 1	Internet	Access Not Successful
C-4.2	С	Υ	Branch	Blocked RSS 2		Access Not Successful
	d	N		Blocked RSS 2		Access Not Successful
	а	Υ		Allowed RSS 1		Access Not Successful
C 4 2	b	N	Domesta	Allowed RSS 1	Intornat	Access Not Successful
C-4.3	С	Υ	Remote	Blocked RSS 2	Internet	Access Not Successful
	d	N		Blocked RSS 2		Access Not Successful

2.6.5 Scenario C-5: Internet access using BYOD

638

639

640

641

- This scenario deals with a request using a successfully authenticated federated ID accessing a resource on the Internet using privately owned devices. For this scenario, it is not needed to perform additional testing depending on the access level (full, limited) towards the resource because the access level is set to be restricted due to the device being BYOD.
- Pre-Condition: The requestor is identified and authenticated. Per configuration, the requestor is
 authorized with limited access to the Internet. Both resources RSS1 and RSS2 are not managed by the
 enterprise. For example, RSS1 could be a gambling site and RSS2 could be a search engine.

650

651

652653

654

655

656

657 658

659

Demonstration: The requestor using a federated ID will attempt to access two resources both located in the public Internet. The resources are not controlled by the enterprise. One resource is allowed, the other one is blocked. The endpoint itself is of type BYOD.

Purpose and Outcome: This demonstration focuses on BYOD endpoint compliance with access of non-enterprise-controlled resources on the internet by a requester with limited internet access.

Table 2-19 Scenario C-5 Demonstrations

Demo	ID	Req EP Compl	Req Loc	RSS Access Policy	RSS Loc	<u>Desired Outcome</u>
	а	Υ		Allowed RSS 1		Access Successful
C F 1	b	N	On-	Allowed RSS 1	lunto um ot	Access Not Successful/Limited
C-5.1	C-5.1 C Y		Prem	Blocked RSS 2	Internet	Access Not Successful
	d	N		Blocked RSS 2		Access Not Successful
Comme	ent:	Compliance	e on the en	dpoint might not	be complet	tely determined.
	а	Υ		Allowed RSS 1		Access Successful
C F 3	b	N	Duonah	Allowed RSS 1		Access Not Successful/Limited
C-5.2	С	Υ	Branch	Blocked RSS 2	Internet	Access Not Successful
	d	N		Blocked RSS 2		Access Not Successful
Comme	ent:	Compliance	e on the en	dpoint might not	be complet	tely determined.
	а	Υ		Allowed RSS 1		Access Successful
0.5.3	b	N	Damata	Allowed RSS 1		Access Not Successful/Limited
C-5.3	C-5.3 c Y		Remote	Blocked RSS 2	Internet	Access Not Successful
	d	N		Blocked RSS 2		Access Not Successful
Comme	ent:	Compliance	e on the en	dpoint might not	be complet	tely determined.

2.6.6 Scenario C-6: Access resources using BYOD

This scenario deals with a request using a successfully authenticated federated ID accessing an enterprise-controlled resource using privately owned devices. For this scenario it is not needed to perform additional testing depending on the access level (full, limited) towards the resource because the access level is set to be restricted due to the device being BYOD.

Pre-Condition: The requestor is identified and authenticated. Per configuration, the requestor is authorized with full access to the resource. The system setup must lower the access level to the resource into a restricted access mode due to the usage of BYOD.

- 660 **Demonstration:** The requestor using a federated ID will attempt to access an enterprise resource using a privately owned device.
- 662 **Purpose and Outcome:** This demonstration focuses on the endpoint device (BYOD), lowering access level rights, and endpoint compliance and location.

Table 2-20 Scenario C-6 Demonstrations

664

Demo	ID	Req. EP Compl	Req. Loc	RSS EP Compl	RSS Loc	<u>Desired Outcome</u>		
	а	Υ		Υ		Access Limited		
C C 1	b	N	On-	Υ	On-	Access Not Successful		
C-6.1	С	Υ	Prem	N	Prem	Access Limited/Restricted		
	d	N		N		Access Not Successful		

Comment: In this set of demonstrations, the desired outcome will be to deny access to the resource in case the endpoint is not compliant. If the endpoint is compliant, but the resource is not compliant, the access is restricted.

15 1101 0	OIIII	Jilalit, tile a	iccess is res	tricteu.	•	_		
C-6.2	а	Υ	Branch	Υ	On-	Access Limited		
C-0.2	b	N	Dianch	Υ	Prem	Access Not Successful		
C-6.3	а	Υ	Remote	Υ	On-	Access Limited		
C-0.3	b	N	Kemote	Υ	Prem	Access Not Successful		
	а	Υ		Υ		Access Limited		
C-6.4	b	N	On-	Υ	Cloud	Access Not Successful		
C-0.4	С	Υ	Prem	N	Cloud	Access Limited/Restricted		
	d	N		N		Access Not Successful		
C C F	а	Υ	Dranch	Υ	Cloud	Access Limited		
C-6.5	р	Ν	Branch	Υ	Cloud	Access Not Successful		
C-6.6	а	Υ	Domoto	Υ	Cloud	Access Limited		
C-0.0	b	N	Remote	Υ	Cioud	Access Not Successful		

673

2.6.7 Scenario C-7: Stolen credential using an enterprise endpoint

- This scenario deals with a request using a stolen credential employing an enterprise endpoint.
- Pre-Condition: The requestor's credential is stolen and is used to attempt accessing an enterprise
 resource using an enterprise endpoint.
- Demonstration: The requestor, using a stolen federated ID, will attempt to access an enterprise
 resource using an enterprise endpoint.
- 671 **Purpose and Outcome:** This demonstration focuses on the requester's federated ID as well as the endpoint status (stolen vs. not stolen).

Table 2-21 Scenario C-7 Demonstrations

Demo	ID	Req Credential	Req Loc	Req EP	RSS Loc	Desired Outcome
	а	Active		Active		Access Successful
C-7.1	b	Active	On-Prem	Flagged Stolen	On Drawn	Access Not Successful
C-7.1	С	Flagged Stolen	On-Prem	Active	On-Prem	Access Not Successful
	d Flagged Stole			Flagged Stolen		Access Not Successful
Commo	ent:	For "Flagged Stol	en" credent	ials, MFA should	fail	
	а	Active		Active		Access Successful
C 7 2	b	Active	Branch	Flagged Stolen	On-Prem	Access Not Successful
C-7.2	C-7.2 c Flagged Stolen		Branch	Active	On-Prem	Access Not Successful
	d Flagged Stolen			Flagged Stolen		Access Not Successful
Commo	ent:	For "Flagged Stol	en" credent	ials, MFA should	fail	
	а	Active		Active		Access Successful
C-7.3	b	Active	Remote	Flagged Stolen	On-Prem	Access Not Successful
C-7.5	С	Flagged Stolen	Kemote	Active	On-Prem	Access Not Successful
	d	Flagged Stolen		Flagged Stolen		Access Not Successful
Commo	ent:	For "Flagged Stol	en" credent	ials, MFA should	fail	
	а	Active		Active		Access Successful
C-7.4	b Active		On-Prem	Flagged Stolen	Cloud	Access Not Successful
C-7.4	С	Flagged Stolen	OII-FIEIII	Active	Cloud	Access Not Successful
	d	Flagged Stolen		Flagged Stolen		Access Not Successful
Commo	ent:	For "Flagged Stol	en" credent	ials, MFA should	fail	

Demo	ID	Req Credential	Req Loc	Req EP	RSS Loc	<u>Desired Outcome</u>
	а	Active		Active		Access Successful
C-7.5	b Active			Flagged Stolen	Classal	Access Not Successful
C-7.5	С	Flagged Stolen	Branch	Active	Cloud	Access Not Successful
	d	Flagged Stolen		Flagged Stolen		Access Not Successful
Comme	ent:	For "Flagged Stol	en" credent	ials, MFA should 1	fail	
	а	Active		Active		Access Successful
C 7 C	b	Active	Domesta	Flagged Stolen	Claved	Access Not Successful
C-7.6	C-7.6 c Flagged Stolen		Remote	Active	Cloud	Access Not Successful
	d	Flagged Stolen		Flagged Stolen		Access Not Successful
Comme	ent:	For "Flagged Stol	en" credent	ials, MFA should f	fail	

2.6.8 Scenario C-8: Stolen credential using BYOD

- This scenario deals with a request using a stolen credential employing a BYOD endpoint.
- Pre-Condition: The requestor's credential is stolen and is used to attempt accessing an enterprise
 resource using a privately owned device (BYOD).
- 678 **Demonstration:** The requestor using a stolen federated ID will attempt to access an enterprise resource using a BYOD endpoint.
- Purpose and Outcome: This demonstration focuses on the requester's federated ID status (stolen vs.
- 681 not stolen).

682 Table 2-22 Scenario C-8 Demonstrations

Demo	ID	Req Credential	Req Loc	Req EP Compliance	RSS Loc	Desired Outcome			
C-8.1 a		Active	On Drom	Υ	On Drom	Access Successful			
C-8.1	b	Flagged Stolen	On-Prem	Υ	On-Prem	Access Not Successful			
		For "Flagged Stol nted access (see C		ials, MFA should 1	fail, BYOD οι	utside compliance must			
C 0 2	а	Active	Branch	Υ	On Drawn	Access Successful			
C-8.2	C-8.2 b Flagged Stolen			Υ	On-Prem	Access Not Successful			
	Comment: For "Flagged Stolen" credentials, MFA should fail, BYOD outside compliance must not be granted access (see C-5/6)								

Demo	D	Req Credential	Req Loc	Req EP Compliance	RSS Loc	Desired Outcome				
C-8.3	а	Active	Remote	Υ	On-Prem	Access Successful				
C-6.5	b	Flagged Stolen	Kemote	Υ	On-Prem	Access Not Successful				
	Comment: For "Flagged Stolen" credentials, MFA should fail, BYOD outside compliance must not be granted access (see C-5/6)									
C 0 1	а	Active	On Drom	Υ	Cloud	Access Successful				
C-8.4	b	Flagged Stolen	On-Prem	Υ	Cloud	Access Not Successful				
		For "Flagged Stol nted access (see C		ials, MFA should	fail, BYOD οι	utside compliance must				
C-8.5	а	Active	Branch	Υ	Cloud	Access Successful				
C-6.5	b	Flagged Stolen	DIGITOTI	Υ	Cloud	Access Not Successful				
		For "Flagged Stol nted access (see C		ials, MFA should	fail, BYOD οι	utside compliance must				
C 0 6	а	Active	Domoto	Υ	Cloud	Access Successful				
C-8.6	C-8.6 b Flagged Stolen Remote Y Cloud Access Not Successful									
Comment: For "Flagged Stolen" credentials, MFA should fail, BYOD outside compliance must not be granted access (see C-5/6)										

2.7 Use Case D: Other-ID Access

Demonstrations in this use case deal with different scenarios using access to enterprise resources as well as non-enterprise resources located on-premises, in the cloud, and on the internet. Each activity demonstrates the capability of authentication from within a given setting. The access is authenticated with an "other ID" using enterprise-owned endpoints (EP) as well as privately owned endpoints (BYOD). Each scenario provides a set of pre-conditions as well as multiple demonstrations.

2.7.1 Scenario D-1: Full/limited resource access using an enterprise endpoint

This scenario deals with a request using different "other-ID" profiles, one with access to all provided resources and one with access to a limited set of resources (e.g., only RSS1 but not RSS2) or with limited functionality while accessing an enterprise-controlled resource (e.g., read-only vs. read/write).

Pre-Condition: The enterprise provides multiple User accounts with different access levels. The P_FULL access profile specifies access to all resources (RSS) within the enterprise and/or access to all capabilities (CAP) of resources within the enterprise. Additionally, the P_LIMITED access profile specifies access to either a subset of the recourses and/or only limited functionality of each resource. Both endpoints' compliance (Compl) is already verified, and systems are authenticated per demonstration policy.

701

702

698 **Demonstration:** Each requestor using an "other ID" will attempt to successfully access an enterprise resource or a functionality of an enterprise resource.

Purpose and Outcome: This demonstration focuses on user privilege, authentication/re-authentication, and endpoint and RSS location, as well as the compliance of endpoints.

Table 2-23 Scenario D-1 Demonstrations

Demo	ID	<u>UP</u>	Location	Au	th St	<u>at</u>	Access	Co	mpl	Desired Outcome
			Req. > RSS	User	EP	RSS		EP	RSS	
	а	01		A+	Α	Α	RSS1	Υ	Υ	Access Successful
	b	01		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	С	01		A-	Α			Υ		Access Not Successful
	d	E2		A+	Α	Α	RSS1	Υ	Υ	Access Not Successful
	е	E2		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	f	E2		A-	Α			Υ		Access Not Successful
	g	E3		A-	Α			Υ		Access Not Successful
D-1.1	h	01	On-Prem →	RA+	Α	Α	RSS1	Υ	Υ	Access Successful
D-1.1	i	01	On-Prem	RA-	Α			Υ		Access Not Successful
	j	01		RA+	Α	Α	RSS1	N	Υ	Access Not Successful
	k	01		RA+	Α	Α	RSS2	N	Υ	Access Limited
	I	01		A+	Α	Α	RSS1	N	Υ	Access Not Successful
	m	01		A+	Α	Α	RSS2	N	Υ	Access Limited
	n	01		A+	Α	Α	RSS1	Υ	N	Access Not Successful
	О	01		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	р	E2		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	а	01		A+	Α	Α	RSS1	Υ	Υ	Access Successful
	b	01		A+	Α	Α	RSS2	Υ	Υ	Access Successful
D-1.2	С	01	Branch →	A-	Α			Υ		Access Not Successful
D-1.2	d	E2	On-Prem	A+	Α	Α	RSS1	Υ	Υ	Access Not Successful
	е	E2		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	f	E2		A-	Α			Υ		Access Not Successful

Demo	ID	<u>UP</u>	Location	<u>Au</u>	th St	at	Access	Co	mpl	Desired Outcome
			Req. > RSS	User	EP	RSS		EP	RSS	
	g	E3		A-	Α			Υ		Access Not Successful
	h	01		RA+	Α	Α	RSS1	Υ	Υ	Access Successful
	i	01		RA-	Α			Υ		Access Not Successful
	j	01		RA+	Α	Α	RSS1	N	Υ	Access Not Successful
	k	01		RA+	Α	Α	RSS2	N	Υ	Access Limited
	I	01		A+	Α	Α	RSS1	N	Υ	Access Not Successful
	m	01		A+	Α	Α	RSS2	N	Υ	Access Limited
	n	01		A+	Α	Α	RSS1	Υ	N	Access Not Successful
	0	01		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	р	E2		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	а	01		A+	Α	Α	RSS1	Υ	Υ	Access Successful
	b	01		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	С	01		A-	Α			Υ		Access Not Successful
	d	E2		A+	Α	Α	RSS1	Υ	Υ	Access Not Successful
	е	E2		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	f	E2		A-	Α			Υ		Access Not Successful
	g	E3		A-	Α			Υ		Access Not Successful
D-1.3	h	01	Remote	RA+	Α	Α	RSS1	Υ	Υ	Access Successful
D-1.5	i	01	On-Prem	RA-	Α			Υ		Access Not Successful
	j	01		RA+	Α	Α	RSS1	N	Υ	Access Not Successful
	k	01		RA+	Α	Α	RSS2	N	Υ	Access Limited
	1	01		A+	Α	Α	RSS1	N	Υ	Access Not Successful
	m	01		A+	Α	Α	RSS2	N	Υ	Access Limited
	n	01		A+	Α	Α	RSS1	Υ	N	Access Not Successful
	0	01		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	р	E2		A+	Α	Α	RSS2	Υ	N	Access Not Successful

Demo	ID	<u>UP</u>	Location	Au	th St	at_	Access	Co	mpl	Desired Outcome
			Req. > RSS	User	EP	RSS		EP	RSS	
	а	01		A+	Α	Α	RSS1	Υ	Υ	Access Successful
	b	01		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	С	01		A-	Α			Υ		Access Not Successful
	d	E2		A+	Α	Α	RSS1	Υ	Υ	Access Not Successful
	е	E2		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	f	E2		A-	Α			Υ		Access Not Successful
	g	E3		A-	Α			Υ		Access Not Successful
D 1 4	h	01	On-Prem →	RA+	Α	Α	RSS1	Υ	Υ	Access Successful
D-1.4	i	01	Cloud	RA-	Α			Υ		Access Not Successful
	j	01		RA+	Α	Α	RSS1	N	Υ	Access Not Successful
	k	01		RA+	Α	Α	RSS2	N	Υ	Access Limited
	I	01		A+	Α	Α	RSS1	N	Υ	Access Not Successful
	m	01		A+	Α	Α	RSS2	N	Υ	Access Limited
	n	01		A+	Α	Α	RSS1	Υ	N	Access Not Successful
	О	01		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	р	E2		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	а	01		A+	Α	Α	RSS1	Υ	Υ	Access Successful
	b	01		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	С	01		A-	Α			Υ		Access Not Successful
	d	02		A+	Α	Α	RSS1	Υ	Υ	Access Not Successful
	е	02		A+	Α	Α	RSS2	Υ	Υ	Access Successful
D-1.5	f	02	Branch →	A-	Α			Υ		Access Not Successful
D-1.5	g	О3	Cloud	A-	Α			Υ		Access Not Successful
	h	01		RA+	Α	Α	RSS1	Υ	Υ	Access Successful
	i	01		RA-	Α			Υ		Access Not Successful
	j	01		RA+	Α	Α	RSS1	N	Υ	Access Not Successful
	k	01		RA+	Α	Α	RSS2	N	Υ	Access Limited

Demo	ID	<u>UP</u>	Location	<u>Au</u>	th St	at_	Access	Co	mpl	Desired Outcome
			Req. > RSS	User	EP	RSS		EP	RSS	
	I	01		A+	Α	Α	RSS1	N	Υ	Access Not Successful
	m	01		A+	Α	Α	RSS2	N	Υ	Access Limited
	n	01		A+	Α	Α	RSS1	Υ	N	Access Not Successful
	О	01		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	р	02		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	а	01		A+	Α	Α	RSS1	Υ	Υ	Access Successful
	b	01		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	С	01		A-	Α			Υ		Access Not Successful
	d	02		A+	Α	Α	RSS1	Υ	Υ	Access Not Successful
	е	02		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	f	02		A-	Α			Υ		Access Not Successful
	g	О3		A-	Α			Υ		Access Not Successful
D-1.6	h	01	Remote →	RA+	Α	Α	RSS1	Υ	Υ	Access Successful
D-1.0	i	01	Cloud	RA-	Α			Υ		Access Not Successful
	j	01		RA+	Α	Α	RSS1	N	Υ	Access Not Successful
	k	01		RA+	Α	Α	RSS2	N	Υ	Access Limited
	I	01		A+	Α	Α	RSS1	N	Υ	Access Not Successful
	m	01		A+	Α	Α	RSS2	N	Υ	Access Limited
	n	01		A+	Α	Α	RSS1	Υ	N	Access Not Successful
	0	01		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	р	02		A+	Α	Α	RSS2	Υ	N	Access Not Successful

2.7.2 Scenario D-2: Full/limited internet access using an enterprise endpoint

This scenario deals with access from an enterprise-owned device to non-enterprise-managed internet resources using different enterprise ID profiles: one with access to the internet, one with limited access to the internet, and one with no access to the internet.

703

704

705

- Pre-Condition: The enterprise provides multiple user accounts with different access levels to the
 internet. The Internet access will be performed using an enterprise-owned endpoint. RSS types are OK
 for approved and not OK for not-approved internet resources. The approval depends on the user's
 policy. User endpoints are checked for compliance (Compl) per demonstration policy.
- 711 **Demonstration:** Each requestor using an enterprise-ID will attempt to successfully access a non-712 enterprise resource.
- 713 **Purpose and Outcome:** This demonstration focuses on the endpoint location as well as the resource location.

Table 2-24 Scenario D-2 Demonstrations

Demo	ID	<u>UP</u>	Location	Auth	<u>Stat</u>	Access	C	ompl	Desired Outcome
			Req. → RSS	User	EP		EP	Out of Hours	
	а	04		A+	Α	URL1	Υ	N	Access Successful
	b	04		A+	Α	URL2	Υ	N	Access Successful
	С	04		A+	Α	URL1	Υ	Υ	Access Successful
	d	04		A+	Α	URL1	Υ	Υ	Access Successful
	е	04		A-	Α		Υ		Access Not Successful
	f	05		A+	Α	URL1	Υ	N	Access Not Successful
	g	05		A+	Α	URL2	Υ	N	Access Successful
	h	05		A+	Α	URL1	Υ	Υ	Access Not Successful
D-2.1	i	05	On-Prem →	A+	Α	URL1	Υ	Υ	Access Not Successful
D-2.1	j	05	Internet	A-	Α		Υ		Access Not Successful
	k	04		RA+	Α	URL1	Υ		Access Successful
	1	04		RA-	Α		Υ		Access Not Successful
	m	04		A+	Α	URL1	N		Access Not Successful
	n	04		A+	Α	URL2	N		Access Successful
	О	05		A+	Α	URL1	N	N	Access Not Successful
	р	05		A+	Α	URL2	N	N	Access Not Successful
D-2.2	а	04	Branch	A+	Α	URL1	Υ	N	Access Successful
D-2.2	b	04	\rightarrow	A+	Α	URL2	Υ	N	Access Successful

Demo	Demo ID		Location	Auth	<u>Stat</u>	Access	C	ompl	Desired Outcome
			Req. → RSS	User	EP		EP	Out of Hours	
	С	04	Internet	A+	Α	URL1	Υ	Υ	Access Successful
	d	04		A+	Α	URL1	Υ	Υ	Access Successful
	е	04		A-	Α		Υ		Access Not Successful
	f	O5		A+	Α	URL1	Υ	N	Access Not Successful
	g	O5		A+	Α	URL2	Υ	N	Access Successful
	h	O5		A+	Α	URL1	Υ	Υ	Access Not Successful
	i	O5		A+	Α	URL1	Υ	Υ	Access Not Successful
	j	O5		A-	Α		Υ		Access Not Successful
	k	04		RA+	Α	URL1	Υ		Access Successful
	ı	04		RA-	Α		Υ		Access Not Successful
					•				
	m	04		A+	Α	URL1	N		Access Not Successful
	n	04		A+	Α	URL2	N		Access Successful
	О	O5		A+	Α	URL1	N	N	Access Not Successful
	р	O5		A+	Α	URL2	N	N	Access Not Successful
	а	04		A+	Α	URL1	Υ	N	Access Successful
	b	04		A+	Α	URL2	Υ	N	Access Successful
	С	04		A+	Α	URL1	Υ	Υ	Access Successful
	d	04		A+	Α	URL1	Υ	Υ	Access Successful
	е	04		A-	Α		Υ		Access Not Successful
	f	O5	Remote	A+	Α	URL1	Υ	N	Access Not Successful
D-2.3	g	O5	\rightarrow	A+	Α	URL2	Υ	N	Access Successful
	h	O5	Internet	A+	Α	URL1	Υ	Υ	Access Not Successful
	i	O5		A+	Α	URL1	Υ	Υ	Access Not Successful
	j	O5		A-	Α		Υ		Access Not Successful
	k	04		RA+	Α	URL1	Υ		Access Successful
	I	04		RA-	Α		Υ		Access Not Successful

Demo ID		<u>UP</u>	P Location	Auth Stat		Access	Compl		<u>Desired Outcome</u>
			Req. → RSS	User	EP		EP	Out of Hours	
	m	04		A+	Α	URL1	N		Access Not Successful
	n	04		A+	Α	URL2	N		Access Successful
	О	05		A+	Α	URL1	N	N	Access Not Successful
	р	O5		A+	Α	URL2	N	N	Access Not Successful

2.7.3 Scenario D-3: Stolen credential using BYOD or enterprise endpoint

- 717 This scenario deals with a request using a stolen credential. It does not matter if the access is performed 718 using an enterprise endpoint or BYOD device.
- 719 **Pre-Condition:** The requestor's credential is stolen and is used to attempt accessing enterprise resource
- 720 RSS1 using an enterprise endpoint. The requesting endpoint and requested resource are both in
- 721 compliance.
- 722 **Demonstration:** Two requests for the same enterprise resource from an enterprise endpoint are
- 723 performed using the same user credentials. The "Real Request" is performed using the latest
- 724 credentials, which are modified/replaced after being reported stolen, and that request can succeed. The
- "Hostile Request" is performed using a stolen enterprise ID. All authentication methods are
- 726 compromised. Re-authentication always follows a previously successful authentication.
- 727 **Purpose and Outcome:** This demonstration focuses on the detection of a stolen requester's enterprise
- 728 ID and enforcement of isolation.

729 Table 2-25 Scenario D-3 Demonstrations

Demo	Demo ID		Location	<u>Auth Stat</u>		Rep.	Desired Outcome	Desired Outcome
			Real Hostile > RSS	Real Req	Hostile Req	Stolen	for Real Request	for Hostile Request
	а	06	On-Prem On-Prem → On-Prem	A+		N	Access Successful	
	b	06		A-		N	Access Not Successful	
D-3.1	С	06		Α	A+	N	Change to Access Limited	Access Not Successful
	d	06		А	A-	N	Keep Access	Access Not Successful

Demo ID		<u>UP</u>	Location	<u>Aut</u>	h Stat	Rep.	Desired Outcome	Desired Outcome
			Real Hostile > RSS	Real Req	Hostile Req	Stolen	for Real Request	for Hostile Request
	е	06			A+	N		Access Successful
	f	06			A-	N		Access Not Successful
	g	06		A+	А	N	Access Not Successful	Change to Access Limited
	h	06		A-	А	N	Access Not Successful	Keep Access
	i	07		A+		Υ	Access Successful	
	j	07		А	A-	Υ	Keep Access	Access Not Successful
	k	07			A-	Υ		Access Not Successful
	ı	07		RA+		Υ	Access Successful	
	m	07			RA-	Υ		Access Not Successful
	n	07			А	Υ		All Sessions Terminated
	0	07		Α		Υ	All Sessions Terminated	
	а	06		A+		N	Access Successful	
	b	06		A-		N	Access Not Successful	
	С	06	On-Prem	А	A+	N	Change to Access Limited	Access Not Successful
D-3.2	d	06	Branch On-Prem	A	A-	N	Keep Access	Access Not Successful
	е	06			A+	N		Access Successful
	f	06			A-	N		Access Not Successful
	g	06		A+	А	N	Access Not Successful	Change to Access Limited

Demo	Demo ID		Location	<u>Aut</u>	h Stat	Rep.	Desired Outcome	Desired Outcome
			Real Hostile > RSS	Real Req	Hostile Req	Stolen	for Real Request	for Hostile Request
	h	06		A-	А	N	Access Not Successful	Keep Access
		ı			ı			
	i	07		A+		Υ	Access Successful	
	j	07		А	A-	Υ	Keep Access	Access Not Successful
	k	07			A-	Υ		Access Not Successful
	ı	07		RA+		Υ	Access Successful	
	m	07			RA-	Υ		Access Not Successful
	n	07			А	Υ		Change to Access Limited
	0	07		A		Υ	Change to Access Limited	
	а	06	-	A+		N	Access Successful	
	b	06		Α-		N	Access Not Successful	
	С	06		Α	A+	N	Change to Access Limited	Access Not Successful
	d	06	Branch	А	A-	N	Keep Access	Access Not Successful
D 2 2	е	06	On-Prem		A+	N		Access Successful
D-3.3	f	06	→ On-Prem		A-	N		Access Not Successful
	g	06		A+	А	N	Access Not Successful	Change to Access Limited
	h	06		A-	А	N	Access Not Successful	Keep Access
					•			
	i	07		A+		Υ	Access Successful	

Demo	Demo ID		Location	Aut	h Stat	Rep.	Desired Outcome	Desired Outcome
			Real Hostile > RSS	Real Req	Hostile Req	Stolen	for Real Request	for Hostile Request
	j	07		Α	A-	Υ	Keep Access	Access Not Successful
	k	07			A-	Υ		Access Not Successful
	I	07		RA+		Υ	Access Successful	
	m	07			RA-	Υ		Access Not Successful
	n	07			А	Υ		Change to Access Limited
	0	07		Α		Υ	Change to Access Limited	
	а	06		A+		N	Access Successful	
	b	06		A-		N	Access Not Successful	
	С	06		Α	A+	N	Change to Access Limited	Access Not Successful
	d	06		Α	A-	N	Keep Access	Access Not Successful
	е	06			A+	N		Access Successful
	f	06	Remote On-Prem		A-	N		Access Not Successful
D-3.4	g	06		A+	А	N	Access Not Successful	Change to Access Limited
	h	06	On-Prem	A-	А	N	Access Not Successful	Keep Access
	i	07		A+		Υ	Access Successful	
	j	07		А	A-	Υ	Keep Access	Access Not Successful
	k	07			A-	Υ		Access Not Successful
	I	07		RA+		Υ	Access Successful	

Demo	Demo ID		Location	Aut	h Stat	Rep.	Desired Outcome	Desired Outcome
			Real Hostile > RSS	Real Req	Hostile Req	Stolen	for Real Request	for Hostile Request
	m	07			RA-	Υ		Access Not Successful
	n	07			А	Υ		Change to Access Limited
	0	07		А		Υ	Change to Access Limited	
	а	06		A+		N	Access Successful	
	b	06		A-		N	Access Not Successful	
	С	06		А	A+	N	Change to Access Limited	Access Not Successful
	d	06		А	A-	N	Keep Access	Access Not Successful
	е	O6			A+	N		Access Successful
	f	06			A-	N		Access Not Successful
	g	06	On-Prem	A+	А	N	Access Not Successful	Change to Access Limited
D-3.5	h	06	Remote → On-Prem	A-	А	N	Access Not Successful	Keep Access
				On-Field				
	i	07		A+		Υ	Access Successful	
	j	07		А	A-	Υ	Keep Access	Access Not Successful
	k	07			A-	Υ		Access Not Successful
	1	07		RA+		Υ	Access Successful	
	m	07			RA-	Υ		Access Not Successful
	n	07			Α	Υ		Change to Access Limited

731732

733

734

735

736

737

738

739

740

741

Demo	Ō	<u>UP</u>	Location	<u>Auth Stat</u>		Rep.	Desired Outcome	Desired Outcome
			Real Hostile > RSS	Real Req	Hostile Req	Stolen	for Real Request	for Hostile Request
0		07		Α		Υ	Change to Access Limited	

2.7.4 Scenario D-4: Full/limited resource access using BYOD

This scenario deals with a request using different enterprise ID profiles, one with access to all provided resources and one with access to a limited set of resources (e.g., only RSS1 but not RSS2) or with limited functionality while accessing an enterprise-controlled resource (e.g., read-only vs. read/write). In this scenario the device used is BYOD.

Pre-Condition: The enterprise provides multiple user accounts with different access levels. The P_FULL access profile specifies access to either all resources (RSS) within the enterprise and/or all capabilities (CAP) of resources within the enterprise. Additionally, the P_LIMITED access profile specifies access to either a subset of the recourses and/or only limited functionality of each resource. Both endpoints' compliance (Compl) is already verified, and systems are authenticated per demonstration policy.

Demonstration: Each requestor using an enterprise ID will attempt to successfully access an enterprise resource or a functionality of an enterprise resource.

Purpose and Outcome: This demonstration focuses on user privilege, authentication/re-authentication, the endpoint and RSS location, as well as the compliance of endpoints.

744 Table 2-26 Scenario D-4 Demonstrations

Demo	Demo ID		<u>UP</u> Location		<u>Auth Stat</u>			Compl		<u>Desired Outcome</u>
			Req. > RSS	User	EP	RSS		EP	RSS	
	а	01		A+	Α	Α	RSS1	Υ	Υ	Access Successful
	b	01		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	С	01		A-	Α			Υ		Access Not Successful
	d	E2	On-Prem	A+	Α	Α	RSS1	Υ	Υ	Access Not Successful
D-4.1	е	E2	\rightarrow	A+	Α	Α	RSS2	Υ	Υ	Access Successful
	f	E2	On-Prem	A-	Α			Υ		Access Not Successful
	g	E3		A-	Α			Υ		Access Not Successful
	h	01		RA+	Α	Α	RSS1	Υ	Υ	Access Successful

Demo	ID	<u>UP</u>	Location	<u>A</u> ı	ıth Sta	a <u>t</u>	Access	Co	mpl	Desired Outcome
			Req. > RSS	User	EP	RSS		EP	RSS	
	i	01		RA-	Α			Υ		Access Not Successful
	j	01		RA+	Α	Α	RSS1	N	Υ	Access Not Successful
	k	01		RA+	Α	Α	RSS2	N	Υ	Access Limited
	1	01		A+	Α	Α	RSS1	N	Υ	Access Not Successful
	m	01		A+	Α	Α	RSS2	N	Υ	Access Limited
	n	01		A+	Α	Α	RSS1	Υ	N	Access Not Successful
	О	01		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	р	E2		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	а	01		A+	Α	Α	RSS1	Υ	Υ	Access Successful
	b	01		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	С	01		A-	Α			Υ		Access Not Successful
	d	02		A+	Α	Α	RSS1	Υ	Υ	Access Not Successful
	е	02		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	f	02		A-	Α			Υ		Access Not Successful
	g	E3		A-	Α			Υ		Access Not Successful
								•		
D-4.2	h	01	Branch →	RA+	Α	Α	RSS1	Υ	Υ	Access Successful
D-4.2	i	01	On-Prem	RA-	Α			Υ		Access Not Successful
	j	01		RA+	Α	Α	RSS1	N	Υ	Access Not Successful
	k	01		RA+	Α	Α	RSS2	N	Υ	Access Limited
	I	01		A+	Α	Α	RSS1	N	Υ	Access Not Successful
	m	01		A+	Α	Α	RSS2	N	Υ	Access Limited
	n	01		A+	Α	Α	RSS1	Υ	N	Access Not Successful
	0	01		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	р	02		A+	Α	Α	RSS2	Υ	N	Access Not Successful
D 4 2	а	01	Remote	A+	Α	Α	RSS1	Υ	Υ	Access Successful
D-4.3	b	01	\rightarrow	A+	Α	Α	RSS2	Υ	Υ	Access Successful

Demo	ID	<u>UP</u>	Location	<u>A</u> ı	uth Sta	a <u>t</u>	Access	Co	mpl	Desired Outcome
			Req. > RSS	User	EP	RSS		EP	RSS	
	С	01	On-Prem	A-	Α			Υ		Access Not Successful
	d	02		A+	Α	Α	RSS1	Υ	Υ	Access Not Successful
	е	02		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	f	02		A-	Α			Υ		Access Not Successful
	g	E3		A-	Α			Υ		Access Not Successful
	h	01		RA+	Α	Α	RSS1	Υ	Υ	Access Successful
	i	01		RA-	Α			Υ		Access Not Successful
	j	01		RA+	Α	Α	RSS1	N	Υ	Access Not Successful
	k	01		RA+	Α	Α	RSS2	N	Υ	Access Limited
	1	01		A+	Α	Α	RSS1	N	Υ	Access Not Successful
	m	01		A+	Α	Α	RSS2	N	Υ	Access Limited
	n	01		A+	Α	Α	RSS1	Υ	N	Access Not Successful
	О	01		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	р	02		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	а	01		A+	Α	Α	RSS1	Υ	Υ	Access Successful
	b	01		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	С	01		A-	Α			Υ		Access Not Successful
	d	02		A+	Α	Α	RSS1	Υ	Υ	Access Not Successful
	е	02		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	f	02	On-Prem	A-	Α			Υ		Access Not Successful
D-4.4	g	О3	\rightarrow	A-	Α			Υ		Access Not Successful
			Cloud							
	h	01		RA+	Α	Α	RSS1	Υ	Υ	Access Successful
	i	01		RA-	Α			Υ		Access Not Successful
	j	01		RA+	Α	Α	RSS1	N	Υ	Access Not Successful
	k	01		RA+	Α	Α	RSS2	N	Υ	Access Limited

Demo	ID	<u>UP</u>	Location	<u>A</u> ı	ıth Sta	a <u>t</u>	Access	Coi	mpl	Desired Outcome
			Req. > RSS	User	EP	RSS		EP	RSS	
	1	01		A+	Α	Α	RSS1	N	Υ	Access Not Successful
	m	01		A+	Α	Α	RSS2	N	Υ	Access Limited
	n	01		A+	Α	Α	RSS1	Υ	N	Access Not Successful
	О	01		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	р	02		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	а	01		A+	Α	Α	RSS1	Υ	Υ	Access Successful
	b	01		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	С	01		Α-	Α			Υ		Access Not Successful
	d	02		A+	Α	Α	RSS1	Υ	Υ	Access Not Successful
	е	02		A+	Α	Α	RSS2	Υ	Υ	Access Successful
	f	02		A-	Α			Υ		Access Not Successful
	g	02		A-	Α			Υ		Access Not Successful
			l		ı	ı		ı		
5.45	h	01	Branch →	RA+	Α	Α	RSS1	Υ	Υ	Access Successful
D-4.5	i	01	Cloud	RA-	Α			Υ		Access Not Successful
	j	01	Cloud	RA+	Α	Α	RSS1	N	Υ	Access Not Successful
	k	01		RA+	Α	Α	RSS2	N	Υ	Access Limited
	I	01		A+	Α	Α	RSS1	N	Υ	Access Not Successful
	m	01		A+	Α	Α	RSS2	N	Υ	Access Limited
	n	01		A+	Α	Α	RSS1	Υ	N	Access Not Successful
	О	01		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	р	02		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	а	01		A+	Α	Α	RSS1	Υ	Υ	Access Successful
	b	01		A+	Α	Α	RSS2	Υ	Υ	Access Successful
D. 4.6	С	01	Remote	A-	Α			Υ		Access Not Successful
D-4.6	d	02	→ Cloud	A+	Α	Α	RSS1	Υ	Υ	Access Not Successful
	е	02	Cloud	A+	Α	Α	RSS2	Υ	Υ	Access Successful
	f	02		A-	Α			Υ		Access Not Successful

750

751

752

Demo	ID	<u>UP</u>	Location	<u>Αι</u>	ıth Sta	<u>at</u>	Access	Compl		<u>Desired Outcome</u>
			Req. > RSS	User	EP	RSS		EP	RSS	
	g	03		A-	Α			Υ		Access Not Successful
	h	01		RA+	Α	Α	RSS1	Υ	Υ	Access Successful
	i	01		RA-	Α			Υ		Access Not Successful
	j	01		RA+	Α	Α	RSS1	N	Υ	Access Not Successful
	k	01		RA+	Α	Α	RSS2	N	Υ	Access Limited
	I	01		A+	Α	Α	RSS1	N	Υ	Access Not Successful
	m	01		A+	Α	Α	RSS2	N	Υ	Access Limited
	n	01		A+	Α	Α	RSS1	Υ	N	Access Not Successful
	0	01		A+	Α	Α	RSS2	Υ	N	Access Not Successful
	р	02		A+	Α	Α	RSS2	Υ	N	Access Not Successful

2.7.5 Scenario D-5: Full/limited internet access using BYOD

This scenario deals with access from an enterprise-owned device to non-enterprise-managed internet resources using different enterprise ID profiles: one with access to the internet, one with limited access to the internet, and one with no access to the internet.

Pre-Condition: The enterprise provides multiple user accounts with different access levels to the internet. The internet access will be performed using a BYOD endpoint. RSS types are OK for approved and not OK for not-approved internet resources. The approval depends on the user's policy. User endpoints are checked for compliance (Compl) per demonstration policy.

753 **Demonstration:** Each requestor using an enterprise ID will attempt to successfully access a non-754 enterprise resource.

Purpose and Outcome: This demonstration focuses on the endpoint location as well as the resource location.

757 Table 2-27 Scenario D-5 Demonstrations

Demo	ID	<u>UP</u>	Location	Auth	<u>Stat</u>	Access	C	ompl	Desired Outcome
			Req. > RSS	User	EP		EP	Out of	
	1							Hours	
	а	04		A+	Α	URL1	Υ	N	Access Successful
	b	04		A+	Α	URL2	Υ	N	Access Successful
	С	04		A+	Α	URL1	Υ	Υ	Access Successful
	d	04		A+	Α	URL1	Υ	Υ	Access Successful
	е	04		A-	Α		Υ		Access Not Successful
	f	O5		A+	Α	URL1	Υ	N	Access Not Successful
	g	O5		A+	Α	URL2	Υ	N	Access Successful
	h	O5		A+	Α	URL1	Υ	Υ	Access Not Successful
D F 1	i	O5	On-Prem →	A+	Α	URL1	Υ	Υ	Access Not Successful
D-5.1	j	O5	Internet	A-	Α		Υ		Access Not Successful
	k	04		RA+	Α	URL1	Υ		Access Successful
	I	04		RA-	Α		Υ		Access Not Successful
	m	04		A+	Α	URL1	N		Access Not Successful
	n	04		A+	Α	URL2	N		Access Successful
	О	05		A+	Α	URL1	N	N	Access Not Successful
	р	05		A+	Α	URL2	N	N	Access Not Successful
	а	04		A+	Α	URL1	Υ	N	Access Successful
	b	04		A+	Α	URL2	Υ	N	Access Successful
	С	04		A+	Α	URL1	Υ	Υ	Access Successful
	d	04		A+	Α	URL1	Υ	Υ	Access Successful
5.5.0	е	04	Branch	A-	Α		Υ		Access Not Successful
D-5.2	f	O5	→ Internet	A+	Α	URL1	Υ	N	Access Not Successful
	g	05	miternet	A+	Α	URL2	Υ	N	Access Successful
	h	O5		A+	Α	URL1	Υ	Υ	Access Not Successful
	i	O5		A+	Α	URL1	Υ	Υ	Access Not Successful
	j	O5		A-	Α		Υ		Access Not Successful

Demo	ID	<u>UP</u>	Location	Auth	<u>Stat</u>	Access	С	ompl	Desired Outcome
			Req. > RSS	User	EP		EP	Out of Hours	
	k	04		RA+	Α	URL1	Υ		Access Successful
	1	04		RA-	Α		Υ		Access Not Successful
	m	04		A+	Α	URL1	N		Access Not Successful
	n	04		A+	Α	URL2	N		Access Successful
	0	O5		A+	Α	URL1	N	N	Access Not Successful
	р	O5		A+	Α	URL2	N	N	Access Not Successful
	а	04		A+	Α	URL1	Υ	N	Access Successful
	b	04		A+	Α	URL2	Υ	N	Access Successful
	С	04		A+	Α	URL1	Υ	Υ	Access Successful
	d	04		A+	Α	URL1	Υ	Υ	Access Successful
	е	04		A-	Α		Υ		Access Not Successful
	f	O5		A+	Α	URL1	Υ	N	Access Not Successful
	g	O5		A+	Α	URL2	Υ	N	Access Successful
	h	O5		A+	Α	URL1	Υ	Υ	Access Not Successful
D-5.3	i	O5	Remote →	A+	Α	URL1	Υ	Υ	Access Not Successful
D-3.3	j	O5	Internet	A-	Α		Υ		Access Not Successful
	k	04		RA+	Α	URL1	Υ		Access Successful
	I	04		RA-	Α		Υ		Access Not Successful
		r			,		,	1	
	m	04		A+	Α	URL1	N		Access Not Successful
	n	04	+	A+	Α	URL2	N		Access Successful
	0	O5		A+	Α	URL1	N	N	Access Not Successful
	р	05		A+	Α	URL2	N	N	Access Not Successful

2.7.6 Scenario D-6: Stolen credential using BYOD

- This scenario deals with a request using a stolen credential. It does not matter if the access is performed using an enterprise endpoint or BYOD device.
- Pre-Condition: The requestor's credential is stolen and is used to attempt accessing enterprise resource
 RSS1 using a BYOD endpoint. The endpoints and requested resources are considered compliant.
- Demonstration: One request is performed and is successful, in parallel using the same user credentials
 from 2 separate devices to one resource. One of the requestors is using a stolen enterprise-ID will
 attempt to access an Enterprise Resource using a BYOD endpoint.
- The "Real Req" always uses the latest credentials which are modified/replaced after being reported stolen. Re-Authentication always follows a previously successful authentication.
- 768 All authentication methods are compromised
- Two requests for the same enterprise resource from at least one BYOD endpoint are performed using the same user credentials. The "Real Request" is performed using the latest credentials, which are modified/replaced after being reported stolen, and that request can succeed. The "Hostile Request" is performed using a stolen enterprise-ID. All authentication methods are compromised. Re-authentication always follows a previously successful authentication.
- Purpose and Outcome: This demonstration focuses on the detection of a stolen requester's enterprise-ID and enforcement of isolation.

776 Table 2-28 Scenario D-6 Demonstrations

Demo	ID	<u>UP</u>	Location	Aut	h Stat	Rep.	Desired Outcome	Desired Outcome
			Real Hostile > RSS	Real Req	Hostile Req	Stolen	for Real Request	for Hostile Request
	а	06		A+		N	Access Successful	
	b	06		A-		N	Access Not Successful	
D-6.1	С	06	On-Prem On-Prem	Α	A+	N	Change to Access Limited	Access Not Successful
D-0.1	d	06	→ On-Prem	А	A-	N	Keep Access	Access Not Successful
	е	06			A+	N		Access Successful
	f	06			A-	N		Access Not Successful

			Real	Auth Stat		Rep.	Desired Outcome	Desired Outcome
			Hostile > RSS	Real Req	Hostile Req	Stolen	for Real Request	for Hostile Request
	g	06		A+	А	N	Access Not Successful	Change to Access Limited
	h	O6		A-	А	N	Access Not Successful	Keep Access
					ı	ı	<u> </u>	
	i	07		A+		Υ	Access Successful	
	j	07		Α	A-	Υ	Keep Access	Access Not Successful
	k	07			A-	Υ		Access Not Successful
	I	07		RA+		Υ	Access Successful	
	m	07			RA-	Υ		Access Not Successful
	n	07			А	Υ		All Sessions Terminated
	0	07		А		Υ	All Sessions Terminated	
	а	06		A+		N	Access Successful	
	b	O6		A-		N	Access Not Successful	
	С	O6		А	A+	N	Change to Access Limited	Access Not Successful
	d	O6	On-Prem	A	A-	N	Keep Access	Access Not Successful
D-6.2	е	06	Branch		A+	N		Access Successful
	f	O6	On-Prem		A-	N		Access Not Successful
	g	O6		A+	А	N	Access Not Successful	Change to Access Limited
	h	O6		A-	А	N	Access Not Successful	Keep Access

Demo	ID	<u>UP</u>	Location	Aut	h Stat	Rep.	Desired Outcome	Desired Outcome	
			Real Hostile > RSS	Real Req	Hostile Req	Stolen	for Real Request	for Hostile Request	
	i	07		A+		Υ	Access Successful		
	j	07		Α	A-	Υ	Keep Access	Access Not Successful	
	k	07			A-	Υ		Access Not Successful	
	I	07		RA+		Υ	Access Successful		
	m	07			RA-	Υ		Access Not Successful	
	n	07			А	Υ		Change to Access Limited	
	0	07		Α		Υ	Change to Access Limited		
	а	06		A+		N	Access Successful		
	b	06	 	A-		N	Access Not Successful		
	С	06		Α	A+	N	Change to Access Limited	Access Not Successful	
	d	06		Α	A-	N	Keep Access	Access Not Successful	
	е	06			A+	N		Access Successful	
D-6.3	f	06	Branch On-Prem		A-	N		Access Not Successful	
D-0.5	g	06	→ On-Prem	A+	А	N	Access Not Successful	Change to Access Limited	
	h	06		A-	А	N	Access Not Successful	Keep Access	
		1			T	T			
	i	07		A+		Υ	Access Successful		
	j	07		A A-			Υ	Keep Access	Access Not Successful
	k	07			A-	Υ		Access Not Successful	

Demo	ID	<u>UP</u>	Location	Aut	h Stat	Rep.	Desired Outcome	Desired Outcome
			Real Hostile > RSS	Real Req	Hostile Req	Stolen	for Real Request	for Hostile Request
	I	07		RA+		Υ	Access Successful	
	m	07			RA-	Υ		Access Not Successful
	n	07			А	Υ		Change to Access Limited
	0	07		Α		Υ	Change to Access Limited	
	а	06		A+		N	Access Successful	
	b	06		A-		N	Access Not Successful	
	С	06		Α	A+	N	Change to Access Limited	Access Not Successful
	d	06		А	A-	N	Keep Access	Access Not Successful
	е	06			A+	N		Access Successful
	f	06			A-	N		Access Not Successful
	g	06	Remote	A+	А	N	Access Not Successful	Change to Access Limited
D-6.4	h	06	On-Prem → On-Prem	A-	А	N	Access Not Successful	Keep Access
			On Frem		T			
	i	07		A+		Υ	Access Successful	
	j	07		А	A-	Υ	Keep Access	Access Not Successful
	k	07			A-	Υ		Access Not Successful
	I	07		RA+		Υ	Access Successful	
	m	07			RA-	Υ		Access Not Successful
	n	07			А	Υ		Change to Access Limited

Demo ID		<u>UP</u>	Location	<u>Aut</u>	h Stat	Rep.	Desired Outcome	Desired Outcome
			Real Hostile > RSS	Real Req	Hostile Req	Stolen	for Real Request	for Hostile Request
	0	07		А		Υ	Change to Access Limited	
	а	06		A+		N	Access Successful	
	b	06		A-		N	Access Not Successful	
	С	06		Α	A+	N	Change to Access Limited	Access Not Successful
	d	06		А	A-	N	Keep Access	Access Not Successful
	е	06			A+	N		Access Successful
	f	06	On-Prem Remote		A-	N		Access Not Successful
	g	06		A+	А	N	Access Not Successful	Change to Access Limited
D-6.5	h	06		A-	A	N	Access Not Successful	Keep Access
	·		→ On-Prem					
	i	07		A+		Υ	Access Successful	
	j	07		А	A-	Υ	Keep Access	Access Not Successful
	k	07			A-	Y		Access Not Successful
	I	07		RA+		Υ	Access Successful	
	m	07			RA-	Y		Access Not Successful
	n	07			А	Y		Change to Access Limited
	О	07		А		Υ	Change to Access Limited	

2.8 Use Case E: Guest: No-ID Access

2.8.1 Scenario E-1: Guest requests public internet access

- 779 For No-ID access, the only deciding factor is the type of device used and any known compliance state of
- 780 the device. Authentication/authorization is not a factor (No-ID). Enterprise resource compliance is
- 781 likewise assumed, as resources would not be visible otherwise.
- 782 **Pre-Condition:** The requestor does not need to authenticate (i.e., guest access). Per configuration, the
- 783 requestor is authorized with default universal access to the resource (i.e., no authentication or
- authorization checks are performed). A request to access the enterprise resource is granted and a
- session is established. The resource is assumed to be in compliance.
- 786 **Demonstration:** Systems can differentiate between device classifications and perform some action
- 587 based on policy to restrict privileged devices (i.e., enterprise-managed, BYOD) based on endpoint
- 788 compliance policy.
- 789 **Purpose and Outcome:** This demonstration focuses on device identification and compliance (when
- 790 applicable).

792

793

777

791 Table 2-29 Scenario E-1 Demonstrations

Demo	Demo ID Locati Subject		Access	Desired Outcome	
E-1.1	а	On Drom	Public resource	Access Successful	
E-1.1	b On-Prem		Public internet	Access Successful	
E-1.2	а	Dronoh	Public resource	Access Successful	
E-1.Z	b	Branch	Public internet	Access Successful	

2.9 Use Case F: Confidence Level

2.9.1 Scenario F-1: User reauthentication fails during active session

- This scenario is based on a successful request with an established session to an enterprise resource
- 795 using an enterprise-owned endpoint. The requestor's reauthentication will fail, reducing the confidence
- 796 level. This leads to terminating the active session.

- Pre-Condition: The requestor is identified and authenticated. Per configuration, the requestor is
 authorized with full access to the resource. A request to access the enterprise resource is granted and a
 session is established.
- 800 **Demonstration:** The reauthentication of the requestor fails, and the session will be terminated.
- Purpose and Outcome: This demonstration focuses on the requester's identification, which fails reauthentication during an active session.

Table 2-30 Scenario F-1 Demonstrations

803

804

805

806

807 808

Demo	ID	Re-auth	Req Loc	RSS Loc	<u>Desired Outcome</u>	
F-1.1	а	Passes	On-Prem	0 0	Session stays active	
F-1.1	b	Fails	On-Prem	On-Prem	Session will be terminated	
F-1.2	а	Passes	Branch	On-Prem	Session stays active	
Γ-1.2	b	Fails	DIGITOTI	On-Prem	Session will be terminated	
F-1.3	а	Passes	Remote	On-Prem	Session stays active	
r-1.5	b	Fails	Kemote		Session will be terminated	
F-1.4	а	Passes	On-Prem	Cloud	Session stays active	
Γ-1.4	b	Fails	Oli-Pielli		Session will be terminated	
F-1.5	а	Passes	Branch	Cloud	Session stays active	
F-1.5	b	Fails	DIGITOTI	Cloud	Session will be terminated	
F-1.6	а	Passes	Remote	Cloud	Session stays active	
L-1.0	b	Fails	remote	Ciouu	Session will be terminated	

2.9.2 Scenario F-2: Requesting endpoint reauthentication fails during active session

This scenario is based on a successful request with an established session to an enterprise resource using an enterprise-owned endpoint. The reauthentication of the requesting endpoint will fail, reducing the confidence level. This leads to terminating the active session.

- 809 Pre-Condition: The requestor is identified and authenticated. Per configuration, the requestor is 810 authorized with full access to the resource. A request to access the enterprise resource is granted and a 811 session is established.
- 812 Demonstration: The reauthentication of the requestor's endpoint fails, and the session will be 813 terminated.
- Purpose and Outcome: This demonstration focuses on the requester's endpoint identification, which 814 815 fails re-authentication during an active session.

816 Table 2-31 Scenario F-2 Demonstrations

Demo	ID	Re-auth	Req. Loc	RSS Loc	<u>Desired Outcome</u>		
F-2.1	а	Passes	On-Prem	0 0	Session stays active		
F-2.1	b	Fails	On-Prem	On-Prem	Session will be terminated		
F-2.2	а	Passes	Branch	On-Prem	Session stays active		
Γ-Ζ.Ζ	b	Fails	Didilcii	On-Prem	Session will be terminated		
F-2.3	а	Passes	Remote	On-Prem	Session stays active		
F-2.5	b	Fails	Kemote	On-Prem	Session will be terminated		
F-2.4	а	Passes	On-Prem	Cloud	Session stays active		
F-2.4	b	Fails	On-Prem		Session will be terminated		
F 2 F	а	Passes	Duamah	Clavel	Session stays active		
F-2.5	b	Fails	Branch	Cloud	Session will be terminated		
F-2.6	а	Passes	Dometo	Claud	Session stays active		
F-2.0	b	Fails	Remote	Cloud	Session will be terminated		

2.9.3 Scenario F-3: Resource reauthentication fails during active session

818 This scenario is based on a successful request with an established session to an enterprise resource. The reauthentication of the resource will fail, reducing the confidence level. This leads to terminating the 820 active session.

817

819

- **Pre-Condition:** The requestor is identified and authenticated. Per configuration, the requestor is
- authorized with full access to the resource. A request to access the enterprise resource is granted and a
- session is established.

828

829

830

831

- **Demonstration:** The reauthentication of the resource fails, and the session will be terminated.
- 825 **Purpose and Outcome:** This demonstration focuses on the resource identification, which fails re-
- authentication during an active session.

Table 2-32 Scenario F-3 Demonstrations

Demo	ID	Re-auth	Req. Loc	RSS Loc	Desired Outcome	
F-3.1	а	Passes	On-Prem	0 0	Session stays active	
F-3.1	b	Fails	On-Prem	On-Prem	Session will be terminated	
F-3.2	а	Passes	Branch	On-Prem	Session stays active	
F-3.2	b	Fails	Branch	On-Prem	Session will be terminated	
F 2 2	а	Passes	Damata	On-Prem	Session stays active	
F-3.3	b	Fails	Remote	On-Prem	Session will be terminated	
F-3.4	а	Passes	On-Prem	Cloud	Session stays active	
r-3.4	b	Fails	On-Prem		Session will be terminated	
F 2 F	а	Passes	Duranah		Session stays active	
F-3.5	b	Fails	Branch	Cloud	Session will be terminated	
F 2.6	а	Passes	Dometo	Claud	Session stays active	
F-3.6	b	Fails	Remote	Cloud	Session will be terminated	

2.9.4 Scenario F-4: Compliance fails during active session

This scenario is based on a successful request with an established session to an enterprise resource using an enterprise-owned endpoint. The endpoint will fall out of compliance, reducing the confidence level. This terminates the session.

836

837

838

839

840

Pre-Condition: The requestor is identified and authenticated. The endpoint used is tested and considered compliant. A request to access the enterprise resource is granted and a session is established.

Demonstration: The requesting endpoint falls out of policy (becomes not compliant), and the session will be terminated. The requesting endpoint is either enterprise-owned or BYOD. It cannot be a guest endpoint for these demonstrations.

Purpose and Outcome: This demonstration focuses on the requester's endpoint compliance, which changes from compliant to not compliant during an active session.

Table 2-33 Scenario F-4 Demonstrations

Demo ID		Req EP Compl	Req Loc	RSS Loc	<u>Desired Outcome</u>		
F-4.1	а	Υ	On-Prem	On-Prem	Session stays active		
F-4.1	b	N	On-Prem	On-Prem	Session will be terminated		
F-4.2	а	Υ	Branch	On-Prem	Session stays active		
F-4.Z	b	N	Branch	On-Prem	Session will be terminated		
F-4.3	а	Υ	Remote	0 . 5	Session stays active		
F-4.5	b	N	Kemote	On-Prem	Session will be terminated		
F-4.4	а	Υ	On-Prem	Cloud	Session stays active		
Г -4.4	b	N	Oll-Fielli		Session will be terminated		
F-4.5	а	Υ	Branch	Cloud	Session stays active		
r-4.5	b	N	Dialicii	Cloud	Session will be terminated		
F-4.6	а	Υ	Remote	Cloud	Session stays active		
1-4.0	b	N	Remote	Cloud	Session will be terminated		

845

846

847848

2.9.5 Scenario F-5: Compliance improves between requests

This scenario is the inverse of scenario F-4. Here, there is an initial rejection due to compliance issues, followed by a mitigation that improves the confidence level. Then a repeat request will be successful and establish a session to an enterprise resource.

Pre-Condition: The requestor is identified and could be authenticated, depending on when authentication takes place in the process. The endpoint used is tested and initially considered noncompliant. The endpoint then improves its compliance status and the request is re-issued. A request to access the enterprise resource is granted and a session is established.

Demonstration: The requesting endpoint is initially out of policy (not compliant) but can remediate the issue and is successful in a repeated request for the same resource.

Purpose and Outcome: This demonstration focuses on the requester's endpoint compliance, which changes from not compliant to compliant before fully establishing a session.

853 Table 2-34 Scenario F-5 Demonstrations

Demo ID		Req EP Compl	Req Loc	RSS Loc	<u>Desired Outcome</u>
F-5.1	а	N	On-Prem	On-Prem	Access Not Successful
F-3.1	b	Υ	Oll-Pielli	Oll-Fielli	Access Successful
F-5.2	а	N	Branch	On-Prem	Access Not Successful
F-3.2	b	Υ	Dialicii	Oll-Fielli	Access Successful
F-5.3	а	N	Remote	On-Prem	Access Not Successful
F-5.5	b	Υ	Kemote		Access Successful
F-5.4	а	N	On-Prem	Cloud	Access Not Successful
F-3.4	b	Υ	On-Prem		Access Successful
F-5.5	а	N	Branch	Cl. I	Access Not Successful
F-3.5	р	Υ	Didilcii	Cloud	Access Successful
	а	N	Remote	Cloud	Access Not Successful
F-5.6	b	Υ	Remote	Cloud	Access Successful

Demo ID	Req EP Compl	Req Loc	RSS Loc	<u>Desired Outcome</u>

3 Functional Demonstration Results

3.1 EIG Crawl Phase Demonstration Results

This section lists the demonstration results for each of the builds that was implemented as part of the EIG crawl phase, as defined in NIST SP 1800-35B: Approach, Architecture, and Security Characteristics.

3.1.1 Enterprise 1 Build 1 (E1B1) Demonstration Results

Table 3-1 lists the results for all EIG crawl phase demonstrations run in Enterprise 1 Build 1 (E1B1). While the technology deployed in E1B1 was able to determine endpoint compliance for mobile devices and prevent noncompliant mobile endpoints from accessing resources, it was not able to determine the compliance status of desktop endpoints and automatically use that as a determining factor in deciding whether access requests originating from that desktop endpoint should be granted. Consequently, the results listed in this section only include demonstrations in which the requesting endpoints are mobile devices. No demonstrations were performed in which the requesting device was a desktop system. In all demonstrations that were conducted, the ZTA functionality included in the build performed as expected.

Table 3-1 Demonstration Results for E1B1 EIG Crawl Phase

Demo ID	Expected Outcome	Observed Outcome	Comments
A-1.1.a-m	N/A	N/A	Demonstration cannot be completed. There is no network-level enforcement present in this build. All devices are already joined to the network. There is no tool that can keep any entity (RSS, EP, BYOD, or guest device) from joining the network based on its authentication status.
A-1.2.a-m	N/A	N/A	Demonstration cannot be completed. There is no network-level enforcement present in this build.
A-1.3.a-f	N/A	N/A	Demonstration cannot be completed. There is no network-level enforcement present in this build.
A-1.4.a-g	N/A	N/A	Cloud-based resources are out of scope until the run phase.
A-2.1.a-i	N/A	N/A	Demonstration cannot be completed. There is no network-level enforcement present in this build.

Demo ID	Expected Outcome	Observed Outcome	Comments
			There is no tool that can reauthenticate any entity (RSS, EP, BYOD, or guest device) and terminate its network access based on authentication status.
A-2.2.a-i	N/A	N/A	Demonstration cannot be completed. There is no network-level enforcement present in this build based on reauthentication status.
A-2.3.a-f	N/A	N/A	Demonstration cannot be completed. There is no network-level enforcement present in this build based on reauthentication status.
A-2.4.a-f	N/A	N/A	Cloud-based resources are out of scope until the run phase.
A-3.1.a, A-3.3.a, A-3.5.a	User request and action is recorded	User login to an applicatio n is logged	Success: Okta records the authentication logs. Administrators can log in to Okta and view logs of when a user logged onto an application and whether the authentication was successful or not.
A-3.1.b, A-3.3.b	API call is recorded	Logs contain relevant API informatio n	Success: Okta logs have relevant information about the authentication between the user and resource.
A-3.2.a-b, A-3.4.a-b, A-3.6.a	N/A	N/A	Cloud-based resources are out of scope until the run phase.
B-1.1.a, B-1.2.a, B- 1.3.a, B-4.1.a, B- 4.2.a, B-4.3.a, D- 1.1.a, D-1.2.a, D- 1.3.a, D-4.1.a, D- 4.2.a, D-4.3.a	Access Successful	Access Successful	Partial success: For the mobile endpoint, user access to resource RSS1 is based on endpoint compliance. However, we cannot validate compliance of RSS1.
B-1.1.b, B-1.2.b, B- 1.3.b, B-4.1.b, B- 4.2.b, B-4.3.b, D- 1.1.b, D-1.2.b, D- 1.3.b, D-4.1.b, D- 4.2.b, D-4.3.b	Access Successful	Access Successful	Partial success: For the mobile endpoint, user access to resource RSS1 is based on endpoint compliance. However, we cannot validate compliance of RSS2.

Demo ID	Expected Outcome	Observed Outcome	Comments
B-1.1.c, B-1.2.c, B- 1.3.c, B-4.1.c, B- 4.2.c, B-4.3.c, D- 1.1.c, D-1.2.c, D- 1.3.c, D-4.1.c, D- 4.2.c, D-4.3.c	Access Not Successful	Access Not Successful	Partial success: Demonstrated user authentication failure at the mobile endpoint, but we cannot validate compliance on RSS1. Partial demonstration completed with user not able to log in to mobile device.
B-1.1.d, B-1.2.d, B- 1.3.d, B-4.1.d, B- 4.2.d, B-4.3.d, D- 1.1.d, D-1.2.d, D- 1.3.d, D-4.1.d, D- 4.2.d, D-4.3.d	Access Not Successful	Access Not Successful	Partial success: Mobile: Based on configuration in Ent1, the E2 is not authorized to access RSS1 based on enterprise governance policy. Also, RSS compliance cannot be demonstrated in this phase. In this case, user is not granted access to RSS1.
B-1.1.e, B-1.2.e, B- 1.3.e, B-4.1.e, B- 4.2.e, B-4.3.e, D- 1.1.e, D-1.2.e, D- 1.3.e, D-4.1.e, D- 4.2.e, D-4.3.e	Access Successful	Access Successful	Partial success: Mobile: User access to RSS2 is based on the EP's compliance. Cannot validate compliance on RSS2. Partial demonstration.
B-1.1.f, B-1.2.f, B- 1.3.f, B-4.1.f, B-4.2.f, B-4.3.f, D-1.1.f, D- 1.2.f, D-1.3.f, D- 4.1.f, D-4.2.f, D-4.3.f	Access Not Successful	Access Not Successful	Partial success: Mobile: User authentication failure is at the endpoint. Cannot validate compliance on RSS1. Partial demonstration completed with user not able to log in to mobile device.
B-1.1.g, B-1.2.g, B- 1.3.g, B-4.1.g, B- 4.2.g, B-4.3.g, D- 1.1.g, D-1.2.g, D- 1.3.g, D-4.1.g, D- 4.2.g, D-4.3.g	Access Not Successful	N/A	Demonstration cannot be completed. Mobile: must have certain tools installed to manage the mobile device and its compliance. The only way this happens is if the user forgets the login password on the mobile device.
B-1.1.h, B-1.2.h, B- 1.3.h, B-4.1.h, B- 4.2.h, B-4.3.h, D- 1.1.h, D-1.2.h, D- 1.3.h, D-4.1.h, D- 4.2.h, D-4.3.h	Access Successful	Access Successful	Success: GitLab session timeout is set to one minute for demonstration purposes. After session timed out, user was re-authenticated.
B-1.1.i, B-1.2.i, B- 1.3.i, B-4.1.i, B-4.2.i, B-4.3.i, D-1.1.i, D-	Access Not Successful	N/A	Success: Only way to do this is to not use Okta FastPass, which would make this case invalid. We

Demo ID	Expected	Observed	Comments
1.2.i, D-1.3.i, D-4.1.i, D-4.2.i, D-4.3.i	Outcome	Outcome	pressed "No" on Okta FastPass and access was denied.
B-1.1.j, B-1.2.j, B- 1.3.j, B-4.1.j, B-4.2.j, B-4.3.j, D-1.1.j, D- 1.2.j, D-1.3.j, D-4.1.j, D-4.2.j, D-4.3.j	Access Not Successful	Access Not Successful	Success: On Ivanti, after initial authentication, implemented a block on the Mobile Iron cloud. After GitLab timed out, re-authentication was unsuccessful.
B-1.1.k, B-1.2.k, B- 1.3.k, B-4.1.k, B- 4.2.k, B-4.3.k, D- 1.1.k, D-1.2.k, D- 1.3.k, D-4.1.k, D- 4.2.k, D-4.3.k	Access Limited	N/A	Partial success: Access to RSS2 is blocked. Currently cannot perform limited access.
B-1.1.l-m, B-1.2.l-m, B-1.3.l-m, B-4.1.l-m, B-4.2.l-m, B-4.3.l-m, D-1.1.l-m, D-1.2.l-m, D-1.3.l-m, D-4.1.l-m, D-4.2.l-m, D-4.3.l-m	Access Denied	Access Denied	Success: User was denied access because the endpoint was non-compliant.
B-1.1.n-p, B-1.2.n-p, B-1.3.n-p, B-4.1.n-p, B-4.2.n-p, B-4.3.n-p, D-1.1.n-p, D-1.2.n-p, D-1.3.n-p, D-4.1.n-p, D-4.2.n-p, D-4.3.n-p	N/A	N/A	Demonstration cannot be run. Unable to perform compliance checks on RSS.
B-1.2.a-p			The results are the same as B-1.1 since network policies allow access from branch to Ent1. See results from B-1.1.
B-1.3.a-p			The results are the same as B-1.1 given that network policies allow the user/device to access the enterprise remotely using a VPN connection. See results from B-1.1.
B-1.4.a-p, B-1.5.a-p, B-1.6.a-p, B-4.4.a-p, B-4.5.a-q, and B- 4.6.a-p	N/A	N/A	Cloud-based resources are out of scope until run phase.

Demo ID	Expected Outcome	Observed Outcome	Comments
B-2.1.a-p, B-2.2.a-p, B-5	N/A	N/A	Out of scope until run phase. Tools are needed to create policies to allow or deny access to internet resources.
B-3, B-6	N/A	N/A	Out of scope until run phase.
B-4			As documented in the rows above, the results of all B-4 use case demonstrations are the same as the results of the B-1 use cases because the device is both authenticated and compliant. In this case, a BYOD device will have to install both the Ivanti Neurons for UEM agent and Okta Verify App. See results from B-1.1 for B-4.1, B-4.2, and B-4.3.
All C Use Cases	N/A	N/A	Demonstrations cannot be performed. Currently, no federation configuration has been set up between Ent1, Ent2, and Ent3.
All D Use Cases			As documented in the rows above, the results of all D use case demonstrations are the same as the results of the B use cases. Note that the user is a contractor and will have access to resources based on need. The Ivanti Neurons for UEM agent and Okta Verify App will have to be installed on the contractor's device, whether it's provided by the enterprise or BYOD.
All E Use Cases	N/A	N/A	Guest (No-ID) access is considered out of scope for the EIG crawl phase.
All F Use Cases	N/A	N/A	Confidence level use cases are considered out of scope for the EIG crawl phase.

3.1.2 Enterprise 2 Build 1 (E2B1) Demonstration Results

<u>Table</u> 3-2 lists the results for all EIG crawl phase demonstrations run in Enterprise 2 Build 1 (E2B1). In all demonstrations that we attempted to conduct, the ZTA functionality included in the build performed as expected. The technology deployed in E2B1 was able to determine endpoint compliance for Android, iOS, Windows, and Mac devices and prevent noncompliant endpoints from accessing private resources. Consequently, compliance of endpoints was observed with health checks from Duo prior to the second-factor authentication.

Table 3-2 Demonstration Results for E2B1 EIG Crawl Phase

Demo ID	Expected	Observed	Comments
	Outcome	Outcome	
A-1.1.a-m	N/A	N/A	Demonstration cannot be completed. There is no network-level enforcement present in this build. All devices are already joined to the network. There is no tool that can keep any entity (RSS, EP, BYOD, or guest device) from joining the network based on its authentication status.
A-1.2.a-m, A-1.3.a-f	N/A	N/A	Demonstration cannot be completed. There is no network-level enforcement present in this build.
A-1.4.a-g	N/A	N/A	Cloud-based resources are out of scope until the run phase.
A-2.1.a-i	N/A	N/A	Demonstration cannot be completed. There is no network-level enforcement present in this build. There is no tool that can reauthenticate any entity (RSS, EP, BYOD, or guest device) and terminate its network access based on authentication status.
A-2.2.a-I, A-2.3.a-f	N/A	N/A	Demonstration cannot be completed. There is no network-level enforcement present in this build based on reauthentication status.
A-2.4.a-f	N/A	N/A	Cloud-based resources are out of scope until the run phase.
A-3.1.a, A-3.3.a, A-3.5.a	User request and action is recorded	User login to an applicatio n is logged	Success: Duo records the authentication logs. Administrators can log in to Duo and view logs of when a user logged onto an application and whether the authentication was successful or not.
A-3.1.b, A-3.3.b	API call is recorded	Logs contain relevant API informatio n	Success: Duo logs have relevant information about the authentication between the user and resource.
A-3.2.a-b, A-3.4.a-b, A-3.6.a	N/A	N/A	Cloud-based resources are out of scope until the run phase.
B-1.1.a, B-1.2.a, B- 1.3.a, B-4.1.a, B-	Access Successful	Access Successful	Partial success: User access to resource RSS1 is based on endpoint compliance. Users much have

Demo ID	Expected Outcome	Observed Outcome	Comments
4.2.a, B-4.3.a, D- 1.1.a, D-1.2.a, D- 1.3.a, D-4.1.a, D- 4.2.a, D-4.3.a			Duo client installed on device for health check. Users also must have Duo Mobile installed on a mobile device to perform second-factor authentication. However, we cannot validate compliance of RSS1 so we label this "partial success".
B-1.1.b, B-1.2.b, B- 1.3.b, B-4.1.b, B- 4.2.b, B-4.3.b, D- 1.1.b, D-1.2.b, D- 1.3.b, D-4.1.b, D- 4.2.b, D-4.3.b	Access Successful	Access Successful	Partial success due to scope: User access to resource RSS2 is based on endpoint compliance. However, we cannot validate compliance of RSS2.
B-1.1.c, B-1.2.c, B- 1.3.c, B-4.1.c, B- 4.2.c, B-4.3.c, D- 1.1.c, D-1.2.c, D- 1.3.c, D-4.1.c, D- 4.2.c, D-4.3.c	Access Not Successful	Access Not Successful	Partial success: Demonstrated user authentication failure at the endpoint, but we cannot validate compliance on RSS1. Partial demonstration completed with user not able to log in to RSS1 due to incorrect credentials.
B-1.1.d, B-1.2.d, B- 1.3.d, B-4.1.d, B- 4.2.d, B-4.3.d, D- 1.1.d, D-1.2.d, D- 1.3.d, D-4.1.d, D- 4.2.d, D-4.3.d	Access Not Successful	Access Not Successful	Partial success: Based on configuration in Ent2, the E2 is not authorized to access RSS1 based on enterprise governance policy. Also, RSS compliance cannot be demonstrated in this phase. In this case, user is not granted access to RSS1.
B-1.1.e, B-1.2.e, B- 1.3.e, B-4.1.e, B- 4.2.e, B-4.3.e, D- 1.1.e, D-1.2.e, D- 1.3.e, D-4.1.e, D- 4.2.e, D-4.3.e	Access Successful	Access Successful	Partial success: User access to RSS2 is based on the EP's compliance. Cannot validate compliance on RSS2. Partial demonstration.
B-1.1.f, B-1.2.f, B- 1.3.f, B-4.1.f, B-4.2.f, B-4.3.f, D-1.1.f, D- 1.2.f, D-1.3.f, D- 4.1.f, D-4.2.f, D-4.3.f	Access Not Successful	Access Not Successful	Partial success: User authentication failure is at the endpoint. Cannot validate compliance on RSS1. Partial demonstration completed with user not able to log in from device.
B-1.1.g, B-1.2.g, B- 1.3.g, B-4.1.g, B- 4.2.g, B-4.3.g, D- 1.1.g, D-1.2.g, D-	Access Not Successful	N/A	Demonstration cannot be completed. Must have certain tools installed to manage the mobile device and its compliance. The only way this happens is if

Demo ID	Expected Outcome	Observed Outcome	Comments
1.3.g, D-4.1.g, D- 4.2.g, D-4.3.g			the user forgets the login password on the mobile device.
B-1.1.h, B-1.2.h, B- 1.3.h, B-4.1.h, B- 4.2.h, B-4.3.h, D- 1.1.h, D-1.2.h, D- 1.3.h, D-4.1.h, D- 4.2.h, D-4.3.h	Access Successful	Access Successful	Success: GitLab session timeout is set to one minute for demonstration purposes. After session timed out, user was re-authenticated.
B-1.1.i, B-1.2.i, B- 1.3.i, B-4.1.i, B-4.2.i, B-4.3.i, D-1.1.i, D- 1.2.i, D-1.3.i, D-4.1.i, D-4.2.i, D-4.3.i	Access Not Successful	Access Not Successful	Success: Only way to do this is to put in a wrong password for failure.
B-1.1.j, B-1.2.j, B- 1.3.j, B-4.1.j, B-4.2.j, B-4.3.j, D-1.1.j, D- 1.2.j, D-1.3.j, D-4.1.j, D-4.2.j, D-4.3.j	Access Not Successful	Access Not Successful	Success: On Duo, implemented a block on devices that do not have firewall enabled. After GitLab timed out, we turned off the firewall on the device and reauthentication was unsuccessful.
B-1.1.k, B-1.2.k, B- 1.3.k, B-4.1.k, B- 4.2.k, B-4.3.k, D- 1.1.k, D-1.2.k, D- 1.3.k, D-4.1.k, D- 4.2.k, D-4.3.k	Access Limited	N/A	Partial success: Access to RSS2 is blocked if EP is not compliant. Currently cannot perform limited access.
B-1.1.l-m, B-1.2.l-m, B-1.3.l-m, B-4.1.l-m, B-4.2.l-m, B-4.3.l-m, D-1.1.l-m, D-1.2.l-m, D-1.3.l-m, D-4.1.l-m, D-4.2.l-m, D-4.3.l-m	Access Denied	Access Denied	Success: User was denied access because the endpoint was non-compliant.
B-1.1.n-p, B-1.2.n-p, B-1.3.n-p, B-4.1.n-p, B-4.2.n-p, B-4.3.n-p, D-1.1.n-p, D-1.2.n-p, D-1.3.n-p, D-4.1.n-p, D-4.2.n-p, D-4.3.n-p	N/A	N/A	Demonstration cannot be run. Unable to perform compliance checks on RSS.
B-1.2.a-p			The results would be the same as B-1.1 since network policies allow access from a branch office to

Demo ID	Expected Outcome	Observed Outcome	Comments
	Outcome	Outcome	Ent2. See results from B-1.1. (Note: Ent2 does not have a branch office. If we were to create a branch office, the network policies will allow the branch office to Ent2. Therefore, it would be part of the Ent2 policies and results would be identical to B-1.1.)
B-1.3.a-p			The results are the same as B-1.1, given that network policies allow the user/device to access the enterprise remotely using a VPN connection. See results from B-1.1.
B-1.4.a-p, B-1.5.a-p, B-1.6.a-p, B-4.4.a-p, B-4.5.a-q, and B- 4.6.a-p	N/A	N/A	Cloud-based resources are out of scope until run phase.
B-2.1.a-p, B-2.2.a-p, B-5	N/A	N/A	Out of scope until run phase. Tools are needed to create policies to allow or deny access to internet resources.
B-3, B-6	N/A	N/A	Out of scope until run phase.
B-4			As documented in the rows above, the results of all B-4 use case demonstrations are the same as the results of the B-1 use cases because the device is both authenticated and compliant. In this case, a BYOD device will have to install Duo client for health check. See results from B-1.1 for B-4.1, B-4.2, and B-4.3.
All C Use Cases	N/A	N/A	Demonstrations cannot be performed. Currently, no federation configuration has been set up between Ent1, Ent2, and Ent3.
All D Use Cases			As documented in the rows above, the results of all D use case demonstrations are the same as the results of the B use cases. Note that the user is a contractor and will have access to resources based on need. The Duo client will have to be installed on the contractor's device, whether it's provided by the enterprise or BYOD. User must also install Duo Mobile on their mobile device for second-factor authentication.

Demo ID	Expected Outcome	Observed Outcome	Comments
All E Use Cases	N/A	N/A	Guest (No-ID) access is considered out of scope for the EIG crawl phase.
All F Use Cases	N/A	N/A	Confidence level use cases are considered out of scope for the EIG crawl phase.

3.1.3 Enterprise 3 Build 1 (E3B1) Demonstration Results

<u>Table</u> 3-3 lists the demonstration results for all EIG crawl phase demonstrations run in Enterprise 3 Build 1 (E3B1). In all demonstrations that we attempted to conduct, the ZTA functionality included in the build performed as expected. The technology deployed in E3B1 was able to determine endpoint compliance for Android, iOS, Windows, and Mac devices and prevent noncompliant endpoints from accessing private resources.

Table 3-3 Demonstration Results for E3B1 EIG Crawl Phase

Demo ID	Expected Outcome	Observed Outcome	Comments	
A-1.1.a-m	N/A	N/A	Demonstration cannot be completed. There is no network-level enforcement present in this build. All devices are already joined to the network. There is no tool that can keep any entity (RSS, EP, BYOD, or guest device) from joining the network based on its authentication status.	
A-1.2.a-m	N/A	N/A	Demonstration cannot be completed. There is no network-level enforcement present in this build.	
A-1.3.a-f	N/A	N/A	Demonstration cannot be completed. There is no network-level enforcement present in this build.	
A-1.4.a-g	N/A	N/A	Cloud-based resources are out of scope until run phase.	
A-2.1.a-i	N/A	N/A	Demonstration cannot be completed. There is no network-level enforcement present in this build. There is no tool that can reauthenticate any entity (RSS, EP, BYOD, or guest device) and terminate its network access based on authentication status.	
A-2.2.a-i	N/A	N/A	Demonstration cannot be completed. There is no network-level enforcement present in this build based on reauthentication status.	

Demo ID	Expected	Observed	Comments	
	Outcome	Outcome		
A-2.3.a-f	N/A	N/A	Demonstration cannot be completed. There is no network-level enforcement present in this build based on reauthentication status.	
A-2.4.a-f	N/A	N/A	Cloud-based resources are out of scope until run phase.	
A-3.1.a, A-3.3.a, A-3.5.a	User request and action is recorded	User login to an application is logged	Success: Azure AD records the authentication logs. Administrators can log in to Azure AD and view logs of when a user logged onto an application and whether the authentication was successful or not.	
A-3.1.b, A-3.3.b	API call is recorded	Logs contain relevant API information	Success: Azure AD logs have relevant information about the authentication between the user and resource.	
A-3.2.a-b, A-3.4.a-b, A-3.6.a	N/A	N/A	Cloud-based resources are out of scope until run phase.	
B-1.1.a	Access Successful	Access Successful	Partial Success: Users access RSS1 based on the EP compliance. Cannot validate compliance of RSS1, so can only partially demonstrate.	
B-1.1.b	Access Successful	Access Successful	Partial Success: Authenticated user access to RSS2 successful. Can only partially demonstrate because cannot validate compliance on RSS2.	
B-1.1.c	Access Not Successful	Access Not Successful	Partial Success: User authentication failure prevents access. Cannot validate compliance on RSS1. Partial demonstration completed with user not able to authenticate.	
B-1.1.d	Access Not Successful	Access Not Successful	Partial Success: Based on configuration in Ent 3, the E2 is not authorized to access RSS1 based on enterprise governance policy. Also, RSS compliance cannot be demonstrated in this phase. In this case, user is not granted access to RSS1.	
B-1.1.e	Access Successful	Access Successful	Partial Success: Authenticated user access to RSS2 successful. Can partially demonstrate. Cannot validate compliance on RSS2.	
B-1.1.f	Access Not Successful	Access Not Successful	Success: User authentication failure prevents access.	

Demo ID	Expected Outcome	Observed Outcome	Comments	
B-1.1.g	Access Not Successful	Access Not Successful	Success: User authentication failure prevents access.	
B-1.1.h	Access Successful	Access Successful	Partial Success: GitLab session timeout is set to one minute for demonstration purposes. After session timed out, user was reauthenticated. Can only partially demonstrate because cannot validate RSS1 compliance.	
B-1.1.i	Access Not Successful	Access Not Successful	Success: Unauthenticated users were prevented from accessing resources.	
B-1.1.j	Access Not Successful	Access Not Successful	Partial Success: Authenticated user access to RSS1 successful. Can partially demonstrate. Cannot validate compliance on RSS1. After GitLab timed out, re-authentication was unsuccessful.	
B-1.1.k	Access Limited	N/A	Not able to demonstrate with current set of technologies. Cannot limit access based on device non-compliance.	
B-1.1.l-p	N/A	N/A	Cannot demonstrate. Unable to perform compliance checks on RSS.	
В-1.2.а-р			Cannot test because there is no branch office in Ent. 3.	
В-1.3.а-р			The results are the same as B-1.1, given that network policies allow the user/device to access the enterprise remotely using a VPN connection. See results from B-1.1.	
B-1.4.a-p, B-1.5.a-p, and B- 1.6.a-p	N/A	N/A	Cloud-based resources are out of scope until run phase.	
B-2, B-5	N/A	N/A	Out of scope until run phase. Tools are needed to create policies to allow or deny access to internet resources.	
B-3, B-6			Out of scope until run phase.	
B-4			All demonstrations here are the same as B-1 since the device is both authenticated and compliant.	
All C Use Cases	N/A	N/A	Demonstrations cannot be performed. Currently, no federation configuration has been set up between Ent1, Ent2, and Ent3.	

890

891

892

893

894

895

Demo ID	Expected Outcome	Observed Outcome	Comments
All D Use Cases			All demonstrations here are the same as B-1 since the device is both authenticated and compliant. Note that the user is a contractor.
All E Use Cases	N/A	N/A	Guest (No-ID) access is considered out of scope for the EIG crawl phase.
All F Use Cases	N/A	N/A	Confidence level use cases are considered out of scope for the EIG crawl phase.

3.1.4 Enterprise 4 Build 1 (E4B1) Demonstration Results

These results will be included in the next version of this draft document.

3.2 EIG Run Phase Demonstration Results

This section lists the demonstration results for each of the builds that was implemented as part of the EIG run phase, as defined in *NIST SP 1800-35B: Approach, Architecture, and Security Characteristics*.

3.2.1 Enterprise 1 Build 2 (E1B2) Demonstration Results

<u>Table</u> 3-4_lists the demonstration results for all EIG run phase demonstrations run in Enterprise 1 Build 2 (E1B2). In all demonstrations that we attempted to conduct, the ZTA functionality included in the build performed as expected. The technology deployed in E1B2 was able to determine endpoint compliance for Windows, Linux, Mac, and mobile devices and prevent noncompliant endpoints from accessing private resources.

Table 3-4 Demonstration Results for E1B2 EIG Crawl Phase

Demo ID	Expected Outcome	Observed Outcome	Comments
A-1.1.a-m	N/A	N/A	Demonstration cannot be completed. There is no network-level enforcement present in this build. Zscaler uses the client connector to allow a user on a device to access specific resources only, whether onprem or remote. Users cannot readily access resources in the enterprise (or network) if they do not have permissions to access them. Resources are not authenticated or checked for compliance in this phase.

Demo ID	Expected Outcome	Observed Outcome	Comments
A-1.2.a-m, A-1.3.a-f, A-1.4.a-g	N/A	N/A	Same as in A-1. Demonstration cannot be completed. There is no network-level enforcement present in this build.
A-2.1.a-I, A-2.2.a-I, A-2.3.a-f, A-2.4.a-f	N/A	N/A	Same as in A-1. Demonstration cannot be completed. There is no network-level enforcement present in this build.
A-3.1.a, A-3.3.a, A-3.5.a	User request and action is recorded	User login to an applicatio n is logged	Success: Okta records the authentication logs. Administrators can log in to Okta and view logs of when a user logged onto an application and whether the authentication was successful or not. Zscaler Private Access (ZPA) records relevant information about the connection between the endpoint and resource.
A-3.1.b, A-3.3.b	API call is recorded	Logs contain relevant API informatio n	Success: Okta records the authentication logs. Administrators can log in to Okta and view logs of when a user logged onto an application and whether the authentication was successful or not. Zscaler ZPA records relevant information about the connection between the endpoint and resource.
A-3.2.a, A-3.4.a, A-3.6.a	User request and action is recorded	User login to an applicatio n is logged	Success: Okta records the authentication logs. Administrators can log in to Okta and view logs of when a user logged onto an application and whether the authentication was successful or not. Zscaler ZPA records relevant information about the connection between the endpoint and resource.
A-3.2.b, A-3.4.b, A-3.6.a	API call is recorded	Logs contain relevant API informatio n	Success: Okta records the authentication logs. Administrators can log in to Okta and view logs of when a user logged onto an application and whether the authentication was successful or not. Zscaler ZPA records relevant information about the connection between the endpoint and resource.
B-1.1.a, B-1.2.a, B-1.3.a, B-4.1.a, B-4.2.a, B-4.3.a, D-1.1.a, D-1.2.a, D-1.3.a, D-4.1.a, D-4.2.a, D-4.3.a	Access Successful	Access Successful	Partial success: User is authenticated via Okta when accessing the resource. User logs into Zscaler client connector as part of login process to the endpoint and policies are applied to the user/endpoint (including laptops, workstations, and mobile devices). User successfully connects to RSS1. However, we cannot validate compliance of RSS1.

Demo ID	Expected Outcome	Observed Outcome	Comments
B-1.1.b, B-1.2.b, B- 1.3.b, B-4.1.b, B- 4.2.b, B-4.3.b, D- 1.1.b, D-1.2.b, D- 1.3.b, D-4.1.b, D- 4.2.b, D-4.3.b	Access Successful	Access Successful	Partial success: User is authenticated via Okta when accessing the resource. User logs into Zscaler client connector as part of login process to the endpoint and policies are applied to the user/endpoint (including laptops, workstations, and mobile devices). User successfully connects to RSS1. However, we cannot validate compliance of RSS1.
B-1.1.c, B-1.2.c, B- 1.3.c, B-4.1.c, B- 4.2.c, B-4.3.c, D- 1.1.c, D-1.2.c, D- 1.3.c, D-4.1.c, D- 4.2.c, D-4.3.c	Access Not Successful	Access Not Successful	Success: Demonstration completed with user not able to log in to resource.
B-1.1.d, B-1.2.d, B-1.3.d, B-4.1.d, B-4.2.d, B-4.3.d, D-1.1.d, D-1.2.d, D-1.3.d, D-4.1.d, D-4.2.d, D-4.3.d	Access Not Successful	Access Not Successful	Partial success: Based on configuration in Ent1, the E2 is not authorized to access RSS1 based on enterprise governance policy. ZPA will deny access to the resource. Also, RSS compliance cannot be demonstrated in this phase. In this case, user is not granted access to RSS1.
B-1.1.e, B-1.2.e, B- 1.3.e, B-4.1.e, B- 4.2.e, B-4.3.e, D- 1.1.e, D-1.2.e, D- 1.3.e, D-4.1.e, D- 4.2.e, D-4.3.e	Access Successful	Access Successful	Partial success: User is authenticated via Okta when accessing the resource. User logs into Zscaler client connector as part of login process to the endpoint and policies are applied to the user/endpoint (including laptops, workstations, and mobile devices). User successfully connects to RSS2. However, we cannot validate compliance of RSS2.
B-1.1.f, B-1.2.f, B- 1.3.f, B-4.1.f, B-4.2.f, B-4.3.f, D-1.1.f, D- 1.2.f, D-1.3.f, D- 4.1.f, D-4.2.f, D-4.3.f	Access Not Successful	Access Not Successful	Success: Without user authentication for the resource the access attempt did not succeed.
B-1.1.g, B-1.2.g, B- 1.3.g, B-4.1.g, B- 4.2.g, B-4.3.g, D- 1.1.g, D-1.2.g, D- 1.3.g, D-4.1.g, D- 4.2.g, D-4.3.g	Access Not Successful	Access Not Successful	Success: Without user authentication for the resource, the access attempt did not succeed.

Demo ID	Expected Outcome	Observed Outcome	Comments
B-1.1.h, B-1.2.h, B- 1.3.h, B-4.1.h, B- 4.2.h, B-4.3.h, D- 1.1.h, D-1.2.h, D- 1.3.h, D-4.1.h, D- 4.2.h, D-4.3.h	Access Successful	Access Successful	Success: GitLab session timeout is set to one minute for demonstration purposes. After session timed out, user was re-authenticated.
B-1.1.i, B-1.2.i, B- 1.3.i, B-4.1.i, B-4.2.i, B-4.3.i, D-1.1.i, D- 1.2.i, D-1.3.i, D-4.1.i, D-4.2.i, D-4.3.i	Access Not Successful	Access Not Successful	Success: After session timeout, user tried to login with incorrect password and was denied.
B-1.1.j, B-1.2.j, B- 1.3.j, B-4.1.j, B-4.2.j, B-4.3.j, D-1.1.j, D- 1.2.j, D-1.3.j, D-4.1.j, D-4.2.j, D-4.3.j	Access Not Successful	Access Not Successful	Success: Device posture failure detected by ZPA so access was denied.
B-1.1.k, B-1.2.k, B- 1.3.k, B-4.1.k, B- 4.2.k, B-4.3.k, D- 1.1.k, D-1.2.k, D- 1.3.k, D-4.1.k, D- 4.2.k, D-4.3.k	Access Limited	N/A	Partial success: Access to RSS2 is blocked. Currently cannot perform limited access.
B-1.1.l-m, B-1.2.l-m, B-1.3.l-m, B-4.1.l-m, B-4.2.l-m, B-4.3.l-m, D-1.1.l-m, D-1.2.l-m, D-1.3.l-m, D-4.1.l-m, D-4.2.l-m, D-4.3.l-m	Access Denied	Access Denied	Success: User was denied access because the endpoint was non-compliant. Device posture failure detected by ZPA.
B-1.1.n-p, B-1.2.n-p, B-1.3.n-p, B-4.1.n-p, B-4.2.n-p, B-4.3.n-p, D-1.1.n-p, D-1.2.n-p, D-1.3.n-p, D-4.1.n-p, D-4.2.n-p, D-4.3.n-p	N/A	N/A	Demonstration cannot be run. Unable to perform compliance checks on RSS.
В-1.2.а-р			The results are the same as B-1.1 since network policies allow access from branch to Ent1. See results from B-1.1.

Demo ID	Expected Outcome	Observed Outcome	Comments
B-1.3.a-p			The results are the same as B-1.1, given that ZPA policies allow the user/device to access the enterprise remotely the same way that user/device would access a resource within the enterprise. See results from B-1.1.
B-1.4.a-p, B-1.5.a-p, B-1.6.a-p, B-4.4.a-p, B-4.5.a-q, and B- 4.6.a-p			Access to cloud-based resources (RSS1 and RSS2) are the same as on-prem. See results from B-1.1.
B-2.1.a-d, B-2.2.a-d, B-2.3.a-d B-5	Access Successful	Access Successful	Success: Employee is granted access to URL1 and URL2 regardless of hourly access time because employees have full access to both URLs at all times per ZScaler policy.
B-2.1.e, B-2.2.e, B- 2.3.e	Access Not Successful	Access Not Successful	Success: The only way the user is not authenticated is if the user inputs the incorrect password or does not have a second factor during Zscaler Client Connector (ZCC) login. With incorrect 1st or 2nd factor, ZCC will fail to connect with ZIA and will not be able to access the internet.
B-2.1f, B-2.2f, B-2.3f	Access Not Successful	Access Not Successful	Success: Contractor is blocked from URL1 as expected per Zscaler policy.
B-2.1g, B-2.2g, B- 2.3g	Access Successful	Access Successful	Success: Contractor is granted access to URL2 as expected per Zscaler policy.
B-2.1.h-I,B-2.2.h-I,B- 2.3.h-i	Access Not Successful	Access Not Successful	Success: Contractor is blocked from accessing URL1 due to failed authentication.
B-2.1.j, B-2.2.j, B-2.3.j	Access Not Successful	Access Successful	The only way the user is not authenticated is if the user inputs the incorrect password or does not have a second factor during ZCC login. Access is successful because internet access is required for ZIA to function. If not authenticated to ZIA, internet access is unrestricted unless blocked by company firewall.
B-2.1.k, B-2.2.k, B- 2.3.k	Access Successful	Access Successful	Success: Employee is granted access after successful reauthentication per Zscaler policy as expected.

Demo ID	Expected Outcome	Observed Outcome	Comments
B-2.1.I, B-2.2.I, B- 2.3.I	Access Not Successful	Access Not Successful	Success: Employee cannot access URL1 or URL2 after reauthentication to Zscaler fails as expected.
B-2.1.m-p, B-2.2.m- p, B-2.3.m-p	N/A	N/A	Demonstration cannot be completed. ZIA does not perform device posture/compliance checks on endpoints without integration of a third-party EPP product.
B-3.1.a, B-3.4.a, B- 3.5.a	Real Req Success	Real Req Success	Success: Real Request successfully authenticated.
B-3.1.b, B-3.4.b, B-3.5.b	Real Req Fail	Real Req Fail	Success: Incorrect credentials were entered, and the Real Request failed as expected.
B-3.1.c, B-3.4.c, B- 3.5.c	Limit Access for Real Request, Deny Access to Hostile Request	N/A	Unable to complete demonstration. Current build does not have the capability to differentiate between the Real Request and Hostile Request in this context.
B-3.1.d, B-3.4.d, B- 3.5.d	Real Request Keep Access, Deny Access to Hostile Request	N/A	Unable to complete demonstration. Current build does not have the capability to differentiate between the Real Request and Hostile Request in this context.
B-3.1.e, B-3.4.e, B- 3.5.e	Hostile Request Successful	Hostile Request Successful	Success: Hostile Request successfully authenticated.
B-3.1.f, B-3.4.f, B- 3.5.f	Hostile Request Unsuccess ful	Hostile Request Unsuccess ful	Success: Incorrect credentials were entered, and the Hostile Request failed as expected.
B-3.1.g, B-3.4.g, B- 3.5.g	Real Request Fail,	N/A	Unable to complete demonstration. Current build does not have the capability to differentiate

Demo ID	Expected Outcome	Observed Outcome	Comments
	Hostile Request Access Limited		between the Real Request and Hostile Request in this context.
B-3.1.h, B-3.4.h, B-3.5.h	Real Request Fail, Hostile Request remains authentic ated	N/A	Unable to complete demonstration. Current build does not have the capability to differentiate between the Real Request and Hostile Request in this context.
B-3.1.i, B-3.4.i, B- 3.5.i	Real Req Success	Real Req Success	Success: Real Request successfully authenticated.
B-3.1.j, B-3.4.j, B-3.5.j	Real Request remains authentic ated, Hostile Request Fail	N/A	Unable to complete demonstration. Current build does not have the capability to differentiate between the Real Request and Hostile Request in this context.
B-3.1.k, B-3.4.k, B- 3.5.k	Hostile Request Fail	Hostile Request Fail	Success: Incorrect credentials were entered, and the Hostile Request failed as expected.
B-3.1.l, B-3.4.l, B- 3.5.l	Real Request Access Successful	Real Requet Access Successful	Success: Real Request successfully reauthenticated.
B-3.1.m, B-3.4.m, B-3.5.m	Hostile Request Access Denied	Hostile Request Access Denied	Success: Hostile Request reauthentication failed.
B-3.1.n, B-3.4.n, B- 3.5.n	N/A	N/A	Demonstration could not be completed due to build not supporting session termination at this level.
B-3.1.o, B-3.4.o, B- 3.5.o	N/A	N/A	Demonstration could not be completed due to build not supporting session termination at this level.

Demo ID	Expected Outcome	Observed Outcome	Comments
B-4			As documented in the rows above, the results of all B-4 use case demonstrations are the same as the results of the B-1 use cases because the device is both authenticated and compliant. In this case, a BYOD device will have to install both the Ivanti Neurons for UEM agent and Okta Verify App. See results from B-1.1 for B-4.1, B-4.2, and B-4.3.
All C Use Cases	N/A	N/A	Demonstrations cannot be performed. Currently, no federation configuration has been set up between Ent1, Ent2, and Ent3.
All D Use Cases			As documented in the rows above, the results of all D use case demonstrations are the same as the results of the B use cases. Note that the user is a contractor and will have access to resources based on need. The Ivanti Neurons for UEM agent and Okta Verify App will have to be installed on the contractor's device, whether it's provided by the enterprise or BYOD.
E-1.1a, E-1.2a	Success	Success	Success: User/device is recognized by Zscaler Internet Access (ZIA) as unmanaged and given access to the internet. Per ZIA enterprise policies, resources on the internet that are deemed safe for access are reachable by the user with no ID, which includes a public resource from Enterprise 1.
E-1.1b, E-1.2b	Success	Success	Success: User/device is recognized by ZIA as unmanaged and given access to the internet. Per ZIA enterprise policies, resources on the internet that are deemed safe for access are reachable by the user with no ID.
All F Use Cases	N/A	N/A	Test cannot be completed without third-party integration with an EPP.

3.2.2 Enterprise 2 Build 2 (E2B2) Demonstration Results

There will not be an EIG run phase build in Enterprise 2, i.e., there will not be an E2B2.

896

3.2.3 Enterprise 3 Build 2 (E3B2) Demonstration Results

<u>Table</u> 3-5_lists the demonstration results for all EIG run phase demonstrations run in Enterprise 3 Build 2 (E3B2). In all demonstrations that we attempted to conduct, the ZTA functionality included in the build performed as expected. The technology deployed in E3B2 was able to determine endpoint compliance for Android, iOS, Windows, and Mac devices and prevent noncompliant endpoints from accessing private resources.

Table 3-5 Demonstration Results for E3B2 EIG Run Phase

Demo ID	Expected Outcome	Observed Outcome	Comments
A-1.1.a-d	Access to Network	Access to Network	Success: Resource has access to network in accordance with Forescout policy.
A-1.1.b, A-1.1.c, A-1.1.g	No Access to Network	No Access to Network	Partial success: In the current configuration, the endpoint has access limited to the local subnet in accordance with Forescout policy.
A-1.1.d	No Access to Network	N/A	Demonstration cannot be completed. By Scenario A-1 definition, a resource has already undergone onboarding.
A-1.1.e	Access to Network	Access to Network	Success: Endpoint has access to network in accordance with Forescout policy.
A-1.1.f	Max. Limited Access to Network	Max. Limited Access to Network	Success: Endpoint has access limited in accordance with Forescout policy.
A-1.1.h	Access to Public Network	N/A	Demonstration cannot be completed. By Scenario A-1 definition, an endpoint has already undergone onboarding.
A-1.1.i	Access to Network	Access to Network	Success: BYOD has access to network in accordance with Forescout policy.
A-1.1.j	Limited Access to Network	Limited Access to Network	Success: Endpoint has access limited to the local subnet in accordance with Forescout policy.
A-1.1.k	No Access to Network	No Access to Network	Partial success: In the current configuration, the endpoint has access limited to the local subnet in accordance with Forescout policy.

Demo ID	Expected Outcome	Observed Outcome	Comments
A-1.1.I	Access to Public Network	N/A	Demonstration cannot be completed. By Scenario A-1 definition, the BYOD has already undergone onboarding.
A-1.1.m	Access to Public Network	Access to Public Network	Success: BYOD has access to network in accordance with Forescout policy.
A-1.2.a-m	Access to Network	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
A-1.3.a	Access to Network	Access to Network	Success: Endpoint has access to network in accordance with Forescout policy.
A-1.3.b	Max. Limited Access to Network	Max. Limited Access to Network	Success: Endpoint has access limited in accordance with Forescout policy.
A-1.3.c	No Access to Network	No Access to Network	Success: Endpoint is denied access to the network after failing to authenticate to the GlobalProtect VPN.
A-1.3.d	Access to Network	Access to Network	Success: BYOD has access to network in accordance with Forescout policy.
A-1.3.e	Max. Limited Access to Network	Max. Limited Access to Network	Success: Endpoint has access limited in accordance with Forescout policy.
A-1.3.f	No Access to Network	No Access to Network	Success: BYOD is denied access to the network after failing to authenticate to the GlobalProtect VPN.
A-1.4.a-g	N/A	N/A	Testing of cloud-based resources and endpoints as subjects is out of scope.
A-2.1.a	Keep Access to Network	Keep Access to Network	Success: Resource has access to network in accordance with Forescout policy.
A-2.1.b	Terminate Access to Network	Limit Access to Network	Partial Success: Resource has access limited to the local subnet in accordance with Forescout policy.

Demo ID	Expected Outcome	Observed Outcome	Comments
A-2.1.c	Terminate Access to Network	Limit Access to Network	Partial Success: Resource has access limited to the local subnet in accordance with Forescout policy.
A-2.1.d	Keep Access to Network	Keep Access to Network	Success: Endpoint has access to network in accordance with Forescout policy.
A-2.1.e	Max. Limited Access to Network	Max. Limited Access to Network	Success: Endpoint has access limited in accordance with Forescout policy.
A-2.1.f	Terminate Access to Network	Limit Access to Network	Partial Success: Resource has access limited to the local subnet in accordance with Forescout policy.
A-2.1.g	Keep Access to Network	Keep Access to Network	Success: BYOD has access to network in accordance with Forescout policy.
A-2.1.h	Max. Limited Access to Network	Max. Limited Access to Network	Success: Endpoint has access limited in accordance with Forescout policy.
A-2.1.i	Terminate Access to Network	Limit Access to Network	Partial success: BYOD has access limited to the local subnet in accordance with Forescout policy.
A-2.2.a-i	N/A	N/A	Demonstration cannot be completed. There is no branch office configured for Enterprise 3.
A-2.3.a	Keep Access to Network	Keep Access to Network	Success: Endpoint has access to network in accordance with Forescout policy.
A-2.3.b	Max. Limited Access to Network	Max. Limited Access to Network	Success: Endpoint has access limited in accordance with Forescout policy.
A-2.3.c	Terminate Access to Network	Terminate Access to Network	Success: Endpoint has access terminated after failing to re-authenticate to the GlobalProtect VPN.
A-2.3.d	Keep Access to Network	Keep Access to Network	Success: BYOD has access to network in accordance with Forescout policy.

Demo ID	Expected Outcome	Observed Outcome	Comments
A-2.3.e	Max. Limited Access to Network	Max. Limited Access to Network	Success: BYOD has access limited in accordance with Forescout policy.
A-2.3.f	Terminate Access to Network	Terminate Access to Network	Success: BYOD has access terminated after failing to re-authenticate to the GlobalProtect VPN.
A-2.4.a,d	Keep Access to Network	Keep Access to Network	Success: Azure is able to allow access to cloud endpoints and resources.
A-2.4.b,c,f	Terminate Access to Network	Terminate Access to Network	Success: Azure is able to limit access to cloud endpoints and resources.
A-2.4.e	Max. Limited Access to Network	Max. Limited Access to Network	Success: Azure is able to limit access to cloud endpoints and resources.
A-3.1.a, A-3.2.a	User request and action is recorded	N/A	User activity and transaction flow is logged. Individual user actions are not visible.
A-3.3.a, A-3.4.a,	User request and action is recorded	N/A	Branch testing is not available for this build.
A-3.5.a, A-3.6.a	User request and action is recorded	N/A	User activity and transaction flow is logged. Individual user actions are not visible.
A-3.1.b, A-3.2.b, A-3.3.b, A-3.4.b	API call is recorded	N/A	Service activity and transaction flow is logged by Forescout. Individual API calls are not visible.
B-1.1.a	Access Successful	Access Successful	Success: Users access RSS1 based on the EP and RSS compliance with Forescout and Azure AD policy.
B-1.1.b	Access Successful	Access Successful	Success: Users access RSS2 based on the EP and RSS compliance with Forescout and Azure AD policy.
B-1.1.c	Access Not Successful	Access Not Successful	Success: User authentication failure to Azure AD prevents access.

Demo ID	Expected Outcome	Observed Outcome	Comments
B-1.1.d	Access Not Successful	Access Not Successful	Success: E2 is not authorized to access RSS1 in accordance with Azure AD policy.
B-1.1.e	Access Successful	Access Successful	Success: Users access RSS2 based on the EP and RSS compliance with Forescout and Azure AD policy.
B-1.1.f, B-1.1.g,	Access Not Successful	Access Not Successful	Success: User authentication failure to Azure AD prevents access.
B-1.1.h	Access Successful	Access Successful	Success: Session timeout is set to one minute for demonstration purposes. After session timed out, user was re-authenticated to Azure AD.
B-1.1.i	Access Not Successful	Access Not Successful	Success: Users were prevented from accessing resources after re-authentication failure to Azure AD.
B-1.1.j	Access Not Successful	Access Not Successful	Success: Initial user authentication to Azure AD was successful and user was granted access to RSS1. After E1 became non-compliant, user access to RSS1 was blocked in accordance with Forescout policy, and the user was unable to re-authenticate to Azure AD.
B-1.1.k	Access Limited	Access Not Successful	Partial success: Initial user authentication to Azure AD was successful and user was granted access to RSS2. In this case, changing the user's access level on RSS2 would require application-level control that is not available at this time. After E1 became non-compliant, user access to RSS2 was blocked in accordance with Forescout policy, and the user was unable to re-authenticate to Azure AD.
B-1.1.I	Access Not Successful	Access Not Successful	Success: After E1 became non-compliant, user access to RSS1 was blocked in accordance with Forescout policy, and the user was unable to authenticate to Azure AD.
B-1.1.m	Access Limited	Access Not Successful	Partial success: In this case, changing the user's access level on RSS2 would require application-level control that is not available at this time. After E1 became non-compliant, user access to RSS2 was blocked in accordance with Forescout

Demo ID	Expected Outcome	Observed Outcome	Comments
	Outcome	Outcome	policy, and the user was unable to authenticate to Azure AD.
B-1.1.n-p	Access Not Successful	Access Not Successful	Success: After the RSS became non-compliant, user access to the RSS was blocked in accordance with Forescout policy, and the user was unable to authenticate to Azure AD.
B-1.2.a-p			Cannot test because there is no branch office in Ent. 3.
B-1.3.a-p			The results are the same as B-1.1, given that network policies allow the user/device to access the enterprise remotely using a VPN connection. See results from B-1.1.
B-1.4.a	Access Successful	Access Successful	Success: Users access RSS1 based on the EP compliance with Forescout and Azure AD policy.
B-1.4.b	Access Successful	Access Successful	Success: Users access RSS2 based on the EP compliance with Forescout and Azure AD policy.
B-1.4.c	Access Not Successful	Access Not Successful	Success: User authentication failure to Azure AD prevents access.
B-1.4.d	Access Not Successful	Access Not Successful	Success: E2 is not authorized to access RSS1 in accordance with Azure AD policy.
B-1.4.e	Access Successful	Access Successful	Success: Users access RSS2 based on the EP and RSS compliance with Forescout and Azure AD policy.
B-1.4.f, B-1.4.g	Access Not Successful	Access Not Successful	Success: User authentication failure to Azure AD prevents access.
B-1.4.h	Access Successful	Access Successful	Success: Session timeout is set to one minute for demonstration purposes. After session timed out, user was re-authenticated to Azure AD.
B-1.4.i	Access Not Successful	Access Not Successful	Success: Users were prevented from accessing resources after re-authentication failure to Azure AD.
B-1.4.j	Access Not Successful	Access Not Successful	Success: Initial user authentication to Azure AD was successful and user was granted access to RSS1. After E1 became non-compliant, user access to RSS1 was blocked in accordance with Forescout

Demo ID	Expected	Observed	Comments
	Outcome	Outcome	policy, and the user was unable to re-authenticate to Azure AD.
B-1.4.k	Access Limited	Access Not Successful	Partial success: Initial user authentication to Azure AD was successful and user was granted access to RSS2. In this case, changing the user's access level on RSS2 would require application-level control that is not available at this time. After E1 became non-compliant, user access to RSS2 was blocked in accordance with Forescout policy, and the user was unable to re-authenticate to Azure AD.
B-1.4.I	Access Not Successful	Access Not Successful	Success: After E1 became non-compliant, user access to RSS1 was blocked in accordance with Forescout policy, and the user was unable to authenticate to Azure AD.
B-1.4.m	Access Limited	Access Not Successful	Partial success: In this case, changing the user's access level on RSS2 would require application-level control that is not available at this time. After E1 became non-compliant, user access to RSS2 was blocked in accordance with Forescout policy, and the user was unable to authenticate to Azure AD.
B-1.4.n-p	N/A	N/A	Demonstration cannot be performed as verification of cloud resource compliance is not available at this time.
B-1.5.a-p	N/A	N/A	Demonstration cannot be performed as branch office is not available at this time.
B-1.6.a-p			In the current implementation, remote users are connected to a VPN that routes network traffic through the on-prem environment. All test results are similar to B-1.4.a-p.
B-2.1.a-d,g,n	Access Successful	Access Successful	Success: Access allowed in accordance with Forescout policy.
B2.1.e,f,l,m,o,p	Access Not Successful	Access Not Successful	Success: Access denied in accordance with Forescout policy.
B-2.2	N/A	N/A	Demonstration cannot be performed as branch office is not available at this time.

Demo ID	Expected	Observed	Comments
	Outcome	Outcome	
B-2.3			In the current implementation, remote users are connected to a VPN that routes network traffic through the on-prem environment. All test results are similar to B-2.1.a-p.
B-3.1.a, B-3.4.a, B-3.5.a	Real Req Success	Real Req Success	Success: Real Request successfully authenticated.
B-3.1.b, B-3.4.b, B-3.5.b	Real Req Fail	Real Req Fail	Success: Incorrect credentials were entered, and the Real Request failed as expected.
B-3.1.c, B-3.4.c, B-3.5.c	Limit Access for Real Request, Deny Access to Hostile Request	N/A	Unable to complete demonstration. Current build does not have the capability to differentiate between the Real Request and Hostile Request in this context.
B-3.1.d, B-3.4.d, B-3.5.d	Real Request Keep Access, Deny Access to Hostile Request	N/A	Unable to complete demonstration. Current build does not have the capability to differentiate between the Real Request and Hostile Request in this context.
B-3.1.e, B-3.4.e, B-3.5.e	Hostile Request Successful	Hostile Request Successful	Success: Hostile Request successfully authenticated.
B-3.1.f, B-3.4.f, B-3.5.f	Hostile Request Unsuccessful	Hostile Request Unsuccessful	Success: Incorrect credentials were entered, and the Hostile Request failed as expected.
B-3.1.g, B-3.4.g, B-3.5.g	Real Request Fail, Hostile Request Access Limited	N/A	Unable to complete demonstration. Current build does not have the capability to differentiate between the Real Request and Hostile Request in this context.
B-3.1.h, B-3.4.h, B-3.5.h	Real Request Fail, Hostile Request remains authenticated	N/A	Unable to complete demonstration. Current build does not have the capability to differentiate between the Real Request and Hostile Request in this context.
B-3.1.i, B-3.4.i, B-3.5.i	Real Req Success	Real Req Success	Success: Real Request successfully authenticated.

Demo ID	Expected Outcome	Observed Outcome	Comments
B-3.1.j, B-3.4.j, B-3.5.j	Real Request remains authenticated, Hostile Request Fail	N/A	Unable to complete demonstration. Current build does not have the capability to differentiate between the Real Request and Hostile Request in this context.
B-3.1.k, B-3.4.k, B-3.5.k	Hostile Request Fail	Hostile Request Fail	Success: Incorrect credentials were entered, and the Hostile Request failed as expected.
B-3.1.l, B-3.4.l, B-3.5.l	Real Request Access Successful	Real Request Access Successful	Success: Real Request successfully reauthenticated.
B-3.1.m, B- 3.4.m, B-3.5.m	Hostile Request Access Denied	Hostile Request Access Denied	Success: Hostile Request reauthentication fails.
B-3.1.n, B-3.4.n, B-3.5.n	Hostile Request Session Terminated	Hostile Request Session Terminated	Success: Azure AD sessions terminated.
B-3.1.o, B-3.4.o, B-3.5.o	Real Request Session Terminated	Real Request Session Terminated	Success: Azure AD sessions terminated.
B-3.2, B-3.3	N/A	N/A	Branch office is not included in Build 3.
B-4			All demonstrations here are the same as B-1 since the device is both authenticated and compliant.
B-5			All demonstrations here are the same as B-2 since the device is both authenticated and compliant.
B-6			All demonstrations here are the same as B-3 since the device is both authenticated and compliant.
All C Use Cases	N/A	N/A	Demonstrations cannot be performed. Currently, no federation configuration has been set up between Ent1, Ent2, and Ent3.
All D Use Cases			All demonstrations here are the same as B-1 since the device is both authenticated and compliant. Note that the user is a contractor.

Demo ID	Expected Outcome	Observed Outcome	Comments
E-1.1.a,b	Access Successful	Access Successful	Success: Guests can access public resources and internet in accordance with policy.
E-1.2.a,b	N/A	N/A	Demonstration cannot be performed as branch office is not available at this time.
All F Use Cases	N/A	N/A	Confidence level use cases are considered out of scope for the EIG run phase.

905 Appendix A List of Acronyms

AD Active Directory

API Application Programming Interface

BYOD Bring Your Own Device

CRADA Cooperative Research and Development Agreement

DNS Domain Name System

E1B1 Enterprise 1 Build 1

E1B2 Enterprise 1 Build 2

E2B1 Enterprise 2 Build 1

E2B2 Enterprise 2 Build 2

E3B1 Enterprise 3 Build 1

E3B2 Enterprise 3 Build 2

E4B1 Enterprise 4 Build 1

EIG Enhanced Identity Governance

EP Enterprise Endpoint

ICAM Identity, Credential, and Access Management

IP Internet Protocol

IT Information Technology

ITL Information Technology Laboratory

MFA Multifactor Authentication

MSV Mandiant Security Validation

NCCoE National Cybersecurity Center of Excellence

NIC Network Interface Card

NIST National Institute of Standards and Technology

OS Operating System

PEP Policy Enforcement Point

SECOND PRELIMINARY DRAFT

PIV Personal Identity Verification

PKI Public Key Infrastructure

RSS Enterprise Resource

SP Special Publication

UEM Unified Endpoint Management

UP User Profile

URL Uniform Resource Locator

VM Virtual Machine

VPN Virtual Private Network

ZCC Zscaler Client Connector

ZIA Zscaler Internet Access

ZPA Zscaler Private Access

ZTA Zero Trust Architecture

Appendix B References

- [1] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, *Zero Trust Architecture*, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-207, Gaithersburg, Md., August 2020, 50 pp. Available: https://doi.org/10.6028/NIST.SP.800-207.
 - [2] P. Grassi, M. Garcia, and J. Fenton, *Digital Identity Guidelines*, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3, Gaithersburg, Md., June 2017, 75 pp. Available: https://doi.org/10.6028/NIST.SP.800-63-3.
 - [3] "National Cybersecurity Center of Excellence (NCCoE) Zero Trust Cybersecurity: Implementing a Zero Trust Architecture," Federal Register Vol. 85, No. 204, October 21, 2020, pp. 66936-66939. Available: https://www.federalregister.gov/documents/2020/10/21/2020-23292/national-cybersecurity-center-of-excellence-nccoe-zero-trust-cybersecurity-implementing-a-zero-trust.