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 Grayeli
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

Aaron Rodriguez
Micah Wilson
Cisco
Herndon, VA

Corey Bonnell
Dean Coclin
DigiCert
Lehi, UT

Ryan Johnson
Dung Lam
F5
Seattle, WA

Neal Lucier
Tom May
Forescout
San Jose, CA

Tim Knudsen
Google Cloud
Mill Valley, CA

Harmeet Singh
Krishna Yellepeddy
IBM
Armonk, NY

Corey Lund
Farhan Saifudin
Ivanti
South Jordan, UT

Hashim Khan
Tim LeMaster
Lookout
Reston, VA

James Elliott
David Pricer
Mandiant
Reston, VA

Clay Taylor
Tarek Dawoud
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
Ivan Anderson
Ping Identity
Denver, CO

Wade Ellery
John Petrutiu
Radiant Logic
Novato, CA

Frank Briguglio
Ryan 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

August 2022

PRELIMINARY DRAFT

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

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

While NIST and the NCCoE address goals of improving management of cybersecurity and privacy risk through outreach and application of standards and best practices, it is the stakeholder's responsibility to 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 recommendation.

National Institute of Standards and Technology Special Publication 1800-35D, Natl. Inst. Stand. Technol. Spec. Publ. 1800-35D, 104 pages, August 2022, CODEN: NSPUE2

FEEDBACK

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.

Comments on this publication may be submitted to: nccoe-zta-project@list.nist.gov.

Public comment period: August 9, 2022 through September 9, 2022

All comments are subject to release under the Freedom of Information Act.

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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 academic institutions work together to address businesses' most pressing cybersecurity issues. This 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 Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in information technology security—the NCCoE applies standards and best practices to develop modular, adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cybersecurity Framework and details the steps needed for another entity to re-create the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Maryland.

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

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication 1800 series) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align with relevant standards and best practices, and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

ABSTRACT

In this project, the NCCOE and its collaborators use commercially available technology to build interoperable, open, standards-based ZTA implementations that align to the concepts and principles in NIST Special Publication (SP) 800-207, *Zero Trust Architecture*. This NIST Cybersecurity Practice Guide explains how commercially available technology can be integrated and used to build various ZTAs. This volume of the practice guide defines the demonstrations that were designed to showcase the ZTA capabilities of the example implementations that have been built to support the use case scenarios in the project description. It also provides the demonstration results for each implementation.

KEYWORDS

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

ACKNOWLEDGMENTS

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

Name	Organization
Michael Friedrich	Appgate
Adam Rose	Appgate
Jonathan Roy	Appgate
Quint Van Deman	Amazon Web Services
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
David Clark	F5
Jay Kelley	F5

Name	Organization
Jamie Lozan	F5
Jason Wilburn	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
Joey Cruz	Microsoft
Janet Jones	Microsoft
Carmichael Patton	Microsoft
Hemma Prafullchandra	Microsoft
Brandon Stephenson	Microsoft
Sarah Young	Microsoft
Spike Dog	MITRE
Sallie Edwards	MITRE
Ayayidjin Gabiam	MITRE
Jolene Loveless	MITRE
Karri Meldorf	MITRE
Kenneth Sandlin	MITRE
Jessica Walton	MITRE
Mike Bartock	NIST
Gema Howell	NIST
Gini Khalsa	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
Bill Baz	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
Andrew Babakian	VMware
Jeffrey Adorno	Zscaler

Name	Organization
Jeremy James	Zscaler
Lisa Lorenzin	Zscaler
Matt Moulton	Zscaler
Patrick Perry	Zscaler

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product 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		
Appgate	IBM	Ping Identity
AWS	Ivanti	Radiant Logic
Broadcom Software	Lookout	SailPoint
Cisco	Mandiant	Tenable
DigiCert	Microsoft	Trellix
F5	Okta	VMware
Forescout	Palo Alto Networks	Zimperium
Google Cloud	PC Matic	Zscaler

DOCUMENT CONVENTIONS

The terms “shall” and “shall not” indicate requirements to be followed strictly to conform to the publication and from which no deviation is permitted. The terms “should” and “should not” indicate that among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited. The terms “may” and “need not” indicate a course of action permissible within the limits of the publication. The 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 required for compliance with the guidance or requirements in this Information Technology Laboratory

(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 of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in 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 currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft 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

Contents

1 Introduction 1

1.1 How to Use this Guide 1

2 Functional Demonstration Playbook 3

2.1 Definitions 3

2.1.1 Network IDs 3

2.1.2 Subject and Requested Resource Types 4

2.1.3 Resource and Querying Endpoint Compliance Classification 4

2.1.4 Desired Outcomes 4

2.1.5 Authentication Status 5

2.2 General Configurations 5

2.2.1 Access Level 6

2.2.2 Access Profiles 6

2.2.3 Resources and Capabilities 6

2.2.4 User Profiles 7

2.3 Demonstration Methodology 8

2.4 Use Case A: Discovery and Identification of IDs, Assets, and Data Flows 10

2.4.1 Scenario A-1: Discovery and authentication of endpoint assets 10

2.4.2 Scenario A-2: Reauthentication of identified assets 12

2.4.3 Scenario A-3: Discovery of transaction flows 14

2.5 Use Case B: Enterprise ID Access 15

2.5.1 Scenario B-1: Full/limited resource access using an enterprise endpoint 16

2.5.2 Scenario B-2: Full/limited internet access using an enterprise endpoint 20

2.5.3 Scenario B-3: Stolen credential using an enterprise endpoint 22

2.5.4 Scenario B-4: Full/limited resource access using BYOD 28

2.5.5 Scenario B-5: Full/limited internet access using BYOD 32

2.5.6 Scenario B-6: Stolen credential using BYOD 34

2.6 Use Case C: Collaboration: Federated-ID Access 40

2.6.1 Scenario C-1: Full resource access using an enterprise endpoint 40

133 2.6.2 Scenario C-2: Limited resource access using an enterprise endpoint 41
134 2.6.3 Scenario C-3: Limited internet access using an enterprise endpoint 42
135 2.6.4 Scenario C-4: No internet access using an enterprise endpoint 43
136 2.6.5 Scenario C-5: Internet access using BYOD 44
137 2.6.6 Scenario C-6: Access resources using BYOD 45
138 2.6.7 Scenario C-7: Stolen credential using an enterprise endpoint 46
139 2.6.8 Scenario C-8: Stolen credential using BYOD 48
140 2.7 Use Case D: Other-ID Access 49
141 2.7.1 Scenario D-1: Full/limited resource access using an enterprise endpoint 49
142 2.7.2 Scenario D-2: Full/limited internet access using an enterprise endpoint 54
143 2.7.3 Scenario D-3: Stolen credential using BYOD or enterprise endpoint 56
144 2.7.4 Scenario D-4: Full/limited resource access using BYOD 61
145 2.7.5 Scenario D-5: Full/limited internet access using BYOD 66
146 2.7.6 Scenario D-6: Stolen credential using BYOD 68
147 2.8 Use Case E: Guest: No-ID Access 74
148 2.8.1 Scenario E-1: Guest requests public internet access 74
149 2.9 Use Case F: Confidence Level 75
150 2.9.1 Scenario F-1: User reauthentication fails during active session 75
151 2.9.2 Scenario F-2: Requesting endpoint reauthentication fails during active session 76
152 2.9.3 Scenario F-3: Resource reauthentication fails during active session 77
153 2.9.4 Scenario F-4: Compliance fails during active session 78
154 2.9.5 Scenario F-5: Compliance improves between requests 79
155 **3 Functional Demonstration Results 80**
156 3.1 EIG Crawl Phase Demonstration Results 80
157 3.1.1 Enterprise 1 Build 1 (E1B1) Demonstration Results 80
158 3.1.2 Enterprise 2 Build 1 (E2B1) Demonstration Results 85
159 3.1.3 Enterprise 3 Build 1 (E3B1) Demonstration Results 85
160 3.1.4 Enterprise 4 Build 1 (E4B1) Demonstration Results 88
161 **Appendix A List of Acronyms 89**
162 **Appendix B References 91**

List of Tables

Table 2-1 Authentication Status Codes 5
Table 2-2 Access Levels 6
Table 2-3 Access Profiles 6
Table 2-4 Resources and Capabilities 7
Table 2-5 User Profiles 7
Table 2-6 Scenario A-1 Demonstrations 10
Table 2-7 Scenario A-2 Demonstrations 13
Table 2-8 Scenario A-3 Demonstrations 15
Table 2-9 Scenario B-1 Demonstrations 16
Table 2-10 Scenario B-2 Demonstrations 20
Table 2-11 Scenario B-3 Demonstrations 23
Table 2-12 Scenario B-4 Demonstrations 28
Table 2-13 Scenario B-5 Demonstrations 32
Table 2-14 Scenario B-6 Demonstrations 35
Table 2-15 Scenario C-1 Demonstrations 40
Table 2-16 Scenario C-2 Demonstrations 41
Table 2-17 Scenario C-3 Demonstrations 43
Table 2-18 Scenario C-4 Demonstrations 44
Table 2-19 Scenario C-5 Demonstrations 45
Table 2-20 Scenario C-6 Demonstrations 46
Table 2-21 Scenario C-7 Demonstrations 47
Table 2-22 Scenario C-8 Demonstrations 48
Table 2-23 Scenario D-1 Demonstrations 50
Table 2-24 Scenario D-2 Demonstrations 54
Table 2-25 Scenario D-3 Demonstrations 57
Table 2-26 Scenario D-4 Demonstrations 62

Table 2-27 Scenario D-5 Demonstrations 66
Table 2-28 Scenario D-6 Demonstrations 69
Table 2-29 Scenario E-1 Demonstrations 74
Table 2-30 Scenario F-1 Demonstrations 75
Table 2-31 Scenario F-2 Demonstrations 76
Table 2-32 Scenario F-3 Demonstrations 77
Table 2-33 Scenario F-4 Demonstrations 78
Table 2-34 Scenario F-5 Demonstrations 79
Table 3-1 Demonstration Results for E1B1 EIG Crawl Phase 81
Table 3-2 Demonstration Results for E3B1 EIG Crawl Phase 85

1 Introduction

To demonstrate the security characteristics supported by each zero trust architecture (ZTA) build that is implemented as part of the NCCoE ZTA project, a variety of use cases have been defined, each of which consists of numerous demonstrations that each have a specific expected outcome. The use cases are designed to showcase ZTA security capabilities under a variety of conditions.

Section 2 of this document describes the use cases that have been defined. It also defines various types of user IDs and endpoints, resources, user and access profiles, assumptions, and other information that is required to fully describe the use cases. The purpose of this section of the document is to guide operators as they perform each demonstration.

Section 3 of this document describes the results of performing these demonstrations using each of the builds that have been implemented.

1.1 How to Use this Guide

This NIST Cybersecurity Practice Guide will help users develop a plan for migrating to ZTA. It demonstrates a standards-based reference design for implementing a ZTA and provides users with the information they need to replicate two different implementations of this reference design. Each of these implementations, which are known as *builds,* are standards-based and align to the concepts and 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 organizations to incorporate ZTA into their legacy environments gradually, in a process of continuous improvement that brings them closer and closer to achieving the ZTA goals that they have prioritized based on risk, cost, and resources.

NIST is adopting an agile process to publish this content. Each volume is being made available as soon as possible rather than delaying release until all volumes are completed. Work continues on implementing the example solutions and developing other parts of the content. As a preliminary draft, we will publish at least one additional draft for public comment before it is finalized.

When complete, this guide will contain four volumes:

- NIST SP 1800-35A: *Executive Summary* – why we wrote this guide, the challenge we address, why it could be important to your organization, and our approach to solving this challenge
- NIST SP 1800-35B: *Approach, Architecture, and Security Characteristics* – what we built and why
- 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 project

- 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)**

Depending on your role in your organization, you might use this guide in different ways:

Business decision makers, including chief security and technology officers, will be interested in the *Executive Summary, NIST SP 1800-35A*, which describes the following topics:

- challenges that enterprises face in migrating to the use of ZTA
- example solution built at the NCCoE
- benefits of adopting the example solution

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.

You might share the *Executive Summary, NIST SP 1800-35A*, with your leadership team members to help 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].

IT professionals and operators who want to implement similar solutions will find the whole practice 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, 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 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.

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 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 with your existing tools and IT system infrastructure. We hope that you will seek products that are congruent with applicable standards and recommended practices.

A NIST Cybersecurity Practice Guide does not describe "the" solution, but example solutions. This is a preliminary draft guide. As the project progresses, the preliminary draft will be updated, and additional volumes will also be released for comment. We seek feedback on the publication's 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

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 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-premises-to-on-premises request; this demonstration does not need to be repeated making the request 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 possible demonstration cases.

This playbook is still under development. Additional scenarios and use cases will be included in the next version as the implementations evolve and add capabilities. For this current draft of the document and 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 scope.

2.1 Definitions

2.1.1 Network IDs

As defined in NIST SP 800-63, an *identity* is an attribute or set of attributes that uniquely identifies a 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.
- **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.

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

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 can be identified and conforms to the enterprise security policy for the resource.

2.1.4 Desired Outcomes

The following definitions are used for desired outcomes:

- **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

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

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

2.2 General Configurations

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.

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

Table 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.

Table 2-3 Access Profiles

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

Table 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.

Table 2-4 Resources and Capabilities

Component	Type	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

Table 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 UP-O1	P_FULL	RSS1 RSS2	Active	Endpoint falls out of compliance
UP-E2 UP-O2	P_LIMITED	RSS2	Active	Endpoint falls out of compliance
UP-E3 UP-O3	none	none	Deactivated or deleted	

User Profile	Access Profile	Resource	Status	Downgrade Trigger Examples
UP-E4 UP-O4	P_FULL	URL1 URL2	Active	Endpoint falls out of compliance
UP-E5 UP-O5	P_LIMITED	URL1 URL2	Active	Endpoint falls out of compliance 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 UP-O7	P_FULL	RSS1	Active	Account reported compromised. 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.

In this document, demonstrations that can utilize automated components are performed by Mandiant Security Validation (MSV). Each demonstration contains an MSV column with a "Y" or "N" denoting whether MSV can be used in that particular demonstration. Demonstrations that cannot be automated are performed manually.

We deployed 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. 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 inter-enterprise 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 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 test what the destructive effects of the malware might be.

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 the initial step before migrating to a ZTA. An enterprise needs to identify and understand the workflows used in business processes, the IDs used, and the resources involved. Then it can move on to creating 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.

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

Discovery here is focused on detecting assets and flows on the network, mapping them to identified assets and flows, and providing access accordingly.

Pre-Condition: Enterprise-owned components (RSS and EP) have already undergone initial onboarding 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-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 network with an "enterprise" segment with resources that can only be accessed by authorized enterprise IDs and a "guest" segment with access to the public internet only.

Demonstration: Connect the device to the network and demonstrate network connectivity.

Purpose and Outcome: This scenario demonstrates the capability to authenticate assets at a specific location and provide enterprise network access.

Table 2-6 Scenario A-1 Demonstrations

Demo ID		MSV	Subj Type	Onboarded/ Registered	Auth Stat	Compl	Subj Loc	Desired Outcome
A-1.1	a	N	RSS	Y	A+	Y	On-Prem	Access to Network
	b		RSS	Y	A+	N		No Access to Network
	c		RSS	Y	A-	---		No Access to Network
	d		RSS	N	---	---		No Access to Network

Demo ID		MSV	Subj Type	Onboarded/ Registered	Auth Stat	Compl	Subj Loc	Desired Outcome
	e		EP	Y	A+	Y		Access to Network
	f		EP	Y	A+	N		Max. Limited Access to Network
	g		EP	Y	A-	---		No Access to Network
	h		EP	N	---	---		Access to Public Network
	i		BYOD	Y	A+	Y		Access to Network
	j		BYOD	Y	A+	N		Limited Access to Network
	k		BYOD	Y	A-	---		No Access to Network
	l		BYOD	N	---	---		Access to Public Network
	m		Guest Dev.	---	---	---		Access to Public Network
Comment: **f & j**: Limited access (only limited RSS or Cap access); **h, l, m**: Unknown assets all treated like guest devices								
A-1.2	a	N	RSS	Y	A+	Y	Branch	Access to Network
	b		RSS	Y	A+	N		No Access to Network
	c		RSS	Y	A-	---		No Access to Network
	d		RSS	N	---	---		No Access to Network
	e		EP	Y	A+	Y		Access to Network
	f		EP	Y	A+	N		Limited Access to Network
	g		EP	Y	A-	---		No Access to Network
	h		EP	N	---	---		Access to Public Network
	i		BYOD	Y	A+	Y		Access to Network
	j		BYOD	Y	A+	N		Limited Access to Network
	k		BYOD	Y	A-	---		No Access to Network
	l		BYOD	N	---	---		Access to Public Network

Demo ID		MSV	Subj Type	Onboarded/ Registered	Auth Stat	Compl	Subj Loc	Desired Outcome
	m		Guest Dev.	---	---	---		Access to Public Network
Comment: **f & j**: Limited access (only limited RSS or Cap access); **h, l, m**: Unknown assets all treated like guest devices								
A-1.3	a	N	EP	Y	A+	Y	Re-mote	Access to Network
	b		EP	Y	A+	N		Max. Limited Access to Net-work
	c		EP	Y	A-	---		No Access to Network
	d		BYOD	Y	A+	Y		Access to Network
	e		BYOD	Y	A+	N		Max. Limited Access to Net-work
	f		BYOD	Y	A-	---		No Access to Network
Comment: **b & e**: Limited access (only limited RSS or Cap access)								
A-1.4	a	N	RSS	Y	A+	Y	Cloud	Access to Network
	b		RSS	Y	A+	N		No Access to Network
	c		RSS	Y	A-	---		No Access to Network
	d		RSS	N	---	---		No Access to Network
	e		EP	Y	A+	Y		Access to Network
	f		EP	Y	A+	N		Max. Limited Access to Net-work
	g		EP	Y	A-	---		No Access to Network
Comment: **f**: Limited access (only limited RSS or Cap access)								

2.4.2 Scenario A-2: Reauthentication of identified assets

Once an asset is identified and authenticated, continuous re-authentication is necessary.

Pre-Condition: The asset (user endpoint, resource) underwent previous authentication and is ready for operation.

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		MSV	Subj Type	Onboarded/ Registered	Auth Stat	Compl	Subj Loc	Desired Outcome
A-2.1	a	N	RSS	Y	RA+	Y	On-Prem	Keep Access to Network
	b		RSS	Y	RA+	N		Terminate Access to Network
	c		RSS	Y	RA-	---		Terminate Access to Network
	d		EP	Y	RA+	Y		Keep Access to Network
	e		EP	Y	RA+	N		Max. Limited Access to Net-work
	f		EP	Y	RA-	---		Terminate Access to Network
	g		BYOD	Y	RA+	Y		Keep Access to Network
	h		BYOD	Y	RA+	N		Max. Limited Access to Net-work
	i		BYOD	Y	RA-	---		Terminate Access to Network
Comment: **e & h**: Limited access (only limited RSS or Cap access)								
A-2.2	a	N	RSS	Y	RA+	Y	Branch	Keep Access to Network
	b		RSS	Y	RA+	N		Terminate Access to Network
	c		RSS	Y	RA-	---		Terminate Access to Network
	d		EP	Y	RA+	Y		Keep Access to Network
	e		EP	Y	RA+	N		Max. Limited Access to Net-work
	f		EP	Y	RA-	---		Terminate Access to Network
	g		BYOD	Y	RA+	Y		Keep Access to Network
	h		BYOD	Y	RA+	N		Max. Limited Access to Net-work
	i		BYOD	Y	RA-	---		Terminate Access to Network

Demo ID		MSV	Subj Type	Onboarded/ Registered	Auth Stat	Compl	Subj Loc	Desired Outcome
Comment: **e & h**: Limited access (only limited RSS or Cap access)								
A-2.3	a	N	EP	Y	RA+	Y	Remote	Keep Access to Network
	b		EP	Y	RA+	N		Max. Limited Access to Network
	c		EP	Y	RA-	---		Terminate Access to Network
	d		BYOD	Y	RA+	Y		Keep Access to Network
	e		BYOD	Y	RA+	N		Max. Limited Access to Network
	f		BYOD	Y	RA-	---		Terminate Access to Network
Comment: **b & e**: Limited access (only limited RSS or Cap access)								
A-2.4	a	N	RSS	Y	RA+	Y	Cloud	Keep Access to Network
	b		RSS	Y	RA+	N		Terminate Access to Network
	c		RSS	Y	RA-	---		Terminate Access to Network
	d		EP	Y	RA+	Y		Keep Access to Network
	e		EP	Y	RA+	N		Max. Limited Access to Network
	f		EP	Y	RA-	---		Terminate Access to Network
Comment: **e**: Limited access (only limited RSS or Cap access)								

2.4.3 Scenario A-3: Discovery of transaction flows

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.

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

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

479 **Table 2-8 Scenario A-3 Demonstrations**

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

480 ## 2.5 Use Case B: Enterprise ID Access

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

483 Each activity demonstrates the capability of authentication from within a given setting. The access is
484 authenticated with an "enterprise-ID" using an enterprise-owned endpoint (EP) as well as a privately
485 owned endpoint (BYOD). Each scenario provides a set of pre-conditions as well as multiple
486 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 either 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		MSV	UP	Location Req. > RSS	Auth Stat			Access	Compl		Desired Outcome
					User	EP	RSS		EP	RSS	
B-1.1	a	N	E1	On-Prem → On-Prem	A+	A	A	RSS1	Y	Y	Access Successful
	b	N	E1		A+	A	A	RSS2	Y	Y	Access Successful
	c	Y	E1		A-	A	---	---	Y	---	Access Not Successful
	d	N	E2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	N	E2		A+	A	A	RSS2	Y	Y	Access Successful
	f	Y	E2		A-	A	---	---	Y	---	Access Not Successful
	g	Y	E3		A-	A	---	---	Y	---	Access Not Successful
	h	N	E1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	N	E1		RA-	A	---	---	Y	---	Access Not Successful
	j	N	E1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	N	E1		RA+	A	A	RSS2	N	Y	Access Limited
	l	N	E1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	N	E1		A+	A	A	RSS2	N	Y	Access Limited
	n	N	E1		A+	A	A	RSS1	Y	N	Access Not Successful

Demo ID		MSV	UP	Location Req. > RSS	Auth Stat			Access	Compl		Desired Outcome
					User	EP	RSS		EP	RSS	
	o	N	E1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	N	E2		A+	A	A	RSS2	Y	N	Access Not Successful
B-1.2	a	N	E1	Branch → On-Prem	A+	A	A	RSS1	Y	Y	Access Successful
	b	N	E1		A+	A	A	RSS2	Y	Y	Access Successful
	c	Y	E1		A-	A	---	---	Y	---	Access Not Successful
	d	N	E2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	N	E2		A+	A	A	RSS2	Y	Y	Access Successful
	f	Y	E2		A-	A	---	---	Y	---	Access Not Successful
	g	Y	E3		A-	A	---	---	Y	---	Access Not Successful
	h	N	E1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	N	E1		RA-	A	---	---	Y	---	Access Not Successful
	j	N	E1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	N	E1		RA+	A	A	RSS2	N	Y	Access Limited
	l	N	E1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	N	E1		A+	A	A	RSS2	N	Y	Access Limited
	n	N	E1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	N	E1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	N	E2		A+	A	A	RSS2	Y	N	Access Not Successful
B-1.3	a	N	E1	Remote → On-Prem	A+	A	A	RSS1	Y	Y	Access Successful
	b	N	E1		A+	A	A	RSS2	Y	Y	Access Successful
	c	N	E1		A-	A	---	---	Y	---	Access Not Successful
	d	N	E2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	N	E2		A+	A	A	RSS2	Y	Y	Access Successful
	f	N	E2		A-	A	---	---	Y	---	Access Not Successful
	g	N	E3		A-	A	---	---	Y	---	Access Not Successful

Demo ID		MSV	UP	Location Req. > RSS	Auth Stat			Access	Compl		Desired Outcome
					User	EP	RSS		EP	RSS	
	h	N	E1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	N	E1		RA-	A	---	---	Y	---	Access Not Successful
	j	N	E1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	N	E1		RA+	A	A	RSS2	N	Y	Access Limited
	l	N	E1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	N	E1		A+	A	A	RSS2	N	Y	Access Limited
	n	N	E1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	N	E1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	N	E2		A+	A	A	RSS2	Y	N	Access Not Successful
B-1.4	a	N	E1	On-Prem → Cloud	A+	A	A	RSS1	Y	Y	Access Successful
	b	N	E1		A+	A	A	RSS2	Y	Y	Access Successful
	c	Y	E1		A-	A	---	---	Y	---	Access Not Successful
	d	N	E2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	N	E2		A+	A	A	RSS2	Y	Y	Access Successful
	f	Y	E2		A-	A	---	---	Y	---	Access Not Successful
	g	Y	E3		A-	A	---	---	Y	---	Access Not Successful
	h	N	E1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	N	E1		RA-	A	---	---	Y	---	Access Not Successful
	j	N	E1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	N	E1		RA+	A	A	RSS2	N	Y	Access Limited
	l	Y	E1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	Y	E1		A+	A	A	RSS2	N	Y	Access Limited
	n	Y	E1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	Y	E1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	Y	E2		A+	A	A	RSS2	Y	N	Access Not Successful

Demo ID		MSV	UP	Location Req. > RSS	Auth Stat			Access	Compl		Desired Outcome
					User	EP	RSS		EP	RSS	
B-1.5	a	N	E1	Branch → Cloud	A+	A	A	RSS1	Y	Y	Access Successful
	b	N	E1		A+	A	A	RSS2	Y	Y	Access Successful
	c	Y	E1		A-	A	---	---	Y	---	Access Not Successful
	d	N	E2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	N	E2		A+	A	A	RSS2	Y	Y	Access Successful
	f	Y	E2		A-	A	---	---	Y	---	Access Not Successful
	g	Y	E3		A-	A	---	---	Y	---	Access Not Successful
	h	N	E1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	N	E1		RA-	A	---	---	Y	---	Access Not Successful
	j	N	E1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	N	E1		RA+	A	A	RSS2	N	Y	Access Limited
	l	N	E1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	N	E1		A+	A	A	RSS2	N	Y	Access Limited
	n	N	E1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	N	E1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	N	E2		A+	A	A	RSS2	Y	N	Access Not Successful
B-1.6	a	N	E1	Remote → Cloud	A+	A	A	RSS1	Y	Y	Access Successful
	b	N	E1		A+	A	A	RSS2	Y	Y	Access Successful
	c	N	E1		A-	A	---	---	Y	---	Access Not Successful
	d	N	E2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	N	E2		A+	A	A	RSS2	Y	Y	Access Successful
	f	N	E2		A-	A	---	---	Y	---	Access Not Successful
	g	N	E3		A-	A	---	---	Y	---	Access Not Successful
	h	N	E1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	N	E1		RA-	A	---	---	Y	---	Access Not Successful
	j	N	E1		RA+	A	A	RSS1	N	Y	Access Not Successful

Demo ID		MSV	UP	Location Req. > RSS	Auth Stat			Access	Compl		Desired Outcome
					User	EP	RSS		EP	RSS	
	k	N	E1		RA+	A	A	RSS2	N	Y	Access Limited
	l	N	E1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	N	E1		A+	A	A	RSS2	N	Y	Access Limited
	n	N	E1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	N	E1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	N	E2		A+	A	A	RSS2	Y	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.

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

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

Table 2-10 Scenario B-2 Demonstrations

Demo ID		MSV	UP	Location Req. > RSS	Auth Stat		Access	Compl		Desired Outcome
					User	EP		EP	Out of Hours	
B-2.1	a	N	E4	On-Prem → Internet	A+	A	URL1	Y	N	Access Successful
	b	N	E4		A+	A	URL2	Y	N	Access Successful
	c	N	E4		A+	A	URL1	Y	Y	Access Successful

Demo ID		MSV	UP	Location Req. > RSS	Auth Stat		Access	Compl		Desired Outcome
					User	EP		EP	Out of Hours	
	d	N	E4		A+	A	URL1	Y	Y	Access Successful
	e	Y	E4		A-	A	---	Y	---	Access Not Successful
	f	N	E5		A+	A	URL1	Y	N	Access Not Successful
	g	N	E5		A+	A	URL2	Y	N	Access Successful
	h	N	E5		A+	A	URL1	Y	Y	Access Not Successful
	i	N	E5		A+	A	URL1	Y	Y	Access Not Successful
	j	Y	E5		A-	A	---	Y	---	Access Not Successful
	k	N	E4		RA+	A	URL1	Y	---	Access Successful
	l	N	E4		RA-	A	---	Y	---	Access Not Successful
	m	N	E4		A+	A	URL1	N	---	Access Not Successful
	n	N	E4		A+	A	URL2	N	---	Access Successful
	o	N	E5		A+	A	URL1	N	N	Access Not Successful
	p	N	E5		A+	A	URL2	N	N	Access Not Successful
B-2.2	a	N	E4	Branch → Internet	A+	A	URL1	Y	N	Access Successful
	b	N	E4		A+	A	URL2	Y	N	Access Successful
	c	N	E4		A+	A	URL1	Y	Y	Access Successful
	d	N	E4		A+	A	URL1	Y	Y	Access Successful
	e	Y	E4		A-	A	---	Y	---	Access Not Successful
	f	N	E5		A+	A	URL1	Y	N	Access Not Successful
	g	N	E5		A+	A	URL2	Y	N	Access Successful
	h	N	E5		A+	A	URL1	Y	Y	Access Not Successful
	i	N	E5		A+	A	URL1	Y	Y	Access Not Successful
	j	Y	E5		A-	A	---	Y	---	Access Not Successful
	k	N	E4		RA+	A	URL1	Y	---	Access Successful
	l	N	E4		RA-	A	---	Y	---	Access Not Successful

Demo ID		MSV	UP	Location Req. > RSS	Auth Stat		Access	Compl		Desired Outcome
					User	EP		EP	Out of Hours	
	m	N	E4		A+	A	URL1	N	---	Access Not Successful
	n	N	E4		A+	A	URL2	N	---	Access Successful
	o	N	E5		A+	A	URL1	N	N	Access Not Successful
	p	N	E5		A+	A	URL2	N	N	Access Not Successful
B-2.3	a	N	E4	Remote → Internet	A+	A	URL1	Y	N	Access Successful
	b	N	E4		A+	A	URL2	Y	N	Access Successful
	c	N	E4		A+	A	URL1	Y	Y	Access Successful
	d	N	E4		A+	A	URL1	Y	Y	Access Successful
	e	Y	E4		A-	A	---	Y	---	Access Not Successful
	f	N	E5		A+	A	URL1	Y	N	Access Not Successful
	g	N	E5		A+	A	URL2	Y	N	Access Successful
	h	N	E5		A+	A	URL1	Y	Y	Access Not Successful
	i	N	E5		A+	A	URL1	Y	Y	Access Not Successful
	j	Y	E5		A-	A	---	Y	---	Access Not Successful
	k	N	E4		RA+	A	URL1	Y	---	Access Successful
	l	N	E4		RA-	A	---	Y	---	Access Not Successful
	m	N	E4		A+	A	URL1	N	---	Access Not Successful
	n	N	E4		A+	A	URL2	N	---	Access Successful
	o	N	E5		A+	A	URL1	N	N	Access Not Successful
	p	N	E5		A+	A	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.

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

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

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

529 **Table 2-11 Scenario B-3 Demonstrations**

Demo ID		MSV	UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
					Real Req	Hostile Req			
B-3.1	a	N	E6	On-Prem On-Prem → On-Prem	A+	---	N	Access Successful	---
	b	Y	E6		A-	---	N	Access Not Successful	---
	c	N	E6		A	A+	N	Change to Access Limited	Access Not Successful
	d	N	E6		A	A-	N	Keep Access	Access Not Successful
	e	N	E6		---	A+	N	---	Access Successful
	f	Y	E6		---	A-	N	---	Access Not Successful
	g	N	E6		A+	A	N	Access Not Successful	Change to Access Limited
	h	N	E6		A-	A	N	Access Not Successful	Keep Access
	i	N	E7		A+	---	Y	Access Successful	---
	j	N	E7		A	A-	Y	Keep Access	Access Not Successful
	k	Y	E7		---	A-	Y	---	Access Not Successful

Demo ID		MSV	UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
					Real Req	Hostile Req			
	l	N	E7		RA+	---	Y	Access Successful	---
	m	N	E7		---	RA-	Y	---	Access Not Successful
	n	N	E7		---	A	Y	---	All Sessions Terminated
	o	N	E7		A	---	Y	All Sessions Terminated	---
Comment: **l, m, n, o**: Initial authentication successful and while authenticated credentials were reported stolen									
B-3.2	a	N	E6	On-Prem Branch → On-Prem	A+	---	N	Access Successful	---
	b	Y	E6		A-	---	N	Access Not Successful	---
	c	N	E6		A	A+	N	Change to Access Limited	Access Not Successful
	d	N	E6		A	A-	N	Keep Access	Access Not Successful
	e	N	E6		---	A+	N	---	Access Successful
	f	Y	E6		---	A-	N	---	Access Not Successful
	g	N	E6		A+	A	N	Access Not Successful	Change to Access Limited
	h	N	E6		A-	A	N	Access Not Successful	Keep Access
	i	N	E7		A+	---	Y	Access Successful	---
	j	N	E7		A	A-	Y	Keep Access	Access Not Successful
	k	Y	E7		---	A-	Y	---	Access Not Successful
	l	N	E7		RA+	---	Y	Access Successful	---
	m	N	E7		---	RA-	Y	---	Access Not Successful

Demo ID		MSV	UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
					Real Req	Hostile Req			
	n	N	E7		---	A	Y	---	Change to Access Limited
	o	N	E7		A	---	Y	Change to Access Limited	---
Comment: **l, m, n, o**: Initial authentication successful and while authenticated credentials were reported stolen									
B-3.3	a	N	E6	Branch On-Prem → On-Prem	A+	---	N	Access Successful	---
	b	Y	E6		A-	---	N	Access Not Successful	---
	c	N	E6		A	A+	N	Change to Access Limited	Access Not Successful
	d	N	E6		A	A-	N	Keep Access	Access Not Successful
	e	N	E6		---	A+	N	---	Access Successful
	f	Y	E6		---	A-	N	---	Access Not Successful
	g	N	E6		A+	A	N	Access Not Successful	Change to Access Limited
	h	N	E6		A-	A	N	Access Not Successful	Keep Access
	i	N	E7		A+	---	Y	Access Successful	---
	j	N	E7		A	A-	Y	Keep Access	Access Not Successful
	k	Y	E7		---	A-	Y	---	Access Not Successful
	l	N	E7		RA+	---	Y	Access Successful	---
	m	N	E7		---	RA-	Y	---	Access Not Successful
	n	N	E7		---	A	Y	---	Change to Access Limited

Demo ID		MSV	UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
					Real Req	Hostile Req			
	o	N	E7		A	---	Y	Change to Access Limited	---
Comment: **l, m, n, o**: Initial authentication successful and while authenticated credentials were reported stolen									
B-3.4	a	N	E6	Remote On-Prem → On-Prem	A+	---	N	Access Successful	---
	b	N	E6		A-	---	N	Access Not Successful	---
	c	N	E6		A	A+	N	Change to Access Limited	Access Not Successful
	d	N	E6		A	A-	N	Keep Access	Access Not Successful
	e	N	E6		---	A+	N	---	Access Successful
	f	Y	E6		---	A-	N	---	Access Not Successful
	g	N	E6		A+	A	N	Access Not Successful	Change to Access Limited
	h	N	E6		A-	A	N	Access Not Successful	Keep Access
	i	N	E7		A+	---	Y	Access Successful	---
	j	N	E7		A	A-	Y	Keep Access	Access Not Successful
	k	Y	E7		---	A-	Y	---	Access Not Successful
	l	N	E7		RA+	---	Y	Access Successful	---
	m	N	E7		---	RA-	Y	---	Access Not Successful
	n	N	E7		---	A	Y	---	Change to Access Limited
	o	N	E7		A	---	Y	Change to Access Limited	---

Demo ID		MSV	UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
					Real Req	Hostile Req			
Comment: **l, m, n, o**: Initial authentication successful and while authenticated credentials were reported stolen									
B-3.5	a	N	E6	On-Prem Remote → On-Prem	A+	---	N	Access Successful	---
	b	Y	E6		A-	---	N	Access Not Successful	---
	c	N	E6		A	A+	N	Change to Access Limited	Access Not Successful
	d	N	E6		A	A-	N	Keep Access	Access Not Successful
	e	N	E6		---	A+	N	---	Access Successful
	f	N	E6		---	A-	N	---	Access Not Successful
	g	N	E6		A+	A	N	Access Not Successful	Change to Access Limited
	h	N	E6		A-	A	N	Access Not Successful	Keep Access
	i	N	E7		A+	---	Y	Access Successful	---
	j	N	E7		A	A-	Y	Keep Access	Access Not Successful
	k	N	E7		---	A-	Y	---	Access Not Successful
	l	N	E7		RA+	---	Y	Access Successful	---
	m	N	E7		---	RA-	Y	---	Access Not Successful
	n	N	E7		---	A	Y	---	Change to Access Limited
	o	N	E7		A	---	Y	Change to Access Limited	---
Comment: **l, m, n, o**: Initial authentication successful and while authenticated credentials were reported stolen									

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.

Table 2-12 Scenario B-4 Demonstrations

Demo ID		MSV	UP	Location Req. > RSS	Auth Stat			Access	Compl		Desired Outcome
					User	EP	RSS		EP	RSS	
B-4.1	a	N	E1	On-Prem → On-Prem	A+	A	A	RSS1	Y	Y	Access Successful
	b	N	E1		A+	A	A	RSS2	Y	Y	Access Successful
	c	N	E1		A-	A	---	---	Y	---	Access Not Successful
	d	N	E2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	N	E2		A+	A	A	RSS2	Y	Y	Access Successful
	f	Y	E2		A-	A	---	---	Y	---	Access Not Successful
	g	Y	E3		A-	A	---	---	Y	---	Access Not Successful
	h	N	E1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	N	E1		RA-	A	---	---	Y	---	Access Not Successful
	j	N	E1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	N	E1		RA+	A	A	RSS2	N	Y	Access Limited
	l	N	E1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	N	E1		A+	A	A	RSS2	N	Y	Access Limited

Demo ID		MSV	UP	Location Req. > RSS	Auth Stat			Access	Compl		Desired Outcome
					User	EP	RSS		EP	RSS	
	n	N	E1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	N	E1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	N	E2		A+	A	A	RSS2	Y	N	Access Not Successful
B-4.2	a	N	E1	Branch → On-Prem	A+	A	A	RSS1	Y	Y	Access Successful
	b	N	E1		A+	A	A	RSS2	Y	Y	Access Successful
	c	Y	E1		A-	A	---	---	Y	---	Access Not Successful
	d	N	E2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	N	E2		A+	A	A	RSS2	Y	Y	Access Successful
	f	Y	E2		A-	A	---	---	Y	---	Access Not Successful
	g	Y	E3		A-	A	---	---	Y	---	Access Not Successful
	h	N	E1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	N	E1		RA-	A	---	---	Y	---	Access Not Successful
	j	N	E1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	N	E1		RA+	A	A	RSS2	N	Y	Access Limited
	l	N	E1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	N	E1		A+	A	A	RSS2	N	Y	Access Limited
	n	N	E1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	N	E1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	N	E2		A+	A	A	RSS2	Y	N	Access Not Successful
B-4.3	a	N	E1	Remote → On-Prem	A+	A	A	RSS1	Y	Y	Access Successful
	b	N	E1		A+	A	A	RSS2	Y	Y	Access Successful
	c	N	E1		A-	A	---	---	Y	---	Access Not Successful
	d	N	E2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	N	E2		A+	A	A	RSS2	Y	Y	Access Successful
	f	N	E2		A-	A	---	---	Y	---	Access Not Successful
	g	N	E3		A-	A	---	---	Y	---	Access Not Successful

Demo ID		MSV	UP	Location Req. > RSS	Auth Stat			Access	Compl		Desired Outcome
					User	EP	RSS		EP	RSS	
	h	N	E1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	N	E1		RA-	A	---	---	Y	---	Access Not Successful
	j	N	E1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	N	E1		RA+	A	A	RSS2	N	Y	Access Limited
	l	N	E1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	N	E1		A+	A	A	RSS2	N	Y	Access Limited
	n	N	E1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	N	E1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	N	E2		A+	A	A	RSS2	Y	N	Access Not Successful
B-4.4	a	N	E1	On-Prem → Cloud	A+	A	A	RSS1	Y	Y	Access Successful
	b	N	E1		A+	A	A	RSS2	Y	Y	Access Successful
	c	Y	E1		A-	A	---	---	Y	---	Access Not Successful
	d	N	E2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	N	E2		A+	A	A	RSS2	Y	Y	Access Successful
	f	Y	E2		A-	A	---	---	Y	---	Access Not Successful
	g	Y	E3		A-	A	---	---	Y	---	Access Not Successful
	h	N	E1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	N	E1		RA-	A	---	---	Y	---	Access Not Successful
	j	N	E1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	N	E1		RA+	A	A	RSS2	N	Y	Access Limited
	l	N	E1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	N	E1		A+	A	A	RSS2	N	Y	Access Limited
	n	N	E1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	N	E1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	N	E2		A+	A	A	RSS2	Y	N	Access Not Successful

Demo ID		MSV	UP	Location Req. > RSS	Auth Stat			Access	Compl		Desired Outcome
					User	EP	RSS		EP	RSS	
B-4.5	a	N	E1	Branch → Cloud	A+	A	A	RSS1	Y	Y	Access Successful
	b	N	E1		A+	A	A	RSS2	Y	Y	Access Successful
	c	Y	E1		A-	A	---	---	Y	---	Access Not Successful
	d	N	E2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	N	E2		A+	A	A	RSS2	Y	Y	Access Successful
	f	Y	E2		A-	A	---	---	Y	---	Access Not Successful
	g	Y	E3		A-	A	---	---	Y	---	Access Not Successful
	h	N	E1		RA+	A	A	RSS1	Y	Y	Access Successful
	j	N	E1		RA-	A	---	---	Y	---	Access Not Successful
	k	N	E1		RA+	A	A	RSS1	N	Y	Access Not Successful
	l	N	E1		RA+	A	A	RSS2	N	Y	Access Limited
	m	N	E1		A+	A	A	RSS1	N	Y	Access Not Successful
	n	N	E1		A+	A	A	RSS2	N	Y	Access Limited
	o	N	E1		A+	A	A	RSS1	Y	N	Access Not Successful
	p	N	E1		A+	A	A	RSS2	Y	N	Access Not Successful
	q	N	E2		A+	A	A	RSS2	Y	N	Access Not Successful
B-4.6	a	N	E1	Remote → Cloud	A+	A	A	RSS1	Y	Y	Access Successful
	b	N	E1		A+	A	A	RSS2	Y	Y	Access Successful
	c	N	E1		A-	A	---	---	Y	---	Access Not Successful
	d	N	E2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	N	E2		A+	A	A	RSS2	Y	Y	Access Successful
	f	N	E2		A-	A	---	---	Y	---	Access Not Successful
	g	N	E3		A-	A	---	---	Y	---	Access Not Successful
	h	N	E1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	N	E1		RA-	A	---	---	Y	---	Access Not Successful

Demo ID		MSV	UP	Location Req. > RSS	Auth Stat			Access	Compl		Desired Outcome
					User	EP	RSS		EP	RSS	
	j	N	E1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	N	E1		RA+	A	A	RSS2	N	Y	Access Limited
	l	N	E1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	N	E1		A+	A	A	RSS2	N	Y	Access Limited
	n	N	E1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	N	E1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	N	E2		A+	A	A	RSS2	Y	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-enterprise resource.

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

Table 2-13 Scenario B-5 Demonstrations

Demo ID		MSV	UP	Location Req. > RSS	Auth Stat		Access	Compl		Desired Outcome
					User	EP		EP	Out of Hours	
B-5.1	a	N	E4	On-Prem → Internet	A+	A	URL1	Y	N	Access Successful
	b	N	E4		A+	A	URL2	Y	N	Access Successful
	c	N	E4		A+	A	URL1	Y	Y	Access Successful
	d	N	E4		A+	A	URL1	Y	Y	Access Successful
	e	Y	E4		A-	A	---	Y	---	Access Not Successful

Demo ID		MSV	UP	Location Req. > RSS	Auth Stat		Access	Compl		Desired Outcome
					User	EP		EP	Out of Hours	
	f	N	E5		A+	A	URL1	Y	N	Access Not Successful
	g	N	E5		A+	A	URL2	Y	N	Access Successful
	h	N	E5		A+	A	URL1	Y	Y	Access Not Successful
	i	N	E5		A+	A	URL1	Y	Y	Access Not Successful
	j	Y	E5		A-	A	---	Y	---	Access Not Successful
	k	N	E4		RA+	A	URL1	Y	---	Access Successful
	l	N	E4		RA-	A	---	Y	---	Access Not Successful
	m	N	E4		A+	A	URL1	N	---	Access Not Successful
	n	N	E4		A+	A	URL2	N	---	Access Successful
	o	N	E5		A+	A	URL1	N	N	Access Not Successful
	p	N	E5		A+	A	URL2	N	N	Access Not Successful
B-5.2	a	N	E4	Branch → Internet	A+	A	URL1	Y	N	Access Successful
	b	N	E4		A+	A	URL2	Y	N	Access Successful
	c	N	E4		A+	A	URL1	Y	Y	Access Successful
	d	N	E4		A+	A	URL1	Y	Y	Access Successful
	e	Y	E4		A-	A	---	Y	---	Access Not Successful
	f	N	E5		A+	A	URL1	Y	N	Access Not Successful
	g	N	E5		A+	A	URL2	Y	N	Access Successful
	h	N	E5		A+	A	URL1	Y	Y	Access Not Successful
	i	N	E5		A+	A	URL1	Y	Y	Access Not Successful
	j	Y	E5		A-	A	---	Y	---	Access Not Successful
	k	N	E4		RA+	A	URL1	Y	---	Access Successful
	l	N	E4		RA-	A	---	Y	---	Access Not Successful
	m	N	E4		A+	A	URL1	N	---	Access Not Successful

Demo ID		MSV	UP	Location Req. > RSS	Auth Stat		Access	Compl		Desired Outcome
					User	EP		EP	Out of Hours	
	n	N	E4		A+	A	URL2	N	---	Access Successful
	o	N	E5		A+	A	URL1	N	N	Access Not Successful
	p	N	E5		A+	A	URL2	N	N	Access Not Successful
B-5.3	a	N	E4	Remote → Internet	A+	A	URL1	Y	N	Access Successful
	b	N	E4		A+	A	URL2	Y	N	Access Successful
	c	N	E4		A+	A	URL1	Y	Y	Access Successful
	d	N	E4		A+	A	URL1	Y	Y	Access Successful
	e	N	E4		A-	A	---	Y	---	Access Not Successful
	f	N	E5		A+	A	URL1	Y	N	Access Not Successful
	g	N	E5		A+	A	URL2	Y	N	Access Successful
	h	N	E5		A+	A	URL1	Y	Y	Access Not Successful
	i	N	E5		A+	A	URL1	Y	Y	Access Not Successful
	j	N	E5		A-	A	---	Y	---	Access Not Successful
	k	N	E4		RA+	A	URL1	Y	---	Access Successful
	l	N	E4		RA-	A	---	Y	---	Access Not Successful
	m	N	E4		A+	A	URL1	N	---	Access Not Successful
	n	N	E4		A+	A	URL2	N	---	Access Successful
	o	N	E5		A+	A	URL1	N	N	Access Not Successful
	p	N	E5		A+	A	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.

563 **Demonstration:** Two requests for the same enterprise resource are performed using the same user
564 credentials. The "Real Request" is performed using the latest credentials, which are modified/replaced
565 after reported stolen, and that request can succeed. The "Hostile Request" is performed using a stolen
566 enterprise-ID. All authentication methods are compromised for the Hostile Request. Re-authentication
567 always follows a previously successful authentication.

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

570 **Table 2-14 Scenario B-6 Demonstrations**

Demo ID		MSV	UP	Location Real Hostile > RSS	Auth Stat		Rep. Sto-len	Desired Outcome for Real Request	Desired Outcome for Hostile Request
					Real Req	Hostile Req			
B-6.1	a	N	E6	On-Prem On-Prem → On-Prem	A+	---	N	Access Successful	---
	b	Y	E6		A-	---	N	Access Not Suc-cessful	---
	c	N	E6		A	A+	N	Change to Access Limited	Access Not Suc-cessful
	d	N	E6		A	A-	N	Keep Access	Access Not Suc-cessful
	e	N	E6		---	A+	N	---	Access Successful
	f	Y	E6		---	A-	N	---	Access Not Suc-cessful
	g	N	E6		A+	A	N	Access Not Suc-cessful	Change to Access Limited
	h	N	E6		A-	A	N	Access Not Suc-cessful	Keep Access
	i	N	E6		A+	---	Y	Access Successful	---
	j	N			A	A-	Y	Keep Access	Access Not Suc-cessful
	k	Y			---	A-	Y	---	Access Not Suc-cessful
	l	N	E6		RA+	---	Y	Access Successful	---
	m	N	E6		---	RA-	Y	---	Access Not Suc-cessful

Demo ID		MSV	UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
					Real Req	Hostile Req			
	n	N	E6		---	A	Y	---	All Sessions Terminated
	o	N	E6		A	---	Y	All Sessions Terminated	---
Comment: **l, m, n, o**: Initial authentication successful and while authenticated credentials were reported stolen									
B-6.2	a	N	E6	On-Prem Branch → On-Prem	A+	---	N	Access Successful	---
	b	Y	E6		A-	---	N	Access Not Successful	---
	c	N	E6		A	A+	N	Change to Access Limited	Access Not Successful
	d	N	E6		A	A-	N	Keep Access	Access Not Successful
	e	N	E6		---	A+	N	---	Access Successful
	f	N	E6		---	A-	N	---	Access Not Successful
	g	N	E6		A+	A	N	Access Not Successful	Change to Access Limited
	h	N	E6		A-	A	N	Access Not Successful	Keep Access
	i	N	E7		A+	---	Y	Access Successful	---
	j	N	E7		A	A-	Y	Keep Access	Access Not Successful
	k	Y	E7		---	A-	Y	---	Access Not Successful
	l	N	E7		RA+	---	Y	Access Successful	---
	m	N	E7		---	RA-	Y	---	Access Not Successful
	n	N	E7		---	A	Y	---	Change to Access Limited

Demo ID		MSV	UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
					Real Req	Hostile Req			
	o	N	E7		A	---	Y	Change to Access Limited	---
Comment: **l, m, n, o**: Initial authentication successful and while authenticated credentials were reported stolen									
B-6.3	a	N	E6	Branch On-Prem → On-Prem	A+	---	N	Access Successful	---
	b	Y	E6		A-	---	N	Access Not Successful	---
	c	N	E6		A	A+	N	Change to Access Limited	Access Not Successful
	d	N	E6		A	A-	N	Keep Access	Access Not Successful
	e	N	E6		---	A+	N	---	Access Successful
	f	N	E6		---	A-	N	---	Access Not Successful
	g	N	E6		A+	A	N	Access Not Successful	Change to Access Limited
	h	Y	E6		A-	A	N	Access Not Successful	Keep Access
	i	N	E7		A+	---	Y	Access Successful	---
	j	N	E7		A	A-	Y	Keep Access	Access Not Successful
	k	N	E7		---	A-	Y	---	Access Not Successful
	l	N	E7		RA+	---	Y	Access Successful	---
	m	N	E7		---	RA-	Y	---	Access Not Successful
	n	N	E7		---	A	Y	---	Change to Access Limited
	o	N	E7		A	---	Y	Change to Access Limited	---

Demo ID		MSV	UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
					Real Req	Hostile Req			
Comment: **l, m, n, o**: Initial authentication successful and while authenticated credentials were reported stolen									
B-6.4	a	N	E6	Remote On-Prem → On-Prem	A+	---	N	Access Successful	---
	b	N	E6		A-	---	N	Access Not Successful	---
	c	N	E6		A	A+	N	Change to Access Limited	Access Not Successful
	d	N	E6		A	A-	N	Keep Access	Access Not Successful
	e	N	E6		---	A+	N	---	Access Successful
	f	Y	E6		---	A-	N	---	Access Not Successful
	g	N	E6		A+	A	N	Access Not Successful	Change to Access Limited
	h	Y	E6		A-	A	N	Access Not Successful	Keep Access
	i	N	E7		A+	---	Y	Access Successful	---
	j	N	E7		A	A-	Y	Keep Access	Access Not Successful
	k	Y	E7		---	A-	Y	---	Access Not Successful
	l	N	E7		RA+	---	Y	Access Successful	---
	m	N	E7		---	RA-	Y	---	Access Not Successful
	n	N	E7		---	A	Y	---	Change to Access Limited
	o	N	E7		A	---	Y	Change to Access Limited	---
Comment: **l, m, n, o**: Initial authentication successful and while authenticated credentials were reported stolen									
B-6.5	a	N	E6	On-Prem	A+	---	N	Access Successful	---

Demo ID		MSV	UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
					Real Req	Hostile Req			
	b	Y	E6	Remote → On-Prem	A-	---	N	Access Not Successful	---
	c	N	E6		A	A+	N	Change to Access Limited	Access Not Successful
	d	N	E6		A	A-	N	Keep Access	Access Not Successful
	e	N	E6		---	A+	N	---	Access Successful
	f	N	E6		---	A-	N	---	Access Not Successful
	g	N	E6		A+	A	N	Access Not Successful	Change to Access Limited
	h	N	E6		A-	A	N	Access Not Successful	Keep Access
	i	N	E7		A+	---	Y	Access Successful	---
	j	N	E7		A	A-	Y	Keep Access	Access Not Successful
	k	N	E7		---	A-	Y	---	Access Not Successful
	l	N	E7		RA+	---	Y	Access Successful	---
	m	N	E7		---	RA-	Y	---	Access Not Successful
	n	N	E7		---	A	Y	---	Change to Access Limited
	o	N	E7		A	---	Y	Change to Access Limited	---
Comment: **l, m, n, o**: Initial authentication successful and while authenticated credentials were reported stolen									

2.6 Use Case C: Collaboration: Federated-ID Access

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.

Pre-Condition: The requestor is identified and authenticated. Per configuration, the requestor is authorized with full access to the resource.

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 2-15 Scenario C-1 Demonstrations

Demo ID		MSV	Req EP Compl	Req Loc	RSS EP Compl	RSS Loc	Desired Outcome
C-1.1	a	Y	Y	On-Prem	Y	On-Prem	Access Successful
	b		N		Y		Access Not Successful
	c		Y		N		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-1.2	a	Y	Y	Branch	Y	On-Prem	Access Successful
	b		N		Y		Access Not Successful
C-1.3	A	N	Y	Remote	Y	On-Prem	Access Successful
	b		N		Y		Access Not Successful
C-1.4	a	Y	Y	On-Prem	Y	Cloud	Access Successful
	b		N		Y		Access Not Successful
	c		Y		N		Access Limited
	d		N		N		Access Not Successful

Demo ID		MSV	Req EP Compl	Req Loc	RSS EP Compl	RSS Loc	Desired Outcome
C-1.5	a	Y	Y	Branch	Y	Cloud	Access Successful
	b		N		Y		Access Not Successful
C-1.6	a	N	Y	Remote	Y	Cloud	Access Successful
	b		N		Y		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.

Pre-Condition: The requestor is identified and authenticated. Per configuration, the requestor is authorized with limited access to the resource.

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

Demo ID		MSV	Req EP Compl	Req Loc	RSS EP Compl	RSS Loc	Desired Outcome
C-2.1	a	Y	Y	On-Prem	Y	On-Prem	Access Limited
	b		N		Y		Access Not Successful
	c		Y		N		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	a	Y	Y	Branch	Y	On-Prem	Access Limited
	b		N		Y		Access Not Successful

Demo ID		MSV	Req EP Compl	Req Loc	RSS EP Compl	RSS Loc	Desired Outcome
C-2.3	a	N	Y	Remote	Y	On-Prem	Access Limited
	b		N		Y		Access Not Successful
C-2.4	a	Y	Y	On-Prem	Y	Cloud	Access Limited
	b		N		Y		Access Not Successful
	c		Y		N		Access Limited
	d		N		N		Access Not Successful
C-2.5	a	Y	Y	Branch	Y	Cloud	Access Limited
	b		N		Y		Access Not Successful
C-2.6	a	N	Y	Remote	Y	Cloud	Access Limited
	b		N		Y		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 limited internet access.

Pre-Condition: The requestor is identified and authenticated. Per configuration, the requestor is authorized with limited access to the Internet.

Demonstration: The requestor using a Federated-ID will attempt to access two resources located in the public Internet. The resources are not controlled by the enterprise. One resource is allowed, the 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 internet access using an enterprise-controlled resource.

606 **Table 2-17 Scenario C-3 Demonstrations**

Demo ID		MSV	Req EP Compl	Req Loc	RSS Access Policy	RSS Loc	Desired Outcome
C-3.1	a	Y	Y	On-Prem	Allowed RSS 1	Internet	Access Successful
	b		N		Allowed RSS 1		Access Not Successful
	c		Y		Blocked RSS 2		Access Not Successful
	d		N		Blocked RSS 2		Access Not Successful
C-3.2	a	Y	Y	Branch	Allowed RSS 1	Internet	Access Successful
	b		N		Allowed RSS 1		Access Not Successful
	c		Y		Blocked RSS 2		Access Not Successful
	d		N		Blocked RSS 2		Access Not Successful
C-3.3	a	N	Y	Remote	Allowed RSS 1	Internet	Access Successful
	b		N		Allowed RSS 1		Access Not Successful
	c		Y		Blocked RSS 2		Access Not Successful
	d		N		Blocked RSS 2		Access Not Successful

607 ### 2.6.4 Scenario C-4: No internet access using an enterprise endpoint

608 This scenario deals with a request using a successfully authenticated Federated-ID accessing a non-
609 enterprise-controlled resource in the public internet using an enterprise-owned endpoint device with
610 internet access disabled.

611 **Pre-Condition:** The requestor is identified and authenticated. Per configuration, the requestor is
612 authorized with no access to the Internet.

613 **Demonstration:** The requestor using a Federated-ID will attempt to access two resources both located
614 in the public Internet. The resources are not controlled by the enterprise. One resource is allowed, the
615 other one is blocked.

616 **Purpose and Outcome:** This demonstration focuses on the endpoint resource compliance with access of
617 non-enterprise-controlled resources on the internet by a requester with no internet access.

618 **Table 2-18 Scenario C-4 Demonstrations**

Demo ID		MSV	Req EP Compl	Req Loc	RSS Access Policy	RSS Loc	Desired Outcome
C-4.1	a	Y	Y	On-Prem	Allowed RSS 1	Internet	Access Not Successful
	b		N		Allowed RSS 1		Access Not Successful
	c		Y		Blocked RSS 2		Access Not Successful
	d		N		Blocked RSS 2		Access Not Successful
C-4.2	a	Y	Y	Branch	Allowed RSS 1	Internet	Access Not Successful
	b		N		Allowed RSS 1		Access Not Successful
	c		Y		Blocked RSS 2		Access Not Successful
	d		N		Blocked RSS 2		Access Not Successful
C-4.3	a	N	Y	Remote	Allowed RSS 1	Internet	Access Not Successful
	b		N		Allowed RSS 1		Access Not Successful
	c		Y		Blocked RSS 2		Access Not Successful
	d		N		Blocked RSS 2		Access Not Successful

619 ### 2.6.5 Scenario C-5: Internet access using BYOD

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

624 **Pre-Condition:** The requestor is identified and authenticated. Per configuration, the requestor is
625 authorized with limited access to the Internet. Both resources RSS1 and RSS2 are not managed by the
626 enterprise. For example, RSS1 could be a gambling site and RSS2 could be a search engine.

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

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

632 **Table 2-19 Scenario C-5 Demonstrations**

Demo ID		MSV	Req EP Compl	Req Loc	RSS Access Policy	RSS Loc	Desired Outcome
C-5.1	a	Y	Y	On-Prem	Allowed RSS 1	Internet	Access Successful
	b		N		Allowed RSS 1		Access Not Successful/Limited
	c		Y		Blocked RSS 2		Access Not Successful
	d		N		Blocked RSS 2		Access Not Successful
Comment: Compliance on the endpoint might not be completely determined.							
C-5.2	a	Y	Y	Branch	Allowed RSS 1	Internet	Access Successful
	b		N		Allowed RSS 1		Access Not Successful/Limited
	c		Y		Blocked RSS 2		Access Not Successful
	d		N		Blocked RSS 2		Access Not Successful
Comment: Compliance on the endpoint might not be completely determined.							
C-5.3	a	N	Y	Remote	Allowed RSS 1	Internet	Access Successful
	b		N		Allowed RSS 1		Access Not Successful/Limited
	c		Y		Blocked RSS 2		Access Not Successful
	d		N		Blocked RSS 2		Access Not Successful
Comment: Compliance on the endpoint might not be completely determined.							

633 ### 2.6.6 Scenario C-6: Access resources using BYOD

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

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

641 **Demonstration:** The requestor using a federated-ID will attempt to access an enterprise resource using
642 a privately owned device.

643 **Purpose and Outcome:** This demonstration focuses on the endpoint device (BYOD), lowering access
644 level rights, and endpoint compliance and location.

645 **Table 2-20 Scenario C-6 Demonstrations**

Demo ID		MSV	Req. EP Compl	Req. Loc	RSS EP Compl	RSS Loc	Desired Outcome
C-6.1	a	N	Y	On-Prem	Y	On-Prem	Access Limited
	b		N		Y		Access Not Successful
	c		Y		N		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.							
C-6.2	a	N	Y	Branch	Y	On-Prem	Access Limited
	b		N		Y		Access Not Successful
C-6.3	a	N	Y	Remote	Y	On-Prem	Access Limited
	b		N		Y		Access Not Successful
C-6.4	a	N	Y	On-Prem	Y	Cloud	Access Limited
	b		N		Y		Access Not Successful
	c		Y		N		Access Limited/Restricted
	d		N		N		Access Not Successful
C-6.5	a	N	Y	Branch	Y	Cloud	Access Limited
	b		N		Y		Access Not Successful
C-6.6	a	N	Y	Remote	Y	Cloud	Access Limited
	b		N		Y		Access Not Successful

646 ### 2.6.7 Scenario C-7: Stolen credential using an enterprise endpoint

647 This scenario deals with a request using a stolen credential employing an enterprise endpoint.

648 **Pre-Condition:** The requestor's credential is stolen and is used to attempt accessing an enterprise
649 resource using an enterprise endpoint.

650 **Demonstration:** The requestor, using a stolen federated-ID, will attempt to access an enterprise
651 resource using an enterprise endpoint.

652 **Purpose and Outcome:** This demonstration focuses on the requester's federated-ID as well as the
653 endpoint status (stolen vs. not stolen).

654 **Table 2-21 Scenario C-7 Demonstrations**

Demo ID		MSV	Req Credential	Req Loc	Req EP	RSS Loc	Desired Outcome
C-7.1	a	Y	Active	On-Prem	Active	On-Prem	Access Successful
	b		Active		Flagged Stolen		Access Not Successful
	c		Flagged Stolen		Active		Access Not Successful
	d		Flagged Stolen		Flagged Stolen		Access Not Successful
Comment: For "Flagged Stolen" credentials, MFA should fail							
C-7.2	a	Y	Active	Branch	Active	On-Prem	Access Successful
	b		Active		Flagged Stolen		Access Not Successful
	c		Flagged Stolen		Active		Access Not Successful
	d		Flagged Stolen		Flagged Stolen		Access Not Successful
Comment: For "Flagged Stolen" credentials, MFA should fail							
C-7.3	a	N	Active	Remote	Active	On-Prem	Access Successful
	b		Active		Flagged Stolen		Access Not Successful
	c		Flagged Stolen		Active		Access Not Successful
	d		Flagged Stolen		Flagged Stolen		Access Not Successful
Comment: For "Flagged Stolen" credentials, MFA should fail							
C-7.4	a	Y	Active	On-Prem	Active	Cloud	Access Successful
	b		Active		Flagged Stolen		Access Not Successful
	c		Flagged Stolen		Active		Access Not Successful
	d		Flagged Stolen		Flagged Stolen		Access Not Successful
Comment: For "Flagged Stolen" credentials, MFA should fail							
C-7.5	a	Y	Active	Branch	Active	Cloud	Access Successful
	b		Active		Flagged Stolen		Access Not Successful
	c		Flagged Stolen		Active		Access Not Successful
	d		Flagged Stolen		Flagged Stolen		Access Not Successful

Demo ID		MSV	Req Credential	Req Loc	Req EP	RSS Loc	Desired Outcome
Comment: For “Flagged Stolen” credentials, MFA should fail							
C-7.6	a	N	Active	Remote	Active	Cloud	Access Successful
	b		Active		Flagged Stolen		Access Not Successful
	c		Flagged Stolen		Active		Access Not Successful
	d		Flagged Stolen		Flagged Stolen		Access Not Successful
Comment: For “Flagged Stolen” credentials, MFA should 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).

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. not stolen).

Table 2-22 Scenario C-8 Demonstrations

Demo ID		MSV	Req Credential	Req Loc	Req EP Compliance	RSS Loc	Desired Outcome
C-8.1	a	Y	Active	On-Prem	Y	On-Prem	Access Successful
	b		Flagged Stolen		Y		Access Not Successful
Comment: For “Flagged Stolen” credentials, MFA should fail, BYOD outside compliance must not be granted access (see C-5/6)							
C-8.2	a	Y	Active	Branch	Y	On-Prem	Access Successful
	b		Flagged Stolen		Y		Access Not Successful
Comment: For “Flagged Stolen” credentials, MFA should fail, BYOD outside compliance must not be granted access (see C-5/6)							
C-8.3	a	N	Active	Remote	Y	On-Prem	Access Successful
	b		Flagged Stolen		Y		Access Not Successful
Comment: For “Flagged Stolen” credentials, MFA should fail, BYOD outside compliance must not be granted access (see C-5/6)							

Demo ID		MSV	Req Credential	Req Loc	Req EP Compliance	RSS Loc	Desired Outcome
C-8.4	a	Y	Active	On-Prem	Y	Cloud	Access Successful
	b		Flagged Stolen		Y		Access Not Successful
Comment: For "Flagged Stolen" credentials, MFA should fail, BYOD outside compliance must not be granted access (see C-5/6)							
C-8.5	a	Y	Active	Branch	Y	Cloud	Access Successful
	b		Flagged Stolen		Y		Access Not Successful
Comment: For "Flagged Stolen" credentials, MFA should fail, BYOD outside compliance must not be granted access (see C-5/6)							
C-8.6	a	N	Active	Remote	Y	Cloud	Access Successful
	b		Flagged Stolen		Y		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.

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.

683 **Table 2-23 Scenario D-1 Demonstrations**

Demo ID		MSV	UP	Location Req. > RSS	Auth Stat			Access	Compl		Desired Outcome
					User	EP	RSS		EP	RSS	
D-1.1	a	N	O1	On-Prem → On-Prem	A+	A	A	RSS1	Y	Y	Access Successful
	b	N	O1		A+	A	A	RSS2	Y	Y	Access Successful
	c	Y	O1		A-	A	---	---	Y	---	Access Not Successful
	d	N	E2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	N	E2		A+	A	A	RSS2	Y	Y	Access Successful
	f	Y	E2		A-	A	---	---	Y	---	Access Not Successful
	g	Y	E3		A-	A	---	---	Y	---	Access Not Successful
	h	N	O1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	N	O1		RA-	A	---	---	Y	---	Access Not Successful
	j	N	O1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	N	O1		RA+	A	A	RSS2	N	Y	Access Limited
	l	N	O1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	N	O1		A+	A	A	RSS2	N	Y	Access Limited
	n	N	O1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	N	O1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	N	E2		A+	A	A	RSS2	Y	N	Access Not Successful
D-1.2	a	N	O1	Branch → On-Prem	A+	A	A	RSS1	Y	Y	Access Successful
	b	N	O1		A+	A	A	RSS2	Y	Y	Access Successful
	c	Y	O1		A-	A	---	---	Y	---	Access Not Successful
	d	N	E2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	N	E2		A+	A	A	RSS2	Y	Y	Access Successful
	f	Y	E2		A-	A	---	---	Y	---	Access Not Successful
	g	Y	E3		A-	A	---	---	Y	---	Access Not Successful
	h	N	O1		RA+	A	A	RSS1	Y	Y	Access Successful

Demo ID		MSV	UP	Location Req. > RSS	Auth Stat			Access	Compl		Desired Outcome
					User	EP	RSS		EP	RSS	
	i	N	O1		RA-	A	---	---	Y	---	Access Not Successful
	j	N	O1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	N	O1		RA+	A	A	RSS2	N	Y	Access Limited
	l	N	O1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	N	O1		A+	A	A	RSS2	N	Y	Access Limited
	n	N	O1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	N	O1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	N	E2		A+	A	A	RSS2	Y	N	Access Not Successful
D-1.3	a	N	O1	Remote → On-Prem	A+	A	A	RSS1	Y	Y	Access Successful
	b	N	O1		A+	A	A	RSS2	Y	Y	Access Successful
	c	Y	O1		A-	A	---	---	Y	---	Access Not Successful
	d	N	E2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	N	E2		A+	A	A	RSS2	Y	Y	Access Successful
	f	N	E2		A-	A	---	---	Y	---	Access Not Successful
	g	N	E3		A-	A	---	---	Y	---	Access Not Successful
	h	N	O1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	N	O1		RA-	A	---	---	Y	---	Access Not Successful
	j	N	O1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	N	O1		RA+	A	A	RSS2	N	Y	Access Limited
	l	N	O1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	N	O1		A+	A	A	RSS2	N	Y	Access Limited
	n	N	O1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	N	O1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	N	E2		A+	A	A	RSS2	Y	N	Access Not Successful
D-1.4	a	N	O1		A+	A	A	RSS1	Y	Y	Access Successful

Demo ID		MSV	UP	Location Req. > RSS	Auth Stat			Access	Compl		Desired Outcome
					User	EP	RSS		EP	RSS	
	b	N	O1	On-Prem → Cloud	A+	A	A	RSS2	Y	Y	Access Successful
	c	Y	O1		A-	A	---	---	Y	---	Access Not Successful
	d	N	E2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	N	E2		A+	A	A	RSS2	Y	Y	Access Successful
	f	Y	E2		A-	A	---	---	Y	---	Access Not Successful
	g	Y	E3		A-	A	---	---	Y	---	Access Not Successful
	h	N	O1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	N	O1		RA-	A	---	---	Y	---	Access Not Successful
	j	N	O1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	N	O1		RA+	A	A	RSS2	N	Y	Access Limited
	l	N	O1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	N	O1		A+	A	A	RSS2	N	Y	Access Limited
	n	N	O1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	N	O1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	N	E2		A+	A	A	RSS2	Y	N	Access Not Successful
D-1.5	a	N	O1	Branch → Cloud	A+	A	A	RSS1	Y	Y	Access Successful
	b	N	O1		A+	A	A	RSS2	Y	Y	Access Successful
	c	Y	O1		A-	A	---	---	Y	---	Access Not Successful
	d	N	O2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	N	O2		A+	A	A	RSS2	Y	Y	Access Successful
	f	Y	O2		A-	A	---	---	Y	---	Access Not Successful
	g	Y	O3		A-	A	---	---	Y	---	Access Not Successful
	h	N	O1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	N	O1		RA-	A	---	---	Y	---	Access Not Successful
	j	N	O1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	N	O1		RA+	A	A	RSS2	N	Y	Access Limited

Demo ID		MSV	UP	Location Req. > RSS	Auth Stat			Access	Compl		Desired Outcome
					User	EP	RSS		EP	RSS	
	l	N	O1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	N	O1		A+	A	A	RSS2	N	Y	Access Limited
	n	N	O1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	N	O1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	N	O2		A+	A	A	RSS2	Y	N	Access Not Successful
D-1.6	a	N	O1	Remote → Cloud	A+	A	A	RSS1	Y	Y	Access Successful
	b	N	O1		A+	A	A	RSS2	Y	Y	Access Successful
	c	N	O1		A-	A	---	---	Y	---	Access Not Successful
	d	N	O2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	N	O2		A+	A	A	RSS2	Y	Y	Access Successful
	f	N	O2		A-	A	---	---	Y	---	Access Not Successful
	g	N	O3		A-	A	---	---	Y	---	Access Not Successful
	h	N	O1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	N	O1		RA-	A	---	---	Y	---	Access Not Successful
	j	N	O1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	N	O1		RA+	A	A	RSS2	N	Y	Access Limited
	l	N	O1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	N	O1		A+	A	A	RSS2	N	Y	Access Limited
	n	N	O1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	N	O1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	N	O2		A+	A	A	RSS2	Y	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.

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.

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

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		MSV	UP	Location Req. → RSS	Auth Stat		Access	Compl		Desired Outcome
					User	EP		EP	Out of Hours	
D-2.1	a	N	O4	On-Prem → Internet	A+	A	URL1	Y	N	Access Successful
	b	N	O4		A+	A	URL2	Y	N	Access Successful
	c	N	O4		A+	A	URL1	Y	Y	Access Successful
	d	N	O4		A+	A	URL1	Y	Y	Access Successful
	e	Y	O4		A-	A	---	Y	---	Access Not Successful
	f	N	O5		A+	A	URL1	Y	N	Access Not Successful
	g	N	O5		A+	A	URL2	Y	N	Access Successful
	h	N	O5		A+	A	URL1	Y	Y	Access Not Successful
	i	N	O5		A+	A	URL1	Y	Y	Access Not Successful
	j	Y	O5		A-	A	---	Y	---	Access Not Successful
	k	N	O4		RA+	A	URL1	Y	---	Access Successful
	l	N	O4		RA-	A	---	Y	---	Access Not Successful
	m	N	O4		A+	A	URL1	N	---	Access Not Successful
	n	N	O4		A+	A	URL2	N	---	Access Successful

Demo ID		MSV	UP	Location Req. → RSS	Auth Stat		Access	Compl		Desired Outcome
					User	EP		EP	Out of Hours	
	o	N	O5		A+	A	URL1	N	N	Access Not Successful
	p	N	O5		A+	A	URL2	N	N	Access Not Successful
D-2.2	a	N	O4	Branch → Internet	A+	A	URL1	Y	N	Access Successful
	b	N	O4		A+	A	URL2	Y	N	Access Successful
	c	N	O4		A+	A	URL1	Y	Y	Access Successful
	d	N	O4		A+	A	URL1	Y	Y	Access Successful
	e	Y	O4		A-	A	---	Y	---	Access Not Successful
	f	N	O5		A+	A	URL1	Y	N	Access Not Successful
	g	N	O5		A+	A	URL2	Y	N	Access Successful
	h	N	O5		A+	A	URL1	Y	Y	Access Not Successful
	i	N	O5		A+	A	URL1	Y	Y	Access Not Successful
	j	Y	O5		A-	A	---	Y	---	Access Not Successful
	k	N	O4		RA+	A	URL1	Y	---	Access Successful
	l	N	O4		RA-	A	---	Y	---	Access Not Successful
	m	N	O4		A+	A	URL1	N	---	Access Not Successful
	n	N	O4		A+	A	URL2	N	---	Access Successful
	o	N	O5		A+	A	URL1	N	N	Access Not Successful
	p	N	O5		A+	A	URL2	N	N	Access Not Successful
D-2.3	a	N	O4	Remote → Internet	A+	A	URL1	Y	N	Access Successful
	b	N	O4		A+	A	URL2	Y	N	Access Successful
	c	N	O4		A+	A	URL1	Y	Y	Access Successful
	d	N	O4		A+	A	URL1	Y	Y	Access Successful
	e	N	O4		A-	A	---	Y	---	Access Not Successful
	f	N	O5		A+	A	URL1	Y	N	Access Not Successful
	g	N	O5		A+	A	URL2	Y	N	Access Successful

Demo ID		MSV	UP	Location Req. → RSS	Auth Stat		Access	Compl		Desired Outcome
					User	EP		EP	Out of Hours	
	h	N	O5		A+	A	URL1	Y	Y	Access Not Successful
	i	N	O5		A+	A	URL1	Y	Y	Access Not Successful
	j	N	O5		A-	A	---	Y	---	Access Not Successful
	k	N	O4		RA+	A	URL1	Y	---	Access Successful
	l	N	O4		RA-	A	---	Y	---	Access Not Successful
	m	N	O4		A+	A	URL1	N	---	Access Not Successful
	n	N	O4		A+	A	URL2	N	---	Access Successful
	o	N	O5		A+	A	URL1	N	N	Access Not Successful
	p	N	O5		A+	A	URL2	N	N	Access Not Successful

2.7.3 Scenario D-3: Stolen credential using BYOD or 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 or BYOD device.

Pre-Condition: The requestor's credential is stolen and is used to attempt accessing enterprise resource RSS1 using an enterprise endpoint. The requesting endpoint and requested resource are both in compliance.

Demonstration: Two requests for the same enterprise resource from an enterprise endpoint are performed using the same user credentials. The "Real Request" is performed using the latest credentials, which are modified/replaced after 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.

710 **Table 2-25 Scenario D-3 Demonstrations**

Demo ID		MSV	UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
					Real Req	Hostile Req			
D-3.1	a	N	O6	On-Prem On-Prem → On-Prem	A+	---	N	Access Successful	---
	b	N	O6		A-	---	N	Access Not Successful	---
	c	N	O6		A	A+	N	Change to Access Limited	Access Not Successful
	d	N	O6		A	A-	N	Keep Access	Access Not Successful
	e	N	O6		---	A+	N	---	Access Successful
	f	N	O6		---	A-	N	---	Access Not Successful
	g	N	O6		A+	A	N	Access Not Successful	Change to Access Limited
	h	N	O6		A-	A	N	Access Not Successful	Keep Access
	i	N	O7		A+	---	Y	Access Successful	---
	j	N	O7		A	A-	Y	Keep Access	Access Not Successful
	k	N	O7		---	A-	Y	---	Access Not Successful
	l	N	O7		RA+	---	Y	Access Successful	---
	m	N	O7		---	RA-	Y	---	Access Not Successful
	n	N	O7		---	A	Y	---	All Sessions Terminated
	o	N	O7		A	---	Y	All Sessions Terminated	---
Comment: **l, m, n, o**: Initial authentication successful and while authenticated credentials were reported stolen									
D-3.2	a	N	O6	On-Prem	A+	---	N	Access Successful	---

Demo ID		MSV	UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
					Real Req	Hostile Req			
	b	N	O6	Branch → On-Prem	A-	---	N	Access Not Successful	---
	c	N	O6		A	A+	N	Change to Access Limited	Access Not Successful
	d	N	O6		A	A-	N	Keep Access	Access Not Successful
	e	N	O6		---	A+	N	---	Access Successful
	f	N	O6		---	A-	N	---	Access Not Successful
	g	N	O6		A+	A	N	Access Not Successful	Change to Access Limited
	h	N	O6		A-	A	N	Access Not Successful	Keep Access
	i	N	O7		A+	---	Y	Access Successful	---
	j	N	O7		A	A-	Y	Keep Access	Access Not Successful
	k	N	O7		---	A-	Y	---	Access Not Successful
	l	N	O7		RA+	---	Y	Access Successful	---
	m	N	O7		---	RA-	Y	---	Access Not Successful
	n	N	O7		---	A	Y	---	Change to Access Limited
	o	N	O7		A	---	Y	Change to Access Limited	---
Comment: **l, m, n, o**: Initial authentication successful and while authenticated credentials were reported stolen									
D-3.3	a	N	O6	Branch On-Prem →	A+	---	N	Access Successful	---
	b	N	O6		A-	---	N	Access Not Successful	---

Demo ID		MSV	UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
					Real Req	Hostile Req			
	c	N	O6	On-Prem	A	A+	N	Change to Access Limited	Access Not Successful
	d	N	O6		A	A-	N	Keep Access	Access Not Successful
	e	N	O6		---	A+	N	---	Access Successful
	f	N	O6		---	A-	N	---	Access Not Successful
	g	N	O6		A+	A	N	Access Not Successful	Change to Access Limited
	h	N	O6		A-	A	N	Access Not Successful	Keep Access
	i	N	O7		A+	---	Y	Access Successful	---
	j	N	O7		A	A-	Y	Keep Access	Access Not Successful
	k	N	O7		---	A-	Y	---	Access Not Successful
	l	N	O7		RA+	---	Y	Access Successful	---
	m	N	O7		---	RA-	Y	---	Access Not Successful
	n	N	O7		---	A	Y	---	Change to Access Limited
	o	N	O7		A	---	Y	Change to Access Limited	---
Comment: **l, m, n, o**: Initial authentication successful and while authenticated credentials were reported stolen									
D-3.4	a	N	O6	Remote On-Prem → On-Prem	A+	---	N	Access Successful	---
	b	N	O6		A-	---	N	Access Not Successful	---
	c	N	O6		A	A+	N	Change to Access Limited	Access Not Successful

Demo ID		MSV	UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
					Real Req	Hostile Req			
	d	N	O6		A	A-	N	Keep Access	Access Not Successful
	e	N	O6		---	A+	N	---	Access Successful
	f	N	O6		---	A-	N	---	Access Not Successful
	g	N	O6		A+	A	N	Access Not Successful	Change to Access Limited
	h	N	O6		A-	A	N	Access Not Successful	Keep Access
	i	N	O7		A+	---	Y	Access Successful	---
	j	N	O7		A	A-	Y	Keep Access	Access Not Successful
	k	N	O7		---	A-	Y	---	Access Not Successful
	l	N	O7		RA+	---	Y	Access Successful	---
	m	N	O7		---	RA-	Y	---	Access Not Successful
	n	N	O7		---	A	Y	---	Change to Access Limited
	o	N	O7		A	---	Y	Change to Access Limited	---
Comment: **l, m, n, o**: Initial authentication successful and while authenticated credentials were reported stolen									
D-3.5	a	N	O6	On-Prem Remote → On-Prem	A+	---	N	Access Successful	---
	b	N	O6		A-	---	N	Access Not Successful	---
	c	N	O6		A	A+	N	Change to Access Limited	Access Not Successful
	d	N	O6		A	A-	N	Keep Access	Access Not Successful
	e	N	O6		---	A+	N	---	Access Successful

Demo ID		MSV	UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
					Real Req	Hostile Req			
	f	N	O6		---	A-	N	---	Access Not Successful
	g	N	O6		A+	A	N	Access Not Successful	Change to Access Limited
	h	N	O6		A-	A	N	Access Not Successful	Keep Access
	i	N	O7		A+	---	Y	Access Successful	---
	j	N	O7		A	A-	Y	Keep Access	Access Not Successful
	k	N	O7		---	A-	Y	---	Access Not Successful
	l	N	O7		RA+	---	Y	Access Successful	---
	m	N	O7		---	RA-	Y	---	Access Not Successful
	n	N	O7		---	A	Y	---	Change to Access Limited
	o	N	O7		A	---	Y	Change to Access Limited	---
Comment: **l, m, n, o**: Initial authentication successful and while authenticated credentials were reported stolen									

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.

Table 2-26 Scenario D-4 Demonstrations

Demo ID		MSV	UP	Location Req. > RSS	Auth Stat			Access	Compl		Desired Outcome
					User	EP	RSS		EP	RSS	
D-4.1	a	N	O1	On-Prem → On-Prem	A+	A	A	RSS1	Y	Y	Access Successful
	b	N	O1		A+	A	A	RSS2	Y	Y	Access Successful
	c	Y	O1		A-	A	---	---	Y	---	Access Not Successful
	d	N	E2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	N	E2		A+	A	A	RSS2	Y	Y	Access Successful
	f	Y	E2		A-	A	---	---	Y	---	Access Not Successful
	g	Y	E3		A-	A	---	---	Y	---	Access Not Successful
	h	N	O1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	N	O1		RA-	A	---	---	Y	---	Access Not Successful
	j	N	O1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	N	O1		RA+	A	A	RSS2	N	Y	Access Limited
	l	N	O1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	N	O1		A+	A	A	RSS2	N	Y	Access Limited
	n	N	O1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	N	O1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	N	E2		A+	A	A	RSS2	Y	N	Access Not Successful
D-4.2	a	N	O1	Branch → On-Prem	A+	A	A	RSS1	Y	Y	Access Successful
	b	N	O1		A+	A	A	RSS2	Y	Y	Access Successful
	c	Y	O1		A-	A	---	---	Y	---	Access Not Successful
	d	N	O2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	N	O2		A+	A	A	RSS2	Y	Y	Access Successful

Demo ID		MSV	UP	Location Req. > RSS	Auth Stat			Access	Compl		Desired Outcome
					User	EP	RSS		EP	RSS	
	f	Y	O2		A-	A	---	---	Y	---	Access Not Successful
	g	Y	E3		A-	A	---	---	Y	---	Access Not Successful
	h	N	O1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	N	O1		RA-	A	---	---	Y	---	Access Not Successful
	j	N	O1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	N	O1		RA+	A	A	RSS2	N	Y	Access Limited
	l	N	O1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	N	O1		A+	A	A	RSS2	N	Y	Access Limited
	n	N	O1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	N	O1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	N	O2		A+	A	A	RSS2	Y	N	Access Not Successful
D-4.3	a	N	O1	Remote → On-Prem	A+	A	A	RSS1	Y	Y	Access Successful
	b	N	O1		A+	A	A	RSS2	Y	Y	Access Successful
	c	N	O1		A-	A	---	---	Y	---	Access Not Successful
	d	N	O2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	N	O2		A+	A	A	RSS2	Y	Y	Access Successful
	f	N	O2		A-	A	---	---	Y	---	Access Not Successful
	g	N	E3		A-	A	---	---	Y	---	Access Not Successful
	h	N	O1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	N	O1		RA-	A	---	---	Y	---	Access Not Successful
	j	N	O1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	N	O1		RA+	A	A	RSS2	N	Y	Access Limited
	l	N	O1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	N	O1		A+	A	A	RSS2	N	Y	Access Limited

Demo ID		MSV	UP	Location Req. > RSS	Auth Stat			Access	Compl		Desired Outcome
					User	EP	RSS		EP	RSS	
	n	N	O1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	N	O1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	N	O2		A+	A	A	RSS2	Y	N	Access Not Successful
D-4.4	a	N	O1	On-Prem → Cloud	A+	A	A	RSS1	Y	Y	Access Successful
	b	N	O1		A+	A	A	RSS2	Y	Y	Access Successful
	c	Y	O1		A-	A	---	---	Y	---	Access Not Successful
	d	N	O2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	N	O2		A+	A	A	RSS2	Y	Y	Access Successful
	f	Y	O2		A-	A	---	---	Y	---	Access Not Successful
	g	Y	O3		A-	A	---	---	Y	---	Access Not Successful
	h	N	O1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	N	O1		RA-	A	---	---	Y	---	Access Not Successful
	j	N	O1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	N	O1		RA+	A	A	RSS2	N	Y	Access Limited
	l	N	O1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	N	O1		A+	A	A	RSS2	N	Y	Access Limited
	n	N	O1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	N	O1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	N	O2		A+	A	A	RSS2	Y	N	Access Not Successful
D-4.5	a	N	O1	Branch → Cloud	A+	A	A	RSS1	Y	Y	Access Successful
	b	N	O1		A+	A	A	RSS2	Y	Y	Access Successful
	c	Y	O1		A-	A	---	---	Y	---	Access Not Successful
	d	N	O2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	N	O2		A+	A	A	RSS2	Y	Y	Access Successful
	f	Y	O2		A-	A	---	---	Y	---	Access Not Successful

Demo ID		MSV	UP	Location Req. > RSS	Auth Stat			Access	Compl		Desired Outcome
					User	EP	RSS		EP	RSS	
	g	Y	O2		A-	A	---	---	Y	---	Access Not Successful
	h	N	O1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	N	O1		RA-	A	---	---	Y	---	Access Not Successful
	j	N	O1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	N	O1		RA+	A	A	RSS2	N	Y	Access Limited
	l	N	O1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	N	O1		A+	A	A	RSS2	N	Y	Access Limited
	n	N	O1		A+	A	A	RSS1	Y	N	Access Not Successful
	o	N	O1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	N	O2		A+	A	A	RSS2	Y	N	Access Not Successful
D-4.6	a	N	O1	Remote → Cloud	A+	A	A	RSS1	Y	Y	Access Successful
	b	N	O1		A+	A	A	RSS2	Y	Y	Access Successful
	c	N	O1		A-	A	---	---	Y	---	Access Not Successful
	d	N	O2		A+	A	A	RSS1	Y	Y	Access Not Successful
	e	N	O2		A+	A	A	RSS2	Y	Y	Access Successful
	f	N	O2		A-	A	---	---	Y	---	Access Not Successful
	g	N	O3		A-	A	---	---	Y	---	Access Not Successful
	h	N	O1		RA+	A	A	RSS1	Y	Y	Access Successful
	i	N	O1		RA-	A	---	---	Y	---	Access Not Successful
	j	N	O1		RA+	A	A	RSS1	N	Y	Access Not Successful
	k	N	O1		RA+	A	A	RSS2	N	Y	Access Limited
	l	N	O1		A+	A	A	RSS1	N	Y	Access Not Successful
	m	N	O1		A+	A	A	RSS2	N	Y	Access Limited
	n	N	O1		A+	A	A	RSS1	Y	N	Access Not Successful

Demo ID		MSV	UP	Location Req. > RSS	Auth Stat			Access	Compl		Desired Outcome
					User	EP	RSS		EP	RSS	
	o	N	O1		A+	A	A	RSS2	Y	N	Access Not Successful
	p	N	O2		A+	A	A	RSS2	Y	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.

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

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

Table 2-27 Scenario D-5 Demonstrations

Demo ID		MSV	UP	Location Req. > RSS	Auth Stat		Access	Compl		Desired Outcome
					User	EP		EP	Out of Hours	
D-5.1	a	N	O4	On-Prem → Internet	A+	A	URL1	Y	N	Access Successful
	b	N	O4		A+	A	URL2	Y	N	Access Successful
	c	N	O4		A+	A	URL1	Y	Y	Access Successful
	d	N	O4		A+	A	URL1	Y	Y	Access Successful
	e	Y	O4		A-	A	---	Y	---	Access Not Successful
	f	N	O5		A+	A	URL1	Y	N	Access Not Successful
	g	N	O5		A+	A	URL2	Y	N	Access Successful
	h	N	O5		A+	A	URL1	Y	Y	Access Not Successful
	i	N	O5		A+	A	URL1	Y	Y	Access Not Successful

Demo ID		MSV	UP	Location Req. > RSS	Auth Stat		Access	Compl		Desired Outcome
					User	EP		EP	Out of Hours	
	j	Y	O5		A-	A	---	Y	---	Access Not Successful
	k	N	O4		RA+	A	URL1	Y	---	Access Successful
	l	N	O4		RA-	A	---	Y	---	Access Not Successful
	m	N	O4		A+	A	URL1	N	---	Access Not Successful
	n	N	O4		A+	A	URL2	N	---	Access Successful
	o	N	O5		A+	A	URL1	N	N	Access Not Successful
	p	N	O5		A+	A	URL2	N	N	Access Not Successful
D-5.2	a	N	O4	Branch → Internet	A+	A	URL1	Y	N	Access Successful
	b	N	O4		A+	A	URL2	Y	N	Access Successful
	c	N	O4		A+	A	URL1	Y	Y	Access Successful
	d	N	O4		A+	A	URL1	Y	Y	Access Successful
	e	Y	O4		A-	A	---	Y	---	Access Not Successful
	f	N	O5		A+	A	URL1	Y	N	Access Not Successful
	g	N	O5		A+	A	URL2	Y	N	Access Successful
	h	N	O5		A+	A	URL1	Y	Y	Access Not Successful
	i	N	O5		A+	A	URL1	Y	Y	Access Not Successful
	j	Y	O5		A-	A	---	Y	---	Access Not Successful
	k	N	O4		RA+	A	URL1	Y	---	Access Successful
	l	N	O4		RA-	A	---	Y	---	Access Not Successful
	m	N	O4		A+	A	URL1	N	---	Access Not Successful
	n	N	O4		A+	A	URL2	N	---	Access Successful
	o	N	O5		A+	A	URL1	N	N	Access Not Successful
	p	N	O5		A+	A	URL2	N	N	Access Not Successful

Demo ID		MSV	UP	Location Req. > RSS	Auth Stat		Access	Compl		Desired Outcome
					User	EP		EP	Out of Hours	
D-5.3	a	N	O4	Remote → Internet	A+	A	URL1	Y	N	Access Successful
	b	N	O4		A+	A	URL2	Y	N	Access Successful
	c	N	O4		A+	A	URL1	Y	Y	Access Successful
	d	N	O4		A+	A	URL1	Y	Y	Access Successful
	e	Y	O4		A-	A	---	Y	---	Access Not Successful
	f	N	O5		A+	A	URL1	Y	N	Access Not Successful
	g	N	O5		A+	A	URL2	Y	N	Access Successful
	h	N	O5		A+	A	URL1	Y	Y	Access Not Successful
	i	N	O5		A+	A	URL1	Y	Y	Access Not Successful
	j	Y	O5		A-	A	---	Y	---	Access Not Successful
	k	N	O4		RA+	A	URL1	Y	---	Access Successful
	l	N	O4		RA-	A	---	Y	---	Access Not Successful
	m	N	O4		A+	A	URL1	N	---	Access Not Successful
	n	N	O4		A+	A	URL2	N	---	Access Successful
	o	N	O5		A+	A	URL1	N	N	Access Not Successful
	p	N	O5		A+	A	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 an enterprise 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.

747 The “Real Req” always uses the latest credentials which are modified/replaced after reported stolen. Re-
748 Authentication always follows a previously successful authentication.

749 All authentication methods are compromised

750 Two requests for the same enterprise resource from at least one BYOD endpoint are performed using
751 the same user credentials. The “Real Request” is performed using the latest credentials, which are
752 modified/replaced after reported stolen, and that request can succeed. The “Hostile Request” is
753 performed using a stolen enterprise-ID. All authentication methods are compromised. Re-authentication
754 always follows a previously successful authentication.

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

757 **Table 2-28 Scenario D-6 Demonstrations**

Demo ID		MSV	UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
					Real Req	Hostile Req			
D-6.1	a	N	O6	On-Prem	A+	---	N	Access Successful	---
	b	Y	O6	On-Prem	A-	---	N	Access Not Successful	---
	c	N	O6	On-Prem	A	A+	N	Change to Access Limited	Access Not Successful
	d	N	O6	On-Prem	A	A-	N	Keep Access	Access Not Successful
	e	N	O6	On-Prem	---	A+	N	---	Access Successful
	f	Y	O6	On-Prem	---	A-	N	---	Access Not Successful
	g	N	O6	On-Prem	A+	A	N	Access Not Successful	Change to Access Limited
	h	N	O6	On-Prem	A-	A	N	Access Not Successful	Keep Access
	i	N	O7	On-Prem	A+	---	Y	Access Successful	---
	j	N	O7	On-Prem	A	A-	Y	Keep Access	Access Not Successful

Demo ID		MSV	UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
					Real Req	Hostile Req			
	k	Y	O7		---	A-	Y	---	Access Not Successful
	l	N	O7		RA+	---	Y	Access Successful	---
	m	N	O7		---	RA-	Y	---	Access Not Successful
	n	N	O7		---	A	Y	---	All Sessions Terminated
	o	N	O7		A	---	Y	All Sessions Terminated	---
Comment: **l, m, n, o**: Initial authentication successful and while authenticated credentials were reported stolen									
D-6.2	a	N	O6	On-Prem Branch → On-Prem	A+	---	N	Access Successful	---
	b	Y	O6		A-	---	N	Access Not Successful	---
	c	N	O6		A	A+	N	Change to Access Limited	Access Not Successful
	d	N	O6		A	A-	N	Keep Access	Access Not Successful
	e	N	O6		---	A+	N	---	Access Successful
	f	Y	O6		---	A-	N	---	Access Not Successful
	g	N	O6		A+	A	N	Access Not Successful	Change to Access Limited
	h	N	O6		A-	A	N	Access Not Successful	Keep Access
	i	N	O7		A+	---	Y	Access Successful	---
	j	N	O7		A	A-	Y	Keep Access	Access Not Successful
	k	Y	O7		---	A-	Y	---	Access Not Successful
	l	N	O7		RA+	---	Y	Access Successful	---

Demo ID		MSV	UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
					Real Req	Hostile Req			
	m	N	O7		---	RA-	Y	---	Access Not Successful
	n	N	O7		---	A	Y	---	Change to Access Limited
	o	N	O7		A	---	Y	Change to Access Limited	---
Comment: **l, m, n, o**: Initial authentication successful and while authenticated credentials were reported stolen									
D-6.3	a	N	O6	Branch On-Prem → On-Prem	A+	---	N	Access Successful	---
	b	Y	O6		A-	---	N	Access Not Successful	---
	c	N	O6		A	A+	N	Change to Access Limited	Access Not Successful
	d	N	O6		A	A-	N	Keep Access	Access Not Successful
	e	N	O6		---	A+	N	---	Access Successful
	f	Y	O6		---	A-	N	---	Access Not Successful
	g	N	O6		A+	A	N	Access Not Successful	Change to Access Limited
	h	N	O6		A-	A	N	Access Not Successful	Keep Access
	i	N	O7		A+	---	Y	Access Successful	---
	j	N	O7		A	A-	Y	Keep Access	Access Not Successful
	k	Y	O7		---	A-	Y	---	Access Not Successful
	l	N	O7		RA+	---	Y	Access Successful	---
	m	N	O7		---	RA-	Y	---	Access Not Successful

Demo ID		MSV	UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
					Real Req	Hostile Req			
	n	N	O7		---	A	Y	---	Change to Access Limited
	o	N	O7		A	---	Y	Change to Access Limited	---
Comment: **l, m, n, o**: Initial authentication successful and while authenticated credentials were reported stolen									
D-6.4	a	N	O6	Remote On-Prem → On-Prem	A+	---	N	Access Successful	---
	b	Y	O6		A-	---	N	Access Not Successful	---
	c	N	O6		A	A+	N	Change to Access Limited	Access Not Successful
	d	N	O6		A	A-	N	Keep Access	Access Not Successful
	e	N	O6		---	A+	N	---	Access Successful
	f	Y	O6		---	A-	N	---	Access Not Successful
	g	N	O6		A+	A	N	Access Not Successful	Change to Access Limited
	h	N	O6		A-	A	N	Access Not Successful	Keep Access
	i	N	O7		A+	---	Y	Access Successful	---
	j	N	O7		A	A-	Y	Keep Access	Access Not Successful
	k	N	O7		---	A-	Y	---	Access Not Successful
	l	N	O7		RA+	---	Y	Access Successful	---
	m	N	O7		---	RA-	Y	---	Access Not Successful
	n	N	O7		---	A	Y	---	Change to Access Limited

Demo ID		MSV	UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
					Real Req	Hostile Req			
	o	N	O7		A	---	Y	Change to Access Limited	---
Comment: **l, m, n, o**: Initial authentication successful and while authenticated credentials were reported stolen									
D-6.5	a	N	O6	On-Prem Remote → On-Prem	A+	---	N	Access Successful	---
	b	Y	O6		A-	---	N	Access Not Successful	---
	c	N	O6		A	A+	N	Change to Access Limited	Access Not Successful
	d	N	O6		A	A-	N	Keep Access	Access Not Successful
	e	N	O6		---	A+	N	---	Access Successful
	f	Y	O6		---	A-	N	---	Access Not Successful
	g	N	O6		A+	A	N	Access Not Successful	Change to Access Limited
	h	N	O6		A-	A	N	Access Not Successful	Keep Access
	i	N	O7		A+	---	Y	Access Successful	---
	j	N	O7		A	A-	Y	Keep Access	Access Not Successful
	k	N	O7		---	A-	Y	---	Access Not Successful
	l	N	O7		RA+	---	Y	Access Successful	---
	m	N	O7		---	RA-	Y	---	Access Not Successful
	n	N	O7		---	A	Y	---	Change to Access Limited
	o	N	O7		A	---	Y	Change to Access Limited	---

Demo ID	MSV	UP	Location Real Hostile > RSS	Auth Stat		Rep. Stolen	Desired Outcome for Real Request	Desired Outcome for Hostile Request
				Real Req	Hostile Req			
Comment: **l, m, n, o**: Initial authentication successful and while authenticated credentials were reported stolen								

2.8 Use Case E: Guest: No-ID Access

2.8.1 Scenario E-1: Guest requests public internet access

For No-ID access, the only deciding factor is the type of device used and any known compliance state of the device. Authentication/authorization is not a factor (No-ID). Enterprise resource compliance is likewise assumed, as resources would not be visible otherwise.

Pre-Condition: The requestor does not need to authenticate (i.e., guest access). Per configuration, the 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.

Demonstration: Systems can differentiate between device classifications and perform some action based on policy to restrict privileged devices (i.e., enterprise-managed, BYOD) based on endpoint compliance policy.

Purpose and Outcome: This demonstration focuses on device identification and compliance (when applicable).

Table 2-29 Scenario E-1 Demonstrations

Demo ID		MSV	Location of Subject.	Access	Desired Outcome
E-1.1	a	Y	On-Prem	Public resource	Access Successful
	b	Y		Public internet	Access Successful
E-1.2	a	Y	Branch	Public resource	Access Successful
	b	Y		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 using an enterprise-owned endpoint. The requestor's reauthentication will fail and reduces the confidence 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.

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 re-authentication during an active session.

Table 2-30 Scenario F-1 Demonstrations

Demo ID		MSV	Re-auth.	Req Loc	RSS Loc	Desired Outcome
F-1.1	a	N	Passes	On-Prem	On-Prem	Session stays active
	b		Fails			Session will be terminated
F-1.2	a	N	Passes	Branch	On-Prem	Session stays active
	b		Fails			Session will be terminated
F-1.3	a	N	Passes	Remote	On-Prem	Session stays active
	b		Fails			Session will be terminated
F-1.4	a	N	Passes	On-Prem	Cloud	Session stays active
	b		Fails			Session will be terminated
F-1.5	a	N	Passes	Branch	Cloud	Session stays active
	b		Fails			Session will be terminated
F-1.6	a	N	Passes	Remote	Cloud	Session stays active
	b		Fails			Session will be terminated

Demo ID	MSV	Re-auth.	Req Loc	RSS Loc	Desired Outcome

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 and reduces the confidence 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.

Demonstration: The reauthentication of the requestor's endpoint fails, and the session will be terminated.

Purpose and Outcome: This demonstration focuses on the requester's endpoint identification, which fails re-authentication during an active session.

Table 2-31 Scenario F-2 Demonstrations

Demo ID		MSV	Re-auth.	Req. Loc	RSS Loc	Desired Outcome
F-2.1	a	N	Passes	On-Prem	On-Prem	Session stays active
	b		Fails			Session will be terminated
F-2.2	a	N	Passes	Branch	On-Prem	Session stays active
	b		Fails			Session will be terminated
F-2.3	a	N	Passes	Remote	On-Prem	Session stays active
	b		Fails			Session will be terminated
F-2.4	a	N	Passes	On-Prem	Cloud	Session stays active
	b		Fails			Session will be terminated
F-2.5	a	N	Passes	Branch	Cloud	Session stays active
	b		Fails			Session will be terminated

Demo ID		MSV	Re-auth.	Req. Loc	RSS Loc	Desired Outcome
F-2.6	a	N	Passes	Remote	Cloud	Session stays active
	b		Fails			Session will be terminated

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

This scenario is based on a successful request with an established session to an enterprise resource. The reauthentication of the resource will fail and reduces the confidence 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.

Demonstration: The reauthentication of the resource fails, and the session will be terminated.

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		MSV	Re-auth	Req. Loc	RSS Loc	Desired Outcome
F-3.1	a	N	Passes	On-Prem	On-Prem	Session stays active
	b		Fails			Session will be terminated
F-3.2	a	N	Passes	Branch	On-Prem	Session stays active
	b		Fails			Session will be terminated
F-3.3	a	N	Passes	Remote	On-Prem	Session stays active
	b		Fails			Session will be terminated
F-3.4	a	N	Passes	On-Prem	Cloud	Session stays active
	b		Fails			Session will be terminated
F-3.5	a	N	Passes	Branch	Cloud	Session stays active
	b		Fails			Session will be terminated

Demo ID		MSV	Re-auth	Req. Loc	RSS Loc	Desired Outcome
F-3.6	a	N	Passes	Remote	Cloud	Session stays active
	b		Fails			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 and reduce the confidence level. This terminates the session.

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		MSV	Req EP Compl	Req Loc	RSS Loc	Desired Outcome
F-4.1	a	N	Y	On-Prem	On-Prem	Session stays active
	b		N			Session will be terminated
F-4.2	a	N	Y	Branch	On-Prem	Session stays active
	b		N			Session will be terminated
F-4.3	a	N	Y	Remote	On-Prem	Session stays active
	b		N			Session will be terminated
F-4.4	a	N	Y	On-Prem	Cloud	Session stays active
	b		N			Session will be terminated

Demo ID		MSV	Req EP Compl	Req Loc	RSS Loc	Desired Outcome
F-4.5	a	N	Y	Branch	Cloud	Session stays active
	b		N			Session will be terminated
F-4.6	a	N	Y	Remote	Cloud	Session stays active
	b		N			Session will be terminated

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 establishes 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.

Table 2-34 Scenario F-5 Demonstrations

Demo ID		MSV	Req EP Compl	Req Loc	RSS Loc	Desired Outcome
F-5.1	a	N	N	On-Prem	On-Prem	Access Not Successful
	b		Y			Access Successful
F-5.2	a	N	N	Branch	On-Prem	Access Not Successful
	b		Y			Access Successful
F-5.3	a	N	N	Remote	On-Prem	Access Not Successful

Demo ID		MSV	Req EP Compl	Req Loc	RSS Loc	Desired Outcome
	b		Y			Access Successful
F-5.4	a	N	N	On-Prem	Cloud	Access Not Successful
	b		Y			Access Successful
F-5.5	a	N	N	Branch	Cloud	Access Not Successful
	b		Y			Access Successful
F-5.6	a	N	N	Remote	Cloud	Access Not Successful
	b		Y			Access Successful

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). In all demonstrations that were conducted, the ZTA functionality included in the build performed as expected. All demonstrations that lend themselves to both manual and automated execution (as described in Section 2.3) were performed twice using both methodologies.

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.

849 **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. 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 application 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 information	Success: Okta logs have relevant information about the authentication between the user and resource.

Demo ID	Expected Outcome	Observed Outcome	Comments
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 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	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		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		Partial success: Mobile: User authentication failure is at the endpoint. Cannot validate compliance on RSS1. Partial demonstration completed with user not able to login to mobile device.

Demo ID	Expected Outcome	Observed Outcome	Comments
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		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-1.2.i, D-1.3.i, D-4.1.i, D-4.2.i, D-4.3.i	Access Not Successful	N/A	Success: Only way to do this is to not use Okta FastPass, which would make this case invalid. We 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,	N/A	N/A	Demonstration cannot be run. Unable to perform compliance checks on RSS.

Demo ID	Expected Outcome	Observed Outcome	Comments
D-1.3.n-p, D-4.1.n-p, D-4.2.n-p, D-4.3.n-p			
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.
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.

Demo ID	Expected Outcome	Observed Outcome	Comments
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

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

3.1.3 Enterprise 3 Build 1 (E3B1) Demonstration Results

Table 3-2 lists the demonstration results for all EIG crawl phase demonstrations run in Enterprise 3 Build 1 (E3B1). In all demonstrations that were conducted, the ZTA functionality included in the build performed as expected. All demonstrations that lend themselves to both manual and automated execution (as described in Section 2.3) were performed twice, using both methodologies.

Table 3-2 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 Outcome	Observed Outcome	Comments
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		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		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	User authentication failure prevents access. Demonstration successful.

Demo ID	Expected Outcome	Observed Outcome	Comments
B-1.1.g	Access Not Successful	Access Not Successful	User authentication failure prevents access. Demonstration successful.
B-1.1.h	Access Successful	Access Successful	GitLab session timeout is set to one minute for demonstration purposes. After session timed out, user was re-authenticated. Partial demonstration. Cannot validate RSS1 compliance.
B-1.1.i	Access Not Successful	N/A	Demonstration successful. 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.
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-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.
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
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.

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
E2B1	Enterprise 2 Build 1
E3B1	Enterprise 3 Build 1
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
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
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.